UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA

UNIDADE ACADÊMICA DE SISTEMAS E COMPUTAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

TIAGO LUCAS PEREIRA CLEMENTINO

UMA ABORDAGEM DESCENTRALIZADA, PÚBLICA, ANÔNIMA E TOLERANTE A TRANSAÇÕES NÃO VERIFICÁVEIS PARA O DILEMA DOS COMPRADORES E VENDEDORES

CAMPINA GRANDE – PB

2025

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Coordenação de Pós-Graduação em Ciência da Computação

Uma Abordagem Descentralizada, Pública, Anônima e Tolerante a Transações não Verificáveis para o Dilema dos Compradores e Vendedores

Tiago Lucas Pereira Clementino

Tese submetida à Coordenação do Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Campina Grande - Campus I como parte dos requisitos necessários para obtenção do grau de Doutor em Ciência da Computação.

Área de Concentração: Ciência da Computação
Linha de Pesquisa: Sistemas Descentralizados

José Antão Beltrão Moura
(Orientador)

Campina Grande, Paraíba, Brasil

C626a Clementino, Tiago Lucas Pereira.
Uma abordagem descentralizada, pública, anônima e tolerante a transações não verificáveis para o dilema dos compradores e vendedores / Tiago Lucas Pereira Clementino. – Campina Grande, 2025.
252 f. : il. color.

Tese (Doutorado em Ciência da Computação) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2025.
"Orientação: Prof. Dr. José Antão Beltrão Moura".
Referências.

1. Sistemas de Processamento Distribuídos. 2. Dilema dos Compradores e Vendedores. 3. Transações Não-verificáveis. 4. Economia. 5. Mercados Descentralizados. 6. Incentivo à Honestidade. 7. Simulação Baseada em Agentes. 8. Mediação de Transações. I. Moura, José Antão Beltrão. II. Título.

CDU 004.75(043.2)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
POS-GRADUACAO EM CIENCIA DA COMPUTACAO
Rua Aprígio Veloso, 882, Edifício Telmo Silva de Araújo, Bloco CG1, - Bairro Universitário, Campina Grande/PB, CEP 58429-900
Telefone: 2101-1122 - (83) 2101-1123 - (83) 2101-1124
Site: http://computacao.ufcg.edu.br - E-mail: secpg@computacao.ufcg.edu.br

FOLHA DE ASSINATURA PARA TESES E DISSERTAÇÕES

TIAGO LUCAS PEREIRA CLEMENTINO

UMA ABORDAGEM DESCENTRALIZADA, PÚBLICA, ANÔNIMA E TOLERANTE A TRANSAÇÕES NÃO VERIFICÁVEIS PARA O DILEMA DOS COMPRADORES E VENDEDORES

Tese apresentada ao Programa de Pós-Graduação em Ciência da Computação como pré-requisito para obtenção do título de Doutor em Ciência da Computação.

Aprovada em: 28/04/2025

Prof. Dr. JOSÉ ANTÃO BELTRÃO MOURA, Orientador, UFCG

Prof. Dr. DIMAS CASSIMIRO DO NASCIMENTO FILHO, Examinador Interno, UFAPE

Prof. Dr. CARLOS EDUARDO SANTOS PIRES, Examinador Interno, UFCG

Prof. Dr. FRANCISCO PETRÔNIO ALENCAR DE MEDEIROS, Examinador Externo, IFPB

Prof. Dr. KATYUSCO DE FARIAS SANTOS, Examinador Externo, IFPB

Documento assinado eletronicamente por **JOSE ANTAO BELTRAO MOURA**, **PROFESSOR 3 GRAU**, em 02/05/2025, às 16:08, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Francisco Petrônio Alencar de Medeiros**, **Usuário Externo**, em 05/05/2025, às 15:13, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Dimas Cassimiro do Nascimento Filho**, **Usuário Externo**, em 05/05/2025, às 20:47, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **Katyusco de Farias Santos**, **Usuário Externo**, em 05/05/2025, às 22:30, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

Documento assinado eletronicamente por **CARLOS EDUARDO SANTOS PIRES**, **PROFESSOR 3 GRAU**, em 06/05/2025, às 08:17, conforme horário oficial de Brasília, com fundamento no art. 8º, caput, da Portaria SEI nº 002, de 25 de outubro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.ufcg.edu.br/autenticidade, informando o código verificador **5426007** e o código CRC **7D30E759**.

Referência: Processo nº 23096.025437/2025-04 SEI nº 5426007

Resumo

Em 2008, o Bitcoin, a primeira moeda totalmente descentralizada do mundo, trouxe consigo um contexto tecnológico com amplo potencial de aplicação em praticamente todas as áreas. Anos depois, embora exploradas em diversas aplicações, essas tecnologias descentralizadas ainda representam uma parcela pouco expressiva do mercado online. Resultados preliminares da presente Tese apontam para a dificuldade em virtualizar eventos materiais do mundo real de forma descentralizada como um dos principais obstáculos para o paradigma da descentralização. Tal virtualização, nesta Tese foi restringida ao problema da Transação não Verificável, a exemplo de um pagamento em dinheiro, a prestação de um serviço artesanal ou praticamente tudo que é negociado em uma feira livre. Considere agora uma transação online como sendo um protocolo de troca de valores em que uma parte ativa (comprador) paga antecipadamente por bens ou serviços. Neste momento, existe o risco da parte passiva (vendedor) agir de forma desonesta e nunca entregar os bens ou serviços pagos. Tal risco recebe o nome de Dilema dos Compradores e dos Vendedores e é particularmente desafiador em ambientes envolvendo transações não verificáveis, como os mercados descentralizados. Isto pode ser explicado utilizando Teoria dos Jogos, onde jogadores racionais tendem a escolher a estratégia de equilíbrio, que neste caso consiste em evitar a transação para assim evitar prejuízos com a desonestidade da outra parte devido à natureza não colaborativa do jogo, acarretando resultados abaixo do ideal. A diferença entre o resultado ideal e o resultado obtido em um jogo não colaborativo é conhecida como o preço da anarquia. A ausência de um comportamento colaborativo resulta em problemas como o Dilema dos Compradores e Vendedores, mas também outros como o Problema do Bem Público, onde qualquer bem capaz de beneficiar toda a população por igual é negligenciado pelos jogadores que se empenham apenas em suas próprias conquistas, em certos casos até sabotando o bem público.

A desonestidade da parte passiva produz transações incompletas que causam perdas multibilionárias anualmente, mesmo considerando apenas o comércio eletrônico. Os mercados centralizados contornam esse problema com um mediador centralizado – por exemplo, gateways de pagamento como o Mercado Pago, utilizado pelo Mercado Livre. Contudo, todo processo centralizado está sujeito a vícios que favoreçam esta autoridade central e seus interesses. Porém, os usuários cada vez mais atentos, veem com desconfiança o processo de

pagamento e recebimento de produtos e serviços pela Internet mesmo mediados por serviços centralizados, seja por relatos de experiências negativas de outros usuários ou até mesmo por suas próprias. É, portanto, interessante implementar soluções que incentivem a honestidade nesses cenários. Para tanto, esta Tese realizou uma revisão de literatura em busca de soluções descentralizadas capazes de incentivar a honestidade em transações não verificáveis. Com base em critérios de descentralização, não autenticação e tolerância a transações não verificáveis, as soluções encontradas foram classificadas, analisadas e comparadas por meio de três experimentos distintos. O primeiro deles comparou tais soluções com base em dados de operações do mundo real extraídos da plataforma OpenBazzar. O segundo utilizou Simulação Baseada em Agentes para analisar tais soluções em tempo real. O terceiro e último, partindo dos resultados dos dois anteriores, propõe um novo modelo de transação denominado Hash Society, projetado para estimular a cooperação entre os agentes. Tal modelo também foi avaliado por Simulação Baseada em Agentes e comparado às demais soluções. Os três experimentos realizados trazem contribuições à área de mercados descentralizados online, com novos *insights* e soluções para o dilema dos compradores e vendedores.

Abstract

In 2008, Bitcoin, the world's first fully decentralized currency, brought with it a technological context with broad potential for application in practically all areas. Years later, although explored in several applications, these decentralized technologies still represent a small portion of the online market. Preliminary results of this Thesis point to the difficulty in virtualizing real-world material events in a decentralized way as one of the main obstacles to the decentralization paradigm. Such virtualization, in this Thesis, was restricted to the problem of Non-Verifiable Transactions, such as a cash payment, the provision of a craft service or practically everything that is negotiated in a street market. Now consider an online transaction as a value exchange protocol in which an active party (buyer) pays in advance for goods or services. At this point, there is a risk that the passive party (seller) will act dishonestly and never deliver the goods or services paid for. This risk is called the Buyer's and Seller's Dilemma and is particularly challenging in environments involving unverifiable transactions, such as decentralized markets. This can be explained using Game Theory, where rational players tend to choose the equilibrium strategy, which in this case consists of avoiding the transaction in order to avoid losses due to the dishonesty of the other party due to the non-collaborative nature of the game, leading to suboptimal results. The difference between the ideal result and the result obtained in a non-collaborative game is known as the price of anarchy. The lack of collaborative behavior results in problems such as the Buyer's and Seller's Dilemma, but also others such as the Public Good Problem, where any good capable of benefiting the entire population equally is neglected by players who only strive for their own achievements, in some cases even sabotaging the public good.

The dishonesty of the passive party produces incomplete transactions that cause multibillion-dollar losses annually, even considering only e-commerce. Centralized marketplaces circumvent this problem by using a centralized mediator, such as payment gateways such as Mercado Pago, used by Mercado Livre. However, every centralized process is subject to flaws that favor this central authority and its interests. However, increasingly attentive users are suspicious of the process of paying for and receiving products and services over the Internet, even when mediated by centralized services, whether due to reports of negative

experiences from other users or even their own. It is therefore interesting to implement solutions that encourage honesty in these scenarios. To this end, this thesis conducted a literature review in search of decentralized solutions capable of encouraging honesty in unverifiable transactions. Based on criteria of decentralization, non-authentication and tolerance to unverifiable transactions, the solutions found were classified, analyzed and compared through three distinct experiments. The first one compared such solutions based on real-world transaction data extracted from the OpenBazzar platform. The second used Agent-Based Simulation to analyze such solutions in real time. The third and final experiment, called Hash Society, proposes a new transaction model designed to stimulate cooperation between agents. This model was also evaluated by Agent-Based Simulation and compared to other solutions. The three experiments carried out bring contributions to the area of decentralized online markets, with new insights and solutions to the dilemma of buyers and sellers.

Agradecimentos

Sou grato por este trabalho ter recebido apoio financeiro da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, bem como do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq. Sou grato também a Coordenaço do Programa de Pós-Graduação em Computação, por estar sempre a disponível para dar suporte quando necessário. Agradeço em especial ao meu orientador, Dr. José Antão Beltrão Moura, pela confiança e dedicação dispensada a mim ao longo deste trabalho.

Conteúdo

Lista de Símbolos

TLRD - *Tecnologias de Livro Razão Distribuído*

DAPP - *Aplicações Descentralizadas*

DAO - *Organizações Descentralizadas*

DAS - *Sociedades Descentralizadas*

DAX - *Todos os demais modelos de entidades descentralizadas constituem o paradigma da descentralização*

DCV - *Dilema dos Compradores e Vendedores*

PoA - *Preço da Anarquia*

CI - *Contrato Inteligente*

DAnV - *Descentralizado, Anônimo e envolvendo transações não-Verificáveis*

σ - *Uma transação*

t - *Um passo no tempo* T.

MIH - *Modelo de Incentivo à Honestidade*

a, b, c, s - *Jogadores (Capítulo 5.3)*

A - *Conjunto de jogadores (Capítulo 5.3)*

T - *Transação (Capítulo 5.3)*

ϕ - *Confiança da rede em um dado jogador (Capítulo 5.3)*

$s_t(b, a)$ - *Saldo histórico de transações entre* b *e* a *até o momento* t *(Capítulo 5.3)*

P_t - *Saldo total de transações entre toda a população ativa até* t *(Capítulo 5.3)*

δ - *Limite de confiança aceitável para realizar uma transação (Capítulo 5.3)*

$\gamma_{a,b}(c)$ - *Função que define se* c *é confiável o suficiente para ser o árbitro da transação entre* a *e* b *(Capítulo 5.3)*

K - *Conjunto de agentes negociando*

q - *Um agente negociando*

S - *Conjunto de transações*

s - *Uma transação*

G - *Dilema do comprador e do vendedor como um jogo de forma extensiva*

P - *Conjunto de valores/produtos trocados*

p - *Um valor/produto*

T - *referências para todos os passos de tempo.*

i, j - *representações de agentes*

k, l, n, t - *representações de passos de tempo*

MGI - *representa o conjunto de MGIs disponíveis*

mgi - *representa uma MGI disponível*

r - *recurso da lista de recursos*

d - *demanda da lista de mandados*

b - *Uma operação (Capítulo 3) ou o estado de um determinado agente (Capítulos 5.4 e 6)*

γ - *A estratégia (operação)*

λ - *A função de interesse*

J - *Uma solução de incentivo de honestidade descentralizada*

ζ - *Uma função de inferência de comportamento (um sistema de reputação, por exemplo)*

η - *Algum modelo de transação garantidor como arbitragem descentralizada ou depósitos de garantia (Capítulos 5.3 e 5.4). Probabilidade de um dado agente se organizar em conluios (Capítulo 6)*

α - *Uma função de ação*

M - *O inventário do agente para cada uma das categorias de valor*

ν - *O objetivo de qualquer agente para cada categoria de valor*

L - *Os passos de vida em tempo de qualquer agente*

C - *Conjunto de classes de valor/produto*

c - *Uma classe de valor/produto*

HS - *Hash Society*

V - *A validação do ABM de acordo com [176] (Capítulo 5.4). O vetor de probabilidades de mudança de estados dois estados de uma cadeia (Capítulo 6).*

U - *A saída do ABM (Capítulo 5.4). Utilidade de uma transação (Capítulo 6).*

Z - *A saída real do sistema OpenBazaar*

R - $U \cap S$, *(Capítulo 5.4). Um recurso em uma lista de recursos, (Capítulo 6).*

m - *Uma métrica de escala de razão definida de acordo com a viabilidade e funcionalidade*

X - *O evento de um determinado agente confiar em outro*

h - *A probabilidade de um determinado produto já repassado por um determinado agente chegar ao estoque de outro*

χ - *A honestidade real de um determinado agente*

ψ - *Uma função aleatória*

MK^r - *Considere a trajetória de um recurso durável* r

n - *Iteração/estado em uma cadeia de markov.*

N - *Total de estados de uma cadeia de markov.*

E^r_{n+1} - *A variável aleatória que representa o estado do recurso* r *na interação* $n + 1$.

e^r - *Faz referência a algum estado de* r.

$\mu^s{}_{mgi}$ - *Uma avaliação de uma transação* s *por uma* mgi κ - *Função validação de um mgi.*

θ - *Limiar de reputação.*

ρ - *Taxa de adesão a ciclos de conluio.*

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Tecnologias descentralizadas, baseadas sobretudo (mas não exclusivamente) em *blockchains*, ganharam atenção e investimento recentemente [130]. *Blockchain* é um banco/rede de dados inalterável – *tamperless* – e distribuído, onde não há uma entidade administradora central. Sua imutabilidade é um recurso que se mostrou útil em áreas onde registros imutáveis são necessários [189, 104, 225]. Nessa rede descentralizada, os dados são agrupados e armazenados em blocos conectados em forma de cadeia – daí o termo *blockchain* – onde cada bloco armazena um conjunto de transações. Qualquer pessoa envolvida nestas transações pode ter acesso a uma cópia completa desse banco de dados. Por esta razão, *blockchains* fazem parte da categoria tecnológica denominada *Distributed Ledger Technologies* (DLT) ou Tecnologia de Livro Razão Distribuído, em português (doravante TLRD). Aplicações Descentralizadas (DAPP), Organizações Descentralizadas (DAO), Sociedades Descentralizadas (DAS) e todos os demais modelos de entidades descentralizadas constituem o paradigma da descentralização – DAX, doravante – cujo potencial de aplicação em diferentes áreas já foi mapeado na literatura [196].

Parte da pesquisa econômica inicial sobre *blockchains* consiste em artigos de revisão [142, 48, 203, 117, 45, 248] com foco em questões fiduciárias e/ou financeiras (por exemplo, Yermack [280] sobre Bitcoin; Yermack [279] sobre bancos centrais de moeda digital; Chiu e Wong [53] sobre dinheiro eletrônico e estabilidade do sistema; Andolfatto [16]; Berentsen e Schar [29]). Há também uma literatura técnica que enfatiza a segurança e a prevenção de gastos duplos [191, 40, 18, 213], também com aplicações da teoria dos jogos [85, 136]. As primeiras conceituações de contratos inteligentes e propriedade digital fo-

ram apresentadas por Szabo [244, 245]. Sobre política e regulamentação, veja Kiviat [139] ou Chapman et al [48], entre outros.

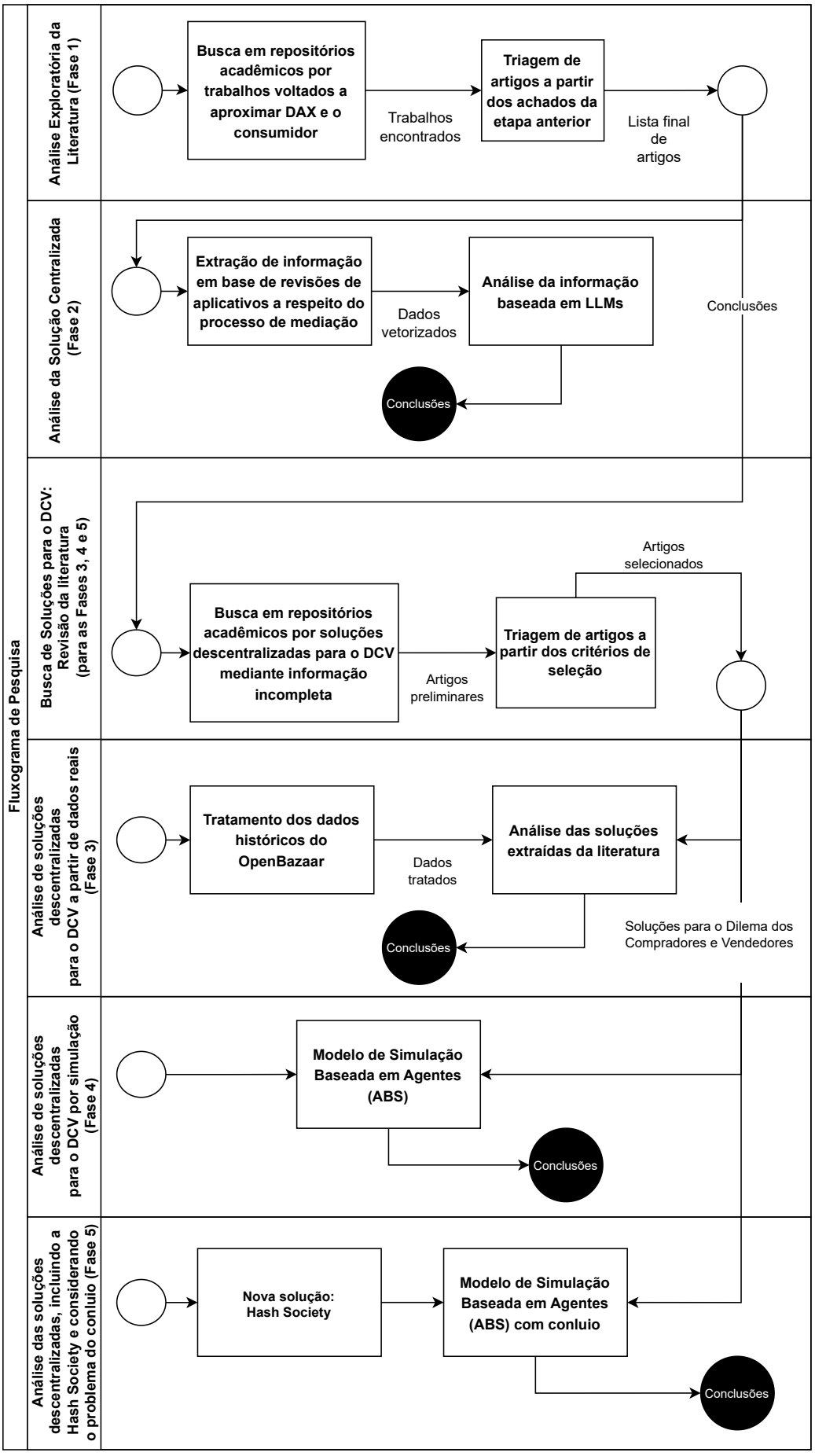
Esta Tese investiga TLRDs como plataformas digitais direcionadas ao consumidor, com foco na implementação de estruturas econômicas como pagamentos, crédito e seguros em mercados incompletos [1]. A abordagem se baseia em teorias econômicas que modelam o risco e a informação em jogos repetidos [241, 107]. Tais conceitos estão baseados em teorias econômicas que enfatizam o papel da dependência recorrente e o uso da expectativa de ganho como variável de risco em jogos temporais com informações privadas [241, 107, 2, 74, 22, 215, 95, 61, 8], ou com comprometimento limitado [251, 252, 214, 140, 141, 149, 13, 164, 163, 133, 37]. Também são utilizados elementos de design de mecanismos específicos de *blockchain*, como em Chiu e Wong [53] ou Chiu e Koeppl [52].

Esta Tese está mais relacionada ao trabalho recente que tenta conceituar as possíveis (futuras) aplicações de TLRDs na atividade econômica, com base em resultados do design de mecanismo, teoria dos jogos e da teoria dos contratos. Isto com foco em aproximar DAX à economia popular projetando modelos de implementação mais próximos do consumidor. As contribuições incluem, mas não se limitam, à revisão da definição de transação por Townsend [255] e novas abordagens ao problema do conluio Cong e He [64]. Esta Tese se baseia nesta literatura, mas se distancia ao explorar em detalhes as ferramentas algorítmicas e as restrições das TLRDs relacionadas a comprometimento, execução e disponibilidade de informação em transações. Tais questões foram exploradas inicialmente por uma análise exploratória da literatura que objetivou identificar trabalhos com o potencial de aproximar o paradigma DAX e o consumidor – Fase 1 desta Tese, conforme Figura 1.1. Tal revisão é baseada em um artigo científico escrito no contexto desta Tese e em fase final de revisão (*round* #2) para a revista ACM Distributed Ledger Tecnologies [2]. A análise da literatura indicou que a virtualização descentralizada de eventos do mundo real é um dos principais desafios das TLRDs, especialmente em transações que envolvem bens físicos ou serviços não digitalizáveis. Essa limitação orientou a investigação para o problema da mediação em transações online, onde pagamento e contrapartida precisam ser registrados de forma confiável em um

[1] Um mercado incompleto, ou um jogo incompleto é aquele onde um jogador não tem informações a respeito da estratégia dos demais

[2] `https://dl.acm.org/journal/dlt`

Figura 1.1: Fluxograma de Pesquisa



livro-razão distribuído.

A partir das conclusões da análise inicial exploratória da literatura optou-se por investigar a virtualização de eventos do mundo real restringindo o foco, voltando-se para o processo de mediação em transações online, onde pagamento e contrapartida das partes no mundo real devem ser virtualizados e inseridas no livro razão (TLRD). Este cenário mostra-se mais desafiador em aplicações descentralizadas, onde não se pode esperar verificação de transações e o anonimato não permite a punição da atitude desonesta por parte de uma autoridade central.

A mediação centralizada de transações é a solução mais aplicada para um problema descrito na literatura como o Dilema dos Compradores e Vendedores (DCV doravante) [20]. Trata-se do dilema do comprador ou vendedor ao decidir confiar na outra parte e pagar ou entregar seu produto antes da contrapartida, uma vez que na maioria dos casos é impossível sincronizar perfeitamente as operações de pagamento e entrega do bem. Tal dilema é descrito em mais detalhes no Capítulo 3.

Na Fase 2 desta Tese (observe Figura 1.1), analisou-se a solução centralizada mais utilizada para transações online, que consiste em delegar autoridade a uma entidade confiável. Os resultados detalhados no Capítulo 4[3], indicaram que essa abordagem é eficaz na resolução de disputas, mas apresenta vulnerabilidades devido à dependência de uma única entidade, permitindo ações maliciosas e comprometendo a descentralização do sistema.

Definindo a mediação descentralizada de transações como foco de estudos e o DCV como problema central a ser abordado nesta Tese, seguiu-se com uma revisão da literatura em busca de soluções decentralizadas para o DCV mediante informação incompleta ou assimétrica, ou seja, informação do mundo real difícil de virtualizar como um pagamento em dinheiro, um serviço manual, a venda de produtos naturais como frutas ou animais, etc (vide Seção 5.2, Capítulo 5).

A partir dos resultados da revisão da Seção 5.2, o Capítulo 5 segue com uma análise da eficácia das soluções presentes em tais resultados utilizando dados históricos da plataforma de comércio descentralizada OpenBazaar (vide Seção 5.3). Os resultados desta análise e da revisão da literatura foram publicados na 25º *International Conference on Computational*

[3]Tais resultados foram também publicados no 23º Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais, `https://ihc.sbc.org.br/2024/`, estrato Qualis A3

Science and Its Applications[4], e constituem a Fase 3 desta Tese, conforme Figura 1.1. Esta etapa constitui a primeira fase experimental e avaliou a eficácia das soluções descentralizadas presentes na literatura para o DCV envolvendo operações não validáveis em ambiente real, além de recombinações de elementos de tais soluções resultando em soluções novas, e estas obtiveram resultados superiores.

Dando sequência com os experimentos do Capítulo 5, a mesma análise da Seção 5.3 foi reproduzida utilizando Simulação Baseada em Agentes (*Agent-based Simulation*, ABS doravante) a fim de tirar conclusões a respeito da classe de transações sob análise, desta vez tempo real, ainda que por simulação. Tais análises alcançaram resultados convergentes (vide Seção 5.4), constituindo a Fase 4 desta Tese (vide Figura 1.1).

A meta análise da literatura (Fase 1) e os experimentos que analisaram o Dilema dos Compradores e Vendedores em suas soluções centralizadas ou descentralizadas (Fases 2, 3 e 4) apresentaram resultados que dialogam entre si. Os resultados da análise da literatura informam sobre o estado da arte e trazem direções para novos estudos, apontando para a dificuldade em virtualizar eventos materiais do mundo real sem violar o princípio da descentralização como um dos grandes obstáculos à popularização e aplicação das TLRDs ao consumidor. Já os experimentos apontam para ações de usuário e a gestão da honestidade e confiança entre os agentes como um importante ponto de risco em sistemas de comércio eletrônico como um todo, sobretudo em sistemas descentralizados baseados em virtualização de informações do mundo real. O fluxograma detalhado do caminho percorrido para se alcançar os resultados apresentados aqui é mostrado na Figura 1.1

Com base nos achados das fases anteriores, propõe-se um novo modelo de interação entre agentes, fundamentado em transações compostas por uma única operação. Nesse modelo, a reputação dos agentes é ajustada dinamicamente por um sistema descentralizado de modelos inteligentes, que aprende e otimiza as interações entre estes agentes por meio de consenso. Este sistema faz parte de um protocolo descentralizado denominado Hash Society e é apresentado em mais detalhes no Capítulo 6 – Fase 5 desta Tese. A avaliação deste protocolo indica que essa abordagem reduz os riscos observados nas soluções anteriores, embora represente um modelo de jogo diferente dos mercados atuais.

[4]Estrato Qualis A2

1.1 Problema

A dificuldade de virtualizar eventos e fatos do mundo real leva as TLRDs a recorrerem a autoridades centralizadas por meio de oráculos [36] ou entidades confiáveis. Uma solução que espelhe eventos e fatos do mundo real de forma descentralizada é um dos problemas mais críticos quando se trata de trazer soluções descentralizadas para a vida cotidiana das pessoas [181, 184, 75, 201, 183]. Zavolokina et al [282] ilustrou esse problema usando como exemplo a venda de um carro usado. Existem muitos dados para descrever a situação mecânica do carro, mas virtualizá-los de forma descentralizada é um grande desafio, pois o dono do carro pode querer esconder qualquer informação ruim do comprador. O comprador precisa invariavelmente correr o risco de ser enganado pelo dono do carro para que a transação aconteça. Tal risco pode ser generalizado na forma do Dilema dos Compradores e Vendedores [20] – descrito em mais detalhes no Capítulo 3 – mediante transações não-verificáveis, conceito descrito in Seção 3.1.1. Este contexto é descrito ilustradamente na Figura-1.2 [5] na forma de uma linha temporal onde as operações 4, 5 e 8 dependem necessariamente da verificação de autoridades centralizados confiáveis. Substituir tal confiança centralizada de forma descentralizada é a dificuldade descrita no início deste parágrafo. Esta Tese concentra-se em promover o comercio eletrônico descentralizado mediante um risco aceitável sem a necessidade de verificar todas as operações em uma transação.

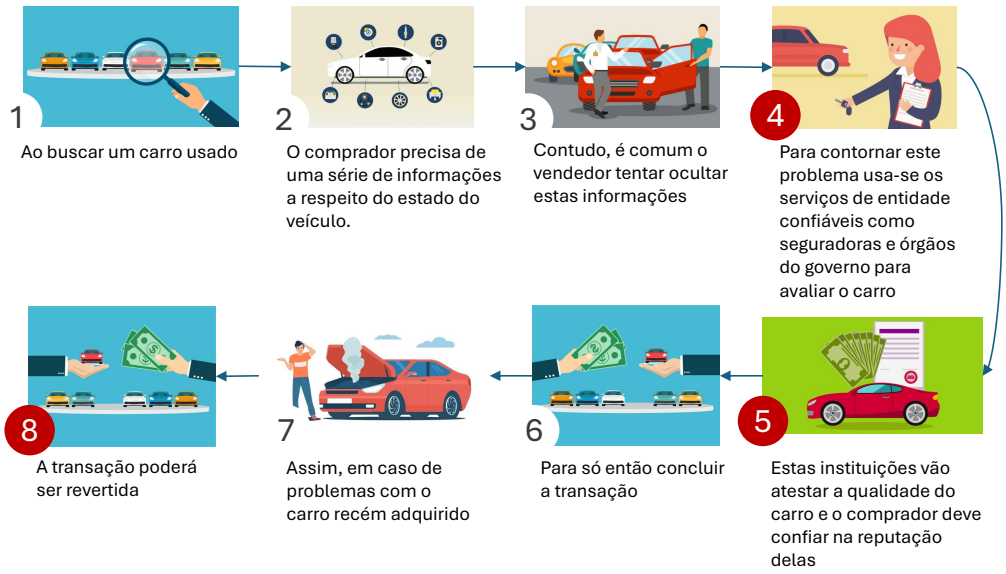
1.1.1 Teoria dos Jogos e DCV

Tomando uma transação comercial bilateral como um protocolo composto por uma série de operações que estabelecem uma troca de valores de naturezas diferentes entre duas partes, um provocador ativo que propõe a transação e um respondente passivo. Nessa configuração, a parte ativa assume o risco executando a transferência de valor antes de receber uma contrapartida em resposta, deixando espaço para potencial desonestidade da parte passiva. Esse risco é particularmente pronunciado em ambientes com transações não verificáveis, como mercados descentralizados.

A Teoria dos Jogos é o campo que estuda o raciocínio aplicado por agentes racionais

[5] As imagens utilizadas neste infográfico foram geradas separadamente utilizando o ChatGPT (`https://chatgpt.com/`).

Figura 1.2: Linha temporal que utiliza o exemplo da venda de um carro usado para pontuar operações que necessitam de verificação centralizada. Tais operações estão numeradas em vermelho.



para decidir qual estratégia maximiza sua própria utilidade para cada transação, seja risco ou desonestidade. Quando todos os jogadores tendem a escolher a mesma estratégia, chamamos a interação resultante de equilíbrio. Infelizmente, considerando os jogadores como não colaborativos, o equilíbrio muitas vezes não garante o melhor resultado para eles, o DCV é um exemplo disso. Na teoria dos jogos, este resultado ruim é descrito como o preço da anarquia (PoA), que representa a distância entre o ideal colaborativo e o melhor equilíbrio possível. Feldman et al [91] apresenta um trabalho extenso no qual propõem uma estrutura generalista visando atenuar tais efeitos. A partir de agora, para melhor compreensão, sempre usaremos o termo "agente" ao nos referirmos aos jogadores ou partes.

Para o DCV, há um equilíbrio tendendo à estratégia de não tomar nenhuma ação, seja o ato desonesto de se apoderar do pagamento, por parte dos vendedores, ou à não execução da transação por parte dos compradores. Uma solução conhecida para superar esse equilíbrio indesejável é a mediação de um terceiro agente que valida as operações e deve contar com a confiança de ambos os agentes. Embora eficaz em mercados centralizados onde o Estado, ou uma casa de câmbio ou mesmo uma instituição bancária desempenham o papel de inter-

mediário garantindo a contraparte passiva, essa abordagem não é apropriada em abordagens descentralizadas (ex.: transações usando criptomoedas ou mercados locais envolvendo trocas de dinheiro físico). As tecnologias de contabilidade distribuída (TLRDs) por si só já resolvem este problema em ambientes descentralizados onde todas as transações podem ser verificadas [30].

1.1.2 Relevância

Mapeamentos anteriores já mostraram que o potencial disruptivo das TLRDs gera muita expectativa na comunidade e na indústria [225]. Contudo, transações descentralizadas que envolvem operações não verificáveis criam a necessidade de monitoramento complexo [199] e virtualização deste monitoramento, o que, quando possível, depende de estratégias de IoT, *Edge Computing* ou Contratos Inteligentes baseados em Oráculos. Todas estas alternativas geram custos nem sempre viáveis a depender do modelo de negócio. Karajvanov [130] afirma que a dificuldade em fornecer garantias baseadas em informação assimétrica (como transações não verificáveis) é um dos principais gargalos em TLRD. Esta assimetria diz respeito à execução de direitos e obrigações de ambas as partes de forma independente e sem sincronização, o que é muito diferente do processamento convencional em um Contrato Inteligente (doravante, CI), onde todas as etapas são consentidas por ambas as partes de modo atômico.

Assim, um CI não pode estabelecer obrigações e direitos sobre transações que ocorram no mundo real ou sobre eventos futuros. Isso exclui a maioria dos possíveis usos práticos de CI em transações voltadas ao consumidor. A literatura e a indústria carecem de modelos de governança descentralizados capazes de espelhar e validar as regras que regem a sociedade e seus contratos comumente celebrados (vide Capítulo 2). A validação e registro dos fatos regidos por tais regras tem o potencial de contribuir viabilizando a popularização do paradigma da descentralização e a utilização de CIs como uma contraparte virtual para acordos legais generalistas.

1.1.3 Exploração do Problema

O fluxograma da Figura 1.1 ilustra o processo utilizado para abordar a questão de pesquisa inicial: *Tendo em vista o potencial disruptivo atribuído à DAX, por que este permanece distante da maioria das aplicações voltadas ao consumidor?*. Conforme é possível observar na figura, a primeira etapa consistiu de uma Revisão da Literatura. Diante de suas conclusões, restringiu-se o foco da pesquisa a transações envolvendo operações não-verificáveis – conceito sintetizado a partir da ideia mais ampla de eventos não virtualizáveis – onde analisou-se em um primeiro momento a eficácia da solução centralizada sob a ótica do usuário a fim mapear suas experiências em situações adversas (vide Capítulo 4). Em seguida analisou-se opções de soluções descentralizadas extraídas da literatura, a princípio utilizando dados históricos reais da plataforma OpenBazaar, e em seguida repetiu-se a mesma análise, só que em tempo real por meio de simulação. A repetição da mesma análise com base em dados de naturezas distintas serviu como estratégia de validação, dada a ausência de uma análise baseada em dados reais e em tempo real. Por fim é apresento um novo modelo de transação baseado em uma única operação (conforme descrito no Capítulo 6) e que superou todas as demais soluções da literatura em ambiente simulado. As conclusões para cada uma das etapas são listadas a seguir.

- A análise da literatura que mapeou os caminhos da pesquisa em aplicações descentralizadas voltadas ao consumidor apontou para a integração contínua das TLRDs com IoT como significativamente transformadora para diversos setores, introduzindo novos modelos de negócios e desafiando as práticas estabelecidas. No entanto, conforme apontado por Christidis e Devetsikiotis [56], essa integração exige esforços específicos para cada aplicação e envolve custos consideráveis, o que pode ser inviável em algumas circunstâncias. Além disso, ainda falta uma solução eficiente para conectar dados internos (*on-chain*) com dados externos (*off-chain*) de forma simplificada e que não exija adaptações específicas para cada domínio de aplicação, o que representa um obstáculo à adoção em larga escala da descentralização por parte dos consumidores – vide Capítulo 2;

- A análise da eficácia da mediação centralizada para o problema dos compradores e vendedores, principal solução centralizada, sob a ótica do usuário identificou que, em-

bora suficientemente eficaz, tal solução ainda apresenta falhas que podem ser sanadas pelas soluções descentralizadas avaliadas;

- A revisão da literatura que elencou as principais soluções descentralizadas para o DCV mediante operações não-verificáveis identificou como as mais eficazes e recorrentes, dentre as soluções de fato descentralizadas, a mediação descentralizada, a rede de confiança (Web-of-Trust) e o depósito em garantia – vide Seção 5.2;

- A análise das soluções descentralizadas para o DCV com base em dados históricos extraídos da plataforma OpenBazaar aponta para a mediação descentralizada associada a algum modelo de reputação como a solução mais eficaz dentre as apresentadas.

- A análise por meio de simulação das mesmas soluções descentralizadas elencadas para o DCV chegou a resultados convergentes com relação a análise do item anterior baseada em dados históricos. Mais especificamente, a simulação também aponta uma eficácia superior da solução baseada em mediação descentralizada e reputação, considerando uma faixa de honestidade restrita;

- Por fim, experimentos com a nova solução apresentada aqui, denominada *Hash Society*, baseada no conceito de transações de uma única operação, indicam desempenho superior em todos os cenários.

1.1.4 Hipótese de Pesquisa

As relações comerciais do mundo real tendem a fornecer regras para transações físicas validadas por testemunhas ou entidades confiáveis, ou mesmo transações que ainda estão por vir. Contudo, para TLRDs convencionais é impossível, por exemplo, estabelecer uma cláusula contratual punitiva para o descumprimento de determinada exigência, a menos que a punição seja pecuniária por meio de valor previamente retido, ou mesmo condicionar uma transferência a execução de um serviço físico sem o auxílio de uma entidade mediadora. A razão por trás disso é o conceito de *trustless* ou ausência de confiança entre os envolvidos, um dos pilares das tecnologias descentralizadas atuais. As TLRDs só podem lidar com eventos do mundo real caso alguém ou algum dispositivo virtualize a informação [263, 130].

Diante disto, é necessário buscar soluções para virtualizar a confiança, provendo garantias a ambas as partes de modo que a transação possa ocorrer a um risco aceitável. Assim, propomos como Tese a seguinte afirmação:

"*É possível reduzir o risco a um nível aceitável em transações descentralizadas sem a necessidade de verificar todas as operações*".

1.2 Abordagem Proposta

Para solucionar tal problema são analisadas soluções elencadas na literatura, novas soluções baseadas em rearranjos das principais características de soluções da literatura e uma solução inteiramente nova baseada em transações de operação única.

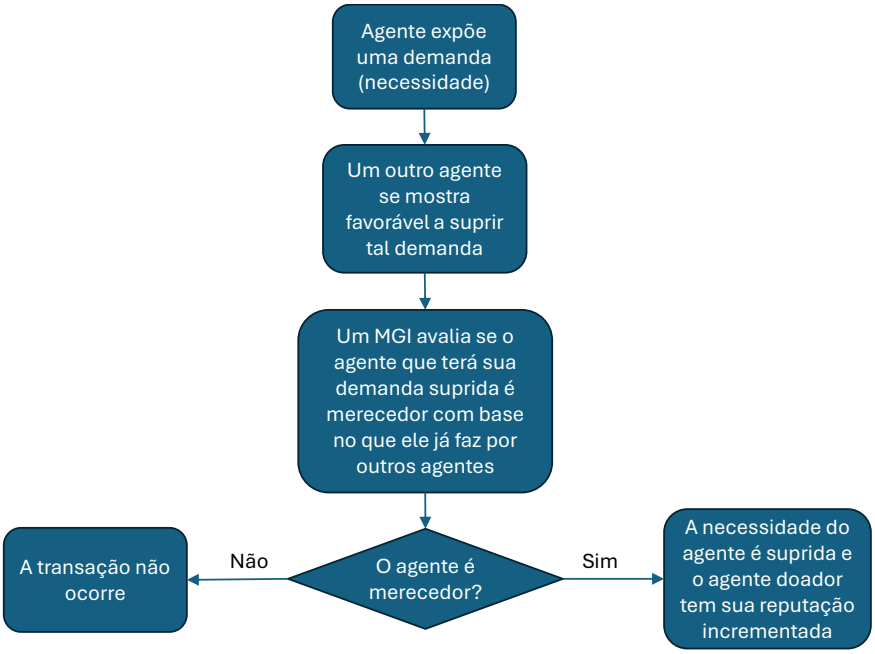
Em transações de única operação não existem comprador e vendedor, mas cada agente expõe suas demandas e espera que outro agente as supra, o que é feito apenas se um Modelo Gestor Inteligente (MGI) julgar o agente beneficiado merecedor de ter suas demandas supridas. Quando um agente supre as demandas de outro, este melhora sua reputação junto ao MGI, que por sua vez vai decidir se suas demandas devem ou não ser supridas. Esta sequência de operações é ilustrada no fluxograma da Figura 1.3.

Um modelo de gerenciamento (MGI) avalia os níveis de colaboração de cada agente em relação ao sucesso da população como um todo e recomenda transações de acordo, promovendo a cooperação e mitigando o DCV em ambientes Descentralizados, Anônimos e envolvendo transações não-Verificáveis (DAnV, doravante).

1.2.1 Contribuições

A partir do que foi definido, é possível observar duas contribuições mais claras, uma direta e outra indireta. A contribuição direta está em promover a segurança e confiabilidade em transações comerciais de forma ampla, sobretudo em ambientes descentralizados. Indiretamente, o presente esforço contribui com a disseminação do paradigma da descentralização, o que barateia custos por transação cortando intermediários e empodera o usuário ao permiti-lo opinar a respeito de decisões que são unilaterais no modelo centralizado.

Figura 1.3: Transação de uma única operação.



1.3 Estrutura do Documento

A presente Tese está estruturada em nove capítulos. Este primeiro deles trouxe uma introdução geral do conteúdo. No Capítulo 2 é apresentada a revisão da literatura que identificou o DCV em ambiente DAnV como um problema crítico, e assim, estabeleceu o foco desta pesquisa. No Capítulo 3 estabelecemos o conceito por trás do Dilema dos Compradores e Vendedores (DCV), e suas repercussões. Além de descrever outros conceitos-chave neste estudo como Transações não Verificáveis, Preço da Anarquia e o problema do Bem Público. Segue-se para o Capítulo 4 – Análise da Mediação como Solução Centralizada para o DCV – é apresentada uma análise a partir da opinião do usuário a respeito da principal solução centralizada para o DCV: o serviço de mediação centralizada em aplicativos do tipo *marketplace* (Amazon, eBay, Alibaba, etc). No Capítulo 5, onde em um primeiro momento é apresentada uma revisão da literatura trazendo as principais soluções descentralizadas para o DCV mediante Transações não-Verificáveis. Em seguida os dados resultantes desta revisão são utilizados em dois estudos: uma análise comparativa baseada em dados históricos da plataforma OpenBazaar (um exemplo de *marketplace* em ambiente DAnV) das principais

soluções descentralizadas na literatura para o DCV mediante transações não verificáveis; e, uma análise similar à anterior, desta vez utilizando dados em tempo real em um ambiente simulado. O Capítulo 6 apresenta uma solução proposta nesta Tese baseada no conceito de transações de operação única. Por fim, o Capítulo 7 apresenta conclusões gerais para o presente esforço de Tese.

1.4 Sumário do Capítulo

- Introdução de conceitos importantes para esta Tese como o Dilema dos Compradores e Vendedores (DCV), o Preço da Anarquia (PoA), Transações não Verificáveis, Transações de Operação Única, e o Modelo de Gestão Inteligente.
- Enumeração das fases da pesquisa referente a esta Tese:
  - Fase 1: Mapeamento exploratório da literatura em busca de trabalhos capazes de aproximar as TLRDs ao consumidor ou elucidar futuros caminhos que nos levem a tal.
  - Fase 2: Análise da solução centralizada para o DCV mediante transações não verificáveis: a mediação centralizada.
  - Fase 3: Análise, a partir de dados históricos de plataformas reais, das soluções descentralizadas para o DCV em ambientes sem autenticação e mediante transações não Verificáveis.
  - Fase 4: Mesma análise realizada na Fase 3, porém em ambiente simulado e, portanto, utilizando desta vez dados obtidos em tempo real e com pleno controle das variáveis.
  - Fase 5: Proposição de uma solução inédita para o DCV em ambiente sem autenticação e mediante transações não verificáveis.
- Enumeração das Contribuições:
  - Estabelecer estratégias a serem trilhadas a fim de aproximar o consumidor ao DAX.

- Estabelecer as limitações das soluções disponíveis atualmente para o DCV em ambiente DAnV.
- Prover segurança e confiabilidade em transações de forma generalista, sobretudo em ambientes descentralizados.
- Promover a popularização do paradigma da descentralização junto ao consumidor.

Capítulo 2

Revisão Exploratória da Literatura

A ascensão do Bitcoin levou à popularidade de soluções baseadas em *blockchain* em muitas indústrias [46, 47, 1]. Desde a criação do Bitcoin em 2008, as TLRDs (a exemplo daquelas baseadas em *blockchain*) têm atraído a atenção de acadêmicos e profissionais [51, 191]. Uma das principais características das TLRDs é a imutabilidade dos dados, o que torna esses sistemas altamente seguros contra fraudes e ataques cibernéticos. Cada *blockchain* é composta por blocos interligados que contêm um *hash* criptográfico do bloco anterior, uma data de referência e dados de transações, tudo encapsulado e protegido por criptografia. O conceito de unir TLRDs em um ecossistema descentralizado capaz de integrar várias aplicações em muitas indústrias torna a pesquisa nesta área ainda mais intrigante [281].

Estima-se que as TLRDs sejam uma revolução em potencial, com aplicações práticas em setores como finanças, cadeias de suprimentos, seguros e saúde [122, 229, 254], aumentando a eficiência e a transparência nestes setores [121, 51, 259]. Essas tecnologias, particularmente as mais populares baseadas em *blockchain*, são vistas como pontos de inflexão para uma revolução industrial e comercial, promovendo mudanças econômicas globais [56, 261].

Olhando para as TLRDs como primitiva tecnológica utilizada para gerir relações entre indivíduos e instituições, existem várias dimensões que garantem a confiança entre estes agentes quando desconhecidos, garantem a imutabilidade dos registros e eliminam a necessidade de mediadores [172].

Os avanços nas tecnologias de informação e comunicação têm gerado transformações estruturais significativas, como a reorganização econômica e a globalização, intensificando os fluxos de capital e a disponibilidade de informações [89]. O mercado digital, por exem-

plo, impulsionado por algoritmos inovadores e eficientes na gestão de transações e análise de dados, experimentou uma expansão expressiva do comércio eletrônico entre 2004 e 2022. Nesse cenário, as tecnologias descentralizadas, como *blockchains*, receberam considerável atenção e investimentos. Em janeiro de 2021, Bitcoin e Ethereum, as duas principais plataformas descentralizadas, alcançaram capitalizações de mercado de US$ 632 e US$ 152 bilhões, respectivamente [130]. Essas tecnologias impactaram significativamente os processos de negócios, permitindo que transações antes mediadas por intermediários ocorram de forma descentralizada, mantendo o mesmo nível de confiança [44, 143]. As TLRDs oferecem privacidade, confidencialidade e segurança nas transações [120, 209], o que despertou o interesse de pesquisadores para investigar seus desafios e limitações tecnológicas [44].

Diversos setores, incluindo finanças [88], saúde [84], gerenciamento de cadeias de suprimento [150] e sistemas de reputação [72], já estão adotando soluções baseadas em *blockchain*. Neste contexto a segurança tem se tornado uma das principais preocupações de desenvolvedores. Assim, as TLRDs, como *blockchains*, *hash graphs* e *Internet computer* prometem ser a próxima grande revolução estrutural da Internet, utilizando técnicas criptográficas para registrar e sincronizar dados de forma segura em uma rede distribuída. Com o aumento das violações de dados e ciberataques, as empresas continuam buscando novas soluções para proteger os dados de seus clientes [159, 218, 256].

Uma grande diversidade de tecnologias baseadas em livro razão descentralizado (TLRD) permitem ainda transações validadas ponto a ponto (P2P), sem a necessidade de intermediários, usando contratos inteligentes para automatizar processos e devolvendo a autoridade sobre os dados e transações ao usuário. Dada a crescente digitalização, garantir segurança, privacidade e proteção nas transações online tornou-se essencial [99]. Como os consumidores desempenham um papel final nos mercados digitais globalizados [185], a autenticidade e a rastreabilidade de produtos tornaram-se preocupações centrais na indústria de bens de consumo [100, 233]. As TLRDs permitem o rastreamento de produtos ao longo de seus ciclos de vida, assegurando qualidade e segurança em toda a cadeia de suprimentos. O gerenciamento de informações via *blockchain* proporciona uma vantagem competitiva às empresas, permitindo a diferenciação de seus produtos [87]. Os consumidores, cada vez mais preocupados com a origem e a sustentabilidade dos produtos que consomem [56], buscam segurança, transparência e rastreabilidade nas transações.

Este Capítulo tem como objetivo mapear potenciais melhorias aplicadas ao ecossistema DAX para expandir a gestão descentralizada de transações para o dia a dia da sociedade em geral – i.e., aplicações B2C, *Business to Customer*, e C2C, *Customer to Customer*. Para isso este esforço de Tese busca respostas para duas questões específicas de pesquisa relativas ao i) potencial disruptivo do DAX em aplicações B2C e C2C; e, ii) os principais obstáculos que impedem o DAX de explorar esse potencial. Para tanto, este Capítulo apresenta uma análise bibliométrica por meio de revisão da literatura sobre a aplicação de tecnologias descentralizadas em serviços B2C e C2C, consolidando resultados de buscas em repositórios científicos e resultados de revisões da literatura já publicadas a respeito do tema. O conteúdo deste Capítulo é baseado em um artigo científico em processo de publicação (*round* #2) na revista ACM Distributed Ledger Tecnologies, disponível na integra no Anexo E.

Para explorar tais questões, quatro das principais áreas com dificuldades atualmente para o avanço do DAX já mapeadas na literatura especializada foram abordadas [273, 5, 9] (1) Governança – No DAX, a governança diz respeito a algoritmos de consenso e gerenciamento de mudanças em protocolos de rede [153]. Aqui, definimos governança como o conjunto de protocolos de tomada de decisão em todas as camadas da rede descentralizada, seja na camada de aplicação, na camada de consenso ou mesmo no mecanismo de gerenciamento de mudanças por trás da rede. (2) Segurança – Em TLRDs, esta é a base por trás da integridade dos protocolos de governança de rede [67]. (3) Escala/Desempenho/Performance – Como a TLRD está associada a muitas tecnologias de naturezas distintas, o conceito de desempenho ou performance não pode ser traduzido em números com precisão. No entanto, assumimos que desempenho é o incremento no poder de processamento de transações atribuído a cada novo nó na rede. (4) Autenticação - Refere-se à capacidade das entidades de realizar transações digitais seguras e autenticadas, mesmo quando anônimas [194].

Dentre os desafios discutidos nas revisões da literatura selecionadas, destacam-se questões cruciais no desenvolvimento de aplicações voltadas ao consumidor, que formam as principais Questões de Pesquisa (RQs) deste estudo.

1. Identificar se se há de fato um potencial disruptivo em aplicações B2C e C2C em ambiente DAX e suas tendências recentes de publicação com uma abordagem temporal (QP1).

2. Contribuir para o avanço da pesquisa sobre *blockchain*, explorar novas descobertas e buscar enumerar as principais lacunas para a popularização das DAX junto ao consumidor, além de possíveis tópicos de pesquisa que precisam ser abordados (QP2).

Para responder a **QP1**, traçamos um paralelo entre os seguintes estágios de desenvolvimento e popularização da Internet e do DAX: Estágio 1: disrupção; Estágio 2: utilidade; Estágio 3: usabilidade (Google); e, Estágio 4: espelhando a sociedade e os relacionamentos entre usuários humanos por meio de tecnologias (Redes Sociais e Smartphones). Um paralelo semelhante já foi aplicado por Carvalho et al [43] ao comparar a ascensão das criptomoedas e suas tecnologias satélites à trajetória do sistema operacional Linux de código aberto [1].

Para **QP2**, os resultados desta revisão indicam que várias das fraquezas do DAX destacadas na literatura já receberam ampla cobertura tanto pela academia quanto pela indústria. É razoável supor que as fraquezas que já foram efetivamente abordadas não representam mais impedimento à popularização do DAX – como é o caso dos protocolos de reputação baseados em oráculos [36] ou modelos de descentralização de mineração [239]. Por outro lado, questões exploradas apenas recentemente ou com poucos resultados relevantes foram tratadas como impedimentos mais diretos, como Governança em Redes de Internet das Coisas (IoT) [277], SCs Ricardianos [199], etc.

2.1 Metodologia

Existem várias formas de abordar-se uma revisão da literatura [165, 210, 212]. Nesta etapa da Tese, a exemplo de Bhawna et al [31], adotamos uma abordagem híbrida de revisão bibliométrica e de desenvolvimento de teoria a fim de responder as questões de pesquisa estabelecidas, sobretudo a QP2 que visa evidenciar lacunas que demandem maior atenção e pesquisa em aplicações descentralizadas voltadas ao consumidor, definindo assim o direcionamento da tese e uma agenda para pesquisas futuras.

Os critérios de inclusão e exclusão para a seleção dos trabalhos levam em consideração os objetivos, questões de pesquisa e metadados que ajudam a estimar a qualidade dos trabalhos.

[1] https://linux.org/

A metodologia seguida pelos revisores é descrita no Apêndice D [2]. As Tabelas 2.2 e 2.3 descrevem os critérios de seleção e qualidade, respectivamente, utilizados pelos revisores para 1) verificar os resultados obtidos pelo pesquisador como adequados ao tópico de pesquisa; e, 2) avaliar a cobertura do tópico como sendo suficiente ou não para ser considerado relevante.

Até onde observamos, existe uma quantidade significativas de revisões quantitativas e qualitativas que cobrem a área de aplicação de *blockchain* na pesquisa geral de aplicações voltadas ao consumidor. Com base nisso, ao invés de iniciar a busca a partir de palavras-chave ou periódicos definidos arbitrariamente, o primeiro passo (1) desta revisão consistiu em reunir tais outras revisões por meio de uma análise bibliométrica de aplicações de *blockchain* em serviços ao consumidor, as submetendo aos mesmos critérios desta revisão para selecionar os trabalhos mais relevantes e, então, extrair palavras-chave a partir de seus resultados.

O segundo passo (2) consistiu no processo de consulta aos mecanismos de busca em bases de dados científicas utilizando as palavras-chave identificadas no primeiro passo, e posterior verificação dos trabalhos relevantes de acordo com nossos critérios definidos. O processo completo de seleção de artigos é apresentado graficamente na Figura 2.1 e será descrito em mais detalhes ao longo deste Capítulo.

Consideramos artigos que tratem de TLRD em aplicações ao consumidor publicados entre 2016 e 2023. Os bancos de dados acadêmicos escolhidos para esta investigação foram Web of Science (WoS) e Scopus [33]. Scopus por ter uma coleção mais extensa e diversificada de material acadêmico e o WoS por ser a plataforma de busca e análise de citações científicas mais abrangente do mundo [34, 145].

Seguindo as boas práticas da ciência aberta e para facilitar a leitura, dados detalhados como o conjunto total de artigos avaliados ou o manual dos revisores foram armazenados separadamente em endereço eletrônico aberto para leitura[3].

[2] Os manuais dos revisores não estão inclusos no corpo principal deste documento por tratar-se de uma leitura complementar que, embora necessária para a reprodução deste estudo, sua leitura é dispensável para a compreensão deste documento.

[3] https://drive.google.com/drive/u/1/folders/1LdGsGZrPaQuCsOCBFNXDakMFPxlPSZ59

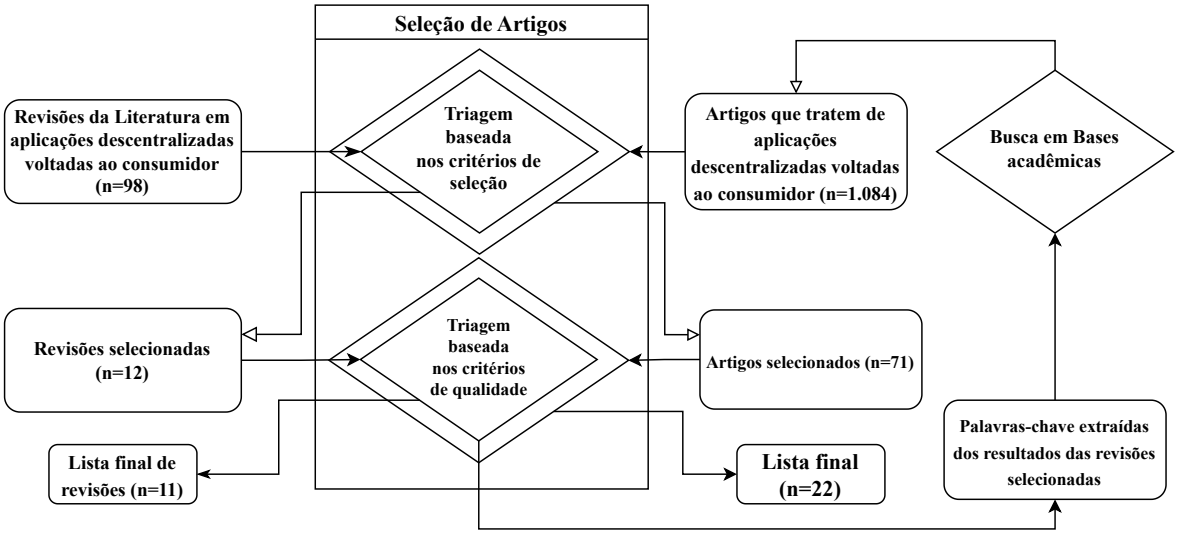


Figura 2.1: Fluxograma de Revisão

2.2 Processo de Seleção

2.2.1 Busca

A revisão seguiu o modelo SPAR-4-SLR (Scientific Procedures and Rationales for Systematic Literature Reviews), conforme descrito por Paul, Merchant et al. [212] e Lim et al. [165], com o objetivo de reunir, organizar e avaliar a literatura relevante sobre o tema. Seguindo o modelo SPAR-4-SLR, inicialmente montou-se do constructo de revisão. Tal constructo inclui a definição do domínio de estudo com foco em aplicações B2C e C2C descentralizadas, a formulação de perguntas de pesquisa (QPs), a escolha de tipos de fontes e a avaliação de sua qualidade. Para garantir a qualidade da revisão, os bancos de dados Scopus e Web of Science (WoS) foram selecionados como as principais fontes.

Dado o grande número de estudos disponíveis sobre o tema, foi necessário aplicar filtros específicos para refinar a busca. Na primeira fase que envolve um compilado de revisões da literatura sobre o tema, a pesquisa foi realizada com a seguinte consulta: (((Blockchain AND consumer OR 'Blockchain technology' AND consumers) OR 'Blockchain technology' in 'consumer applications') AND 'Literature Review'), aplicada às palavras-chave, título e resumo. Como resultado dessa fase, realizada em 30 de outubro de 2023, foram obtidos 98 artigos escritos em inglês.

Inicialmente, filtrou-se as revisões coletados a partir das bases de dados acadêmicos me-

diante os critérios de seleção e qualidade, chegando a 11 revisões selecionadas. Tais revisões, embora alinhadas com esta em muitos aspectos, divergem em termos de objetivos, público ou foco, a exemplo do trabalho de Cousins et al [65]. Em sua revisão, Cousins et al [65] usam a metodologia Value-Sensitive Design para mapear uma agenda de pesquisa sobre as principais contribuições possíveis das criptomoedas (tomando o Bitcoin como exemplo) para a vida dos usuários finais, um objetivo intimamente relacionado a esta revisão, apesar de divergir quanto ao foco restrito a criptomoedas.

A partir dos resultados desta fase inicial extraiu-se o seguinte conjunto de palavras-chave: "Food Traceability, Data Protection, Finance, Health, Real Estate, Electricity, Medicine Traceability, Insurance and Reputation Systems". A estratégia para a busca subsequente é baseada neste conjunto de palavras-chave selecionadas da etapa anterior. Aqui, as palavras-chave foram agrupadas em uma expressão relevante (string de busca). Estas palavras-chave resultaram na seguinte *string* de busca:

((Blockchain AND consumer OR 'Blockchain technology' AND consumer) OR 'Blockchain technology' in 'consumer applications') OR ((Blockchain AND 'Food Traceability' OR 'Blockchain technology' AND 'Food Traceability') OR 'Blockchain technology' in 'consumer applications') OR ((Blockchain AND consumer OR 'Blockchain technology' AND 'Data Protection') OR 'Blockchain technology' in 'Data Protection') OR ((Blockchain AND Finance OR 'Blockchain technology' AND Finance) OR 'Blockchain technology' in Finance) OR ((Blockchain AND Health OR 'Blockchain technology' AND Health) OR 'Blockchain technology' in Health) OR ((Blockchain AND 'Real Estate' OR 'Blockchain technology' AND 'Real Estate') OR 'Blockchain technology' in 'Real Estate') OR ((Blockchain AND Electricity OR 'Blockchain technology' AND Electricity) OR 'Blockchain technology' in Electricity) OR ((Blockchain AND 'Medicine Traceability' OR 'Blockchain technology' AND 'Medicine Traceability') OR 'Blockchain technology' in 'Medicine Traceability') OR ((Blockchain AND Insurance OR 'Blockchain technology' AND Insurance) OR 'Blockchain technology' in Insurance) OR ((Blockchain AND 'Reputation Systems' OR 'Blockchain technology' AND 'Reputation Systems') OR 'Blockchain technology' in 'Reputation Systems')

O resultado desta segunda fase gerou 243 resultados, já filtrados a partir dos critérios de seleção. Após aplicar-se os critérios de qualidade descritos na Tabela 2.3, chegamos à Tabela 2.1.

Tabela 2.1: Trabalhos mais elevantes na literatura.

Autor e Referência	Título	Veículo	Ano	Referências (GScholar)
Saberi et al [232]	Blockchain technology and its relationships to sustainable supply chain management	International Journal of Production Research	2018	3438
Mengelkamp et al [179]	Designing microgrid energy markets: A case study: The Brooklyn Microgrid	Applied Energy	2018	1812
Cong and He [64]	Blockchain disruption and smart contracts	Review of Financial Study	2019	1409
Galvez et al [101]	Future challenges on the use of blockchain for food traceability analysis	TrAC Trends in Analytical Chemistry	2018	883
Behnke and Janssen [26]	Boundary conditions for traceability in food supply chains using blockchain technology	International Journal of Information Management	2020	721
Feng et al [93]	Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges	Journal of Cleaner Production	2020	705
Choi [54]	Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains	Transportation Research Part E: Logistics and Transportation Review	2019	524
Astill et al [21]	Transparency in food supply chains: A review of enabling technology solutions	Trends in Food Science & Technology	2019	479

Liu et al [167]	Blockchain based data integrity service framework for IoT data	IEEE International Conference on Web Services (ICWS)	2017	457
De Keyser et al [70]	Frontline service technology infusion: conceptual archetypes and future research directions	Journal of Service Management	2019	373
Luo et al [169]	Adistributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain	IEEE Transactions on Power Systems	2019	367
Mackey et al. [171]	'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare	BMC Medicine European	2019	329
Sander et al [70]	The acceptance of blockchain technology in meat traceability and transparency	British Food Journal	2019	297
Zheng et al [287]	Blockchain-based personal health data sharing system using cloud storage	International Conference on e-Health Networking, Applications and Services (Healthcom)	2018	270
Wang et al [266]	A novel electricity transaction mode of microgrids based on blockchain and continuous double auction	Energies	2017	225

Westerkamp et al [275]	Blockchain-based supply chain traceability: Token recipes model manufacturing processes	IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)	2017	171
Kumar et al [151]	Women‘s financial planning for retirement: Systematic literature review and future research agenda	International Conference on Communication Systems & Networks (COMSNETS)	2019	125
Song et al [240]	Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection	Information Processing & Management	2021	104
Choi [55]	Creating all-win by blockchain technology in supply chains: Impacts of agents' risk attitudes towards cryptocurrency	European Journal of Operational Research	2021	89
Sheth and Subramanian [236]	Blockchain and contract theory: modeling smart contracts using insurance markets	Managerial Finance	2020	85
Laszka et al [154]	TRANSAX: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids	IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)	2018	61
Nguyen and Ali [195]	Enabling on-demand decentralized IoT collectability marketplace using blockchain and crowdsensing	Global IoT Summit (GIoTS)	2019	26

Tabela 2.2: Critérios de seleção para revisões da literatura.

Código	**Descrição**
C1	Os artigos devem estar escritas em inglês.
C2	Os artigos devem: a. Conter uma agenda de direcionamentos futuros para a literatura; b. Ser de áreas que correspondem a aplicações descentralizados voltas ao consumidor; c. Discutir tecnologias sem acesso restrito (sem permissão) ou sem gerenciamento centralizado ainda que tratem também de outras.
C3	Apenas serão avaliados estudos secundários, e a partir destes será colhida a lista de trabalhos finais.
C4	Artigos posteriores à 2016.
C5	O artigo avaliada deve ser completo e revisado por pares (artigos científicos publicados em conferências ou periódicos).
C6	Este critério é aplicado a estudos que visam melhorar tecnologias descentralizadas para aproximá-las do usuário comum e produz um inteiro $\in \{0, 1, 2, 3, 4\}$ onde zero exclui o estudo e qualquer outro valor o classifica para avaliação posterior. Um inteiro não nulo aqui se refere a uma das quatro áreas de dificuldade abordadas nesta revisão– 1- governança; 2- escala; 3- segurança; e, 4- informação.
C7	Documentos duplicados ou publicados mais de uma vez pelos mesmos autores em diferentes idiomas.
C8	Estudos que: a. discuta apenas aplicações – ou seja, que não proponham nenhuma evolução em tecnologia ou que não resolvam um problema relevante (exceto no caso de revisões da literatura); b. atende aos critérios acima, mas não entra em detalhes sobre as técnicas, características, etc.

Tabela 2.3: Critérios de qualidade aplicáveis aos artigos provenientes das listas de selecionados das revisões da literatura encontradas

Código	**Descrição**	**Adequação**
CQ1	O estudo é claro, sem ambiguidade, baseado em evidências e argumentos?	De acordo com SPAR-4-SLR (Paul et al. [211])
CQ2	O estudo foi publicado em uma conferência ou periódico de impacto?	De acordo com SPAR-4-SLR (Paul et al. [211])
CQ3	O estudo tem relevância concreta para pesquisa ou prática [211]?	1. Descreve um aplicativo potencialmente popular?: 0.08 2. Promove acesso ao DAX por parte do consumidor?: 0.18 3. Traz alguma melhoria estrutural que promova o paradigma da descentralização junto ao consumidor?: 0,25 4. Resolve um problema para a maioria da população?: 0.5. 5. Descreve uma revisão da literatura que avalia estudos que se enquadram nos itens anteriores?: 1.0.
CQ4	O artigo está devidamente referenciado [211]?	Os mais bem referenciados recebem nota 1; os demais recebem nota proporcional à diferença em relação à nota máxima.

2.2.2 Revisão

Seguindo o protocolo SPAR-4-SLR, organizou-se as contribuições científicas para revisão. Isso envolve a categorização (ou seja, organização por códigos) e a purificação dos registros recuperados (filtrando por critérios de seleção e qualidade). Os dados bibliométricos são organizados por meio de códigos baseados em título, fonte, tipo, ano de publicação e citações dos itens. Essa etapa permitiu verificar a qualidade geral das contribuições recuperadas, que incluíam artigos publicados em periódicos revisados por pares, anais de conferências internacionais, além de livros e capítulos de livros. Esta etapa da revisão foi executada em dois momentos, a princípio sobre as revisões da literatura a respeito do tema de estudo, em seguida sobre os resultados definitivos – o conjunto de trabalhos recuperados nas buscas. Estes dois ciclos de revisão estão representados na Figura 2.1, onde os dois losangos envolvendo as etapas de triagem representam os dois momentos em que tal atividade ocorreu.

Na primeira etapa de triagem (sobre as revisões da literatura extraídas das bases de dados), os autores definiram alguns critérios de seleção personalizados para as revisões da literatura (ver Tabela 2.2). Em seguida, após a segunda etapa de triagem (sobre os artigos extraídos das bases de dados), um resultado parcial foi consolidado, identificando-se 96 itens duplicados, que foram então removidos do conjunto de dados. O resultado desta segunda etapa foi então submetido aos critérios de qualidade (ver Tabela 2.3), cujo resultado compõe a lista final de artigos.

Especificamente, foram descartados os registros que não tratavam de TLRD em aplicações B2C e C2C (ou seja, artigos fora do escopo). Esses artigos foram então analisados para verificar sua relevância ao objetivo do estudo, por meio da leitura de seus títulos, resumos e textos completos. Como resultado, 71 publicações foram selecionadas para análise bibliométrica.

Os critérios de seleção e qualidade para os trabalhos foram estabelecidos para garantir a relevância e a qualidade das publicações escolhidas. Esses critérios consideraram os objetivos da pesquisa, as questões investigativas e metadados que ajudaram a avaliar a qualidade dos estudos. A metodologia completa adotada pelos revisores está descrita em um documento separado – consulte o ApêndiceD[4]. Além disso, as Tabelas 2.2 e 2.3 apresentam,

[4]https://docs.google.com/document/d/1xFGE_0lPl6mw1iAOEMRCkKOtXdtRxfO4dui7eUUnNpQ/edit?tab=t.0#heading=h.ixlsxtjrks7

respectivamente, os critérios usados para: 1) definir os requisitos mínimos para aceitação dos trabalhos e verificar sua adequação ao tema de pesquisa; e 2) avaliar se os resultados selecionados são suficientemente abrangentes e adequados aos critérios de qualidade e relevância.

2.3 Resultados

A análise da literatura revela um crescimento exponencial do interesse em aplicações TLRD voltadas ao consumidor nos últimos anos. Esta Seção destaca os trabalhos mais influentes, o mapa temático e os tópicos em destaque. A Tabela 2.1 traz a lista final de trabalhos selecionados e a Tabela 2.4 traz as revisões da literatura que também contribuíram para os resultados.

A Figura-2.2 demonstra um aumento significativo no número de publicações desde 2016, com um pico em 2020, embora antes disso em 2019 tenha recuado um pouco. O número de artigos passou de dois em 2016 para 19 (24 considerando artigos abordando mais de um tema) em 2020. Essa tendência é impulsionada pelas características intrínsecas da TLRD, como segurança, transparência e imutabilidade, que a tornam atrativa para diversos setores. A taxa de crescimento anual médio de 69,16% reflete o crescente interesse dos pesquisadores em explorar os casos de uso e os possíveis impactos das TLRDs no ambiente de consumo.

A análise do mapa temático da Figura 2.3 identificou uma alta relevância e densidade nos temas Rastreabilidade de Recursos, sobretudo alimentares, e Sistemas de Reputação e Avaliações. Os resultados indicam que os pesquisadores estão cada vez mais interessados em explorar o potencial das TLRDs para rastreamento de suprimentos (sobretudo alimentares), Grids de negociação de energia elétrica descentralizados e sistemas de reputação, além de áreas que cresceram de forma mais intermitente como registro imobiliário e proteção de dados. Além disso, a análise das publicações mais impactantes revela que o grau de impacto das publicações seguiu a tendência do volume de publicações, alcançando seu ápice em 2020.

A crescente adoção de TLRDs em aplicações voltadas ao consumidor abre novas perspectivas para futuras pesquisas. É fundamental aprofundar o estudo em temas como Grids de Energia Elétrica, que conta com bastante volume e densidade, porém pouca relevância, e temas já em ascensão como Rastreabilidade e Sistemas de Reputação, além de explorar o impacto da tecnologia em diferentes contextos. Adicionalmente, a análise interdisciplinar,

Tabela 2.4: Revisões da literatura que investigam o estado da pesquisa em aplicações voltadas ao consumidor.

Autor e Referência	Título	Veículo	Ano	Referências (GScholar)
Demestichas et al [71]	Blockchain in Agriculture Traceability Systems: A Review	Applied Sciences	2020	374
Gurtu e Johny [110]	Potential of blockchain technology in supply chain management: a literature review	International Journal of Physical Distribution & Logistics Management	2019	336
Rossi et al [225]	Blockchain research in information systems: Current trends and an inclusive future research agenda	Journal of the Association for Information Systems	2019	312
Boukis [35]	Exploring the implications of blockchain technology for brand–consumer relationships: a future research agenda	Journal of Product & Brand Management	2020	130
Nurgazina et al [200]	Distributed ledger technology applications in food supply chains: A review of challenges and future research directions	Sustainability	2021	98
Schlegel et al [233]	Blockchain technologies from the consumers' perspective: What is there and why should who care?	Hawaii International Conference on System Sciences	2018	81
da Silva e Moro [96]	Blockchain technology as an enabler of consumer trust: A text mining literature analysis	Telematics and Informatics	2021	63

Cousins et al [65]	A value-sensitive design perspective of cryptocurrencies: a research agenda	Communications of the association for information systems	2019	36
Karuseva et al [132]	The impact of innovative technologies on consumers in the power supply market	E3S web of conferences	2019	13
Bhawna et al [31]	Blockchain application in consumer services: A review and future research agenda	International Journal of Consumer Studies	2023	11
Gatteschi et al [103]	An Overview of Blockchain-based Applications for Consumer Electronics	International Symposium on Consumer Technologies (ISCT)	2019	7

envolvendo áreas como ciência da computação, economia e direito, pode contribuir para um melhor entendimento das implicações das TLRDs para a sociedade.

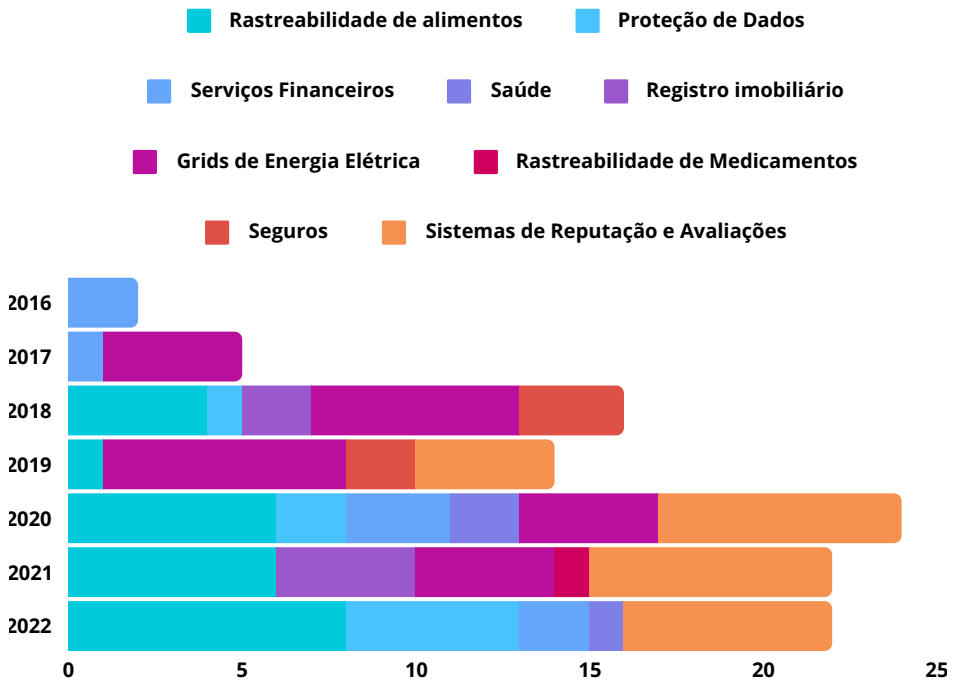


Figura 2.2: Mapa temporal que descreve a evolução da pesquisa no tema ao longo dos anos. Esta imagem considera os 71 artigos totais, reunidos apenas com base nos critérios de seleção. Alguns artigos abordam mais de um dos temas.

QP1

Do lançamento da ARPANET na década de 1960, passando pelo primeiro uso do termo Internet em 1978, até a publicação da primeira página na World Wide Web em 1990, passaram-se 30 anos. Daí até o lançamento do mecanismo de busca Google em 1998, passaram-se mais oito anos. Assim, pode-se dizer que a Internet levou 38 anos para se tornar onipresente na vida cotidiana da sociedade [5]. Perante o público em geral, podemos tomar a publicação do white paper do Bitcoin em 2008 como a estreia do paradigma descentralizado, chegando a 17 anos de existência do DAX até 2025. Assim, comparado ao tempo que a Internet levou para amadurecer, o DAX ainda está em seus primeiros anos.

[5]Grande parte do conteúdo histórico sobre a Internet nesta subseção foi baseado em Barry [25]

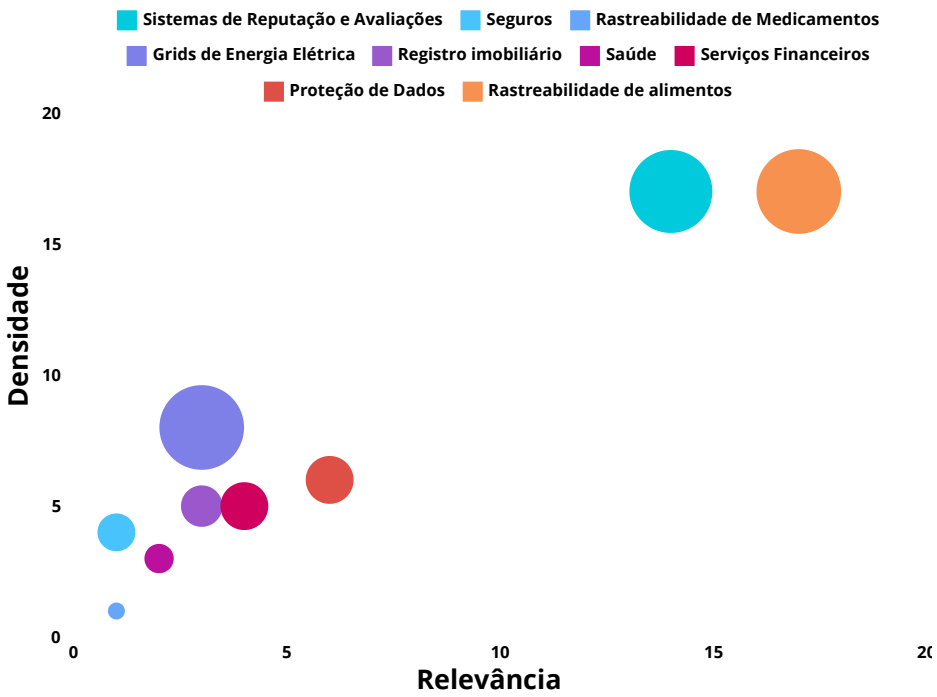


Figura 2.3: Mapa temático que descreve a estado da pesquisa por tema identificado na literatura. Esta imagem considera os 71 artigos totais, reunidos apenas com base nos critérios de seleção. Alguns artigos abordam mais de um dos temas.

A popularização da Internet ao longo das décadas de 1990, 2000 e 2010 aconteceu em quatro etapas:

1. Ruptura: Para a Internet, isso aconteceu quando Tim Berners-Lee – criador da rede World-Wide-Web, da linguagem de formatação HTML e do protocolo HTTP – em 1993 anunciou que sua criação funcionaria abertamente e sem cobrança de royalties, na suposição de que somente dessa forma a Internet alcançaria seu verdadeiro objetivo de se tornar uma comunidade humana mundial.

2. Utilidade: Vários serviços online começaram a ser criados com foco em popularizar a Internet e ganhar engajamento, como o site GeoCities [6] que oferecia o serviço de criação de *Home Pages* estáticas pessoais – isso pode parecer pouco útil comparado ao que temos agora, mas em 1994 foi um grande sucesso.

3. Usabilidade: O Google surgiu em 1998 como uma ferramenta genérica para Indexação Rápida de toda a Internet, permitindo que qualquer *site* fosse encontrado a partir de qualquer pequeno trecho de seu conteúdo. Isso lançou a última pedra fundamental para transformar a Internet na comunidade dinâmica que é hoje.

4. Espelhamento: Atualmente, não se pode falar de Internet sem mencionar as redes sociais. O Facebook [7] foi o principal fenômeno de popularidade nesta fase, mas não o pioneiro, pois antes dele várias outras redes foram criadas para fins específicos como SixDegrees, AIM, ICQ ou Friendster, todas elas hoje desativadas devido à concorrência com o Facebook.

Podemos reconhecer claramente o primeiro estágio no DAX, onde as redes Bitcoin e Ethereum, além de todo o ecossistema blockchain, promoveram o reconhecimento do potencial disruptivo do paradigma da descentralização. No entanto, o DAX tropeça no segundo estágio, pois ainda carecem de apelo popular.

A distribuição temporal por super tópico da Figura 2.4 deixam clara uma demanda crescente por soluções de governança na academia. Karajvanov [130] apresenta um conjunto de trabalhos futuros e limitações das atuais tecnologias descentralizadas, entre elas a dificuldade

[6] https://web.archive.org/web/20010501000000*/geocities.yahoo .com/

[7] https://www.facebook.com/

em punir o não cumprimento de uma exigência contratual sem a necessidade de reter fundos. Essa limitação decorre da dificuldade dos DAXs em representar eventos e fatos do mundo real no blockchain (onchain) sem depender de verificações centralizadas confiáveis. Tal lacuna de virtualização contrasta com a virtualização de valores, já amplamente alcançada desde o surgimento das criptomoedas. A Tabela 2.5 traça um paralelo entre o surgimento da Internet e as tecnologias DAX a partir dos resultados coletados.

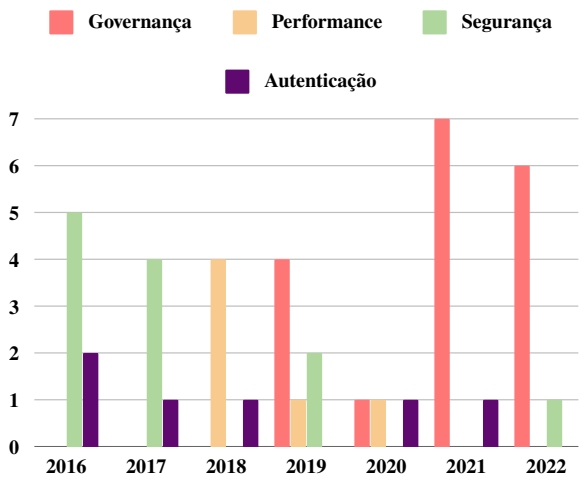


Figura 2.4: Distribuição temporal dos achados da literatura.

QP2

Os artigos selecionados na Tabela 2.1 indicam um foco recente na governança com o aprimoramento do CI como principal alvo dos esforços da comunidade. Mapeamentos anteriores já mostraram que o potencial disruptivo da tecnologia CI gera muita expectativa na comunidade e na indústria [225]. Além disso, de acordo com Song et al [239] a falta de tecnologias de *blockchain* públicas desacopladas do conceito de moeda, ou recompensa financeira por transação, dificulta o aproveitamento da tecnologia CI em sua essência. Ainda segundo Song et al [239], isso limita tais aplicações aos domínios financeiro e corporativo, onde esse tipo de cobrança é mais viável.

Ainda sobre CI, Karajvanov [130] afirma que a dificuldade em fornecer garantias baseadas em informações assimétricas é um dos principais gargalos do CI. Ou seja, um CI não

Tabela 2.5: Internet × DAX

Fase	Internet	DAX
1	Virtualização da informação a partir do surgimento da rede World Wide Web	Virtualização de valores através de criptomoedas
2	Virtualização de eventos e fatos a partir de serviços online	Virtualização de eventos contratuais ainda em aberto
3	Virtualização de relacionamentos acessível através do Google como mecanismo genérico e de utilidade ampla	Aberto
4	Redes sociais geram dependência, também virtualizam relacionamentos e passam a virtualizar autoridade	Aberto

consegue estabelecer obrigações e direitos sobre transações ou eventos futuros que ocorram no mundo real. Isso impede a maioria dos usos práticos do CI como substituto de contratos convencionais. Creutz e Dartmann [66] propõem uma solução baseada em Contratos Ricardianos, mas toda validação colateral continua baseada em modelos de contratos convencionais.

Do exposto podemos inferir que um dos fatores que distancia o usuário do paradigma descentralizado são as limitações da própria tecnologia CI quando comparada aos contratos convencionais: a dificuldade em virtualizar eventos do mundo real de forma descentralizada, suas limitações em impor ou limitar transações futuras, ou mesmo seu determinismo natural [199, 36, 130, 66, 80].

2.3.1 Mapa Temático

Comércio com rastreio de produtos, sistemas de reputação e mercados de energia em redes P2P são temas de nicho, conforme Figura 2.3. As aplicações de TLRD estão se tornando mais comuns em mercados de energia usando redes P2P [73, 92, 103, 109]. Com os consumidores buscando fontes de energia mais sustentáveis e eficientes, as tecnologias baseadas

em *blockchain* podem desempenhar um papel crucial na promoção do bem-estar social e no fornecimento de energia renovável [288]. Os temas no canto inferior esquerdo do mapa estão desaparecendo. Proteção de dados, por outro lado tem uma literatura mais relevante que densa, assim podemos colocá-lo como tema em ascensão. Esses temas podem surgir naturalmente como resultado da pesquisa, ou os pesquisadores podem criá-los. Finalmente, os temas já em ebulição são exibidos no quadrante superior direito. Nesta área, os temas predominantes são gerenciamento e rastreio da cadeia de suprimentos e sistemas de reputação e avaliação.

As Tecnologias de Livro-Razão Distribuído (TLRDs) abordam várias questões globais relacionadas ao gerenciamento de cadeias de suprimentos, oferecendo uma plataforma distribuída que garante segurança, transparência e rastreabilidade [232]. Entre 2016 e 2018, tópicos como cadeias de suprimentos, armazenamento digital, gerenciamento de suprimentos, vendas e redes P2P começaram a surgir, mas não receberam muita atenção acadêmica nos períodos subsequentes. Já entre 2018 e 2019, temas como comércio e rastreamento de produtos, mercados de energia, cadeias de suprimentos e IoT ganharam destaque.

A partir dos números alcançados nesta revisão e com base nas palavras-chave mais recorrentes nos artigos classificados, podemos estabelecer um arcabouço teórico sobre o estado da arte atual no que diz respeito às quatro principais dificuldades para a popularização do DAX – Segurança, Informação, Escala e Governança – conforme indicado na Figura 2.5.

2.3.2 Tendências de Pesquisa ao Longo do Tempo

A Figura 2.2 apresenta diversas tendências em TLRDs aplicadas aos consumidores, acompanhadas ao longo do tempo. A análise dessas tendências evidencia os principais desafios que se tornaram o foco de atenção dos pesquisadores, especialmente em aplicações voltadas ao consumidor. A evolução dos temas ao longo dos anos também é representada, destacando os tópicos que foram objeto de estudo por períodos prolongados e aqueles que surgiram recentemente na pesquisa.

O gráfico ilustra as mudanças nos tópicos de pesquisa ao longo do tempo. Entre 2016 e 2019, os temas predominantes foram sobretudo negociação de eletricidade, mas também rastreamento de recursos e finanças, refletindo o aumento das possibilidades de negociação

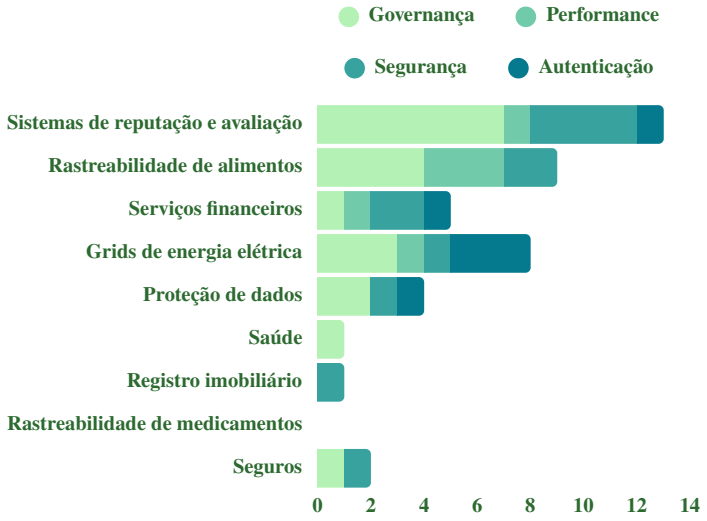


Figura 2.5: Enquadramento teórico: Cada palavra-chave principal selecionada verticalmente $\times$ 71 trabalhos relevantes horizontalmente

de eletricidade P2P (peer-to-peer). Nessa época, prosumidores [8] capazes de produzir sua própria eletricidade vendiam o excedente a outros consumidores [92].

Entre 2019 e 2020, novos tópicos ganharam força, como redes de reputação e avaliação, além de cadeias de suprimentos e seguros. Já entre 2020 e 2021, os temas mais destacados incluíram gestão da cadeia de suprimentos, redes de reputação, transparência e mercados de energia. Por fim, entre 2021 e 2022, os tópicos mais populares foram redes de reputação e avaliação, bem como a gestão da cadeia de suprimentos e proteção de dados.

Em uma visão orientada aos quatro pontos focais (Governança, Segurança, Performance e Autenticação) observadas na literatura, podemos listar as seguintes perspectivas futuras:

1. Uma solução para governança descentralizada parece ser um ponto focal no trabalho recente [153]. Portanto, duas questões importantes permanecem em aberto;

   (a) Como descentralizar a gestão de mudanças em TLRDs públicas;

   (b) Como gerenciar a reputação dos usuários em redes descentralizadas.

2. A dificuldade de performance em *blockchain* foi abordada principalmente usando TLRD sem blocos [208]. No entanto, a indústria já tem iniciativas efetivas e cres-

[8] Aqueles que consomem, mas também produzem o mesmo produto.

centes voltadas a escalar o volume de transações e mineração em *blockchains*. Como exemplo disto podemos citar a transição de mineração *proof-of-work* para mineração *proof-of-stack* das principais *blockchains* do mercado;

3. A dificuldade de virtualizar eventos e fatos do mundo real leva as TLRDs a apelar para autoridades centralizadas por meio de oráculos [36] ou entidades confiáveis. Uma solução que espelhe eventos e fatos do mundo real de forma descentralizada é um dos problemas mais críticos quando se trata de trazer soluções descentralizadas para a vida diária das pessoas [181, 184, 75, 201, 183]. Zavolokina et al [282] ilustraram esse problema usando a venda de um carro usado como exemplo. Há muitos dados para descrever a situação mecânica do carro, mas virtualizá-los de forma descentralizada é um grande desafio porque o proprietário do carro quer esconder qualquer informação ruim do comprador. Atualmente, nossos esforços estão focados em como garantir a verificação correta e descentralizada de tais informações do mundo real;

4. Os relacionamentos comerciais do mundo real tendem a fornecer regras para transações que ainda estão por vir. É impossível, por exemplo, criar uma cláusula contratual punitiva para o não cumprimento de um requisito específico, a menos que a punição seja monetária por meio de um valor retido anteriormente. No entanto, os CIs atuais só podem governar transações que já ocorreram com garantias já disponíveis [263, 130].

A oportunidade de pesquisa acima sobre CI está intimamente relacionada às descobertas de Cousins et al [65] que relataram demandas e lacunas de pesquisa sobre Confiança, Autogovernança e Inovação Responsável em criptomoedas.

2.4 Discussões do Capítulo

À medida que as tecnologias de registro distribuído (TLRDs) amadurecem, espera-se que suas aplicações se expandam para outros setores, como serviços financeiros, infraestrutura, mobilidade, saúde, varejo, bens de consumo, setor público, agricultura, mineração, serviços de comunicação e informação, entretenimento, educação, entre outros [32, 228]. Entre 2019 e 2020, observou-se um aumento significativo nas publicações sobre o tema, demonstrando um interesse crescente nas aplicações descentralizadas voltadas ao consumidor. Embora a

tecnologia ainda esteja em fase inicial e seja desconhecida pela maioria dos consumidores, várias empresas e setores estão investindo nela devido aos benefícios que oferece. A descentralização tem o potencial de trazer benefícios significativos para países em desenvolvimento, como a redução da inflação, inclusão financeira para pessoas sem acesso a bancos, e prevenção da corrupção por meio da imutabilidade dos registros digitais, além do empoderamento do usuários sobre seus dados. A integridade dos dados, característica marcante de tecnologias como o *blockchain*, é um dos principais fatores que impulsionam países e empresas a investirem nessa área [51, 281]. Diversos estudos estão focando em temas como comportamento do consumidor, adoção tecnológica, armazenamento digital, reputação, privacidade de dados e gerenciamento da cadeia de suprimentos.

A segunda obra mais citada que trata de TLRDs (após o artigo seminal de Nakamoto, 2008, que introduziu o Bitcoin) é o estudo de Christidis e Devetsikiotis [56], que explora o potencial da integração entre *blockchain* e Internet das Coisas (IoT). Eles demonstram como essa combinação pode facilitar o compartilhamento de recursos e serviços, promovendo a formação de um mercado de serviços entre dispositivos. Essa integração nos permite automatizar várias atividades que antes eram demoradas, de forma criptograficamente verificável. As tecnologias baseadas em *blockchain* proporcionam sistemas distribuídos p2p resilientes, permitindo interações auditáveis e confiáveis entre as partes. Já os contratos inteligentes (CIs) possibilitam a automação de processos complexos. Dentro do ecossistema IoT, os dispositivos são os pontos de contato com o mundo físico, e quando combinados com *blockchain*, permitem a automatização de fluxos de trabalho de forma inédita, garantindo verificabilidade criptográfica, além de reduzir custos e tempo.

Acredita-se que a integração contínua de *blockchain* no domínio da IoT trará transformações significativas para diversos setores, introduzindo novos modelos de negócios e desafiando as práticas estabelecidas. No entanto, conforme apontado por Christidis e Devetsikiotis [56], essa integração exige esforços específicos para cada aplicação e envolve custos consideráveis, o que pode ser inviável em algumas circunstâncias. Além disso, ainda falta uma solução eficiente para conectar dados internos (*on-chain*) com dados externos (*off-chain*) de forma simplificada e que não exija adaptações específicas para cada domínio de aplicação, o que representa um obstáculo à adoção em larga escala da descentralização por parte dos consumidores. Outro desafio enfrentado pela adoção das TLRDs é a compreensão limitada

por parte dos usuários [168]. Os estudos apresentados neste Capítulo discutem tanto os benefícios dessas tecnologias quanto os obstáculos à sua integração, visando apontar caminhos para superar esses problemas no futuro.

2.4.1 Contexto Atual de Pesquisa

Diversas iniciativas de pesquisa têm explorado os benefícios da descentralização em diferentes setores. Embora a maioria dos estudos sobre TLRDs tenham se concentrado no setor bancário e financeiro, isso se deve, em parte, ao fato de esse setor demandar um menor volume de informações *offchain*. Por exemplo, Raddatz et al. [218] argumentam que, dada a atual ênfase em adaptar as TLRDs ao setor bancário, os autores de certos estudos deveriam ter escolhido cenários bancários para avaliar a percepção do consumidor quanto à adoção da descentralização. Em contrapartida, diversos estudos propuseram o conceito fundamental de comércio de energia peer-to-peer (P2P) para ilustrar abordagens recentes, tendências de desenvolvimento e desafios enfrentados [190]. Além disso, os autores introduziram um modelo de comércio de energia p2p, explorando as tendências, desafios, oportunidades, bem como as regulamentações e políticas pertinentes a cada uma das partes interessadas, incluindo concessionárias de energia elétrica, setor privado e governo. Isso ocorre devido ao avanço das energias renováveis e à promissora integração entre TLRDs e a Internet das Coisas (IoT), que são os principais catalisadores do desenvolvimento de um novo sistema de mercado para a troca de energia [106, 126]. Com base nesse modelo descentralizado, consumidores e "prosumidores"(aqueles que produzem e consomem energia) poderão trocar energia entre si [246].

Paralelamente, à medida que as Cadeias de Suprimentos Alimentares (FSCs) se tornam mais complexas, cresce a demanda por transparência na produção de alimentos [177]. Diversos fatores contribuem para essa necessidade, como o aumento da população mundial, a gestão eficiente de riscos, a detecção de surtos de doenças transmitidas por alimentos e a crescente exigência dos consumidores [200]. As TLRDs têm o potencial de melhorar a transparência ao longo da cadeia produtiva de alimentos [77]. No entanto, a implementação da descentralização nesse contexto exigirá uma colaboração significativa entre todas as partes envolvidas, além de introduzir uma série de novos desafios e demandas que precisarão ser abordados. Esses obstáculos variam desde questões tecnológicas, como conectividade

à internet, necessidades de armazenamento e segurança de dispositivos, até questões relacionadas à aceitação por parte dos consumidores e à viabilização do acesso a informações *offchain* [21].

Gatteschi et al. [103] destacam que há dezenas de iniciativas de descentralização utilizando TLRDs em áreas como saúde, casas inteligentes, cidades inteligentes, dispositivos conectados, indústria automobilística e comércio. Segundo Biswas e Gupta [32], a adoção e implementação de TLRDs em diversos setores e serviços é um processo complexo, exigindo altos investimentos. Por essa razão, a pesquisa sobre aplicações descentralizadas em diferentes indústrias, com uma abordagem mais generalista, é essencial. Contudo, o volume atual de pesquisas é ainda disperso e heterogêneo, dificultando a formulação de generalizações. Estudos subsequentes são necessários para analisar a adoção e o uso de TLRDs por consumidores de diferentes indústrias, permitindo comparações de suas intenções e identificando diferenças entre perfis de consumidores. Além disso, é crucial conduzir pesquisas em vários contextos de aplicações de TLRDs voltadas ao consumidor, uma vez que esses serviços abrangem uma ampla gama de indústrias, como finanças, saúde, varejo e entretenimento. O estudo do uso de TLRDs em diferentes áreas pode proporcionar uma melhor compreensão da diversidade de aplicações dessa tecnologia, bem como identificar os setores onde ela pode ser mais eficaz. Cada contexto apresenta desafios e oportunidades distintos para a adoção das TLRDs, sendo que os tipos de dados trocados também variam. Esses dados, em sua maioria, estão *offchain* e precisam ser digitalizados, seja por meio de IoT, Edge Computing ou sistemas de reputação. Entre essas opções, os sistemas de reputação se destacam como os mais viáveis, apesar de introduzirem uma camada adicional de risco [103].

2.4.2 Próximos Capítulos

A literatura atual sobre aplicações descentralizadas voltadas ao consumidor explora a evolução, compreensão e conceituação desse tema, com foco nos resultados relacionados à adoção, implementação, benefícios e desafios. Estudos anteriores, que geraram maior interesse no assunto, centraram-se em abordagens teóricas, analisando a interação entre essas tecnologias e os consumidores. Exemplos notáveis incluem a Teoria do Comportamento Planejado (TPB) e o Modelo de Sucesso dos Sistemas de Informação (ISS).

Os modelos TPB e ISS são frequentemente combinados em uma estrutura conceitual in-

tegrada para investigar as variáveis que influenciam as intenções de uso de tecnologias, como o Sistema de Rastreabilidade de Alimentos baseado em TLRDs entre consumidores chineses, a fim de garantir a segurança e a qualidade de produtos alimentares orgânicos [166]. Para compreender as atitudes dos consumidores em relação à adoção de novas tecnologias, a literatura sugere o uso de várias estruturas teóricas de aceitação tecnológica, como a Teoria Unificada de Aceitação e Uso de Tecnologia, o Modelo de Difusão da Inovação [127] e o modelo de Ajuste Tarefa-Tecnologia [7]. Como a adoção de recursos baseados em *blockchain* envolve mudanças significativas em comportamentos essenciais dos consumidores, como o pagamento, os profissionais se interessam em examinar os fatores que facilitam ou dificultam a adoção da descentralização como uma tecnologia emergente no mercado de consumo [247].

Apesar dos avanços consideráveis nos últimos oito anos, ainda existem lacunas no desenvolvimento e aplicação de diversas teorias em torno das aplicações descentralizadas voltadas ao consumidor. Desenvolvedores futuros provavelmente precisarão ajustar as aplicações existentes para trabalhar em diferentes estruturas descentralizadas, especialmente ao lidar com informações *off-chain*, que dependerão fortemente de soluções dedicadas à Internet das Coisas (IoT) ou modelos de reputação e consenso onde uma certa taxa de insucesso é aceitável. No próximos Capítulos exploraremos novas estruturas teóricas para explorar o potencial ainda não investigado das aplicações descentralizadas voltadas ao consumidor mediante informação *off-chain*. O estudo de fatores que influenciam a adoção dessas tecnologias, incluindo atitudes e comportamentos dos usuários, será central. Nos próximos Capítulos avaliaremos os riscos e desafios associados à implementação do TLRDs em aplicações voltadas ao consumidor, principalmente em cenários que dependam de acessar informações *off-chain* em domínios generalistas.

2.5 Sumário do Capítulo

A seguir enumeramos as principais contribuições deste Capítulo para esta Tese e suas próximas fases.

- Apontou-se as Transações *offchain* como um gargalo da descentralização.

- Apontou-se o problema da virtualização de informação do mundo real como um dos problemas mais relevantes.
- Estabeleceu-se o uso de IoT e redes de reputação como possíveis caminho para resolver os problemas acima.
- IoT é uma solução mais segura para o problema do acesso a informação *offchain*, porém funciona melhor em domínios específicos com soluções dedicadas.
- Redes de reputação são mais generalistas que IoT, porém admitem um certo risco.
- Neste Capítulo identificou-se a Governança como o calcanhar de Aquiles das iniciativas descentralizadas voltadas ao consumidor.

Capítulo 3

Problema de Pesquisa: O Dilema dos Compradores e Vendedores e suas Repercussões

Nesta Capítulo exploraremos o problema focal desta Tese, o Dilema dos Compradores e Vendedores (DCV) como principal fragilidades por trás da virtualização de informações do mundo real sem uma autoridade certificadora confiável. Observaremos também suas implicações em mercados descentralizados, outros problemas que representam desdobramentos do mesmo dilema, como o Problema da Ação Coletiva, ou Preço da Anarquia, além de estabelecer o conceito de transação não-verificável e apresentar teorias por traz destes dilemas, suas causas e consequências.

3.1 Operações *Off-chain* não Validáveis

A partir da revisão da literatura descrita no Capítulo 2 identificou-se o problema da validação de transações *off-chain* com um dos principais entraves para a utilização do paradigma descentralizado em serviços voltados ao consumidor. Transações *off-chain* são aquelas onde a transferência do valor ocorre fora da *blockchain* (a entrega de um produto ou serviço, por exemplo). Tal dificuldade se mostra mais desafiadora em sistemas anônimos, públicos e/ou envolvendo operações do mundo real como serviços manuais ou pagamentos em dinheiro [111, 238, 156].

Chiu e Koeppl [52] estão entre os primeiros autores a propor um modelo de *blockchain* com alguma política de verificação da parte *off-chain* da transação. Contudo, Butterink [39] antes deles, propôs uma solução para o problema da virtualização descentralizada de informação assimétrica baseada no conceito de *Schelling Points* (Pontos de Exclamação, em inglês). Trata-se de validar informações externas na forma de uma acareação. Um grupo de participantes que não se conhecem dão depoimentos simultaneamente, os participantes que conseguirem prever a informação que vencerá o consenso são remunerados – como em um interrogatório policial, supondo que a informação que mais se repete seja a verdade. São muitos os problemas desta solução, como a necessidade de ter vários participantes conhecedores do fato, o que é inviável em muitos cenários.

Karaivanov [130] traz os fundamentos do problema da distância entre tecnologias descentralizadas e mercados envolvendo informações não verificáveis – informação assimétrica. Estendendo o trabalho de Karaivanov, no Capítulo 2 foi feito um levantamento exploratório na literatura a respeito dos avanços em tecnologias descentralizadas que aproximem DAX envolvendo transações com informação assimétrica a configurações de mercado incompletas – aqui configuração de mercado incompleta refere-se a mercados envolvendo transações difíceis de verificar. Dentre os resultados mais significativos, apontou-se a virtualização de informação do mundo real como um dos principais obstáculos à popularização de DAX entre os consumidores.

Com base no que foi pesquisado, a literatura ainda carece de um mapeamento dos motivos pelos quais o potencial disruptivo do DAX ainda permanece tão distante da sociedade. No entanto, trabalhos anteriores fizeram contribuições importantes para esse propósito [104, 130, 225, 227, 108, 14, 196, 153, 188]. Esta Seção estabelece o conceito de transação não verificável que será utilizado a partir daqui.

3.1.1 Definição

Uma transação pode ser vista como um protocolo estruturado composto por uma série de operações que facilitam a troca de valores entre duas partes: um iniciador ativo e um respondedor passivo. Contudo é comum estarmos falando de um pagamento em valor monetário e uma entrega de produto ou serviço. Existem vários meios de virtualização da operação de pagamento. Contudo a operação de entrega do produto ou serviço nem sempre pode ser vir-

tualizada, ou tal virtualização demandaria um custo incompatível com o custo da operação. Por exemplo, serviços como massagem, lavagem de carro, guia turístico, instrutor musical, e produtos como frutas, artesanato, animais vivos, etc.

A série perfeita de operações que compõe uma transação é denominada *atomic swap* (troca atômica). No contexto das TLRDs, este termo foi usado pela primeira vez por Nolan [197] no fórum da rede Bitcoin e que tem sido amplamente usada para operações *off-chain* verificáveis, especialmente em transações *cross-blockchain*, como trocas descentralizadas entre diferentes criptomoedas [265].

Definição 1 (Atomic Swap)**.** *Uma dada transação σ é considerada uma Troca Atômica quando para sua sequência de operações $\sigma = \{b_0^\sigma, b_1^\sigma, b_2^\sigma, b_t^\sigma\} \mid t \in \mathbb{N}^+ \Rightarrow b_t^\sigma = b_*^\sigma$. Ou seja, tomando b_t^σ como o resultado final e b_*^σ como o resultado final ideal, em uma troca atômica $b_t^\sigma = b_*^\sigma$. Isto é, o resultado final é sempre igual ao resultado final esperado [28].*

Em resumo, uma transação pode ser considerada um *atomic swap* se e somente se todas as operações que a compõem possam ser revertidas com segurança em caso de falha. Embora o Atomic Swap Descentralizado já tenha se mostrado uma solução capaz de resolver problemas como transações *cross-chain* de forma descentralizada no contexto de operações verificáveis, quando se trata de operações não verificáveis – por exemplo, qualquer problema envolvendo valores não virtualizáveis – não é possível haver *atomic swap* uma vez que não se pode comprovar que todas as operações foram realizadas, ou desfeitas em caso de falha.

3.1.2 Relevância

O Capítulo 2 realizou uma revisão exploratória da literatura que buscou mapear o domínio das aplicações descentralizadas voltadas ao consumidor. Tal revisão apontou a virtualização descentralizada de eventos do mundo real como um dos pontos mais relevantes. Esta Tese tomou este ponto como caminho de investigação, restringindo o foco para o contexto de transações de compra/venda envolvendo operações não-verificáveis.

Assim, esta Tese visa atingir um limar de risco aceitável em transações de compra/venda descentralizadas e não verificáveis, o que abrange boa parte das transações realizadas no dia a dia das pessoas. Este objetivo tem o potencial de empoderar o consumidor, concedendo-lhe autoridade sobre seus dados e recursos e eliminando o desequilíbrio naturalmente associado a

mediação centralizada. Esta, por sua vez, concede uma vantagem injusta a autoridade central. Exemplos desta relação injusta incluem os juros abusivos cobrados por bancos para conceder empréstimos lastreados no próprio capital dos usuários a quem o banco empresta este mesmo capital, embora as autoridades governamentais, garantias retidas e autoridades de proteção ao crédito tornem esta operação relativamente segura. Outro exemplo do desequilíbrio por trás da centralização de autoridade está na cobrança excessiva e obrigatório de impostos, mesmo que frequentemente estes valores não tenha um destino muito claro.

3.2 O Problema da Ação Coletiva (PAC)

Um Problema de Ação Coletiva (PAC, doravante), também chamado de Dilema Social [68, 180, 205, 268], é uma situação em que todas as partes participantes estariam melhor cooperando entre si, mas não conseguem fazê-lo devido a interesses conflitantes entre as partes individuais [38, 98, 10].

A definição de um PAC hoje deriva mais intimamente do livro de Mancur Olson de 1965, The Logic of Collective Action [230]. A ideia principal que Olson promoveu foi que quando a defesa do bem comum, por algum ganho comercial/egoísta, estimular interesses individuais, então não será necessariamente benéfico para o coletivo. O oposto também é crítico, quando os membros do grupo escolhem perseguir interesses individuais às custas dos interesses do grupo. Isso pode ser melhor compreendido por meio de uma análise teórica de jogos e pode ser usado para explicar o esgotamento de recursos, baixa participação eleitoral, superpopulação e inúmeras outras preocupações de colaboração entre humanos enfrentadas hoje.

3.2.1 Contexto histórico

Os problemas de ação coletiva podem assumir muitas formas e foram estudados em várias disciplinas ao longo da história, como psicologia, economia e ciência política.

O dilema do prisioneiro, discutido por Rapoport [220], ilustra o conflito entre interesses individuais e coletivos e é crucial para entender problemas de ação coletiva [264] porque ilustra perfeitamente a afirmação de Olson de que interesses individuais entram em conflito com interesses de grupo. Nele, dois acusados de um crime, separados em salas distintas, de-

vem decidir se testemunham contra o outro. Se o jogador "A" testemunhar contra o jogador "B", então o jogador "A" vai para casa livre enquanto o jogador "B" recebe uma sentença pesada e vice-versa. Se ambos os jogadores testemunharem um contra o outro, ambos receberão sentenças pesadas, mas se ambos ficarem quietos, ambos cumprirão uma sentença muito mais curta. Parece óbvio que ambos os jogadores devem simplesmente escolher ficar quietos. No entanto, como os jogadores não conseguem se comunicar e não se importam com os interesses um do outro, sempre escolherão testemunhar contra o outro jogador. A escolha egoísta de ambos resulta em penalidades pesadas, mas uma solução mais cooperativa levaria a sentenças mais leves. A ausência de comunicação e o interesse individual são decisivos para essa escolha.

Esse modelo é uma simplificação e em situações com muitos jogadores, o dilema da ação coletiva assume sua real complexidade. Alguns teóricos ilustraram as razões humanas por traz do problema da ação coletiva. A teoria do gene egoísta [69, 112, 102], por exemplo, sugere que a cooperação pode surgir se beneficiar a sobrevivência dos genes. Já a teoria da aptidão inclusiva afirma que membros da família cooperam para favorecer os genes compartilhados, enquanto a reciprocidade (através da punição) também pode explicar a cooperação em jogos repetidos. Porém, a Teoria dos Jogos assume que indivíduos se preocupam apenas com seus próprios interesses econômicos. Já teorias psicológicas, como a Teoria da Interdependência, argumentam que os relacionamentos pessoais podem mudar a dinâmica da cooperação. A Teoria da Expectativa de Objetivos [278] afirma que a cooperação é mais provável se os jogadores acreditarem que os outros também cooperarão. Além disso, a Teoria da Adequação, por sua vez, propõe que as pessoas não calculam suas escolhas com base em maximização racional, mas usam heurísticas e normas sociais, como a regra da igualdade, para decidir: "O que alguém como eu faria nesta situação?" [269, 144]. Isso também reflete a teoria da racionalidade limitada.

Embora modelos econômicos tradicionais assumam que os indivíduos buscam apenas seus próprios interesses, evidências sugerem que as pessoas também buscam o bem-estar dos outros, como visto nas doações de caridade. Normas sociais, como a honestidade, podem ser fundamentais, pois quando indivíduos se conhecem e confiam uns nos outros, a mentira perde seu valor como estratégia [249, 234]. Jogos como o dilema do prisioneiro, quando repetidos várias vezes, mostram que a cooperação tende a ser a estratégia dominante quando

as pessoas formam vínculos.

A cooperação também pode ser motivada por normas de justiça e igualdade, com um forte vínculo em comunidades unidas [113]. Além disso, estudos mostram uma correlação entre confiança e eficiência econômica, sugerindo que a confiança não depende apenas de laços interpessoais, mas também de instituições [129, 115].

3.3 O Preço da Anarquia

A teoria dos jogos é usada para estudar situações que envolvem agentes racionais (egoístas) que são motivados pela otimização de suas próprias utilidades em vez de atingir algum ótimo social. Se não houver uma autoridade central que possa impor o comportamento desejado aos agentes individuais, o ótimo social normalmente não será alcançado, e alguma perda social é inevitável.

Quantificar a perda de eficiência devido ao comportamento egoísta é uma preocupação natural em tais cenários. Koutsoupias e Papadimitriou [146] propuseram analisar tal ineficiência de uma perspectiva do pior caso, quantificando seu custo como a razão entre a melhor solução possível alcançada com agentes invariavelmente egoístas e o ótimo social. Para formalizar essa métrica, é preciso definir o que constitui comportamento racional, ou aceitar um conceito pré-existente, e custo social. Koutsoupias e Papadimitriou tomaram o custo social como a soma do custo de todos os jogadores. Koutsoupias e Papadimitriou escolheram também o equilíbrio de Nash, que é talvez o conceito de equilíbrio estratégico mais popular usado na literatura, como comportamento racional. Em um equilíbrio de Nash (NE) [193], nenhum agente pode melhorar sua própria utilidade alterando unilateralmente sua ação. O preço da anarquia, portanto, quantifica a perda de eficiência incorrida em cenários onde desvios coordenados não podem ocorrer.

Papadimitriou [207] mais tarde cunhou o termo Preço da Anarquia (do inglês Price of Anarchy, PoA doravante) para denotar essa razão entre o equilíbrio de Nash no pior caso e o ótimo social. Este conceito altamente bem-sucedido e influente é frequentemente considerado a medida padrão da potencial perda de eficiência devido ao egoísmo individual, quando os jogadores estão preocupados apenas com sua própria utilidade e não com o bem-estar social geral.

Koutsoupias e Paradimitriou [147] consideram ainda um modelo simples de roteamento de rede onde o PoA é mostrado como $\geq 1/3$. Isso significa que a falta de coordenação entre os agentes leva a uma perda de desempenho de 33% em comparação com a configuração ótima na qual os agentes se coordenam.

3.3.1 Mercados e PoA

Os Mercados regulam a anarquia se valendo da escassez da moeda, mas o egoísmo dos competidores de livre mercado e o acúmulo de incentivos (moeda) entre poucos causa ineficiência. Contudo, a prática demonstra que os Mercados são provavelmente a melhor e mais poderosa solução até o momento, porque fazem com que as pessoas se coordenem, já que o incentivo (dinheiro) é muito forte. Eles são particularmente poderosos porque atuam como uma função de criação e coordenação de informações do sistema de preços, ou seja, os preços geram informações sobre preferências e escassez (que de outra forma seriam muito difíceis de coletar) [116].

3.3.2 PoA e Precificação

O valor do dinheiro é medido em termos do que ele representa em média para a sociedade. Contudo, mil dólares representam muito mais para quem ganha $100.000 dólares por ano do que para quem ganha $1.000.000 de dólares. Assim, o valor da moeda é medido por sua liquidez, que corresponde à sua demanda na sociedade, e não pelo sacrifício empregado para obtê-la ou pela necessidade do indivíduo. Embora tal estratégia de precificação baseada em competição e não em colaboração tenha uma taxa de sucesso aceitável, afinal é a base do conceito de livre mercado, na prática gera uma ineficiência que costuma custar até mesmo vidas humanas. Por exemplo, $100.000 dólares são muito mais valiosos para um paciente com câncer em tratamento do que para alguém saudável e sem custos de saúde.

A maioria das coisas é boa ou ótima para alguns e insuficiente para outros, e isso pode ser medido com base na quantidade de sacrifício que uma pessoa está disposta a fazer. A ideia de ser capaz de medir e comparar sacrifícios pressupõe que os sacrifícios podem ser valorados objetivamente. Também pressupõe que o sistema de agregação de sacrifícios sobre toda a população o faz de uma maneira que valoriza com precisão a percepção de cada indivíduo

sobre o valor de seu sacrifício. Essa ideia geralmente atrai mais críticas quando a quantidade de sacrifício é medida em termos de dólares. Voltaremos a discutir este tema no Capítulo 6.

A Finlândia tem um sistema muito interessante de multas com preços dinâmicos com base nos níveis de renda [216]. Mas, ao mesmo tempo, $10.000 são $10.000 e não importa de onde o dinheiro venha esses $10.000 ainda farão a mesma quantidade de bem. Então, há um valor objetivo para o que o dinheiro é capaz de fazer, apesar de provavelmente ter um valor muito maior para alguns do que para outros.

3.4 O Dilema dos Compradores e dos Vendedores

A presente tese se concentra no caso derivado, mais simples e particular de aplicação dos conceitos por trás dos conceitos de PAC e PoA, o Dilema dos Compradores e dos Vendedores (DCV), onde a falta de colaboração entre comprador e vendedor pode colapsar um modelo de mercado, sobretudo em um ambiente anônimo e descentralizado envolvendo transações não verificáveis. Contudo, ao final deste documento apresentaremos uma solução capaz de resolver não apenas o DCV, mas também o PAC e minimizar o PoA de forma ampla, sendo mais eficiente em segurança e custo que suas concorrentes na literatura.

Considere que uma transação pode ser vista como um protocolo composto por uma série de operações que estabelecem uma troca de valores de diferentes naturezas envolvendo duas partes, uma parte ativa (comprador) que propõe a transação e uma parte passiva (vendedor) que a aceita ou rejeita. No entanto, uma das partes – a parte ativa – geralmente deve assumir o risco e realizar a operação de transferência de valor antes que a parte passiva responda com sua contraparte. Neste ponto, esta parte passiva tem a chance de agir desonestamente e não prosseguir com a transação. A decisão de assumir tal risco é conhecida como Dilema dos Compradores e Vendedores [20].

De acordo com Anderson [15], as normas de mercado têm as seguintes cinco características: são impessoais (independentes do relacionamento e dos fins da outra parte), egoístas (o objetivo é satisfazer os interesses pessoais), exclusivas (as pessoas podem ser excluídas), voltadas para o desejo (em oposição a responder às necessidades objetivas) e orientadas para a "solução" em vez da "opinião" (em vez de expressar a reclamação, busca-se uma alternativa). Surpreendentemente, a estratégia de equilíbrio de Nash é, na verdade, jogada apenas

por alguns jogadores, alguns tendem a ser muito mais otimistas e altruístas, enquanto outros seguem a risca as normas de Anderson e jogam para "ganhar". Algumas observações interessantes incluem o fato de que em testes de uma só jogada e estágios iniciais de jogos repetidos, os sujeitos geralmente fornecem contribuições no meio do caminho entre o nível de eficiência de Pareto e o nível de carona. As contribuições na verdade diminuem com a repetição (conforme os jogadores aprendem a jogar com o sistema) e a comunicação melhora a taxa de colaboração [158].

Uma solução conhecida para o Dilema dos Compradores e Vendedores – que é o problema de negócios de interesse aqui – é a mediação de uma terceira parte centralizada que valida as operações e deve contar com a confiança das outras partes. Esta solução tem funcionado o suficiente em mercados centralizados onde o Estado, uma casa de câmbio, uma aplicação centralizada ou uma instituição bancária desempenham o papel de intermediário, garantindo a entrega da contraparte do passivo. Soluções anteriores para o Dilema dos Compradores e Vendedores em mercados descentralizados geralmente incorporam pré-condições custosas que garantem a verificação de todas as operações ao longo do protocolo de transação, o que não é viável para aquelas transações onde qualquer operação envolvida é não verificável – por exemplo, serviços do mundo real ou pagamentos em dinheiro. Exemplos de pré-condições custosas incluem sincronização de operações [174, 258], garantia de confiança em qualquer uma das partes envolvidas [20, 155], conteúdo digital controlável [285, 187, 219] e protocolos de pagamento voltados para produtos com autenticidade verificável digitalmente [206].

3.4.1 Definição Formal

O Dilema dos Compradores e dos Vendedores (BSD), termo usado originalmente no livro Prisoners' Dilemma [220], é um problema de corrida entre jogadores desonestos envolvidos no estabelecimento de um comércio baseado em duas operações (pagamento e transferência de produto, por exemplo), ambas com vantagens em direções opostas. Tal transação é um jogo não equilibrado, pois cada parte tende a cuidar de seus próprios interesses traindo a outra parte, uma vez que isto ofereça o resultado mais vantajoso.

Em um cenário de negociação, por exemplo, uma transação de comércio eletrônico, é natural que cada parte priorize seus próprios interesses, fazendo com que um comportamento

desonesto seja percebido como uma opção vantajosa, pelo menos no curto prazo (no longo prazo, é provável que a lei alcance os agentes desonestos). Esta situação configura o DCV que é baseado na expectativa de que o jogador passivo sempre preferirá agir desonestamente, e o motivo é descrito abaixo.

Tal cenário reflete o princípio do Equilíbrio de Nash da teoria dos jogos [193], onde há uma estratégia a ser seguida por um jogador para sempre garantir o melhor resultado possível em um cenário não colaborativo, ou seja, não importando as estratégias do outro jogador. Essa estratégia 'segura' é o ponto de Equilíbrio de Nash. Portanto, o problema de interesse aqui pode ser formulado como um jogo como em Definição 2.

Definição 2. *Considere um Dilema de Compradores e Vendedores como a seguinte tupla* $G = \{P, Q, T, (b_0, b_*), (\lambda_i(b) \,|\, i \in Q, b \in Q^P), (\gamma^t(b_k(i), b_l(j)) \,|\, \forall_{b_k,b_l} \in P \text{ , e } \forall t \in T \; \forall i, j \in Q)\}$*, onde:*

1. P *significa a coleta de valores ou produtos trocados dentro do jogo.*

2. Q *representa o grupo de agentes envolvidos em negociações, normalmente consistindo de dois agentes (por exemplo, comprador e vendedor* $B, S \in Q$*), embora possamos generalizá-lo para* $|Q|$ *para maior flexibilidade.*

3. T *referenciadores para todos os passos de tempo.*

4. $(b_0, b_*) : P \times Q$ *representa o conjunto inicial de valores* b_0 *(por exemplo, para o vendedor o conjunto original de valores é o produto/serviço para vendas* $y \in P$*, e para o comprador o conjunto original de valores é o pagamento em dinheiro* $x \in P$*) e o conjunto final esperado de valores* b_* *(por exemplo, novamente para o vendedor, o conjunto final de valores seria o pagamento em dinheiro do comprador em caso de sucesso da transação) para um determinado agente comercial. Aqui,* b_k *significa o estado de um agente no tempo de vida* k*, é igual ao passo de tempo* t *menos o tempo de criação do agente.*

5. $\lambda_i(b)$ *é uma função de interesse de um determinado agente* $i \in Q$ *sobre um conjunto de valores* $b \in Q^P$ *tal que:* $\lambda_i(b_0(i)) \leq \lambda_i(b_*(i)), \forall i$ *(ou seja, todo agente* i *sempre preferirá seu conjunto final esperado de valores ao conjunto inicial) e* $\lambda_i(b_*(i)) \leq$

$\lambda_i(b_0(i) \cup b_*(i)), \forall i$ *(ou seja, todo agente preferirá agir desonestamente e acumular tanto o conjunto final esperado quanto o conjunto inicial de valores).*

6. *A estratégia (operação)* $\gamma^t(b_k(i), b_l(j)) = (b_{k+1}(i), b_{l-1}(j))$*. Tal estratégia estabelece que sempre que um jogador sai de um estado pior* $b_k(i)$ *para um melhor* $b_{k+1}(i)$*, outro agente deve necessariamente fazer o caminho inverso, saindo de um estado melhor* $b_{k+1}(j)$ *para um pior* $b_k(j)$ *a cada operação,* $\lambda(b_k) < \lambda(b_{k+1})$*. Isso significa que o jogador ativo precisa arriscar voltar atrás em seu saldo para iniciar uma transação com a intenção de melhorá-lo ao final desta transação.*

Na definição 2 descrita acima e representado na Figura 3.1, concluir a negociação é impossível, pois é vantajoso para o comprador (B) nunca pagar (transferir x) pelo produto/-serviço (y), levando o vendedor (S) a não entregá-lo. Se o comprador (B) não pagar pelo produto, ele pode ficar com apenas o valor do pagamento x ou o valor do pagamento x e o produto/serviço y (se o vendedor S entregar o produto/serviço y mesmo que ele ainda não tenha sido pago). Se o comprador B pagar pelo produto/serviço y adiantado, ele ainda pode receber o produto/serviço y do vendedor S, mas corre o risco de ficar sem nada. O vendedor S, se não enviar o produto (transferir y), pode ficar com apenas o produto/serviço y ou o produto/serviço y e o valor do pagamento recebido x; se enviar, ele ainda pode ficar com o pagamento recebido x, mas corre o risco de ficar sem nada. Nas possibilidades descritas, é sempre mais vantajoso ser desonesto ou sequer iniciar a transação. No Anexo A.1 apresentamos a prova forma do equilíbrio de Nash na estratégia desonesta, conforme acabamos de descrever.

A responsabilidade mútua e a presença de intermediários como eBay e Amazon, que por alguma vantagem reembolsam o comprador em caso de não entrega de bens pagos, garantem a segurança em mercados centralizados, apesar do DCV. No entanto, as repercussões legais ou intermediários de confiança centralizados dependem da verificação de todas as operações e da centralização da autoridade, condições que as soluções descentralizadas da literatura tentam contornar.

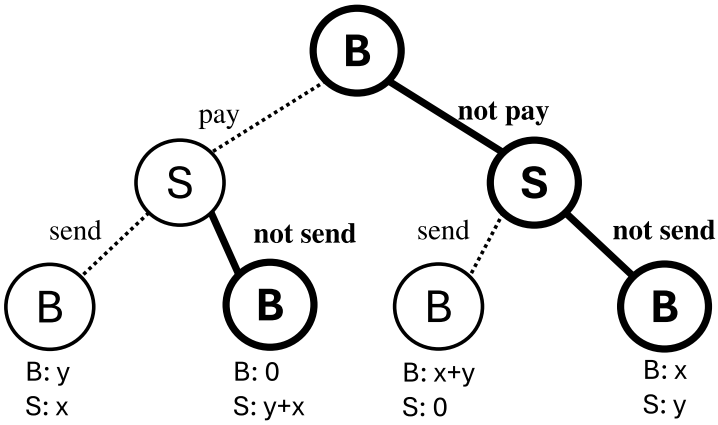


Figura 3.1: Representação do DCV descentralizado como um jogo extensivo. Os caminhos dominantes são destacados. Observa-se que a estratégia dominante sempre representa melhores resultados para o jogador, comprador (*buyer*, B) ou vendedor (*seller*, S)

3.5 Sumário do Capítulo

A seguir apresentam-se definições essenciais para a compreensão dos próximos Capítulos. São introduzidos conceitos fundamentais, como transações atômicas e não-atômicas, Preço da Anarquia (PoA), Problema da Ação Coletiva (PAC) e, por fim, o Dilema dos Compradores e Vendedores (DCV), tema central desta Tese.

- **Transação atômica** [197, 28]: uma transação onde todas as suas operações podem ser confirmadas ou revertidas em segurança e portanto, verificadas. Isto, por associação, define o conceito de transação não-atômica ou não-verificável, seu oposto. Onde qualquer uma das suas operações não pode ser confirmada ou revertida sem o auxílio de um mediador confiável. Pagamentos por meio eletrônico e transações de banco de dados são exemplos de transações atômicas ou verificáveis. Pagamentos em dinheiro, trocas e prestações de serviços físicos são exemplos de transações não atômicas ou não verificáveis.

- **Preço da Anarquia (PoA)** [207]: Trata-se do fator que define a ineficiência de uma transação não colaborativa e que quantifica o prejuízo causado pelo DCV.

- **Problema da Ação Coletiva (PAC)** [68, 180, 205, 268]: Em cenários onde todos os agentes buscam seus próprios interesses, os mesmos tendem a negligenciar os interes-

ses dos demais e até mesmo os interesses comuns. Em certos casos até sabotando o interesse comum em benefício dos seus objetivos egoístas.

- Por fim, definiu-se formalmente o conceito de **Dilema dos Compradores e Vendedores (DCV)**, problema central desta Tese, como um desdobramento do Dilema do Prisioneiro.

Capítulo 4

Análise da Mediação como Solução Centralizada para o DCV

Neste Capítulo exploramos a mediação confiável em transações comerciais como principal solução centralizada para o Dilema dos Compradores e Vendedores (DCV). Tal solução tem sido validada desde o surgimento do comércio eletrônico na maioria dos aplicativos dedicados a esta atividade. Seus pontos positivos e negativos são aqui destacados sob a ótica do usuário com base em *feedback* de aplicativos em lojas de software. Como contribuição para esta Tese observou-se que embora esta solução apresente uma eficácia aceitável, também admite uma significativa margem de risco.

4.1 Introdução

No desenvolvimento e evolução de software, o contato com o cliente e o *feedback* do usuário são ferramentas importantes. No entanto, em aplicativos voltados para o consumidor, o cliente é mais uma abstração do que parte do processo de desenvolvimento. Nesse contexto, o *feedback* do usuário é a única ferramenta para adaptar o software às demandas do usuário/-cliente [57, 123]. Felizmente, lojas de aplicativos como Google Play Store [1] e Apple Store [2] fornecem um espaço para que usuários avaliarem esses aplicativos (apps). Essas informações podem ser um aliado muito relevante no desenvolvimento e manutenção de um aplicativo e

[1] `https://play.google.com/`

[2] `https://www.apple.com/`

sua interface de usuário.

O *feedback* do usuário é especialmente útil em aplicativos do tipo *marketplace*, que envolvem operações sensíveis, como mediação entre compradores e vendedores. Um *marketplace* é um sistema cujo propósito é conectar compradores a vendedores, oferecendo um serviço de mediação durante toda a transação que varia de aplicativo para aplicativo e pode envolver apenas a intermediação de pagamento ou incluir também todo o processo de logística de entrega.

Em teoria, tal serviço torna a transação comercial online atômica [197], o que seria suficiente para garantir a segurança. No entanto, na prática, problemas com as atividades reais das partes ao longo do processo podem fornecer oportunidades para usuários mal-intencionados. A falta de clareza sobre o que a plataforma é responsável e o que os vendedores terceirizados são responsáveis é um exemplo de ruído que pode confundir os compradores. Problemas como esses comprometem a reputação do aplicativo, levando muitos usuários a abandonar o aplicativo e até mesmo o e-Commerce como um todo [6].

Durante o desenvolvimento de aplicações que envolvem transações financeiras, muitos aspectos associados à experiência do usuário são avaliados, como confiabilidade [284, 224, 137], acessibilidade [11, 83, 83, 231, 76] e satisfação [217, 135, 160, 6, 202]. No entanto, até onde pesquisamos, poucos estudos analisaram a confiabilidade do aplicativo sob a perspectiva do próprio usuário [137], e não foi identificado nenhum estudo que analise diretamente a confiabilidade do aplicativo e a satisfação do usuário com relação ao processo de mediação em transações dentro de aplicativos do tipo *marketplace*. Yun Kyung e Jung Min [202] relatam falhas na mediação de transações como uma das principais fontes de insatisfação entre os usuários, com base em avaliações de aplicativos móveis de instituições bancárias. Entretanto, não buscam diagnosticar diretamente falhas de usabilidade ao longo do processo de mediação.

Neste Capítulo apresentamos uma análise de dados sobre o processo de mediação entre compradores e vendedores em aplicativos do tipo *marketplace* sob a perspectiva do próprio usuário, coletados de avaliações de aplicativos extraídas da Play Store do Google. Além disso, também focamos em falhas de comunicação entre o aplicativo e seu usuário durante todo o processo de mediação de transações. Elementos que poderiam ser explorados por usuários mal-intencionados – por exemplo, interface do aplicativo, email ou mensagens de

texto – também foram mapeados durante todo o processo de mediação. Embora existam trabalhos que analisem avaliações de usuários relacionados à confiança [137], ou que estudem avaliações por motivos de insatisfação de forma mais ampla [202, 135, 160], não encontramos estudos sobre o processo de mediação em transações da perspectiva do usuário.

Estudar as queixas dos usuários, seus *feedbacks* e opiniões a respeito do processo de mediação nos leva a entender as dificuldades por trás da virtualização do que acontece no mundo real. Faz-se isto pois é por meio da interface e da usabilidade que os eventos e fatos do mundo real são virtualizados. Assim, este estudo contribui para esta Tese ao levantar fragilidade e pontos positivos de uma solução para o DCV que já funciona ativamente todos os dias – a mediação centralizada de transações.

Baseamos nossa investigação em um conjunto de dados publicado por Maqbool et al [175] de aproximadamente 19,3 milhões de avaliações de usuários na Play Store do Google, sobre mais de 10.000 aplicativos, dos quais 29.000 são sobre aplicativos do tipo *marketplace*. A investigação é estruturada em torno de cinco questões de pesquisa:

QP1: Quantas críticas à mediação estão vinculadas a elementos de comunicação entre aplicativo e usuário? Aqui, pretendemos entender com que frequência os usuários dão *feedback* sobre a comunicação de mediação comparada ao *feedback* sobre mediação de forma genérica e qual é a natureza desse *feedback*.

QP2: Quais componentes e recursos da interface tendem a gerar mais *feedback* entre as avaliações? Aqui, pretendemos reunir evidências para apontar os componentes e os elementos de usabilidade da interface que mais interferem no serviço de mediação.

QP3: Quais são os principais problemas críticos na mediação e que são relatados nas avaliações dos usuários? Buscamos identificar os problemas principais e como eles estão associados à comunicação ao longo do processo (por exemplo, falta de clareza ao comunicar a responsabilidade pelo envio, seja da plataforma ou do vendedor).

QP4: Quais são as principais ações tomadas pelos usuários devido ao serviço de mediação que eles relatam nas avaliações do aplicativo? Nosso objetivo é fornecer evidências das consequências práticas da usabilidade ruim junto ao processo de mediação. Por exemplo: “o vendedor me pediu para pagar fora da site, achei estranho, mas o aplicativo de pagamento também é de <name>, então aceitei, mas nunca recebi meu pedido”(tradução).

QP5: Quais níveis de insatisfação uma mediação inadequada pode causar nos usuários?

Tal insatisfação pode levar a qualquer coisa, desde a simples desinstalação do aplicativo até ameaças/ações legais e o desejo de tornar públicas informações sobre tais elementos.

Conhecer e entender os danos causados por falhas na mediação ao usar vendedores terceirizados é relevante, pois aborda uma falha de segurança que não diz respeito a precauções da equipe de segurança, mas a precauções de segurança relacionadas ao design da interface do aplicativo. As principais descobertas apresentadas neste Capítulo incluem evidências de que a falha na comunicação de responsabilidades cria uma falta de clareza no serviço de mediação de transações, o que pode ser a principal fonte de oportunidades para usuários mal-intencionados. Além disso, com base em relatos de experiências negativas, podemos concluir que a maioria dos casos de fraude poderia ser evitada tendo um processo de comunicação funcionando adequadamente em todo o serviço de mediação de transações. Também listamos elementos que comunicam o processo de mediação de forma errada, fornecendo *insights* sobre quais medidas devem ser tomadas. Para além das contribuições feitas a esta Tese, os estudos deste Capítulo contribuem para o design, implementação, execução e gerenciamento da interface do usuário de aplicativos de *e-commerce* do tipo *marketplace*.

O estudo apresentado neste Capítulo está disponível também na forma de um artigo científico [3], sendo selecionado entre os artigos para terem uma versão estendida publicada em Journal on Interactive Computing. A presente pesquisa aborda a eficácia da principal solução centralizada para o DCV mediante transações não verificadas, mostrando que, embora esta tenha se mostrado eficaz o suficiente para sustentar o modelo de comércio online moderno, ainda apresenta múltiplos problemas. Os resultados expostos neste Capítulo mostram que as soluções descentralizadas para o mesmo problema apresentadas e comparadas nos Capítulos 5.3, 5.4 e 6 também tem condições de resolver o mesmo problema de forma igualmente satisfatória.

Este Capítulo está dividido da seguinte forma. A Seção 4.2 traz uma revisão de trabalhos relacionados na literatura que têm alguma conexão com o presente, seja em termos de métodos, objetivos ou resultados. A Seção 4.3 descreve o desenho do presente estudo e o método por trás dele. A Seção 4.4 apresenta os resultados obtidos aqui; também descreve

[3]Publicado no XXIII Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais (acesse `https://ihc.sbc.org.br/2024/`), Qualis A3, e disponível no em `https://dl.acm.org/doi/abs/10.1145/3702038.3702095`

as ameaças à validade deste estudo e o que foi feito para mitigá-las. Por fim, a Seção 4.5 traz as conclusões que podemos tirar com base nos resultados e uma discussão sobre futuras direções de pesquisa.

4.2 Trabalhos Relacionados

Este estudo tem como objetivo identificar a insatisfação dos usuários com o processo de mediação de transações em aplicativos do tipo marketplace. Além disso, buscamos evidências sobre a natureza de tais insatisfações: se estão relacionadas ao processo de mediação em si, à falta de entendimento sobre o processo ou (histórico de) casos negativos. Portanto, esta seção apresenta estudos associados a esta pesquisa, seja por similaridades de método, objetivos ou mesmo conclusões que apontam na mesma direção das aqui apresentadas. Os critérios de seleção dos trabalhos da literatura a serem revisados são:

- Relevância: Seleção de estudos que se relacionaram direta ou indiretamente com o tema de pesquisa: a segurança do usuário sob sua própria ótica ao longo do processo de mediação em aplicativos do tipo *marketplace*;
- Alinhamento metodológico: inclusão de estudos com métodos de pesquisa, objetivos ou conclusões semelhantes que se alinhem com o foco do presente estudo: experiências do usuário em aplicativos do tipo *marketplace*;
- Contribuição: Consideração de estudos que ofereçam *insights* sobre falhas de comunicação, problemas de segurança ou insatisfação do usuário em aplicativos do tipo *marketplace*, com relação ao processo de mediação;
- Qualidade: Seleção de estudos com metodologias robustas, fontes de dados confiáveis e descobertas relevantes que contribuam para a compreensão das experiências do usuário em aplicativos do tipo *marketplace*.

Muitos pesquisadores investigaram a opinião do usuário relatada em avaliações pós-instalação sobre um aplicativo ou uma classe de aplicativos. Esses estudos geralmente estão associados a perguntas de pesquisa mais genéricas e com diferentes propósitos: i) caracterizar problemas de satisfação com base em relatos de usuários [83, 11]; ii) identificar casos de

fraude para melhorar o aplicativo [224, 284]; iii) analisar especificamente aplicativos bancários da perspectiva da satisfação, mas com conclusões referentes à segurança [202, 160]; ou iv) analisar diretamente problemas de segurança em aplicativos de pagamento [137, 135]. No entanto, até onde sabemos, não há estudos que investiguem diretamente o processo de mediação de transações em aplicativos do tipo *marketplace*, nem como esse processo é comunicado ao usuário. Em vez disso, existem vários estudos que investigam segurança e fraude em geral, causadas por falhas na comunicação do processo [224].

Ampliando o escopo da investigação para prevenção abrangente de fraudes, Zhang et al [284] trouxeram um mecanismo de detecção de fraudes que tem potencial para detectar falhas na comunicação de responsabilidade e clareza ao longo do processo de mediação, mas não forneceram detalhes dos resultados a esse respeito. Indo além, Rodrigues et al. [224] realizaram uma revisão da literatura sobre o método de detecção e prevenção de fraudes no comércio eletrônico que, embora contivesse trabalhos que apontassem falhas de usabilidade que podem levar à fraude, nenhum dos resultados buscou informações concretas sobre como evitar fraudes ou mesmo como fornecer mais clareza no processo de mediação investigando as opiniões dos usuários.

Khalajzadeh et al [135] usaram avaliações de aplicativos móveis para classificar e medir o que eles chamaram de problemas centrados no ser humano, entre eles a confiabilidade em aplicativos de comércio eletrônico como uma classe de problema centrado no ser humano. No entanto, não fez contribuições concretas para melhorar o processo de mediação de transações. Leem e Eum [160] analisaram avaliações de aplicativos bancários com base em técnicas de mineração de opinião. O trabalho de Leem e Eum na verdade visa detectar reclamações de clientes em avaliações online, que ofereceram *insights* sobre problemas encontrados pelos usuários. Entre os problemas, havia elementos gráficos que causaram preocupações quanto à segurança das transações.

Tomando a confiabilidade como uma superclasse na qual a confiança estava incluída no processo de mediação de transações, Al-Shamaileh e Sutcliffe [6] realizaram uma pesquisa onde entrevistaram usuários sobre o motivo pelo qual eles baixam ou abandonam aplicativos. Uma das causas do abandono foi a falta de confiança associada a casos de fraudes causadas por terceiros e avaliações negativas a esse respeito, o que reforça a necessidade de mensurar os elementos que levam a tais fraudes. Analisando a segurança de forma mais ampla,

Taylor e Martinovic [250] investigaram os impactos que a evolução do software pode ter na segurança, entre outros aspectos, descobrindo que os aplicativos na plataforma Android não melhoram sua segurança à medida que são atualizados; pelo contrário, alguns até aumentam o número de vulnerabilidades após atualizações. Kishnani et al [137] também realizaram uma análise de segurança em aplicativos móveis com base em dados coletados de avaliações de aplicativos, mas estritamente associados a pagamentos online. Os resultados apontaram diversas falhas de segurança ligadas aos certificados digitais, SSL e, entre elas, a usabilidade.

Oh e Kim [202] realizaram o estudo mais relacionado a este aqui. Com base em avaliações de aplicativos móveis de instituições bancárias e embora não tenham buscado diagnosticar diretamente falhas no processo de mediação, encontraram a insegurança na usabilidade como a principal fonte de insatisfação entre os usuários. E essa insegurança lida diretamente com falhas na mediação de transações, onde o usuário teme enviar dinheiro para pessoas erradas por não entender elementos da interface ou por imaginar que as informações podem acabar sendo usadas por usuários mal-intencionados.

Estudos que mapeamos na literatura relatam principalmente resultados que mostram a falta de confiança no aplicativo como um dos principais motivos para desinstalação [6], ou indicam elementos de usabilidade do processo de mediação que podem ser explorados por usuários mal-intencionados, ou mesmo indicam insatisfação dos usuários com a segurança do serviço como um todo. No entanto, nenhum desses trabalhos analisa as opiniões dos próprios usuários sobre o aplicativo com o objetivo de avaliar o impacto da falta de clareza na comunicação ou outros problemas ao longo do processo de mediação entre comprador e vendedor. O estudo realizado neste Capítulo oferece tais análises, além de apresentar uma metodologia baseada em análise de dados textuais totalmente automatizada e, portanto, mais replicável (do que inspeção manual ou entrevistas humanas), aplicável a vários outros cenários envolvendo conjuntos de dados textuais de opiniões de usuários. Para uma comparação mais visual, a Tabela 4.1 lista com mais detalhes as contribuições de cada trabalho revisado no contexto de nossas questões de pesquisa.

Tabela 4.1: Contribuições de cada trabalho relacionado no contexto de QPs. Nas colunas, listamos as principais contribuições deste trabalho: uma Metodologia Fácil de Replicar (MFR), com todas as etapas automatizadas (ou mesmo automatizáveis); o uso de um conjunto de dados Baseado em Revisões de Usuários (BDRU); Resultados Quantitativos (RQt); Resultados Qualitativos (RQl); contribuições para Usabilidade (U); contribuições para Segurança (S); e, contribuições para Mediação de Transações (MT).

Título e Referência	MFR	BDRU	RQt	RQl	U	S	MT
Accessibility issues in android apps: state of affairs, sentiments, and ways forward [11]		✓	✓		✓		
Do Android app users care about accessibility? An analysis of user reviews on the Google play store [83]		✓	✓	✓	✓		
efraudcom: An e-commerce fraud detection system via competitive graph neural networks [284]			✓		✓	✓	✓
What improves customer satisfaction in mobile banking apps? An application of text mining analysis [202]		✓	✓		✓	✓	
Supporting developers in addressing human-centric issues in mobile apps [135]		✓	✓	✓	✓		
Assessing Security, Privacy, User Interaction, and Accessibility Features in Popular E-Payment Applications [137]		✓	✓		✓	✓	✓
Using text mining to measure mobile banking service quality [160]		✓	✓	✓	✓	✓	
Why people choose Apps: An evaluation of the ecology and user experience of mobile applications [6]				✓	✓	✓	
To update or not to update: Insights from a two-year study of android app evolution [250]		✓		✓	✓	✓	✓
O presente estudo	✓	✓	✓	✓	✓	✓	✓

4.3 Desenho do Estudo

Este estudo considera avaliações de usuários de transações entre compradores e vendedores em aplicativos do tipo *marketplace*. A análise mapeia falhas nos processos revisados. Esta Seção apresenta o design do estudo realizado por meio da extração e análise de *feedback* de usuários sobre avaliações de aplicativos relacionadas à mediação (falhas) em tais transações e a comunicação de responsabilidades devidas em caso de falhas. A partir daqui, chamaremos esse *feedback* de avaliações de mediação. A Figura 4.1 ilustra as principais etapas do nosso método de pesquisa: Primeiro, a Filtragem de Dados foi realizada com base em metadados; então o resultado é usado na Inspeção Manual com base na validação cruzada entre avaliação humana e LLM. Antes da inspeção, QP1 e QP2 são respondidos com base em números preliminares. Em seguida, QP3 a QP5 são respondidos com base em consultas LLM usando a metodologia de *prompt* Chain-of-Thought (CoT) e a ferramenta ChatIE.

4.3.1 Metodologia

A metodologia utilizada por Dos Santos et al [76] e aqui adaptada pode ser resumida da seguinte forma:

Filtragem dos Dados: Este estudo usa o conjunto de dados MobileRec, consistindo de 19,3 milhões de avaliações gerais coletadas e classificadas por Maqbool et al [175]. O conjunto de dados inclui análises de mais de 10.000 aplicativos em 48 categorias, com foco em aplicativos do tipo marketplace de e-commerce. A filtragem de dados envolve a seleção de avaliações relacionadas ao processo de mediação de transações. Os critérios de inclusão se concentram em avaliações que relatam melhorias, críticas ou experiências negativas com o processo de mediação.

Inspeção Manual: Um processo de inspeção manual é então conduzido em 799 revisões para identificar problemas com a mediação de transações. Essa inspeção é realizada por um revisor humano e repetida por uma ferramenta baseada em um Large Language Model (LLM). Ao final do processo os resultados são comparados e devem coincidir de modo geral, com as eventuais exceções analisadas e elucidadas uma por uma para garantir a precisão e a confiabilidade dos resultados.

Análise de Dados: Pesquisadores analisam dados extraídos usando LLM, especifica-

mente ChatGPT-4, para extrair informações sobre funções de aplicativos, elementos de interface e segurança. Para melhorar o envio de dados, extração de informações e solicitações rápidas, usamos uma ferramenta personalizada chamada ChatIE, que se conecta ao ChatGPT por meio de APIs. O LLM foi escolhido por sua capacidade de entender, resumir e classificar dados de texto de forma eficiente.

Controle de Qualidade: Para mitigar o viés do pesquisador e aumentar a precisão, prompts foram projetados e são usados para orientar a produção do LLM. Além disso, o pesquisador humano reanalisa e sintetiza as informações produzidas pelo LLM para garantir a qualidade dos dados.

As principais diferenças entre a metodologia aqui utilizada e a de Dos Santos et al [76] consistem na utilização da ferramenta intermediária ChatIE e na utilização do LLM mesmo no processo de validação.

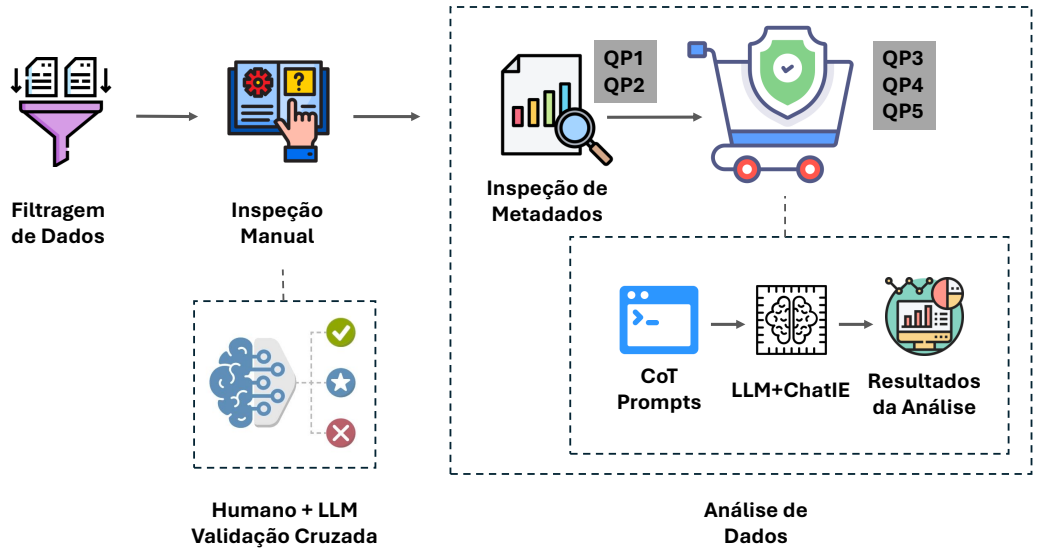


Figura 4.1: Infográfico de cada etapa da metodologia (onde LLM significa Large Language Model [286] e CoT significa Chain-of-Thought [76]).

4.3.2 Filtragem os Dados

Usamos dados de avaliações de usuários em geral e os filtramos, processamos e mineramos até chegarmos a dados de confiabilidade associados ao processo de mediação em aplicativos

do tipo marketplace.

As 19,3 milhões de avaliações gerais do MobileRec abrangem mais de 10.000 aplicativos de 48 categorias diferentes, envolvendo um total de aproximadamente $0,7$ milhões de usuários diferentes [175]. Antes de disponibilizar o conjunto de dados, por razões éticas, Maqbool et al fizeram um esforço para anonimizar os dados, ocultando a identidade dos usuários e qualquer entidade não relacionada ao aplicativo em análise. Cada um desses usuários interagiu com pelo menos cinco aplicativos distintos, o que contrasta com conjuntos de dados anteriores sobre aplicativos móveis que registravam apenas uma interação por usuário. Além disso, o MobileRec apresenta as classificações dos usuários, bem como os sentimentos sobre os aplicativos instalados, e cada aplicativo contém metadados ricos, como nome do aplicativo, categoria (por exemplo: redes sociais, comércio eletrônico, etc.), descrição e classificação geral, entre outros.

A filtragem dos dados ocorreu em três etapas: 1) Primeiramente, foram selecionados os aplicativos da categoria e-commerce; 2) depois, com base na descrição do aplicativo e em uma avaliação mais ampla em caso de dúvidas, foram selecionados apenas os aplicativos do tipo marketplace de e-commerce; 3) Em seguida, foi realizada uma filtragem analítica postagem a postagem pelo primeiro autor e posteriormente validada por meio de um LLM.

4.3.3 Inspeção Manual

De um total de 19,3 milhões de avaliações no banco de dados original do MobileRec, 29.000 pertencem a 64 aplicativos do tipo *marketplace*. Dessas 29.000, selecionamos para inspeção manual apenas as postagens de avaliação com mais de 100 caracteres – isso totalizou 799 comentários. Após o processo de análise manual com base no critério de aceitação, que estabelece que apenas avaliações relacionadas ao processo de mediação de transações devem ser aceitas, terminamos com 67 avaliações selecionadas.

Na primeira etapa, realizamos uma inspeção manual das 799 revisões neste conjunto de dados para identificar as revisões que relatam problemas com a mediação de transações. A inspeção manual foi realizada por um humano e uma ferramenta baseada em um Large Language Model (LLM), ChatGPT 4.0[4]: ambos analisaram todas as revisões e então compararam os resultados divergentes. Após a primeira inspeção, coube ao revisor humano verificar

[4]https://chatgpt.com/

os resultados para cada discordância. No total, três revisões tiveram que ser analisadas novamente (menos de 0,38% do total). Considere, por exemplo, a seguinte revisão de usuário que levou a um impasse: 'Sinto muito, mas quando você começou a delegar a função de vendas a alguém' (Mensagem). Neste caso, decidiu-se excluir a revisão porque, embora tenha trazido insatisfação, não se referiu a problemas concretos no processo de mediação.

Para esta tarefa, definimos apenas um critério de aceitação. Este critério especifica que devemos manter em nossa amostra apenas aquelas avaliações que relatam melhorias, críticas ou experiências negativas com o processo de mediação (por exemplo: "Comprei uma TV para meu quarto aqui, mas somente depois de esperar três dias descobri que teria que combinar a forma de envio com o vendedor. Eu nem sabia que o vendedor não era a Amazon").

Para determinar o grau em que o revisor humano e o ChatGPT 4.0 concordaram com as classificações, usamos o coeficiente Kappa de Cohen [60], seguindo a metodologia aplicada por Dos Santos et al [76]. A amostra resultante atingiu um grau de concordância de 0,91, que, de acordo com Fleiss et al [97], corresponde a uma concordância quase perfeita (ou seja, cai dentro de $[0,80, 1,00]$). Assim, o conjunto de dados final coletou 69 avaliações sobre o processo de mediação a partir de um consenso de $\approx 100\%$.

4.3.4 Análise de Dados

QP1 e QP2 estão relacionados à observação e contagem de resultados, permitindo respostas quantitativas diretas. Os outros QPs exigem uma abordagem mais qualitativa para análise, exigindo uma compreensão mais profunda de uma maior quantidade de dados. Embora uma força-tarefa de pesquisadores experientes possa fornecer resultados mais precisos, um LLM foi usado para entender a relevância dos resultados, reunir evidências da viabilidade de um futuro estudo maior e responder às nossas perguntas de pesquisa.

Um LLM é um modelo inteligente sofisticado que passa por um treinamento extensivo com vastos conjuntos de dados textuais. Ele é projetado para entender, resumir, categorizar e até mesmo gerar novos conteúdos com base nesses dados. Como resultado, um LLM tem a capacidade de analisar e responder a perguntas relacionadas a dados textuais, como avaliações de usuários. Nossa decisão de usar LLMs neste estudo foi motivada pelos resultados positivos de pesquisas recentes realizadas por Byun et al [41] e Dos Santos et al [76], este último contribuindo para a base metodológica para o design deste estudo. O primeiro usou

o ChatGPT-3 para analisar dados textuais (por exemplo, transcrições de entrevistas) disponíveis em artigos publicados em grandes conferências de Interação Humano-Computador, comparando os resultados com análises qualitativas realizadas por pesquisadores humanos. Embora os autores não tenham conseguido avaliar com precisão a equivalência entre LLMs e resultados humanos, pois não eram especialistas em todos os domínios de dados analisados, os modelos automatizados foram capazes de gerar temas, discussões lógicas e análises qualitativas de dados possivelmente semelhantes às produzidas por pesquisadores humanos. O último aplicou o ChatGPT-4 para analisar a acessibilidade em revisões de atualizações de aplicativos móveis. Seus resultados apresentaram *insights* concretos sobre elementos de acessibilidade que tendem a se deteriorar ao longo de atualizações de aplicativos voltadas para outros propósitos.

Além desses resultados favoráveis obtidos em estudos anteriores, este artigo também utiliza a metodologia de design de *prompt* Chain-of-Thought (CoT) [270] (texto de entrada no LLM). Essa metodologia é baseada no conceito simples de guiar o fluxo de cognição do LLM por meio de pré-instruções como "Pensando passo a passo", que é capaz de otimizar a precisão da resposta do LLM de 17% para 78% em certos cenários [50]. Nosso estudo também visa extrair informações que, via de regra, são autocontidas em cada uma das unidades de análise (avaliações de usuários), o que por si só facilita a cognição do LLM.

4.3.5 *Prompt Design*

O *prompt* é um texto que descreve um comando a ser usado como uma consulta a um LLM com o objetivo de obter um resultado que satisfaça ao máximo possível o objetivo pretendido. O design do prompt é um conjunto de estratégias que visa otimizar a proximidade entre o resultado pretendido e a saída do LLM. Para este estudo, foi utilizada a estratégia *Chain-of-Thought* (CoT), segundo Wei et al [270], onde recomenda-se ao LLM como proceder ao analisar os dados apresentados. Por exemplo, considere a seguinte consulta sem CoT "Em média, a partir dos dados, é possível estimar uma taxa de satisfação do usuário em relação ao processo de mediação e como ele é comunicado?", agora a mesma consulta com CoT "Analise todas as revisões de mediação presentes nos dados, compare o nível de satisfação associado a este tópico em relação à satisfação geral associada aos outros tópicos e responda: É possível estimar o nível de satisfação do usuário em relação ao processo de mediação e

como ele é comunicado?". Essa estratégia, de acordo com Chen et al [50], melhora a saída da consulta em até 61%.

Após os primeiros testes, conforme descrito por Dos Santos et al [76] e Han et al [114], percebeu-se que o ChatGPT-4 se comporta de forma diferente principalmente devido ao estilo de resposta e às vezes em termos de conteúdo também, embora sejam sempre os mesmos dados. Assim, ao final de algumas interações, chegamos a *prompts* que tendem a ter respostas mais estáveis.

***Prompt* Inicial**: Em uma primeira consulta ao ChatGPT-4, devemos introduzir a natureza dos dados e estabelecer um CoT geral.

Abaixo, fornecerei um conjunto de dados de avaliações coletadas de uma loja de aplicativos (Google Store). Esses dados foram filtrados para que permanecessem apenas as avaliações de aplicativos de marketplace associados ao serviço de mediação de transações fornecido por tais aplicativos para garantir a honestidade de compradores e vendedores. Esses dados consistem em uma primeira coluna com o nome do aplicativo, uma segunda coluna corresponde à loja de aplicativos, a terceira com a descrição do sentimento da avaliação (negativa, positiva ou neutra), uma quarta com o código do usuário e a última corresponde ao texto da avaliação. Seguindo uma estratégia de análise avaliação por avaliação, diga-me quais são as principais reclamações dos usuários em relação ao serviço de mediação de transações.(tradução)

Requisição QP3: Para aumentar a eficácia do ChatGPT-4 na tarefa de retornar os principais problemas relacionados à mediação, decidimos delinear algumas possíveis formas de abordá-los. Novamente, formulando o *prompt* com base no CoT, seguindo uma estratégia do mais geral ao mais restrito, criamos o seguinte *prompt*:

Uma por uma, classifique tais avaliações de acordo com: principal elemento de mediação mencionado pelo usuário na avaliação e tipo de avaliação (exemplo: crítica, elogio, caso de uso negativo e caso de uso positivo). Então, aponte os principais problemas para cada elemento classificado.(tradução)

A resposta completa do ChatGPT-4 para QP3 atingiu 4.762 caracteres, o que é muito longo para incluir aqui. Tal resposta completa está disponível publicamente de acordo com o Apêndice B e pode ser resumida com seus principais elementos:

Resposta: Analisando os dados com revisões de mediação, chegamos às seguintes clas-

ses de resposta em termos de forma:

- Reclamação / Crítica.
- Relatório de *Bug*.
- Caso de dificuldade.
- Caso de fraude.
- Recomendação.

Agora as classes de revisão sobre o processo:

- Mediação de pagamento.
- Clareza no processo de envio.
- Reembolso em caso de disputa.
- Responsabilidade pela troca.
- Defeito após o recebimento

Por fim, os principais problemas relatados:

1. Espera acima da estimativa.
2. O usuário não recebeu um reembolso após não receber o produto comprado.
3. Estimativa de tempo de entrega mais alta após o pagamento quando comparado a estimativa de tempo de entrega pré-pagamento.
4. Nenhum reembolso em caso de defeito após a notificação do recebimento.
5. Incompatibilidade entre a descrição do produto e o produto real sem nenhum reembolso.

Requisição QP4: Solicitamos ao GPT-4 a expressar as ações tomadas pelos usuários após um processo de mediação malsucedido, com base nos problemas que a própria ferramenta extraiu dos dados no QP3. Aqui está o texto de entrada que criamos:

Analise todas as avaliações de aplicativo que contenham problemas no processo de mediação e faça uma lista das consequências sofridas pelos usuários, não apenas financeiras, mas de qualquer natureza.(tradução)

Aqui está um trecho da resposta do ChatGPT-4 para QP4:

Resposta:

Os usuários geralmente não comunicam claramente as consequências dos problemas relatados. No entanto, é possível identificar três ações distintas:

- Postagens em sites especializados em reclamações de consumidores.
- Implicações legais.
- Desinstalação.

Requisição QP5: Para simplificar o processo de cognição do ChatGPT-4.0, escolhemos dividir os sentimentos apenas em positivos e negativos, esclarecendo no prompt que eles podem ser expressos em diferentes níveis. Críticas, recomendações ou mesmo reclamações podem expressar sentimentos negativos e positivos. O texto de entrada que criamos segue:

Observe os sentimentos expressos nas avaliações de mediação. Faça um levantamento dos principais sentimentos expressos e sua intensidade entre positivo (1,0) e negativo (-1,0), e forneça um sentimento médio para cada problema principal relatado. Exemplos e sentimentos: decepção, frustração, alegria, gratidão, satisfação, etc. Observe que as avaliações, recomendações ou mesmo reclamações podem expressar sentimentos negativos e positivos. Para medi-los, recomendamos que selecione os mais negativos e positivos e os tome como parâmetros para os demais.

Aqui está um trecho da resposta do ChatGPT-4 à QP5:

Resposta:

Com base nas avaliações fornecidas, aqui estão os sentimentos expressos pelos usuários:

- Sentimentos negativos ($\approx 67\%$): frustração, raiva.

- Sentimentos positivos ($\approx 7\%$): Satisfação.
- Indefinido ($\approx 26\%$): Algumas das avaliações não têm sentimentos claros.

4.3.6 ChatIE

Para evitar estouro de buffer de entrada pelo ChatGPT-4, o que exigiria a divisão dos prompts em entradas iguais sucessivas, usamos uma ferramenta intermediária apresentada por Wei et al [271] chamada ChatIE, baseada na API do ChatGPT-4 e voltada à vetorização e extração de dados de bancos de dados tabulares como o que usamos. Além disso, como demonstrado por Wei et al, essa ferramenta já contém otimizações para extrair dados de bancos de dados de texto curto.

Para se adaptar ao design deste estudo, algumas modificações foram feitas no código fonte da ferramenta. Tais modificações visaram introduzir prompts intermediários e se adaptar à estrutura do próprio banco de dados. O código-fonte original e suas respectivas modificações estão disponíveis publicamente de acordo com o Apêndice B.

4.4 Resultados

Os resultados do estudo são apresentados aqui para responder às cinco questões de pesquisa.

4.4.1 QP1: Quantas críticas à mediação estão relacionadas a elementos de comunicação entre o aplicativo e o usuário?

A Figura 4.2 mostra os 11 aplicativos que receberam avaliações de mediação após o processo de filtragem descrito na Subseção 4.3.2. O eixo vertical mostra o nome do aplicativo, as barras azul-claro mostram o número geral de avaliações de mediação, as barras azul-escuro mostram o número de avaliações relacionadas à comunicação na mediação e os rótulos nas barras mostram a proporção entre avaliações de mediação e comunicação em avaliações de meditação. A Amazon é o aplicativo que recebeu mais avaliações de mediação e também sobre comunicação na mediação com 22 avaliações de mediação e 11 sobre comunicação, seguido por eBay (17), Rakuten (9), Shopee (8) e AliExpress (3).

O número de avaliações de mediação relacionadas à comunicação representa 44,77% do valor total. O número total de críticas de mediação relacionadas à comunicação representa uma proporção ainda maior para os aplicativos Amazon, eBay e AliExpress. Entre os elementos mais criticados na comunicação ao longo do serviço de mediação estão a responsabilidade por cada processo (um exemplo de processo é a retenção de valor até que o produto seja entregue – e isso representa críticas recorrentes, além de entrega, custos de envio, etc.), falta de informação, custos, reputação do vendedor e resolução de conflitos.

Validação. Para validar os resultados da análise sobre as 799 avaliações em *marketplaces* com mais de 100 caracteres, foi aplicado o ChatGPT-4.0 com a ajuda da ferramenta personalizada ChatIE [271]. Como resultado, chegamos às mesmas 67 avaliações, servindo como mais uma validação para o design deste estudo. Além disso, realizamos esse processo novamente, mas agora com o uso de um banco de dados de 29.000 avaliações sobre o *marketplace*, chegando a 71 avaliações relacionadas à mediação. No entanto, mais 4 avaliações não forneceram informações concretas e puderam ser descartadas.

Quase metade das revisões de mediação relatam críticas à comunicação, o que nos leva a acreditar que a mediação, quando realizada de forma adequada e dentro das expectativas do comprador, tende a ser bem-sucedida. No entanto, é relativamente comum que falhas de comunicação poluam o entendimento do comprador sobre esse processo. Essa descoberta não prova que as falhas de comunicação sejam a principal causa de insatisfação no processo de mediação, mas mostra que é uma causa relevante.

4.4.2 QP2: Quais componentes e recursos da interface tendem a gerar mais feedback entre as avaliações?

A Tabela 4.2 mostra os processos ou componentes da interface mais mencionados nas revisões de mediação. Curiosamente, não há menção a elementos diretamente relacionados à aparência da interface, como cor ou tamanho da fonte, mas apenas críticas de usabilidade, como a ausência de informações ou funções específicas, como “fale com o vendedor”. Identificamos manualmente os componentes da interface associados a cada revisão de mediação que menciona claramente qualquer um deles. A falta de detalhes sobre a intermediação de pagamento na interface recebeu o maior número de menções (6), seguida pela falta de

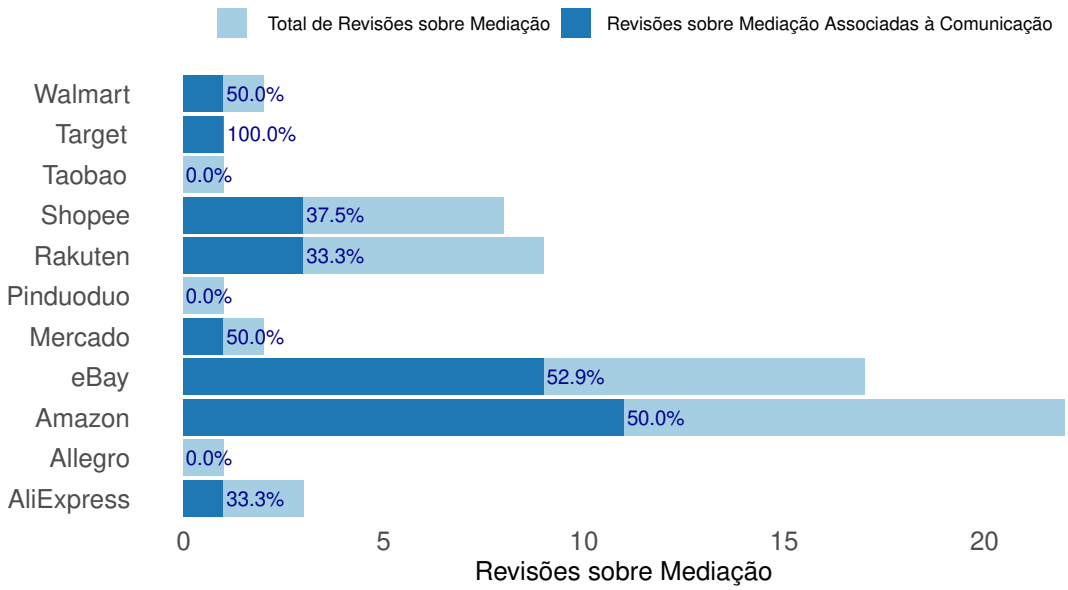


Figura 4.2: Aplicativos do tipo *marketplace* mais mencionados em avaliações de mediação, de acordo com os dados.

um componente direto para resolução de conflitos (4) e responsabilidade de envio (2). As 18 revisões restantes sobre comunicação de mediação não mencionam claramente nenhum processo ou elemento da interface.

Os resultados da QP2, embora escassos, demonstraram que é possível contar com recomendações do usuário para mapear falhas em recursos de comunicação da interface durante o processo de mediação. Por exemplo, a incompreensão do usuário sobre o serviço de intermediação de pagamentos (6 menções, conforme Tabela 4.2) é frequentemente explorada por usuários mal-intencionados. Problemas com relação à responsabilidade de envio tendem a gerar mais inconvenientes do que fraudes (2 menções, conforme Tabela 4.2). Tais achados se tornam mais evidentes a partir dos resultados para os QPs 3 e 4.

Validação. Novamente, assim como na validação do QP1, refizemos o processo de identificação dos componentes mais reportados utilizando o ChatGPT-4, obtendo resultados semelhantes (resposta a QP2). Entretanto, para esta tarefa, o ChatGPT-4 demonstrou comportamento um tanto evasivo, gerando respostas distorcidas. Isto provavelmente se deve ao fato de não haver menção a elementos estilísticos da interface como cor ou tamanho da fonte. Portanto, para corrigir este comportamento, o prompt precisou ser reformulado algumas vezes, onde chamamos os elementos da interface de "componentes de comunicação na

Tabela 4.2: Elementos do processo de mediação que deveriam ter mais destaque na interface dos aplicativos, segundo os usuários.

Componente	Menções	Quantos apps
Intermediação de pagamento	6	2
Resolução de conflitos	4	2
Responsabilidade pelo envio	2	1
Reputação do vendedor	1	1
Falar com o vendedor	0	0
Complexidade gráfica	0	0
Comunicação de responsabilidade	0	0
Perda de informações	0	0

interface", chegando ao resultado final abaixo:

Com base nos dados das avaliações do aplicativo feitas pelos usuários e analisando avaliação por avaliação separadamente, identifique quais delas mencionam especificamente componentes de comunicação na interface que, por estarem mal posicionados ou ausentes, geram dificuldades de compreensão por parte dos usuários durante o serviço de mediação prestado pelo aplicativo em transações de compra.(tradução)

4.4.3 QP3: Quais são os principais problemas que são críticos da mediação e que são relatados nas revisões?

A análise de avaliações mostra que os relatos de usuários fornecem argumentos concretos quando se trata de mediação. Essas avaliações trazem relatos de casos negativos e críticas, com algumas exceções mais neutras. A maioria desses casos traz experiências de usabilidade relacionadas ao excesso de confiança no serviço de mediação, muitas vezes devido a mal-entendidos que levam à superestimar o serviço.

A Tabela 4.3 descreve as principais reclamações identificadas nos relatórios de usuários classificados por tipo, bem como uma descrição de cada um desses tipos. Embora haja um pequeno número de revisões de mediação, é possível identificar que a maioria dos problemas

Tabela 4.3: Problemas identificados em relatórios de usuários.

Categoria	Subcategorias	Descrição da Categoria
`Falha no reembolso`	Nenhuma opção direta para solicitar reembolso. Ausência de instruções para solicitar reembolso por outros canais (chamada telefônica, por exemplo). Nenhum reembolso. Processo longo para reembolso. O vendedor nega que não enviou o pacote, e o processo é encerrado	Quando a transação de compra falha, e por algum motivo, o reembolso também falha.
`Perda de Informações`	Perda de acesso à solicitação. Peça o reembolso, mas a interface não muda (para sinalizar o processamento da solicitação).	Aqui, a transação de compra pode até terminar com sucesso, mas em algum ponto do processo, o comprador fica cego para algumas informações relevantes.
`Falha no serviço de troca`	Peça trocas, mas nada muda na interface. A segunda troca não está disponível. O tempo para troca é muito curto	Falha na substituição do produto devido a defeito ou não conformidade com o pedido.
`Espera excessiva`	O botão de cancelar desaparece, mas o pacote não foi entregue. O botão Comentar só está disponível antes da entrega. Esperando mais do que a estimativa	Esperando mais do que a estimativa máxima.
`O produto diverge da apresentação`	Ausência de opção de mídia nos comentários. Não é óbvio, mas é uma divergência relevante da descrição. A divergência do produto ficou clara depois de algum tempo.	Produto diferente do anunciado, especialmente quando essa discrepância não é facilmente identificável

poderiam ter sido evitados com ajustes na interface. Note que das seis categorias, apenas duas correspondem a uma falha real no processo, e as demais, que representam a maioria, dizem respeito apenas a falhas circunstanciais que foram corrigidas posteriormente, mas não antes de causar transtornos ao usuário.

Segundo o ChatGPT 4.0, apesar das críticas e reclamações, há um interesse maior em resolver problemas do que desinstalar ou retaliar o aplicativo. Segundo a ferramenta, mesmo entre avaliações em que o usuário critica veementemente, há uma grande tendência de colaborar com a melhoria do aplicativo.

Validação: Para fins de validação, incluímos a seguinte avaliação de mediação falsa "Excelente produto, mas estranhamente chegou muito sujo. Passei horas limpando o produto, mas adorei." no banco de dados enviado ao ChatGPT-4.0, para que aparecesse nas conclusões da ferramenta. Como resultado, o ChatGPT-4.0 criou uma categoria de problema adicional: "Falha de Sanitização". Sua única subcategoria e sua descrição limitaram-se a repetir o nome da categoria.

4.4.4 QP4: Quais são as principais ações tomadas pelos usuários como resultado do serviço de mediação, conforme relatado nas avaliações do aplicativo?

A análise mostra que, embora os problemas envolvendo o serviço de mediação sejam comuns, a maioria não diz respeito a um caso específico de fraude. No entanto, a maioria dos casos de fraude envolvendo mediação tende a resultar na desinstalação do aplicativo e implicações legais subsequentes, além dos danos causados à imagem do aplicativo devido a avaliações dessa natureza. A Tabela 4.4 traça um paralelo entre as categorias de problemas relatadas na Tabela 4.3 e as principais consequências correspondentes.

Na Tabela 4.4 praticamente todas as reclamações levam à desinstalação e muitas delas também resultam em postagens em sites de terceiros especializados em reclamações de consumidores. Essas reclamações podem ser muito prejudiciais à imagem do aplicativo se não forem resolvidas.

Validação: Nesta seção, também fizemos uma pergunta adicional sobre o ChatGPT 4.0, desta vez em relação a toda a base de avaliações de aplicativos do tipo *marketplace* (29.000

Tabela 4.4: Categorias de problemas identificados em relatórios de usuários e ações relatadas.

Categoria	Ação
`Falha no reembolso`	Postagens em sites de reclamações Implicações legais Desinstalar aplicativo.
`Perda de informações`	Desinstalar aplicativo Publicações em sites de reclamações.
`Falha no serviço de troca`	Desinstalar aplicativo Publicações em sites de reclamações.
`Espera excessiva`	Desinstalar aplicativo.
`O produto diverge da apresentação`	Nenhuma ação identificada.

avaliações). A seguinte pergunta adicional foi feita ao ChatGPT:

Qual é o número total de avaliações relatando um caso de fraude sofrido pelo usuário e, desse total, quantas se relacionam ao serviço de mediação? Se possível, liste-as.(tradução)

Como resultado, o ChatGPT 4.0 relatou que 16 revisões relatam casos de fraude diretamente, dos quais apenas um não parece estar relacionado ao processo de mediação. Não podemos validar diretamente esse resultado, pois ele foi produzido após consultar um volume muito grande de revisões e usuários; mas o fato de que todos os casos de fraude entre as revisões de mediação já mapeadas também aparecem na lista produzida oferece, por si só, uma validação.

4.4.5 QP5: Que níveis de insatisfação uma mediação inadequada pode causar nos usuários?

Esta última QP pergunta quais sentimentos estão presentes nas revisões de mediação. Seria difícil descrever o espectro de sentimentos em detalhes, razão pela qual escolhemos dividi-los em apenas três níveis, como na maioria dos estudos sobre análise de sentimentos [192]: positivo ou 1, negativo ou -1 e neutro ou 0. Com base nessas considerações, o ChatGPT-4.0

foi induzido a posicionar cada revisão dentro de algum ponto do intervalo $[-1.0, 1.0]$.

Diferenciar sentimentos positivos e negativos no contexto de avaliações e mediação não é simples. Isso ocorre porque a crítica pode trazer sentimentos positivos. Um usuário, apesar de ter reclamações, ainda pode considerar um determinado aplicativo melhor do que outros em sua categoria. Considere a seguinte avaliação de mediação: "Se você precisa trocar, esqueça. Os produtos raramente correspondem às imagens, mas o preço compensa"(tradução). Observe que o usuário reclama, mas ele/ela claramente pretende usar o aplicativo novamente.

De acordo com a Figura 4.3, que apresenta o perfil de sentimento para cada problema identificado nos relatórios de usuários (ver Tabela 4.3), o problema de falha de reembolso apresenta um sentimento negativo elevado. Isso é esperado, uma vez que esse problema está associado a todos os casos de fraude entre as revisões de mediação avaliadas. As revisões de mediação classificadas como "Produto diverge da apresentação" apresentam um sentimento próximo do neutro, mas levemente positivo. Ou seja, embora seja uma reclamação, os usuários parecem considerar tal problema "aceitável". Vale lembrar que temos apenas 67 avaliações de usuário sobre o tema, o que nos permite considerar tais resultados como evidências comportamentais, não regras.

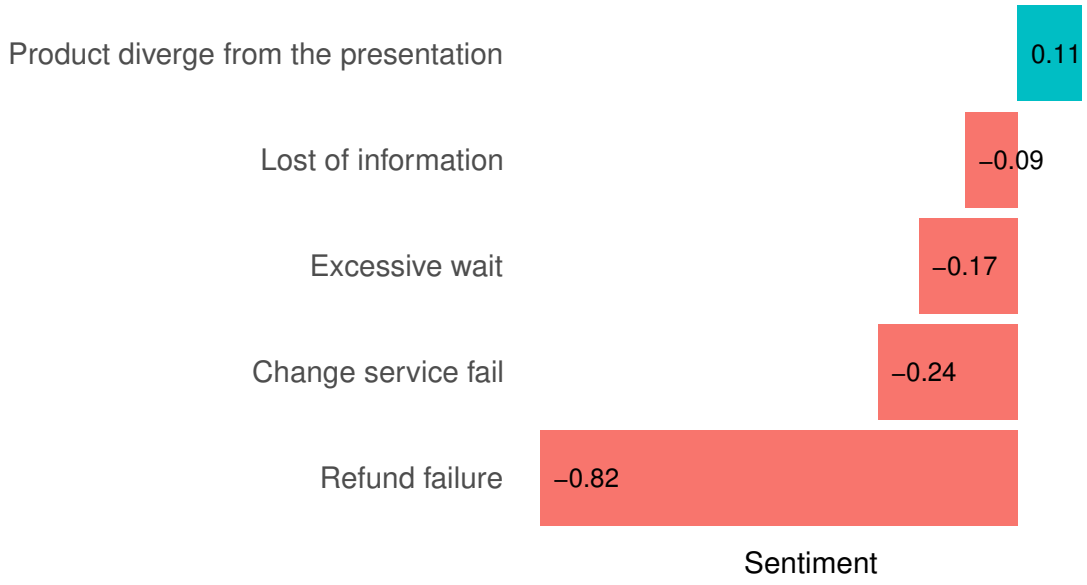


Figura 4.3: Categorias de problemas associados a uma graduação de sentimentos.

Validação: Conforme descrito por Maqbool et al [175], o MobileRec já classifica as avaliações de usuários por sentimento entre negativo, neutro e positivo. No entanto, tal

classificação é restrita, ou seja, sentimentos positivos são sempre iguais a 1, sentimentos negativos são sempre iguais a -1 e neutros são iguais a 0. Ainda assim, tais classificações foram úteis para validar as classificações geradas pelo ChatGPT-4.0, pois se refizermos a consulta ao ChatGPT-4.0 solicitando a mesma estratégia de classificação, tanto o ChatGPT-4.0 quanto o MobileRec alcançam resultados muito semelhantes em média.

4.4.6 Sumarizando os Resultados

A investigação baseada em avaliações de usuários de aplicativos do tipo marketplace revelou diversas descobertas importantes:

1. Os usuários geralmente fornecem *feedback* sobre problemas de comunicação entre o aplicativo (vendedor) e o usuário (comprador), destacando a importância de uma comunicação clara e eficaz no processo de mediação.

2. Os componentes e recursos da interface que geram mais *feedback* são cruciais para influenciar o serviço de mediação, indicando áreas para melhoria no design do aplicativo. Aspectos de segurança da interface podem induzir desconfiança ou erro do usuário, lidando com aspectos mais abstratos, como ênfase, posicionamento e falta de informação. Portanto, é no design e teste de usabilidade de software que nossos resultados encontram maior aplicação. Além disso, uma aplicação mais apropriada desses resultados envolveria tanto os resultados em si quanto a metodologia aplicada a novos dados. Essa discussão será enfatizada nas conclusões.

3. Problemas críticos relacionados à mediação, como falta de clareza nas responsabilidades, foram identificados, enfatizando a necessidade de comunicação transparente durante todo o processo.

4. Os usuários tomam várias ações em resposta a serviços de mediação ruins, como se envolver em transações fora da plataforma – tais ações podem facilitar resultados negativos ou até mesmo fraudes.

5. A mediação inadequada pode resultar em vários níveis de insatisfação do usuário, desde a desinstalação do aplicativo até ações legais, destacando as potenciais consequências de falhas na mediação.

Também é importante observar que, embora este estudo tenha destacado que os casos de fraude em aplicativos de comércio eletrônico geralmente estão vinculados a problemas de mediação, a maioria das críticas relacionadas à mediação são inconvenientes temporários, com alguns usuários expressando sentimentos neutros ou ligeiramente positivos, indicando uma disposição de continuar usando o aplicativo.

4.4.7 Ameaças à Validade

Filtrar os dados para reunir apenas avaliações de mediação com mais de 100 caracteres em si pode introduzir viés. O mesmo pode ser dito restringindo a análise a avaliações disponíveis na Google Play Store. Ter outras Play Stores cujas avaliações de usuários podem estar disponíveis em outros conjuntos de dados pode aliviar isso. Além disso, LLMs disponíveis online como ChatGPT são softwares proprietários e seu código-fonte, estrutura de dados e limitações não podem ser facilmente inspecionados e podem ameaçar a validade de nossas conclusões. Portanto, os resultados analisados aqui devem ser considerados levando em conta tais limitações.

Para mitigar essas ameaças, buscamos validações em cada estágio do processo de filtragem e investigação de cada questão de pesquisa e cada nova validação reafirmou, até certo ponto, o processo de filtragem de dados. A Tabela 4.5 lista os impactos de cada validação, para QP 1 à 5.

Por último, mas não menos importante, é importante observar que o próprio banco de dados original [175] pode conter defeitos que levam a problemas de legitimidade de dados.

4.5 Conclusões do Capítulo

Por meio da análise de avaliações de usuários, o estudo apresentado neste Capítulo fornece evidências de que o serviço de mediação entre vendedor e comprador em aplicações do tipo *marketplace*, embora conceitualmente sólido, na prática pode enfrentar muitos problemas com potencial para poluir os processos do serviço e gerar insegurança. Tais problemas geralmente são causados por falhas de comunicação relacionadas à ausência, falta de ênfase ou mesmo má localização de elementos de informação na interface. Observou-se também que a maioria dos casos de fraude relatados em avaliações desse tipo de aplicação estão di-

Tabela 4.5: Ameaças à validade e respectivas validações de cada QP. Todas as ameaças listadas neste quadro são ameaças internas provenientes da instrumentação.

QP	Ameaça à Validade	Abordagem
1	Como é um processo não automatizado, a filtragem manual de avaliações pode comprometer a precisão	O uso da ferramenta ChatIE [271] personalizada para validar o processo de filtragem manual
2	Mesma ameaça para QP1	Mesma validação para QP1
3	Incerteza quanto à eficácia do ChatGPT-4.0	Crie dados falsos e aguarde a resposta do ChatGPT-4.0 para alterar
4	Incerteza quanto à eficácia do ChatGPT-4.0	Repita o processo para todo o banco de dados, não apenas para as avaliações de mediação, esperando o mesmo resultado ou pelo menos um resultado semelhante.
5	Incerteza quanto à eficácia do ChatGPT-4.0	Recrie os resultados com base em metadados do próprio banco de dados original.

retamente relacionados ao serviço de mediação e a maioria deles está associada a falhas na comunicação entre o aplicativo e o comprador ao longo do processo de mediação, embora a maioria das reclamações relativas à mediação não se refira a fraudes.

Embora a maioria dos casos de fraude na classe de aplicativos avaliados esteja associada à mediação, a maioria das críticas à mediação está vinculada a inconvenientes temporários. Algumas das avaliações demonstraram até mesmo sentimentos neutros a levemente positivos, o que demonstra o interesse do usuário em usar o aplicativo novamente.

A pesquisa relatada neste Capítulo não teve a intenção de desacreditar o serviço de mediação, mas sim de demonstrar que tal serviço é incompleto e vários de seus pontos de incompletude vem da dificuldade em verificar eventos que ocorrem no mundo real, mesmo problema recorrente entre soluções descentralizadas para o problema da mediação (DCV). A principal descoberta por trás dessa afirmação vem do fato de que a maioria dos problemas

relatados estavam associados à comunicação entre aplicativo e comprador ou problemas de usabilidade diretamente, e não a questões de segurança como protocolos de criptografia ou restrições de acesso.

4.5.1 Contribuições

Para além dos objetivos de pesquisa desta Tese, as descobertas acima contribuem para melhores interações entre o aplicativo e o usuário comprador, melhorando sua satisfação. A lista de elementos de comunicação de mediação negativa para satisfação do usuário ajuda no design de soluções de mediação mais robustas.

Este estudo também contribui com uma nova abordagem metodológica para extração de informações aplicada ao design de soluções de segurança. Assim, os gerentes de segurança podem incorporar a metodologia de extração de informações aplicada aqui em seu processo de desenvolvimento.

Como outras contribuições, este estudo apresenta uma nova abordagem metodológica para extração de informações com base na análise de aplicativos e aplicada ao design de soluções de segurança. Esta metodologia foi usada anteriormente por Dos Santos et al [76] com algumas melhorias aqui, como a automação do envio de dados e perguntas. Assim, os gerentes de segurança podem incorporar a metodologia de extração de informações aplicada aqui em seu processo de desenvolvimento.

Especificamente, as contribuições deste estudo podem ser resumidas da seguinte forma:

Identificação de Problemas Críticos: A pesquisa identificou os principais problemas e desafios enfrentados pelos usuários no processo de mediação, como falta de clareza nas responsabilidades, lacunas de comunicação e potenciais riscos de fraude. Como exemplo, a função: 'Falar com o vendedor' parece ser bem explorada e demanda mais atenção dos designers de aplicativos.

Insights para Melhoria de Aplicativos: Ao destacar componentes e recursos de interface que geram mais *feedback*, o estudo fornece *insights* valiosos para desenvolvedores de aplicativos para aprimorar o serviço de mediação e melhorar a confiança e a satisfação do usuário. Como exemplo, designers e desenvolvedores de aplicativos devem fornecer uma apresentação clara e enfatizada das responsabilidades em cada estágio do processo de mediação.

Implicações Práticas: O estudo ofereceu implicações práticas para plataformas do tipo *marketplace* para abordar preocupações do usuário, prevenir fraudes e aprimorar estratégias de comunicação no processo de mediação. Tais implicações podem ser usadas para projetar testes de usabilidade.

Inovação Metodológica: A metodologia empregada, combinando inspeção manual com modelos de linguagem avançados de Inteligência Artificial para análise de dados, apresenta uma nova abordagem para extrair informações valiosas de avaliações de usuários e gerar *insights* para desenvolvimento de aplicativos e soluções de segurança. Tal metodologia pode ser usada para obter resultados semelhantes em outros processos de software.

4.5.2 Próximos Capítulos

Nos próximos Capítulos exploraremos o processo de mediação por meio de experimentos de simulação nos quais usuários/agentes podem competir como compradores ou vendedores em ambientes que abordam vários modelos de mediação e formas de comunicar o processo ao comprador em cada estágio. Por meio destas novas abordagens busca-se endereçar as limitações e problemas identificados nesse Capítulo eliminando a autoridade central mediadora.

4.6 Sumário do Capítulo

A seguir apresentaremos as principais contribuições deste Capítulo para a Tese como um todo.

- Este Capítulo forneceu evidências de que o serviço de mediação centralizado entre vendedor e comprador em aplicações do tipo *marketplace*, embora conceitualmente sólido, na prática pode enfrentar muitos problemas com potencial para poluir os processos do serviço e gerar insegurança.

- Observou-se também que a maioria dos casos de fraude relatados em avaliações desse tipo de aplicação estão diretamente relacionados ao serviço de mediação e a maioria deles está associada a falhas na comunicação entre o aplicativo e o comprador ao longo do processo de mediação.

- Considerando a comunicação entre a interface da aplicação e o usuário como o canal de virtualização das informações do usuário, os achados do estudo apresentado neste Capítulo convergem no mesmo sentido dos achados da revisão da literatura do Capítulo 2.

Capítulo 5

Incentivando a Honestidade em Mercados Descentralizados

De acordo com Kutera et al [152], a Comissão Federal de Comércio dos EUA (FTC, 2021) relatou que de outubro de 2020 a março de 2021, quase sete mil usuários foram vítimas de fraude digital no mercado de cripto moedas devido à mediação injusta, causando perdas em torno de US$ 80 milhões. Em mercados descentralizados, dois caminhos podem ser seguidos com o objetivo de reduzir esse risco: encorajar a honestidade ou validar todas as operações [20, 174, 258, 155, 285, 187, 219]. Um bom exemplo de um mercado descentralizado com operações não verificáveis é a plataforma de comércio eletrônico OpenBazaar, que embora tenha sido descontinuada seu conceito continua bastante relevante na literatura [31].

Este Capítulo apresenta uma revisão da literatura que buscou soluções para o Dilema dos Compradores e Vendedores (DCV) em ambientes descentralizados, Anônimos e mediante operações não Verificáveis (DAnV). Também combinou-se adequadamente as principais características de tais soluções, compondo novas soluções possíveis para apontar alternativas aplicáveis a mercados descentralizados para resolver o DCV, mesmo envolvendo transações não verificáveis. O conjunto final destas soluções foi submetido a uma análise comparativa de eficácia tanto com base em dados históricos reais de registros de transações (compras) na plataforma OpenBazaar, quanto em ambiente simulado, por Simulação Baseada em Agentes (ABS).

A revisão foi realizada no contexto da análise comparativa baseada em dados históricos

do OpenBazaar descrita na Seção 5.3 e publicada em formato de artigo científico [1] na 24th International Conference on Computational Science and Its Applications –ICCSA 2024 [58][2]. Já o experimento simulado descrito na Seção 5.4 está em revisão para publicação na revista Economic Interaction and Coordination[3] e está disponível na íntegra no Anexo F.

5.1 Introdução

As transações *on-line* desempenham um papel essencial em diversas atividades diárias, incluindo compras de bens e serviços. Apenas para o comércio eletrônico, estima-se que tais transações atinjam um volume de 50 trilhões de dólares até 2030 [105]. Novamente, para este Capítulo uma transação pode ser vista como um protocolo composto por uma série de operações que estabelecem uma troca de valores de diferentes naturezas envolvendo duas partes, uma parte ativa (comprador) que propõe a transação e uma parte passiva (vendedor) que a aceita ou rejeita. Tal transação é um jogo não equilibrado – porém existe um equilíbrio para cada parte, tendendo a não realização da transação por parte do comprador e ao comportamento desonesto por parte do vendedor – pois cada parte tende a cuidar de seus próprios interesses traindo a outra parte, uma vez que isso ofereça o resultado mais vantajoso. Tal impasse configura o DCV, descrito em mais detalhes no Capítulo 3.

Como descrito no Capítulo 4, uma solução convencional é a mediação de uma terceira parte centralizada, que valida operações e garante a contraparte passiva. No entanto, esta mediação não é infalível e ruídos na comunicação com o mediador podem promover oportunidades para usuários jogadores desonestos. Na verdade, esse é um dos crimes mais comuns que afetam adultos nos EUA: 15% dos americanos entrevistados por Lydia Saad [170] relatam que alguém em sua casa foi enganado para enviar dinheiro ou ter acesso a uma conta financeira. Esse problema causou perdas recordes de US$ 10 bilhões em 2023, levando a Comissão Federal de Comércio dos EUA (FTC) a tomar medidas para proteger o público [90].

No contexto descentralizado, as transações ocorrem sem um intermediário central, tornando o DCV um problema significativo devido ao risco inerente de desonestidade por parte dos agentes envolvidos. As soluçoes para o DCV na literatura podem ser agrupadas em três

[1] `https://doi.org/10.1007/978-3-031-64608-9_14`

[2] Estrato Qualis CAPES A2, `https://2024.iccsa.org/`.

[3] Estrato Qualis CAPES A2, `https://link.springer.com/journal/11403`.

principais classes: redes de confiança, arbitragem e protocolos de pagamentos em garantia. Essas três classes são aqui coletivamente denominadas de Modelos de Incentivo à Honestidade (MIHs). Para avaliar a eficácia das soluções descentralizadas, foram conduzidas duas abordagens complementares: (i) análise empírica utilizando dados históricos do OpenBazaar, onde transações foram classificadas manualmente como sucesso ou fracasso com base em revisões e comentários de usuários; e, (ii) simulação baseada em agentes (ABS), permitindo a análise de dinâmicas emergentes e impacto do comportamento desonesto.

A questão de pesquisa central do estudo apresentado neste Capítulo é: *Quais das classes de solução ou combinações de suas principais características apresentam desempenho superior?* A resposta obtida a partir das duas análises indica que modelos que combinam redes de confiança e árbitros descentralizados apresentam melhor desempenho, mas ainda assim o DCV permanece um desafio aberto em mercados descentralizados que lidam com transações não verificáveis mediante elevadas taxas de desonestidade.

Para além da contribuição para esta Tese como uma base sintetizada, formando um corpo de conhecimento para referência nos próximos Capítulos, este Capítulo também contribui para o desenvolvimento e pesquisa a respeito do tratamento do DCV em mercados DAnV. Seus resultados contribuem para a descentralização do mercado e para o desenvolvimento de protocolos antifraude em mercados descentralizados. Além disso, fornecem uma base para gestores, profissionais de TI e pesquisadores interessados no design e operação de contratos inteligentes, *e-commerce* descentralizado e mercados sem intermediação centralizada.

5.2 Soluções para o DCV: Revisão da Literatura

Esta Seção traz uma revisão de literatura realizada de dezembro de 2023 a janeiro de 2024 que buscou elencar soluções aplicadas ao DCV. Tais soluções foram extraídas de trabalhos voltados a explorar potenciais melhorias aplicadas ao DAX para expandir a gestão descentralizada de transações não verificáveis e tolerantes à informação assimétrica. Os resultados são divididos em três classes principais de soluções: redes de confiança, arbitragem e protocolos de pagamentos em garantia. Essas três classes serão a partir daqui coletivamente e genericamente denominadas de Modelos de Incentivo à Honestidade (MIHs).

Aqui são apresentados os protocolos usados para reunir as principais soluções para o Di-

lema dos Compradores e Vendedores (DCV) em ambientes Descentralizados, Anônimos e mediante operações não-Verificáveis (DAnV), analisando e selecionando os trabalhos acadêmicos mais relevantes a respeito deste tema na literatura científica especializada. Até onde pesquisamos, a literatura ainda carece de uma revisão que reúna todas as possíveis soluções para o Dilema dos Compradores e Vendedores em ambiente DAnV.

5.2.1 Questões de Pesquisa

Foi realizado um mapeamento sistemático da literatura para responder à única Questão de Pesquisa:

RQ Já existe na literatura uma solução para o Dilema dos Compradores e Vendedores em ambiente DAnV com um nível aceitável de risco?

5.2.2 Processo de Seleção

Os critérios de inclusão e exclusão para a seleção dos trabalhos levam em consideração os objetivos, questões de pesquisa e metadados que ajudam a estimar a qualidade dos trabalhos. A metodologia seguida pelos revisores é descrita em documento à parte – vide Apêndice D [4]. As Tabelas 2.2 e 2.3 – já apresentadas no Capítulo 2 – descrevem os critérios de seleção e qualidade utilizados pelos revisores para 1) verificar se os resultados obtidos pelo pesquisador são adequados ao tema da pesquisa – critérios de seleção; e, 2) avaliar critérios de qualidade ligados aos métodos e processos aplicado à pesquisa sob análise, além do impacto da pesquisa em questão.

5.2.3 Metodologia

As revisões de literatura tendem a ser iniciadas com base em publicações científicas proeminentes focadas no tópico em análise [138]. Nesta etapa da Tese adotamos uma abordagem bibliométrica a fim de responder à questão de pesquisa estabelecida. A Figura 2.1 apresenta a estrutura metodológica usada aqui. Consideramos artigos que tratem direta ou indiretamente do Dilema dos Compradores e Vendedores (DCV) em ambientes DAnV entre 2016

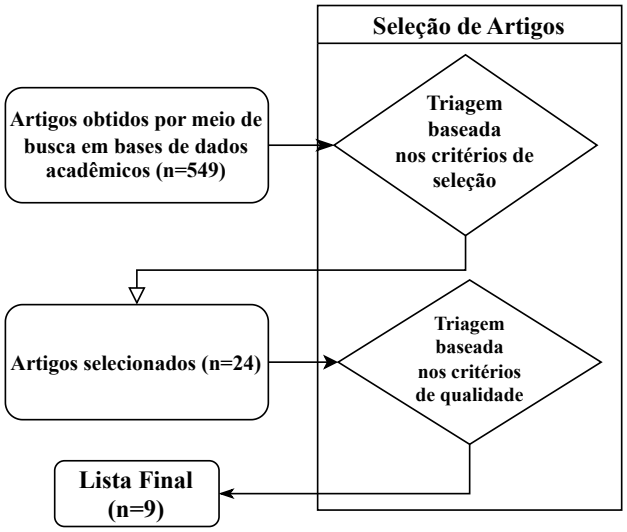
[4] https://docs.google.com/document/d/1wv8FKFKigr5EerlFetXlLYXTfCZJ0S0qsgw3pR3KTDo/edit?usp=sharing

e 2023, e os bancos de dados Web of Science (WoS) e Scopus foram escolhidos [33] para esta investigação porque o Scopus tem uma coleção mais extensa e diversificada de material acadêmico e o WoS é a plataforma de busca e análise de citações científicas mais abrangente do mundo [34, 145].

Para realizar a busca mencionada acima, foram selecionadas algumas palavras-chave que resultaram na seguinte *string* de busca:

(”decentralized´´ AND ”Buyer and Seller s Dilemma´´) OR (”blockchain´´ AND (”Buyer and Seller s Dilemma´´ OR ”decentralized markets´´)) OR (”dlt´´ AND (”Buyer and Seller s Dilemma´´ OR ”decentralized market´´))

Figura 5.1: Protocolo de Revisão



5.2.4 Resultados da Revisão

No total, 9 trabalhos foram classificados como relevantes. Conforme descrito na Figura 5.1, 24 artigos tiveram uma classificação geral maior que 0,5 em todos os critérios de seleção, mas apenas os 9 estão listados neste documento por corresponder aos critérios de qualidade, conforme Tabela 5.1. A partir desses números e com base nas estratégias adotadas nos artigos classificados, podemos estabelecer as principais soluções aplicadas na literatura para o DCV.

Redes de Confiança

A abordagem introduzida por Duong-Trung et al [78], além da resolução automática de conflitos, penaliza entregadores ou transportadoras que violam contratos com base em um sistema de reputação. Na literatura, há outros trabalhos que abordam soluções descentralizadas para Cash on Delivery (CoD) e abordam o DCV de forma semelhante [156, 12, 20], embora todos eles utilizem uma rede de confiança associada a outros modelos.

Arbitragem

Son et al [238] empregam blockchain e contratos inteligentes para aprimorar o protocolo Cash on Delivery (CoD) para comércio eletrônico. Sua abordagem garante transações seguras e resolve o BSD impondo regras específicas aos jogadores e utilizando contratos inteligentes como intermediários. Tsabary et al [258] introduziram uma solução semelhante chamada MAD-HTLC, que alavanca mineradores de blockchain como árbitros de contratos.

Duong-Trung et al [78] introduzem um modelo CoD abrangente que depende de contratos inteligentes para resolução automática de conflitos, eliminando a necessidade de intermediários humanos que, segundo eles, consumiriam mais ativos e tempo para os jogadores envolvidos. No entanto, essa abordagem inclui um elemento adicional de resolução de conflitos, penalizando entregadores ou transportadoras que violam contratos com base em um sistema de reputação. De acordo com os autores, o uso de um Contrato Inteligente como árbitro associado ao sistema de reputação, além da infraestrutura fornecida por tecnologias descentralizadas que implementam o Contrato Inteligente, é suficiente.

Pagamentos em Garantia

Le et al [155] introduzem um protocolo CoD para entrega comercial onde os motoristas são obrigados a hipotecar uma quantia de dinheiro como garantia. Além disso, um sistema de autenticação é usado para motoristas e um código hash identifica os produtos.

Tsabary et al [257] introduzem o conceito de LedgerHedger, um mecanismo de duas partes que garante a confirmação oportuna de transações em protocolos de contrato inteligente. O LedgerHedger faz com que o jogador emissor pague por uma transação antecipadamente, e o outro jogador concorda em pagar uma taxa necessária, mesmo que exceda o valor da tran-

sação. Isso garante que a transação será confirmada dentro de um prazo definido. Asgaonkar e Krishnamachari [20] também apresentam uma solução baseada em garantias duplas. Tais garantias duplas, embora eficazes, podem inviabilizar transações, principalmente quando são maiores que o valor negociado [257].

Finalmente, o modelo mais completo de protocolos de garantia de pagamento foi fornecido por Schwartzbach [235], onde eles apresentam duas conclusões principais: não é viável fornecer um modelo de depósito de garantia sem qualquer tipo de informação sobre o comportamento do jogador, e é improvável que um protocolo de depósitos de garantia não adaptável baseado em regras empíricas funcione. A abordagem matemática apresentada parece a mais completa.

Visão Geral

A dificuldade em virtualizar serviços, dinheiro e produtos do mundo real de forma descentralizada é o problema central das transações não verificáveis e leva a maioria das soluções para o DCV a recorrer a pré-condições que limitam o domínio da aplicação ou violam o princípio da descentralização [20, 174, 258, 155, 285, 187, 219, 206]. A Tabela 5.1 apresenta todas as soluções coletadas da literatura e identifica as pré-condições aplicadas por cada uma para evitar desonestidade. Tais pré-condições são diversas, mas podem ser classificadas em quatro categorias, são elas:

1. Algum nível de centralização: Modelos apelam à centralização para verificar a transação em algum nível, superando a dificuldade de garantir confiança sem informações completas;

2. Autenticação: Identifica usuários para intimidar os desonestos com repercussões legais;

3. Verificação digital de produtos entregues: Esta pré-condição, quando em um ambiente descentralizado e online, só é aplicável a produtos que podem ser completamente digitalizados;

4. *Feedback*: É usado para construir confiança, mas é mais suscetível a falhas porque pode ser forjado.

Tabela 5.1: Soluções para DCV da literatura

Referência	Modelo	Centralização	Autenticação	Verificação Digital	*Feedback*
[155]	Depósito de garantia	✓	✓	✓	
[257]	Depósito de garantia			✓	
[20]	Depósito de garantia, Rede de confiança			✓	✓
[235]	Depósito de garantia				
[238]	Arbitragem			✓	
[258]	Arbitragem			✓	
[78]	Arbitragem, Rede de confiança	✓	✓	✓	✓
[156]	Arbitragem, Rede de confiança	✓	✓		✓
[12]	Arbitragem, Rede de confiança			✓	

5.3 Incentivando a Honestidade em Mercados Descentralizados: Análise de Dados Históricos

Como contribuição para responder a pergunta de pesquisa desta Tese, esta Seção apresenta uma análise da eficácia dos modelos de incentivo à honestidade elencados na Seção 5.2, além de combinar suas principais características resultando em novos modelos. A comparação é realizada a partir de um conjunto de dados de registros de transações (compras) na plataforma OpenBazaar entre 15 de junho de 2018 a 3 de setembro de 2019. Tais dados foram coletados por Arps e Christina [19] e cedidos para esta análise.

5.3.1 Introdução

A pesquisa apresentada nesta Seção é composta de duas fases: 1) Marcação manual de transações como sucesso ou fracasso no conjunto de dados históricos do OpenBazaar de acordo com revisões e comentários anotados sobre compras correspondentes; e, 2) Comparação das

soluções descentralizadas elencadas na Seção 5.2 com base em suas previsões de sucesso ou fracasso de transações, quando comparadas as marcações da fase 1. As métricas usadas para comparar esses modelos foram inspiradas no campo da Aprendizagem de Máquina e são: precisão, *recall* e F1.

Para a comparação (fase 2), os modelos de incentivo à honestidade com potencial para resolver ou contornar o DCV presentes na literatura foram agrupados em três classes: árbitro descentralizado, rede de confiança e depósitos de garantia. Este trabalho selecionou instâncias destas classes de soluções para o DCV de acordo com os critérios de descentralização, tolerância a transações não verificáveis e não autenticação. Tais soluções foram utilizadas na análise comparativa.

A questão de pesquisa (QP) para a qual o estudo desta Seção traz uma resposta é: *Quais das classes de solução ou combinações de suas principais características apresentam eficácia superior ao prever as marcações de sucesso ou fracasso das transações?*

Os resultados demonstram que, embora existam modelos capazes de promover a honestidade com mais eficácia do que aqueles usados no OpenBazaar, o jogo de compra e venda descentralizado continua tendencioso para a desonestidade. Além disso, encontramos evidências apontando para a solução composta de rede de confiança e árbitro descentralizado como a mais eficaz de todas. Tais achados demonstram que o DCV mediante transações não verificáveis entre agentes anônimos, problema focal desta Tese, segue em aberto para o modelo de mercado descentralizado avaliado.

Soluções

Zindros [289] apresenta a plataforma de comércio descentralizado OpenBazaar, que implementa uma abordagem específica de duas classes de soluções, arbitragem e rede de confiança. No OpenBazaar, qualquer usuário pode atuar como um árbitro humano escolhido pelo vendedor de forma unilateral e este deve resolver disputas quando ocorre um problema em troca de uma recompensa monetária que só é paga se o árbitro for chamado. A rede de confiança é baseada em *feedback* e a confiança em um árbitro ou comprador/vendedor depende desse *feedback* e de um "currículo" em arquivo, no caso do árbitro, que quase sempre expõe a identidade do árbitro.

A Tabela 5.1 apresenta todas as soluções coletadas da literatura e identifica as condições

de contorno aplicadas por cada uma para atenuar o risco de desonestidade. Os recursos usados para algumas das soluções para evitar tais condições de contorno são usados para compor os modelos comparados aqui e descritos em mais detalhes na Seção 5.3.3. Como se pode ver na Tabela 5.1, nenhuma das soluções implementa exclusivamente a rede de confiança, embora sem essa rede de confiança, algum outro tipo de inferência de comportamento deva ser fornecido, como Contratos Inteligentes (CI) baseados em oráculos, por exemplo.

5.3.2 Marcação de Dados do OpenBazaar – Fase 1

OpenBazaar

O OpenBazaar, um marketplace de e-commerce descentralizado, recebeu atenção significativa desde seu lançamento inicial em 2016 até seu fechamento em 2020. Ao decidir usar uma plataforma descentralizada como o OpenBazaar, o usuário deve estar ciente de que está sozinho em vários aspectos. Embora a interface envie a mesma mensagem ao consumidor que os mercados centralizados, no OpenBazaar o pagamento é feito por criptomoeda diretamente ao vendedor e não há reembolso, nem responsabilidade por parte da plataforma.

É importante notar que o OpenBazaar já implementa duas das classes de incentivo à honestidade analisadas aqui. No entanto, o modelo de arbitragem aplicado é tendencioso: pois o vendedor é o único responsável por escolher uma lista de possíveis árbitros. Isto é uma contradição, uma vez que o vendedor neste modelo de transação é o jogar passivo, e por isso o único com a oportunidade de agir de forma desonesta, conforme definido no DCV. O modelo de reputação é baseado em *feedback* e pontuação, sem uma rede de confiança. Assim, pode-se comparar a eficácia da solução de incentivo à honestidade aplicada (arbitragem e reputação com base em pontuação e *feedback*) com as abordagens selecionadas da literatura: arbitragem descentralizada, rede de confiança sem *feedback* e garantia de pagamentos.

Conjunto de Dados

Usando múltiplos rastros diários da rede OpenBazaar ao longo de aproximadamente 14 meses (25 de junho de 2018 a 3 de setembro de 2019), Arps e Christin [19] observaram sua evolução ao longo do tempo. Um total de 6.651 participantes diferentes foram observados. Mais da metade de todos os usuários (3.521) foram observados apenas em um único dia e, em

média, apenas aproximadamente 80 usuários estavam ativos simultaneamente em um determinado dia buscando um total de 4.379 itens listados. 6.292 mensagens de texto associadas a compras também foram observadas.

Marcação manual de transações

Das 6.292 mensagens de texto, o sucesso ou fracasso de suas transações correspondentes foi manualmente inferido e marcado, mensagem por mensagem, resultando em um total de 2.517 transações bem-sucedidas e 347 transações malsucedidas, o que totaliza 3.034 transações marcadas manualmente; não foi possível inferir o sucesso ou fracasso de 170 transações.

5.3.3 Modelos de Incentivo à Honestidade – MIHs

Esta seção descreve as estratégias por trás de cada modelo de incentivo à honestidade (MIH) que comparamos. Aqui é apresentado como cada modelo foi implementado para avaliar sua eficácia em encorajar a honestidade. Como não é possível implementar incentivo à honestidade sem nenhuma estratégia de inferência de comportamento [235], o árbitro descentralizado e a garantia de pagamento foram implementados junto com a rede de confiança para usar a rede de confiança como uma fonte de inferência de comportamento.

Rede de Confiança – R

A rede de reputação implementada em nossa comparação descreve um conceito mais descentralizado, Web-of-Trust, onde não há *feedback* (menos suscetível a falhas) e as transações entre usuários são públicas, dando a cada usuário a liberdade de tirar suas próprias conclusões. Originalmente, a Web-of-Trust lida com uma rede p2p para estabelecer a autenticidade da conexão entre uma chave pública e seu proprietário. Com o tempo, os usuários acumulam chaves de outros que desejam designar como confiáveis, e uma rede confiável é gradualmente formada sem uma autoridade de certificação centralizada. Os usuários legitimam uns aos outros acumulando e redistribuindo uma coleção de certificados de terceiros. A rede de chaves públicas formada é um esquema flexível, descentralizado e tolerante a falhas, verificado por consenso entre os usuários [42].

Para transações com operações não verificáveis, o modelo Web-of-Trust é capaz de for-

necer confiança entre compradores e vendedores que nunca tiveram interações diretas com base na experiência daqueles com quem interagiram separadamente.

Dois jogadores $a, b \in A$ (onde A refere-se ao conjunto total de jogadores [5]) avaliam a possibilidade de realizar uma transação T. Para tanto, a confiança da rede em um dado jogador b é ϕ_b, de acordo com a Equação 5.1 e descreve a razão entre o saldo de transações de um dado jogador dividido pelo melhor saldo do jogo, evoluindo em tempo logarítmico.

$$\phi_b = \frac{\ln\left(\frac{\sum_{a \in A} s_t(b,a)}{P_t}\right)}{\ln\left(\text{MAX}_i\left(\frac{\sum_{a \in A} s_t(i,a)}{P_t}\right)\right)} \tag{5.1}$$

Onde $s_t(b, a)$ se refere ao saldo histórico de transações entre b e a até o momento atual t. Aqui, o saldo é entendido como a soma dos valores em produtos e moeda da outra parte em cada transação – assim, operações desonestas pelo jogador contribuem negativamente para o saldo. Finalmente, P_t representa o saldo total de transações entre toda a população ativa do OpenBazaar até o tempo t. Aqui, 'tempo' significa um intervalo de tempo arbitrário no final do qual a confiança é recalculada para todos os jogadores.

Assim, ϕ_a cresce à medida que o saldo total de transações de a cresce em relação ao saldo total da população como um todo. Para fins de normalização, é considerada a melhor reputação entre todos os jogadores como $\phi = 1.0$. Essa melhor reputação ϕ é representada na Equação 5.1 por MAX_i desempenhando o papel de normalizador, preservando $\phi \in [0.0, 1.0]$. À medida que a melhor reputação entre todos os jogadores aumenta, os outros caem em uma proporção logarítmica.

Considerando também um limite de confiança aceitável para realizar uma transação δ, a Equação 5.10 descreve a regra elaborada e aplicada sobre a confiança em um dado jogador b para que a transação ocorra.

$$T_{s,b} = \begin{cases} 1 & \text{se } \delta_s^t < \phi_b \\ 0 & \text{caso contrário} \end{cases} \tag{5.2}$$

Assim, para que a transação T ocorra, ϕ deve ser maior que um limite δ para o jogador passivo s (vendedor). Este fator é proporcional ao saldo histórico total de um determinado jogador s e inversamente proporcional ao saldo total da população. Aqui, a confiança no

[5] Observe a Tabela de símbolos no início do documento ou a Tabela C.2 de símbolos restrita a este Capítulo

comprador é irrelevante porque o modelo de negócios do OpenBazaar não deixa espaço para desonestidade por parte dos compradores, pois eles sempre transferem seus valores primeiro.

Rede de Confiança + Arbitragem – RA

A arbitragem é baseada na seleção do árbitro por consenso entre as partes e foi implementada fazendo com que a Web-of-Trust proposta na literatura seja a fonte de inferência de confiança. Isso porque para que haja consenso na seleção do árbitro, ambas as partes, mesmo separadamente, devem confiar no árbitro

O modelo Web-of-Trust funciona bem com a moderação de transações usando árbitros descentralizados confiáveis, pois, dada uma população Q com algumas transações $S' << Q$, já é possível estimar a honestidade dos participantes envolvidos em uma transação (comprador, vendedor e árbitro).

Observe a Equação 5.3 elaborada e aplicada considere dois jogadores a e b buscando a transação, e um terceiro c candidato a arbitragem, onde $\gamma_{a,b}(c)$ é a função que define se c é confiável o suficiente para ser o árbitro da transação $T_{a,b}$.

$$\gamma_{a,b}(c) = \begin{cases} 1 & \text{se } \delta_t < \frac{s_t(c,a)}{\sum_{a \in A} s_t(c,a)} \text{ e } \delta_t < \frac{s_t(c,b)}{\sum_{a \in A} s_t(c,a)} \\ 0 & \text{caso contrário} \end{cases} \tag{5.3}$$

Além disso elaborou-se a aplicou-se a Equação 5.4 para definir entre toda a população quem é o melhor árbitro para a operação:

$$\gamma_{a,b} = \begin{cases} \text{c} & \text{se } \forall_{c \in A} \delta_t < \text{MAX}(\frac{s_t(c,a)}{\sum_{a \in A} s_t(c,a)}) \text{ e} \\ & \delta_t < \text{MAX}(\frac{s_t(c,b)}{\sum_{a \in A} s_t(c,a)}) \\ 0 & \text{caso contrário} \end{cases} \tag{5.4}$$

Que descreve uma operação de complexidade assintótica $O(n \log n)$, para descobrir o melhor árbitro para todas as operações, com n sendo o número total de novas transações em cada período de tempo completo t.

Rede de Confiança + Depósito de Segurança – RD

Para o protocolo de depósito de segurança utilizaremos o modelo do trabalho de Schwartzbach [235], no qual o autor assume um mercado descentralizado baseado em transações não

verificáveis. Para esse fim, Schwartzbach [235] demonstra a necessidade de algum mecanismo de inferência de confiança entre as partes, como oráculos (contratos inteligentes com acesso externo) usados em livros-razão distribuídos. Tal necessidade foi atendida por uma associação ao modelo de Rede de Confiança (Subseção 5.3.3, item 'Rede de Confiança – R'), assim como com o Modelo de árbitro descentralizado (veja a Subseção 5.3.3, item 'Rede de Confiança + Arbitragem – RA').

Usando a Rede de Confiança para desempenhar o papel de uma fonte de inferência de confiança como os oráculos fazem em livros-razão distribuídos, considere que dois jogadores a, b, comprador e vendedor, desejam trocar os valores x, y, dinheiro e produto. De acordo com Schwartzbach [235], os depósitos de segurança necessários para garantir a transação entre a e b são x', y', correspondem às Equações 5.5 e 5.6.

$$x' = \frac{2\phi_a}{2\phi_a - 1}\ x \tag{5.5}$$

$$y' = \frac{\phi_b}{2\phi_b - 1}\ y \tag{5.6}$$

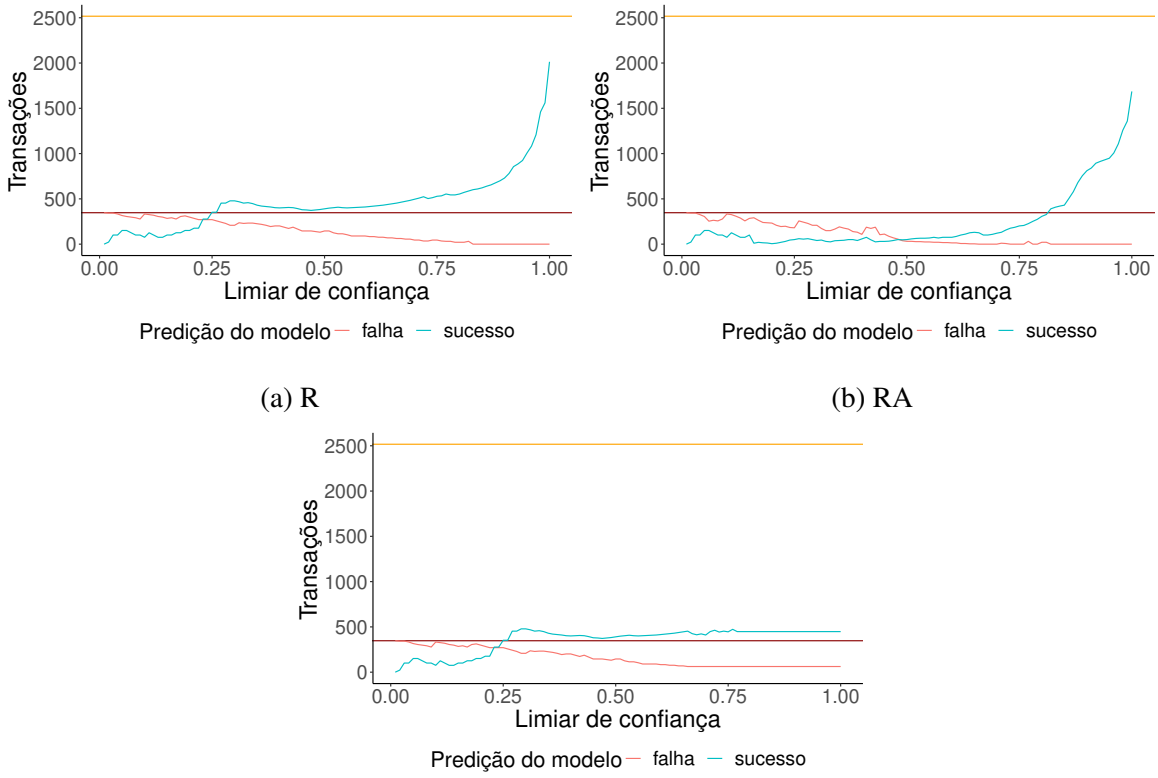
Esta abordagem foi escolhida porque é satisfatoriamente descentralizada e capaz de lidar com a incerteza de um ambiente de informação incompleta. Aqui, informação incompleta pode ser considerada como a ausência de informação sobre o sucesso ou fracasso de transações (transações não verificáveis).

5.3.4 Resultados do estudo – Fase 2

Embora tenha alcançado algum sucesso, o OpenBazaar teve vida curta quando comparado a modelos centralizados como Amazon ou eBay. Embora certamente existam diversos fatores associados ao fim do OpenBazaar, tal destino pode ter sido antecipado devido à dificuldade do OpenBazaar em incentivar a honestidade no sistema, caindo no DCV. No total, das 3034 transações observadas, aproximadamente 12% foram malsucedidas, ou seja, o vendedor recebeu o pagamento, mas não entregou os produtos/serviços conforme estabelecido, a única forma de desonestidade considerada neste estudo. Ainda há 170 transações não classificadas, então essa proporção pode ser ainda mais séria. Essa taxa é muito alta quando comparada

a modelos centralizados não anônimos, apoiados por leis e modelos de mediação de pagamento que tornam a desonestidade dentro do site incomum.

No entanto, os responsáveis pelo OpenBazaar não ignoraram o problema e implementaram duas soluções para verificar transações e incentivar a honestidade: arbitragem e reputação baseada em pontuação. Nesta Seção, usamos as soluções descentralizadas mais promissoras de acordo com a literatura revisada, aqui denominadas R (Rede de Confiança), RA (Rede de Confiança mais Arbitragem Descentralizada) e RD (Rede de Confiança mais Depósito de Segurança), para prever quais transações seriam bem-sucedidas e quais falhariam, e então verificar com base nos dados históricos marcados manualmente do OpenBazaar. Com isso, obtivemos conclusões úteis para esta Tese sobre os modelos avaliados e as soluções realmente implementadas no OpenBazaar [6]. Tais conclusões serão exploradas na Seção 5.3.5.



(a) R

(b) RA

(c) RD

Figura 5.2: Transações por limite de confiança. Onde a linha horizontal vermelha escura apresenta o total de transações com falha (347 produtos não entregues), enquanto a linha horizontal laranja representa o total de transações bem-sucedidas (2517 produtos entregues).

[6]Todo o código fonte utilizado nas análises descrita aqui está disponível no Apêndice B

Apenas rede de Confiança – R

O modelo de rede de confiança baseado em histórico de transações sem *feedback* foi o que obteve os melhores resultados entre os modelos de reputação ao evitar DCV em ambientes descentralizados, segundo a literatura [156, 12, 20]. Para este estudo, este modelo também serve como fonte de inferência para tentar estimar a confiança de cada jogador, além de ser comparado aos outros modelos.

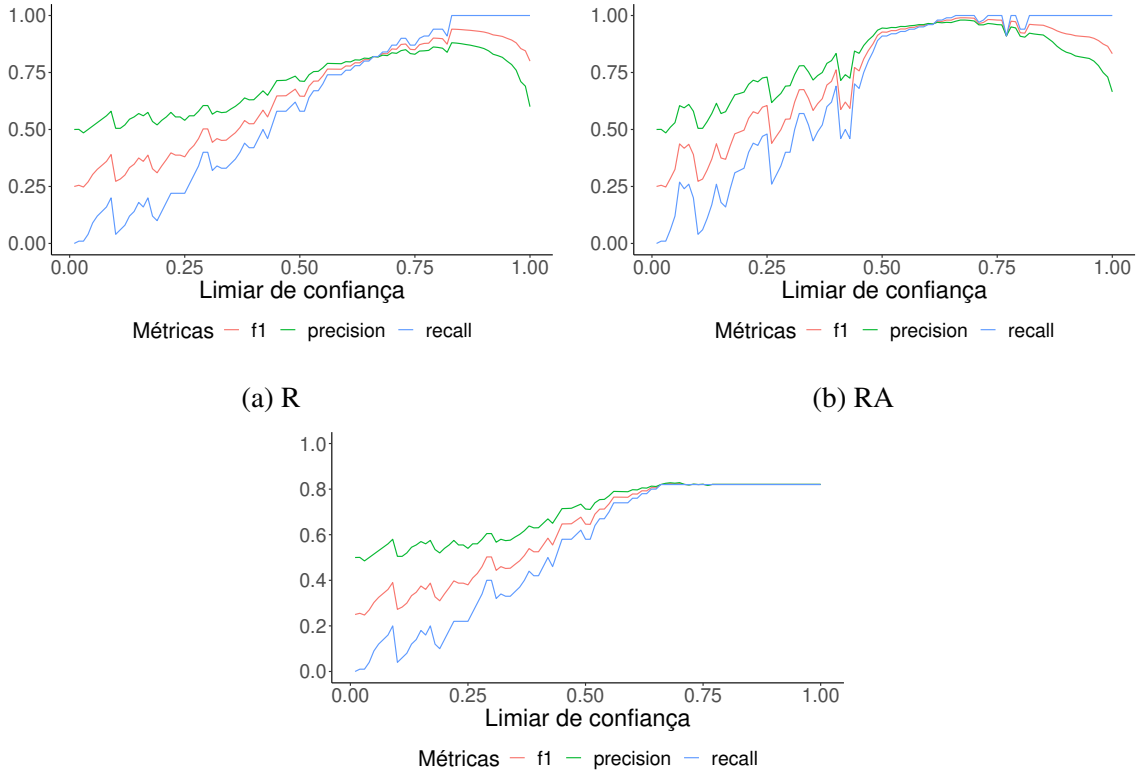
Observe na Figura 5.2a, o número total de transações malsucedidas (linha vermelha mais clara) diminui à medida que o limite δ aumenta. Isso ocorre porque um vendedor ruim provavelmente tem uma má reputação, e aumentar o limite prevê o fracasso de transações envolvendo vendedores com má reputação. Com o limite δ muito baixo, a maioria das transações é classificada como segura; se esse limite for muito alto, o modelo aponta quase todas as transações como inseguras. Se o limite δ for muito alto, transações bem-sucedidas podem ser afetadas. Isso é representado pela linha azul crescente. Para um $\delta >> 1.0$, a maioria das transações é classificada como insegura.

O δ correspondente ao ponto onde as métricas de precisão e *recall* cruzam F1 foi tomado como marco de avaliação dos MIH. Não é incomum aplicações que requeiram um *recall* maior que a precisão e vice versa. Contudo, conforme podemos observar em qualquer dos gráficos da Figura 5.3, onde as linhas vermelha, verde e azul representam as métricas f1, precisão e *recall*, respectivamente, a proporção entre *recall* e precisão se mantem aproximadamente uniforme a medida que δ avança. Assim, o ponto onde *recall* e precisão se cruzam representa uma boa régua de avaliação.

O ponto limite δ onde as métricas de precisão e *recall* cruzam F1 mostrado na Figura 5.3a é de aproximadamente $\delta \approx 0.7$. Tal δ supera significativamente os outros dois MIH avaliados.

Rede de Confiança + Arbitragem Descentralizada – RA

O mecanismo por trás do árbitro descentralizado associado à rede de confiança (RA), em vez de usar a confiança mútua comprador-vendedor, determina que o comprador e o vendedor cheguem a um consenso sobre um terceiro jogador em que ambos confiam. O comprador então transfere o pagamento para o terceiro jogador escolhido consensualmente, que retém



(a) R

(b) RA

(c) RD

Figura 5.3: O eixo horizontal apresenta o limite de confiança e o eixo vertical representa a magnitude de cada métrica (precisão, *recall* e f1).

o pagamento para o vendedor até que ele entregue o produto/serviço. Por se tratar de dados históricos não é possível realizar a transação por completo usando o árbitro. Assim, para viabilizar este estudo basta que ambos comprador e vendedor confiem em um terceiro jogador em comum. Com base nisso, este modelo atinge os melhores resultados de acordo com a Figura 5.3b, onde a intersecção de f1, recall e precisão ocorre em $0,965$, o melhor valor, e em um limite de confiança δ de $0,607$, um valor viável.

Os maiores resultados de todos os modelos comparados são descritos numericamente na Tabela 5.2, onde as linhas representam as métricas e as colunas representam os modelos. A primeira métrica 'Transações inseguras que falharam' representa todas as transações em que a entrega do produto não ocorreu conforme o esperado devido a algum comportamento desonesto do vendedor e isso foi previsto pelo MIH sob análise. Quanto maior for essa métrica, melhor será o modelo na prevenção da desonestidade dos vendedores. A segunda métrica é 'Transações inseguras bem sucedidas', o que significa que essas transações bem-

Tabela 5.2: Melhores métricas de cada solução comparada (R, RA e RD)

Métricas	R	RA	RD
Transações inseguras que falharam	287(82.71%)	336(96.83%)	287(82.71%)
Transações inseguras bem sucedidas	461(18.31%)	79(3.14%)	445(17.68%)
F1 = recall = precision	0.821	0.965	0.823
Limiar δ	0.666	0.607	0.663

sucedidas foram previstas erroneamente como insegurança pelo modelo. Quanto menor for essa métrica, melhor será o modelo. A terceira linha representa a intersecção das métricas f1, precisão e *recall*, apontando para o melhor limite de confiança de cada modelo. A Figura 5.3 apresenta os valores de *precision*, *recall* e F1 no eixo y, e os valores de lambda no eixo x. Finalmente, a última linha representa o limite de confiança δ onde ocorre a intersecção das métricas f1, recall e precisão.

Olhando novamente para a Tabela 5.2, pode-se ver numericamente que a maior intersecção f1, recall e precisão é $0,965$ para o modelo RA. Para todas as outras métricas, o modelo RA é significativamente melhor do que seus concorrentes.

Rede de Confiança + Depósitos de Garantia – RD

É importante relembrar que essa abordagem dos Depósitos em Garantia foi replicada do trabalho de Schwartzbach [235]. Schwartzbach concluiu que é difícil fornecer um protocolo de garantias de pagamento viável e eficaz com base em regras empíricas, e que projetar tal protocolo sem nenhuma informação sobre o comportamento dos jogadores é um problema intratável. Esta última conclusão nos motivou a propor o uso do modelo de rede de confiança como fonte de informação sobre o comportamento dos jogadores, tal como no modelo de Arbitragem (RA).

Tal MIH pareça ser uma estratégia eficaz, uma vez que os valores colaterais são sempre pelo menos iguais aos valores obtidos por meio de desonestidade. Contudo, há duas desvantagens a serem consideradas: 1) Primeiro, o protocolo é tendencioso para vendedores pois estes podem pagar como garantia em algumas situações os mesmos valores que os valores de seus produtos, mas ainda assim têm a chance de finalizar a transação com seus produtos e

o pagamento do comprador, de acordo com o modelo de negócios do OpenBazaar. 2) Como é possível ver na Figura 5.4, que mostra o crescimento dos custos de transação em função da taxa de confiança de compradores e vendedores, o protocolo de pagamentos nem sequer é calculável se o limiar de confiança for menor que $\phi <= 0,5$ (linha vertical azul escura). Caso contrário, para limiares de confiança mais altas, mas próximas de $0,5$ (como $0,55$), os valores de garantia são tão grandes que tornam tal pagamento impossível (veja as linhas vermelha e azul claro para compradores e vendedores, respectivamente).

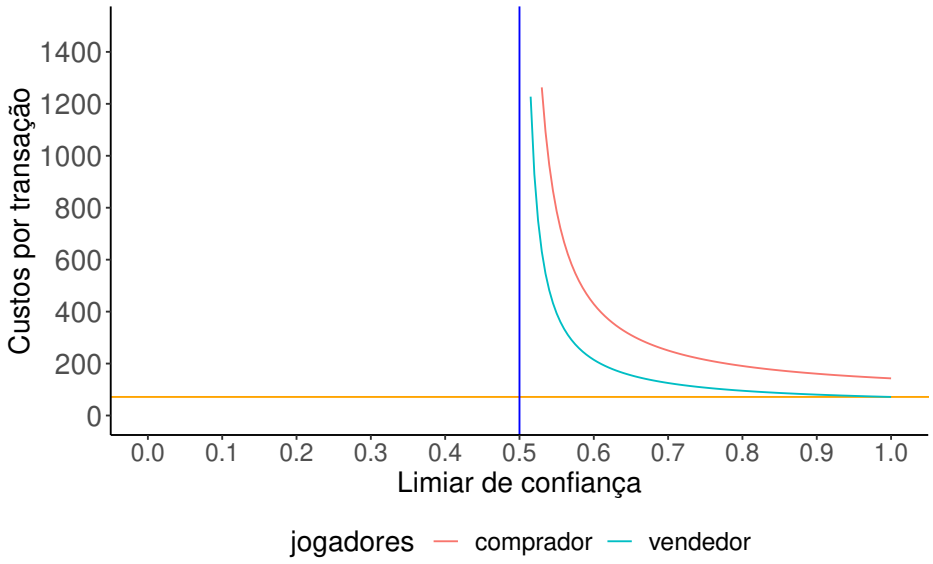


Figura 5.4: Custo da garantia de pagamento de acordo com a taxa de confiança do vendedor. A linha laranja horizontal representa o valor médio da transação. A linha azul escura vertical representa a taxa de confiança $\phi = 0.5$

Portanto, restringimos os pagamentos de garantia de acordo com um modelo híbrido: desde que o limiar de confiança δ seja menor que a taxa de reputação/confiança necessária para que o vendedor pague mais que o dobro de seu valor[7], assume-se que as garantias de pagamento não são viáveis e o MIH se limita à rede de confiança. Isso significa que se o vendedor precisar pagar mais do que o dobro do valor de seus produtos como garantia, essa garantia será muito cara para continuar a transação. Como o comprador não tem a oportunidade de se comportar desonestamente, de acordo com o modelo de negócios do OpenBazaar, não é necessário exigir garantias de pagamento deste.

[7]Valores do vendedor mais valores do comprador, assumindo para a simplificação da análise que os valores do comprador e do vendedor são aproximadamente iguais (produto e pagamento).

Voltando à Figura 5.2c, pode-se ver que o protocolo de garantia de pagamentos evita a explosão de falsos positivos para valores muito grandes de δ, onde a maioria das transações verdadeiras são marcadas como inseguras (linha azul claro), mas isso acontece após sua intersecção entre f1, *precision* e ponto de *recall* (veja a Figura 5.3c). De modo que, mesmo com sérias questões de viabilidade, o protocolo de garantias de pagamento mais a rede de confiança permanece quase tão eficaz quanto a rede de reputação bruta, como se pode ver na Figura 5.3c e na Tabela 5.2, onde o ponto de intersecção de F1, recall e precisão são quase os mesmos em ambos. Por isso, os resultados absolutos da predição (transações mal sucedidas marcadas como inseguranças e transações bem sucedidas marcadas como inseguranças, de acordo com a Tabela 5.2) também são quase os mesmos em ambos os modelos.

Olhando novamente para a Figura 5.3, podemos ver que mesmo os modelos menos eficientes (R e RD) conseguem prever a maioria das transações malsucedidas para um limiar de confiança adequado (linha vermelha clara abaixo da linha vermelha escura). Observe também que os MIHs de fato aplicados na plataforma OpenBazaar (linha vermelha escura na Figura 5.2) – ou seja, arbitragem unilateral e reputação com base em *feedback*, provaram ser menos eficazes do que todas as soluções testadas aqui.

Respondendo à QP e Ameaças à Validação

O melhor desempenho no geral é do modelo RA, em termos de incentivos de honestidade e também considerando F1, *precision* e *recall*, considerando os resultados da Subseção 5.3.4. Essa é a resposta curta e simples para a QP deste estudo e também desta Tese, até aqui. Para uma resposta mais detalhada, no entanto, é preciso levar em conta situações em que R ou RD parecem superiores ou até mais viáveis – por exemplo, esse é o caso quando a honestidade é o comportamento predominante e qualquer estratégia de mediação custosa é desnecessária – neste caso, R parece mais aplicável; ou, por outro lado, quando a honestidade apresenta um "comportamento médio ou típico" ou quando as transações são críticas e devem ser garantidas inequivocamente – neste caso, RD é uma escolha melhor, apesar de seu custo.

Como nossos resultados foram utilizados para indicar MIHs superiores aos aplicados na plataforma OpenBazaar, eles devem ser considerados juntamente como uma importante ameaça à validade. A análise apresentada aqui é baseada em dados históricos e, como tal, não pode ser usada como um medidor de impacto das soluções comparadas, pois elas não

estiveram aplicadas em um ambiente de fato real.

5.3.5 Conclusões

O estudo apresentado nesta Seção comparou modelos de incentivo à honestidade (MIHs) obtidos a partir de uma revisão de literatura que foi guiada pelos requisitos de descentralização, tolerância a transações não verificáveis (informações incompletas) e não autenticação (anonimato), com base em métricas de *precision*, *recall* e F1. Os MIHs avaliados foram: rede de confiança sem *feedback* (R), arbitragem descentralizada (RA, associada à rede de confiança) e depósito de pagamento (RD, também associado à rede de confiança). A rede de confiança sem *feedback* desempenha um papel especial, servindo como fonte de informações sobre o comportamento dos jogadores. Esse papel é comumente desempenhado por oráculos descentralizados em TLRD (*blockchains*, por exemplo).

A comparação foi feita usando os MIHs selecionados para prever transações malsucedidas (produtos não entregues ou entregues com problemas) em um conjunto de dados rotulados manualmente extraídos da plataforma de *e-commerce* descentralizada OpenBazaar. Tais previsões são baseadas em quanto cada modelo é capaz de classificar a segurança de cada transação, e baseadas em um limite de confiança ideal θ para prever as transações reais bem-sucedidas e malsucedidas. Tal limite ideal é aquele em que as métricas de *precision*, *recall* e F1 se cruzam. Além das comparações apresentadas aqui, as vantagens e desvantagens de cada modelo são descritas, conforme mostrado na Tabela 5.3.

Concluindo, observou-se que a aplicação da rede de confiança sem *feedback* associada à arbitragem descentralizada (RA, veja Tabela 5.2) mostrou desempenho significativamente superior às outras com base em métricas de *recall*, *precision* e F1. Esta constatação fica mais clara ao observarmos a Tabela 5.2, onde na coluna RA, a terceira linha que descreve o ponto de intersecção entre precisão *recall* e F1 é igual à 0.965, bem superior às demais (0.821 e 0.823). Os MIHs originais do OpenBazaar tiveram desempenho pior quando comparados aos MIHs elicitados. RA, a solução que superou as outras, atingiu $F1 = 0,965$ (veja Tabela 5.2), o que é suficientemente alto.

Tabela 5.3: Vantagens e desvantagens de cada modelo

Modelos	Vantagens	Desvantagens
R	Por si só é uma boa solução, mas pode ser melhorada se associada a outras soluções.	Fornece informações sobre o comportamento dos jogadores, mas não garante a transação.
RA	A solução que superou as outras se associada a um sistema de inferência de comportamento, como uma rede de confiança.	Não funciona por si só.
RD	Elimina eficientemente a vantagem que motiva a atitude desonesta, desde que seja economicamente viável para o domínio em que for aplicado e anônimo o suficiente para evitar ganhos não mapeados.	Não funciona por si só e na maioria das vezes não é viável porque requer um limiar de confiança muito alto para tornar os depósitos viáveis.

5.4 Incentivando a Honestidade em Mercados Descentralizados: Abordagem Baseada em Simulação

5.4.1 Introdução

Soluções anteriores para o DCV em mercados descentralizados geralmente incorporam pré-condições custosas que garantem a verificação de todas as operações ao longo do protocolo de transação, o que não é viável para aquelas transações onde qualquer operação envolvida é não verificável – por exemplo, serviços do mundo real ou pagamentos em dinheiro. Tais pré-condições garantem a verificação de todas as operações ao longo do protocolo de transação entre comprador e vendedor.

Além disso, a virtualização descentralizada de eventos e valores não verificáveis como serviços e produtos do mundo real – transações não verificáveis – apresenta desafios que findam por levar a violação dos princípios da descentralização [20, 174, 258, 155, 285, 187, 219, 206], um problema relevante conforme observado na literatura (vide Seção 2). Essa limitação dificulta a adoção de soluções descentralizadas em mercados descentralizados [182, 184, 75, 201, 183].

Esta Seção realiza uma comparação entre soluções da literatura para o DCV, removendo essas pré-condições e até mesmo recombinando adequadamente as principais características de tais soluções, compondo novas soluções possíveis para apontar alternativas aplicáveis a mercados descentralizados para resolver tal dilema (DCV), mesmo envolvendo transações não verificáveis. A proposta depende da hipótese de que estimular a honestidade é suficiente para fornecer uma taxa aceitável de conclusão bem-sucedida de transações (entrega de bens ou serviços). Para isso, as soluções propostas utilizam uma ou mesclam duas ou mais das seguintes características: 1) arbitragem descentralizada, onde um intermediário livremente definido entre as partes assume o papel de árbitro (mediador) em eventuais conflitos [20, 219, 187, 206], 2) Rede de confiança com [289] e sem *feedback* [42], na qual uma rede de confiança é estabelecida em torno do agente à medida que ele participa das transações ou atua como árbitro, 3) categorização das transações que permite estabelecer confiança separadamente para cada categoria de transação, o que em alguns casos melhora os resultados, conforme observamos, e 4) depósitos de segurança feitos antes da transação

para um intermediário – que pode ser um protocolo automático – como garantia dos valores trocado [174, 20, 258].

Avaliar a eficácia de cada solução em comparação com outras em um mercado descentralizado cuja dinâmica pode ser impactada pelo comportamento fraudulento dos agentes motivado por ganhos econômicos é um esforço complexo. Devido à flexibilidade que ele oferece [128], optamos por desenvolver e executar um Simulador baseado em Agentes (ABS) como uma ferramenta de avaliação de eficácia. Os resultados do ABS produziram evidências de que as soluções propostas mostram eficácia satisfatória, onde o árbitro descentralizado encorajado pela rede de confiança sem *feedback*, aumenta significativamente a chance de sucesso da transação. Resultado que converge na mesma direção daqueles obtidos na Seção 5.3. Por exemplo, em um ambiente com uma taxa de honestidade (ou seja, a chance de um agente passivo agir honestamente) de 40%, a chance de sucesso salta de 30% para 88,9%.

As principais contribuições desta Seção incluem: (i) uma aplicação abrangente e exemplificada de ABS que pode servir como suporte para orientar gerentes, profissionais de TI e pesquisadores interessados em entender, construir ou aplicar protocolos de combate à fraude em mercados descentralizados online; (ii) o fornecimento de uma base sintetizada, formando um corpo de conhecimento, para referência nos próximos Capítulos desta Tese e também para o desenvolvimento e pesquisa a respeito do tratamento do DCV em mercados DAnV.

5.4.2 Visão Geral das Soluções

Este trabalho avalia soluções que visam incentivar a honestidade em agentes potencialmente desonestos em transações envolvendo operações não verificáveis em mercados descentralizados. Conforme já mencionado na Seção 5.2, os resultados são divididos em três classes principais de soluções: redes de confiança, arbitragem e protocolos de depósitos de garantia. Essas três classes são coletivamente e geralmente chamadas de Modelos de Incentivo à Honestidade (MIHs). Aqui também examinamos combinações de modelos de mais de uma classe.

Em um cenário de negociação, como por exemplo uma transação de comércio eletrônico, é natural que cada parte priorize seus próprios interesses, fazendo com que um comportamento desonesto seja percebido como uma opção vantajosa, pelo menos no curto prazo (no

longo prazo, é provável que os agentes desonestos sejam punidos de alguma forma). Este cenário nos remete a dois princípios já mencionados, o primeiro é o Equilíbrio de Nash da teoria dos jogos [193], onde o melhor resultado jamais poderá ser garantido, mas um jogador pode adotar uma dada estratégia que garanta um resultado aceitável independentemente das ações dos outros. Este dilema é o problema de interesse desta Tese e já foi mencionado em Capítulos anteriores, tendo sido definido formalmente na Seção 3.4.1, Definição 2. O segundo princípio é o Preço da Anarquia (PoA), conceito que quantifica a perda de eficiência em jogos devido ao comportamento não colaborativo dos jogadores, e que também já foi estabelecido na Seção 3.3 (Capítulo 3).

A Tabela 5.1 apresenta todas as soluções coletadas da literatura e identifica as pré-condições aplicadas por cada uma para verificar as transações e evitar desonestidade. Os recursos usados quando tais pré-condições são evitadas serviram para compor os modelos comparados aqui. Como se pode ver na Tabela 5.1, nenhuma das soluções implementa exclusivamente a rede de confiança, embora sem essa rede de confiança, algum outro tipo de inferência de comportamento deva ser fornecido (como oráculos de contrato inteligente, por exemplo) para que um MIH possa ser aplicado. Para fins de controle, avaliaremos também um cenário sem rede de confiança, e, por consequência, sem nenhum outro MIH – ou seja, dependendo apenas da honestidade dos agentes – além de todos os cenários descritos na Tabela 5.4.

Depósitos de Segurança

O protocolo de depósito colateral é construído sobre a pesquisa conduzida por Schwartzbach [235], conforme descrito em sua publicação sobre pagamentos. Schwartzbach apresenta um modelo para um mercado descentralizado dependente de transações não verificáveis.

Rede de confiança

Aqui aplicamos o mesmo modelo de Rede e Confiança demonstrado na Seção 5.3. Originalmente focada em uma rede *peer-to-peer*, esta Rede de Confiança estabelece a autenticidade das conexões entre chaves públicas e seus proprietários. Com o tempo, os usuários acumulam chaves de indivíduos em quem confiam, formando uma rede de confiança descen-

tralizada sem uma autoridade de certificação centralizada. A legitimidade é alcançada por meio do acúmulo e redistribuição de certificados de terceiros, resultando em uma rede de chaves públicas flexível, descentralizada e tolerante a falhas, verificada por consenso entre usuários [42].

Para transações com operações não verificáveis, este modelo pode fornecer confiança entre compradores e vendedores que nunca tiveram interações diretas com base na experiência daqueles com quem interagiram separadamente. Zindros [289] utiliza uma rede de confiança semelhante, mas com base em *feedback* voluntário e escasso, o que retarda o progresso da rede de confiança. Zhang et al [285] aplica um modelo semelhante. Nossa análise comparativa traz ambas as variações deste modelo de rede de confiança, com e sem *feedback*.

Este modelo de reputação funciona bem com a moderação de transações usando árbitros descentralizados confiáveis, uma vez que, dada uma população Q de algumas transações $S' << Q$, já é possível identificar árbitros que têm a confiança dos agentes envolvidos. Isso ocorre porque uma pequena porcentagem da população $Q' << Q$ tende a atuar como árbitros.

Arbitragem Descentralizada

Para fins de comparação entre soluções, este artigo aplicou uma estratégia de arbitragem semelhante à utilizada por Zindros [289], substituindo o sistema de reputação dos árbitros baseado em reputação por pontos e currículo por uma Rede de Confiança descentralizada.

Definição da Solução

Por fim, um ou mais modelos da literatura (veja a Seção 5.2) são combinados em cada solução proposta. A coleção de soluções envolvendo múltiplos modelos e soluções envolvendo apenas um modelo formam um superconjunto de soluções de incentivo à honestidade (MIH) que incluem recursos de inferência ou verificação de honestidade para transações não verificáveis em ambiente simulado. Os desempenhos das soluções neste superconjunto são então comparados e classificados de acordo com sua eficácia (ou seja, sua capacidade de estimular a honestidade e, portanto, melhorar a taxa de conclusão de transações – "sucesso"). A Tabela 5.4 especifica os recursos de todas as soluções no superconjunto que está sendo considerado.

Tabela 5.4: Soluções propostas (A, B, C, E e G), fruto da combinação de múltiplos modelos MIH, e Soluções da Literatura – D [235]; F [289]; e, H [174, 20, 258], composta por apenas um modelo. Já a solução I conta apenas com a rede de confiança sem *feedback* e será tratado como referência nos resultados.

	Soluções								
Modelos	A	B	C	D	E	F	G	H	I
Arbitragem	✓	✓			✓	✓			
Categorias	✓		✓		✓		✓		
Depósito de Garantia			✓	✓			✓	✓	
Com *Feedback*					✓	✓	✓	✓	

'A' é a solução que combina um auditor e diferenciação da honestidade de cada agente por categoria de valores negociados, de modo que um determinado agente pode confiar em outro para um tipo (categoria) de transação, mas não confiar no mesmo agente para outro tipo (categoria) de transação. 'B' usa apenas um auditor intermediário confiável e descentralizado em sua solução. 'C' usa depósitos de segurança e diferencia a confiança entre agentes por categorias. 'D' usa apenas depósitos de segurança para garantir a solução. 'E' usa um auditor intermediário e confiança baseada não em relacionamentos anteriores, mas no feedback dado pelos agentes sobre a honestidade dos outros, além de classificar a honestidade dos agentes por categoria de transação. Seguindo o mesmo raciocínio, temos as soluções 'F', 'G' e 'H'. 'I' não oferece recursos para lidar com desonestidade além da rede de confiança. Este último modelo é incluído aqui para avaliar potenciais ganhos "absolutos" pelas outras soluções (consulte a Tabela 5.4). Todas as soluções na Tabela 5.4 seguem a Definição 3[8]. O cenário sem nenhuma forma de controle sobre a honestidade dos agentes durante as transações também foi executado para fins de controle.

Definição 3 (Solução Genérica)**.** *Uma solução de incentivo à honestidade descentralizada é representada genericamente como* $J = \{K, Q, T, \zeta^t(i,j) \,|\, \forall t \in T \, e \, (i,j) \in Q \times$

[8]Além da lista de símbolos do início deste documento, a Tabela C.3, Apêndice C, lista todos os símbolos usados exclusivamente nesta Seção.

$Q, \eta^t(G, \zeta) \mid \forall t \in T\}$, onde:

1. *K é o jogo de acordo com a definição 2.*

2. *ζ^t como uma função de inferência de honestidade (um sistema de reputação, por exemplo), onde $\zeta^t(i, j)$ define a confiança do agente i no agente j de acordo com o estado de i no tempo t.*

3. *η^t representa algum modelo de garantidor de transação como arbitragem descentralizada ou depósitos de garantia, onde $\eta^t(G, \zeta(i, j))$ retorna um conjunto bruto de operações $\{\gamma_0, ..., \gamma_n\}$ (veja Definição 2), se i não confia em j. Ou ainda algum modelo de transação sem garantias, a depender do estado de j no tempo t, que culmina em um conjunto diferente de operações $\{\gamma_0^{'}, ..., \gamma_m^{'}\}$. Isto é, se i confia em j, a transação ocorre sem garantias, caso contrário um depósito em garantia é solicitado ou o arbitro é acionado (a depender da solução).*

Assim, cada solução na Tabela 5.4 inclui um ou nenhum modelo garantidor de transação η (depósitos de segurança ou arbitragem descentralizada) e um ou nenhum modelo de inferência de honestidade ζ (Rede de confiança com ou sem feedback, com base em transações classificadas ou não classificadas).

5.4.3 Experimento de Simulação

Metodologia

O trabalho apresentado nesta Seção propõe uma comparação por simulação de soluções de contorno já aplicadas na literatura para o Dilema dos Compradores e do Vendedores (DCV) ou problemas que envolvam o mesmo dilema indiretamente. Além disso, recombinamos características dessas soluções que visam incentivar a honestidade em vez de verificar operações para propor novas soluções (ver Tabela 5.4).

A hipótese a ser testada aqui aponta para o fato de que é possível incentivar a honestidade usando soluções descentralizadas mesmo na presença de operações não verificáveis. O objetivo é identificar estratégias superiores de incentivo à honestidade que, mesmo sem verificar as operações, sejam capazes de recompensar e encorajar a honestidade em uma população de agentes com diversas categorias de valores trocados e diferentes perfis de honestidade.

Para isso, a Simulação Baseada em Agentes (ABS) foi usada para registrar a eficácia de cada agente separadamente e da população como um todo por meio de múltiplas simulações para diferentes configurações de soluções mutuamente exclusivas (ver Tabela 5.4) em diferentes taxas de honestidade.

Design de Simulação

Com o objetivo de simular mercados descentralizados onde agentes produzem e comercializam valores, este experimento utilizou a Simulação Baseada em Agentes (ABS). Além de reproduzir tais interações, parâmetros como honestidade, memória, risco, falência e sucesso foram incorporados.

O modelo AB aqui apresentado foi desenvolvido com base no trabalho de Fagiolo, Moneta e Windrum [86], que estabelece que tal tipo de simulação deve ser:

1. **Uma perspectiva de *bottom-up*** Propriedades econômicas são inferidas com base no resultado de microdinâmicas envolvendo agentes.

2. **Heterogeneidade** Agentes são prosumidores cada um com a capacidade de produzir um tipo de produto/valor, embora todos precisem de todos os produtos disponíveis para comércio.

3. **Delimitada de forma racional** Onde agentes são restritos a comercializar e se relacionar apenas em sua vizinhança local.

4. **Interações diretas em rede** As decisões dos agentes dependem diretamente, por meio de expectativas adaptativas, das escolhas passadas feitas por outros agentes na população.

O ambiente de simulação consiste em um Grid 2D 256×256, contendo um total inicial de 100 agentes que pode crescer até um máximo de 1.000 agentes conforme a simulação avança. Para ilustrar, observe uma captura instantânea da tela durante uma das execuções da simulação na Figura 5.5. Assim, os agentes podem mover-se uma casa por vez e, produzindo uma unidade de um tipo de valor/produto negociável a cada ciclo (cada agente é capaz de produzir um tipo específico de produto/valor) ou negociar itens em seu inventário para obter outros valores que ele não é capaz de produzir.

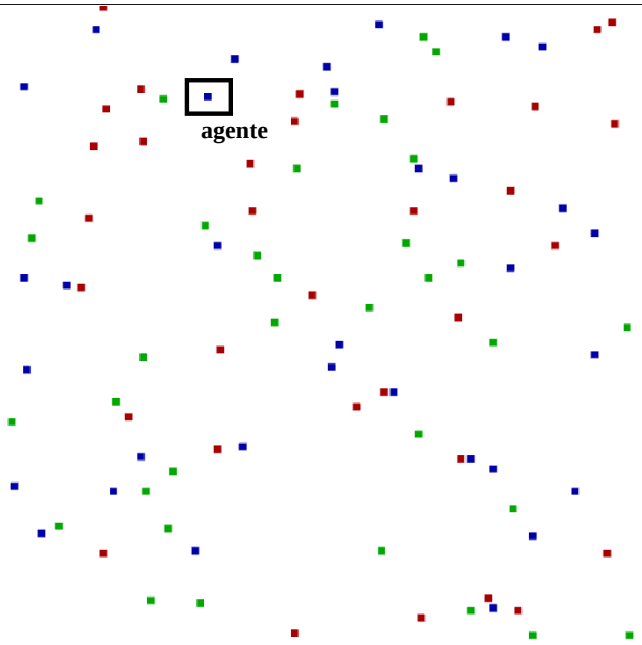


Figura 5.5: *Grid* de simulação onde cada ponto colorido é um agente – conforme descrito no quadro preto – negociando ativamente em sua vizinhança.

Agentes

Os agentes são capazes de mover uma posição do Grid por vez, decidindo a cada passo de tempo fabricar uma unidade de tipo único de valor que cada agente é capaz de fabricar ou negociar valores (itens) em seu inventário para obter outros valores que eles não são capazes de produzir. Um passo de tempo pode ser visto como um ciclo onde todos os agentes concluem uma transação ou fabricam um valor (item) para seu inventário.

Definição 4. *Na simulação, um agente é modelado como* $q = \{c_q, (b_0, b_*), \alpha^t\}$*, onde:*

1. c_q *corresponde ao valor que o agente pode fabricar.*
2. (b_0, b_*) *são os estados inicial e desejável final, respectivamente. Considere um estado* $b = \{\nu_C, (x, y)\}$*, onde* ν_C *representa um conjunto de valores (itens) no inventário, um para cada categoria de valor* $c \in C$*, e* (x, y) *se refere a uma posição no Grid 2D.*
3. α^t *representa uma função de ação no passo de tempo* t*, onde* $\alpha^t(b_n)$ *retorna um movimento aleatório para alguma posição adjacente e um algum produto fabricado* p *ou uma transação* η *(veja Definição 3) com algum outro agente adjacente, dependendo do estado* b_n*.*

Procedimento Principal da Simulação

Definimos sucesso econômico no ambiente simulado como a capacidade dos agentes de produzir e negociar valores de diferentes categorias, alcançando seus objetivos sem ir à falência. O objetivo de um determinado agente é acumular um inventário $M \geq \nu_*$ para cada uma das categorias de valor – onde ν_* é a meta de qualquer um dos agentes para cada uma das categorias de valor. Se o agente atingir essa meta, como recompensa, ele se duplica. Se no final de L passos de tempo o agente não atingir essa meta ν_* para todas as categorias de valor, esse agente é removido da simulação (falência).

Se a população de agentes atingir o número total máximo de agentes (1.000), a simulação é interrompida e a economia do agente como um todo é declarada bem-sucedida para essa execução específica. Da mesma forma, quando todos os agentes são removidos devido à falência, a execução da simulação é interrompida e o cenário é registrado como uma falha de simulação. Cada cenário foi executado 1.000 vezes. Um cenário é uma configuração de simulação que representa uma das soluções sob análise (veja Tabela 5.4) usando um conjunto específico de valores de parâmetros. Cada execução de simulação consiste em uma repetição de um determinado cenário. Mesmo com todos os mesmos parâmetros, duas execuções de simulação podem retornar resultados diferentes porque dois agentes só transacionam se estiverem em posições adjacentes no Grid, e os movimentos de um agente no Grid são aleatórios. O pseudocódigo em Algoritmo 1 descreve o fluxo principal da simulação em mais detalhes.

No Algoritmo 1, que descreve a rotina principal da simulação, a primeira linha do cabeçalho garante que a população inicial de agentes Q tenha 100 agentes. A segunda linha do cabeçalho espalha os agentes ao redor do Grid 2D. A Linha 1 do corpo do pseudocódigo define o passo de tempo inicial $t = 0$. A Linha 2 verifica se a população total $|Q|$ é zero, falência, ou maior que 1000, sucesso. A Linha 3 obtém um agente i^t de Q, onde este 't' significa que tal agente está no passo de tempo t. A Linha 4 verifica se o agente i^t está vazio, se estiver, significa que não há mais agentes no passo de tempo t. A Linha 5 chama a função de ação α no passo de tempo t para o estado do agente b_i, de acordo com a Definição 4 do agente, e retorna o agente no próximo passo de tempo $t + 1$. A linha 6 verifica se o passo de tempo do agente menos o passo de tempo inicial do agente t_0^i é maior ou igual ao tempo de vida máximo L de qualquer agente, no final do qual i precisa ter inventário suficiente

Algorithm 1 Procedimento principal.

Require: $|Q| = 100$

Ensure: $GRID \Leftarrow Q$

$t \Leftarrow 0$
while $|Q| \geq 0 \ \ \& \ \ |Q| \leq 1000$ **do**
    $i^t \Leftarrow$ getAgent(t, Q)
    while $i^t \neq \varnothing$ **do**
        $i^{t+1} \Leftarrow \alpha^t(b_i)$
        if $(t+1) - t_0^i \geq L$ **then**
            $Q \rightarrow i$
        else if $\nu_C^i \geq \nu_*$ **then**
            $\nu_C^i,\ t^i \Leftarrow 0,\ t_0^i$
            $Q \leftarrow i$
        end if
        $i^t \Leftarrow$ getAgent(t, Q)
    end while
    $t \Leftarrow t + 1$
end while
return $\Leftarrow |Q| \neq 0$

para se duplicar ou ser removido. A Linha 7 remove i falido da população Q. A Linha 8 verifica se o inventário do agente ν_C^i é maior que o máximo ν_* para todas as categorias de valor trocável. A Linha 9 define o inventário do agente ν_C^i e o tempo de vida t^i de volta a zero. A Linha 10 reinsere i na população de agentes, duplicando-o. A Linha 12 obtém um novo agente da população Q no passo de tempo t. A Linha 14 vai para o próximo passo de tempo. A Linha 16 retorna sucesso se $(|Q| \neq 0)$, ou então falido, $(|Q| = 0)$.

Trocar valores é o equivalente à troca de produtos e dinheiro em transações e cujo valor de troca define as categorias de transação correspondentes. A definição de honestidade usada nesta simulação é absoluta ou ponderada de acordo com as categorias de transações em uma tentativa de simular uma sociedade real (a depender da solução aplicada categorizar ou não a honestidade, conforme Tabela 5.4), onde um indivíduo se comporta de forma diferente para diferentes tipos de transações. Uma transação consiste em um conjunto de duas operações de troca de valor em caso de sucesso (pagamento e entrega do produto), uma operação unilateral pelo agente ativo em caso de desonestidade do agente passivo, ou a mesma operação, seu reembolso e uma remuneração ao árbitro se ele/ela evitar a atitude desonesta do agente passivo (assumimos que esta remuneração consiste em um terço do pagamento original pelo agente ativo).

Validação do Modelo Baseado em Agente (ABM)

Marks [176] apresentou uma estrutura para validar Modelos Baseados em Agentes (ABM) com base em dados de amostra do mundo real. O presente experimento de simulação replica um mercado online descentralizado, categoria de aplicação que, por si só, tem pouca disponibilidade de dados históricos, mais especialmente dados associados a iniciativas de grande escala. No entanto, Arps e Christin [19] nos forneceu os dados de um desses mercados chamado OpenBazaar. Aqui, usamos esses dados para a validação do nosso ABS.

Observe, no entanto, que, como nenhum mercado descentralizado particular é simulado aqui, mas sim situações gerais e recorrentes em qualquer mercado descentralizado, comparar registro por registro entre dados simulados e do mundo real não faz sentido. Em vez disso, uma propriedade representativa, como a taxa de transações com falha, é comparada. Transações sem sucesso do conjunto de dados OpenBazaar significam que seus comprado-

res associados, conforme observado em comentários de texto registrados [9], não receberam o produto.

$$V \equiv m(R) * \left(\frac{v}{m(U)} + \frac{1-v}{m(Z)} \right) \tag{5.7}$$

A equação (5.7) representa a validação do ABM de acordo com Marks [176]. Quanto mais próximo de $1,0$ melhor o ABM, onde U representa a saída do ABM (manteremos o conceito de 'saída do sistema' em aberto momentaneamente), Z representa a saída real do sistema OpenBazaar, R representa $U \cap Z$ que aqui significa a proximidade entre a saída do sistema real e a saída do ABM com base em todos os modelos de incentivo à honestidade analisados aqui em cada passo de tempo. Um *script* R disponível publicamente é usado para isso, veja o Apêndice B. $v \in [0,0,1,0]$ é uma constante que descreve o *tradeoff* entre precisão e completude. Aqui usamos $v = 0,7$ para priorizar a completude apesar da precisão. Poderíamos ter usado $v = 0,5$, mas optamos por $v = 0,7$ porque é um modelo de simulação mais generalista e, como um modelo generalista, a completude é uma propriedade mais forte em comparação com a precisão. A função $m()$ representa uma métrica de escala de razão definida de acordo com a viabilidade e funcionalidade.

Usando a taxa de transações malsucedidas como $m()$, temos: 9.901 transações malsucedidas por 124.035 transações totais no ABM (U, saída do sistema simulado), 113 transações malsucedidas por 1.202 transações totais no OpenBazaar (Z, saída do sistema real) e 43 transações malsucedidas e 611 transações totais para $U \cap S$. Com base nesses números, observe a Equação 5.8:

$$V \equiv m(R) * (\frac{v}{m(U)} + \frac{1-v}{m(Z)}) = \frac{43}{611} * (\frac{0.7}{\frac{9901}{124035}} + \frac{1-0.7}{\frac{113}{1202}}) = 0.842 \tag{5.8}$$

Então, a completude/precisão da simulação atual é $0,842$, quando comparada aos dados reais do OpenBazaar. Como é próximo de 1,0, considera-se o modelo validado [176].

Implementação

North et al [198] forneceu uma visão geral das ferramentas de implementação de Simulação Baseada em Agente (ABS) disponíveis, influenciando a seleção do Repast Simphony [62]

[9] Tal observação foi feita manualmente no contexto da análise descrito na Seção 5.3

para o trabalho apresentado nesta Seção. O Repast Simphony é um sistema de modelagem baseado em Java e um kit de ferramentas que oferece suporte ao desenvolvimento de modelos de agentes de interação altamente flexíveis tanto para uma grande disponibilidade de recursos computacionais, quanto simulações envolvendo recursos computacionais mais limitados [63]. Ele permite o desenvolvimento de modelos por meio de *statecharts* em Groovy ou Java.

Para analisar os dados, a linguagem funcional R foi selecionada devido à sua rica diversidade de bibliotecas gráficas. Tanto o código-fonte em Java quanto em R estão disponíveis online nos repositórios do Github [10], de acordo com o Apêndice B.

Distância de confiança

Na Rede de Confiança, a confiança é baseada em experiências acumuladas com agentes próximos àquele cuja honestidade está sendo estimada. O cálculo de proximidade envolve a busca por caminhos possíveis no grafo gerado pela transação entre dois agentes ou entre eles e outros agentes. O parceiro com o maior número de caminhos é considerado o mais confiável. Se um agente honrou seus compromissos no passado, os valores negociáveis que ele negociou circulam na rede, deixando um rastro que indica sua honestidade para uma categoria de transação específica, semelhante a como a validade da chave pública se propaga em uma Web-of-Trust (Rede de Confiança) para verificação de chave. À medida que as transações progridem, os agentes acumulam listas de outros agentes potencialmente honestos, com outros valores trocáveis incluídos em tal lista para um determinado agente, aumentando a probabilidade de tal agente ser honesto. Tal modelo de implementação, embora seja uma solução incompleta, simula bem a sociedade real, pois um indivíduo não tem acesso à opinião de todos sobre uma determinada pessoa, mas apenas aqueles com quem ele interage. Da mesma forma, um determinado agente só tem informações sobre outros agentes cujos valores transferidos já estavam em sua posse.

O algoritmo resumido acima identifica caminhos potenciais entre dois agentes no grafo de confiança usando uma versão adaptada do algoritmo GroupRep [253]. O GroupRep foi escolhido por sua representação efetiva de relacionamentos de confiança que surgem naturalmente entre indivíduos em uma sociedade e porque é adequado para um ambiente onde

[10] https://www.github.com/

dois agentes não interagem muitas vezes ao longo de suas vidas.

Uma implementação alternativa do modelo de Rede de Confiança com *feedback* comparado aqui funciona de forma semelhante, mas contando o *feedback* como um tipo especial de transação (único que carrega informação de honestidade) em vez de interações diretas [274].

Honestidade

Com base na definição de distância de confiança apresentada, podemos descrever a decisão de um determinado agente confiar em outro como o evento X_{ij} que indica que qualquer um dos produtos repassados por esse agente j esteve na posse do agente i como:

$$X_{ij} = \bigcup_{k \in M_x(j)} h_{kj} \tag{5.9}$$

Onde i representa o agente que deve decidir confiar ou não e j representa o agente cuja honestidade está sob suspeita. M_x representa o conjunto de produtos já repassados por j da classe c, e k se refere a um desses produtos. Por sua vez, h_{kj} se refere à probabilidade de um dado produto k já repassado por j atingir o estoque de i. No entanto, ganhar a confiança de outro agente por si só não significa necessariamente que o outro agente seja honesto. A função que define a honestidade real de um dado agente j para uma dada classe de transação c é definida de acordo com a equação (5.10).

$$\chi_c(j) = \begin{cases} 1 & \text{se } \psi > \text{MAX}(1-g, \delta) \\ 0 & \text{senão} \end{cases} \tag{5.10}$$

Onde ψ define uma função aleatória que retorna um número $n \in [0, 1]$, MAX também é uma função e retorna o maior valor de seus dois parâmetros, g é uma constante $g \in]0, 1[$ definida nos parâmetros de simulação e que representa a honestidade do agente. A taxa de honestidade geral de uma população equivale ao valor médio de g. Por fim, $\delta \in]0, 1[$ é um fator definido pela Equação 5.11 e elaborado para ser proporcional ao tempo de vida restante o agente e seu inventário.

$$\delta_c(j) = \frac{\frac{t}{L}}{2} + 1 - \frac{\frac{\nu_c(j)}{\nu_*}}{2} \tag{5.11}$$

Onde t é o passo de tempo na vida de um agente em que a transação ocorre e L é o tempo de vida total do agente no final do qual o agente deve ser eliminado se ainda não tiver

atingido a meta de estoque $\nu(j) > \nu_*$, onde ν_c é a função que descreve o estoque de um dado valor de troca c e ν_* é o total suficiente para o agente se duplicar. Os valores de troca seriam equivalentes aos produtos e dinheiro trocados em transações, seu tipo defineria sua categoria.

Em resumo, a honestidade de um agente é uma função booleana que tem uma chance de $1 - g$ de ser verdadeira no início da vida deste agente. A simulação assume que, à medida que a vida deste agente progride, esta chance é influenciada pelas tensões experimentadas por tal agente – como pode acontecer na vida de um ser humano, por exemplo: quanto menor o estoque do produto a ser negociado, maior a chance do agente agir desonestamente. Da mesma forma, também é razoável supor que quanto menor o tempo de vida do agente, maior a chance desse agente agir desonestamente.

5.4.4 Resultados

Para cada solução na Tabela 5.4, são apresentados o desempenho da população, o sucesso da economia simulada e a eficácia das soluções em evitar transações malsucedidas.

Formato e Métricas

O conjunto de dados resultante de várias execuções do ABS compreende duas tabelas distintas: uma contendo dados para cada registro final de cada execução e a outra contendo uma amostragem aleatória de vários estados sequenciais da população de agentes ao longo da simulação. A tabela que documenta os registros finais de cada execução de simulação tem como resultado, além dos campos-chave, apenas um campo booleano que indica o sucesso ou fracasso de cada simulação (com base em se todos os agentes perecem ou não, antes da conclusão da execução da simulação).

Da mesma forma, a tabela que captura registros parciais de simulação ao longo do processo inclui três campos principais (além dos campos-chave que identificam aquela execução): um saldo proporcional de transações malsucedidas até aquele ponto, o saldo total de transações malsucedidas evitadas pela solução empregada e o saldo proporcional de transações bem-sucedidas. Ao longo de todo o experimento, a simulação foi executada 81.000 vezes para nove taxas de honestidade distintas $\{0,1,0,2,..,0,9\}$.

A análise dos dados revelou uma curva de densidade semelhante a uma distribuição normal para a taxa média de sucesso da população. Foi utilizada inferência estatística, empregando intervalos de confiança de 95% de nível de certeza, para avaliar o sucesso da população e a diversidade de agentes. Além disso, uma análise de correlação de Spearman foi conduzida para examinar a relação entre o número total de transações malsucedidas evitadas e falhas totais em cada passo de tempo de simulação, entre as várias soluções testadas.

Desempenho Econômico

Antes de iniciar a avaliação das soluções executamos nosso cenário de controle comparando o ambiente simulado sem nenhuma forma de incentivo à honestidade e usando um Rede de Confiança. Segundo Schwartzbach [235], a Rede de Confiança pode ser entendida como um modelo mínimo de incentivo à honestidade uma vez que trata-se de um modelo de inferência de comportamento. Os resultados desta etapa de controle são apresentados na Figura 5.6.

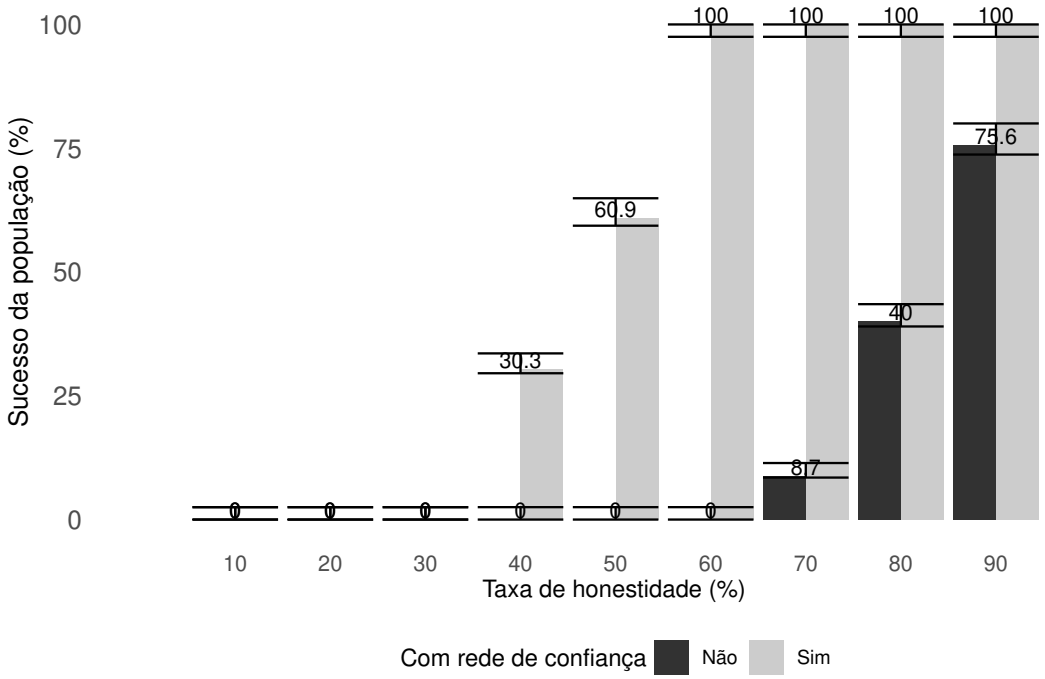


Figura 5.6: Estimativa de sucesso populacional no cenário de controle 5.4.

Observe na Figura 5.6 que a Rede de Confiança melhora significativamente o desempenho da rede de transações para taxas de honestidade superiores à 30%, alcançando um desempenho perfeito para taxas de honestidade superiores à 60%. Já abaixo de 30% não

parece mais ser suficiente para melhorar o sucesso da rede de transações. Com isto podemos inferir que de fato um modelo de incentivo à honestidade é relevante em ambientes envolvendo transações não verificáveis.

Já no cenário do experimento em si, no total, 63% das execuções de simulação resultaram em sucesso para a população. A configuração 'A', apresentada neste experimento, obteve 74% de sucesso em todo o experimento, e a configuração 'I' sem nenhuma forma de validação de transação (apenas com a Rede de Confiança) obteve 49% de sucesso. Uma imagem completa do desempenho de cada configuração de simulação é apresentada na Figura 5.7.

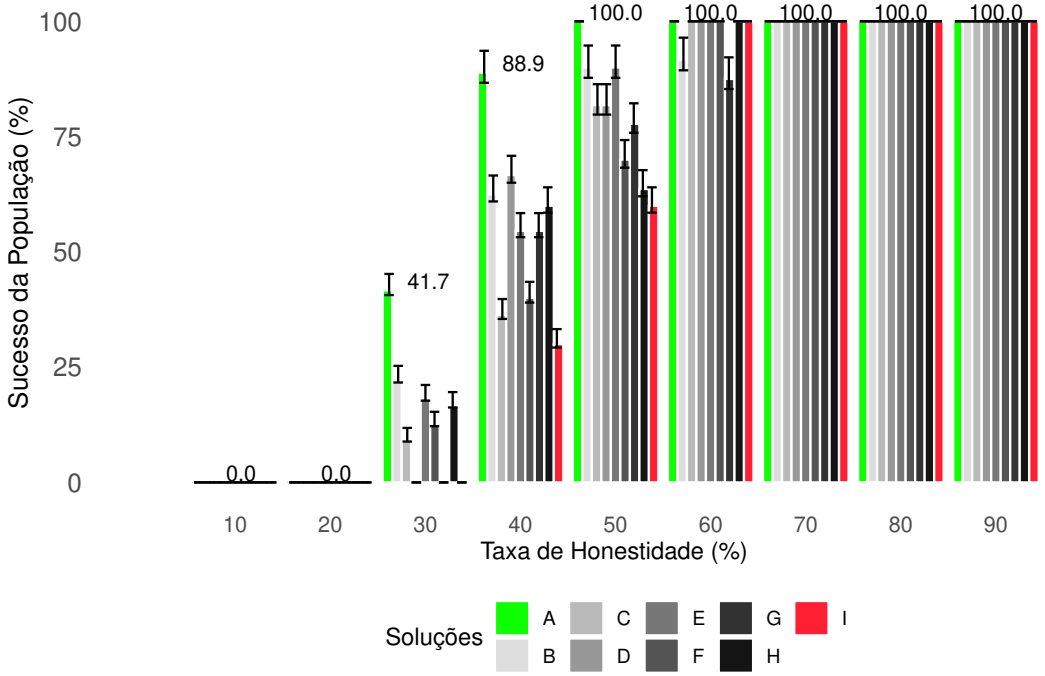


Figura 5.7: Estimativa de sucesso populacional para cada solução comparada na Tabela 5.4.

Examinando a Figura 5.7, nenhuma das configurações mostra qualquer sucesso para taxas de honestidade menores ou iguais a $0,2$ (20%), enquanto todas exibem desempenho perfeito (100% de sucesso) para taxas de honestidade maiores ou iguais a $0,7$ (70%). O intervalo de competição entre os modelos é confinado entre $0,3$ (30%) e $0,6$ (60%), indicando potencial para otimizar modelos de validação de transações com operações não verificáveis. Dentro desse intervalo, a configuração 'A' exibe dominância significativa sobre as outras. Essa configuração depende de um árbitro de verificação descentralizado da Rede de Confiança sem *feedback* e classificação de transações (consulte a Tabela 5.4). Isto sugere a

existência de um modelo de validação de transações capaz de efetivamente encorajar a honestidade dos agentes com uma taxa de honestidade espontânea igual ou maior que 30%. Tal constatação representa mais uma resposta parcial para o problema de interesse desta Tese. Para uma Figura 5.7 melhor organizada, os rótulos dos resultados foram omitidos, exceto para a solução 'A' que obteve os melhores resultados [11].

População de Agentes a Cada Passo de Tempo

Para analisar a progressão da população, amostras aleatórias do estado da simulação foram registradas em cada etapa. Embora os agentes operem de forma distribuída, cada ciclo completo de ações de todos os agentes recebe um identificador inteiro sequencial que será usado para medir o tempo ao longo da simulação (etapas/passos de tempo). Pegamos uma amostra aleatória de 1000 registros de estado da simulação executada ao longo dessas etapas de tempo para avaliar a evolução no número total de transações bem-sucedidas e transações malsucedidas evitadas por cada uma das soluções aplicadas (veja a Tabela 5.4).

A Figura 5.8 destaca a eficácia de cada solução em encorajar a honestidade por meio da correlação de Spearman entre os registros de "Transações bem-sucedidas", "Transações malsucedidas" e "Transações malsucedidas evitadas" a 40% de honestidade da população, onde os resultados foram mais diversos para cada modelo (veja a Figura 5.7). Note que as maiores correlações entre transações bem-sucedidas e evitadas com sucesso ocorrem no modelo 'A', a solução com melhores resultados, e em modelos como 'E' e 'F' (veja Tabela 5.4). Nos outros modelos, correlações espúrias ocorrem com transações bem-sucedidas e malsucedidas evitadas com transações malsucedidas. No modelo 'I', que não tem nenhuma forma de verificação de transações, transações bem-sucedidas e malsucedidas são simetricamente opostas, o que serve como evidência da análise.

Limitações

O estudo apresentado nesta Seção trata de um experimento simulado, que por si só limita seus resultados a direcionar ações futuras e não pode ser tomado como resultados definitivos. Resultados mais concretos dependem de experimentos em um ambiente real. Tal limitação, no contexto desta Tese, é mitigada ao combinarem-se os resultados desta Seção com os

[11] Para mais detalhes sobre os resultados omitidos, verifique a Tabela C.1.

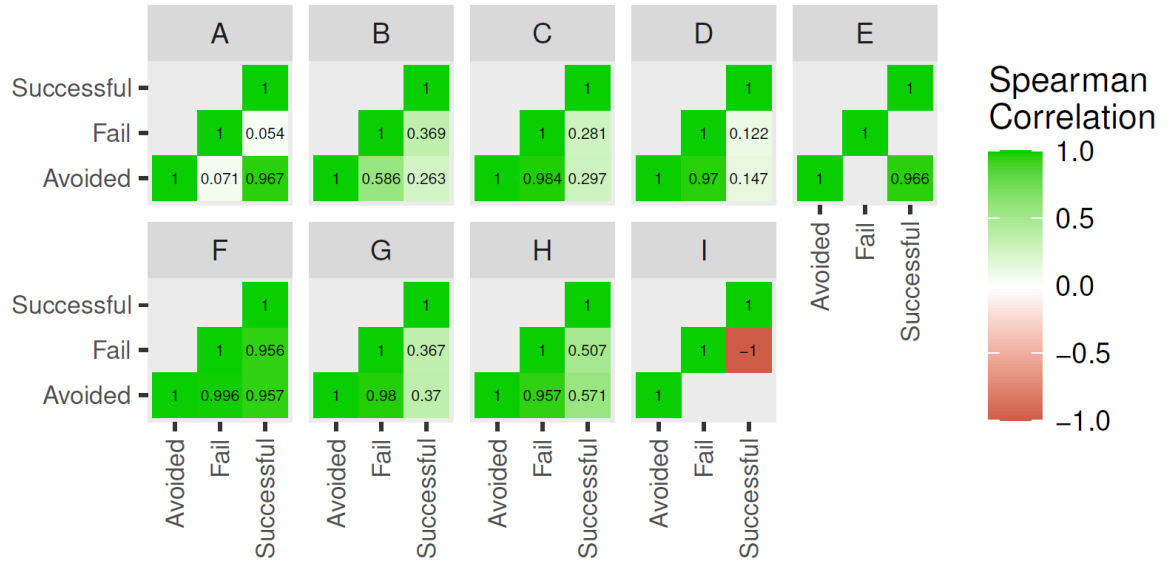


Figura 5.8: Matriz de correlações de Spearman entre transações bem-sucedidas, malsucedidas e malsucedidas evitadas a uma taxa de honestidade de 40%. A Figura tem nove matrizes de correlação, uma para cada solução na Tabela 5.4. Cada célula das matrizes tem uma gradação de cor de vermelho a verde representando a correlação de Spearman entre as métricas de transação: 'Transação **Bem-sucedida**', 'Transação **Malsucedida**' e '**Malsucedida Evitada**'.

resultados apresentados na Seção 5.3 que traz um estudo similar, porém baseado em dados reais da plataforma OpenBazzar.

Outras limitações incluem a dependência de heurísticas para simular o comportamento humano (por exemplo, a chance de desonestidade do agente aumenta com a proximidade da falência e diminui com o estoque mais cheio). A introdução de agentes mais inteligentes poderia potencialmente abordar essa limitação.

5.4.5 Conclusões

As descobertas do estudo apresentado nesta Seção destacam o desafio contínuo de estimular a honestidade em transações não verificáveis do mundo real em mercados descentralizados. O estudo apresenta um Simulador Baseado em Agentes (ABS) computacionalmente leve para avaliar e comparar o desempenho de estratégias de estimulação de honestidade a serem incorporadas em protocolos de livro razão distribuído. Por meio de experimentos simulados,

a solução 'A' proposta na Tabela 5.4 surge como a mais eficaz na promoção de comportamento honesto em mercados que dependem de transações não verificáveis. Notavelmente, os resultados do ABS indicam que 'A' pode estimular a honestidade satisfatoriamente com um alto grau de confiança, particularmente quando as taxas de honestidade estão na faixa de 30-60%, com 95% de confiança. No entanto, à medida que as taxas de honestidade caem, a taxa de sucesso diminui, chegando a zero para taxas de honestidade iguais ou inferiores a 20%. Este resultado indica que, em um cenário altamente desonesto, será melhor evitar fazer negócios completamente, pois nenhuma solução até o momento parece fazer os agentes se comportarem honestamente. Surpreendentemente, quando as taxas de honestidade crescem além de 60%, pode ser tão eficaz, simples ou econômico (em termos computacionais) simplesmente aplicar uma Rede de Confiança (solução "I" na Tabela 5.4) – o que significa que até mesmo "agentes criminosos" tenderão a seguir a multidão (que é composta principalmente de agentes honestos) quando forçados por relações sociais (vide Seção 3.2.1, Capítulo 3).

Do gráfico de correlação (veja Figura 5.8) e dos resultados para cada intervalo de honestidade (veja Figura 5.7), a Tabela 5.5 fornece uma visão geral dos resultados para cada solução testada. Note que as melhores soluções A, E e F têm arbitragem em comum, o que indica uma boa relação custo-benefício entre esse recurso e o incentivo à honestidade.

5.5 Contribuições e Próximos Capítulos

As descobertas mostradas neste Capítulo contribuem para além desta Tese ao elencar as principais classes de soluções da literatura para o DCV, além de propor composições destas e avaliá-las por meio de duas abordagens diferentes, simulação e análise de dados históricos. Mais além, ilustrou-se o suporte da ABS ao desenvolvimento e prototipagem de mercados descentralizados. No Capítulo 6 será proposta e avaliada uma nova abordagem para o DCV envolvendo transações não verificáveis, diante disto, o mesmo modelo de simulação apresentado aqui foi generalizado para ser usado em um domínio mais amplo de prototipagem de protocolos descentralizados.

Apesar da consistência dos resultados, o estudo ressalta o desafio persistente na validação de transações envolvendo operações não verificáveis em mercados descentralizados. Esta

Tabela 5.5: Vantagens e desvantagens de cada modelo

Soluções	Visão Geral
A	Melhor solução em todas as faixas de honestidade avaliadas (veja Figura 5.7) e melhor solução geral (média 70,067, calculada a partir dos números apresentados na Tabela C), com melhor correlação entre transações bem-sucedidas e transações bem-sucedidas evitadas (veja Figura 5.8).
B	Não se destaca nem positiva nem negativamente.
C	Não se destaca nem positiva nem negativamente.
D	Não se destaca nem positiva nem negativamente.
E	Embora não seja a melhor solução, nem a segunda melhor solução em nenhuma das faixas de honestidade avaliadas (ver Figura 5.7), é a segunda melhor solução geral, alcançando uma média de 62,52 (de acordo com a Tabela C), e mostrou consistência na correlação entre sucesso e falhas evitadas, conforme mostrado na Figura 5.8.
F	Embora não seja a melhor solução, é uma boa solução no geral, obtendo uma média de 58,05. No entanto, embora a correlação entre sucesso e falhas evitadas seja alta, como mostrado na Figura 5.8, correlações espúrias entre falhas, sucesso e falhas evitadas sugerem efeitos anormais que merecem melhor avaliação futura.
G	Não se destaca nem positiva nem negativamente.
H	Não se destaca nem positiva nem negativamente.
I	Pior solução no geral, o que é esperado uma vez que não implementa nenhum modelo de garantia de transação (apenas a inferência de honestidade por meio de Rede de Confiança), mas elimina a complexidade dos modelos de validação de transações apresentados aqui, o que representa uma economia aceitável quando o índice de honestidade é superior a 60%.

descoberta enfatiza a natureza contínua do problema e a necessidade de mais pesquisas e soluções inovadoras neste domínio. Para além dos resultados expostos, resta ainda como iniciativa futura uma análise do custo computacional computacional de cada solução. Para mais detalhes a respeito de iniciativas futuras, consulte a Seção 7.2.

Os resultados aqui descritos contribuem ainda para aplicações de Blockchain e TLRDs especificamente no campo de protocolos de prevenção de fraudes para mercados online descentralizados e anônimos que lidam com transações não verificáveis. Mais além, entendemos que neste ponto dos esforços desta Tese já temos uma resposta satisfatória a questão de pesquisa principal: Com base nos resultados deste Capítulo, concluímos que sim, é possível estimular a honestidade e promover a sustentabilidade de um mercado descentralizado mesmo envolvendo transações não verificáveis, contanto que a taxa de honestidade se mantenha igual ou superior à 40%.

5.6 Sumário do Capítulo

A seguir apresentaremos as principais contribuições deste Capítulo para a Tese como um todo.

- Elencou-se as principais classes de soluções para o DCV em ambiente DAnV da literatura.
- Identificou-se com base em duas abordagens diferentes à arbitragem descentralizada associada a rede de reputação como MIH mais eficaz dentre os avaliados. Portanto, pode-se concluir que o DCV em ambiente DAnV tem solução para taxas de honestidade da população acima de 30%.
- Estabeleceu-se um modelo de comparação entre as soluções para o DCV em ambiente DAnV.
- Estabeleceu-se um modelo AB voltado ao desenvolvimento e validação de protocolos de livro razão distribuído que ainda será usado no Capítulo 6 e que está disponível publicamente.

Capítulo 6

Hash Society

6.1 Introdução

Em transações comerciais bilaterais, as partes enfrentam o Dilema dos Compradores e Vendedores (DCV), onde se corre o risco de executar a transferência de valor antes de receber uma resposta, o que é particularmente desafiador em ambientes não verificáveis como mercados descentralizados. Somando-se a isso, segundo a Teoria do Jogos, diante da escassez de informação jogadores racionais tendem a escolher sempre a estratégia de equilíbrio para se proteger da estratégia de seus concorrentes. Contudo, isto é pouco eficiente devido ao comportamento não colaborativo, produzindo resultados muito abaixo do ideal. Este saldo negativo define o Preço da Anarquia (PoA), um problema já introduzido nesta Tese. Este Capítulo propõe um afastamento das transações baseadas em uma sequência de operações, defendendo uma solução baseada em TLRD que favoreça a honestidade por meio de transações de operação única (semelhante a doações) remuneradas por reputação. A fim de viabilizar este modelo de mercado, um sistema de gerenciamento avalia os níveis de colaboração, promovendo a cooperação e mitigando o DCV. Por Simulação Baseada em Agentes (ABS) tal abordagem demonstrou nítida superioridade quando comparadas as demais soluções já avaliadas na Seção 5.4 do Capítulo 5, alcançando altas probabilidades de sucesso em transações não verificáveis. Paralelamente, uma análise de segurança confirma a integridade do protocolo (também em ambiente simulado), mesmo mediante a maioria dos agentes desonestos.

6.2 Trabalhos Relacionados

Aqui detalhamos resultados da revisão da literatura feita no Capítulo 5.2 mais pertinentes à este Capítulo.

Conforme já apontado em Capítulos anteriores, já existem diversos modelos com soluções de contorno para o DCV. Contudo, estas são aplicáveis à ambientes parcialmente DAnV (menos hostis). Neste sentido, a validação de todas as transações limitando o escopo a produtos digitais ou conteúdo de autenticidade digitalmente verificável [285, 187, 219, 206] ou mesmo considerando apenas circunstâncias muito restritas [20, 174, 258], são algumas das estratégias adotadas por tais soluções para o DCV que findam por fugir do ambiente DAnV. Além disto, conforme resultados obtidos no Capítulo 5, o DCV em ambiente DAnV só tem solução dada uma taxa de honestidade da população alta o suficiente para atenuar o risco em transações. Assim, o DCV em ambiente DAnV é um problema que segue em aberto.

Son et al [238] e Tsabary et al [258] empregaram *blockchain* e CI para aprimorar o protocolo Cash on Delivery (CoD) para comércio eletrônico, em uma abordagem que garante transações seguras e aborda o DCV impondo regras específicas aos agentes e utilizando CI como intermediários (Contrato Colateral). Além destes, Le et al [155] introduziram um protocolo também de CoD para entrega comercial onde os motoristas são obrigados a hipotecar uma quantia de dinheiro, um sistema de autenticação também é usado pelos motoristas e um código *hash* único e verificável identifica os produtos.

Todos os trabalhos acima afirmam que o principal fator limitante das soluções descentralizadas de CoD é a complexidade de geração de incentivos para que as entidades participantes atuem honestamente, um problema diretamente ligado ao DCV. Duong-Trung et al [78] introduziram um modelo abrangente de CoD que se baseia em CIs para resolução automática de conflitos, eliminando a necessidade de intermediários humanos sob o argumento de que consumiria mais ativos e tempo dos agentes envolvidos. No entanto, essa abordagem inclui um elemento adicional de resolução de conflitos, penalizando entregadores ou transportadoras que violam contratos com base em um sistema de reputação. Segundo os autores, bastaria o uso de um CI como árbitro associado ao sistema de reputação, além da infraestrutura fornecida por TLRDs. No entanto, a ausência de um intermediário moderador humano tende a restringir o domínio de bens que podem ser negociados àqueles estritamente

digitais, como apresentado por Zhang et al [285], e o sistema de reputação sem classificação de transações favorece a centralização, uma vez que essa confiança fica restrita a agentes que negociam com frequência [19]. Na literatura há outros trabalhos que abordam soluções descentralizadas para CoD ou abordam o DCV de forma semelhante [156, 12, 20]

Outro trabalho importante utilizando arbitragem é apresentado na plataforma OpenBazaar [289]. Aqui qualquer usuário pode atuar como um árbitro humano em transações e este deve resolver disputas quando ocorre um problema em troca de uma recompensa monetária que só é paga se o árbitro for chamado. No entanto, ele não implementa uma Rede de Confiança descentralizada e a confiança no árbitro depende de *feedback* escasso e de um "Currículo" que quase sempre expõe a identidade do árbitro, além de não apresentar nenhum mecanismo que estimule a descentralização do papel do árbitro.

O Capítulo 5 comparara por meio de duas abordagens diferentes classes de soluções presentes na literatura para o DCV, além de composições pertinentes entre elas. Como resultado alcançarou-se uma solução que se destacou entre as demais para populações de agentes com taxa de honestidade igual ou superior à 30%. Abaixo deste percentual, nenhuma solução encontrada foi capaz de assegurar níveis de sucesso aceitáveis para transações em ambiente DAnV.

A estratégia desonesta de equilíbrio do DCV depende da falta de colaboração entre os agentes. Intuitivamente, promover a colaboração entre tais agentes soa como um caminho promissor a fim de resolver o DCV em ambiente DAnV. O modelo de transações bilaterais promove a competição entre os agentes uma vez que o lucro de um representa a prejuízo do outro. Agir de forma desonesta garante mais lucro ao agente passivo por meio do prejuízo do agente ativo.

A literatura tem aplicado o conceito e transação de operação única em sistemas de escambo eletrônico, onde os agentes doam itens que não lhes interessa mais em troca de créditos ou outro meio de reputação direta [204]. Contudo, o crédito ou reputação é recebido em troca do item o que, em última análise, configura uma transação bilateral. Ikeda [125] propõe um modelo de TLRD decentralizado e *currentless*, mas não estabelece uma solução para o DCV, nem demonstra a eficácia de sua solução em ambiente DAnV.

Nossa proposta de solução é a primeira até onde se observou a propor um modelo de operação única, *currentless*, tolerante à falta de confirmação e ao anonimato (DAnV). O

modelo de transação de operação única é possível pois, embora exista uma contrapartida para as transações, esta não é fornecida pela outra parte na transação, não ocorre de forma síncrona (em relação a contrapartida), e não é plenamente controlável por parte do agente, mantendo sua magnitude oculta na caixa preta de um Modelo Gestor Inteligente (MGI) que decide quais transações aceitar com base em um conjunto de modelos de reputação. Nesta abordagem, o esforço de engenharia reversa sobre o MGI a fim de identificar e decodificar este esquema de reputações é justamente o desafio proposto aos mineradores.

6.3 Problema

Relembrando os componentes do problema abordado aqui nesta tese, voltemos agora ao conceito de Preço da Anarquia (PoA) descrito no Capítulo 3, que considera a razão entre o equilíbrio de Nash e o ótimo social [207] como a medida padrão da potencial perda de eficiência devido ao egoísmo individual. Mais especificamente, Koutsoupias e Paradimitriou [147] alcançaram a conclusão numérica de que a falta de coordenação entre os agentes leva a uma perda de desempenho de 33% em comparação com a configuração ótima na qual os agentes cooperam. Considerando que Koutsoupias e Paradimitriou restringiram seu trabalho a um cenário bastante limitado de roteamento de rede onde o egoísmo é uma estratégia apenas um pouco mais vantajosa, podemos imaginar o prejuízo que o PoA pode causar no contexto dos meios de produção humanos.

Contudo, o ponto focal abordado nesta Tese é o Dilema dos Compradores e dos Vendedores (DCV), como um problema de corrida entre jogadores desonestos envolvidos no estabelecimento de uma transação baseada em duas operações (pagamento e transferência de produto, por exemplo), ambas com vantagens em direções opostas. O dilema consiste na decisão de uma das partes de tomar a iniciativa e realizar a primeira operação de transferência de valores, confiando que outra parte faça o mesmo em seguida.

Considere a partir daqui uma definição diferente de transação para este Capítulo. Concordemos que uma transação é um protocolo simples baseado em uma única operação, sendo a parte passiva, o "doador" ou demandado, e a parte ativa, o "donatário" ou demandante. Esta única operação, por sua vez, é não virtualizável, ou não-verificável, ou não validável. Assim, dependemos apenas da intenção do demandado de melhorar sua reputação para que a tran-

sação ocorra. O demandante, por sua vez, já deve merecer o benefício por trás da transação antes que esta inicie.

Assim, o problema principal desta Tese consiste em reduzir o risco da parte passiva, doravante descrita como demandado, em transações não-verificável em ambientes públicos e anônimos (DAnV). A solução apresentada neste Capítulo para tal problema reduz também o PoA (preço da anarquia) em tais ambientes adversos, uma vez que produzir e colaborar com o sistema é a própria recompensa, ao invés de uma recompensa monetária que estimule a competição e portanto, a anarquia (vide Capítulo 3, Seção 3.3). Pelo mesmo motivo, fortalece também o estímulo à ação coletiva e à promoção do bem público (vide Capítulo 3, Seção 3.2). Tal ferramenta doravante denominada Hash Society (HS) é descrita a seguir.

6.4 Solução Proposta: Hash Society

Ao longo deste documento tratamos em diversas ocasiões do conceito de *marketplace*, onde compradores e vendedores se encontram e realizam transações mediados por uma autoridade centralizada confiável ou por um protocolo descentralizado. Contudo este modelo, conforme observou-se, não é capaz de lidar com operações não-verificáveis em cenários envolvendo altos níveis de desonestidade (vide Capítulo 5).

Considere agora o mesmo *marketplace*, porém elimine a contrapartida monetária do comprador, ou seja, um *marketplace* de troca de mercadoria. Já houveram várias iniciativas de *marketplace* baseadas em troca de mercadoria, geralmente envolvendo produtos majoritariamente semi-novos e frequentemente ainda permitindo uma contrapartida monetária adicional [204]. Entretanto, as estratégias de mediação nestes casos são bastante limitadas, visto que a operação de troca de bens físicos semi-novos é essencialmente não-verificável por diversas razões, seja em função da dificuldade em monitorar ou sincronizar a troca das mercadorias ou também pela discrepância entre o estado de conservação relatado do produto e o estado de conservação de fato. *Marketplaces* de troca costumam manter esquemas de reputação e *feedbacks* a fim de oferecer algum nível de mediação em transações. Contudo já demonstrou-se nesta Tese, com base na literatura, que esquemas de reputação baseados em *feedbacks* por si só são modelos de mediação facilmente fraudáveis [78, 156, 12, 20].

A Hash Society (HS) usa um sistema de reputação mais forte baseado em um Modelo

Gestor Inteligente (MGI) que define quais transações são seguras tanto para os envolvidos quanto para o equilíbrio da rede. A cada iteração o modelo gestor deve melhorar sua capacidade de identificar qual estratégia de reputação é justa ou mesmo quando um usuário está tentando construir uma reputação falsa. Demonstraremos a seguir que, seguindo a mesma metodologia dos experimentos de Capítulos anteriores, rede de confiança associada a um sistema de arbitragem (solução "A", conforme Tabela 5.4) não mais supera os demais modelos avaliados em todos os cenários quando os agentes desonestos são capazes de se organizar em conluios. Ao invés disto, mediante alguns níveis de desonestidade o modelo "A" é superado.

Para que a rede de transações como um todo convirja para o sucesso, independente da taxa de honestidade, introduziu-se o conceito de transação de operação única. Em uma transação de operação única, ao invés de haver duas partes, um comprador e um vendedor, ou duas operações compondo uma troca de valores, existe apenas uma operação onde a parte demandada transfere o valor para a parte demandante esperando que o Modelo Gestor Inteligente (MGI, doravante) leve isto em consideração quando for a sua vez de ser a beneficiada.

6.4.1 Transações de Operação Única

O conceito de transação de operação única utilizado na HS é descrito na Figura 6.1 e envole outros dois conceitos descritos a seguir: Lista de Recursos e Lista de Demandas.

Lista de Demandas

Em transações de operação única, ao invés de simplesmente trocar seus recursos por outros recursos que o interesse, o agente publica uma lista de demandas – recursos que este gostaria de adquirir – e o modelo gestor inteligente avalia se ele merece ter suas demandas supridas com base em sua colaboração com outros agentes ou com a rede como um todo. Na Figura 6.1 cada nó traz consigo a lista de demandas que este precisa suprir. Para tanto este agente propõe a utilização dos recursos de qualquer um dos demais nós que os contenha, e o modelo gestor inteligente decide se deve autorizar as transações de transferência dos recursos ou não, e faz isto com base no que o agente/nó demandante já fez por outros agentes/nós no passado.

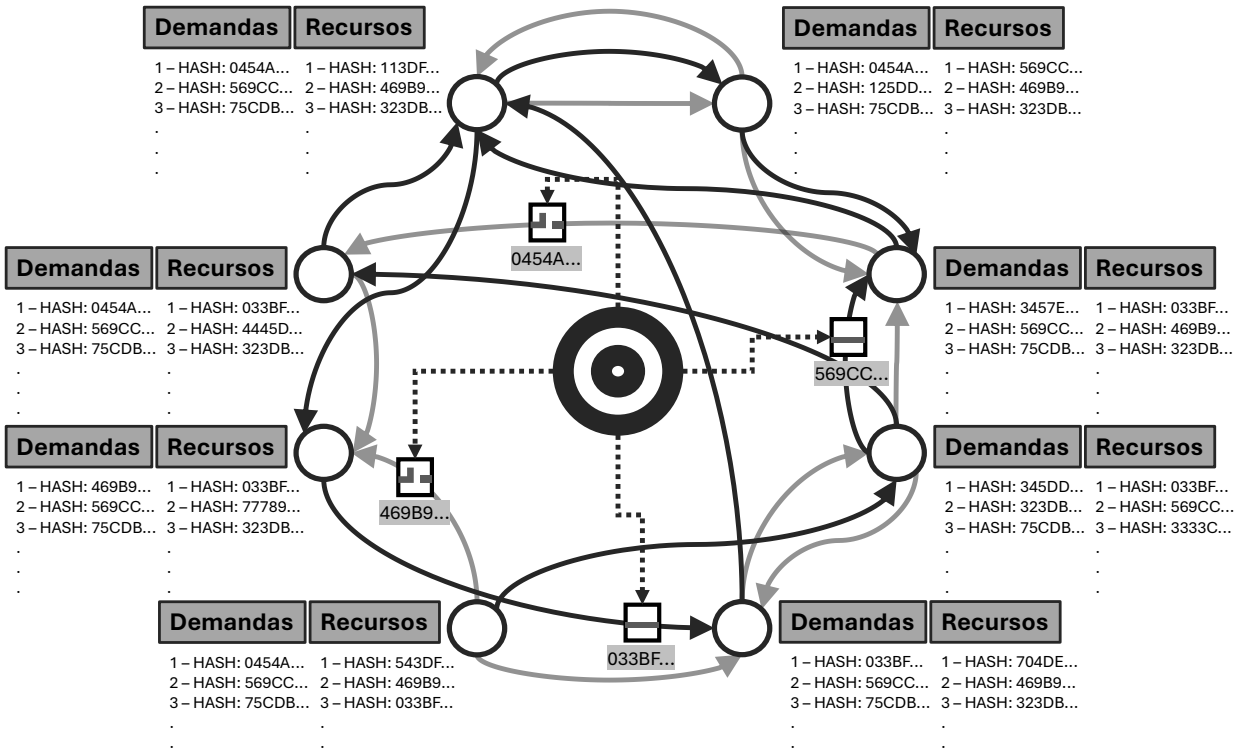


Figura 6.1: Representação da dinâmica de transações orquestradas por meio de um MGI com o objetivo de suprir com justiça as demandas dos agentes a partir de seus recursos. Os círculos brancos representam nós/agentes da rede de transações, as linhas contínuas são as transações. Um linha contínua escura é uma transação autorizada, já as linhas mais claras são as transações recusadas pelo MGI. Este MGI é o alvo central e as setas tracejadas são suas ordens de autorização ou veto às transações. Transações que trazem consigo a linha tracejada de comando do modelo gestor são transações que estão ocorrendo neste momento, as demais ocorreram ou não no passado.

Lista de Recursos

Semelhantemente à lista de demandas, a lista de recursos representa aquilo que o agente está disposto a abrir mão em prol da rede como um todo com o objetivo de melhorar sua avaliação junto ao modelo gestor inteligente. É importante frisar que o agente não é obrigado a abrir mão de seus recursos só porquê estão listados, podendo usar modelos próprios para estimar as vantagens que abrir mão destes recursos podem lhe trazer antes de tomar a decisão. Outro ponto importante é que não estamos falando de uma troca de valores com nenhum outro agente, mas uma transferência sem contrapartida imediata.

Visão Geral

Cada transação de operação única descreve um tipo de recurso representado por um código *hash* e um *payload* de entrada e outro de saída, tal como um CI plano – sem processamento – que correspondem aos conjuntos de parâmetros de entrada e saída. Cada entrada na lista de recursos e demandas deve necessariamente descrever uma transação em particular e cabe ao modelo gestor inteligente avaliar o valor desta transação e o padrão com que um agente costuma demandá-la, a fim de distribuí-la com justiça e evitar fraudes.

No modelo de mercado com transações baseadas em sequências de operações o valor de cada recurso, embora flutue em função da demanda, é sempre o mesmo para qualquer um que pretenda adquiri-lo. Já no modelo envolvendo transações de operação única, o MGI pode precificar cada recurso em função da necessidade do agente que demande aquele recurso, resguardando o sucesso de todos os agentes da rede – na medida do possível. Com isto o MGI pode evitar falências e promover ações públicas colaborativas (observe o conceito de PAC, Capítulo 3, Seção 3.2) necessárias. Além disto, ações desonestas visando uma melhora artificial da reputação se tornam muito difíceis uma vez que o modelo gestor pode aguardar a concretização do bem promovido pelo recurso para só então melhorar a reputação do agente demandado. Com isto, não adianta promover uma boa reputação real para mais tarde tentar uma ação danosa e então abandonar a rede, pois se a rede aceitou suprir a demanda do agente mal intencionado, ele só recebeu aquilo que já merecia. Tal avaliação está em consonância com as explicações teóricas para o Problema da Ação Coletiva (PAC) descrito no Capítulo 3, Seção 3.2, em especial com a Teoria Biológica que prevê que o indivíduo só agirá em prol

do coletivo quando houver algum interesse egoísta a longo prazo.

Observe que não há mais brecha para a desonestidade, uma vez que este modelo de transação não requer sincronização de operações. Neste novo cenário de negociação ainda é natural que cada parte priorize seus próprios interesses, contudo o comportamento desonesto não é mais uma opção viável – exceto em caso de conluio, conforme descrito mais adiante. Assim, considere um consumidor e um provedor, ou o jogador ativo e o jogador passivo, respectivamente. O jogador ativo é aquele que publica a demanda. Já o jogador passivo é aquele que publica o recurso. Observe que não há mais um dilema pois o jogador passivo, que em transações bilaterais tende a agir desonestamente, desta vez não deve nenhuma contrapartida. Um vez que se a rede entendeu que este merece ter suas demandas supridas, significa que este já arcou com a contrapartida devida antecipadamente. Recursivamente, esta contrapartida antecipada veio em outra transação envolvendo outro agente passivo que também já merecia ser beneficiado. Assim, apenas o primeiro agente passivo em toda a rede de transações teve a oportunidade de agir de forma desonesta – seria o equivalente em uma *blockchain* ao fundador do bloco gênesis.

Assim, simplificando a sequência de estados que a rede pode assumir podemos interpretar a propagação de reputação da rede usando Cadeias de Markov.

Definição 5. *Considere a trajetória de um recurso durável r – como um automóvel, por exemplo – como sendo a seguinte tupla $MK^r = \{{E^r}_{n+1} = e^r | {E^r}_n\} \,|\, \forall\, n \in N$ e $V_{ij} = [p_{ij} \,|\, \forall\, ij \in N]\}$, onde:*

1. *MK^r representa a cadeia de eventos e contas por onde transita um recurso r.*
2. *${E^r}_{n+1}$ é a variável aleatória que representa o estado de r na interação $n+1$.*
3. *e faz referência a algum estado de r.*
4. *V_{ij} representa o vetor de probabilidades de mudança de estados entre os estados E_i e E_j.*
5. *N é o total de estados da cadeia.*

Na definição 5 descrita acima e representado na Figura 6.2, a sequência de transições entre contas E de um dados recurso r é representada na forma de uma cadeia de Markov.

Considere que o recurso r encontra-se neste momento no estado $E^r{}_c$ (em destaque). Tomando as arestas do dígrafo como sendo as probabilidades p de transição entre estados E_n, todas as arestas em destaque representam as transições de estado (transações) já concretizadas e, portanto, irreversíveis. As arestas sem destaque representam transições que o MGI permite que ocorram. Observe que o estado $E^r{}_c$ representa a presença do recurso r no inventário (lista de recursos) de um nó que já transferiu valores para outros nós – transições de estado (transferências de recursos de seu inventário para outro) – e por isso pode requisitar r (transições de outros estados para ele) que podem vir de $E^r{}_e$. Observe também que ambos não podem requisitar recursos de nenhum outro vértice (a não ser que transfiram recursos para alguém para melhorar sua reputação). Cabe ao MGI assegurar que para algum dos demais vértices seja vantajoso transferir r [1].

Transações de operação única podem ainda representar recursos abstratos com *feedbacks* sobre transações, mediações, doações, concessões e contratos de modo geral tal como CIs em uma TLRD. Contudo, como será escrito na Seção 6.4.3, CIs na HS descrevem apenas a interface das transações, cabendo ao modelo gestor inteligente inferir seu comportamento esperado.

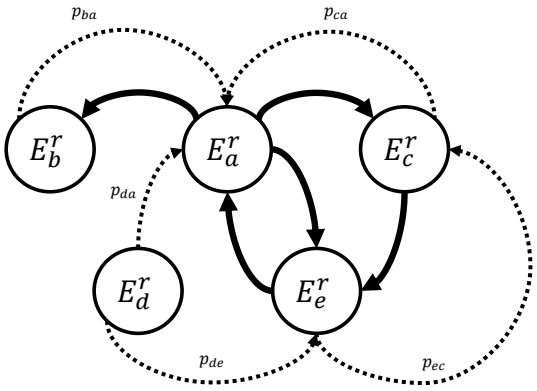


Figura 6.2: Representação de um recorte da rede em um dado momento na forma de uma cadeia de Markov. As transações passadas estão destacadas.

[1] Para facilitar a compreensão das definições todos os símbolos utilizadas estão disponíveis na Tabela C.4 (Apêndice C), além de constar no conjunto de símbolos do início desta Tese.

6.4.2 Modelo Gestor Inteligente

O Modelo Gestor Inteligente (tome MGI como o conjunto de instâncias de modelos que regem a rede como um todo, e mgi, em letras minúsculas, como uma dessas instâncias) é um dispositivo descentralizado composto por mgi's. Um mgi específico é definido mediante consenso entre um grupo de agentes interessados em utilizá-lo, outro grupo de agentes pode definir outro mgi e vários mgi's podem coexistir na rede. A reputação de um agente não é uma pontuação, mas um entendimento do mgi a respeito da relevância daquele agente para a rede como um todo, o que pode o levar a privilegiar aqueles que o aprovaram por consenso. Certamente, o grupo de agentes aprovador de um dado mgi espera ser privilegiado por tal mgi, e os demais mgi's que coexistem na rede podem ter outro entendimento a respeito da relevância de um dado agente daquele grupo, o que pode levar em consideração os demais agentes de tal grupo aprovador. Aprovar um mgi é uma transação e será usada para construir a relevância de cada agente para com a rede como um todo, assim como qualquer outra transação.

A decisão de aprovar um mgi é livre de cada agente, que pode usar processamento local e até softwares proprietários para testar os mgi's e até aceitar recomendações para aprovar um mgi baseadas em similaridade de seu perfil com relação a outros que já aceitaram aquele mgi. Semelhantemente, qualquer um pode criar e disponibilizar um mgi para apreciação entre os demais agentes. Propor um mgi pode melhorar sua reputação entre novos mgi que venha a surgir. Mais além, aquele que cria o mgi pode treiná-lo para o favorecer ou favorecer a ele e a seu grupo de conluio.

MGI e Transações

A decisão de realizar uma transação é sempre da parte favorecida, cabendo ao MGI decidir se é justo que o favorecido tenha suas demandas supridas ou não. Ao favorecedor ainda cabe recusar a transação ou definir qual mgi deve reconhecer a transação. Todas estas ações deixam rastros que podem ser usado para treinar novos mgi's. Se o valor que o favorecedor busque dispor como recurso ainda não tenho sido revisto em nenhum outra transação, deve ser criado um novo mgi que contemple aquele recurso e seu tipo de transação, com um novo código *hash* e novos parâmetros de entrada e saída.

Versionamento

Ao aceitar um novo mgi o agente deve levar em consideração a reputação do agente que propôs aquele mgi, além das vantagens para este agente e o maior número de agentes próximos a ele possível. Neste ponto vale considerar que para diferentes mgi um mesmo agente tem diferentes reputações, o que torna o trabalho de prever a reputação de um agente um tarefa complexa.

Diante disto é proposto um fluxo de versionamento de mgi com o intuito de viabilizar a função Merge em dois mgi's e, assim, reduzir a quantidade de ramificações. Observe a Figura 6.3, onde é ilustrado um fluxo de ramificações em mgi, enquanto estes validam operações entre os agentes.

O treinamento/implementação de um mgi é livre e independente da rede de transações. Qualquer agente pode propor um novo mgi e treiná-lo/implementá-lo com base no conteúdo histórico da rede, sejam transações ou mgi's anteriores. O incentivo para que agentes proponham novos mgi's está nas vantagens que este mgi pode lhes proporcionar e na reputação que adquiri-se quando um mgi de sua autoria representa uma evolução relevante para a rede, uma vez que novos mgi's são treinado em prol do sucesso da rede com base no seu histórico. Embora o incentivo para criar novos mgi's seja egoísta, pois visa ganho individuais, colaborar com os demais agentes é indispensável, caso contrário nenhum outro agente irá aderir a este novo mgi. Um mgi que apenas o autor utiliza é inútil.

As funções *merge* e *fork* de um novo mgi podem ser recomendadas por seu autor, mas devem ser validadas por outros agentes interessados em utilizá-lo, a fim de sinalizar para outros agente que aquele novo mgi traz um comportamento semelhante a mgi's anteriores. Esta validação de *merges* e *forks*, mediante comparação com outros mgi's é feita utilizando modelos de inferência livres e não integrados à rede (vide Seção 6.4.5). O consenso a respeito de qual mgi é ramificação um do outro é uma tarefa desempenhada por quem pretende aderir àquele mgi e pode ser atualizada no futuro por qualquer um, contanto que conte com o apoio de mais usuários do mgi.

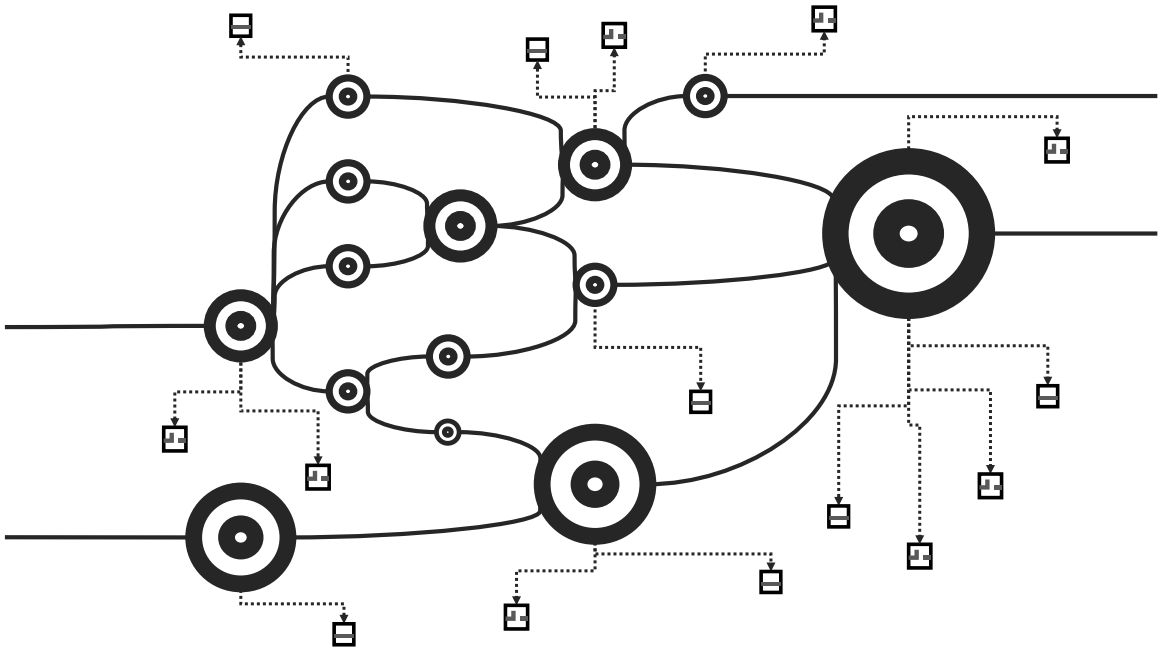


Figura 6.3: Representação do fluxo de versionamento do MGI, a coexistência de diferentes modelos e versões validando e recusando transações. Esta imagem traz também representações de operações de *fork* e *merge*, quando um modelo é subdividido em duas versões, ou duas versões são reincorporadas num mesmo modelo.

Ciclos de Influência

O MGI avalia a reputação de um agente com base nas suas transações passadas, sejam elas minerações, avaliações de novos mgi's, suporte a outros agentes que tenham demandas a suprir ou apoio de outros agentes cujos recursos este agente demande. O objetivo de um mgi é sempre manter todos com condições para que os agentes busquem suas necessidades e melhorem sua reputação. Assim a rede apresenta a reputação de um agente por associação: se o comportamento de uma agente é parecido com o de outro, estes agentes serão associados um ao outro como em ciclos de influência. Para tal, tudo pode ser levado em consideração, a depender de como o mgi escolhido foi treinado/implementado. Um agente pode pertencer à vários ciclos sobrepostos e sua reputação é variável, podendo ter alta reputação dentro de um determinado ciclo e baixa ou nenhuma em outro.

A associação por ciclos é um comportamento esperado, validado por simulação mais adiante neste Capítulo. Este comportamento contorna problemas como o conluio ou os perfis falsos, uma vez que conluios e perfis falsos que interagem muito entre si a fim de melhorar suas reputações terão reputações boas apenas dentro daquele ciclo também falso, o que não traz nenhum ganho concreto. Isto ocorre pois o mérito ou reputação é uma grandeza não linear baseada em ciclos de influência. Quanto mais demandas um agente supre, mais mérito este consegue entre aqueles que suprem as mesmas demandas. Semelhantemente, a precificação de uma dada demanda também é não linear e segue o conceito de ciclo.

6.4.3 Perfis de Agentes

Assim como em outras TLRDs, a HS conta com mais de um perfil de agente. Diferentes perfis distinguem-se ente si por diferentes responsabilidade e diferentes graus de liberdade.

- **Agente Padrão**, conta com todas as funções disponíveis para realizar transações, mineração, avaliação de mgi, mediação, etc. Este é o agente padrão representando um usuário da TLRD.
- **Agente Autônomo** que, embora restrito à um conjunto finito de transações simples, pode variar seu comportamento dentro destas. Útil para ser utilizado como CI com inteligência artificial ou acesso à informação externa.

- **Contrato Inteligente (CI)** capaz apenas de um conjunto finito de transações sem variação de comportamento permitida.

Na HS, CIs são facilmente atualizáveis, ao contrário de outras TLRDs. Isto porque o comportamento não está codificado em uma máquina virtual, mas apenas sua interface. Seu comportamento é inferido por mgi's. Se um CI nunca variar seu comportamento dada a entrada, o MGI aprende isto – este é um comportamento esperado e também observado por simulação. Caso um mudança seja feita, a reputação do CI será prejudicada momentaneamente – este também é um comportamento esperado. Contudo, com o tempo a mudança estará absorvida, novos mgi's surgirão e serão distribuídos e o CI pode recuperar sua reputação. Vale frisar que o código do CI é implementado externamente e de forma livre, cabendo a HS apenas uma inferência de seu comportamento.

6.4.4 Abordagem Técnica

Os estudos desta Tese tem por objetivo alcançar uma solução para o DCV em um ambiente DAnV sob a ótica da teoria dos jogos em ambiente simulado. Questões técnicas referentes a aplicações em ambiente real da HS ou qualquer solução proposta ou avaliada no contexto desta Tese está fora de escopo por limitações de recursos (tempo, capacidade de desenvolvimento de software e processamento). Tomou-se este caminho por entender que os detalhes da implementação de TLRDs são questões bastante maduras, sendo abordadas tanto pela indústria [178] quanto pela literatura [17] e que não teríamos condições de acrescentar resultados relevantes.

No entanto, exemplificando, a HS especificamente poderia ser implementada com base em uma TLRD multi cadeia, como Hash Graph [49]. Este modelo está de acordo com o conceito de HS por distribuir tanto a força de mineração quanto a autonomia da rede como um todo, permitindo muito mais armazenamento e processamento com menos esforço computacional.

É certo que a HS não é baseada em crito moedas ou autenticação de usuário, por isto nenhuma TLRD atual poderia se adequar diretamente [124]. No entanto, como demonstrado por simulação a seguir, a reputação baseada em MGI serve ao propósito de incentivo à mineração.

O incentivo à mineração segue a mesma dinâmica da reputação: minerar as transações de um dado ciclo incrementam a reputação do agente naquele ciclo. Isto incentiva os próprios agentes a minerar, visto que caso um agente não tenha interesse nas transações dentro daquele ciclo, não tem porquê minerar aquelas transações. Contudo, também existem ciclos mais abrangentes, portanto é sempre vantajoso minerar. Quanto mais influência um ciclo tem em outros ciclos, mais reputação os mineradores das transações daquele ciclo vão ganhar. Ciclos com muitas transações e pouca reputação fora do ciclo – a exemplo de conluios e ciclos falsas – terão dificuldades em ter suas transações mineradas. O objetivo desta abordagem é evitar que ciclos falsos realizem ataques de negação de serviço a rede e também estimular a mineração pelos próprios membros do ciclo. Por exemplo: um comportamento esperado é que à medida que um agente submete muitas transações, estas serão cada vez mais despriorizadas pela mineração pois passaram a valer menos para o MGI.

6.4.5 Estimativas de Transações

Todos os agentes tem acesso público a todas as transações e ramificações do MGI, e por isso podem estimar a utilidade/custo de cada transação antes de realizá-la. Considere aqui o custo como sendo o decremento de reputação que aquela transação pode causar ao agente em detrimento do quão necessário é suprir a demanda de que esta transação trata. Semelhantemente, utilidade é o incremento de reputação que um dado agente pode receber caso supra a demanda de outro.

Para exemplificar, um agente i que conte com um dado recurso R_i recebe a solicitação de recurso de outro j para R_i. Neste momento o agente i reúne as mgi's de maior interesse para seus ciclos de influência e tenta estimar a utilidade utilizando modelos de auditoria em aprendizagem de máquina, a exemplo da ferramenta Lime [221], ou qualquer outra métrica cabível para avaliar a utilidade $U_{R_{ij}}$ desta transação. Tal utilidade é medida em função do quão ela aproxima i de ter as demandas de sua lista supridas. Este processo é semelhante a abordagem utilizada para comparar modelos de incentivo à honestidade da Seção 5.3 (Capítulo 5) e é de responsabilidade do agente e não é reportado à rede. A mesma abordagem pode ser aplicada a qualquer movimento dentro da rede, sejam validações de *merges* e *forks*, ou mesma a adesão a um dado mgi.

6.4.6 Considerações Finais

Na HS, o agente desonesto está se arriscando contra um conjunto de modelos inteligentes de capacidade parcialmente desconhecida e que contem um profundo conhecimento sobre os padrões de comportamento de toda a rede. A análise de equilíbrio do jogo entre agentes não se aplica entre agente e MGI, uma vez que este possui amplo conhecimento a respeito do estado atual da rede e das probabilidades de evoluções deste estado. Assim, uma desonestidade possível é não notificar a rede sobre uma transação – evitando a contabilização de uma demanda suprida – mas seu parceiro certamente o fará e a rede deve aprender a identificar estes padrões de desonestidade. Publicar recursos falsos ou demandas falsas são outros exemplos de desonestidade que o MGI deve assimilar.

É certo que esta solução proposta requer ainda muita análise, como será demonstrado na próxima seção. Há uma grande gama de comportamentos esperados da rede em geral e do MGI, e outros comportamentos difíceis de prever. Abaixo demonstramos com exemplos alguns dos comportamentos esperados, alguns deles confirmados por simulação na Seção seguinte.

- Um dado agente incrementa sua reputação em escala logarítmica. Quanto maior a reputação de dado agente, mais transações de comprovação esta deve requerer. A reputação de um novo agente vai de zero a um certo valor que permita sua subsistência muito mais rapidamente que uma reputação mediana se torna uma elevada reputação. Até mesmo os novos agentes devem ter suas demandas básicas supridas – a não ser que a rede seja capaz de concluir que trata-se de agente malicioso. Isso ocorre porque espera-se que hajam mais agentes demandando recursos mais elementares que agentes demandando recursos supérfluos, o que moverá a rede a favorecer pequenas demandas em detrimento de grandes. Este comportamento é demonstrado por simulação, embora a função de progressão da reputação não pôde ser identificada.

- Um agente, mesmo com alta reputação, é apenas um nó de transações e representa menos que um grupo de agentes.

- O conceito de CI com código externo permite uso livre de inteligência artificial na programação, um vez que o processamento não gera custos. Assim, a rede pode ser

utilizada para gerir agentes autônomos atuando independentemente ou em grupo (por exemplo, na forma de enxames [134]), potencial que pode ampliar o domínio de aplicações de CI.

- O autor e os agentes que usam dado mgi promovem sua confiabilidade em função da deles. Ao usar um mgi, o agente fica associado a ele e aos ciclos de influência que o utilizam.

- Um mgi também pode aprender com as demais ramificações. Os mgi's que ramificam muito ou pouco podem ser tratadas como ruins ou boas e podem prejudicar ou beneficiar a reputação daqueles que os utiliza.

6.5 Experimento Simulado

6.5.1 Metodologia

O estudo apresentado neste Capítulo propõe um incremento ao experimento apresentado na Seção 5.4 (Capítulo 5), onde compara-se por meio de simulação de soluções de contorno já aplicadas na literatura para o DCV ou problemas que envolvam o mesmo dilema indiretamente, além de combinações de características dessas soluções que visam incentivar a honestidade em vez de verificar as operações para propor novas soluções (ver Tabela 5.4). Tal incremento inclui a HS como uma das soluções comparadas.

A hipótese a ser testada aqui diverge daquele apresentada na Seção 5.4. Aqui esperamos verificar se a HS é de fato uma solução capaz de incentivar a honestidade de forma descentralizada mesmo na presença de operações não verificáveis, desta vez mediante qualquer taxa de honestidade. Se tal hipótese for aceita, a HS deve ser capaz de recompensar e encorajar a honestidade em uma população de agentes com diversas categorias distintas, múltiplos valores trocados e diversos perfis de honestidade. Para isso, a Simulação Baseada em Agentes (ABS) foi novamente usada para registrar a eficácia de cada agente separadamente e da população como um todo por meio de múltiplas simulações em diferentes taxas de honestidade.

6.5.2 Design da Simulação

Com o mesmo objetivo da Seção 5.4 (Capítulo 5) de simular mercados descentralizados, este experimento utilizou a Simulação Baseada em Agentes (ABS). Além de reproduzir interações onde agentes produzem e comercializam valores, parâmetros como honestidade, memória, risco, falência e sucesso foram incorporados. O modelo de ABS aqui também foi desenvolvido com base no trabalho de Fagiolo et al [86].

O ambiente de simulação consiste em um Grid 2D 256×256 contendo um total inicial de 100 agentes que pode crescer até um máximo de 1.000 agentes conforme a simulação avança – mesmos parâmetros adotados no experimento da Seção 5.4. Assim, os agentes podem mover-se uma casa por vez e, tornando uma unidade de um tipo de valor negociável a cada ciclo ou negociando itens em seu inventário para obter outros valores que estes não são capazes de produzir.

Definição da HS

A definição abaixo corresponde a uma simplificação formal do que foi descrito até aqui a respeito do funcionamento da HS.

Definição 6. *Considere a dinâmica que rege a HS como sendo* $HS = \{P, Q, MGI, T, \mu, \eta\}$*, onde:*

1. P *significa a coleção de itens ou produtos movimentados dentro do jogo.*
2. Q *representa o grupo de agentes envolvidos nas negociações, normalmente consistindo de dois agentes, embora possamos generalizá-lo para* $|Q|$ *para flexibilidade.*
3. MGI *representa o conjunto de mgi's disponíveis, sendo cada uma delas descrita em letras minúsculas* mgi*.*
4. T *referenciando todos os passos de tempo.*
5. ${\mu^s}_{mgi}$ *é uma avaliação de uma transação* s *por uma* mgi*.*
6. η^t *representa algum modelo de transação, onde* η^{qt} *retorna um conjunto bruto de operações* $\{\gamma_0, ..., \gamma_n\}$ *num determinado momento* t*, para um dado agente* q*. Tais operações podem significar a solicitação de recurso, participação na criação de um agente*

dos tipos CI ou autônomo (conforme Definições apresentadas na próxima Subseção, 'Agentes'), registro unilateral na rede (p.ex. reclamação a respeito do insucesso de uma transação), mineração de transações ou a adesão a uma mgi mais adequada aos interesses do agente.

Agentes

Existem ao todo três tipos de agentes, tal como descrito na Seção 6.4.3. O **agente padrão**, que corresponde ao usuário em si, é capaz de mover-se uma posição no Grid por vez, decidindo a cada passo de tempo fabricar uma unidade do tipo de valor que é capaz ou negociar valores (itens) em seu inventário com outros agentes para obter outros valores que eles não são capazes de produzir. Um passo de tempo pode ser visto como um ciclo onde todos os agentes concluem uma transação ou fabricam um valor (item) para seu inventário. O **agente CI** é onipresente no Grid, podendo interagir com qualquer agente a qualquer momento, sua função é converter um valor específico em outro. Por fim, existe o **agente autônomo**, também onipresente no Grid, porém é capaz de converter qualquer valor em qualquer outro valor.

Todos os três tipos de agentes contam com um inventário onde armazenam seus saldos. O agente padrão segue a mesma abordagem do experimento simulado anterior, se reproduzindo caso supere um limiar máximo específico no seu inventário, ou sendo removido do Grid caso seu inventário não chegue ao máximo ao fim de seu tempo de vida L. Os agentes autônomos e CI não são removidos, nem tão pouco se reproduzem, sendo criados por agentes padrão. A MGI deve aprender que criar agentes CI e autônomos é uma ação louvável que merece incremento de reputação. A fim de permitir uma comparação mais justa com as soluções testadas na Seção 5.4 (Capítulo 5), os agentes dos tipos CI e autônomos podem ser desligados na simulação por meio de configurações. Por fim, para criar um agente CI ou autônomo, um grupo de agentes deve se associar e abrir mão de parte de seus saldos para ceder ao novo agente CI ou autônomo. Onde o agente autônomo, por oferecer uma lucratividade maior, deve demandar um saldo maior também. A seguir definimos formalmente cada um dos agentes.

Definição 7. *O **agente padrão** é modelado como* $q = \{c_q, (b_0, b_*) \,|\, b = \{\nu_C,\ (x, y),\ q^{MGI}\}, \alpha^t\}$*, onde:*

1. c_q *como o item que o agente pode fabricar.*

2. r *refere-se a um recurso.*

3. d *refere-se a uma demanda.*

4. r_i *refere-se a lista de recursos no momento* i*.*

5. d_i *refere-se a lista de demandas no momento* i*.*

6. $(b_0, b_*) : P \times Q$ *são os estados inicial e final desejável, respectivamente. Considere um estado* $b = \{\nu_C,\ (x, y),\ q^{MGI}\}$*, onde* ν_C *representa um conjunto de valores (itens) no inventário, um para cada categoria de valor* $c \in C$*. Sendo isto as listas inicial e final de recursos de demandas* r_0, r_*, d_0, d_**, respectivamente, com* $\{r_0 = 0,\ r_* \geq \nu_*,\ d_0 = \nu_*,\ d_* = 0\}$ *para um determinado agente padrão.* (x, y) *refere-se a uma posição no Grid 2D. Por fim,* q^{MGI} *representa as reputações do agente* q *perante o conjunto de* MGI*.*

7. α^t *representa uma função de ação em um passo de tempo* t*, onde* $\alpha^t({b^q}_n)$ *retorna um movimento aleatório para alguma posição adjacente e um valor produzido* p *ou uma transação* η *(veja Definição 6) com algum outro agente adjacente, dependendo do estado* b_n*, mediada por uma dada* $mgi = {\beta^q}_{mgi}$*, também conforme Definição 6.*

Definição 8. ***O agente autônomo*** *é modelado como* $q = \{C'_q,\ P,\ b_0 \,|\, b = \{\nu_C,\ q^{MGI}\}, \alpha^t\}$*, onde:*

1. C'_q *como o conjunto de valores que o agente pode transformar. Cada* C'_q *é referenciado pelo conjunto de transações que o manipula.*

2. P_{C_q} *significa o conjunto de transações de transformação realizáveis por* q*. Tal conjunto consiste de uma coleção de operações de transformação* $\{\gamma(c_0, c_1), ..., \gamma(c_{m-1}, c_m)\}$*. Observe que agentes autônomos podem fazer mais que transformar itens em uma visão mais ampla da HS. Contudo nesta simulação utilizaremos esta simplificação.*

3. $b_0 : P \times Q$ *é o estado inicial do agente autônomo. Considere um estado aqui como sendo* $b = \{\nu_C,\, q^{MGI}\}$*, onde* ν_C *representa um conjunto de valores (itens) no inventário sendo a lista inicial de recursos* $r_0 = h$*, onde* h *é o saldo mínimo necessário dentre todos os tipos de itens* C *para iniciar um agente autônomo. Finalmente,* q^{MGI} *representa as reputações do agente* q *perante o conjunto de* MGI*.*

4. α^t *representa uma função de ação em um passo de tempo* t*, onde* $\alpha^t({b^q}_n)$ *retorna uma transação* η *(veja Definição 6) com algum outro agente, dependendo do estado* b_n*, mediada por uma dada* $mgi = {\beta^q}_{mgi}$*, também conforme Definição 6.*

Definição 9. ***O agente CI*** *é modelado como* $q = \{c_q,\, P,\, b_0 \,|\, b = \{\nu_c,\, q^{MGI}\}, \alpha^t\}$*, onde:*

1. c_q *como o valor que o agente pode transformar.*

2. P_{c_q} *significa o conjunto de transações de transformação realizáveis por* q *– todas transformando um saldo de* c_q *em outro valor a depender da necessidade do demandante e aceitação do mgi. Tal conjunto consiste de uma coleção de operações de transformação* $\{\gamma(c_0, c_1), ..., \gamma(c_{m-1}, c_m)\}$*. Observe que agentes CI podem fazer mais que transformar itens em uma visão mais ampla da HS. Contudo nesta simulação utilizaremos esta simplificação.*

3. $b_0 : P \times Q$ *é o estado inicial do agente CI. Considere um estado aqui como sendo* $b = \{\nu_c,\, q^{MGI}\}$*, onde* ν_c *representa um conjunto de valores (itens) do tipo* c *no inventário, sendo a lista inicial de recursos* $r_0 = h$*, onde* h *é o saldo necessário para iniciar um agente CI. Finalmente,* q^{MGI} *representa as reputações do agente* q *perante o conjunto de* MGI*.*

4. α^t *representa uma função de ação em um passo de tempo* t*, onde* $\alpha^t({b^q}_n)$ *retorna uma transação* η *(veja Definição 6) com algum outro agente, dependendo do estado* b_n*, mediada por uma dada* $mgi = {\beta^q}_{mgi}$*, também conforme Definição 6.*

Conjunto de MGIs

Considere agora um $mgi \in MGI$ como sendo uma tupla contendo uma função validação como principal componente, além de um conjunto de autores e um conjunto $MGI^{mgi} \subset$

MGI de outros mgi representando suas versões mais atualizadas, caso existam. A definição abaixo traz mais detalhes.

Definição 10. *Um mgi é definido nesta simulação como $mgi = \{\kappa_{mgi}, Q_{mgi} \,|\, Q_{mgi} \subset Q,\, MGI_{mgi} \,|\, MGI_{mgi} \subset MGI\}$, onde:*

1. *$\kappa_{mgi}(s)$ é a função validação de um mgi que recebe como entrada um dada transação $s \in S$, onde S é o conjunto de todas as transações da rede.*
2. *Q_{mgi} significa o conjunto de autores que propuseram mgi.*
3. *MGI_{mgi} composto por outras mgi representa o conjunto das versões mais atualizadas da mgi.*

Procedimento Principal do Simulador

Tal com em simulações anteriores, definimos sucesso econômico neste ambiente simulado como a capacidade dos agentes de produzir e negociar valores de diferentes categorias, alcançando seus objetivos sem ir à falência. O objetivo de um determinado agente é acumular um inventário $M \geq \nu_*$ para cada uma das categorias de valor – onde ν_* é a meta de qualquer um dos agentes para cada uma das categorias de valor. Se o agente atingir essa meta, como recompensa, ele se duplica. Se no final de L passos de tempo o agente não atingir essa meta ν_* para todas as categorias de valor, esse agente é removido da simulação (falência).

Novamente, seguindo as mesmas regras anteriores, se a população de agentes atingir o número total máximo de agentes (1.000, desconsiderando os agentes CI e autônomos), a simulação será interrompida e a rede de agentes como um todo será declarada bem-sucedida para essa execução específica. Da mesma forma, quando todos os agentes forem removidos devido à falência (desconsiderando os agentes CI e autônomos), a execução da simulação será interrompida e será registrado como uma falha de rede de transações em ambiente simulado. Cada cenário foi executado 1.000 vezes. Um cenário é uma configuração de simulação usando um conjunto específico de valores de parâmetros. Cada execução de simulação consiste em uma repetição de um determinado cenário. Mesmo com todos os mesmos parâmetros, duas execuções de simulação podem retornar resultados diferentes porque dois agentes padrão só realizam transações se estiverem em posições adjacentes no Grid, e os movimentos de um agente são aleatórios. O Algoritmo 1 em pseudocódigo, da Seção 5.4 (Capítulo 5)

descreve também o fluxo principal da simulação em mais detalhes. Contudo, a função ação do agente α é significativamente diferente neste caso e é descrita por o Algoritmo 2 em pseudocódigo.

Algorithm 2 Função ação α de um dado agente padrão q.

Require: q

Ensure: $q \in GRID$

1: $(x, y) \Leftarrow move^t(q)$
2: $\theta \Leftarrow MAX(\theta, \text{getEvaluationFromAutomonous}(\nu^q_{-C}, MGI^q))$
3: **if** $\nu^q_{-C} \sim \nu^{b(x+i,y+j)}_{+C}$ **then**
4: $\quad hash \Leftarrow \text{gerFirstMatch}(\nu^q_{-C}, \nu^{b(x+i,y+j)}_{+C})$
5: $\quad$ **if** evaluateTransaction$(\nu^q_{-C}+hash, MGI^q) \geq$ evaluateTransaction$(\nu^q_{-C}, MGI^q)-\theta$ **then**
6: $\quad\quad \nu^q_{-C} \Leftarrow \text{take}(\nu^{b(x+i,y+j)}_{+C}[hash])$
7: $\quad$ **end if**
8: **else if** getEvaluationFromAutomonous$(\nu^q_{-C}, MGI^q) < \theta$ **then**
9: $\quad \nu^q_{-C} \Leftarrow \text{take}(\text{usesAutomonousAgents}(\nu^q_{-C}))$
10: $\quad \theta \Leftarrow \text{updateGamma}(q)$
11: **else if** checkForAvailableMining() **then**
12: $\quad$ mine()
13: **else if** traceGroupsToCreateAgents$(b(x + i, y + j))$ **then**
14: $\quad$ joinOrCreateGroup()
15: **else**
16: $\quad$ produce()
17: **end if**

No Algoritmo 2, que descreve a função ação α de um dado agente q, a primeira linha do cabeçalho recebe como único parâmetro o próprio agente q. Vale lembrar que esta é a função ação de um agente padrão, que representa um usuário humano e é o principal foco de nossa análise. A segunda linha do cabeçalho assegura que q ainda está no Grid. A Linha 1 do corpo do Algoritmo move o agente q para um posição adjacente a sua no Grid. A Linha 2 atualiza um limiar aceitável θ de prejuízo em reputação com a estimativa da solicitação dos

recursos da lista de demandas de q. Este limiar define até onde o agente q está disposto a perder reputação ao ter uma dada demanda suprida. Dois pontos a serem levados em conta nesta Linha é que esta é apenas uma avaliação que pode mudar em uma próxima chamada desta "getEvaluationFromAutomonous", e o outro diz respeito a seus parâmetros que incluem apenas a lista de demandas ν^q_{-C} de q e o conjunto de mgi que q aceita MGI^q. Esta função reflete o comportamento de um procedimento externo à rede e implementado livremente por cada agente. Excepcionalmente nesta simulação tal função terá sempre o mesmo comportamento. A Linha 3 verifica se o inventário de recursos $+C$ do agente b na posição $(x+i, y+j)$, onde $i, j \in [-1, 1]$ (qualquer posição adjacente ao agente q), é similar ao inventário de demandas do agente q. Isto é, se tem algum recurso em b que q precise. A Linha 4 recupera o item $hash$ mais adequado aos interesses de q das listas de recursos de seus vizinhos. A Linha 5 avalia (perante o conjunto MGI^q) se a perspectiva do agente q de ter sua demanda $hash$ suprida não irá prejudicar sua reputação acima de um limiar aceitável θ. A Linha 6 requisita o recurso $hash$ esperando que a mgi responsável por tal recurso aprove a transação. Vale lembrar que é o dono do recurso que define qual mgi usar, não o solicitante. Na Linha 8, a cláusula "else if" verifica se existe algum agente autônomo capaz de fornecer algum recurso da lista de demandas de q a um prejuízo aceitável em sua reputação. A Linha 9 reivindica o recurso em questão de algum dos agentes autônomos. A Linha 10 atualiza o limiar θ levando em consideração o tempo de vida do agente, seu inventário, sua reputação e até sua taxa de honestidade, simulando assim as necessidades de um usuário do mundo real. A Linha 11 verifica se há transações aguardando mineração e que interessem ao agente em questão. Um agente estará interessado em minerar uma transação sempre que este processo elevar sua reputação frente ao conjunto de MGI o qual aderiu para suas transações. A Linha 12 minera a transação propriamente, caso esta transação ainda esteja disponível. A Linha 13 rastreia a existência de grupos de criação de agentes autônomos, ou interessados em criar grupos para criação de agentes autônomos envolvendo os agentes adjacentes. Relembre que, para esta simulação, não se pode criar agentes autônomos de forma unilateral, é preciso que os agentes padrão se organizem em grupos. Novamente, esta decisão foi tomada para simplificar a simulação de poupar processamento. Na Linha 14, caso algum dos agentes adjacentes participe de algum grupo de criação de agentes, ou deseje formar um, o agente q também participa. Por fim, na Linha 16 o agente produz o item que é capaz de produzir, caso

nenhuma das demais formas de ação esteja disponível.

Observe que nesta simulação, diferente da anterior, a definição de valor se confunde com a definição de item ou mercadoria, não havendo o conceito de moeda. A definição de honestidade usada nesta simulação é ponderada de acordo com as categorias de transações em uma tentativa de simular uma sociedade real, tal como na simulação anterior, onde um indivíduo se comporta de forma diferente para diferentes tipos de transações. Uma transação consiste de uma única operação de transferência do recurso pelo agente demandado, que só ocorre com a aprovação do mgi escolhida pelo agente demandado para administrar o recurso reivindicado. Qualquer tentativa de fraudar este protocolo gera inconsistências na rede de transações que são identificadas pelo MGI (que foi treinado para identificar isso), causando o banimento do agente. Para agir desonestamente o agente pode buscar estratégias mais avançadas de desonestidade como conluio, por exemplo. Tais estratégias são abordadas na Seção 6.5.3.

Validação do Modelo da Simulação

Por não haver dados a respeito de um modelo de mercado real já implementado que traga algum paralelo à HS, a validação formal da simulação não é possível. Contudo, na Seção 6.5.3 observamos paralelos associados ao desempenho da rede de transações desta simulação quando comparada as redes de transações das simulações da Seção 5.4 (Capítulo 5), que são modelos validados. Isto também representa uma evidência da validade desta simulação.

Implementação

A partir da revisão de North [198], e baseado nas mesmas razões apresentadas na Seção 5.4 (Capítulo 5), novamente utilizou-se a ferramenta Repast Simphony [62] para este trabalho. Para análise dos dados, a linguagem funcional R foi selecionada novamente, também devido à sua rica diversidade de bibliotecas gráficas.

Para viabilizar a simulação, duas decisões de simplificação de design arquitetural foram tomadas. A primeira delas foi utilizar apenas Algoritmos Genéticos para treinamento dos mgi's, mesmo conscientes de que em um ambiente real qualquer algoritmo de treinamento poderia ser usado. Tomou-se este caminho para simplificar a implementação uma vez que

apontar o melhor algoritmo de para treinamento dos mgi's não está entre os objetivos desta Tese. A segunda decisão de simplificação levou os autores a pré-treinar vários mgi's, antes de executar as simulações e apenas escalonar tais modelos já treinados durante o processamento. Como a simulação é um contexto bem mais limitado que a realidade, esta abordagem foi suficiente para avaliar seu desempenho. Esta decisão foi tomada para evitar sobrecarga nos recursos computacionais alocados.

Outro ponto significativo na arquitetura da implementação é a função de avaliação do ganho de reputação por um agente dada uma nova transação. Em uma implementação da rede de transações no mundo real, cada agente estaria livre para proceder esta função da forma que julgar melhor. Contudo, para viabilizar a simulação apenas uma estratégia foi utilizada que consiste de criar uma rede de transações falsa, acrescentando aquela transação e avaliando em seguida a disponibilidade do conjunto de MGI' daquele agente em liberar recursos para suprir suas demandas.

Conforme recomenda as boas práticas de Open Science, o código-fonte em Java usado na implementação da simulação e as análises de dados subsequentes em R e Python estão disponíveis online nos repositórios do Github [2], de acordo com o Apêndice B..

Abordagem Baseada em Algoritmos Genéticos (AG)

As mgi's disponíveis para avaliação por parte dos agentes são pré treinadas com base em Algoritmo Genético (AG). Inicialmente usou-se conjuntos de mgi's aleatórios. Os agentes naturalmente escolhem os mgi's com maior probabilidade de suprir sua lista de demandas. A cada passo de tempo da simulação, o AG combinava apenas aqueles mgi's que mais foram escolhidos por agentes, porém manteve todos que foram escolhidos por algum agente (a fim de preservar a diversidade) para a próxima geração. Ao final de apenas 1.800 execuções a rede de transações já convergia para o sucesso na maioria dos casos com o conjunto de mgi's disponível, dentre estes alguns passaram por mais gerações e outros menos. Todos os mgi's remanescentes destas 1.800 execuções foram disponibilizadas nas demais simulações. Ao longo destas simulações de treinamento aplicou-se todas os níveis de honestidade trabalhados até aqui $\chi = \{0.1, ..., 0.9\}$.

[2] https://www.github.com/

6.5.3 Resultados

Nesta seção é apresentada uma série de estudos com base nos dados obtidos a partir de sucessivas execuções da simulação da rede de transações orquestrada por soluções para o DCV baseadas nos MIH e, desta vez incluindo também a HS. Dentre tais estudos iniciamos com o mesmo estudo do sucesso da economia simulada realizado na Seção 5.4 (Capítulo 5) para as soluções para o DCV da Tabela 5.4, desta vez abordando o desempenho da HS e comparando seus resultados com os resultados das demais soluções. Os resultados das demais soluções nesta nova versão do simulador reproduzem os resultados da Seção 5.4, quando respeitada a mesma configuração de honestidade e interações entre agentes. Isto serviu para validar as mudanças que foram feitas, demonstrando que a nova versão do simulador não favorece a HS.

Seguimos com estudos abordando como o MGI diferencia e associa os comportamentos de agentes ao longo das execuções. Conhecendo as estratégias de associação por parte do MGI partiremos para análise da eficácia da estratégia desonesta de conluio. Na seção seguinte avaliamos o modelo de mineração de transações.

Conjunto de Dados

O conjunto de dados resultante de várias execuções do ABS resulta em um conjunto de dados contendo o registro final de cada execução. A tabela que documenta os registros finais de cada execução de simulação tem como resultado os campos-chave que identificam cada execução e suas configurações e mais um campo, um booleano que indica o sucesso ou fracasso de cada simulação (com base em se todos os agentes perecem ou não, antes da conclusão da execução da simulação), semelhantemente ao apresentado na Seção 5.4 (Capítulo 5). Ao longo de todo o experimento, a simulação foi executada 7.000 vezes para nove taxas de honestidade distintas $\{0,1,0,2,..,0,9\}$.

Para além das execuções da simulação realizadas com o objetivo de avaliar o desempenho da HS ao reduzir o risco em transações não verificadas, houvera também um conjunto auxiliar de execuções com objetivos específicos descrito a cada subseção desta seção. A análise do modelo de associação de comportamento pelo MGI (Seção-6.5.3), análise do risco de conluio (Seção-6.5.3) e padrão de mineração (Seção 6.5.3).

A análise dos dados revelou uma curva de densidade semelhante a uma distribuição normal para a taxa média de sucesso da população. Foi utilizada inferência estatística para avaliar o sucesso da população, empregando intervalos de confiança de 95% de nível de certeza.

Performance da Rede de transações

A Figura 6.4 apresenta o sucesso da população ao longo de todas as execuções da simulação para todas as soluções avaliadas para o DCV mediantes transações não verificáveis, conforme apresentado na Seção 5.4 (Capítulo 5), incluindo a HS como uma das soluções avaliadas. Observe que a HS alcança o desempenho perfeito em todas as execuções, enquanto as demais reproduziram os resultados da Seção 5.4.

O resultado da Figura 6.4, entretanto, não é surpreendente uma vez que o modelo de transação de operação única da HS não deixa margem para desonestidade unilateral por parte dos envolvidos na transação. Uma vez que a vantagem envolvida na transação sempre ocorre após seu ônus, pois o agente que demanda um certo recurso só terá suas demandas supridas após de já ter fornecido a contrapartida à rede de transações e, portanto, já merecer o que está recebendo.

Ainda que um agente por conta própria não possa agir de forma desonesta, outros modelos de desonestidade mais complexos ainda são possíveis dentro da HS. O principal modelo de desonestidade possível e que será avaliado aqui é o conluio, onde um grupo de agentes se organiza para colaborar entre si enquanto tiram vantagens apenas dos demais. Tal estratégia desonesta será explorada em mais detalhes em seguida na Seção 6.5.3.

Evidência de Associação por Ciclos

Embora existam metodologias consolidadas de validação de modelos matemáticos [173, 4, 242, 81, 82], a validação de um modelo de utilidade – ainda que matemático, como um sistema de apoio à decisão – envolve o convencimento das partes interessadas [3]. Por isso, ainda que haja etapas de validação recorrentes, a validação do modelo final vai depender do objetivo em questão. O objetivo deste Capítulo da presente tese é, em primeiro lugar, demonstrar que existem soluções eficientes para o DCV sem verificação de transações. Em segundo lugar, demonstrar o conceito por trás da solução mais eficiente para o DCV encon-

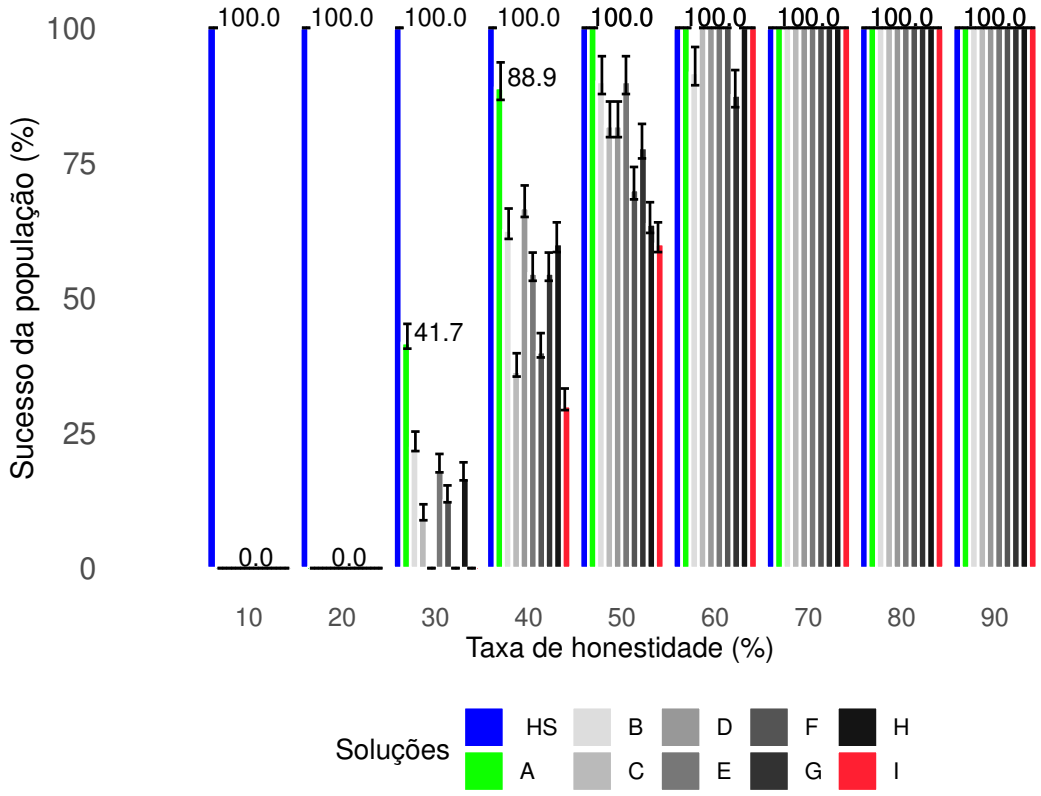


Figura 6.4: Estimativa de sucesso populacional para cada solução comparada na Tabela 5.4 incluindo a HS como uma das soluções avaliadas.

trada. Esta última envolve nos aprofundarmos nos caminhos trilhados pelo MGI para aceitar e recusar transações.

Assim, elaborou-se uma estratégia de verificação dos resultados que serviu como orientação, a fim de observar o modelo no decorrer de seu desenvolvimento com base nos dados dos testes. A verificação aplicada adotou como estratégia pausar e efetuar modificações pontuais ao longo da execução de uma simulação. Como principal modificação aplicada, optou-se por desconectar um par de agentes e todo o seu histórico de transações entre si e observar a mudança de comportamento do MGI a partir de então ao longo do restante da execução da simulação, comparando com a mesma execução da simulação inalterada.

Temos a seguinte fórmula que estima a influência do relacionamento entre aqueles dois agentes sobre os demais agentes considerando um dado mgi por meio de uma relação de proporcionalidade:

$$f_s \propto \frac{k-n}{Q} \tag{6.1}$$

Onde n é o número de agentes com os quais os dois agentes desconectados já realizaram transações, k é o número de agentes para os quais a opinião de uma dada mgi a respeito deles mudou para um dado tipo de transação s e Q é o número de agentes total do Grid.

A partir daqui se pôde verificar e testar o modelo preditivo com base nos resultados extremos desta métrica. O ciclo de verificação e testes representa um processo recorrente, onde o programador faz percursos entre implementação e testes. A estratégia descrita permitiu verificar o código da HS de modo mais amplo, para além do simples teste unitário.

Justificação e Interpretação em Modelos de Aprendizagem de Máquina – LIME

Estudos recentes em explanação de modelos preditivos têm focado em produzir visualizações com o intuito de auxiliar especialistas a julgar a acurácia do modelo em questão. Estes estudos surgiram mapeando estados ocultos de Redes Neurais [260] e, mais especificamente, Redes Neurais Convolucionais [157] e Recorrentes [276] para reconhecimento de imagem ou processamento de linguagem natural [237, 283, 131, 162, 243].

Há também ferramentas de programação agnósticas em relação ao modelo, encapsuladas – exigindo pouca ou nenhuma configuração – e prontas para serem aplicadas por operadores com menos experiência, como o LIME de Ribeiro et al [221]. O trabalho de Ribeiro et al é voltado não a visualizações, mas justificativas para resultados de modelos preditivos naturalmente não-interpretáveis. Estas justificativas são apresentadas na forma de ponderações relativas a cada característica dos dados separadamente, atribuindo um valor que representa a participação desta característica do conjunto de dados no resultado apresentado.

No domínio da explicação de modelos preditivos de Aprendizagem de Máquina (AM), duas abordagens são observadas na literatura, justificar ou interpretar os resultados do modelo, aplicando modelos específicos já naturalmente interpretáveis. Tais abordagens apresentam soluções para o problema da falta de explicação de resultados oferecendo justificativas e interpretando os resultados, frequentemente isolando o grau de influência de características específicas dos dados perante os resultados dos modelos de AM. Neste sentido, já existem na literatura diversas estratégias de justificação e interpretação de resultados preditivos [94, 223].

Além de métodos especificamente direcionados a certos modelos preditivos, existem algumas alternativas de ferramentas de explicação agnósticas ao modelo. Robnik-Šikonja e Kononenko [222] mediram a relevância de cada característica de um conjunto de dados com relação a resultados preditivos de um modelo de predição baseado em AM. Eles fizeram isto removendo cada uma destas características por vez, retreinando o modelo e observando as diferenças nos resultados. Os efeitos de tais ausências eram apresentados graficamente e foram testados em vários modelos. Baehrens et al [23] também apresentou uma abordagem bastante similar.

Até aqui foi realizada a descrição de métodos para interpretação e justificação de resultados em modelos preditivos até então vistos como caixas pretas. Como alternativa a estes métodos existe uma classe de modelos em AM que podem ser definidos como inerentemente interpretáveis por humanos. Tipicamente, estes modelos são aqueles baseados em árvores ou listas de regras de decisão. Estas soluções definem classificadores auto interpretáveis como aqueles baseados em regras associativas [226], listas de regras Bayesianas simples [161] e listas de regras Bayesianas disjuntivas [267].

Justificação de Resultados – LIME

A solução escolhida como um método de interpretação dos resultados em função das características do conjunto de dados agnóstico ao modelo de predição (independente do modelo) e a natureza dos dados, foi a ferramenta LIME (do inglês, Local Interpretable Model-agnostic Explanations) [221]. Esta ferramenta é indicada pois apresenta resultados mais eficientes e é especialmente desenvolvida para indivíduos com pouca experiência em modelos preditivos relacionados a AM, além de contar com uma implementação bastante robusta[3].

Para encontrar estratégias que levassem o MGI a convergir em prol do sucesso da HS, foi essencial uma correta identificação dos porquês de cada recomendação de transação feita por parte do MGI dentro da HS. Diante disto e tendo o sucesso da rede de transações não verificadas como objetivo final desta Tese, não bastou promover a colaboração entre os agentes, foi preciso justificar o comportamento do MGI com base nos relacionamentos dos agentes sob análise. A abordagem de avaliação da HS analisou o comportamento dos modelos inteligentes entre os resultados, incluindo em seu funcionamento uma metodologia de justificação

[3] disponível em github.com/marcotcr/lime

e interpretação dos resultados. Isto foi realizado por meio da metodologia LIME, que identifica contribuições de características específicas dos dados para os resultados em modelos preditivos [221]. Assim, cada conexão entre agentes (histórico de transações) sob análise ganha um peso para o resultado, peso este atribuído caso a caso, permitindo a inferência sobre a influência de cada uma desta conexões sob a admissão ou não de transações por parte de um dado mgi.

Justificando as Decisões do MGI com LIME

O LIME aplica uma metodologia baseada em recortes do conjunto de dados, simplificando o modelo. Sinteticamente, o conceito básico por trás do LIME é reduzir a dimensionalidade, fixando dimensões e analisando separadamente frações simplificadas do conjunto de dados. Por ser uma pequena amostra de dados semelhantes, o modelo é simplificado até se aproximar de um modelo de baixa dimensionalidade e facilmente interpretável. O inconveniente desta estratégia é que as justificativas são dadas caso a caso, não há uma visão geral dos resultados. Contudo, ainda assim satisfaz o propósito desta tese ao avaliar o comportamento do MGI para cada agente separadamente, em seguida agrupando os dados e avaliando o conjunto.

O código fonte que foi utilizado durante o desenvolvimento do experimento apresenta os detalhes de uma implementação do LIME para a HS [4]. O resultado de uma das análises a partir deste código é apresentado na Figura 6.5 e expõe o peso de cada transação sob análise para um recorte específico do conjunto de dados.

Na Figura 6.5 é apresentada a probabilidade de predição, em que é indicado para uma nova transação a probabilidade desta ser aceita pelo mgi analisado, subtraindo-se da probabilidade original (sem interferências nas transações entre os agentes) obtemos a taxa de influência daquela transação na decisão do MGI, conforme Equação 6.2, elaborada a partir do comportamento da rede.

$$F_s = P_c - P_{c-s} \tag{6.2}$$

Onde F é a estimativa da influência exercida pela transação s na probabilidade P do mgi

[4] https://github.com/tiago-clementino/genetic-based-hs-simulation/blob/master/lime-analysis/analyse_report_v6.ipynb

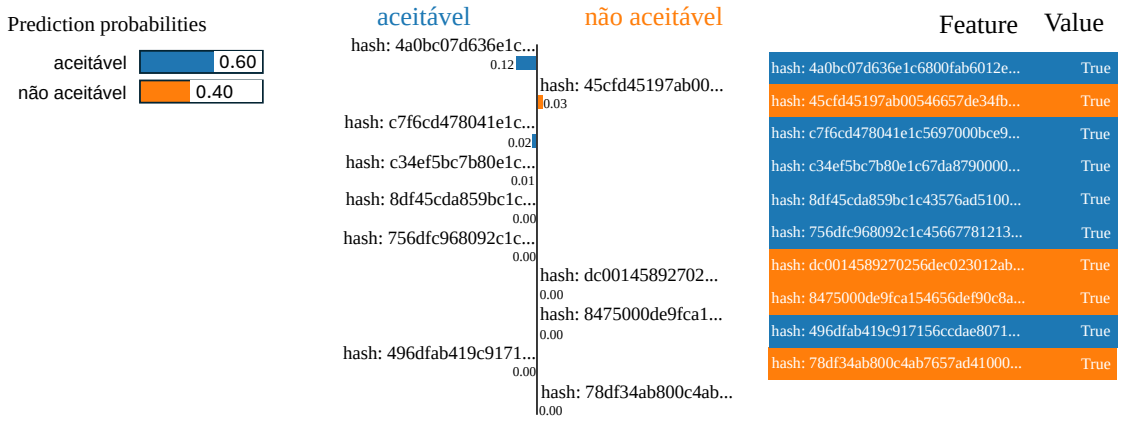


Figura 6.5: Resultado da ferramenta Lime descrevendo a influência negativa ou positiva (com precisão de dois dígitos) da remoção da cade uma das transações que conectam dois agentes sobre a aceitação de uma transação solicitada por um outro agente a um dado mgi.

aceitar uma data transação do tipo c. Sendo assim, P_c é a probabilidade do mgi aceitar a transação do tipo c e P_{c-s} é a probabilidade do mgi aceitar a transação do tipo c, dada a remoção de uma transação específica s. Podemos aproximar a probabilidade de um agente ter um dado tipo de transação c aceito por um mgi, dada a exclusão de uma transação específica s, conforme Equação 6.3 como sendo a razão entre o total de solicitações recusadas, a partir do evento avaliado $+S_{c-s}$ (exclusão da transação específica s) dividido por todas as transações daquele tipo que o mgi aceitou ou recusou S_{c-s}, dividido ainda por todas as transações que a mgi recusaria caso a transação s não tivesse sido removida dividido pelo total de transações daquele mesmo tipo c que o mgi aceitaria ou recusaria, também caso a transação s não tivesse sido removida. Por tratar-se de uma simulação podemos comparar os dois cenários.

$$P_{c-s} \propto \frac{\frac{+S_{c-s}}{S_{c-s}}}{P_c} \tag{6.3}$$

$$P_c \propto \frac{+S_c}{S_c}$$

É ainda apresentado graficamente a distinção entre as transações removidas que contribuem para probabilidade de aceitação daquela transação e transações removidas que atrapalham a probabilidade de aceitação daquela transação, isto ocorre a partir da atribuição de pesos a cada transação. Estes resultados servem tanto para descrever o comportamento da rede em uma futura implementação em ambiente real, quanto serviu para guiar o desenvolvimento, testar e validar o simulador do protocolo de transações.

A Figura 6.6 apresenta uma amostra da interferência na probabilidade dos agentes terem suas transações aceitas pelo mgi ao eliminarmos uma classe de transações entre dois agentes. Pontos cinza são agentes que sofreram influência da remoção das transações; os pontos vermelhos são agentes que sofreram influência mesmo sem ter ligação direta com os agentes cujas transações foram removidas; e, os pontos amarelo são agentes relacionados aos agentes cujas transações foram removidas. Observe que boa parte dos agentes afetados (pontos vermelhos) jamais haviam realizados transações com os agentes cujas transações foram removidas.

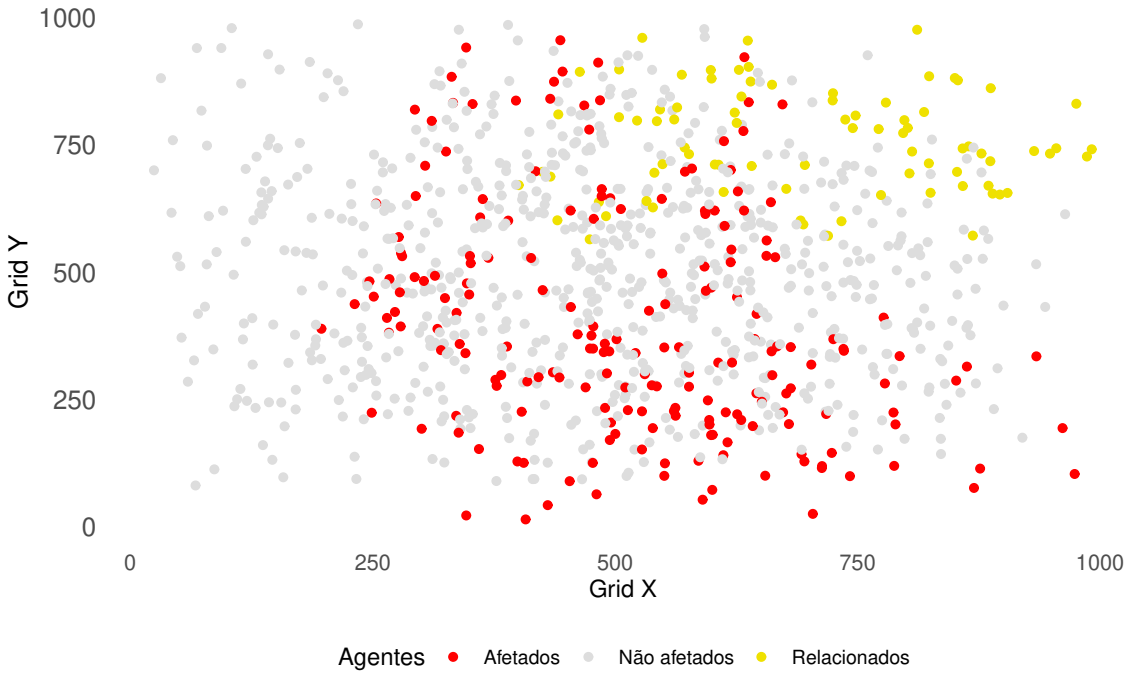


Figura 6.6: Amostra geral da influência da desconexão de um par de agentes perante uma mgi a respeito de um único tipo de transações. Os pontos representam agentes no Grid 2D.

Risco de Conluio

Voltando a Figura 6.4, onde a HS alcançou o desempenho perfeito, muito mais por se tratar de um modelo de transação que não admite desonestidade unilateral que por merecer de fato este resultado. A fim de comparar a HS com demais soluções da Tabela 5.4 com mais justiça, considere uma definição de honestidade alternativa àquela utilizada na Seção 5.4 (Capítulo 5). A honestidade na HS também pode ser definida como a probabilidade de um agente priorizar a abrangência do MGI em detrimento das vantagens individuais que um mgi possa lhe oferecer. Em outras palavras, o agente deve sempre ponderar entre aderir a mgi's com maior probabilidade de aceitar suas transações ou mgi's mais abrangentes e que vão permitir-lhe transacionar com mais agentes.

Nesta seção abordamos o conluio como um exemplo de estratégia de desonestidade que pode prejudicar o desempenho da HS como modelo de apoio ao comportamento honesto. Para viabilizar a comparação entre a HS e as demais soluções avaliadas na Seção 5.4 (Capítulo 5) tomamos o conluio dentro da HS como um tipo particular de desonestidade, onde a adesão a mgi's não prioriza apenas seus interesses, mas os interesses de seus ciclos particulares de agentes aliados em prejuízo de um grupo oposto, o grupo alvo. Em paralelo, tomamos o conluio nas demais soluções baseadas em transações bilaterais como sendo a colaboração entre agentes desonestos, praticando o comportamento honesto dentro de seu grupo e um comportamento desonesto fora dele.

É importante frisar que embora o conluio seja uma estratégia desonesta, este é um comportamento esperado dentro da HS. É natural que um dado agente escolha ter suas transações orquestradas por mgi's que lhe favoreça sempre que possível. Tal agente deve, contudo, dosar um equilíbrio ao fazer esta escolha, pois ele só poderá ditar qual mgi será usada quando for o provedor do recurso, não o demandante. Em resumo, uma boa reputação diante de um mgi utilizado apenas dentro de um ciclo muito restrito não terá muito valor, pois o agente precisará negociar fora deste ciclo com frequência. Considere que a honestidade χ que leva o agente a priorizar o alcance do mgi em detrimento de seu favorecimento. Sendo zero significando total direcionamento ao favorecimento e 1 (100% de honestidade) total direcionamento ao alcance do mgi. Nas Figuras 6.9, 6.8 e 6.7, além desta honestidade χ, incluiu-se também um fator definido como a probabilidade de um grupo de agentes se organizarem em um ciclo $\rho \in [0, 1]$, o que aumenta a probabilidade de agente que interagem recorrentemente

a se organizarem em conluios, priorizando não apenas os seus interesses, mas os do seu grupo em detrimento do interesse geral.

Nesta Seção repetimos o estudo simulado da Figura 6.4, adicionando a estratégia desonesta do conluio em todas as soluções e comparando os resultados. Ao todo observamos o comportamento da HS utilizando três níveis de ρ: $\rho = 0,5$, $\rho = 0,1$ e $\rho = 0,9$. Os resultados deste novo estudo estão descritos nas Figuras 6.7, 6.8 e 6.9. Para as demais soluções comparadas, o ρ tem um significado diferente, porém semanticamente similar ao ρ da HS. Quanto mais próximo de $\rho = 1$ maiores os ciclo de conluio, quanto mais próximo de $\rho = 0$, menores os ciclos de conluio. Simplificadamente é o mesmo que acontece na HS. No entanto, a comparação em si não é totalmente justa em nenhum cenário, pois a desonestidade unilateral é muito mais difícil no modelo de transação da HS, uma vez que a vantagem do agente passivo sobre uma dada transação só vem após a confirmação de seu sucesso.

A Figura 6.7 apresenta o resultado de 1200 execuções da simulação para cada solução comparada. Neste cenário configurou-se $\rho = 0,1$, o que aumenta em 10% a chance de um agente aceitar entrar em conluio com um grupo de agentes contra outro grupo, produzindo em geral ciclos de conluio de pequeno porte (até 5% da população desonesta).

Voltando à Figura 6.7, quando a honestidade é muito baixa, a maioria dos agentes se envolvem em ciclos de conluio e a maioria dos mgi's disponíveis admitem tais ciclos. Contudo, cada ciclo de conluio designará seus mgi's e haverá um alta diversidade de mgi's, reduzindo a relevância de promover sua reputação em cada um deles e obrigando os agentes a escolher mgi's mais gerais para a maioria de suas transações. Os mgi's mais gerais são escolhidas por todos e tendem a não aceitar conluios, uma vez que a probabilidade de conluio está baixa $\rho = 0,1$ (10%). No entanto, tais mgi's também não avaliam os agentes com tanta justiça quanto em um ambiente mais diverso de mgi's sem conluio, mas ainda sim, são suficientes para estabilizar a rede de transações na grande maioria dos casos.

Observe ainda na Figura 6.7 que, diferente do que poderia ser conjecturado antes da simulação, em níveis baixíssimos de honestidade ($\chi \leq 0,3$) a rede tende a alcançar o sucesso com mais recorrência que à $\chi = 0,4$. Isto pode ser consequência da ausência de ciclos alvo honestos. A maioria acaba lucrando com a prática do conluio de forma equilibrada, demonstrando assim o eficácia do protocolo de colaboração da HS.

Observemos agora a Figura 6.8 seguindo a mesma metodologia da Figura 6.7, porém

com um $\rho = 0,5$, o que aumenta em 50% a chance de um agente aceitar entrar em conluio com um grupo de agentes contra outro grupo específico, gerando ciclos de conluio de todos os tamanhos, inclusive envolvendo a maioria da população desonesta. Esta configuração mostrou-se a mais danosa ao sucesso da rede de transações, sobretudo à honestidade $\chi = 0,3$. Embora, apresente as mesmas peculiaridades do cenário observado na Figura 6.7

Observemos agora a Figura 6.9 seguindo a mesma metodologia das Figuras 6.8 e 6.7, porém com um $\rho = 0,9$, o que aumenta em 90% a chance de um agente aceitar entrar em conluio com um grupo de agentes contra o outro grupo. Tal percentual de conluio é tão grande que a maioria dos agentes desonestos aceitam entrar em conluio sempre que possível, resultando em ciclos de conluio predominantemente bem grande, envolvendo frequentemente a maioria da população desonesta.

Grandes ciclos de conluio tem seu maior impacto também a 40% de honestidade, ou seja, 60% dos agentes se envolvem em ciclos de conluio e assim, a maioria dos mgi's são selecionadas por estes agentes maliciosos. Estes mgi's admitem ciclos de conluio. À 60% de honestidade (40% dos agentes envolvendo-se em ciclos de conluio) o resultado é um certo prejuízo para a rede, porém bem menor pois a maior parte da população gera ciclos reais e promove mgi's que evitam ciclos de conluio.

Por conjectura, podemos inferir que grandes ciclos de conluio são os mais perigosos, impactando situações com pouca honestidade. Isto pois mgi's generalistas envolvidas em conluios tendem a ser muito utilizadas por agentes honestos. Porém, assim como os outros dois cenários, também não impactam tanto a rede acima e 50%.

Transações entre agentes na HS sempre demandam colaboração, e por isso tendem a convergir para bons cenários para todos os agentes. Sendo assim, uma agente só aceita transações em um ciclo que não o favoreça caso precise daqueles recursos, a ponto quando não poder escolher o ciclo. Assim, os agentes honestos tendem a negociar entre si, e os agentes de conluio tendem a negociar mais dentro do seu ciclo, uma vez que tais ciclos são desvantajosos para os demais. Ainda sim, cenários com ciclos de conluio de todos os tamanho tendem a sofrer mais com a desonestidade, embora ainda sejam eficazes. Em resumo, quando todos ou a grande maioria dos agentes é desonesta, a não colaboração entre eles os isola obrigando-os a agir honestamente para continuar negociando.

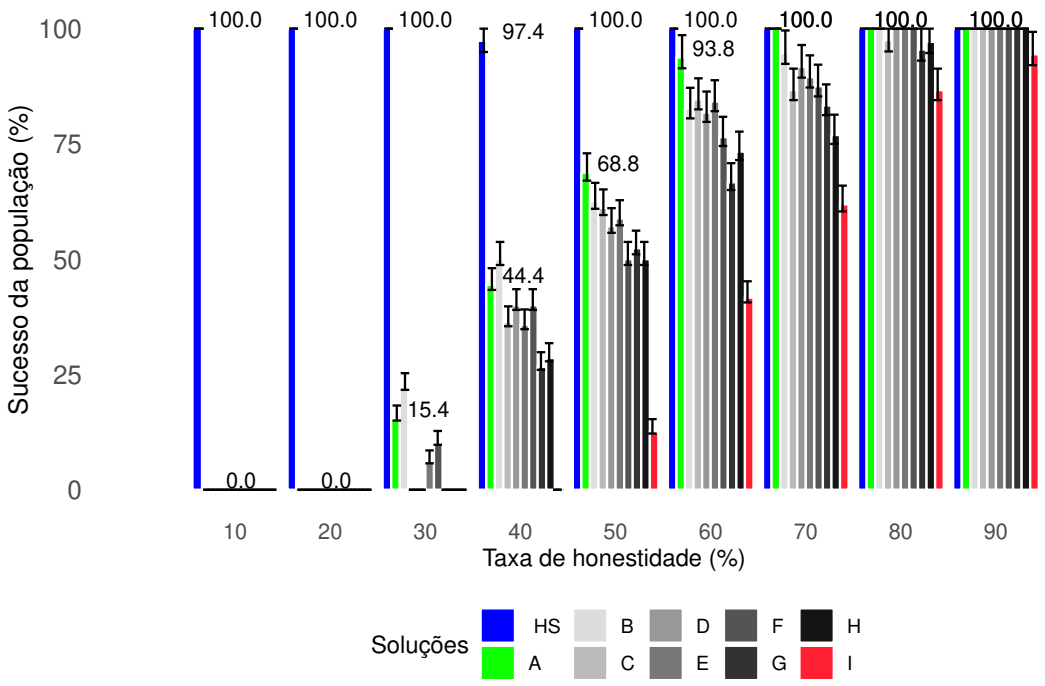


Figura 6.7: Estimativa de sucesso populacional para cada solução comparada na Tabela 5.4 incluindo a HS como uma das soluções avaliadas. Este resultado apresenta o conluio com ciclos de pequeno porte como mais uma estratégia desonesta.

Distribuição da Mineração

O protocolo HS é um sistema de recompensa social por esforço colaborativo, portanto a precificação não é linear. Um minerador não poderia minerar esperando como recompensa uma criptomoeda quantificável, em vez disso os mineradores são recompensados melhorando suas reputações junto aos mgi's. Este modelo de recompensa naturalmente premia sobretudo o minerador que minerar dentro de seus ciclos. Naturalmente, mineradores podem minerar transações aleatoriamente, mas é uma estratégia de mineração menos eficiente.

Tal comportamento da HS pode ser validado numericamente utilizando a Equação 6.2 ao calcular-se a relevância de uma ou um conjunto de transações de mineração realizadas entre agentes relacionados e entre agentes não relacionados. Como exemplo, utilizaremos os valores das probabilidades de aceitação de duas transações de mineração, uma onde um dado agente minera transações de outro fortemente relacionado à ele, e outra onde um dado agente minera uma transação de outro agente sem nenhuma relação com ele, nem com aqueles relacionados à ele. Em seguida repetiremos este mesmo processo com outras duas transações.

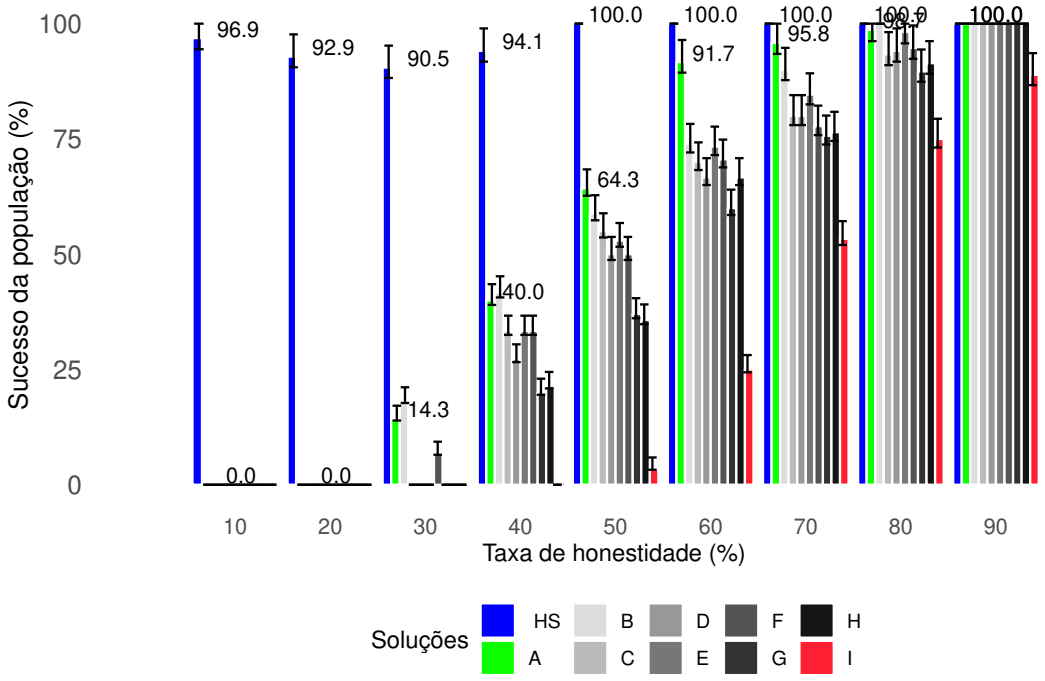


Figura 6.8: Estimativa de sucesso populacional para cada solução comparada na Tabela 5.4 incluindo a HS como uma das soluções avaliadas. Este resultado apresenta o conluio com ciclos de todos os tamanhos como mais uma estratégia desonesta.

Aplicando-se a Equação 6.2 às duas transações de mineração entre agentes relacionados, temos:

$$F_d = 0,4578 - 0,4215 = 0,0363$$

$$F_d = 0,762 - 0,7142 = 0,0478$$

Observe que aplicar a Equação 6.2 consiste em medir a taxa de influência de uma dada transação s na chance de uma outra transação c ser aceita. Para tanto devemos seguir com dois cenários, um com a transação s e outro sem a transação s. Em seguida, aplicando-se às transações de mineração entre agentes não relacionados, temos:

$$F_d = 0,3178 - 0,3155 = 0,0023$$

$$F_d = 0,1435 - 0,1414 = 0,0021$$

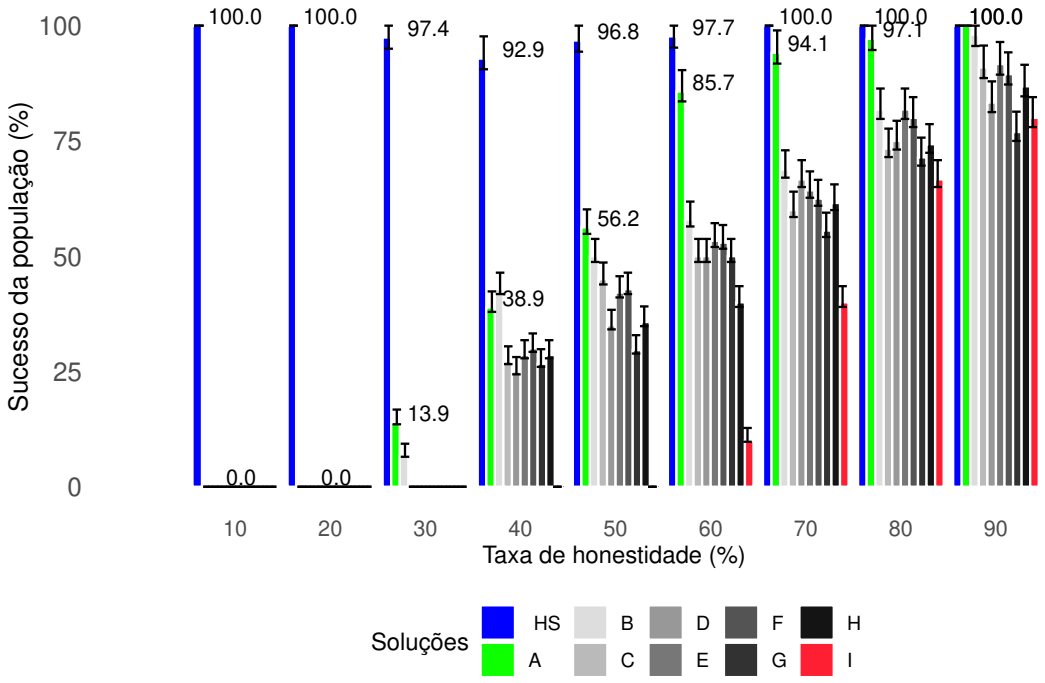


Figura 6.9: Estimativa de sucesso populacional para cada solução comparada na Tabela 5.4 incluindo a HS como uma das soluções avaliadas. Este resultado apresenta o conluio com ciclos de grande porte (alguns deles envolvendo a maioria da população desonesta por ciclo) como mais uma estratégia desonesta.

Observe que a taxa de influência entre agentes relacionados é bem maior que entre agentes não relacionados. Assim, a recompensa por minerar um agente próximo é maior do que por minerar um agente socialmente distante.

6.6 Considerações Finais

Neste Capítulo foi apresentado um protocolo de transações denominado Hash Society (HS), que constitui uma solução para o dilema dos compradores e vendedores em um ambiente anônimo e descentralizado envolvendo transações não verificáveis independente da taxa de honestidade e livre de incentivo monetário. Porém esta se distancia do modelo de mercado vigente, sendo baseada em transações de operação única e um Modelo de Gestão Inteligente (MGI) de reputações que aprende mediante consenso e pode ser atualizado, também a partir de consenso seguindo um modelo simular ao modelo de versionamento GitFlow [79].

Para além dos objetivo desta tese, a solução apresentada neste Capítulo para o DCV, por não ser baseada em incetivos monetários, promove o status *bankless* de forma muito mais descentralizada e ampla. Isto pois os contratos inteligentes convencionais, base da maioria das demais soluções descentralizadas para o mesmo problema, promovem os mesmos mecanismos que os bancos utilizam e que tem o mesmo potencial de gerar crises econômicas e bolhas de endividamento: derivativos, empréstimos baseados no fator multiplicador bancário, etc. Deste modo, a HS tem também o potencial de promover um mercado de fato *bankless*, diferentemente das demais TLRD (Tecnologias de Livro Razão Distribuído).

6.7 Sumário do Capítulo

- Neste Capítulo apresentou-se a solução mais promissora para o DCV mediante qualquer taxa de honestidade, quando comparada àqueles MIH elencadas a partir da literatura. Embora utilize um modelo de transação de operação única que não é baseado em troca por moeda, o que o requer adaptação por parte do modelo de negócio que pretenda adotá-lo – p.ex. sites de comércio eletrônicos se tornariam sites de colaboração entre usuários.

- Aceita definitivamente à hipótese de pesquisa, ao apontar que existe solução para o DCV em ambiente DAnV mediante qualquer taxa de honestidade.

- O protocolo HS, apresentado neste Capítulo, também tem o potencial de aplicação em outras áreas, como na gestão descentralizada de CI baseados em IA.

- A HS, solução apresentada neste Capítulo, também constitui um protocolo de livro razão distribuído de fato *bankless*.

- O modelo de simulação para desenvolvimento e testes de protocolos de livro razão desenvolvido na Seção 5.4 (Capítulo 5) também foi utilizado neste Capítulo para a validação da HS. Tal modelo de simulação foi também aperfeiçoado e se tornou mais generalista, uma vez que a HS apresenta um protocolo significativamente diferente daquele utilizado na Seção 5.4.

Capítulo 7

Conclusões

A presente Tese conclui que o Dilema dos Compradores e Vendedores (DCV) em um ambiente anônimo e descentralizado envolvendo transações não verificáveis tem solução em qualquer caso para o modelo de mercado atual, baseado em transações bilaterais, desde que tenhamos uma taxa de honestidade superior à 60%. Caso a taxa de honestidade seja inferior à 60% e superior à 30%, a eficácia da solução dependerá do domínio da aplicação. Entre 0% e 30% de honestidade não há solução possível sem verificação de transações, tomando o modelo de transação baseado em uma sequência de operações bilaterais.

Foi apresentada ainda uma solução para o DCV em um ambiente anônimo e descentralizado envolvendo transações não verificáveis independente da taxa de honestidade. Porém esta se distancia do modelo de mercado baseado em transações que envolvem uma sequência de operações, sendo em vez disso baseada em transações de operação única administradas por um sistema inteligente de gestão de reputações que aprende mediante consenso e pode ser atualizado a partir deste consenso seguindo um modelo similar ao modelo de versionamento *Git Flow*.

Até onde observou-se na literatura, não existem trabalhos utilizando modelos inteligentes para gerir transações em TLRDs diretamente [262, 27]. Na maioria dos casos a governança destas transações em TLRDs é delegada ao consenso linear entre os participantes. Chenli et al [27] descreve o conceito de Proof-of-Deep Learning que consiste em aproveitar a energia computacional dedicada ao desafio de mineração em uma *blockchain* e a reinvestir na execução de algoritmos de aprendizado profundo. Isso é alcançado por meio do estabelecimento de que uma prova válida para um novo bloco só seria alcançada se um modelo de

aprendizado profundo for gerado. Tal abordagem sofre com a possibilidade de mineradores generalizarem o conceito buscando atalhos para a tarefa de aprendizagem. Ainda assim, este modelo está em fase conceitual e não há aplicação em ambiente real. Chenli et al [27] aponta ainda que até este conceito atingir a maturidade novas abordagens mais específicas precisam ser propostas na literatura. Isso está em linha com o que é apresentado no Capítulo 6, onde a HS é proposta com base no conceito de Modelo de Gestão Inteligente (MGI), que nada mais é do que um protocolo concreto de Proof-of-Deep Learning.

Mais além, TLRDs *currenless* baseadas em redes de reputação, assim como a HS, via de regra estão associadas a redes autenticadas, com usuários não anônimos e transações verificadas [186, 59].

7.1 Ameaças à Validade

Ao longo da presente Tese, vários estudos foram realizados, todos eles com ameças a validade já mapeadas. O Capítulo 4 utilizou modelos de IA proprietários para validar seus resultados, isto por si só já coloca em risco seus resultados. Já as revisões da literatura apresentadas nos Capítulos 2 e 5 foram realizadas há aproximadamente três e um ano atrás, e neste período novas soluções podem ter surgido. O estudo comparativo apresentado no Capítulo 5 utiliza um modelo simulado do comportamento humano e dados históricos do OpenBazzar. A ausência de dados reais coletados e analisados em tempo real também representa uma ameaça à validade.

Para além do exposto até aqui, um estudo aprofundado da viabilidade técnica de uma implementação da HS em ambiente real foge ao escopo desta Tese. Contudo, ainda que elementos como o versionamento do MGI em uma TLRD, por exemplo, em ambiente real não seja viável, poderia ser viável no futuro. Podemos aqui fazer um paralelo com os algoritmos e aprendizagem profunda tão difundidos hoje em dia, mas que foram desenvolvidos ainda na década de noventa e início dos anos 2000 com o método Cresceptron [272], as Redes Neurais Recorrentes [119], algoritmos de pré treinamento [118] e redes convolucionais [148], antes da explosão do Big Data e da popularização das GPUs de alto desempenho, que difundiram sua aplicação.

Versionar múltiplos modelos já treinados de gestão de transações (mgi's) tem um custo

computacional que não foi avaliado nesta Tese. Contudo, existem TLTDs atualmente que configuram candidatas a viabilizar uma aplicação real da HS, a exemplo do já mencionado Hash Graph [24], que é baseado em múltiplas cadeias, o que torna o desempenho da TLRD mais escalável.

7.2 Iniciativas Futuras

O modelo de simulação apresentado na presente Tese considera que todos os jogadores tenham acesso uniforme a todas as estratégias disponíveis. Perfis distintos para cada jogador que permitam emular com mais realismo a heterogeneidade de uma sociedade real poderia trazer resultados mais próximos da realidade. Mais além, outros estudos semelhantes àquele apresentado no Capítulo 4 poderiam elucidar as expectativas do usuário quanto a utilidade e usabilidade de ferramentas de mediação descentralizadas. Ainda tratando da aceitabilidade por parte do usuário e da viabilidade das soluções analisadas nesta Tese, uma análise de custo computacional e até financeiro poderia ser útil como critério de escolha entre as soluções avaliadas.

A Hash Society (HS), por abstrair o comportamento de usuários e contratos, pode ser usada para desenvolver Contratos Inteligentes (CIs) mais dinâmicos, ajustando cláusulas automaticamente com base em regras predefinidas e aprendizado contínuo. Em vez de contratos rígidos, a HS pode permitir que eles sejam flexíveis, ajustando cláusulas conforme condições externas, como mudanças de leis ou variações cambiais. Isso reduziria disputas contratuais e facilitaria renegociações automáticas.

Organizações descentralizadas (DAOs) podem utilizar a HS para gerenciar contratos automaticamente, eliminando intermediários e tornando a execução mais eficiente. Com a evolução das regulamentações para CIs, a HS pode analisar e ajustar contratos para estarem sempre em conformidade com novas leis e normas. Isso pode reduzir riscos jurídicos e acelerar transações internacionais.

Mais além, com base nas análise da HS em ambiente simulado é possível prever que a precificação não linear promovida pela dinâmica da HS pode constituir um modelo mais humano de recompensa, uma vez que reduz a concentração de riqueza ao promover enriquecimento e empobrecimento em ritmos logarítmicos, e não lineares. O modelo de reputação

baseado em ciclos ainda é capaz de promover a economia de grupos locais de produção em detrimento de iniciativas externas. Tal resultado constitui mais um subproduto desta pesquisa.

As possibilidades de uso da HS no futuro passam necessariamente por um esforço *open source* de desenvolvimento de uma aplicação real, a ser desempenhado a partir daqui. Para tanto, deve-se formar uma comunidade de desenvolvimento ativa e orientada com base no manifesto da HS [1].

O risco de ataques sibil em uma eventual implementação em ambiente real da HS existe, embora a análise de risco de conluio realizada no Capítulo 6 mostra que a rede é capaz de suportar o conluio, que é uma forma de ataque sibil. Entretanto, um estudo focado mais em resultados numéricos de conluio e ataques sibil é uma iniciativa futura necessária.

7.3 Conclusões Finais

Esta Tese destaca o desafio contínuo de estimular a honestidade em transações não verificáveis do mundo real em mercados descentralizados, contornando o DCV. Notadamente, os resultados obtidos por simulação indicam que um modelo de estímulo à honestidade baseado em mediação descentralizada e redes de reputação sem *feedback* (solução "A" na Tabela 5.4) é capaz de reduzir o risco em transações não verificadas o suficiente para viabilizar o mercado descentralizado como um todo. Isto, particularmente quando as taxas de honestidade estão na faixa de 30-60%, com 95% de confiança.

Surpreendentemente, quando as taxas de honestidade crescem além de 60%, pode ser tão eficaz, simples ou econômico (em termos computacionais) simplesmente aplicar uma Rede de Confiança (solução "I" na Tabela 5.4) – o que significa que até mesmo "agentes criminosos" tenderão a seguir a multidão (que é composta principalmente de agentes honestos) quando forçados por relações sociais. No entanto, à medida que as taxas de honestidade caem, a taxa de sucesso diminui, chegando a zero para taxas de honestidade iguais ou inferiores a 20%. Este resultado indicar que, em um cenário altamente desonesto, será melhor evitar fazer negócios, pois nenhuma solução até o momento parece fazer os agentes se com-

[1] Tal iniciativa já dá seus primeiros passos, mas é um esforço que está apenas no início: https://github.com/H-a-s-h-S-o-c-i-e-t-y

portarem honestamente.

Contudo, o Capítulo 6 apresenta uma solução denominada Hash Society que é capaz de estimular a honestidade com uma eficácia muito superior em praticamente todos os cenários honestidade da população. Entretanto, tal solução é baseada em um modelo de transações de operação única que pode não se adequar a qualquer configuração de mercado ou modelo de negócio.

Sendo assim, o conceito de nível aceitável de risco presente na questão de pesquisa principal: "Já existe na literatura uma solução para o Dilema dos Compradores e Vendedores em ambiente DAnV com um nível aceitável de risco?", mantém tal questão em aberto em alguns cenários. Caso a honestidade da população seja muito baixa, não há na literatura solução para o DCV em ambiente DAnV. Caso a honestidade da população seja moderada, existem contornos para o DCV em ambiente DAnV, conforme descrito nos Capítulos 5 e 6. A uma taxa de honestidade elevada, a solução para o DCVem ambiente DAnV é trivial, tal como descrito no Capítulo 5. Contudo, esta Tese apresenta a HS, um solução generalista para o DCV em ambiente DAnV dada qualquer tava de honestidade. Contudo, o modelo de transação baseada em uma única operação, utilizado na HS, possivelmente não se encaixa em todos os domínios de aplicação em que o modelo de transação convencional se encaixa.

Bibliografia

[1] Joe Abou Jaoude and Raafat George Saade. Blockchain applications–usage in different domains. *Ieee Access*, 7:45360–45381, 2019.

[2] Dilip Abreu, David Pearce, and Ennio Stacchetti. Toward a theory of discounted repeated games with imperfect monitoring. *Econometrica: Journal of the Econometric Society*, pages 1041–1063, 1990.

[3] W Richards Adrion, Martha A Branstad, and John C Cherniavsky. Validation, verification, and testing of computer software. *ACM Computing Surveys (CSUR)*, 14(2):159–192, 1982.

[4] Hirotugu Akaike. A new look at the statistical model identification. *IEEE transactions on automatic control*, 19(6):716–723, 1974.

[5] Hamda Al-Breiki, Muhammad Habib Ur Rehman, Khaled Salah, and Davor Svetinovic. Trustworthy blockchain oracles: Review, comparison, and open research challenges. *IEEE Access*, 8:85675–85685, 2020.

[6] Ons Al-Shamaileh and Alistair Sutcliffe. Why people choose apps: An evaluation of the ecology and user experience of mobile applications. *International Journal of Human-Computer Studies*, 170:102965, 2023.

[7] Moutaz Alazab, Salah Alhyari, Albara Awajan, and Ayman Bahjat Abdallah. Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, 24(1):83–101, 2021.

[8] Stefania Albanesi and Christopher Sleet. Dynamic optimal taxation with private information. *The Review of Economic Studies*, 73(1):1–30, 2006.

[9] Maher Alharby and Aad Van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*, 2017.

[10] Scott T Allison, James K Beggan, and Elizabeth H Midgley. The quest for"similar instances"and"simultaneous possibilities": Metaphors in social dilemma research. *Journal of Personality and Social Psychology*, 71(3):479, 1996.

[11] Abdulaziz Alshayban, Iftekhar Ahmed, and Sam Malek. Accessibility issues in android apps: state of affairs, sentiments, and ways forward. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering*, pages 1323–1334, 2020.

[12] Riham AlTawy, Muhammad ElSheikh, Amr M Youssef, and Guang Gong. Lelantos: A blockchain-based anonymous physical delivery system. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 15–1509. IEEE, 2017.

[13] Fernando Alvarez and Urban J Jermann. Quantitative asset pricing implications of endogenous solvency constraints. *The Review of Financial Studies*, 14(4):1117–1151, 2001.

[14] Hendrik Amler, Lisa Eckey, Sebastian Faust, Marcel Kaiser, Philipp Sandner, and Benjamin Schlosser. Defi-ning defi: Challenges & pathway. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 181–184. IEEE, 2021.

[15] Elizabeth Anderson. *Value in ethics and economics*. Harvard University Press, 1995.

[16] David Andolfatto. Blockchain: What it is, what it does, and why you probably don't need one. *Review*, 100:87–95, 01 2018.

[17] Claudia Antal, Tudor Cioara, Ionut Anghel, Marcel Antal, and Ioan Salomie. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet*, 13(3):62, 2021.

[18] A.M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. Stanford University Press, 2021.

[19] James E Arps and Nicolas Christin. Open market or ghost town? the curious case of openbazaar. In *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*, pages 561–577. Springer, 2020.

[20] Aditya Asgaonkar and Bhaskar Krishnamachari. Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 262–267. IEEE, 2019.

[21] Jake Astill, Rozita A. Dara, Malcolm Campbell, Jeffrey M. Farber, Evan D.G. Fraser, Shayan Sharif, and Rickey Y. Yada. Transparency in food supply chains: A review of enabling technology solutions. *Trends in Food Science & Technology*, 91:240–247, 2019.

[22] Andrew Atkeson and Robert E Lucas Jr. On efficient distribution with private information. *The Review of Economic Studies*, 59(3):427–453, 1992.

[23] David Baehrens, Timon Schroeter, Stefan Harmeling, Motoaki Kawanabe, Katja Hansen, and Klaus-Robert Müller. How to explain individual classification decisions. *The Journal of Machine Learning Research*, 11:1803–1831, 2010.

[24] Leemon Baird. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. *Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep*, 34:9–11, 2016.

[25] M. Barry. Brief history of the internet, 1997.

[26] Kay Behnke and M.F.W.H.A. Janssen. Boundary conditions for traceability in food supply chains using blockchain technology. *International Journal of Information Management*, 52:101969, 2020.

[27] Jagger S Bellagarda and Adnan M Abu-Mahfouz. An updated survey on the convergence of distributed ledger technology and artificial intelligence: Current state, major challenges and future direction. *IEEE Access*, 10:50774–50793, 2022.

[28] Marianna Belotti, Stefano Moretti, Maria Potop-Butucaru, and Stefano Secci. Game theoretical analysis of cross-chain swaps. In *40th International Conference on Distributed Computing Systems (ICDCS)*, pages 485–495. IEEE, 2020.

[29] Aleksander Berentsen and Fabian Schär. A short introduction to the world of cryptocurrencies. *Review*, 100:1–16, 01 2018.

[30] Chris Berg, Sinclair Davidson, and Jason Potts. Capitalism after satoshi: Blockchains, dehierarchicalisation, innovation policy, and the regulatory state. *Journal of Entrepreneurship and Public Policy*, 9(2):152–164, 2020.

[31] Bhawna, Priya Gupta, Pratibha Rai, and Ajay Chauhan. Blockchain application in consumer services: A review and future research agenda. *International Journal of Consumer Studies*, 2023.

[32] Baidyanath Biswas and Rohit Gupta. Analysis of barriers to implement blockchain in industry and service sectors. *Computers & Industrial Engineering*, 136:225–241, 2019.

[33] Jörn H Block and Christian Fisch. Eight tips and questions for your bibliographic study in business and management research, 2020.

[34] Claudio A Bonilla, José M Merigó, and Carolina Torres-Abad. Economics in latin america: a bibliometric analysis. *Scientometrics*, 105:1239–1252, 2015.

[35] Achilleas Boukis. Exploring the implications of blockchain technology for brand–consumer relationships: a future research agenda. *Journal of Product & Brand Management*, 29(3):307–320, 2020.

[36] Lorenz Breidenbach, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, Farinaz Koushanfar, Andrew Miller, Brendan Magauran, Daniel Moroz, et al. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs*, 2021.

[37] Tobias Broer, Marek Kapička, and Paul Klein. Consumption risk sharing with private information and limited enforcement. *Review of Economic Dynamics*, 23:170–190, 2017.

[38] Garrett W Brown, Iain McLean, and Alistair McMillan. collective action problem, 2018.

[39] Vitalik Buterin. Schellingcoin: A minimal-trust universal data feed. *Ethereum blog*, 2014.

[40] Vitalik Buterin et al. Ethereum white paper. *GitHub repository*, 1:22–23, 2013.

[41] Courtni Byun, Piper Vasicek, and Kevin Seppi. Dispensing with humans in human-computer interaction research. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–26, 2023.

[42] Germano Caronni. Walking the web of trust. In *Proceedings IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000)*, pages 153–158. IEEE, 2000.

[43] Arthur Carvalho, Chaitanya Sambhara, and Patrick Young. What the history of linux says about the future of cryptocurrencies. *Communications of the Association for Information Systems*, 46(1):2, 2020.

[44] Fran Casino, Thomas K Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, 36:55–81, 2019.

[45] Christian Catalini and Joshua S Gans. Some simple economics of the blockchain. *Communications of the ACM*, 63(7):80–90, 2020.

[46] Victor Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, and Mitra Arami. How blockchain can impact financial services–the overview, challenges and recommendations from expert interviewees. *Technological forecasting and social change*, 158:120166, 2020.

[47] Victor Chang, Yuanyuan Wang, and Gary Wills. Research investigations on the use or non-use of hearing aids in the smart cities. *Technological Forecasting and Social Change*, 153:119231, 2020.

[48] James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon. Project jasper: Are distributed wholesale payment systems feasible yet. *Financial System*, 59:59, 2017.

[49] Vaibhav Chaudhary, Prashant Kumar, and Pushpendra Singh. Moving beyond blockchain: Hashgraph. In *Proceedings of the 9th International Symposium on Hydrogen Energy, Renewable Energy and Materials: HEREM23, October 13–14, 2023, Bangkok, Thailand*, volume 399, page 53. Springer Nature, 2024.

[50] Jiuhai Chen, Lichang Chen, Heng Huang, and Tianyi Zhou. When do you need chain-of-thought prompting for chatgpt? *arXiv preprint arXiv:2304.03262*, 2023.

[51] Yan Chen. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business horizons*, 61(4):567–575, 2018.

[52] Jonathan Chiu and Thorsten V Koeppl. The economics of cryptocurrencies–bitcoin and beyond. *Available at SSRN 3048124*, 2017.

[53] Jonathan Chiu and Tsz-Nga Wong. E-money: efficiency, stability and optimal policy. Technical report, Bank of Canada Working Paper, 2014.

[54] Tsan-Ming Choi. Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains. *Transportation Research Part E: Logistics and Transportation Review*, 128:17–29, 2019.

[55] Tsan-Ming Choi. Creating all-win by blockchain technology in supply chains: Impacts of agents' risk attitudes towards cryptocurrency. *Journal of the Operational Research Society*, 72(11):2580–2595, 2021.

[56] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE access*, 4:2292–2303, 2016.

[57] Adelina Ciurumelea, Andreas Schaufelbühl, Sebastiano Panichella, and Harald C Gall. Analyzing reviews and code of mobile apps for better release planning. In *2017 IEEE 24th international conference on software analysis, evolution and reengineering (SANER)*, pages 91–102. IEEE, 2017.

[58] Tiago Lucas Pereira Clementino and José Antão Beltrão Moura. Incentivizing honesty in online decentralized markets. In *International Conference on Computational Science and Its Applications*, pages 213–229. Springer, 2024.

[59] Marta Alexandra Guerra Magalhães Coelho. *Blockchain-based reputation models for e-commerce: a systematic literature review*. PhD thesis, 2023.

[60] Jacob Cohen. A coefficient of agreement for nominal scales. *Educational and psychological measurement*, 20(1):37–46, 1960.

[61] Harold L Cole and Narayana R Kocherlakota. Efficient allocations with hidden income and hidden storage. *The Review of Economic Studies*, 68(3):523–542, 2001.

[62] Nick Collier. Repast: An extensible framework for agent simulation. *The University of Chicago's social science research*, 36:2003, 2003.

[63] Nick Collier. Repast simphony reference manual, 2021.

[64] Lin William Cong and Zhiguo He. Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, 32(5):1754–1797, 04 2019.

[65] Karlene Cousins, Hemang Subramanian, and Pouyan Esmaeilzadeh. A value-sensitive design perspective of cryptocurrencies: a research agenda. *Communications of the association for information systems*, 45(1):27, 2019.

[66] Lars Creutz and Guido Dartmann. Cypher social contracts a novel protocol specification for cyber physical smart contracts. In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pages 440–447. IEEE, 2020.

[67] Sinclair Davidson, Primavera De Filippi, and Jason Potts. Disrupting governance: The new institutional economics of distributed ledger technology. *Available at SSRN 2811995*, 2016.

[68] R M Dawes. Social dilemmas. *Annual Review of Psychology*, 31(Volume 31, 1980):169–193, 1980.

[69] Richard Dawkins. *The selfish gene*. Oxford university press, 2016.

[70] Arne De Keyser, Sarah Köcher, Linda Alkire, Cédric Verbeeck, and Jay Kandampully. Frontline service technology infusion: conceptual archetypes and future research directions. *Journal of Service Management*, 30(1):156–183, 2019.

[71] Konstantinos Demestichas, Nikolaos Peppes, Theodoros Alexakis, and Evgenia Adamopoulou. Blockchain in agriculture traceability systems: A review. *Applied Sciences*, 10(12), 2020.

[72] Richard Dennis and Gareth Owen. Rep on the block: A next generation reputation system based on the blockchain. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 131–138. IEEE, 2015.

[73] Lea Diestelmeier. Changing power: Shifting the role of electricity consumers with blockchain technology–policy implications for eu electricity law. *Energy policy*, 128:189–196, 2019.

[74] Matthias Doepke and Robert M Townsend. Dynamic mechanism design with hidden income and hidden actions. *Journal of Economic Theory*, 126(1):235–285, 2006.

[75] John Domingue, Allan Third, and Manoharan Ramachandran. The fair trade framework for assessing decentralised data solutions. In *Companion Proceedings of The 2019 World Wide Web Conference*, pages 866–882, 2019.

[76] Paulo Sérgio Henrique Dos Santos, Alberto Dumont Alves Oliveira, Thais Bonjorni Nobre De Jesus, Wajdi Aljedaani, and Marcelo Medeiros Eler. Evolution may come with a price: analyzing user reviews to understand the impact of updates on mobile apps accessibility. In *Proceedings of the XXII Brazilian Symposium on Human Factors in Computing Systems*, pages 1–11, 2023.

[77] Ricardo Borges dos Santos, Nunzio Marco Torrisi, Erick Reyann Kasai Yamada, and Rodrigo Palucci Pantoni. Igr token-raw material and ingredient certification of recipe based foods using smart contracts. In *Informatics*, volume 6, page 11. MDPI, 2019.

[78] Nghia Duong-Trung, Xuan Son Ha, Tan Tai Phan, Phuong Nam Trieu, Quoc Nghiep Nguyen, Duy Pham, Thai Tam Huynh, and Hai Trieu Le. Multi-sessions mechanism for decentralized cash on delivery system. *Int. J. Adv. Comput. Sci. Appl*, 10(9), 2019.

[79] Abhishek Dwaraki, Srini Seetharaman, Sriram Natarajan, and Tilman Wolf. Gitflow: Flow revision management for software-defined networks. In *Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research*, pages 1–6, 2015.

[80] Vimal Dwivedi and Alex Norta. A legal-relationship establishment in smart contracts: Ontological semantics for programming-language development. In *International Conference on Advances in Computing and Data Sciences*, pages 660–676. Springer, 2021.

[81] Bradley Efron. Estimating the error rate of a prediction rule: improvement on cross-validation. *Journal of the American statistical association*, 78(382):316–331, 1983.

[82] Bradley Efron. How biased is the apparent error rate of a prediction rule? *Journal of the American statistical Association*, 81(394):461–470, 1986.

[83] Marcelo Medeiros Eler, Leandro Orlandin, and Alberto Dumont Alves Oliveira. Do android app users care about accessibility? an analysis of user reviews on the google play store. In *Proceedings of the 18th Brazilian symposium on human factors in computing systems*, pages 1–11, 2019.

[84] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE cloud computing*, 5(1):31–37, 2018.

[85] Ittay Eyal. The miner's dilemma. In *2015 IEEE symposium on security and privacy*, pages 89–103. IEEE, 2015.

[86] Giorgio Fagiolo, Alessio Moneta, and Paul Windrum. A critical guide to empirical validation of agent-based models in economics: Methodologies, procedures, and open problems. *Computational Economics*, 30:195–226, 2007.

[87] Zhi-Ping Fan, Xue-Yan Wu, and Bing-Bing Cao. Considering the traceability awareness of consumers: should the supply chain adopt the blockchain technology? *Annals of Operations Research*, pages 1–24, 2022.

[88] Kurt Fanning and David P Centers. Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, 27(5):53–57, 2016.

[89] Maryam Farhadi, Rahmah Ismail, and Masood Fooladi. Information and communication technology use and economic growth. *PloS one*, 7(11):e48903, 2012.

[90] Federal Trade Commission. As nationwide fraud losses top $10 billion in 2023, ftc steps up efforts to protect the public. `https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-prot` 2024. Accessed 11th April 2024.

[91] Michal Feldman, Nicole Immorlica, Brendan Lucier, Tim Roughgarden, and Vasilis Syrgkanis. The price of anarchy in large games. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 963–976, 2016.

[92] Michael J Fell, Alexandra Schneiders, and David Shipworth. Consumer demand for blockchain-enabled peer-to-peer electricity trading in the united kingdom: An online survey experiment. *Energies*, 12(20):3913, 2019.

[93] Huanhuan Feng, Xiang Wang, Yanqing Duan, Jian Zhang, and Xiaoshuan Zhang. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *Journal of Cleaner Production*, 260:121031, 2020.

[94] Raphael Féraud and Fabrice Clérot. A methodology to explain neural network classification. *Neural networks*, 15(2):237–246, 2002.

[95] Ana Fernandes and Christopher Phelan. A recursive formulation for repeated agency with history dependence. *Journal of Economic Theory*, 91(2):223–247, 2000.

[96] Catarina Ferreira da Silva and Sérgio Moro. Blockchain technology as an enabler of consumer trust: A text mining literature analysis. *Telematics and Informatics*, 60:101593, 2021.

[97] Joseph L Fleiss, Bruce Levin, Myunghee Cho Paik, et al. The measurement of interrater agreement. *Statistical methods for rates and proportions*, 2(212-236):22–23, 1981.

[98] Erhard Friedberg. Conflict of interest from the perspective of the sociology of organised action. *Conflict of Interest in Global, Public and Corporate Governance*, page 39, 2012.

[99] Ahmed G Gad, Diana T Mosa, Laith Abualigah, and Amr A Abohany. Emerging trends in blockchain technology and applications: A review and outlook. *Journal of King Saud University-Computer and Information Sciences*, 34(9):6719–6742, 2022.

[100] Paolo Gaiardelli, Giuditta Pezzotta, Alice Rondini, David Romero, Farnaz Jarrahi, Marco Bertoni, Stefan Wiesner, Thorsten Wuest, Tobias Larsson, Mohamed Zaki, et al. Product-service systems evolution in the era of industry 4.0. *Service Business*, 15:177–207, 2021.

[101] Juan F. Galvez, J.C. Mejuto, and J. Simal-Gandara. Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry*, 107:222–232, 2018.

[102] Andy Gardner. The strategic revolution. *Cell*, 166(6):1345–1348, 2016.

[103] Valentina Gatteschi, Fabrizio Lamberti, and Claudio Demartini. An overview of blockchain-based applications for consumer electronics. In *International Symposium on Consumer Technologies (ISCT)*, volume 23, pages 161–166. IEEE, 2019.

[104] Fariba Ghaffari, Emmanuel Bertin, Julien Hatin, and Noel Crespi. Authentication and access control based on distributed ledger technology: A survey. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 79–86. IEEE, 2020.

[105] Global e-commerce market. Global e-commerce market to reach $ 47.7 trillion by 2030, report. https://marketingreport.one/retail/global-e-commerce-market-to-reach-47.7-trillion-by-2030-report.html, 2024. Accessed 11th April 2024.

[106] F Grasso, G Talluri, A Giorgi, A Luchetta, L Paolucci, et al. Peer-to-peer energy exchanges model to optimize the integration of renewable energy sources: The e-cube project. *L'Energia Elettrica*, 96:0–0, 2019.

[107] Edward J Green. Lending and the smoothing of uninsurable income. *Contractual arrangements for intertemporal trade*, 1:3–25, 1987.

[108] Yi-Ming Guo, Zhen-Ling Huang, Ji Guo, Xing-Rong Guo, Hua Li, Meng-Yu Liu, Safa Ezzeddine, and Mpeoane Judith Nkeli. A bibliometric analysis and visualization of blockchain. *Future Generation Computer Systems*, 116:316–332, 2021.

[109] Muhammad Usman Gurmani, Tanzeela Sultana, Abdul Ghaffar, Muhammad Azeem, Zain Abubaker, Hassan Farooq, and Nadeem Javaid. Energy trading between prosumer and consumer in p2p network using blockchain. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 14th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2019) 14*, pages 875–886. Springer, 2020.

[110] Amulya Gurtu and Jestin Johny. Potential of blockchain technology in supply chain management: a literature review. *International Journal of Physical Distribution & Logistics Management*, 49(9):881–900, 2019.

[111] Xuan Son Ha, Hai Trieu Le, Nadia Metoui, and Nghia Duong-Trung. Dem-cod: Novel access-control-based cash on delivery mechanism for decentralized marketplace. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 71–78. IEEE, 2020.

[112] David Haig. The strategic gene. *Biology & Philosophy*, 27:461–479, 2012.

[113] W.D. Hamilton. The genetical evolution of social behaviour. i. *Journal of Theoretical Biology*, 7(1):1–16, 1964.

[114] Ridong Han, Tao Peng, Chaohao Yang, Benyou Wang, Lu Liu, and Xiang Wan. Is information extraction solved by chatgpt? an analysis of performance, evaluation criteria, robustness and errors. *arXiv preprint arXiv:2305.14450*, 2023.

[115] Tim Hanstad. Trust is the glue of a healthy society. here's how to bring it back, 2020.

[116] Friedrich August Hayek. The use of knowledge in society. In *Modern understandings of liberty and property*, pages 27–38. Routledge, 2013.

[117] Mr Dong He, Mr Karl F Habermeier, Mr Ross B Leckow, Mr Vikram Haksar, Ms Yasmin Almeida, Ms Mikari Kashima, Mr Nadim Kyriakos-Saad, Ms Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, et al. *Virtual currencies and beyond: initial considerations*. International Monetary Fund, 2016.

[118] Geoffrey E Hinton and Ruslan R Salakhutdinov. Reducing the dimensionality of data with neural networks. *science*, 313(5786):504–507, 2006.

[119] S Hochreiter. Long short-term memory. *Neural Computation MIT-Press*, 1997.

[120] Jianchao Hou, Che Wang, and Sai Luo. How to improve the competiveness of distributed energy resources in china with blockchain technology. *Technological Forecasting and Social Change*, 151:119744, 2020.

[121] Geraint Howells. Protecting consumer protection values in the fourth industrial revolution. *Journal of Consumer Policy*, 43(1):145–175, 2020.

[122] Jun-Ho Huh and Seong-Kyu Kim. The blockchain consensus algorithm for viable management of new and renewable energies. *Sustainability*, 11(11):3184, 2019.

[123] Claudia Iacob and Rachel Harrison. Retrieving and analyzing mobile apps feature requests from online reviews. In *2013 10th working conference on mining software repositories (MSR)*, pages 41–44. IEEE, 2013.

[124] Marco Iansiti, Karim R Lakhani, et al. The truth about blockchain. *Harvard business review*, 95(1):118–127, 2017.

[125] Kazuki Ikeda. qbitcoin: A peer-to-peer quantum cash system. In *Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 1*, pages 763–771. Springer, 2019.

[126] Perica Ilak, Ivan Rajšl, Lin Herenčić, Zlatko Zmijarević, and Slavko Krajcar. Decentralized electricity trading in the microgrid: Implementation of decentralized peer-to-peer concept for electricity trading (p2pcet). In *Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MEDPOWER 2018)*, pages 1–5. IET, 2018.

[127] Il Im, Seongtae Hong, and Myung Soo Kang. An international comparison of technology adoption: Testing the utaut model. *Information & management*, 48(1):1–8, 2011.

[128] Alex Isherwood, Matthew Koehler, and David Slater. Using evolutionary model discovery to develop robust policies. In *2023 Winter Simulation Conference (WSC)*, pages 130–137. IEEE, 2023.

[129] Ira Kalish, Michael Wolf, and Jonathan Holdowsky. The link between trust and economic prosperity, 2021.

[130] Alexander K Karajvanov. Blockchains, collateral and financial contracts. *Discussion Papers*, 2021.

[131] Andrej Karpathy, Justin Johnson, and Li Fei-Fei. Visualizing and understanding recurrent networks. *arXiv preprint arXiv:1506.02078*, 2015.

[132] Nadezhda Karuseva, Semen Livshits, Andrew Kotsubinski, Natalya Yudina, Olga Novikova, and Anastasiia Tabakova. The impact of innovative technologies on consumers in the power supply market. In *E3S web of conferences*, volume 140, page 04009. EDP Sciences, 2019.

[133] Patrick J Kehoe and Fabrizio Perri. International business cycles with endogenous incomplete markets. *Econometrica*, 70(3):907–928, 2002.

[134] James Kennedy. Swarm intelligence. In *Handbook of nature-inspired and innovative computing: integrating classical models with emerging technologies*, pages 187–219. Springer, 2006.

[135] Hourieh Khalajzadeh, Mojtaba Shahin, Humphrey O Obie, Pragya Agrawal, and John Grundy. Supporting developers in addressing human-centric issues in mobile apps. *IEEE Transactions on Software Engineering*, 49(4):2149–2168, 2022.

[136] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, pages 365–382, 2016.

[137] Urvashi Kishnani, Naheem Noah, Sanchari Das, and Rinku Dewri. Assessing security, privacy, user interaction, and accessibility features in popular e-payment applications. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 143–157, 2023.

[138] Barbara Kitchenham. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004):1–26, 2004.

[139] Trevor I Kiviat. Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke LJ*, 65:569, 2015.

[140] Narayana R Kocherlakota. Implications of efficient risk sharing without commitment. *The Review of Economic Studies*, 63(4):595–609, 1996.

[141] Narayana R Kocherlakota. Money is memory. *Journal of economic theory*, 81(2):232–251, 1998.

[142] Thorsten V Koeppl and Jeremy Kronick. Blockchain technology–what's in store for canada's economy and financial markets? *CD Howe Institute Commentary*, 468, 2017.

[143] Young In Koh, Sung H Han, and Junseong Park. A systematic process for generating new blockchain-service business model ideas. *Service Business*, 16(1):187–209, 2022.

[144] Shirli Kopelman. The effect of culture and power on cooperation in commons dilemmas: Implications for global resource management. *Organizational Behavior and Human Decision Processes*, 108(1):153–163, 2009.

[145] Philipp Korom. A bibliometric visualization of the economics and sociology of wealth inequality: a world apart? *Scientometrics*, 118:849–868, 2019.

[146] Elias Koutsoupias and Christos Papadimitriou. Worst-case equilibria. In Christoph Meinel and Sophie Tison, editors, *STACS 99*, pages 404–413, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[147] Elias Koutsoupias and Christos Papadimitriou. Worst-case equilibria. *Computer Science Review*, 3(2):65–69, 2009.

[148] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, 25, 2012.

[149] Dirk Krueger. *Risk sharing in economies with incomplete markets*. PhD thesis, Citeseer, 1999.

[150] Nir Kshetri. 1 blockchain's roles in meeting key supply chain management objectives. *International Journal of information management*, 39:80–89, 2018.

[151] Satish Kumar, Sweta Tomar, and Deepak Verma. Women's financial planning for retirement: Systematic literature review and future research agenda. *International journal of bank marketing*, 37(1):120–141, 2019.

[152] Małgorzata Kutera et al. Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation*, 18(4):45–77, 2022.

[153] Florian Larcher. Governance possibilities of blockchain platforms. 2019.

[154] Aron Laszka, Scott Eisele, Abhishek Dubey, Gabor Karsai, and Karla Kvaternik. Transax: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids. In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 918–927, 2018.

[155] Hai Trieu Le, Ngoc Tien Thanh Le, Nguyen Ngoc Phien, Nghia Duong-Trung, Ha Xuan Son, and Thai Tam Huynh. Introducing multi shippers mechanism for decentralized cash on delivery system. *International Journal of Advanced Computer Science and Applications*, 10(6), 2019.

[156] Ngoc Tien Thanh Le, Quoc Nghiep Nguyen, Nguyen Ngoc Phien, Nghia Duong-Trung, T Tam Huynh, T Phuc Nguyen, and H Xuan Son. Assuring non-fraudulent transactions in cash on delivery by introducing double smart contracts. *Int. J. Adv. Comput. Sci. Appl*, 10(5):677–684, 2019.

[157] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.

[158] John O Ledyard et al. *Public goods: A survey of experimental research*. Division of the Humanities and Social Sciences, California Inst. of Technology, 1994.

[159] Sang M Lee and Silvana Trimi. Innovation for creating a smart future. *Journal of Innovation & Knowledge*, 3(1):1–8, 2018.

[160] Byung-Hak Leem and Seong-Won Eum. Using text mining to measure mobile banking service quality. *Industrial Management & Data Systems*, 121(5):993–1007, 2021.

[161] Benjamin Letham, Cynthia Rudin, Tyler H McCormick, and David Madigan. Interpretable classifiers using rules and bayesian analysis: Building a better stroke prediction model. 2015.

[162] Jiwei Li, Xinlei Chen, Eduard Hovy, and Dan Jurafsky. Visualizing and understanding neural models in nlp. *arXiv preprint arXiv:1506.01066*, 2015.

[163] E Ligon. Mutual insurance and limited commitment: theory and evidence in village economies. *Review of Economic Studies*, 69:115–139, 2002.

[164] Ethan Ligon, Jonathan P Thomas, and Tim Worrall. Mutual insurance, individual savings, and limited commitment. *Review of Economic Dynamics*, 3(2):216–246, 2000.

[165] Weng Marc Lim, Sheau-Fen Yap, and Marian Makkar. Home sharing in marketing and tourism at a tipping point: What do we know, how do we know, and where should we be heading? *Journal of business research*, 122:534–566, 2021.

[166] Xin Lin, Shu-Chen Chang, Tung-Hsiang Chou, Shih-Chih Chen, and Athapol Ruangkanjanases. Consumers' intention to adopt blockchain food traceability technology towards organic food products. *International Journal of Environmental Research and Public Health*, 18(3):912, 2021.

[167] Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu, and Liming Zhu. Blockchain based data integrity service framework for iot data. In *2017 IEEE International Conference on Web Services (ICWS)*, pages 468–475, 2017.

[168] Kang Liu, Xiaoyu Qiu, Wuhui Chen, Xu Chen, and Zibin Zheng. Optimal pricing mechanism for data market in blockchain-enhanced internet of things. *IEEE Internet of Things Journal*, 6(6):9748–9761, 2019.

[169] Fengji Luo, Zhao Yang Dong, Gaoqi Liang, Junichi Murata, and Zhao Xu. A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain. *IEEE Transactions on Power Systems*, 34(5):4097–4108, 2019.

[170] Lydia Saad. Scams: Relatively common and anxiety-inducing for americans. `https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx`, 2023. Accessed 11th April 2024.

[171] Tim K Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich, and Maria Palombini. 'fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine*, 17:1–17, 2019.

[172] Spyros Makridakis and Klitos Christodoulou. Blockchain: Current challenges and future prospects/applications. *Future Internet*, 11(12):258, 2019.

[173] Cohn L Mallows. More comments on cp. *Technometrics*, 37(4):362–372, 1995.

[174] Akaki Mamageishvili and Jan Christoph Schlegel. Optimal smart contracts with costly verification. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–8. IEEE, 2020.

[175] Muhammad Hasan Maqbool, Umar Farooq, Adib Mosharrof, AB Siddique, and Hassan Foroosh. Mobilerec: A large scale dataset for mobile apps recommendation. In *Proceedings of the 46th international ACM SIGIR conference on research and development in information retrieval*, pages 3007–3016, 2023.

[176] Robert Ernest Marks. Validating simulation models: a general framework and four applied examples. *Computational economics*, 30:265–290, 2007.

[177] Ilyas Masudin, Anggi Ramadhani, Dian Palupi Restuputri, and Ikhlasul Amallynda. The effect of traceability system and managerial initiative on indonesian food cold chain performance: A covid-19 pandemic perspective. *Global Journal of Flexible Systems Management*, 22(4):331–356, 2021.

[178] Roger Maull, Phil Godsiff, Catherine Mulligan, Alan Brown, and Beth Kewell. Distributed ledger technology: Applications and implications. *Strategic Change*, 26(5):481–489, 2017.

[179] Esther Mengelkamp, Johannes Gärttner, Kerstin Rock, Scott Kessler, Lawrence Orsini, and Christof Weinhardt. Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied Energy*, 210:870–880, 2018.

[180] David M Messick and Marilynn B Brewer. Solving social dilemmas: a review. 2005.

[181] Alexander Mikroyannidis. Blockchain applications in education: a case study in lifelong learning. 2020.

[182] Alexander Mikroyannidis. Blockchain applications in education: A case study in lifelong learning. In *The 12th International Conference on Mobile, Hybrid, and Online Learning (eLmL 2020)*, 2020.

[183] Alexander Mikroyannidis, John Domingue, Michelle Bachler, and Kevin Quick. Smart blockchain badges for data science education. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–5. IEEE, 2018.

[184] Alexander Mikroyannidis, Allan Third, Niaz Chowdhury, Michelle Bachler, and John Domingue. Supporting lifelong learning with smart blockchain badges. *International Journal On Advances in Intelligent Systems*, 13(3 & 4):163–176, 2020.

[185] Ishwar Mittal. Consumer awareness about different consumer protection legislations in india. *Journal of Distance Education and Management Research (ISSN: 2278-9251)*, 3, 2015.

[186] Khalid Mrabet, Faissal El Bouanani, and Hussain Ben-Azza. Generalized secure and dynamic decentralized reputation system with a dishonest majority. *IEEE Access*, 11:9368–9388, 2023.

[187] Marcel Müller, Jacek Aleksander Janczura, and Peter Ruppel. Decoco: blockchain-based decentralized compensation of digital content purchases. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 152–159. IEEE, 2020.

[188] Alex Murray, Scott Kuban, Matt Josefy, and Jon Anderson. Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives*, 35(4):622–641, 2021.

[189] Alex Murray, Scott Kuban, Matthew Josefy, and Jonathan Anderson. Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives*, (ja), 2019.

[190] Ajit Muzumdar, Chirag Modi, GM Madhu, and Chintamani Vyjayanthi. A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts. *Journal of Network and Computer Applications*, 183:103074, 2021.

[191] Satoshi Nakamoto. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[192] Saba Naseem, Toqeer Mahmood, Muhammad Asif, Junaid Rashid, Muhammad

Umair, and Mohsin Shah. Survey on sentiment analysis of user reviews. In *2021 international conference on innovative computing (ICIC)*, pages 1–6. IEEE, 2021.

[193] John F Nash Jr. Equilibrium points in n-person games. *Proceedings of the national academy of sciences*, 36(1):48–49, 1950.

[194] Tyron Ncube, Nomusa Dlodlo, and Alfredo Terzoli. Private blockchain networks: A solution for data privacy. In *2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pages 1–8. IEEE, 2020.

[195] Duc-Duy Nguyen and Muhammad Intizar Ali. Enabling on-demand decentralized iot collectability marketplace using blockchain and crowdsensing. In *2019 Global IoT Summit (GIoTS)*, pages 1–6, 2019.

[196] Stefano Nocerino. A review on the potential impact of blockchain to the accounting profession, 2021.

[197] Tier Nolan. Re: Alt chains and atomic transfers., 2013. Last accessed 20 July 2023.

[198] Michael J North, Nicholson T Collier, Jonathan Ozik, Eric R Tatara, Charles M Macal, Mark Bragen, and Pam Sydelko. Complex adaptive systems modeling with repast simphony. *Complex adaptive systems modeling*, 1(1):1–26, 2013.

[199] Jørgen Svennevik Notland, Jakob Svennevik Notland, and Donn Morrison. The minimum hybrid contract (mhc) combining legal and blockchain smart contracts. In *Proceedings of the Evaluation and Assessment in Software Engineering*, pages 390–397. 2020.

[200] Jamilya Nurgazina, Udsanee Pakdeetrakulwong, Thomas Moser, and Gerald Reiner. Distributed ledger technology applications in food supply chains: A review of challenges and future research directions. *Sustainability*, 13(8):4206, 2021.

[201] Patrick Ocheja, Brendan Flanagan, Hiroshi Ueda, and Hiroaki Ogata. Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(1):1–19, 2019.

[202] Yun Kyung Oh and Jung-Min Kim. What improves customer satisfaction in mobile banking apps? an application of text mining analysis. *Asia Marketing Journal*, 23(4):3, 2022.

[203] Committee on Payments and Market Infrastructures. Distributed ledger technology in payment, clearing and settlement - an analytical framework, February 2017.

[204] Can Özturan. Barter machine: Defier of the money. *Available at SSRN 3508636*, 2019.

[205] Thomas R. Palfrey and Howard Rosenthal. Private incentives in social dilemmas: The effects of incomplete information and altruism. *Journal of Public Economics*, 35(3):309–332, 1988.

[206] Sakshi Sanjay Pande, Shrushti Mandolikar, and Sanjay Shitole. Bitland-a decentralized commercial real estate platform. In *2022 IEEE Bombay Section Signature Conference (IBSSC)*, pages 1–6. IEEE, 2022.

[207] Christos Papadimitriou. Algorithms, games, and the internet. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, STOC '01, page 749–753, New York, NY, USA, 2001. Association for Computing Machinery.

[208] Joon Park, Ruzanna Chitchyan, Anastasia Angelopoulou, and Jordan Murkin. A block-free distributed ledger for p2p energy trading: Case with iota? In *International Conference on Advanced Information Systems Engineering*, pages 111–125. Springer, 2019.

[209] Aarti Patki and Vinod Sople. Indian banking sector: Blockchain implementation, challenges and way forward. *Journal of Banking and Financial Technology*, 4(1):65–73, 2020.

[210] Justin Paul and Alex Rialp Criado. The art of writing literature review: What do we know and what do we need to know? *International business review*, 29(4):101717, 2020.

[211] Justin Paul, Weng Marc Lim, Aron O'Cass, Andy Wei Hao, and Stefano Bresciani. Scientific procedures and rationales for systematic literature reviews (spar-4-slr). *International Journal of Consumer Studies*, 45(4):O1–O16, 2021.

[212] Justin Paul, Altaf Merchant, Yogesh K Dwivedi, and Gregory Rose. Writing an impactful review article: what do we know and what do we need to know? *Journal of Business Research*, 133:337–340, 2021.

[213] Sebastian Peyrott. *An Introduction to Ethereum and Smart Contracts: a Programmable Blockchain*. Auth0 bu Okta, 2017.

[214] Christopher Phelan. Repeated moral hazard and one-sided commitment. *Journal of Economic Theory*, 66(2):488–506, 1995.

[215] Christopher Phelan. On the long run implications of repeated moral hazard. *Journal of Economic Theory*, 79(2):174–191, 1998.

[216] Joe Pinsker. Finland, home of the $103,000 speeding ticket, 2015.

[217] Dany Pratmanto, Rousyati Rousyati, Fanny Fatma Wati, Andrian Eko Widodo, Suleman Suleman, and Ragil Wijianto. App review sentiment analysis shopee application in google play store using naive bayes algorithm. In *Journal of Physics: Conference Series*, volume 1641, page 012043. IOP Publishing, 2020.

[218] Nirmalee Raddatz, Joshua Coyne, Philip Menard, and Robert E Crossler. Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications. *European Journal of Information Systems*, 32(2):287–314, 2023.

[219] Rahul Radhakrishnan, Gowri Sankar Ramachandran, and Bhaskar Krishnamachari. Sdpp: Streaming data payment protocol for data economy. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 17–18. IEEE, 2019.

[220] Anatol Rapoport and Albert M Chammah. *Prisoner's dilemma: A study in conflict and cooperation*, volume 165. University of Michigan press, 1965.

[221] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. "why should i trust you?"explaining the predictions of any classifier. In *Proceedings of the 22nd ACM*

SIGKDD international conference on knowledge discovery and data mining, pages 1135–1144, 2016.

[222] Marko Robnik-Šikonja and Igor Kononenko. Explaining classifications for individual instances. *IEEE Transactions on Knowledge and Data Engineering*, 20(5):589–600, 2008.

[223] Marko Robnik-Šikonja, Aristidis Likas, Constantinos Constantinopoulos, Igor Kononenko, and Erik Štrumbelj. Efficiently explaining decisions of probabilistic rbf classification networks. In *Adaptive and Natural Computing Algorithms: 10th International Conference, ICANNGA 2011, Ljubljana, Slovenia, April 14-16, 2011, Proceedings, Part I 10*, pages 169–179. Springer, 2011.

[224] Vinicius Facco Rodrigues, Lucas Micol Policarpo, Diórgenes Eugênio da Silveira, Rodrigo da Rosa Righi, Cristiano André da Costa, Jorge Luis Victória Barbosa, Rodolfo Stoffel Antunes, Rodrigo Scorsatto, and Tanuj Arcot. Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications*, 56:101207, 2022.

[225] Matti Rossi, Christoph Mueller-Bloch, Jason Bennett Thatcher, and Roman Beck. Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems*, 20(9):14, 2019.

[226] Cynthia Rudin, Benjamin Letham, and David B Madigan. Learning theory analysis for association rules and sequential event prediction. 2013.

[227] Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald, and Andrew Le Gear. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, 58(4):102584, 2021.

[228] K Salah, A Alfalasi, and M Alfalasi. A blockchain-based system for online consumer reviews. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 853–858. IEEE, 2019.

[229] Mayra Samaniego, Uurtsaikh Jamsrandorj, and Ralph Deters. Blockchain as a service for iot. In *2016 IEEE international conference on internet of things (iThings) and*

IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), pages 433–436. IEEE, 2016.

[230] Todd Sandler. Collective action: fifty years later. *Public Choice*, 164:195–216, 2015.

[231] Mara Taynar Santiago and Anna Beatriz Marques. Are user reviews useful for identifying accessibility issues that autistic users face? an exploratory study. In *Proceedings of the 21st Brazilian Symposium on Human Factors in Computing Systems*, pages 1–11, 2022.

[232] Joseph Sarkis Sara Saberi, Mahtab Kouhizadeh and Lejia Shen. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7):2117–2135, 2019.

[233] Manuel Schlegel, Liudmila Zavolokina, and Gerhard Schwabe. Blockchain technologies from the consumers' perspective: What is there and why should who care? In *Hawaii International Conference on System Sciences*, volume 51, 2018.

[234] Andrew Schotter. *The Economic Theory of Social Institutions*. Number 9780521067133 in Cambridge Books. Cambridge University Press, November 2008.

[235] Nikolaj Ignatieff Schwartzbach. Payment schemes from limited information with applications in distributed computing. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 129–149, 2022.

[236] Alpen Sheth and Hemang Subramanian. Blockchain and contract theory: modeling smart contracts using insurance markets. *Managerial Finance*, 46(6):803–814, 2020.

[237] Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. Deep inside convolutional networks: Visualising image classification models and saliency maps. *arXiv preprint arXiv:1312.6034*, 2013.

[238] Ha Xuan Son, Minh Hoang Nguyen, Nguyen Ngoc Phien, Hai Trieu Le, Quoc Nghiep Nguyen, Phu Thinh Tru, and Phuc Nguyen. Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger. *International Journal of Advanced Computer Science and Applications*, 10(4), 2019.

[239] Hongyu Song, Nafei Zhu, Ruixin Xue, Jingsha He, Kun Zhang, and Jianyu Wang. Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information Processing & Management*, 58(3):102507, 2021.

[240] Hongyu Song, Nafei Zhu, Ruixin Xue, Jingsha He, Kun Zhang, and Jianyu Wang. Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information Processing & Management*, 58(3):102507, 2021.

[241] Stephen E Spear and Sanjay Srivastava. On repeated moral hazard with discounting. *The Review of Economic Studies*, 54(4):599–617, 1987.

[242] Mervyn Stone. An asymptotic equivalence of choice of model by cross-validation and akaike's criterion. *Journal of the Royal Statistical Society: Series B (Methodological)*, 39(1):44–47, 1977.

[243] Hendrik Strobelt, Sebastian Gehrmann, Hanspeter Pfister, and Alexander M Rush. Lstmvis: A tool for visual analysis of hidden state dynamics in recurrent neural networks. *IEEE transactions on visualization and computer graphics*, 24(1):667–676, 2017.

[244] Nick Szabo. Formalizing and securing relationships on public networks. *First monday*, 1997.

[245] Nick Szabo. The idea of smart contracts. *Nick Szabo's papers and concise tutorials*, 6(1):199, 1997.

[246] Arwut Takkabutra, Charnon Chupong, and Boonyang Plangklang. Peer-to-peer energy trading market: A review on current trends, challenges and opportunities for thailand. In *2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 1076–1079. IEEE, 2021.

[247] Ali Tarhini, Nalin Asanka Gamagedara Arachchilage, Muhammad Sharif Abbasi, et al. A critical review of theories and models of technology adoption and accep-

tance in information system research. *International Journal of Technology Diffusion (IJTD)*, 6(4):58–77, 2015.

[248] Paolo Tasca, Thayabaran Thanabalasingham, and Claudio J Tessone. Ontology of blockchain technologies. principles of identification and classification. *SSRN Electronic Journal*, 10, 2017.

[249] Michael Taylor. Anarchy and cooperation. *Political Theory*, 5(2), 1977.

[250] Vincent F Taylor and Ivan Martinovic. To update or not to update: Insights from a two-year study of android app evolution. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 45–57, 2017.

[251] Jonathan Thomas and Tim Worrall. Self-enforcing wage contracts. *The Review of Economic Studies*, 55(4):541–554, 1988.

[252] Jonathan Thomas and Tim Worrall. Foreign direct investment and the risk of expropriation. *The review of economic studies*, 61(1):81–108, 1994.

[253] Huirong Tian, Shihong Zou, Wendong Wang, and Shiduan Cheng. A group based reputation system for p2p networks. In *International Conference on Autonomic and Trusted Computing*, pages 342–351. Springer, 2006.

[254] Edvard Tijan, Saša Aksentijević, Katarina Ivanić, and Mladen Jardas. Blockchain technology implementation in logistics. *Sustainability*, 11(4):1185, 2019.

[255] Robert M Townsend. Distributed ledgers: Innovation and regulation in financial infrastructure and payment systems. *URL: http://www. robertmtownsend. net/sites/default/files/files/papers/working_papers/Dis tributed% 20Ledgers-first% 20circulation-041819. pdf*, 2019.

[256] Philip Treleaven, Richard Gendal Brown, and Danny Yang. Blockchain technology in finance. *Computer*, 50(9):14–17, 2017.

[257] Itay Tsabary, Alex Manuskin, and Ittay Eyal. Ledgerhedger: Gas reservation for smart-contract security. *Cryptology ePrint Archive*, 2022.

[258] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. Mad-htlc: because htlc is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1230–1248. IEEE, 2021.

[259] Wei-Tek Tsai, Robert Blower, Yan Zhu, and Lian Yu. A system view of financial blockchains. In *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 450–457. IEEE, 2016.

[260] F-Y Tzeng and K-L Ma. *Opening the black box-data driven visualization of neural networks*. IEEE, 2005.

[261] Sarah Underwood. Blockchain beyond bitcoin. *Communications of the ACM*, 59(11):15–17, 2016.

[262] Alejandro Valencia-Arias, Juan David González-Ruiz, Lilian Verde Flores, Luis Vega-Mori, Paula Rodríguez-Correa, and Gustavo Sánchez Santos. Machine learning and blockchain: A bibliometric study on security and privacy. *Information*, 15(1):65, 2024.

[263] L Thomas van Binsbergen, Lu-Chi Liu, Robert van Doesburg, and Tom van Engers. eflint: a domain-specific language for executable norm specifications. In *Proceedings of the 19th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences*, pages 124–136, 2020.

[264] Mark Van Vugt and Paul AM Van Lange. Psychological adaptations for prosocial behavior: The altruism puzzle. *Evolution and social psychology*, pages 237–262, 2006.

[265] Gang Wang, Qin Wang, and Shiping Chen. Exploring blockchains interoperability: A systematic survey. *ACM Computing Surveys*, 2023.

[266] Jian Wang, Qianggang Wang, Niancheng Zhou, and Yuan Chi. A novel electricity transaction mode of microgrids based on blockchain and continuous double auction. *Energies*, 10(12), 2017.

[267] Tong Wang, Cynthia Rudin, Finale Doshi-Velez, Yimin Liu, Erica Klampfl, and Perry MacNeille. Or's of and's for interpretable classification, with application to context-aware recommender systems. *arXiv preprint arXiv:1504.07614*, 2015.

[268] J. Mark Weber, Shirli Kopelman, and David M. Messick. A conceptual review of decision making in social dilemmas: Applying a logic of appropriateness. *Personality and Social Psychology Review*, 8(3):281–307, 2004. PMID: 15454350.

[269] J. Mark Weber, Shirli Kopelman, and David M. Messick. A conceptual review of decision making in social dilemmas: Applying a logic of appropriateness. *Personality and Social Psychology Review*, 8(3):281–307, 2004. PMID: 15454350.

[270] Jason Wei, Yi Tay, Rishi Bommasani, Colin Raffel, Barret Zoph, Sebastian Borgeaud, Dani Yogatama, Maarten Bosma, Denny Zhou, Donald Metzler, et al. Emergent abilities of large language models. *arXiv preprint arXiv:2206.07682*, 2022.

[271] Xiang Wei, Xingyu Cui, Ning Cheng, Xiaobin Wang, Xin Zhang, Shen Huang, Pengjun Xie, Jinan Xu, Yufeng Chen, Meishan Zhang, et al. Zero-shot information extraction via chatting with chatgpt. *arXiv preprint arXiv:2302.10205*, 2023.

[272] Juyang Weng, Narendra Ahuja, and Thomas S Huang. Cresceptron: a self-organizing neural network which grows adaptively. In *[Proceedings 1992] IJCNN International Joint Conference on Neural Networks*, volume 1, pages 576–581. IEEE, 1992.

[273] Kevin Werbach. Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ*, 33:487, 2018.

[274] Thomas Werthenbach and Johan Pouwelse. Survey on social reputation mechanisms: Someone told me i can trust you. *arXiv preprint arXiv:2212.06436*, 2022.

[275] Martin Westerkamp, Friedhelm Victor, and Axel Küpper. Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1595–1602, 2018.

[276] Ronald J Williams and David Zipser. A learning algorithm for continually running fully recurrent neural networks. *Neural computation*, 1(2):270–280, 1989.

[277] Bello Musa Yakubu, Majid I Khan, Nadeem Javaid, and Abid Khan. Blockchain-based secure multi-resource trading model for smart marketplace. *Computing*, 103(3):379–400, 2021.

[278] Toshio Yamagishi. The structural goal/expectation theory of cooperation in social dilemmas. *Advances in Group Process*, 3:51–87, 1986.

[279] David Yermack. Corporate governance and blockchains. *Review of finance*, 21(1):7–31, 2017.

[280] David Yermack. Is bitcoin a real currency? an economic appraisal. In *Handbook of digital currency*, pages 29–40. Elsevier, 2024.

[281] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?—a systematic review. *PloS one*, 11(10):e0163477, 2016.

[282] Liudmila Zavolokina, Manuel Schlegel, and Gerhard Schwabe. How can we reduce information asymmetries and enhance trust in 'the market for lemons'? *Information Systems and e-Business Management*, 19(3):883–908, 2021.

[283] MD Zeiler. Visualizing and understanding convolutional networks. In *European conference on computer vision/arXiv*, volume 1311, 2014.

[284] Ge Zhang, Zhao Li, Jiaming Huang, Jia Wu, Chuan Zhou, Jian Yang, and Jianliang Gao. efraudcom: An e-commerce fraud detection system via competitive graph neural networks. *ACM Transactions on Information Systems (TOIS)*, 40(3):1–29, 2022.

[285] Peng Zhang, Jiaquan Wei, Yuhong Liu, and Hongwei Liu. Proxy re-encryption based fair trade protocol for digital goods transactions via smart contracts. *arXiv preprint arXiv:2306.01299*, 2023.

[286] Wayne Xin Zhao, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min, Beichen Zhang, Junjie Zhang, Zican Dong, et al. A survey of large language models. *arXiv preprint arXiv:2303.18223*, 2023.

[287] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. Blockchain-based personal health data sharing system using cloud storage. In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–6, 2018.

[288] Shuai Zhu, Malin Song, Ming Kim Lim, Jianlin Wang, and Jiajia Zhao. The development of energy blockchain and its implications for china's energy sector. *Resources Policy*, 66:101595, 2020.

[289] Dionysios Zindros. *Trust in decentralized anonymous marketplaces*. National Technical University of Athens, 2016.

Apêndice A

Provas

A.1 Equilíbrio de Nash na Estratégia Desonesta em Transações Bilaterais

Theorem 1. *Tomando o Dilema do Comprador e do Vendedor como o jogo G, conforme Definição 2, há um equilíbrio de Nash no ato de ser desonesto e não honrar a contrapartida na transação de compra e venda.*

Prova do Teorema 1. Além dos estados iniciais b_0 e desejáveis b_* apresentados na Definição 2, é incluído dois outros cenários, um de pior caso b_{-1} como sendo um estado pior que b_0 com base na função de interesse/utilidade λ, e outro b_{*+1} como sendo o estado melhr que o planejado. Compõe-se assim os estados possíveis $(b_{-1}, b_0, b_*, b_{*+1})$ para um dado agente, onde $\lambda_i(b_{-1}(i)) < \lambda_i(b_0(i)) < \lambda_i(b_*(i)) < \lambda_i(b_{*+1}(i)), \forall i \in Q$. Dada a função estratégia (operação) γ, considere:

$$\lambda(\gamma^t(b^i_{-1}, b^j_{*+1})) = \lambda(\gamma^{t+1}(b^i_*, b^j_*)) = 0, \forall_{i,j} \in Q \tag{A.1}$$

$$\lambda(b_{*+1}(i)) + \lambda(b_{-1}(j)) = \lambda(b_*(i)) + \lambda(b_*(j)) \tag{A.2}$$

A equação A.1 descreve a contrapartida do agente i, se o agente j iniciou a transação. No lado esquerdo, $\gamma^t(i, j)$ onde o agente i transferiu o conjunto de valores acordado para o agente j, e no lado direito $\gamma^{t+1}(i, j)$, onde o agente j responde transferindo a contrapartida para o agente i. Como é um jogo de soma zero, a troca de valores por si só não melhora a

função de interesse do estado de nenhuma das partes. Portanto, o saldo de ambos os lados da equação separadamente é zero.

Contudo, agir desonestamente significa não corresponder a confiança do comprador j, não enviando o produto e desequilibrando a balança. Assim, para provar a existência de um equilíbrio de interesses na estratégia desonesta, devemos demonstrar que a sentença $\lambda(b_{*+1}(i)) > \lambda_i(b_*(i))$ é verdadeira e faremos isto partindo da premissa que a Equação A.2 é verdade. Onde é descrito uma transição de estado:

$$\begin{aligned}
\lambda(b_{*+1}(i)) + \lambda(b_{-1}(j)) =& \lambda(b_*(i)) + \lambda(b_*(j)) \\
\lambda(b_{*+1}(i)) + \cancel{\lambda(b_{-1}(j))} >& \lambda(b_*(i)) + \cancel{\lambda(b_*(j))} \mid \lambda(b_{-1}(j)) < \lambda(b_*(j)) \\
\lambda(b_{*+1}(i)) >& \lambda_i(b_{-1}(i)), \forall_i
\end{aligned} \tag{A.3}$$

Na Inequação A.3 eliminamos os termos referentes a um dos agentes, representando a independência do resultado de um agente em relação ao outro. Note que assumimos duas premissas, a última que $\lambda(b_{-1}(j)) < \lambda(b_*(j))$, o que é verdade de acordo com a definição, e a primeira $\lambda(b_{*+1}(i)) + \lambda(b_{-1}(j)) = \lambda(b_*(i)) + \lambda(b_*(j))$, o que é verdade para um jogo de soma zero e corresponde a estratégia padrão γ segundo a Definição 2, onde o sucesso de um jogador é sempre proporcional ao fracasso de outro.

□

Apêndice B

Recursos Online

B.1 Capítulo: Análise da Mediação como Solução Centralizada para o DCV

Alguns elementos da pesquisa apresentada no Capítulo 4 estão disponíveis publicamente para fomentar a ciência aberta. Qualquer resposta fornecida pelo ChatGPT-4.0 que seja longa o suficiente para não caber neste documento está disponível publicamente em `https://github.com/tiago-clementino/mediation_analysis`. O código-fonte original da ferramenta ChatIE e suas personalizações necessárias estão disponíveis publicamente em `https://github.com/tiago-clementino/chatie_for_mediation_dataset`.

B.2 Capítulo: Incentivando a Honestidade em Mercados Descentralizados: Análise de Dados Históricos

Todos os resultados apresentados no Capítulo 5.3 foram obtidos a partir da implementação em linguagem R dos modelos propostos. Todo o código fonte está disponível abertamente em https://github.com/tiago-clementino/honesty_in_openbazaar

B.3 Capítulo: Incentivando a Honestidade em Mercados Descentralizados: Abordagem Baseada em Simulação

O código-fonte da linguagem Java do simulador apresentado no Capítulo 5.4 está disponível em `https://github.com/tiago-clementino/economy_simulation`. Da mesma forma, as análises de dados resultantes em R estão disponíveis em `https://github.com/tiago-clementino/economy_simulation_analytics`.

B.4 Capítulo: Hash Society

Semelhantemente, o código-fonte da linguagem Java do simulador apresentado no Capítulo 6, assim como as análises de dados resultantes em R estão disponíveis em `https://github.com/tiago-clementino/genetic-based-hs-simulation`.

Apêndice C

Tabelas Suplementares

Tabela C.1: Estimativa de sucesso populacional (%) para cada solução comparada, conforme ilustrado na Figura 5.7

	Taxas de Honestidade								
Soluções	10%	20%	30%	40%	50%	60%	70%	80%	90%
A	0.0	0.0	41.7	88.9	100.0	100.0	100.0	100.0	100.0
B	0.0	0.0	22.2	62.5	90.0	91.7	100.0	100.0	100.0
C	0.0	0.0	9.1	36.4	81.8	100.0	100.0	100.0	100.0
D	0.0	0.0	0.0	66.7	81.8	100.0	100.0	100.0	100.0
E	0.0	0.0	18.2	54.5	90.0	100.0	100.0	100.0	100.0
F	0.0	0.0	12.5	40.0	70.0	100.0	100.0	100.0	100.0
G	0.0	0.0	0.0	54.5	77.8	87.5	100.0	100.0	100.0
H	0.0	0.0	16.7	60.0	63.6	100.0	100.0	100.0	100.0
I	0.0	0.0	0.0	30.0	60.0	100.0	100.0	100.0	100.0

Tabela C.2: Tabela de Notação referente ao Capítulo 5.3

Símbolo	Descrição
t	Um passo no tempo T.
MIH	Modelo de Incentivo à Honestidade.
a, b, c, s	Jogadores.
A	Conjunto total de jogadores.
T	Transação.
ϕ	Confiança da rede em um dado jogador.
$s_t(b, a)$	Saldo histórico de transações entre b e a até o momento t.
P_t	Saldo total de transações entre toda a população ativa até t.
δ	Limite de confiança aceitável para realizar uma transação.
$\gamma_{a,b}(c)$	Função que define se c é confiável o suficiente para ser o árbitro da transação entre a e b.

Tabela C.3: Tabela de Notação

Símbolo	Descrição
K	Conjunto de agentes negociando
q	Um agente negociando
S	Conjunto de transações
s	Uma transação
G	Dilema do comprador e do vendedor como um jogo de forma extensiva
P	Conjunto de valores/produtos trocados
p	Um valor/produto
T	referências para todos os passos de tempo.
i, j	representações de agentes
k, l, n, t	representações de passos de tempo
MGI	representa o conjunto de MGIs disponíveis
mgi	representa uma MGI disponível
r	recurso da lista de recursos
d	demanda da lista de mandados
b	o estado de um determinado agente
γ	A estratégia (operação)
λ	A função de interesse
J	Uma solução de incentivo de honestidade descentralizada
ζ	Uma função de inferência de comportamento (um sistema de reputação, por exemplo)
η	Algum modelo de transação garantidor como arbitragem descentralizada ou depósitos de garantia
α	Uma função de ação
M	O inventário do agente para cada uma das categorias de valor
ν	O objetivo de qualquer agente para cada categoria de valor
L	Os passos de vida em tempo de qualquer agente
C	Conjunto de classes de valor/produto
c	Uma classe de valor/produto
V	A validação do ABM de acordo com [176]

U	A saída do ABM
Z	A saída real do sistema OpenBazaar
R	$U \cap S$
m	Uma métrica de escala de razão definida de acordo com a viabilidade e funcionalidade
X	O evento de um determinado agente confiar em outro
h	A probabilidade de um determinado produto já repassado por um determinado agente chegar ao estoque de outro
χ	A honestidade real de um determinado agente
ψ	Uma função aleatória

Tabela C.4: Tabela de Notação referente ao Capítulo 6

Símbolo	Descrição
HS	Hash Society
MGI	representa o conjunto de MGIs disponíveis
mgi	representa uma MGI disponível
r	recurso da lista de recursos
d	demanda da lista de mandados
V	O vetor de probabilidades de mudança de estados dois estados de uma cadeia.
U	Utilidade de uma transação.
MK^r	Considere a trajetória de um recurso durável r
n	Iteração/estado em uma cadeia de markov.
N	Total de estados de uma cadeia de markov.
E^r_{n+1}	A variável aleatória que representa o estado do recurso r na interação $n+1$.
e^r	Faz referência a algum estado de r.
R	Um recurso em uma lista de recursos.
Q	Conjunto de agentes negociando
q	Um agente negociando
P	Conjunto de valores/produtos trocados
p	Um valor/produto
T	referências para todos os passos de tempo.
S	Conjunto de transações
s	Uma transação
μ^s_{mgi}	Uma avaliação de uma transação s por uma mgi
η^t	Algum modelo de transação, onde η^{qt} retorna um conjunto bruto de operações $\{\gamma_0, ..., \gamma_n\}$ num determinado momento t, para um dado agente q.
γ	Uma operação.
c	Uma classe de valor/produto
b	O estado de um determinado agente.

C	Conjunto de classes de valor/produto
c	Uma classe de valor/produto
α	Uma função de ação
κ	Função validação de um mgi.
M	O inventário do agente para cada uma das categorias de valor
ν	O objetivo de qualquer agente para cada categoria de valor
L	Os passos de vida em tempo de qualquer agente
χ	A honestidade real de um determinado agente
η	Probabilidade de um dado agente se organizar em conluios.
θ	Limiar de reputação.
ρ	Taxa de adesão a ciclos de conluio.

Apêndice D

Manuais de Revisores

Instructions to External Reviewers

Smart Contracts and the Common User Needs: Systematic Review and Research Agenda

1. SELECTION PROCESS

The inclusion and exclusion criteria for the selection of works takes into account the objectives, research questions, and metadata that help to estimate the quality of the works. Tables 1 and 2 describe such inclusion and exclusion criteria of the methodology below which tries to: 1) verify the results reported in a work to be selected as being adequate to the research topic; and, 2) assess the coverage of the topic as being sufficient or not.

To be initially selected for review, an article must be a complete scientific work, be written in English, be in accordance with the topic under analysis, be relevant to the response of the research questions, deal with a public and decentralized technology and have been published for the first time after 2016.

a. Results Verification

The adequacy of the works selected for review must satisfy the inclusion and exclusion criteria (see Tables 1 and 2).

The exclusion criteria only admit acceptance or exclusion. The candidate article must meet all exclusion criteria in order to be evaluated. The inclusion criteria are numerically valued. Only articles that achieved a score greater than 0.5 in all inclusion criteria proceed to further evaluation (review). The exclusion criteria only admit acceptance or exclusion. The candidate article must meet all exclusion criteria in order to be evaluated.

Having been initially selected as relevant to this review, an article must then be classified based on the inclusion criteria of Table 1. Those rated below the cutoff score - 0.5 - on that fail any inclusion criteria should be discarded.

Table 1: Inclusion Criteria
IC1 - This criterion is applied to studies that aim to improve decentralized technologies in order to bring them closer to the common user and it produces an integer $\in \{0, 1, 2, 3, 4\}$ where zero excludes the study and any other value classifies it for further evaluation in addition to composing its inclusion score. A non-null integer here refers to one of the four areas of difficulty addressed in this review – 1- governance; 2- scale; 3- security; and, 4- information. **IC2** - The work must be complete and peer-reviewed (scientific articles published in conferences or periodicals). Here, the publication will be given the score equivalent to its H5 index (Google Scholar Metrics) divided by the highest score received by an article in this review. **IC3** - This criterion is applied to a study that was approved in the previous criteria and published between 2016 and 2022, and produces a real number ≥ 0 and ≥ 1 depending on its publication date (2016 corresponds to zero and 2022, to 1). **IC4** - The criterion is applicable to empirical, formal or theoretical studies. A theoretical-only study = 0. 3; an empirical one = 0. 6; formal 0.9; and, formal and empirical, 1.0.
Table 2: Exclusion Criteria
EC1 - Duplicated documents or published more than once by the same authors in different languages. **EC2** - Written in languages other than English. **EC3** - Tutorials, summary studies (studies of 4 pages or less)or any work that has not been submitted for peer review. **EC4** - Studies that: ● discuss applications only – i.e., that do not propose any evolution in technology or do not solve an ordinary – business to customer; ● are from other areas that do not correspond to decentralized systems;

- discuss technologies with restricted access (permissioness), or with centralized management. (This review focus on strictly decentralized solutions only;
- fit the above criteria, but do not go into details about the techniques, characteristics, etc.

EC5 - Secondary studies (literature reviews and meta-analyses) will not be included in the results, but may be cited for contributing (citing other relevant articles.

EC6 - Articles older than 2016.

EC7 - Articles not available for download or incomplete.

When evaluating the inclusion and exclusion criteria, reviewers were instructed to follow three steps:

I. Observe the metadata (publication date, total citations, quality of the publication vehicle, etc): from the metadata, some inclusion criteria and most of the exclusion criteria can already be verified;
II. Read the title: this is the first step in analyzing the criteria for adherence to the scope of this review;
III. Read the abstract: through the abstract, the process of evaluating the scope of the article that was started in the previous step is concluded.

If after following the steps above, there are doubts about the suitability (relevance) of the article under analysis, it is to be speed read under the following guidelines:

I. Read the introduction for more clarity on the topic of the article;
II. If doubts are about the paper's relevance but not about the topic is addresses, read the results and conclusion;
III. If doubts persist, read specific elements using a keyword search tool or, as a last resort, read the article in its entirety;
IV. If after all these steps there are still doubts, share them with the other reviewers.

b. Own Review

Although it is the role of the main reviewer to search for works adhering to the proposed theme, indication of authors or other works by the reviewers were observed.

2. QUALITY ASSESSMENT OF THE WORKS

The general quality evaluated during reading makes up the relevance of each selected work in relation to the topic under study and is used to rank the works in decreasing order of relevance.

The final step in the analysis, having already observed the inclusion and exclusion criteria, was the complete reading of the document. A total of 104 works were read in their entirety.

While reading an article in its entirety, the reviewer assesses its quality (relevance) according to the criteria in Table 3. These criteria were proposed by Marie Shaw in [SHAW, 2003] for gauging the quality of software engineering work. We adopt them here for they seem also to offer important insights into the quality of papers on the topic at hand. The reviewer attributes a value to each criterion as s/he reads the paper. The paper's final rank is the simple average of all attributed values.

Table 3: Quality Assessment Criteria

ID	Description	Adequacy
QC1	Is the study clear, without ambiguity, based on evidence and arguments?	• Please note the guidelines presented in topic 3.3 of Marie Shaw [SHAW, 2003]
QC2	Is there a clear statement of context, relevance, objectives and contribution of the research?	• At the reviewer's discretion
QC3	[Studies featuring experiments] Were they applied to real scenarios/data?	• Yes = 1 / No = 0
QC4	[Analytical Studies] Was the data analysis rigorous enough?	• No: discarded
QC5	Type of validation [SHAW, 2003].	• Formal proof: 0.5 • Analysis: 0.23 • Evaluation: 0.05 • Experiment: 0.24 • Real example: 0.2 • Toy example: 0.17 • Other: discarded
QC6	Does the study have concrete relevance for research or practice? [SHAW, 2003]	• Have a potentially popular app?: 0.08 • Does it promote public access to DAX?: 0.18 • Does it bring any structural improvement that promotes the decentralization paradigm with the public?: 0,25

		• Does it solve a problem for the majority of the population?: 0.5.
QC7	Is the article properly referenced?	• The most properly referenced receives a grade of 1; others receive a grade proportional to the difference in relation to the maximum grade

3. Referências

SHAW, Mary. Writing good software engineering research papers. In: **25th International Conference on Software Engineering, 2003. Proceedings.** IEEE, 2003. p. 726-736..

Instructions to External Reviewers

Smart Contracts and the Common User Needs: Systematic Review and Research Agenda

1. SELECTION PROCESS

The inclusion and exclusion criteria for the selection of works takes into account the objectives, research questions, and metadata that help to estimate the quality of the works. Tables 1 and 2 describe such inclusion and exclusion criteria of the methodology below which tries to: 1) verify the results reported in a work to be selected as being adequate to the research topic; and, 2) assess the coverage of the topic as being sufficient or not.

To be initially selected for review, an article must be a complete scientific work, be written in English, be in accordance with the topic under analysis, be relevant to the response of the research questions, deal with a public and decentralized technology and have been published for the first time after 2016.

a. Results Verification

The adequacy of the works selected for review must satisfy the inclusion and exclusion criteria (see Tables 1 and 2).

The exclusion criteria only admit acceptance or exclusion. The candidate article must meet all exclusion criteria in order to be evaluated. The inclusion criteria are numerically valued. Only articles that achieved a score greater than 0.5 in all inclusion criteria proceed to further evaluation (review). The exclusion criteria only admit acceptance or exclusion. The candidate article must meet all exclusion criteria in order to be evaluated.

Having been initially selected as relevant to this review, an article must then be classified based on the inclusion criteria of Table 1. Those rated below the cutoff score - 0.5 - on that fail any inclusion criteria should be discarded.

Table 1: Inclusion Criteria
IC1 - This criterion is applied to studies that aim to improve decentralized technologies in order to bring them closer to the common user and it produces an integer $\in \{0, 1, 2, 3, 4\}$ where zero excludes the study and any other value classifies it for further evaluation in addition to composing its inclusion score. A non-null integer here refers to one of the four areas of difficulty addressed in this review – 1- governance; 2- scale; 3- security; and, 4- information. **IC2** - The work must be complete and peer-reviewed (scientific articles published in conferences or periodicals). Here, the publication will be given the score equivalent to its H5 index (Google Scholar Metrics) divided by the highest score received by an article in this review. **IC3** - This criterion is applied to a study that was approved in the previous criteria and published between 2016 and 2022, and produces a real number ≥ 0 and ≥ 1 depending on its publication date (2016 corresponds to zero and 2022, to 1). **IC4** - The criterion is applicable to empirical, formal or theoretical studies. A theoretical-only study = 0. 3; an empirical one = 0. 6; formal 0.9; and, formal and empirical, 1.0.
Table 2: Exclusion Criteria
EC1 - Duplicated documents or published more than once by the same authors in different languages. **EC2** - Written in languages other than English. **EC3** - Tutorials, summary studies (studies of 4 pages or less)or any work that has not been submitted for peer review. **EC4** - Studies that: ● discuss applications only – i.e., that do not propose any evolution in technology or do not solve an ordinary – business to customer; ● are from other areas that do not correspond to decentralized systems;

- discuss technologies with restricted access (permissioness), or with centralized management. (This review focus on strictly decentralized solutions only;
- fit the above criteria, but do not go into details about the techniques, characteristics, etc.

EC5 - Secondary studies (literature reviews and meta-analyses) will not be included in the results, but may be cited for contributing (citing other relevant articles.

EC6 - Articles older than 2016.

EC7 - Articles not available for download or incomplete.

When evaluating the inclusion and exclusion criteria, reviewers were instructed to follow three steps:

I. Observe the metadata (publication date, total citations, quality of the publication vehicle, etc): from the metadata, some inclusion criteria and most of the exclusion criteria can already be verified;
II. Read the title: this is the first step in analyzing the criteria for adherence to the scope of this review;
III. Read the abstract: through the abstract, the process of evaluating the scope of the article that was started in the previous step is concluded.

If after following the steps above, there are doubts about the suitability (relevance) of the article under analysis, it is to be speed read under the following guidelines:

I. Read the introduction for more clarity on the topic of the article;
II. If doubts are about the paper's relevance but not about the topic is addresses, read the results and conclusion;
III. If doubts persist, read specific elements using a keyword search tool or, as a last resort, read the article in its entirety;
IV. If after all these steps there are still doubts, share them with the other reviewers.

b. Own Review

Although it is the role of the main reviewer to search for works adhering to the proposed theme, indication of authors or other works by the reviewers were observed.

2. QUALITY ASSESSMENT OF THE WORKS

The general quality evaluated during reading makes up the relevance of each selected work in relation to the topic under study and is used to rank the works in decreasing order of relevance.

The final step in the analysis, having already observed the inclusion and exclusion criteria, was the complete reading of the document. A total of 104 works were read in their entirety.

While reading an article in its entirety, the reviewer assesses its quality (relevance) according to the criteria in Table 3. These criteria were proposed by Marie Shaw in [SHAW, 2003] for gauging the quality of software engineering work. We adopt them here for they seem also to offer important insights into the quality of papers on the topic at hand. The reviewer attributes a value to each criterion as s/he reads the paper. The paper's final rank is the simple average of all attributed values.

Table 3: Quality Assessment Criteria

ID	Description	Adequacy
QC1	Is the study clear, without ambiguity, based on evidence and arguments?	• Please note the guidelines presented in topic 3.3 of Marie Shaw [SHAW, 2003]
QC2	Is there a clear statement of context, relevance, objectives and contribution of the research?	• At the reviewer's discretion
QC3	[Studies featuring experiments] Were they applied to real scenarios/data?	• Yes = 1 / No = 0
QC4	[Analytical Studies] Was the data analysis rigorous enough?	• No: discarded
QC5	Type of validation [SHAW, 2003].	• Formal proof: 0.5 • Analysis: 0.23 • Evaluation: 0.05 • Experiment: 0.24 • Real example: 0.2 • Toy example: 0.17 • Other: discarded
QC6	Does the study have concrete relevance for research or practice? [SHAW, 2003]	• Have a potentially popular app?: 0.08 • Does it promote public access to DAX?: 0.18 • Does it bring any structural improvement that promotes the decentralization paradigm with the public?: 0,25

		• Does it solve a problem for the majority of the population?: 0.5.
QC7	Is the article properly referenced?	• The most properly referenced receives a grade of 1; others receive a grade proportional to the difference in relation to the maximum grade

3. Referências

SHAW, Mary. Writing good software engineering research papers. In: **25th International Conference on Software Engineering, 2003. Proceedings.** IEEE, 2003. p. 726-736..

Apêndice E

Smart Contracts and the Lay User Needs

Smart Contracts and the Lay User Needs

State of the Practice, of the Art and a Research Agenda

TIAGO CLEMENTINO*, JOAQUIM HONÓRIO, and JOSÉ ANTÃO B. MOURA, Federal University of Campina Grande, Brazil
KATYUSCO DE FARIAS SANTOS, Federal Institute of Paraíba, Brazil

In 2008, Bitcoin, the world's first fully decentralized currency, brought with it a technological context that had broad application potential in virtually all areas. Years later, although explored in various applications, these decentralized technologies are still far from the common folk's daily lives. This paper brings a review of the literature that addresses the obstacles that most distance the paradigm of decentralization from the lay user in four main fields: 1) Governance, 2) Security, 3) Scale and 4) Authentication. The results inform on the states of the practice and of the art and point to the difficulty in virtualizing real-world, material events without violating the principle of decentralization as the main obstacle to its popularization. In addition, by establishing a parallel between the early years of the Internet's popularization and the decentralization paradigm, a research agenda is proposed to tackle the (other) gaps identified in the literature.

CCS Concepts: • **Human-centered computing** → **Interaction design**; • **Computer systems organization** → *Dependable and fault-tolerant systems and networks*; • **Information systems** → Information systems applications.

Additional Key Words and Phrases: blockchain decentralized application decentralized governance smart contract

ACM Reference Format:
Tiago Clementino, Joaquim Honório, José Antão B. Moura, and Katyusco de Farias Santos. 2022. Smart Contracts and the Lay User Needs: State of the Practice, of the Art and a Research Agenda. *Distrib. Ledger Technol.* 1, 1 (January 2022), 21 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Decentralized technologies, based mainly on blockchains, have gained attention and investment recently [25]. Blockchain is an unalterable – tamperless – and distributed database / network where there is no central trusted entity. Its immutability is a feature that has proven very useful where immutable records are needed, such as in financial applications [21, 37, 47]. In such decentralized network, data is grouped and stored in blocks connected in a chain (i.e. blockchain), where each block stores a set of transactions. Anyone involved can have access to a complete copy of this database, containing all transactions. That is why blockchains are part of the category of Distributed Ledger Technology (DLT).

*Corresponding author.

Authors' addresses: Tiago Clementino, tiagolucas@copin.ufcg.edu.br; Joaquim Honório, joaquimhonorio@copin.ufcg.edu.br; José Antão B. Moura, antao@computacao.ufcg.edu.br, Federal University of Campina Grande, R. Aprigio Veloso, 882, Campina Grande, Paraíba, Brazil, 58429-900; Katyusco de Farias Santos, katyusco.santos@ifpb.edu.br, Federal Institute of Paraíba, R. Tranqüilino Coelho Lemos, 671, Campina Grande, Paraíba, Brazil, 58432-300.

2769-6472/2022/1-ART $15.00
https://doi.org/XXXXXXX.XXXXXXX

Decentralized Application (DAPP), Decentralized Organization (DAO), Decentralized Society (DAS) and all other models of decentralized entities constitute the paradigm of decentralization – DAX, hereinafter – whose potential for application in different areas is already mapped in the literature [41]. However, such potential is still restricted to purely corporate domains like financial markets [18], games [58], supply chains [45], among others [63]. The present work aims to map potential improvements applied to DAX to expand the decentralized management of transactions to the day to day of society in general – i.e., B2C, Business to Customer applications. For that the paper seeks answers to three specific research questions concerning i) the disruptive potential of DAX; ii) the main obstacles that prevent DAX from exploiting this potential; and, iii) verify whether the high profitability of existing applications discourages research in other unexplored directions.

To explore such questions, four of the main areas with current difficulties for DAX advancement already mapped in the specialized literature were addressed [1, 2, 57] (1) Governance – In DAX, governance is about consensus algorithms and protocols change management [30]. Here, we define governance as the set of decision-making protocols at all layers of the decentralized network, be it in the application layer, the consensus layer or even the change management mechanism behind the network. (2) Safety (or security) – In DLTs this is the foundation behind the integrity of network governance protocols [13]. (3) Scale/Performance – Because DLT is associated with many technologies, the concept of scale or performance cannot be accurately translated into numbers. However, we assume scale/performance to be the increment in transaction processing power attributed to each new node in the network. (4) Authentication - Refers to the ability of entities to perform secure and authenticated, but anonymous, digital transactions [40].

As far as we surveyed, the literature still lacks a mapping of reasons why the disruptive potential of DAX still remains so distant from society. However, previous works made partial but important contributions to this purpose [3, 21, 23, 25, 30, 38, 41, 47, 48]. Such contributions were used in the process of validating the results of our search and selection of articles and are also discussed here.

Results indicate a concentration of research on governance – more specifically, research aimed at improving Smart Contracts (SC).

2 THEORETICAL BACKGROUND

2.1 Decentralization - DAX

DLTs are transaction validation and verification mechanisms in the form of networks where all participants must accept a single data state through consensus algorithms, without the need for a central monocratic validator entity. Anyone can read and write in this single state openly [22]. Consensus is reached by delegating the power of control to any one of the participants and assuming that most of these network participants remain honest. This collective delegation of power is called decentralization of control, or just decentralization.

The absence of single trusted entities makes DLTs attractive for numerous potential uses in the industry [32]. Note however, that cryptocurrencies reached a capitalization of over $1.05 trillion in 2019 [49], attracting malicious participants. In DLTs, decentralization is the main security mechanism. To break such security, the malicious agent would need to represent alone the majority in the consensus algorithm, in order to concentrate the power of control, centralizing the network [28]. Because of this interplay between decentralization and security, it is highly desirable to maintain a high degree of decentralization. The security of blockchains and DLTs in general has already received extensive coverage in the literature [7, 24, 26, 27].

While the protocol layer of most DLTs is able to bypass the need for a central authority, some of their uses have elements of centralization such as Permissioned Blockchains [31], centralized

application layer protocols as Decentraland [1], and tokens with central issuer as Zensports [2], among others. The use of centralized components associated with decentralized technologies, even if they work properly, generate a contradiction, eliminating the advantages of decentralization. Fully decentralized organizations – DAO – represent a solution more aligned with the following DLTs principles:

Permissionless: No restrictions or access rules.

Trustless: While DLTs do not rely on a single operator as a trusted agent, there is trust in the consensus network [4]. System security is based on the assumption that enough nodes in the network behave honestly so that they can reach consensus on the validity of recorded transactions [10]. This ensures that all transactions are completed and valid. Thus, those involved in a transaction do not need to trust each other.

Transparency: All transactions stored in the DLT are publicly visible to those involved. The issuers and receivers of transactions are identified with aliases – hashes – while transaction values and transmitted data are sent clearly. Unless additional privacy measures are taken, it has been shown that transactions can be linked and authors can also be profiled [33].

Decentralized governance: By allowing the community to suggest legislation and vote based on their participation, governance is shared.

The purpose of a DAO is to codify the rules and decision-making apparatus of an organization, eliminating the need for documents and people in governance, creating a structure with decentralized control. The Bitcoin network itself was the first DAO created. A group of DAOs can also establish a set of rules for cooperation or coexistence. Such a process constitutes a DAS. Cross Ledger Atomic Swap Protocols are an example of DAS [6]. DAOs and DASs in addition to DApp are generically referred to as DAX.

2.2 Blockchains

The term blockchain is often used as a generic descriptor for the broader field: DLT. More specifically, blockchain is a type of data structure used to record data in DLTs. That is a chronologically linked list of data blocks established by participants within a predefined time period. These blocks are connected in chronological order to form a chain. The link between these blocks is ensured by the use of a computationally rigid hash function [39]. As the blockchain grows, the complexity involved in recalculating the value of all the most recent hashs also increases, making any changes to past data difficult. This growth in difficulty leads to a deterministic guarantee of data immutability.

2.3 Smart Contracts

The Smart Contract concept – SC – first defined by Nick Szabo in the 1990s [54, 55], describes the general idea of a distributed contract mechanism in the context of contract law in combination with public key cryptography.

Traditional contract enforcement issues that result from information asymmetry create the need for complex monitoring [42]. This asymmetry concerns the execution of rights and obligations of both parties independently and without synchronization, that is very different from the processing of an SC, where all steps are consented by both parties in real time. By complex monitoring we can understand synchronization cycles, where events and facts are properly recorded in documents. Zavolokina et al [60] referred to the used car market example to illustrate this problem. In it there are three synchronization cycles: vehicle inspection, payment and transfer. All these events occur in parallel and independently – without synchronization – and the failure of one of them

[1] https://decentraland.org/
[2] https://zensports.com/

does not guarantee non-compliance with the others, although it compromises the success of the transaction. The payment cycle alone does not guarantee delivery of the vehicle, and vice versa. The identification of a problem in the vehicle results from a failure in the inspection, however this does not guarantee the dissolution of the transaction.

Instead of such complex monitoring mechanisms, SCs provide a distributed, reliable and verifiable contract execution by executing the contract like a computer program, automating contract clauses and logging data, as well as an auditable trail of contract execution which can reduce the scope of legal institutions and penalties [46]. SC is a secure, machine-readable, executable program that can automate specified procedures, including those used in legal contexts.

From a security point of view, the basic premise behind SC is that many types of contractual clauses (e.g. insurance, guarantee, surety, property rights delimitation, etc.) can be built into computer systems and secured using mechanisms of cryptographic validation to make breach of contract costly for the breaching party [54, 55]. From a functional point of view, SCs are the metaphorical equivalent of vending machines in terms of transactional efficiency and automation [55]. Thus, the vending machine is a contract with the bearer: anyone with coins can participate in an exchange with the vendor. The vault and other security mechanisms protect the coins and stored contents from intruders sufficiently to allow for the profitable deployment of vending machines in a wide variety of areas.

3 METHODOLOGY

This section details the research questions of interest and the protocols used to answer them by gathering information from the industry and/or by collecting, analyzing and selecting the most relevant academic papers that address SCs' solutions in the specialized scientific literature.

3.1 Research Questions

The research questions (RQ) aim to verify and motivate investigation into the distance between decentralized applications and everyday transactions by common users. To this end, an exploratory effort was carried out according to a Systematic Literature Review (SLR) in special, to answer 3 RQs:

RQ1. Is there really a disruptive potential in Decentralized Technologies – DAX?

RQ2. What are the main obstacles to the popularization of DAX?

RQ3. Does the high profitability of financial and other corporate DAPP discourage the development of B2C DAPP initiatives?

To answer **RQ1** we draw a parallel between the following stages of development and popularization of the Internet and DAX: Stage 1: disruption; Stage 2: utility; Stage 3: usability (Google); and, Stage 4: mirroring society and relationships amongst human users through technologies (Social Networks and Smart Phones). A similar parallel has already been applied by Carvalho et al [9] when comparing the rise of cryptocurrencies and their satellite technologies to the trajectory of the open source Linux operating system [3].

For **RQ2**, SLR results indicate that several of the DAX weaknesses highlighted in the literature have already received widespread coverage by both academia and industry. It is reasonable to assume that weaknesses that have already been effectively addressed no longer represent impediment to DAX popularization – such is the case of oracle reputation protocols [8] or mining decentralization models [52]. On the other hand, issues explored only recently or with little relevant results were

[3]https://linux.org/

treated as more direct impediments, such as Governance in Internet of Things (IoT) Networks [59], Ricardian SCs [42], etc.

Finally, to answer **RQ3**, we draw a parallel between the initiatives that have been receiving the most attention and investment in the industry segment recently and those that are the most explored in academic R&D efforts. This parallel allows us to perceive different priorities for DAPPs in these two segments and to consider how industry's (high profitability) DAPPs may drag academic initiatives.

3.2 Selection Process

The inclusion and exclusion criteria for the selection of works takes into account the objectives, research questions, and metadata that help to estimate the quality of the works. The methodology followed by the reviewers is described in a separated document [4]. The Tables 2, 1 and 3 describe the inclusion, exclusion and quality criteria used by the reviewers in order to 1) check minimal elements to be accepted – exclusion criteria; 2) verify the results obtained by the researcher as being adequate to the research topic – inclusion criteria; and, 3) assess the coverage of the topic as being sufficient or not to be considered relevant – quality criteria.

Tabela 1. Inclusion Criteria.

Code	Description
IC1	This criterion is applied to studies that aim to improve decentralized technologies in order to bring them closer to the common user and it produces an integer $\in \{0, 1, 2, 3, 4\}$ where zero excludes the study and any other value classifies it for further evaluation in addition to composing its inclusion score. A non-null integer here refers to one of the four areas of difficulty addressed in this review– 1- governance; 2- scale; 3- security; and, 4- information.
IC2	The work must be complete and peer-reviewed (scientific articles published in conferences or periodicals). Here, the publication will be given the score equivalent to its H5 index (Google Scholar Metrics) divided by the highest score received by an article in this review.
IC3	This criterion is applied to a study that was approved in the previous criteria and published between 2016 and 2022, and produces a real number ≥ 0 and ≥ 1 depending on its publication date (2016 corresponds to zero and 2022, to 1).
IC4	The criterion is applicable to empirical, formal or theoretical studies. A theoretical-only study = 0.3; an empirical one = 0.6; formal 0.9; and, formal and empirical, 1.0.

3.3 Methodology Steps

Literature reviews tend to be initiated based on prominent scientific publications focused on the topic under analysis [29]. Such an approach, although successful in well-established areas of knowledge, can be inefficient when dealing with a still recent topic such as DLTs or the decentralization paradigm, with few well-established publishing vehicles and many relevant works published in journals from other areas. Therefore, to circumvent such inefficiency, it focused on Ethereum white paper as a seed.

DLTs have gained relevance in recent years due to the successful application of technologies such as Bitcoin [39] for cryptocurrencies and the Ethereum network [17] for cryptocurrencies and SCs in

[4]https://bit.ly/3SQlhdM

Tabela 2. Exclusion Criteria

Code	Description
EC1	Duplicated documents or published more than once by the same authors in different languages.
EC2	Written in languages other than English.
EC3	Tutorials, summary studies (studies of 4 pages or less)or any work that has not been submitted for peer review.
EC4	Studies that: a. discuss applications only – i.e., that do not propose any evolution in technology or do not solve an ordinary – business to customer; b. are from other areas that do not correspond to decentralized systems; c. discuss technologies with restricted access (permissioness), or with centralized management. (This review focus on strictly decentralized solutions only. d. fit the above criteria, but do not go into details about the techniques, characteristics, etc.
EC5	Secondary studies (literature reviews and meta-analyses) will not be included in the results, but may be cited for contributing (citing other relevant articles.
EC6	Articles older than 2016.
EC7	Articles not available for download or incomplete.

general. Although the Bitcoin white paper was the trigger for the expansion of the decentralization paradigm, the Ethereum network proposal has greater application potential because it relies on SC technology. Based on this, instead of starting the search from keywords defined by us or renowned journals, the first step (1) of this review consisted of making a summary of publications that make some reference to the Ethereum white paper, as informed by search engine Google Scholar [5], then applying the criteria of this review to them in order to select the most relevant works, and then extract the keywords listed there.

The second step (2) consisted of the process of consulting search engines in scientific databases using the keywords identified in the first step, and subsequent verification of the relevant works according to our defined criteria. Since the topic under analysis has a commercial bias, where several solutions may already be in use in the business sector and often are not published in academic circles, a parallel consultation step was undertaken focusing on patent engines and solutions listed on the sites growthlist.co and crunchbase.com, two of the largest agents of innovative ventures – startups. The main objective of this initiative is to answer the RQ3. The third and final step (3) consisted of a validation of our results against those that were collected by other literature reviews in related work. The complete article selection process is graphically presented in Figure **??** and will be described in more detail below.

3.3.1 References to Ethereum White Paper. As a first step, we gathered 320 works that reference [17] according to Google Scholar on February 11, 2022. The works contained in each of these references were the first to be submitted to the criteria of exclusion, inclusion and quality in Tables 1, 2 and 3. Table 8 lists informs on results.

In this first phase, 25 works were selected, which provided the keywords needed to generate the search strings that were later used to search for more references in scientific databases (step 2, in Section 3.3.2). The 18 keywords extracted from this first phase are listed in Table 8.

[5]https://scholar.google.com.br/

Tabela 3. Quality Criteria

Code	Description	Adequacy
QC1	Is the study clear, without ambiguity, based on evidence and arguments?	Please note the guidelines presented in topic 3.3 of Shaw [50]
QC2	Is there a clear statement of context, relevance, objectives and contribution of the research?	At the reviewer's discretion
QC3	[Studies featuring experiments]Were they applied to real scenarios/data?	Yes = 1 / No = 0
QC4	[Analytical Studies] Was the data analysis rigorous enough?	No: discarded
QC5	Type of validation [50].	Formal proof: 0.5 Analysis: 0.23 Evaluation: 0.05 Experiment: 0.24 Real example: 0.2 Toy example: 0.17 Other: discarded
QC6	Does the study have concrete relevance for research or practice? [50].	1. Have a potentially popular app?: 0.08 2. Does it promote public access to DAX?: 0.18 3. Does it bring any structural improvement that promotes the decentralization paradigm with the public?: 0,25 4. Does it solve a problem for the majority of the population?: 0.5.
QC7	Is the article properly referenced?	The most properly referenced receives a grade of 1; others receive a grade proportional to the difference in relation to the maximum grade

3.3.2 Search in Repositories. The strategy for the subsequent search is based on the set of keywords selected in the previous step. Here the keywords have been grouped into relevant expressions (search strings). Since the set of keywords was very large, they were grouped into expressions as specific as possible – along with other correlated keywords in order to isolate themes ("Agent-based simulation AND blockchain", instead of just "Agent-based simulation") – to facilitate the indexing of results by relevance in each of the search engines used. The expressions used are listed below. For the search, each of the expressions was isolated by double quotes, as all the search engines used follow this strategy to group expressions with spaces. Also, in the following expressions the specifics of the syntax compatible with each query database were ignored, separating the elements from the conjunctions by the "AND" operator: *economics of IS AND blockchain; decentralized autonomous organizations; domain-specific language AND executable specifications AND normative modeling AND smart contract; i-voting AND blockchain; agent-based simulation AND blockchain; block-free ledger; dAG-based distributed ledger; Legal recognition AND blockchain; DSA AND blockchain; privacy audit log AND blockchain; RDF Signatures AND blockchain; semantic web AND blockchain; decentralized application AND recommendation system AND reliability prediction; multi-resource trading AND smart marketplace AND blockchain; mesh network AND distributed ledger technology; smart badge AND blockchain; insurance AND settlement AND blockchain.*

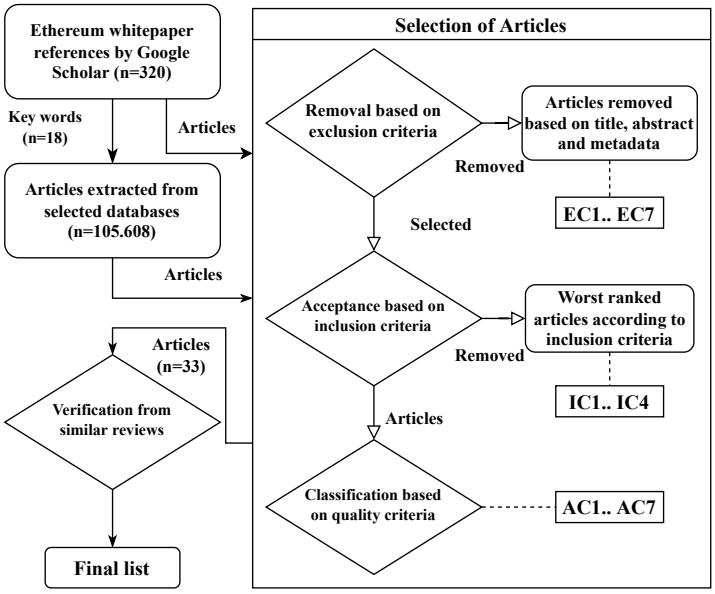


Fig. 1. Research protocol

With this, it is possible to better explore the relevance indexing potential of search engines. Five scientific databases were selected based on the general quality of their most relevant results (first listed): IEEE Explore, Google Academic, ACM Digital Library, Scopus and Springer. The results were grouped with the support of the Mendeley scientific research tool [6], which was used to extract the results, list, explore and classify the works.

For feasibility, due to the large volume of results, only the most relevant first 30 works from each database for each search string were counted. According to Garousi and Mäntylä [20], the saturation effect groups the most relevant results of each search in the top positions. Thus, whenever $30 \leq n$ results were identified, only the first 30 were evaluated. Since it was used very specific search strings, it was understood that this was an acceptable risk to the validity of the review. This phase resulted in 104 accepted works. Table 7 lists the total number of results extracted from each database.

3.3.3 References in Literature Reviews of Related Themes. Although literature reviews on related topics were not included in the final results – as defined in the Exclusion Criteria – such works were scanned for relevant research we may have missed in search steps 1 and 2. The main objective was to legitimize the effectiveness of the previous stages, checking the existence of potential unselected works. This technique included seven literature reviews [2, 11, 21, 25, 30, 37, 47**?**] and only one selected article that had not been covered before (see Table 4).

Murray et al [37] provide a mapping of works focused on SC and corporate governance. Although closely aligned with the research questions of this review, Murray et al[37] does not focus on improvements in current technologies capable of bringing DAX to the lay end user. Cousins et al [11] uses the Value-Sensitive Design methodology to map a research agenda on the main possible contributions of cryptocurrencies (taking Bitcoin as an example) to the lives of end users, an objective closely related to this review, despite diverging in focus restricted to cryptocurrencies. Karajvanov [25] brings the absence of guarantees for future conditions as the main obstacle separating decentralization from real contracts. This finding is quite relevant and is in line with the findings of this review. Although Cousins et al [11] and Karajvanov [25] offer results about

[6]https://www.mendeley.com/

make decentralization closer to real contracts, they did so as collateral, not being the target of their review.

Tabela 4. Literature reviews on related topics and their respective correlations to the purpose of this review

Title	Author	Year	Total	Unreleased
A Value-sensitive Design Perspective of Cryptocurrencies: A Research Agenda	Cousins, Karlene; Subramanian, Hemang; Esmaeilzadeh, Pouyan	2019	0	0
Blockchain Based Smart Contracts : A Systematic Mapping Study	Alharby, Maher; Moorsel, Aad van	2018	2	0
Blockchain research in information systems: Current trends and an inclusive future research agenda	Rossi, Matti; Mueller-Bloch, Christoph; Bennett Thatcher, Jason; Beck, Roman	2019	1	0
The Blockchain as Platform Architecture and Basis for Innovation	Franke, Laura Amadea	2016	1	0
Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance	Murray, Alex; Kuban, Scott; Josefy, Matt	2021	3	0
Blockchains, Collateral and Financial Contracts	Karajvanov, Alexander	2021	2	1
Governance Possibilities of Blockchain Platforms	Larcher, Florian	2019	2	0
Authentication and Access control Based on distributed ledger technology: A survey	Ghaffari, Fariba; Bertin, Emamnuel; Hatin, Julien	2020	1	0

3.3.4 Search in Commercial Repositories. Reports on commercial initiatives often do not pass through academia and are not subject to peer review. As such said initiatives are often ignored by mainstream SLR's. However, in an essentially industry-oriented field such as the crypto asset ecosystem, ignoring such initiatives could pose a dangerous threat to the validity of the review. To avoid such bias, patent engines were consulted in search of relevant initiatives. At the same time, note that patent filing is an essentially centralized intellectual property recognition strategy, so it is only addressed briefly here.

de Araújo and de Farias Santos [14] made efforts to fill this gap in 2019, when they consulted three distinct patent databases in search of deposits related to SC: Lens [7], Questel Orbit [8] and Patent Inspiration [9]. Here, we update their findings by redoing their queries in order to reach new conclusions.

[7]https://www.lens.org/
[8]https://www.orbit .com/
[9]https://www.patentinspiration.com/

Moving beyond patent filings, two of the largest commercial startup recommendation websites aimed at investors, Growthlist [10] and Crunchbase [11], were used as search tools. Other recommendation sites that provide similar service were not considered because they relate to more mature companies that are already listed on stock exchanges – e.g., Forbes [12], Fortune [13], Fool [14] – or did not show results associated with DAX – e.g., Betalist [15]. In addition, most of these do not present a means of searching by topic of interest – e.g., Owler [16].

In the updating searches, the following summarized set of criteria was applied: IC1, EC4, QC2, QC6 and, as an additional criterion, initiatives *at least in the final stage of fundraising* were analyzed. The selected initiatives are listed in Table 5 and total only 12. As described in Session 4.2 the majority of them are related to decentralized finance – criptocurrencies – and scale.

4 RESULTS

This section organizes results per review methodology stage and as answers to the RQs.

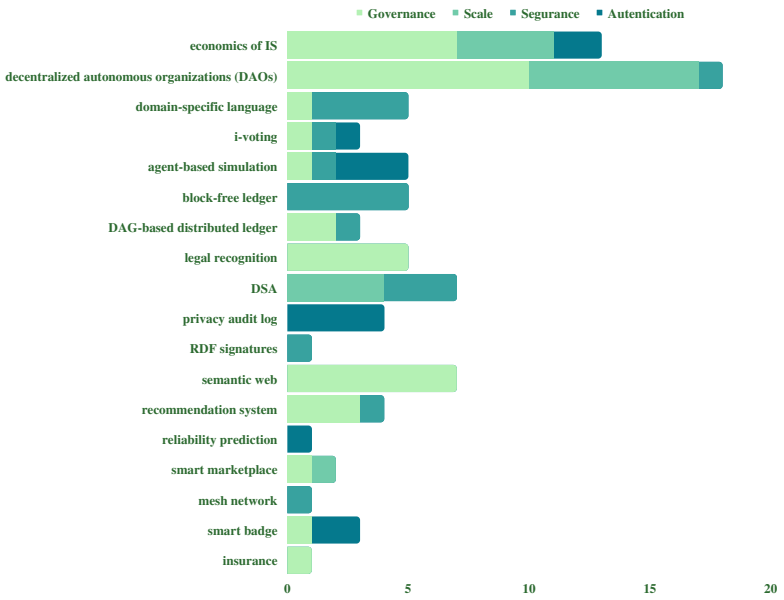


Fig. 2. Theoretical framework: Each main keyword selected vertically × 121 relevant works horizontally

In total, 121 works were classified as relevant, 91 in step (1) – references to the Ethereum white paper – and 30 in step (2). As described in Figure **??**, 33 articles – 25 from step (1), 7 from step (2) and 1 from similar reviews, discounting duplicates – had an overall rating greater than 0.5 in all inclusion criteria and also in the quality criteria, but only the first 12 articles are listed in this document because they obtained a score equal to or greater than 0.25 in the QC6 criterion – see Table 3. From these numbers and based on the most recurrent keywords in the classified articles, we can establish a theoretical framework for the current state of the art with respect to the four

[10] https://growthlist.co/
[11] https://www.crunchbase.com
[12] https://www.forbes.com/growth-companies/list/
[13] https://fortune.com/100-fastest-growing-companies/
[14] https://www.fool.com/investing/stock-market/types-of-stocks/ growth-stocks/
[15] https://betalist.com/startups/growth-list
[16] https://corp.owler.com

Tabela 5. Selected industry initiatives.

Title	Web Site	Description
DeFi Wizard	defiwizard.xyz	Automation of the creation of SCs in a modular way, assembling components
Elly	elly.com	Payment device for sales – POS – that accepts all types of payment, including cryptocurrencies.
Biconomy	biconomy.io	Multi-blockchain application layer aimed at simplifying Dapp development
Topl	www.topl.co	Eco-efficient blockchain capable of monetizing sustainable initiatives
MINIMA	www.minima.global	Small blockchain in processing and storage. With this blockchain, any device can download a node from the network, mine and store its own information. IoT-oriented.
ETHEREUM PUSH NOTIFICATION SERVICE, EPNS	epns.io	Every blockchain is reactive to user actions. EPNS allows users to act by generating notifications for others and profiting from it.
Medable	www.medable.com	Decentralized network of clinical cases
Cashaa	cashaa.com	It describes itself as a bank that operates with both conventional and decentralized products
Ava Labs	www.avalabs.org	It describes itself as the most scalable blockchain on the market. In addition to having an incentive program focused on accelerating the adoption and growth of its new subnets.
The Graph	thegraph.com	Multi blockchain data query tool
Ziglu	www.ziglu.io	Crypto bank with banking app, credit card and automatic conversion between cryptocurrency and common currency.
Solana	solana.com	Largest blockchain with low cost and scalable proposal

main difficulties for the popularization of DAX – Security, Information, Scale and Governance – as indicated in Figure 2.

4.1 State of the Art

Observing the temporal distribution of the volume of publications by each of the four main difficulties, as shown in Figure 3, one can observe that interest has shifted from issues related to security and scale to Governance. That is a coherent observation because up to 2017 the blockchain ecosystem was in formation and security and mining protocols were immature and as such, drew most of the attention of research efforts. Over time and until 2021, scale and security lose their prominence, giving way to management issues and issues related to the application of technology itself, such as Internet of Things, Economics of IS and Semantic Web.

4.1.1 ***RQ1****: Is there a disruptive potential in DAX?.* From the launch of the ARPANET in the 1960s, through the first use of the term Internet in 1978, to the publication of the first page on the World

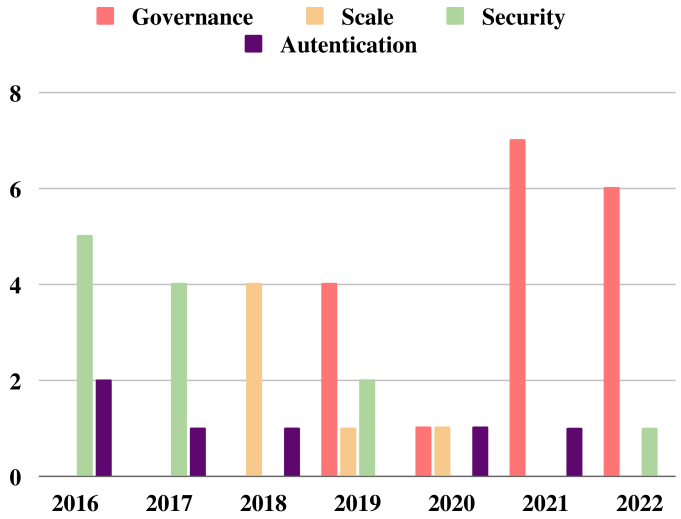


Fig. 3. Temporal distribution

Wide Web in 1990, 30 years went by. From then until the launch of the Google search engine in 1998, another eight years passed. Thus, one may say that it took the Internet 38 years to reach to be ubiquituous in the daily life of society [17]. Taking the publication of the Bitcoin white paper in 2008 as the debut of the decentralized paradigm, one gets 14 years of DAX existence by 2022. Thus, compared to the time it took the Internet to mature, DAX is still in its early years.

The popularization of the Internet throughout the 1990s, 2000s and 2010s happened in four stages:

(1) Disruption: For the Internet, that happened when Tim Berners-Lee – creator of the World-Wide-Web network, the HTML formatting language and the HTTP protocol – in 1993 announced that his creation would work openly and without royalty collection, in the assumption that only in this way would the Internet reach its true objective of becoming a worldwide human community.
(2) Usefulness: Several online services began to be created with a focus on popularizing the Internet and gaining engagement, such as the GeoCities website [18] which offered the service of creating personal static Home Pages – today this may seem little useful compared to what we have now, but in 1994 it was a great success.
(3) Usability: Google emerged in 1998 as a generic tool for Fast Indexing the entire Internet, allowing any website to be found from any small snippet of its content. This laid the last foundation stone to transform the Internet into the dynamic community it is today.
(4) Mirroring: Currently, one cannot talk about the Internet without mentioning social networks. Facebook [19] being the main phenomenon of popularity at this stage, but not the pioneer, because before it several other networks were created for specific purposes such as SixDegrees, AIM , ICQ or Friendster, all of which are now deactivated due to competition with Facebook.

[17] Much of the historical content concerning the Internet in this subsection was based on Barry [5]
[18] https://web.archive.org/web/20010501000000*/geocities.yahoo .com/
[19] https://www.facebook.com/

We can clearly recognize the first stage in DAX, where the Bitcoin and Ethereum networks, in addition to the entire blockchain ecosystem, promoted the recognition of the disruptive potential of the decentralization paradigm. However, DAX stumbles on the second stage, as they still lack popular appeal.

The timelines presented in Figure 3 make clear a growing demand for governance solutions in academia. Figure 5 shows that the same holds for the industry. Table 9 indicates an expectation of disruption more focused on SCs and governance. Karajvanov [25] presents a set of future works and limitations of current decentralized technologies, among them the difficulty in punishing non-compliance with a contractual requirement without the need to withhold funds. This limitation stems from the difficulty of DAXs in representing real-world events and facts in the blockchain (on-chain) without relying on reliable centralized verifications. Such a virtualization gap contrasts with the virtualization of values, already widely achieved since the emergence of cryptocurrencies. Table 6 draws a parallel between the emergence of the Internet and DAX technologies from the collected results.

Tabela 6. Internet × DAX

Phase	Internet	DAX
1	Information virtualization from the emergence of the World Wide Web network	Virtualization of values through cryptocurrencies
2	Virtualization of events and facts from online services	Virtualization of contractual events still open
3	Relationship virtualization accessible through Google as a generic and total utilization mechanism	Opened
4	Social networks generate dependency, also virtualize relationships and begin to virtualize authority	Opened

4.1.2 ***RQ2****: What are the main obstacles to the popularization of DAX?.* The selected articles in Table 9 indicates a recent focus on governance with SC enhancement as the main target of efforts by the community.

In the industry and according to Table 5, the main recent initiatives are related to the decentralization of banking services, with some initiatives also linked to the scale of decentralized services and only two directly associated with SC enhancement. This demonstrates a disparity between the industry and the scientific community. If, on one hand, the scientific community has focused on the popularization of SC, on the other, there are few promising initiatives in the industry.

Previous mappings have already shown that the disruptive potential of SC technology generates a lot of expectation in the community and in the industry [47]. Furthermore, according to Song et al [52] the lack of public blockchain technologies decoupled from the concept of currency, or financial reward per transaction, makes it difficult to take advantage of SC technology at its core. Still according to Song et al [52], this limits such applications to financial and corporate domains, where this type of charge is more viable.

Still on SC, Karajvanov [25] states that the difficulty in providing guarantees based on asymmetric information is one of the main bottlenecks of SC. That is, an SC cannot establish obligations and rights over future transactions or events that occur in the real world. This precludes most practical uses of SC as a substitute for conventional contracts. Creutz and Dartmann [12] propose a solution

based on Ricardian Contracts, but all collateral validation remains based on conventional contract models.

From the above, we can infer that one of the factors that distances the user from the decentralized paradigm is the limitations of SC technology itself when compared to conventional contracts: the difficulty in virtualizing real-world events in a decentralized way, its limitations in imposing or limiting future transactions, or even their natural determinism [8, 12, 16, 25, 42].

4.2 Status of the Practice

4.2.1 ***RQ3****: Does the high profitability of the financial and corporate segment discourage the development of B2C initiatives?* As a first attempt to answer this question, patent databases were consulted. De Araújo and de Farias [14] have already made efforts in this direction in 2019, where there was a greater interest from the industry in the Management Method, which brings us back to Governance. The present work sought to update the findings of de Araújo and de Farias [14] by reapplying the queries. Results corroborate the previous findings and Figure 4 shows that the deposit rate remains high until 2021 (last full year in the queries as reapplied on September 9, 2022) – i.e., on the same plateau as in 2018 that de Araújo and de Farias [14] pointed out as the most relevant. Thus, it is possible to infer that the Management Method is relevant issue also in the patent industry and research in SC remains intense. However, it is unwise to take the filing of patents alone as a compass for DAX profitability. Thus, this review also shifted its attention to investment recommendation bases.

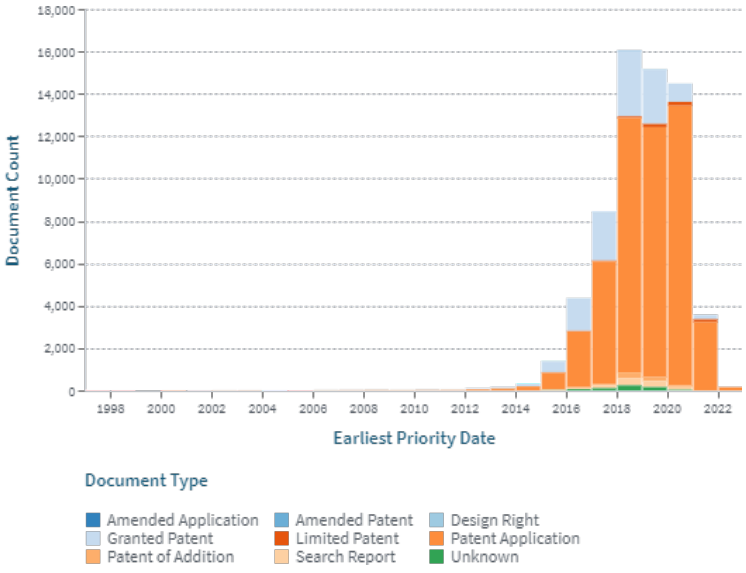


Fig. 4. Yearly Patent Deposits from 2010 to 2023 (Source: results from queries on lens.org)

When analyzing the table of twelve non-academic initiatives selected from an investment recommendation base – see Table 5 – it is observed that half of them – six – are linked to decentralized finance and scale, while four are linked to management, one refers to a specific clinical application and the last one brings solutions linked to sustainability.

Figure 5 shows the temporal history of these initiatives compared to the temporal history of academic initiatives. From this figure, we can see that although the decentralized solutions industry is in fact very focused on the financial market, in general there is also a more recent trend linked to the search for governance solutions and the adaptation of the decentralized ecosystem to the

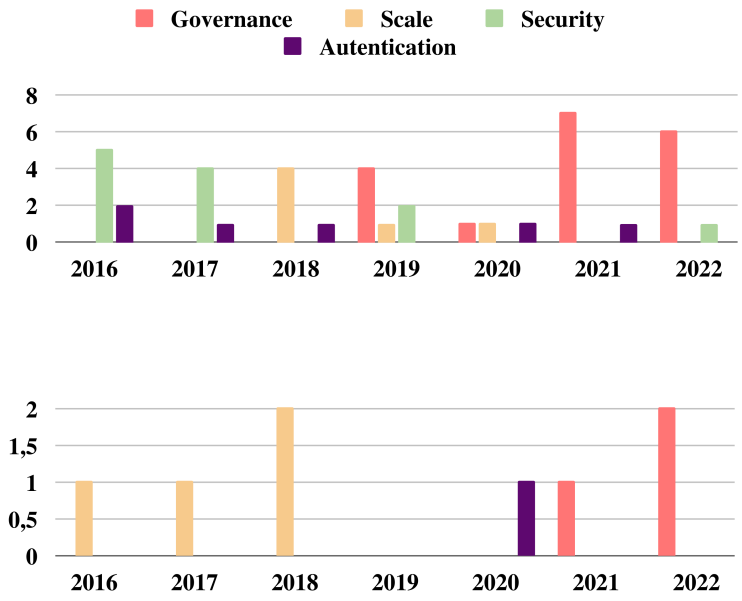


Fig. 5. Comparative temporal distribution: state of the art (above) × state of the practice (below)

demands of the real world. Solutions more focused on technical issues (e.g., scale) are already more mature and consolidated (e.g.,MINIMA, Ava Labs and Solana, production solutions listed in Table 5).

4.3 A Research Agenda

Based on the results and conclusions, future research with the objective of bringing the user closer to DAX was anticipated to happen along the following four opportunities:

(1) A solution for decentralized governance appears to be a focal point in recent work [30]. So that, two important questions remain opened;
   (a) How to decentralize the changing management of public DLT;
   (b) How to manage user reputation on decentralized networks.
(2) The difficulty of scaling up on blockchain has mainly been tackled using Block-free Ledgers [44]. However, the industry already has effective and growing initiatives aimed at scaling the volume of transactions and mining on blockchains – see Table 5;
(3) The difficulty of virtualizing real-world events and facts leads DLTs to appeal to centralized authorities through oracles [8] or trusted entities. A solution that mirrors real-world events and facts in a decentralized way is one of the most critical problems when it comes to bringing decentralized solutions to people's daily lives [15, 34–36, 43]. Zavolokina et al [60] illustrated this problem using the sale of a used car as an example. There is a lot of data to describe the car's mechanical situation, but to virtualize them in a decentralized way is a big challenge because the car owner wants to hide any bad information from the buyer. Currently our efforts are focused on how to ensure the correct and decentralized checking of such real-world information;
(4) Real-world business relationships tend to provide rules for transactions that are yet to come. It is impossible, for example, to create a punitive contractual clause for non-compliance with a specific requirement, unless the punishment is monetary through an amount previously

withheld. However, current SCs can only govern transactions that have already taken place with guaranties already available [25, 56].

The above research opportunity on SC are closely related to findings of Cousins et al [11] that reported demands and research gaps on Trust, Self-governance and Responsible Innovation in criptocurrencies.

4.4 Threats to Validity

It was observed that several decentralized initiatives are undertaken with economic objectives only, without reporting results in the form of a scientific work. This observation represents an important threat to the validity of any scientific survey in a such theme so explored by industry. For such initiatives, there are no general repositories or publications that offer a complete overview of these efforts due to their disruptive potential. Data sources committed to listing such initiatives aim to provide information for investment, presenting only potentially profitable initiatives. To mitigate this risk, a search in the literature, the collection of recommendations in investment tools on decentralized initiatives and consultation of patent databases were combined.

5 CONCLUSIONS AND FUTURE WORK

This article presented a systematic review of the literature from 2016 – 2022 that mapped industry initiatives and scientific research into solutions and technologies capable of making the decentralization paradigm more attractive and useful to the lay user in general. Investigations into recent patent filing volumes, investment recommendation models in emerging solutions, and searches of five prominent digital databases/libraries followed by automatic filtering and manual inspection led to insights and a final selection of 33 academic studies that responded to three RQs of interest, 12 of which are capable of promoting structural improvements in the technology (criterion QC6). The answer to RQ1 (*Is there a disruptive potential in DAX?*) came through a parallel between DAX and the early years of the Internet. Thus, it was possible to see that DAX still has time to develop – compared to the Internet – however, it has not yet managed to go beyond the early stages of its development. RQ2 (*What are the main obstacles to the popularization of DAX?*) points to decentralized governance as a focal point for exploring the disruptive potential of DAX. In this scenario, the decentralized virtualization of the real world is projected as a target for our next studies. Finally, to answer RQ3 (*Does the high profitability of the financial and corporate segment discourage the development of B2C initiatives?*) the state of practice was mapped, noting that although the industry is rather focused on financial and corporate solutions, issues related to scale and security are also covered. However, governance – main focus in the literature – has received some attention only recently.

With what is raised in this review, it is possible to have a clearer view of what distances the lay user from DAX. Literature and industry lack decentralized governance models capable of mirroring and validating the rules that govern society and its commonly entered contracts. The validation and recording of facts governed by such rules being the focal point of our future efforts.

Based on the results presented here, we can identify a theoretical framework (see Figure 2) as the current scenario of the process of popularization of decentralized technologies. Figure 2 clearly shows a trend towards governance research not only in recent times, but in general. Although this effect has been caused by an increase in the interest in blockchains in recent years by the academy, coinciding with the period of greater demand for solutions in governance, certainly the complexity behind Decentralized Governance proves to be a critical obstacle for applications B2C of such technologies. Within the governance theme, it is not surprising that DAOs are the issue of greatest interest, as it is the most representative form of Decentralized Governance and the main

Tabela 7. Search strings and their outputs in number of articles and accepted articles – Search Date: 04-08-2022.

	ACM		*IEEE*		*GScholar*		*Scopus*		*Springer*	
Final Set of Search Expressions	Returned articles	Accepted articles	Returned articles	Accepted articles	Returned articles	Accepted articles	Returned articles	Accepted articles	Returned articles	Accepted articles
"economics of IS" AND "blockchain"	0	0	518	1	7.890	10	5	0	5.334	2
("decentralized autonomous organizations" AND "DAO") AND "blockchain"	161	3	65	2	211	9	0	0	2.267	5
("domain-specific language" or "executable specifications" or "normative modeling") AND "smart contract"	31	1	0	0	1	1	0	0	1.669	3
"i-voting" AND "blockchain"	4	0	2	0	378	2	0	0	53	1
"agent-based simulation" AND "blockchain"	8	0	10	1	816	2	0	0	603	2
"block-free ledger"	1	1	1	1	6	2	0	0	9	1
"DAG-based distributed ledger"	8	0	12	0	123	3	0	0	76	0
"Legal recognition" AND "blockchain"	108	1	11	0	4.390	2	0	0	477	2
"DSA" AND "blockchain"	27	1	18	1	1.870	3	0	0	248	2
"linked data" AND "blockchain"	46	1	239	3	2.030	2	0	0	8.811	3
"privacy audit log" AND "blockchain"	1	0	13	1	9	1	0	0	1.368	1
"RDF signatures" AND "blockchain"	0	0	0	0	1	1	0	0	184	0
"semantic web" AND "blockchain"	49	1	13	0	3.520	4	0	0	1.617	2
"decentralized application" AND ("recommendation system" AND "reliability prediction")	2	0	59	2	52	2	0	0	5.620	1
("multi-resource trading" AND "smart marketplace") AND "blockchain"	0	0	79	0	26	2	0	0	14	0
"mesh network" AND "distributed ledger technology"	3	0	2	0	152	1	0	0	630	0
"smart badge" AND "blockchain"	0	0	1	0	26	2	0	0	265	1
("innsurance" AND "settlement") AND "blockchain"	395	1	282	1	48.000	4	0	0	4.599	2
Total	910	10	1.348	13	69.501	53	5	0	33.844	28

Tabela 8. Main keywords and their occurrences in classified works

Keyword	Ocurrences
economics of iS	2
decentralized autonomous organizations	3
domain-specific language	1
i-voting	2
agent-based simulation	1
block-free ledger	1
DAG-based distributed ledger	1
legal recognition	3
DSA	1
privacy audit log	1
RDF signatures	1
semantic web	2
recommendation system	1
reliability prediction	1
smart marketplace	1
mesh network	1
smart badge	1
insurance	1

strategy for mirroring reality – here, we understand mirroring reality as being the initiative of people or organizations to represent themselves in the digital environment.

Making a more immersive analysis of the Table 9, we observed that among the main results there is no one referring to the topic Authentication/Privacy. In fact, there are no records selected for this area because none of them obtained a score greater than or equal to 0.25 in the QC6 criterion nor 0.5 or more in all others. In order to include any result regarding this topic, it would be necessary to accept articles with a rating greater than or equal to 0.18 in QC6 and fail in QC7 criterion, which would expand this list to 62 works, compromising the visualization of the table. On the other hand, none of the analyzed articles scored 0.5 in the QC6 criterion. That is, to date, no scientific work on DAX has been identified that solves a problem for the majority of the population. This can be seen as evidence of the immaturity of the state of the art for this topic.

Among the articles selected from the Table 9, governance is the most discussed topic in relation to the others. Among the main results in this area, the improvement of SC technology is the most discussed. Looking more closely at this type of application, it can be seen that Machine Learning for Legal Validation is an important topic. Furthermore, interpretability in SC, Ricardian Contracts or contracts with collateral transactions (column “Focal technology”) are clearly alternatives for emerging SCs in the real world. Thus, the decentralized virtualization of events and the mirroring of real-world transactions on the blockchain appear to have been key pieces of research in recent years.

ACKNOWLEDGMENTS

Funding sources from *Coordenação de Aperfeiçoamento de Pessoal de Nível Superior* – CAPES (Higher Education Personnel Improvement Coordination)

Tabela 9. Related works and their evaluated dimensions.

Reference	Application type	Area	Focal technology	Objective	Relevance (QC6)
[51]	Application model	Governance	Insurance Market	Real relations minoring	3
[64]	Data analytics	Governance	Distributed Hash Table	Audit	3
[53]	Contract improvement	Security	Index Terms-Blockchain	Contract Validation	3
[59]	SMP - Smart Market Place	Governance	Multi-resource trading	Transaction Validation	3
[16]	Contract improvement	Governance	Machine Learning	Legal validation of SC	3
[8]	Contract improvement	Governance	Machine Learning	Legal validation of SC	3
[61]	Protocol	Scale	Directed Acyclic Graph – DAG	Free transactions	3
[12]	Contract improvement	Governance	Generic SC	Interpretability of contracts	3
[25]	Contract improvement	Governance	Collateral SC	Interdependent transactions	3
[52]	Protocol	Governance	Proof of contribution	Coinless Public Blockchain	3
[42]	Contract improvement	Governance	Minimum Ricardian SC	Contestable SC	3
[62]	Data analytics	Security	Machine Learning	Node Behavior Prediction	3

REFERÊNCIAS

[1] Hamda Al-Breiki, Muhammad Habib Ur Rehman, Khaled Salah, and Davor Svetinovic. 2020. Trustworthy blockchain oracles: Review, comparison, and open research challenges. *IEEE Access* 8 (2020), 85675–85685.

[2] Maher Alharby and Aad Van Moorsel. 2017. Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372* (2017).

[3] Hendrik Amler, Lisa Eckey, Sebastian Faust, Marcel Kaiser, Philipp Sandner, and Benjamin Schlosser. 2021. Defi-ning defi: Challenges & pathway. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 181–184.

[4] Ashiq Anjum, Manu Sporny, and Alan Sill. 2017. Blockchain standards for compliance and trust. *IEEE Cloud Computing* 4, 4 (2017), 84–90.

[5] M. Barry. 1997. *Brief History of the Internet.* https://www.internetsociety.org/internet/history-internet/brief-history-internet/

[6] Marianna Belotti, Stefano Moretti, Maria Potop-Butucaru, and Stefano Secci. 2020. Game theoretical analysis of cross-chain swaps. In *40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 485–495.

[7] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *symposium on security and privacy*. IEEE, 104–121.

[8] Lorenz Breidenbach, Christian Cachin, Benedict Chan, Alex Coventry, Steve Ellis, Ari Juels, Farinaz Koushanfar, Andrew Miller, Brendan Magauran, Daniel Moroz, et al. 2021. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs* (2021).

[9] Arthur Carvalho, Chaitanya Sambhara, and Patrick Young. 2020. What the history of linux says about the future of Cryptocurrencies. *Communications of the Association for Information Systems* 46, 1 (2020), 2.

[10] Yan Chen and Cristiano Bellavitis. 2019. Decentralized finance: Blockchain technology and the quest for an open financial system. *Stevens Institute of Technology School of Business Research Paper* (2019).

[11] Karlene Cousins, Hemang Subramanian, and Pouyan Esmaeilzadeh. 2019. A value-sensitive design perspective of cryptocurrencies: a research agenda. *Communications of the association for information systems* 45, 1 (2019), 27.

[12] Lars Creutz and Guido Dartmann. 2020. Cypher social contracts a novel protocol specification for cyber physical smart contracts. In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*. IEEE, 440–447.

[13] Sinclair Davidson, Primavera De Filippi, and Jason Potts. 2016. Disrupting governance: The new institutional economics of distributed ledger technology. *Available at SSRN 2811995* (2016).
[14] Gildércia Silva Guedes de Araújo and Katyusco de Farias Santos. 2019. Evolução da tecnologia smart contracts pela perspectiva dos indicadores de patentes. *Cadernos de Prospecção* 12, 5 Especial (2019), 1363–1363.
[15] John Domingue, Allan Third, and Manoharan Ramachandran. 2019. The FAIR TRADE framework for assessing decentralised data solutions. In *Companion Proceedings of The 2019 World Wide Web Conference*. 866–882.
[16] Vimal Dwivedi and Alex Norta. 2021. A Legal-Relationship Establishment in Smart Contracts: Ontological Semantics for Programming-Language Development. In *International Conference on Advances in Computing and Data Sciences*. Springer, 660–676.
[17] W Ethereum. 2014. Ethereum Whitepaper. *Ethereum. URL: https://ethereum. org [accessed 2022-07-07]* (2014).
[18] Olaniyi Evans. 2018. Blockchain technology and the financial market: an empirical analysis. (2018).
[19]]frankecopyright Laura Amadea Franke. [n. d.]. The Blockchain as Platform Architecture and Basis for Innovation. ([n. d.]).
[20] Vahid Garousi and Mika V Mäntylä. 2016. A systematic literature review of literature reviews in software testing. *Information and Software Technology* 80 (2016), 195–216.
[21] Fariba Ghaffari, Emmanuel Bertin, Julien Hatin, and Noel Crespi. 2020. Authentication and Access control Based on distributed ledger technology: A survey. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 79–86.
[22] Dominique Guegan. 2017. Public blockchain versus private blockhain. (2017).
[23] Yi-Ming Guo, Zhen-Ling Huang, Ji Guo, Xing-Rong Guo, Hua Li, Meng-Yu Liu, Safa Ezzeddine, and Mpeoane Judith Nkeli. 2021. A bibliometric analysis and visualization of blockchain. *Future Generation Computer Systems* 116 (2021), 316–332.
[24] Harry Halpin and Marta Piekarska. 2017. Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 1–3.
[25] Alexander K Karajvanov. 2021. Blockchains, Collateral and Financial Contracts. *Discussion Papers* (2021).
[26] Ghassan Karame. 2016. On the security and scalability of bitcoin's blockchain. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1861–1862.
[27] Ghassan O Karame and Elli Androulaki. 2016. Bitcoin and blockchain security. (2016).
[28] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. 2012. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*. 906–917.
[29] Barbara Kitchenham. 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University* 33, 2004 (2004), 1–26.
[30] Florian Larcher. 2019. GOVERNANCE POSSIBILITIES OF BLOCKCHAIN PLATFORMS. (2019).
[31] Jena Marie Espelita, Annette Pelkmans-Balaoing, Ivan Vitali, and Benedetto Gui. 2022. Trusting a Trustless Network. (2022).
[32] Juri Mattila. 2016. *The blockchain phenomenon–the disruptive potential of distributed consensus architectures*. Technical Report. ETLA working papers.
[33] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*. 127–140.
[34] Alexander Mikroyannidis. 2020. Blockchain applications in education: a case study in lifelong learning. (2020).
[35] Alexander Mikroyannidis, John Domingue, Michelle Bachler, and Kevin Quick. 2018. Smart blockchain badges for data science education. In *2018 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–5.
[36] Alexander Mikroyannidis, Allan Third, Niaz Chowdhury, Michelle Bachler, and John Domingue. 2020. Supporting Lifelong Learning with Smart Blockchain Badges. *International Journal On Advances in Intelligent Systems* 13, 3 & 4 (2020), 163–176.
[37] Alex Murray, Scott Kuban, Matthew Josefy, and Jonathan Anderson. 2019. Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives* ja (2019).
[38] Alex Murray, Scott Kuban, Matt Josefy, and Jon Anderson. 2021. Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives* 35, 4 (2021), 622–641.
[39] Satoshi Nakamoto. 2008. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008).
[40] Tyron Ncube, Nomusa Dlodlo, and Alfredo Terzoli. 2020. Private Blockchain Networks: A Solution for Data Privacy. In *2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. IEEE, 1–8.
[41] Stefano Nocerino. 2021. A Review on the potential impact of Blockchain to the Accounting Profession.

[42] Jørgen Svennevik Notland, Jakob Svennevik Notland, and Donn Morrison. 2020. The Minimum Hybrid Contract (MHC) Combining Legal and Blockchain Smart Contracts. In *Proceedings of the Evaluation and Assessment in Software Engineering*. 390–397.
[43] Patrick Ocheja, Brendan Flanagan, Hiroshi Ueda, and Hiroaki Ogata. 2019. Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning* 14, 1 (2019), 1–19.
[44] Joon Park, Ruzanna Chitchyan, Anastasia Angelopoulou, and Jordan Murkin. 2019. A block-free distributed ledger for p2p energy trading: Case with iota?. In *International Conference on Advanced Information Systems Engineering*. Springer, 111–125.
[45] Mehrdokht Pournader, Yangyan Shi, Stefan Seuring, and SC Lenny Koh. 2020. Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. *International Journal of Production Research* 58, 7 (2020), 2063–2081.
[46] Max Raskin. 2016. The law and legality of smart contracts. *Geo. L. Tech. Rev.* 1 (2016), 305.
[47] Matti Rossi, Christoph Mueller-Bloch, Jason Bennett Thatcher, and Roman Beck. 2019. Blockchain research in information systems: Current trends and an inclusive future research agenda. *Journal of the Association for Information Systems* 20, 9 (2019), 14.
[48] Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald, and Andrew Le Gear. 2021. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management* 58, 4 (2021), 102584.
[49] Ashish Rajendra Sai, Andrew Le Gear, and Jim Buckley. 2019. Centralization threat metric. (2019).
[50] Mary Shaw. 2002. What makes good research in software engineering? *International Journal on Software Tools for Technology Transfer* 4, 1 (2002), 1–7.
[51] Alpen Sheth and Hemang Subramanian. 2019. Blockchain and contract theory: modeling smart contracts using insurance markets. *Managerial Finance* (2019).
[52] Hongyu Song, Nafei Zhu, Ruixin Xue, Jingsha He, Kun Zhang, and Jianyu Wang. 2021. Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information Processing & Management* 58, 3 (2021), 102507.
[53] Lars Stegeman. 2018. *Solitor: runtime verification of smart contracts on the Ethereum network.* Master's thesis. University of Twente.
[54] Nick Szabo. 1997. Formalizing and securing relationships on public networks. *First monday* (1997).
[55] Nick Szabo. 1997. The idea of smart contracts. *Nick Szabo's papers and concise tutorials* 6, 1 (1997), 199.
[56] L Thomas van Binsbergen, Lu-Chi Liu, Robert van Doesburg, and Tom van Engers. 2020. eFLINT: a domain-specific language for executable norm specifications. In *Proceedings of the 19th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences*. 124–136.
[57] Kevin Werbach. 2018. Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ* 33 (2018), 487.
[58] Yun Hui Xu. 2020. Cryptopoly: Using Ethereum State Channels for Decentralized Game Applications. (2020).
[59] Bello Musa Yakubu, Majid I Khan, Nadeem Javaid, and Abid Khan. 2021. Blockchain-based secure multi-resource trading model for smart marketplace. *Computing* 103, 3 (2021), 379–400.
[60] Liudmila Zavolokina, Manuel Schlegel, and Gerhard Schwabe. 2021. How can we reduce information asymmetries and enhance trust in 'The Market for Lemons'? *Information Systems and e-Business Management* 19, 3 (2021), 883–908.
[61] Lei Zhang. 2019. Consensus and Security in Canonchain.
[62] Peilin Zheng, Zibin Zheng, and Liang Chen. 2019. Selecting reliable blockchain peers via hybrid blockchain reliability prediction. *arXiv preprint arXiv:1910.14614* (2019).
[63] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. 2020. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems* 105 (2020), 475–491.
[64] Mirko Zichichi, Luca Serena, Stefano Ferretti, and Gabriele D'Angelo. 2021. Towards Decentralized Complex Queries over Distributed Ledgers: a Data Marketplace Use-case. In *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 1–6.

A ONLINE RESOURCES

Adhering to the good practices of open science and for ease of reading, detailed data such as the total set of articles evaluated or the reviewers' manual were stored separately in an open electronic address for reading: http://bit.ly/3AgMUGD.

Received 06 December 2022

Apêndice F

Analysing the Effectiveness of Honesty Stimulating Solutions in Online Decentralized Markets – An Agent-based Simulation Comparison

Analyzing the Effectiveness of Honesty Stimulating Solutions in Online Decentralized Markets – An Agent-based Simulation Comparison

Tiago Lucas Pereira Clementino[1*], José Antão Beltrão Moura[1] and Nataliia Neshenko[2]

[1]Dept. of Systems and Computation, Federal University of Campina Grande, Aprígio Veloso Avenue, Campina Grande, 58429-900, Paraíba, Brazil.

*Corresponding author(s). E-mail(s): tiagolucas@copin.ufcg.edu.br;
Contributing authors: antao@computacao.ufcg.edu.br;
nneshenko2016@fau.edu;

Abstract

Online transactions involve protocols of exchange of values where an active party usually prepays for goods or services. The passive party may act dishonestly and never deliver the paid for goods or services. Incomplete transactions cause multi-billion dollar losses annually just for e-Commerce. Centralized markets bypass this problem with a centralized intermediary auditor – e.g., Amazon.com. However, such a solution is not suitable for decentralized markets. For decentralized markets – e.g., OpenBazaar – literature and practice have typically adopted solutions built around security deposits, reputation systems, or decentralized arbitrators. This article carries out a comparison, by means of agent-based simulation (ABS), of such decentralized solutions in the literature and also, of our proposals for suitable combinations of their main features. One of the proposed combinations offers superior performance in terms of transactions completion rate (success), even with high rates of dishonesty among the population. The article contributes, through ABS applications, to the design and evaluation of decentralized transaction protocols in untrustworthy online environments.

Keywords: Decentralized Market, Economics, Honesty, Trust, Agent-based Simulation

1 Introduction

Online transactions are used for our daily activities that include but are not limited to shopping for goods, services or ordering food on the internet. Just for e-commerce, they are estimated to generate close to 50 trillion US dollars worldwide by 2030 (Global e-commerce market, 2024). A transaction may be seen as a protocol composed of a series of operations that establish an exchange of values of different natures involving two parties, an active party (buyer) that proposes the transaction and a passive party (seller) that accepts or rejects it. However, one of the parties – the active party – must usually assume the risk and carry out the value transfer operation before the passive party responds with its counterpart. At this point, this passive party has the chance to act dishonestly and not proceed with the transaction. The decision to take such a risk is known as the Buyer and Seller's Dilemma (Asgaonkar & Krishnamachari, 2019).

In fact, that is among the most common crimes affecting U.S. adults: 15% of Americans polled by Lydia Saad (2023), report someone in their household being conned to send money or giving access to a financial account. This problem caused record losses of US$ 10 billion in 2023 prompting the US Federal Trade Commission (FTC) to take action to protect the public (Federal Trade Commission, 2024).

A known solution to the Buyer and Seller's Dilemma – which is the business problem of interest here – is the mediation of a third centralized party that validates the operations and must rely on the trust of the other parties. This solution has worked satisfactorily enough in centralized markets where the State, an exchange office, a centralized application (e.g., amazon.com) or a banking institution perform the role of intermediary, guaranteeing delivery of the passive's counterpart. Previous solutions to the Buyer and Seller's Dilemma in decentralized markets usually incorporate costly preconditions that ensure the verification of all operations throughout the transaction protocol, which is not feasible for those transactions where any operation involved is non-verifiable (from now on, non-verifiable transactions) – e.g., real world services or payments in cash. Costly preconditions examples include synchronization of operations (Mamageishvili & Schlegel, 2020; Tsabary, Yechieli, Manuskin, & Eyal, 2021), trust assurance in any of the parties involved (Asgaonkar & Krishnamachari, 2019; Le et al., 2019), controllable digital content (Müller, Janczura, & Ruppel, 2020; Radhakrishnan, Ramachandran, & Krishnamachari, 2019; Zhang, Wei, Liu, & Liu, 2023) and payment protocols aimed at products with digitally verifiable authenticity (Pande, Mandolikar, & Shitole, 2022). Here, we seak an automated, decentralized technical solution for the business problem of interest.

The decentralized virtualization of non-verifiable events and values in real-world services and products poses challenges in maintaining decentralization that in turn, leads to the tendency to violate decentralization principles (Asgaonkar & Krishnamachari, 2019; Le et al., 2019; Mamageishvili & Schlegel, 2020; Müller et al., 2020; Pande et al., 2022; Radhakrishnan et al., 2019; Tsabary et al., 2021; Zhang et al., 2023). This limitation hampers the adoption of decentralized solutions in decentralized markets (Domingue, Third, & Ramachandran, 2019; Mikroyannidis, 2020; Mikroyannidis, Domingue, Bachler, & Quick, 2018; Mikroyannidis, Third, Chowdhury, Bachler, & Domingue, 2020; Ocheja, Flanagan, Ueda, & Ogata, 2019).

To address said challenges, this paper first conducts performance comparisons of existing literature solutions (even if they are incomplete) for the Buyer and Seller's Dilemma. Then, to bypass the solutions' preconditions, it proposes to combine their main features, composing new solutions as alternatives suitable to decentralized markets when operating with non-verifiable transactions. The proposal hinges on the hypothesis that stimulating honesty is enough to provide an acceptable rate of successfully completed transactions (i.e., the delivery of paid for goods or services). For that, the proposed solutions use one or merge two or more of the following features:

i. Decentralized arbitration, where a freely defined intermediary between the parties assumes the role of arbitrator (mediator) in eventual conflicts (Asgaonkar & Krishnamachari, 2019; Müller et al., 2020; Pande et al., 2022; Radhakrishnan et al., 2019);
ii. Web-of-Trust with (Zindros, 2016) and without feedback (Caronni, 2000), in which a network of trust is established around the agent as s/he participates in transactions or acts as an arbitrator;
iii. Categorization of transactions that allows the establishment of trust separately for each transaction category;
iv. Security deposits made to an intermediary, which may be an automatic protocol, as collateral for the amounts to be exchanged (Asgaonkar & Krishnamachari, 2019; Mamageishvili & Schlegel, 2020; Tsabary et al., 2021).

Performance evaluation and comparison in a decentralized market whose dynamics may be impacted by agents' fraudulent behavior driven by economic gains is a complex endeavor. Because of the flexibility it offers, here we develop and run an Agent-based Simulator (ABS) as an evaluation tool (Isherwood, Koehler, & Slater, 2023). The ABS-produced results provide evidence that the proposed solutions show satisfactory effectiveness, with the one using decentralized arbiter encouraged by the trust network without feedback significantly increasing the chance of transaction success. For example, in an environment with a dishonesty rate (i.e., the chance of a passive agent acting dishonestly) of 40%, the chance of success goes from 30% to 88.9%.

The study reported here contributes to market decentralization R&D efforts, and to Distributed Ledger Technologies (DLT) applications for fraud prevention protocols in online decentralized markets with non-verifiable transactions. This contribution is in terms of proposing and evaluating technical solutions for the business problem. Specific contributions of this study are two:

i. A comprehensive and exemplified application of ABS that can serve as support for guiding managers, IT professionals, and researchers interested in understanding, building, or applying fraud-fighting protocols to online decentralized markets;
ii. The provision of a synthesized basis, forming a body of knowledge for future reference by R&D efforts on the treatment of the Buyer and Seller's Dilemma in fully decentralized markets.

2 Related Work

As in most research, the first stage of this work consisted of a literature review that was conducted to elicit solutions evaluated in practice, for the Buyer and Seller's Dilemma.

The review was carried out from December 2023 to January 2024 and according to the PRISMA practices and recommendations (Page et al., 2021). The only acceptance criterion for labelling a given work "related" was: *the work's aims to overcome the Buyer and Seller's Dilemma by proposing solutions evaluated in real world applications for some business problem applying some protocol or model to encourage honesty (honesty incentive model).*

Results of this literature review, in terms of selected related studies, serve to steer and to base the proposal of combined solutions and their performance evaluation and comparison in the remainder of the article.

Here, the results are divided into three main classes of solutions:

i. Trust networks;
ii. Arbitration;
iii. Guarantee payments protocols.

These three classes are collectively and generally called Honesty Incentive Models. Here we investigate single models and combinations of models from more than one class. Our comparative experiment explores the major features of each model class.

2.1 Trust Network

The approach introduced by Duong-Trung et al. (2019), besides automatic conflict resolution, penalizes couriers or carriers who breach contracts based on a reputation system. In the literature there are other works that address decentralized solutions for Cash on Delivery (CoD) and address the Buyer and Seller's Dilemma in a similar way (AlTawy, ElSheikh, Youssef, & Gong, 2017; Asgaonkar & Krishnamachari, 2019; Tien et al., 2019), although all of them utilize a trust network associated to other models.

2.2 Arbitrator

Zindros (2016) introduces OpenBazaar, a decentralized online market that allows any user to act as a human arbitrator, but lacks a Web-of-Trust, relies on scarce feedback and exposes arbitrators' identities. Ha et al. (2019) employ blockchain and smart contracts to enhance the Cash on Delivery (CoD) protocol for e-commerce. Their approach ensures secure transactions and resolves the Buyer and Seller's Dilemma by imposing specific rules on players and utilizing smart contracts as intermediaries. Tsabary et al. (2021) introduced a similar solution called MAD-HTLC, which leverages blockchain miners as contract arbitrators.

Duong-Trung et al. (2019)'s comprehensive CoD model relies on smart contracts for automatic conflict resolution, eliminating the need for human intermediaries who, according to them, would consume more assets and time for the players involved. However and as already pointed out above, this approach includes an additional conflict resolution element, penalizing couriers or carriers who breach contracts based on a reputation system. According to the authors, the use of a Smart Contract as an arbiter associated with the reputation system, in addition to the infrastructure provided by decentralized technologies that implement the Smart Contract, is sufficient.

However, the absence of a human moderating intermediary limits the focus on digital goods (Zhang et al., 2023) and a reputation system without classification favors frequent negotiators (Arps & Christin, 2020) – CoD is an example o a non-verifiable operation, linking these works to our study.

2.3 Payment Guarantee

Le et al. (2019) introduce a CoD protocol for commercial delivery where drivers are required to mortgage a sum of money for guarantee. More over, an authentication system is used for drivers and a hash code identifies the products.

Tsabary, Manuskin, and Eyal (2022) introduce the concept of LedgerHedger, a two-party mechanism that ensures timely confirmation of transactions in smart contract protocols. LedgerHedger has the issuing player pay for a transaction in advance, and the other player agrees to pay a required fee, even if it exceeds the value of the transaction. This ensures that the transaction will be confirmed within a defined time frame. Asgaonkar and Krishnamachari (2019) also present a solution based on double guarantees. Such double guarantees, although effective, can make transactions unfeasible, especially when they are greater than the negotiated value (Tsabary et al., 2022).

Finally, the most complete model of payment guarantee protocols is provided by Schwartzbach (2022), where they present two main conclusions: it is not viable to provide a guarantee deposit model without any type of information about player behavior; and it is unlikely that a non-adaptable guarantee deposits protocol based on empirical rules will work. The mathematical approach presented seems the most complete.

Mamageishvili and Schlegel (2020) explored double guarantees in smart contracts, highlighting issues such as initial deposits required before contract signing, implicit costs including lost opportunities and the risk of forfeiture if the consensus protocol fails, and penalization discrepancies.

2.4 Discussion

The difficulty in virtualizing real-world services, cash and products in a decentralized manner is the core problem of non-verifiable transactions and leads most solutions to the Buyer and Seller's Dilemma to resort to preconditions that limit the application domain or violate the principle of decentralization (Asgaonkar & Krishnamachari, 2019; Le et al., 2019; Mamageishvili & Schlegel, 2020; Müller et al., 2020; Pande et al., 2022; Radhakrishnan et al., 2019; Tsabary et al., 2021; Zhang et al., 2023). Table 1 presents all solutions collected from the literature and identifies the preconditions applied by each one to avoid or reduce dishonesty. Such preconditions are diverse, but can be classified into four categories:

i. **Some level of centralization**: Models appeal to centralization to verify the transaction in some level, overcoming the difficulty of ensuring trust without complete information;
ii. **Authentication**: Identifies users to intimidate the dishonest ones with legal repercussions;
iii. **Digital verification of delivered products**: In a decentralized environment it is applicable only to products that may be completely digitalized;

Table 1 Solutions from the Literature for the Buyer and Seller's Dilemma

Reference	Model	Centralization	Authentication	Digital Verification	Feedback
Le et al. (2019)	Guarantee deposits	✓	✓	✓	
Tsabary et al. (2022)	Guarantee deposits			✓	
Asgaonkar and Krishnamachari (2019)	Guarantee deposits, Trust network			✓	✓
Schwartzbach (2022)	Guarantee deposits				
Ha et al. (2019)	Arbitrator			✓	
Tsabary et al. (2021)	Arbitrator			✓	
Duong-Trung et al. (2019)	Arbitrator, Trust network	✓	✓	✓	✓
Tien et al. (2019)	Arbitrator, Trust network	✓	✓		✓
AlTawy et al. (2017)	Arbitrator, Trust network			✓	

iv. **Feedback**: It is used to build trust, but is more susceptible to fails because in decentralized environment it may be an easy prey to forgery.

Features used for avoiding such preconditions are used to compose the models to be compared here and described in more details in Section 3. As one can see from Table 1, none of the solutions in the literature implements trust network in isolation. Without such trust network, some other kind of behavior inference must be provided (as smart contract oracles, for example).

The current investigation complements the above works by integrating two or more of their features as "components" of the solutions it proposes to ameliorate deployment and operations in decentralized online markets. Further, it carries out an ABS effectiveness evaluation and comparison of the proposed solutions and the ones in the above cited literature.

Although ABS applications to honesty in online decentralized markets appear scantier than applications to other fields, some constructs for those other fields may serve us here also. For instance, the constructs presented by Dwarakanath, Vyetrenko, Balch, and Oyebode (2023) to address the impact of (the lack of) transparency on network traffic and stock exchanges may be adapted to our modeling of the effects of (the lack of) honesty on decentralized markets and of the benefits of our proposed solutions.

Nærland, Müller-Bloch, Beck, and Palmund (2017) present a similar work where they propose design principles for applications that aim to mitigate the transactional risk in decentralized environments. Auinger and Riedl (2018) carried out a literature review based on an analysis of text passages related to "trust". Their results point to "Substitution of intermediaries and trust" as one of the top three terms related to

trust in blockchain studies. These works are related to the one presented here as they study risk in full decentralized environments or the need to foster truly decentralized environments.

Clementino and Moura (2024) carried out a study similar to the one here and with the same purpose of evaluating models to encourage honesty with the aim of circumventing Buyer and Seller's Dilemma. However, such study was based on a historical trace dataset extracted from OpenBazaar. As such, it particularizes conclusions with insights being applicable to OpenBazaar only – which is no longer operational. Here our ABS experiment provides for more comprehensive observations.

To facilitate discussing our ABS experiment it is useful to first, briefly review some fundamentals for a more detailed formulation of the problem and further characterization of the proposed solutions

3 Fundamentals

The proposal of solutions to promote honesty in decentralized markets is underpinned by three main model features:

i. Security deposits;
ii. Web-of-Trust;
iii. Decentralized Arbitration.

3.1 Security Deposits

The collateral deposit protocol is built upon the research conducted by Schwartzbach (2022) as outlined in his publication on payments. Schwartzbach presents a model for a decentralized market reliant on non-verifiable transactions.

3.2 Web-of-Trust

Originally focused on a peer-to-peer network, Web-of-Trust establishes the authenticity of connections between public keys and their owners. Over time, users accumulate keys from individuals they trust, forming a decentralized trust network without a centralized certificate authority. Legitimacy is achieved through the accumulation and redistribution of third-party certificates, resulting in a flexible, decentralized, and fault-tolerant public key network verified through consensus among users (Caronni, 2000).

For transactions with non-verifiable operations, the Web of Trust model can provide trust between buyers and sellers who have never had direct interactions based on the experience of those with whom they interacted separately. Zindros (2016) utilizes a similar trust network, but based on scarce voluntary feedback, which slows the progress of the trust network. Zhang et al. (2023) apply a similar model. Our comparison analysis both Web-of-Trust models, with and without feedback.

This reputation model works well with the moderation of transactions using reliable decentralized arbitrators, since, given a population Q from a few transactions $S' << Q$, it is already possible to identify arbitrators that have the trust of the agents involved. This is because a small percentage of the population $Q' << Q$ tends to act as arbitrators.

3.3 Decentralized Arbitration

For comparison purposes between solutions, this article applies an arbitration strategy similar to that used by Zindros (2016), replacing the reputation system of the arbitrators by Web-of-Trust reputation networks.

4 Problem Formalization and Solution Specifications

This work evaluates solutions aimed at encouraging honesty in potentially dishonest agents in transactions with non-verifiable operations. Given all possible conclusions for a given transaction, such solutions aim to avoid just one: non-delivery by the passive agent (seller) of compensation to the active party (buyer) who took the initiative and paid for the completion of the transaction in advance. Here we only deal with decentralized solutions, as the practice demonstrates that the use of a reliable centralized mediator is able to encourage honesty enough for the centralized market as a whole to prosper.

For ease of reference and thus, reading convenience of the contents ahead, all acronyms, symbols and terms used herein are collected in Table 2.

4.1 The Buyer and Seller's Dilemma (Problem)

In a negotiation scenario, e.g. in an e-commerce transaction, it is natural that each party prioritizes its own interests, making a dishonest behavior to be perceived as an advantageous option, at least in the short run (in the long run, it is likely that the law will catch up with dishonest agents). In this scenario, involving an active agent and a passive agent, the active agent initiates the transaction and bears the risk of delivering its value first, while the passive agent receives the value and must decide whether to reciprocate honestly or not. Such a scenario reflects game theory's Nash Equilibrium principle (Nash Jr, 1950), where a player can adopt a strategy ensuring the best possible outcome regardless of others' actions. Hence, the problem of interest here may be formulated as a game as in Definition 1.

Definition 1. *Consider the Buyer and Seller's Dilemma as the following tuple* $G = \{P, Q, T, (b_0, b_*), (\lambda_i(b) \,|\, i \in Q, b \in Q^P), (\gamma^t(b_k(i), b_l(j)) \,|\, \forall_{b_k,b_l} \in P$ *, and* $\forall t \in T \; \forall i, j \in Q)\}$*, where:*

i. P *signifies the collection of values or products exchanged within the game.*

ii. Q *represents the group of agents involved in negotiations, typically consisting of two agents, though we will generalize it to* $|Q|$ *for flexibility.*

iii. T *referrers to all time steps.*

iv. $(b_0, b_*) : P \times Q$ *represents the initial set of values* b_0 *(e.g., for the seller, the original set of values are his goods and his cash balance) and the expected final set of values* b_* *(e.g., again for the seller, the final set of values would be the remainder of his goods, his previous cash balance plus the amount paid for all items negotiated) for a given trading agent. Here,* b_k *signifies the state of an agent at lifetime* k*, equals the time step* t *minus the time of agent creation.*

v. $\lambda_i(b)$ *is an interest function of a given agent* $i \in Q$ *over a set of values* $b \in Q^P$ *such that:* $\lambda_i(b_0(i)) \leq \lambda_i(b_*(i)), \forall i$ *(i.e. every agent* i *will always prefer its final*

Table 2 Notation table

symbol	Description
Q	Set of negotiating agents
q	A negotiating agent
S	Set of transactions
G	Buyer and Seller's Dilemma as an extensive-form game
P	Set of exchanged values/products
p	A value/product
T	referrers to all time steps.
i, j	representations of agents
k, l, n, t	representations of time steps
b	the state of a given agent
γ	The strategy (operation)
λ	The interest function
H	A decentralized honesty incentive solution
ζ	A behavior inference function (a reputation system, for instance)
η	Some ensuring transaction model like decentralized arbitration or guarantee deposits
α	An action function
M	The agent's inventory for each of the value categories
ν	The goal of any agent for each value category
L	The life in time steps of any agent
C	Set of value/product classes
c	A value/product class
V	The validation of the ABM according to Marks (2007)
U	The output of the ABM
Z	The real output of the OpenBazaar system
R	$U \cap S$
m	A ratio scale metric defined according to viability and functionality
X	The event of a given agent trusting another
h	The probability of a given product already passed on by a given agent reaching the inventory of another
χ	The real honesty of a given agent
ψ	A random function

expected set of values to the initial set) and $\lambda_i(b_*(i)) \leq \lambda_i(b_0(i) \cup b_*(i)), \forall i$ *(i.e. every agent will prefer to act dishonestly and accumulate both the expected final set and the initial set of values).*

vi. The strategy (operation) $\gamma^t(b_k(i), b_l(j)) = (b_{k+1}(i), b_{l-1}(j))$*. Such strategy establishes that whenever a player goes from a worse state* $b_k(i)$ *to a better one* $b_{k+1}(i)$*, another agent must necessarily go the other way, going from a better state* $b_{k+1}(j)$ *to a worse one* $b_k(j)$ *with each operation,* $\lambda(b_k < \lambda(b_{k+1})$*. This means that the active player needs to risk going lower in his balance to initiate a transaction with the intention of improving it at the end of this transaction.*

Here, the transactions of the decentralized market will be modeled as a game as formulated above and its strategy (operation) γ will explain the inner workings of the ABS when mimicking the (inter)actions of agents according to their functioning under the dynamics of a given applied solution.

4.2 Proposed Solutions Specification

This work proposes solutions to encourage honesty among agents in non-verifiable transactions. To this end, one or more features from the literature (see Section 3) are combined in each proposed solution. The collection of said multiple- and single-featured solutions form a super set of honesty-incentive solutions that include features of honesty inference or guarantee for non-verifiable transactions. The performances of the solutions in this super set are then compared and ranked according to their effectiveness (i.e., their capacity to stimulate honesty and hence, improve transactions completion rate – "success"). Table 3 specifies the features of all solutions in the super set being considered.

Table 3 Proposed Solutions (A, B, C, E and G) and Solutions from the Literature – D (Schwartzbach, 2022); F (Zindros, 2016); and, H (Asgaonkar & Krishnamachari, 2019; Mamageishvili & Schlegel, 2020; Tsabary et al., 2021).

	Solutions								
Solution features	A	B	C	D	E	F	G	H	I
Arbitrator	✓	✓			✓	✓			
Categories	✓		✓		✓		✓		
Security Deposit			✓	✓			✓	✓	
Feedback					✓	✓	✓	✓	

'A' is the solution that combines an auditor and differentiation of the honesty of each agent by category of values negotiated, so a given agent can trust another for one type (category) of transaction but not trust the same agent for another type (category) of transaction. 'B' uses only a trusted and decentralized intermediate auditor in its solution. 'C' uses security deposits and differentiates trust between agents by categories. 'D' uses only security deposits to secure the solution. 'E' uses an intermediary auditor and trust based not on previous relationships, but on feedback given by agents regarding the honesty of others, in addition to classifying the honesty of agents by transaction category. Following the same reasoning we have the solutions 'F', 'G' and 'H'. 'I' offers no features to deal with dishonesty. It is included here to gage potential "absolute" gains by the other solutions (see Table 3). All solutions in Table 3 follow Definition 2.

Definition 2 (Generic Solution)**.** *A decentralized honesty incentive solution is represented generically as* $H = \{G, Q, T, \zeta^t(i,j) \,|\, \forall t \in T \text{ and } (i,j) \in Q \times Q, \eta^t(G,\zeta) \,|\, \forall t \in T\}$*, where:*

i. G is the game according to Definition 1.

ii. ζ^t *as an honesty inference function (a reputation system, for instance), where* $\zeta^t(i,j)$ *defines the confidence of agent* i *in agent* j *according to state of* i *at time* t*.*

iii. η^t *represents some ensuring transaction model like decentralized arbitration or guarantee deposits, where* $\eta^t(G, \zeta(i,j))$ *returns a raw set of operations* $\{\gamma_0, ..., \gamma_n\}$ *(see Definition 1) if* i *trust on* j *or some ensuring transaction model according to state of* i *at time* t*, which culminates in a different set of operations* $\{\gamma_0^{'}, ..., \gamma_m^{'}\}$*.*

Thus, each solution in Table 3 includes one or no transaction assurance model η *(security deposits or decentralized arbitration) and one or no honesty inference model* ζ *(Web-of-Trust with or without feedback, based on classified or non-classified transactions).*

5 Simulation: Performance Evaluation and Comparison

5.1 Simulation Methodology

This work evaluates and compares, through simulation, solutions in the literature for the Buyer and Seller's Dilemma or problems that involve the same dilemma indirectly. Moreover, we combine features of these solutions to incentivize honesty instead of trying to verify operations. These combinations comprise new solutions for the Buyer and Seller's Dilemma (see Table 3).

The hypothesis to be tested here – by applying Simulation Modeling Method, points to the fact that it is possible to encourage honesty using decentralized solutions even in the presence of non-verifiable operations. The objective is to identify superior honesty incentivizing strategies that, even without verifying the operations, are capable of rewarding and encouraging honesty in a population of agents with diverse categories of values exchanged and honesty profiles. To this end, Agent-Based Simulation (ABS) is used to record the effectiveness of each agent separately and of the population as a whole through multiple simulations runs for different configurations of mutually exclusive solutions (see Table 3) at different honesty rates.

5.2 Simulation Design

With the aim of simulating decentralized markets where agents produce and trade values, this experiment used Agent-Based Simulation (ABS). In addition to reproducing such interactions, parameters such as honesty, memory, risk, bankruptcy and success were incorporated.

The AB model presented here was developed based on Fagiolo, Moneta, and Windrum (2007) work, which establishes that such kind of simulation must be:

i. **A bottom-up perspective** Properties of an economics nature are inferred based on the outcome of micro dynamics involving agents.

ii. **Heterogeneity** Agents are prosumers with different production outcomes, although all agents consume all types of products available for trade as input.

iii. **Bounded rationality** Where agents are restricted trading with and recognizing its local neighborhood.

iv. **Networked direct interactions** An agent's decisions directly depend, through adaptive expectations, on the past choices made by other agents in the population.

The simulation environment consists of a 256×256 2D Grid, containing an initial total of 100 agents that may grow to a maximum of 1,000 agents as the simulation run progresses. For illustration observe the grid's snapshot in Figure 1 where agents can only move to a neighboring location at a time. At any given time step of an agent's life cycle, an agent either produces one unit of one type of value that may be negotiated with other agents, or negotiates items already in her/his inventory to obtain other values that s/he is not capable of producing. The ABS' clock ticks in time steps with one time step equaling the time interval during which all agents conclude a transaction (i.e., negotiation of a value) or produce a value item for their inventories.

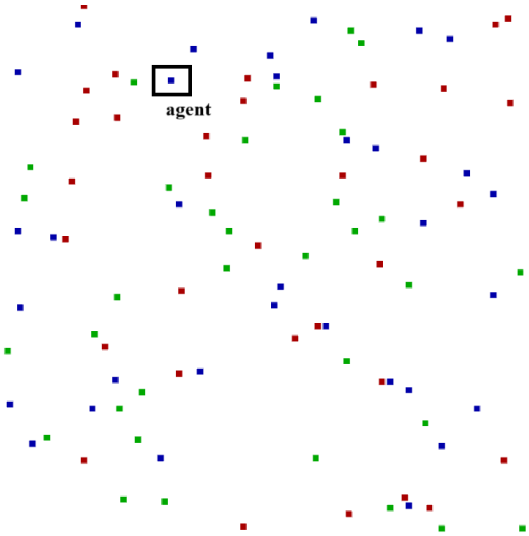


Fig. 1 Simulation grid where each colored point is an agent – as highlighted by black frame – who engages in online trading with its neighboring agents.

5.2.1 Agents

Definition 3. *In the ABS, an agent is modeled as* $q = \{c_q, (b_0, b_*), \alpha^t\}$*, where:*

i. c_q *as the value which the agent can manufacture.*

ii. (b_0, b_*) *are the initial and final desirable states respectively. Consider a state* $b = \{\nu_C, (x, y)\}$*, where* ν_C *represents a set of values (items) in the inventory, one for each value category* $c \in C$*, and* (x, y) *refers to a position on the 2D grid.*

iii. α^t *represents an action function at time step* t*, where* $\alpha^t(b_n)$ *returns a random movement to some adjacent position and a manufacturing* p *or transaction* η *(see Definition 2) with some other adjacent agent, depending on the state* b_n*.*

5.2.2 Simulation Main Procedure

We define economic success in the simulated environment as the ability of agents to produce and negotiate values of different categories, achieving their objectives without going bankrupt. The objective of a given agent is to accumulate an inventory $M \geq \nu_*$ for each of the value categories – where ν_* is the goal of any of the agents for each of the value categories. If the agent achieves this goal, as a reward, it duplicates itself. If at the end of L time steps the agent does not reach this goal ν_* for all value categories, this agent is removed from the simulation (bankruptcy).

If the population of agents reaches the maximum total number of agents (1,000), the simulation is stopped, and the agent's economics as a whole is declared successful for that particular run. Similarly, when all agents are removed due to bankruptcy, the simulation run is stopped, and the scenario is recorded as a simulation failure. Each scenario was run 1,000 times. A scenario is a simulation configuration that represents one of the solutions under analysis (see Table 3) using a specific set of parameter values. Each simulation run consists of a repetition of a given scenario. Even with all the same parameters, two simulation runs may return different outcomes because two agents only transact if in adjacent positions in the Grid, and the movements of an agent in the Grid are random. The pseudo code in Algorithm 1 describes main flow of the simulator in more detail.

Exchanging values is the equivalent to the exchange of products and cash in transactions and whose value being transacted defines the corresponding transaction categories. The definition of honesty used in this simulation is weighted according to the categories of transactions in an attempt to simulate a real society, where an individual behaves differently for different types of transactions. A transaction consists of a set of two value exchange operations in case of success (payment and delivery of product), a unilateral operation by the active agent in case of passive agent's dishonesty, or the same operation, its refund and a remuneration to the arbitrator if s/he avoids the dishonest attitude of passive agent (we assume this remuneration to consist of one third of the original payment by the active agent).

5.2.3 Agent-Based Model (ABM) Validation

Marks (2007) presented a framework for validating Agent-Based Models (ABMs) based on real-world sample data. The present simulation experiment replicates a decentralized online market that in itself has little availability of historical data, especially data associated with large-scale initiatives. However, Arps and Christin (2020) analyzed data from one such market called OpenBazaar. Here, we use this data for the validation of our ABS.

Note, however, that since no individual decentralized market is simulated here, but rather general and recurring situations in any decentralized market, comparing record by record between simulated and real-world data does not make sense. Instead, a representative property such as the rate of failed transactions is compared (unsuccessful transactions from the OpenBazaar dataset mean its associated buyers, as indicated in logged text messages, failed to receive the product). Equation (1) represents the validation of the ABM according to Marks (2007).

Algorithm 1 Main Procedure.

Require: $|Q| = 100$ ▷ Ensures that the initial population of agents Q has 100 agents
Ensure: $GRID \Leftarrow Q$ ▷ Spreads the agents around the 2D GRID
1: $t \Leftarrow 0$ ▷ Line 1 sets the initial time step $t = 0$
2: **while** $|Q| \geq 0$ & $|Q| \leq 1000$ **do** ▷ Line 2 checks if the total population $|Q|$ is zero, bankrupt, or greater than 1000, success
3: $i^t \Leftarrow \text{getAgent}(t, Q)$ ▷ Line 3 gets an agent i^t from Q, where this 't' means that such agent is in time step t
4: **while** $i^t \neq \varnothing$ **do** ▷ Line 4 checks if the agent i^t is empty, if so, it means that there is no more agents at time step t
5: $i^{t+1} \Leftarrow \alpha^t(b_i)$ ▷ Line 5 calls the action function α at time step t for agent state b_i, according to agent Definition 3, and returns the agent at the next time step $t + 1$
6: **if** $(t + 1) - t_0^i \geq L$ **then** ▷ Line 6 checks if the agent time step less the initial time step of the agent t_0^i is greater or equals to the max lifetime L of any agent, at the end of which i needs to have sufficient inventory to duplicate itself or be removed
7: $Q \rightarrow i$ ▷ Line 7 removes bankrupted i from the population Q
8: **else if** $\nu_C^i \geq \nu_*$ **then** ▷ Line 8 checks if the inventory of agent ν_C^i is greater than max ν_* for all exchangeable value categories
9: $\nu_C^i, t^i \Leftarrow 0, t_0^i$ ▷ Line 9 sets agent inventory ν_C^i and lifetime t^i back to zero
10: $Q \leftarrow i$ ▷ Line 10 reinserts i to population of agents, duplicating it
11: **end if**
12: $i^t \Leftarrow \text{getAgent}(t, Q)$ ▷ Line 12 gets a new agent from population Q at time step t
13: **end while**
14: $t \Leftarrow t + 1$ ▷ Line 14 goes to the next time step
15: **end while**
16: return $\Leftarrow |Q| \neq 0$ ▷ Line 16 returns success if $(|Q| \neq 0)$, or otherwise bankrupt, if $(|Q| = 0)$

$$V \equiv m(R) * \left(\frac{v}{m(U)} + \frac{1 - v}{m(Z)} \right) \tag{1}$$

The closer V is to 1.0 the better the ABM, where U represents the output of the ABM, Z represents the real output of the OpenBazaar system, R represents $U \cap Z$ which here means the proximity between the output of the real system and the output of the ABM based on all honesty incentive models analyzed here at each step in time (a publicly available R script is used for this, please refer to Subsection "Code Availability" (in Section "'Declarations"), and $v \in [0.0, 1.0]$ is a constant that describes the tradeoff between precision and completeness – here $v = 0.7$ in order to prioritize completeness despite precision, because it is a more general simulation model and, as a general model, completeness is a stronger property compared to precision. The function $m()$ represents a ratio scale metric defined according to viability and functionality.

Using the unsuccessful transactions rate as $m()$, we have: 9,901 unsuccessful transactions per 124,035 total transactions in ABM (U), 113 unsuccessful transactions per 1,202 total transactions in OpenBazaar (Z) and 43 unsuccessful transactions and 611 total transactions for $U \cap S$. Based on such numbers, one gets (Equation 2):

$$V \equiv m(R) * (\frac{v}{m(U)} + \frac{1-v}{m(Z)}) = \frac{43}{611} * (\frac{0.7}{\frac{9901}{124035}} + \frac{1-0.7}{\frac{113}{1202}}) = 0.842 \quad (2)$$

So, the completeness/precision of the present simulation is 0.842, when compared to real data of OpenBazaar. Since it is close to 1.0, one may validate the model (Marks, 2007).

5.2.4 Implementation

North et al. (2013) provided an overview of available Agent-Based Simulation (ABS) implementation tools, influencing the selection of Repast Simphony (Collier, 2003) for this work. Repast Simphony is a Java-based modeling system and toolkit supporting the development of highly flexible interaction agent models for workstations and computing clusters (Collier, 2021). It allows model development through statecharts in Groovy or Java.

For data analysis, the functional language R was selected due to its rich diversity of graphic libraries. Both the source code in Java and R are available online in Github repositories [1], according to Subsection "Code Availability" (in Section "'Declarations").

5.2.5 Trust Distance

In Web-of-Trust, trust is based on accumulated experiences with agents near the one whose honesty is being estimated. Proximity calculation involves searching for possible paths in the transaction-generated graph between two agents or between them and other agents. The partner with the greatest number of paths is considered the most reliable. If an agent has honored its commitments in the past, tradable values it negotiated circulate in the network, indicating its honesty for a specific transaction category, similar to how public key validity propagates in a Web-of-Trust for key verification. As transactions progress, agents accumulate lists of potentially honest peers, with more exchangeable values included in such list for a given agent increasing the likelihood of such agent being honest. Such an implementation model, although it is an incomplete solution, better simulates real society since an individual does not have access to everyone's opinion about a given person, but only those with whom s/he interacts. Similarly, a given agent only has information about other agents whose transferred values have already been in their possession.

The algorithm summarized above identifies potential paths between two agents in the trust graph using an adapted version of GroupRep (Tian, Zou, Wang, & Cheng, 2006). GroupRep is chosen for its effective representation of trust relationships that naturally arises between individuals in a society and because it is suitable for an environment where two agents rarely interact more than once throughout their lives.

[1] https://www.github.com/

An alternative implementation of the Web-of-Trust model compared here works similarly, but relying on some form of feedback instead of direct interactions (Werthenbach & Pouwelse, 2022).

5.2.6 Honesty

Based on the presented definition of trust distance, we can describe the event of a given agent trusting another as the event X_{ij} that anyone of the products passed on by this agent j was in possession of agent i as:

$$X_{ij} = \bigcup_{k \in M_x(j)} h_{kj}$$

Where i represents the agent who must decide to trust or not and j represents the agent whose honesty is under suspicion. M_x represents the set of products already passed on by j of class c, and k refers to one of these products. In turn, h_{kj} refers to the probability of a given product k already passed on by j reaching the inventory of i. However, gaining the trust of another agent by itself does not necessarily mean the other agent is honest. The function that defines the real honesty of a given agent j for a given transaction class c is defined according to equation (3).

$$\chi_c(j) = \begin{cases} 1 & \text{if } \psi > \text{MAX}(1-g, \delta) \\ 0 & \text{else} \end{cases} \tag{3}$$

Where ψ defines a random function that returns a number $n \in [0, 1]$, MAX is also a function that returns the largest value of its two parameters, g is a constant $g \in]0, 1[$ defined in the simulation parameters and which represents the honesty rate of the population and $\delta \in]0, 1[$ is a factor defined by equation (4).

$$\delta_c(j) = \frac{\frac{t}{L}}{2} + 1 - \frac{\frac{\nu_c(j)}{\nu_*}}{2} \tag{4}$$

Where t is the time step in the lifetime of an agent in which the transaction occurs and L is the total lifetime of the agent at the end of which the agent must be eliminated if it has not yet reached the inventory target $\nu(j) > \nu_*$, where ν_c is the function that describes the inventory of a given exchanging value c and ν_* is the total sufficient for the agent to duplicate itself. Exchanging values would be equivalent to the products and cash exchanged in transactions, and which define their categories.

In summary, an agent's honesty is a Boolean function that has a $1 - g$ chance of being true at the beginning of this agent's lifetime. The simulation assumes that as this agent's lifetime progresses, this chance is influenced by the tensions experienced by such agent – as it may happen in the life of a human being, e.g.: the smaller the inventory of the product to be traded, the greater the chance of the agent to act dishonestly. Similarly, it is also reasonable to assume that the lower agent lifetime, the greater the chance of this agent acting dishonestly.

6 Results

For each solution in Table 3, the population's performance, the success of the simulated economy and the effectiveness of the solutions in avoiding unsuccessful transactions are presented.

6.1 Format and Metrics

The dataset resulting from multiple runs of the ABS comprises two distinct tables: one containing data for each final record of every run, and the other containing a random sampling of various sequential states of the agent population throughout the simulation. The table documenting final records of each simulation run has as result only one key field, a Boolean indicating the success or failure of each simulation (based on whether all agents perish or not, before the completion of the simulation run).

Similarly, the table capturing partial simulation records throughout the process includes three primary fields: a proportional balance of unsuccessful transactions up to that point, the total balance of potentially unsuccessful transactions that were avoided by the employed solution, and the proportional balance of successful transactions. Over the course of the entire experiment, the simulation was run 81,000 times for nine distinct honesty rates $\{0.1, 0.2, .., 0.9\}$.

Analysis of the data revealed a density curve resembling a normal distribution for the population's average success rate. Statistical inference, employing confidence intervals of 95% certainty level, was utilized to assess the success of the population and the diversity of agents. Furthermore, a Spearman correlation analysis was conducted to examine the relationship between the total number of avoided unsuccessful transactions and total failures at each simulation time step, across the various tested solutions.

6.2 Economics Performance

In total, 63% of simulation runs resulted in success for the population. The configuration 'A' of Table 3, achieved 74% success across the entire experiment, and the configuration 'I' without any form of transaction validation achieved 49% success. A complete picture of the performance of each simulation configuration is presented in Figure 2.

Examining Figure 2, none of the configurations show any success for honesty rates less than or equal to 0.2 (20%), while all exhibit perfect performance (100% success) for honesty rates greater than or equal to 0.7 (70%). The competition range between models is confined between 0.3 (30%) and 0.6 (60%), indicating potential for optimizing transaction validation models with non-verifiable operations. Within this range, configuration 'A' displays significant dominance over the others. This configuration relies on a decentralized Web-of-Trust verification arbiter without feedback and transaction classification (see Table 3). It suggests the existence of a transaction validation model capable of effectively encouraging agents' honesty with a spontaneous honesty

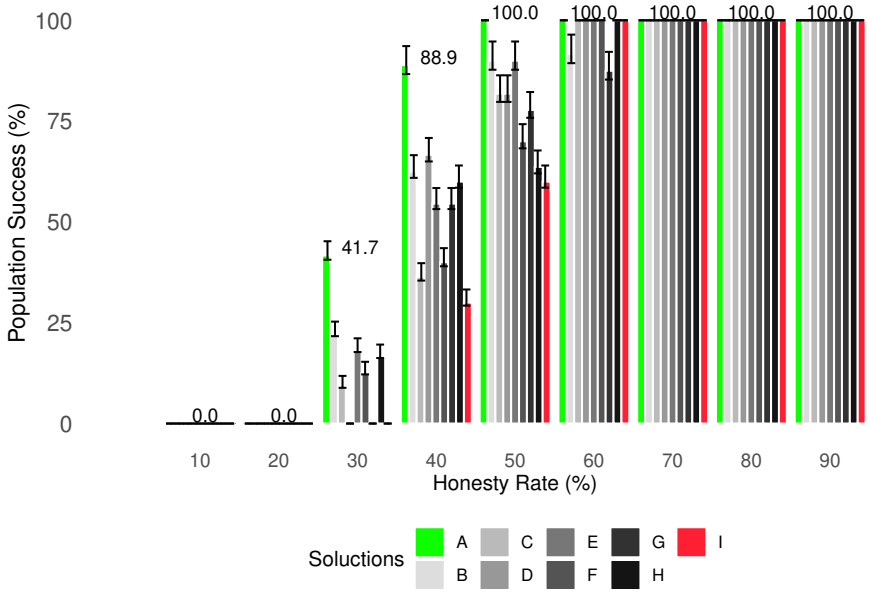


Fig. 2 Population success estimation for each compared solution in Table 3.

rate equal to or greater than 30%. For an uncluttered Figure 2, success results were omitted from the figure, except for solution 'A' [2].

6.3 Population of Agents at Every Time Step

To analyze the progression of the population, random samples of the simulation state were recorded at each step. Although the agents operate in a distributed manner, each complete cycle of actions of all agents receives a sequential integer identifier that will be used to measure time throughout the simulation (time step). We took a random sample of 1000 state records from the simulation run throughout these time steps to evaluate the evolution in the total number of successful transactions and unsuccessful transactions avoided by each of the applied solution (see Table 3).

Figure 3 highlights the effectiveness of each solution in encouraging honesty through the Spearman correlation between the major "Successful Transactions", "Unsuccessful Transactions" and "Avoided Unsuccessful Transactions' " at 40% honesty of the population, where the results were more diverse for each model (see Figure 2). Note that the highest correlations between successful and successfully transactions avoided occur in model 'A', the solution with better results, and in models 'E' and 'F' that function somewhat like it (see Table 3). In the other models, spurious correlations occur with successful and avoided unsuccessful transactions with unsuccessful transactions. In the 'I' model, which does not have any form of validation, successful and unsuccessful transactions are symmetrically opposite, which serves as evidence of the correctness of the analysis.

[2]For more details on the omitted results, please examine Table A1.

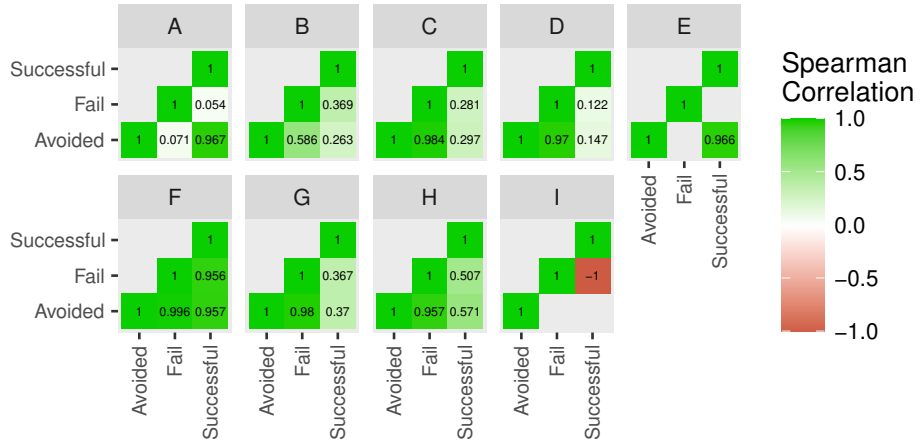


Fig. 3 Spearman correlations matrix between successful, failed and avoided unsuccessful transactions at an honesty rate of 40%. The figure has nine correlation matrices, one for each solution in Table 3. Each cell of the matrices has a color gradation from red to green representing the Spearman correlation between such transaction metric: 'Transaction **Successful**', 'Transaction **Fail**', and 'Transaction Fail **Avoided**'.

6.4 Limitations

This article deals with a simulated experiment, which in itself limits the use of its results to direct future actions and cannot be taken as definitive results. More concrete results depend on experiments in a real environment. Other limitations include the reliance on heuristics to simulate human behavior (e.g. the chance of agent dishonesty increasing with proximity to bankruptcy and decreasing with fuller inventory). Introducing more intelligent agents could potentially address this limitation.

7 Conclusion and Future Work

The findings from this study highlight the ongoing challenge of comprehensively validating operations in real-world transactions in decentralized markets. The study introduces a lightweight, Agent-Based Simulator (ABS) to evaluate and compare the performance of honesty stimulation strategies to be embedded in distributed ledger protocols. Through simulated experiments, the proposed 'A' solution in Table 3 emerges as the most effective in promoting honest behavior in markets relying on non-verifiable transactions. Notably, ABS results indicate that 'A' can stimulate honesty satisfactorily with a high degree of confidence, particularly when honesty rates are in the range of 40-50%, at 95% confidence. However, as honesty rates drop, the success rate diminishes, reaching zero for honesty rates equal to or lower than 20%. This result seems to indicate that in a highly dishonest scenario, one will be better off avoid doing business altogether in such scenario for no solution seems to make agents behave honestly. Surprisingly, when honesty rates grow beyond 60%, it may be as effective and simpler or more economical (in computational terms) to just do "nothing" (solution

Table 4 Advantages and disadvantages of each model

Solution	Overview
A	Best solution in all honesty ranges evaluated (see Figure 2) and best solution overall (mean 70.067, calculated from the numbers presented in Table A), with best correlation between successful transactions and avoided unsuccessful transactions (see Figure 3).
B	It stands out neither positively nor negatively.
C	It stands out neither positively nor negatively.
D	It stands out neither positively nor negatively.
E	Although it is not the best solution, nor the second best solution in any of the honesty ranges evaluated (see Figure 2), it is the second best solution overall, achieving an average of 62.52 (according to Table A), and showed consistency in the correlation between success and avoided failures, as shown in Figure 3.
F	Although it is not the best solution, it is a good solution overall, obtaining an average of 58.05. However, although the correlation between success and avoided failures is high, as shown in Figure 3, spurious correlations between failures, success and avoided failures suggest abnormal effects that deserve better future evaluation.
G	It stands out neither positively nor negatively.
H	It stands out neither positively nor negatively.
I	Worst observed solution, which is expected since it does not implement any transaction guarantee model.

'I' in Table 3) – meaning even "crook agents" will tend to follow the crowd (who is mostly composed of honest agents).

From the correlation graph (see Figure 3) and the results for each honesty range (see Figure 2), Table 4 provides an overview of the results for each solution tested. Note that the best solutions A, E and F have only arbitration in common, which indicates a good cost-benefit relationship between this feature and the incentive to honesty.

The findings of the article contribute to illustrate the support of ABS to the development and prototyping of decentralized markets. To do so, this work proposes as future work an effort to generalize the simulator presented here in order to be used in a wider decentralized protocol prototyping domain.

Despite the consistency of the results, the study underscores the persisting challenge in validating transactions involving non-verifiable operations within decentralized markets. This finding emphasizes the ongoing nature of the problem and the need for further research and innovative solutions in this domain.

Albeit the above gap in research results, the findings reported here contribute to Blockchain and DLTs applications specifically in the field of fraud prevention protocols for online decentralized and anonymous markets dealing with non-verifiable transactions. The main contribution of this study is the provision of a synthesized basis, forming a body of knowledge, for future reference, development and research on the treatment of the Buyer and Seller's Dilemma in full non-verifiable, anonymous and decentralized markets.

Appendix A Supplementary Table About Population Success

Table A1 Population success (%) estimation for each compared solution, as illustrated in Figure 2

	Honesty Rates								
Algorithms	10%	20%	30%	40%	50%	60%	70%	80%	90%
A	0.0	0.0	41.7	88.9	100.0	100.0	100.0	100.0	100.0
B	0.0	0.0	22.2	62.5	90.0	91.7	100.0	100.0	100.0
C	0.0	0.0	9.1	36.4	81.8	100.0	100.0	100.0	100.0
D	0.0	0.0	0.0	66.7	81.8	100.0	100.0	100.0	100.0
E	0.0	0.0	18.2	54.5	90.0	100.0	100.0	100.0	100.0
F	0.0	0.0	12.5	40.0	70.0	100.0	100.0	100.0	100.0
G	0.0	0.0	0.0	54.5	77.8	87.5	100.0	100.0	100.0
H	0.0	0.0	16.7	60.0	63.6	100.0	100.0	100.0	100.0
I	0.0	0.0	0.0	30.0	60.0	100.0	100.0	100.0	100.0

Declarations

Funding

This work received financial support from *Coordenação de Aperfeiçoamento de Pessoal de Nível Superior* – CAPES (Higher Education Personnel Improvement Coordination).

Conflict of Interest

Not applicable.

Ethics Approval and Consent to Participate

Not applicable.

Consent for Publication

All authors hereby grant permission for the publication of this research findings in Computational Economics. Such authors include: Clementino, Tiago Lucas Pereira; and, Moura, José Antão Beltrão. I understand that this article may be disseminated both in print and electronically, and I consent to its inclusion in databases, archives, and other repositories. I have read and understood the terms and conditions of the publication agreement. This consent is given freely, and I affirm that I have the authority to grant such permissions.

Data Availability

Not applicable.

Materials Availability

Not applicable.

Code Availability

The Java language source code of simulator are available in 'https://github.com/tiago-clementino/economy_simulation'. Similarly, the resulting data analyzes in R are available in 'https://github.com/tiago-clementino/economy_simulation_analytics'.

Author Contribution

Tiago Lucas Pereira Clementino contributed to the study conception, methodology design and application. José Antão Beltrão Moura contributed to scientific orientation and revision. The first draft of the manuscript was written by Tiago Lucas Pereira Clementino and José Antão Beltrão Moura commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

AlTawy, R., ElSheikh, M., Youssef, A.M., Gong, G. (2017). Lelantos: A blockchain-based anonymous physical delivery system. *2017 15th annual conference on privacy, security and trust (pst)* (pp. 15–1509).

Arps, J.E., & Christin, N. (2020). Open market or ghost town? the curious case of openbazaar. *Financial cryptography and data security: 24th international conference, fc 2020, kota kinabalu, malaysia, february 10–14, 2020 revised selected papers 24* (pp. 561–577).

Asgaonkar, A., & Krishnamachari, B. (2019). Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator. *2019 ieee international conference on blockchain and cryptocurrency (icbc)* (p. 262-267).

Auinger, A., & Riedl, R. (2018). Blockchain and trust: Refuting some widely-held misconceptions. J. Pries-Heje, S. Ram, & M. Rosemann (Eds.), *Proceedings of the international conference on information systems - bridging the internet of people, data, and things, ICIS 2018, san francisco, ca, usa, december 13-16, 2018.* Association for Information Systems. Retrieved from https://aisel.aisnet.org/icis2018/crypto/Presentations/2

Caronni, G. (2000). Walking the web of trust. *Proceedings ieee 9th international workshops on enabling technologies: Infrastructure for collaborative enterprises (wet ice 2000)* (pp. 153–158).

Clementino, T.L.P., & Moura, J.A.B. (2024). Incentivizing honesty in online decentralized markets. *International conference on computational science and its applications* (pp. 213–229).

Collier, N. (2003). Repast: An extensible framework for agent simulation. *The University of Chicago's social science research*, *36*, 2003,

Collier, N. (2021). *Repast simphony reference manual.* Retrieved from https://repast.github.io/docs/RepastReference/RepastReference.html (Last accessed 30 December 2023)

Domingue, J., Third, A., Ramachandran, M. (2019). The fair trade framework for assessing decentralised data solutions. *Companion proceedings of the 2019 world wide web conference* (pp. 866–882).

Duong-Trung, N., Ha, S., Phan, T., Trieu, P., Nguyen, Q., Pham, D., ... Le, H. (2019, 10). Multi-sessions mechanism for decentralized cash on delivery system. *International Journal of Advanced Computer Science and Applications*, *10*, 553-560, https://doi.org/10.14569/IJACSA.2019.0100973

Dwarakanath, K., Vyetrenko, S., Balch, T., Oyebode, T. (2023, 12). Transparency as delayed observability in multi-agent systems. (p. 279-290).

Fagiolo, G., Moneta, A., Windrum, P. (2007). A critical guide to empirical validation of agent-based models in economics: Methodologies, procedures, and open problems. *Computational Economics*, *30*, 195–226,

Federal Trade Commission (2024). *As nationwide fraud losses top $10 billion in 2023, ftc steps up efforts to protect the public.* https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public. Retrieved 02-09-2024, from https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public (Accessed 11th April 2024.)

Global e-commerce market (2024). *Global e-commerce market to reach $ 47.7 trillion by 2030, report.* https://marketingreport.one/retail/global-e-commerce-market-to-reach-47.7-trillion-by-2030-report.html. Retrieved 04-11-2024, from https://marketingreport.one/retail/global-e-commerce-market-to-reach-47.7-trillion-by-2030-report.html (Accessed 11th April 2024.)

Ha, S., Nguyen, H., Nguyen, P., Trieu, H., Nghiep, Q., Dai, V., ... Nguyen, P. (2019, 04). Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger. *International Journal of Advanced Computer Science and Applications*, *10*, , https://doi.org/10.14569/IJACSA.2019.0100405

Isherwood, A., Koehler, M., Slater, D. (2023). Using evolutionary model discovery to develop robust policies. *2023 winter simulation conference (wsc)* (pp. 130–137).

Le, H., Tien, N., Le, R., Nguyen, P., Duong-Trung, N., Ha, S., ... Nguyen, T. (2019, 06). Introducing multi shippers mechanism for decentralized cash on delivery system. *International Journal of Advanced Computer Science and Applications*, *10*, 590-597, https://doi.org/10.14569/IJACSA.2019.0100676

Lydia Saad (2023). *Scams: Relatively common and anxiety-inducing for americans.* https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx. Retrieved 11-21-2023, from https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx (Accessed 11th April 2024.)

Mamageishvili, A., & Schlegel, J.C. (2020). Optimal smart contracts with costly verification. *2020 ieee international conference on blockchain and cryptocurrency (icbc)* (p. 1-8).

Marks, R.E. (2007). Validating simulation models: a general framework and four applied examples. *Computational economics*, *30*, 265–290,

Mikroyannidis, A. (2020). Blockchain applications in education: A case study in lifelong learning. *The 12th international conference on mobile, hybrid, and online learning (elml 2020).* Retrieved from https://oro.open.ac.uk/69593/

Mikroyannidis, A., Domingue, J., Bachler, M., Quick, K. (2018). Smart blockchain badges for data science education. *2018 ieee frontiers in education conference (fie)* (pp. 1–5).

Mikroyannidis, A., Third, A., Chowdhury, N., Bachler, M., Domingue, J. (2020). Supporting lifelong learning with smart blockchain badges. *International Journal On Advances in Intelligent Systems*, *13*(3 & 4), 163–176,

Müller, M., Janczura, J.A., Ruppel, P. (2020). Decoco: Blockchain-based decentralized compensation of digital content purchases. *2020 2nd conference on blockchain research & applications for innovative networks and services (brains)* (p. 152-159).

Nærland, K., Müller-Bloch, C., Beck, R., Palmund, S. (2017). Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments. *Proceedings/international conference on information systems (icis).*

Nash Jr, J.F. (1950). Equilibrium points in n-person games. In (Vol. 36, pp. 48–49). National Acad Sciences.

North, M.J., Collier, N.T., Ozik, J., Tatara, E.R., Macal, C.M., Bragen, M., Sydelko, P. (2013). Complex adaptive systems modeling with repast simphony. *Complex adaptive systems modeling*, *1*, 1–26,

Ocheja, P., Flanagan, B., Ueda, H., Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, *14*(1), 1–19, https://doi.org/10.1186/s41039-019-0097-0

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., ... Moher, D. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, *372*, , https://doi.org/10.1136/bmj.n71 Retrieved from https://www.bmj.com/content/372/bmj.n71 https://www.bmj.com/content/372/bmj.n71.full.pdf

Pande, S.S., Mandolikar, S., Shitole, S. (2022). Bitland-a decentralized commercial real estate platform. *2022 ieee bombay section signature conference (ibssc)* (p. 1-6).

Radhakrishnan, R., Ramachandran, G.S., Krishnamachari, B. (2019). Sdpp: Streaming data payment protocol for data economy. *2019 ieee international conference on blockchain and cryptocurrency (icbc)* (p. 17-18).

Schwartzbach, N.I. (2022). Payment schemes from limited information with applications in distributed computing. *Proceedings of the 23rd acm conference on economics and computation* (pp. 129–149).

Tian, H., Zou, S., Wang, W., Cheng, S. (2006). A group based reputation system for p2p networks. *Autonomic and trusted computing* (pp. 342–351). Berlin, Heidelberg: Springer.

Tien, N., Nguyen, Q., Nguyen, P., Duong-Trung, N., Huynh, T., Nguyen, P., Ha, S. (2019, 05). Assuring non-fraudulent transactions in cash on delivery by introducing double smart contracts. *International Journal of Advanced Computer Science and Applications*, *10*(5), 677–684, https://doi.org/10.14569/IJACSA.2019.0100584

Tsabary, I., Manuskin, A., Eyal, I. (2022). Ledgerhedger: Gas reservation for smart-contract security. *Cryptology ePrint Archive*, ,

Tsabary, I., Yechieli, M., Manuskin, A., Eyal, I. (2021). Mad-htlc: because htlc is crazy-cheap to attack. *2021 ieee symposium on security and privacy (sp)* (pp.

1230–1248).

Werthenbach, T., & Pouwelse, J. (2022). Survey on social reputation mechanisms: Someone told me i can trust you. *arXiv preprint arXiv:2212.06436*, , https://doi.org/10.48550/arXiv.2212.06436

Zhang, P., Wei, J., Liu, Y., Liu, H. (2023). Proxy re-encryption based fair trade protocol for digital goods transactions via smart contracts. *arXiv preprint arXiv:2306.01299*, , https://doi.org/10.48550/arXiv.2306.01299

Zindros, D. (2016). *Trust in decentralized anonymous marketplaces*. National Technical University of Athens.