UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

ANDERSON KLEBER DANTAS

BLOCKCHAIN E POSSÍVEIS APLICAÇÕES

CAMPINA GRANDE - PB

2024

ANDERSON KLEBER DANTAS

BLOCKCHAIN E POSSÍVEIS APLICAÇÕES

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Orientador : Thiago Emmanuel Pereira da Cunha Silva

CAMPINA GRANDE - PB

2024

ANDERSON KLEBER DANTAS

BLOCKCHAIN E POSSÍVEIS APLICAÇÕES

Trabalho de Conclusão Curso apresentado ao Curso Bacharelado em Ciência da Computação do Centro de Engenharia Elétrica e Informática da Universidade Federal de Campina Grande, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA:

Thiago Emmanuel Pereira da Cunha Silva

Orientador – UASC/CEEI/UFCG

Andrey Elísio Monteiro Brito

Examinador – UASC/CEEI/UFCG

Francisco Vilar Brasileiro

Professor da Disciplina TCC – UASC/CEEI/UFCG

Trabalho aprovado em: 05 de Junho de 2024.

CAMPINA GRANDE - PB

RESUMO

Este artigo explora o potencial transformador e as aplicações no mundo real da tecnologia blockchain. Inicialmente, este documento discute as principais funcionalidades do blockchain, incluindo seu sistema de consenso distribuído e imutável que suporta criptomoedas como o Bitcoin por meio de mecanismos como prova de trabalho. Ele entra em contratos inteligentes, enfatizando as capacidades do Ethereum que ultrapassam simples transações monetárias para permitir aplicações complexas graças à sua linguagem Turing-completa e máquina virtual. Um foco significativo é colocado nas implicações dos tokens não fungíveis (NFTs) para a propriedade de ativos digitais e físicos, destacando como eles suportam representações digitais únicas no blockchain. Outra inovação discutida é o conceito de “Soulbound Tokens” (SBTs), que são projetados para representar atributos intransferíveis como identidade e reputação dentro de uma estrutura descentralizada. Por fim, o artigo mostra o papel crucial dos “oráculos”, que ligam a blockchain aos dados do mundo real, ilustrando o seu impacto nos sistemas financeiros tradicionais através de algoritmos e contratos inteligentes. Portanto, por meio de uma análise abrangente, o artigo articula o vasto potencial da blockchain para inovar múltiplos setores, enfatizando a importância do desenvolvimento colaborativo para garantir a segurança e a conformidade regulatória no aproveitamento eficaz da tecnologia blockchain.

Blockchain and possible applications

ABSTRACT

This paper explores the transformative potential and real-world applications of blockchain technology. Initially, this document discusses blockchain's core functionalities, including its distributed and immutable ledger system that supports cryptocurrencies like Bitcoin through mechanisms like proof of work. It goes into smart contracts, emphasizing Ethereum's capabilities which surpass simple currency transactions to enable complex applications due to its Turing-complete language and virtual machine. Significant focus is placed on the implications of non-fungible tokens (NFTs) for digital and physical asset ownership, highlighting how they support unique digital representations on the blockchain. Another discussed innovation is the concept of "Soulbound Tokens" (SBTs), which are designed to represent non-transferable attributes like identity and reputation within a decentralized framework. Finally, the paper shows the crucial role of “oracles”, which bridge the blockchain with real-world data, illustrating its impact on traditional financial systems through algorithms and smart contracts. Therefore, through a comprehensive analysis, the paper articulates blockchain's vast potential to innovate multiple sectors, stressing the importance of collaborative development to ensure security and regulatory compliance in harnessing blockchain technology effectively.

Blockchain e Possíveis Aplicações

Anderson K. Dantas
Universidade Federal de Campina Grande
Campina Grande, Paraíba, Brasil
anderson.dantas@ccc.ufcg.edu.br

ABSTRACT

This paper explores the transformative potential and real-world applications of blockchain technology. Initially, this document discusses blockchain's core functionalities, including its distributed and immutable ledger system that supports cryptocurrencies like Bitcoin through mechanisms like proof of work. It goes into smart contracts, emphasizing Ethereum's capabilities which surpass simple currency transactions to enable complex applications due to its Turing-complete language and virtual machine. Significant focus is placed on the implications of non-fungible tokens (NFTs) for digital and physical asset ownership, highlighting how they support unique digital representations on the blockchain. Another discussed innovation is the concept of "Soulbound Tokens" (SBTs), which are designed to represent non-transferable attributes like identity and reputation within a decentralized framework. Finally, the paper shows the crucial role of “oracles”, which bridge the blockchain with real-world data, illustrating its impact on traditional financial systems through algorithms and smart contracts. Therefore, through a comprehensive analysis, the paper articulates blockchain's vast potential to innovate multiple sectors, stressing the importance of collaborative development to ensure security and regulatory compliance in harnessing blockchain technology effectively.

RESUMO

Este artigo explora o potencial transformador e as aplicações no mundo real da tecnologia *blockchain*. Inicialmente, este documento discute as principais funcionalidades do *blockchain*, incluindo seu sistema de consenso distribuído e imutável que suporta criptomoedas como o *Bitcoin* por meio de mecanismos como prova de trabalho. Ele entra em contratos inteligentes, enfatizando as capacidades do *Ethereum* que ultrapassam simples transações monetárias para permitir aplicações complexas graças à sua linguagem Turing-completa e máquina virtual. Um foco significativo é colocado nas implicações dos *tokens* não fungíveis (NFTs) para a propriedade de ativos digitais e físicos, destacando como eles suportam representações digitais únicas no *blockchain*. Outra inovação discutida é o conceito de “*Soulbound Tokens*” (SBTs), que são projetados para representar atributos intransferíveis como identidade e reputação dentro de uma estrutura descentralizada. Por fim, o artigo mostra o papel crucial dos “oráculos”, que ligam a *blockchain* aos dados do mundo real, ilustrando o seu impacto nos sistemas financeiros tradicionais através de algoritmos e contratos inteligentes. Portanto, por meio de uma análise abrangente, o artigo articula o vasto potencial da *blockchain* para inovar múltiplos setores, enfatizando a importância do desenvolvimento colaborativo para garantir a segurança e a conformidade regulatória no aproveitamento eficaz da tecnologia *blockchain*.

Palavras-Chave

Blockchain, Contratos Inteligentes, Sistemas financeiros Oráculos, Ativos não-fungíveis. Ativos digitais e físicos.

1. Introdução

A tecnologia *blockchain* tem demonstrado um potencial transformador significativo, ultrapassando as fronteiras do setor financeiro, e permeando diversas áreas da sociedade e da economia. Assim, esta abordagem apresenta uma exploração detalhada das funcionalidades e aplicações do *blockchain*, desde suas origens com o *Bitcoin* até inovações recentes como contratos inteligentes e *tokens* não fungíveis (NFTs). Além disso, discute-se a importância dos oráculos que integram dados do mundo real à *blockchain*, a emergência dos tokens vinculados à identidade chamados *Soulbound Tokens* (SBTs), e as implicações legais e operacionais que acompanham a adoção desta tecnologia. Este estudo também aborda os desafios de segurança cibernética e as necessidades de adaptação regulatória que são cruciais para a integração eficaz e segura do blockchain em sistemas existentes, visando uma compreensão abrangente e crítica da trajetória futura dessa tecnologia disruptiva.

2. Blockchain

Uma cadeia de blocos (*blockchain*) é uma forma de armazenar transações de maneira distribuída e com garantias de imutabilidade e persistência. As transações são armazenadas em um conjunto chamado bloco e os membros da rede fazem isso a intervalos regulares por meio de um processo conhecido como prova de trabalho ou prova de participação. Vários participantes da rede podem compartilhar e armazenar dados de forma transparente e segura com a ajuda dessa tecnologia de registro distribuído. Novos dados são inseridos em intervalos regulares por participantes da rede de acordo com as regras da rede.

O primeiro uso de *blockchain* ocorreu em 2008 quando Satoshi Nakamoto, uma pessoa ou grupo de pessoas anônima(s) no auge da crise econômica do subprime se divulgou um artigo intitulado de *Bitcoin: A Peer-to-Peer Electronic Cash System* (Bitcoin: Um sistema de dinheiro eletrônico de ponto-a-ponto) Onde são discutidas as bases de um sistemas de pagamentos digitais sem a presença de um terceiro confiável e que previne o gasto duplo e sem a necessidade de um emissor centralizado de novas unidades monetárias. Novas unidades dessa moeda são criadas a partir do processo de prova de trabalho onde um membro da rede seleciona transações pendentes do *mempool* (piscina de memória, em tradução livre) e tenta realizar o processo de prova de trabalho que

consiste em calcular o *hash* do bloco concatenado com um nonce (número de uso único) até que o hash tenha uma quantidade específica de zeros no início do hash. Caso um minerador consiga realizar a prova de trabalho antes dos demais concorrentes, essa informação é propagada e validada pelos participantes da rede e recebe novos bitcoins em sua carteira. A carteira do minerador faz parte das informações do bloco e quando ele é adicionado a *blockchain* ele pode movimentar essas moedas livremente. Depois disso, o ciclo se repete com os mineradores realizando prova de trabalho para tentar incluir o bloco subsequente. Como existe essa cadeia de eventos, é possível identificar qual a origem de cada unidade monetária em posse de uma carteira, podendo-se identificar em quais datas cada unidade foi transacionada.

A prova de trabalho permitiu a criação de um mecanismo de consenso *trustless* (sem confiança, em tradução livre) que permitiu os nós da participantes concordarem num conjunto de atualizações para o estado das transações do Bitcoin. Além disso, a prova de trabalho se tornou um mecanismo que previne ataques cibernéticos ao mesmo tempo em que permite a livre participação no processo de consenso. Isso resolveu o problema político de definir quem pode influenciar o processo de consenso. Isso é alcançado através de uma barreira financeira em vez da atribuição de um terceiro confiável ou entidade única e centralizada.

Carteiras num sistema de *blockchain* são uma abstração utilizada para representar pares de chave pública/privada. Uma chave pública pode mostrar quantas unidades monetárias um participante tem, mas sua chave privada é a única maneira de criar e assinar transações que enviam o dinheiro de sua carteira para outro(s) endereço(s) na rede. Essas transações pendentes posteriormente serão processadas pelo processo de prova de trabalho descrito anteriormente.

Transações na rede bitcoin são implementadas através da sua linguagem de *"scripting"* que suporta a implementação de operações na rede. Seu uso básico é para movimentar o saldo de carteiras que consiste em *Unspent Transaction Output* (UTXO, saídas de transações não gastas, em tradução livre) que serão usadas como inputs para a criação de novas UTXOs com valor diferente. Para realizar uma transação o usuário consome uma ou mais UTXO que possui para criar uma ou mais saídas. Tipicamente, o usuário consome duas novas criações próprias, uma para quem deseja fazer o pagamento e outra para um endereço de sua propriedade para que receba o "troco" dessa no final do processo. De maneira oculta, uma transação de bitcoin é uma sequência de passos onde o usuário que a inicia realiza os seguintes passos:

> i) Verifica se as entradas possuem valor maior ou igual às saídas;
>
> ii) Valida se a assinatura fornecida corresponde a do proprietário da transação.

O Bitcoin utiliza uma linguagem chamada *Bitcoin Script*, que é intencionalmente não Turing-completa. Essa decisão de design visa a segurança e a prevenção de loops infinitos que poderiam, potencialmente, paralisar a rede. No entanto, essa limitação também impede a implementação de contratos inteligentes mais complexos e dinâmicos no *blockchain* do Bitcoin. Como resultado, o *Bitcoin Script* é adequado principalmente para funções simples, como transferências condicionais de fundos, mas não suporta aplicações mais avançadas que exigem uma lógica de programação mais flexível e abrangente.

3. Contratos Inteligentes

Contratos inteligentes é um mecanismo suportado por algumas redes de *blockchain* onde um usuário pode criar um programa que será executado pela *blockchain* automaticamente. Seus usos mais comuns são criação de *tokens*, ativos digitais não fungíveis e propriedade inteligente. Eles também permitem a implementação de programas com regras arbitrárias, permitindo assim que sejam implementados contratos inteligentes e esses podem ser utilizados para se implementar entidades como DAOs (*Decentralized Autonomous Organizations*, "Organizações Autônomas Descentralizadas" em tradução livre).

3.1 Ethereum

O *Ethereum* foi projetado como uma plataforma descentralizada que supera essas limitações, permitindo o desenvolvimento e a execução de contratos inteligentes por meio de uma linguagem Turing-completa. Ele introduziu a *Ethereum Virtual Machine* (EVM), que é o ambiente de execução para esses contratos. Isso abre um vasto campo de possibilidades, permitindo aos desenvolvedores criar aplicações descentralizadas (dApps) que podem variar de aplicações mais sérias sistemas financeiros autônomos, sistemas de votação e gestão de identidade mas também servindo como base para criação dos famigerados NFTs.

A plataforma *Ethereum* permite que esses contratos sejam escritos, testados e implementados de maneira eficiente, oferecendo um ambiente robusto para inovação. Além disso, o modelo de "gás" do *Ethereum*, onde os usuários pagam por cada operação executada no contrato em função de sua complexidade computacional, ajuda a manter a rede segura e eficiente ao desincentivar operações desnecessariamente caras ou mal otimizadas.

No *Ethereum*, cada operação que ocorre na rede, seja uma transação simples de envio de Ether ou a execução de um contrato inteligente, requer uma certa quantidade de poder computacional. O gás é a unidade que mede esse custo computacional. Ele serve para limitar a quantidade de trabalho que é necessária para executar transações e contratos inteligentes, evitando assim o abuso dos recursos da rede. Cada tipo de operação na rede *Ethereum* tem um custo específico em gás, definido pelo protocolo do *Ethereum*. Além do custo em gás, os usuários devem definir quanto estão dispostos a pagar por cada unidade de gás, o que é conhecido como o "preço do gas". Esse preço é geralmente medido em Gwei, que é uma fração muito pequena de um Ether (1 Ether = 1 bilhão de Gwei). O preço do gás pode variar significativamente, influenciado pela demanda por recursos de computação na rede. Quando a rede está muito ativa, o preço do gás tende a aumentar. Quando você envia uma transação, você especifica um "limite de gás", que é a quantidade máxima de gás que você está disposto a usar para sua transação, e o "preço do gas", que é quanto você está disposto a pagar por unidade de gás. O produto do gás usado por uma transação e o preço do gás é o custo total que você paga, que é deduzido do seu saldo em Ether. Se a quantidade de gás consumida por uma transação for menor do que o limite estabelecido, o Ether não será devolvido à conta do usuário. No entanto, se a transação excede o limite de gás, a transação é revertida, mas o gás que foi consumido até o ponto de falha não é devolvido, como uma penalidade por estimar mal o custo necessário. O sistema de gás é vital para a saúde da rede

Ethereum. Ele não só evita que a rede seja sobrecarregada por transações que requerem uma quantidade excessiva de poder de computação, mas também ajuda a prevenir ataques de negação de serviço (DoS), onde alguém tenta sobrecarregar a rede intencionalmente.

Os padrões ERC (*Ethereum Request for Comments*) são propostas técnicas que os desenvolvedores submetem para consideração na comunidade *Ethereum*. Eles definem padrões para vários aspectos dos contratos inteligentes na rede *Ethereum*, facilitando a interoperabilidade entre *tokens*, contratos e outros serviços descentralizados. O ERC-20, por exemplo, é um padrão popular para a criação de *tokens* fungíveis, enquanto o ERC-721 é crucial para a implementação de *tokens* não fungíveis (NFTs).

Na rede *Ethereum*, existem dois tipos principais de contas: Contas de Propriedade Externa (EOAs, do inglês *"Externally Owned Accounts"*) e Contas de Contratos. Ambas são fundamentais para o funcionamento da rede, mas possuem funções e características distintas. Uma EOA é controlada por uma pessoa ou entidade que possui a chave privada associada à conta. Não há código associado a uma EOA e ela é usada para enviar transações que podem incluir mensagens simples para outros endereços ou chamadas a funções de um contrato inteligente. O acesso e controle sobre uma EOA dependem exclusivamente da chave privada. Quem possui a chave privada pode autorizar transações a partir dessa conta. As EOAs podem iniciar transações. Isso inclui transferência de ether, criação de contratos inteligentes e interação com contratos inteligentes existentes na rede. Uma conta de contrato é uma conta que tem um código associado a ela, que é executado sempre que a conta recebe uma transação ou mensagem. Essa conta não é controlada por uma chave privada, mas pelo código do contrato inteligente que define seu comportamento. O código do contrato é escrito em uma linguagem de programação de alto nível, como Solidity, que é compilado para bytecode e executado pela Máquina Virtual *Ethereum* (EVM). O código pode definir regras para modificar o estado do contrato, criar novas transações e interagir com outras contas. Contas de contrato não podem iniciar transações por conta própria. Elas só executam seu código e respondem quando uma transação ou mensagem é enviada para elas, seja por uma EOA ou por outro contrato.

4. Ativos não fungíveis

Fungibilidade é uma propriedade de bens ou ativos que indica que as unidades individuais são intercambiáveis e cada unidade é indistinguível de outra da mesma espécie. Um bem fungível pode ser substituído por outro bem idêntico, e ele mantém o mesmo valor independentemente de sua particularidade. Por exemplo, uma nota de 10 reais pode ser trocada por qualquer outra nota de 10 reais sem perder valor ou utilidade, pois todas as notas de 10 reais são consideradas iguais em termos de valor monetário. Em contraste, bens não fungíveis são aqueles que não podem ser substituídos por outros de igual valor porque cada item tem características únicas que afetam seu valor. Exemplos de itens não fungíveis incluem imóveis e obras de arte. Cada um desses itens é único; por exemplo, mesmo duas pinturas do mesmo artista podem ter valores significativamente diferentes devido a diferenças em popularidade, condição, história, etc. A fungibilidade é um conceito crucial em economia e finanças porque facilita e simplifica as transações através de um denominador comum. A fungibilidade assegura que os participantes do mercado possam negociar bens e ativos sem ter que inspecionar cada unidade individualmente para variações de valor.

Tokens Não Fungíveis (NFTs) são ativos digitais que representam a propriedade de bens únicos, tanto digitais quanto físicos, em uma *blockchain*. Diferentemente dos *tokens* fungíveis, como criptomoedas, que são intercambiáveis e possuem valor equivalente entre si, cada NFT é distinto e não pode ser trocado de forma equivalente com outro NFT. Os NFTs são implementados utilizando padrões de contrato inteligente como o ERC-721 e o ERC-1155 na *Ethereum*, que permitem a codificação de metadados associados ao *token* e garantem a exclusividade e rastreabilidade de cada item. A natureza não fungível dos NFTs os torna ideais para representar a propriedade de itens exclusivos, como obras de arte digitais, colecionáveis, propriedades virtuais em jogos, e até mesmo direitos autorais e licenças. Os NFTs possibilitam a monetização de bens digitais e a criação de novos modelos de economia digital, onde os emissores desses ativos podem vendê-los diretamente para o consumidor sem intermediários, com garantia de autenticidade e proveniência dos bens através da tecnologia *blockchain*. Os NFTs são "cunhados" quando alguém interage com o contrato inteligente para criar um novo NFT. Isso geralmente envolve fornecer os detalhes do NFT, como a imagem ou o arquivo digital associado, e pagar uma taxa, que pode ser em criptomoeda, para registrar essa transação na *blockchain*.

Para rastrear a propriedade de objetos físicos usando contratos inteligentes, cada objeto precisa ser representado digitalmente na *blockchain*. Isso é frequentemente feito através da tokenização, onde cada item é associado a um único *token*. Esse *token* pode ser um *Token* Não Fungível (NFT) se cada item for único (e.g., carros com números de série distintos) ou um *token* fungível para itens que são idênticos em especificações e valor. O contrato inteligente deve ser projetado para registrar a propriedade, transferências de propriedade e quaisquer regras ou restrições relativas ao objeto. Quando um item é produzido ou vendido pela primeira vez, ele é registrado no contrato inteligente com detalhes como número de série, especificações técnicas, data de produção, e o endereço da *blockchain* do proprietário atual. O contrato deve incluir funções que permitam a transferência segura de propriedade do *token* (e, portanto, do item físico) de um endereço para outro, possivelmente incluindo verificações ou autorizações, como a confirmação de pagamento. Apesar de não existir essa funcionalidade especificada diretamente por uma ERC, é possível implementar um contrato que realiza a troca atômica da titularidade, ou seja, ao mesmo tempo em que o pagamento é efetuado a titularidade é transferida. Neste último caso, o pagamento fica restrito a ser realizado apenas através da *blockchain*, o que pode ser dificultoso para um usuário leigo.

5. Registros de pessoas

Soulbound Tokens (SBTs) representam um conceito emergente no domínio da tecnologia *blockchain*, caracterizados por serem *tokens* digitais não transferíveis que visam encapsular a identidade, a reputação e os atributos pessoais de um indivíduo na esfera digital. Esta nova classe de *tokens* foi popularizada pelo cofundador da *Ethereum*, Vitalik Buterin, e outros colaboradores, através de um artigo intitulado Decentralized Society: Finding Web3's Soul (Sociedade Descentralizada: Encontrando a alma da Web, em tradução livre), que discute o potencial dos SBTs para fundamentar uma "sociedade descentralizada". Em contraste com os NFTs tradicionais, que são transferíveis e podem ser

negociados em mercados abertos, os SBTs são vinculados à identidade do titular e não podem ser transferidos, o que implica uma série de aplicações possíveis em registros de pessoas, certificações e documentos legais, tais como vacinas, diplomas e carteiras de habilitação.

O uso de SBTs no registro de pessoas possui um alto potencial para aplicação em autenticação e verificação de identidades. Acessar dados de um indivíduo através de um *token* vinculado à sua identidade digital, facilitaria uma série de interações sociais e econômicas ao mesmo tempo em que é possível garantir a segurança ou a privacidade. O *token* poderia conter informações criptografadas, como data de nascimento, nacionalidade e outros dados biográficos, acessíveis apenas por entidades autorizadas mediante consentimento explícito do titular.

No contexto de registros de vacinação, os SBTs podem desempenhar um papel crucial ao armazenar o histórico de vacinação de uma pessoa. Isso não só simplifica o processo de verificação em pontos de controle de saúde, como também auxilia na manutenção de registros médicos precisos e seguros. Um SBT de vacinação poderia ser atualizado por profissionais de saúde autorizados a cada nova dose recebida, garantindo que as informações sejam mantidas atualizadas e facilmente acessíveis por hospitais, clínicas e outras instituições de saúde.

A aplicação de SBTs na emissão de diplomas pode facilitar a emissão e verificação de credenciais acadêmicas de forma rápida e a prova de fraudes. Instituições de ensino poderiam emitir diplomas como SBTs, que seriam armazenados na *blockchain* e poderiam ser verificados instantaneamente por empregadores ou outras instituições educacionais. Isso eliminaria a necessidade de processos de validação manuais e reduziria significativamente a incidência de diplomas falsos.

Os SBTs podem ser utilizados como um método eficiente e seguro de armazenamento e verificação de carteiras de motorista. As autoridades de trânsito poderiam emitir tais *tokens*, que registram informações como a data de emissão, categorias de veículos autorizados e datas de expiração. Tais *tokens* ajudariam na rápida verificação da validade das licenças por autoridades policiais e outros organismos relevantes, sem a necessidade de consulta a bases de dados centralizadas.

6. Oráculos

Os oráculos são entidades essenciais para viabilizar as interações entre *blockchains* e o mundo exterior. Eles são mecanismos ou serviços que fornecem dados externos aos contratos inteligentes executados em redes *blockchain*, que por si só são incapazes de acessar informações fora de seu sistema. A necessidade de oráculos surge da natureza fechada e determinística das *blockchains*, que, embora ofereça segurança e imutabilidade, limita sua capacidade de interagir diretamente com dados externos ou eventos do mundo real. Os oráculos são contratos inteligentes que podem ser atualizados de maneira a refletir mundo externo para as *blockchains*, permitindo que contratos inteligentes reajam a entradas não registradas na *blockchain*. Sem oráculos, contratos inteligentes seriam capazes apenas de utilizar eventos e informações presentes diretamente na *blockchain*, restringindo significativamente suas aplicações práticas.

Oráculo de software: analisam preços de ativos, resultados de eventos esportivos e condições meteorológicas online. Eles extraem dados de fontes externas na internet e os alimentam diretamente para a *blockchain*.

Oráculo de hardware: obtém dados do mundo físico, como informações de sensores ou sistemas de telemetria.

Oráculo inbound: traz dados do mundo externo para as *blockchains*, enquanto oráculos outbound permitem que as *blockchains* enviem comandos para o mundo externo, como, por exemplo, pagamento a um sistema quando certas condições são cumpridas.

Apesar de sua utilidade, os oráculos representam um ponto de vulnerabilidade potencial dentro do ecossistema de *blockchain*, pois a entrada de dados incorretos pode levar a resultados errôneos ou manipulações mal-intencionadas. Isso é frequentemente referido como o "problema do oráculo". Além disso, a dependência de oráculos pode introduzir uma certa centralização em um sistema que, de outra forma, é descentralizado. Para combater os riscos associados aos oráculos, várias estratégias podem ser implementadas como:

Diversificação de Fontes: utilizar múltiplas fontes de dados e diferentes oráculos para verificar a mesma informação, aumentando a confiabilidade dos dados recebidos.

Contratos de Reputação: implementar sistemas em que a confiabilidade dos oráculos é rastreada e verificada, potencialmente penalizando aqueles que fornecem dados falsos.

Circuitos de Segurança: criar mecanismos que permitam a intervenção humana ou automática caso os dados fornecidos pareçam ser anômalos ou fora dos padrões esperados.

Oráculos são uma adição crucial aos ecossistemas de *blockchain*, permitindo uma ampla gama de aplicações que requerem interações com o mundo real. No entanto, seu *design* e implementação devem ser cuidadosamente considerados para proteger contra vulnerabilidades e garantir a integridade das operações de *blockchain*. À medida que a tecnologia de oráculos evolui, também evolui a capacidade de contratos inteligentes de responder de maneira segura e confiável a condições complexas do mundo real.

7. Apostas Descentralizadas

De acordo com dados da Anbima (Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais) 14% da população brasileira participou de apostas online, enquanto apenas 2% da população investiu em ações. Muitas vezes as apostas são realizadas em plataformas sediadas fora do Brasil, fugindo das regulações nacionais nesses mercados, bem como qualquer tipo de auditoria.

Com apostas descentralizadas, as regras do jogo ou os termos da aposta são codificados como parte do contrato inteligente. Isso significa que todas as partes envolvidas têm acesso às mesmas regras, que são claras, transparentes e não podem ser alteradas uma vez que o contrato seja implantado na *blockchain*.

Os oráculos desempenham um papel crucial na integração de informações do mundo real em contratos inteligentes utilizados para apostas esportivas em plataformas *blockchain*. Ao fornecer dados externos aos contratos inteligentes, os oráculos permitem que esses contratos reajam a eventos esportivos reais, facilitando a execução justa e transparente de apostas descentralizadas. Deve-se selecionar oráculos confiáveis que possam fornecer dados precisos e atuais sobre eventos esportivos. É crucial escolher

oráculos que tenham uma boa reputação e um histórico comprovado de confiabilidade e precisão. Os desenvolvedores do contrato inteligente devem configurar o contrato para interagir com esses oráculos específicos, definindo claramente quais dados serão necessários (por exemplo, resultados de jogos, estatísticas de jogadores, etc.) e em que formato esses dados devem ser fornecidos. Para garantir a integridade das apostas, mecanismos de segurança devem ser implementados, tais como:

- **Verificação de Consenso:** usar múltiplos oráculos para confirmar o resultado de um evento esportivo, mitigando o risco de dados incorretos ou manipulação.
- **Validação de Dados:** programar verificações para assegurar que os dados recebidos estão dentro de parâmetros razoáveis, descartando dados que pareçam ser errôneos ou manipulados.

8. Implicações Legais e Adequações Regulatórias do Uso de Blockchain

À medida que a tecnologia *blockchain* continua a evoluir e a ser adotada em diversas áreas, surgem importantes considerações legais e a necessidade de adequações regulatórias. A natureza descentralizada, transparente e imutável da *blockchain* apresenta tanto oportunidades quanto desafios para o sistema jurídico atual.

8.1 Implicações Legais do Uso de Blockchain

A implementação da tecnologia *blockchain* em setores como financeiro, saúde, imobiliário e jurídico levanta diversas questões legais. Um dos principais desafios é a responsabilidade legal em uma rede descentralizada. Tradicionalmente, a responsabilidade recai sobre entidades centralizadas, como bancos ou empresas. No entanto, em uma rede de *blockchain*, onde não há um ente central, determinar quem é responsável por erros ou violações pode ser complexo. Embora a *blockchain* ofereça segurança aprimorada, sua natureza imutável pode entrar em conflito com leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. A LGPD inclui direitos como a correção e exclusão de dados pessoais, o que é um desafio devido à imutabilidade da *blockchain*. O dilema entre a natureza imutável da *blockchain* e a capacidade de alterar ou excluir informações pessoais é um problema jurídico e técnico relevante e muita pesquisa e desenvolvimento nessa área ainda deve ser realizada. Além disso, questões como a jurisdição e a aplicabilidade da lei ainda são uma área cinzenta devido à natureza global da *blockchain*. Transações e contratos podem envolver partes de diferentes países, cada um com suas próprias leis e regulamentos. Isso levanta a questão de qual legislação aplicar em caso de disputa.

8.2 Necessidades de Adequação Regulatória

Para que a *blockchain* alcance seu pleno potencial, são necessárias claras diretrizes regulatórias. Reguladores de todo o mundo estão começando a reconhecer a necessidade de desenvolver *frameworks* que não apenas protejam os consumidores e garantam a integridade do mercado, mas também fomentem a inovação.

Uma área que necessita de atenção regulatória é a definição legal de ativos digitais. Diferentes jurisdições atualmente têm abordagens variadas para classificar criptomoedas e *tokens*, o que pode levar a incertezas e inconsistências regulatórias. Uma abordagem coordenada poderia ajudar a estabelecer uma classificação clara e uniforme, facilitando o comércio e a tributação desses ativos.

Além disso, a regulamentação dos contratos inteligentes é essencial, pois eles são uma das aplicações mais promissoras da tecnologia *blockchain*. Os legisladores precisarão considerar como os contratos inteligentes se enquadram nas leis de contrato existentes e se novas leis são necessárias para abordar questões específicas relacionadas a sua execução automática.

Com o aumento das ameaças cibernéticas e fraudes associadas a ativos digitais, é imperativo que haja regulamentos rigorosos em relação à segurança das redes de *blockchain*. Estes regulamentos ajudariam a garantir a proteção de dados sensíveis e a confiança do usuário na tecnologia.

9. Riscos Operacionais no Uso de Blockchain

A implementação de tecnologia *blockchain*, embora traga inovação e eficiência em várias áreas, também envolve riscos operacionais significativos. Dois dos principais riscos operacionais incluem ataques de hackers e os custos flutuantes associados à execução de contratos inteligentes devido aos picos no preço do gás no *Ethereum*.

9.1 Ataques de Hackers

Embora a *blockchain* seja geralmente segura por design, devido à sua descentralização e ao uso de criptografia avançada, as aplicações construídas sobre ela, como as exchanges de criptomoedas e os contratos inteligentes, podem ter vulnerabilidades. Estas vulnerabilidades podem ser exploradas por hackers.

Por exemplo, os contratos inteligentes, apesar de executarem operações automaticamente com base nas condições predefinidas, são apenas tão seguros quanto o código em que são escritos. Erros de programação ou lógica podem ser explorados para realizar ataques, como os ataques de reentrância, onde um contrato externo malicioso pode fazer várias chamadas a um contrato vulnerável dentro de uma única transação.

Outro risco significativo é o de ataques ao nível do protocolo, como ataques de 51%, onde um grupo de mineradores controla mais de 50% do poder de mineração da rede e pode influenciar o processo de validação de transações, permitindo a duplicação de gastos ou até mesmo reverter transações.

9.2 Custos de Execução de Contratos e Flutuações de Preço de Gás

Um segundo risco operacional relaciona-se com o custo de execução de contratos inteligentes em *blockchains* que utilizam o sistema de gás, como o *Ethereum*. O gás é a unidade de medida que quantifica o custo de execução de operações no *Ethereum*, visando compensar os mineradores pelo poder computacional utilizado.

Os preços do gás podem variar dramaticamente com base na demanda pela rede. Em períodos de alto tráfego, como durante lançamentos de grandes ICOs ou movimentos de mercado significativos, o custo do gás pode aumentar exponencialmente. Essa volatilidade pode tornar a operação de contratos inteligentes financeiramente inviável temporariamente e impactar

negativamente as operações empresariais que dependem desses contratos para funções rotineiras.

9.3 Mitigação dos Riscos Operacionais

Para mitigar esses riscos, as organizações devem adotar várias estratégias. Primeiro, a revisão e auditoria frequentes do código dos contratos inteligentes por especialistas em segurança são essenciais para prevenir vulnerabilidades. Além disso, é importante implementar medidas de segurança robustas em todas as aplicações *blockchain* para proteger contra ataques externos.

Em relação à volatilidade dos custos do gás, uma abordagem é monitorar ativamente os preços e ajustar as transações durante períodos de menor demanda. Outra solução é utilizar plataformas de *blockchain* alternativas que ofereçam um modelo de custo de gás mais previsível ou que operem sem custos de gás para execução de contratos.

10. Conclusão

Ao longo deste artigo, exploramos a vasta gama de aplicações e o potencial revolucionário da tecnologia *blockchain*, bem como as implicações legais, necessidades regulatórias e riscos operacionais associados ao seu uso. Desde a sua origem com o Bitcoin até suas aplicações em contratos inteligentes e além, a *blockchain* promete transformar diversos setores da sociedade e da economia. Com casos de uso que se estendem desde sistemas de votação até gestão de identidade e mercados de arte digitais, o impacto potencial da *blockchain* é vasto e multifacetado.

As discussões sobre as implicações legais revelaram que a intersecção da *blockchain* com leis existentes, como a LGPD no Brasil, exige uma consideração cuidadosa, especialmente em relação à proteção de dados e responsabilidades legais em uma infraestrutura descentralizada. As regulamentações precisarão evoluir para acompanhar o ritmo das inovações tecnológicas, garantindo que tanto os benefícios quanto os riscos sejam adequadamente gerenciados.

Os riscos operacionais, como ataques de hackers e a volatilidade dos custos associados ao uso de contratos inteligentes, também são considerados críticas. Estes riscos exigem que as organizações implementem estratégias proativas de mitigação para proteger suas operações e garantir a confiabilidade e eficácia da tecnologia *blockchain*.

A colaboração entre desenvolvedores de *blockchain*, reguladores, juristas e profissionais de segurança cibernética será essencial para moldar um ambiente em que a *blockchain* possa prosperar sem comprometer a segurança ou a conformidade regulatória. A criação de padrões globais e a harmonização das leis podem facilitar uma adoção mais ampla e mais segura desta tecnologia promissora.

Em conclusão, enquanto navegamos por este território inovador e complexo, é imperativo que continuemos a explorar, experimentar e educar, preparando o caminho para um futuro em que a tecnologia *blockchain* possa alcançar seu potencial máximo de forma segura e ética. Através de um diálogo contínuo e colaboração entre todos os *stakeholders*, podemos garantir que os benefícios da *blockchain* sejam realizados enquanto seus desafios são prontamente endereçados.

11. Agradecimentos

Primeiramente gostaria de agradecer a minha mãe Valdinez Dantas quem sempre me apoiou durante o curso e me deu motivação para seguir apesar das adversidades. Gostaria de agradecer as grandes mentes por trás da *blockchain* suas inovações como Satoshi Nakamoto (seja lá quem for), Vitalik Buterin, Nick Szabo, Hal Finney e Adam Back. Por fim, gostaria de agradecer ao Fernando Ulrich e Guilherme Rennó por todos os anos de trabalho divulgando ideias de liberdade e descentralização.

12. Referências

[1] Daly, L. What are Colored Coins?
link: https://www.fool.com/terms/c/colored-coins/

[2] Ethereum Whitepaper.
link: https://ethereum.org/en/whitepaper/

[3] Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain. link: https://www.investopedia.com/terms/g/gas-ethereum.asp

[4] Lima, M. 14% da população brasileira apostou ao menos uma vez em 2023; mais ricos apostam mais. link: https://www.infomoney.com.br/onde-investir/14-da-populacao-brasileira-apostou-ao-menos-uma-vez-em-2023-mais-ricos-apostam-mais/

[5] Matta, G. L. A Lei Geral de Proteção de Dados e o Direito ao Esquecimento. link: https://www.repositorio.ufal.br/bitstream/123456789/10339/1/A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20e%20o%20direito%20ao%20esquecimento.pdf

[6] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. link: https://bitcoin.org/bitcoin.pdf

[7] Ohlhaver, P., Weyl, E. G., Buterin, V. Decentralized Society: Finding Web3's Soul. link: https://deliverypdf.ssrn.com/delivery.php?ID=060100116086003024119080082101065076000050041076022024096096094109098087118078065127048021127015040030058018018030010092123100126094082050028023024008000118004121077009082021110000096117080122126106079108007016118125120009122106027086065089008027017009&EXT=pdf&INDEX=TRUE

[8] Oráculos: conectando contratos inteligentes com dados do mundo real. link: https://fastercapital.com/pt/contente/Oraculos--conectando-contratos-inteligentes-com-dados-do-mundo-real.html

[9] Quais são os benefícios do full node de Bitcoin? link: https://www.mercadobitcoin.com.br/economia-digital/bitcoin/quais-sao-os-beneficios-do-full-node-de-bitcoin

[10] Rhodes, D. What is Bitcoin Script? Unveiling Its Role in Bitcoin.
link: https://komodoplatform.com/en/academy/bitcoin-script/

[11] Soares, X. Como os blocos são adicionados a um Blockchain, explicado de forma simples link: https://www.coindesk.com/pt-br/learn/how-blocks-are-added-to-a-blockchain-explained-simply/

[12] Unspent transaction output. link: https://en.wikipedia.org/wiki/Unspent_transaction_output

Sobre o Autor:

Anderson K. Dantas é estudante de Ciência da Computação pela Universidade Federal de Campina Grande. Ele atua como Consultor e Desenvolvedor de *Software* para empresas nacionais e internacionais desenvolvendo projetos de larga escala e alta disponibilidade.