Resumo: Blockchain GoLedger Módulo 1

Gabriel dos Santos Schmitz

Outubro 2024

This document delves into the evolution of value exchange and the emergence of blockchain technology, focusing on Bitcoin as a decentralized digital currency that revolutionized traditional finance. By eliminating the need for intermediaries, blockchain allows secure peer-to-peer transactions through cryptographic principles, using structures like UTXOs and Merkle trees to ensure integrity. Bitcoin's Proof of Work (PoW) mechanism underpins its consensus model, though it has significant environmental costs, prompting some blockchains to adopt alternatives like Ethereum's Proof of Stake (PoS). Since its inception, Bitcoin has evolved from a niche asset to a widely recognized store of value and payment method, even gaining status as legal tender in some countries.

Gabriel dos Santos Schmitz: UTFPR. Eu agradeço colegas e orientador por comentários e discussões úteis. Este trabalho foi apoiado por Grupo PQC UTFPR

1. Origem e Usos de Blockchain

. A atribuição de valor a objetos é uma atividade subjetiva e marginal, ou seja, dependente das circunstâncias e da percepção individual. Cada pessoa confere valor de forma particular, mesmo que influenciada pela opinião de outros. Historicamente, as primeiras transações comerciais foram realizadas por meio do escambo, onde um objeto A era trocado por um objeto B, sendo que B era mais valioso para um lado da transação e A para o outro. Essa forma de troca, entretanto, apresenta limitações: se um indivíduo possui grande quantidade de um item que não lhe interessa, o escambo pode se tornar ineficaz ou inviável. Surge, então, a necessidade de um item com valor de troca *universal* — a moeda.

. O primeiro tipo de moeda adotado foi o gado bovino, na Grécia, seguido pelo uso de sal como moeda de troca, o que originou a palavra "salário" que utilizamos até hoje. Para ilustrar uma moeda arcaica, o curso utiliza as pedras Rai das Ilhas Yap, que variavam de tamanho entre 3 cm e 3 m. Essas pedras possuíam um valor associado tanto ao seu tamanho quanto à sua história, conferindo ao proprietário status e riqueza. Em uma analogia mais moderna, temos os NFTs (Tokens Não Fungíveis), que possuem valor artístico e são valorizados pela sua unicidade, assegurada por um *hash* que garante a autenticidade e indivisibilidade do item, de forma semelhante a uma obra de arte única.

. Assim, a tecnologia de blockchain oferece um meio seguro e verificável de estabelecer e manter a autenticidade e a propriedade de ativos digitais, de forma descentralizada, com potencial para diversos usos além das transações financeiras, como contratos inteligentes e autenticação digital.

FIGURE 1. Pedras Rai e NFT

2. Do Livro Razão ao Blockchain

. Os primeiros livros-razão surgiram por volta de 5000 a.C., quando as sociedades passaram a registrar seus bens e transações. Antes disso, as pessoas mantinham apenas o que conseguiam carregar, limitando o potencial de acumulação e troca de recursos. Com o avanço das trocas comerciais, esses registros se tornaram essenciais para documentar a posse de bens e acordos de troca. Na atualidade, o *ledger* digital, popularizado pelo advento do Bitcoin, representa uma evolução significativa desses antigos livros-razão, funcionando como um registro de todas as transações da rede de forma cronológica e linear, sem a necessidade de uma entidade centralizadora.

. Inicialmente, os livros-razão tradicionais tinham um formato simples, com uma única entrada por linha. Com o tempo e o aumento da complexidade das transações, tornaram-se mais detalhados, passando a incluir a história das transações de ambas as partes envolvidas, além dos registros de débitos e créditos, que refletiam de forma mais precisa o fluxo de ativos.

. No contexto do Bitcoin e das criptomoedas, o *ledger* digital, conhecido como *blockchain*, possui o papel fundamental de manter a transparência e a confiança na rede. Esse livro-razão digital requer que todas as transações sejam registradas em sequência, desde a criação do primeiro bloco, garantindo a integridade e a imutabilidade dos dados. Dessa forma, o blockchain opera como uma estrutura descentralizada que possibilita o armazenamento seguro e público de informações, tornando-se um elemento central para diversas aplicações, incluindo contratos inteligentes e autenticações digitais.

3. Fidúcia e o Papel dos Intermediários

. Em uma transação de troca de produtos, valores ou serviços, certos elementos fundamentais garantem que o processo seja justo e satisfatório para ambas as partes. Primeiramente, cada participante deve avaliar o valor que atribui ao item trocado, pois essa percepção de valor assegura que ambas as partes se sintam beneficiadas com a transação. A confiança (ou fidúcia) entre as partes é igualmente crucial, pois transações comerciais dependem de uma relação de credibilidade que evita a necessidade de intervenções externas. Em muitos casos, são exigidas garantias adicionais para assegurar que cada lado cumpra suas obrigações, promovendo assim uma troca mais segura e confiável.

. Conforme argumentado por Aristóteles, esses elementos são ainda mais eficientes quando potencializados pela introdução da moeda, um meio de troca que substitui o escambo direto e facilita o comércio. Segundo o filósofo, a moeda cumpre três funções

essenciais: age como meio de troca, permitindo transações mais ágeis; como unidade de conta, permitindo a comparação objetiva entre valores de diferentes bens e serviços; e como reserva de valor, possibilitando o acúmulo de riqueza ao longo do tempo. Para que a moeda cumpra bem seu papel, deve possuir características específicas, como durabilidade, divisibilidade, transportabilidade e valor intrínseco. O registro adequado das transações, feito em sistemas como livros-razão ou em tecnologias mais modernas como o blockchain, contribui para a transparência e rastreabilidade, completando o ciclo de troca com segurança.

. A necessidade de garantias em uma transação está diretamente ligada ao nível de confiança entre as partes. Quanto maior a confiança, menor a exigência de garantias, pois cada parte tem mais certeza do cumprimento do acordo. Quando a confiança é baixa, as garantias devem ser maiores, sendo comum recorrer a um intermediário para gerenciar essas garantias e formalizar o processo. Esse intermediário precisa ser confiável para ambas as partes e ter a responsabilidade de registrar a transação. Exemplos de intermediários incluem cartórios, que gerenciam registros para diversos setores; a Justiça, que atua como mediadora de disputas; a Previdência, para o gerenciamento de contribuições e aposentadorias; e os bancos, que, no sistema financeiro, gerenciam e guardam valores monetários.

. A história dos sistemas de valor reflete uma evolução constante, desde o uso de pedras e conchas até metais preciosos que serviram como lastro para as moedas emitidas por governos. O fim do sistema Bretton Woods trouxe uma mudança significativa, substituindo moedas lastreadas em ativos por moedas fiduciárias, cujo valor é baseado na confiança dos usuários no emissor — geralmente um governo — em vez de ativos tangíveis.

. O sistema financeiro moderno exerce um papel fundamental ao realizar funções como guarda de valor, registro de transferências e concessão de empréstimos. Historicamente, esses registros eram centralizados em livros-razão, mas evoluíram para livros-razão distribuídos (DLT), uma prática que teve origem no Império Romano e que hoje se beneficia das tecnologias digitais. No entanto, a governança desses sistemas nem sempre é infalível, o que pode abrir brechas para fraudes, como evidenciado pela crise do subprime de 2008, que expôs falhas significativas na gestão de ativos e no controle de crédito no mercado financeiro.

4. Bitcoin

. Em novembro de 2008, Satoshi Nakamoto lançou um paper intitulado A Peer-to-Peer Electronic Cash System, que estabeleceu os fundamentos para o Bitcoin e seu sistema de

transações eletrônicas em uma rede distribuída. O documento descreveu a criação de um "ativo" digital cuja propriedade é registrada em um ledger público (blockchain) e operado em uma rede peer-to-peer. Esse sistema permite que transações ocorram entre usuários de forma descentralizada, sem a necessidade de uma autoridade central, resultando na criação do Bitcoin como o conhecemos hoje.

. O protocolo do Bitcoin funciona através de um mecanismo de identificação onde cada usuário é representado por uma chave pública e protegida por uma chave privada, que funciona como uma senha. Transações são realizadas e enviadas para a rede, onde aguardam validação. Os computadores da rede, conhecidos como "mineradores", competem para agrupar essas transações em blocos válidos. Esse processo de validação envolve a resolução de problemas matemáticos complexos, recompensando o minerador que consegue resolver o problema com o direito de incluir o próximo bloco na blockchain.

. A estrutura de blocos no Bitcoin utiliza um encadeamento de hashes para manter a sequência e a integridade dos registros. Cada bloco contém um hash do bloco anterior, formando uma cadeia ininterrupta que confirma a sequência das transações. Essa metodologia possibilita que transações ocorram entre pessoas ou entidades que não se conhecem ou confiam entre si, em uma rede que também não oferece confiança intrínseca, mas que, ainda assim, garante segurança e integridade.

. Para manter o controle de saldos e prevenir gastos duplos, o Bitcoin adota o conceito de UTXO (Unspent Transaction Output). Esse sistema armazena o "troco" de transações, que são saldos remanescentes disponíveis para uso em transações futuras. Esse mecanismo permite que o Bitcoin mantenha um controle eficiente dos saldos sem que seja necessário verificar todo o histórico do ledger, garantindo a continuidade das operações financeiras na rede de forma descentralizada e segura.

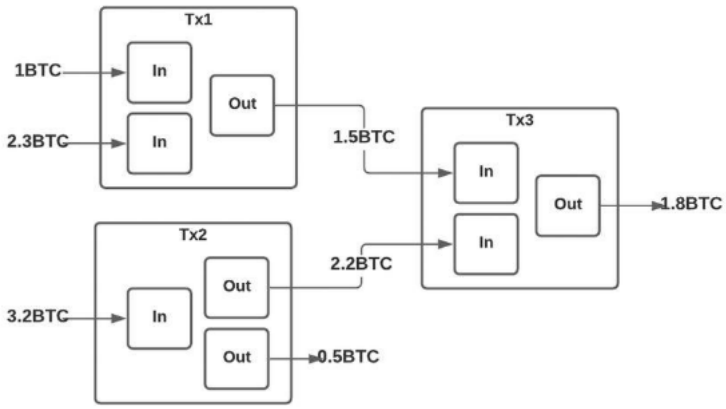

FIGURE 2. UTXO

Transação Bitcoin

- **Entrada:**
  - Conjunto de UTXOs (Unspent Transaction Outputs)
- **Saída:**
  - UTXO (novo output gerado para o destinatário)
  - Transferência
  - *Fee* (taxa para mineradores pela validação da transação)

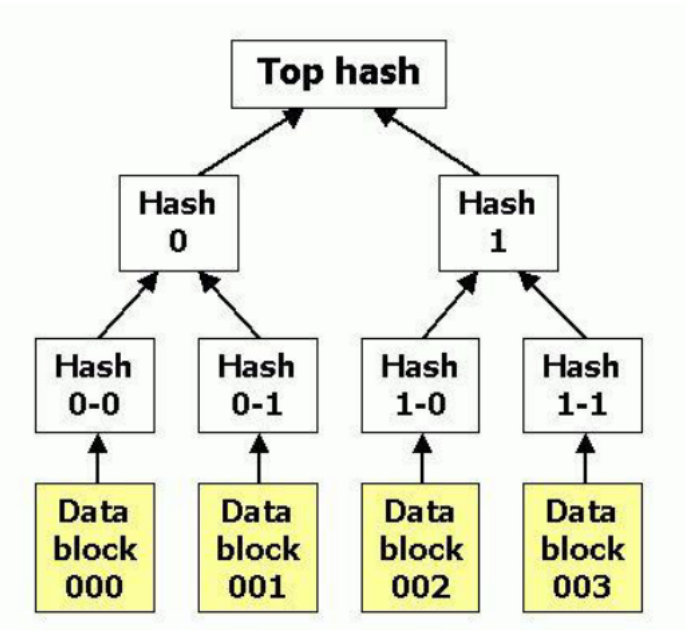

FIGURE 3. UTXO

Árvore de Merkle

Bloco Bitcoin

- **Tamanho:**
  - 1 MB
- **Estrutura:**
  - Árvore de Merkle
  - Utilizada para garantia de integridade e velocidade

. O consenso no Bitcoin é garantido pelo mecanismo de Prova de Trabalho (PoW), que exige um alto gasto de tempo e energia, resultando em uma rede confiável e resistente a manipulações. Esse consenso é não-determinístico, o que significa que forks (bifurcações) na blockchain podem ocorrer, levando a reorganizações para resolver quais transações são válidas. A Prova de Trabalho, embora eficaz em garantir segurança, tem uma alta pegada de carbono, com um consumo estimado superior a 50 TWh por ano entre Bitcoin e Ethereum. Cada transação de Bitcoin consome aproximadamente 1 kWh de energia.

. Atualmente, novos blockchains estão adotando alternativas mais sustentáveis, como o Ethereum, que migrou para Prova de Participação (PoS) após o Merge, visando reduzir o impacto ambiental. A rede Bitcoin, no entanto, continua acessível para qualquer máquina participar e qualquer usuário realizar transações, garantindo a descentralização e a abertura da rede através de pares de chaves gerados aleatoriamente com o algoritmo ECDSA.

. Satoshi Nakamoto revolucionou ao criar um ledger digital público e distribuído com o Bitcoin, integrando tecnologias como redes peer-to-peer, assinaturas digitais e o conceito de ativo digital escasso. Além disso, Nakamoto incorporou um sistema de validação de transações não gastas (UTXO) e usou teoria dos jogos na mineração para resolver fraudes e garantir consenso.

. Desde sua criação, o valor do Bitcoin evoluiu drasticamente, passando de uma moeda com pouco valor, como em 2010, quando 10.000 Bitcoins compraram duas pizzas, para uma unidade valendo cerca de 15.000 dólares em 2022. Hoje, o Bitcoin é visto como reserva de valor, opção de investimento, meio de pagamento e até como moeda nacional em países como El Salvador.