Resumo: Blockchain GoLedger Módulo 2

Gabriel dos Santos Schmitz

Novembro 2024

This document explores public ledgers and Distributed Ledger Technology (DLT) as the foundation for blockchain, a decentralized system where transactions are securely recorded without central authority. Public ledgers allow transparent transaction tracking, while DLT distributes ledger copies across multiple participants to establish trust. Consensus protocols like Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA) maintain data integrity by validating blocks, ensuring a secure record in blockchain networks. Privacy measures, such as separate chains and off-chain storage, protect sensitive data, while tools like Zero Knowledge Proofs (ZKP) enhance security without compromising privacy. Blockchain elements—wallets, nodes, and oracles—facilitate its functionality, while the Byzantine General's Problem illustrates consensus challenges in unreliable networks.

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

Available at https://github.com/gabrielzschmitz/research/tree/main/summaries/ESR-BlockchainCourse

1. Ledgers Públicos

. Um ledger público é uma lista de transações acessível a todas as partes interessadas, que pode ser estruturado de forma permissionada (com controle sobre quem pode escrever) ou não-permissionada (aberta para qualquer participante). Exemplos incluem uma conta-corrente bancária, que funciona como um ledger privado, e o placar de um jogo de futebol, que é um ledger público.

. Em um ledger público, pessoas como Bob, Alice, Charlie e outros podem registrar e verificar transações, garantindo uma ordem cronológica. Neste cenário, qualquer um pode adicionar uma linha, o que torna o processo de registro mais transparente, mas também exige mecanismos para evitar alterações fraudulentas.

. Para evitar que uma pessoa, como Bob, escreva transações em nome de outra, como Alice, são necessários métodos de autenticação que confirmem a identidade de quem realiza cada transação, prevenindo tentativas de fraude e garantindo a integridade das entradas.

. Para autenticar transações, utiliza-se uma chave pública (pk) e um segredo (sk) para cada participante. As funções Sign e Verify trabalham juntas: Sign cria uma assinatura com base no conteúdo e no segredo da pessoa, e Verify valida essa assinatura com a chave pública correspondente, resultando em uma verificação boolean.

. Já para evitar duplicidade, como se Bob tentasse copiar e colar uma linha já assinada, é adicionado um identificador único para cada linha. Esse ID impede que transações sejam repetidas sem um novo registro único, reforçando a autenticidade e originalidade das transações no ledger. Isto ocorre pois o ID é usado na geração do hash da transação.

2. DLTs

. Para que todos possam acessar e confiar no ledger, é essencial que exista confiança entre as partes. A descentralização é facilitada pelo compartilhamento de mensagens entre os participantes, como Alice, Bob, Charlie e outros, para que cada um receba uma cópia atualizada do ledger.

. A Distributed Ledger Technology (DLT) permite que múltiplas cópias de um ledger sejam distribuídas entre os participantes. Esse conceito de registros distribuídos remonta a práticas antigas, como no sistema financeiro do Império Romano, onde informações eram compartilhadas de forma descentralizada.

. Para garantir a segurança no envio de informações entre partes e mitigar falhas e ataques, é necessário um protocolo de consenso. Esse protocolo ajuda a sincronizar as mensagens e resolver problemas de consistência no ledger distribuído, garantindo que as informações sejam confiáveis e atualizadas.

. Consenso é o processo de decisão coletiva entre as partes. Por exemplo, um grupo pode decidir um caminho usando a maioria simples ou um método em que alguns votos (como de personagens azuis) têm mais peso. Consenso permite que os participantes concordem em uma decisão comum, mesmo em cenários complexos.

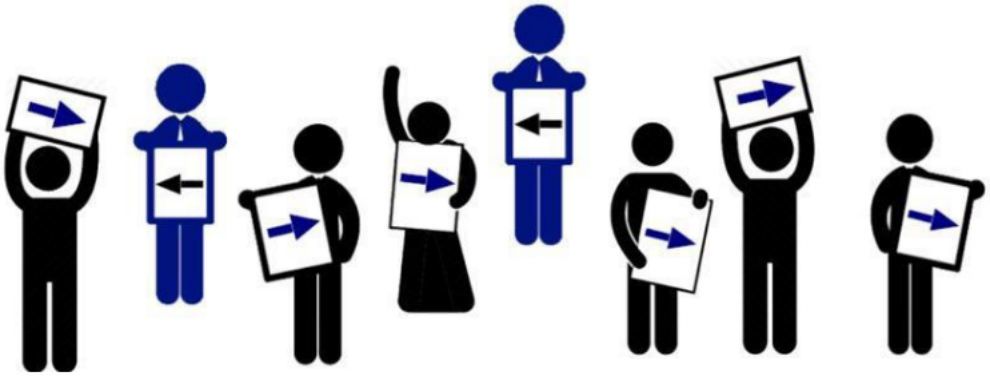

FIGURE 1. Exemplo de Consenso

. Mensagens e transações são agrupadas em blocos, com a gravação do próximo bloco sendo decidida pelas regras de consenso. Esse método de consenso vincula tempo e esforço a registros confiáveis, conectando cada bloco ao anterior por meio de hashes. Assim, qualquer alteração em um bloco altera os hashes subsequentes, protegendo a integridade da cadeia.

. DLT, consenso e blocos conectados formam o protocolo de confiança digital, que possibilita a existência de um ledger digital público e distribuído. Nesse sistema, as transações são compartilhadas e assinadas pelos participantes, e um protocolo de consenso é utilizado para resolver disputas, garantindo a integridade e confiança no registro das operações.

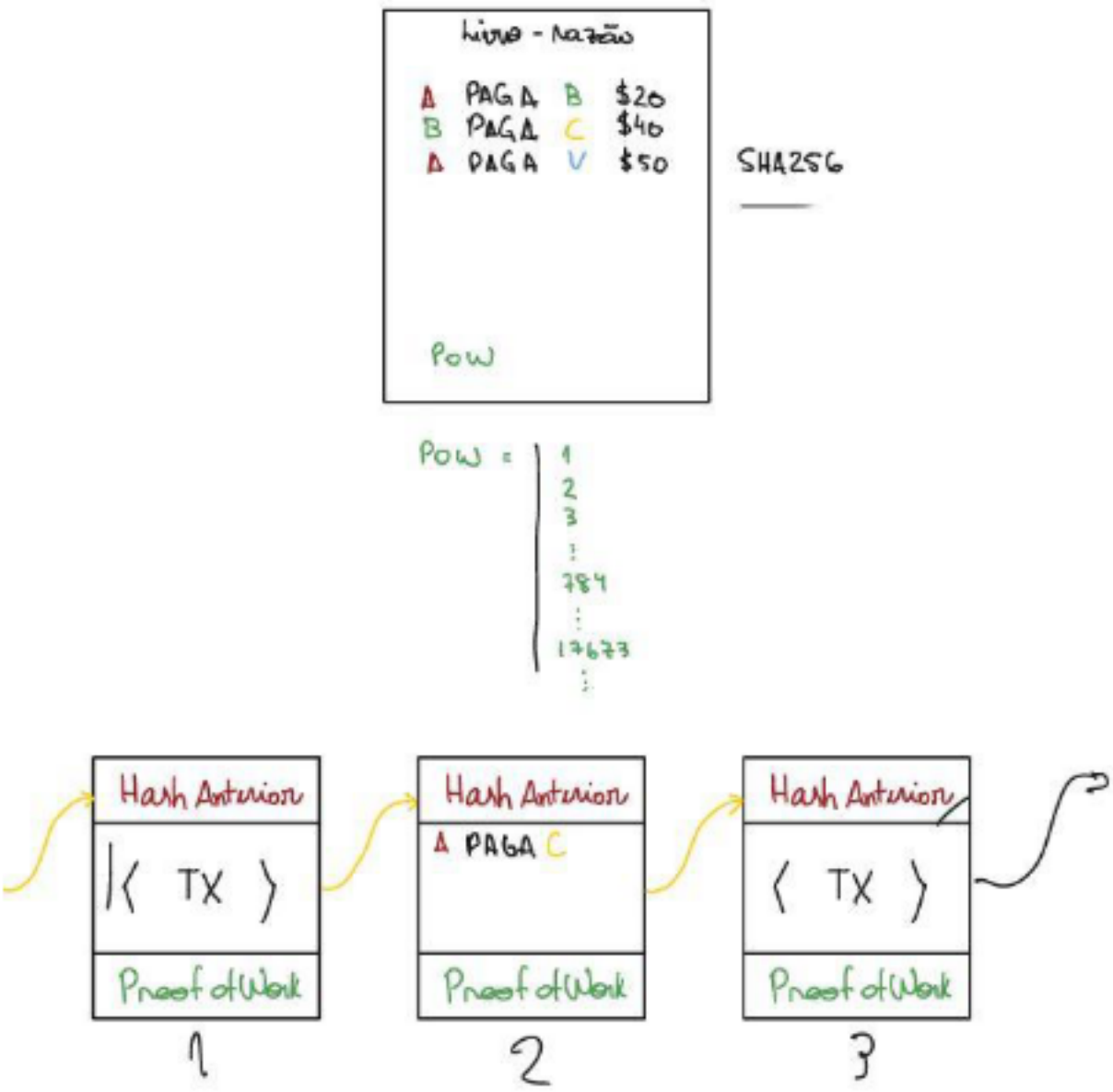

FIGURE 2. DLT + Consenso + Blocos Conectados

3. Conceitos Blockchain

. Blockchain é uma tecnologia de ledger distribuído (DLT) com redundância peer-to-peer, onde as transações são assinadas digitalmente e armazenadas em blocos. Esses blocos são encadeados por meio do hash do bloco anterior, formando uma sequência cronológica. As transações podem conter dados ou programas, e um protocolo de consenso é usado para registrar permanentemente cada bloco na rede.

. Os principais componentes de um blockchain incluem transações, nós (nodes), blocos, o ledger, estado atual (state), contratos inteligentes (smart contracts), rede peer-to-peer, consenso e oráculos. Esses elementos interagem para manter a integridade, segurança e funcionalidade de toda a rede.

. Wallets são plataformas ou dispositivos que gerenciam pares de chaves, identificando pessoas ou entidades que realizam transações na rede. Elas armazenam as chaves privadas e podem operar com criptomoedas ou em redes permissionadas. A segurança pode incluir assinaturas de hardware, autenticação em dois fatores e biometria, além de apresentar o histórico de transações e o saldo de criptomoedas.

. Hierarchical deterministic keys (chaves determinísticas hierárquicas) são geradas por meio de mnemônicos — palavras escolhidas de um conjunto finito —, conforme a proposta BIP-0039. Essas palavras permitem a criação de chaves previsíveis, garantindo consistência e segurança nas transações.

. Nodes são dispositivos que executam o software de blockchain, formando uma rede peer-to-peer distribuída. Eles se conectam com outros nodes e participam da validação de blocos e do algoritmo de consenso. Existem diferentes tipos de nodes: validadores (mineradores ou notários), archive nodes (que armazenam todo o histórico de dados), full nodes (para validação e armazenamento) e light nodes (que apenas armazenam cabeçalhos de blocos).

. Oráculos são fontes externas de dados que alimentam o blockchain com informações do mundo real, criando uma ponte entre sistemas externos e o ledger distribuído. Os dados de oráculos precisam ser convertidos em ativos no blockchain, com fontes variando desde APIs de clima até dispositivos IoT para contagem de produtos.

. O World State é o registro do último estado válido do blockchain, refletindo as mudanças mais recentes. Cada blockchain permissionado usa um banco de dados para armazenar seu World State. Por exemplo, se João vende uma BMW para Mauro, o World State atualizaria para indicar Mauro como o novo proprietário da BMW.

4. Privacidade Blockchain

. A separação em múltiplas chains permite a criação de diferentes ledgers para aumentar a privacidade em uma rede blockchain. Cada ledger pode ter controle de acesso independente, limitando quem pode visualizá-lo. A segurança pode ser garantida pelo

monitoramento das operações de leitura registradas, permitindo um controle mais restrito e personalizado sobre os dados.

. Algumas blockchains suportam o conceito de dados privados, armazenando informações confidenciais em bancos de dados transientes, localizados fora do ledger principal. Essa integração off-chain permite que apenas partes autorizadas acessem dados específicos, protegendo a privacidade sem comprometer a segurança do sistema blockchain.

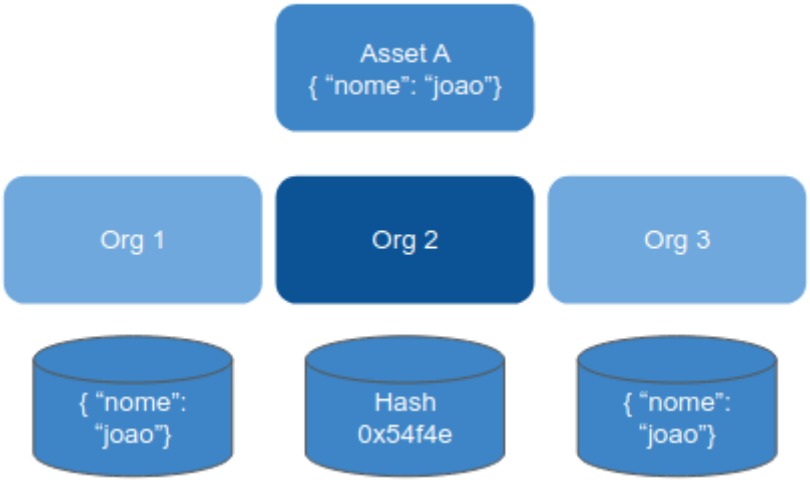

FIGURE 3. Off-chain integrada

. Zero Knowledge Proof (ZKP) é um método que permite provar o conhecimento de uma informação sem revelá-la. Em um exemplo ilustrativo, Alice, que é daltônica, quer garantir que duas luvas sejam da mesma cor. Bob, que conhece as cores, responde a Alice se as luvas são iguais, sem revelar a cor. Alice repete o teste várias vezes; a probabilidade de Bob acertar por sorte diminui exponencialmente com o número de repetições ($(1/2)^n$), tornando a resposta de Bob confiável.

5. Consenso

. O consenso em blockchain inclui mecanismos para assegurar a integridade das transações. Em blockchains não-permissionados, não há garantia de que os nós são confiáveis. Já em modelos permissionados, os participantes são identificados, permitindo controle sobre quem pode propor e validar transações, aumentando a segurança contra ações maliciosas.

. Problema do General Bizantino, dilema matemático, formulado nos anos 80, ilustra as dificuldades de coordenação em redes com comunicações não confiáveis. Imagine batal-

hões cercando um castelo que precisam atacar ou recuar simultaneamente para o sucesso. No entanto, as mensagens entre eles podem ser atrasadas, corrompidas, reordenadas ou interceptadas pelo inimigo, complicando a coordenação e destacando a necessidade de consenso confiável para garantir ações unificadas.

. O PoW foi o primeiro mecanismo de consenso blockchain, projetado para evitar o "double spending" (gasto duplo). Nele, mineradores competem para resolver um problema de hash, e o bloco minerado é validado pela rede. Esse processo é não-determinístico e resiliente ao problema bizantino, embora tenha desafios como a reorganização de cadeias (forks) e ausência de penalidades diretas para mineradores mal-intencionados.

. No PoS, validadores com criptomoedas como colateral competem para registrar novos blocos. Um validador é escolhido aleatoriamente, enquanto os outros verificam a transação. Se houver fraude, o validador é penalizado com a perda do colateral. Esse sistema é bizantinamente tolerante a falhas (BFT), oferecendo uma alternativa mais eficiente ao PoW.

. No PoA, validadores autorizados e identificados registram as transações e validam blocos. Novos validadores precisam ser aprovados para entrar na rede. Esse método pode ser BFT ou não, dependendo das configurações, e é utilizado em redes onde a identidade e a autoridade dos validadores são importantes para o funcionamento seguro e eficiente da blockchain.