FGV EMAp
ESCOLA DE MATEMÁTICA APLICADA

Relatório Blockchain

Sofia Lakschevitz
e
Edilton Brandão

Rio de Janeiro
2024

Sumário

1 Introdução

A blockchain surgiu junto com o Bitcoin em 31 de outubro de 2008 [7]. Naquele dia, Satoshi Nakamoto, pseudônimo da pessoa – ou pessoas – por trás da criptomoeda, publicou o white paper (guia) do BTC, intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System" [6] (Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer).

Cabe ressaltar, no entanto, que Nakamoto não usa exatamente a palavra "blockchain" no documento. Ao longo das nove páginas do material, ele cita apenas os termos "block" e "chain" separados. O termo blockchain, portanto, é um tipo de buzzword (palavra da moda) criado pelo próprio mercado.

2 SHA-256: A Função de Hash na Blockchain

2.1 O que é o SHA-256

A função hash é uma função matemática que transforma qualquer bloco de dados em uma série de caracteres de tamanho fixo composta por números e letras chamada hash. Essa função foi criada para ser resistente à colisão e irreversível, ou seja, qualquer mínima alteração nos dados de entrada resulta num hash imprevisível e significativamente diferente e, por ser uma função unilateral, é praticamente impossível obter os dados originais a partir da série de caracteres.

Um tipo de algoritmo que utiliza funções hash para manter a segurança e integridade de dados digitais é o SHA, Secure Hash Algorithm que tem como sua principal premissa o fato de que o hash é irreversível e único. Uma das versões desse algoritmo é o SHA-2, que foi projetado pela Agência de Segurança Nacional dos Estados Unidos (NSA) junto com o Instituto Nacional de Padrões e Tecnologia (NIST), com o objetivo de introduzir um sucessor ao conjunto SHA-1 que, devido a sua velocidade, produzindo valores hash com apenas 160 bits, é mais suscetível a ataques de colisão, em que diferentes entradas podem produzir o mesmo hash, e ataques de força bruta, em que um invasor tenta todas as entradas possíveis para encontrar uma correspondência ao hash. [8]

A família SHA-2 inclui funções hash com diferentes comprimentos de saída, que são mais seguras graças à criação de hashs com um número maior de bits e com a introdução de novas operações matemáticas. O algoritmo utilizado na blockchain é o SHA-256, que gera um hash de 256 bits (64 caracteres) e passa por várias rodadas de processamento, criando um alto grau de resistência contra ataques.

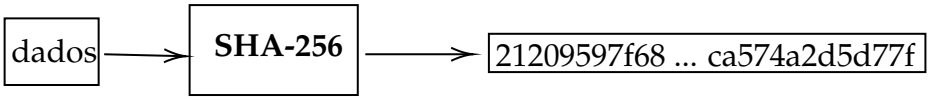

Figura 1: Representação esquemática do SHA-256

2.2 Propriedades

O SHA-256 é um dos algoritmos mais utilizados para o equilíbrio entre segurança e custo computacional de geração, pois é muito eficiente para a alta resistência à colisão que possui. Ele é composto pelos seguintes passos [2]:

Passo 1: Preparação dos Dados de Entrada O dado de entrada, que pode ser de qualquer tamanho, é preenchido com bits extra, para garantir que ele cabe em pedaços de tamanho fixo.

Passo 2: Início O SHA-256 começa com uns valores de hash iniciais constantes, predefinidos e derivados de partes fracionárias das raízes quadradas dos primeiros 8 números primos.

Passo 3: Processamento dos Dados em Blocos Os dados preparados são divididos em blocos de 512 bits.

Passo 4: Função de Compressão Cada bloco é processado em 64 rodadas de operações lógicas, de adições modulares e de trocas de bits, assegurando que uma pequena mudança no dado de entrada vai alterar drasticamente o resultado.

Passo 5: Hash Final Depois do processamento de todos os blocos, os hashs finais são combinados para produzir um hash com 256 bits que é uma impressão digital única da informação original.

A partir desse processo, o SHA-256 possui diversas propriedades que garantem a segurança e integridade dos dados. São elas:

Resistência à Colisão: É estatisticamente improvável que dois dados de entrada distintos produzam o mesmo valor hash.

Efeito Avalanche: Pequenas mudanças nos dados de entrada levam a mudanças significativas no hash, criando um efeito dominó por todos os dados de saída.

Determinismo: Dada a mesma entrada, o SHA-256 gera o mesmo hash de saída.

Resistência à Pré-Imagem: É extremamente difícil de encontrar o dado de entrada a partir do hash final.

Resistência à Segunda Pré-Imagem: É desafiador encontrar uma entrada diferente que produza o mesmo hash que outra entrada dada.

Como resultado dessas propriedades [5], este algoritmo é utilizado em assinaturas digitais, armazenamento de senhas, aplicações de verificação da integridade de dados, certficados SSL/TLS, distribuição de software e criptomoedas.

2.3 Importância na Blockchain

Uma das principais aplicações do SHA-256 está na Blockchain que é um mecanismo que armazena dados sobre transações entre usuários em uma cadeia de blocos e é um processo que demanda transparência, segurança, integridade e consistência devido a sensibilidade dos dados envolvidos. O SHA-256 ajuda a manter essas características primordiais, quando, para cada bloco da cadeia é atribuído um valor hash único baseado em todas as transações armazenadas dentro dele e no hash do bloco

anterior, e quando um bloco é minerado com o processo de Proof of Work (PoW) que valida as transações armazenadas e adiciona o bloco na blockchain.

Além de assegurar os atributos necessários de uma blockchain, o SHA-256 é um algoritmo que é considerado seguro, já que possui fortes propriedades criptográficas que o tornam altamente resistente à ataques. Um ataque conhecido é o Length Extension Attack, que ocorre quando o invasor inclui informação extra num dado e ainda consegue produzir um hash válido, mas pode ter o risco mitigado com a implementação de técnicas como HMAC (Hash-based Message Authentication Code). Adicionalmente, existe o ataque de força bruta, no qual o invasor tenta todas as entradas possíveis até achar uma que corresponde ao hash final escolhido, mas é inviável devido a vasta possibilidades de dados de entrada (o número de combinações possíveis para um hash de 256 bits é extremamente alto). Existe também a computação quântica, que tem o potencial de quebrar muitos sistemas criptográficos atuais, resolvendo problemas mais rapidamente do que computadores clássicos, mas hoje o SHA-256 permanece seguro contra esse tipo de ataque.

Desse modo, a segurança do SHA-256 permite que ele seja utilizado globalmente em várias aplicações críticas desde proteger comunicação na internet a proteger moedas digitais.

3 Blockchain

3.1 O que é Blockchain

Blockchain é um mecanismo de banco de dados descentralizado, imutável e compartilhado que registra informações sobre transações entre usuários em uma cadeia de blocos, utilizando criptografia para garantir a segurança dos dados. Diferentemente de outros tipos de bancos de dados, a blockchain não é controlada por uma autoridade, mas por uma rede peer-to-peer. Ou seja, cada computador participante da rede (também chamado de nó) possui uma cópia da blockchain, garantindo transparência, e para que um novo bloco seja adicionado ou qualquer alteração seja feita, é preciso da aprovação de cada um deles, verificando a validade dos dados.

À medida que cada transação ocorre, ela é registrada em um "bloco"de dados com todas as suas informações. Cada bloco, depois de atingir certo número de transações registradas e obter o consenso de todos os nós da rede de que os dados são válidos, é adicionado à cadeia de modo linear e cronológico. E, como dito anteriormente, os blocos da blockchain sempre possuem um hash baseado em suas transações e no bloco anterior, o que auxilia na sua imutabilidade, já que mudando os dados de uma transação, o hash final do bloco muda drasticamente e este erro pode ser facilmente verificado através da comparação entre as cópias da comunidade.

3.2 Estrutura básica

A estrutura de um bloco da blockchain é constituída por, basicamente, quatro partes: os dados, o nonce, o hash do bloco anterior e o hash do bloco em questão.

Nos dados de cada bloco estão localizadas todas as transações com as suas respectivas informações como o que ou quantas criptomoedas foram transferidas, quem foi o pagante, quem foi o recebedor e em que data e em qual horário o envio foi realizado.

O nonce (abreviação de "number used once") é um número pseudo-randômico, encontrado pelo processo de mineração, que modifica o hash final do bloco para ficar de acordo com o nível de dificuldade da rede. Ele é necessário para garantir a segurança da blockchain no processo de mineração, impedindo que uma transação seja submetida repetidamente por más intenções.

O hash do bloco anterior é o hash formado pelas mesmas informações sobre o bloco anterior através do algoritmo SHA-256. E, similarmente, o hash do bloco vigente é criado a partir de todas as três partes anteriores, também pelo SHA-256.

Uma vez que o hash final do bloco é composto pelos dados das transações, pelo nonce e pelo hash do bloco anterior, a blockchain vira um mecanismo mais válido e mais difícil de ser violado. [3]

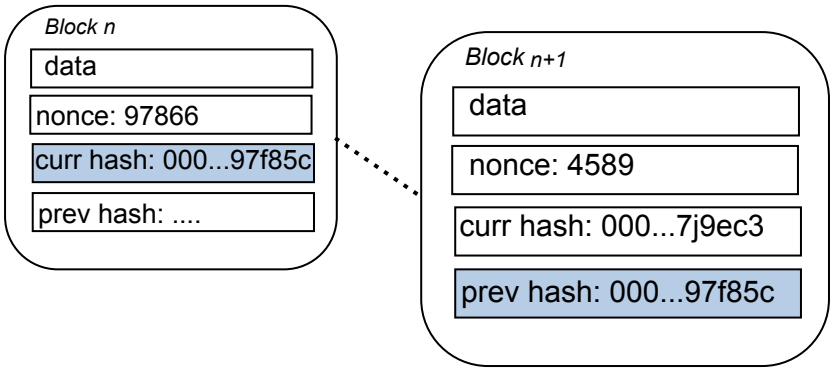

Figura 2: Representação da estrutura de um bloco na Blockchain

3.3 Chave pública e privada

Um recurso de segurança para identificar de forma exclusiva os membros da blockchain é a criptografia de chaves pública e privada.

Cada nó possui uma chave privada, que é um código que deve ser mantido em sigilo para assinar transações, e, criada a partir dela, uma chave pública, que é um código que pode ser compartilhado com os outros integrantes da rede para receber transações e verificar assinaturas digitais.

Ao registrar uma transação, o usuário utiliza a sua chave privada para criar uma assinatura digital única. Quando o bloco no qual a transação está localizada e criptografada passa pelo algoritmo de consenso, todos os nós da rede precisam confirmar a legitimidade dos dados. Para isso, eles utilizam a chave pública do usuário que criou a transação para descriptografá-la e verificar se ela foi, de fato, assinada por sua chave privada. Como ambas as chaves são processadas pelo SHA-256 e a relação entre

as duas chaves é estabelecida por meio de uma função matemática unidirecional, é inviável calcular a chave privada a partir da chave pública.

Dessa forma, a criptografia de chaves pública e privada adiciona uma camada adicional de segurança, impedindo a falsificação e garantindo a integridade das transações na blockchain. [1]

3.4 Mineração

Mineração é o processo pelo qual redes especializadas de computadores verificam as novas transações de um bloco de dados para adicioná-los à rede blockchain. Um desses algoritmos de validação é o Proof of Work (PoW) que é utilizado em diversas redes blockchain.

Conforme o PoW, para cada bloco, os mineradores (rede de computadores) utilizam recursos computacionais substanciais e um alto poder de processamento em uma espécie de corrida para resolver problemas matemáticos complexos e realizar uma abordagem de tentativa e erro com o objetivo de descobrir o nonce correto. Esse nonce é o valor que, quando combinado com os dados do bloco, gera um hash (utilizando o SHA-256) que começa com uma quantidade específica de zeros. O número de zeros determina a dificuldade do problema: quanto maior a quantidade de zeros, mais difícil é encontrar o nonce correto. O primeiro minerador a encontrar o nonce que gera o hash desejado, com o consenso dos membros da rede, adiciona o novo bloco à blockchain e ganha uma recompensa, como, por exemplo, bitcoins.

Adicionalmente, o número médio de tentativas no PoW é automaticamente ajustado para garantir que um bloco novo seja gerado a cada 10 minutos em média. Esse ajuste de dificuldade é diretamente relacionado ao poder de hashing dedicado à rede. Ou seja, quanto maior o poder computacional da rede (mais mineradores tentando resolver o problema), maior deve ser a dificuldade para manter a média de 10 minutos para a validação de um bloco.

A mineração é crucial para a segurança e acuracidade dos dados na blockchain, além de ser o processo que, no caso das criptomoedas, introduz novas moedas para circulação. [4]

4 Trabalho computacional

O projeto computacional consistiu na criação de um site chamado MiniChain, com o objetivo de ilustrar os conceitos fundamentais de uma blockchain. Este projeto abrange a criação de blocos, mineração, validação de integridade e manipulação de dados para simular a segurança e imutabilidade características dessa tecnologia. O site pode ser acessado em `https://minichain.onrender.com`, e o repositório do trabalho está disponível no GitHub `https://github.com/edilton-bs/MiniChain`.

5 Conclusão

A tecnologia blockchain se destaca como uma solução robusta para garantir a segurança e a integridade de dados em um ambiente digital. O algoritmo SHA-256

desempenha um papel central nesse contexto, proporcionando resistência à colisões, determinismo e o efeito avalanche, que são essenciais para assegurar a imutabilidade e a confiabilidade das informações registradas. O equilíbrio entre segurança e custo computacional do SHA-256 o tornam indispensável na construção de sistemas baseados em blockchain, permitindo que sejam superados desafios como a proteção de dados e a construção de confiança digital. Assim, a blockchain, sustentada por fundamentos criptográficos consistentes, consolida-se como uma ferramenta essencial no gerenciamento de informações.

Referências

[1] Blockchain.com. *What are public and private keys and how do they work?* Accessed: Dec. 4, 2024. 2024. URL: https://support.blockchain.com/hc/en-us/articles/4417082520724-What-are-public-and-private-keys-and-how-do-they-work.

[2] SSL Dragon. *O que é o Algoritmo SHA-256?* Acesso em: 04 dez. 2024. 2024. URL: https://www.ssldragon.com/pt/blog/que-e-algoritmo-sha-256/.

[3] GeeksforGeeks. *Blockchain Structure*. Accessed: Dec. 4, 2024. 2024. URL: https://www.geeksforgeeks.org/blockchain-structure/.

[4] Investopedia. *Proof of Work (PoW) em Blockchain*. Acesso em: 04 dez. 2024. 2024. URL: https://www.investopedia.com/terms/p/proof-work.asp.

[5] Madan. *A Deep Dive into SHA-256: Working Principles and Applications*. Acessado em: 04 de dezembro de 2024. 2023. URL: https://medium.com/@madan_nv/a-deep-dive-into-sha-256-working-principles-and-applications-a38cccc390d4.

[6] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[7] Wikipedia. *Blockchain*. Acessado em: 04 de dezembro de 2024. 2024. URL: https://pt.wikipedia.org/wiki/Blockchain.

[8] Wikipedia. *SHA-2*. Acessado em: 04 de dezembro de 2024. 2024. URL: https://pt.wikipedia.org/wiki/SHA-2.