A Matemática Discreta Por trás do Bitcoin: Blockchain

Florianópolis, 3 de novembro de 2025

Mathias Petry Peixoto
Artur de Faria Rodrigo
Daniela Oliveira de Ambrosio

Introdução:

Este trabalho tem como objetivo apresentar as aplicações da Matemática Discreta no funcionamento do blockchain no Bitcoin, tecnologia que se tornou uma das maiores inovações do século XXI. A escolha do tema se deve ao fato de o blockchain ser uma aplicação prática de fundamentos matemáticos que tornam possível a criação de sistemas descentralizados, confiáveis e resistentes a fraudes.

Entre os principais conceitos da disciplina relacionados ao tema estão a aritmética modular, presente nas funções de hash e responsável por garantir a integridade dos blocos; o Teorema do Pombal, que aborda a possibilidade teórica de colisões nos algoritmos de resumos criptográficos; e a teoria dos números, especialmente na parte de aritmética modular, fundamenta a criptografia assimétrica. Essa, por sua vez, emprega algoritmos como o ECDSA, os quais possibilitam as assinaturas digitais, essenciais para a autenticação de transações.

Além disso, conceitos de combinatória e probabilidade discreta são aplicados na prova de trabalho, mecanismo de consenso que envolve a geração e a verificação de números específicos durante a mineração de novos blocos. Por fim, a própria cadeia de blocos é organizada como um grafo, demonstrando como diversos conceitos da disciplina se conectam diretamente com a tecnologia blockchain.

O trabalho busca mostrar como a confiança no blockchain não depende de instituições ou autoridades centrais, mas da própria matemática.

Aplicação:

O que é Blockchain?

A blockchain é uma estrutura de dados formada por uma sequência de blocos encadeados, como um grafo, onde cada bloco registra um conjunto de transações validadas por criptografia assimétrica e protegidas por funções de hash. Esses blocos estão distribuídos entre diversos computadores interligados, sem um servidor central, o que torna o sistema descentralizado e imutável. O Bitcoin, tem uma rede de blockchain pública, sendo este, o tipo que nos aprofundaremos mais neste trabalho. A sua cadeia de blocos funciona como um registro público que armazena todas as transferências da criptomoeda de forma segura, transparente e resistente a fraudes.

1. O funcionamento das funções hash e a matemática discreta por trás:

1.1 O que é função hash:

Uma Função Hash é um algoritmo matemático que faz com que uma entrada de qualquer tamanho tenha uma saída com um tamanho fixo, chamada de valor de hash. É como uma "impressão digital" do dado, útil para verificar a integridade de arquivos, pois qualquer alteração no conteúdo original resulta em um hash completamente diferente. Dentre as funções hash existem diversos tipos de algoritmos diferentes que mudam o tamanho da saída, usando mais ou menos bits. Nesse PDF iremos nos referir ao algoritmo SHA-256, que produz uma hash de 64 caracteres hexadecimais (256 bits).

1.2 Contexto de aplicação do hash

Dentro da tecnologia de blockchain a função hash tem como uma de suas várias aplicações a ligação entre os blocos e funciona da seguinte forma: O hash do bloco anterior é incluído dentro do novo bloco. Isso cria uma corrente de dependência entre os blocos, se alguém tentar alterar qualquer dado em um bloco antigo, o hash desse bloco muda, e, consequentemente, o hash de todos os blocos

seguintes também se torna inválido, Essa propriedade é chamada de efeito avalanche.

A entrada da função também não é aleatória. Cada bloco do blockchain contém um cabeçalho com várias informações, como: o hash do bloco anterior, resumo das transações (chamado de merkle root), a data e hora (timestamp), um número aleatório (nonce) e outros dados técnicos.

O sistema combina todas essas informações e calcula seu hash com o algoritmo SHA-256. No caso do Blockchain, o hash final do bloco é obtido aplicando o SHA-256 duas vezes: ***Hash do bloco = SHA256(SHA256(cabeçalho do bloco))***

Essas funções trabalham com números binários de tamanho fixo **X** e realizam operações que precisam permanecer dentro desse limite. Sempre que um cálculo ultrapassa o valor máximo possível, o resultado “volta ao início”, ou seja, é reduzido módulo 2^x, conforme definido pela aritmética modular.

Durante o cálculo do hash, são feitas somatórias, rotações e deslocamentos binários, todas operando sob essas restrições modulares. Isso garante que cada passo produza resultados consistentes e imprevisíveis, mantendo a integridade do algoritmo. Graças à aritmética modular, mesmo pequenas mudanças nos dados de entrada geram valores de hash completamente diferentes, um comportamento essencial para a segurança e irreversibilidade das funções hash e, consequentemente, para a confiabilidade da blockchain, além de permitir uma verificação rápida (o hash permite confirmar a validade de um bloco sem precisar ler todas as transações).

1.3 Colisões:

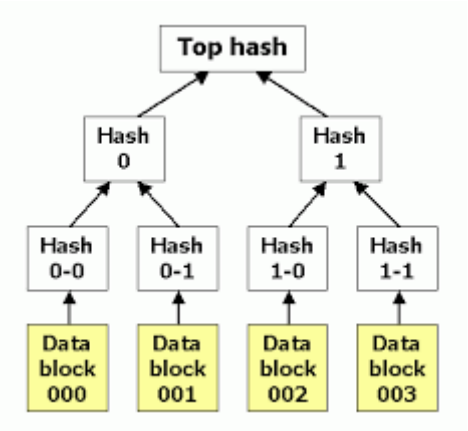
As funções hash podem apresentar colisões (quando duas entradas diferentes geram o mesmo valor), algo inevitável matematicamente pelo princípio de Pombal, já que o domínio é infinito e o número de saídas é limitado (2^{256}). No entanto, na prática, os algoritmos de hash usados na blockchain tornam extremamente difícil produzir duas mensagens diferentes com o mesmo hash, devido à resistência criptográfica do SHA-256.

Além disso, cada nó mantém sua própria mempool (memory pool), que é o espaço onde ficam as transações pendentes antes de entrarem em um bloco. Nesse processo, o nó rejeita qualquer transação duplicada, ou seja, impede que duas transações com o mesmo TxID coexistam ao mesmo tempo.

Assim, apesar da possibilidade matemática de colisões, evidenciada pelo Teorema de Pombal, a combinação entre a resistência do SHA-256 e a validação distribuída da rede faz com que a ocorrência prática dessas colisões seja considerada muito improvável.

1.4 Árvore de Merkle e Nonce:

A Árvore de Merkle é uma estrutura de dados utilizada na blockchain para organizar e verificar transações de forma eficiente e segura. Ela funciona como uma árvore binária, na qual cada folha representa o hash de uma transação, e cada nó intermediário é o hash da combinação dos nós filhos. No topo dessa estrutura está o Merkle root, um único hash que resume todas as transações de um bloco.



O nonce (do inglês number used once, ou “número usado uma vez”) é um valor numérico variável incluído nos dados antes da geração de uma função hash. Sua função é alterar o resultado da hash sem modificar as informações principais do conteúdo. O objetivo do nonce é de variar o hash a ponto de chegar na condição requerida do hash do próximo bloco, parte que envolve a prova de trabalho que abordaremos posteriormente. Dessa forma, o nonce é fundamental para manter a unicidade, imprevisibilidade e segurança criptográfica dos hashes gerados para cada bloco.

1.5 Conceitos de matemática discreta relacionados:

As funções de hash, apoiadas em princípios da matemática discreta como as estruturas combinatórias (árvores e grafos), formam a base lógica da segurança da blockchain. Elas garantem a integridade e a unicidade, preparando terreno para os mecanismos de autenticação (criptografia assimétrica) e consenso (prova de trabalho).

2. Criptografia, Assinatura Digital e Confiabilidade:

2.1 Criptografia Assimétrica:

O modelo no qual existe um par de chaves: pública e privada, é chamado de criptografia assimétrica, pois ao utilizar uma chave para criptografar um dado, ele só pode ser descriptografado usando a outra chave. E esse é o mecanismo responsável por viabilizar a segurança da rede citado no artigo de Satoshi Nakamoto.

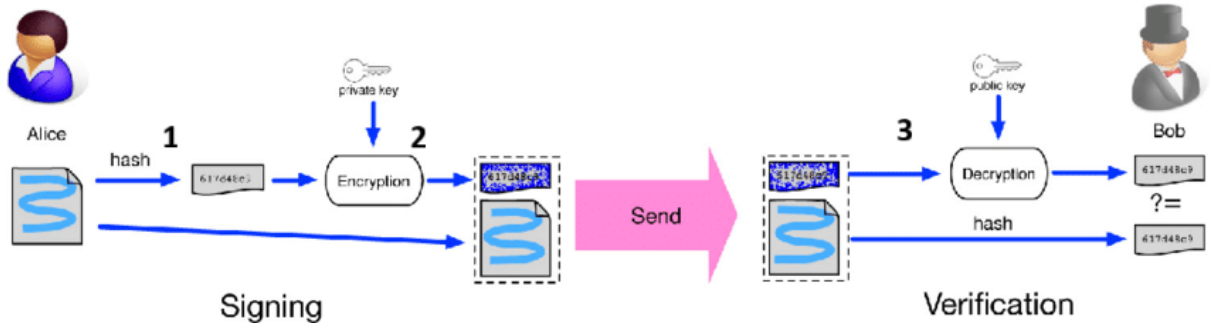
- **Chave privada:** Deve ser guardada em segredo.
- **Chave pública:** É divulgada livremente entre a rede, funcionando como um endereço.

Para ingressar na blockchain do Bitcoin, o usuário precisa instalar um aplicativo, também chamado de carteira digital, que permite que ele realize transações. A carteira contém o par de chaves, que são números utilizados nos cálculos matemáticos, o algoritmo mais utilizado no contexto de Blockchain para a geração desse par de chaves é o ECDSA: Algoritmo de Assinatura Digital de Curva Elíptica, cujo funcionamento é sustentado graças a aritmética modular.

2.2 Assinatura Digital:

Para que os dados de uma transação sejam validados e aceitos pela rede, é necessário que o usuário que deseja realizar a transferência prove a sua autoria. Este processo é realizado através da assinatura digital, que não é uma criptografia do dado, mas sim uma prova matemática da posse da chave privada. O processo segue os seguintes passos:

1 Usando o Hash: Primeiro, todos os dados da transação contidos no cabeçalho são submetidos a uma função *hash* criptográfica (como o SHA-256), gerando um resumo único e de tamanho fixo (como visto anteriormente).
2 Assinatura: O usuário então utiliza sua chave privada para realizar uma operação matemática complexa sobre esse *hash*, gerando um par de valores numéricos (como os valores *r* e *s* no ECDSA). Este par de valores é a Assinatura Digital.
3 Verificação: A transação e a assinatura são transmitidas à rede de mineradores. Qualquer nó pode usar a chave pública do usuário e o *hash* da transação para verificar a autenticidade da assinatura.



Dessa forma, assinatura digital garante:

- **Autenticidade:** porque somente o detentor da chave privada poderia ter assinado, já que ela é secreta.
- **Integridade:** pois se a transação for alterada, a assinatura se torna inválida graças a natureza das funções hash.

3. Prova de trabalho

3.1 O papel do minerador:

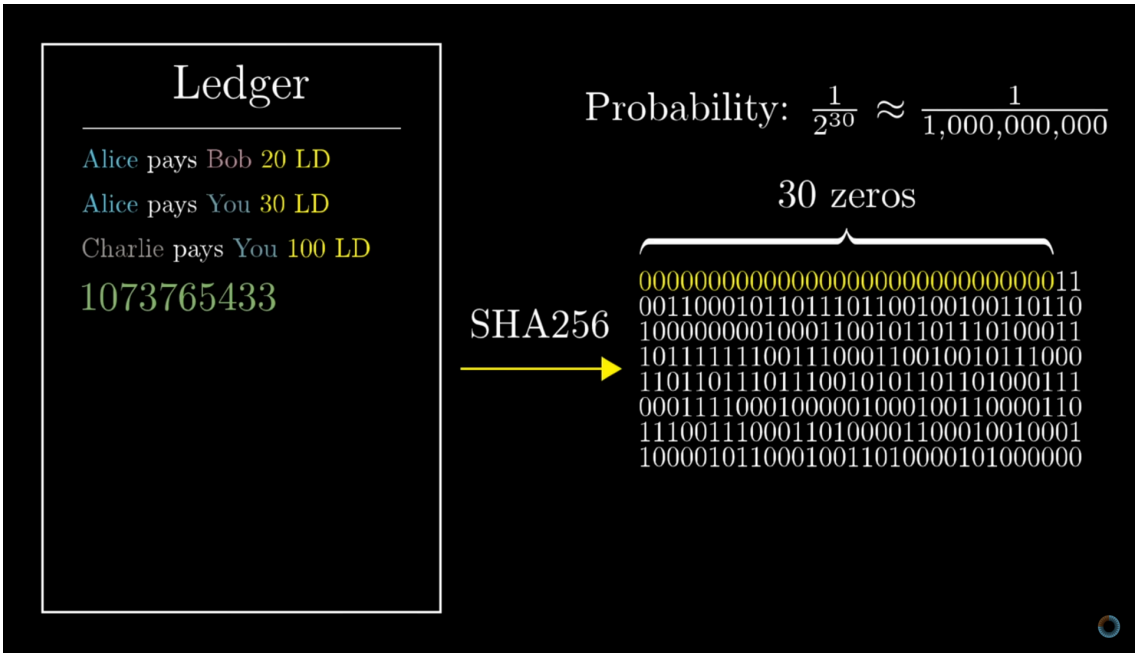
Os mineradores são pessoas que validam transações e registram novos blocos na blockchain. Eles reúnem transações pendentes da **mempool** e tentam formar um bloco válido. Para isso, competem para resolver um desafio matemático complexo que demanda um investimento de recursos financeiros em equipamentos com grande capacidade computacional e alto consumo energético, como discutido no artigo de *SORIA (2023)*. Quando conseguem resolver o desafio corretamente e o bloco é validado pela rede, os mineradores são recompensados com bitcoins. Caso o bloco contenha erros ou tentativas de fraude, o trabalho é rejeitado, e todo o

investimento em energia e tempo é perdido, fato que torna economicamente inviável tentar falsificar algo no sistema.

3.2 Conceito de Prova de Trabalho e sua relação com matemática discreta:

A Prova de Trabalho é um **mecanismo de consenso utilizado na blockchain do Bitcoin** (existem outras formas de obter consenso que são utilizadas em outras aplicações). A Prova de Trabalho define quem adiciona o próximo bloco à blockchain, partindo do desafio matemático citado, que consiste em encontrar um número (nonce) que, ao ser combinado com os dados do bloco e processado por uma função dupla de SHA-256, gere um hash de uma forma específica como for definido pela rede. Na prática, isso significa produzir um hash que possua um certo número de **zeros à esquerda.**

Esse processo envolve probabilidade discreta e combinatória, pois cada tentativa representa uma combinação distinta de entradas, e apenas uma entre bilhões satisfaz a condição exigida. **Devido a essa dificuldade probabilística descrita para encontrar o nonce, podemos garantir confiabilidade na geração de novos blocos.** Quanto maior o poder computacional do minerador, maiores são suas chances de encontrar o hash válido.



3.3 Como a Prova de Trabalho garante o consenso:

A rede adota como legítima a **cadeia com o maior trabalho acumulado**, ou seja, aquela em que se investiu mais poder computacional (mais blocos). Para fraudar o sistema, seria necessário refazer as provas de trabalho anteriores (pois cada bloco tem um hash baseado nos dados do bloco anterior) e ainda superar **mais de 50% do poder computacional global** para continuar fraudando os próximos blocos e se manter como a cadeia mais longa, o que é praticamente impossível.

Essa dinâmica garante o que chamamos de **consenso** dentro da blockchain, em que a integridade dos blocos é verificada coletivamente. Essa verificação é possível porque **todos os usuários mantêm uma cópia completa da blockchain**, e a cada 10 minutos mineradores geram novos blocos carregando o hash do anterior, garantindo transparência e confiabilidade a todo o sistema.

Os autores deste trabalho utilizaram de LLMs para melhoria de texto e compreensão de conceitos complexos relacionados ao funcionamento da tecnologia de blockchain.

Referências:

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. *15.S12 Blockchain and Money — Fall 2018*. Disponível em: http://www.youtube.com/playlist?list=PLUl4u3cNGP63UUkfL0onkxF6MYgVa04Fn. Acesso em: 7 nov. 2025.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [S.l.: s.n.], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 7 nov. 2025.

RIBEIRO, L. *Introdução à Blockchain e Contratos Inteligentes: apostila para iniciantes*. Relatório Técnico – INE/UFSC, Florianópolis, 2021. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/221495/RT-INE2021-1.pdf. Acesso em: 7 nov. 2025.

SORIA, J. Optimal mining in proof-of-work blockchain protocols. *Future Generation Computer Systems*, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S1544612322007863. Acesso em: 12 nov. 2025.

SONG, J. *Programming Bitcoin*. [S.l.: s.n.], [20--]. Disponível em: https://cdn.bookey.app/files/pdf/book/en/programming-bitcoin.pdf. Acesso em: 7 nov. 2025.

VILA REAL, Sérgio. *Funções hash na blockchain* [vídeo]. Disponível em: https://www.youtube.com/watch?v=H5__Qgtlg6k. Acesso em: 7 nov. 2025.

XU, X. et al. *Blockchain: Principles and Applications*. Disponível em: https://dl.acm.org/doi/10.1145/3205230.3205238. Acesso em: 7 nov. 2025.

3BLUE1BROWN. *How does Bitcoin actually work?* [vídeo]. 2017. Disponível em: https://www.youtube.com/watch?v=bBC-nXj3Ng4. Acesso em: 7 nov. 2025.