BLOCKCHAIN

BLOCKCHAIN

LISTA DE FIGURAS

SUMÁRIO

1 CONCEITOS DA TECNOLOGIA BLOCKCHAIN

A tecnologia Blockchain (cadeia de blocos) é definida de forma simples como um livro-razão descentralizado e distribuído que registra a rastreabilidade de um ativo digital. Desde a sua criação, os dados em uma blockchain não podem ser modificados e excluídos, o que a torna uma tecnologia disruptiva para setores como pagamentos, ativos digitais, segurança, entre tantos outros.

Desde sua criação, um dos grandes problemas que a blockchain nasceu para resolver foi o gasto duplo. Não é possível enviar o mesmo ativo para duas pessoas, algo que pode acontecer dentro de um banco de dados, dependendo da arquitetura com que ele foi criado. Explico logo abaixo:

Imagine que duas pessoas estão fazendo uma transação de dinheiro, vamos supor que o remetente tenha enviado corretamente o dinheiro de seu banco, não há chance de a transação falhar, certo? Na verdade, há várias coisas que podem dar errado, incluindo:

- Algo pode ter dado errado no banco de dados (como um problema técnico).
- A conta do remetente pode ter sido hackeada.
- Os limites de transferência do dia podem ter sido excedidos.
- Debitado de uma conta, nunca creditado no outro lado.
- Problemas com dados.

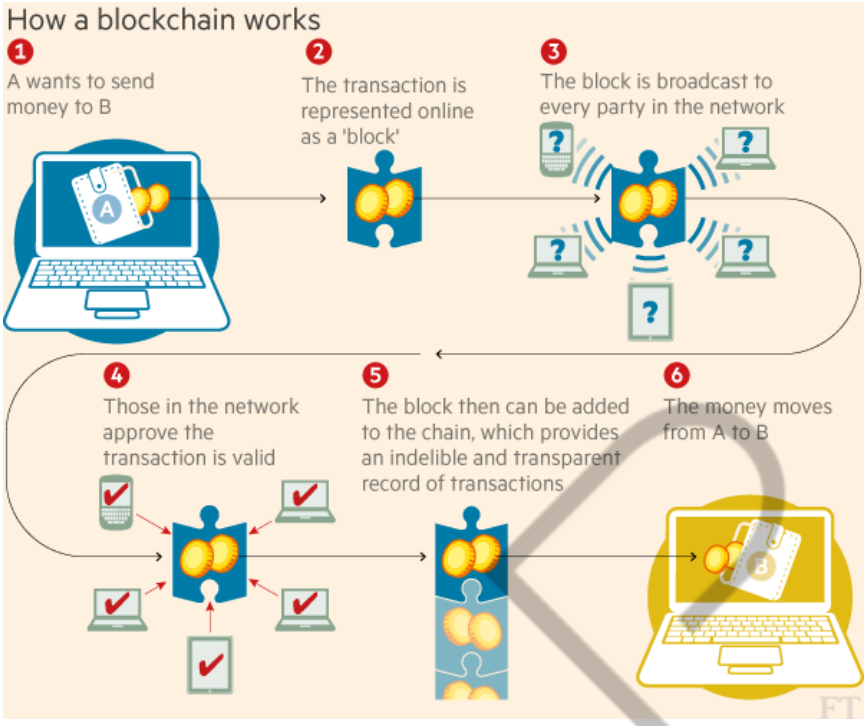


Figura 1 - Como a blockchain funciona

Fonte: https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/

Todas essas transações são armazenadas na estrutura de livro-razão digital. Em termos práticos, funciona como uma planilha contendo todos os inúmeros nós de uma rede e tem o histórico de todas as compras feitas por cada nó. As informações contidas no livro digital são altamente seguras e a assinatura digital protege contra adulterações.

A parte mais interessante desse livro é que qualquer um pode ver os dados, mas ninguém pode corrompê-los. Podemos fazer uma analogia ao Google Spreadsheet, em que qualquer pessoa com acesso pode inserir informações em tempo real, já no caso da blockchain funciona da mesma forma, no entanto, só é possível inserir não podendo deletar e nem alterar o dado que outro participante já inseriu.

De forma geral:

- Blockchain é um banco de dados que armazena blocos de dados criptografados e os encadeia para formar uma única fonte de verdade cronológica para os dados.

- Os ativos digitais são distribuídos em vez de copiados ou transferidos, criando um registro imutável de um ativo.
- O ativo é descentralizado, permitindo acesso total em tempo real e transparência ao público.
- Um registro transparente de alterações preserva a integridade do documento, o que cria confiança no ativo.
- As medidas de segurança inerentes ao Blockchain e o livro-razão público o tornam uma tecnologia primordial para quase todos os setores.

"O objetivo de usar a blockchain é permitir que as pessoas – em particular, as pessoas que não confiam umas nas outras – compartilhem dados valiosos de maneira segura e inviolável" - Revisão de Tecnologia do MIT.

Para entender como funciona a blockchain, é necessário entender o que está por de trás dos blocos: nós (nonce) e mineradores.

1.1 Blocos

Em um nível alto, um bloco consiste em uma lista de dados. Uma "cadeia" é um conjunto de blocos de dados que cresce constantemente ao longo de um período de tempo. Se a transação estiver inserida na blockchain, será extremamente difícil ou impossível alterar esses dados. Isso torna a blockchain um meio único de armazenar dados valiosos.

Imagine uma torre digital de blocos, sobre a qual um novo bloco de dados é adicionado a cada 10 minutos a partir do "bloco de gênese" original na base da torre. Isso é exatamente o que acontece na rede Bitcoin. Os dados em cada bloco consistem em transações financeiras transmitidas por usuários da rede juntamente com evidências criptográficas de que essas transações são válidas.

A figura abaixo mostra como os blocos são encadeados.

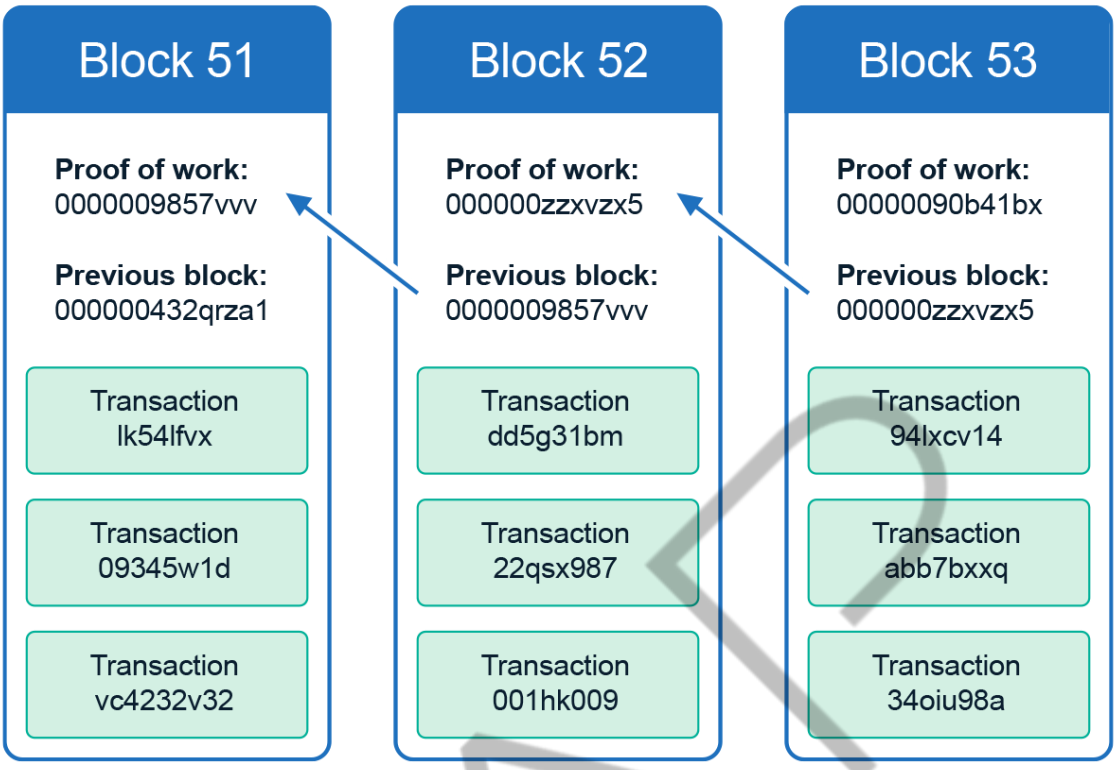


Figura 2 – Encadeamentos de blocos
Fonte: https://ghostvolt.com/articles/blockchain_intro.html

1.2 Mineração

Mineração é a extração da moeda digital usando equipamentos especiais, ou seja, computadores potentes.

Quando a criptomoeda apareceu pela primeira vez, ela poderia ser minerada usando um computador simples. Com o tempo, os mineradores começaram a aprimorar os equipamentos.

A mineração é a junção de blocos que armazenam informações sobre transações. Como resultado, eles formam uma cadeia contínua e consistente.

Para anexar um bloco, é necessário resolver um determinado problema matemático decifrando o algoritmo da criptomoeda. Caso o equipamento encontre a resposta correta, seu dono recebe uma recompensa em forma de moedas digitais, ou seja, recebe Bitcoin.

Ao mesmo tempo, quanto mais os mineradores buscam resolver o problema, mais difícil é encontrar a resposta certa e o custo aumenta.

Abaixo uma imagem ilustrando como funciona a mineração do bitcoin.

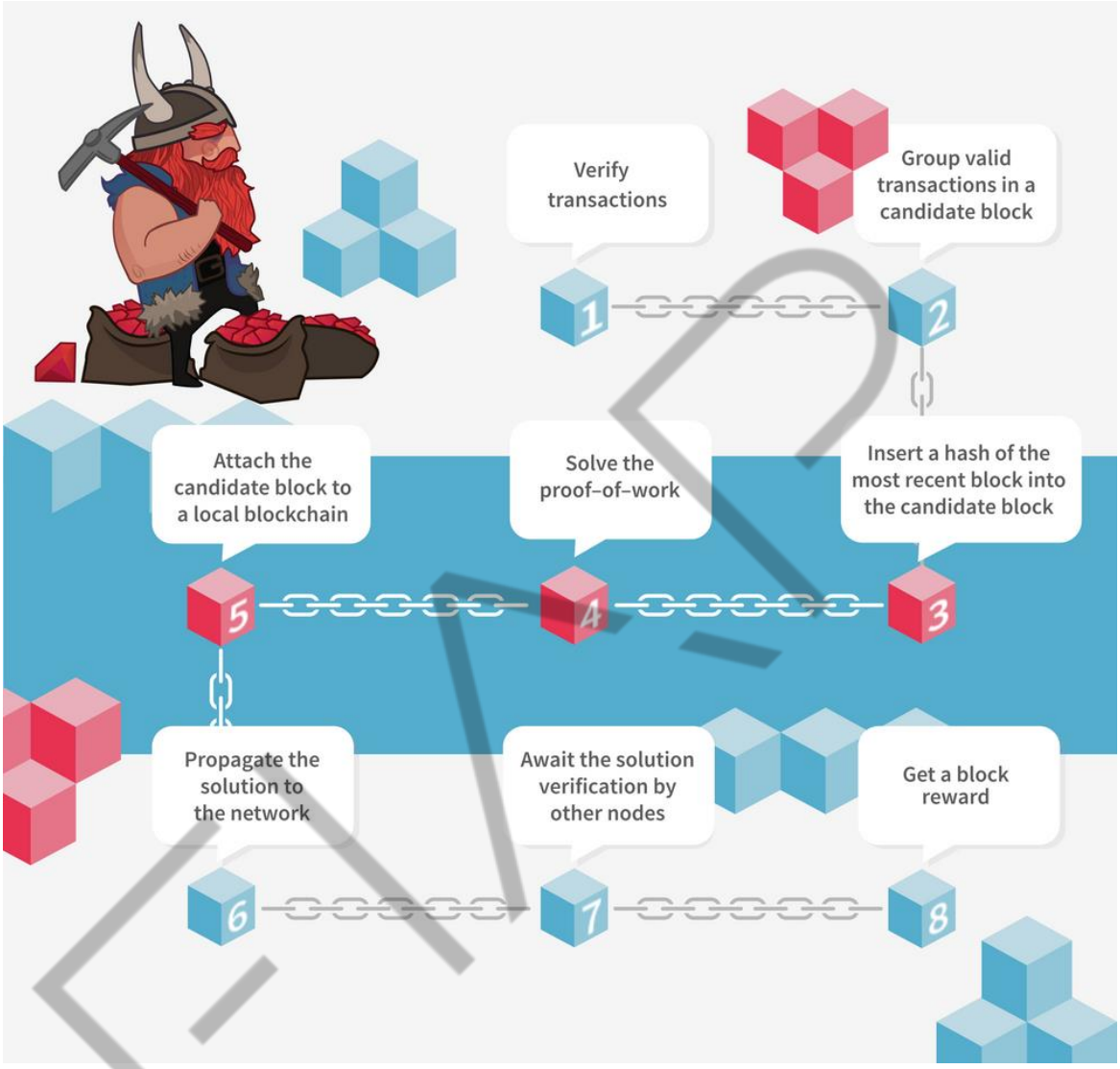


Figura 3 - Mineração
Fonte: https://blog.ragnarson.com/2016-12-01-blockchains-a-brief-introduction/

1.3 Nó (Node)

O termo “nó” é utilizado para cada transação registrada cronologicamente e distribuída para uma série de dispositivos conectados. Esses dispositivos são chamados de nós. Esses nós se comunicam dentro da rede e transferem informações sobre transações e novos blocos.

É um componente crítico da infraestrutura blockchain. Ajuda a manter a segurança e a integridade da rede. O principal objetivo de um nó blockchain é verificar cada lote de transações de rede, chamado de blocos. Cada nó é distinguido dos outros por um identificador único.

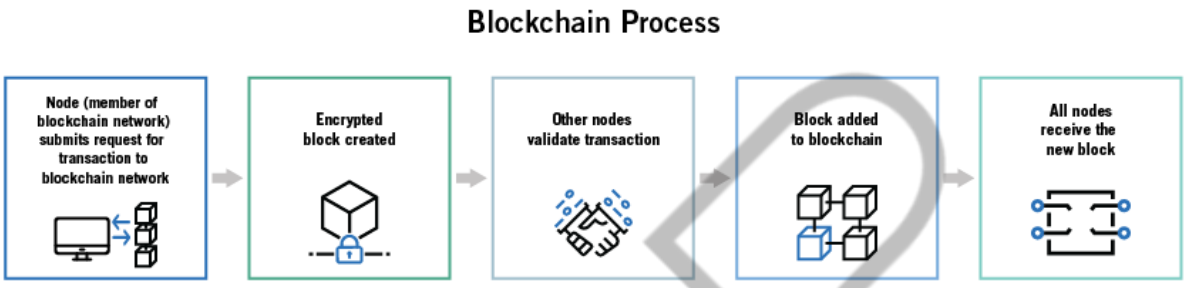


Figura 4 - Nós

Fonte: https://www.jdsupra.com/legalnews/an-overview-of-blockchain-in-supply-3023363/

Existem basicamente quatro tipos de nós:

1. **Full nodes:** executam a função de manter e distribuir cópias de todo o registro da blockchain, validando o histórico da blockchain e retransmitindo-o para outros nós na rede.
2. **Super nodes:** operam 24 horas por dia para conectar os full nodes uns aos outros e espalhar a blockchain por toda a rede. Os super nodes servem como retransmissores de informações ou redistribuição para garantir que todos tenham a cópia correta da blockchain do Bitcoin.
3. **Light nodes:** executam funções semelhantes aos full nodes, mas em uma capacidade menor. Eles contêm pequenas porções da blockchain em oposição à cópia inteira.
4. **Mining nodes:** resolvem problemas computacionais complexos usando hardware especializado por meio de “mineração”, o processo de criação e adição de novos blocos à blockchain. Os mineradores bem-sucedidos recebem uma recompensa em Bitcoin por criar o novo bloco.

1.4 Início da Blockchain: Criptomoedas

Figura 5 - Criptomoedas

Fonte: https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122

O uso mais conhecido da Blockchain são as criptomoedas. Criptomoedas são moedas digitais (ou tokens), como Bitcoin, Ethereum ou Litecoin, que podem ser usadas para comprar bens e serviços.

Assim como uma forma digital de dinheiro, a criptomoeda pode ser usada para comprar tudo, desde seu almoço até sua próxima casa. Ao contrário do dinheiro, a criptomoeda usa a blockchain para atuar como um livro público e um sistema de segurança criptográfico aprimorado, para que as transações online sejam sempre registradas e protegidas. O apelo das criptomoedas é que tudo está registrado em um livro público e protegido por criptografia, fazendo um registro irrefutável, com carimbo de data/hora e seguro de cada pagamento.

Aqui estão algumas das principais razões pela adoção crescente das criptomoedas:

- A segurança da Blockchain torna o roubo muito mais difícil, pois cada criptomoeda tem seu próprio número identificável irrefutável que é anexado a um proprietário.
- A criptografia reduz a necessidade de moedas e bancos centrais individualizados - Com blockchain, a criptografia pode ser enviada para qualquer lugar e qualquer pessoa do mundo sem a necessidade de troca de moeda ou sem interferência de bancos centrais.
- Grandes corporações estão adotando a ideia de uma moeda digital baseada em blockchain para pagamentos. Em fevereiro de 2021, a Tesla anunciou que investiria US$ 1,5 bilhão em Bitcoins e o aceitaria como pagamento por seus carros.

Sobre o bitcoin:

- Sua criação até hoje ainda é um mistério.
- Seu criador se intitula Satoshi Nakamoto. Nakamoto: é a pessoa ou pessoas que desenvolveram o bitcoin.
- Eles são anônimos e usam pseudônimos.

Até 2010, Nakamato estava ativo online, discutindo o desenvolvimento do bitcoin.

1.5 Whitepaper do Bitcoin

A publicação do “white paper” do bitcoin foi em 2008.

Desde então, ao redor do mundo, detetives amadores e especialistas em computação e muitos outros vêm tentando descobrir quem Nakamoto era – ou é. Porque quem criou o bitcoin é uma pessoa extremamente rica, e o enigma é uma história atraente.

A seguir, uma breve linha do tempo de alguns dos eventos mais importantes e notáveis no desenvolvimento da blockchain.

2008

- Satoshi Nakamoto, um pseudônimo para uma pessoa ou grupo, publica “Bitcoin: A Peer to Peer Electronic Cash System”.

2009

- A primeira transação bem-sucedida de Bitcoin (BTC) ocorre entre o cientista da computação Hal Finney e o misterioso Satoshi Nakamoto.

2010

- O programador Laszlo Hanycez, na Flórida, concluiu a primeira compra usando Bitcoin - duas pizzas Papa John's. Hanycez transferiu 10.000 BTC's, no valor de cerca de US$ 60,00 na época. Hoje vale alguns milhões e a comunidade comemora esse dia como Bitcoin Pizza Day.
- O valor de mercado do Bitcoin excede oficialmente US$ 1 milhão.

2011

- 1 BTC = $ 1USD, dando a paridade da criptomoeda com o dólar americano.
- Electronic Frontier Foundation, Wikileaks e outras organizações começam a aceitar Bitcoin como doações.

2012

- Blockchain e criptomoeda são mencionadas em programas de televisão populares como The Good Wife, injetando blockchain na cultura pop.
- A Bitcoin Magazine foi lançada por um dos desenvolvedores do Bitcoin Vitalik Buterin.

2013

- O valor de mercado do BTC ultrapassou US$ 1 bilhão.
- O Bitcoin atingiu US$ 100/BTC pela primeira vez.

- Buterin publica o artigo “Ethereum Project” sugerindo que a blockchain tenha outras possibilidades além do Bitcoin (por exemplo, contratos inteligentes).

2014

- A empresa de jogos Zynga, The D Las Vegas Hotel e Overstock.com começam a aceitar Bitcoin como pagamento.
- O Projeto Ethereum de Buterin é financiado por meio de uma Oferta Inicial de Moedas (ICO) arrecadando mais de US$ 18 milhões em BTC e abrindo novos caminhos para a blockchain.
- R3, um grupo de mais de 200 empresas de blockchain, é formado para descobrir novas maneiras de implementar blockchain em tecnologia.
- PayPal anuncia integração com Bitcoin.

2015

- O número de comerciantes que aceitam BTC excede 100.000.
- A NASDAQ e a empresa de blockchain de San Francisco Chain se unem para testar a tecnologia para negociar ações em empresas privadas.

2016

- A gigante da tecnologia IBM anuncia uma estratégia de blockchain para soluções de negócios baseadas em nuvem.
- O governo do Japão reconhece a legitimidade da blockchain e das criptomoedas.

2017

- Bitcoin atinge US$ 1.000/BTC pela primeira vez.
- O valor de mercado de criptomoedas atinge US$ 150 bilhões.
- O CEO do JP Morgan, Jamie Dimon, diz acreditar na blockchain como uma tecnologia futura, dando ao sistema de contabilidade um voto de confiança de Wall Street.

- O Bitcoin atinge seu máximo histórico em US$ 19.783,21/BTC.
- Dubai anuncia que seu governo será movido à blockchain até 2020.

2018

- O Facebook se compromete a iniciar um grupo de trabalho em blockchain e sugere a possibilidade de criar sua própria criptomoeda.
- A IBM desenvolve uma plataforma bancária baseada em blockchain, com grandes bancos como Citi e Barclays assinando.

2019

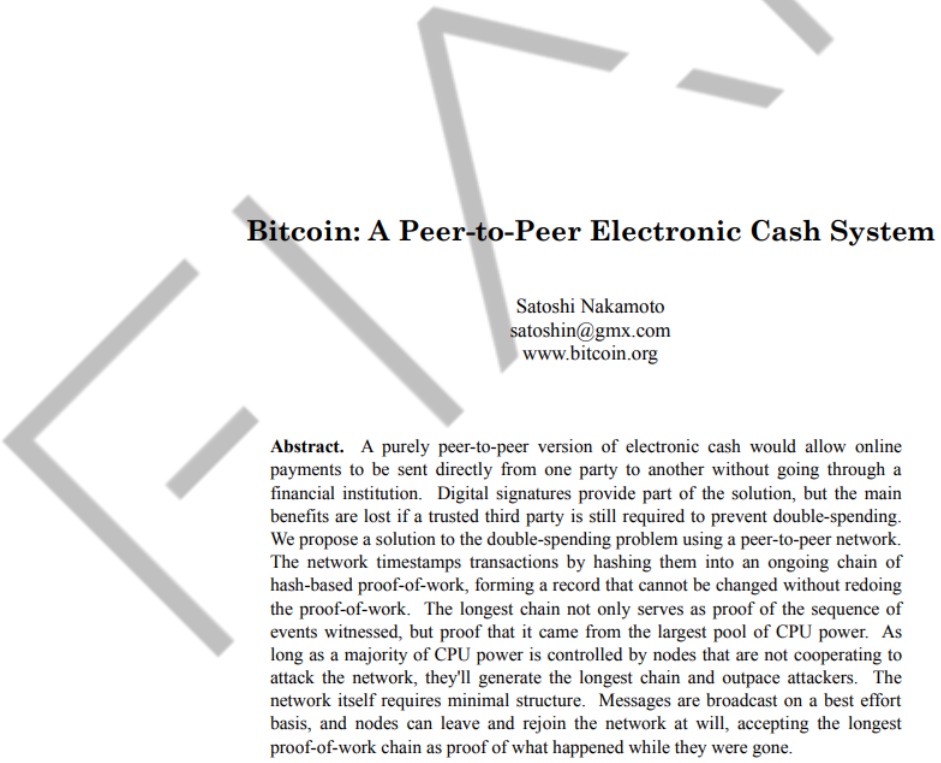
- O presidente da China, Ji Xinping, abraça publicamente a blockchain, enquanto o banco central da China anuncia que está trabalhando em sua própria criptomoeda.
- O CEO do Twitter & Square, Jack Dorsey, anuncia que a Square contratará engenheiros de blockchain para trabalhar nos futuros planos de criptomoedas da empresa.
- A Bolsa de Valores de Nova York (NYSE) anuncia a criação da Bakkt - uma empresa de carteira digital que inclui negociação de criptomoedas.

2020

- Bitcoin quase chega a US$ 30.000 até o final de 2020.
- PayPal anuncia que permitirá que usuários comprem, vendam e mantenham criptomoedas.
- As Bahamas se tornam o primeiro país do mundo a lançar sua moeda digital do banco central, apropriadamente conhecida como “Sand Dollar”.
- Blockchain se torna um jogador chave na luta contra a COVID-19, principalmente para armazenar com segurança dados de pesquisas médicas e informações de pacientes.

2021

- O detentor corporativo nº 1 do Bitcoin é o Grayscale Bitcoin Trust. Eles detêm 654.885 Bitcoins, ou 3,12% da oferta total.
- O detentor corporativo nº 2 do Bitcoin é a MicroStrategy. Eles detêm 124.391 Bitcoins.
- Bitcoin tornou-se moeda legal ao lado do dólar americano em El Salvador em 2021.
- Existem 16.531 criptomoedas listadas no CoinMarketCap.com
- Houve 485.814 contratos de token criados no Ethereum.
- De acordo com o CoinATMRadar, existem 34.479 caixas eletrônicos criptográficos controlados por 603 operadores em 77 países.
- A Coinbase abriu seu capital em 2021 e tem um valor de mercado (valor total de todas as ações) de US$ 60 bilhões, 39 alcançaram esse nível em 2021.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figura 6 – Whitepaper Bitcoin
Fonte: https://bitcoin.org/bitcoin.pdf

Clique aqui para ler o whitepaper do Bitcoin.

2. Fundamentação Tecnológica Blockchain

No nível mais básico, a tecnologia blockchain é composta por algoritmos de criptografia. O criador da blockchain, Satoshi Nakamoto, desenvolveu um sistema no qual a confiança que tradicionalmente depositamos nas organizações para manter registros confiáveis (como bancos) é transferida para a blockchain e os algoritmos criptográficos que ele usa.

O objetivo da blockchain é criar um registro distribuído, descentralizado e confiável do histórico do sistema. A blockchain mais famosa, o Bitcoin, usa esse registro para armazenar o histórico de transações, para que as pessoas possam fazer e receber pagamentos na blockchain do Bitcoin e confiar que seu dinheiro não será perdido ou roubado.

Para atingir esse nível de confiança, a blockchain usa alguns algoritmos criptográficos como blocos de construção. As funções de hash e a criptografia de chave pública são cruciais para a funcionalidade e a segurança do ecossistema blockchain.

2.1 Hash

Uma função hash é uma função matemática que pode receber qualquer número como entrada e produz uma saída em um intervalo fixo de números. Por exemplo, funções de hash de 256 bits (que são comumente usadas em blockchain), produzem saídas no intervalo de 0 a 2256.

Para ser considerada segura, uma função de hash precisa ser resistente a colisões, isso significa que é extremamente difícil (ao ponto de ser quase impossível) encontrar duas entradas que criem a mesma saída de hash. Conseguir isso requer alguns recursos diferentes:

- Nenhuma fraqueza na função hash.
- Um grande número de saídas possíveis.
- Uma função de hash unidirecional (não pode derivar a entrada da saída).
- Entradas semelhantes produzem saídas muito diferentes.

Se uma função de hash atender a esses requisitos, ela poderá ser usada em blockchain. No entanto, se algum desses requisitos for violado, a segurança da blockchain estará em risco.

Blockchain depende muito de funções de hash seguras para garantir que as transações não possam ser modificadas após serem armazenadas no livro-razão.

Para melhorar esse conceito, uma função hash recebe uma entrada de qualquer comprimento e cria uma saída de comprimento fixo.

Aqui está um exemplo usando um tipo de função hash chamada md5:

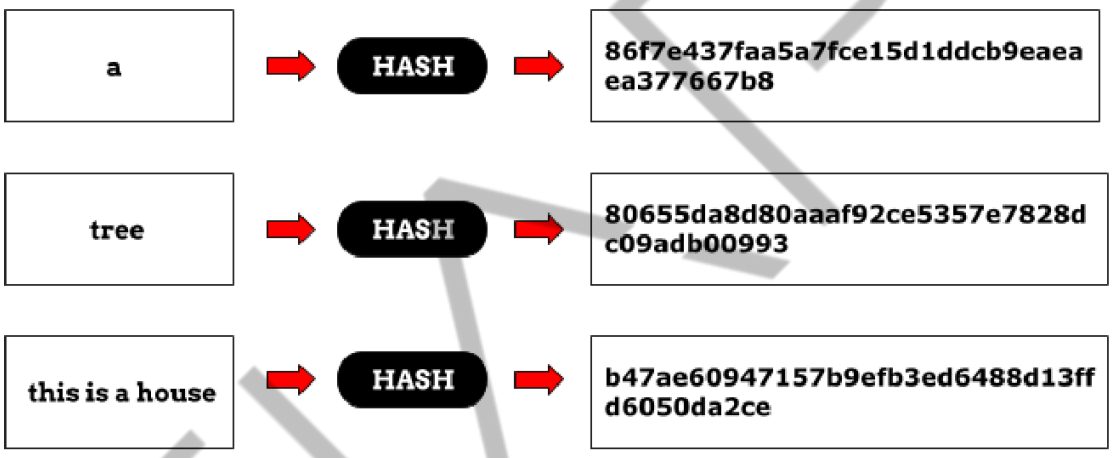


Figura 7- Hash

Fonte: https://wiki.bi0s.in/crypto/hash-function/

É preciso uma string de entrada que crie uma sequência de letras e números aleatórios “a0680c04c4eb53884be77b4e10677f2b”. Isso é chamado como o resumo da mensagem. Também é conhecida como a impressão digital. Isso ocorre para que não haja como modificar essa sequência de caracteres. Se eu tentar modificar para “Eu devo à minha irmã $ 2”, o resumo da mensagem será completamente diferente.

2.2 Criptografia de chave pública

Outro algoritmo criptográfico usado na tecnologia blockchain é a criptografia de chave pública. Esse tipo de criptografia também é amplamente utilizado na Internet, pois possui muitas propriedades úteis. Com a criptografia de chave pública, você pode:

- Criptografar uma mensagem para que apenas o destinatário pretendido possa lê-la.
- Gerar uma assinatura digital comprovando que você enviou uma determinada mensagem.
- Verificar se uma mensagem não foi modificada no percurso.

Na criptografia de chave pública, todos têm duas chaves de criptografia diferentes: uma privada e uma pública. Sua chave privada é um número aleatório que você gera e mantém em segredo. Ele é usado para descriptografar mensagens e gerar assinaturas digitais.

Sua chave pública é derivada de sua chave privada e, como o nome sugere, foi projetada para ser distribuída publicamente. É usada para criptografar mensagens para você e gerar assinaturas digitais. Seu endereço (para onde as pessoas enviaram transações) na blockchain normalmente é derivado de sua chave pública.

A segurança da criptografia de chave pública é baseada em duas coisas. A primeira é o sigilo de sua chave privada. Se alguém puder adivinhar ou roubar sua chave privada, terá controle total de sua conta na blockchain. Isso permite que realize transações em seu nome e descriptografe os dados destinados a você. A maneira mais comum de a blockchain ser “hackeada” é que as pessoas não protejam sua chave privada, sempre a guarde em um local seguro!

A outra suposição principal da criptografia de chave pública é que os algoritmos usados são seguros. A criptografia de chave pública é baseada em problemas matemáticos “difíceis”, em que realizar uma operação é muito mais fácil do que revertê-la. Por exemplo, é relativamente fácil multiplicar dois números, mas é difícil fatorar o resultado. Da mesma forma, é fácil realizar a exponenciação, mas difícil

calcular logaritmos. Como resultado, é possível criar esquemas em que os computadores sejam capazes de realizar a operação fácil, mas não a difícil.

A segurança desses problemas “difíceis” é o motivo pelo qual você costuma ver artigos sobre computadores quânticos quebrando blockchain. Devido à forma como os computadores quânticos funcionam, fatoração e logaritmos não são muito mais difíceis do que multiplicação e exponenciação, então a criptografia de chave pública tradicional não funciona mais. No entanto, existem outros problemas que ainda são “difíceis” para os computadores quânticos, portanto, a ameaça dos computadores quânticos à blockchain pode ser corrigida com uma simples atualização.

2.3 Formação de blocos

Blockchain é uma coleção de blocos que são encadeados para criar um todo contínuo. Entenda como funciona:

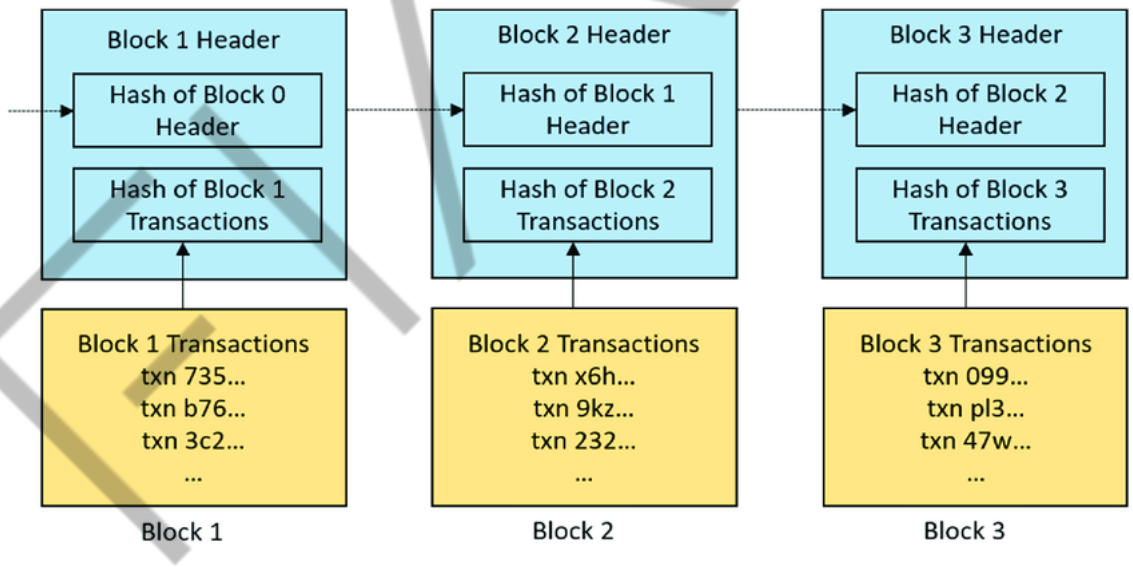


Figura 8 - Formação de blocos

Fonte: https://www.researchgate.net/figure/A-simplified-example-of-how-blocks-are-chained-to-form-a-blockchain-Notice-that-each_fig1_332215097

A imagem acima ilustra a estrutura básica de um bloco em uma blockchain. Cada quadro amarelo representa uma transação dentro do bloco. Embora uma transação possa representar uma transação literal (ou seja, uma transferência de valor) em blockchains como o Bitcoin.

A segurança dos blocos no livro digital depende da segurança da criptografia de chave pública. Cada transação e bloco na blockchain são assinados digitalmente por seu criador. Isso permite que qualquer pessoa com acesso à blockchain valide facilmente que cada transação é autenticada (ou seja, enviada por alguém que possui a conta associada) e não foi modificada desde a criação. A integridade e autenticidade dos blocos da cadeia também são asseguradas pela assinatura digital do criador do bloco.

2.4 Encadeamento

Cada bloco equivale a uma única página no livro-razão. Para combinar esses slides em um todo contínuo, a blockchain faz uso de funções de hash.

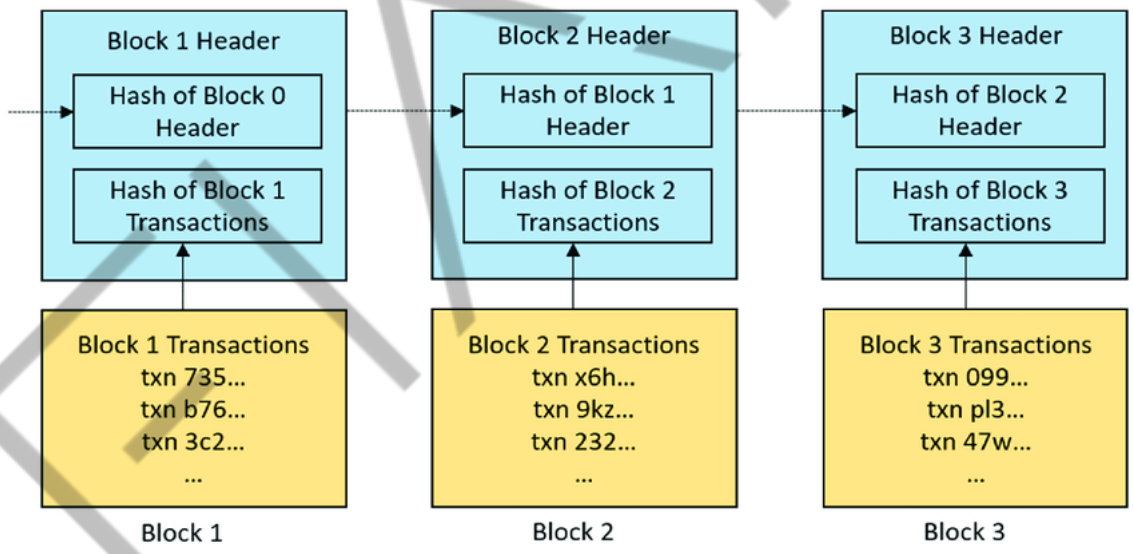


Figura 9 - Blocos

Fonte: https://www.researchgate.net/figure/A-simplified-example-of-how-blocks-are-chained-to-form-a-blockchain-Notice-that-each_fig1_332215097

Na imagem acima, você pode ver as funções de hash ligando cada bloco. Cada bloco contém o hash do bloco anterior como parte de seu cabeçalho de bloco (a seção que não contém dados de transação).

O fato de cada bloco ser dependente do anterior é significativo devido à resistência à colisão das funções de hash. Se alguém quiser forjar o bloco 1 na

imagem, tem duas opções: encontrar outra versão do bloco 1 que tenha o mesmo hash ou forjar todos os blocos após o 2 também. A primeira deve ser impossível (devido à resistência à colisão) e a outra deve ser difícil ou impossível, já que a blockchain é projetada para dificultar o forjamento de um único bloco.

A segurança da parte “cadeia” da blockchain é baseada na resistência à colisão da função hash que ela usa. Se alguém puder encontrar uma maneira de gerar outra versão do bloco 1 que tenha o mesmo hash, as suposições de imutabilidade da blockchain serão quebradas e você não poderá confiar que qualquer transação permanecerá no livro distribuído.

3. PLATAFORMA BLOCKCHAIN

A blockchain foi projetada para armazenar um livro-razão distribuído confiável e compartilhado, que representa todo histórico da rede blockchain.

3.1 A rede peer-to-peer Blockchain

Blockchains usam uma arquitetura de rede diferente da maioria dos serviços da Web aos quais estamos acostumados. Esses serviços usam uma arquitetura cliente-servidor, na qual o servidor atua como uma única fonte de verdade e os clientes se conectam diretamente a ele para fazer upload ou download de dados de aplicativos. Por exemplo, quando você usa um cliente e-mail como o Gmail, seu e-mail não vai diretamente do seu computador para o do destinatário. Em vez disso, você faz o upload para os servidores do Gmail e o destinatário faz o download da mensagem do Gmail para ler.

Esse sistema é simples e eficaz, mas depende do servidor do Gmail para ser um intermediário confiável no processo. Blockchain não é grande em intermediários confiáveis, então ela usa uma rede ponto a ponto, em que cada nó da rede se comunica diretamente com outros nós.

A maioria das redes blockchains usa um sistema de transmissão no qual, se um nó tiver cinco pares, cada mensagem recebida de um é enviada para os outros quatro. Dessa forma, as mensagens se espalham pela rede por muitos caminhos e ninguém tem controle total sobre as comunicações, fazendo com que a informação se espalhe muito rápido.

A principal implicação do modelo peer-to-peer para a rede blockchain é que a rede subjacente precisa ser capaz de suportá-la. Como cada peer precisa ser capaz de se conectar a todos os outros peers, você não pode efetivamente ter uma rede blockchain distribuída em uma rede com níveis de confiança variados sem comprometer a blockchain ou a segurança da rede. Além disso, o estilo de comunicação “broadcast” da blockchain significa que requer uma grande quantidade de largura de banda para funcionar corretamente. A incapacidade de suportar isso pode ter impactos negativos na segurança e eficácia da blockchain.

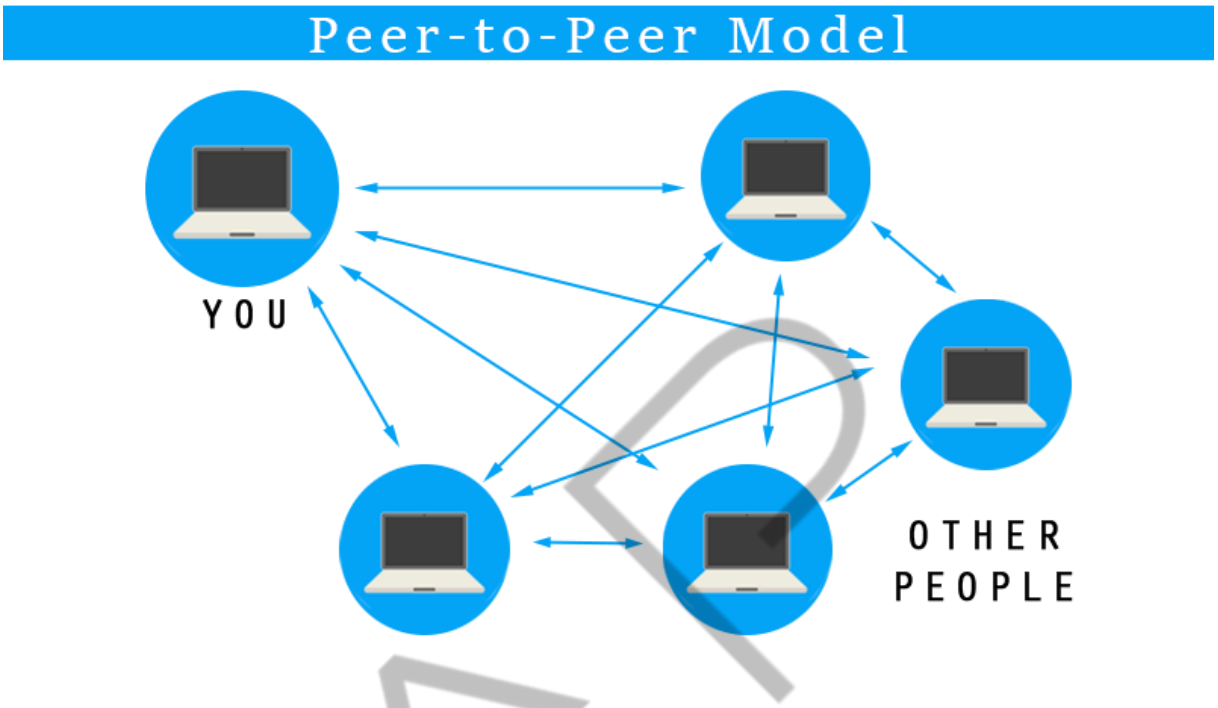


Figura 10 - Modelo peer-to-peer

Fonte: https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-v1/p2p/arquitetura.html

4. ALGORITMO DE CONSENSO

Em um sistema financeiro tradicional, os bancos centralizam o poder mantendo o controle do livro-razão que informa quanto valor é armazenado em cada conta. Se surgir uma disputa sobre o livro-razão, o banco tem a autoridade final para decidir qual é a versão oficial.

Blockchain é projetada para remover autoridades centralizadoras como bancos. Em vez disso, a rede blockchain mantém um registro compartilhado e descentralizado com cada nó da rede mantendo uma cópia e atualizando-a à medida em que cada novo bloco é criado.

O desafio com isso é garantir que todos os nós façam as mesmas atualizações em suas cópias do livro-razão com cada bloco. Como a rede não possui uma autoridade consistente para criar a versão oficial do livro-razão, ela escolhe uma autoridade temporária para criar e compartilhar cada bloco. O mecanismo para fazer isso é chamado de algoritmo de consenso blockchain.

4.1 Fundamentos do consenso

O trabalho do algoritmo de consenso é garantir que o controle da blockchain seja descentralizado para que nenhum usuário tenha a capacidade de controlar a rede. O meio pelo qual isso é feito é tornar o controle da rede blockchain dependente do controle de um recurso escasso.

Não importa qual algoritmo de consenso você escolha, tudo se resume ao fato de que o controle de um recurso escasso equivale a poder na blockchain. Na Prova de Trabalho, esse recurso é o poder computacional, em Proof of Stake, é a criptomoeda da blockchain.

A lógica por trás do uso de um recurso escasso como análogo para alimentar a blockchain é que ele permite o uso de incentivos econômicos para proteger a blockchain. A Lei da Oferta e da Demanda diz que: se houver aumento da demanda por um recurso com oferta limitada, o preço aumenta.

Quando um invasor tenta obter o controle de uma rede blockchain (para realizar um ataque de 51% ou similar), ele precisa adquirir mais recursos escassos para fazê-

lo. Como resultado, eles aumentam a demanda pelo recurso, o que aumenta o preço para adquiri-lo. Espera-se que o custo para adquirir recursos suficientes para realizar um ataque bem-sucedido esteja além dos recursos do invasor. Caso contrário, temos ataques bem-sucedidos de 51% contra blockchains, o que certamente aconteceu em redes menores de criptomoedas.

4.2 Como os algoritmos comuns implementam o consenso

Quando Satoshi Nakamoto criou o Bitcoin, era o único blockchain existente. O whitepaper Bitcoin descreveu o algoritmo de consenso de Prova de Trabalho usado na rede Bitcoin. Desde então, muitos outros algoritmos de consenso foram desenvolvidos para diferentes implementações de blockchain. Desses, o Proof of Stake também recebe muita atenção, em parte devido à sua presença no roteiro do Ethereum.

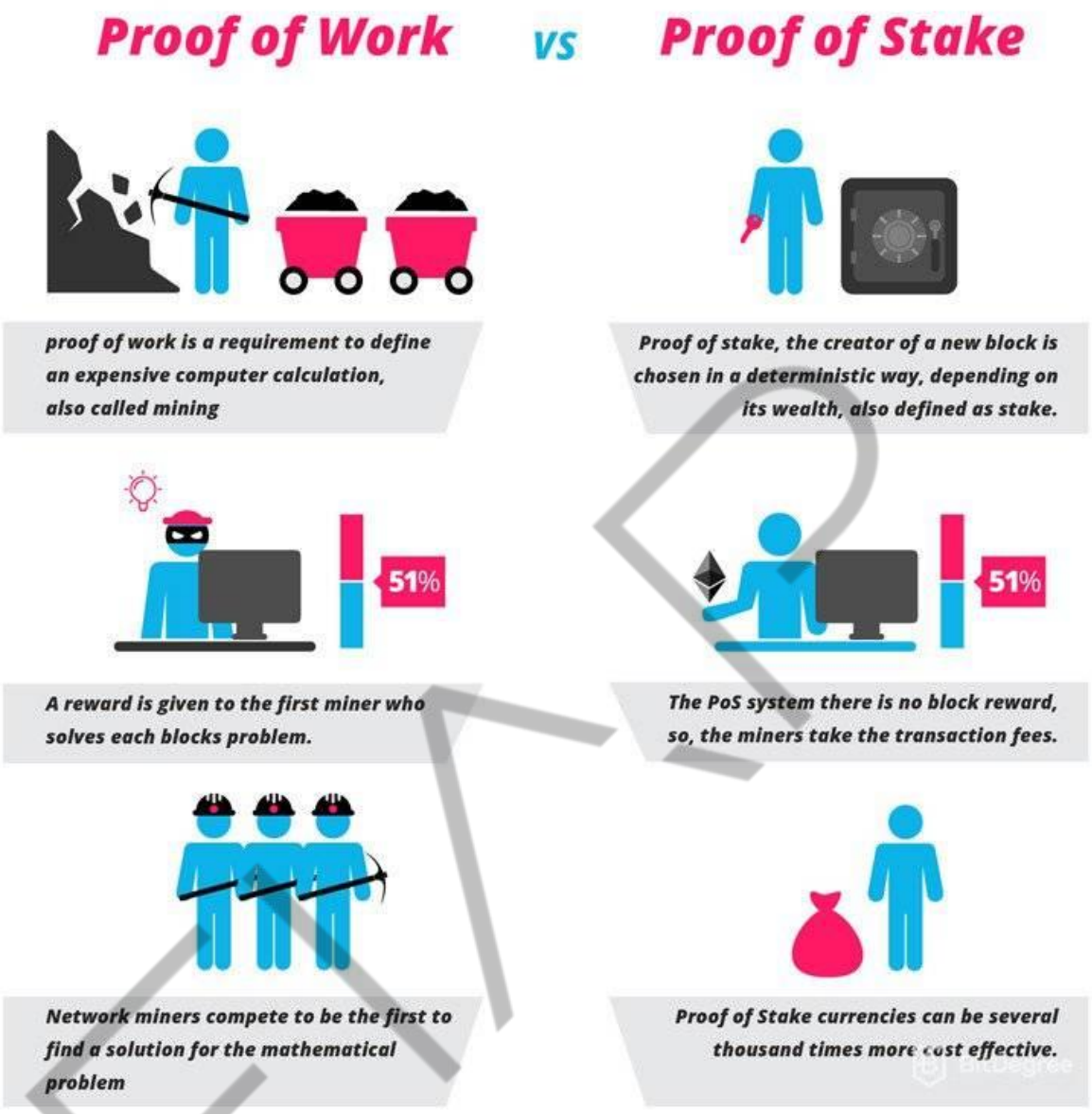


Figura 11 - Proof of work versus proof of stake

Fonte: https://br.bitdegree.org/crypto/tutoriais/proof-of-work-vs-proof-of-stake

4.3 Prova de Trabalho

A Prova de Trabalho é o algoritmo de consenso original e, como o próprio nome sugere, envolve fazer as pessoas trabalharem. Na Prova de Trabalho, os mineradores são aqueles que tentam criar um novo bloco. A maneira como o criador do bloco é selecionado é implementando uma corrida em que o vencedor cria o bloco (e ganha as recompensas associadas).

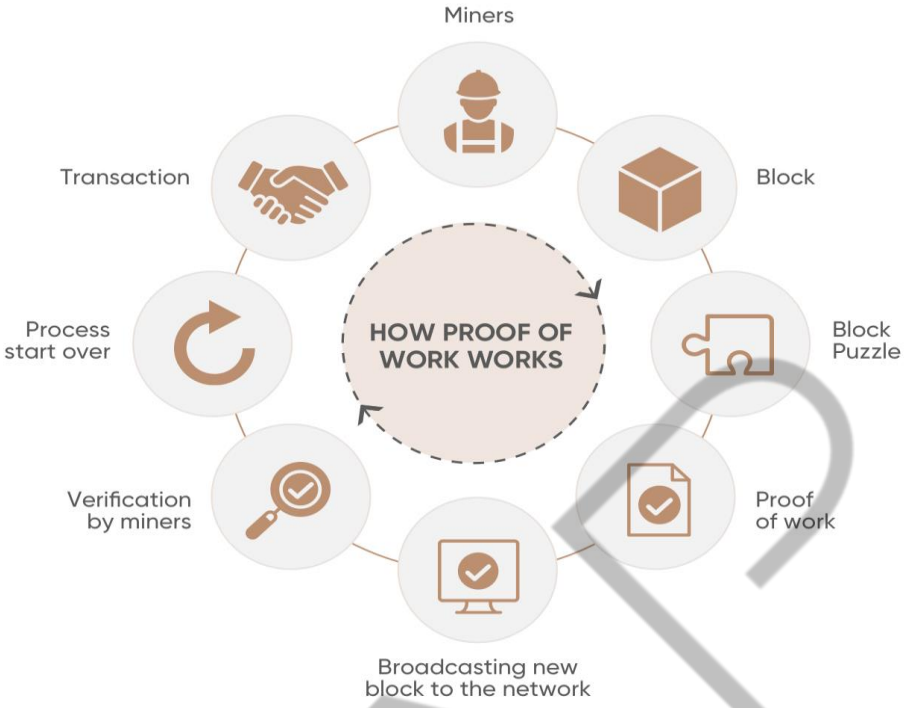


Figura 12 - Como funciona a prova de trabalho

Fonte: https://capital.com/proof-of-work-pow-definition

Essa corrida envolve a criação de um bloco válido, em que a condição de validade é que o cabeçalho do bloco tenha um valor menor que um determinado limite. Devido às propriedades das funções de hash, a melhor maneira de fazer isso é adivinhando aleatoriamente. Como resultado, os mineradores na rede tentam hashes aleatórios até que se depare com um nonce que cria a saída de hash desejada. O primeiro minerador a encontrar um bloco válido o transmite para o resto da rede para construir o próximo bloco.

O principal problema com o Proof of Work é que o critério para a criação do bloco é a capacidade de criar um bloco válido. Não há nada que diga que dois mineradores diferentes não podem encontrar versões diferentes do bloco ao mesmo tempo. Se isso ocorrer, uma blockchain divergente pode ser criada com diferentes partes da rede sendo construídas em cima de diferentes blocos. Blockchain resolve isso usando a regra do bloco mais longo, que diz que, em um conflito entre duas versões da blockchain, a mais longa deve ser aceita.

A Prova de Trabalho também tenta minimizar a probabilidade de blockchains divergentes usando o conceito de dificuldade. O valor limite que o hash de um cabeçalho de bloco válido deve ser menor do que pode ser atualizado de forma distribuída. A dificuldade é atualizada em intervalos regulares para que a criação de blocos (com o poder computacional atual da rede blockchain) ocorra na taxa de blocos desejada.

4.4 Prova de participação

A Proof of Stake adota uma abordagem diferente para proteger a blockchain usando um recurso escasso. Em vez de usar o poder computacional escasso (como Proof of Work), o Proof of Stake usa a escassa criptomoeda da blockchain.

Proof of Stake funciona muito como investir em uma empresa. Ao dar parte do seu dinheiro para uma empresa, você tem o direito de receber dividendos de investidores. No Proof of Stake, você promete não gastar uma parte de sua criptomoeda (ou apostar) em troca da chance de ser um criador de blocos (e ganhar as recompensas associadas).

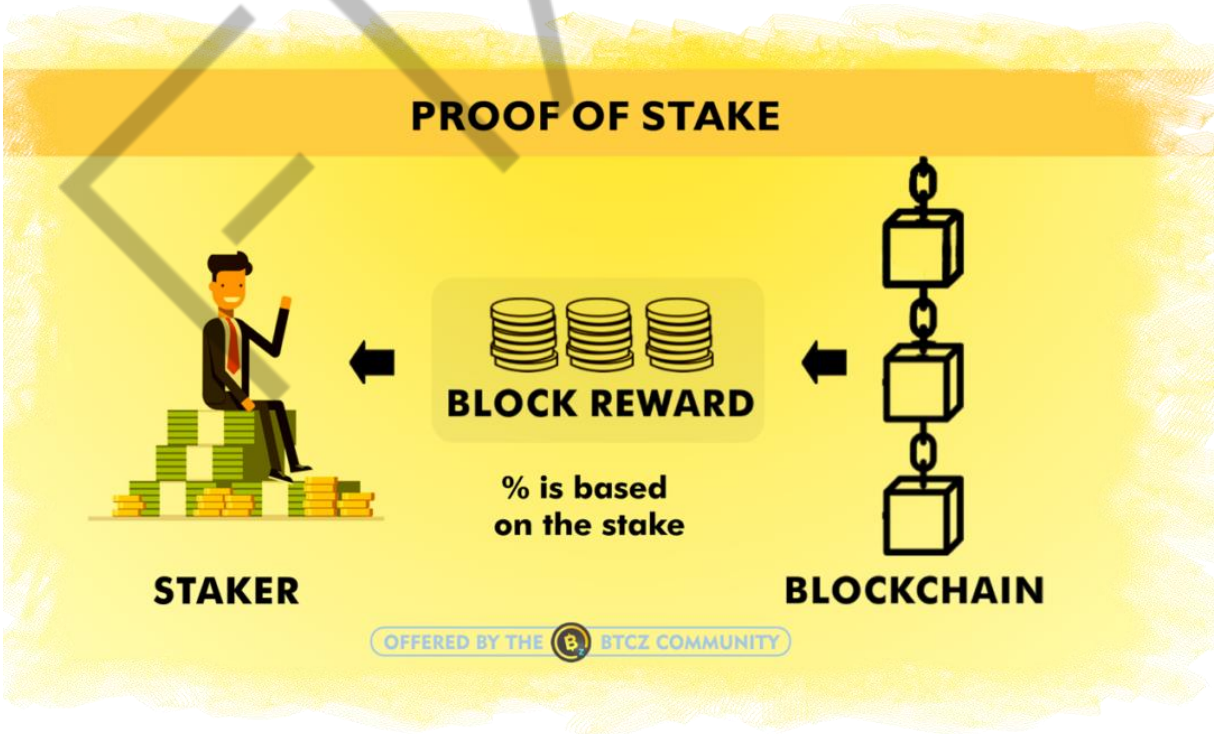


Figura 13 - Como funciona a prova de participação
Fonte: https://getbtcz.com/what-is-proof-of-stake/?lang=pt

A mecânica de como os criadores de blocos são selecionados com base nas apostas varia de acordo com a implementação. Em algumas implementações, a probabilidade de ser selecionado é diretamente proporcional ao tamanho da aposta do usuário. Em outros, o conceito de idade da moeda é introduzido e os apostadores que não foram selecionados para criar um bloco em algum momento têm uma probabilidade maior de serem selecionados. Independentemente disso, o controle de mais criptomoedas apostadas no Proof of Stake equivale a um maior controle sobre a blockchain.

5. ATAQUE DE 51%

Um ataque de 51% ocorre quando um único minerador de criptomoeda ou grupo de mineradores obtém o controle de mais de 50% da blockchain de uma rede. Esses ataques são uma das ameaças mais significativas para as pessoas que usam e compram criptomoedas.

O cenário de ataque de 51% é raro, em grande parte devido à logística, hardware e custos necessários para realizá-lo. Mas um ataque de bloco bem-sucedido pode ter consequências de longo alcance para o mercado de criptomoedas e para aqueles que investem nele.

Quando ocorre uma transação de criptomoeda, seja ela Bitcoin ou outra moeda digital, os blocos recém-extraídos devem ser validados por um consenso de nós ou computadores conectados à rede. Uma vez que essa validação ocorre, o bloco pode ser adicionado à cadeia.

A blockchain contém um registro de todas as transações que qualquer pessoa pode visualizar a qualquer momento. Esse sistema de manutenção de registros é descentralizado, o que significa que nenhuma pessoa ou entidade tem controle sobre ele. Diferentes nós ou sistemas de computador trabalham juntos para minerar, de modo que o hashrate de uma rede específica também é descentralizado.

Quando a maioria do hashrate é controlada por um ou mais mineradores em um ataque de 51%, no entanto, a rede de criptomoedas é interrompida. Os responsáveis por um ataque de 51% seriam então capazes de:

- Excluir novas transações do registro.
- Modificar a ordem das transações.
- Impedir que transações sejam validadas ou confirmadas.
- Bloquear outros mineradores de minerar moedas ou tokens dentro da rede.
- Reverter transações para gastar moedas em dobro.

Todos esses efeitos colaterais de um ataque de bloco podem ser problemáticos para investidores de criptomoedas e para aqueles que aceitam moedas digitais como forma de pagamento.

Por exemplo, um cenário de gasto duplo permitiria que alguém pagasse por algo usando criptomoeda e revertesse a transação após o fato. Eles efetivamente seriam capazes de manter o que compraram junto com a criptomoeda usada na transação, enganando o vendedor.

Um ataque de 51% não é uma ocorrência comum, mas não é algo que possa ser ignorado. Para investidores de criptomoedas, o maior risco associado a um ataque de 51% pode ser a desvalorização de uma determinada moeda digital.

A forma de se proteger contra a possibilidade de um ataque de 51% é investindo em redes blockchains maiores e mais estabelecidas versus redes menores. Quanto mais uma blockchain cresce, mais difícil se torna para um minerador desonesto realizar um ataque a ela. Redes menores, por outro lado, podem ser mais vulneráveis a um ataque de bloco.

REFERÊNCIAS

ARORA, Shivam. What is Bitcoin Mining? How Does It Work, Proof of Work and Facts You Should Know. **Simplilearn**. Disponível em <https://www.simplilearn.com/bitcoin-mining-explained-article>. Acesso em: 06 dez. 2022.

BLOCKCHAIN. **Wikipedia**. Disponível em <https://en.wikipedia.org/wiki/Blockchain>. Acesso em: 06 dez. 2022.

GUPTA, Ruchi. Se você entender a função da Hash, você entenderá a Blockchain. **Guia do bitcoin**. Disponível em <https://guiadobitcoin.com.br/noticias/se-voce-entender-a-funcao-da-hash-voce-entendera-a-blockchain/>. Acesso em: 06 dez. 2022.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em: 06 dez. 2022.

NJOROGE, Ephraim. Understanding a 51% Attack on the Blockchain. **Section**. 15 dez. 2021. Disponível em <https://www.section.io/engineering-education/understanding-the-51-attack-on-blockchain/#:~:text=A%2051%25%20attack%20happens%20when,and%20order%20of%20new%20transactions>. Acesso em: 06 dez. 2022.

WESTON, Georgia. The Significance Of Nonce In Blockchain. **101blockchains**. 27 abr. 2022. Disponível em <https://101blockchains.com/nonce-in-blockchain/>. Acesso em: 06 dez. 2022.

WHAT is blockchain and how does it work? **Synopsys**. Disponível em <https://www.synopsys.com/glossary/what-is-blockchain.html>. Acesso em: 06 dez. 2022.

WHAT is blockchain technology? **IBM**. Disponível em https://www.ibm.com/topics/what-is-blockchain. Acesso em: 06 dez. 2022.