NewCA$H

Ano 2018

Descomplicando o Bitcoin

BLOCKCHAIN

eBOOK 2

newc.com.br

ÍNDICE

BLOCKCHAIN

BLOCKCHAIN É UMA TECNOLOGIA DE REGISTROS DIGITAIS DESCENTRALIZADOS

A blockchain é formada de registros que são gerados, registrados e autenticados numa rede p2p distribuída através dos softwares mineradores (tema do ebook 3). Esses registros têm autenticidade e imutabilidade. Em outras palavras, a blockchain é um livro-razão (termo técnico da contabilidade) usado para registrar todas as transações de Bitcoin no mundo, que pode ser consultado e auditado por qualquer pessoa através da internet.

A Blockchain do Bitcoin trabalha com criptografia SHA-256, contém uma chave pública em forma de HASH (algo como: 3G5XdNiQuKHXAccEDqwFUwyhUEr3kw5oKq) que é usada como referência à ID de uma transação.

O protocolo da blockchain foi programado para ser o controlador e limitador do Bitcoin, pois a quantidade de blocos que é gerado que permite que as transações sejam confirmadas e que novos Bitcoins possam ser gerados, limitando em tempo, demanda, e quantidade a sua produção e fluxo.

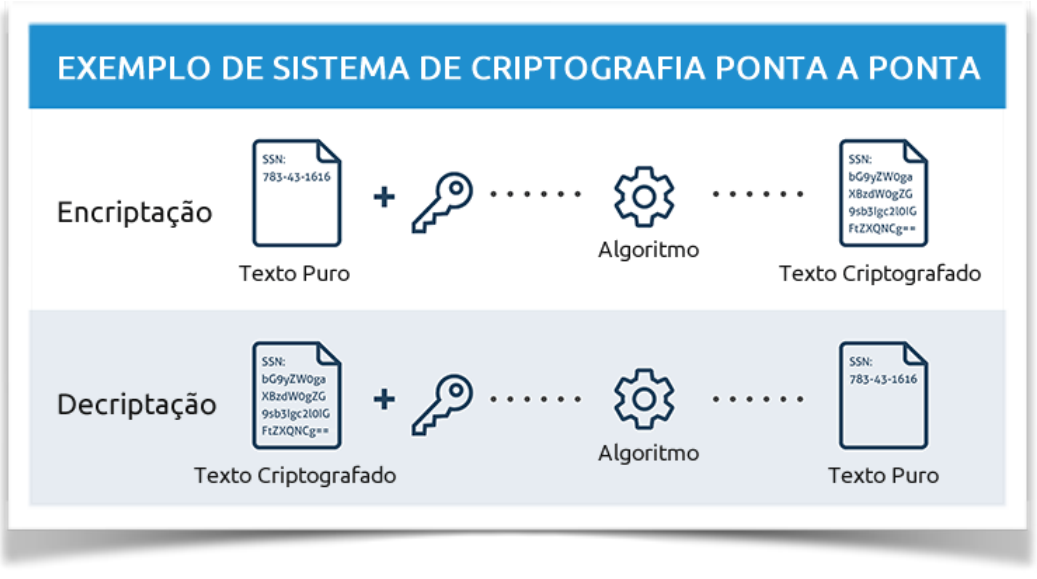
Conforme as transações e a quantidade de mineradores aumentam, a complexidade e dificuldade de processamento dos dados dessa rede também aumentam, tornando essa equação ideal para controle inflacionário e uma espécie de reserva de valor virtual, contendo assim alguns aspectos do ouro que conhecemos, como por exemplo: escasso e difícil de encontrar, pois quanto mais se minerar e extrair ouro, mais difícil se torna de encontrar. Esses princípios fazem com que muitos vejam o Bitcoin como "ouro digital".

A Blockchain também tem algumas utilizações que vão além do mero uso como moeda. Ela também pode ser usada como registro de documentos e contratos inteligentes (smart-contracts, em inglês).

CRIPTOGRAFIA

A CRIPTOGRAFIA É UMA ESPÉCIE DE MATEMÁTICA AVANÇADA

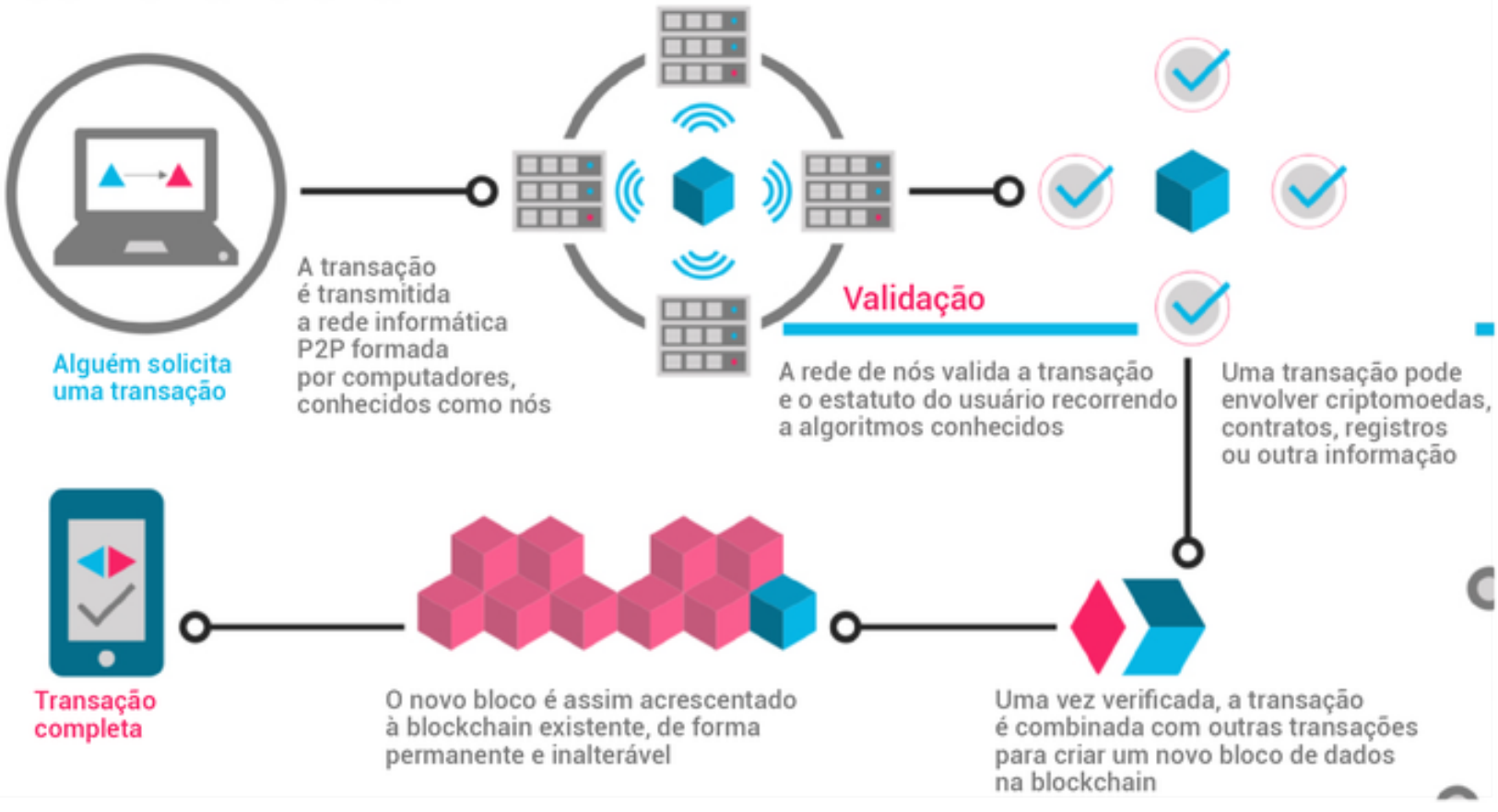
Ela é fundamental nas transações do Bitcoin, que são adicionadas ao livro registro (Blockchain) com o objetivo principal torná-lo à prova de violação evitando, assim, gastos duplos e qualquer fraude no sistema. O Bitcoin é conhecido como o protocolo da segurança.



Para que um bloco de uma transação seja autenticado pelos mineradores, os mineradores pegam todos os detalhes das transações contidas naquele bloco e aplicam uma fórmula matemática que transforma aqueles dados em hash. Outra característica dos hashes é que se você mudar apenas um dos caracteres ele se transformará em um hash completamente diferente.

Cada bloco tem um hash específico. O hash subsequente é atrelado ao hash anterior, e assim, sucessivamente, fazendo que o hash de um bloco sempre esteja atrelado ao anterior.

Assim, por exemplo, quando foi criado o primeiro bloco, ele serviu de base para o segundo hash, e este último, por sua vez, para o terceiro hash, e assim sucessivamente. Em outras palavras, o segundo bloco possui informações do primeiro. E o terceiro bloco possui informações do segundo e assim sucessivamente. Isso torna o sistema especialmente difícil de ser hackeado, uma vez que para mudar alguma coisa, o atacante teria que ter força computacional suficiente para alterar o passado, o que é impraticável em termos da tecnologia atual.



VISUALIZANDO A TECNOLOGIA

CONHEÇA O CICLO DE TRANSAÇÃO DO BITCOIN.

- Abrir Carteira e Escanear Endereço
- Preencher quantidade e taxa (algumas carteiras não tem a opção de editar a taxa)
- Enviar Processo automático:
- A transação é assinada com a chave privada de sua carteira
- A transação é propagada e validada pelos nós da rede
- Mineradores incluem próximo bloco a ser minerado
- A transação é minerada (compensada)
- O minerador que resolver o PoW (Proof of Work) mais rapidamente propaga o bloco
- Os nós verificam o resultado e registram bloco na blockchain
- Surge a primeira confirmação desta transação
- Novas confirmações aparecem assim que verificadas pelos nós

New CA$H

A EXCHANGE MAIS SEGURA E INOVADORA DO BRASIL!

Acesse: newc.com.br