**Blockchain**

Sumário

[O que é Blockchain? 3](#_Toc187773883)

[Criptomoedas 3](#_Toc187773884)

[O que é um bloco? 4](#_Toc187773885)

[Ledger 4](#_Toc187773886)

[Miners 5](#_Toc187773887)

[Surgimento da blockchain 7](#_Toc187773888)

[Tipos de carteiras 7](#_Toc187773889)

# O que é Blockchain?

São informações ou dados unidos em bloco e interligados formando uma corrente. Os benefícios incluem:

* Rastreabilidade
* Transparência
* Segurança nas negociações
* Redução de custos e prazos

Um exemplo poderia ser dado na indústria imobiliária, imagine adquirir um apartamento, em cerca de 10 minutos, sem a intermediação de imobiliária, banco ou cartório.

A segurança é essencial, para verificar se não é fraude veja as validações e confirmações de outros usuários(mineradores).

Nisto, um registro digital permanente de compra e venda é gerado, distribuindo para toda a rede e a transação é arquivada em todos os computadores da rede.

**Curiosidade:** A ucrânia foi o primeiro país a usar a tecnologia Blockchain na comercialização de imóveis. As negociações são feitas por meio de contratos inteligentes (Smart Contracts) da rede Ethereum.

# Criptomoedas

As criptomoedas são ativos que possuem uma documentação sobre o seu projeto a White paper é um documento sobre um sistema ponto a ponto de dinheiro eletrônico.

Cada transação é guardada em um livro razão ao qual chamamos de Ledger, onde é armazenado todos os registros de lançamentos contábeis seja, crédito ou débito de uma organização, este livro razão é público e possui um banco de dados descentralizado e distribuído.

Uma transação pode ser diferenciada das demais pela sua hash, ou seja, o seu identificador único de transação, que é obtido por meio de uma função hash que recebe como entrada os demais dados da transação.

As suas moedas podem ser guardadas em um wallet, no caso é uma carteira digital que armazena criptomoedas, chaves privadas e públicas.

* Chave Privada: Conhecida apenas pelo seu proprietário.
* Chave Pública: É publicada e distribuída na rede.

A hash de cada bloco aponta para o bloco anterior. Todas as transações que um bloco possui são identificadas criptograficamente por uma hash. No cabeçalho do bloco, as transações são identificadas por uma hash única chamada Merkle Root Hash, que representa a raiz de uma árvore de transações conhecida como markle tree. Outra menção que vale a pena ser dita é que a hash compila dados de qualquer tamanho para um tamanho fixo, por exemplo, uma hash SHA-256 (Secure Hah Algorithm) produz uma saída de 256 bits para qualquer dado de origem.

# O que é um bloco?

Um bloco nada mais é do que um conjunto de transações ou informações validadas.

O bloco inicial de uma transação é conhecido como genêsis, ele não possui registro de transações de outros blocos; por isso o bloco anterior sempre é representado no campo de hash valor 0. Tendo isso alterar o bloco 1 é impraticável.

# Ledger

Agora vamos falar um pouco mais sobre a ledger, ou seja, o livro-razão público de transações blockchain. Irei comentar primeiro algumas de suas desvantagens:

* Alto risco de perda ou destruição de dados 🡺 O usuário da rede deve confiar que o controlador central está fazendo cópias de segurança (Backups) de todas as transações do sistema.
* Validação única 🡺 Os usuários da rede precisam confiar que o controlador central está validando cada transação recebida.
* Registro único 🡺 Os usuários da rede precisam confiar que o controlador central está registrando todas as transações recebidas.
* Risco de alteração 🡺 Os usuários da rede precisam confiar que o controlador central não está alterando transações passadas.

Cada nó da rede distribuída possui uma cópia do livro-razão. Dessa forma, qualquer modificação do livro-razão seria facilmente reconhecida pelos demais nós. E estes nós entrando em um acordo sobre a nova situação do ledger é denominado consenso.

O dispositivo ledger serve como uma autenticação de 2 fatores para as suas transações. Em outras palavras, cada interação feita através da carteira precisa ser confirmada no próprio dispositivo. Como resultado ninguém pode interagir com a sua cripto de forma remota.

Os usuários podem submeter transações para inclusão na blockchain por meio de algum nó na rede.

Os nós que realizam essa inclusão são denominados mineradores (miners).

Eles adicionam novos blocos com transações que estavam pendentes de validação ou informações recém-validadas.

Cada transação é realizada diretamente entre as partes (peer-to-peer), validadas por todos os nós (nodes) e incluída na blockchain pelos mineradores, formando uma cadeia de blocos com informações criptografadas (hash) que ficam registradas e armazenadas em toda a rede, funcionando como um livro-caixa-digital (ledger), tornando-se um histórico para a próxima vez que houver negociação.

**Curiosidade:** Refugiados na Jordânia no supermercado tazweed, podem fazer compras pagas por meio da leitura da íris ocular. Sistema conhecido como “Eye-Pay”, usado para distribuir ajuda em dinheiro para alimentos a mais de 100.000 refugiados sírios na Jordânia.

# Miners

Quando uma transação é solicitada, os miners a recebem e competem para resolver a equação.

Cada minerador terá um grupo de transações pendentes a serem incluídas. Eles selecionam o bloco e tentam resolver o desafio.

Para resolver o desafio, os mineradores realizam uma prova de trabalho. O desafio consiste em incrementar o valor Nonce do bloco, até que a hash do bloco apresente um determinado número de zeros iniciais. Conforme a blockchain aumenta, o número de zeros aumenta, aumentando também a dificuldade.

O minerador que consegue resolver o desafio transmite a solução para a rede, para que a sua prova de trabalho seja validada pelos demais miners.

Os outros miners verificam a prova de trabalho validando ou não o bloco.

Dependendo da exigência da rede para a operação de mineração, uma máquina pode não ser o suficiente para resolver o desafio e incluir um bloco. Dessa forma, pequenos mineradores podem se juntar para resolver o desafio coletivamente, e os ganhos são divididos entre todos de acordo com o processamento de cada máquina. Alguns dos motivos do alto custo de mineração são:

* Alto custo das máquinas (hardware)
* Necessidade de instalação de sistemas de refrigeração devido ao calor gerado pelos processadores e a necessidade de ter a temperatura controlada para otimizar o poder de processamento.
* Necessidade de um cluster (grupo) de máquinas para aumentar o poder de processamento e velocidade para obtenção da solução do bloco.
* Necessidade de um espaço físico exclusivo para as máquinas devido ao calor e o barulho gerado pelas várias ventoinhas das máquinas.

A recompensa a ser paga ao minerador quando ele conseguir incluir um bloco na cadeia é chamado de coinbase.

E a prova de trabalho é normalmente chamada de Proof of work ou apenas Pow.

A rotina computacional por trás da mineração. A prova de trabalho mais conhecida por um minerador consiste em obter do bloco candidato uma hash que apresente um certo número de zeros iniciais.

Um novo bloco só pode ser aceito quando sua hash contiver 5 zeros. Essa é a dificuldade alvo. Por exemplo:

00000E6CC2661A6E263A391D88530B72C4491E43A0567BE6C5C

Eu citei em alguma parte do texto a palavra nonce, e antes que gere conflito irei explicar, nonce é a quantidade de tentativas utilizadas para encontrar uma hash válida, que contenha a quantidade de zeros iniciais determinada pelo grau de dificuldade.

Cada hash é composta por números de bloco, hash anterior, marcação de tempo, dados e nonce, submetidos ao algoritmo de criptografia que gera assim, a hash de bloco.

**Nota:** devo explicar que toda moeda alternativa à bitcoin, no mercado é denominada como altcoin.

# Surgimento da blockchain

Criado em 2008 por um autor anônimo que utiliza o pseudônimo de Satoshi Nakamoto, a blockchain surgiu como um protocolo de transação descentralizado que utiliza a rede P2P com participantes não confiáveis, sem depender de uma autoridade central. A utilização dessa tecnologia permite o compartilhamento seguro e descentralizado de informações sem a dependência de terceiros.

Uma das possibilidades que se pode pensar é que a blockchain pode ajudar a criar uma rede IOT descentralizada.

# Tipos de carteiras

Existem dois tipos de wallets que podemos usar:

* Hot Wallet 🡺 Melhor para negócios e transações
* Cold Wallet 🡺 Melhor proteção para grandes quantias.

As hot wallets são armazenadas em disco rígido de um computador, em um celular, ou servidores de criptomoedas e serviços especiais, elas são fáceis de usar, mas requer medidas de segurança aprimoradas. Não apenas sendo uma dica para a hot wallet, mas para qualquer carteira digital, se a sua chave digital estiver na internet, ela pode ser facilmente hackeada.

Para que não seja necessário apontar todos os nomes ou termos importantes de blockchain deixarei aqui o link de um dicionário cripto: [Dicionário Cripto: Os 70 Principais Termos De A A Z!](https://blog.bitso.com/pt-br/criptomoedas/dicionario-cripto) .

Como pode ver até agora falamos bastante sobre segurança e descentralização, o que me leva a falar do trilema da Blockchain:

* Segurança
* Descentralização
* Escalabilidade

Normalmente um projeto blockchain não pode ter os 3, fazendo com que um seja menos valorizado no projeto e depois criando uma layer (camada) para revestir o que falta.

# Layers

A camada 0 é a infraestrutura subjacente que sustenta a existência e operação do blockchain, fundamentando redes como bitcoin e Ethereum. Engloba a internet, o hardware e as conexões necessárias.

A camada 1 é onde reside a segurança baseada em imutabilidade. Ela é incumbida de administrar os processos de consenso, as linguagens de programação, o tempo de bloqueio, a resolução de disputas, além de estabelecer regras e parâmetros que mantem a operacionalidade básica de uma rede blockchain.

As redes sobrepostas a camada base são empregados para aprimorar a escalabilidade, removendo certas operações da camada 1. Isso é a camada 2.

A camada 3 é onde os projetos se manifestam como interface do usuário, ocultando a complexidade técnica subjacente. As aplicações transformam a funcionalidade da blockchain em soluções práticas para que problemas do mundo real, tornando a tecnologia blockchain acessível e aplicável em diversos contextos.