

Fundamentos da Blockchain

Cassiano Peres

DIO Tech Education Analyst

Sobre Mim

- Analista e desenvolvedor de sistemas
- Empreendedor
- Apaixonado pela liberdade
- Fã de criptomoedas e da economia descentralizada

 cassiano-dio

 peres-cassiano

Objetivo Geral

Neste módulo vamos abordar os conceitos relacionados à base da Blockchain, desde seus aspectos teóricos até a sua implementação.

Pré-requisitos

- Conhecimento básico em JavaScript;
- Noções de redes de computadores;
- Conhecimento fundamental de criptografia e algoritmos.

Percurso

Etapa 1

O que é blockchain?

Etapa 2

O caso do bitcoin

Etapa 3

Conceitos de criptografia na Blockchain

Percurso

Etapa 4

Entendendo a criptografia SHA-256

Etapa 5

Simulando transações

Etapa 6

Sobre carteiras e endereços bitcoin

Etapa 1

O que é blockchain?

Introdução

Nesta aula vamos falar sobre a blockchain, suas características, como ela funciona e como é utilizada na prática



Introdução

A blockchain pode ser considerada um **livro de razão pública** que registra **transações** com o objetivo de garantir a **imutabilidade** e **confiabilidade** dos registros.



Introdução

A blockchain guarda informações como, por exemplo, a transferência de criptomoedas entre carteiras ou o registro de informações em um contrato inteligente.



A história da blockchain

O conceito de uma blockchain não é novo, sendo descrita em 1991 pelos cientistas Stuart Haber e W. Scott Stornetta, com a proposta de um sistema de autenticação de documentos digitais que não pudesse ser fraudado.



W. Scott Stornetta



Stuart Haber

A história da blockchain

Outro cientista e criptógrafo chamado Hal Finney criou um novo conceito chamando **Proof of Work (PoW)** para a validação dos novos blocos inseridos na blockchain.



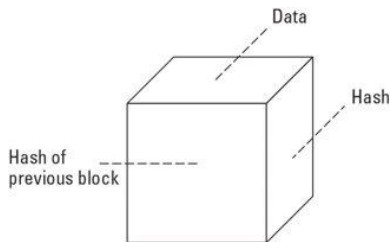
Hal Finney

Como funciona a blockchain?

A blockchain é sustentada por meio de uma rede **Peer-to-Peer** (ponto a ponto) onde cada nó que compõe a rede possui sua própria cópia dos dados.

Como funciona a blockchain?

Cada bloco da blockchain possui um **identificador único** também chamado de ***hash*** e o hash do bloco anterior, formando assim uma cadeia de blocos sequenciais.

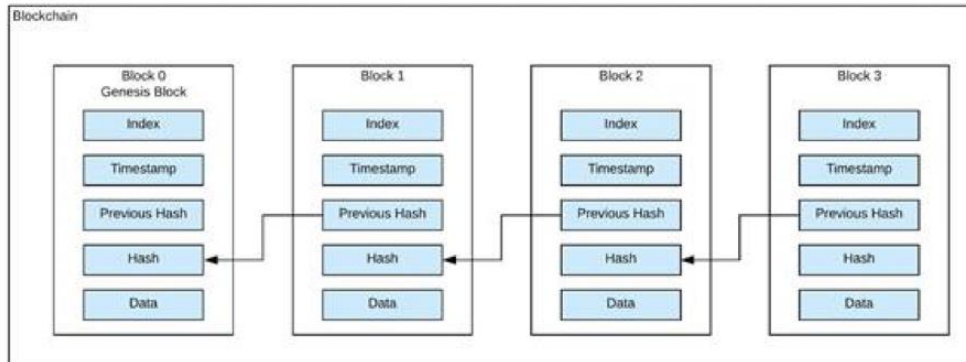


O que são os blocos

Os blocos são a parte fundamental da blockchain, pois carregam todos os dados registrados ao longo do tempo em uma blockchain.

O que são os blocos

Cada bloco possui uma estrutura de informações que o identificam e os dados das transações registradas.



Estrutura do bloco

- **Index:** o número sequencial do bloco;
- **Timestamp:** carimbo de data e hora de geração do bloco;
- **PreviousHash:** hash do bloco anterior;

Estrutura do bloco

- **Hash:** assinatura digital do bloco calculado com base no seu conteúdo;
- **Data:** os dados dos blocos (payload), como as transações.

Pilares da blockchain

- **Descentralização:** não há uma autoridade central para validação dos dados;
- **Imutabilidade dos dados:** cada nó que compõe a rede possui sua cópia dos dados, fornecendo redundância;

Pilares da blockchain

- **Segurança:** garantida pela criptografia;
- **Registros distribuídos:** a rede blockchain é composta de vários **nós** que compartilham o poder computacional;

Pilares da blockchain

- **Consenso:** a validação é feita por meio de algoritmos de consenso que comparam os dados dos nós.

Etapa 2

O caso do Bitcoin

Introdução

O Bitcoin foi o primeiro caso de adoção global de uma criptomoeda baseada em blockchain.



Introdução

O Bitcoin foi criado por um pseudônimo chamado Satoshi Nakamoto, que pode ser uma pessoa, empresa ou uma equipe de desenvolvedores.



Sobre a criptomoeda

- 1 BTC valia uma fração de um centavo de dólar no início de 2010;
- Em 2011, ultrapassou 1 USD;
- No final de 2017, chegou a quase 20.000,00 USD;
- Em novembro de 2021 alcançou os 68.000 USD.

Sobre a criptomoeda

No dia 22 de maio de 2010 foi realizada a primeira compra utilizando o bitcoin como forma de pagamento, onde duas pizzas no valor de US\$ 45,00 foram compradas por 10.000 bitcoins;



Sobre a criptomoeda

- Tem um *supply* definido em 21 milhões de unidades;
- A "taxa" de **mineração** (emissão) de novos bitcoins é constante e cai periodicamente (inflação controlada);
- O último bitcoin será minerado no ano de 2140.

Características do bitcoin

- Descentralizado e distribuído
- Anônimo
- Transparente
- Imutável

Descentralização

Os sistemas financeiros convencionais estão todos subordinados a autoridades e governos, que impõem as regras para sua utilização, sendo assim **sistemas centralizados**.

Descentralização

Dessa forma o sistema pode ser manipulado de acordo com o interesse e poder de pessoas, o que pode tornar desvantajoso e sem transparência.

Descentralização

Além disso há o problema do único ponto de falha, que pode comprometer o sistema por falta de redundância.

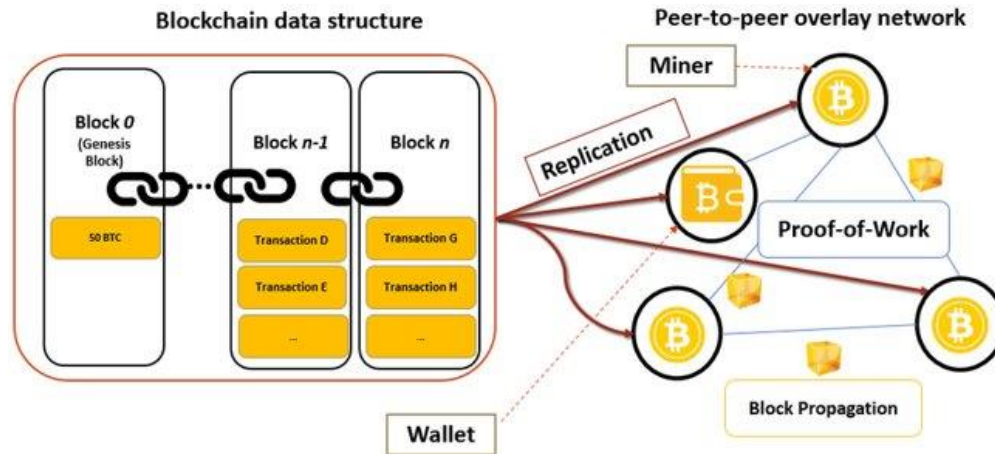
Descentralização

O bitcoin é descentralizado em todos os seus aspectos, inclusive o desenvolvimento de atualizações que são decididas em consenso pela equipe desenvolvedora.

Descentralização

Toda a sua arquitetura está baseada em nós **descentralizados e distribuídos** que possuem cópias iguais dos registros de transações, sendo validados por **algoritmo de consenso**.

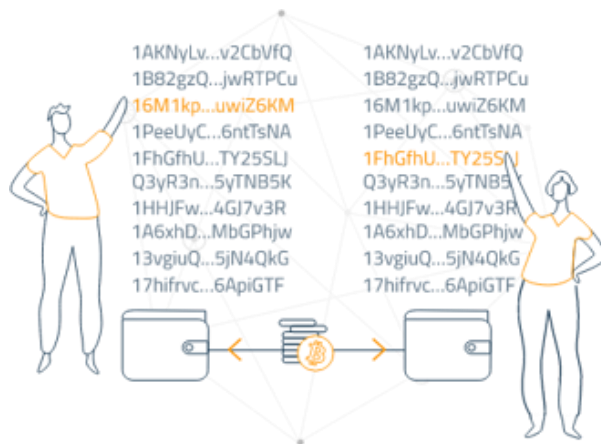
Descentralização



Anonimato

Essa característica se refere ao fato de não ser necessário atrelar uma identidade de uma pessoa a uma carteira de bitcoin.

Anonimato

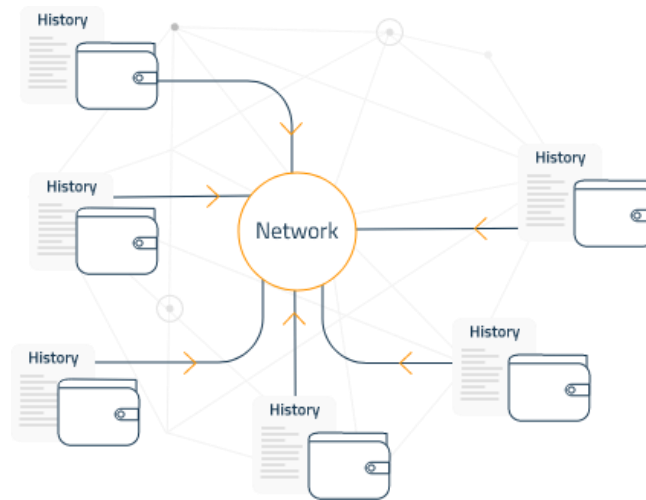


Transparência

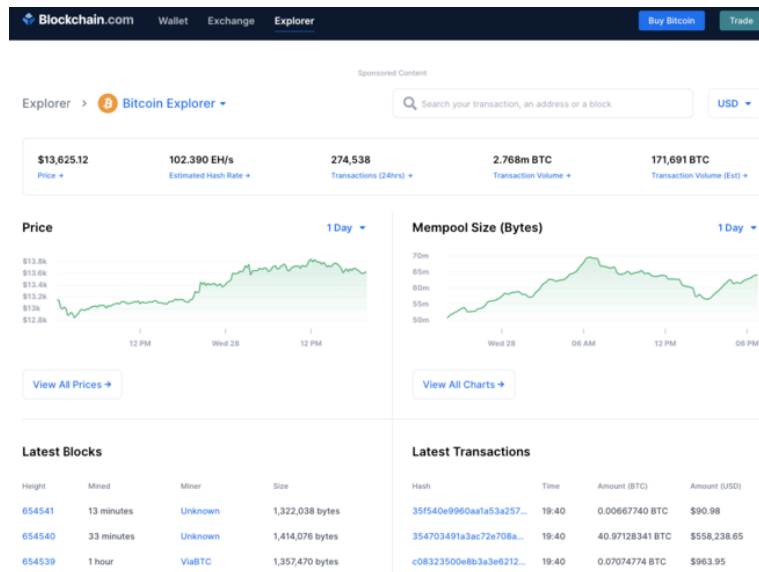
Todas as transações registradas na blockchain do bitcoin são **públicas** permitindo a qualquer pessoa verificar as transações.

Geralmente é feito através de **buscadores de blocos**.

Transparência



Transparência



Imutabilidade

Uma transação feita no bitcoin é impossível de ser revertida.
Isso se dá por causa da replicação dos registros nos nós da rede Bitcoin.

Imutabilidade



Desafios

- Regulamentações
- Chaves perdidas
- Volatilidade do preço

Conclusão

O bitcoin foi um caso de disrupção nos sistemas de pagamento, oferecendo uma opção descentralizada, transparente, segura e confiável de transacionar valores.

Etapa 3

Conceitos de criptografia na Blockchain

Introdução

Nesta etapa vamos falar de um conceito fundamental por trás de toda a tecnologia blockchain, a **criptografia**.

Introdução

Criptografia é a conversão de dados de um formato legível para um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.



Introdução

A segurança de uma criptografia é diretamente proporcional à sua complexidade, o que exigirá mais esforço e recursos para ser quebrada, sendo mais resistente contra ataques do tipo **força bruta**.

Técnicas de criptografia

Existem duas técnicas mais utilizadas para a criptografia de dados, sendo a criptografia de **chave simétrica** e **chave assimétrica**.

Chave simétrica

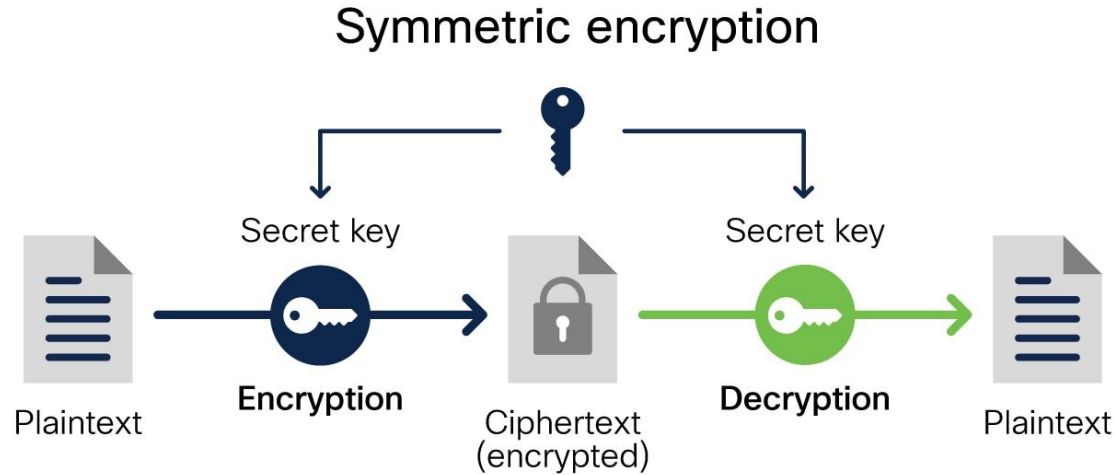
Também conhecida como criptografia de **chave privada**. A chave usada para **codificar** é a mesma usada para **decodificar**, sendo a melhor opção para **usuários individuais** e **sistemas fechados**.

Chave simétrica

Caso contrário, a chave privada deve ser enviada ao destinatário, porém aumenta o risco de comprometimento se for interceptada por um terceiro.

Esse método é mais rápido do que o método assimétrico.

Chave simétrica



Chave assimétrica

Nesse método duas chaves diferentes, **uma pública e uma privada**, que são vinculadas matematicamente.

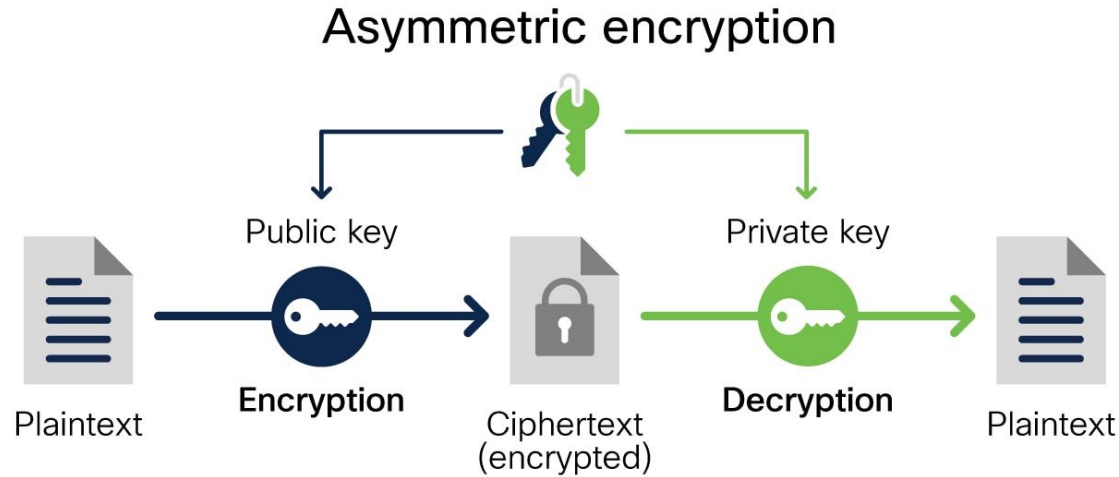
Essencialmente, as chaves são apenas grandes números emparelhados um ao outro, mas não são idênticos, daí o termo **assimétrico**.

Chave assimétrica

A chave privada é mantida em segredo pelo usuário, e a chave pública também é disponibilizada ao público em geral.

Essa é a criptografia utilizada para a **geração de carteiras no Bitcoin.**

Chave assimétrica



Carteiras no Bitcoin

No Bitcoin e em outras criptomoedas semelhantes existem as **carteiras**, que na prática são uma coleção de chaves privadas para que se possa gerar transações.

Bitcoin Address

1E1144JV6R7TCmj3B6Zjpofqf9EqP9vLKJm

Private Key

6JCG34xv2a040op1BfSwPicBNUNCuk9Ht1qWMgWoMJWJpownAAi

Public Key

0798694TR67C50Z680FVRD54SX9L833137Y30K70062CCEF18L5213I9R471P0107

Carteiras no Bitcoin

Para a geração de carteiras, utiliza-se um algoritmo de **dispersão criptográfica** ou **função hash** criptográfica, onde é praticamente impossível de inverter, isto é, de recriar o valor de entrada utilizando somente o valor de dispersão.

Conclusão

O bitcoin foi um caso de disrupção nos sistemas de pagamento, oferecendo uma opção descentralizada, transparente, segura e confiável de transacionar valores.

Etapa 4

Entendendo a criptografia SHA-256

Introdução

Nesta etapa vamos explorar um pouco mais do SHA-256, o algoritmo responsável pela criptografia dos blocos e das carteiras na blockchain.

Introdução

Este algoritmo criptográfico foi desenvolvido pelo Agência de Segurança Nacional dos Estados Unidos (NSA) e do Instituto Nacional de Padrões e Tecnologia (NIST).

Sobre o SHA-256

O SHA-256, do inglês "Secure Hash Algorithm", é uma função criptográfica utilizada como base do sistema de prova de trabalho do Bitcoin.

Sobre o SHA-256

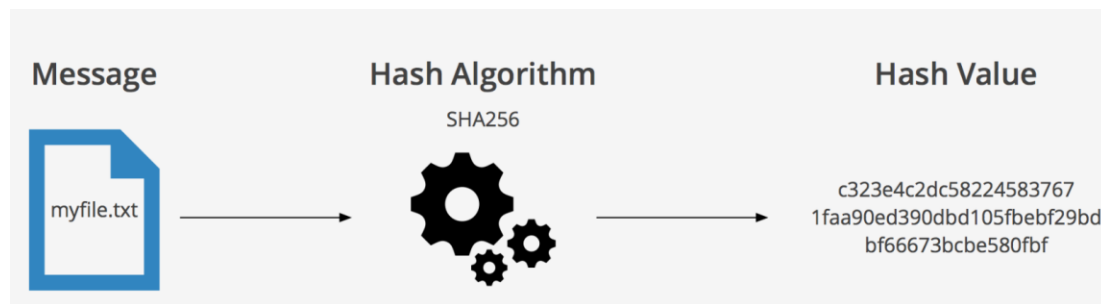
O objetivo é gerar **hashes** ou códigos exclusivos com base em um padrão com o qual documentos ou dados do computador possam ser protegidos contra qualquer agente externo que deseje modificá-los.

Sobre o SHA-256

No caso do Bitcoin, o SHA-256 é usado para o processo de mineração (criação de bitcoins), mas também no processo de geração endereços de bitcoin. Isso se deve ao alto nível de segurança que oferece.

Sobre o SHA-256

A função SHA-256 recebe uma entrada de **tamanho aleatório** e a converte em uma saída de **tamanho fixo de 256 bits**.



Sobre o SHA-256

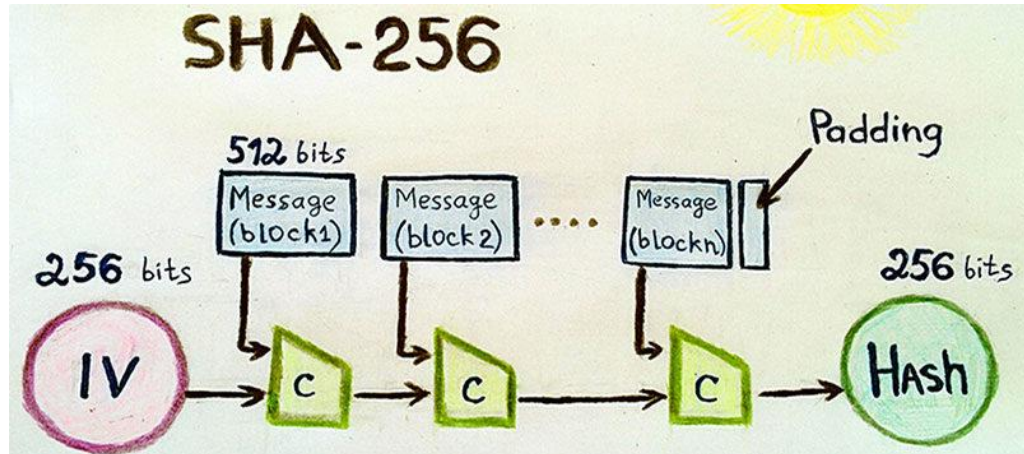
Vamos simular a conversão de alguns dados utilizando o SHA-256.

[Conversor online de SHA-256](#)

Propriedades do SHA-256

A função SHA-256 na mineração do Bitcoin se dá quando um **nó** se torna elegível a fim de colocar novos blocos dentro da blockchain.

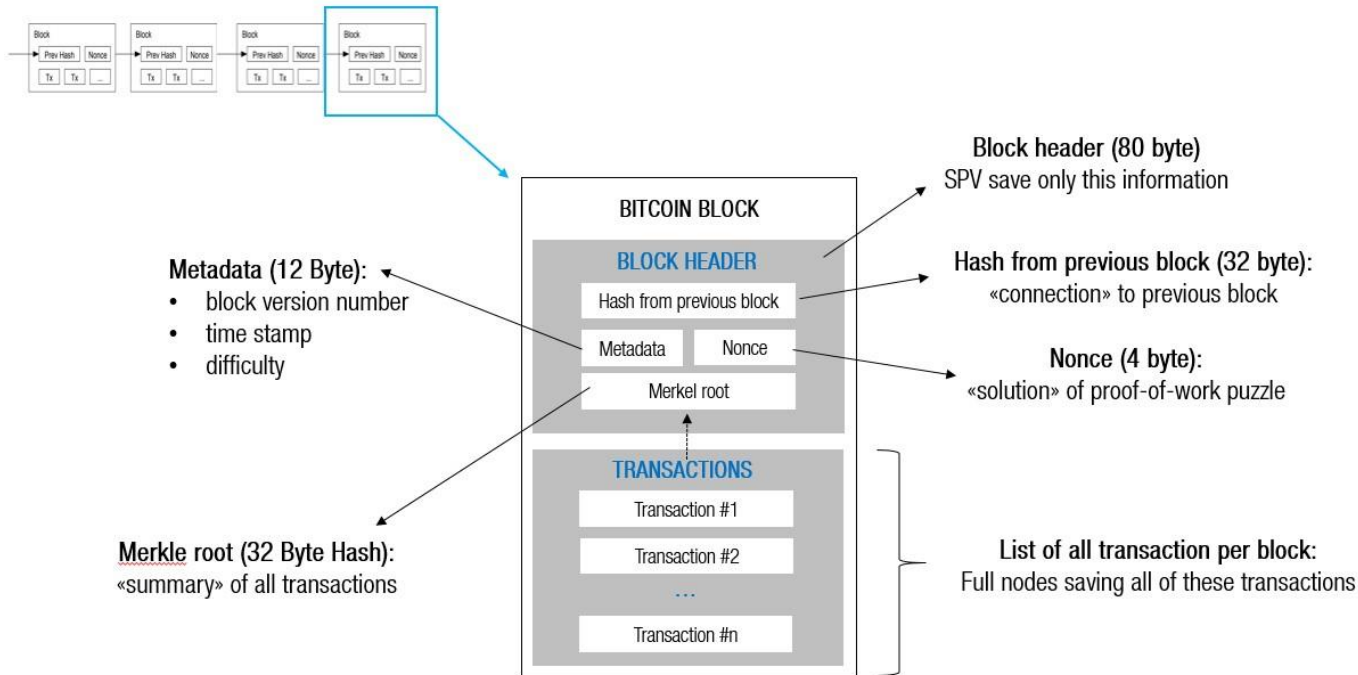
Propriedades do SHA-256



Propriedades do SHA-256

Para ser um bloco válido o bloco deve ter os seguintes atributos:

Propriedades do SHA-256



Propriedades do SHA-256

Versão: número da versão do software Bitcoin

Hash do bloco anterior: referência ao hash do bloco anterior

Raiz de Merkle: um hash representativo das transações incluídas no bloco

Propriedades do SHA-256

Registro de data e hora: o horário em que o bloco foi criado

Target: algoritmo de prova de trabalho para o bloco

Nonce: a variável usada no processo de prova de trabalho

Conclusão

Nesta etapa nós vimos o papel da criptografia no contexto da blockchain e a sua importância fundamental.

Etapa 5

Simulando transações

Introdução

Nesta aula vamos simular transações em uma blockchain semelhante à do Bitcoin.

Hash	Block	Blockchain	Distributed	Tokens	Coinbase
------	-------	------------	-------------	--------	----------

Peer A

Block:

1

Nonce:

16651

Coinbase:

\$ 100.00

->

Anders

Tx:

Prev:

00

Hash:

0000438d7625b86a6f366545b1929975a0d3f1f8847e56cc587caddb01

Mine

Block:	# 2		
Nonce:	215458		
Coinbase:	\$ 100.00	->	Anders
Tx:	\$ 10.00	From: Anders	-> Sophia
	\$ 20.00	From: Anders	-> Lucas
	\$ 15.00	From: Anders	-> Emily
	\$ 15.00	From: Anders	-> Madison
Prev:	000043bd7625b86a6f366545b1929975a0d3ff1f8847e36c557caddb0		
Hash:	0000baae68c2a60f9a56355438d97c67a215494fce6f17064d9314f1		

Block:	#	3	
Nonce:	146		
Coinbase:	\$	100.00	
Tx:	\$	10.00	From:
	\$	5.00	From:
	\$	20.00	From:
Prev:	0000baaab68c2a60f9a6fa56355		
Hash:	0000df1d632b734f5a5fc126a0f		
Mine			

Peer B

Block: # 1

Nonce: 16651

Block: # 2

Nonce: 215458

Block: # 3
Nonce: 146

Introdução

Para isto vamos utilizar um simulador de transações disponível no seguinte [link](#).

Etapa 6

Sobre carteiras e endereços bitcoin

Introdução

Nesta etapa vamos falar de como podemos armazenar criptomoedas por meio de carteiras.



O que são carteiras?

Uma carteira, ou **wallet**, é uma espécie de conta bancária de bitcoin, onde por meio do **endereço público** depositamos e com a chave privada sacamos.

O que são carteiras?

No contexto de criptomoedas, carteiras se referem também à estrutura de dados usadas no gerenciamento das **chaves** do usuário.

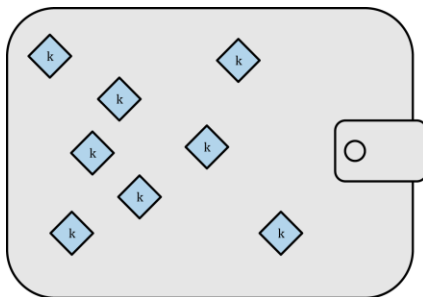
O que são carteiras?

Existem no caso do Bitcoin, alguns tipos de carteiras:

- Não-determinística;
- Determinística;
- HD – *Hierarchical Deterministic*;
- Mnemonic – BIP 39

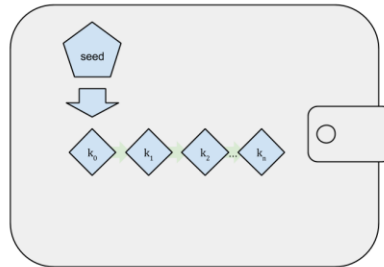
Carteiras não-determinísticas

A primeira versão das carteiras, onde são geradas 100 chaves privadas na inicialização, porém tal número de chaves não tem um gerenciamento muito prático.



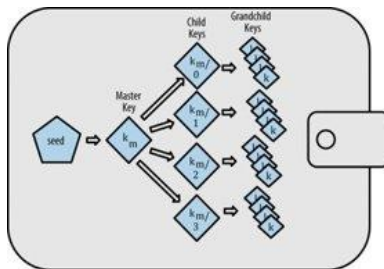
Carteiras determinísticas

Contém as chaves privadas derivadas de uma semente – *seed* - podendo gerar inúmeros endereços.



Carteiras HD

Parecida com a determinística, possui uma hierarquia de chaves que partem de uma mesma semente – *seed*.



Mnemonic

Cria uma sequência de palavras em inglês, fáceis de escrever, armazenar e importar.

Exemplo de mnemonic:


**army van defense carry jealous true
garbage claim echo media make crunch**

O que são endereços?

Um endereço de criptomoedas é uma espécie de "número de conta bancária" onde são depositados os fundos.


Um usuário pode criar inúmeros endereços, sem limites.

O que são endereços?





Address

bc1q9d4ywgfnd8h43da5tpcxcn6ajv590cg6d3t
g6axemvljvt2k76zs50tv4q



Balance	24,954.9595474 BTC · 1,104,481,554.61 USD
Total received	24,954.9595474 BTC · 1,016,208,948.29 USD
Total spent	0 BTC · 0 USD

 Wallet statement

 Get tax report

Tipos de endereços

Existem atualmente três tipos de endereços no ***Bitcoin Core***:

- P2PKH
- P2SH
- bech32

P2PKH – *Pay-to-Pubkey Hash*

É o primeiro e mais utilizado formato de endereço, também chamado de *legacy* e sempre começa com o número **1**.

Possui as taxas de transferência mais caras pois não é compatível com os novos tipos de endereços.

1PvPOdEYstMbpqTRn8Au3m3HEg7xJbECS3

P2SH – *Pay-to-Script Hash*

- É um formato baseado em compatibilidade, com funcionalidades mais elaboradas que o formato legacy.
- Muito utilizado em carteiras ***multisig***, onde mais de uma carteira assinando é necessária para autorizar uma transação.

P2SH – *Pay-to-Script Hash*

- Começa sempre com o número 3.

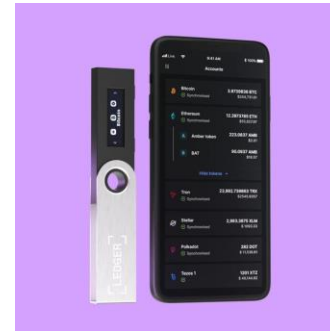
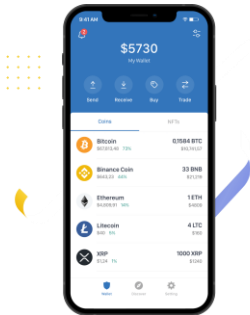
3G45p1GpEZ75NNmQvaicnyyiWrnqDhDMJi

BECH32 – Segwit Nativo

- Segwit significa *segregated witness*, ou testemunha segregada;
- Reduziu o custo das transações e aumentou o tamanho dos blocos;
- Suporta o Lightning Network.

Tipos de carteiras

Existem diversas formas de gerenciar carteiras de criptomoedas, como hardware wallets, paper wallets, desktop e mobile wallets.



Conclusão

Chegamos ao final do nosso curso, onde pudemos explorar os fundamentos relacionados à blockchain e exploramos o caso do Bitcoin.

Desafio de Projeto

**Criando e utilizando a sua
carteira de criptomoedas**

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

