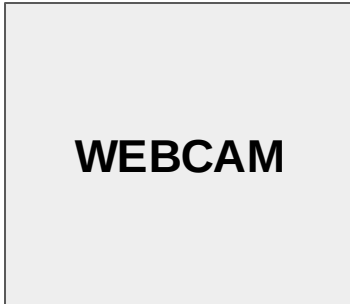
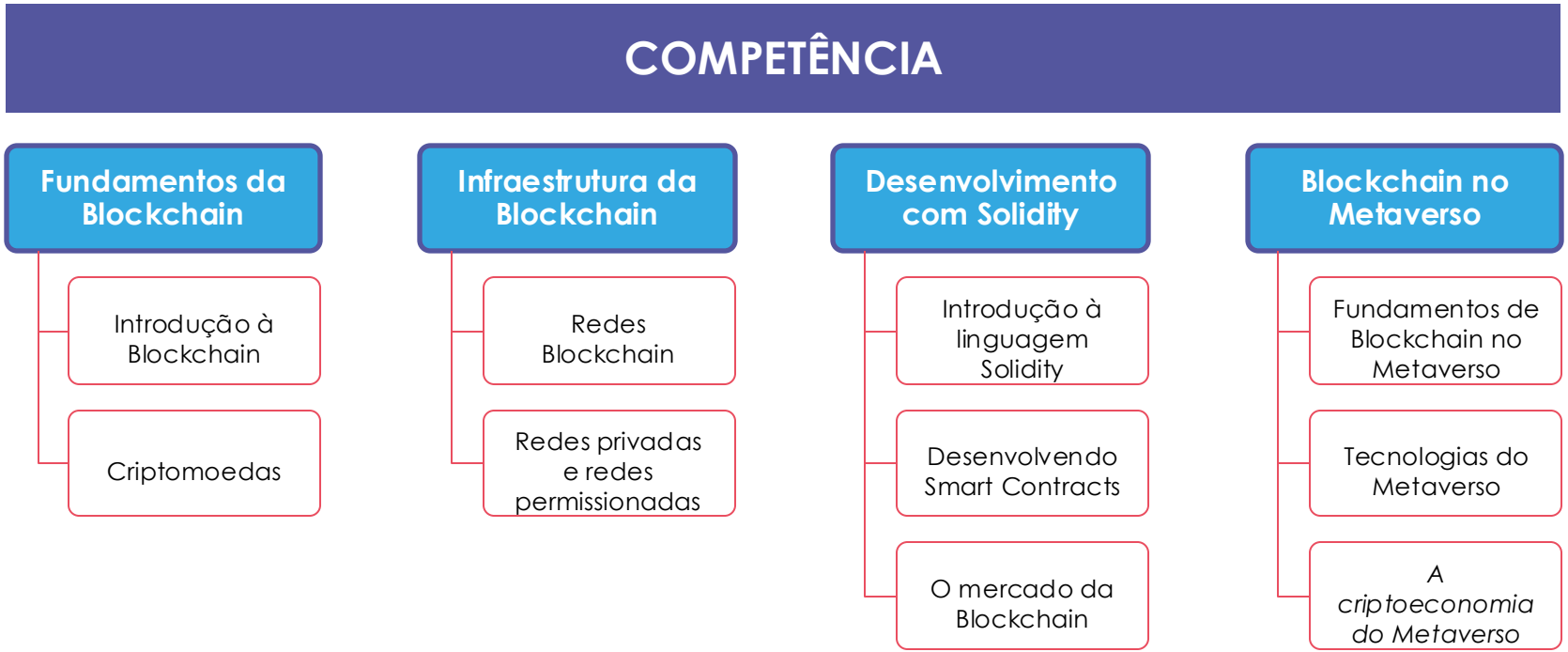
Espaço da webcam

Em todos os slides, evite escrever ou usar imagens que possam ocupar a área mostrada ao lado, pois ela representa o espaço reservado para a webcam.

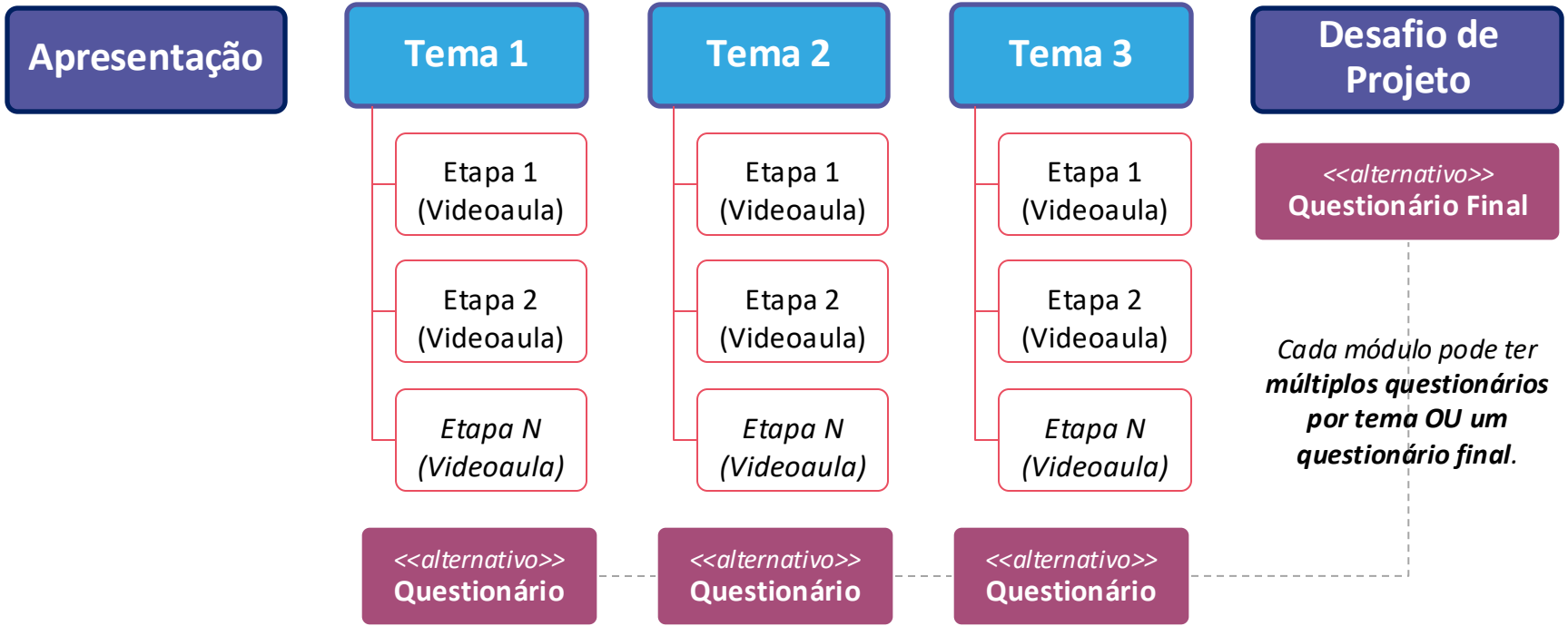


Estrutura das Trilhas



Nesse contexto, **"Módulos" são "Subcompetências".**

Estrutura dos Módulos



Cada **Etapa deve ter, idealmente, em torno de 15 minutos** (isso pode variar, principalmente em videoaulas práticas). Analogamente, recomendamos que cada **Tema tenha entre 2 e 4 horas**.

Introdução à Linguagem Solidity

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 realacionados à base da Blockchain, desde seus aspectos teóricos até a sua implementação.

Pré-requisitos

- Conhecimento básico em JavaScript, C++ ou Python;
- Noções de redes de computadores;
- Conhecimento fundamental de criptografia e algoritmos.

Percurso

Etapa 1	Características da Linguagem
Etapa 2	Tipos de dados
Etapa 3	Métodos no Solidity

Percurso

Etapa 4	Bibliotecas
Etapa 5	Storage, Memory e variáveis de estado
Etapa 6	Structures e Arrays

Percurso

Etapa 7	Configurações de ambiente
Etapa 8	A IDE Remix
Etapa 9	Criando o seu primeiro Smart Contract com Solidity

Etapa 1

Características da Linguagem

Introdução

Neste curso vamos conhecer a linguagem Solidity, utilizada para o desenvolvimento de *Smart Contracts*.

Introdução

Neste curso vamos compreender conceitos fundamentais da linguagem Solidity, possibilitando o desenvolvimento de aplicações práticas.

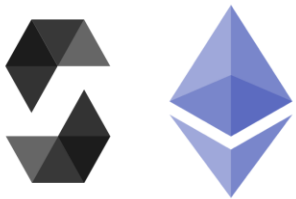
A linguagem Solidity

O Solidity é uma linguagem de **alto nível** e **orientada a contratos**.

Possui uma sintaxe simples, voltada para o registro e leitura de **transações** em contratos inteligentes na blockchain

A linguagem Solidity

É uma linguagem muito influenciada pelas linguagens Python, C++ e JavaScript e foi projetada para ser executada sobre a ***Ethereum Virtual Machine*** (EVM).



A linguagem Solidity

Pode ser utilizada para desenvolver contratos como votações, crowdfunding, rastreabilidade de ativos, NFT's, entre outros

A plataforma Ethereum

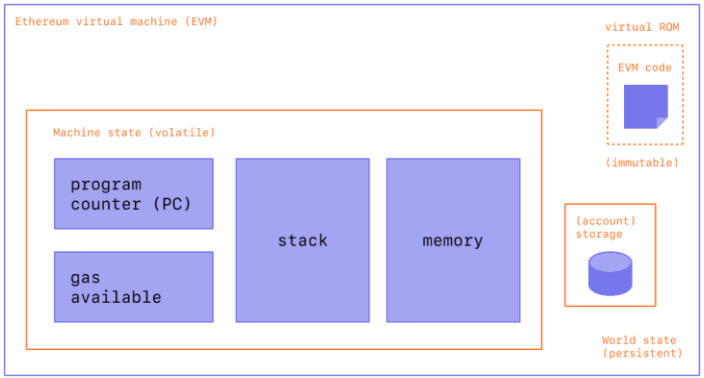
É uma plataforma descentralizada de blockchain que suporta os **contratos inteligentes**, aplicações que executam de forma independente, sem *downtime*, censura, fraude ou interferência de terceiros.

A plataforma Ethereum

Foi criado em 2015 por um time liderado por **Vitalik Buterin**, e o ***Ether*** (criptomoeda relacionada à plataforma) é a segunda criptomoeda mais valiosa do mundo, atrás apenas do Bitcoin.

Ethereum Virtual Machine

Também conhecida como EVM, é o ambiente para a execução de contratos inteligentes do Ethereum.

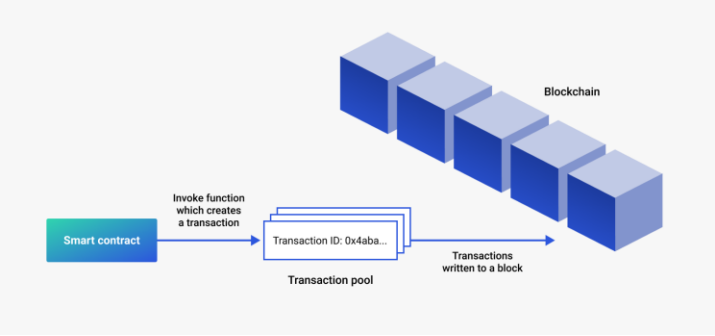


Smart Contracts

É um protocolo direcionado para verificar e garantir de forma digital a performance e a confiabilidade de um contrato, sendo um intermediário entre as partes.

Smart Contracts

Dessa forma as transações são rastreáveis e irreversíveis, deixando para a criptografia a garantia de veracidade dos dados



Smart Contracts

Um Smart Contract baseado em Solidity é uma coleção de **funções** e **dados**, e está registrado em um endereço na blockchain do Ethereum

Smart Contracts

```
pragma solidity ^0.5.0;

contract SolidityTest {

   constructor() public{

   }

   function getResult() public view returns(uint){

      uint a = 1;

      uint result = a * 2;

      return result;

   }
```

Conclusão

Nesta aula vimos de forma panorâmica as características do Solidity e da plataforma Ethereum.

Nas etapas seguintes veremos de forma mais detalhadas essas características.

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, schegou 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.

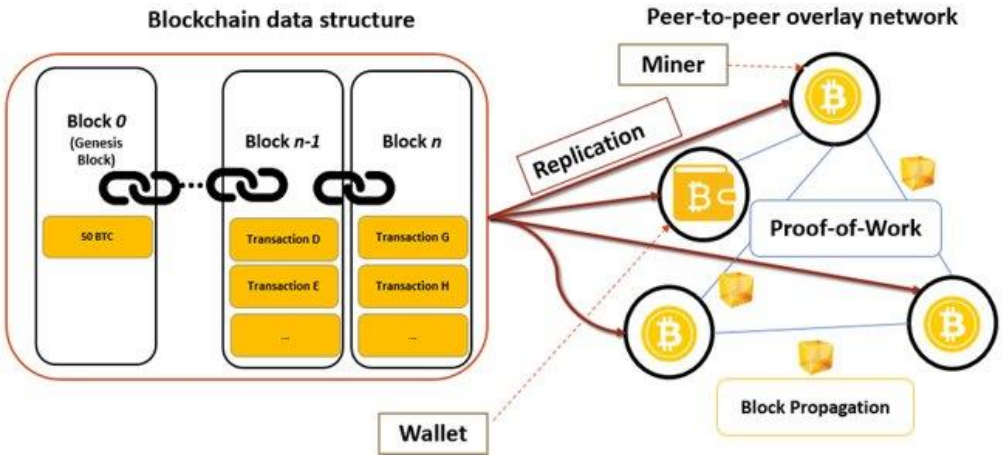
Descentralização

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

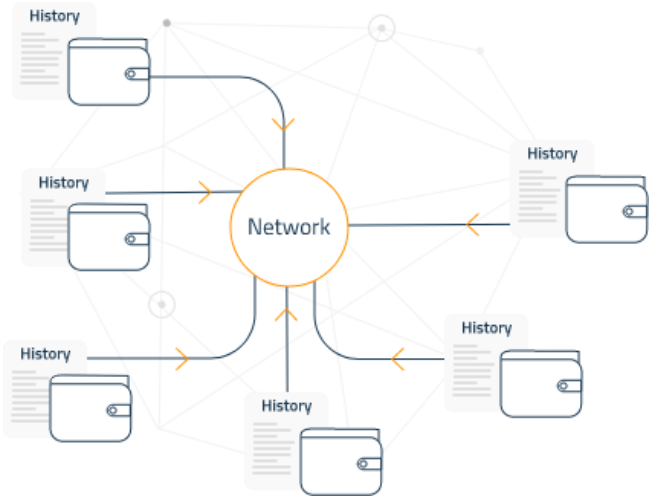

1AKNyLv...v2CbVfQ
1B82gzQ...jwRTPCu
16M1kp...uwiZ6KM
1PeeUyC...6ntTsNA
1FhGfhU...TY25SLJ
Q3yR3n...5yTNB5K
1HHJFw...4GJ7v3R
1A6xhD...MbGPhjw
13vgiuQ...5jN4QkG
17hifrvc...6ApiGTF
1AKNyLv...v2CbVfQ
1B82gzQ...jwRTPCu
16M1kp...uwiZ6KM
1PeeUyC...6ntTsNA
1FhGfhU...TY25SNJ
Q3yR3n...5yTNB5K
1HHJFw...4GJ7v3R
1A6xhD...MbGPhjw
13vgiuQ...5jN4QkG
17hifrvc...6ApiGTF

Transparência

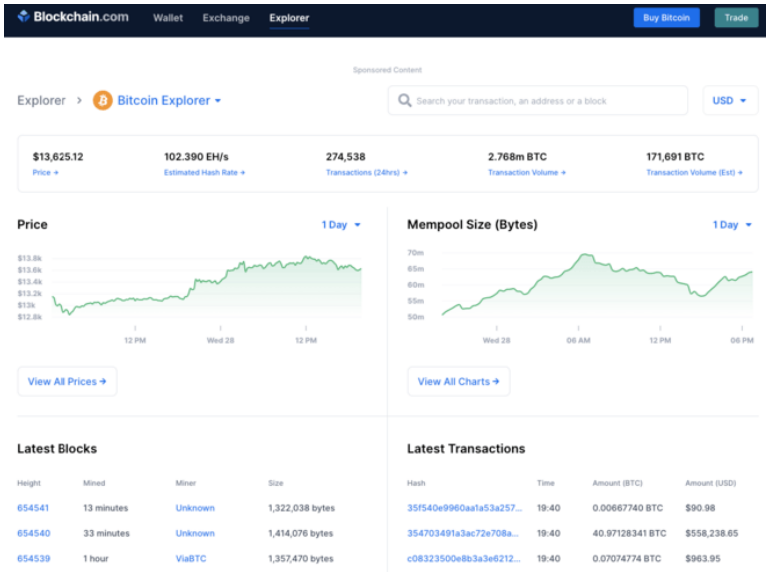
Todas as transações registradas na blockchain do bitcoin são **públicas** permitindo a qualquer pessoa verificar as transações.

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

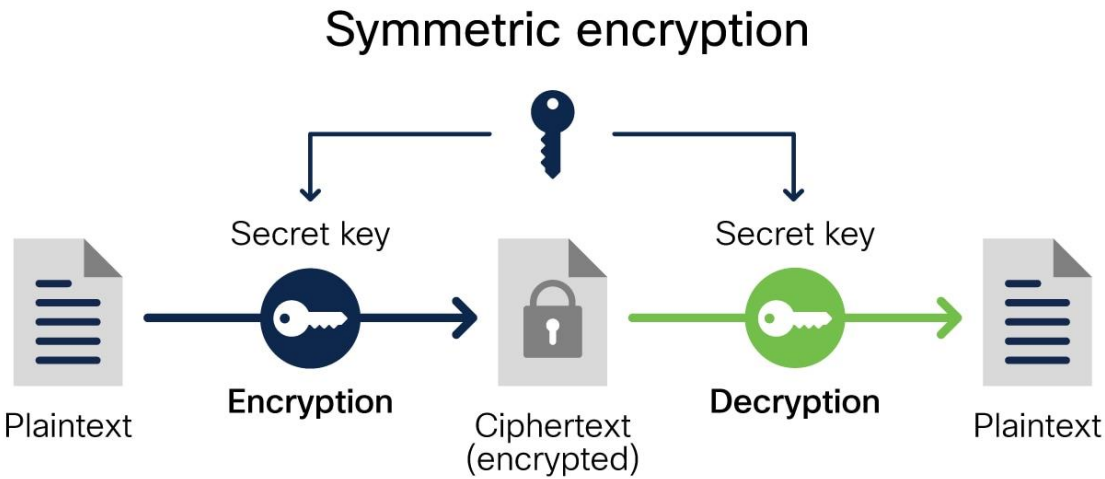
Também conhecida como criptografia de **chave privada**. A chave usada para **codificar** é a mesma usada para **decodificar**, sendo a melhor opção para **usuários individuais** e **sistemas fechados**.

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.

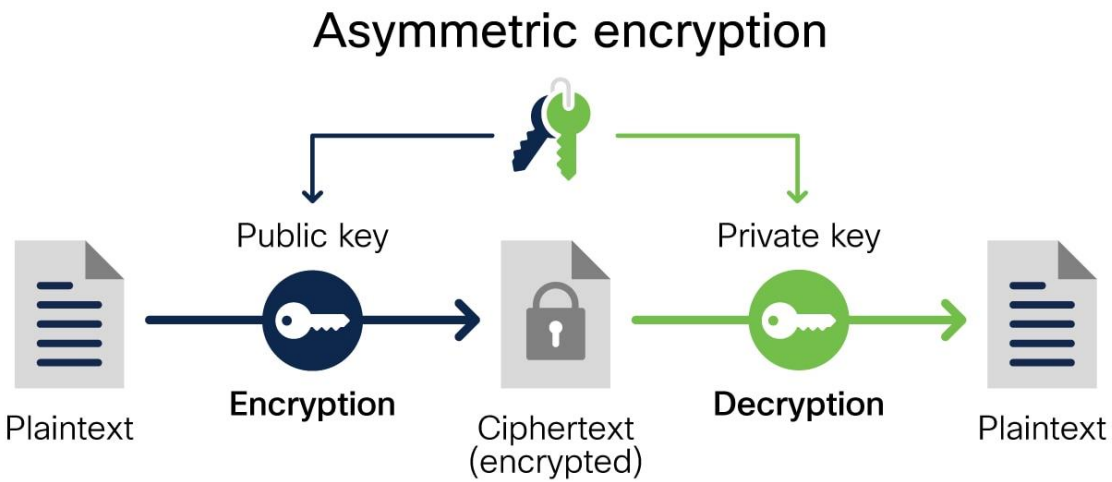
Essencialmente, as chaves são apenas grandes números emparelhados um ao outro, mas não são idênticos, daí o termo **assimétrico**.

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.

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 te 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

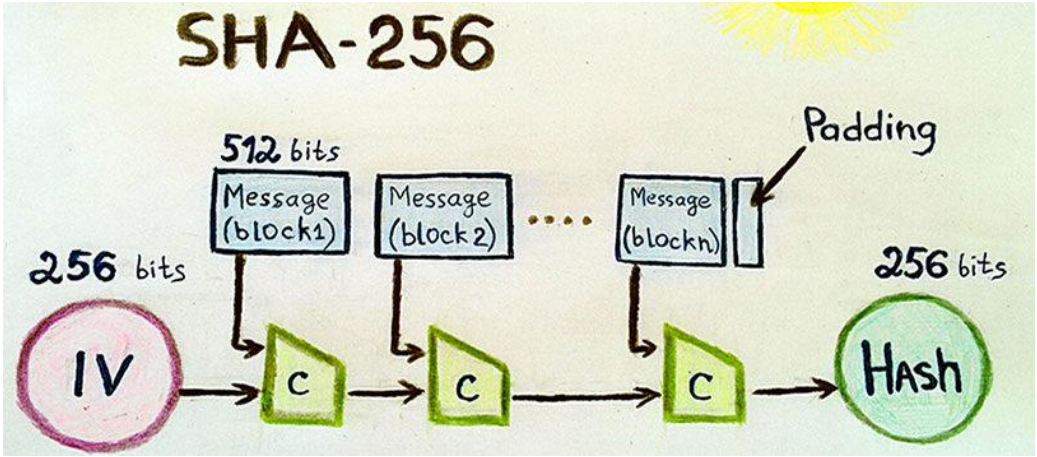
Vamos simular a conversão de alguns dados utilizando o SHA-256.

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.

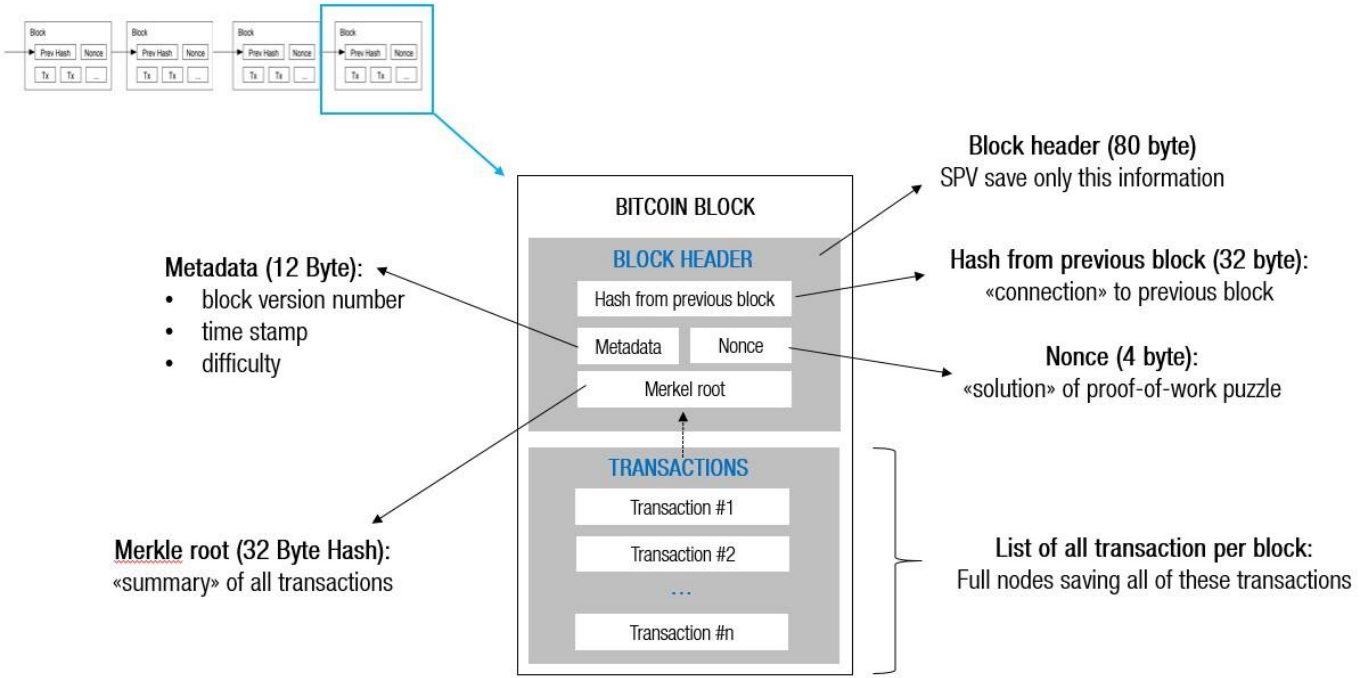
Propriedades do SHA-256



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: algoritimo 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

O que são redes P2P

Tópico da Etapa 1

Conteúdo...

Etapa 6

Ledgers e registros imutáveis

Tópico da Etapa 1

Conteúdo...

Etapa 7

Algoritmos de consenso

Tópico da Etapa 1

Conteúdo...

Etapa 8

O problema dos generais bizantinos

Tópico da Etapa 1

Conteúdo...

Etapa 9

Sobre hard e soft forks

Tópico da Etapa 1

Conteúdo...

Etapa 10

Tipos de ataques contra a blockchain

Tópico da Etapa 1

Conteúdo...

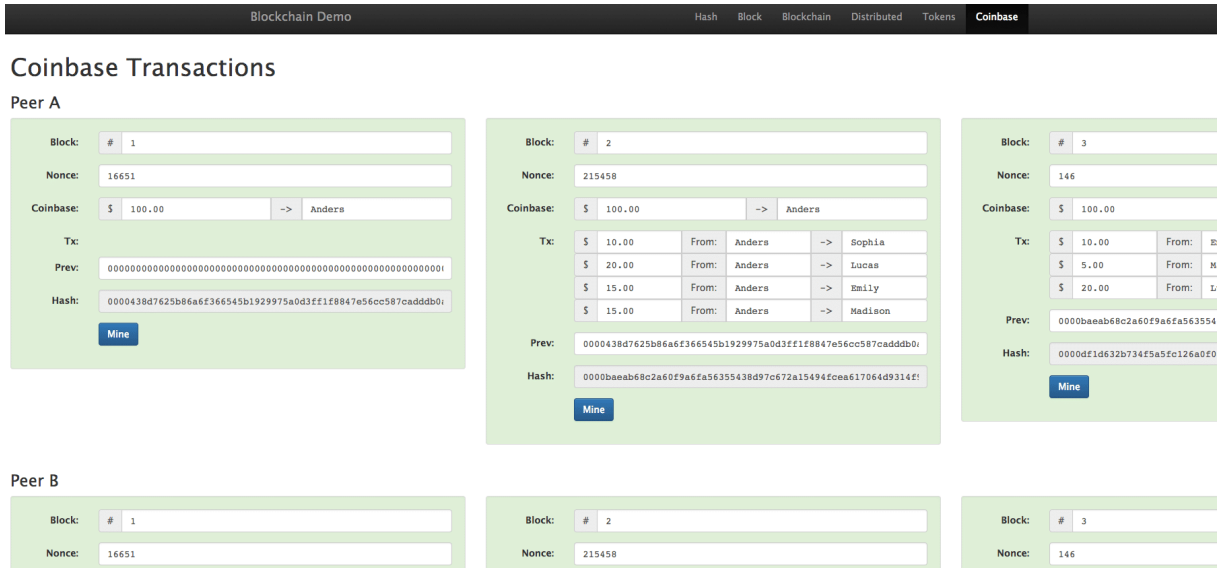
Etapa 11

Simulando transações

Introdução

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

Introdução


Blockchain Demo
Hash
Block
Blockchain
Distributed
Tokens
Coinbase
Coinbase Transactions
Peer A
Block: # 1
Nonce: 16651
Coinbase: $ 100.00 -> Anders
Tx:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0
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: 0000438d7625b86a6f366545b1929975a0d3ff1f8847e56cc587cadddb0
Hash: 0000baeab68c2a60f9a6fa56355438d97c672a15494fcea617064d9314f
Mine
Block: # 3
Nonce: 146
Coinbase: $ 100.00
Tx: $ 10.00 From:
$ 5.00 From:
$ 20.00 From:
Prev: 0000baeab68c2a60f9a6fa563554
Hash: 0000df1d632b734f5a5fc126a0f0
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 12

Como a blockchain está mudando a história

Tópico da Etapa 1

Conteúdo...

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)