

Como funciona a Blockchain?

Fundamentos da Blockchain

Juliana Mascarenhas

Tech Education Specialist DIO / Owner @Simplificandoredes
e @SimplificandoProgramação

Mestre em modelagem computacional | Cientista de dados

@in/juliana-mascarenhas-ds/





<https://github.com/julianazanelatto>

Juliana Mascarenhas

Tech Education Specialist

@SimplificandoRedes

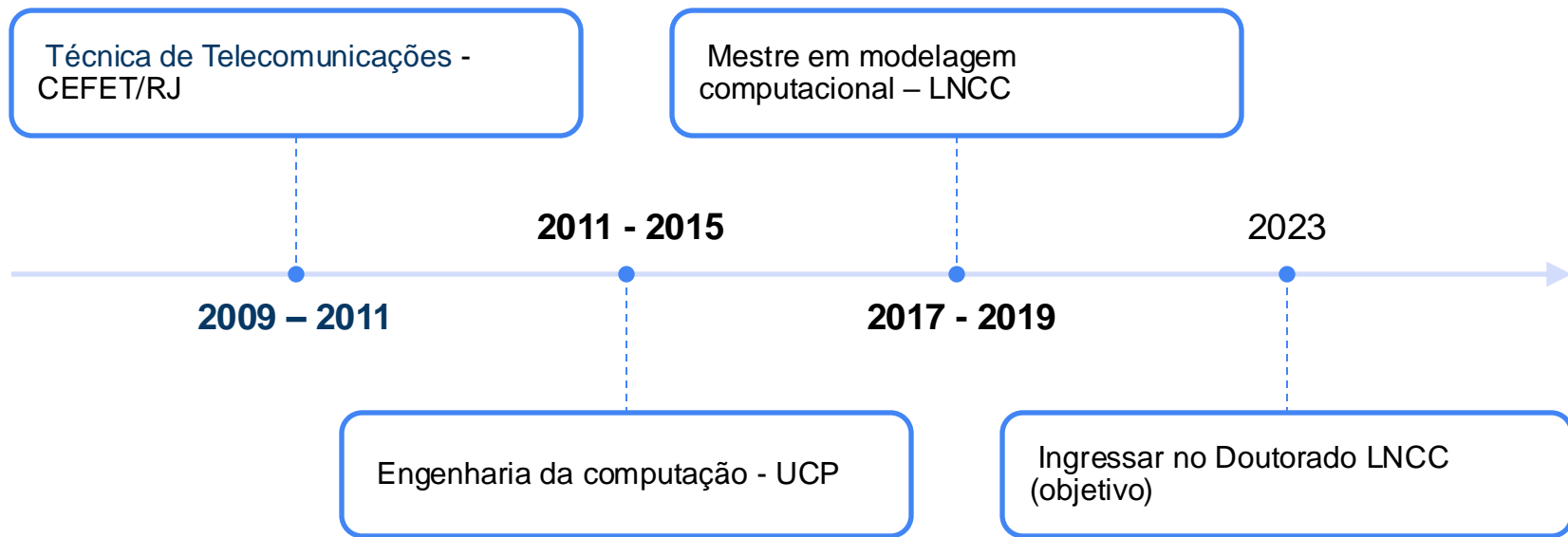
@SimplificandoProgramação

Cientista de dados

Desenvolvedora Java/Python

Me Modelagem Computacional - LNCC

Sobre Mim



Objetivo Geral

Entender o funcionamento operacional da Blockchain. Assim, estaremos estudando temas como estrutura, validação de transações e blocos, sistemas distribuídos, mecanismos de consenso entre outros conceitos relacionados.

Pré-requisitos

- Liste aqui os pré-requisitos para o tema, desde configurações do ambiente até as noções básicas necessárias para uma melhor assimilação do conteúdo

Percurso

Etapa 1

Blockchain: Um arcabouço Tecnológico

Etapa 2

Ledgers e Registros Imutáveis

Etapa 3

Transações e Blocos

Etapa 4

Como garantir a origem dos eventos ?

Percurso

Etapa 5

Inserção de Blocos e Bifurcações

Etapa 6

Blockchain e suas categorias

Etapa 7

Modificações Estruturais

Etapa 8

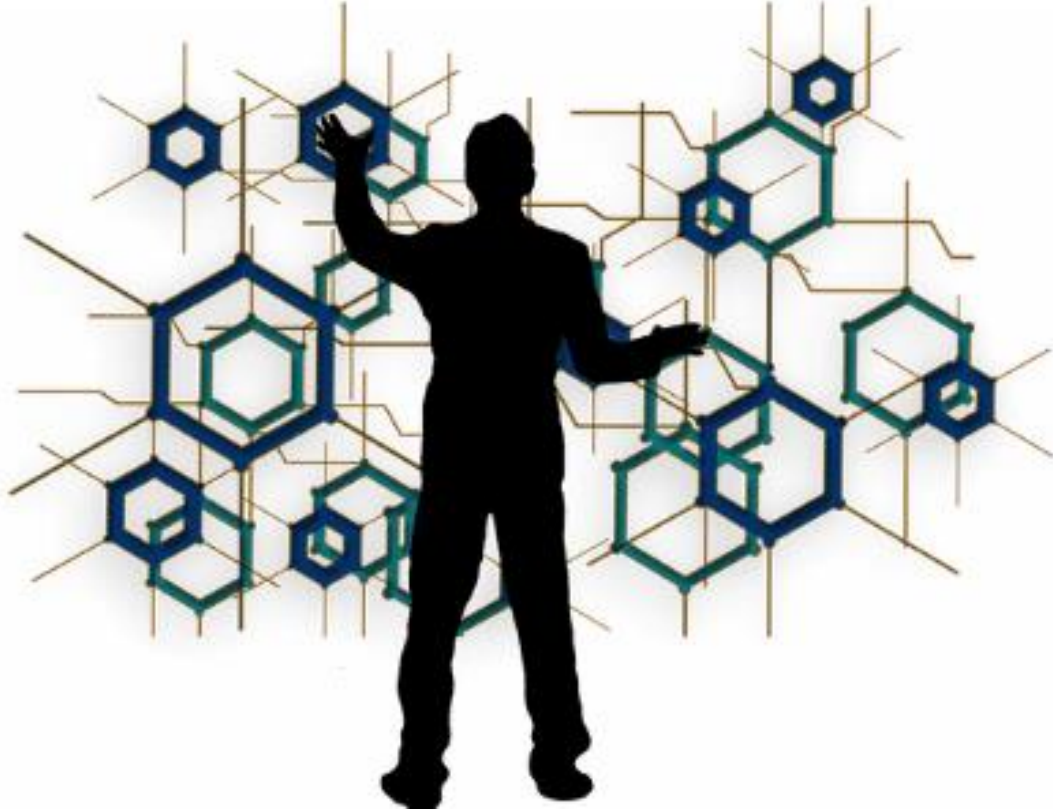
Desafios da Blockchain

Etapa 1

Blockchain: um arcabouço tecnológico

// Fundamentos da Blockchain

O que é a Blockchain?



O que é a Blockchain?

Blockchain é um banco de dados de registros distribuído ou livro razão público de todas as transações ou eventos realizados e compartilhados com os participantes da rede.

[AIR, 2016]

Contextualizando

Tempo

Processamento

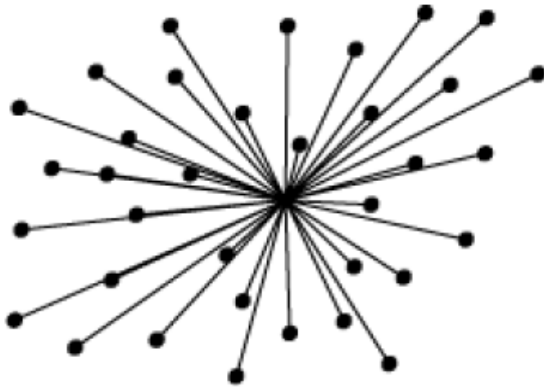
Aplicações

Performance

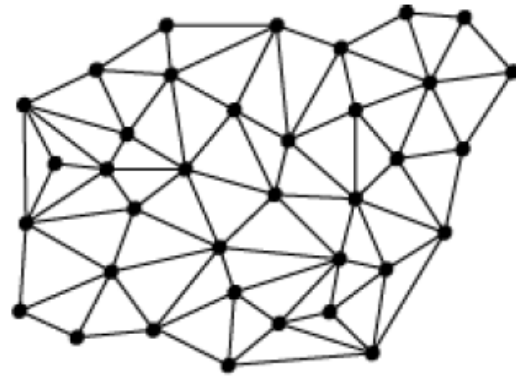


Blockchain

Centralizado

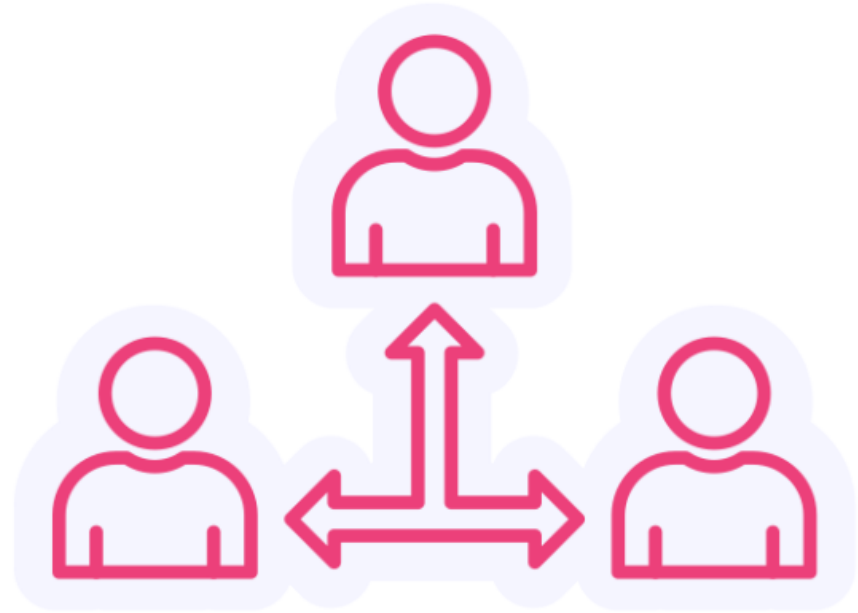
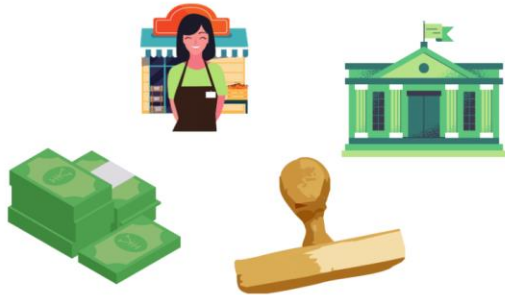


Distribuído



Blockchain

Trusted Third Party

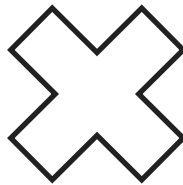


O que é a Blockchain?

Singularidade

Ownership

Privado



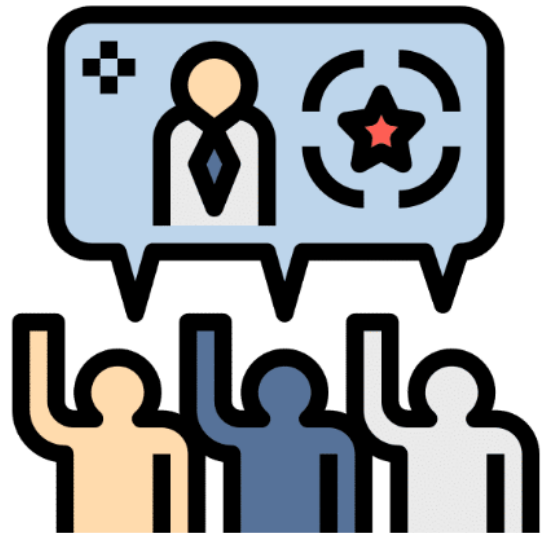
Distribuído

Consenso

Público

Premissas

- Os nós são confiáveis?
- Os nós participam do consenso
- Na criptografia confiamos
- Trabalho recompensado
- Colaboração



O que é a Blockchain?

Características

- Imutabilidade
- Irrefutabilidade
- Disponibilidade
- Integridade

- Transparência
- Visibilidade
- Desintermediação
- Pseudo-anonimidade

Difusão e armazenamento

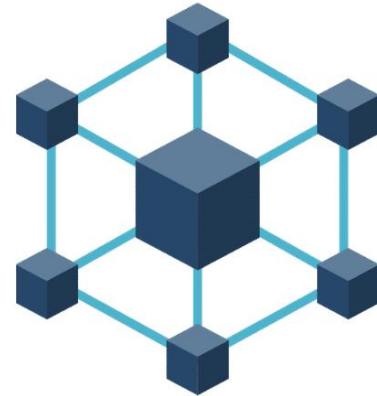
Tradicional



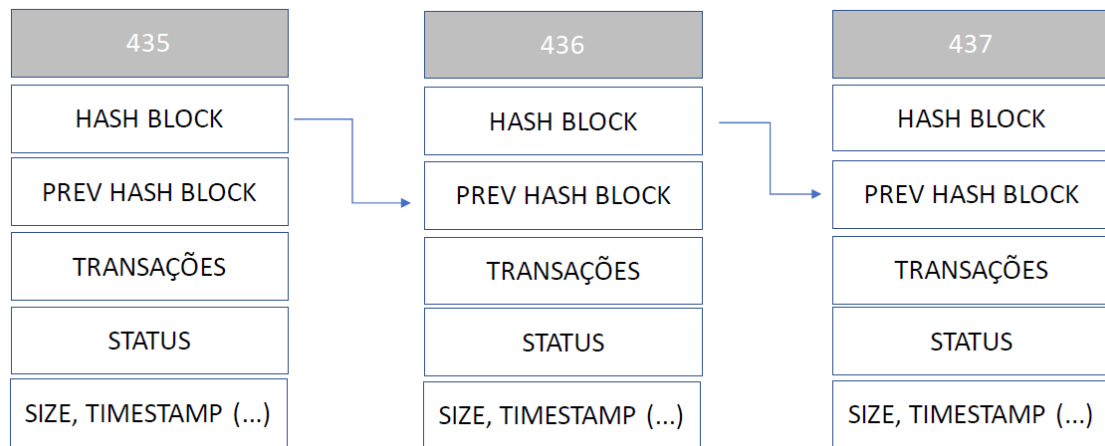
Distribuído



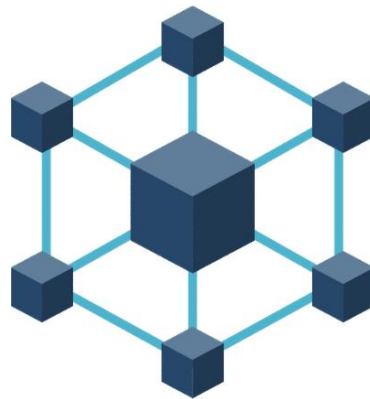
Blockchain



Difusão e armazenamento



Blockchain

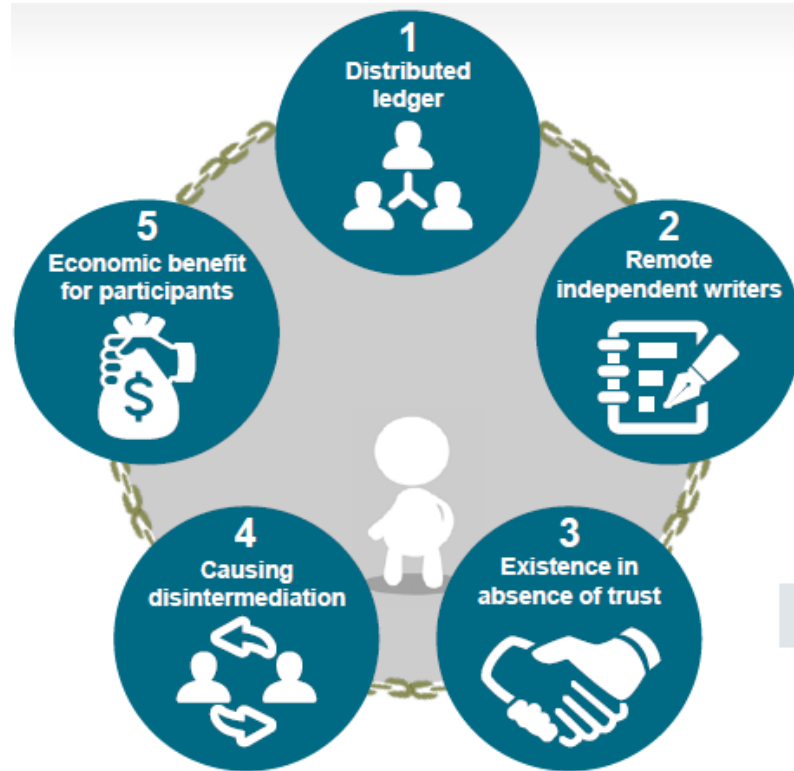


O que é a Blockchain?

- Rede P2P
- Processamento concentrado nos nós da rede
- Consenso Distribuído
- Anonimissidade
- Criptografia

Tecnologias
presentes na
Blockchain

Difusão e armazenamento

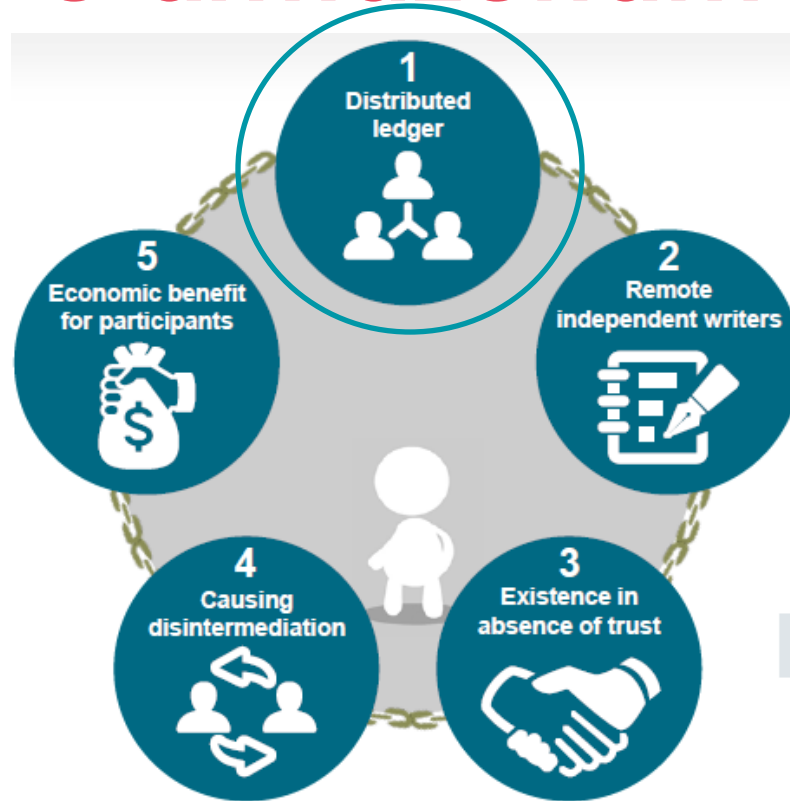


Etapa 2

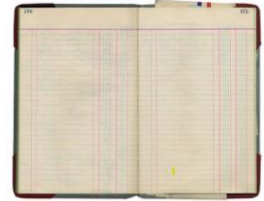
O que são Legder e Registros Imutáveis?

// Fundamentos da Blockchain

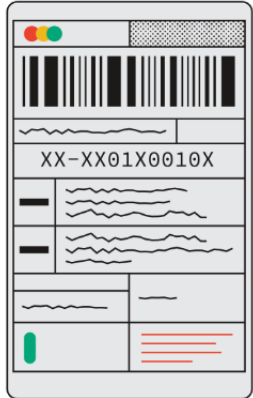
Difusão e armazenamento



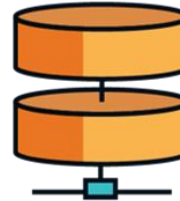
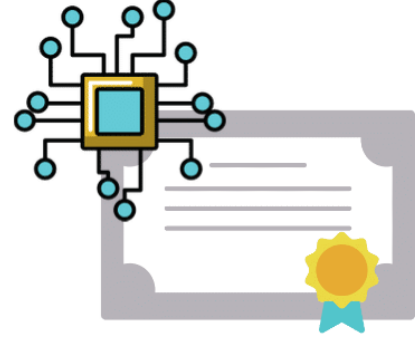
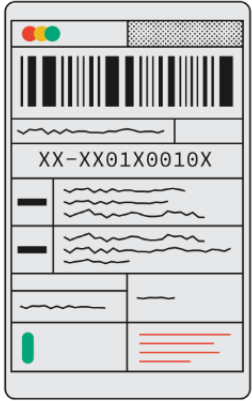
Registros



Históricamente utilizamos meio físicos para armazenar informações sobre nossos acordos e transações

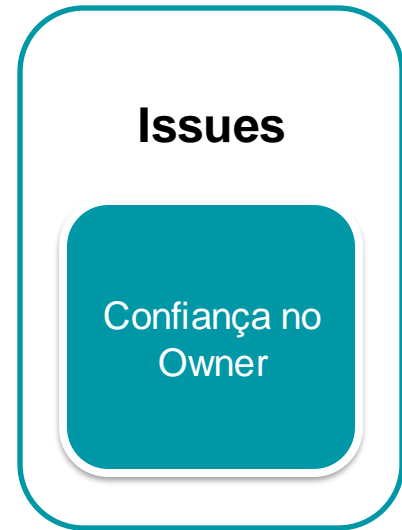


Registros



Ledgers Centralizadas

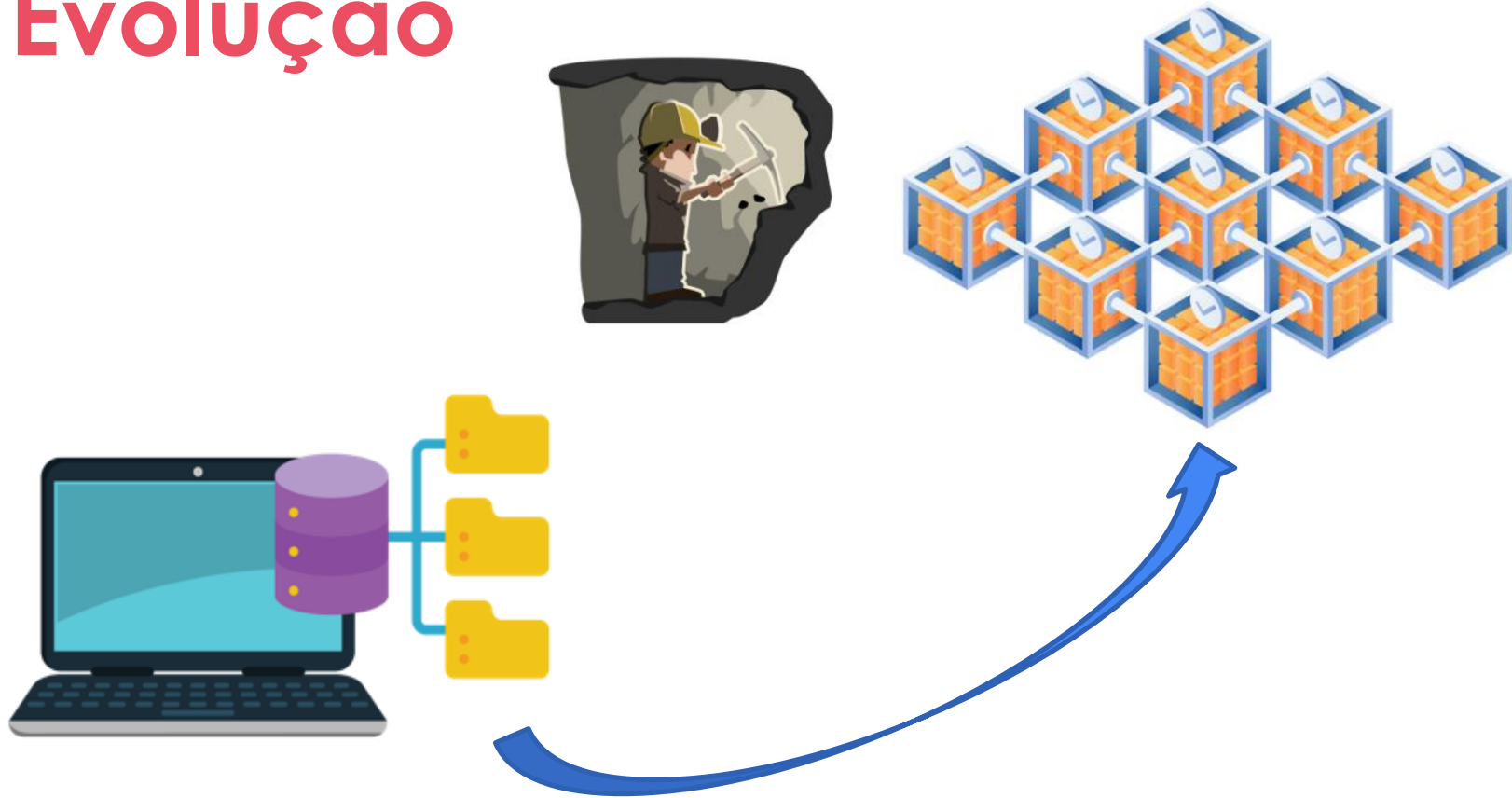
- Registros hackeados ou perdidos
- Validação de transações
- Inclusão das listas de transação
- Alteração de parâmetros das transações



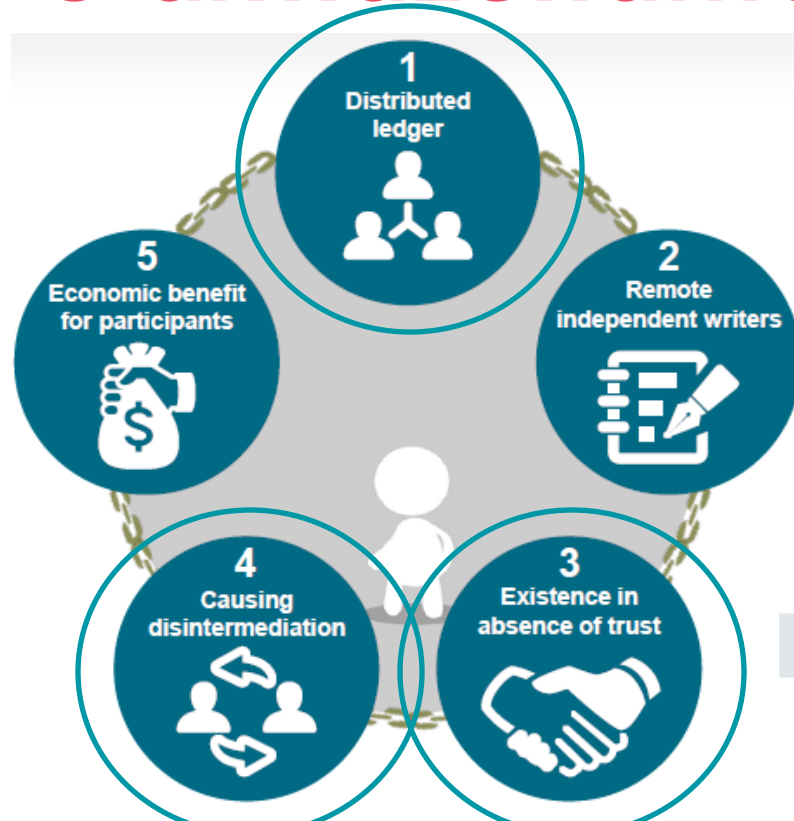
Evolução



Evolução



Difusão e armazenamento



O que é a Blockchain?

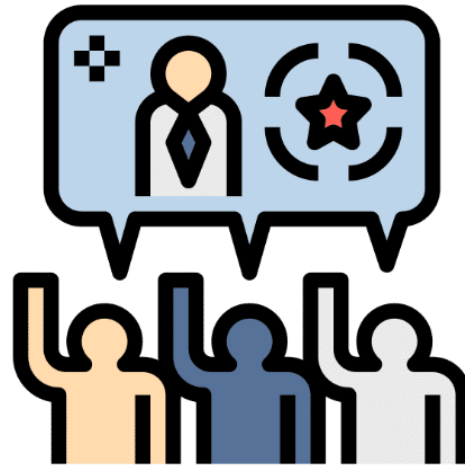
Características

- Imutabilidade
- Irrefutabilidade
- Disponibilidade
- Integridade

- Transparência
- Visibilidade
- Desintermediação
- Pseudo-anonimidade

Blockchain

- Rede mantem o registro
- Transação pública
- Validada pela rede
- Não alterável

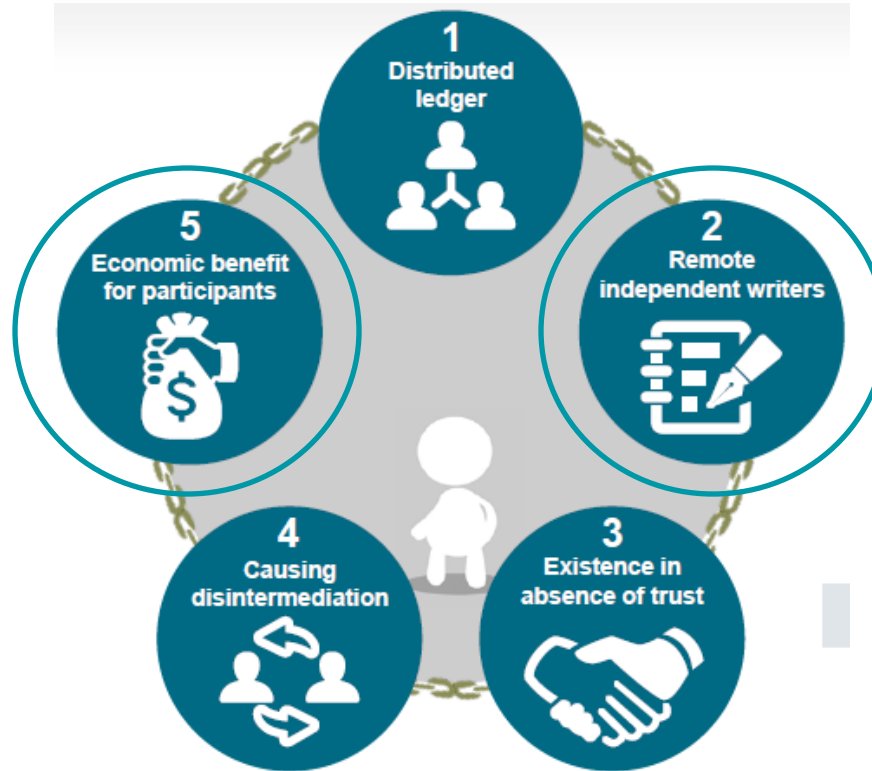


Etapa 3

Organização da Blockchain: Blocos e Transações

// Fundamentos da Blockchain

Difusão e armazenamento

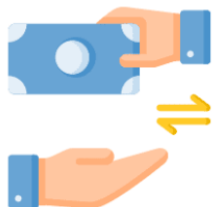


Organização da Chain

- Como os eventos são registrados?
- Qual a estrutura?
- Como garantir sua autenticidade e confiabilidade?

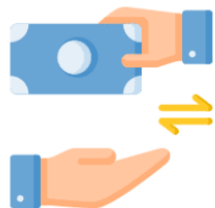
Organização da Chain

- Como os eventos são registrados?
- Qual a estrutura?
- Como garantir sua autenticidade e confiabilidade?



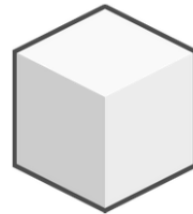
Organização da Chain

- Como os eventos são registrados?
- Qual a estrutura?
- Como garantir sua autenticidade e confiabilidade?



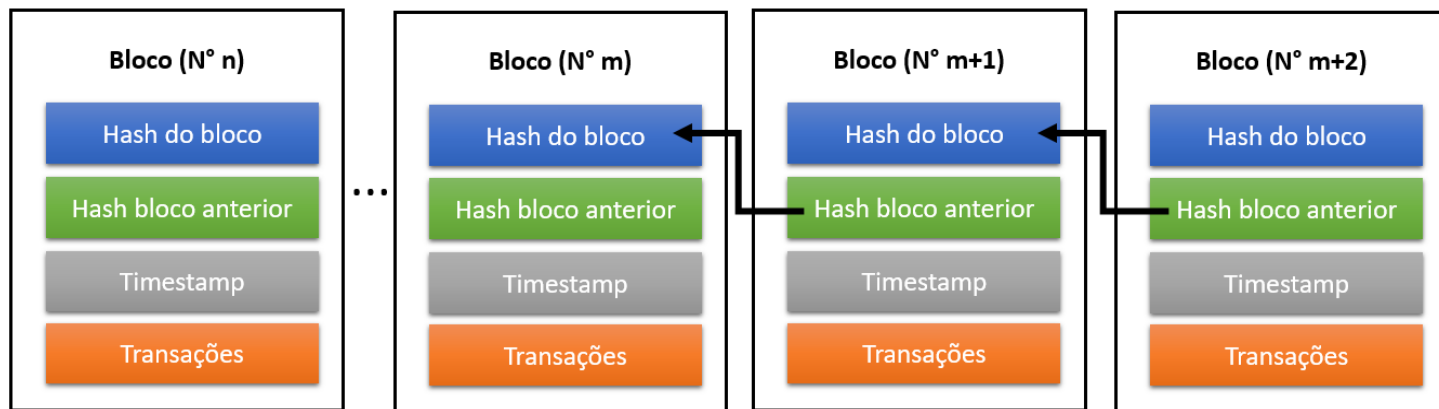
Transações

Timestamp



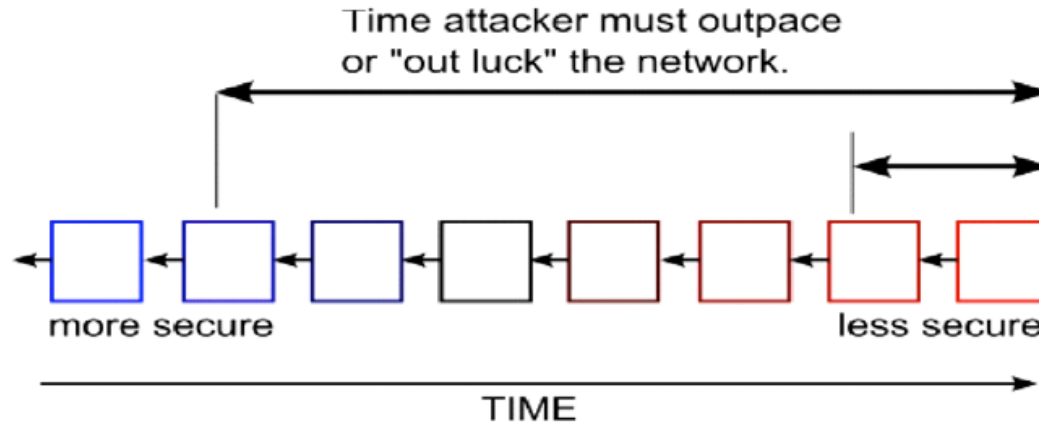
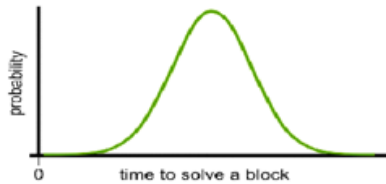
Blocos

Encadeamento dos Blocos



Tempo x Segurança

Probability Distribution of Block Solving Time

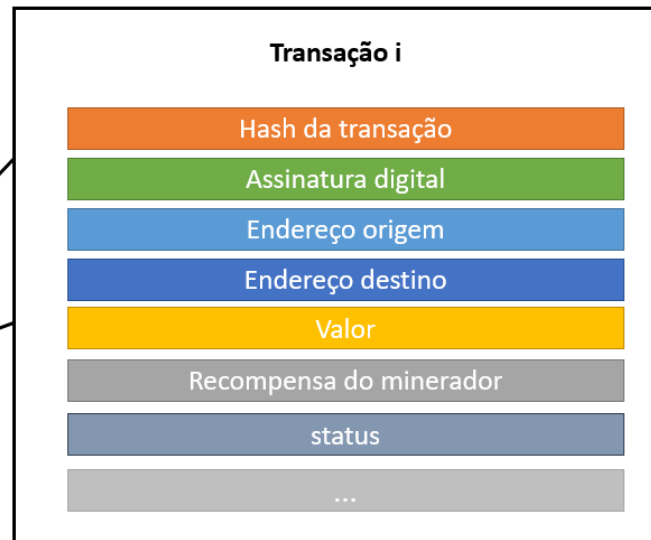
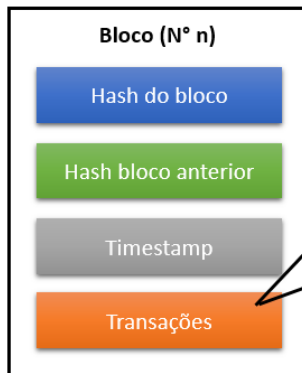


Transações

Concessão

Acordo

Ato de transigir

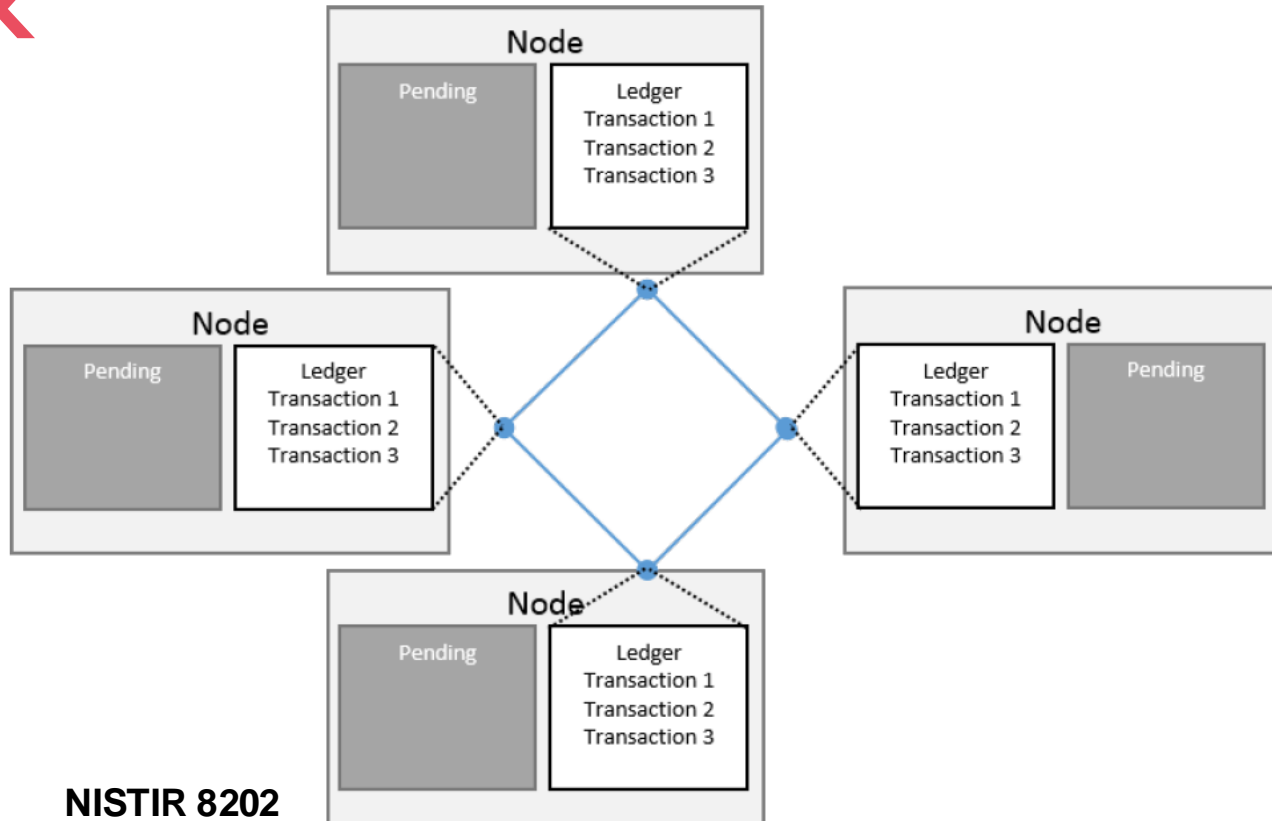


Transações

TRANSAÇÃO

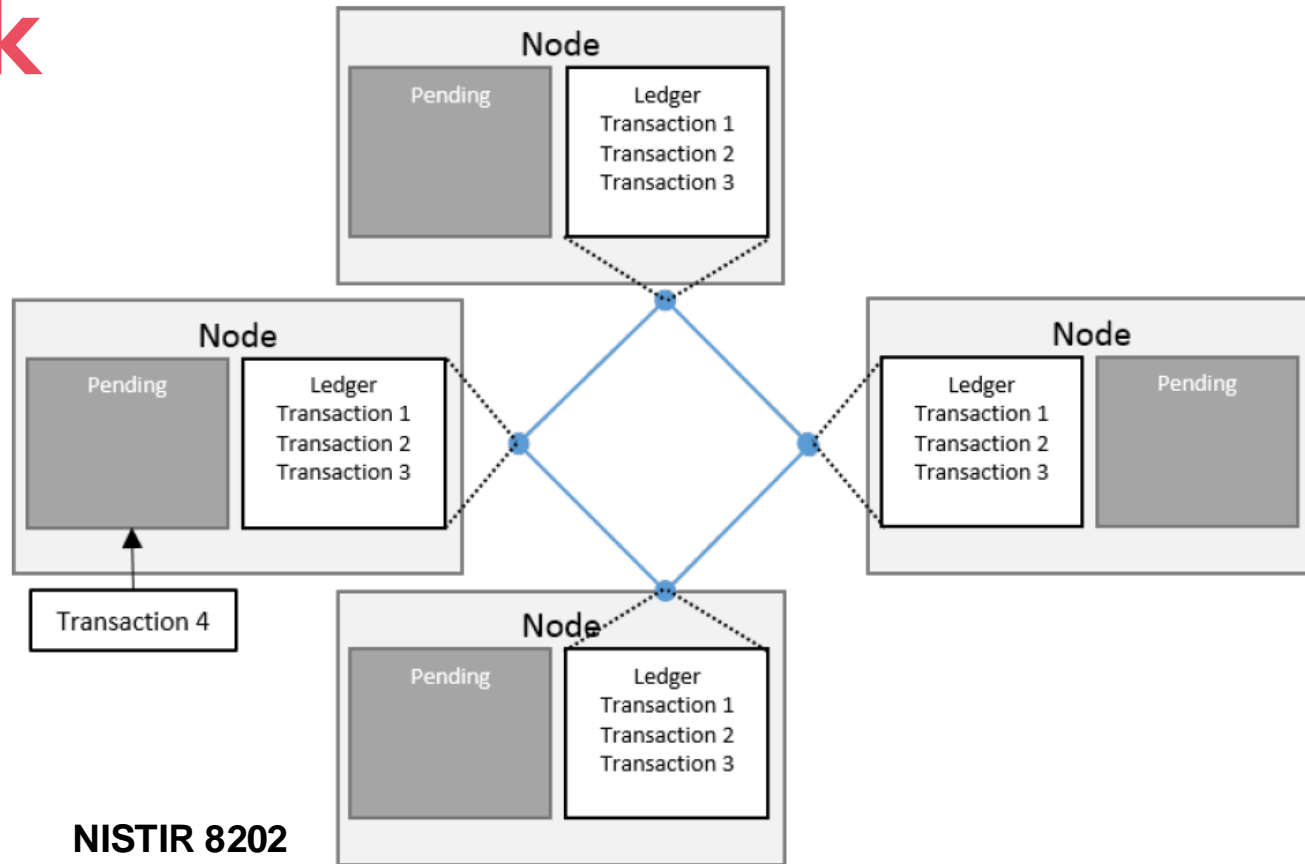
Hash da transação:	0xedb229b7bc150ac9c13bdd63545152bf2d8e78bfae1bad66e20d4b4c7f906162
Número do bloco:	8528949
Timestamp:	1568178260
Endereço de origem:	0x63c7baf43a823f766dc6de0aecdfdedbefe8613d
Endereço de destino:	0x1dd9c9b6987588028a37656e201b58220f08f732
Valor:	0.8708 Ether
...	...
Input (dados):	0x

Work



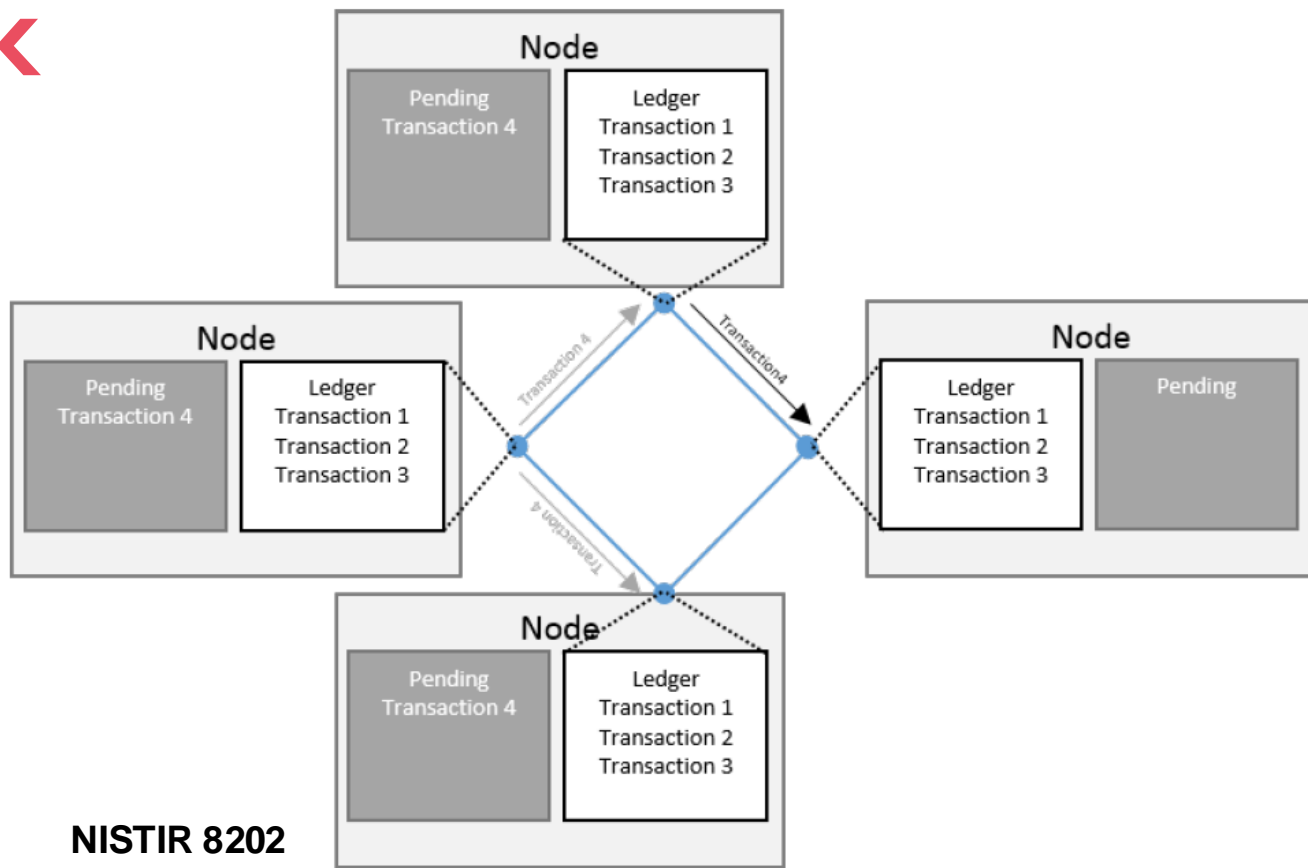
NISTIR 8202

Work



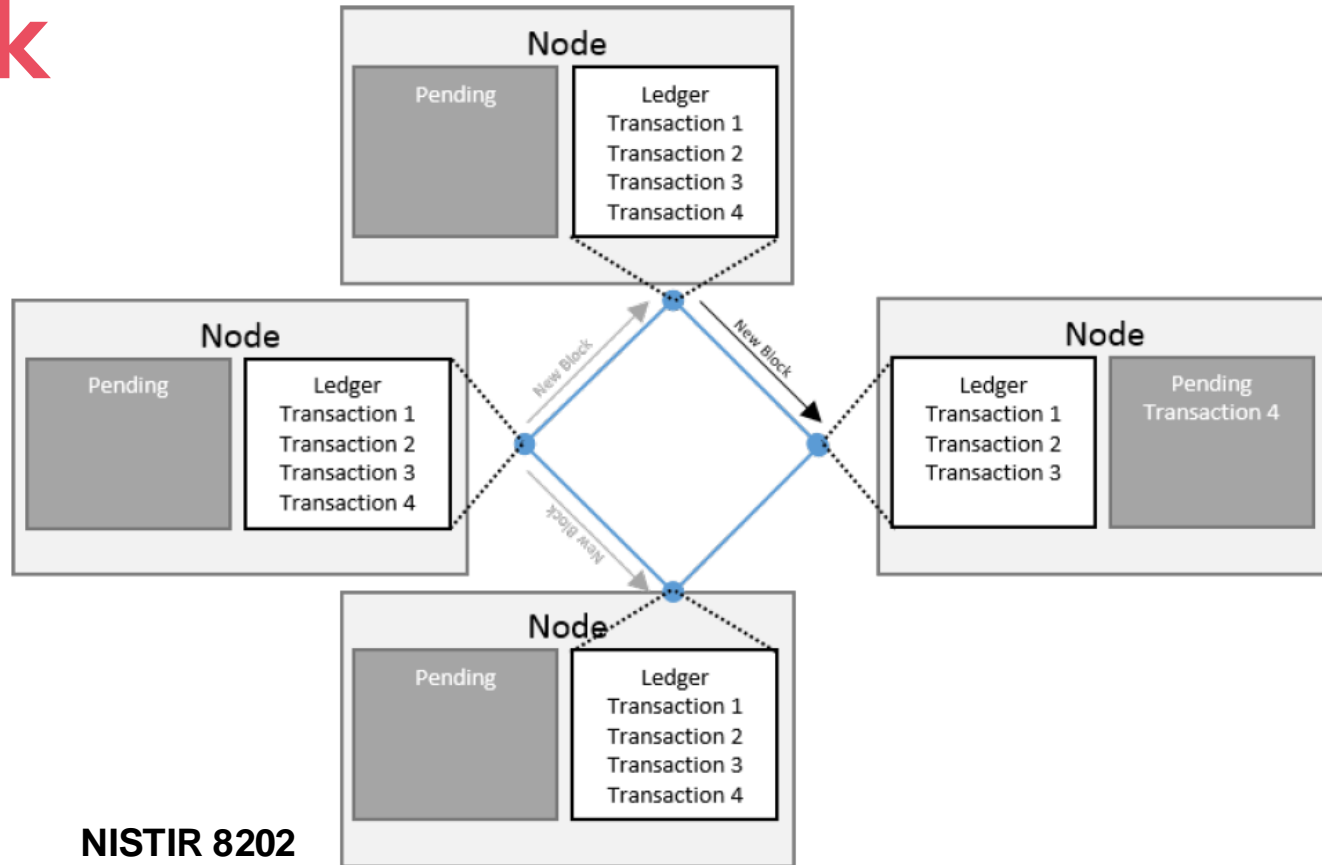
NISTIR 8202

Work



NISTIR 8202

Work



NISTIR 8202

Organização das Transações

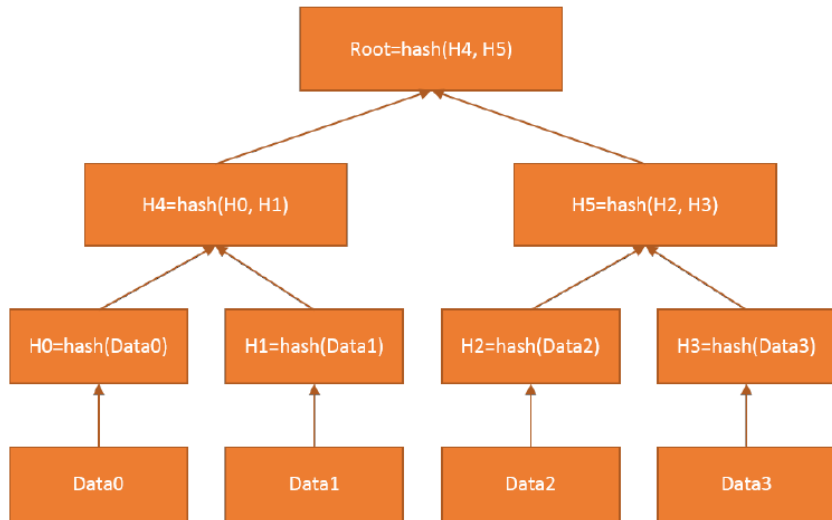
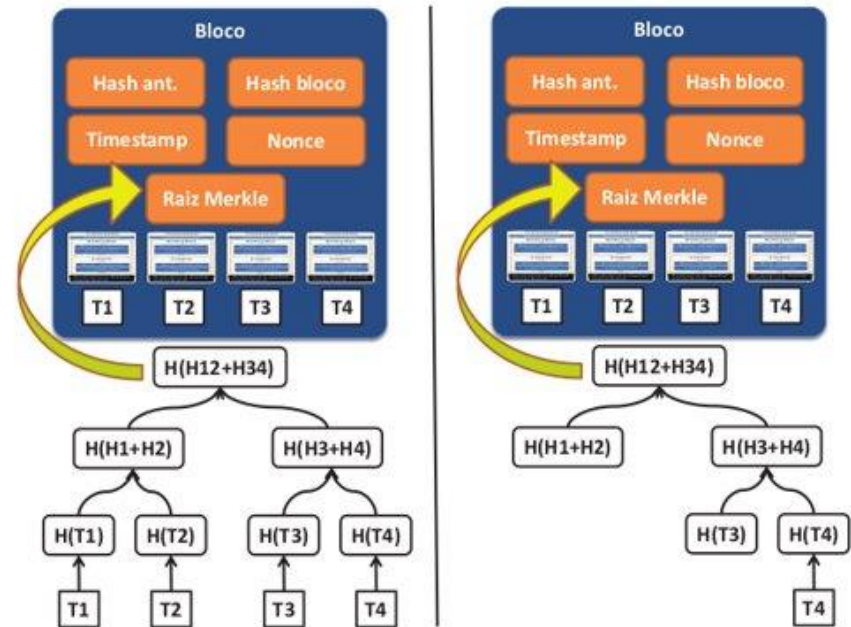
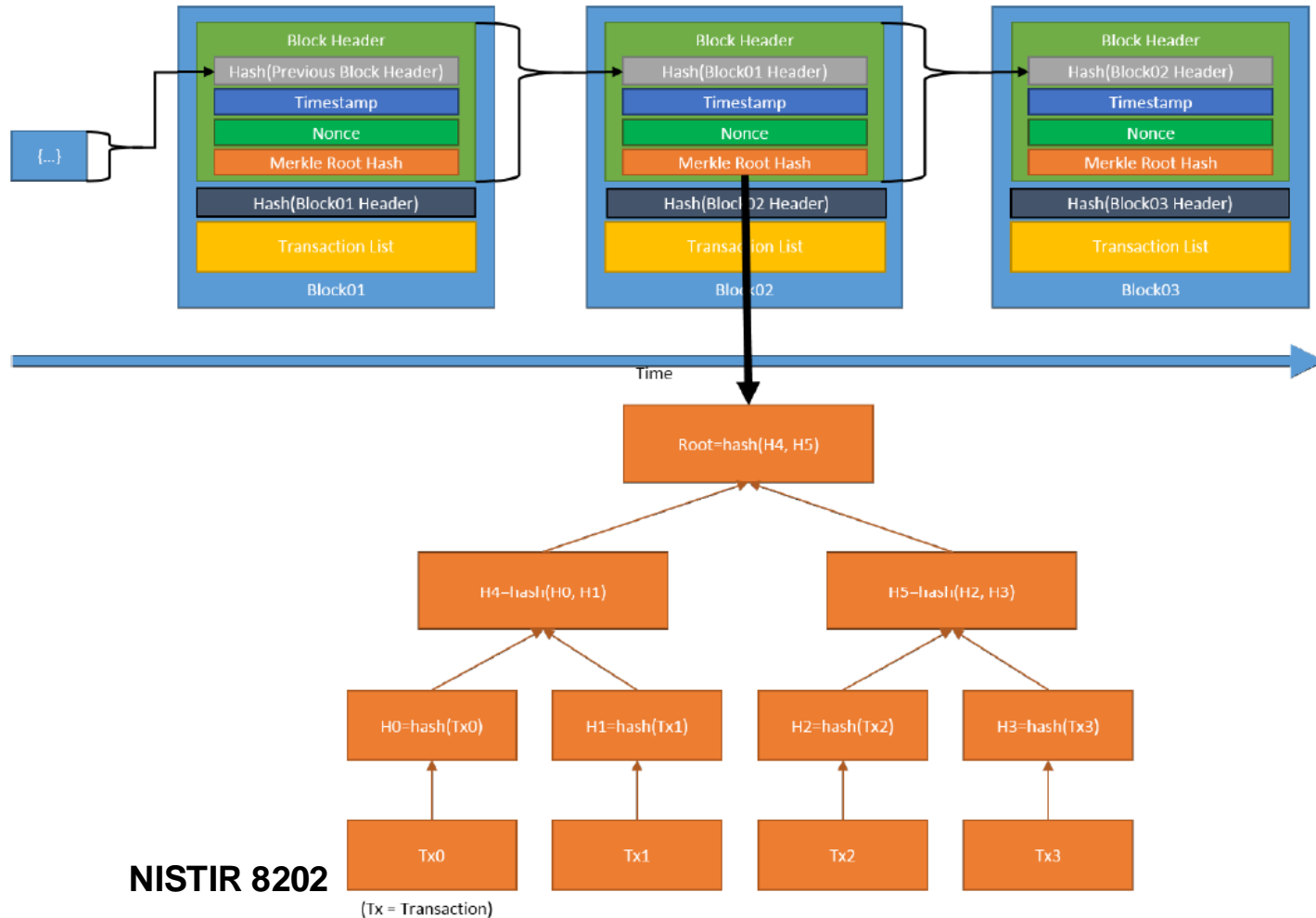


Figure 5: Example of a Merkle Tree

NISTIR 8202

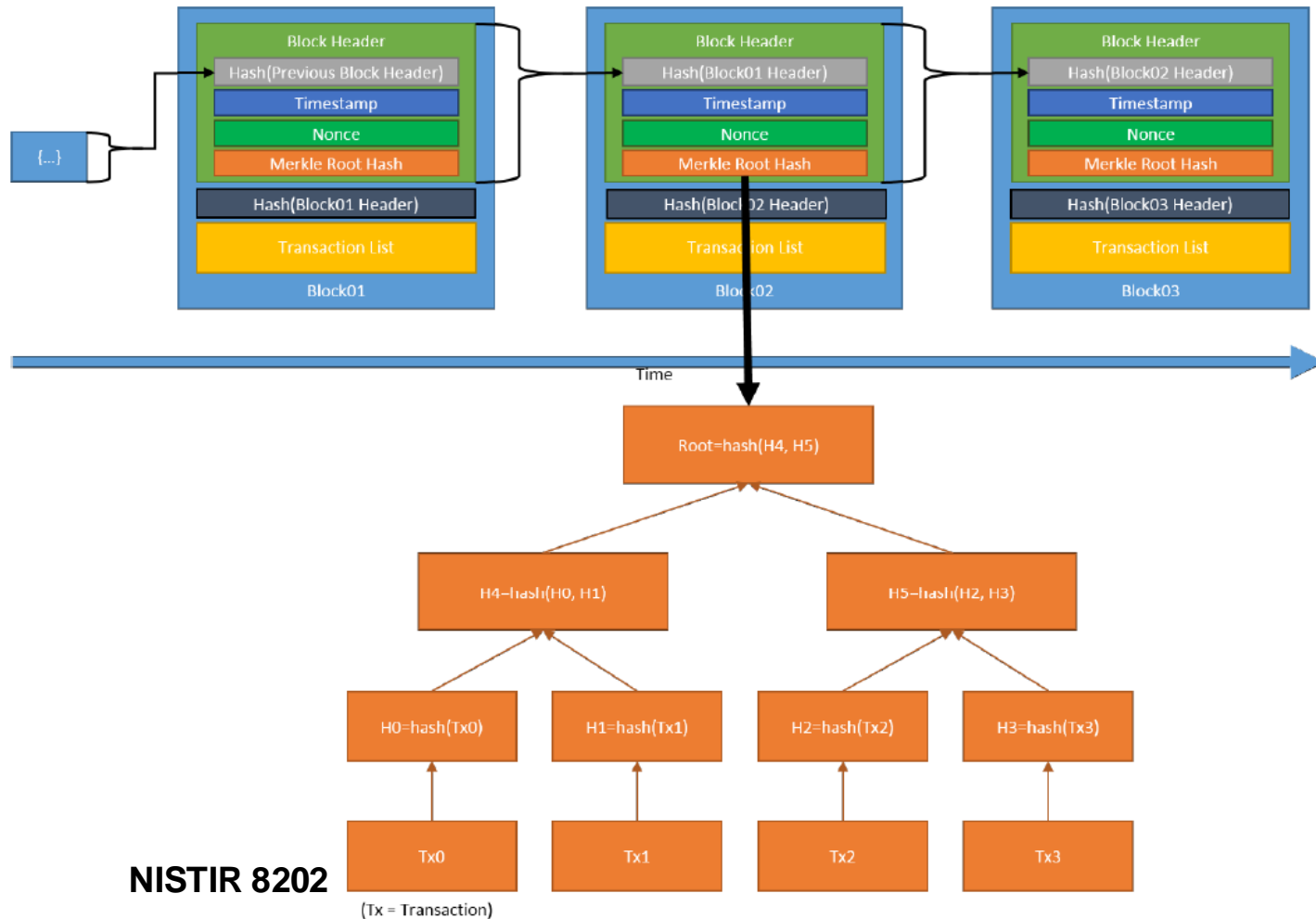




Etapa 4

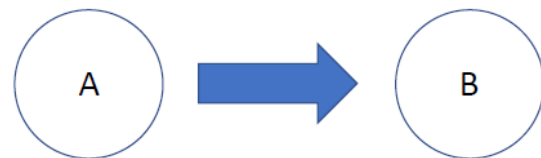
Como Garantir a origem dos eventos na Blockchain?

// Fundamentos da Blockchain

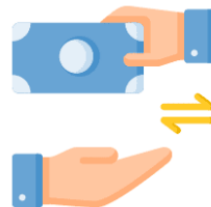


Perguntas...

- É possível roubar?
- DoS – Bloqueando a Transação?
- Como garantir o remetente?
- Um usuário pode usar o mesmo amount em transações distintas?
- Qual garantia de inserção da minha transação em um bloco?
- Como garantir que o bloco não se altere?
- Por que não posso modificar a Blockchain?



Transações

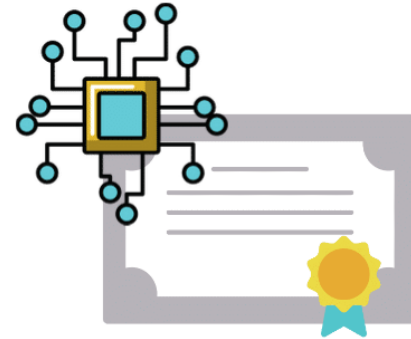
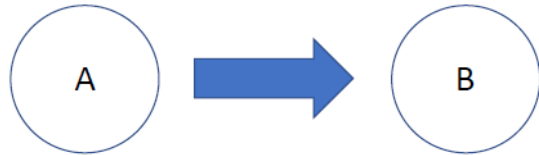


Autenticidade

Sigend by : assinatura digital

Pkb: chave pública de B

$H()$: hash da transação



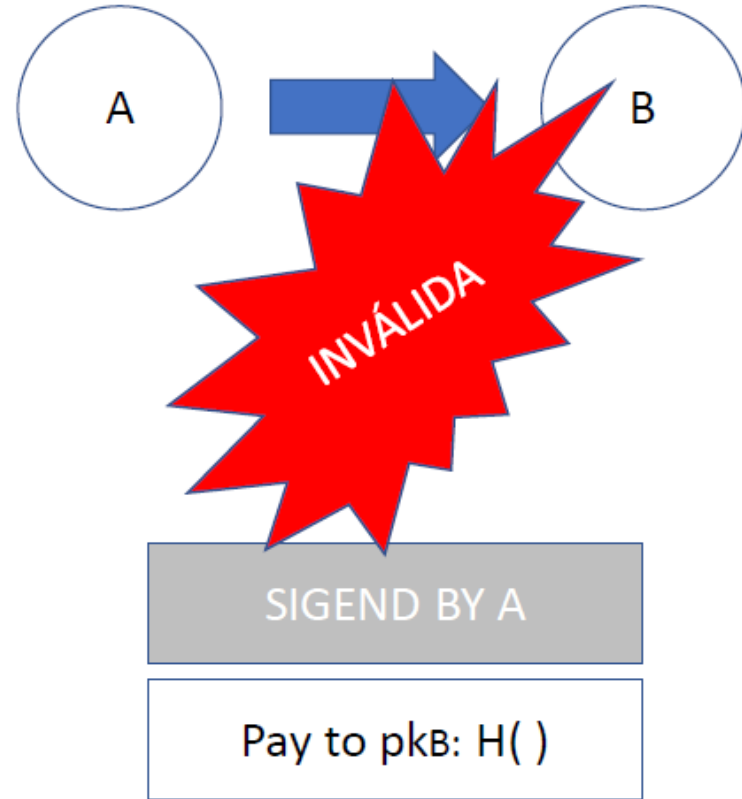
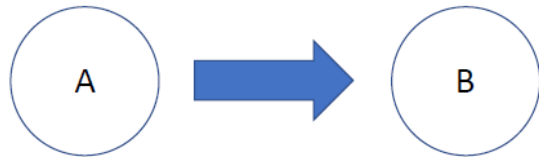
SIGEND BY A

Pay to pkb: $H()$

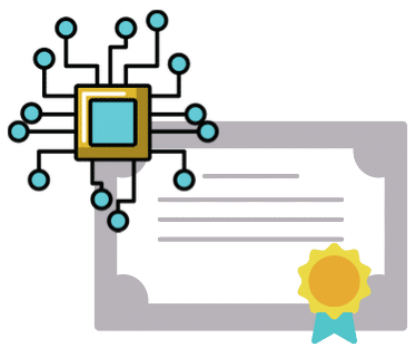
Autenticidade

Cenários

- Falha na autenticação
- Double spending
(Resolvido pelo Bitcoin)



Autenticidade



SIGEND BY A

Pay to pkB: $H()$

BLOCO SERÁ INSERIDO
NO BLOCKCHAIN

Nº BLOCO

ENDEREÇO TX1

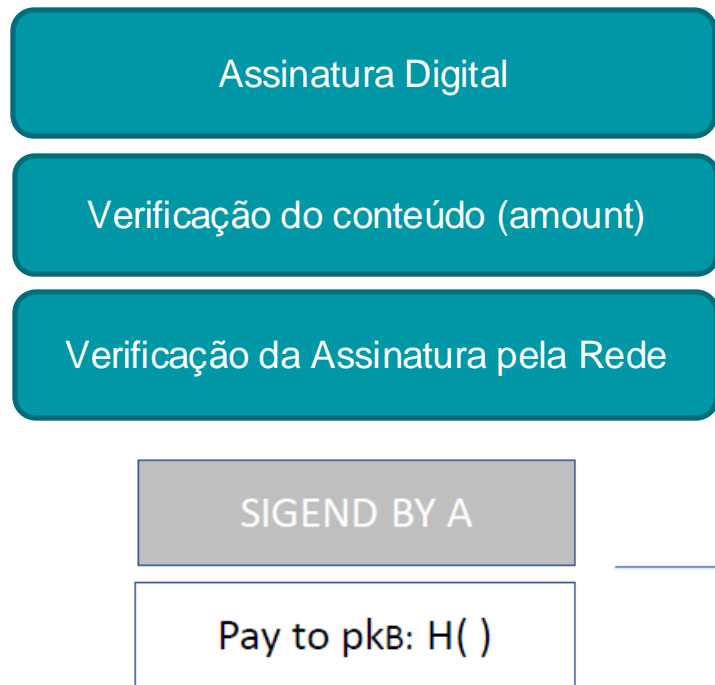
ENDEREÇO TX

ENDEREÇO TX2

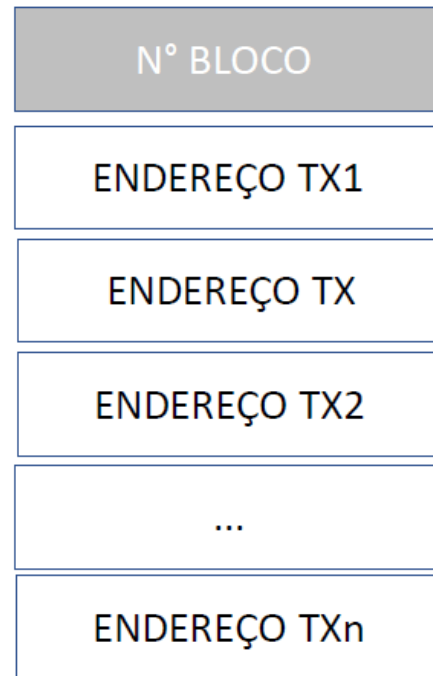
...

ENDEREÇO TXn

Autenticidade

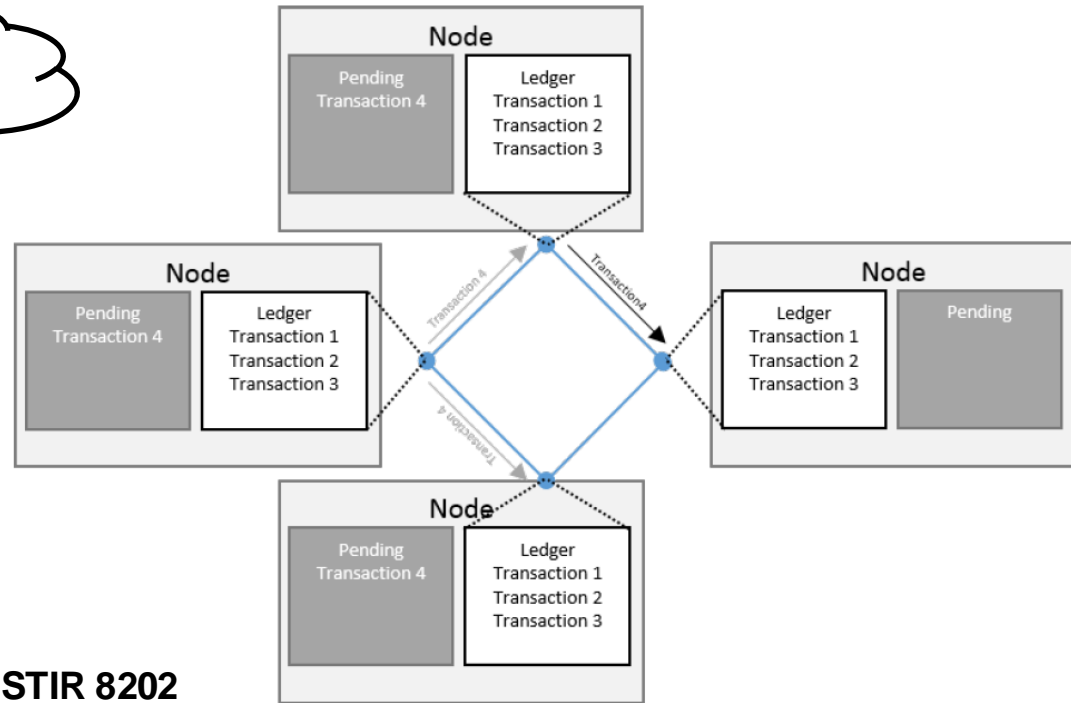


BLOCO SERÁ INSERIDO
NO BLOCKCHAIN



Consenso

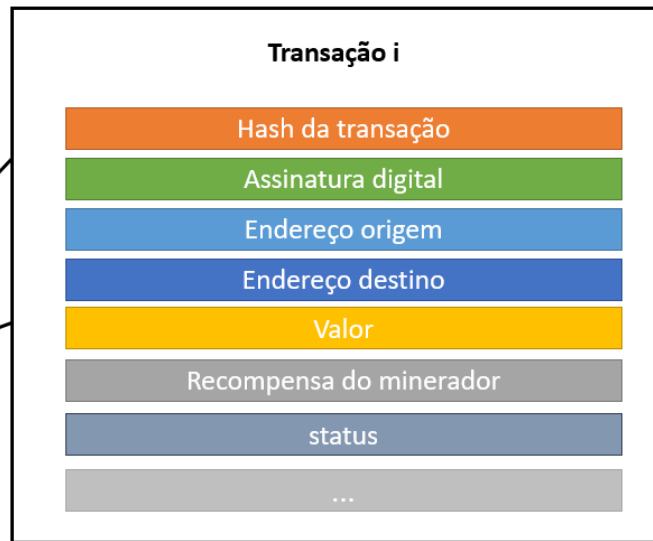
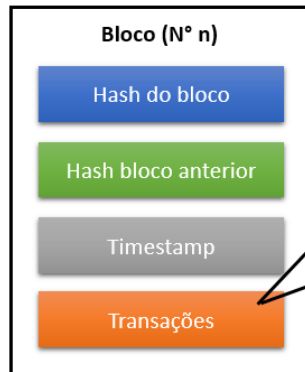
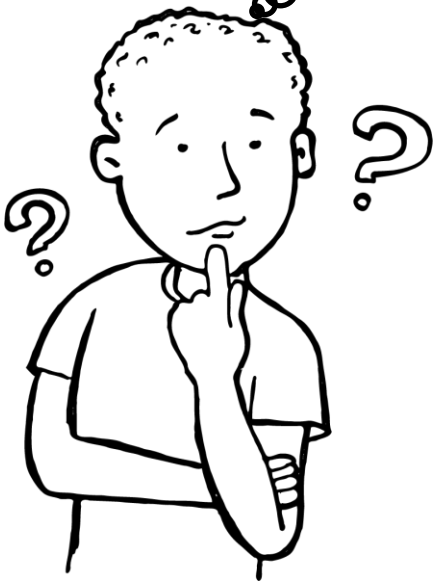
As transações



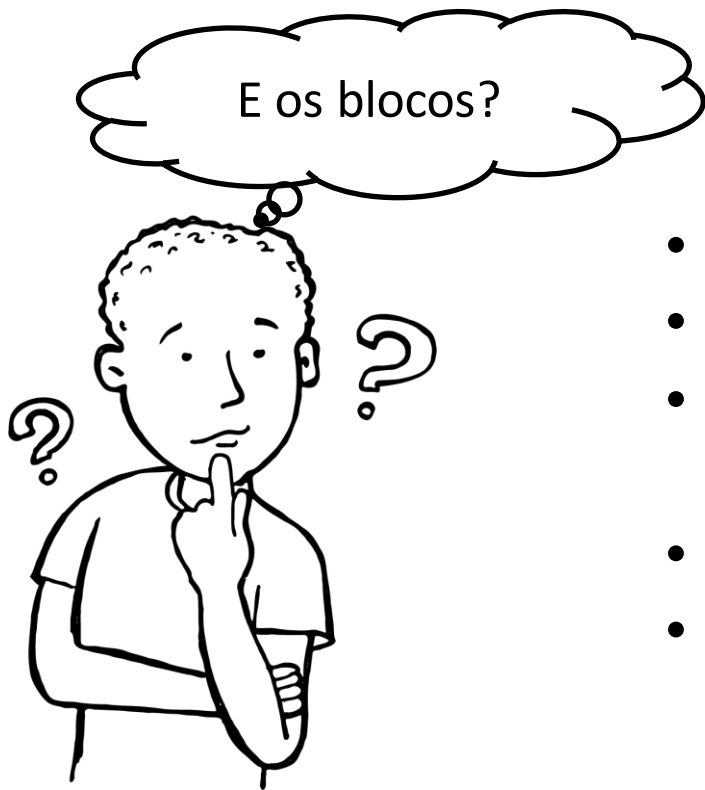
NISTIR 8202

Consenso

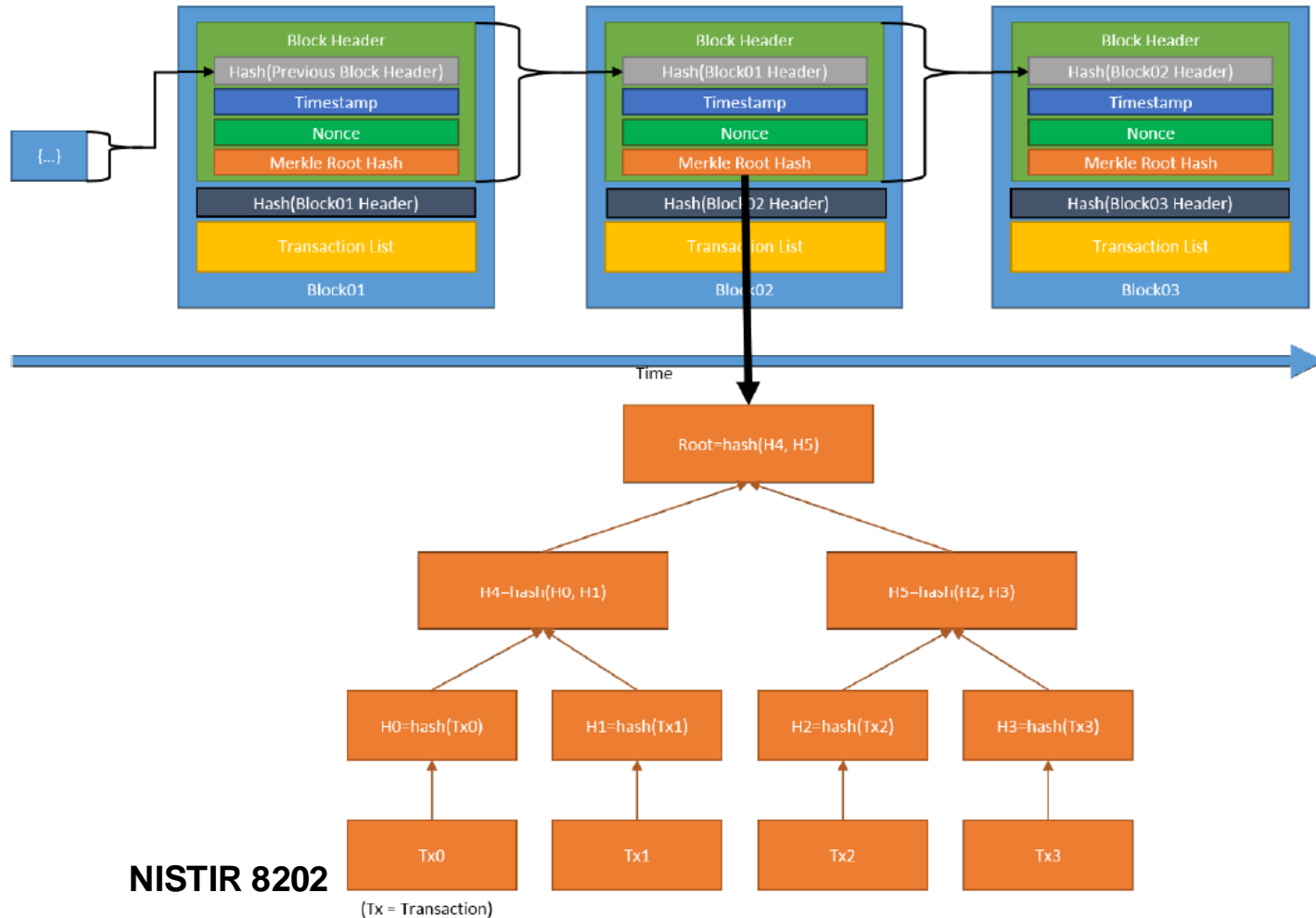
Agrupamento



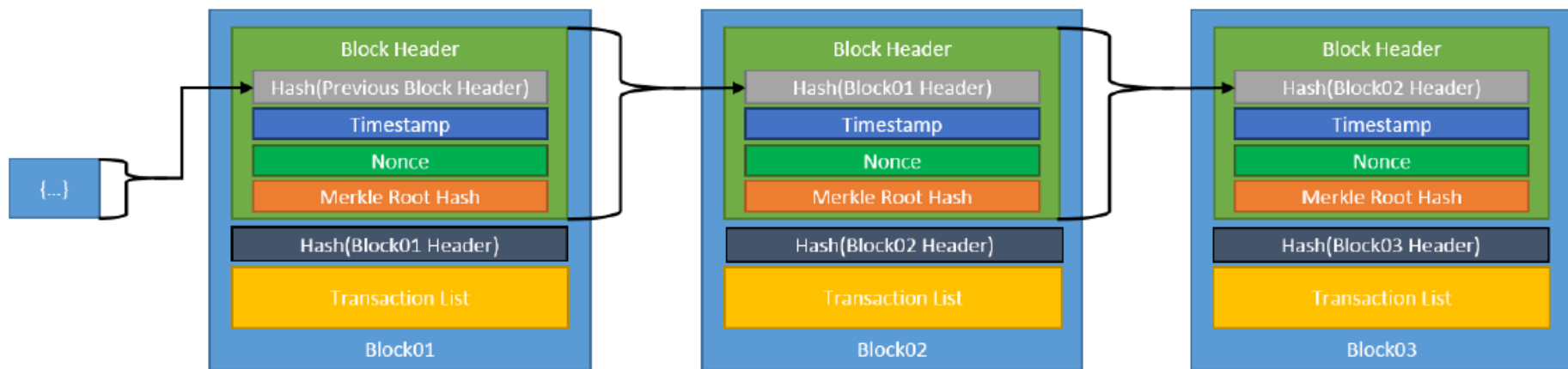
Consenso



- Nós mineradores
- Criptografia por Hash 256 bits
- Desafio Criptográfico
- Mecanismos de consenso
- Incentivos



Encadeamento de Blocos



Consenso



- As transações podem não ser incluídas em um bloco?
- Mais de um bloco pode ser validado com mesmo timestamp?
- Como resolver?

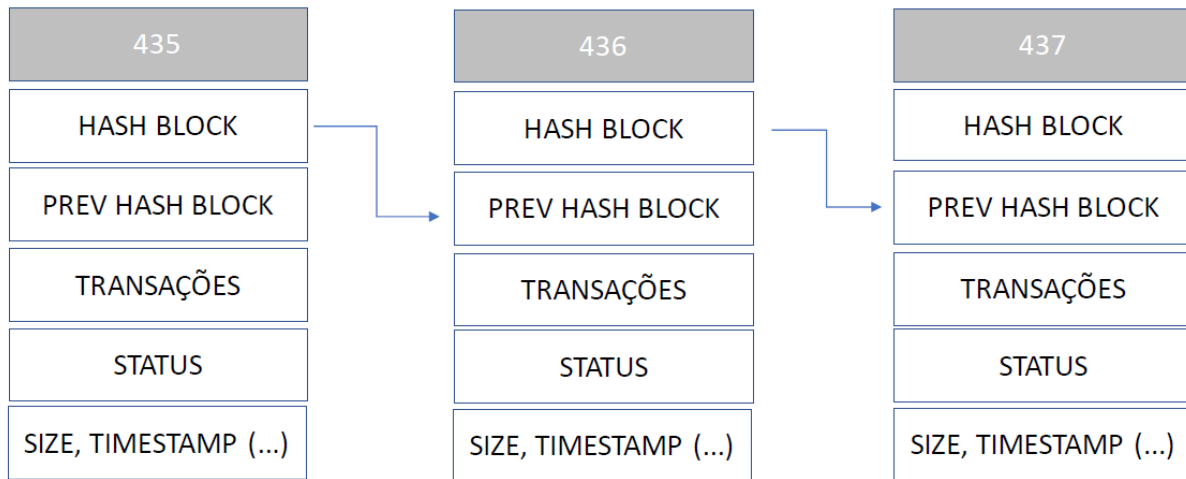
Etapa 4

Inserção de Blocos e Bifurcações

// Fundamentos da Blockchain

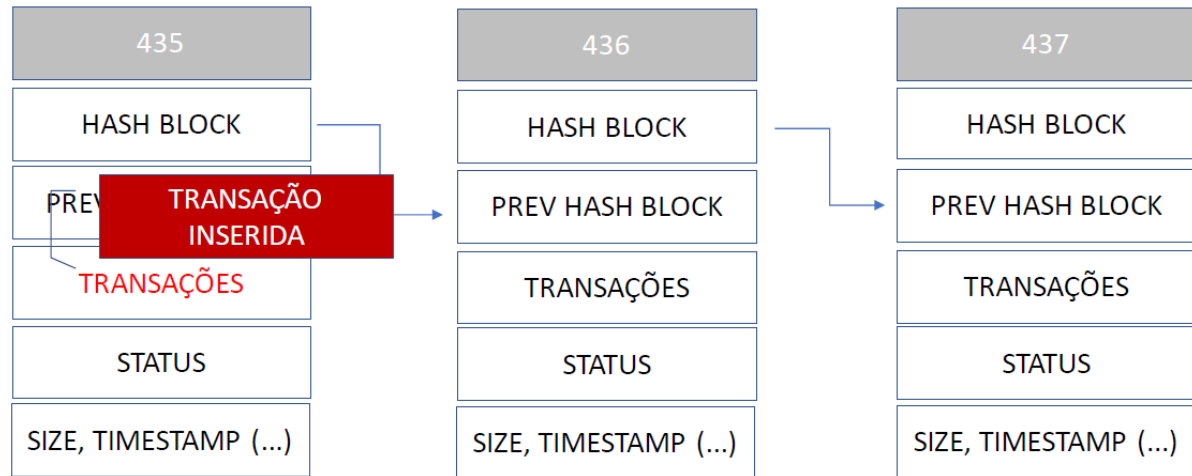
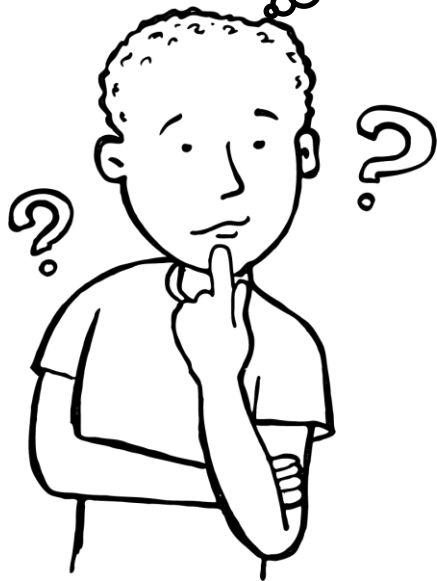
Bifurcação

Por que acontece os forks?



Bifurcação

Por que acontece os forks?

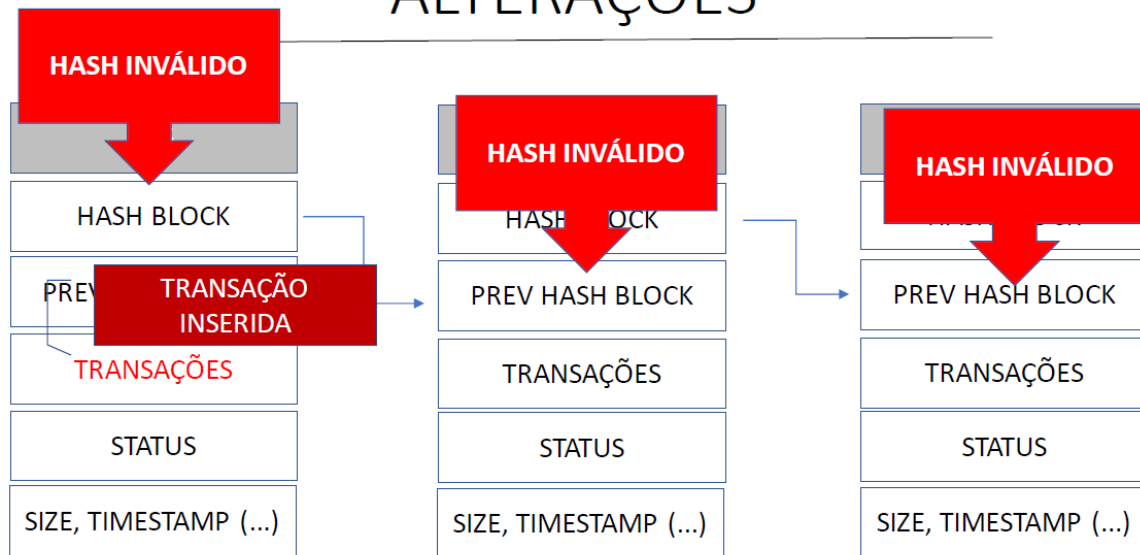


Bifurcação

Por que acontece os forks?

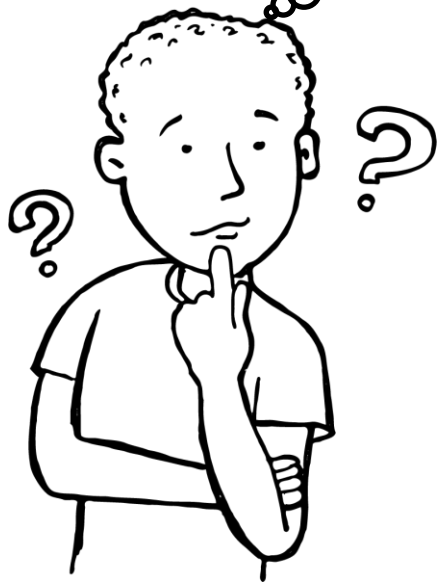


ALTERAÇÕES

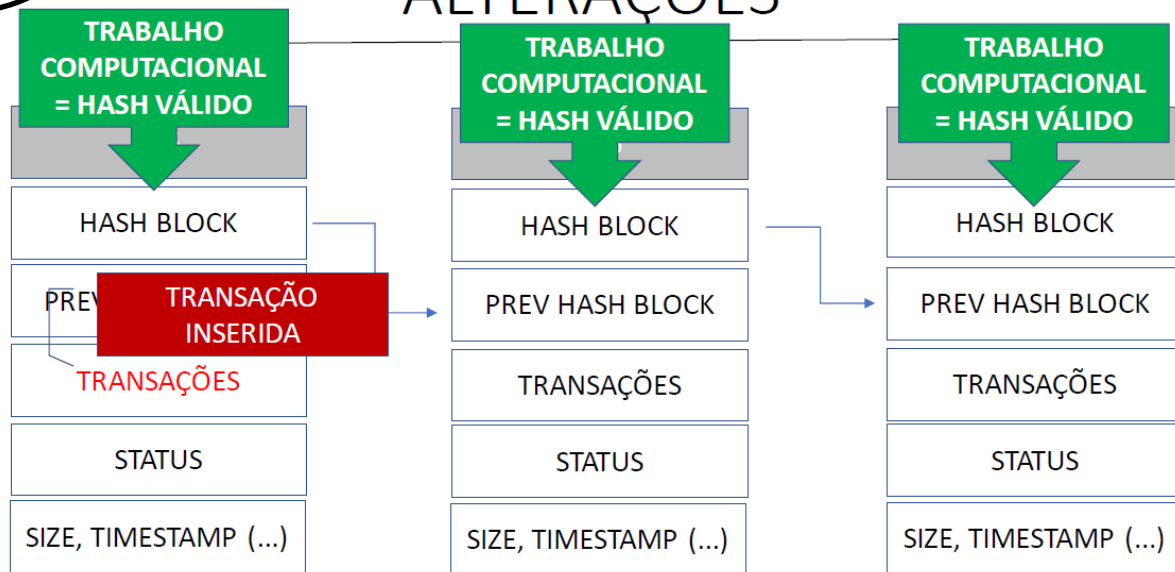


Bifurcação

Por que acontece os forks?



ALTERAÇÕES

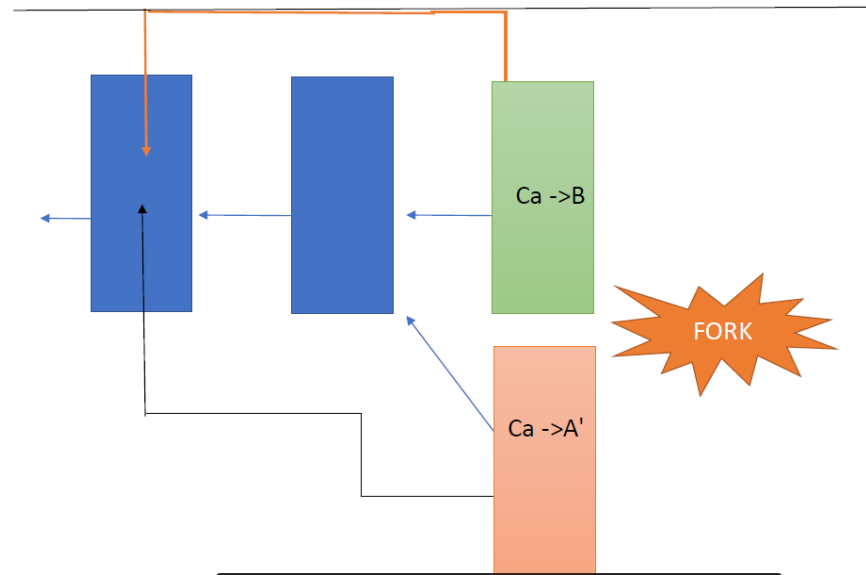


Bifurcação

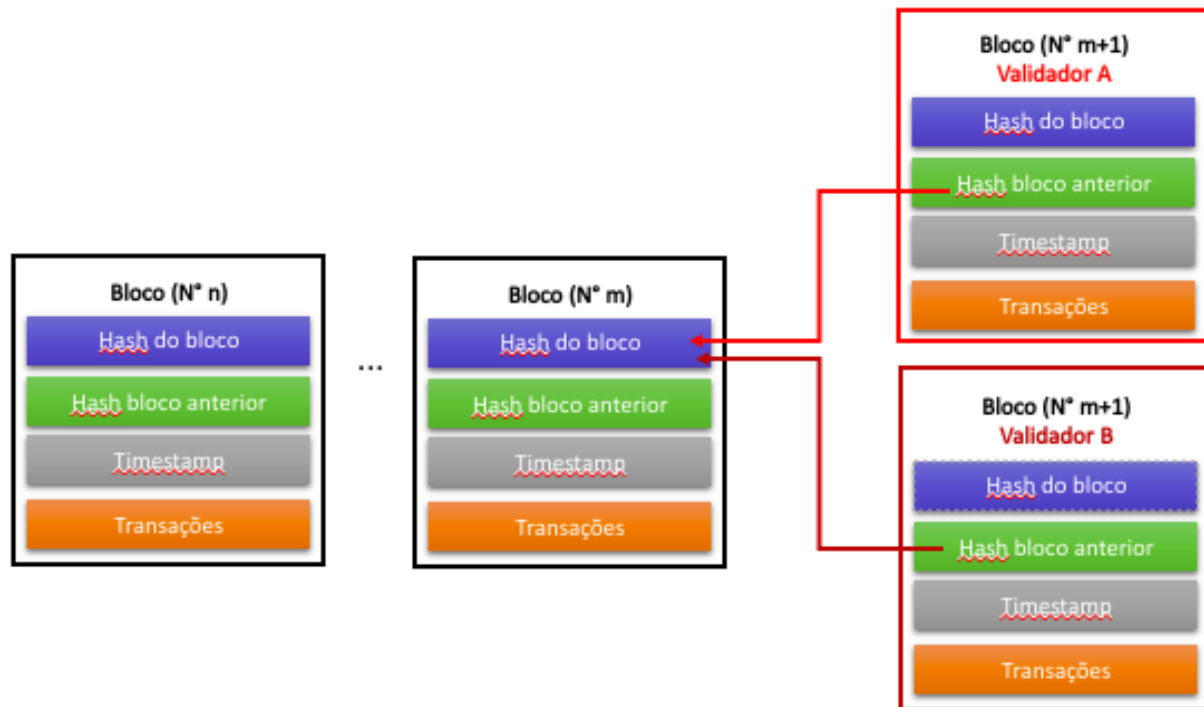


- As transações podem não ser incluídas em um bloco?
- **Mais de um bloco pode ser validado com mesmo timestamp?**
- **Como resolver?**

Mais de um Bloco?



Mais de um bloco?



Consenso

Dúvidas?



ESCUTANDO AS MENSAGENS

Lista de Blocos 1

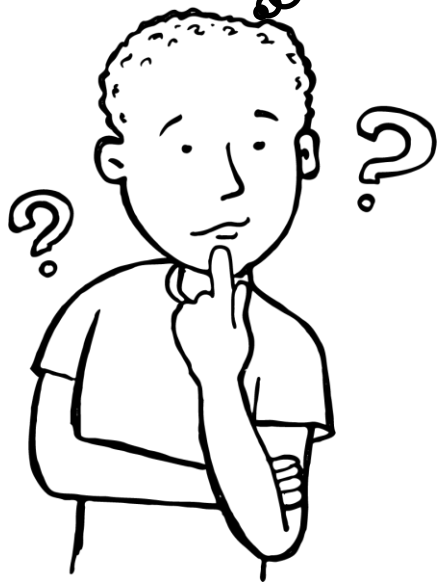


Lista de Blocos 2



Consenso

Dúvidas?



QUAL A LISTA CORRETA?

Lista de Blocos 1



Lista de Blocos 2



Consenso

Dúvidas?



Lista de Blocos 2

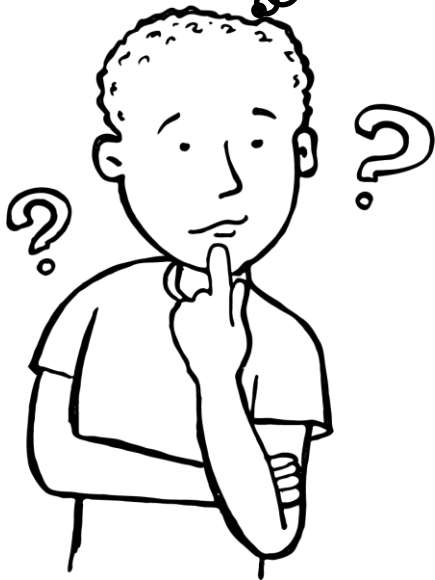


Lista de Blocos 1



Consenso

Dúvidas?



Lista de Blocos 2



Lista de Blocos 1



Consenso

Dúvidas?



Lista de Blocos 2



Lista de Blocos 1



Consenso

Dúvidas?



Lista de Blocos 2

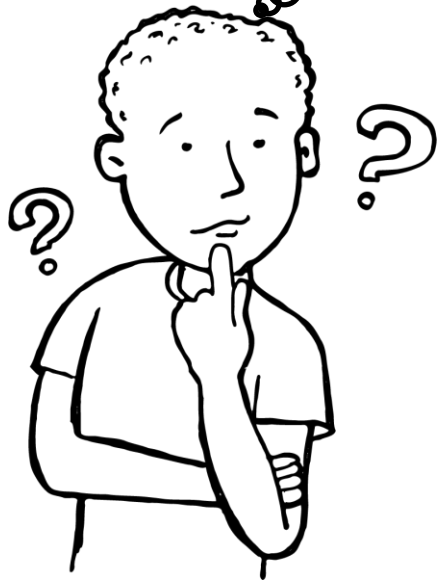


Lista de Blocos 1



Consenso

Dúvidas?



Lista de Blocos 2



Lista de Blocos 1

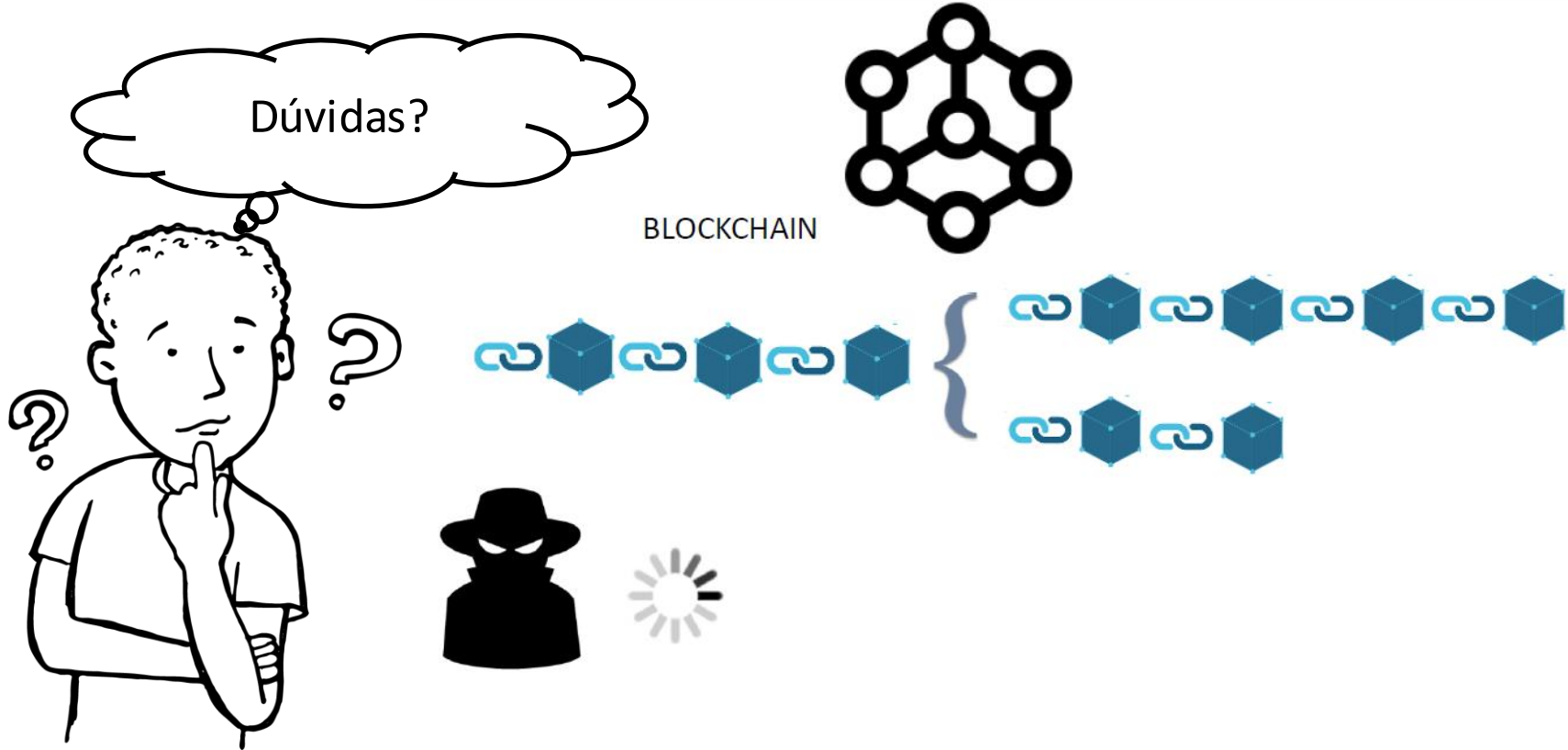


Consenso

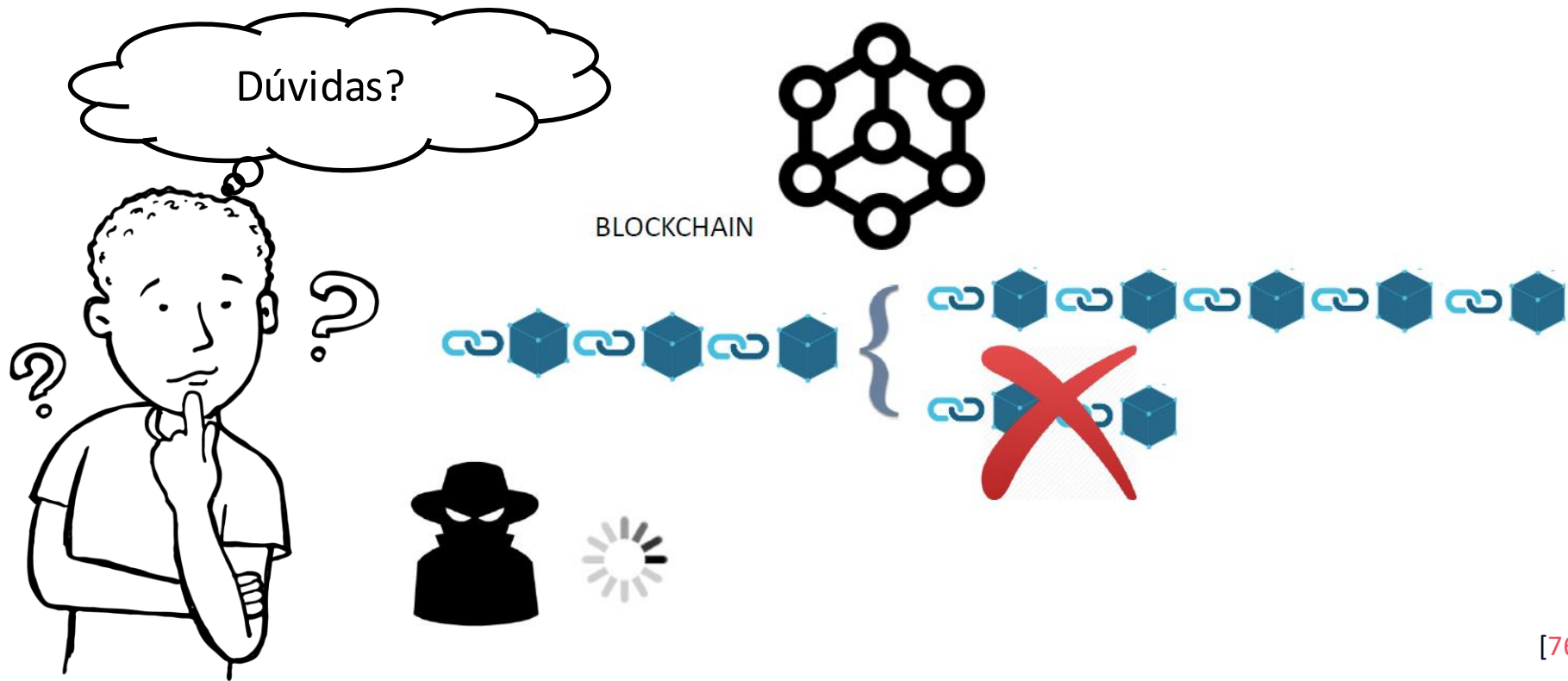


O maior bloco é o que será
considerado válido!

Consenso



Consenso

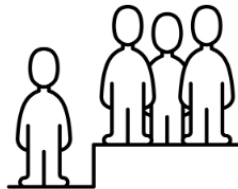


Modificações estruturais

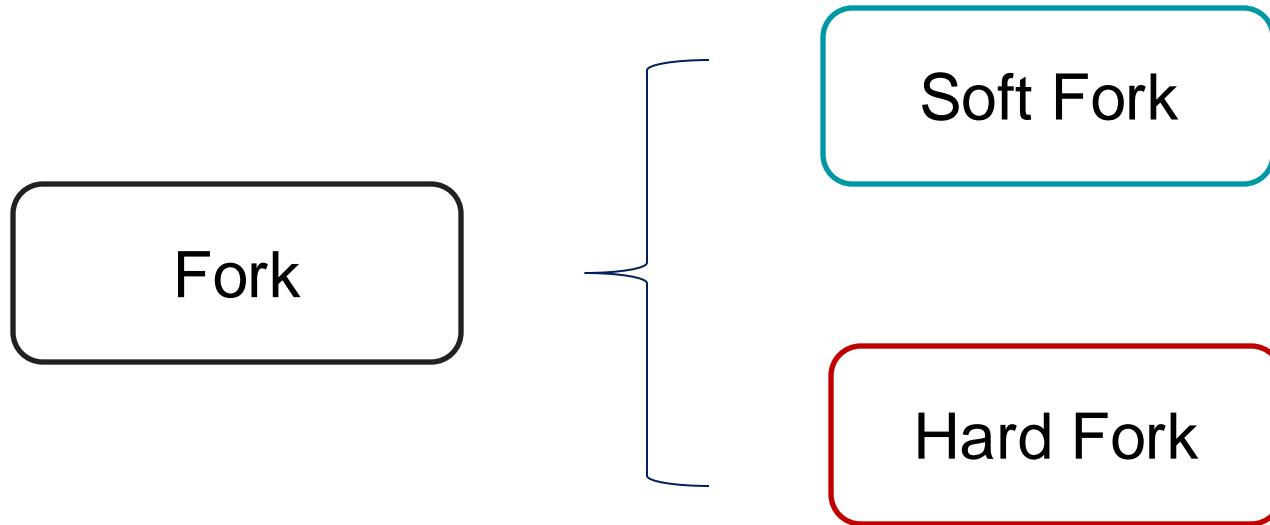
- Atualizações de softwares e plataformas

Como ocorre na blockchain?

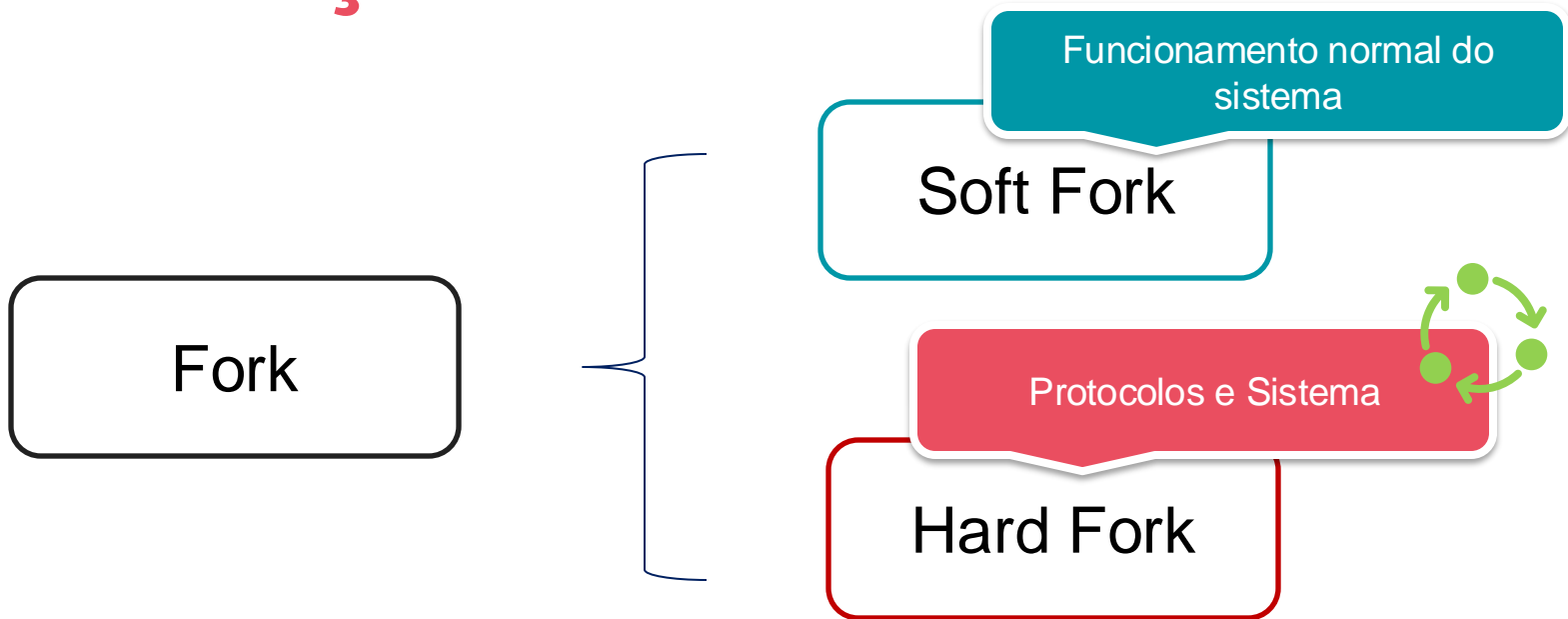
- Consenso
- Atualização do sistema



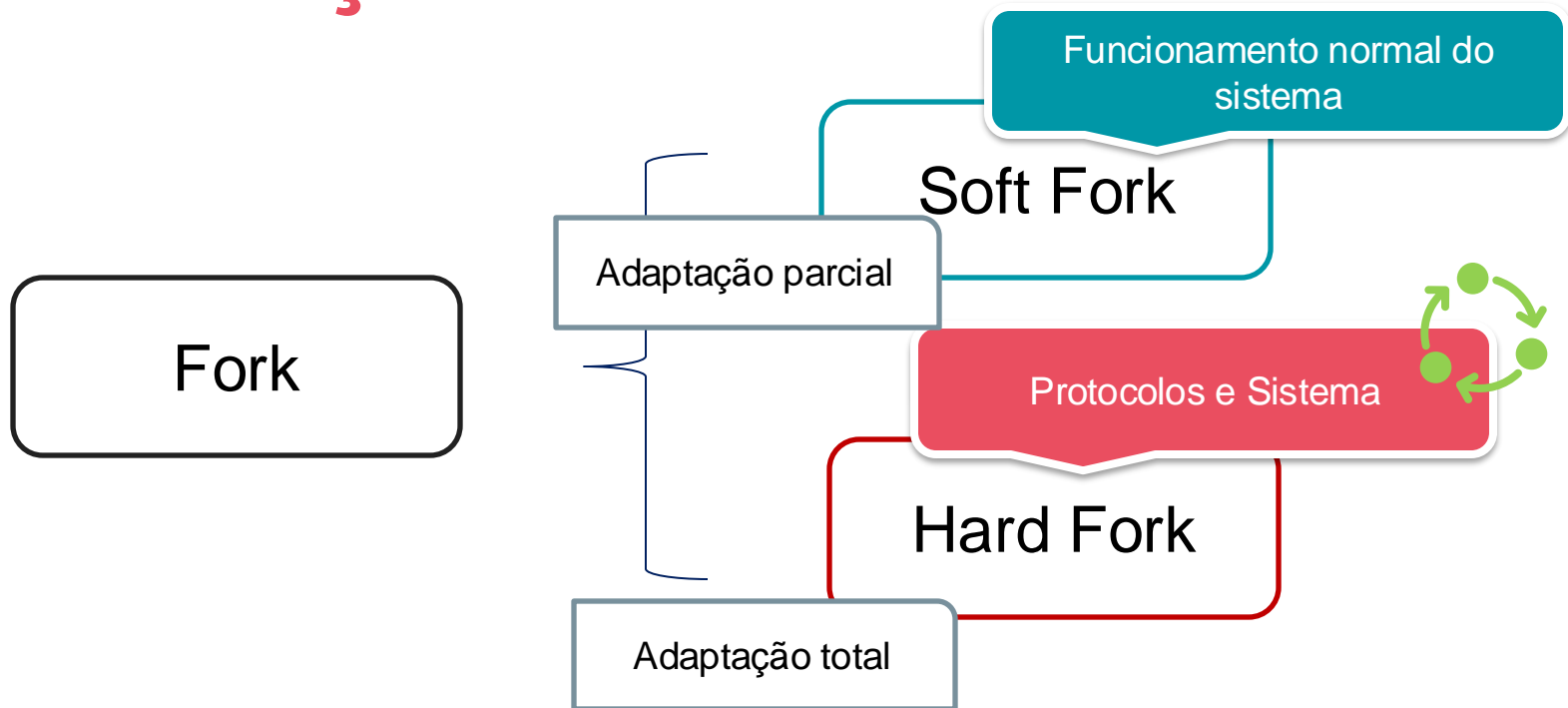
Modificações estruturais



Modificações estruturais



Modificações estruturais



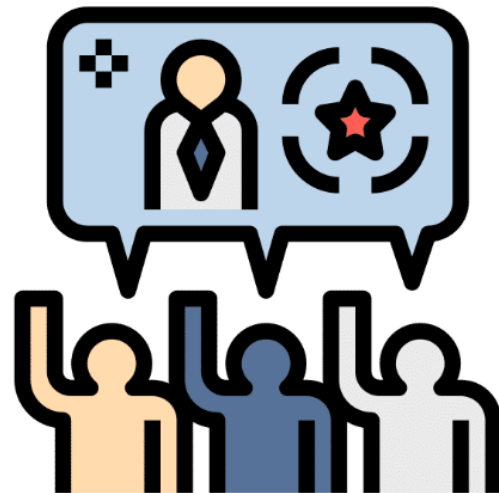
Etapa 5

Mecanismos de Consenso - Blockchain

// Fundamentos da Blockchain

Consenso

- Como os blocos são incluídos na Blockchain?
- Qualquer um pode fazer atualização da sua cópia da chain?



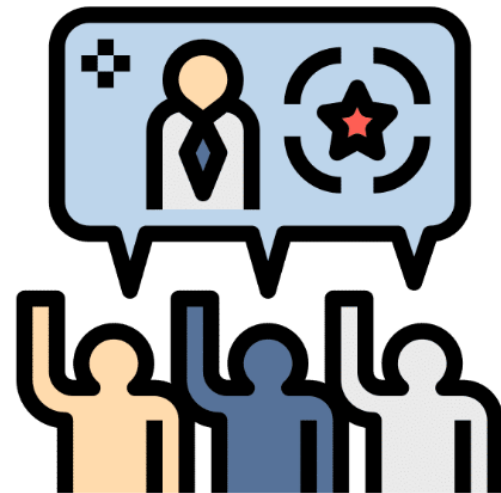
Consenso

- Como os blocos são incluídos na Blockchain?

Hash dos blocos

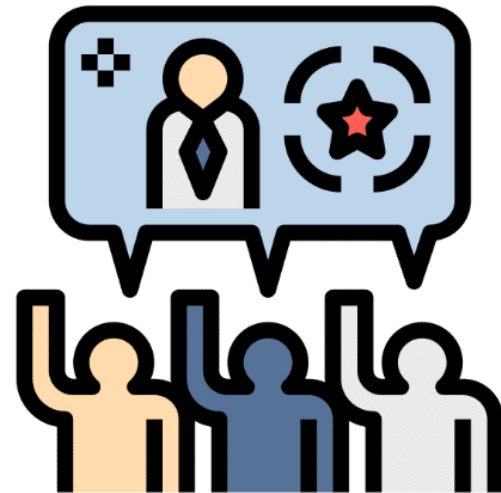
Trabalho
computacional

Consenso da Rede



Consenso

- Conceito de Sistemas ditribuídos
- Manutenção do estado
- Consistência de informações
- Problema: generais bizantinos



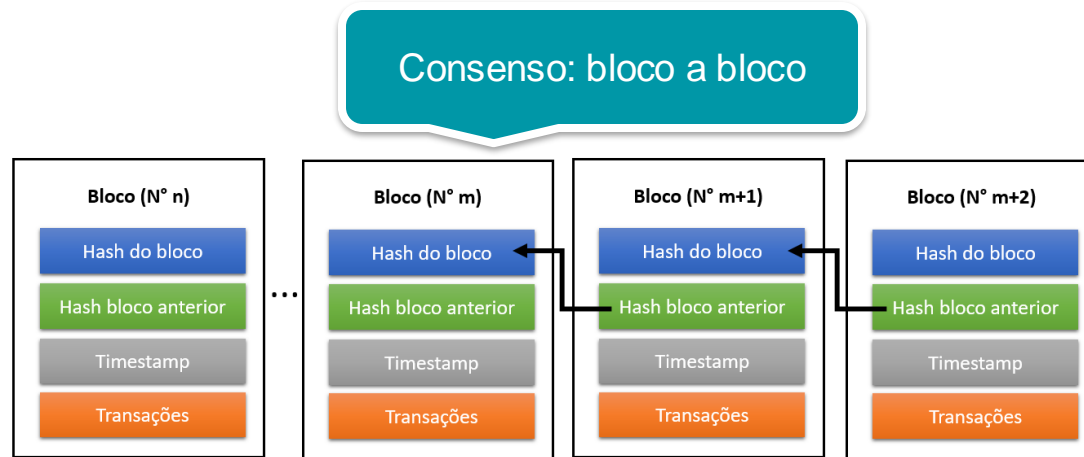
Mecanismos de consenso

Algoritmo de consenso

- Diretrizes e regras
- Recursos utilizados

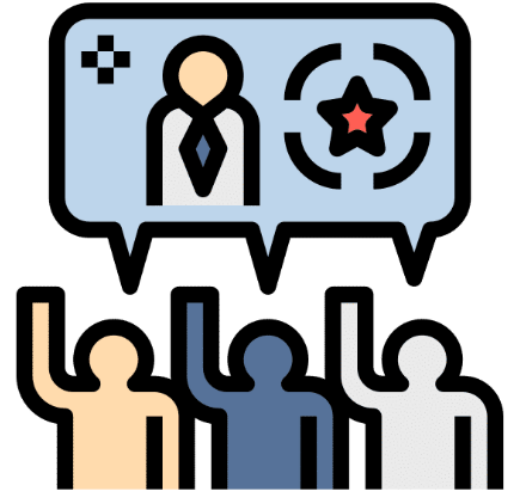


Mecanismos de consenso



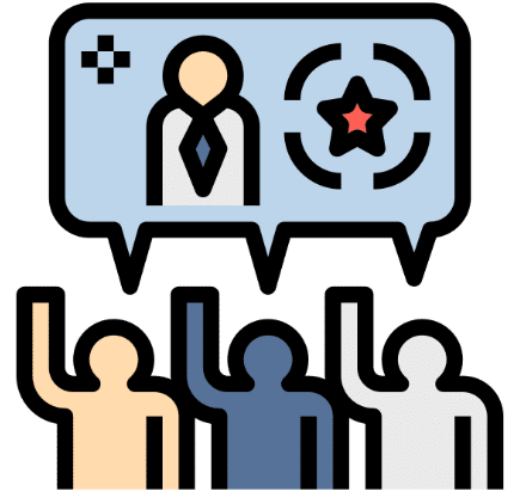
Algoritmos existentes

- Practical byzantine fault tolerance (BPFT)
- Proof of Work (PoW)
- Proof of Stake (PoS)
- Leased Proof of Stake (LPoS)
- Proof of Capacity (PoC)



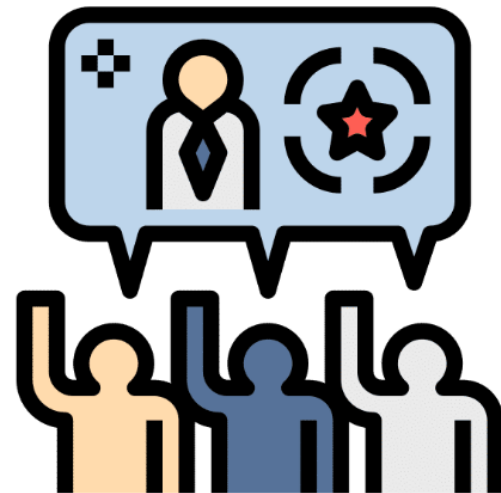
Algoritmos existentes

- Practical byzantine fault tolerance (BPFT)
- **Proof of Work (PoW)**
- **Proof of Stake (PoS)**
- Leased Proof of Stake (LPoS)
- Proof of Capacity (PoC)



Algoritmos existentes

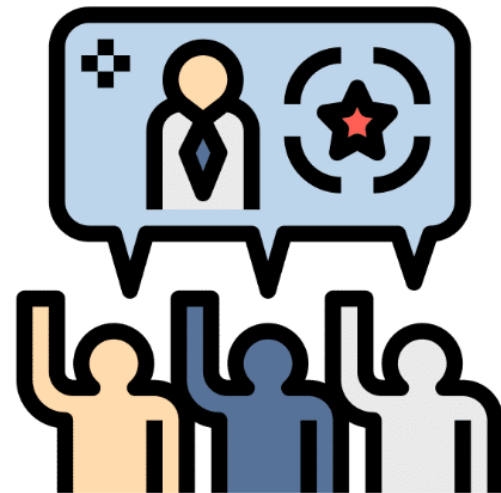
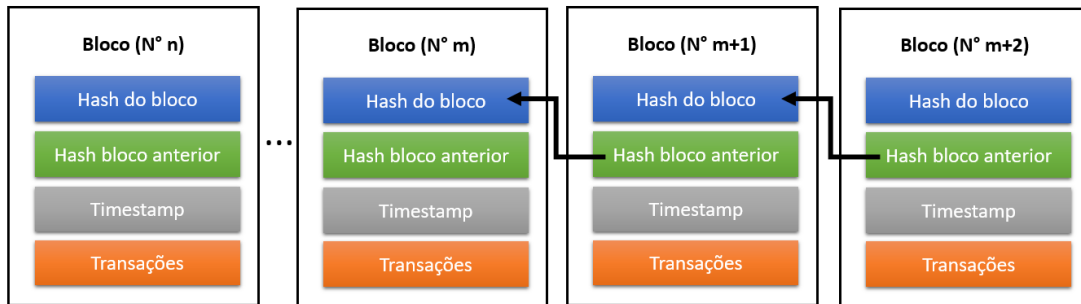
- Practical byzantine fault tolerance (BPFT)
- **Proof of Work (PoW)**
- **Proof of Stake (PoS)**
- Leased Proof of Stake (LPoS)
- Proof of Capacity (PoC)



Modificações - Hard Fork

Consenso

- Qualquer um pode fazer atualização da sua cópia da chain?



Etapa 6

Blockchain e suas Categorias

// Fundamentos da Blockchain

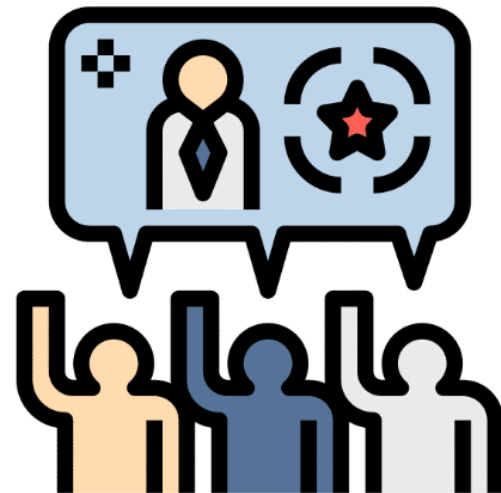
Categorias

- Características da plataforma
- Nível de permissão

Híbridas

Públicas

Permissionadas



Categorias

Públicas



- Não-permissionadas
- Resistência a censura
- Anonimato
- Transparência de eventos

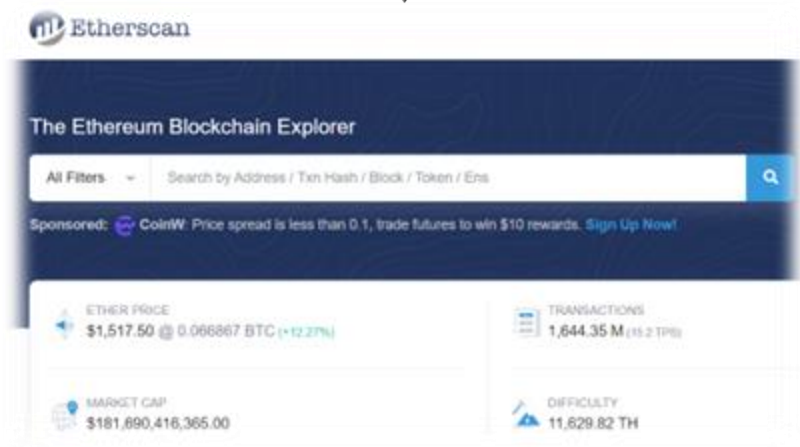


Premissa: Existência de usuários maliciosos



Categorías

Públicas

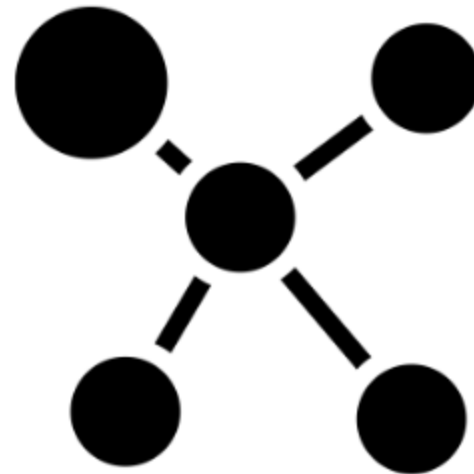


Categorias

Permissionadas

- Ambiente empresarial
- Ambiente governamental

~~Transparência (dados públicos)~~

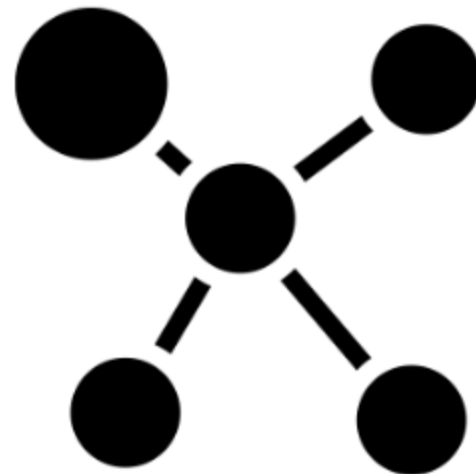


Categorias

Permissionadas

- Ambiente empresarial
- Ambiente governamental

~~Transparência (dados públicos)~~



Dados sensíveis

Categorias

Permissionadas

TRADE+LENS

- Ambiente empresarial
- Ambiente governamental



~~Transparência (dados públicos)~~

r3. HYPERLEDGER

Corda (Consórcio R3)

Categorias

Permissionadas



Fonte: hyperlegder.org



HYPERLEDGER



Community Stewardship and Technical, Legal, Marketing, Organizational Infrastructure

Frameworks



Permissionable smart contract machine (EVM)



Permissioned with channel support



WebAssembly-based project for building supply chain solutions



Decentralized identity



Mobile application focus



Permissioned & permissionless support; EVM transaction family

Tools



Infrastructure for peer-to-peer interactions



Blockchain framework benchmark platform



As-a-service deployment



Model and build blockchain networks



View and explore data on the blockchain



Ledger interoperability



Advanced transaction execution and state management

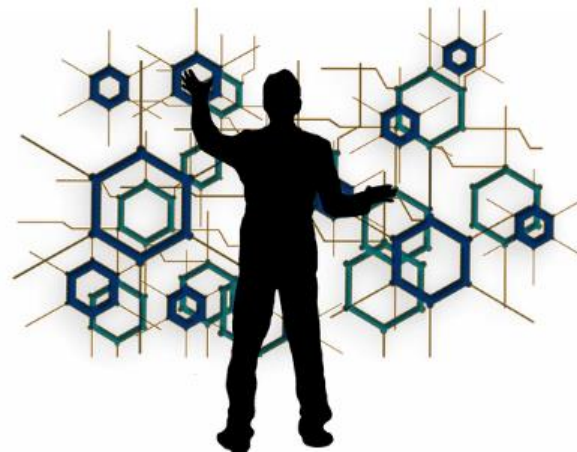


Shared Cryptographic Library

Categorias

Híbridas

- Privacidade parcial
- Tokens próprios



Tokens



Função na rede

Nodes emissores

Categorias

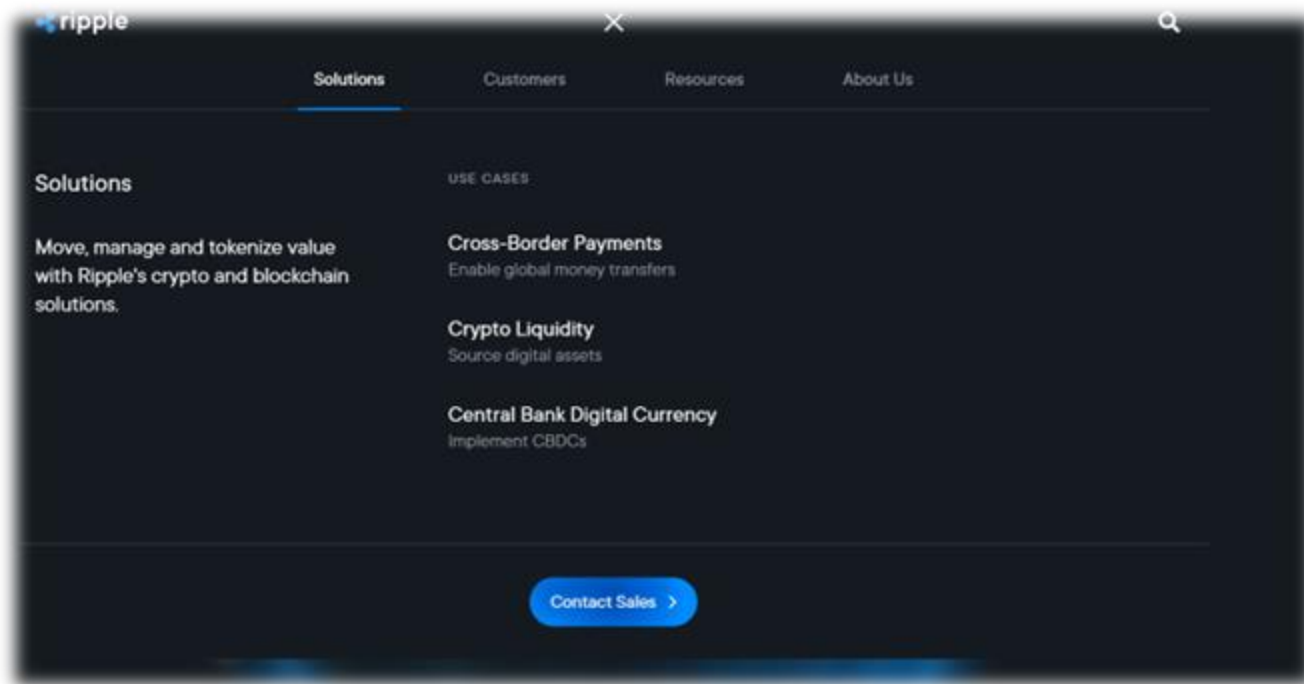
Híbridas



The screenshot shows the XinFin website homepage. At the top left is the XinFin logo. The navigation bar includes links for Home, XDC Network, XDC Utility, Developer Portal, Resource, Quick Tools Guide, and Apply For Funding. The main heading reads "Enterprise Ready Hybrid Blockchain For Global Trade and Finance". Below this, a subheading states "Combining the power of Public & Private blockchains with Interoperable Smart Contracts". Two buttons are visible: "JOIN AS NETWORK NODE" and "Open Source Wallet". On the right side, there is a video player showing a diagram of a hybrid blockchain network with nodes A and B connected to a central play button icon.

Categorías

Híbridas



Etapa 7

Desafios relacionados a Blockchain

// Fundamentos da Blockchain

Desafios

Relacionados a tecnologia

Dependentes do Contexto

Desafios

- Alto gasto computacional
- Ataque 51%
- Gargalo na validação de Transações

Relacionados a tecnologia

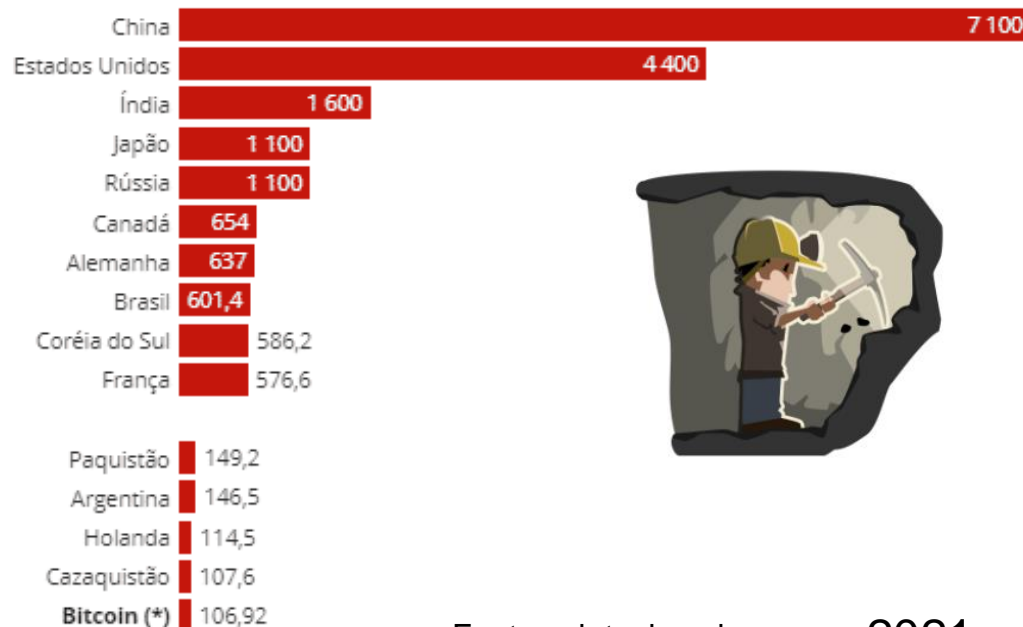
Desafios

Relacionados a tecnologia

Consumo de energia por país x bitcoin

Criptomoeda já demanda mais energia elétrica do que países com mais de 100 milhões de habitantes, como as Filipinas

■ Consumo (TWh)



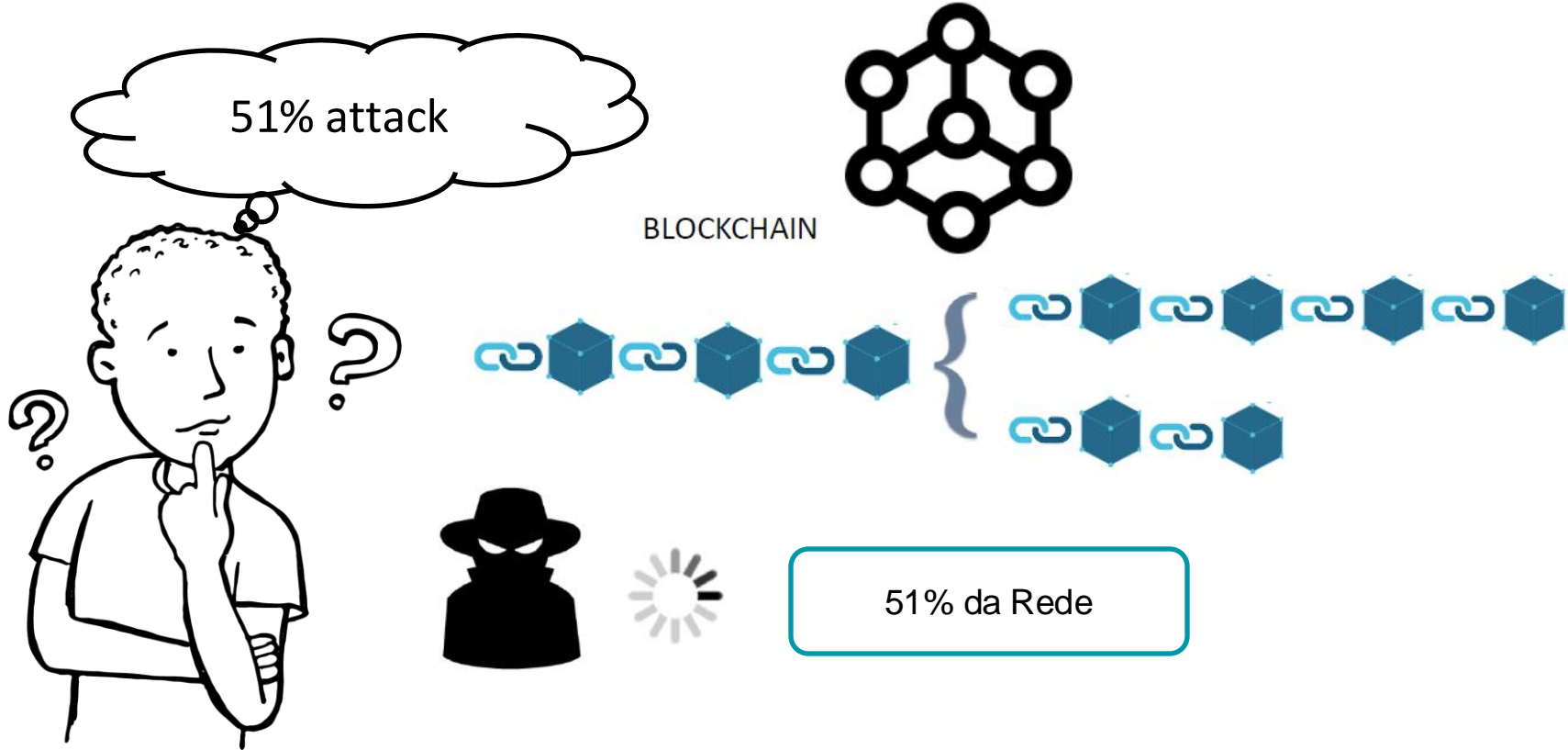
Fonte: criptonizando.com

2021

Desafios



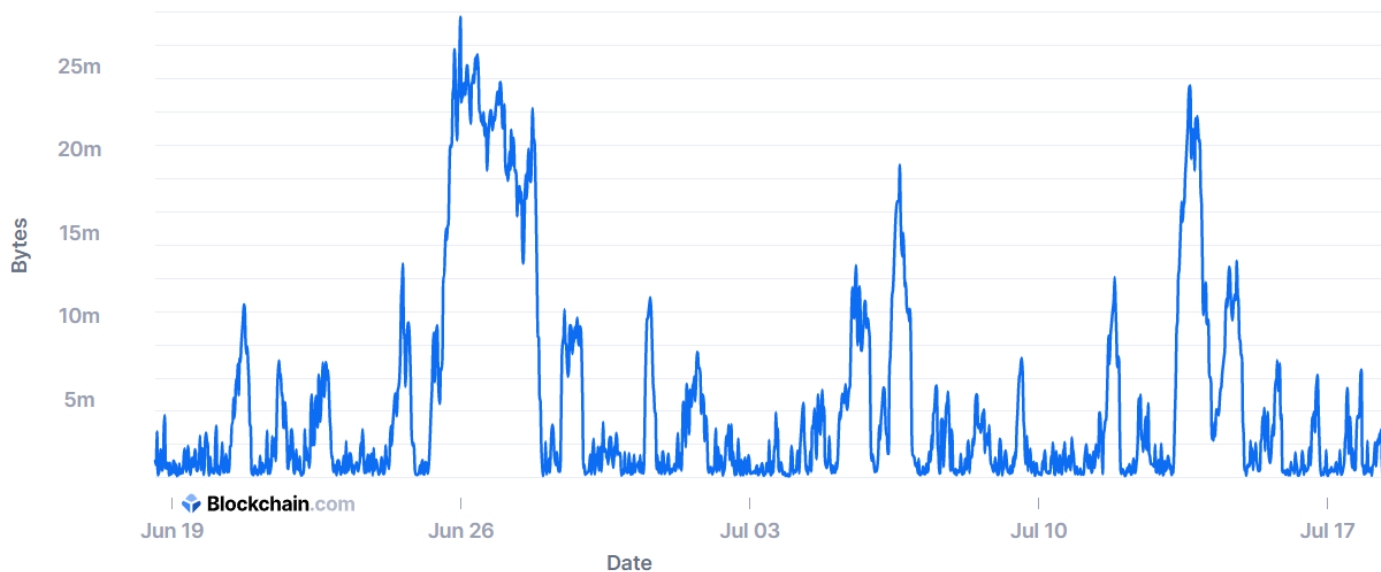
Consenso



Desafios

Tamanho do mempool (bytes)

O tamanho agregado em bytes de transações a aguardar confirmação.



30 dias 60 dias 180 dias 1 ano 3 anos Tempo todo

Valores não processados Média de 7 dias Média de 30 dias

Desafios

- Hacking de exchanges
- Erro de código não intencional
- Regulação governamental
- Volatilidade

Dependentes do Contexto

Para saber mais

Draft **NISTIR 8202** - Blockchain Technology Overview

Dissertação de mestrado: **Modelagem e Análise Temporal da Rede de Transações de uma Plataforma de Consenso Distribuído**

<http://tede.incc.br/handle/tede/299>

An Overview of the Current State of Cryptocurrencies and Blockchain Technology - November 15, 2017

<https://www.criptofacil.com/blockchain-publica-privada-e-hibrida-entenda-as-diferencas-entre-elas/>

<https://www.criptofacil.com/blockchain-publica-privada-e-hibrida-entenda-as-diferencas-entre-elas/>

Para saber mais

<https://www.techtarget.com/searchitoperations/tip/Blockchain-An-immutable-ledger-to-replace-the-database>

<https://acervolima.com/papel-do-blockchain-na-ciberseguranca/#:~:text=Os%20dados%20das%20transa%C3%A7%C3%B5es%20s%C3%A3o,de%20maneira%20segura%20e%20protegida>

<https://aws.amazon.com/pt/what-is/blockchain/>

<https://cointimes.com.br/esqueca-o-rg-credenciais-em-nft-chegaram-para-ficar-afirma-relatorio/>

Dúvidas?

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

