

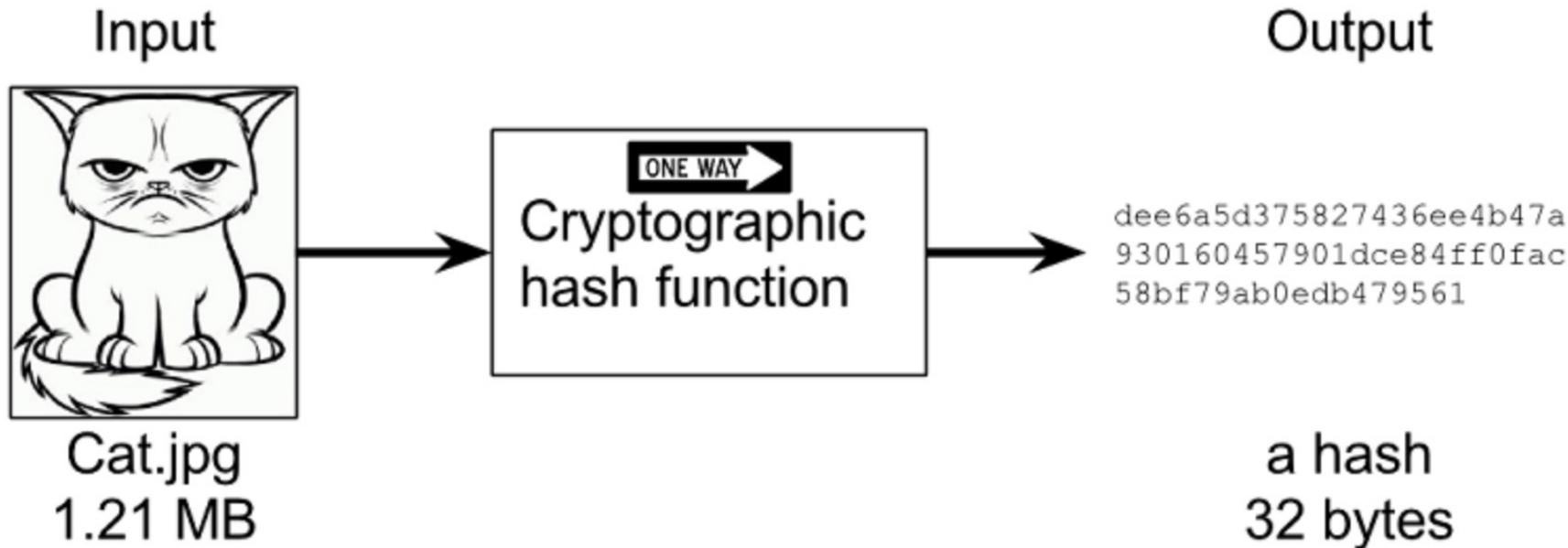
Sumário

- O que é blockchain?
- Principais componentes
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

Principais componentes da blockchain

- Funções Hash
- Livro-contábil imutável
- Mineração
- Protocolo de consenso

Componente 1: funções Hash



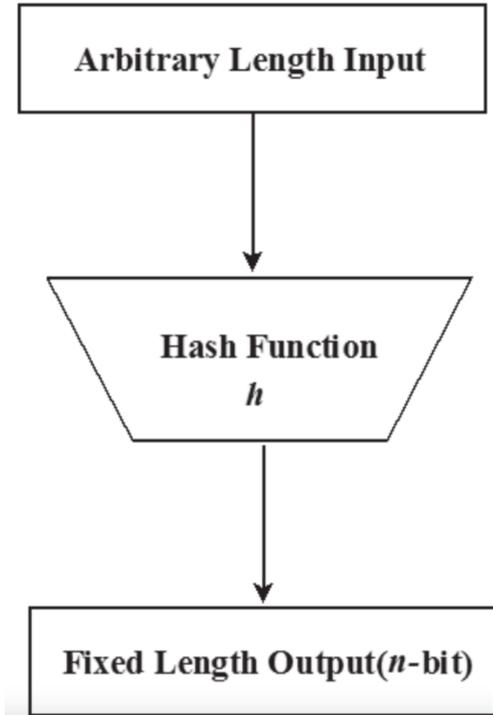
Source: manning

O que é uma função hash?

- Funciona como uma **impressão digital**
- **Difícil** haver **duas pessoas com a mesma digital**
- Assim como uma pessoa, um documento pode ter uma impressão digital
 - Um vídeo, uma transação e assim por diante

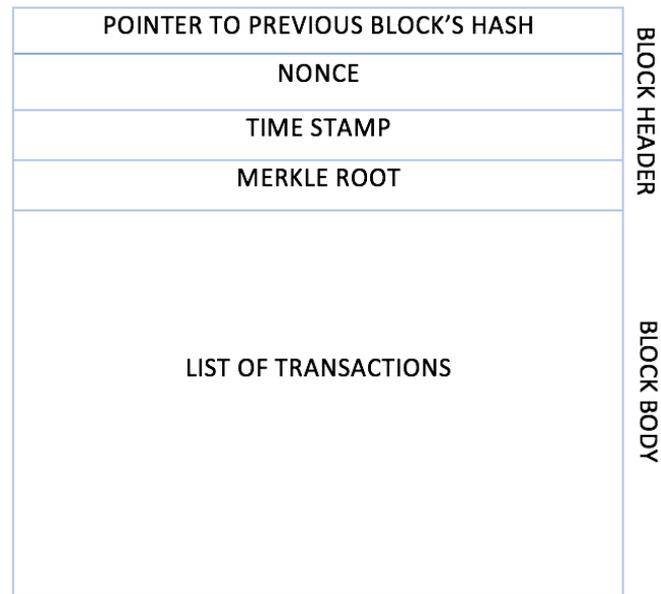


What is Biometrics? | Touchless Biometric ...
tbs-biometrics.com



Estrutura do bloco blockchain com Hash

- Merkle root contém o hash do bloco
- O hash é quem **assegura a imutabilidade** do bloco
- **Efeito avalanche**



Jó Ueyama

bed0d388a0d3d8df4ed97ddcea18e89bf6e6f92050014c421db1ee0519a0d2d7

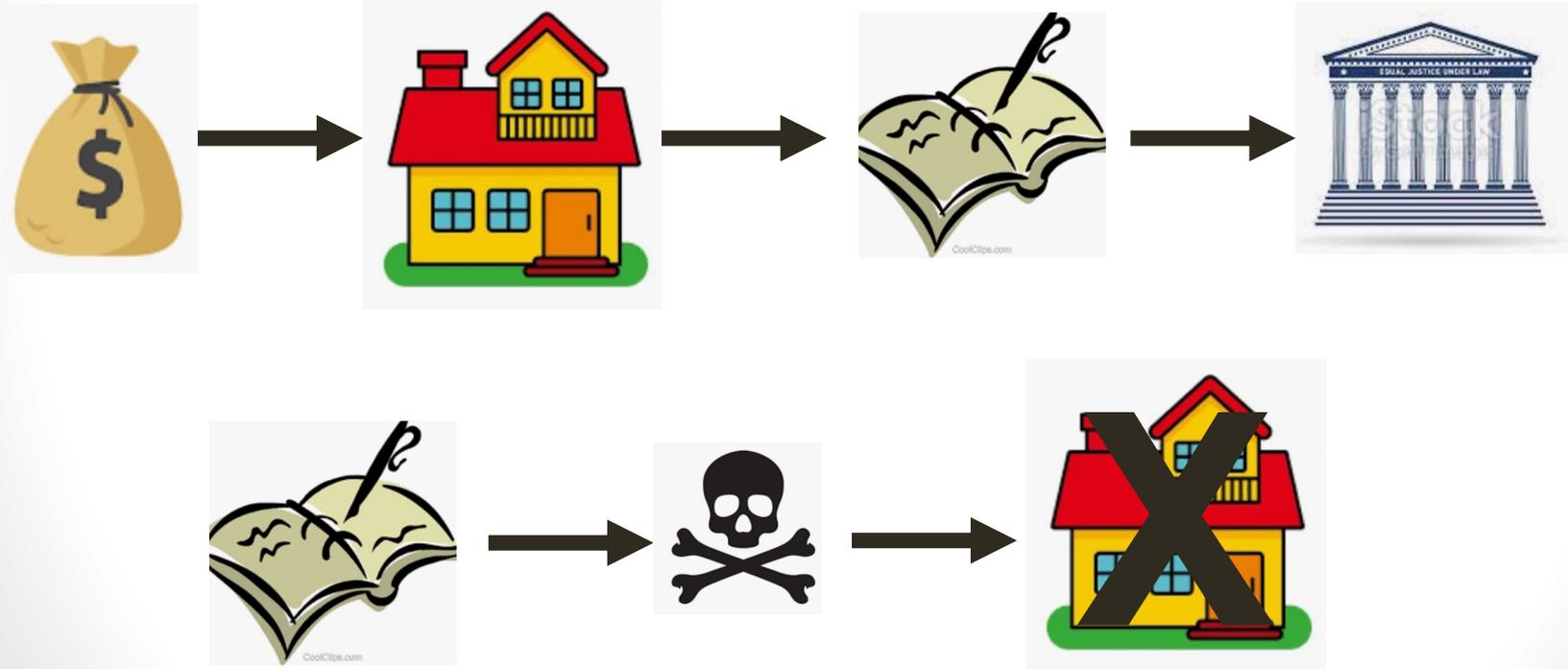
Jo Ueyama

d1c93206a46b1a9c9f24519580771170a187c7b387145e035df5e5050fefb5b2

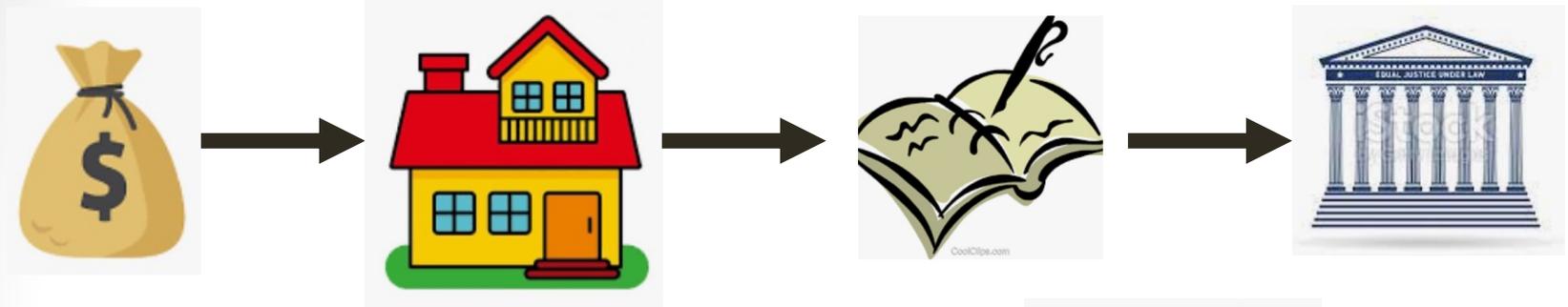
Principais componentes da blockchain

- Funções Hash
- Livro-contábil imutável
- Mineração
- Protocolo de consenso

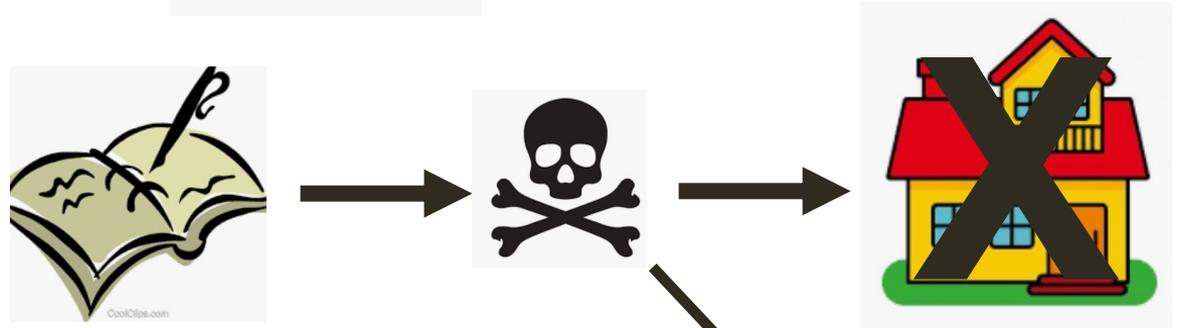
Livro-contábil imutável



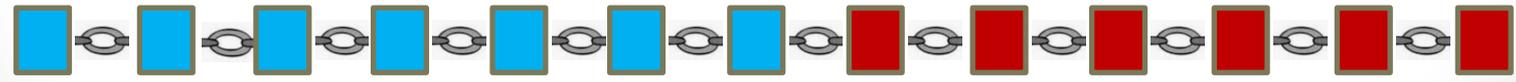
Livro-contábil imutável c/ blockchain



Ledger tradicional

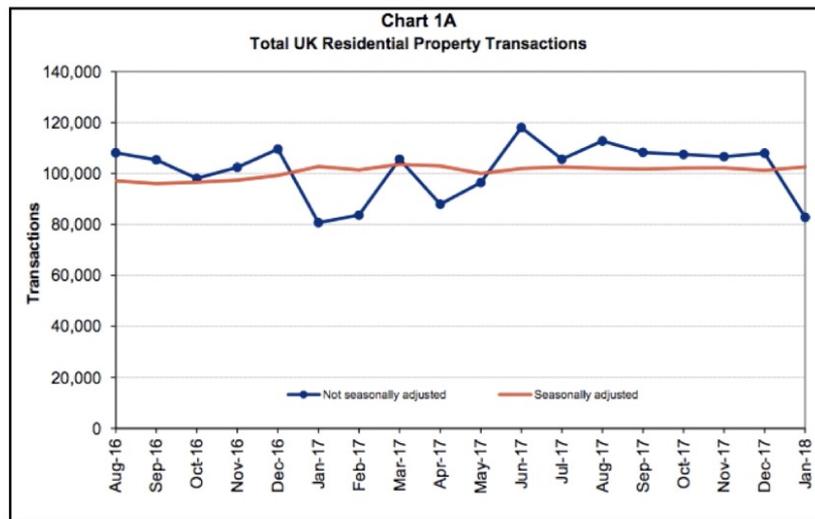


Blockchain



Livro-contábil imutável

- No cenário real: mudança de títulos residenciais acima de GBP40K
- Algo em torno de 100 transações por hora
- Suscetível a erros e fraudes



Source: <https://www.gov.uk>

Principais componentes da blockchain

- Funções Hash
- Livro-contábil imutável
- Mineração
- Protocolo de consenso

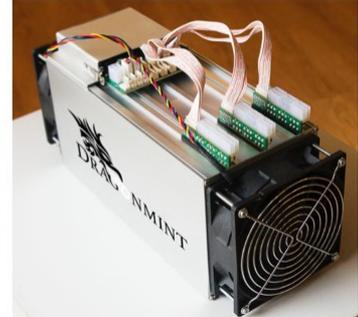
Mineração de blocos

- É como cadeados com segredo
 - É difícil de adivinhar
 - Toma bastante tempo para testar
 - 10.000 tentativas com segredo de 4 dígitos
 - Ganha quem tem maior poder computacional
 - O mesmo ocorre com a mineração
- Mas por outro lado é fácil de testar o segredo desde que ele tenha sido fornecido
 - Trabalho de nodos pares na blockchain



High Quality Padlock Solid Br...
aliexpress.com

Mining systems



Quatro plataformas de hardware: CPU, GPU, FPGA e um ASIC

Principais componentes da blockchain

- Funções Hash
- Livro-contábil imutável
- Mineração
- Protocolo de consenso

Protocolo de consenso

- É fácil atingir um acordo em cliente/servidor
 - O servidor “manda” e detém as regras
 - O cliente confia no servidor
 - P.ex., o cliente confia no Banco do Brasil
- Mas em um ambiente sem um intermediário confiável?
- Ambiente com nodos que podem estar defeituosos
- Ambiente carece de regras para se chegar a um consenso
- Alguém tem que mandar? Mas quem? O protocolo de consenso
- **Protocolo que dita o acordo entre os nodos não-confiáveis sobre os dados na blockchain**
- P.ex., quem vai criar o novo bloco?

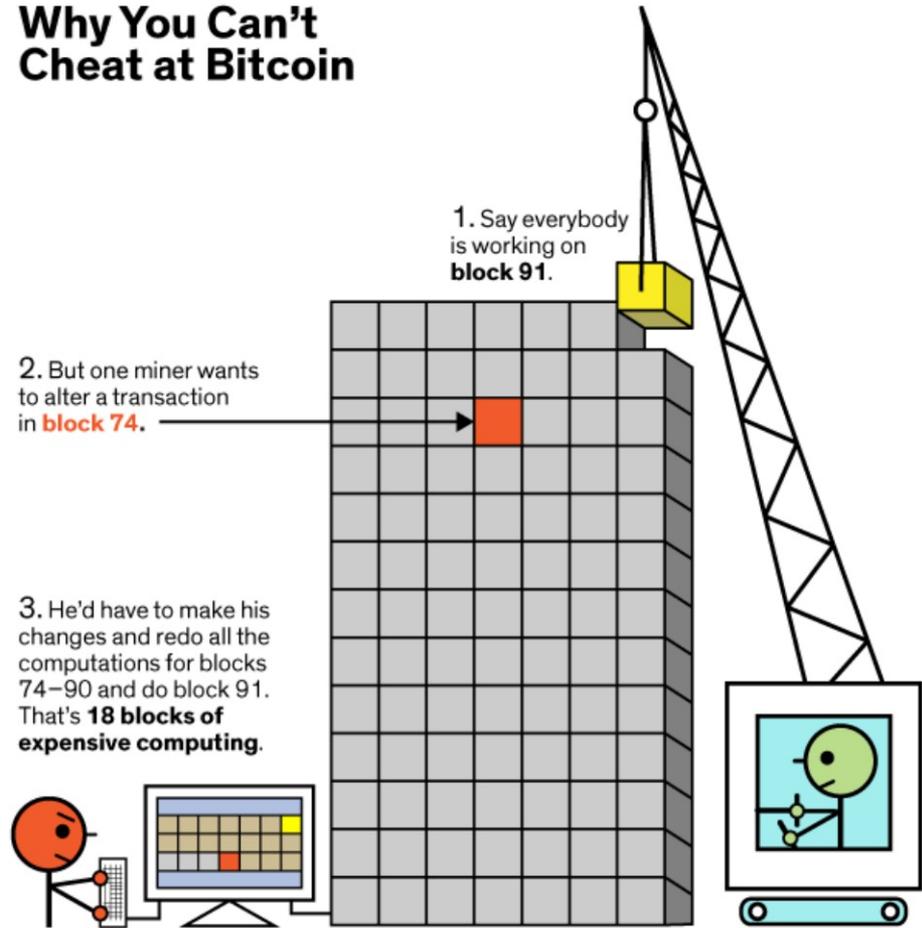
Proof of Work (PoW)

- Adotado no Bitcoin (SHA256) e no Ethereum (KECCAK-256)
- Os nodos competem entre si para encontrar o padrão de hash
- Normalmente com cerca de 18 zeros na frente
- Este padrão é ajustado periodicamente

- Como o custo computacional é alto, isto seria um **desincentivo para os *hackers***

Por que é difícil atacar o Bitcoin?

Why You Can't Cheat at Bitcoin



4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

For Bitcoin Blockchain details

- Check out <https://btcscan.org/>

Sumário

- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

O que é Ethereum

- Ethereum e Bitcoin são baseados na blockchain (são amigos)



Brandon Hinojos Best Stories of the Year!, Lifestyl...
rprnmag.com

O que é o Ethereum?

- Foi criado em 2013 por Vitalik Buterin, pesquisador e programador de criptomoedas
- Prover o uso do blockchain para **qualquer uso além das criptomoedas**
- Levar a filosofia do blockchain para **diversos domínios de aplicação**
- Amplo uso dos **smart contracts**
- Permitir programar a blockchain com linguagens genéricas como Javascript



O que é Ethereum?

- A ideia é ter um supercomputador descentralizado

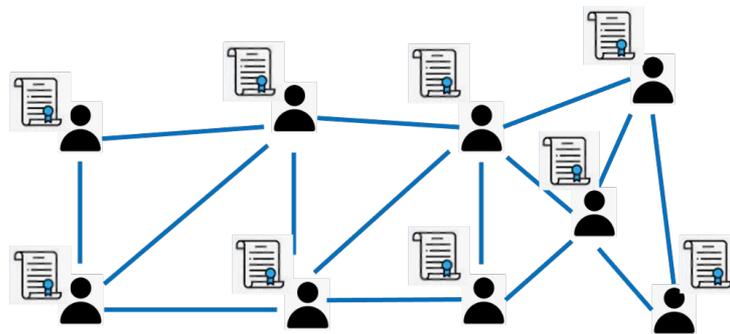
<https://etherscan.io/nodetracker>

- Executar uma variedade de aplicações

- Baseado em blockchain

- Não armazena apenas dados de transações

- Armazena códigos



Blockchain e Ethereum

Bitcoin	Ethereum
Mais criptomoeda	Mais plataforma blockchain
Compra e venda de criptomoeda (financeiro)	Criado para aplicações descentralizadas
Consenso através da prova de trabalho	Consenso da prova de trabalho e prova de participação

Redes Ethereum

- Todas
 - Mesma forma de armazenar dados
 - Mesma forma de acessar dados
- **Main network**
 - Moeda “real”
 - Por quê? Foi combinado previamente
- **Test network**
 - Testar os contratos inteligentes
 - Testar atualizações de protocolos

Sumário

- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

O que é um contrato inteligente?

- Um programa (código) que é armazenado e executado em um blockchain
- Blockchain não armazena apenas transações
- Mas códigos também!

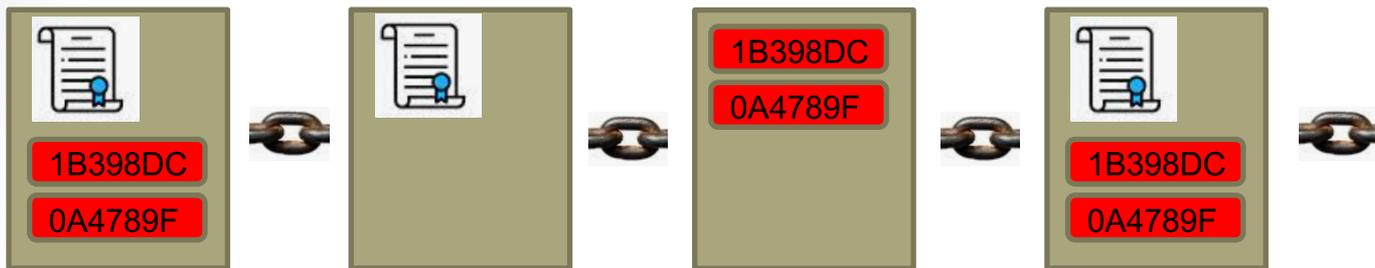
Linguagens

- Solidity
- Java script
- Golang (by Google)



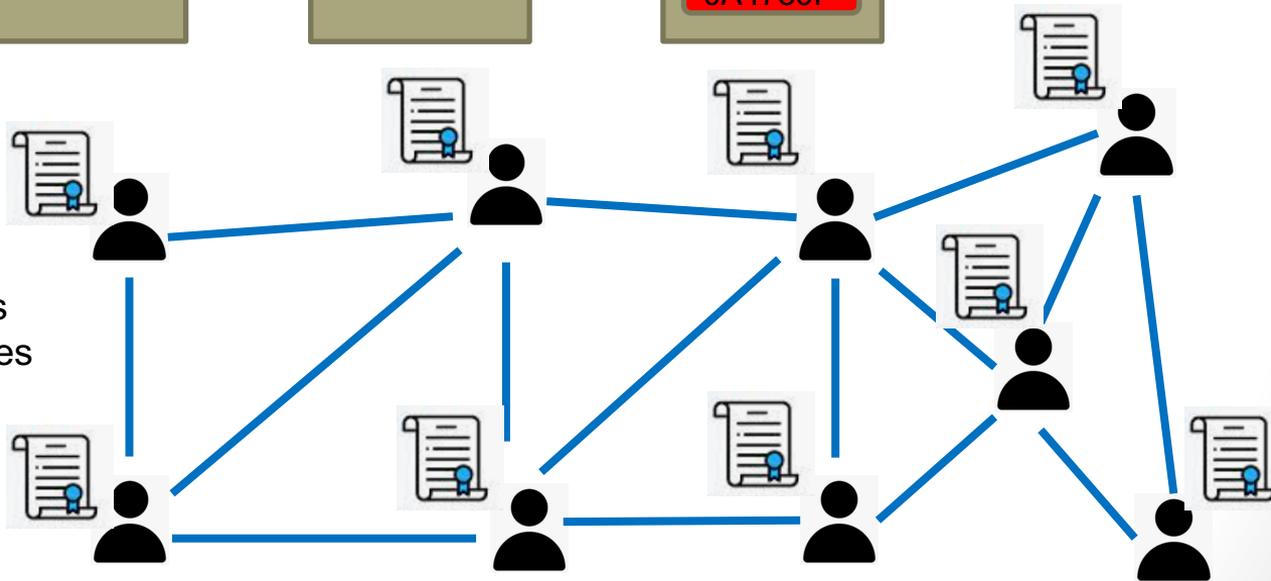
What Are Smart Contracts? [Ultimate Beginner's ...
blockgeeks.com

O que é contrato inteligente?



Cada nodo tem:

1. Histórico dos contratos inteligentes
2. Histórico das transações
3. Estado atual dos contratos inteligentes



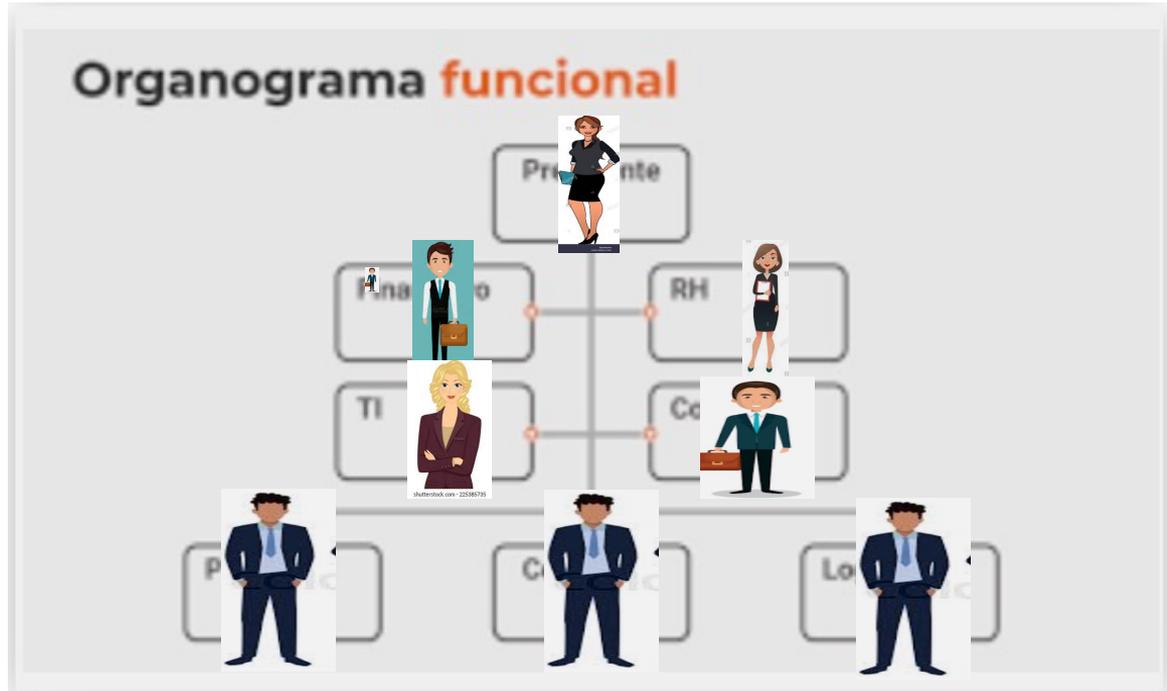
Prática com contratos

- https://remix-ide.readthedocs.io/en/latest/create_deploy.html
- <https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html>

Sumário

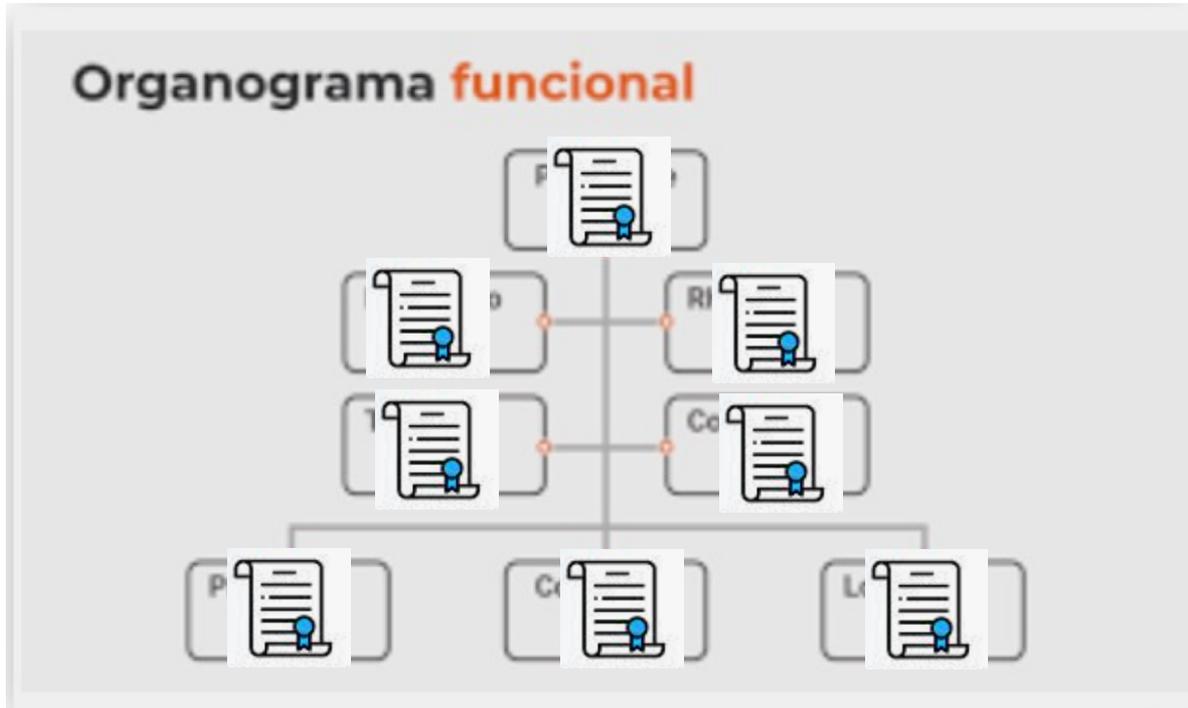
- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

DAO



Organograma: Como Apresentar a Estrutura Empres...
blog.tangerino.com.br

DAO



Organograma: Como Apresentar a Estrutura Empres...
blog.tangerino.com.br

Exemplos de DAOs

- Nexus Mutual – empresa de seguros
- DASH – Usuários conhecidos como Masternodes rodam no DAO
- Flamingo DAO – plataforma de NFT
- Gitcoin – seleciona os projetos bons usando avaliadores executados como DAO

Jun 1, 2021, 08:00am EDT | 17,306 views

Forbes

What Are DAOs And Why You Should Pay Attention

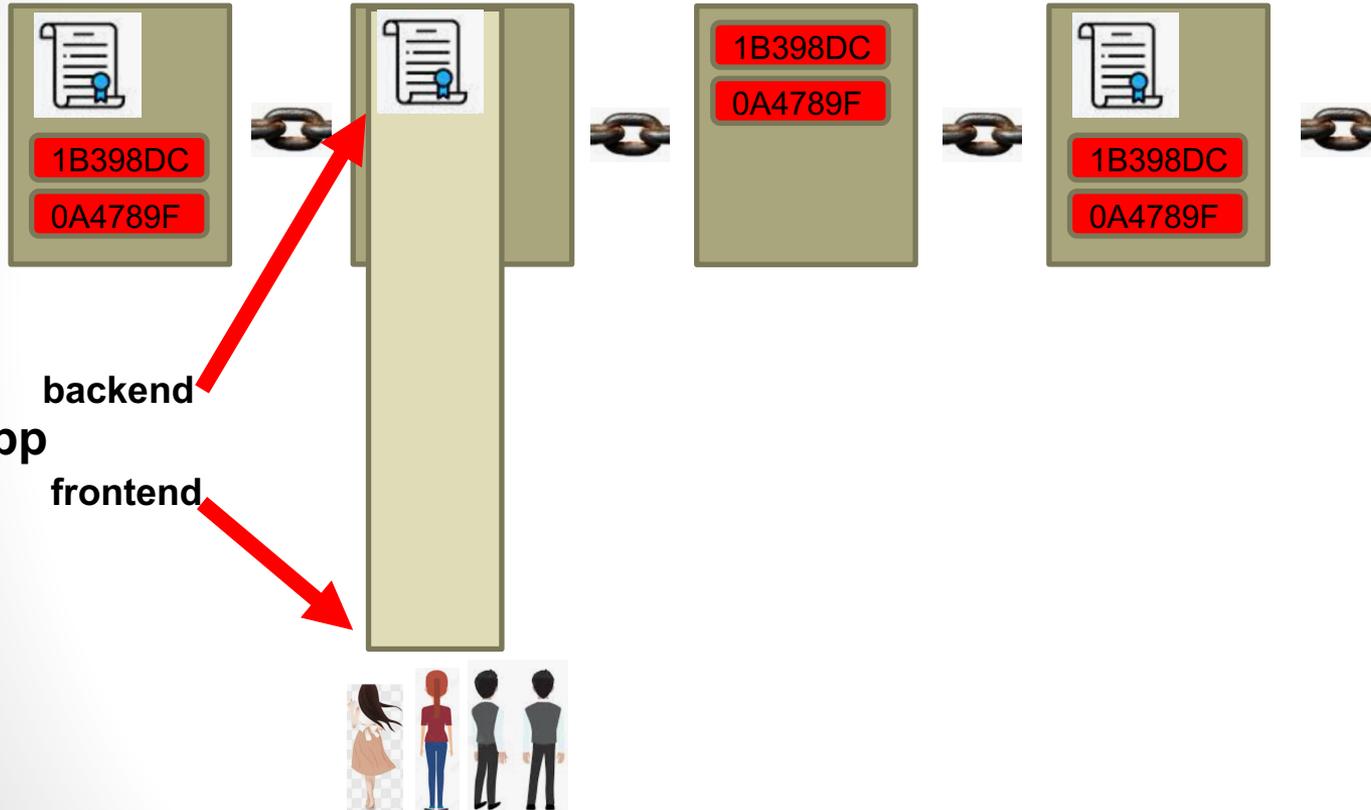
Sumário

- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

O que é DApp?

- DApps são aplicações:
 - descentralizadas
 - executadas em redes P2P, como blockchain
- Diferença com as aplicações convencionais?
 - Não é centralizado
 - O seu código está no **contrato inteligente**
- Vantagem chave?
 - Não há SPOF (*single point of failure*)

Dapps



O que é Dapp?

- Dapps possuem dois componentes
 - Frontend, uma interface para interagir com o contrato inteligente
 - Backend que é o contrato inteligente com que interage
- O contrato inteligente provê uma API usada para interagir com o contrato

Exemplo de Dapp

- Steemit é um twitter, mas no blockchain
- Acessar <https://steemit.com>
- Vantagem do steemit?
 - Não há um elemento central que cria as políticas de remuneração
 - Transparência, toda as postagens são rastreáveis

Sumário

- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- DAO
- Dapps
- Oportunidades
- Pesquisas

Oportunidades

- NFT
- DeFi
- CBDC

O que é NFT?

- Primeiro Tweet do Jack Dorsey foi vendido por quase US\$ 3 MI
- O valor é de quem vende e o item comercializado



Jack Dorsey sells his first tweet ever as an NFT fo...
uaebarq.ae

O que é NFT?

- Nyan cat vendido por US\$602K



Nyan Cat NFT Sold for \$602.000 - Play to Earn
playtoearn.online

O que é NFT?

- Non fungible token
- Não é “trocável” diferente de uma nota de R\$20
- Não é “trocável” como um domínio “amazon.com.br”
- Em resumo: um bem digital armazenado na blockchain
- É um **investimento!**
 - Usa-se GAS para criar o bloco com a transação do NFT
 - Em torno de US\$100
- **Token** é o registro de um ativo em formato digital
 - Registram-se o valor, o proprietário entre outros

O que é NFT?

- NFTs são tokens **criptográficos únicos** em uma blockchain
- Não podem ser duplicados
- A "tokenização" (registro) desses ativos tangíveis do mundo real torna a compra, venda e negociação mais eficientes
- Reduz a probabilidade de fraude

Exemplos de NFT

- Qualquer bem digital
- Nome de domínio
- Uma arte, música
 - Posso imitar e desenhar uma réplica, mas a original tem um preço
- Desenho animado

- Pode ser uma única peça ou várias itens; pode ganhar royalties em cada venda
- Fica na MV **Ethereum**

Plataformas do NFT

- A propriedade pode ser fracionada
- Rarible rarible.com
- Opensea opensea.io
- Há a necessidade de usar a carteira do Ethereum como o Metamask
- Metamask e o coinbase são as mais usadas
- Usa a **rede principal** do Ethereum
- A demanda do Ethereum irá crescer por conta do NFT e do DeFi (próximo assunto)



101 Blockchains



Fungible

VS



Non-Fungible

Carro como um bem não fungível

- Um carro adquirido por Bob e Alice
- No ato da compra, mesmo valor, massss
- Terão dois preços diferentes depois de um ano
- **Histórico de Kilometragem**, revisões na **concessionária**? Foi **batido**?

BINANCE NFT

Unleash your creativity

With Binance NFT's beginner-friendly minting feature, verified Binance users can create their own NFTs in just a few clicks! Start minting your own NFTs with Binance NFT today!

[Saiba Mais](#)

CREATE

YOUR OWN NFT COLLECTION NOW!

Fene Apê NFT vendido a 0.86 BUSD 6 minutos atrás

Coleções Recomendadas

NFTs
Caixas Misteriosas
< >
Mais

HALO OFFICIAL(BSC) ✓

Volume **1531074.21 USD** Preço Mínimo **3000 USD**

22bullets Magic DJ Show ✓

Volume **880 USD** Preço Mínimo **88 USD**

Honey Shots ✓

Volume **18702.87 USD** Preço Mínimo **44.84 USD**

Coleções em Destaque 7 dias

Sumário

- O que é blockchain?
- Principais componentes
- Ethereum
- Contratos Inteligentes
- Dapps
- DAO
- Oportunidades
- Pesquisas