

Blockchain e Smart Contracts - Ethereum



Fundamentos da Blockchain

Juliana Mascarenhas

Tech Education Specialist DIO / Owner @Simplificandoredes
e @SimplificandoProgramação

Mestre em modelagem computacional | Cientista de dados

@in/juliana-mascarenhas-ds/



Objetivo Geral

A capacidade da Blockchain é intensificada com a utilização dos contratos inteligentes. Contudo, é preciso estar atento a possíveis falhas de segurança geradas por esses scripts dentro da rede. Iremos desvendar as propriedades do Ethereum, segunda cripto mais utilizada no mercado.

Percurso

Etapa 1

Título da Etapa 1

Etapa 2

Título da Etapa 2

Etapa 3

Título da Etapa 3

Etapa 1

Como funciona a plataforma Ethereum?

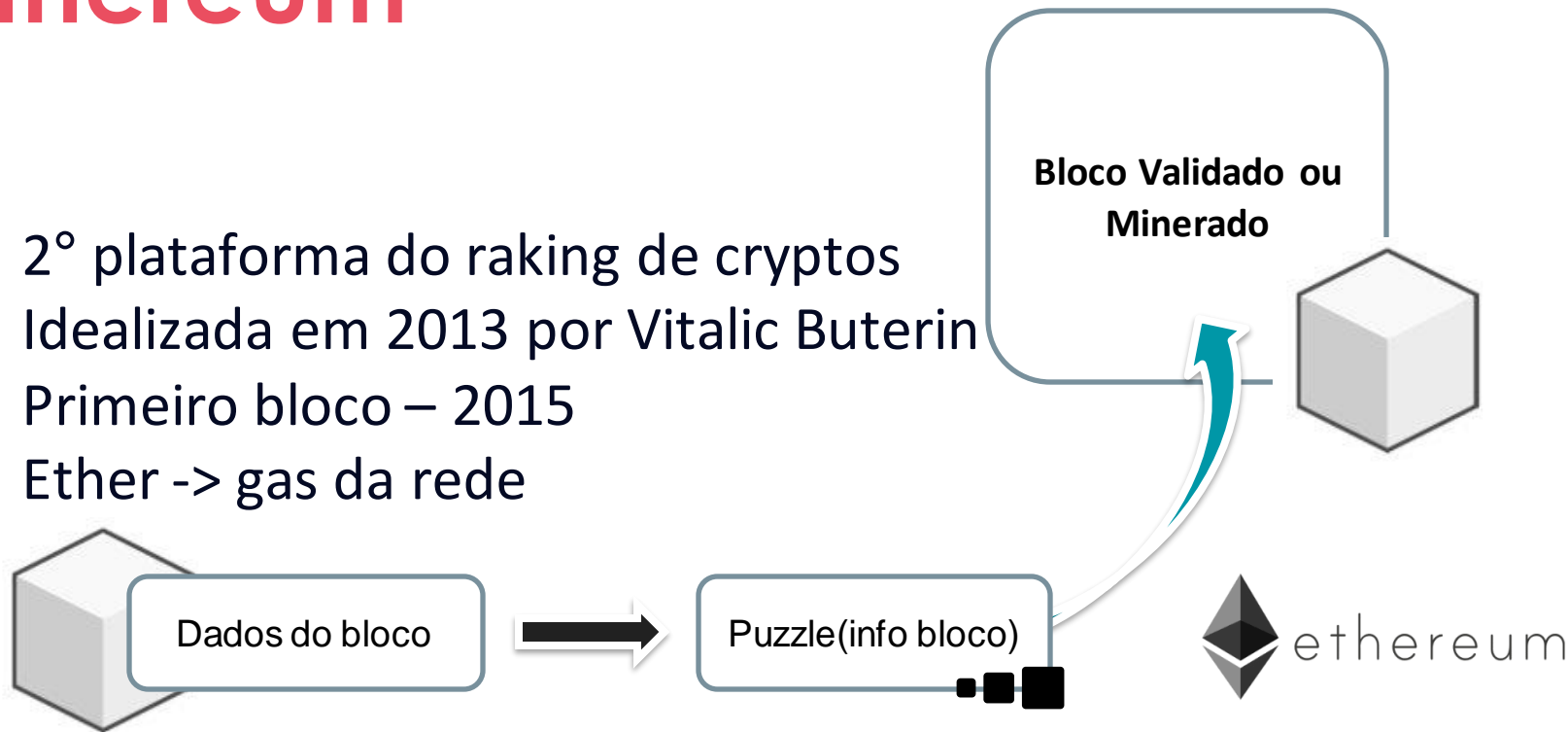
// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

Ethereum

- 2º plataforma do raking de cryptos
- Idealizada em 2013 por Vitalic Buterin
- Primeiro bloco – 2015
- Ether -> gas da rede

Ethereum

- 2º plataforma do raking de cryptos
- Idealizada em 2013 por Vitalic Buterin
- Primeiro bloco – 2015
- Ether -> gas da rede

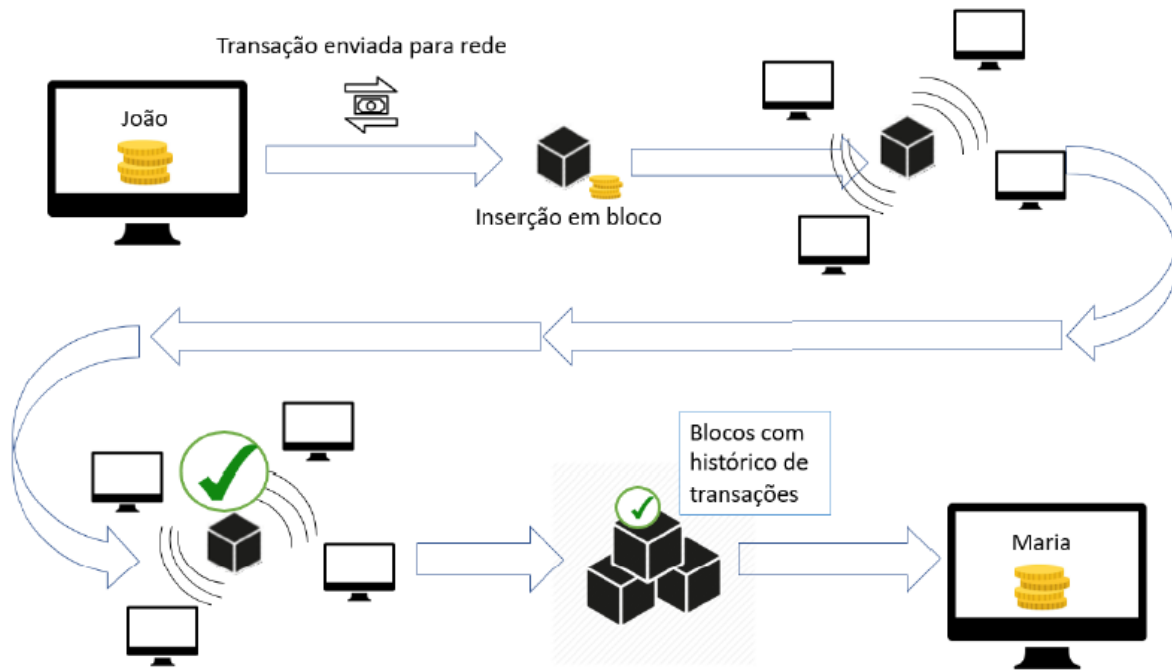


Ethereum

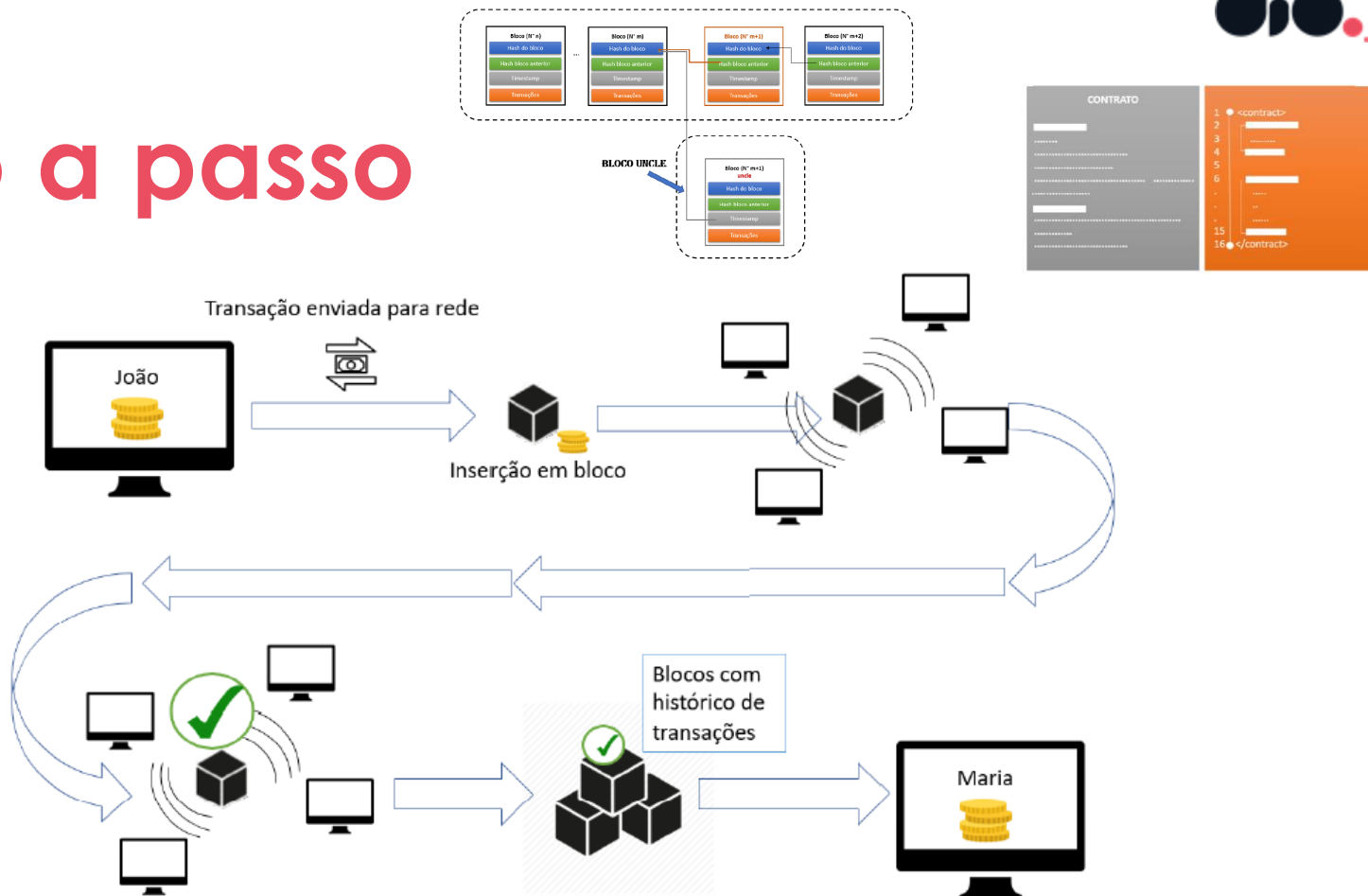
- 2º plataforma do raking de cryptos
- Idealizada em 2013 por Vitalic Buterin
- Primeiro bloco – 2015
- Ether -> gas da rede



Passo a passo



Passo a passo



Transações no Ethereum

Transaction Details

Sponsored: bc.game - Win up to 1 BTC Everyday! Live casino • 20k slots [Play Now](#)

Overview Logs (1) State Comments

Transaction Hash: 0x081740b3d977b0edc55034e832371b04534ec3a73977056a1b038bd9924b ⓘ

Status: Success

Block: 15173348 2 Block Confirmations

Timestamp: 42 secs ago (Jul-19-2022 01:31:38 PM +UTC) | Confirmed within 30 secs

From: 0x0f00c0e39d81b0e3ab9e00c3ea15ac790933ca ⓘ

Interacted With (To): Contract 0xa0b86991c6218b36c1d19d4a2e9eb0ce30056b48 (Centre: USD Coin) ⓘ

Tokens Transferred: From 0x0f00c0e39d81b0e3ab9e00c3ea15ac790933ca To 0x25af9e43e4111a For: 70,000 (\$70,140.00) USD Coin (USDC)

Value: 0 Ether (\$0.00)

Transaction Fee: 0.004312006032634375 Ether (\$0.77)

Gas Price: 0.00000005700743359 Ether (55.708743359 Gwei)

Gas Limit & Usage by Txn: 65,163 | 65,625 (99.19%)

Gas Fees: Base: 64.708743359 Gwei | Max: 102.394020095 Gwei | Max Priority: 1 Gwei

Burnt & Txn Savings Fees: Burnt: 0.004248380032534375 Ether (\$0.67) | Txn Savings: 0.00245760239289375 Ether (\$0.75)

Others: Txn Type: 2 (EIP-1559) | Nonce: 29 | Position: 220

Input Data:





```
Function: transfer(address to, uint256 value)
MethodID: 0xa9059cbb
[0]: 0000000000000000000000000000000000000000000000000000000000000000
[1]: 0000000000000000000000000000000000000000000000000000000000000000
```

[View Input As](#) [Decode Input Data](#)



[Click to see Less](#)

Private Note: To access the Private Note feature, you must be [Logged In](#)



Transações no Ethereum

Overview	Logs (1)	State	Comments
Transaction Hash:	0x081740b3c9578b6edcc55034e8323716c4534ec3a73f7765da1b038bd89f2f4b 		
Status:	✓ Success		
Block:	15173348 2 Block Confirmations		
Timestamp:	42 secs ago (Jul-19-2022 01:31:38 PM +UTC) Confirmed within 30 secs		
From:	0xcfdcc6e395d81b9e3ab6e008c3ea15ac790653ca 		
Interacted With (To):	Contract 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48 (Centre: USD Coin) ✓ 		
Tokens Transferred:	» From 0xcfdcc6e395d81b... To 0x25afde43e4111a... For 70,000 (\$70,140.00)  USD Coin (USDC)		

Transações no Ethereum

❓ Value:	0 Ether (\$0.00)
❓ Transaction Fee:	0.004312005032934375 Ether (\$6.77)
❓ Gas Price:	0.000000065706743359 Ether (65.706743359 Gwei)
❓ Gas Limit & Usage by Txn:	66,163 65,625 (99.19%)
❓ Gas Fees:	Base: 64.706743359 Gwei Max: 102.394020965 Gwei Max Priority: 1 Gwei
❓ Burnt & Txn Savings Fees:	 Burnt: 0.004246380032934375 Ether (\$6.67)  Txn Savings: 0.00240760259289375 Ether (\$3.78)
❓ Others:	Txn Type: 2 (EIP-1559) Nonce: 29 Position: 220

Transações no Ethereum

❓ Value:	0 Ether (\$0.00)
❓ Transaction Fee:	0.004312005032934375 Ether (\$6.77)
❓ Gas Price:	0.000000065706743359 Ether (65.706743359 Gwei)
❓ Gas Limit & Usage by Txn:	66,163 65,625 (99.19%)
❓ Gas Fees:	Base: 64.706743359 Gwei Max: 102.394020965 Gwei Max Priority: 1 Gwei
❓ Burnt & Txn Savings Fees:	 Burnt: 0.004246380032934375 Ether (\$6.67)  Txn Savings: 0.00240760259289375 Ether (\$3.78)
❓ Others:	Txn Type: 2 (EIP-1559) Nonce: 29 Position: 220

Transações no Ethereum

[illegible]

Blocos



Overview

Comments

Block Height:

15173391

<

>

Timestamp:

9 mins ago (Jul-19-2022 01:40:23 PM +UTC)

Transactions:

218 transactions

and

42 contract internal transactions

in this block

Mined by:

0x7f101fe45e6649a6fb8f3f8b43ed03d353f2b90c (Flexpool.io) in 3 secs

Block Reward:

2.278217118332765803 Ether (2 + 0.84213278135137786 + 0.0625 - 0.626415663018612057)

Uncles Reward:

1.5 Ether (1 uncle at Position 0)

Difficulty:

11,972,443,132,411,369

Total Difficulty:

54,363,691,341,136,588,644,865

Size:

54,195 bytes

Gas Used:

13,111,521 (43.71%)

-13% Gas Target

Gas Limit:

30,000,000

Base Fee Per Gas:

0.000000047775972217 Ether (47.775972217 Gwei)

Burnt Fees:

0.626415663018612057 Ether

Extra Data:

Flexpool/S1/US-East - Toronto (Hex:0x466c6578706f6f6c2f53312f55532d45617374202d20546f726f6e746f)

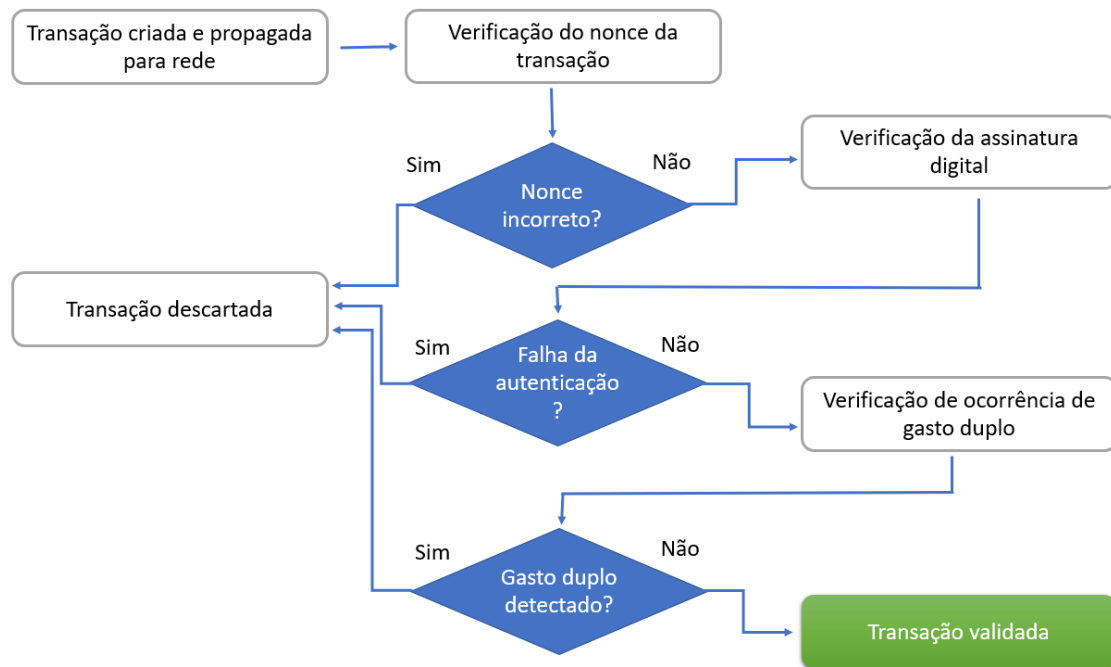
Click to see more

Blocos

② Hash:	0x16cd0d5d741064d0235577ee2b276b1cf5c373693d32609e4545afebd8682c00
② Parent Hash:	0xc82e14997a31a019f47e255712aec5a0a88656d76fd4f917385d6ae88823c157
② Sha3Uncles:	0x77837c18c5c9e6a2e75307f6f6cf3ddef452a787c57d30f6f25b0c84b6942910
② StateRoot:	0xf13d453219763928b06860652b0e5cc867d1f90a891ca8a241ccea6299442fa3
② Nonce:	0x3c4f52a1a0472bbf

[Click to see less](#) ↑

Processo de verificação



Etapa 2

O que são Contratos Inteligentes?

// Fundamentos da Blockchain/Blockchain e Smart Contracts - Ethereum

Smart Contracts

- Nick Szabo 1994
- Uso criptocurrencys
- Duas partes interessadas
- Protocolo auto executável
- Scripts



Smart Contracts

- Processa e toma ações de acordo com regras do contrato
- Qualquer informações pode ser utilizada. Não apenas financeiro
- Blockchain
 - > Facilita o registro



Smart Contracts

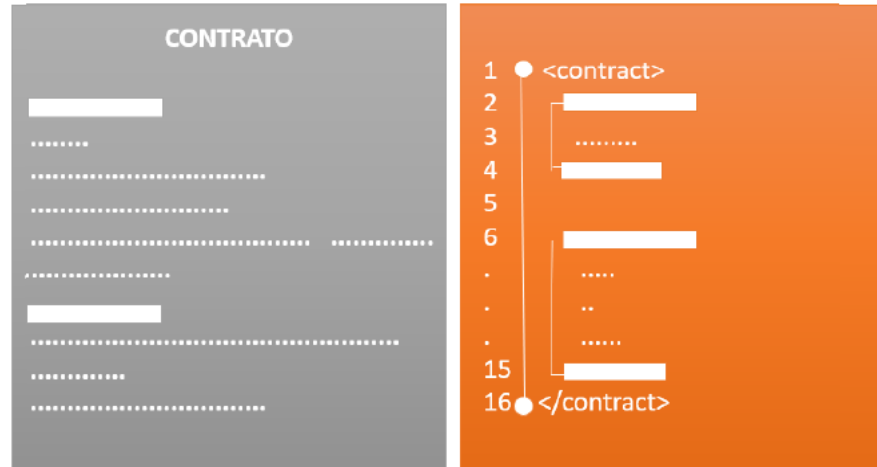


Figura 9 – Exemplo comparativo de contratos

Smart Contracts



- Lógica de negócios
- Linguagem de programação
- Execução de instruções baseada em condições (algoritmo)
- Solidity

Armazenamento

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) {
        storedData = x;
    }

    function get() constant returns (uint) {
        return storedData;
    }
}
```

Smart Contracts

Submoeda

```
pragma solidity ^0.4.0;

contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter;
    mapping (address => uint) public balances;

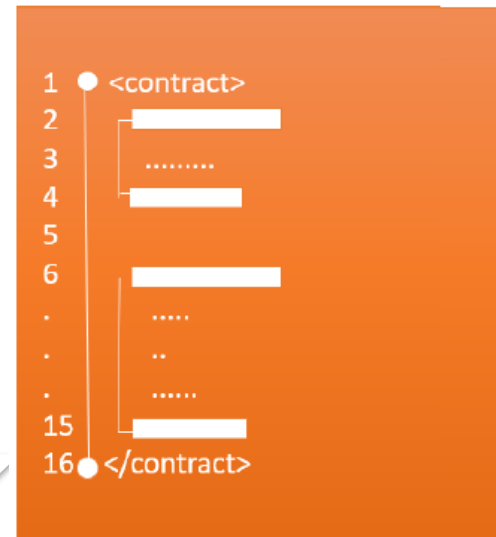
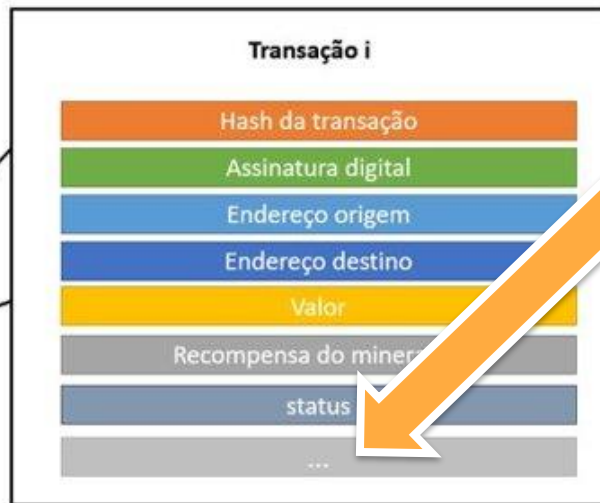
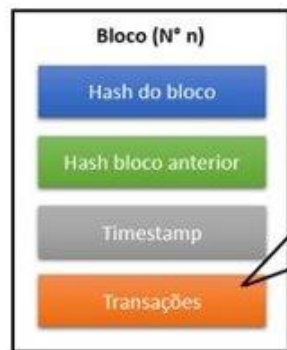
    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() {
        minter = msg.sender;
    }

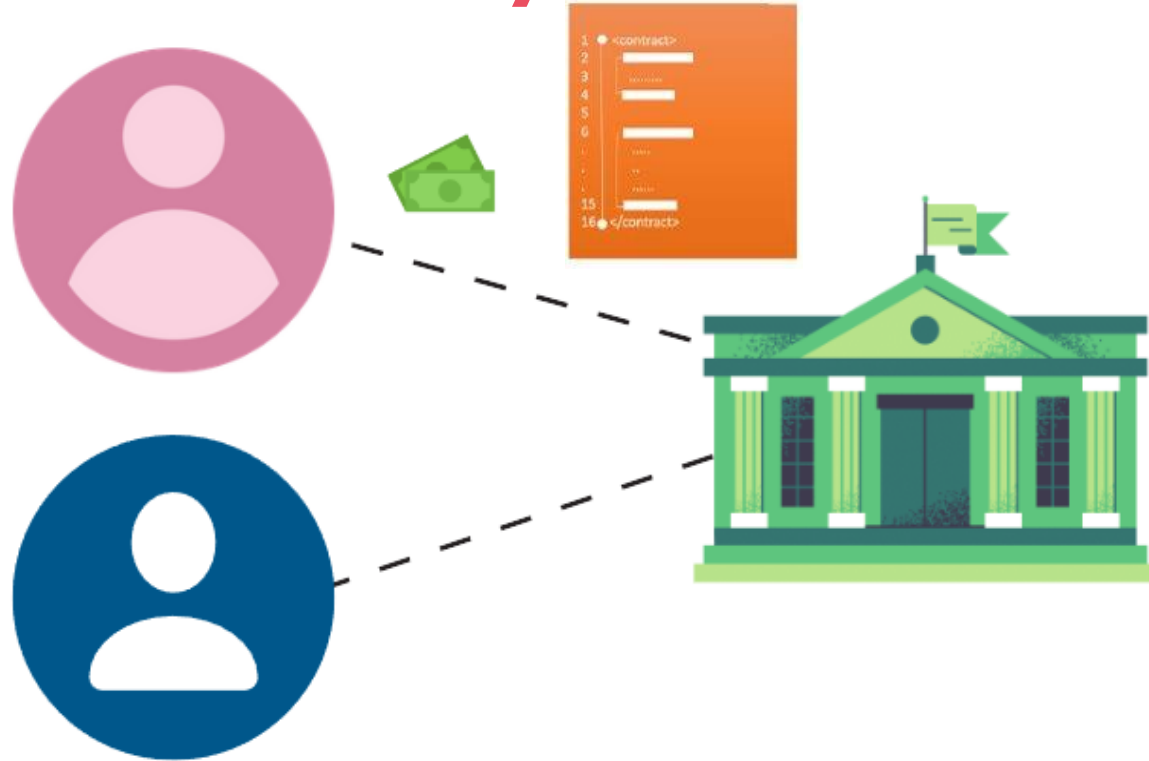
    function mint(address receiver, uint amount) {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        Sent(msg.sender, receiver, amount);
    }
}
```

Smart Contracts



Central Authority



Smart Contracts



Smart Contracts

Mecanismo de consenso

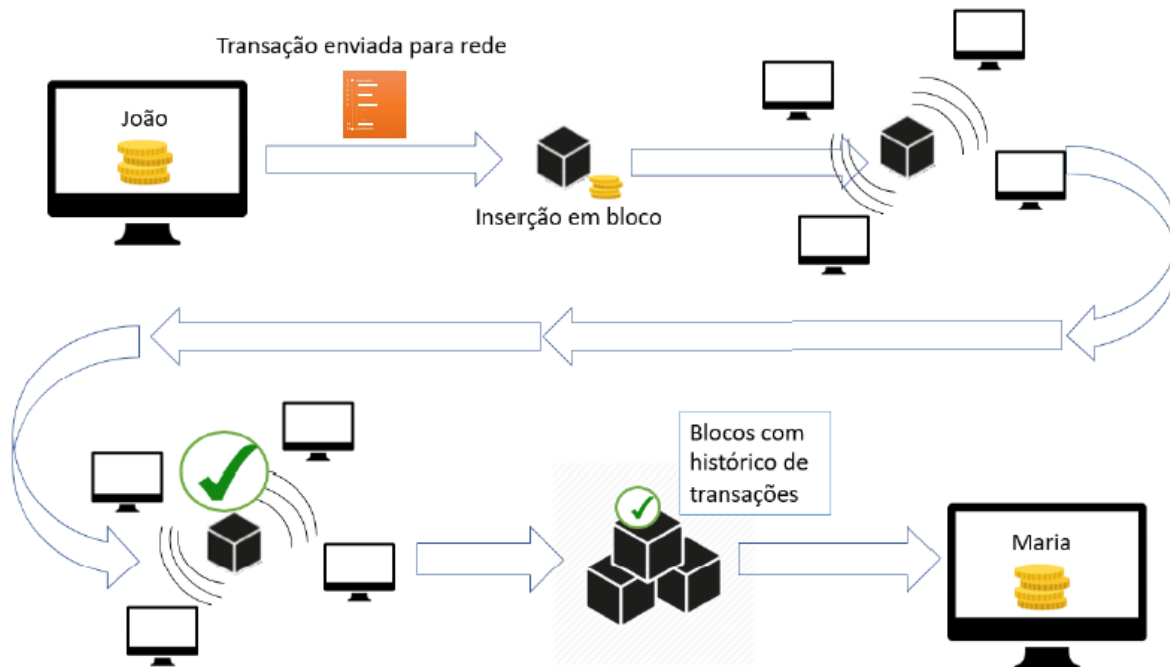


Execução distribuída

Passo a passo

Verificação de
autenticidade

Verificação do
saldo

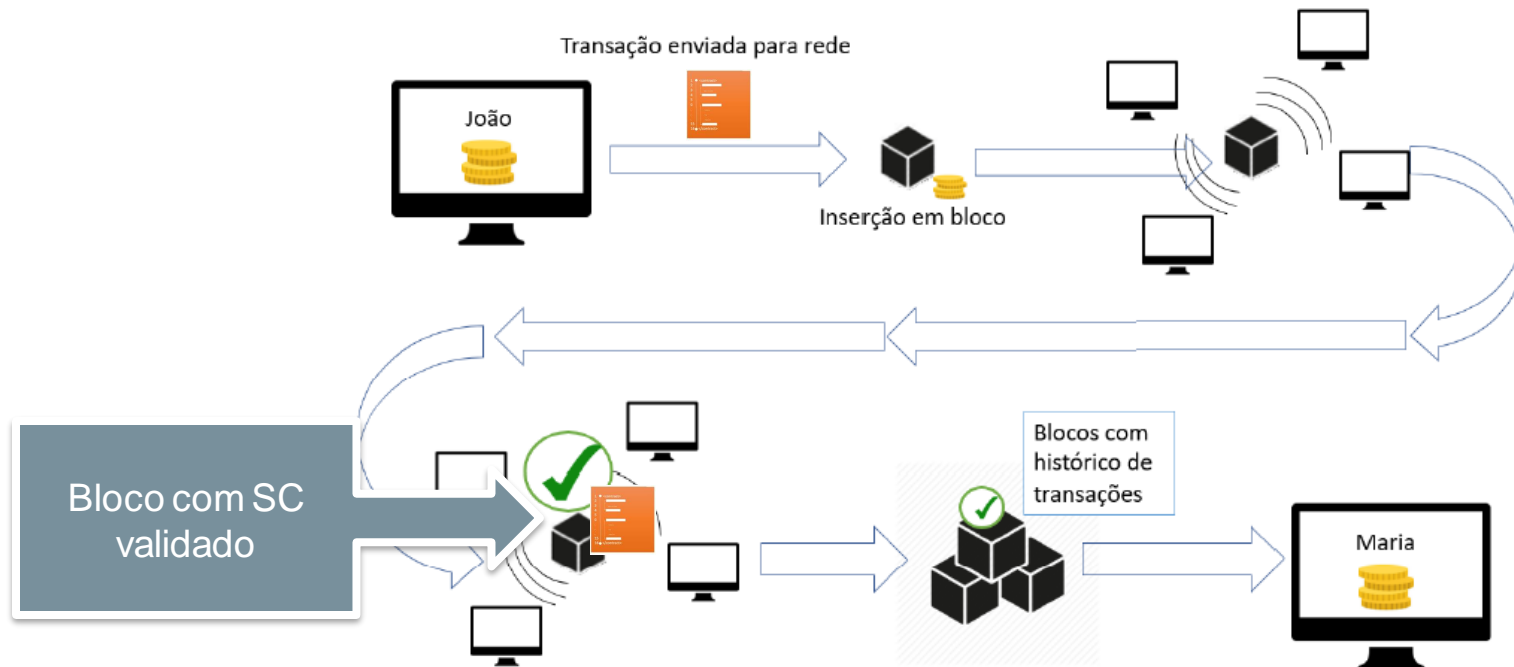


Passo a passo

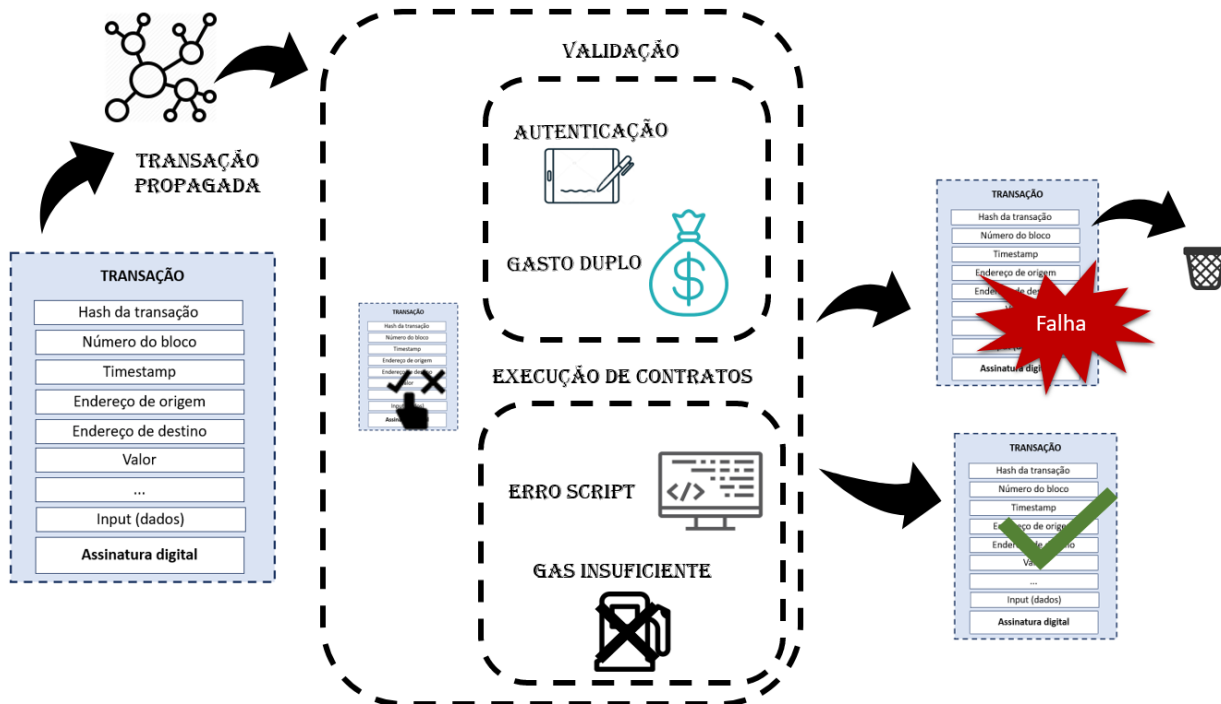
Verificação de
autenticidade

Verificação do
saldo

Mudança de estado



Percurso no Ethereum



Smart Contracts

DELEGATECALL()

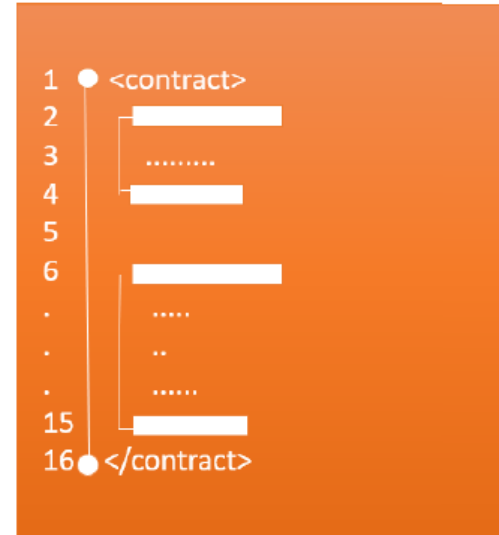
RETURN()

- Contract Creation: **create()**
- Message Call: **call()**

STATICCALL()

REVERT()

CALLCODE()



Smart Contracts

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

BERLIN VERSION 3078285 – 2022-07-13

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

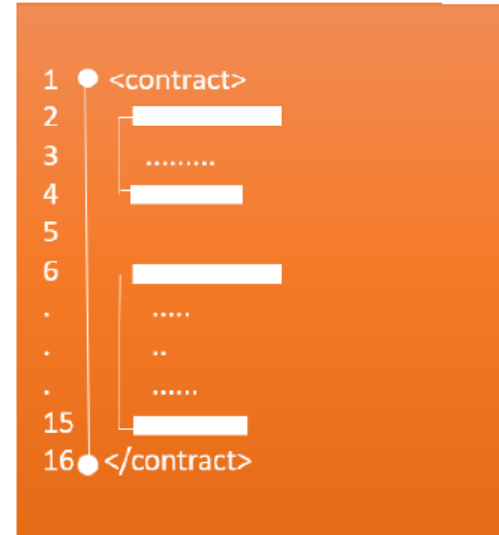
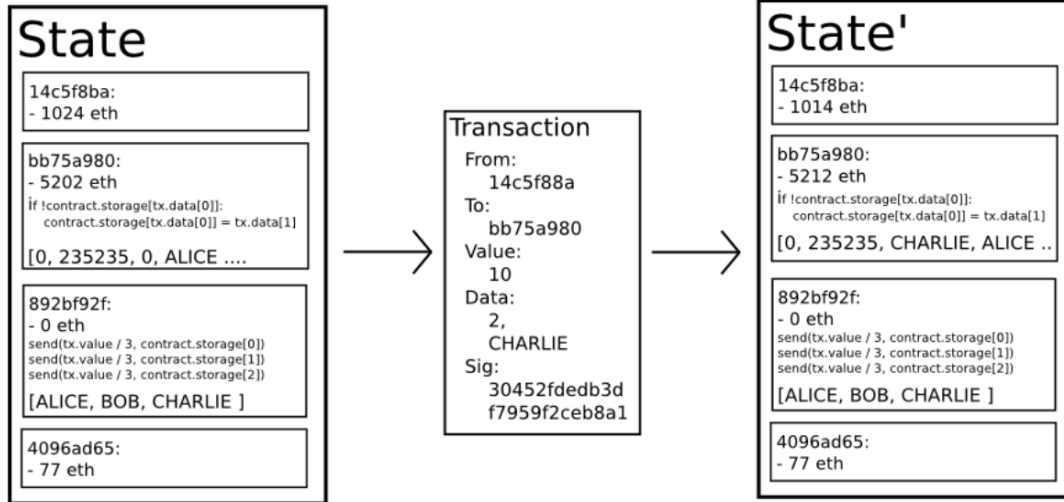
ABSTRACT. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

```

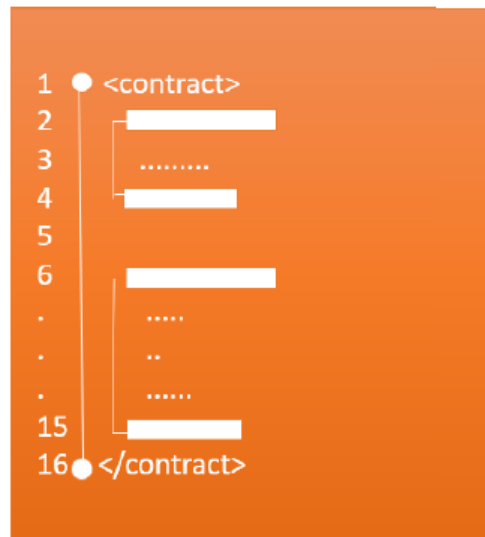
1 ● <contract>
2   ┌───────────────────┐
3   │ .....             │
4   └───────────┐
5                 │
6   ┌───────────────────┐
7   │ .....             │
8   │ ..                │
9   │ .....             │
10  │ .....             │
11  │ .....             │
12  │ .....             │
13  │ .....             │
14  │ .....             │
15 └───────────┐
16 ● </contract>
  
```


Smart Contracts



Vulnerabilidade

- Falhas na codificação
- Informação sensíveis expostas
- Controle de acesso
- Reentrancy
- DoS



Vulnerabilidade

Reentrancy

- Chama função do atacante

ex:

```
function withdraw(uint _amount) external{
    require(balances[msg.sender] >= _amount);
    msg.sender.transfer(_amount);
    balances[msg.sender] -= _amount;
}
```

Etapa 3

Mineração com Uncle Block & PoS – Proof of Stake

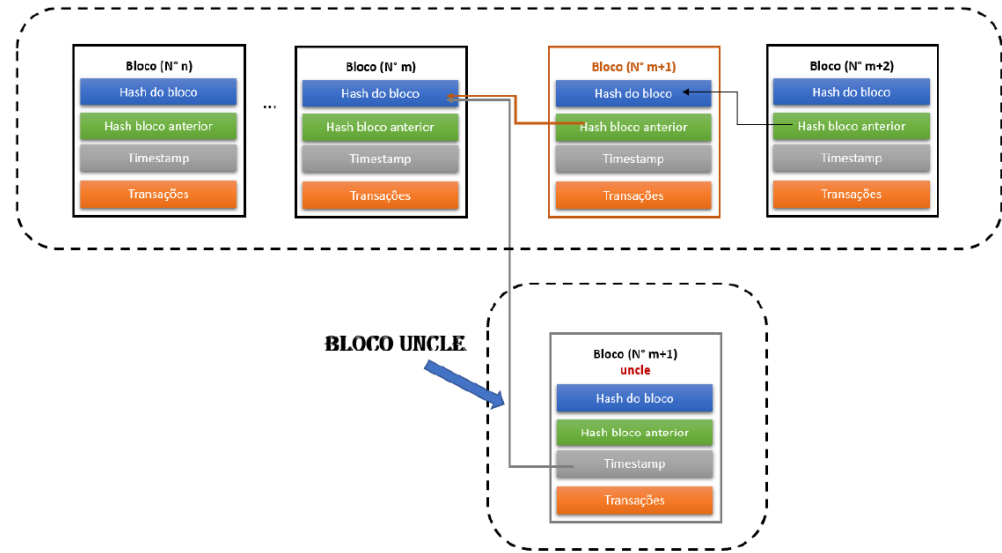
// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

PoW

- Poder computacional
- Puzzles matemáticos
- Gasto energético
- Competição

PoW + Uncle Block

- Poder computacional
- Puzzles matemáticos
- Gasto energético
- Competição



PoS – Proof of Stake

- Mineração virtual
- Não há trabalho computacional
- Requisitos: quantidade de moedas
- Escolha probabilística



PoS – Proof of Stake

- Validação != Mineração
- Permissão (%) -> 1% coins = 1% para validar



PoS – Proof of Stake

Vantagem

- Baixo consumo de energia

Custo reduzido



PoS – Proof of Stake

Requisitos

- Possui balanço positivo
- Certa quantidade de criptomoedas
- Quantidade: Mínimo de mil ether
Vitalik



PoS – Proof of Stake

Consenso por aposta

- Apostam contra o protocolo onde o bloco será minerado
- Recompensa
- Penalidade



PoS – Proof of Stake

Recompensa

- O escolhido pode validar o bloco
- Recebe o valor investido depois da validação do bloco
- Terá fee do bloco após a migração?



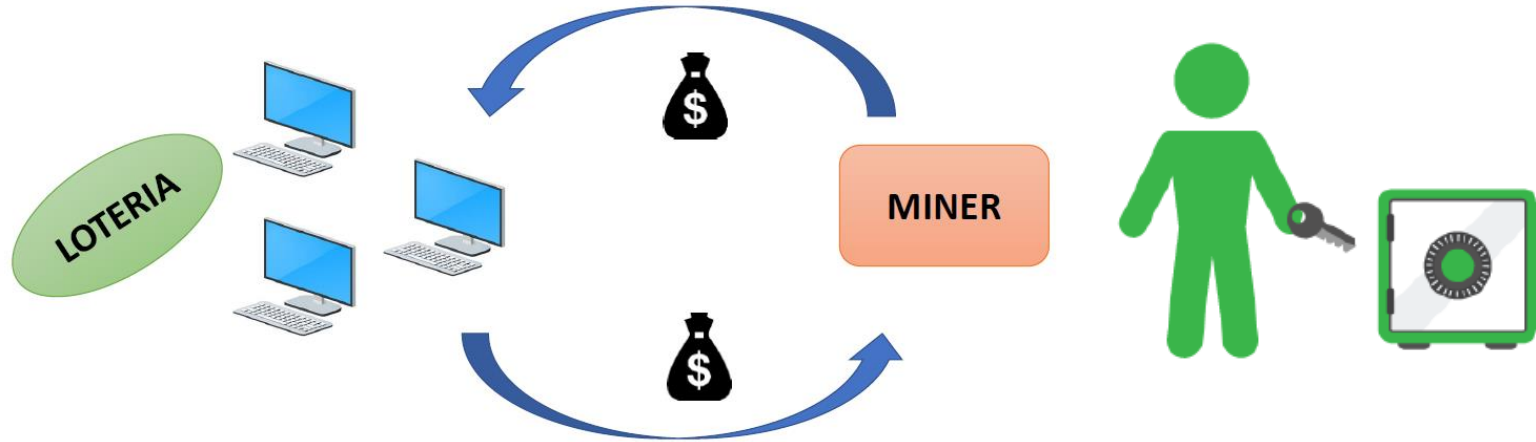
PoS – Proof of Stake

PoS

- Limita o abuso de poder de mineração
- Torna mais difícil ataques de 51%



PoS – Proof of Stake



PoS – Proof of Stake

- **PoW:** Ataque aos mineradores da rede causa danos ou invalida as operações
- **PoS:** Atacar a rede custaria 10 bilhões de dólares. Além disso, perderia o dinheiro no processo



Issues

Problema PoS

- Ricos tomam o poder
- Nós que possuem mais de 51% da rede começam a reescrever a história.



Etapa 4

Transações Internas e Externas

// Fundamentos da Blockchain/Blockchain e Smart Contracts - Ethereum

Transações

Transferência de valores

Criação/Manipulação de
contratos



Transações

Classificação

- Internas
- Externas

Transações

Classificação

- Internas
- Externas

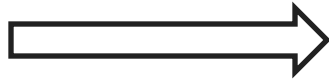


Transações

Sem registro

Classificação

- Internas
- Externas

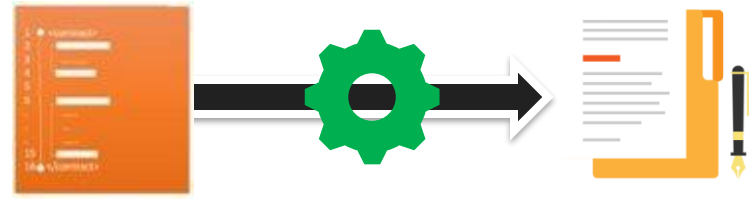


Criação

Acionamento

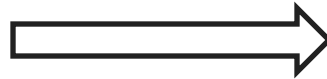


Transações



Classificação

- Internas
- Externas



Etapa 5

Ether e Tokens na Plataforma Ethereum

// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

Ether & Tokens

Ether (ETC)



ethereum

Ether & Tokens

Tokens?

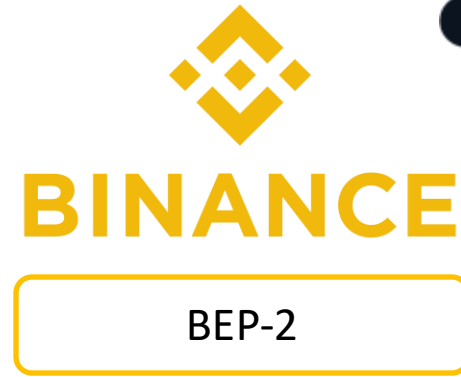
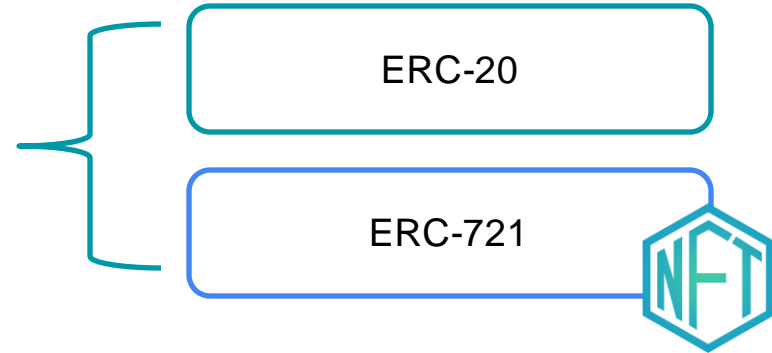
- Ether (native token)
- Assets externos a Blockchain

Ether & Tokens

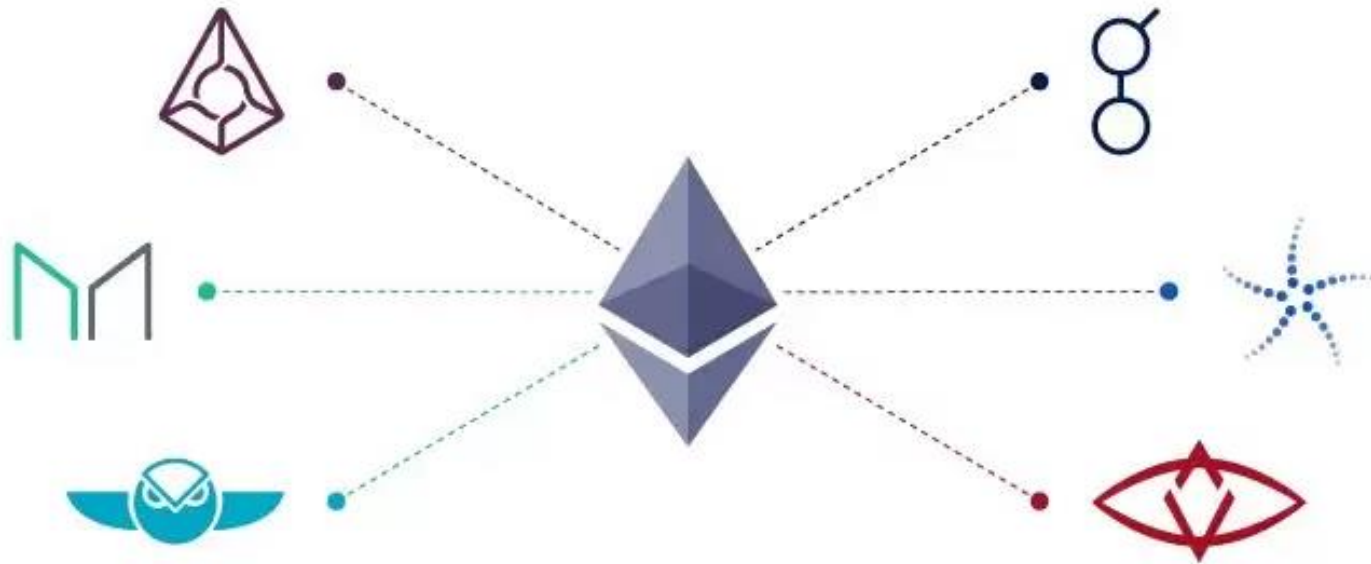


Tokens?

- Ether (native token)
- Assets externos a Blockchain



Ether & Tokens



Fonte: portal do bitcoin

Ether & Tokens



	ethereum	ethereum tokens
concept	smart contracts platform	digital assets on top of ethereum
market cap (as of may 2017)	~\$17 billion	~\$1.5 billion
native currency	ether	augur (rep), golem (gnt), aragon (ant), & many more
founder	vitalik buterin and team	varies by project
release method	presale raised \$18M in bitcoin	typically through crowd sales

Tokens



- Predicted Market
- Criadores: Joey Krug e Jack Peterson
- Trade: valor gatilho para venda

Ethereum token called Reputation (REP)

Tokens Golem

- Criado por Julian Zawistowski
- Venda de poder computacional
- Ideia: supercomputador comum



Golem Network Token (GNT)

Etapa 6

Hard Forks na Plataforma Ethereum

// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

História do Ethereum

Gray Glacier

Jun-30-**2022** 10:54:04 AM +UTC

 Block number: [15,050,000](#)

ETH price: \$1,069 USD

[ethereum.org on waybackmachine](#)

2022

<https://ethereum.org/en/history/>

História do Ethereum

Arrow Glacier

Dec-09-2021 07:55:23 PM +UTC

 Block number: [13,773,000](#)

ETH price: \$4111 USD

[ethereum.org on waybackmachine](#)

2021

<https://ethereum.org/en/history/>

História do Ethereum

Arrow Glacier

Dec-09-2021 07:55:23 PM +UTC

 Block number: [13,773,000](#)

ETH price: \$4111 USD

[ethereum.org on waybackmachine](#)

Altair

London

Berlin

2021

<https://ethereum.org/en/history/>

Início do Ethereum

- Frontier – bloco zero
- Frontier thawing – bloco 200.000
- DAO fork – bloco 1.920.00 (**2016**)



2015

<https://ethereum.org/en/history/>

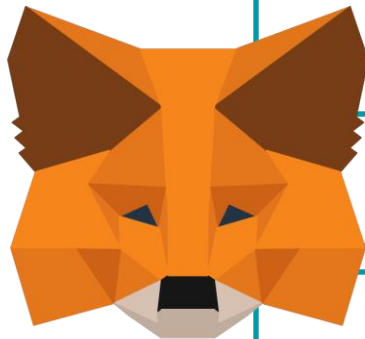
Etapa 7

O que é a Carteira Metamask?

// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

Metamask

- Carteira Digital
- Popularidade
- Controle financeiro
- Hot wallet



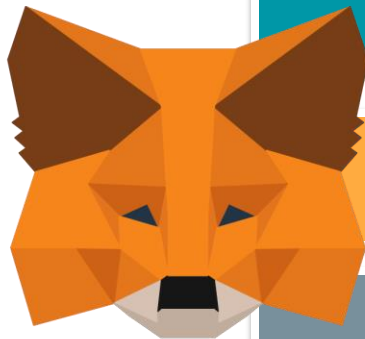
Interface simplificada

18 idiomas

Backup das carteiras

Metamask

- Carteira Digital
- Popularidade
- Controle financeiro



Tokens diferentes

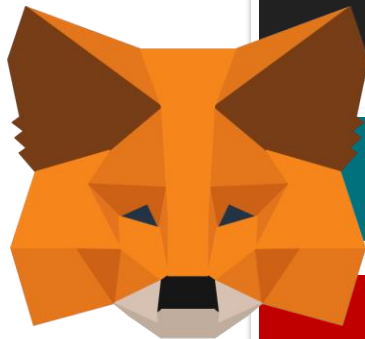
Integração com dApps

Bloqueio de phishing

Plataforma Gratuita

Metamask

- Carteira Digital
- Popularidade
- Controle financeiro



Mobile & Web

opensource

Ter ether

Gerenciamento de tokens e conta Ethereum

Etapa 8

Criando um carteira na rede do Ethereum

// Fundamentos da Blockchain/Blockchain e Smart Contracts - Ethereum

Criando sua 1ª carteira

Usaremos a
Metamesk para criar
nossa primeira
carteira conectada a
Ethereum



METAMASK

Features ▾

Support ▾

About ▾

Build ▾

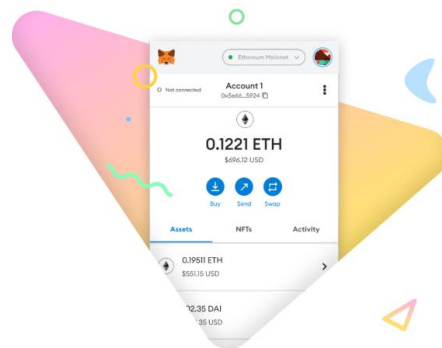
Download



A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 30 million users worldwide.

Download for




Etapa 9

Analizando as transações pelo etherscan.io

// Fundamentos da Blockchain/Blockchain e Smart
Contracts - Ethereum

Explorando o Etherscan.io


HomeBlockchainTokensResourcesMoreSign In


The Ethereum Blockchain Explorer


All Filters

Search by Address / Txn Hash / Block / Token / Ens


Q


Sponsored:  Get your first free 200 \$TFS. [Register, play, stake and get profit!](#)

 **ETHER PRICE**
\$1,521.14 @ 0.06935 BTC (+4.61%)

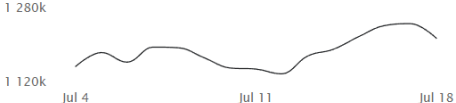
 **TRANSACTIONS**
1,645.06 M (13.9 TPS)

MED GAS PRICE
19 Gwei (\$0.61)

 **MARKET CAP**
\$182,136,571,069.00

 **DIFFICULTY**
11,822.64 TH

HASH RATE
915,473.77 GH/s

ETHEREUM TRANSACTION HISTORY IN 14 DAYS


Latest Blocks

Bk	15171377	Miner: 2Miners: PPLNS	2,04251 Eth
	12 secs ago	149 txns in 16 secs	
Bk	15171376	Miner: Hive	
	28 secs ago	101 txns in 16 secs	

Latest Transactions

Tx	0xe7c6a9aaa39e...	From 0xdbd19cf006f6f1e6e15...	0 Eth
	12 secs ago	To 0xdac17f958d2ee523a2...	
		258b640...	0.00656 Eth
		4779...	

This website uses cookies to improve your experience and has an updated [Privacy Policy](#). [Got It](#)

Etapa 10

Entendendo um pouco mais da rede Ethereum

// Fundamentos da Blockchain/Blockchain e Smart Contracts - Ethereum

Caracterização da rede

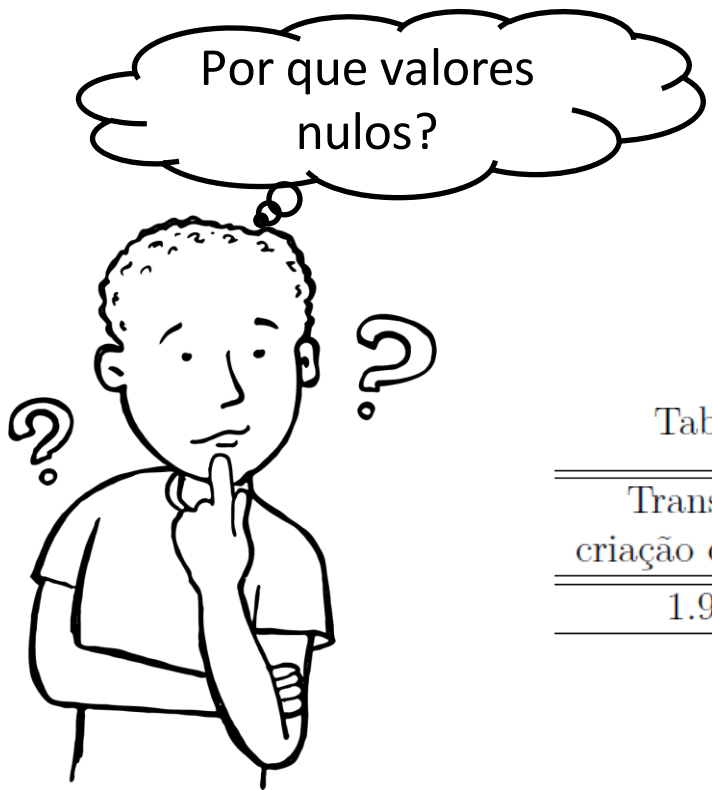
Transações externas

2015 - ~2018

Tabela 1 – Transações do Ethereum.

Transações com transferência de fundos	Transações com valor de zero ether
185.305.549	113.928.481

Caracterização da rede



Por que valores
nulos?

Transações externas

2015 - ~2018

Tabela 2 – Tipos de transações com valores nulos.

Transações de criação de contratos	Outras transações	Transações de transferência de tokens
1.916.517	53.922.826	60.005.655

Caracterização da rede



Por que valores
nulos?


Transações externas

2015 - ~2018

Tabela 3 – Número total de transações em cada ano, transações com valores nulos e porcentagem dessas transações nulas no total de transações.

Período	Total de transações	Transações com valores nulos	Porcentagem
2015	266.853	60.029	22.50%
2016	13.662.805	1.506.201	11.02%
2017	103.003.372	33.573.437	32.59%
2018	182.301.000	78.788.814	43.22%
Total	299.234.030	113.928.481	38.07%

Caracterização da rede



Por que valores
nulos?

Transações externas

2015 - ~2018

Tabela 4 – Número médio e máximo de transações por bloco em cada ano.

Período	Média de transações	Máximo de transações
2015	2	151
2016	4	228
2017	25	381
2018	54	381

Caracterização da rede



Figura 20 – Endereços ativos – perspectiva temporal.

Caracterização da rede

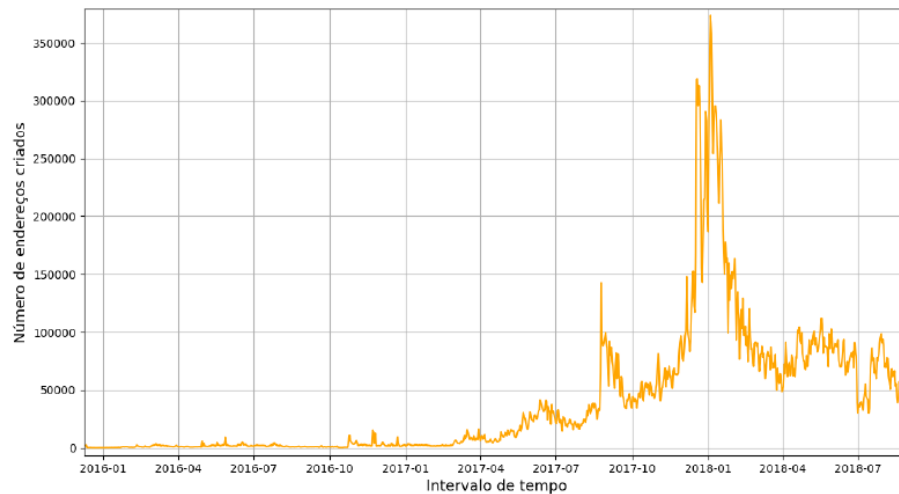


Figura 21 – Endereços criados – perspectiva temporal.

Caracterização

O Bitcoin
influencia?

Correlação: 0,98



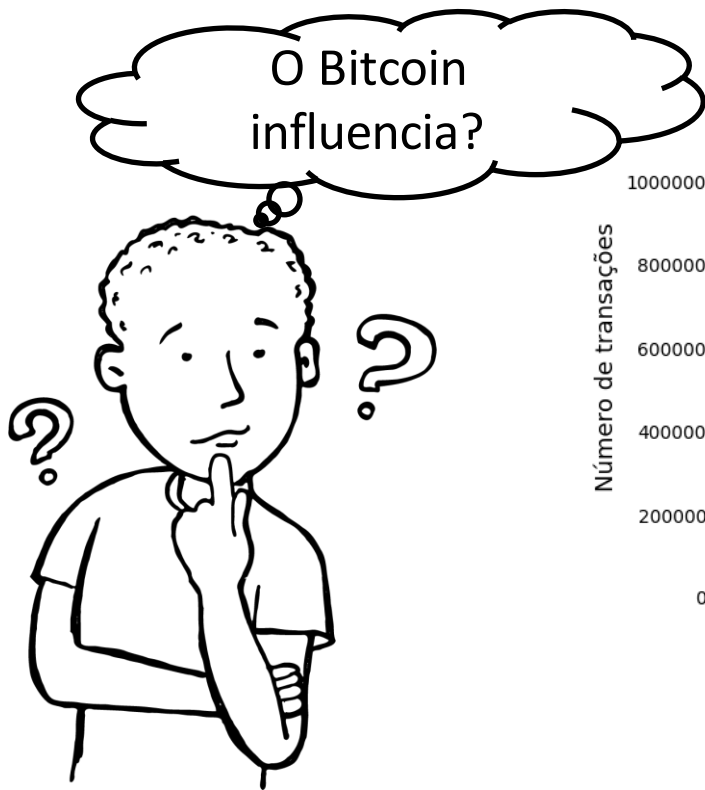
Figura 24 – Cotação do ether (em USD) no período de análise.



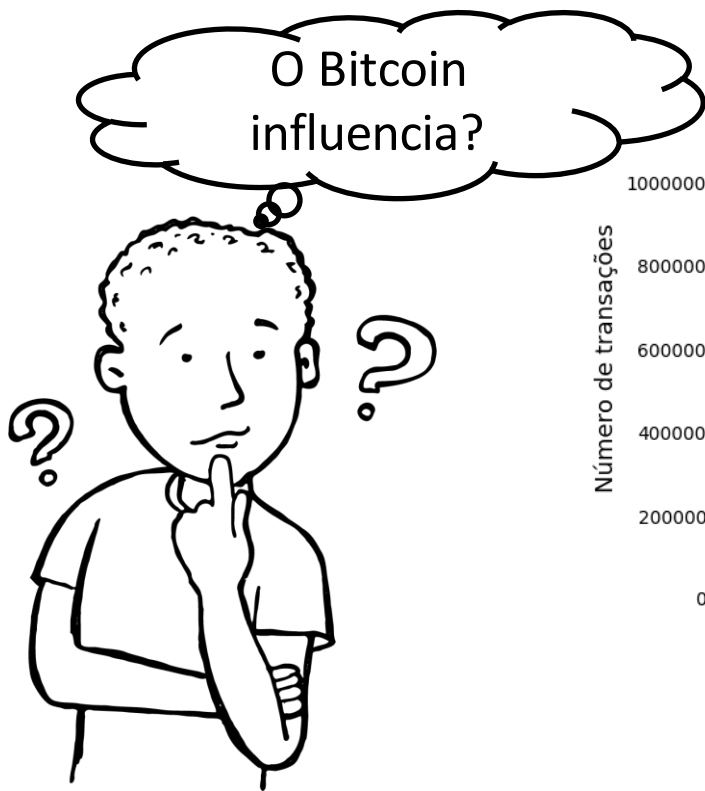
Figura 25 – Cotação (USD) Bitcoin no período de análise.



Caracterização

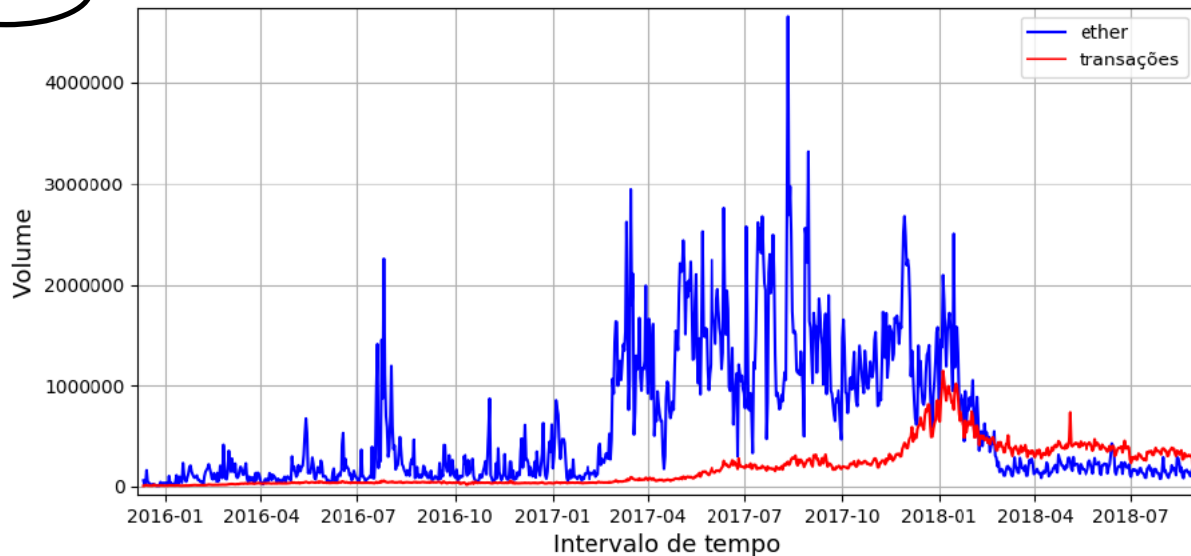


Caracterização



Caracterização

O Bitcoin
influencia?



Dúvidas?

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



Links Úteis

- **Referências:**

- [Yellow Paper - ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BERLIN VERSION 3078285– 2022-07-13](#)
- [White paper: A Next-Generation Smart Contract and Decentralized Application Platform \(Original whitepaper\)](#)
- [White paper Ethereum online](#)

Plataforma de scan de transações/blocos [Etherscan.io](#)

Para saber mais

<https://ethereum.org/pt-br/developers/docs/smart-contracts/>

<https://ethereum.org/en/developers/docs/accounts/>

<https://etherscan.io/>

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

<https://portaldobitcoin.uol.com.br/o-passo-a-passo-para-criar-e-usar-uma-carteira-metamask/>

<https://metamask.io/>

Para saber mais

<https://solidity-portuguese.readthedocs.io/pt/latest/introduction-to-smart-contracts.html>

<https://github.com/ethereum/wiki/wiki/%5BPortuguese%5D-White-Paper/>

<https://cointelegraph.com.br/news/the-vulnerabilities-of-smart-contracts>

<https://www.mentebinaria.com.br/artigos/seguran%C3%A7a-web3-vulnerabilidades-em-smart-contracts-r87/>

<https://ethereum.org/en/history/>

<https://portaldobitcoin.uol.com.br/tudo-sobre-ethereum/>

Para saber mais

<https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/#:~:text=Tokens%20often%20represent%20assets%20and,smart%20contract%20standard%2Dcompliant%20token>

<https://blog.coinbase.com/a-beginners-guide-to-ethereum-tokens-fbd5611fe30b>

<https://blog.b2bstack.com.br/o-que-e-metamask/>