

# Introdução às Tecnologias Blockchain

## Visão Geral

---

Prof. Rogério Aparecido Gonçalves<sup>1</sup>  
[rogerioag@utfpr.edu.br](mailto:rogerioag@utfpr.edu.br)

<sup>1</sup>Universidade Tecnológica Federal do Paraná (UTFPR)  
Departamento de Computação (DACOM)  
Campo Mourão - Paraná - Brasil

Semana de Informática (SEINFO 2023)  
**SEINFO2023**  
Introdução às Tecnologia Blockchain



# Agenda i

1. Introdução
2. Conceitos e Fundamentos de Blockchain
3. Bitcoin
4. Contratos Inteligentes
5. Ethereum
6. Prática: Instalando o Cliente Ethereum: Geth
7. Prática: Criando uma Rede Ethereum Privada

# Agenda ii

- 
- 8. Prática: Instalando o Solidity
  - 9. Prática: Introdução ao Web3
  - 10. Prática: Introdução à Tokenização
  - 11. Referências

# Introdução

---



**Figura 1:** Rogério Gonçalves  
(RAG)

Doutor em Ciência da Computação, é professor na UTFPR - Campus Campo Mourão. É revisor do journal Springer Computing e de algumas conferências.

**Interesse em:** Arquitetura de Computadores, Computação Paralela, Computação Heterogênea, Compiladores e Runtimes e Tecnologias Blockchain.

## Ementa

Introdução às Tecnologias Blockchain. Smart Contracts. Ethereum e Solidity. Ferramentas de Desenvolvimento e Frameworks. Redes de Testes e Clientes. Introdução a Web3. Tokenização.

## Pré-requisitos

Saber um pouco de Java Script.

# Objetivos

- Apresentação de uma Visão Geral sobre o Ecossistema de Tecnologias relacionadas a **Blockchain**. Surgimento e contexto histórico vinculado ao *Bitcoin*. Mas o foco principal está na rede **Ethereum** e componentes do seu Ecossistema. Falaremos um pouco sobre a \_\_Ethereum Virtual Machine (EVM)\_\_ e Contratos Nativos. Além disso, uma perspectiva do usuário é apresentada, mostrando a estrutura dos blocos do *blockchain* da *Ethereum*, *Wallets* e softwares clientes, nós e mineradores, ferramentas e **APIs**, protocolos e Linguagens de Programação Suportados.

# Conceitos e Fundamentos de Blockchain

---

# Interesse no termo “blockchain” ao longo do tempo

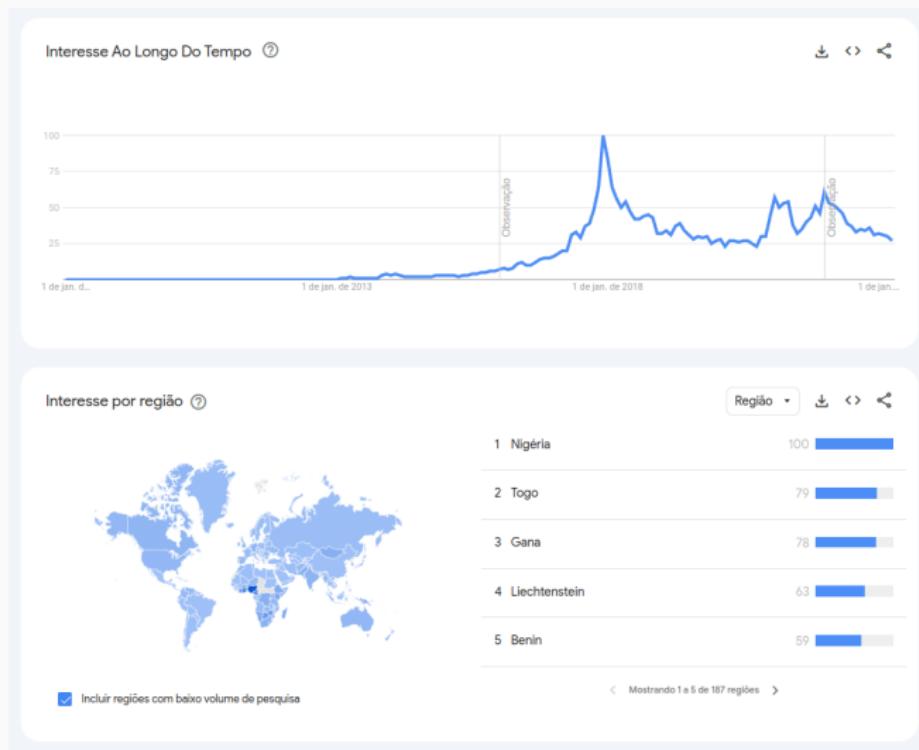


Figura 2: Pesquisas sobre o termo “blockchain” Fonte: Google Trends

# Como um Blockchain funciona

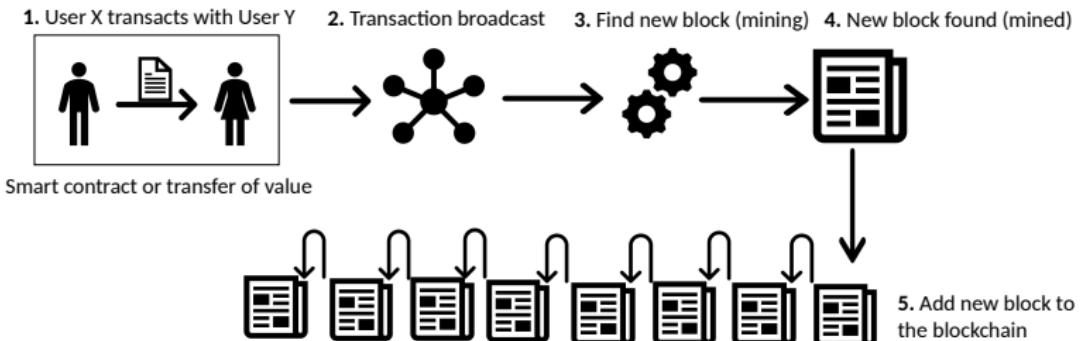


Figura 3: Funcionamento de um Blockchain

# Definição de Blockchain

## Definição de Layman

*Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.*

## Definição Técnica

*Blockchain is a peer-to-peer distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.*

## Definição de Blockchain ii

---

- *Peer-to-peer*
- *Distributed Ledger* (livro-razão distribuído)
- *Criptograficamente Seguro*
- *Append Only* (Permitido somente anexar novos blocos)
- Atualizável via consenso dos pares.

# Como a Tecnologia Blockchain foi desenvolvida i

1950s – Hash functions

1970s – Merkle trees - hashes in a tree structure

1970s *continued* – Research in distributed systems, consensus, state machine replication

1980s – Hash chains for secure logins

1990s – *e-Cash for e-payments*

1991 – Secure timestamping of digital documents.

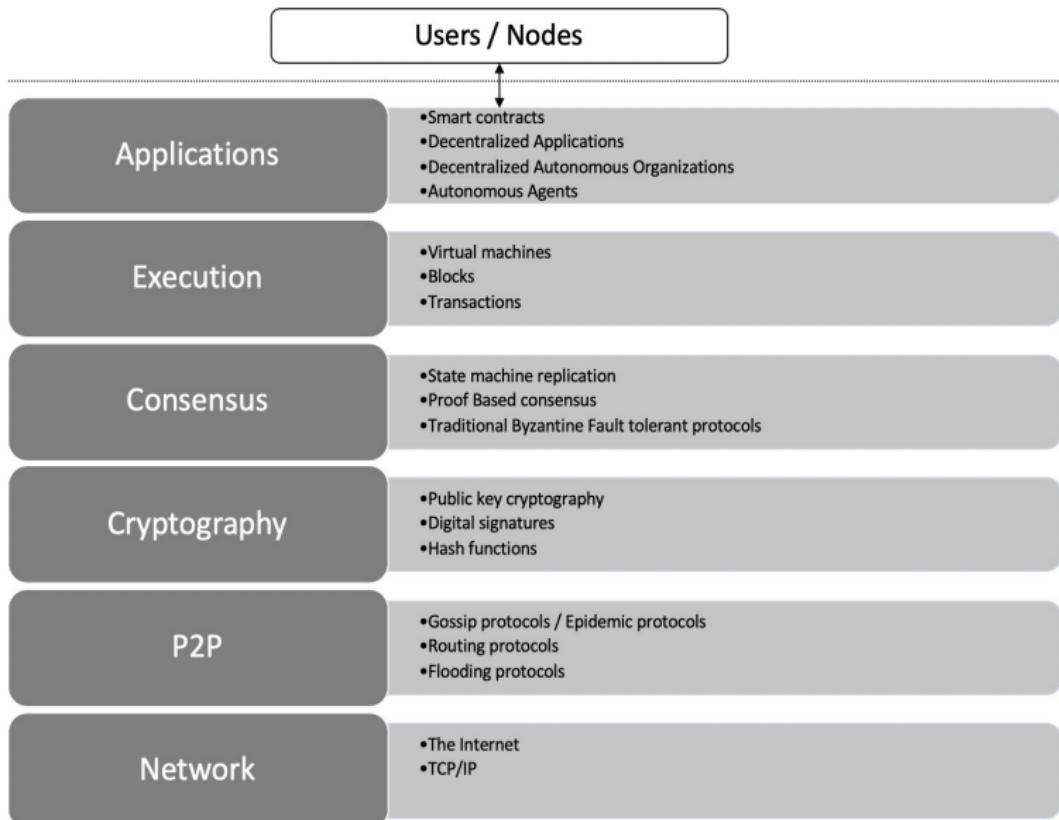
1992 – Hashcash idea to combat junk emails

1994 – S/KEY application for Unix login.

1997/2002 – *Hashcash*

2008/2009 – Bitcoin (the first blockchain)

# Visão Arquitetural de um Blockchain



# Estrutura Genérica de um Blockchain

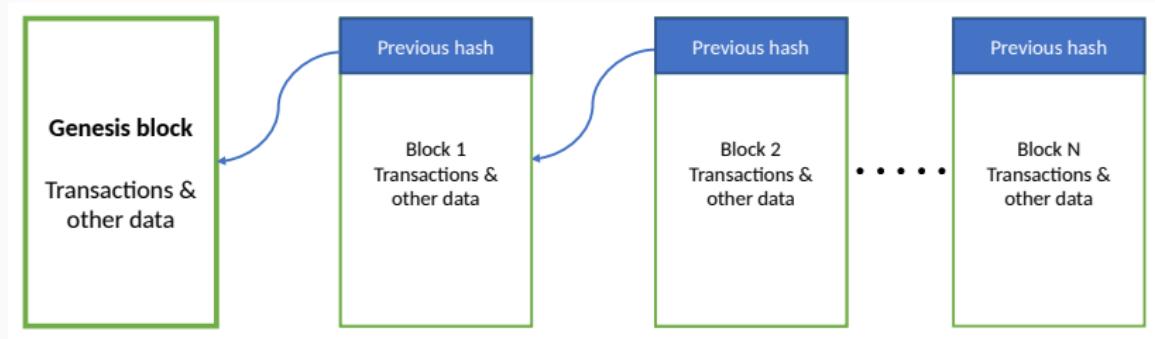


Figura 4: Estrutura Genérica de um Blockchain

# Estrutura Genérica de um bloco i

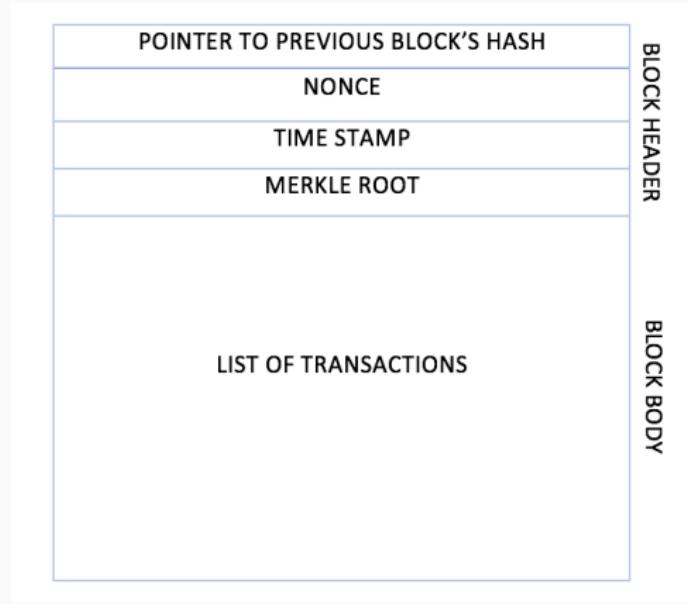


Figura 5: Estrutura de um Bloco

# Elementos Genéricos de um Blockchain

- Endereços
- Contas
- Transações
- Blocos
- Redes *Peer-to-peer*
- Scripting ou Linguagens de Programação
- Virtual machines
- Máquinas de Estado
- Nós (nodes)
- Contratos Inteligentes (*Smart contracts*)

## Leitura Recomendada

### Capítulo 1: Blockchain 101

Livro: IMRAN BASHIR. Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

# Bitcoin

---

- Surgiu em 2008/2009, sendo a primeira rede *Blockchain*.
- Rede voltada para a Criptomoeda – **Bitcoin (BTC)**.

- Passos de como enviar e receber pagamentos:
  - A transação começa com um remetente assinando a transação com sua chave privada.
  - A transação é serializada para que possa ser transmitida pela rede.
  - A transação é transmitida para a rede.
  - Mineradores que escutam transações pegam a transação.
  - A transação é verificada quanto à sua legitimidade pelos mineradores.
  - A transação é adicionada ao bloco candidato/proposto para mineração.
  - Uma vez minerado, o resultado é transmitido para todos os nós da rede *Bitcoin*.
  - Normalmente, neste momento, os usuários aguardam até seis confirmações para serem recebidas antes que uma transação seja considerada final; no entanto, uma transação pode ser considerada final na etapa anterior.

- As confirmações servem como um mecanismo adicional para garantir que haja probabilidade muito baixa de uma transação ser revertida, mas, caso contrário, uma vez que um bloco minerado seja finalizado e anunciado, as transações dentro desse bloco serão finais nesse ponto.

# Chaves Criptográficas i

- Private keys in Bitcoin
  - Private keys are used to digitally sign the transactions, proving ownership of the bitcoins.
- Public keys in Bitcoin
  - Public keys are used by nodes to verify that the transaction has indeed been signed with the corresponding private key.
- Addresses in Bitcoin
  - A Bitcoin address is created by taking the corresponding public key of a private key and hashing it twice, first with the SHA256 algorithm and then with RIPEMD160.



QR code of the Bitcoin address  
1ANAgGG8bikEv2fYsTBnRUmxB7QUcK58wt



From [bitaddress.org](http://bitaddress.org),  
a private key and Bitcoin address  
in a paper wallet

# Script i

---

- Simple stack-based language used to describe how bitcoins can be spent and transferred
- Evaluated from left to right using a Last in, First Out (LIFO) stack
- Composed of two components: elements and operations.
- Scripts use various operations (opcodes) to define their operations.

- Here are some examples of a few useful opcodes used in the Script language on the Bitcoin blockchain.

## Opcodes ii

Opcode	Description
OP_CHECKSIG	This takes a public key and signature and validates the signature of the hash of the transaction. If it matches, then TRUE is pushed onto the stack; otherwise, FALSE is pushed.
OP_EQUAL	This returns 1 if the inputs are exactly equal; otherwise, 0 is returned.
OP_DUP	This duplicates the top item in the stack.
OP_HASH160	The input is hashed twice, first with SHA-256 and then with RIPEMD-160.
OP_VERIFY	This marks the transaction as invalid if the top stack value is not true.
OP_EQUALVERIFY	This is the same as OP_EQUAL, but it runs OP_VERIFY afterward.
OP_CHECKMULTISIG	This instruction takes the first signature and compares it against each public key until a match is found and repeats this process until all signatures are checked. If all signatures turn out to be valid, then a value of 1 is returned as a result; otherwise, 0 is returned.
OP_HASH256	The input is hashed twice with SHA-256.
OP_MAX	This returns the larger value of two inputs.

# Blocos i

- A estrutura de um Bloco Bitcoin é mostrado na tabela:

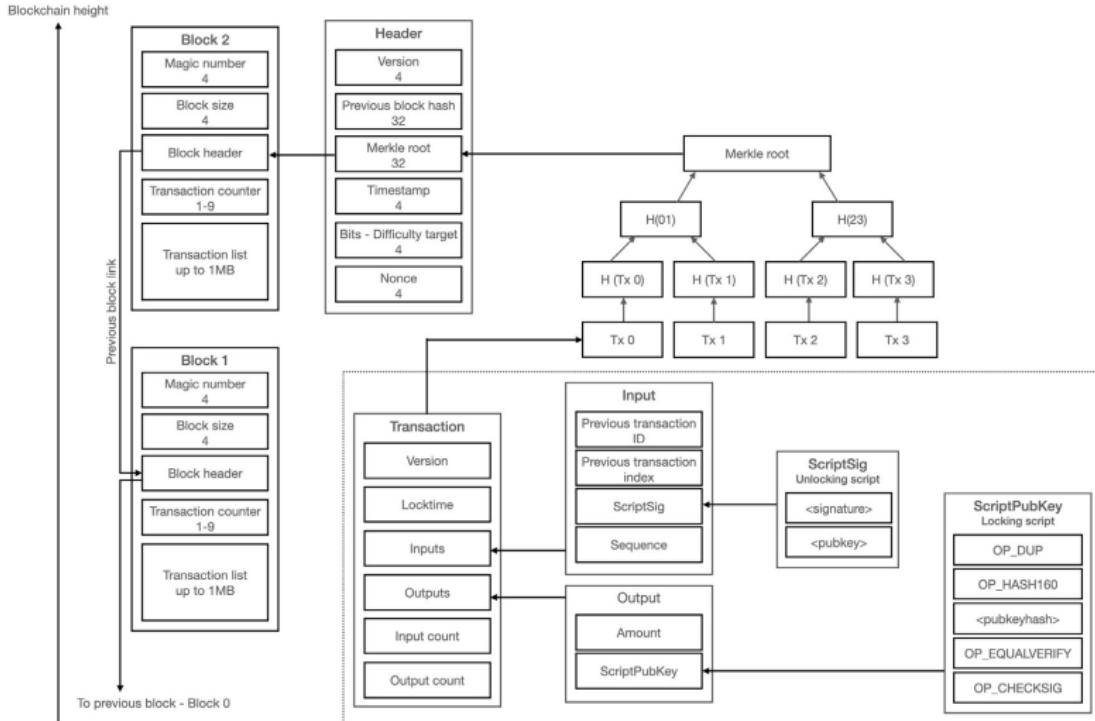
Field	Size	Description
Block size	4 bytes	The size of the block.
Block header	80 bytes	This includes fields from the block header described in the next section.
Transaction counter	Variable	The field contains the total number of transactions in the block, including the coinbase transaction. Size ranges from 1-9 bytes.
Transactions	Variable	All transactions in the block.

# Blocos ii

- A estrutura do cabeçalho de um bloco:

Field	Size	Description
Version	4 bytes	The block version number that dictates the block validation rules to follow.
Previous block's header hash	32 bytes	This is a double SHA256 hash of the previous block's header.
Merkle root hash	32 bytes	This is a double SHA256 hash of the Merkle tree of all transactions included in the block.
Timestamp	4 bytes	This field contains the approximate creation time of the block in Unix-epoch time format. More precisely, this is the time when the miner started hashing the header (the time from the miner's location).
Difficulty target	4 bytes	This is the current difficulty target of the network/block.
Nonce	4 bytes	This is an arbitrary number that miners change repeatedly to produce a hash that is lower than the difficulty target.

# Uma Visualização da Blockchain do Bitcoin



## Bloco Genesis

O Bloco Genesis ou bloco #0 foi *hardcoded* (codificado) por suas características especiais: ele é o único que não aponta para nenhum bloco anterior. No seu *hash* foi encriptado o bloco junto com a mensagem *“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”*, manchete do jornal naquele dia. Além de servir como prova datada, a manchete escolhida representa justamente uma crítica ao sistema bancário.

Bloco Genesis ii

# THE TIMES



Saturday January 3 2009 timesonline.co.uk No 6933 £1.50



Max SC, min-SC

## Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today! [Purchase Inside](#)

### Israel prepares to send tanks and troops into Gaza



Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of strikes. [News, page 3](#)

## Chancellor on brink of second bailout for banks

### Billions may be needed as lending squeeze tightens

Frances Elman, Economic Political Editor  
Gary Oldman, *Guerrilla Kitchen*

Allan's Barking has been forced to make do with a £100-a-month pension while he waits to pay off billions more in debts. The 60-year-old pensioner has lost his job twice since the credit crunch began, but has held on to his home by offering his pensioner status to companies offering him cheaper rates instead of the "new assets". The Times has learned...  
The Bank of England revealed yesterday that, despite economic pressure, the banks continued lending to the financial sector at a rate slightly higher than before the credit crisis.

The Bank is required to take out money from its reserves to meet the new rules. It will have to sell off £100bn worth of assets to do so. Despite the new rules, the Bank said it would still be creating credit to support the economy.

But the latest figures from the Bank of England show that the lending squeeze has got worse. In December, the amount of loans to the private sector fell by £1.5bn to £100 billion.

That is double the previous month's fall and marks the third consecutive month of falls. The latest figures also show that the number of people unable to get a loan has risen sharply.

It is not clear whether the new rules will be effective or if they will simply encourage banks to lend less. Some experts believe that the new rules will encourage banks to lend less.

The Chancellor of the Exchequer, Gordon Brown, has said that the new rules will help to restore lending levels. However, the Treasury has been

urging the Bank of England to take more steps to encourage lending, such as cutting interest rates further.

The Treasury would take half of the cost of bailing out the banks and the other half would come from the government bonds. The new scheme would be aimed at helping the economy through the creation of a stable environment for lending.

The idea was first put forward by Henry Paulson, the US Treasury secretary, in October last year. It was designed to help the US economy by buying

shares in failing companies.

Continued on page 4, [Economy, page 4](#)

### Michael Sheen Frost, Nixon and me

Magazine



### Working mums So that's how she does it

BobyniKo!



### Detox in style The best spas on the planet

New!



### Salmon Rushdie I Won't Marry Again

Page 22, 23



### Great Killing? Guide to the FA Cup Third Round

Sport



**Fonte:** <https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp>

# Bloco Genesis iii

```
/**  
 * Build the genesis block. Note that the output of its generation  
 * transaction cannot be spent since it did not originally exist in the  
 * database.  
 *  
 * CBlock(hash=0000000000019d6, ver=1, hashPrevBlock=0000000000000000, hashMerkleRoot=  
 * CTxTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)  
 * CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030  
 * CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)  
 * vMerkleTree: 4a5e1e  
 */  
  
static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int  
const CAmount& genesisReward)  
{  
    const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second b  
    const CScript genesisOutputScript = CScript() << ParseHex("04678afdb0fe5548271967  
    return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits  
}
```

# A carteira de Satoshi

- Carteira: [1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#)

The screenshot shows the Blockchain.com Bitcoin Explorer interface for the address [1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#). The address has transacted 3,455 times and received a total of 88.5544405 BTC (\$1,286,882.09) with a current value of \$1,286,882.09.

**Address**

Format	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Transactions	3,455
Total Received	88.5544405 BTC
Total Sent	0.0000000 BTC
Final Balance	88.5544405 BTC

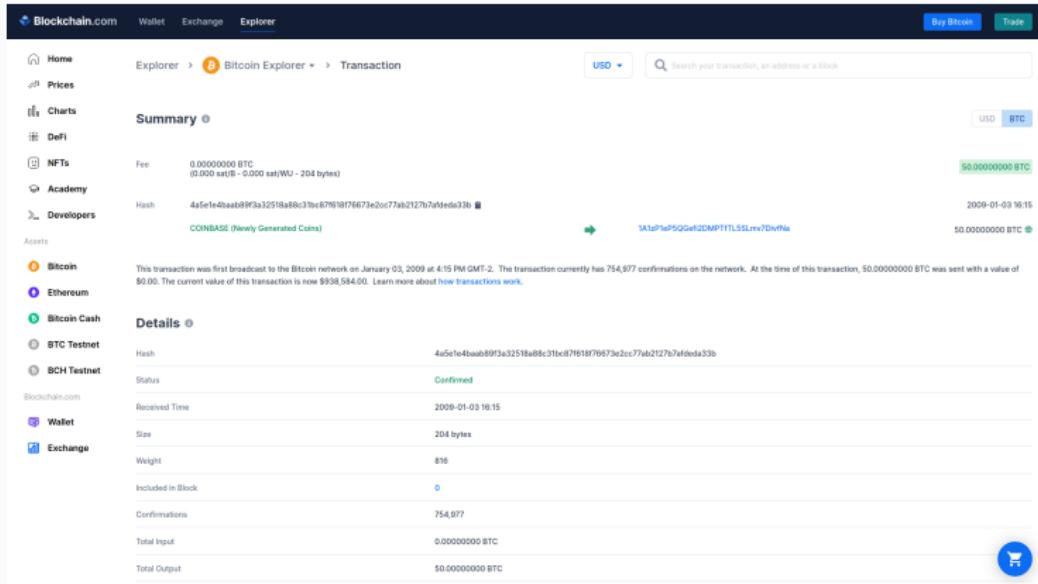
**Transactions**

Date	Fee	Hash	From	To	Value
2022-09-19 11:43	0.00005788 BTC (9.807 sat/B - 4160 sat/WU - 500 bytes) (16.626 sat/vByte - 348 virtual bytes)	bb7620043cc1b054adde33bf09bb7b689553931e52fb99tb9785e243d94055			+0.00123604 BTC
	0.00000144 BTC (0.640 sat/B - 0.251 sat/WU - 225 bytes) (1.000 sat/vByte - 144 virtual bytes)	3GRmWBLJBxJwNz2G5Tos2bCmsRqj6fGD 394KacQFmCs2oCq3yDzvBzA2wYhrW7Q 34dYmHgtsqjCUtKox7u5yNadX2zyfrw	0.00688038 BTC	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa	0.00123604 BTC
			0.00261901 BTC	b1cg3nwyRedvLqkHf9cQy53sgu4dgstgn@h2	0.01000609 BTC
			0.00180000 BTC		

Figura 6: [1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa](#)

# A carteira de Satoshi ii

- Essa primeira transação foi incluída no bloco #0, sob o hash  
`4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b.`



The screenshot shows the Blockchain.com Explorer interface. The left sidebar lists various blockchain networks: Home, Prices, Charts, DeFi, NFTs, Academy, Developers, Assets, Bitcoin, Ethereum, Bitcoin Cash, BTC Testnet, BCH Testnet, Wallet, and Exchange. The main content area is titled "Summary" and shows the following details for the transaction:

- Fee:** 0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 204 bytes)
- Hash:** 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
- Recipient:** 1A1dp1eP5QGeL2DMP7fTL55Lmz7DvNa
- Value:** 50.00000000 BTC
- Date:** 2009-01-03 16:15
- Details:** This transaction was first broadcast to the Bitcoin network on January 03, 2009 at 4:15 PM GMT-2. The transaction currently has 754,977 confirmations on the network. At the time of this transaction, 50.00000000 BTC was sent with a value of \$0.00. The current value of this transaction is now \$938,584.00. Learn more about [how transactions work](#).

The "Details" section provides the following information:

Field	Value
Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Status	Confirmed
Received Time	2009-01-03 16:15
Size	204 bytes
Weight	816
Included in Block	0
Confirmations	754,977
Total Input	0.00000000 BTC
Total Output	50.00000000 BTC

Figura 7: `4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b`

# A carteira de Satoshi iii

The screenshot shows the WhatsOnChain website interface for the Bitcoin address 1A1zP1eP5QGefi2DMPTfTL5Lmv7DivfNa. The top navigation bar includes links for API, About, Classic View, English, Mexican, BSV, New Block ON/OFF, and a search bar. The main content area displays the address details, a QR code, and a transaction history table.

**Address:** 1A1zP1eP5QGefi2DMPTfTL5Lmv7DivfNa

**Balance:** 67.97456184 BSV

**Script Hash:** 8801df4e368ea28f8dc0423bcf7a4923e3a12d387c875e47a8cfb  
f98b5c39161

**Script Public Key:** 76a91462e907b15cbf27d5425399ebf6f0fb50eb88f1888ac

**First Seen:** 2009-01-03 18:10:05

**Transaction:** 1,162

**Details** **JSON**

**Transactions:** 1,162

Index	Transaction ID	Tag
#1	3387418addb4927299e5032f515aa442a6587de54677f90a93b8fe7798e648 2011-05-13 21:04:05	+ 0.91 BSV
#0	4a5e1e4baab09f3a3251ba88c31bc87f610f76673e2cc77eb2127b7fededa33b	

Figura 8: 1A1zP1eP5QGefi2DMPTfTL5Lmv7DivfNa

# A carteira de Satoshi iv

- Detalhes da Transação:

The screenshot shows the WhatsOnChain interface for a specific Bitcoin transaction. At the top, there are navigation links for 'APB', 'About', 'Classic View', 'English', 'Mandarin', 'CSV', 'New Block', and a search bar. The main title of the page is 'Transaction' with the hash '4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b'. Below the title, there are tabs for 'Details', 'Scripts', and 'JSON'. The 'Details' tab is selected. The transaction details are as follows:

Block #0	Timestamp (utc)
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b66a8ce26f	2009-01-03 18:15:05
Fees Collected	Version
0 BSV	1
Confirmations	Size
757,989	204 B

Below this, there is a 'Hex' section containing the raw transaction bytes:

```
04ffff985d810445546865205469605732030332f4a618e02f323b3039204380810e63856c4c6f72200f6e20627269606b206f66207365636  
f6e4206261890c6f757420666f722062815e6b73
```

Under the 'Decoded' heading, the output message is displayed:

```
yyETHE Times 03/Jan/2009 Chancellor on brink of second bailout for banks
```

At the bottom, the transaction's inputs and outputs are summarized:

1 Input	Total Input: 50 BSV	1 Output	Total Output: 50 BSV
#0 Carried Newly minted coins	50 BSV	#0 1A1zP1ePSQGeft1Z0MPYTL5SLm7DifvNs	50 BSV

Figura 9: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

# A carteira de Satoshi v

- Scripts

The screenshot shows the WhatsOnChain interface for a transaction. At the top, there are navigation links for API, About, Classic View, English, Market, CSV, New Block, and a search bar. Below the header, the transaction ID is displayed: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b. The main content area has tabs for Details, Scripts (which is selected), and JSON. Under Input Scripts, the script hash is shown: 04ffff001d010445440652054696d05732830332f4a616e2f323030392843d8616e83656c6c8f72206f6e2062722896e6b200f66287365636f6e64206261696c8f757420666f722062616e6b73. Under Output Scripts, the script hash is shown: 04678afdb8fe5548271967f1a87138b7105cd6a829e83909a87962e0ea1f61deb649f6bc3f4cef38c4f35504e51e112de5c984df7ba888d578a4c782b6bf11d5f\_0P\_CHECKSIG.

API About Classic View

English Market CSV New Block

Search Block height/hash, txid, address

Transaction 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Details Scripts JSON

Input Scripts

04ffff001d010445440652054696d05732830332f4a616e2f323030392843d8616e83656c6c8f72206f6e2062722896e6b200f66287365636f6e64206261696c8f757420666f722062616e6b73

Output Scripts

04678afdb8fe5548271967f1a87138b7105cd6a829e83909a87962e0ea1f61deb649f6bc3f4cef38c4f35504e51e112de5c984df7ba888d578a4c782b6bf11d5f\_0P\_CHECKSIG

TAAL API

WOC API

Cookies Policy

Terms of Use

About

Contact us

Privacy

PoweredByTAAL

© 2022 TAAL Distributed Information Technologies Inc.

Join Group

Follow Us

WOC Services Status

## A carteira de Satoshi vi

- JSON

# A carteira de Satoshi vii

The screenshot shows the Whatsonchain.com interface for the Bitcoin address `1A1zP1ePSQGeft12DMPTfTL5SLav7D1vfNa`. The address has a balance of `67.9928777 BSV`. The first transaction was seen on `2009-01-03 18:15:05`. A QR code is provided for the address. The transaction history lists two recent transactions:

Index	Transaction ID	Tag
#18413	4922c19661c9942f03196be5c02cafe1b34b13fb49899801112dfcbfb76547	+ 1e-8 BSV
#18412	46306a97eab7f95645669e7488920b719d382fb93c6a3da2bd9ec447c6243b	+ 1e-8 BSV

Figura 10: Saldo em 14/04/2023

# A carteira de Satoshi viii

The screenshot shows the blockchain.com website interface. On the left, there's a sidebar with various navigation links: Início, Preços, Gráficos, NFTs, DeFi, Academia, Notícias, Programadores, Wallet, Exchange, Bitcoin, Ethereum, Bitcoin Cash, BTC Testnet, BCH Testnet, and Português. The main content area displays the balance of the Bitcoin address 1A1zPfPqGefZDmPTTlSSumv7DnVha. The balance is listed as 72.61224698 BTC or \$2.21k USD. Below the balance, there's a summary section with details about the address's history, including its creation date (2009-01-04) and its ownership by Satoshi Nakamoto. A banner for BC.GAME crypto casino is visible. At the bottom, a transaction history table shows two recent transactions: one from 1A1zPfPqGefZDmPTTlSSumv7DnVha to another address (1A1zPfPqGefZDmPTTlSSumv7DnVha) and one from 1A1zPfPqGefZDmPTTlSSumv7DnVha to the same address.

Figura 11: Saldo em 14/04/2023 Fonte: blockchain.com

# Quem é Satoshi Nakamoto?

The screenshot shows a news article from CanalTech. The title is "Elon Musk afirma em tweet que ele não é o criador da criptomoeda Bitcoin". Below the title is a photo of Elon Musk in a dark environment with pipes and equipment. A sidebar on the left says "Aquele produto que você tá procurando tá aqui!". To the right of the main content are ads for Intel notebooks and a "Mais Lidas" sidebar.

**Elon Musk afirma em tweet que ele não é o criador da criptomoeda Bitcoin**

Por Redação | 28 de Novembro de 2017 às 16h56

[compartilhar](#)

Aquele produto que você tá procurando tá aqui!

Justamente no dia em que o Bitcoin teve uma alta significativa e atingiu os US\$ 10 mil, o empresário Elon Musk decidiu se posicionar sobre os boatos que afirmam que Satoshi Nakamoto, o misterioso criador da criptomoeda Bitcoin, seria um pseudônimo do empresário, a fim de se manter anônimo quanto à criação. Em resposta ao usuário @ThisIsSandeeG, que enviou um link explicando o boato a Musk e pedindo confirmação do próprio sobre o caso, o empresário fez a seguinte afirmação:

<https://go.gle/dkxgJ>

1 Crítica Fome de Sucesso | Filme traz boa análise social ainda que com erros

2 Quem são e quanto ganham motoristas e entregadores de apps no Brasil?

3 Materia escuro distorce luz antiga do Big Bang e confirma teoria de Einstein

4 Cientistas descobrem como levar

Figura 12: Elon Musk Fonte: CanalTech

# Quem é Satoshi Nakamoto? ii

The screenshot shows a news article from livecoins.com.br. The title is "Há 8 anos, revista expôs vida de Satoshi Nakamoto... e foi processada". The main image is a portrait of Dorian Nakamoto holding up a driver's license. On the left, there are social media sharing buttons for Facebook, Twitter, and LinkedIn. Below the image, a caption reads: "Dorian Nakamoto, apontado falsamente como criador do Bitcoin devido ao seu nome". The text of the article discusses a Newsweek cover from 2009 that claimed Nakamoto was the creator of Bitcoin, which led to legal issues. The right side of the screen displays a sidebar with "Últimas notícias" (Recent news) featuring links to other articles about Bitcoin mining in Paraguay, the Bank of Brazil, and Megupload.

Figura 13: Dorian Nakamoto Fonte: Livecoins

# Quem é Satoshi Nakamoto? iii

The screenshot shows a news article from livecoins.com.br. The title is "Criador do Linux diz ser Satoshi Nakamoto, o criador do Bitcoin". The article discusses a modification in the Linux kernel source code where Linus Torvalds signed off as "Satoshi Nakamoto". Below the article is a photo of Linus Torvalds, a man with glasses and a black t-shirt, sitting at a desk. To the right of the main article are several sidebar elements: a thumbnail for "O Primeiro SUV Abarth Do Mundo", a section for "Últimas notícias" with a snippet about a power theft in Paraguay, and two other news items: one about a central bank's stance on cryptocurrencies and another about the founder of Megaupload.

Linus Torvalds diz ser Satoshi Nakamoto, o criador do Bitcoin

A modificação também pode ser uma maneira não muito discreta de dizer aos geeks que ele é de fato Satoshi Nakamoto, algo que seria crível porque ele tem as habilidades para isso e alguns fatos se encaixam na história do Bitcoin.

Linus Torvalds

Linus Torvalds, o criador do sistema operacional Linux, parece ter modificado uma única linha no Kernel do Linux e incluiu uma afirmação de que ele é Satoshi Nakamoto. A modificação diz "eu sou Satoshi", o que pode ser uma brincadeira ou uma afirmação real de que ele criou o Bitcoin.

Linus Torvalds já foi suspeito de ser Satoshi Nakamoto, em parte porque ele criou o Git, que se acredita ter inspirado a blockchain, e em parte

O Primeiro SUV Abarth Do Mundo

Na fronteira com Brasil, Paraguai fecha mineradora de criptomoedas suspeita de roubar energia

"Criptomoedas tiram o sono de quem apostou nisso", diz Banco Central

Citando Luiz, criador do Megaupload fala sobre fim da hegemonia do dólar

Hackers atacam plataforma

Figura 14: Linus Torvalds Fonte: Livecoins

# Quem é Satoshi Nakamoto? iv

The screenshot shows a web browser window with multiple tabs open. The active tab displays an article from Cointelegraph.com.br. The article's title is "Criador do Linux 'volta atrás' e diz que não é Satoshi Nakamoto". It features a cartoon illustration of a man in a suit and mask holding a gold coin. Below the article, there is a social media sharing bar and a footer notice about cookies. To the right of the main content, there are two sidebar columns: one for the editor's choice and another for the latest news. At the bottom, there is a video player showing a YouTube video and a banner for the latest news on Twitter.

WALTER BARROS 01 FEB 2022

## Criador do Linux 'volta atrás' e diz que não é Satoshi Nakamoto

Linus Torvalds havia modificado uma linha do núcleo do sistema operacional de código aberto Linux para adicionar a frase "Eu sou Satoshi"



O que parecia ser a resposta para um dos grandes mistérios da tecnologia, o nome do criador do sistema operacional de código aberto Linux, Linus Torvalds, como a pessoa por trás do codinome Satoshi Nakamoto, criador do Bitcoin (BTC), caiu por terra esta semana. Uma história que veio à tona nos últimos dias, quando Linus Torvalds modificou uma linha do núcleo do sistema operacional e preencheu "Nome = Eu sou

ESCOLHA DO EDITOR

**Preço do Bitcoin ultrapassa US\$ 31.000 e Ethereum lidera chegada da 'altseason'**

Binance fecha parceria com CBF e vai dar NFT de graça do Campeonato Brasileiro, o Brasileirão

Dominância do Bitcoin é abalada pelo rally do ETH após atualização Shapella

Na volta a gente compra: investidores perderam valorização de 82% adiando compras de Bitcoin

Tribunal dos EUA emite intimação para Justin Sun, da Tron, e ameaça julgá-lo 'à revelia'

Cointelegraph YOUTUBE

ÚLTIMAS NOTÍCIAS NO TWITTER

A Cointelegraph.com usa Cookies para prover a melhor experiência para você.

ACEITAR

17:00 14/04/2023

Figura 15: Linus Torvalds Fonte: cointelegraph

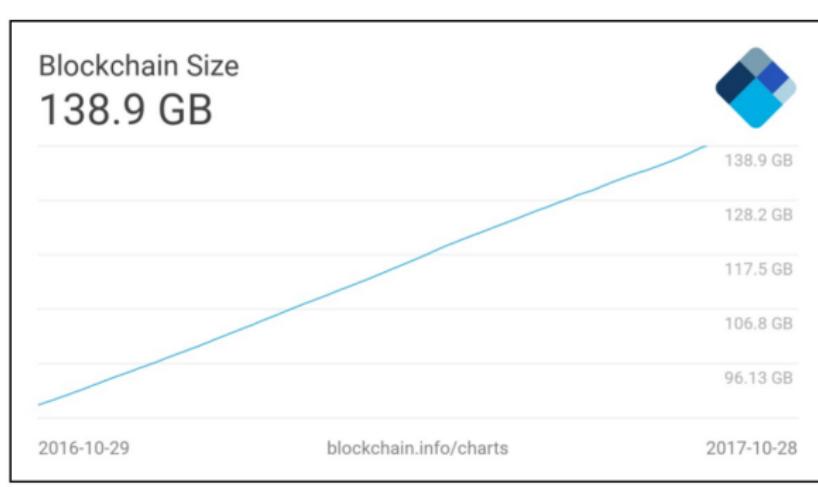
# Quem é Satoshi Nakamoto? v



Figura 16: Steve Jobs  
Fonte: Exame 10/04/2023

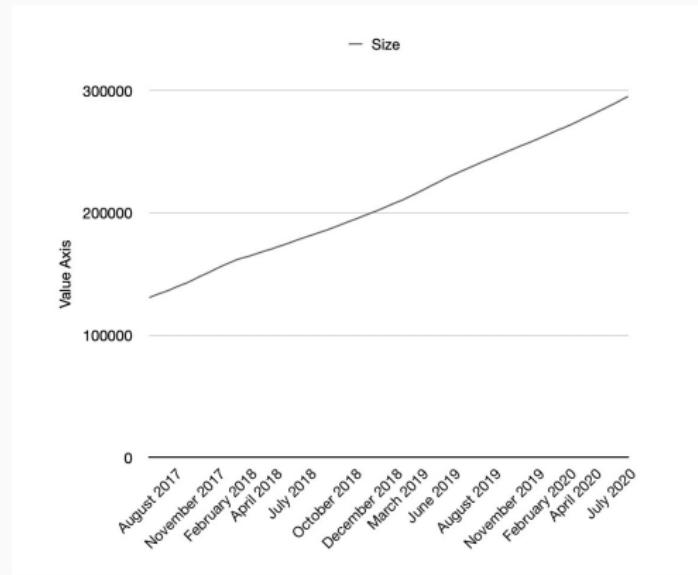
# Tamanho do Blockchain do Bitcoin

- O Blockchain do Bitcoin tinha em **October 29, 2017**, aproximadamente: **139GB**



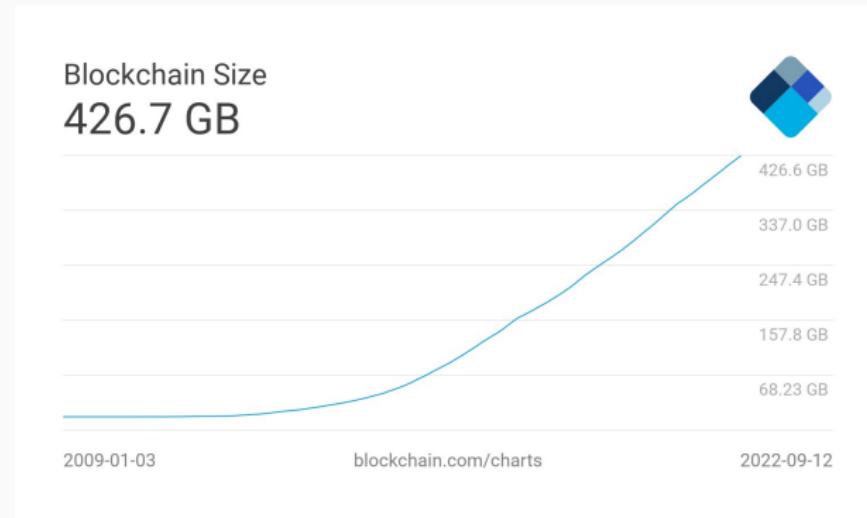
# Tamanho do Blockchain do Bitcoin ii

- A figura mostra a evolução de Aug 2017 para Jul 2020.  
Aproximadamente, *286GB*.



# Tamanho do Blockchain do Bitcoin iii

- A figura mostra a evolução de Jan 2009 para Set 2022.  
Aproximadamente, **426.7GB**.



- Fonte: <https://www.blockchain.com/charts/blocks-size>

# Tamanho do Blockchain do Bitcoin iv

- Tamanho em 14/04/2023: 472.9GB

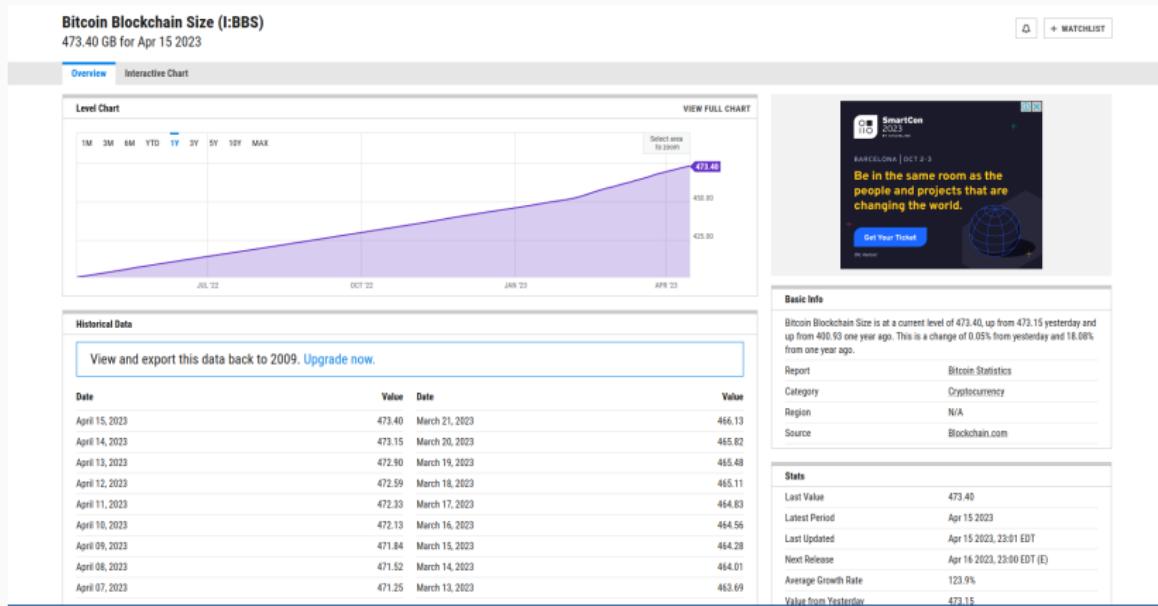


Figura 17: Tamanho em 14/04/2023 Fonte: ycharts

# Consumo de Energia i

- Pico em Janeiro de 2022: 204.5  $TWh$  por ano.

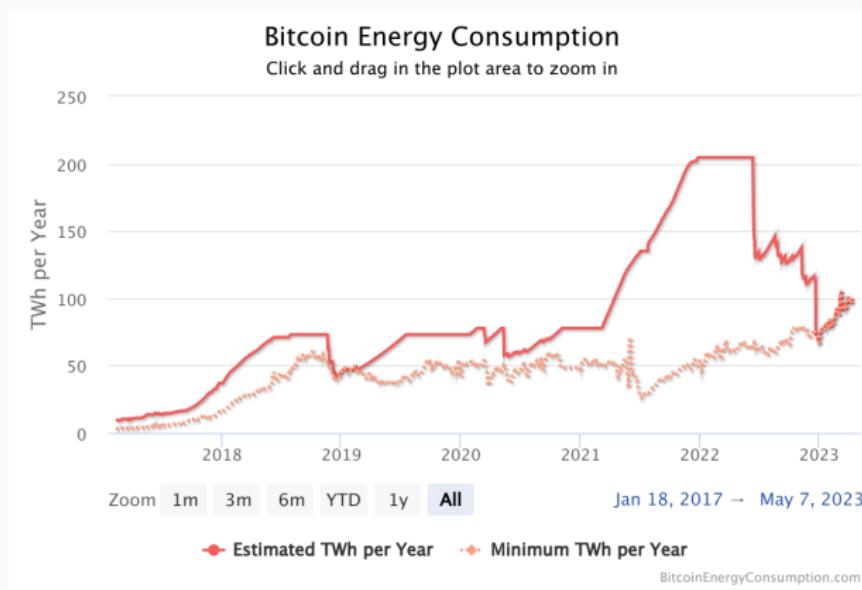


Figura 18: Consumo de Energia Fonte: digiconomist

## Consumo de Energia ii

---

Artigo: “Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin” (December 2022); *Bitcoin’s biggest competitor, Ethereum, has reduced its electrical energy requirement by at least 99.84% by changing its method of production.*

## Leitura Recomendada

Capítulo 5/6: Introduction Bitcoin: IMRAN BASHIR. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

# Contratos Inteligentes

---

## Definição

*“A smart contract is an electronic transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.”*

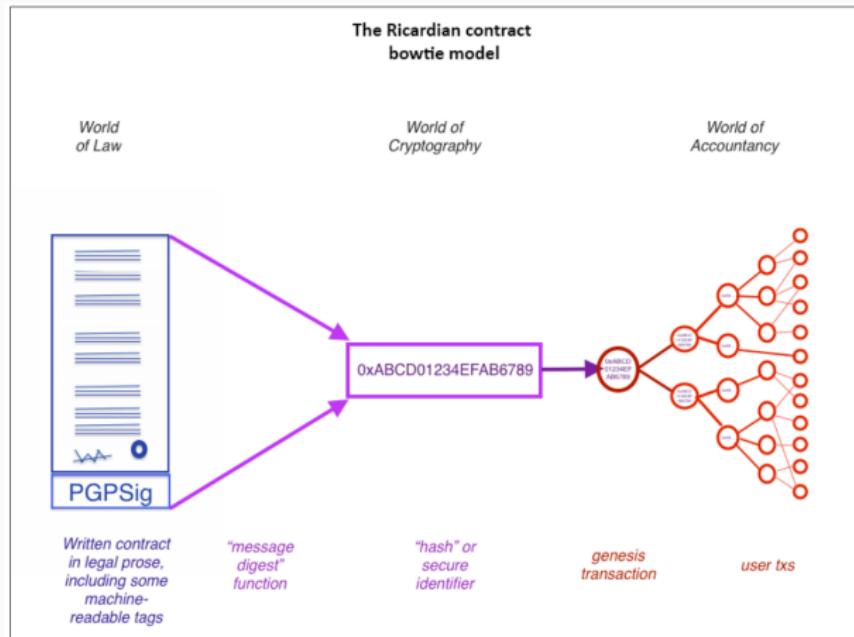
– Nick Szabo

- Nick Szabo apresentou a teoria de smart contracts nos anos 1990, no artigo *Formalizing and Securing Relationships on Public Networks* (Szabo 1997).

- Teoria apresentada quase 20 anos antes do potencial real e benefícios de contratos inteligentes serem apreciados.
- Antes do surgimento do *Bitcoin* e outras plataformas mais avançadas nesse ponto, como a *Ethereum*.
- Um contrato inteligente é um programa de computador que representa um acordo entre as partes que é automaticamente executado.

# Contratos Ricardianos i

- Proposta no artigo *Financial Cryptography in 7 Layers*<sup>1</sup>, por Ian Grigg, no final dos anos 1990s.



<sup>1</sup><https://iang.org/papers/fc7.html>

## Leitura Recomendada

Capítulo 9/10: Smart Contracts: IMRAN BASHIR. Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

# Ethereum

---

- Vitalik Buterin conceitualizou Ethereum em Novembro de 2013.
- A ideia central proposta foi o desenvolvimento de uma linguagem **Turing-completa** para permitir o desenvolvimento de programas arbitrários (contratos inteligentes) para *blockchain* e Aplicações Descentralizados (DApps).
- Este conceito difere do Bitcoin, onde a linguagem de **script** é limitada e permite apenas as operações necessárias.

# Ethereum – Overview ii

## ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER PETERSBURG VERSION 4ea7b96 – 2020-06-08

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.

Figura 19: O *Ethereum Yellow Paper*<sup>2</sup>

- O *Ethereum Yellow Paper* foi escrito por Dr. Gavin Wood, o fundador do *Ethereum* e da *Parity* (<http://gavwood.com>), e serve como uma especificação formal do protocolo da *Ethereum*.
- As implementações de clientes **Ethereum** seguem as especificações de protocolo definidas no artigo.

---

<sup>2</sup><http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html#developer-tools>

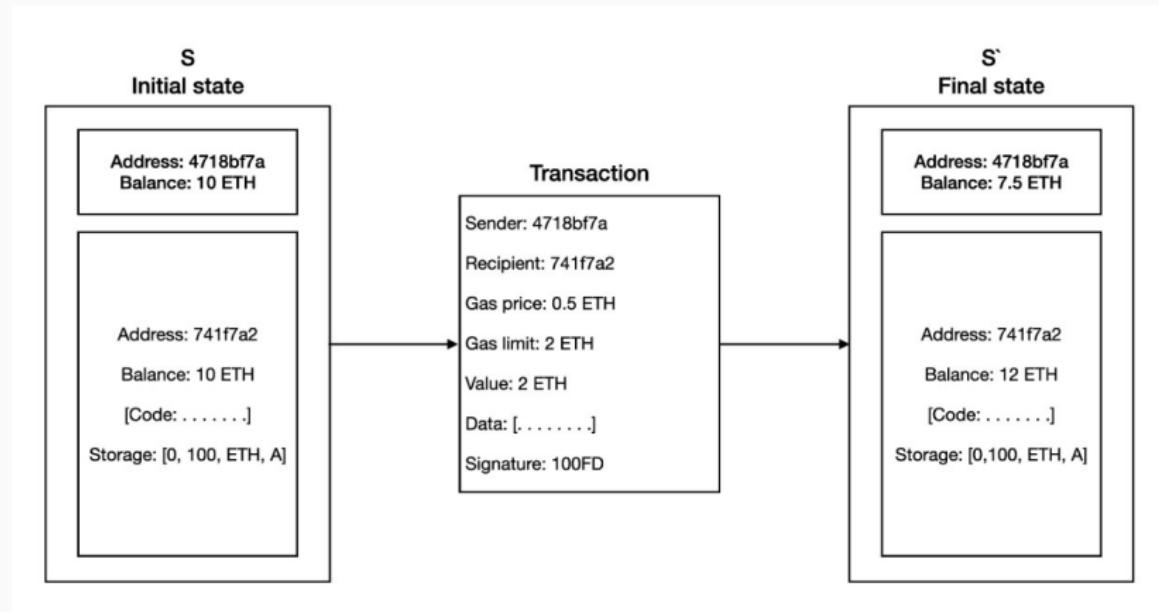
# Ethereum Releases i

---

- A primeira versão da *Ethereum*, denominada **Olympic**, foi liberada em Maio de 2015.
- Dois meses mais tarde, a versão chamada de **Frontier** foi liberada em Julho.
- Outra versão, a **Homestead** com várias melhorias foi liberada em Março de 2016.
- A release chamada de **Muir Glacier**, que atrasou a **difficulty bomb** (<https://eips.ethereum.org/EIPS/eip-2384>).
- Um grande lançamento antes disso foi **Istanbul**, que incluiu mudanças em torno de privacidade e dimensionamento capacidades.
- Uma lista completa com todas as *releases* anunciadas é mantida em <https://github.com/ethereum/go-ethereum/releases>.

# A Blockchain Ethereum i

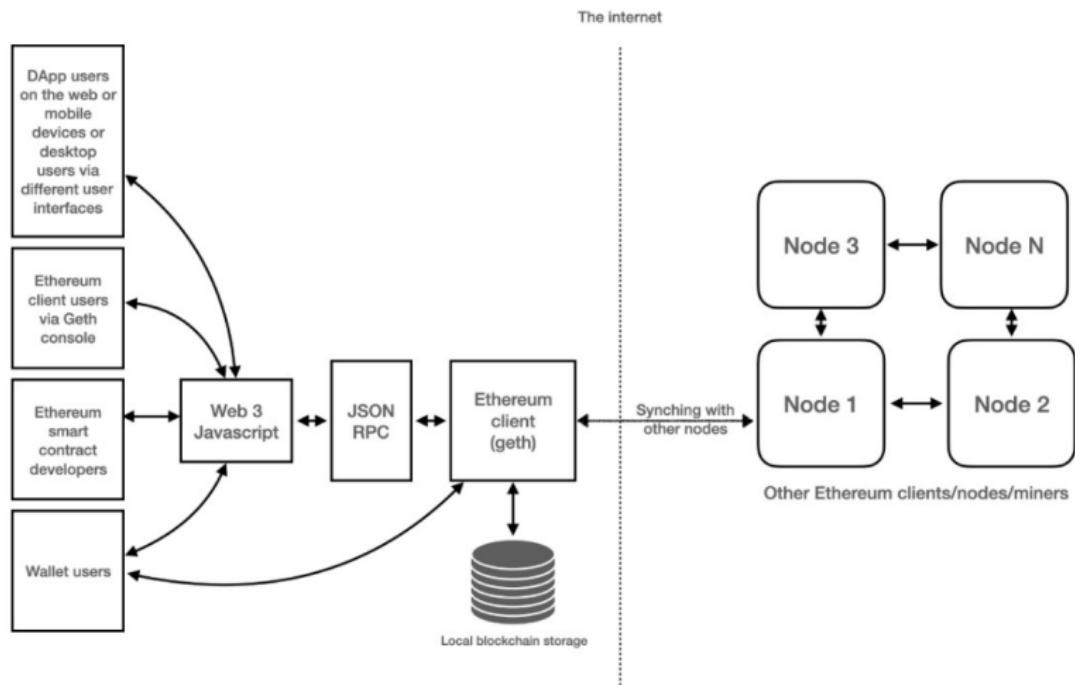
- O Ethereum, assim como qualquer outro *blockchain*, pode ser visualizado como uma máquina de estado baseada em transações.



- A ideia principal da *blockchain* da *Ethereum*, um estado gênese é transformado em um estado final executando transações de forma incremental.
- A transformação final é então aceita como a versão absoluta e indiscutível do estado.
- A função de transição de estado *Ethereum* é mostrada, onde a execução de uma transação resultou em uma transição de estado.

- O caso de uso mais comum da rede *Ethereum* é o envio e o recebimento de pagamentos.
- Para isso, o usuário assina a transação e a envia, que se propaga na rede, momento em que os mineradores a pegam, verificam e iniciam a Prova de Trabalho (PoW).
- Se PoW for bem sucedida, o bloco com a transação é finalizado e propagado, e um novo bloco é adicionado à cadeia
- Para enviar e receber transações, um software de carteira é usado: por exemplo, carteiras são usadas em dispositivos móveis.

# Arquitetura de Alto Nível da Ethereum



A rede *Ethereum* é uma rede *peer-to-peer* onde os nós participantes mantêm a *blockchain* e contribuem para o mecanismo de consenso. As redes podem ser divididas em três tipos, com base nos requisitos e uso.

## A mainnet

A **mainnet** é a atual rede *Ethereum*. Seu ID de rede é 1 e seu ID de cadeia (*chain*) é também 1. Os IDs de rede e de cadeia são usados para identificar a rede. Um explorador de blocos que mostra informações detalhadas sobre blocos e outras métricas relevantes estão disponíveis em <https://etherscan.io>, que pode ser usado para explorar a blockchain Ethereum.

# Rede Ethereum ii

## Testnets

Existem um número de redes de testes (testnets) disponíveis para Ethereum. Elas tem como objetivo fornecer um ambiente de testes para contratos inteligentes e DApps antes de serem implantados para produção na rede *blockchain*. Além disso, sendo redes de teste, elas permitem experimentos e pesquisa. A principal testnet é chamada **Ropsten**, que contém todas as características de outras redes de propósito especial menores que foram criados para fins específicos. Por exemplo, outras redes de teste incluem **Kovan** e **Rinkeby**, que foram desenvolvidos para testar as versões do **Byzantium**. As mudanças que foram implementados nessas redes de teste menores também foram implementados em **Ropsten**. Agora a rede de teste **Ropsten** contém todas as propriedades de **Kovan** e **Rinkeby**.

## Redes Privadas

As *private nets* são redes privadas que podem ser criadas gerando-se um novo *genesis block*. Este é geralmente o caso em redes *blockchain* privadas, onde um grupo privado de entidades iniciam sua rede *blockchain* e a usam como uma blockchain autorizada ou de consórcio.

# Elementos do Ecossistema Ethereum i

---

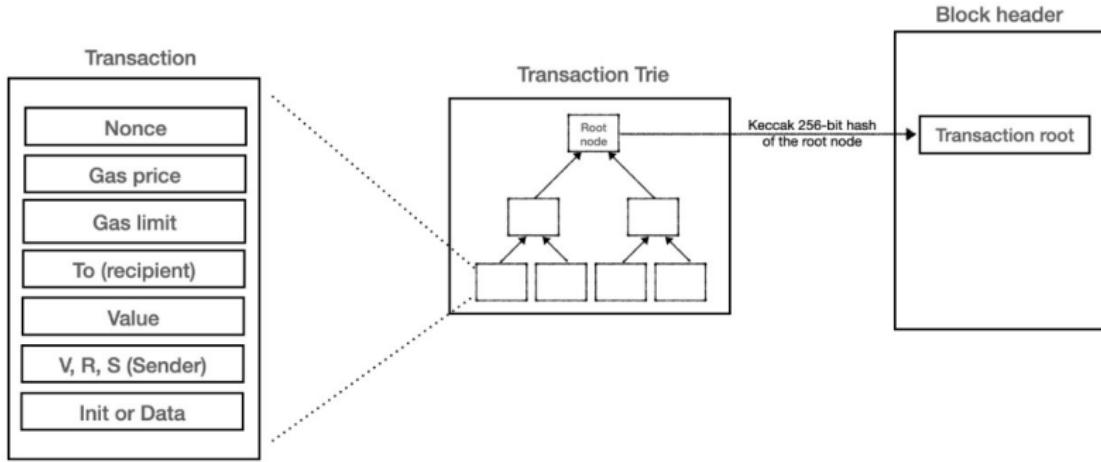
- Chaves e Endereços
- Contas
- Transações e mensagens
- Criptomoeda/Tokens Ether
- A Ethereum Virtual Machine (EVM)
- Smart contracts e contratos nativos.

- EOAs: *Externally Owned Accounts*. Contas de usuários representadas por um endereço.
- CAs: *Contract accounts*. Criadas como resultado do *deployment* de um contrato inteligente, também representado por um endereço.

# Transações e Árvore de Transações (trie) i

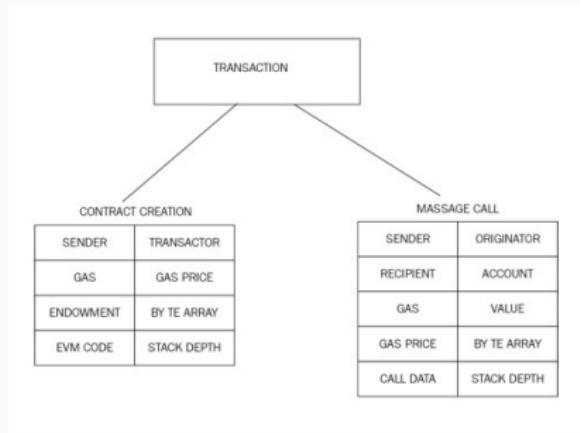
## Transações

Uma transação no *Ethereum* consiste em vários campos, como mostrado aqui, junto com a *transaction trie*. O diagrama também mostra a relação entre a tentativa de transação e o cabeçalho do bloco.



# Tipos de Transações i

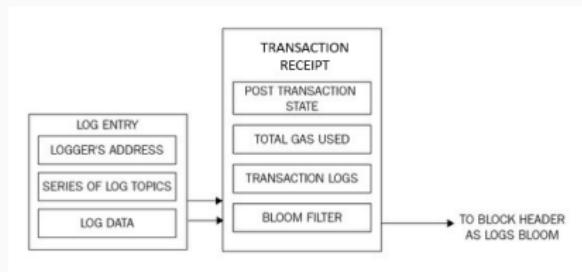
- Existem três tipos de transações:
  - Criação de Contrato
  - *Call*
  - Transferência de Valor



O diagrama mostra a criação do contrato e as transações de chamada, com campos obrigatórios.

# Recibos de Transações i

- Recibos de Transações (transaction receipts) são gerados como resultado da execução de transações.
- Logs também são atualizados em conformidade.
- Ambas as estruturas de dados contêm vários campos, conforme mostrado abaixo:

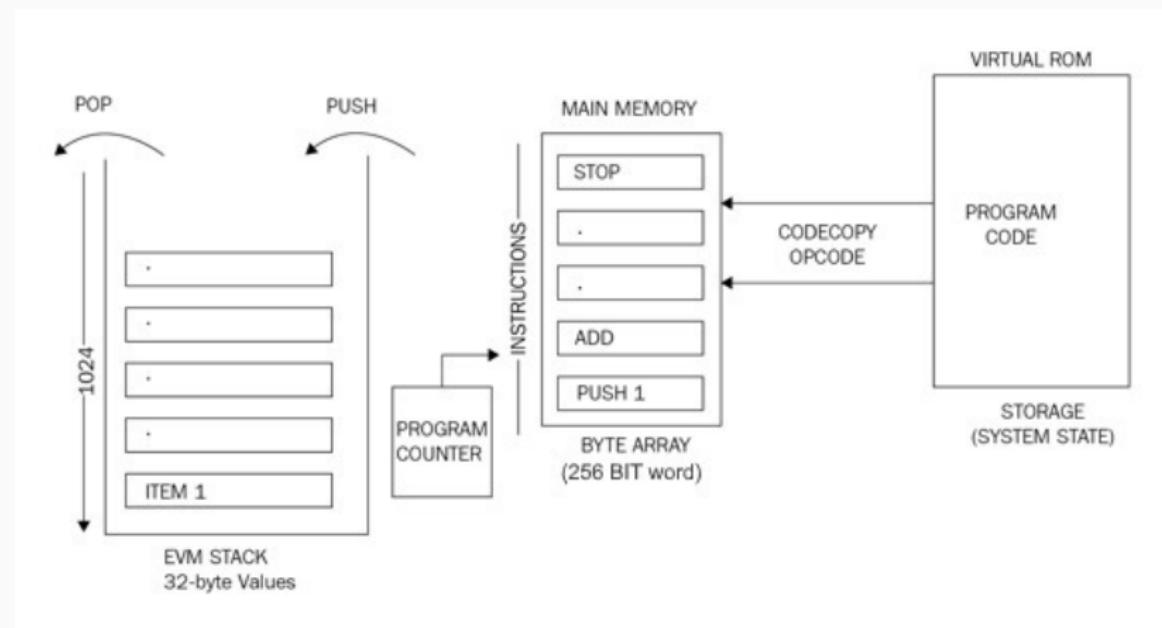


# A Ethereum Virtual Machine (EVM) i

---

- Stack size based on LIFO queue: Last In, First Out.
- 1024 stack depth limit
- Turing complete but limited by gas, making it quasi-Turing complete
- Big-endian design
- Storage available to EVM
  - Memory
  - Storage
  - Stack

# EVM operation design



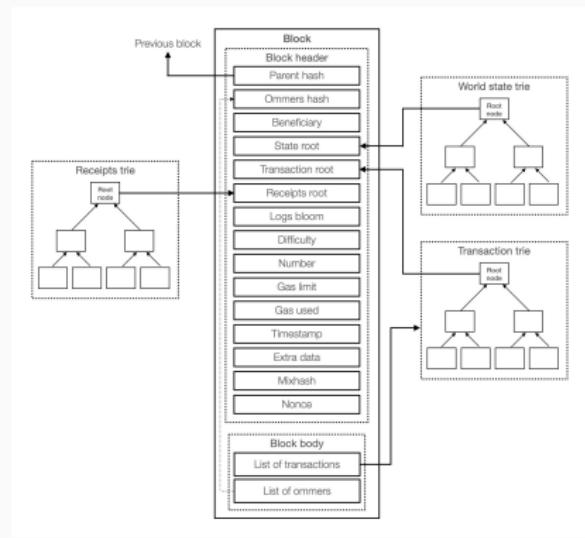
# Contratos Nativos i

---

- Existem nove contratos pré-compilados ou contratos nativos na versão Ethereum Istanbul:
  - *The elliptic curve public key recovery function*
  - *The SHA-256-bit hash function*
  - *The RIPEMD-160-bit hash function*
  - *The identity/datacopy function*
  - *Big mod exponentiation function*
  - *Elliptic curve point addition function*
  - *Elliptic curve scalar multiplication*
  - *Elliptic curve pairing*
  - *Blake2 compression function 'F'*

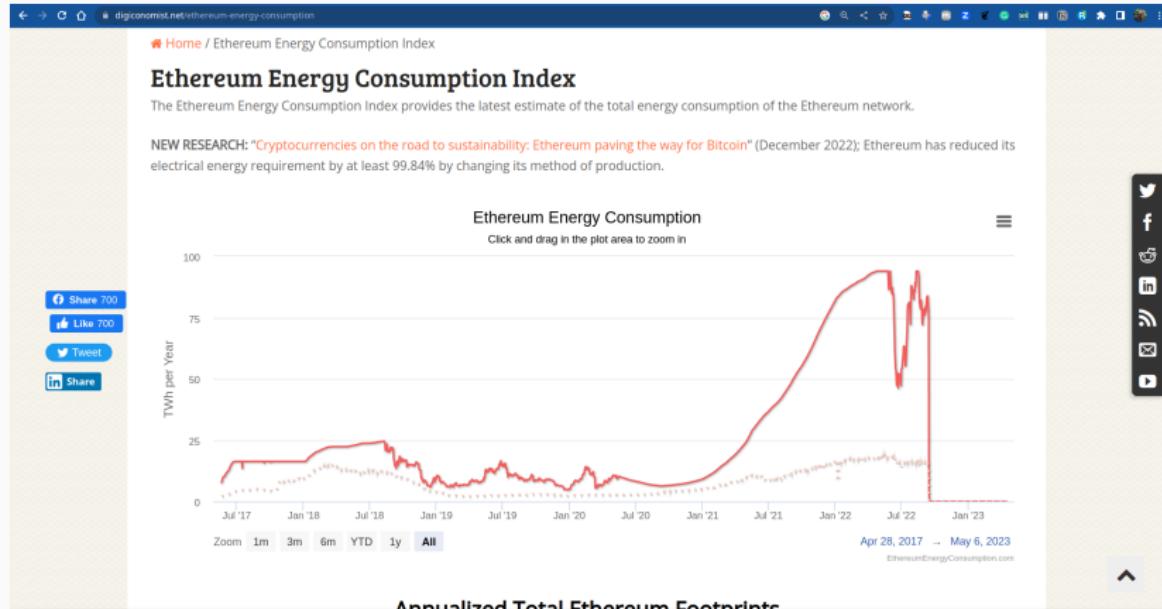
# Blocks e Blockchain i

Um bloco *Ethereum* consiste em vários campos, conforme diagrama. *State root*, *transaction root* e *receipts root* são *root hashes* de suas respectivas árvores.



- Com a última atualização **Merge** que trocaram a *Proof of Work* (PoW) pela *Proof of Stake* (PoS) tendo como uma das motivações a questão ambiental. Houve um grande impacto no consumo de energia.

# Consumo de Energia ii



- *Wallets* (Carteiras)
- *Light clients* (softwares clientes)
- Existem três tipos de sincronização de clientes:
  - **Full:** Nesse modo de sincronização, o cliente **Geth** faz um *download* completo da *blockchain* para o nó local. Isso significa que ele obtém todos os cabeçalhos e corpos dos blocos e valida todas as transações e blocos desde o bloco *genesis*.

- **Fast:** Neste modo é feito o *download* completo, mas somente recupera e verifica somente os **64** blocos anteriores ao bloco corrente. Depois disso, ele verifica os novos blocos na íntegra. Não reproduz e verifica todas as transações históricas desde o bloco *genesis*, em vez disso, ele só faz os *downloads* de estado. Isso também reduz significativamente o tamanho do disco do banco de dados *blockchain*. Este é o modo padrão de sincronização do cliente **Geth**.
- **Light:** Este é o modo mais rápido e apenas baixa e armazena o estado atual. Nesse modo, o cliente não baixa nenhum bloco histórico e processa apenas os blocos mais novos.
- No início de 2020, o tamanho do *blockchain Ethereum* era de aproximadamente **210GB**, baixar e manter isso pode ser um problema.

- Em 18 de outubro de 2022 o tamanho chegava a **966.06GB**, segundo [ycharts](#).
- Em 16 de abril de 2023 o tamanho está em **914.81GB**.

# Wallets e Software Clientes iv

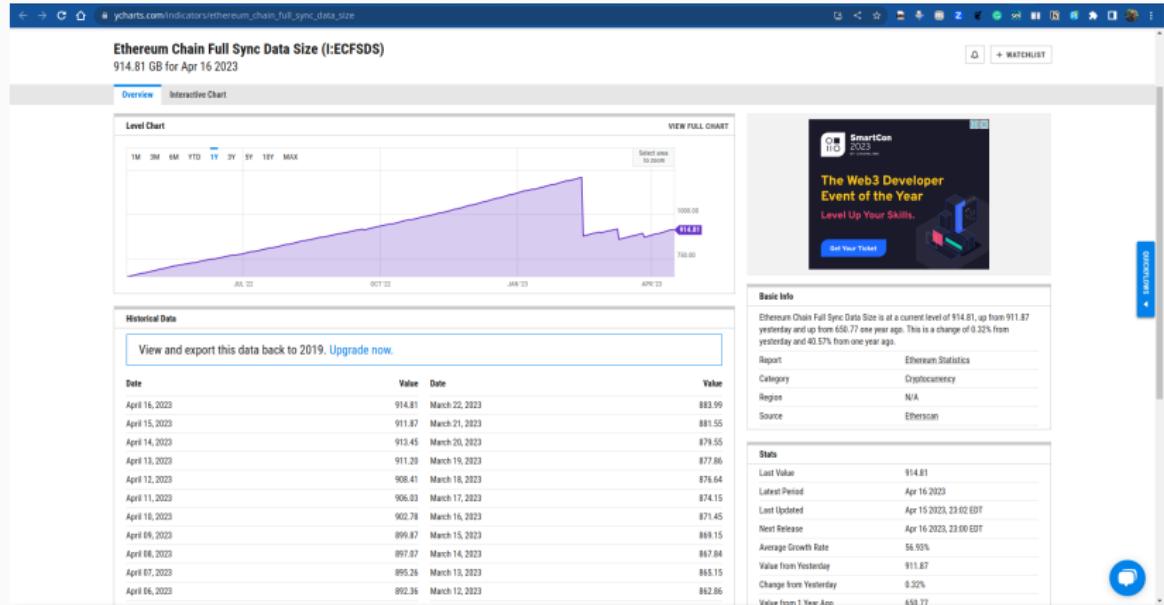
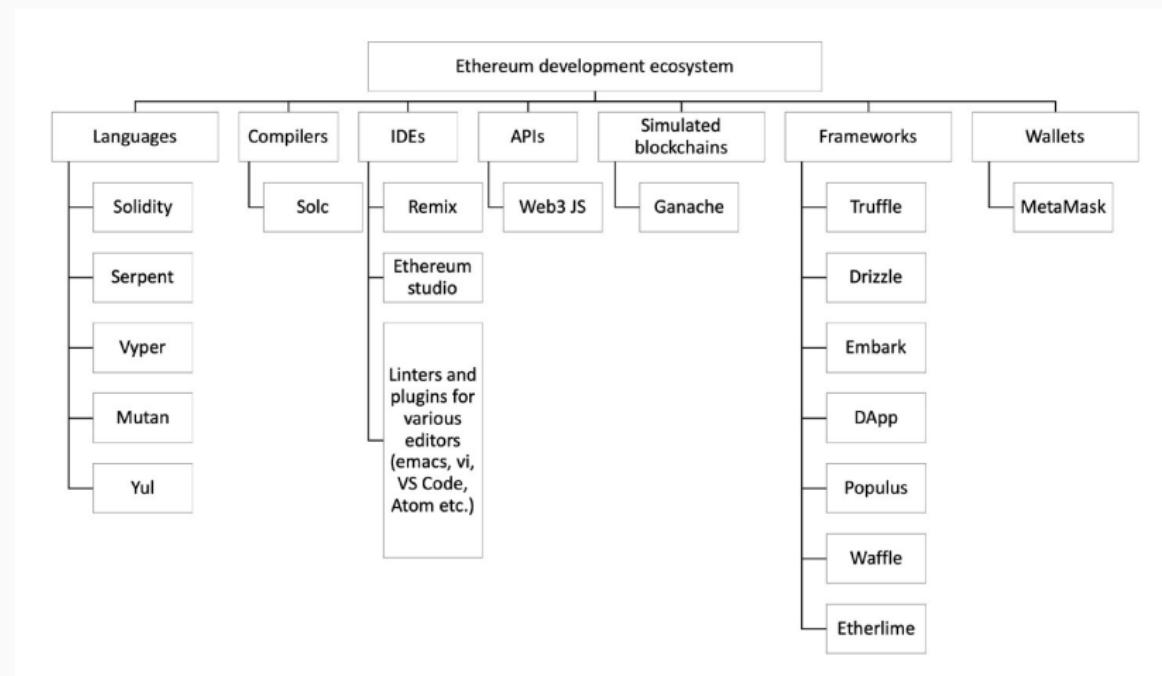


Figura 20: Ethereum chain full sync data size Fonte: [ycharts](#)

- A mineração é o processo pelo qual novos blocos são selecionados por meio de um mecanismo de consenso e adicionados ao *blockchain*.
- O processo segue os seguintes passos:
- Ficam ouvindo as transações transmitidas na rede Ethereum e determina as transações a serem processadas.
- Determinam quais blocos são válidos e os obsoletos.
- Atualiza a conta (account balance) com a recompensa ganha pela mineração bem sucedida de um bloco.
- Finalmente, um novo estado válido é computado e o bloco é finalizado.

- Ethash é o nome do algoritmo de **Proof of Work** que era usado no **Ethereum**.

# Taxonomia do Ecossistema de Componentes de Desenvolvimento Ethereum i



- **Solidity:** É uma linguagem de alto nível desenvolvida para *Ethereum*. Tem se tornado a linguagem padrão para escrever contratos para *Ethereum*. O código é ser compilado e transformado em *bytecode*, é necessário utilizar o compilador **solc**.
- **Vyper:** Essa linguagem é uma linguagem experimental semelhante ao Python que está sendo desenvolvida para trazer segurança, simplicidade e auditabilidade ao desenvolvimento de contratos inteligentes.
- **Yul:** Esta é uma linguagem intermediária que tem a capacidade de compilar para diferentes back-ends, como EVM e eWasm. Os objetivos de projeto do Yul incluem principalmente legibilidade, fluxo de controle fácil, otimização, verificação formal e simplicidade.

- **Mutan:** Esta é uma linguagem de estilo Go, que foi descontinuada no início de 2015 e não é mais usada.
- **LLL:** Linguagem semelhante ao *Low-Level Lisp-Like*, daí o nome LLL, também não é mais usada.
- **Serpent:** Esta é uma linguagem simples e limpa parecida com Python. Ela não é mais usado para desenvolvimento de contratos e não é suportado pela comunidade.
- Leia mais sobre Solidity e Recursos de Desenvolvimento de DApps em **DAPP DEVELOPMENT FRAMEWORKS<sup>3</sup>**

---

<sup>3</sup><http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html#developer-tools>

# Linguagem Solidity

---

- Uma Linguagem de Domínio Específico (DSL)
- *Contract-oriented language*
- JavaScript / C-like
- Amplamente utilizada
- Estaticamente Tipada

- **Ganache**
  - Simula um *Blockchain Ethereum* pessoal com uma interface com usuário, comumente usada no desenvolvimento e testes.
- **Ganache-cli**
  - Versão linha de comando do **Ganache** tem como pre-requisito **NodeJS**.

# Ferramentas e Bibliotecas ii

The screenshot shows a blockchain explorer interface with the following details:

**ACCOUNTS** | **BLOCKS** | **TRANSACTIONS** | **CONTRACTS** | **EVENTS** | **LOGS** | SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK: 0 | GAS PRICE: 20000000000 | GAS LIMIT: 6721975 | HARDFORK: PETERSBURG | NETWORK ID: 5777 | RPC SERVER: HTTP://127.0.0.1:7545 | MINING STATUS: AUTOMINING | WORKSPACE: JAZZY-GIRL

**MNEMONIC**: kick abstract strong shrug forward enlist puppy reunion elephant hip suffer base

**HD PATH**: m/44'/60'/0'/\*/account\_index

ADDRESS	BALANCE	TX COUNT	INDEX	EDIT
0x2366e9848803cB00CB82E6E6De3F6D17C4AA9ADA	100.00 ETH	0	0	🔗
0x6805940005154aEdfe6a00A39C588ED668E64D9D	100.00 ETH	0	1	🔗
0x56C21294F4e17dF32486b3d4D12E72D023861edF	100.00 ETH	0	2	🔗
0xAfACDB553412071bB538E36d57ED92d6745C5f94	100.00 ETH	0	3	🔗
0x694AE93a42C43B8E3d10c3F6769Adf2566C1863B	100.00 ETH	0	4	🔗

# Frameworks i

---

- Truffle
  - Framework de desenvolvimento para Ethereum com recursos para implantação, teste e depuração.

```
[rogerio@ryzen-nitro execution]$ truffle
Truffle v5.8.2 - a development framework for Ethereum

Usage: truffle <command> [options]

Commands:
  truffle build      Execute build pipeline (if configuration present)
  truffle compile   Compile contract source files
  truffle config    Set user-level configuration options
  truffle console   Run a console with contract abstractions and commands
                    available
  truffle create    Helper to create new contracts, migrations and tests
  truffle dashboard Start Truffle Dashboard to sign development transactions
                    using browser wallet
  truffle db        Database interface commands
  truffle debug    Interactively debug any transaction on the blockchain
  truffle deploy   (alias for migrate)
  truffle develop  Open a console with a local development blockchain
  truffle exec     Execute a JS module within this Truffle environment
```

# Frameworks ii

```
truffle help      List all commands or provide information about a specific command
truffle init      Initialize new and empty Ethereum project
truffle migrate    Run migrations to deploy contracts
truffle networks   Show addresses for deployed contracts on each network
truffle obtain     Fetch and cache a specified compiler
truffle opcode     Print the compiled opcodes for a given contract
truffle preserve   Save data to decentralized storage platforms like IPFS and Filecoin
truffle run        Run a third-party command
truffle test       Run JavaScript and Solidity tests
truffle unbox      Download a Truffle Box, a pre-built Truffle project
truffle version    Show version number and exit
truffle watch      Watch filesystem for changes and rebuild the project automatically
```

## Options:

--help	Show help	[boolean]
--version	Show version number	[boolean]

See more at <https://trufflesuite.com/docs/>

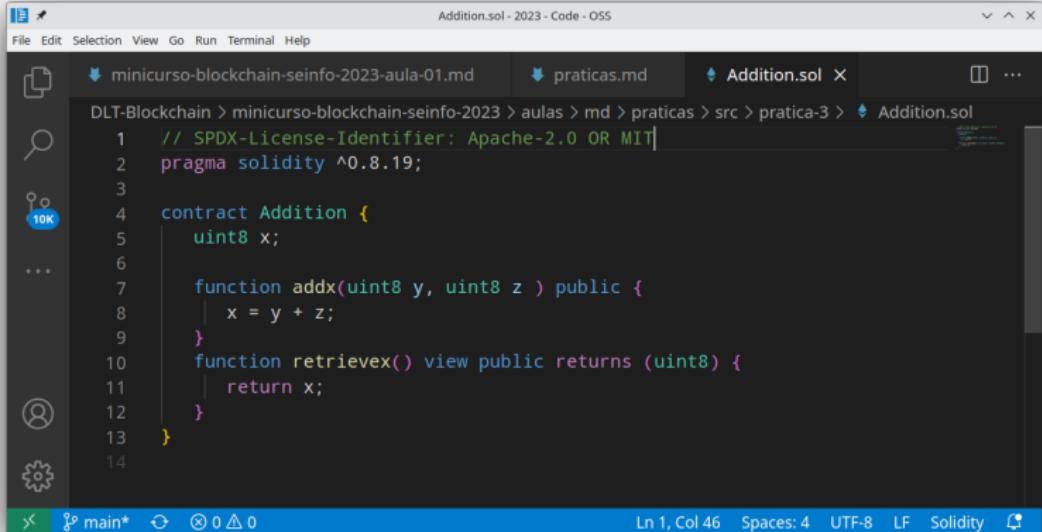
For Ethereum JSON-RPC documentation see <https://ganache.dev>

[rogerio@ryzen-nitro execution]\$

- Drizzle
  - Um conjunto de bibliotecas de *frontend* para o desenvolvimento de interfaces *web*.
  - Torna o desenvolvimento *frontend* para DApps fácil.
  - Tem o NodeJS como pré-requisito.
  - Baseado no *Redux store*.
  - Mantém uma biblioteca de componentes **React**.

- A escrita de contratos inteligentes é basicamente a escrita de código fonte do contrato em **Solidity** em um editor de texto.
- Existem *plugins* e extensões disponíveis para os editores mais comuns, tais como Vim, Atom, VSCode, que fornecem *syntax highlighting* e formatadores para código fonte **Solidity**.
- Plugin VSCode para Solidity

# Desenvolvimento e Implantação ii



The screenshot shows the Visual Studio Code (VSCode) interface with the following details:

- Title Bar:** Addition.sol - 2023 - Code - OSS
- Menu Bar:** File Edit Selection View Go Run Terminal Help
- File Explorer:** Shows a tree structure with the file path: DLT-Blockchain > minicurso-blockchain-seinfo-2023 > aulas > md > pratica > src > pratica-3 > Addition.sol. A file named minicurso-blockchain-seinfo-2023-aula-01.md is also listed.
- Code Editor:** Displays the Solidity code for the `Addition` contract:

```
1 // SPDX-License-Identifier: Apache-2.0 OR MIT
2 pragma solidity ^0.8.19;
3
4 contract Addition {
5     uint8 x;
6
7     function addx(uint8 y, uint8 z ) public {
8         x = y + z;
9     }
10    function retrievex() view public returns (uint8) {
11        return x;
12    }
13 }
14
```
- Bottom Status Bar:** Shows the current file is main\*, line 1, column 46, spaces: 4, encoding: UTF-8, line separator: LF, and the language mode is Solidity.

Figura 21: Plugin VSCode para Solidity

# Leitura Recomendada

## Leitura Recomendada

### Capítulo 11: Ethereum 101

Livro: [IMRAN BASHIR](#). Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

### Capítulo 12: Futher Ethereum

Livro: [IMRAN BASHIR](#). Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

Prática: Instalando o Cliente

*Ethereum: Geth*

---

# Prática: Criando uma Rede Ethereum Privada

---

## Prática: Instalando o Solidity

---

# Prática: Instalando o Solidity

---

## Prática: Introdução ao Web3

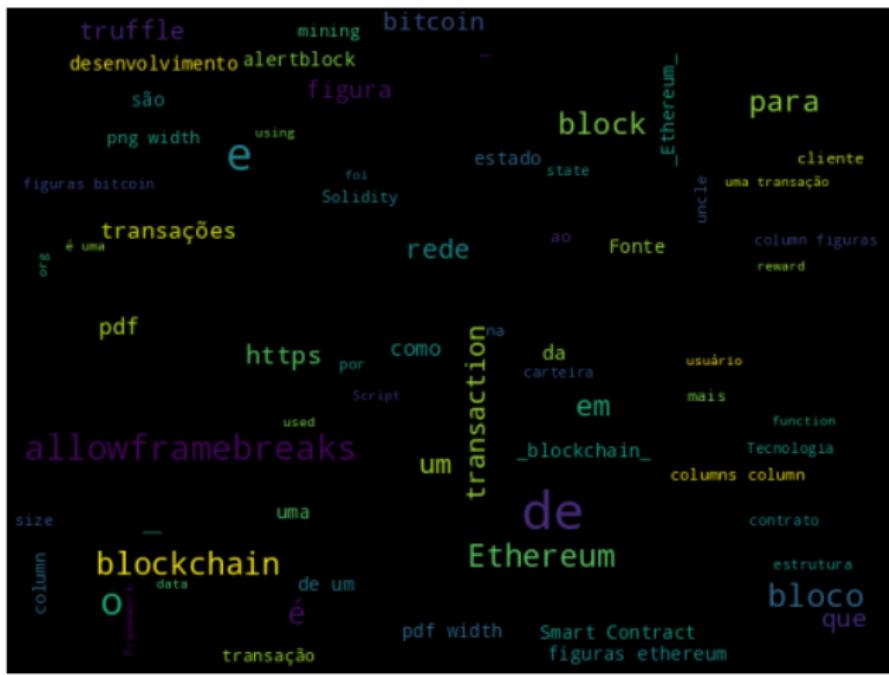
---

## Prática: Introdução à Tokenização

---

# Prática: Introdução à Tokenização

## *Word Cloud*



## Referências

---

# Referências i

---

Szabo, Nick. 1997. "Formalizing and Securing Relationships on Public Networks." *First Monday* 2(9). <http://dblp.uni-trier.de/db/journals/firstmonday/firstmonday2.html#Szabo97>.