

APUSCOIN: Criando uma criptomoeda do zero com Python e Linux

#crypto #python #linux #blockchain #apus



Histórico Tchelinux

- **2018 [bioinformática]:**
 - Software Livre e Bioinformática: do DNA ao medicamento
- **2019 [web scraping]:**
 - Web Scraping: a arte de automatizar a recuperação de informação na Web
- **2020 [deep learning]:**
 - IA versus COVID-19
- **2021 [high performance]:**
 - Alta performance em IA: uma abordagem prática em Linux



O que é criptografia?

O que é criptografia?



Definição

A criptografia é o estudo e a prática de enviar mensagens seguras e encriptadas entre duas ou mais partes. A criptografia permite a realização de transações de moedas digitais sob pseudónimo, seguras e "trustless", ou seja, sem um banco ou outro intermediário.

Porque é que a criptografia é importante?

As criptomoedas baseiam-se totalmente em ideias criptográficas. O Bitcoin foi inventado por uma pessoa (ou grupo de pessoas) sob o pseudónimo Satoshi Nakamoto, que propôs a ideia sob a forma de um livro branco publicado num fórum de discussão de criptografia em 2009.

O que é



BLOCKCHAIR Search for transactions, addresses, blocks and embedded text data...

Bitcoin · Transactions **Bitcoin transaction** API

200% on Deposit \$

A criptografia é baseada em hashes.

Transaction hash
1810e267c0f7ac947672a70992b1a7266bb12a04eed616d40f33f5e60f1c1ffc

Transaction status
Confirmed · 2 of 6 confirmations
Block id 733,184

Amount transacted ?
0.00353392 BTC · 140.59 USD

Transaction fee ?
0.0000741 BTC · 2.95 USD

Fee per vbyte
1 satoshi

Additional info Transaction receipt

Senders 50

1JMNxue9Z497qgxNbGC3md3mFQuQZ
Unsx
0.00001698 BTC · 0.68 USD

Recipients

bc1qppeskrjpe0rt
p4apdjs0mu5n
0.00353392 BTC · 140.59 USD

BLOCKCHAIR – Um dos primeiros exploradores de Blockchain.

O q

English | [Español](#) | [Français](#) | [ελληνικά](#) | [italiano](#) | [Deutsch](#)
[Česky](#) | [Magyar](#) | [日本語](#) | [简体中文](#) | [Русский](#) | [português](#)



bitaddress.org

Geração de hashes
online



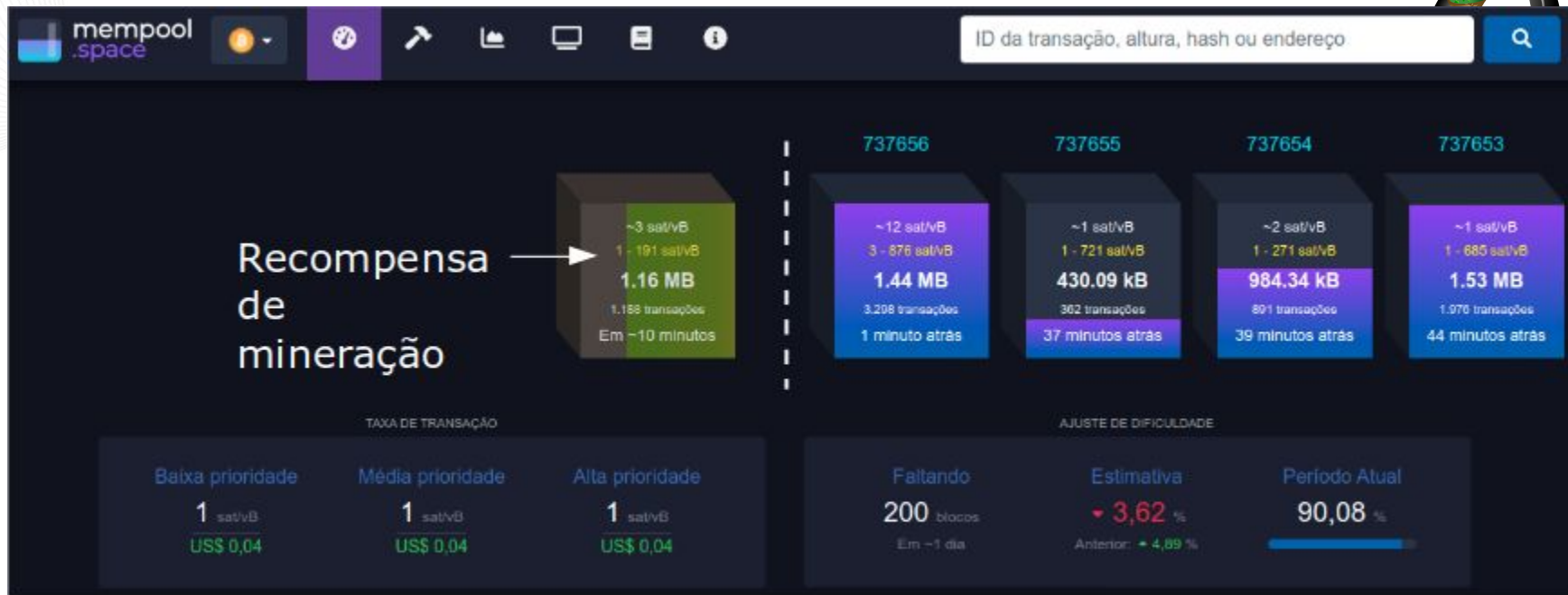
Open Source JavaScript Client-Side Bitcoin Wallet Generator



6%	6%	6%	Brain Wallet
6%	6%	Wallet Details	
Generating Bitcoin Address... MOVE your mouse around to add some extra randomness... 6% OR type some random characters into this textbox <input type="text"/>			
67431fae2cc1ad609156457b42bebb25214218381d4ecec118466b4393c713832 456f86eba555d51a2bcfb4aa9260bfcdf657600665c5ac306c2e2f8b72f7ce914 f7c02158bd4d3eb1afe9c2ac06a960c367d1f999ac3fe0c9d6802aade5a932322 99d860d1ce4dfd2ba6c590c2162b5234455e67e7f251261ee5b53e9d627e517e1 b1e719b3f1ce423ba972e2776384d836438b83291b8b87e4df8414f6e51fc0a17 6dce5b033e07a3bdaf0fc1a8c7b0f08ab52dd2c9c56bba013d0a94d6ddac413a8 939151f539b15d428d23733cd3408c0857c9927838aace6ec3600b19098d41fda 9ad6ca2c0b936477ff26081bbd84181ea5b4609f83cd4702a2bb9dfc5			

BITADDRESS – Gerador de hashes para carteiras Bitcoin.

O que é criptografia?






MEMPOOL – Lista de transações a serem mineradas.

O que é criptografia?



Grandes mineradores

Últimos blocos

Altura	Pool	Transações	Tamanho
737656	 Foundry USA	3.298	1.44 MB
737655	 Poolin	362	430.09 kB
737654	 SlushPool	891	984.34 kB
737653	 Foundry USA	1.976	1.53 MB
737652	 BTC.com	2.100	1.61 MB
737651	 AntPool	2.025	1.28 MB

[View more »](#)

Últimas transações

ID da transação	Quantia	Dólar	Taxa
fdbb4...5569e	3,215 BTC	US\$ 93.681	15,9 sat/vB
62d53...dbb49	0,1001 BTC	US\$ 2.916	2,70 sat/vB
33045...fd899	0,2676 BTC	US\$ 7.798	13,1 sat/vB
f672f...b26c8	0,0189 BTC	US\$ 550	3,81 sat/vB
09e18...a8208	0,0002 BTC	US\$ 6	2,66 sat/vB
c977d...bac4b	0,1409 BTC	US\$ 4.107	3,84 sat/vB

MEMPOOL – Lista de transações a serem mineradas.

O qu



 **bitaddress.org**
Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet Paper Wallet Bulk Wallet Brain Wallet
Vanity Wallet Split Wallet Wallet Details

Generate New Address Print

Bitcoin Address

Chave Pública



SHARE

14f1aMNF9Pgav8yRyS8xSpwG3zXmuY6o6b

Chave Privada

SECRET



Private Key

Kyye4LJLWXjom1R37R6oBVpuEFSCqzeLsiJz5mkEVpDc4SxNUyFL

ENTENDENDO AS CHAVES DO BITCOIN – Chave pública versus Chave privada.

O que é chave privada?



Endereço Bitcoin



Chave pública



1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9

Chave privada

abacate beleza ourico
remendo pausa longo
trancar timido veludo
rua titulo jarra

Chave privada



5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn

O que é chave privada?

Onde deve guardar as suas chaves privadas?



À semelhança de qualquer palavra-passe, é crucial manter as suas chaves privadas em segurança. As duas principais formas de as manter sob controlo são:

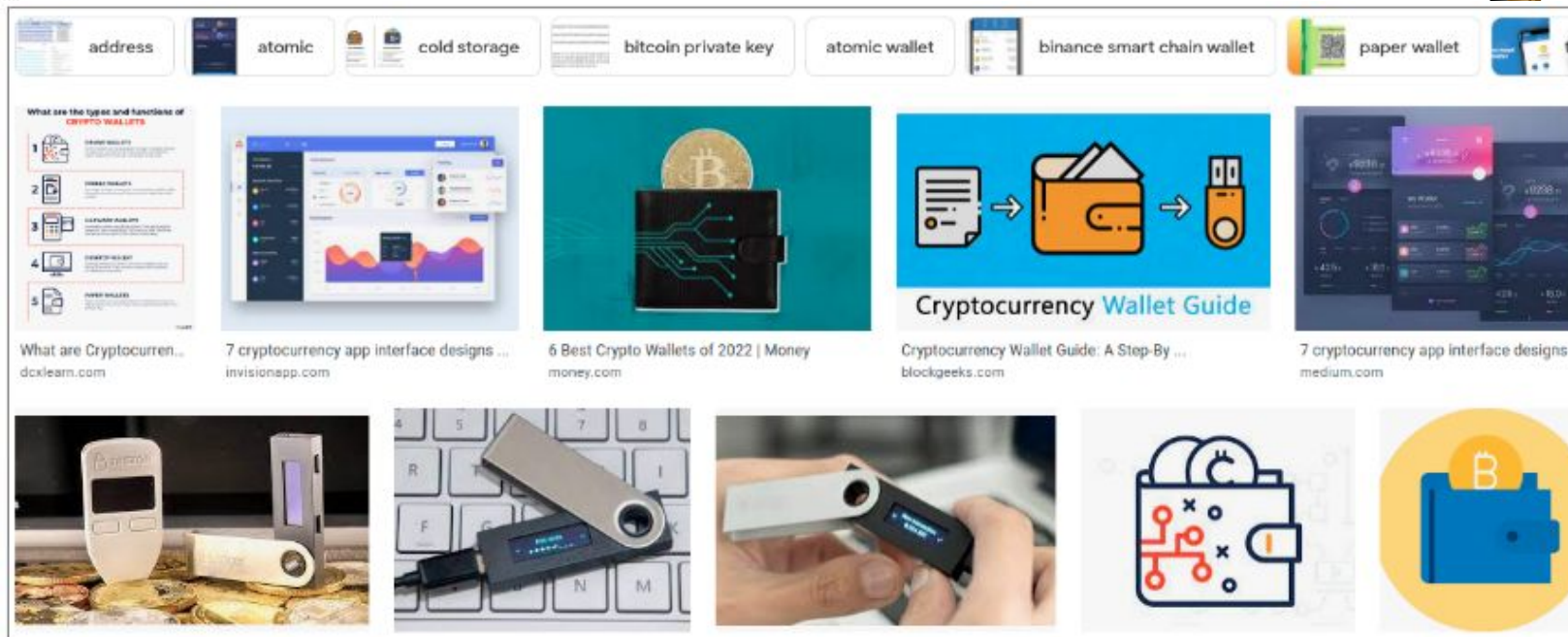
- **Armazená-las online numa carteira de criptomoedas:** a opção melhor e mais simples para a maior parte das pessoas consiste em usar uma carteira virtual, como a oferecida pela Coinbase, para gerir as suas chaves privadas. Estas são conhecidas como carteiras "quentes".

← **Hot wallet**

- **Armazená-las offline num local seguro:** alguns investidores optam por manter as respetivas chaves privadas num computador que não esteja ligado à internet, escritas em papéis ou até memorizadas.

← **Cold wallet**

O que é chave privada?



CARTEIRAS DO BITCOIN – Quentes “hot” ou Frias “cold”.



O que é criptomoeda?

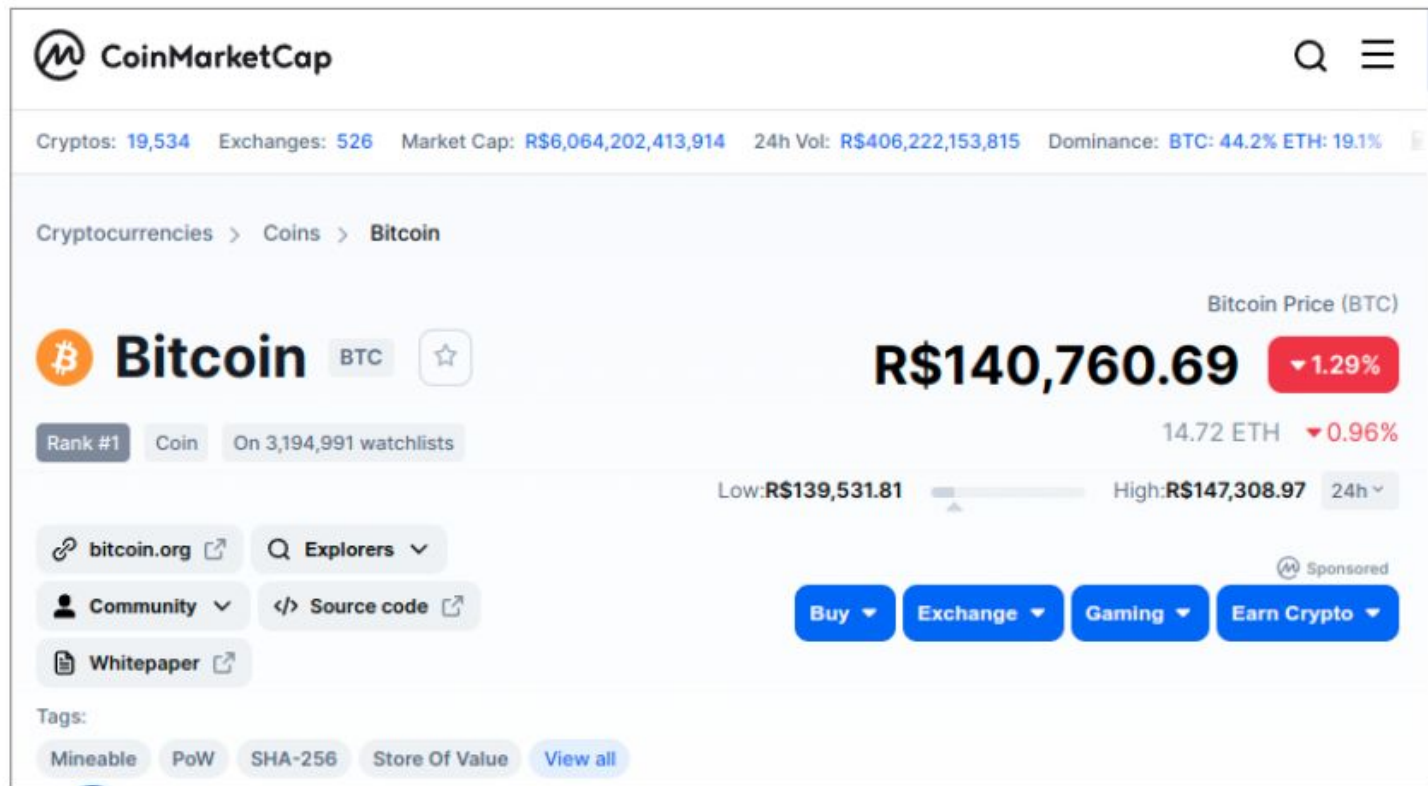
O que é criptomoeda?



#	Nome	Preço	Variação	Gráfico	Negociar
1	 Bitcoin BTC	R\$ 140.399,84	-3,46%		comprar
2	 Ethereum ETH	R\$ 9.529,02	-2,75%		comprar
3	 Cardano ADA	R\$ 2,48	-4,93%		comprar
4	 Solana SOL	R\$ 238,14	-5,44%		comprar

COINBASE – Visualizando as cotações das criptomoedas.



O q



CoinMarketCap

Cryptos: 19,534 Exchanges: 526 Market Cap: R\$6,064,202,413,914 24h Vol: R\$406,222,153,815 Dominance: BTC: 44.2% ETH: 19.1%

Cryptocurrencies > Coins > Bitcoin




 **Bitcoin** BTC 




Rank #1 Coin On 3,194,991 watchlists



Bitcoin Price (BTC)
R\$140,760.69 ▼ 1.29%

14.72 ETH ▼ 0.96%


Low: R\$139,531.81 High: R\$147,308.97 24h

 bitcoin.org  Explorers 

 Community  Source code 

 Whitepaper 

Tags: Mineable PoW SHA-256 Store Of Value [View all](#)

 Sponsored

[Buy](#) [Exchange](#) [Gaming](#) [Earn Crypto](#)



COINMARKETCAP – Visualizando os detalhes de um projeto cripto.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

WHITEPAPER – Uma descrição completa de uma criptomoeda.

O que



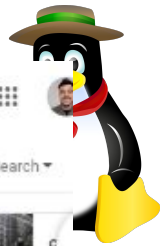
ICO – Oferta inicial de ativos virtuais ou oferta inicial de moedas.

O que é criptomoeda?



O que é mineração de criptomoedas?

A maioria das criptomoedas é "minada" através de uma rede descentralizada (também conhecida como peer-to-peer) de computadores. Mas a mineração não gera apenas mais Bitcoin ou Ethereum - é também o mecanismo que atualiza e protege a rede verificando constantemente o livro razão do blockchain público e adicionando novas transações.


[antminer](#)

[miner](#)

[mining](#)

[farm](#)

[bitcoin miner](#)

[logo](#)

[antpool](#)

[ethereum](#)

[asic](#)

[c](#)


BITMAIN
bitmain.com



Bitmain Antminer S9 13.5 TH ...
shopee.com.br



Bitmain lança minerador de Bitcoin que ...
cointelegraph.com.br



BITMAIN
bitmain.com



Bitcoin Bitmain Antminer Differnet L...
pt.dhgate.com



BITMAIN – Um dos maiores pools de mineração do mundo.



O que é um protocolo?

O que é um protocolo?



Definição

Os protocolos são conjuntos de regras básicas que permitem a partilha de dados entre computadores. Para as criptomoedas, estabelecem a estrutura do blockchain: a base de dados distribuída que permite que o dinheiro digital seja trocado de forma segura na internet.

Porque é que os protocolos são importantes?

Os protocolos permitem que as criptomoedas sejam descentralizadas através do blockchain, o que significa que estão distribuídas por uma rede de computadores sem hub central ou autoridade.

O que é um protocolo?



Protocolo no código

Search or jump to... Pull requests Issues Marketplace Explore

bitcoin / bitcoin Public Watch 3.9k Fork 32.2k Star 63.5k

<> Code Issues 602 Pull requests 405 Projects 6 Security Insights

master 7 branches 266 tags Go to file Add file Code

hebasto Merge bitcoin-core/gui#587: refactor: Replace `GUIUtil::ObjectInvo...` ✓ be7a5f2 22 hours ago 33,532 commits

.github	doc: Remove label from good first issue template	2 years ago
.tx	qt: Update transfex resource blob to 23.0	3 months ago
build-aux/m4	build: stop overriding user CXXFLAGS	20 days ago
build_msvc	Revert "build: Specify zeromq port explicitly for MSVC builds"	10 days ago
ci	ci: Make log verbose in error case only	9 days ago

About

Bitcoin Core integration/staging tree

bitcoincore.org/en/download

c-plus-plus cryptography bitcoin p2p

cryptocurrency

Readme MIT License 63.5k stars 3.9k watching

BITCOIN CORE – Projeto disponível no GitHub.



O que é blockchain?

O que é blockchain?

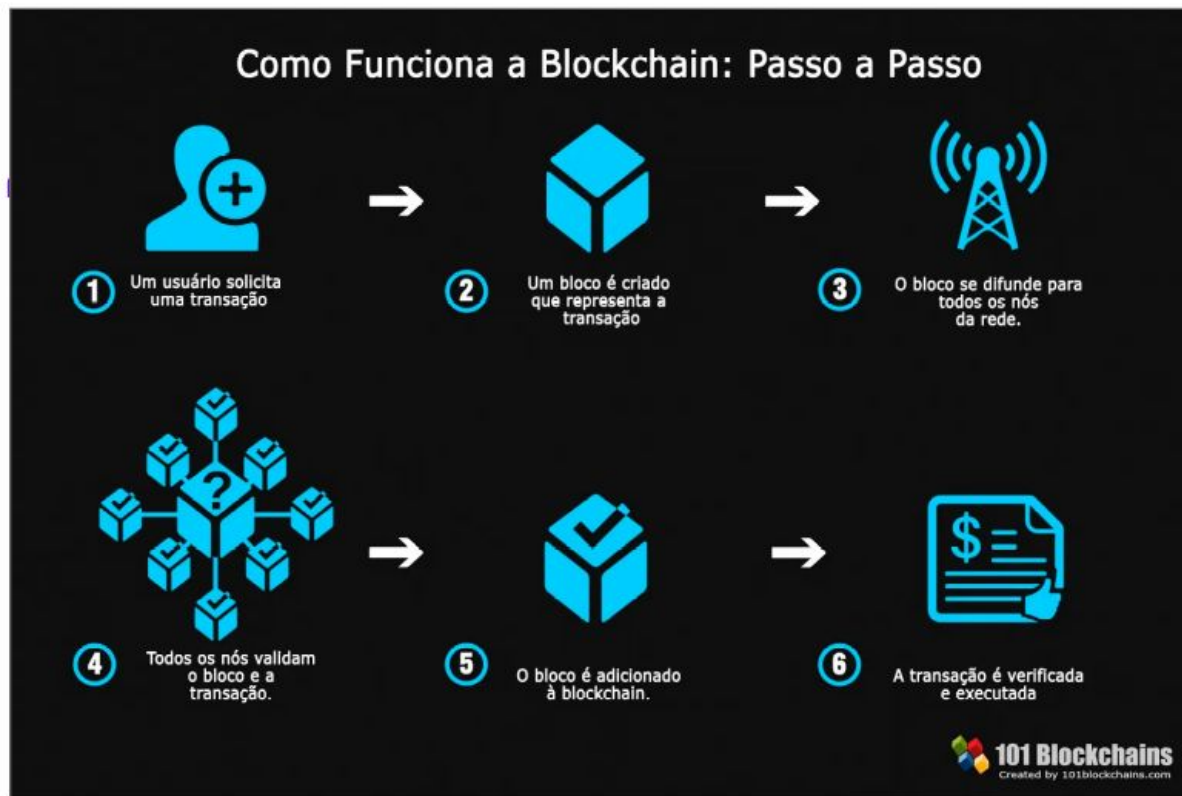


Na sua forma mais básica, um blockchain é uma lista de transações que qualquer pessoa pode ver e verificar. O blockchain Bitcoin, por exemplo, contém um registo de cada vez que alguém enviou ou recebeu bitcoins.

As criptomoedas e a tecnologia de blockchain que as capacita tornam possível transferir valor online sem a necessidade de um intermediário, tal como um banco ou empresa de cartões de crédito.

Imagine uma alternativa aberta e global a todos os serviços financeiros que utiliza atualmente, acessível com pouco mais do que um smartphone e ligação à internet.

O que é



BLOCKCHAIN – Como funciona a tecnologia.



O que é um fork?

O que é um fork?



Porque é que isso é importante?

Um fork ocorre para tornar uma criptomoeda mais segura ou adicionar outras funcionalidades.

- **Soft fork:** foram utilizados para introduzir novas funções ou funcionalidades, geralmente ao nível da programação, de Bitcoin e Ethereum. Uma vez que o resultado final é um só blockchain, as alterações são retrocompatíveis com os blocos pré-fork.
- **Hard fork:** um hard fork ocorre quando o código se altera de tal modo que a nova versão deixa de ser retrocompatível com blocos mais antigos. Neste cenário, o blockchain divide-se em dois: o blockchain original e uma nova versão que segue um novo conjunto de regras.



Criando a nossa própria moeda

Criando a nossa própria moeda



APUSCOIN

Run Terminal He

node_01.py X

node_01.py > ...

```
9 # Parte 1 - Cria a moeda Apuscoin (transações)
10
11 class Blockchain:
12     # função de inicialização
13     def __init__(self): # "self" usa as variáveis do objeto
14         self.chain = [] # lista Python como o bloco
15         # cria uma lista para as transações: as transações são adicionada
16         self.transactions = []
17         # cria o bloco gênese
18         self.create_block(proof = 1, previous_hash = '0')
19         # adiciona os nós participantes da rede através de um set (mais o
20         self.nodes = set()
21
22     # função que cria um bloco com suporte a transações e adiciona ao blo
23     def create_block(self, proof, previous_hash): # faz o link com o blo
24         # cria o dicionário com as 5 chaves do bloco: índice, timestamp,
25         # importante: o bloco é criado depois ser de minerado (proof-of-w
26         block = {
27             'index': len(self.chain) + 1,
28             'timestamp': str(datetime.datetime.now()),
```

Principais referências

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-cryptography>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-private-key>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-cryptocurrency>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-blockchain>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-fork>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-bitcoin-halving>

<https://www.coinbase.com/pt/learn/crypto-basics/what-is-a-protocol>

<https://polkadot.network/>

<https://coinmarketcap.com/currencies/polkadot-new/>

<https://holdbtc100.com/>

<https://www.pagcripto.com.br/>

<https://coinmarketcap.com/currencies/bitcoin/>

<https://mempool.space/pt/>