

UNIVERSIDADE DA REGIÃO DA CAMPANHA
CENTRO DE CIÊNCIAS EXATAS E AMBIENTAIS
CURSO DE SISTEMAS DE INFORMAÇÃO
FLISOL/BAGÉ

Introdução às criptomoedas: criando a sua própria moeda como o Bitcoin!

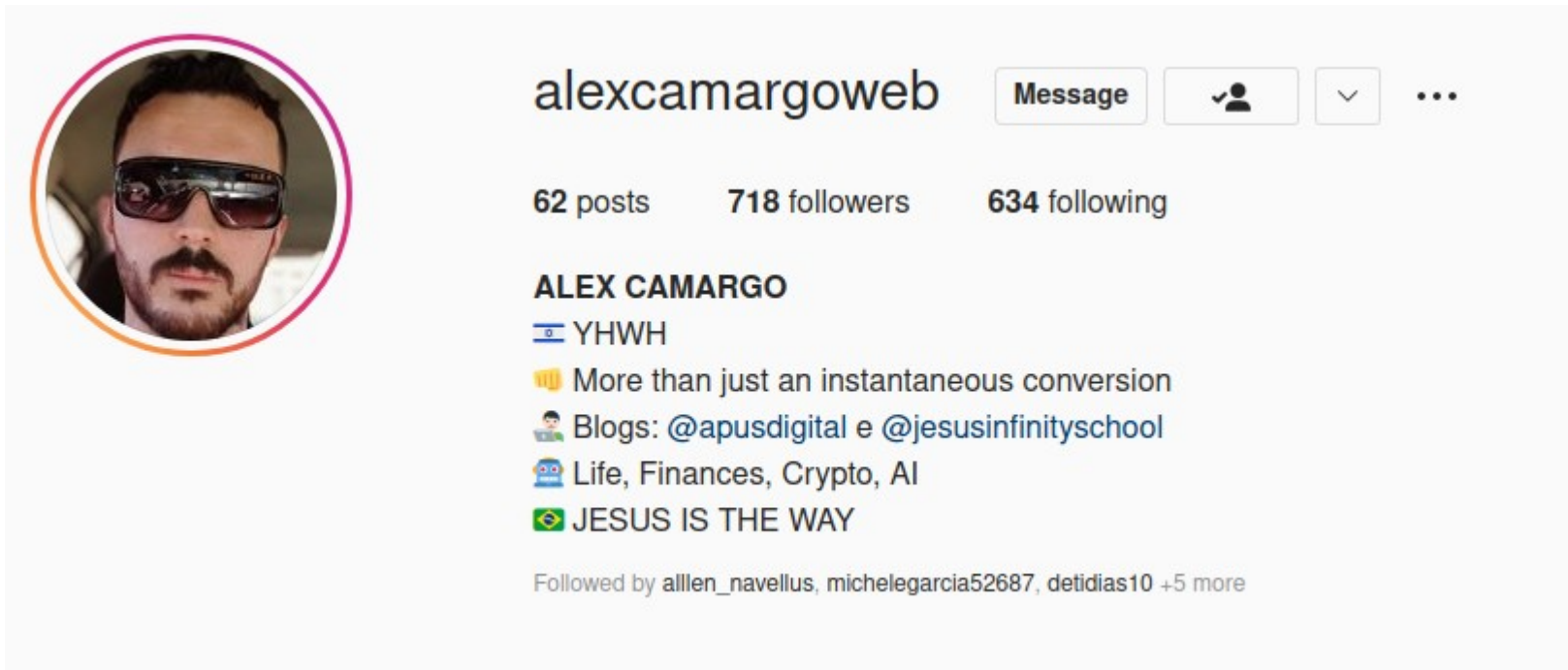
Por: Alex Camargo e Ezequiel Tavares

@alexcamargoweb @ezequiel_tav



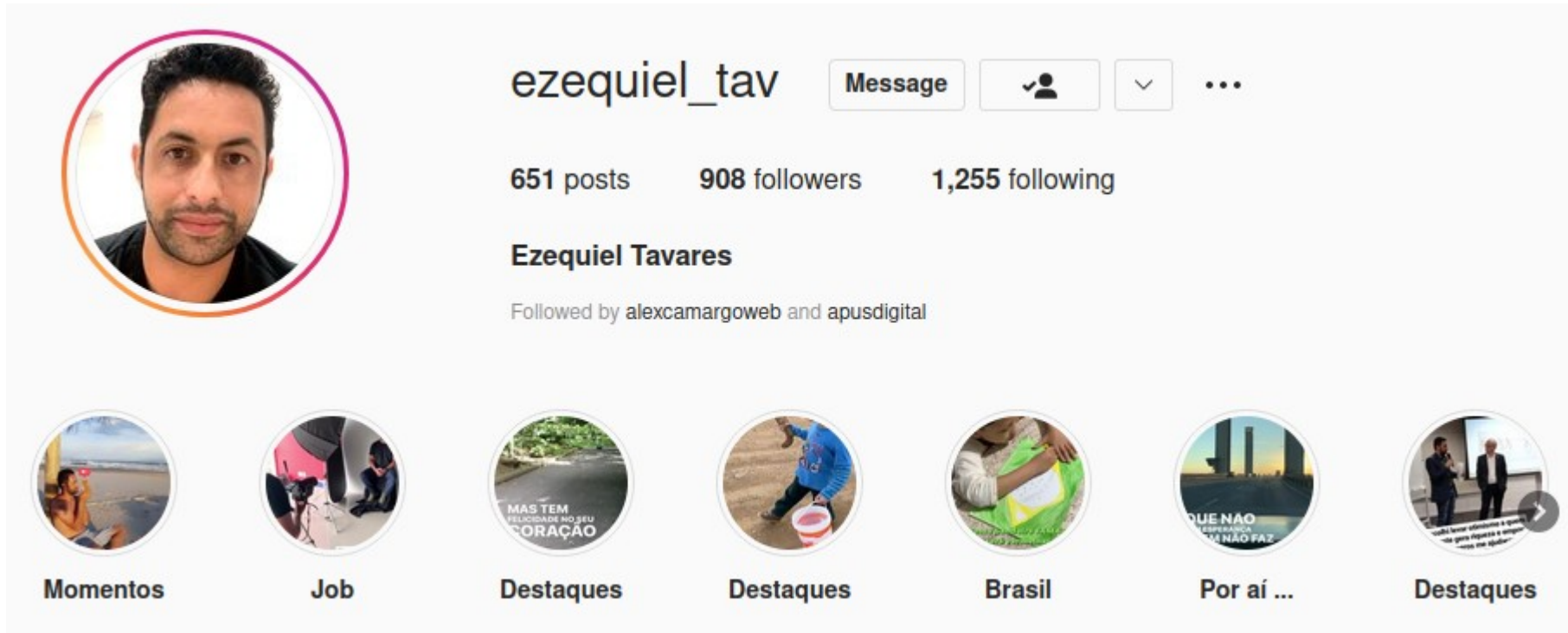
Abril/2022

Os autores



#metodologiasageis #visaocomputacional #python #linux
 #ubuntu #centos #aws #googlecolab #bioinformatica
 #criptomoedas #teologia #arqueologia #astronomia #musica

Os autores



The image shows the Instagram profile of ezequiel_tav. The profile picture is a circular portrait of a man with dark hair and a beard. The username 'ezequiel_tav' is displayed in a large font, with a 'Message' button and a dropdown menu to its right. Below the username, the statistics are shown: '651 posts', '908 followers', and '1,255 following'. The full name 'Ezequiel Tavares' is listed, followed by the text 'Followed by alexcamargoweb and apusdigital'. At the bottom, there is a row of seven story highlights with circular thumbnails and labels: 'Momentos', 'Job', 'Destaques', 'Destaques', 'Brasil', 'Por aí ...', and 'Destaques'.

#metaverso #criptomoedas #blockchain #metodologiasageis
#devmobile #robotica #impressao3D #música #causasanimal

O que veremos a seguir

Da teoria ao código =)

- ☐ **O que é a criptografia?**
- ☐ **O que é uma chave privada?**
- ☐ **O que é criptomoeda?**
- ☐ **O que é um protocolo?**
- ☐ **O que é um fork?**
- ☐ **O que é um blockchain?**
- ☐ **O que é uma divisão de Bitcoins?**
- ☐ **Curiosidades sobre o Bitcoin**
- ☐ **Criando a sua própria moeda**
- ☐ **Referências**

O que é a criptografia?



O que é a 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 a criptografia?


BLOCKCHAIR

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


 Bitcoin · Transactions

Bitcoin transaction
API


200% on Deposit \$

Transaction hash
1810e267c0f7ac947672a70992b1a7266bb12a04eed616d40f33f5e60f1c1ffc

Amount transacted ?
0.00353392 BTC · 140.59 USD

Transaction fee ?
0.0000741 BTC · 2.95 USD

Fee per vbyte
1 satoshi


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

Additional info
 Transaction receipt

Senders 50
1JMNnxue9Z497qgxNbGC3md3mFQuQZ
 Unsx
 0.00001698 BTC · 0.68 USD

Recipient
bc1qppeskrjpe0rt
p4apdjs0mu5n
 0.00353392 BTC · 140.59 USD

O que é uma chave privada?



O que é uma chave privada?

Chave privada

Uma chave privada é como uma palavra-passe, uma sequência de letras e números, que lhe permite aceder e gerir os seus fundos em criptomoedas.

Ao comprar criptomoedas pela primeira vez, são emitidas duas chaves: uma chave pública, que funciona como um endereço de e-mail (o que significa que pode partilhá-la em segurança com outras pessoas, permitindo-lhe enviar ou receber fundos), e uma chave privada, que geralmente é uma sequência de letras e números (e que não deve ser partilhada com quem quer que seja).

O que é uma chave privada?



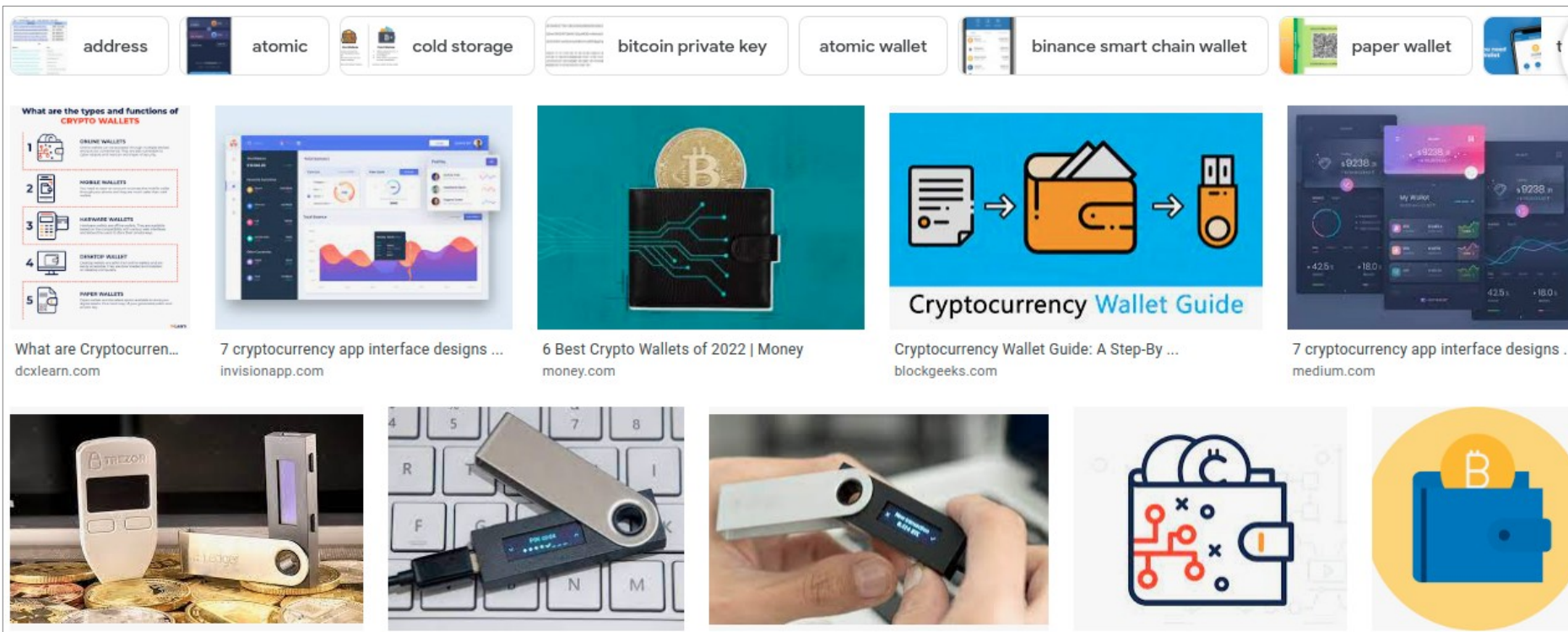
O que é uma chave privada?

Onde deve guardar as suas chaves privadas?

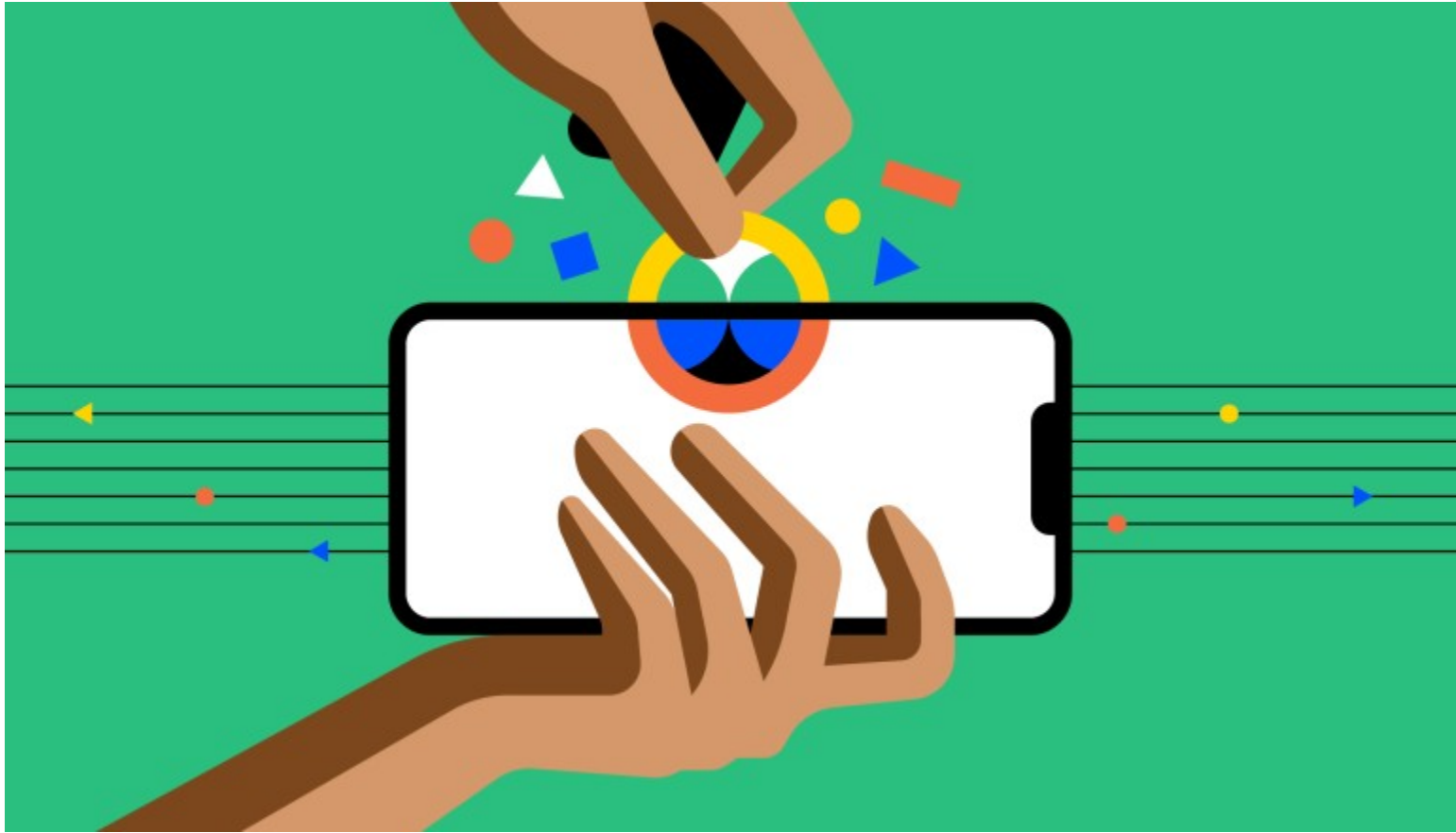
À semelhança de qualquer palavra-passe, é crucial manter as suas chaves privadas em segurança. As duas principais formas de as manter sob controlo são:

- **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".
- **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.

O que é uma chave privada?



O que é criptomoeda?



O que é criptomoeda?



No seu núcleo, a criptomoeda é, **normalmente, dinheiro digital descentralizado criado para ser utilizado na internet**. Bitcoin, lançada em 2008, foi a primeira criptomoeda e permanece, de longe, a maior, mais influente e a mais conhecida. Na década que se seguiu, Bitcoin e outras criptomoedas, tais como Ethereum, cresceram como alternativas digitais ao dinheiro emitido por governos.

As criptomoedas são **a primeira alternativa ao sistema bancário tradicional** e têm fortes vantagens sobre os métodos de pagamento anteriores e as tradicionais classes de ativos. Pense nelas como Dinheiro 2.0. -- um novo tipo de dinheiro que é nativo à internet.

O que é criptomoeda?

coinbase

Preços Recursos Indivíduos Empresas Desenvolvedores Coinbase Entrar Começar

#	Nome	Preço	Variação	Gráfico	Negociar
1	 Bitcoin BTC	R\$ 190.773,47	-1,20%		comprar
2	 Ethereum ETH	R\$ 14.235,70	-1,19%		comprar
3	 Cardano ADA	R\$ 4,32	-1,41%		comprar
4	 Solana SOL	R\$ 490,94	+1,14%		comprar

O que é criptomoeda?

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.

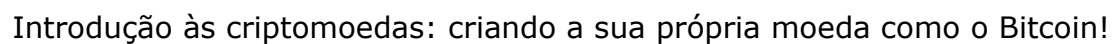
1. Introduction

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

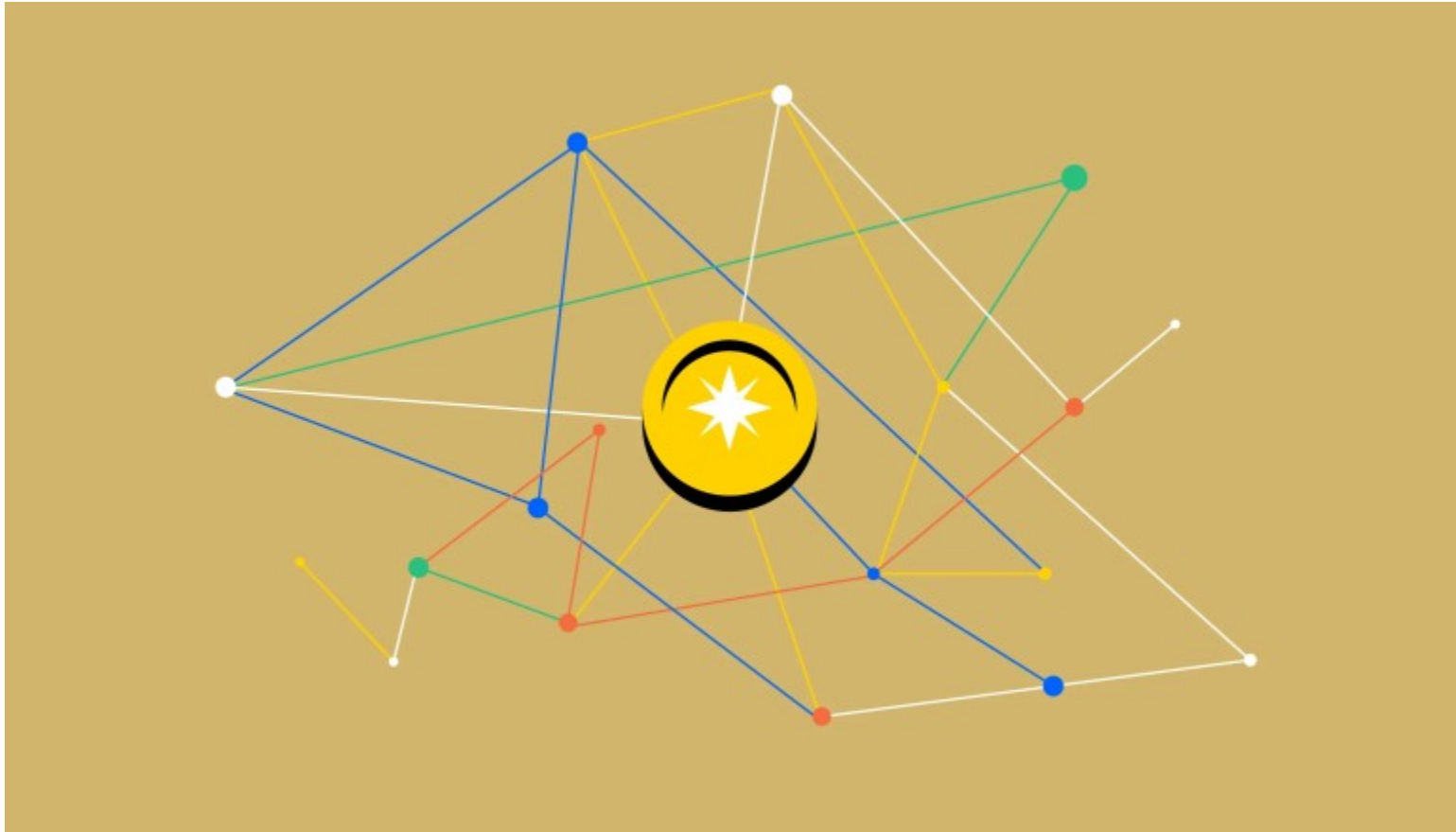
O que é criptomoeda?

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.



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?

GitHub interface for the `bitcoin/bitcoin` repository.

Navigation: Pull requests, Issues, Marketplace, Explore

Repository: `bitcoin / bitcoin` (Public)

Stats: Watch 3.9k, Fork 32.2k, Star 63.5k

Code, Issues (602), Pull requests (405), Projects (6), Security, Insights

Branches: master, 7 branches, 266 tags

Buttons: Go to file, Add file, Code

About: Bitcoin Core integration/staging tree

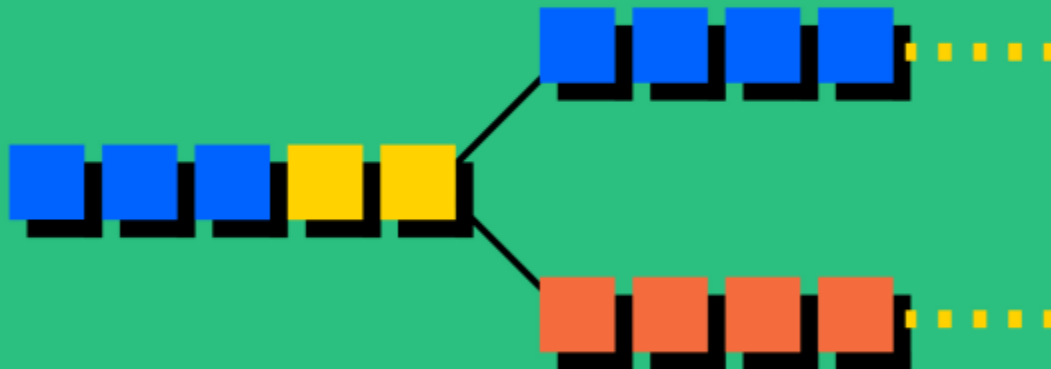
Link: bitcoincore.org/en/download

Tags: c-plus-plus, cryptography, bitcoin, p2p, cryptocurrency

Readme, MIT License, 63.5k stars, 3.9k watching

Commit	Message	Time
hebasto Merge bitcoin-core/gui#587: refactor: Replace `GUIUtil::ObjectInvo...	doc: Remove label from good first issue template	2 years ago
be7a5f2	qt: Update transifex resource blob to 23.0	3 months ago
	build: stop overriding user CXXFLAGS	20 days ago
	Revert "build: Specify zeromq port explicitly for MSVC builds"	10 days ago
	ci: Make log verbose in error case only	9 days ago

O que é um fork?



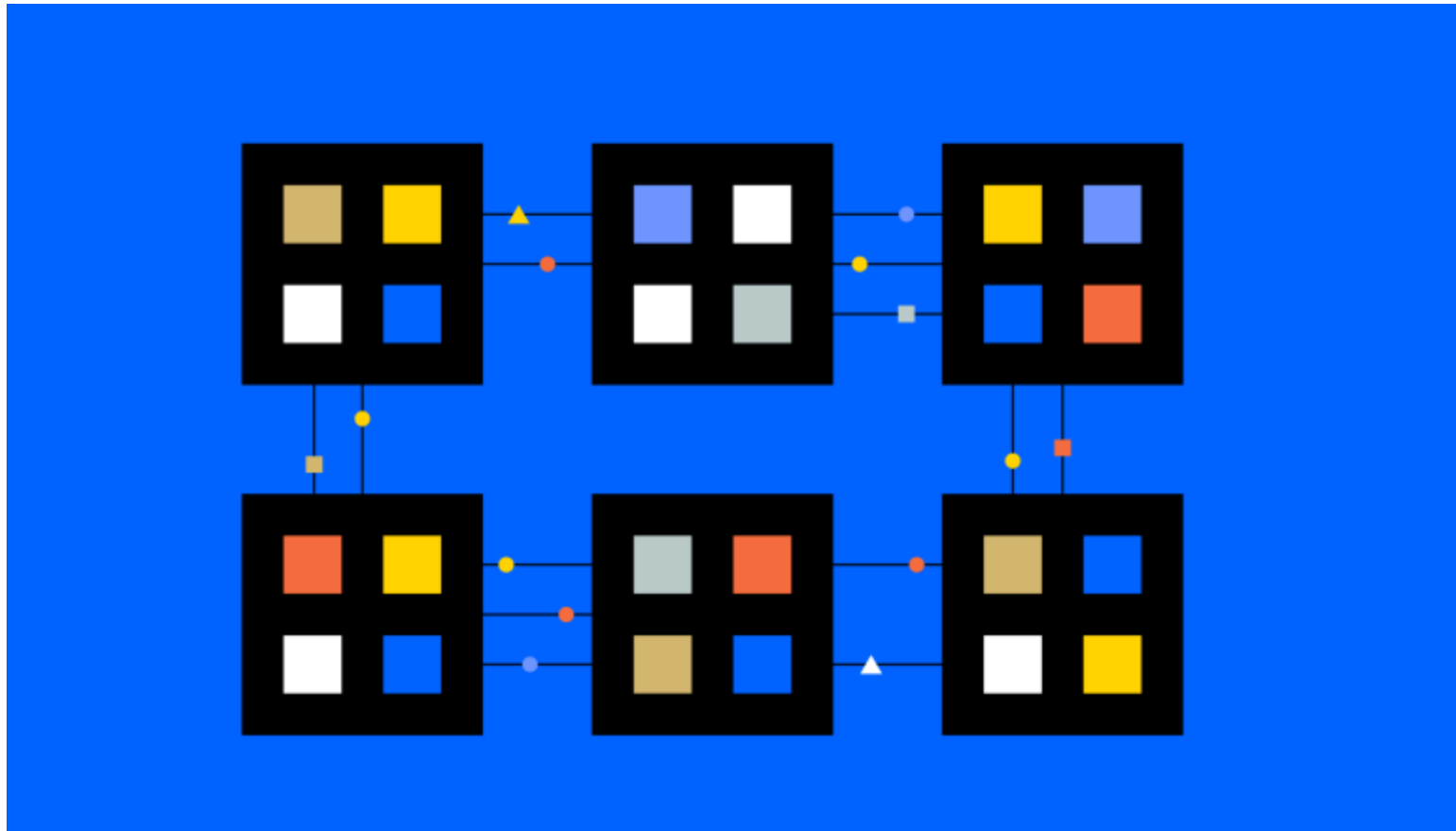
O que é um fork?

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.

O que é um blockchain?



O que é um 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.

Como Funciona a Blockchain: Passo a Passo



1 Um usuário solicita uma transação



2 Um bloco é criado que representa a transação



3 O bloco se difunde para todos os nós da rede.



4 Todos os nós validam o bloco e a transação.

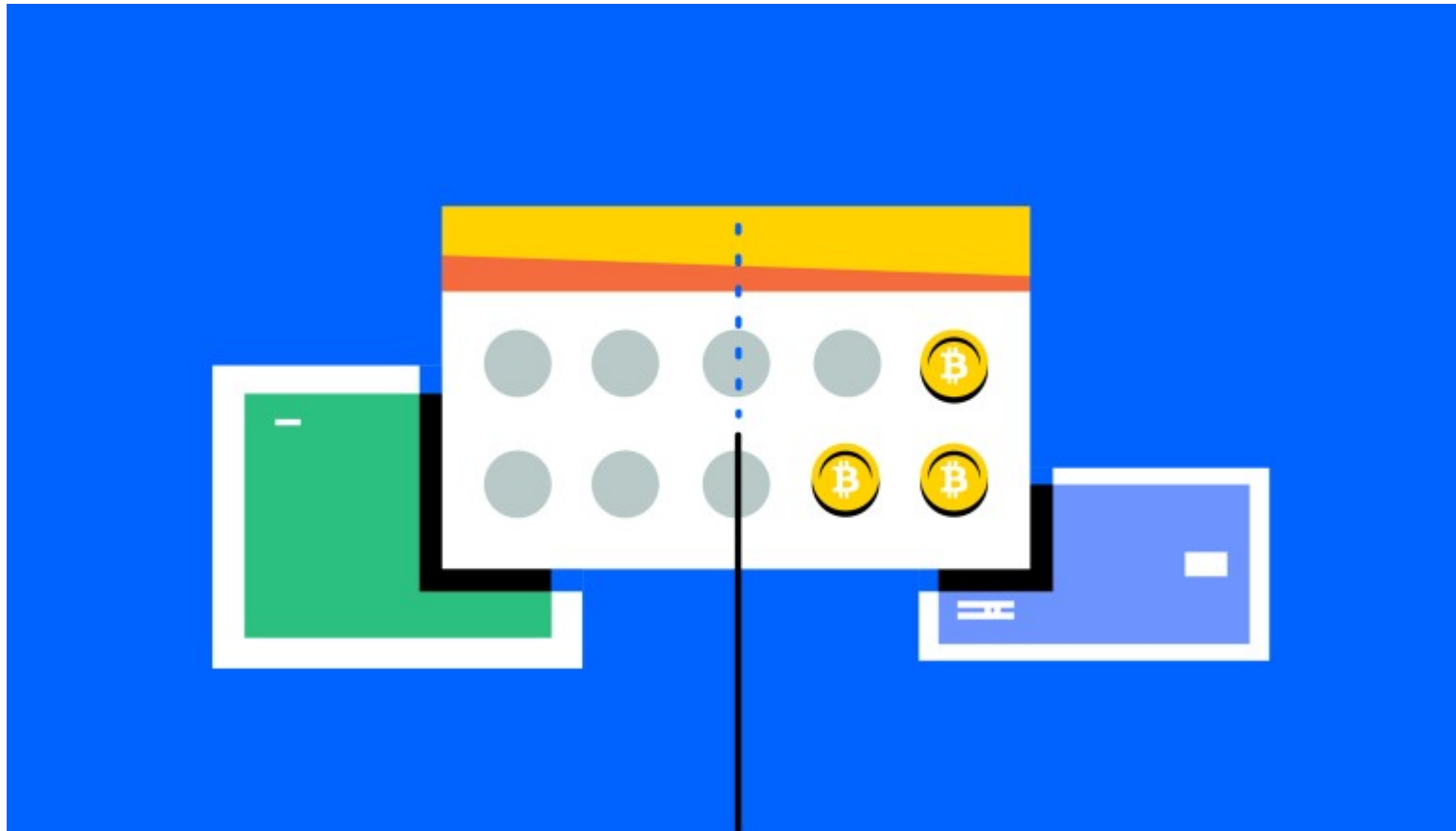


5 O bloco é adicionado à blockchain.



6 A transação é verificada e executada

O que é uma divisão de Bitcoins?



O que é uma divisão de Bitcoins?

Definição

A cada quatro anos, o valor de bitcoins concedidas aos mineiros é reduzido para metade, até que a totalidade dos 21 milhões de bitcoins tenham sido virtualmente minerados (provavelmente perto do ano 2140). O mecanismo de divisão contribui para que a bitcoin seja um recurso escasso e resistente à inflação.

- Tal como o ouro, a Bitcoin é minerada, mas isso é efetuado eletronicamente através de uma rede global de computadores que competem para verificar as transações de bitcoins.
- Os mineiros são recompensados em bitcoins. No início de 2020, foram entregues 12,5 novas bitcoins a cada 10 minutos. Em maio, a recompensa foi dividida, ou seja, foi reduzida para 6,25 novas bitcoins a cada 10 minutos.



50



2009

BITCOIN HALVING

25



2012

12.5



2016

6.25



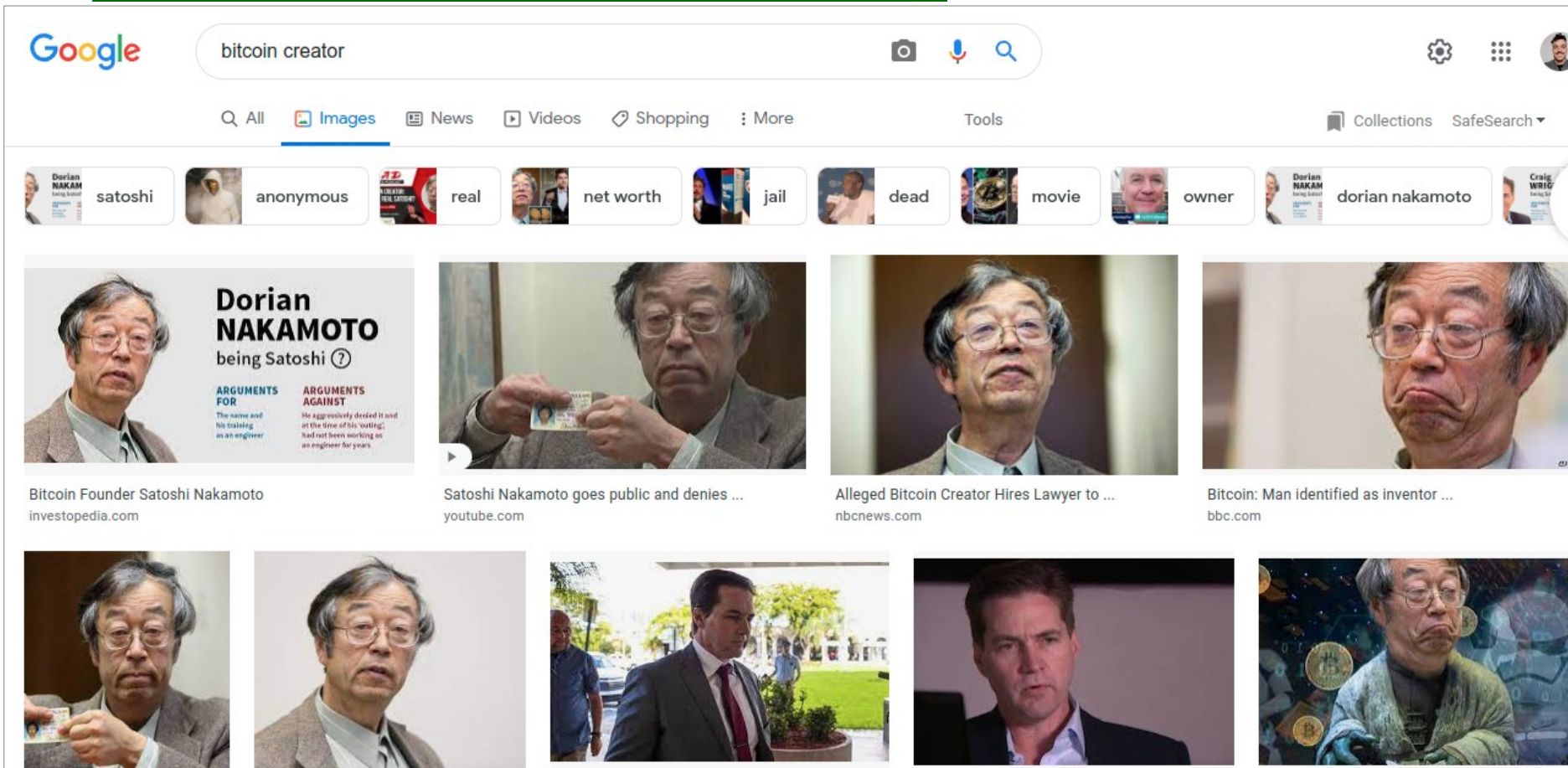
2020

Curiosidades sobre o Bitcoin

1 -- Até hoje, ninguém viu o criador da bitcoin

Em meados de 2008, um desenvolvedor identificado apenas como Satoshi Nakamoto publicou um estudo sobre o funcionamento de um mercado virtual e deu origem à criptomoeda mais famosa do mundo. A identidade de Nakamoto, no entanto, nunca foi comprovada.

Curiosidades sobre o Bitcoin



A screenshot of a Google search for "bitcoin creator". The search bar shows the query "bitcoin creator". Below the search bar, there are tabs for "All", "Images", "News", "Videos", "Shopping", and "More". The "Images" tab is selected. Below the tabs, there are several image thumbnails with labels: "satoshi", "anonymous", "real", "net worth", "jail", "dead", "movie", "owner", "dorian nakamoto", and "Craig Wright". Below the thumbnails, there are several image results with captions:

- Dorian NAKAMOTO being Satoshi ?** (with sub-headings "ARGUMENTS FOR" and "ARGUMENTS AGAINST") from investopedia.com.
- Satoshi Nakamoto goes public and denies ...** from youtube.com.
- Alleged Bitcoin Creator Hires Lawyer to ...** from nbcnews.com.
- Bitcoin: Man identified as inventor ...** from bbc.com.
- Other images showing Satoshi Nakamoto holding a Bitcoin card, a man in a suit, and a man in a green jacket.

Curiosidades sobre o Bitcoin

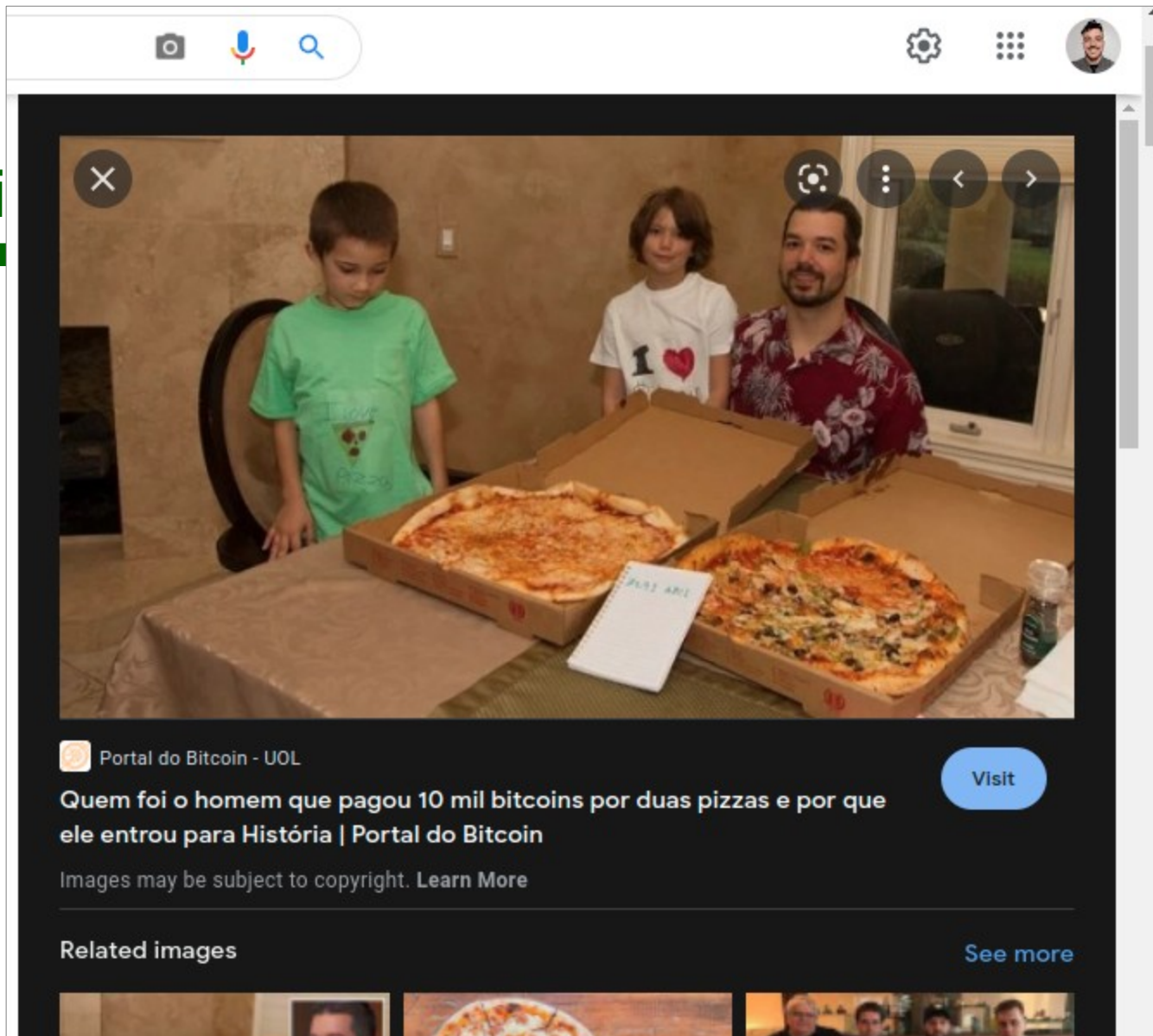
1 -- Até hoje, ninguém viu o criador da bitcoin

Em meados de 2008, um desenvolvedor identificado apenas como Satoshi Nakamoto publicou um estudo sobre o funcionamento de um mercado virtual e deu origem à criptomoeda mais famosa do mundo. A identidade de Nakamoto, no entanto, nunca foi comprovada.

2 -- 10 mil bitcoins por duas pizzas

A primeira transação comercial com bitcoins foi feita no dia 22 de maio de 2010. Naquele dia, um programador gastou 10 mil bitcoins em duas pizzas. O valor pode até parecer absurdo, mas naquela época não era lá muita coisa.

Curi



Curiosidades sobre o Bitcoin

3 -- O valor de mercado da bitcoin é maior que o do McDonald's e o da Disney

Se todos as bitcoins existentes forem multiplicados pela cotação da moeda, o valor ultrapassaria os 170 bilhões de dólares.

4 -- A criptomoeda já foi dividida duas vezes

Hoje, além da próprio bitcoin, existe a bitcoin cash e a bitcoin gold. As novas versões surgiram em agosto e outubro deste ano, respectivamente, após um conflito de membros da comunidade sobre a escolha de uma atualização de um software. Originalmente, o design da bitcoin limita a quantidade de informação em sua rede, visando a proteção de ataques cibernéticos.

Curiosidades sobre o Bitcoin

BCH vs. BTG		
	Bitcoin Cash	Bitcoin Gold
Hashing Function	Uses the SHA-256 mining algorithm	Uses the Equihash mining algorithm
Mining	Can be mined on ASIC miners	ASIC miner resistant
Protocol	SecureSigs protocol	SegWit protocol
Where to Buy	Available on popular exchanges	Not available on popular exchanges
Total Supply	19 million in circulation	17.5 million in circulation

Curiosidades sobre o Bitcoin

5 -- Muitas bitcoins já foram para o lixo

Desde que a moeda digital foi criada, em 2008, foram registrados alguns casos de pessoas que jogaram no lixo HDs com suas preciosas bitcoins.

Curiosidades sobre o Bitcoin

Google bitcoin trash search

3d illustration million bitcoin hard drive bin cfl james howells lost bitcoin wallet waste containment bloc

Man lost \$127 million worth of bitcoin ...
cnbc.com

Lost Bitcoin Wallet ...
iflscience.com

Bitcoin worth 34 billion rupees thrown ...
hindustannewshub.com

Man Accidentally Threw Bitcoin Worth ...
newsweek.com

2013
THE NEWS
SHEPARD
SMITH
BRITISH I.T. WORKER THROWS OUT BITCOIN
HARD DRIVE WORTH MORE THAN \$350M

Lost Bitcoin Wallet ...
iflscience.com

bitcoin fortune offers \$70 million ...
cnn.com

This man's lost bitcoin are now worth ...
wired.co.uk

Lost \$378 Million Bitcoin Fortune ...
u.today

Accidentally Dumped Bitc...
news18.com

Criando a sua própria moeda

```
node_01.py - flisol-2022 - V...
Run Terminal Help
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()),
```



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://exame.com/invest/mercados/10-curiosidades-sobre-a-bitcoin-a-rainha-das-criptomoedas/>