VIVER DE RENDA ₵RIPTO

Módulo 1

Computação Quântica

O Bitcoin vai Cair Até Quando?

Plataforma da Paradigma

Algumas **Perguntas Comuns**

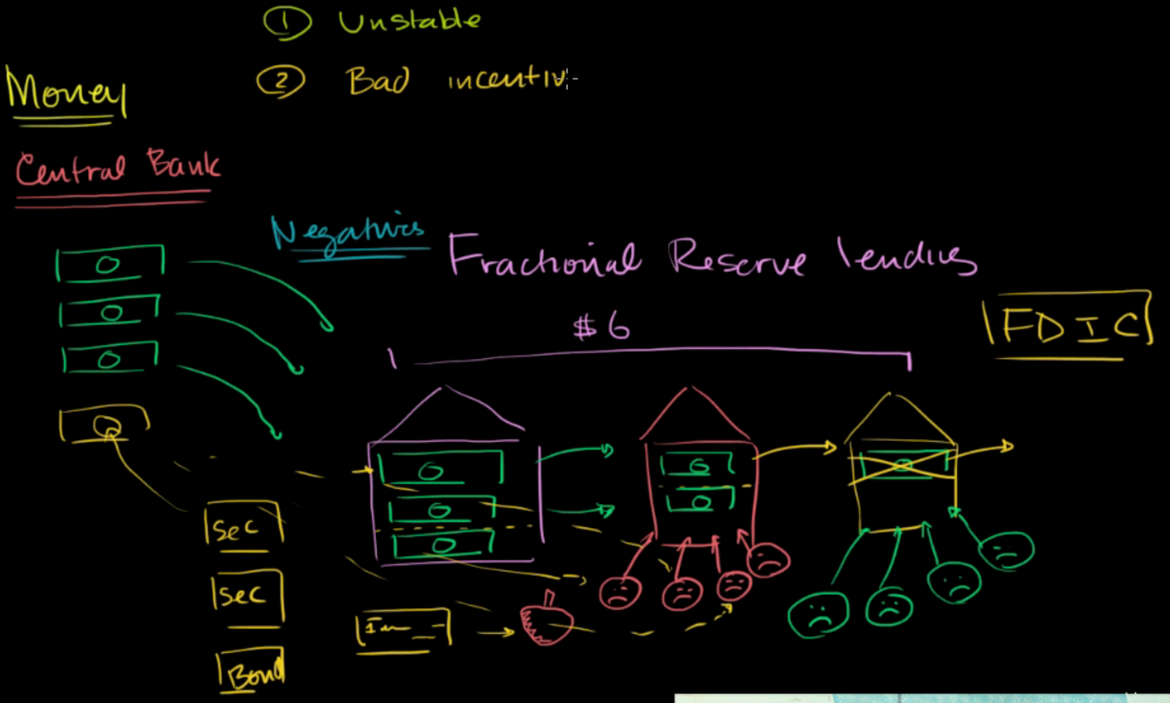
Quanto Comprar

Onde Comprar

Planilha do Bônus

Ninguém entende o sistema por completo!

Ninguém entende o sistema por completo!



O Bitcoin é uma seita quase religiosa!

O Bitcoin é uma seita quase religiosa!

Chorando na Bandeira do Brasil™
@marquinhoroitma

Follow

Hoje eu vi um jornalista chamar o Bitcoin de "uma moeda inventada"

Translate Tweet

6:12 AM - 15 Dec 2017

4,550 Retweets **9,406** Likes

46 4.6K 9.4K

Chorando na Bandeira do Brasil™
@marquinhoroitma

Follow

Hoje eu vi um jornalista chamar o Bitcoin de "uma moeda inventada"

em oposição às outras moedas, que a natureza nos deu

Translate Tweet

6:12 AM - 15 Dec 2017

4,550 Retweets **9,406** Likes

46 4.6K 9.4K

VAMOS COMEÇAR COM UMA HISTÓRIA...

EM 2014, ELES **DOARAM**

U$ 500 MIL

PRA COLEGAS DE CLASSE. EM **BITCOIN**.

04-29-14 | FAST FEED

Every MIT Undergraduate Will Receive $100 In Bitcoin This Fall

With $500,000 in funding, the MIT Bitcoin Project will distribute Bitcoins to the undergraduate student body, who can do with them as they please.

3108
ALUNOS SE INSCREVERAM

U$ 100
PARA CADA

U$ 336
CUSTAVA 1 BTC, NA ÉPOCA

30%
NEM CHEGOU A FAZER UMA WALLET

11%
VENDEU NOS PRIMEIROS **14 DIAS**

25%
VENDEU NOS PRIMEIROS **4 MESES**

14%
SEGUIA “MOVIMENTANDO" AS MOEDAS, NA ÚLTIMA MEDIÇÃO

~DE 11.400 ALUNOS NO CAMPUS...
3.8% "ENTENDERAM A MENSAGEM",
E SEGUEM NO BITCOIN ATÉ HOJE

OS **U$ 500 MIL**
DO EXPERIMENTO HOJE VALEM
~U$ 50 MILHÕES

Jeremy Rubin
BTC Core Dev

Dan Elitzer
Nascent Capital

Sam Trabucco
Alameda Research

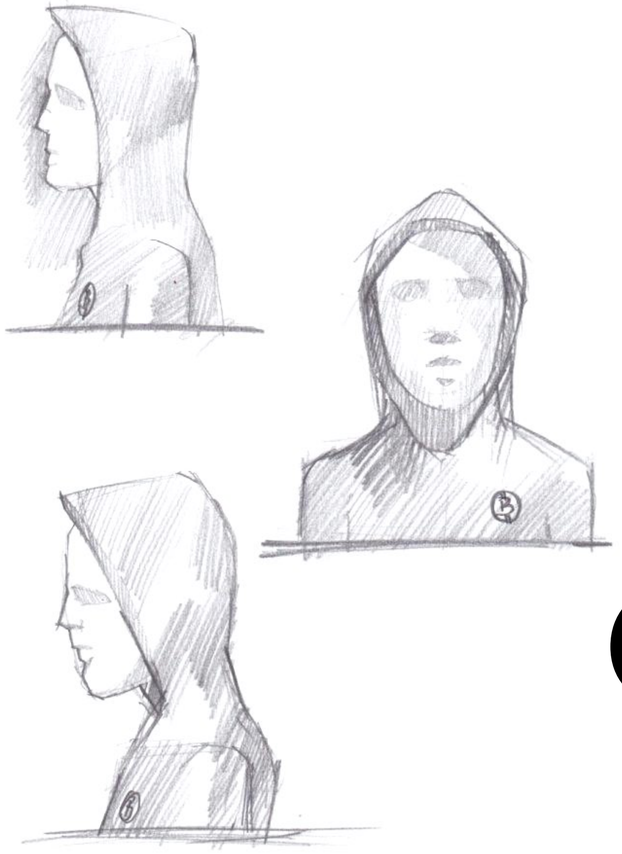
~DE 11.400 ALUNOS NO CAMPUS...
3.8% "ENTENDERAM A MENSAGEM",
E SEGUEM NO BITCOIN ATÉ HOJE

ESPERO QUE MAIS DE
3.8% DE VOCÊS ESTEJAM COLHENDO
OS FRUTOS DAQUI A 7 ANOS

Objetivos de **Hoje**

De Onde Vem o Bitcoin
Como Funcionam Os Ciclos do Mercado
("Qual é a Melhor Hora de Comprar")
A Diferença Entre Bitcoin e Altcoins

Próxima Aula: Comprando, Guardando & Monitorando Moedas
(e 7 Falácias em que Quase Todo Mundo Acredita)



Parte 1

O Mito de Satoshi

BITCOIN

A PEER-TO-PEER ELECTRONIC CASH SYSTEM

SATOSHI NAKAMOTO • OCTOBER 31, 2008

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.*

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

31 de Outubro, 2008

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

A ideia não era nova para os CypherPunks

As an amusing thought experiment, imagine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from $100 trillion to $300 trillion. With 20 million coins, that gives each coin a value of about $10 million.

So the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1! Even if the odds of Bitcoin succeeding to this degree are slim, are they really 100 million to one against? Something to think about...

Hal

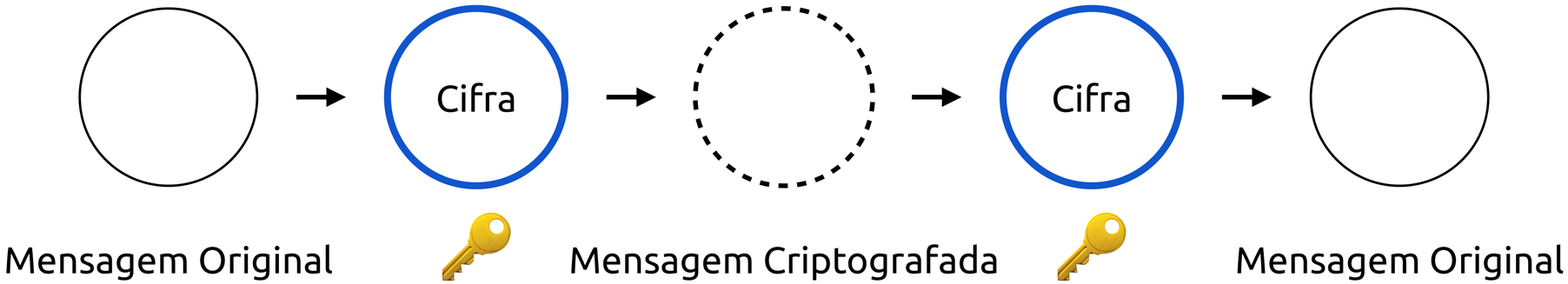
Cypher -> Cifra -> Criptografia

Cypher -> Cifra -> Criptografia

Um ramo da **matemática** dedicado
a **decifrar** e **proteger** **segredos**

A **Segunda Guerra acabou**, em parte, por conta de uma **vulnerabilidade criptográfica.**

Criptografia **Simétrica**



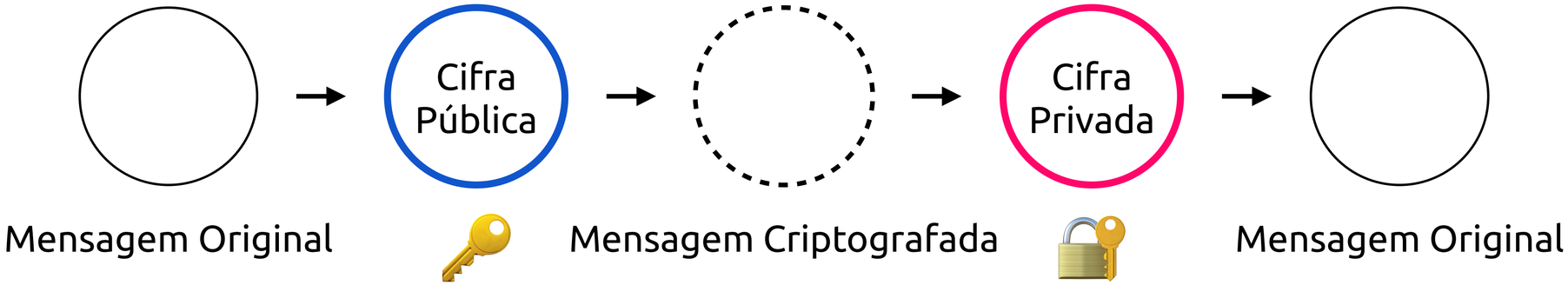
Criptografia foi por muito tempo “**segredo militar**” - classificada até mesmo como **munição**.

Criptografia foi por muito tempo “**segredo militar**” - classificada até mesmo como **munição**.

E **se fosse assim até hoje**, na internet seria impossível de se **comunicar de forma privada** - seria mais fácil de te **espionarem, discriminarem** e **subjugarem.**

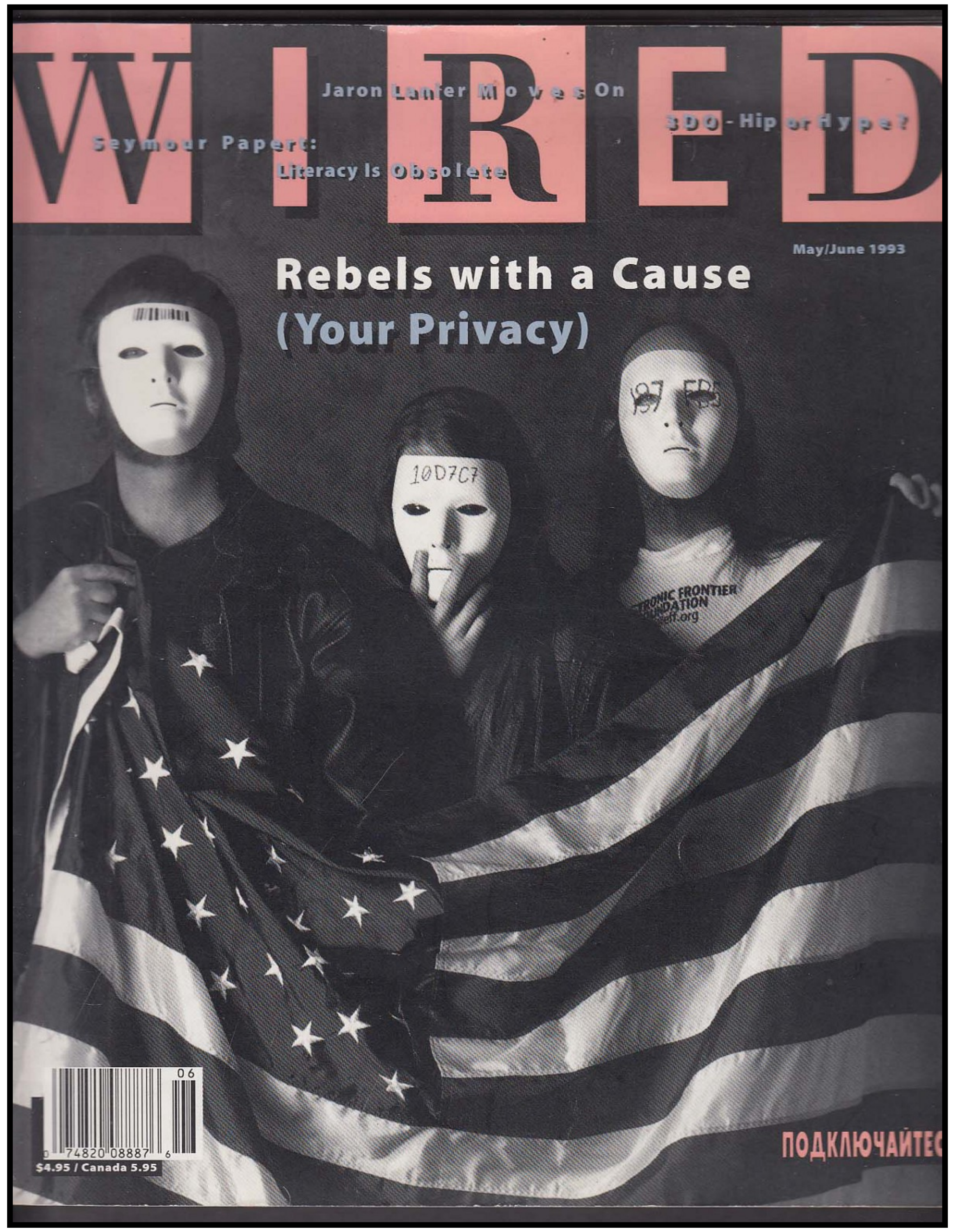
Criptografia **Simétrica**

Criptografia **Assimétrica**

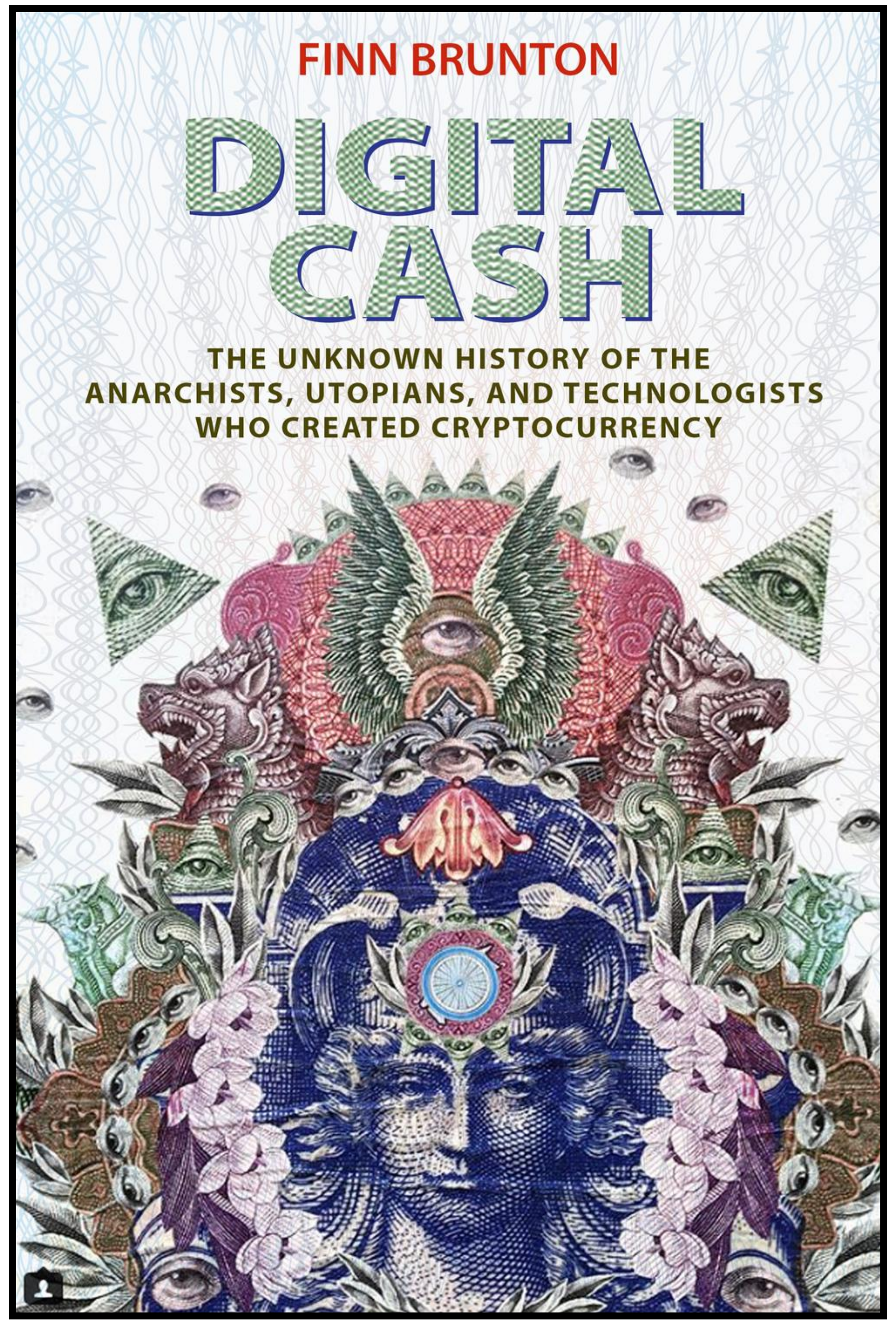



-RSA-Algorithm-PERL


WARNING: THIS MAN IS CLASSIFIED AS A MUNITION
U.S. ITAR/EAR REGULATIONS - RSA IN THREE LINES OF PERL
FEDERAL LAW PROHIBITS TRANSFER OF THIS MAN TO FOREIGNERS


WIRED
Jaron Lanier Moves On
3DO - Hip or Hype?
Seymour Papert:
Literacy Is Obsolete
May/June 1993
Rebels with a Cause
(Your Privacy)
$4.95 / Canada 5.95
ПОДКЛЮЧАЙТЕС


"BENEDICT CUMBERBATCH IS OUTSTANDING"
"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
"AN INSTANT CLASSIC"
★★★★★
"A SUPERB THRILLER"
★★★★
★★★★ ★★★★
THE IMITATION GAME
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
BASED ON THE INCREDIBLE TRUE STORY
IN CINEMAS NOVEMBER 14


FINN BRUNTON
DIGITAL CASH
THE UNKNOWN HISTORY OF THE ANARCHISTS, UTOPIANS, AND TECHNOLOGISTS WHO CREATED CRYPTOCURRENCY

ecash — 1983

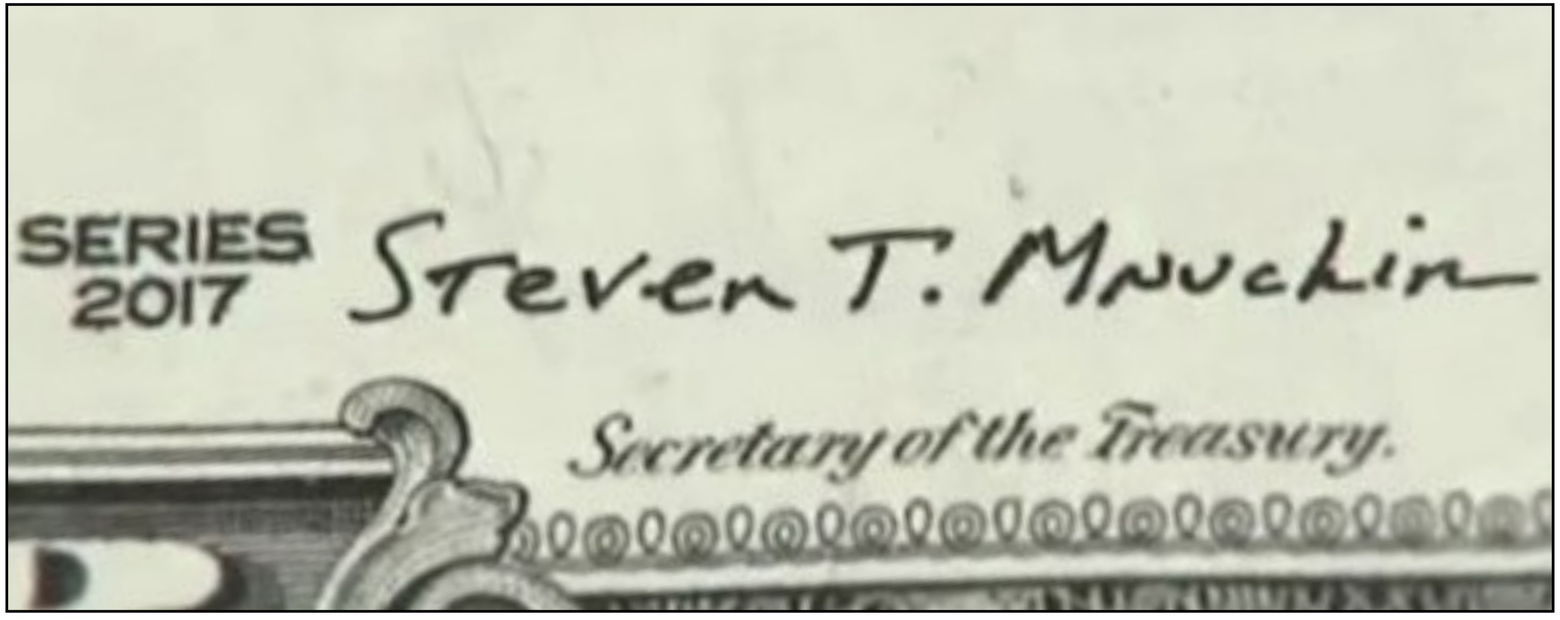
DiGi CASH — 1995

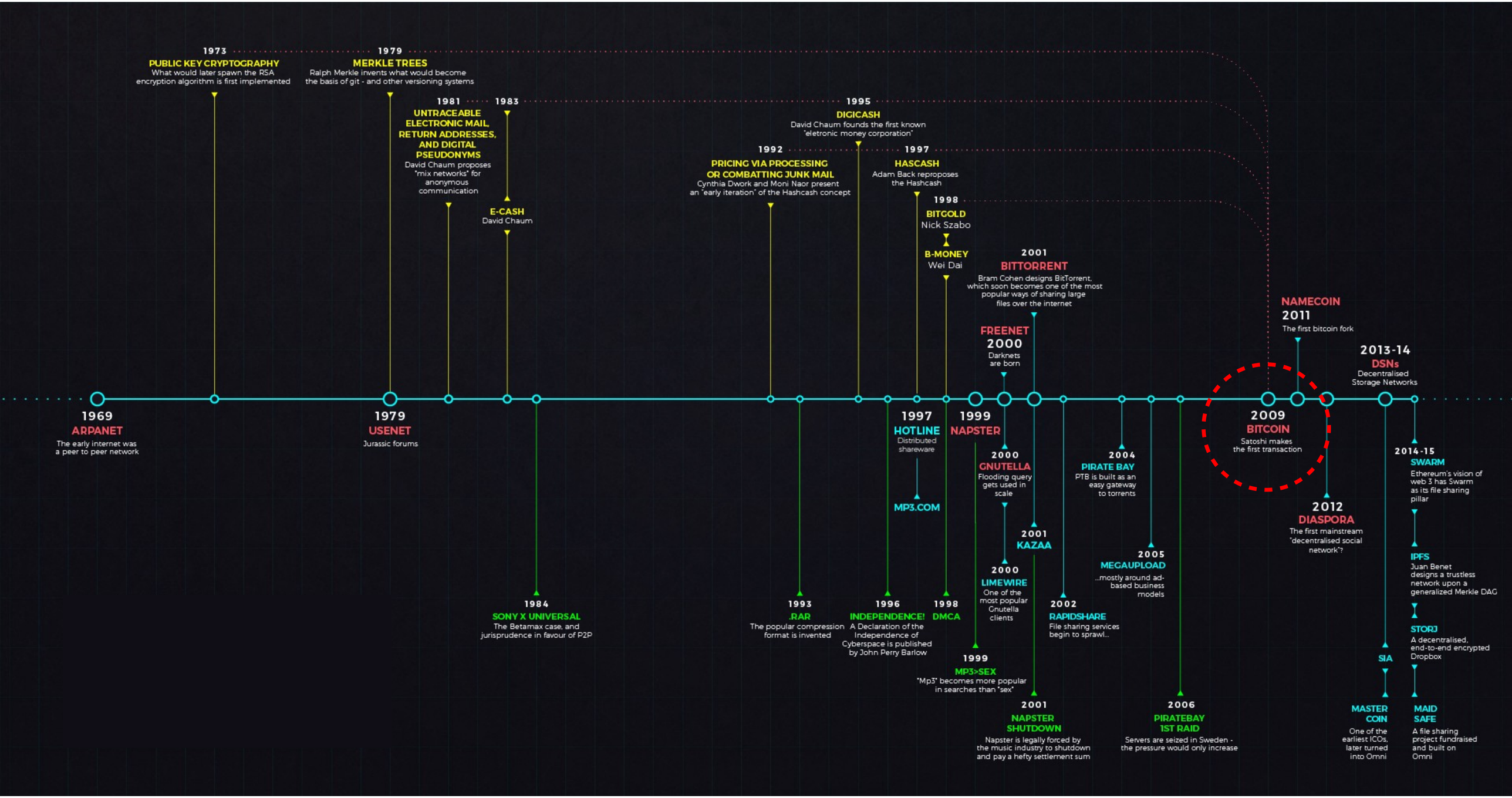
Hashcash — 1997

BIT GOLD — 1998

b-money — 1998

2009

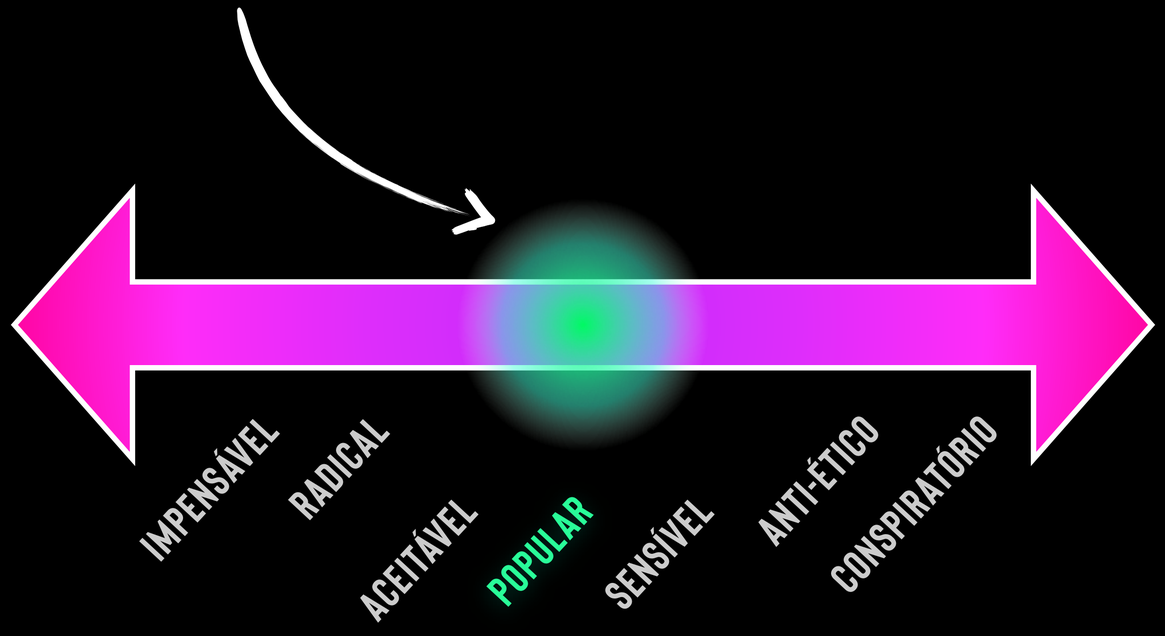



1969
ARPANET
The early internet was a peer to peer network
1973
PUBLIC KEY CRYPTOGRAPHY
What would later spawn the RSA encryption algorithm is first implemented
1979
USENET
Jurassic forums
1979
MERKLE TREES
Ralph Merkle inwents what would become the basis of git - and other versioning systems
1981
UNTRACEABLE ELECTRONIC MAIL, RETURN ADDRESSES, AND DIGITAL PSEUDONYMS
David Chaum proposes "mix networks" for anonymous communication
1983
E-CASH
David Chaum
1984
SONY X UNIVERSAL
The Betamax case, and jurisprudence in favour of P2P
1992
PRICING VIA PROCESSING OR COMBATTING JUNK MAIL
Cynthia Dwork and Moni Naor present an "early iteration" of the Hashcash concept
1993
.RAR
The popular compression format is invented
1995
DIGICASH
David Chaum founds the first known "eletronic money corporation"
1996
INDEPENDENCE!
A Declaration of the Independence of Cyberspace is published by John Perry Barlow
1997
HASCASH
Adam Back reproposes the Hashcash
1997
HOTLINE
Distributed shareware
MP3.COM
1998
BITGOLD
Nick Szabo
B-MONEY
Wei Dai
1998
DMCA
1999
NAPSTER
1999
MP3>SEX
"Mp3" becomes more popular in searches than "sex"
2000
FREENET
Darknets are born
2000
GNUTELLA
Flooding query gets used in scale
2000
LIMEWIRE
One of the most popular Gnutella clients
2001
BITTORRENT
Bram Cohen designs BitTorrent, which soon becomes one of the most popular ways of sharing large files over the internet
2001
KAZAA
2001
NAPSTER SHUTDOWN
Napster is legally forced by the music industry to shutdown and pay a hefty settlement sum
2002
RAPIDSHARE
File sharing services begin to sprawl...
2004
PIRATE BAY
PTB is built as an easy gateway to torrents
2005
MEGAUPLOAD
...mostly around ad-based business models
2006
PIRATEBAY 1ST RAID
Servers are seized in Sweden - the pressure would only increase
2009
BITCOIN
Satoshi makes the first transaction
NAMECOIN
2011
The first bitcoin fork
2012
DIASPORA
The first mainstream "decentralised social network"?
2013-14
DSNs
Decentralised Storage Networks
2014-15
SWARM
Ethereum's vision of web 3 has Swarm as its file sharing pillar
IPFS
Juan Benet designs a trustless network upon a generalized Merkle DAG
STORJ
A decentralised, end-to-end encrypted Dropbox
SIA
MASTER COIN
One of the earliest ICOs, later turned into Omni
MAID SAFE
A file sharing project fundraised and built on Omni

JANELA DE OVERTON

Paradigma Education

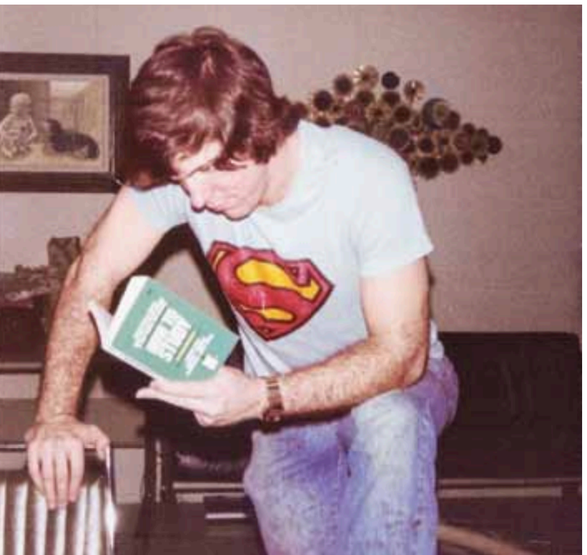
A GAMA DE IDEIAS TOLERÁVEIS NO DISCURSO PÚBLICO



As an amusing thought experiment, imagine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from $100 trillion to $300 trillion. With 20 million coins, that gives each coin a value of about $10 million.

So the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1! Even if the odds of Bitcoin succeeding to this degree are slim, are they really 100 million to one against? Something to think about...

Hal



halfin
@halfin

Running bitcoin

10:33 PM · Jan 10, 2009 ·

CRYONICS
2nd Quarter 2019 | Vol 40, Issue 2 www.alcor.org

Member Profile: Hal Finney
page 3

Case Report: A-1990
page 12

Victor Frankenstein and the Modern Quest for the Secrets of Life
page 30

ALCOR
ALCOR LIFE EXTENSION FOUNDATION
The World's Leader in Cryonics

Os **CypherPunks** já **conheciam a história**: se **houvesse alguém** que **pudesse ser perseguido**… este alguém o seria

Por isso que, em **2011**, **Satoshi** nos **deixou**

Satoshi's Final Email to Gavin Andresen

April 26, 2011 by bitcoincash

The following email is the last known verified email correspondence from Satoshi Nakamoto. Gavin replied to the email to inform Satoshi that he had been invited to speak at an event put on by an organization under the CIA. Satoshi never replied.

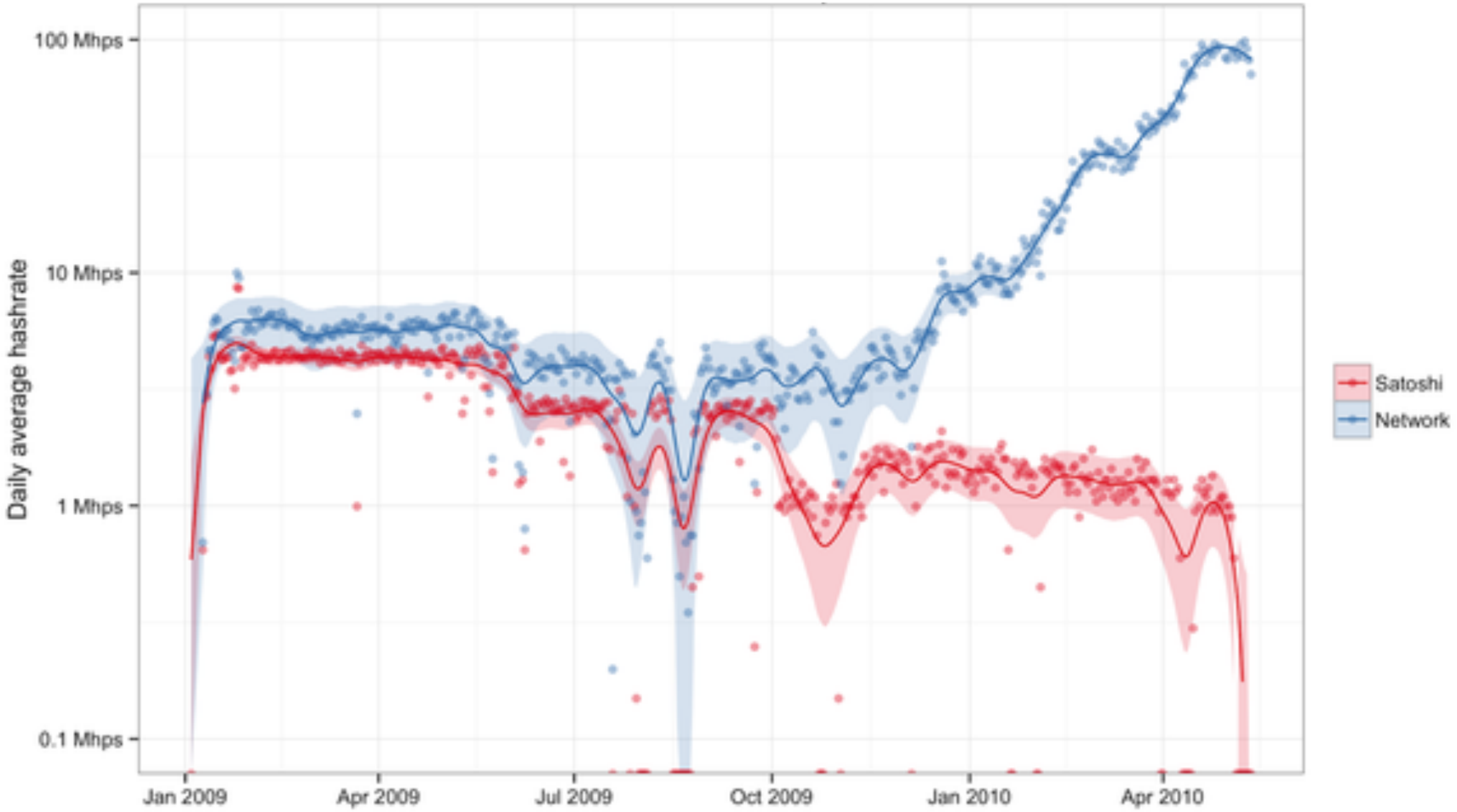
> I wish you wouldn't keep talking about me as a mysterious shadowy figure, the press just turns that into a pirate currency angle. Maybe instead make it about the open source project and give more credit to your dev contributors; it helps motivate them.

From: Satoshi Nakamoto <satoshin@gmx.com>
Date: Sat, Apr 23, 2011 at 3:40 PM
To: Mike Hearn <mike@plan99.net>

> I had a few other things on my mind (as always). One is, are you planning on rejoining the community at some point (eg for code reviews), or is your plan to permanently step back from the limelight?

I've moved on to other things. It's in good hands with Gavin and everyone.

O **poder** computacional de **Satoshi VS.** o **“resto da rede”**



E o **Hal Finney**?

E o **Hal Finney**?

Em **2014**, **Hal Finney** nos **deixou**

ANDY GREENBERG SECURITY 08.28.2014 11:06 PM

Bitcoin's Earliest Adopter Is Cryonically Freezing His Body to See the Future

"He's always been optimistic about the future," says Hal Finney's wife, Fran. "Every new advance, he embraced it, every new technology. Hal relished life, and he made the most of everything."

Hal
VIP
Sr. Member

Activity: 314
Merit: 1873

Bitcoin and me (Hal Finney)
March 19, 2013, 08:40:02 PM
Merited by Vlad2Vlad (100), EFS (100), fillippone (60), OgNasty (50), suchmoon (50), fr4nkthetank (50), EmilioMann (50), HagssFIN (50), Rw13enlib88 (50), HCLivess (50), icey (50), boomboom (50), monsanto (42), ChekaZ (40), cAPSLOCK (20), joniboini (20), Brucelats (20), nathalie20 (13), amishmanish (11), BayAreaCoins (10), wizzardTim (10), ebliever (10), redsn0w (8), jyap (8), ETFbitcoin (7), mindrust (5), Lucius (5), dbshck (5), Lutpin (5), o_e_l_e_o (5), DdmrDdmr (5), bitmover (5), xtraelv (5), Jeremycoin (5), Corrosive (5), 100action (5), Dabs (4), bitbollo (4), mprep (3), Ratimov (3), casinocoin (3), vapourminer (2), JayJuanGee (2), batang_bitcoin (2), bones261 (2), duesoldi (2), stortz (2), The Bitcoin Zap (2), RodeoX (1), Stunna (1), Searing (1), Gyrsur (1), tbearhere (1), BitcoinFX (1), Abiky (1), jojo69 (1), Oceat (1), franckuestein (1), pawel7777 (1), edgar (1), Raja_MBZ (1), JanpriX (1), Cluster2k (1), krogothmanhattan (1), Lucasgabd (1), dannybrown (1), TheFuzzStone (1), Paolo.Demidov (1), Gleb Gamow (1), okae (1), Bthd (1), ruletheworld (1), DireWolfM14 (1), Blowon (1), Toxic2040 (1), Artemis3 (1), elianite (1), jtipt (1), solosequenosenada (1), VB1001 (1), zasad@ (1), _Miracle (1), famososMuertos (1), Ilsk (1), dimastegar (1), chimk (1), 5ensei (1), hakka (1), Financisto (1), TheWolf666 (1), Q2kc (1), thefiniteidea (1), astrocity1981 (1), M-BTC (1), surikat85 (1), nullama (1), jameswell (1), pocketart (1), cyberpunk01 (1), rickC137 (1), exfortuna (1)

#1

I thought I'd write about the last four years, an eventful time for Bitcoin and me.

For those who don't know me, I'm Hal Finney. I got my start in crypto working on an early version of PGP, working closely with Phil Zimmermann. When Phil decided to start PGP Corporation, I was one of the first hires. I would work on PGP until my retirement. At the same time, I got involved with the Cypherpunks. I ran the first cryptographically based anonymous remailer, among other activities.

Fast forward to late 2008 and the announcement of Bitcoin. I've noticed that cryptographic graybeards (I was in my mid 50's) tend to get cynical. I was more idealistic; I have always loved crypto, the mystery and the paradox of it.

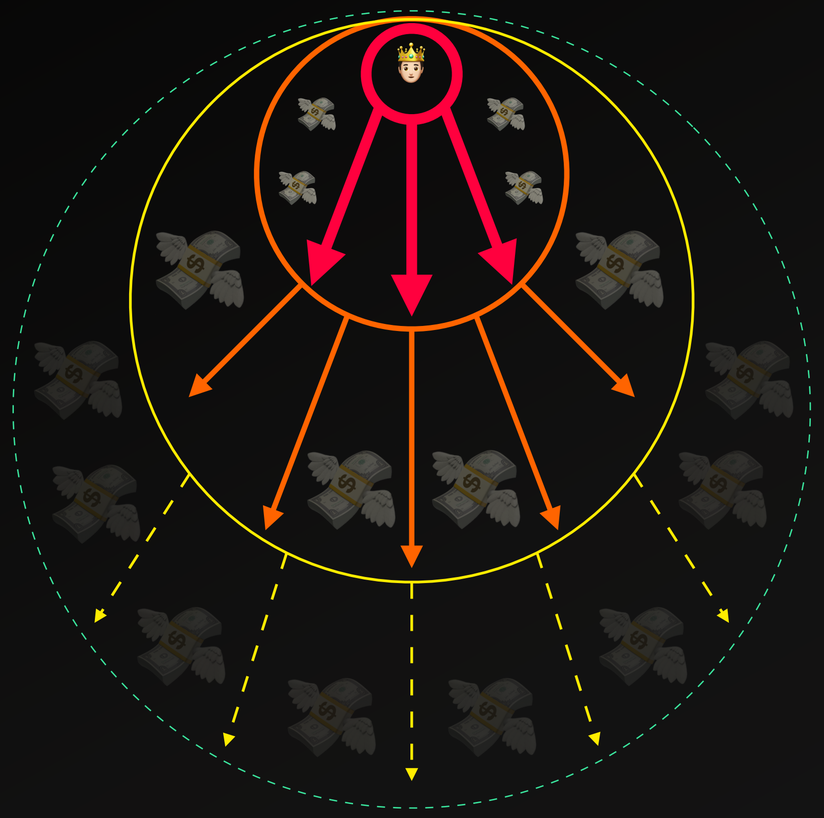
When Satoshi announced Bitcoin on the cryptography mailing list, he got a skeptical reception at best. Cryptographers have seen too many grand schemes by clueless noobs. They tend to have a knee jerk reaction.

I was more positive. I had long been interested in cryptographic payment schemes. Plus I was lucky enough to meet and extensively correspond with both Wei Dai and Nick Szabo, generally acknowledged to have created ideas that would be realized with Bitcoin. I had made an attempt to create my own proof of work based currency, called RPOW. So I found Bitcoin facinating.

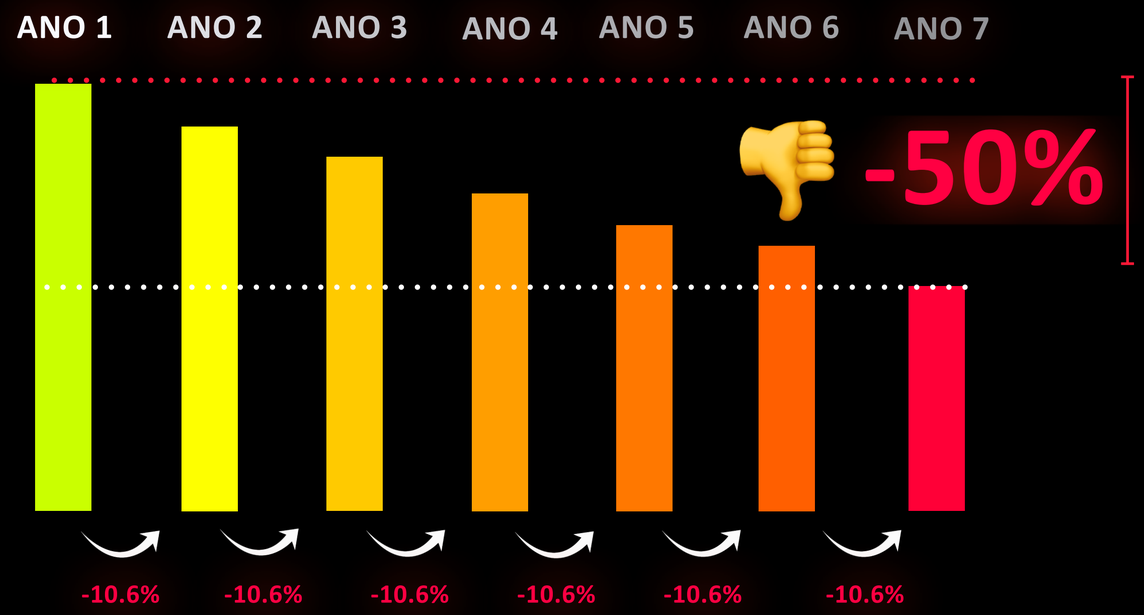
Parte 2

Seu Dinheiro é Programado Pra Perder Valor

Efeito *Cantillion*

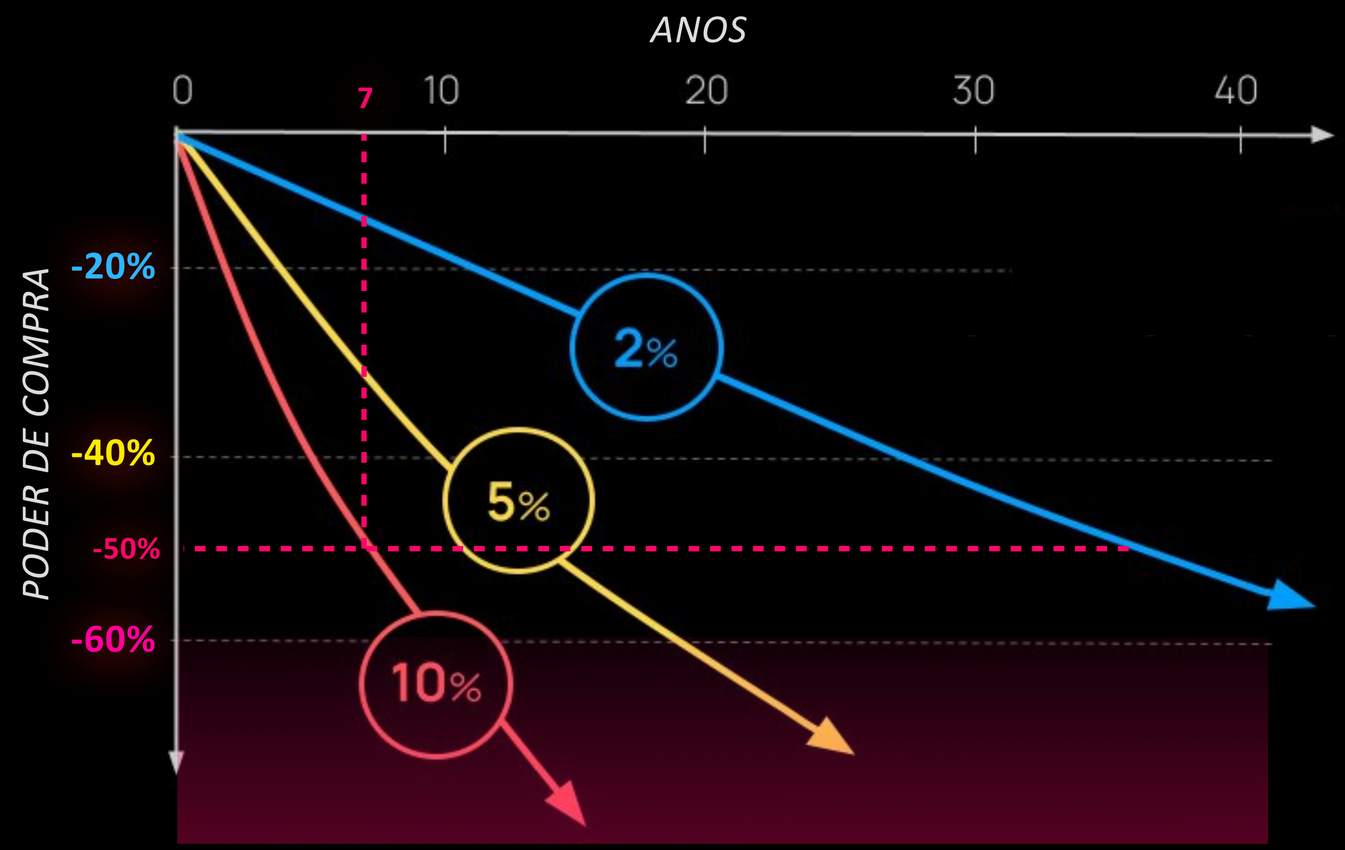


Uma inflação de **10.6%** **ao ano** reduz o
valor do dinheiro **pela metade** em 7 anos.



É assim que o **dinheiro**, como funciona, é **programado**
pra **empobrecer** quem usa ele para **poupar**.

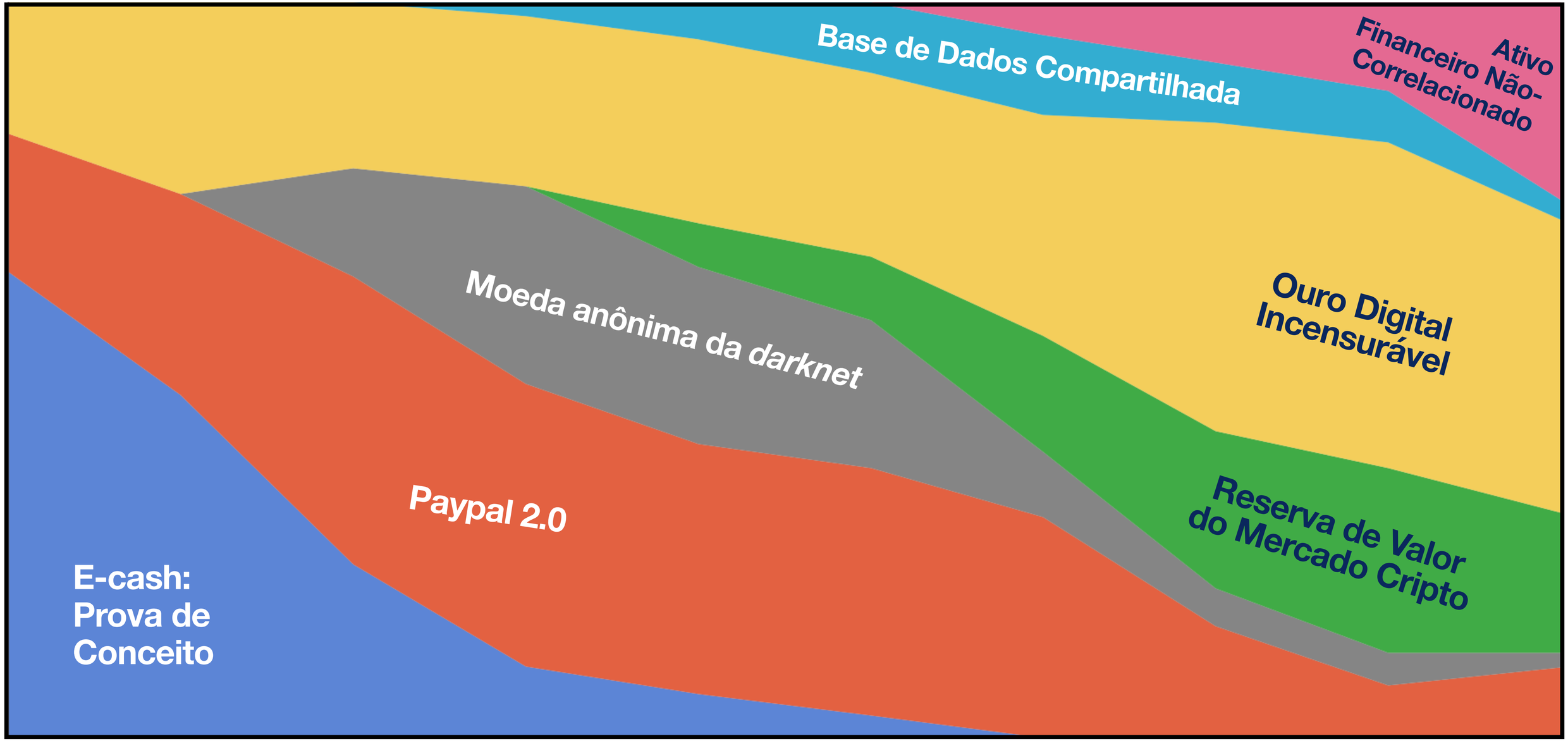
IMPACTO DA INFLAÇÃO
NO SEU PODER DE COMPRA



FONTE: ANILSAIDSO // TRADUÇÃO: PARADIGMAEDU

Fonte: Visions of Bitcoin (Nic Carter & Hasu)

Narrativas do Bitcoin ao Longo dos Anos



Uma **definição simples**:

O **Bitcoin** é **um dinheiro programado** pra **ganhar valor** (ao contrário dos outros).

⚠️ Não significa que não vai cair!

Só que a **natureza** deste dinheiro **é diferente.**

SUB-SEÇÃO (K) DO 31° U.S. CODE § 5112

The Secretary may **mint and issue platinum bullion coins and proof platinum coins** in accordance with such specifications, designs, varieties, quantities, denominations, and inscriptions as the Secretary, in the Secretary's discretion, may prescribe from time to time.

Treasury Secretary Janet Yellen said on Tuesday that she wouldn't consider the idea, calling it a "gimmick." She's right that the trillion-dollar coinage would require using the U.S. Mint to perform a function for which it was never intended, but that doesn't dissuade its backers. This month my Opinion

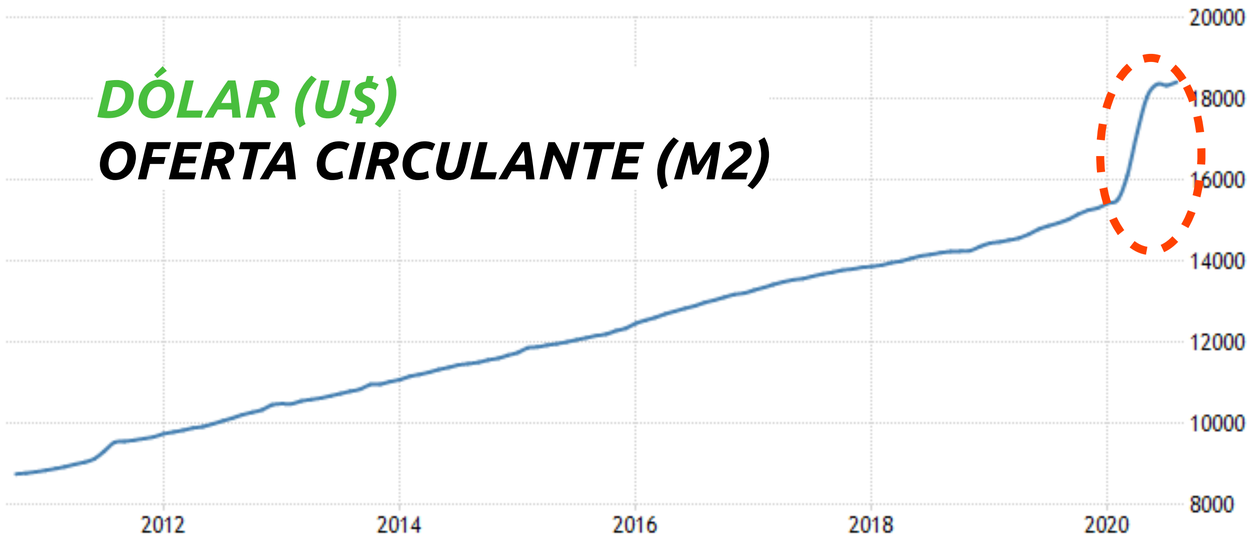
I asked Buchanan about that today. He said he is worried that minting the coin could undermine public faith in money. The government's acceptance of money to pay taxes isn't enough to sustain its value if no one else accepts it, he said: "You don't want to make the crisis worse by creating a stunt that makes everybody say, 'Wait a minute, what's going on here?'" (Buchanan says the debt ceiling statute is unconstitutional and the Treasury Department should "continue to issue normal debt in normal ways.")

A “Não-Política” Monetária

de **Satoshi Nakamoto**

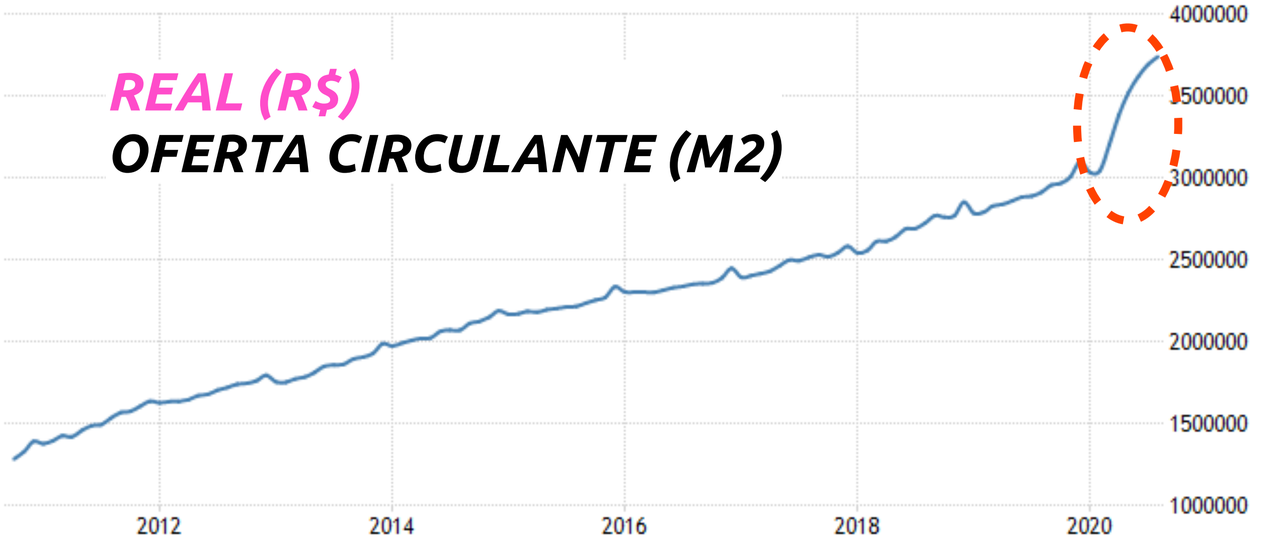
Halving: a cada ~4 anos, a emissão de moedas desacelera pela metade. Até chegar num limite de 21 milhões.

DÓLAR (U$)
OFERTA CIRCULANTE (M2)



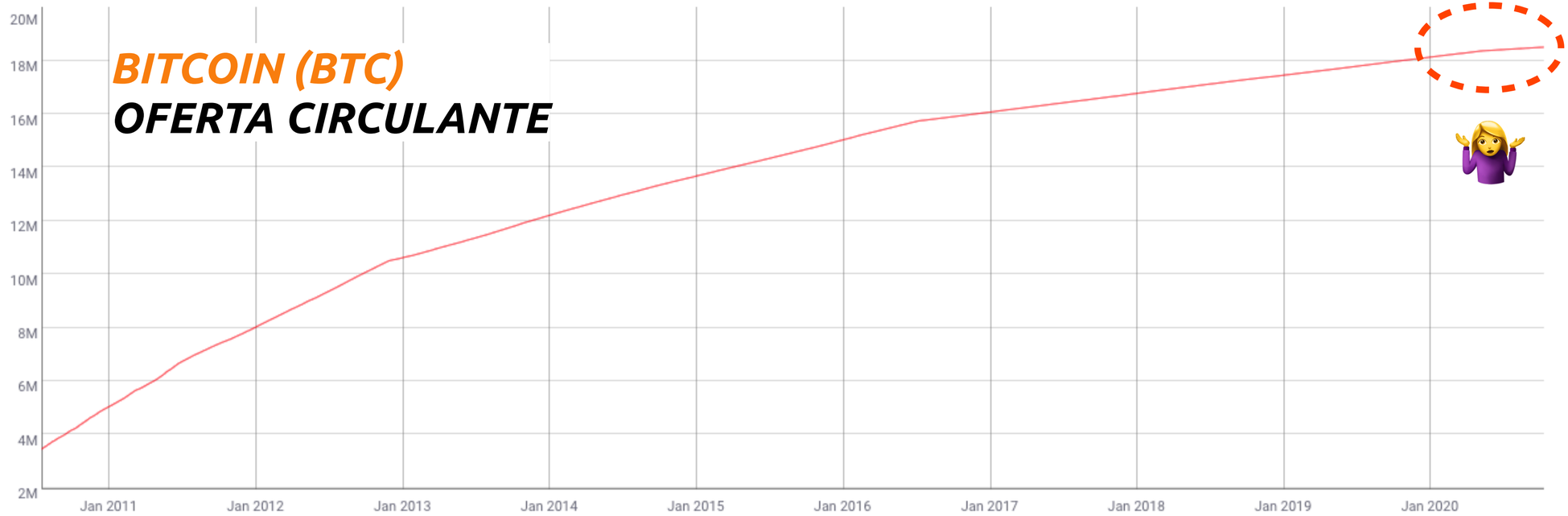
SOURCE: TRADINGECONOMICS.COM | FEDERAL RESERVE

REAL (R$)
OFERTA CIRCULANTE (M2)



SOURCE: TRADINGECONOMICS.COM | BANCO CENTRAL DO BRASIL

BITCOIN (BTC)
OFERTA CIRCULANTE



FONTE: COINMETRICS

1) Sem confisco **2)** Sem censura **3)** Sem mais inflação **4)** Qualquer um pode verificar 1-3

Poderia **nunca ter ganho valor**… mas **ganhou**

laszlo
Full Member

Activity: 199
Merit: 149

Re: Pizza for bitcoins?
May 21, 2010, 09:33:45 PM #10

I just think it would be interesting if I could say that I paid for a pizza in bitcoins

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

laszlo
Full Member

Activity: 199
Merit: 149

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM #11

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

sirius
Bitcoiner
Sr. Member

Re: Pizza for bitcoins?
May 22, 2010, 10:10:25 PM #12

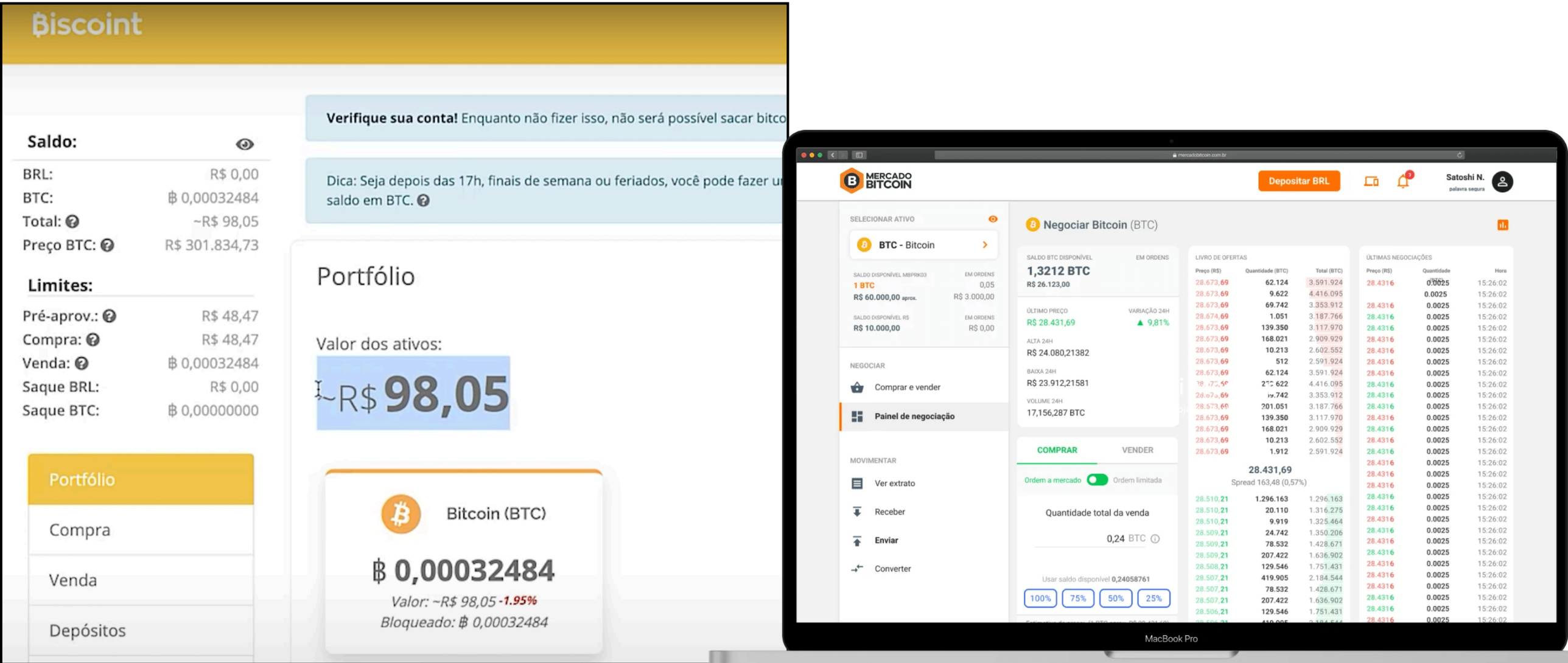
Congratulations laszlo, a great milestone reached

Parte 3

O Bitcoin Por Dentro

Endereços, Carteiras, Transações e Blocos

A Maioria das Pessoas Só Conhece o Bitcoin Via Corretoras



O Bitcoin é uma Base de Dados (tipo uma Planilha de Excel)

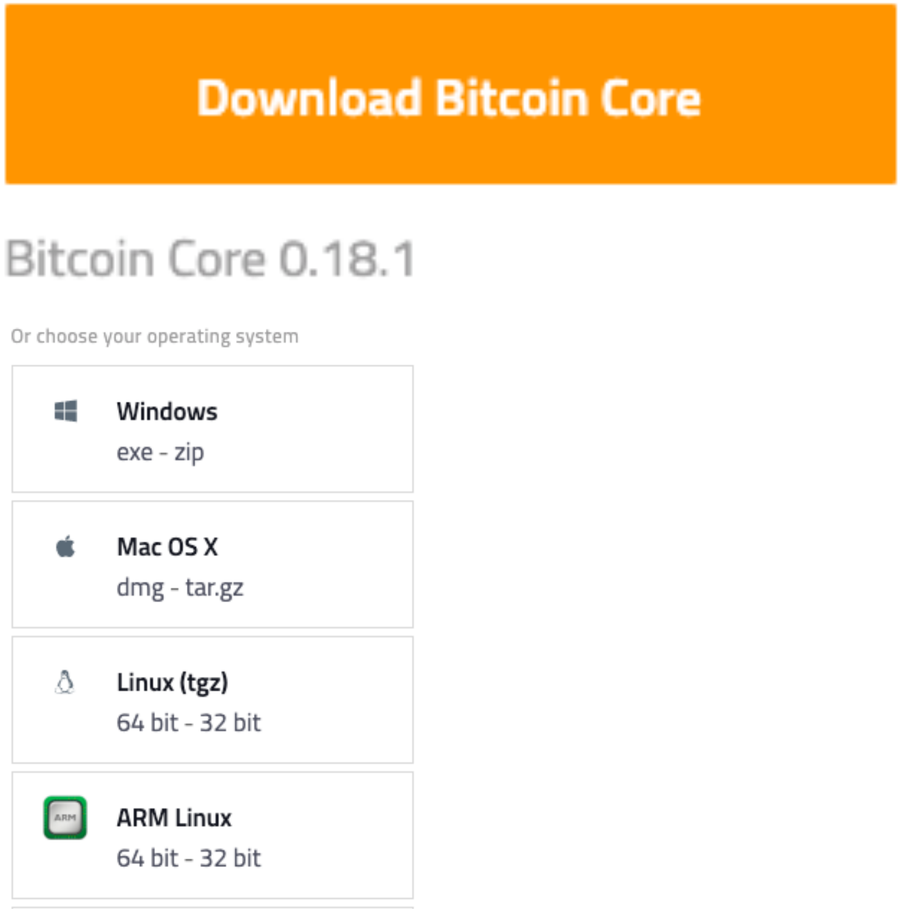
O Bitcoin é uma Base de Dados (tipo uma Planilha de Excel)

Endereço -> Uma “coluna nessa planilha”
Carteira -> Interface para ler o “conteúdo de um endereço”
Bloco -> Uma linha nova nessa planilha
Transação -> Movimento de um valor de uma célula pra outra

Exchange/Corretora -> Interface que abstrai tudo isso,
e é mantida por uma empresa

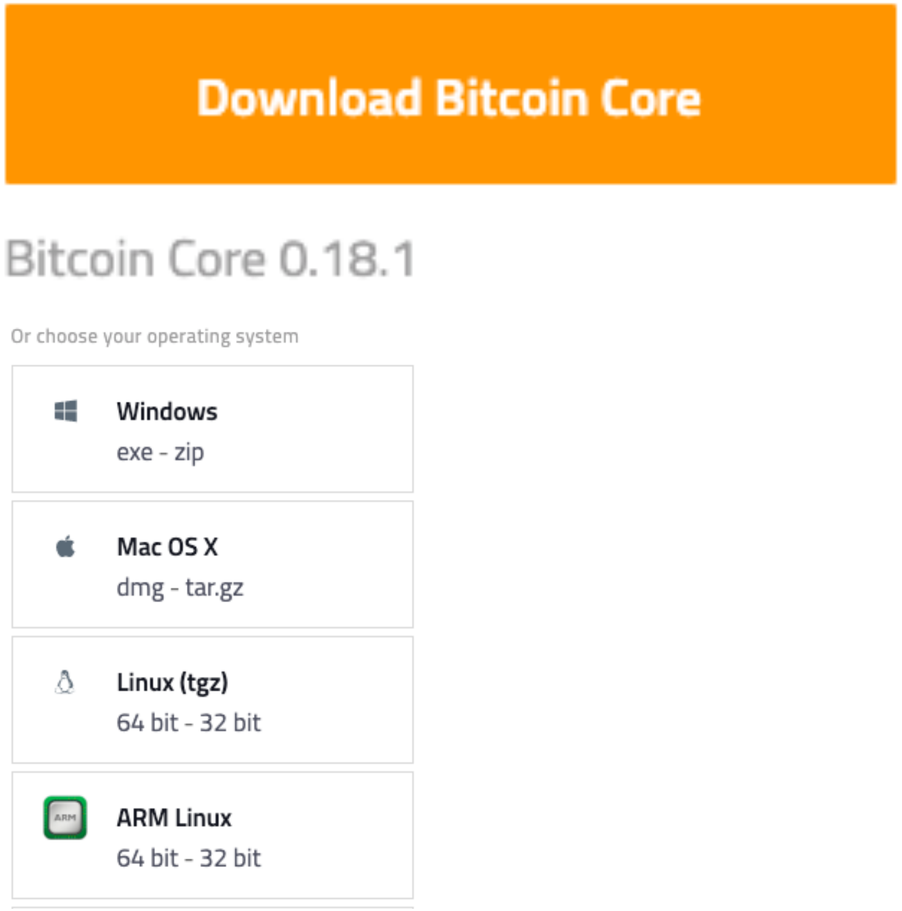
* Aguenta aí que nós vamos visualizar isso

Qualquer Pessoa Pode Manter uma Cópia dessa “Planilha” (ser um “nó”)



Um programa de computador

https://bitcoin.org/en/download



Linux

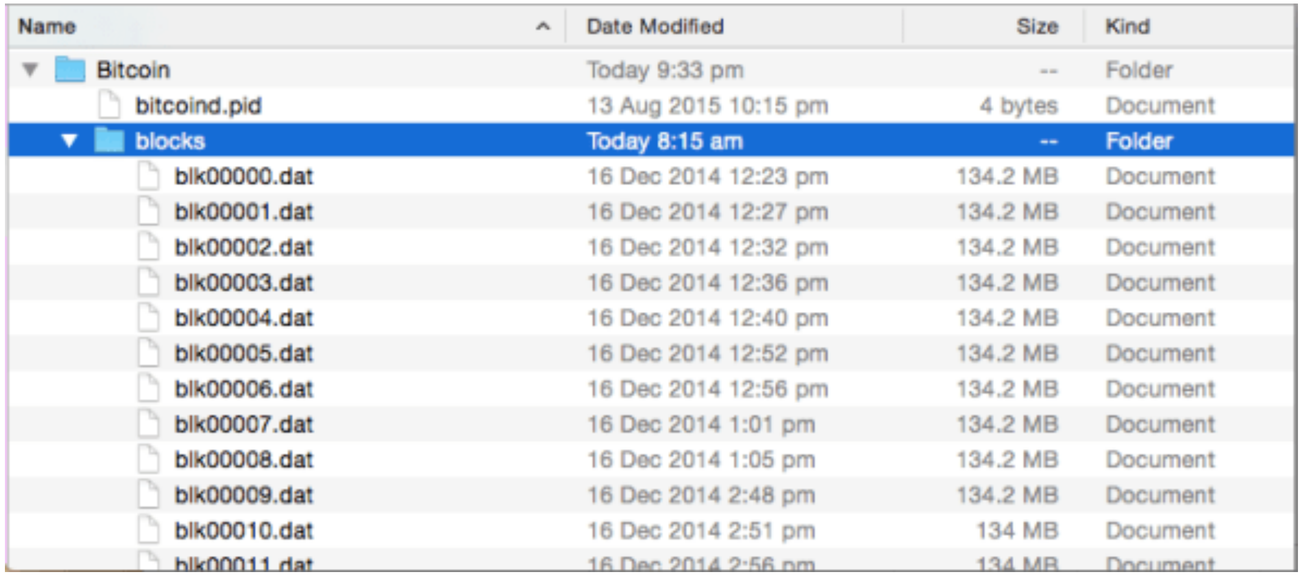
```
/home/[username]/.bitcoin/blocks/
```

Windows

```
C:\Users\[username]\AppData\Roaming\Bitcoin\
```

Mac

```
~/Library/Application Support/Bitcoin/
```

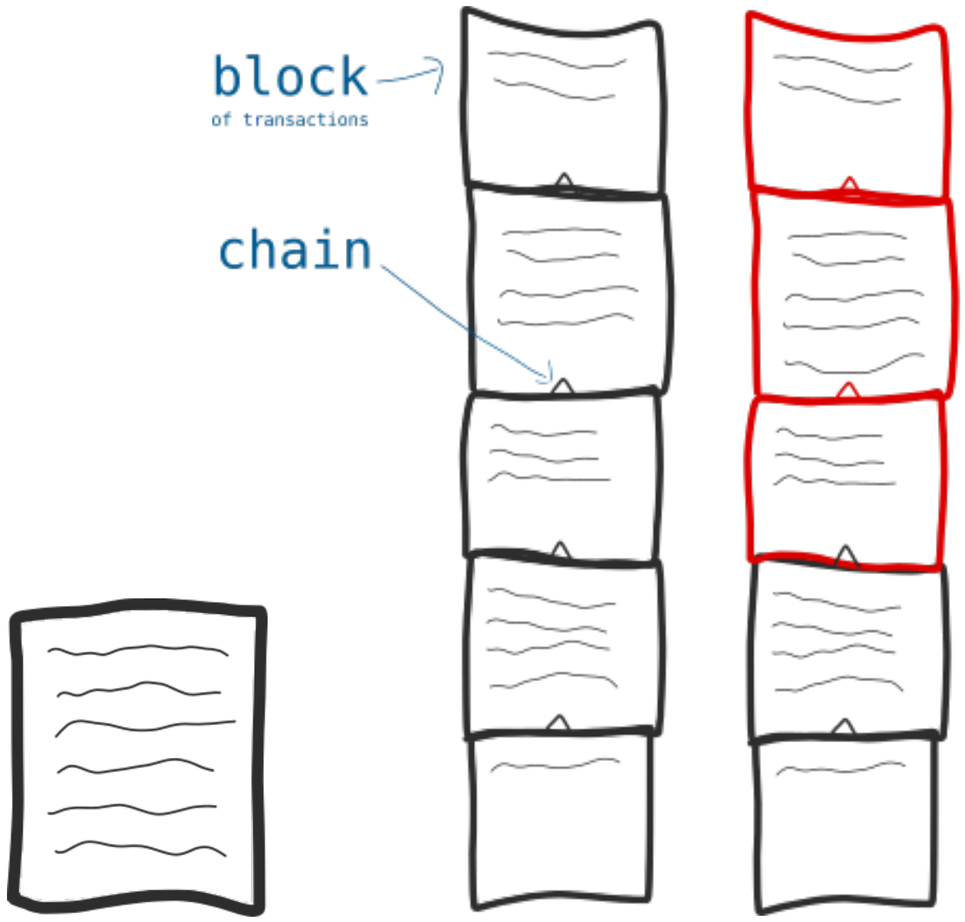


Name	Date Modified	Size	Kind
Bitcoin	Today 9:33 pm	--	Folder
bitcoind.pid	13 Aug 2015 10:15 pm	4 bytes	Document
blocks	Today 8:15 am	--	Folder
blk00000.dat	16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat	16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat	16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat	16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat	16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat	16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat	16 Dec 2014 12:56 pm	134.2 MB	Document
blk00007.dat	16 Dec 2014 1:01 pm	134.2 MB	Document
blk00008.dat	16 Dec 2014 1:05 pm	134.2 MB	Document
blk00009.dat	16 Dec 2014 2:48 pm	134.2 MB	Document
blk00010.dat	16 Dec 2014 2:51 pm	134 MB	Document
blk00011.dat	16 Dec 2014 2:56 pm	134 MB	Document

Um programa de computador

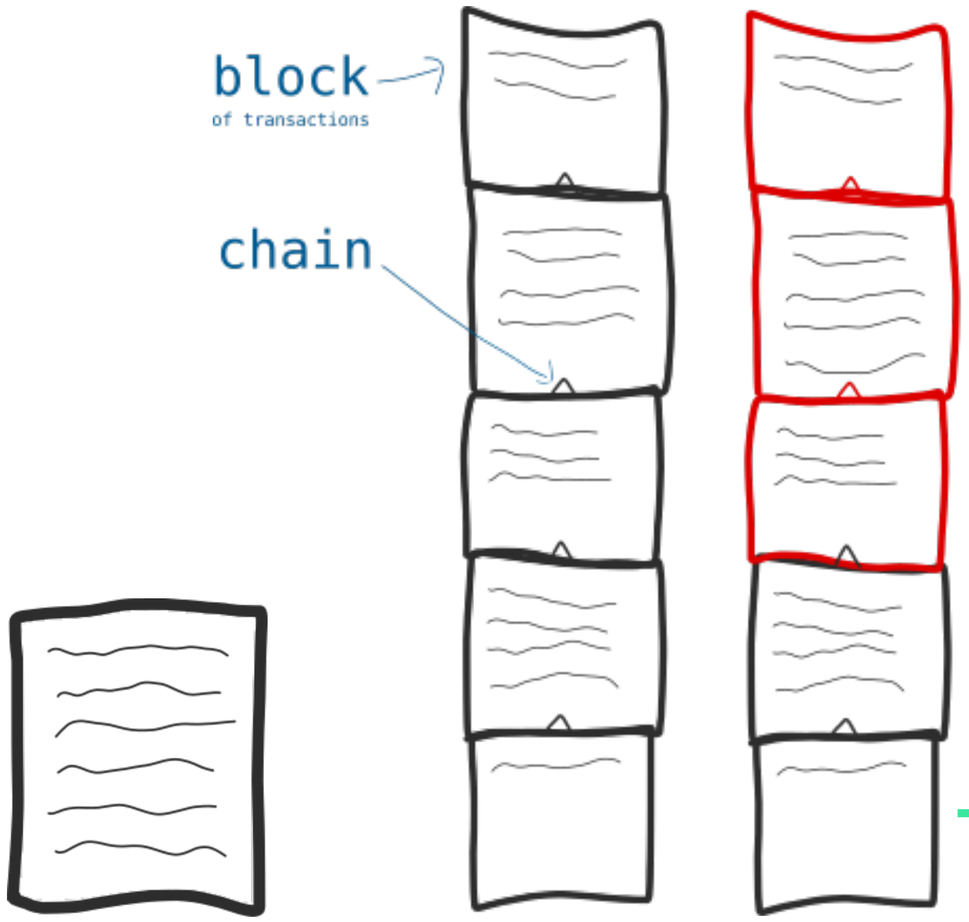
https://bitcoin.org/en/download

O que é blockchain?



Um arquivo que lista toda transação já feita

(entre usuários desse programa)



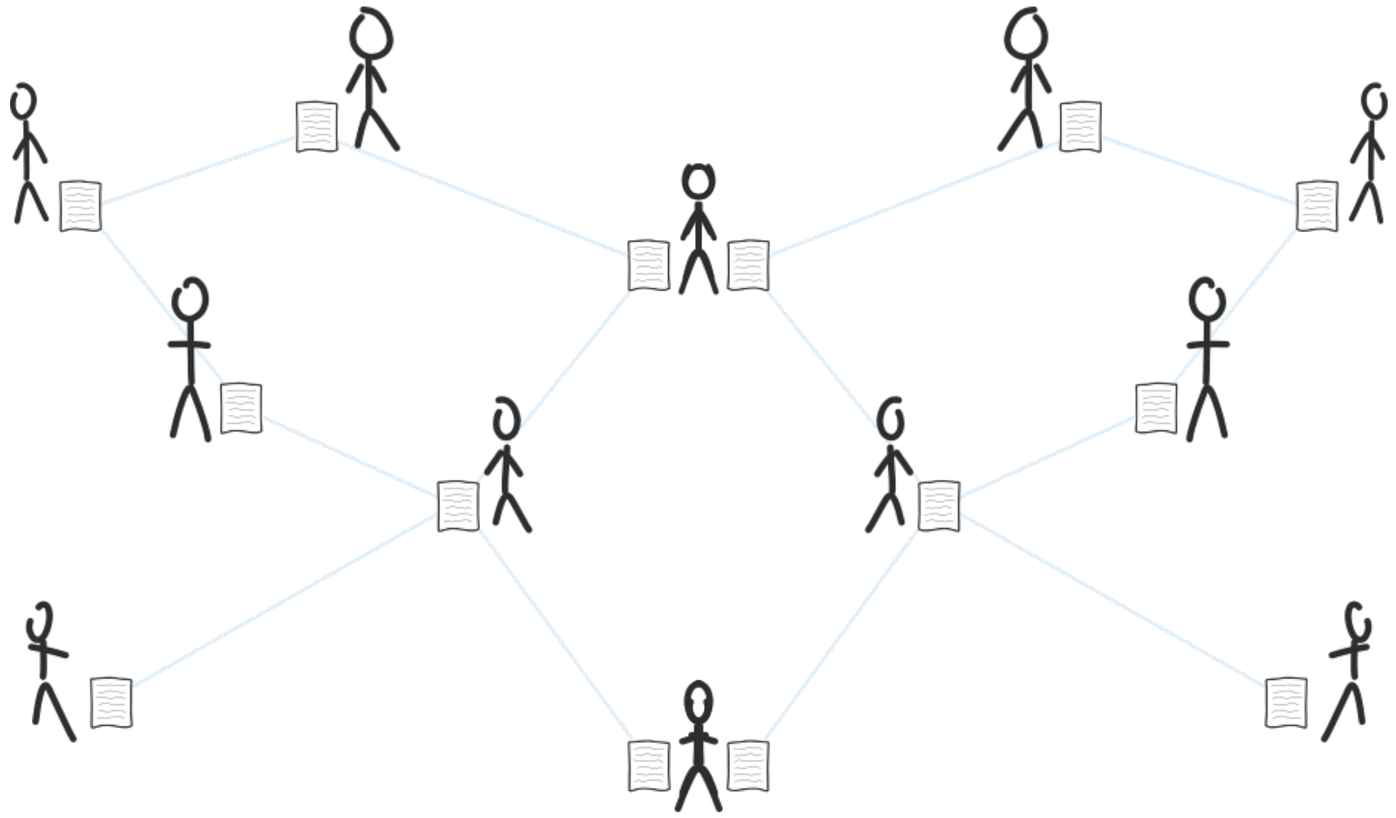

```
$ hexdump -C -s 8 -n 285 blk00000.dat

00000008  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000018  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000028  00 00 00 00 3b a3 ed fd  7a 7b 12 b2 7a c7 2c 3e  |....;...z{..z.,>|
00000038  67 76 8f 61 7f c8 1b c3  88 8a 51 32 3a 9f b8 aa  |gv.a......Q2:...|
00000048  4b 1e 5e 4a 29 ab 5f 49  ff ff 00 1d 1d ac 2b 7c  |K.^J}._I......+||
00000058  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  |................|
00000068  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000078  00 00 00 00 00 00 ff ff  ff ff 4d 04 ff ff 00 1d  |..........M.....|
00000088  01 04 45 54 68 65 20 54  69 6d 65 73 20 30 33 2f  |..EThe Times 03/|
00000098  4a 61 6e 2f 32 30 30 39  20 43 68 61 6e 63 65 6c  |Jan/2009 Chancel|
000000a8  6c 6f 72 20 6f 6e 20 62  72 69 6e 6b 20 6f 66 20  |lor on brink of |
000000b8  73 65 63 6f 6e 64 20 62  61 69 6c 6f 75 74 20 66  |second bailout f|
000000c8  6f 72 20 62 61 6e 6b 73  ff ff ff ff 01 00 f2 05  |or banks........|
000000d8  2a 01 00 00 00 43 41 04  67 8a fd b0 fe 55 48 27  |*....CA.g....UH'|
000000e8  19 67 f1 a6 71 30 b7 10  5c d6 a8 28 e0 39 09 a6  |.g..q0..\..(.9..|
000000f8  79 62 e0 ea 1f 61 de b6  49 f6 bc 3f 4c ef 38 c4  |yb...a..I..?L.8.|
00000108  f3 55 04 e5 1e c1 12 de  5c 38 4d f7 ba 0b 8d 57  |.U......\8M....W|
00000118  8a 4c 70 2b 6b f1 1d 5f  ac 00 00 00 00           |.Lp+k.._.....|)
0000125
```

```
f9beb4d91d0100000100000000000000000000000000000000000000000000000000000000000000000000000000000003ba3edfd7a7b12b27ac72c3e67768f617fc81bc3888a51323a9fb8aa4b1e5e4a29ab5f49ffff001d1dac2b7c0101000000010000000000000000000000000000000000000000000000000000000000000000000000000000ffffffff4d04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436861696e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73ffffffff0100f2052a01000000434104678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5fac00000000
```

Um arquivo que lista toda transação já feita

(entre usuários desse programa)



convencem

baixam
(escolhem)

executam

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Feb 28 2019 10:57:42 GMT-0300 (Brasilia Standard Time).

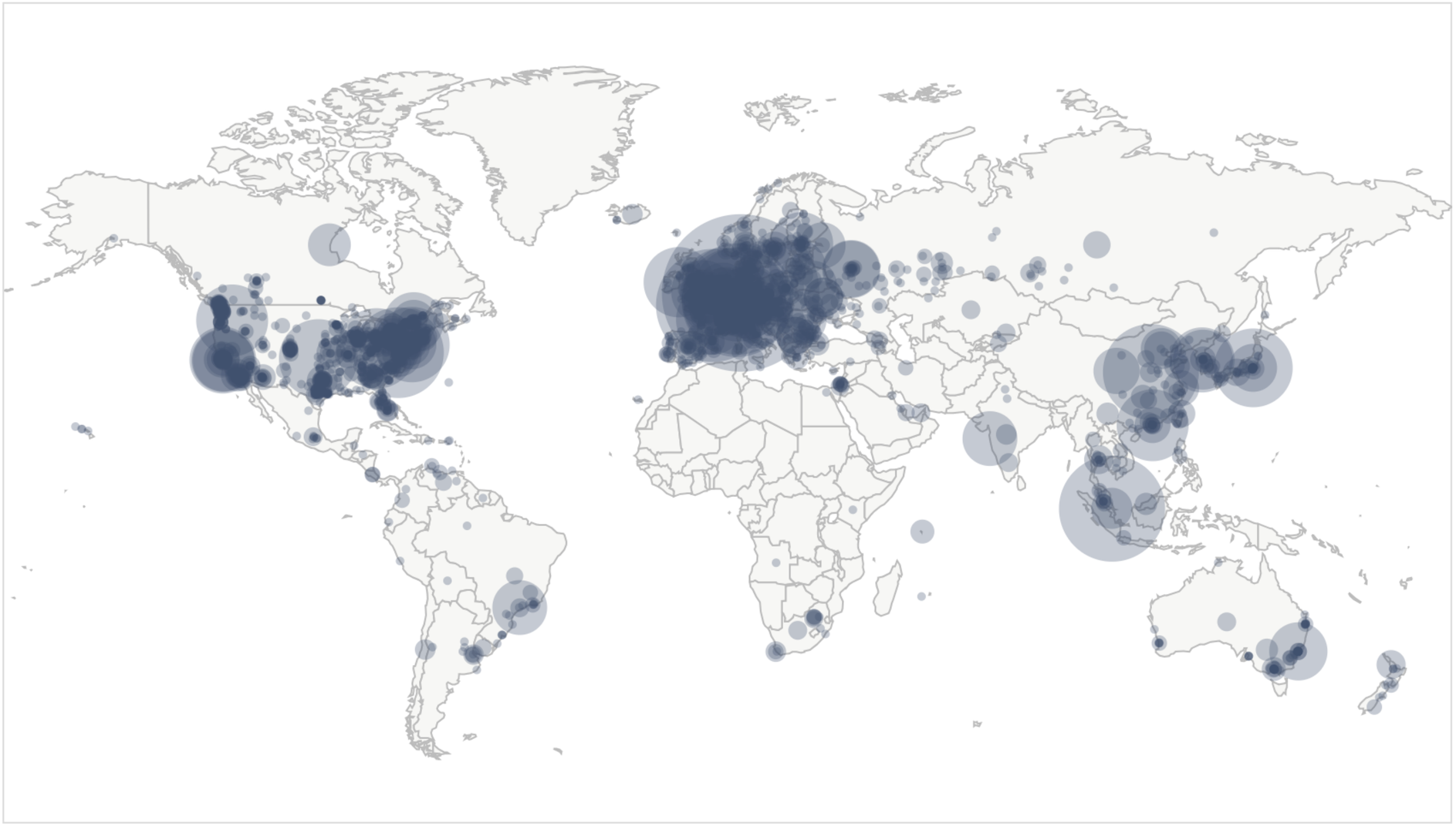
10498 NODES

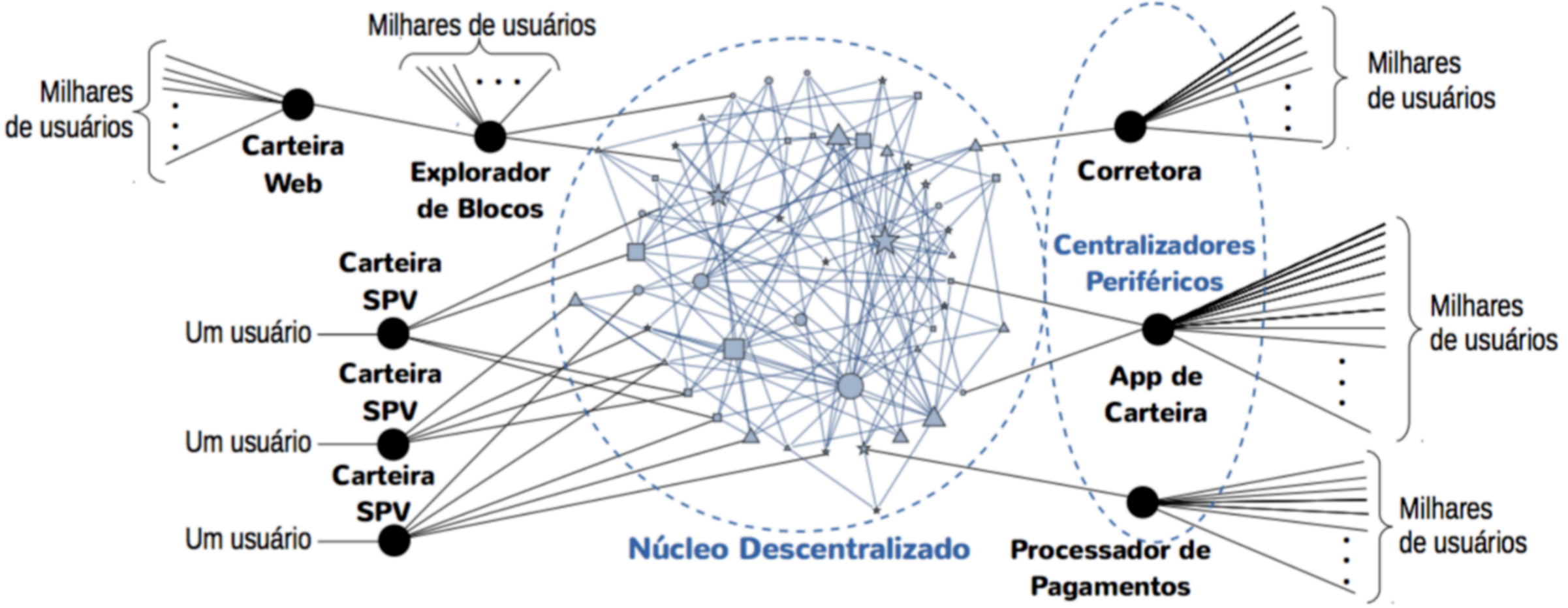
24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2590 (24.67%)
2	Germany	2032 (19.36%)
3	France	692 (6.59%)
4	Netherlands	525 (5.00%)
5	Canada	398 (3.79%)
6	China	375 (3.57%)
7	United Kingdom	352 (3.35%)
8	Singapore	310 (2.95%)
9	Russian Federation	281 (2.68%)
10	Japan	246 (2.34%)

More (104) »




Milhares de usuários
Milhares de usuários
Carteira Web
Explorador de Blocos
Corretora
Milhares de usuários
Carteira SPV
Um usuário
Centralizadores Periféricos
Carteira SPV
Um usuário
App de Carteira
Milhares de usuários
Carteira SPV
Um usuário
Núcleo Descentralizado
Processador de Pagamentos
Milhares de usuários

.bitcoin/blocks/blk.dat.*

Células da Planilha = UTXOs

Visualizando UTXOs Na Cadeia de Blocos

Bloco 1

	Satoshi
1	50 BTC

...

Bloco 7

Bloco 8

	Satoshi	Hal
Bloco 1	50 BTC	
Bloco 2	50 BTC	
Bloco 3	50 BTC	
Bloco 4	0.25 BTC	10 BTC
Bloco 5	0.10 BTC	3.5 BTC
Bloco 6		50 BTC
Bloco 7	5 BTC	
Bloco 8		7 BTC

Bloco 9

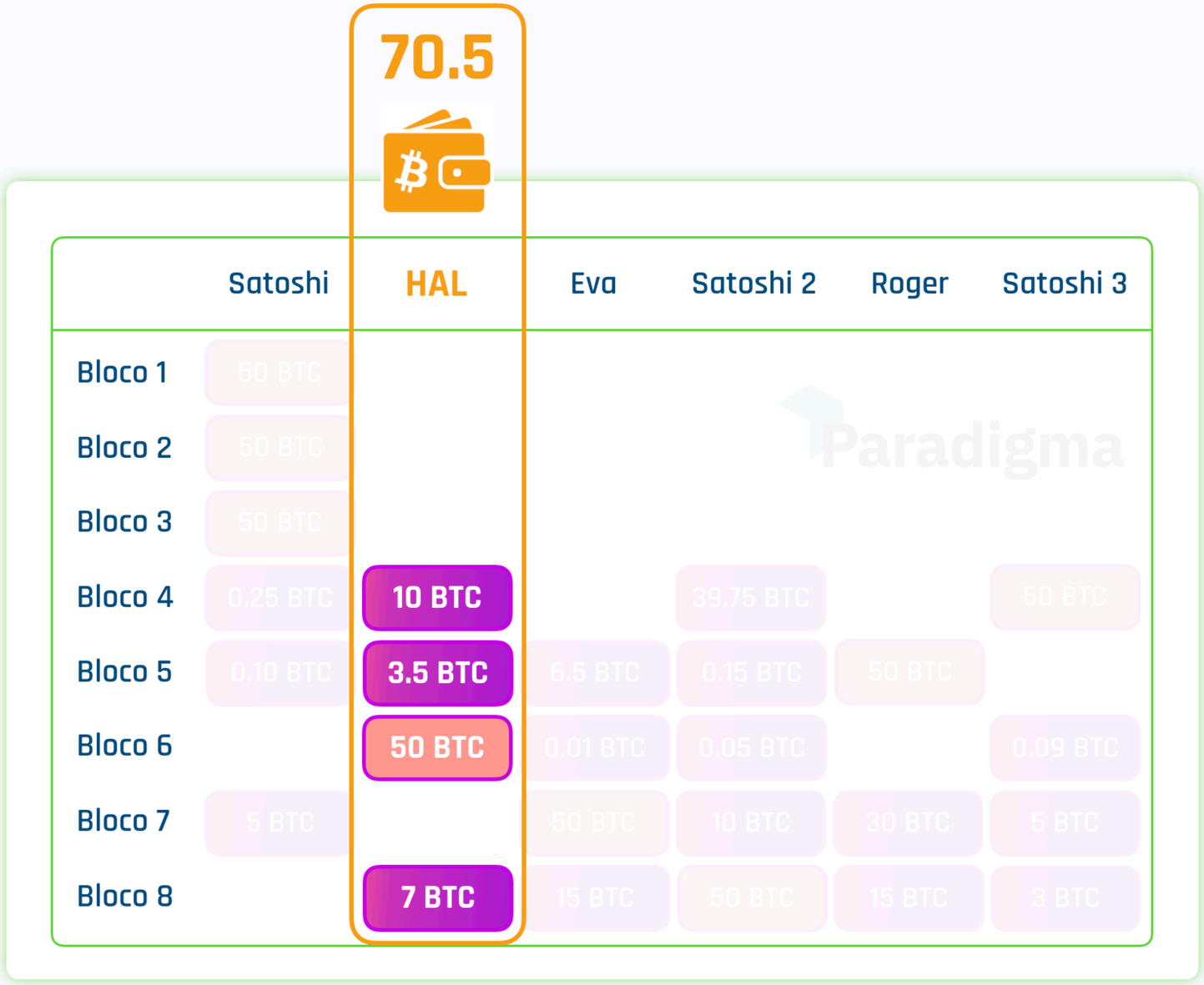
	Satoshi	Hal	Eva	Satoshi 2	Roger	Satoshi 3
Bloco 1	50 BTC					
Bloco 2	50 BTC					
Bloco 3	50 BTC					
Bloco 4	0.25 BTC	10 BTC		39.75 BTC		50 BTC
Bloco 5	0.10 BTC	3.5 BTC	6.5 BTC	0.15 BTC	50 BTC	
Bloco 6		50 BTC	0.01 BTC	0.05 BTC		0.09 BTC
Bloco 7	5 BTC		50 BTC	10 BTC	30 BTC	5 BTC
Bloco 8		7 BTC	15 BTC	50 BTC	15 BTC	3 BTC
Bloco 9	1 BTC	50 BTC	14 BTC	0.27 BTC	6 BTC	2 BTC

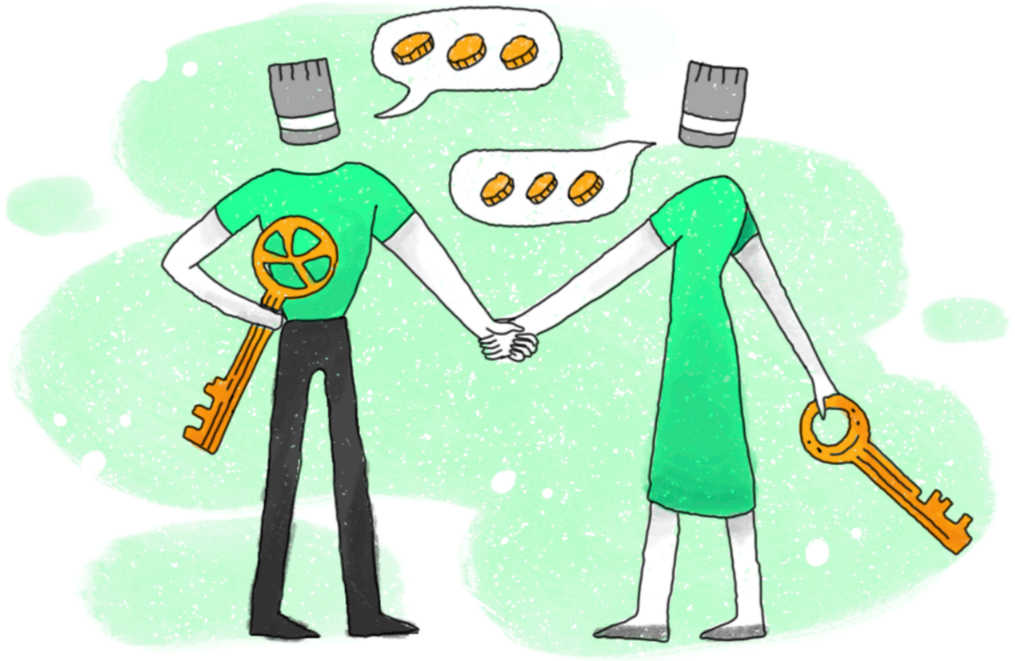
Tudo começou com o bloco 1.
Nele, foi criado o 1º UTXO:
50 bitcoin, ao controle de Satoshi.

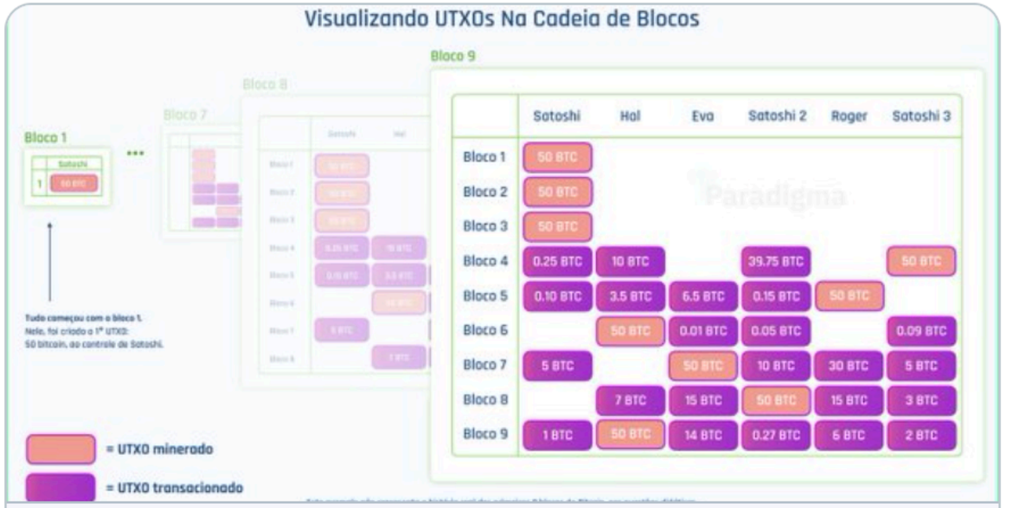
= UTXO minerado

= UTXO transacionado

Este exemplo não representa a história real dos primeiros 9 blocos do Bitcoin, por questões didáticas.


70.5
Satoshi
HAL
Eva
Satoshi 2
Roger
Satoshi 3
Bloco 1
50 BTC
Bloco 2
50 BTC
Bloco 3
50 BTC
Bloco 4
0.25 BTC
10 BTC
39.75 BTC
50 BTC
Bloco 5
0.10 BTC
3.5 BTC
6.5 BTC
0.15 BTC
50 BTC
Bloco 6
50 BTC
0.01 BTC
0.05 BTC
0.09 BTC
Bloco 7
5 BTC
50 BTC
10 BTC
30 BTC
5 BTC
Bloco 8
7 BTC
15 BTC
50 BTC
15 BTC
3 BTC
Paradigma





O que é um UTXO?

Unspent Transaction Output? É hora de entender o que significa através de 3 metáforas: Planilha de Excel, Bonecas Russas e ...

post.paradigma.education

Cada célula (UTXO) pode conter qualquer valor de BTC

Você não precisa comprar 1 BTC inteiro 😅

1 sat = ฿ 0.00000001
10 sats = ฿ 0.0000001
100 sats = ฿ 0.000001
1.000 sats = ฿ 0.00001
10.000 sats = ฿ 0.0001
100.000 sats = ฿ 0.001
1.000.000 sats = ฿ 0.01
10.000.000 sats = ฿ 0.1
100.000.000 sats = ฿ 1

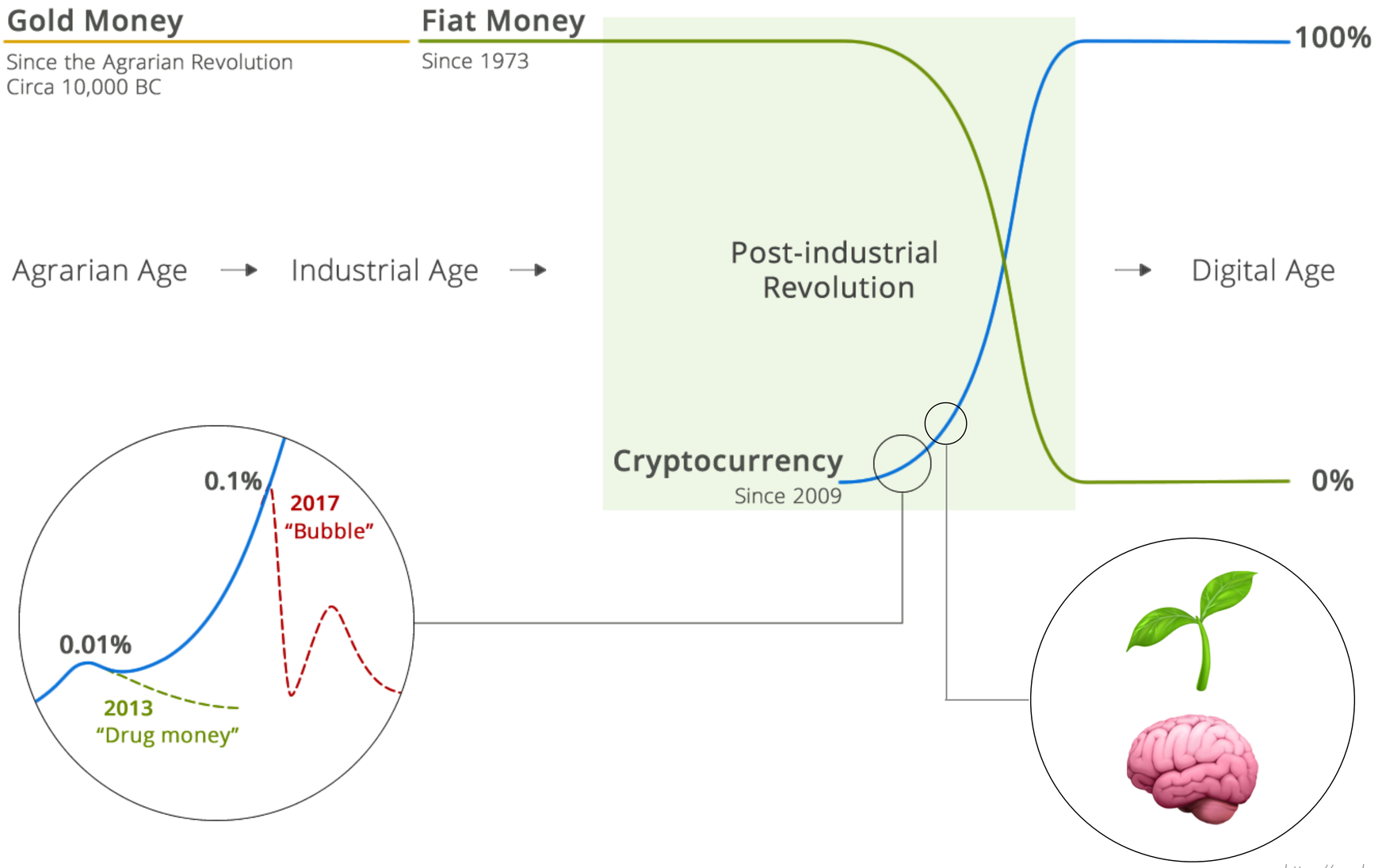
Lucho Poletti

Parte 4

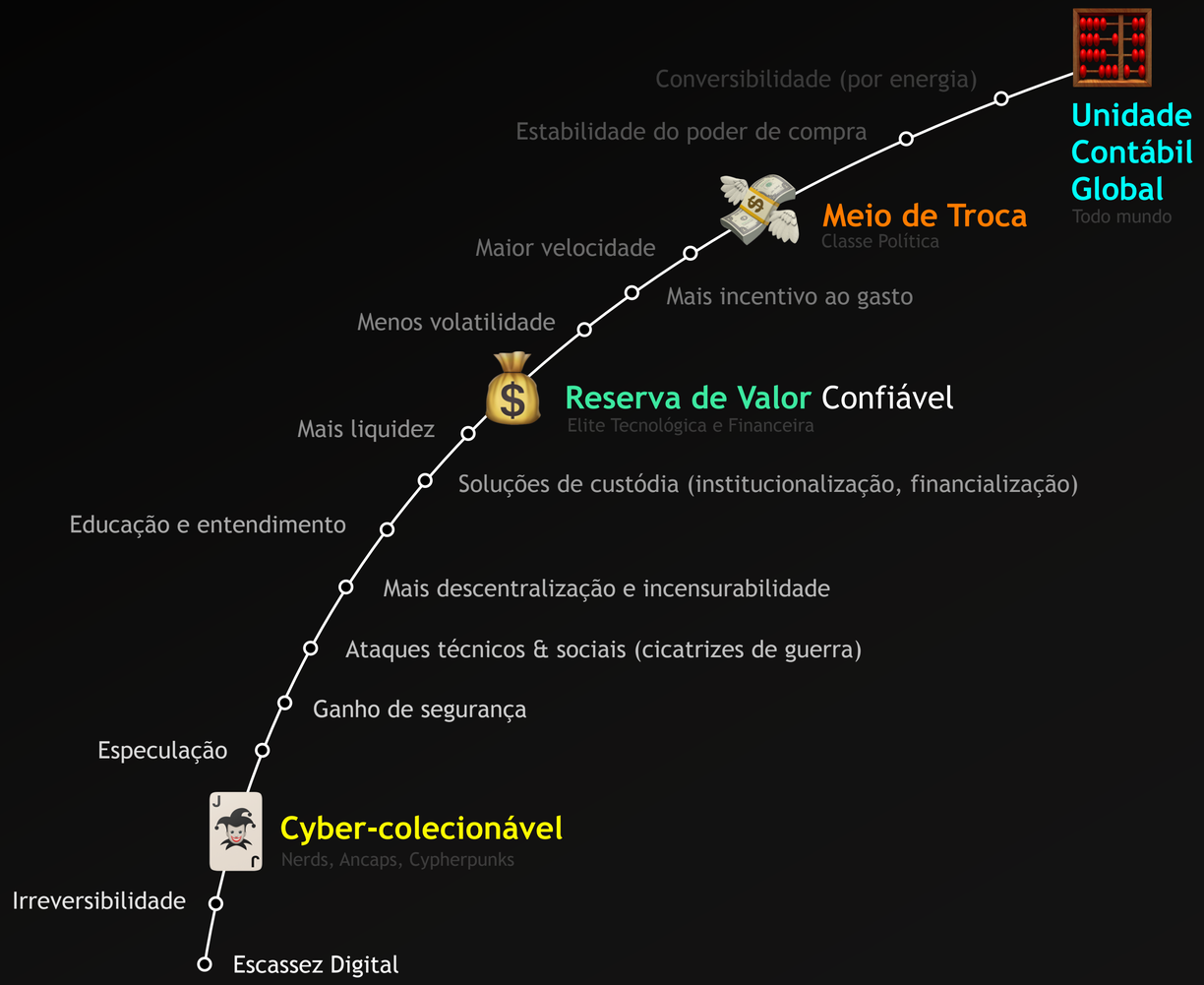
A Teoria dos Ciclos

E os “*halvings*" como “Copas do Mundo”

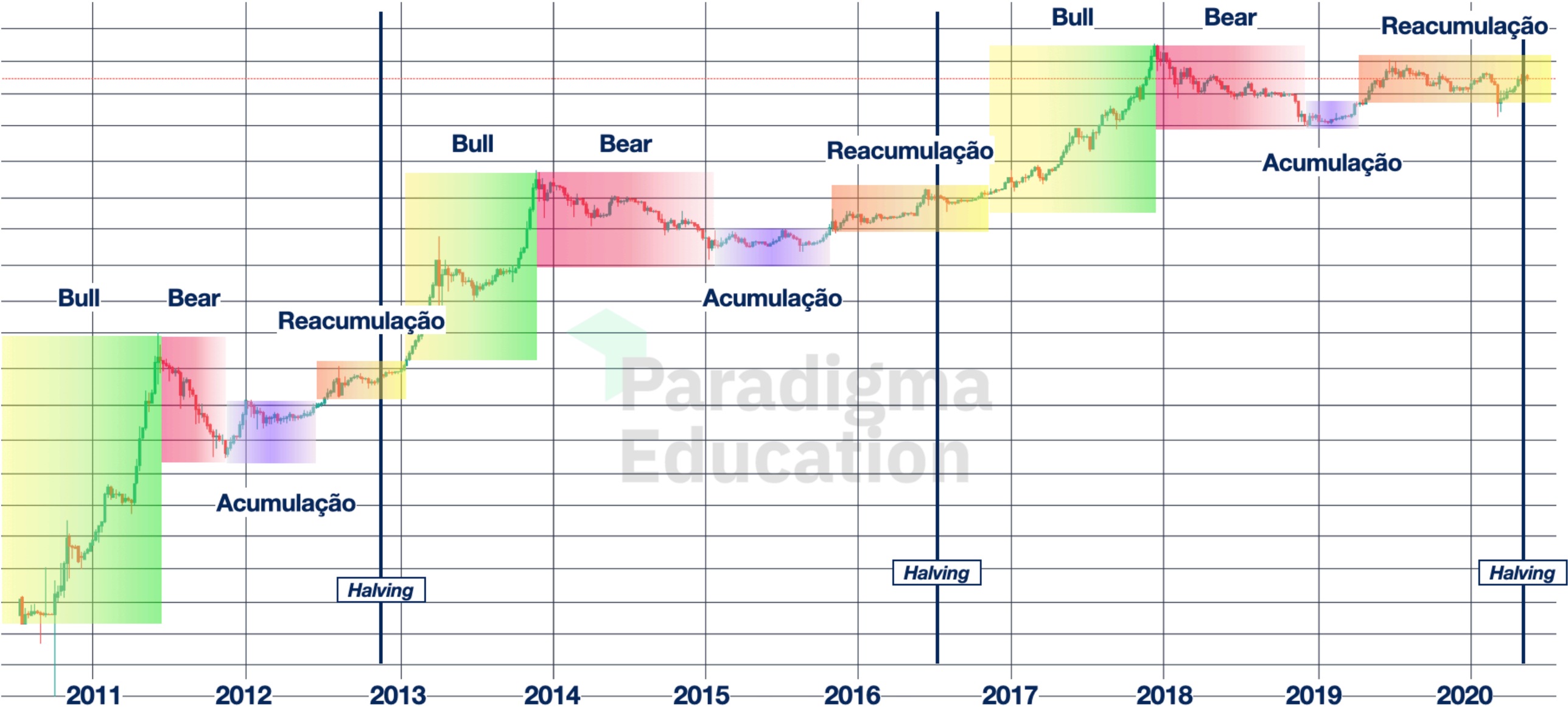
Um horizonte de centenas de anos



https://woobull.com/the-10-000-year-view-of-cryptocurrency/



Efeito *Lindy*

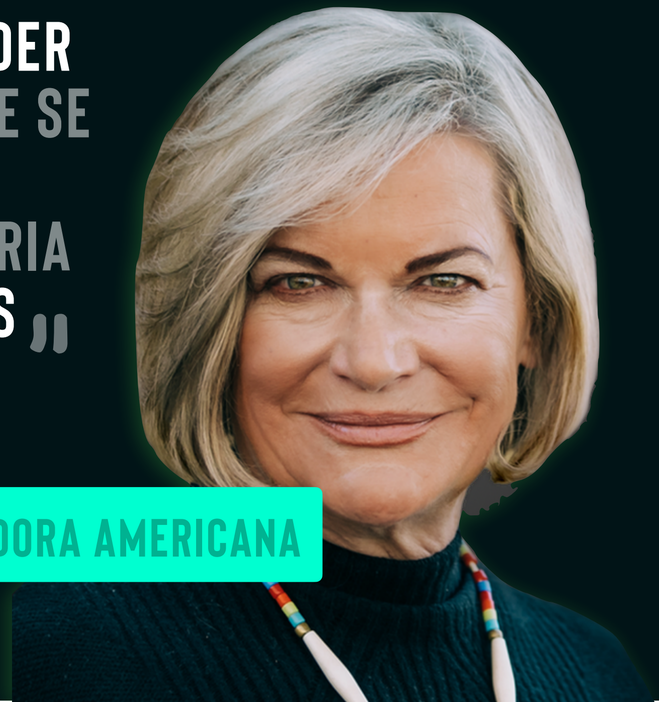

Bull
Bear
Acumulação
Reacumulação
Bull
Bear
Acumulação
Reacumulação
Bull
Bear
Acumulação
Reacumulação
Halving
Halving
Halving
Paradigma Education
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020


34000.00
18000.00
9500.00
4700.00
2300.00
1200.00
600.00
300.00
150.00
75.00
37.50
19.50
9.50
5.00
2.60
1.30
0.65
0.33
0.17
0.09
0.04
0.02
0.01
2012
26 Nov '12
2014
2015
2016
04 Jul '16
2017
2018
2019
2020
11 May '20
2021

Um **Grande Reset…?**

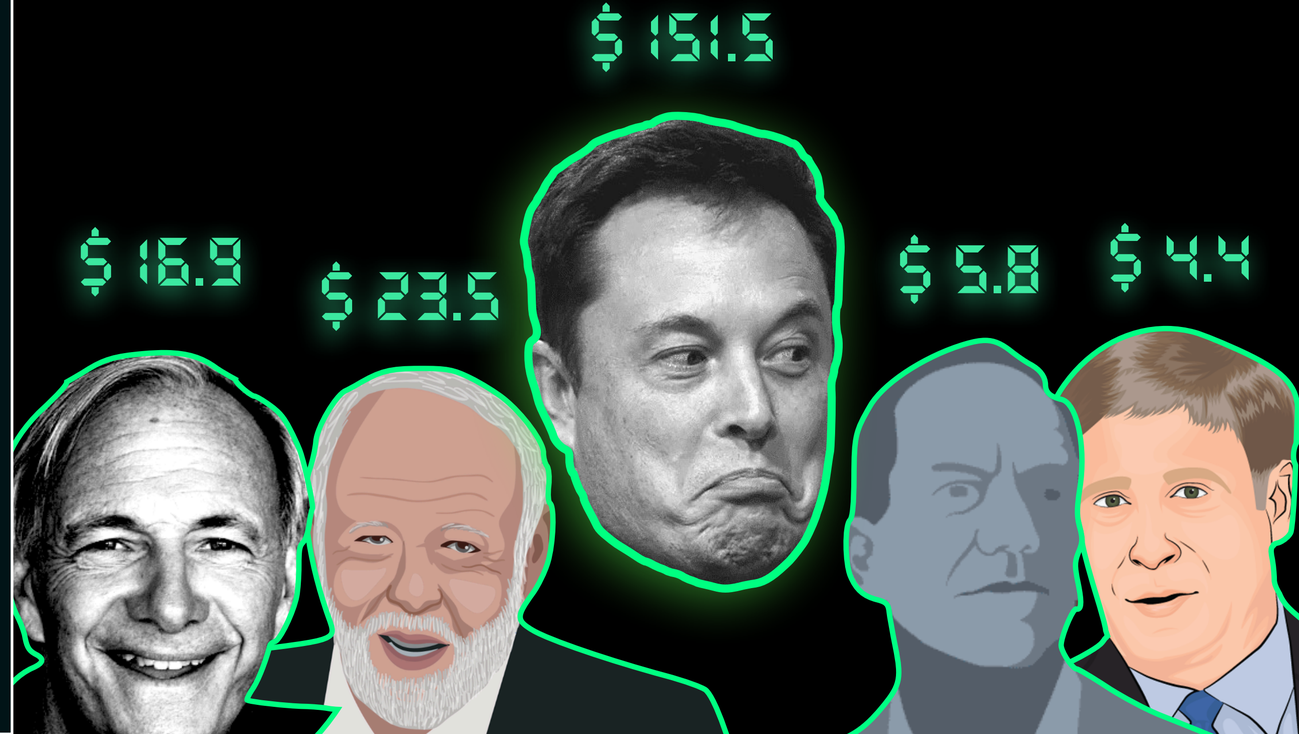
"O BITCOIN UNE O POVO NUM TEMPO CADA VEZ MAIS DIVIDIDO E POLITIZADO"

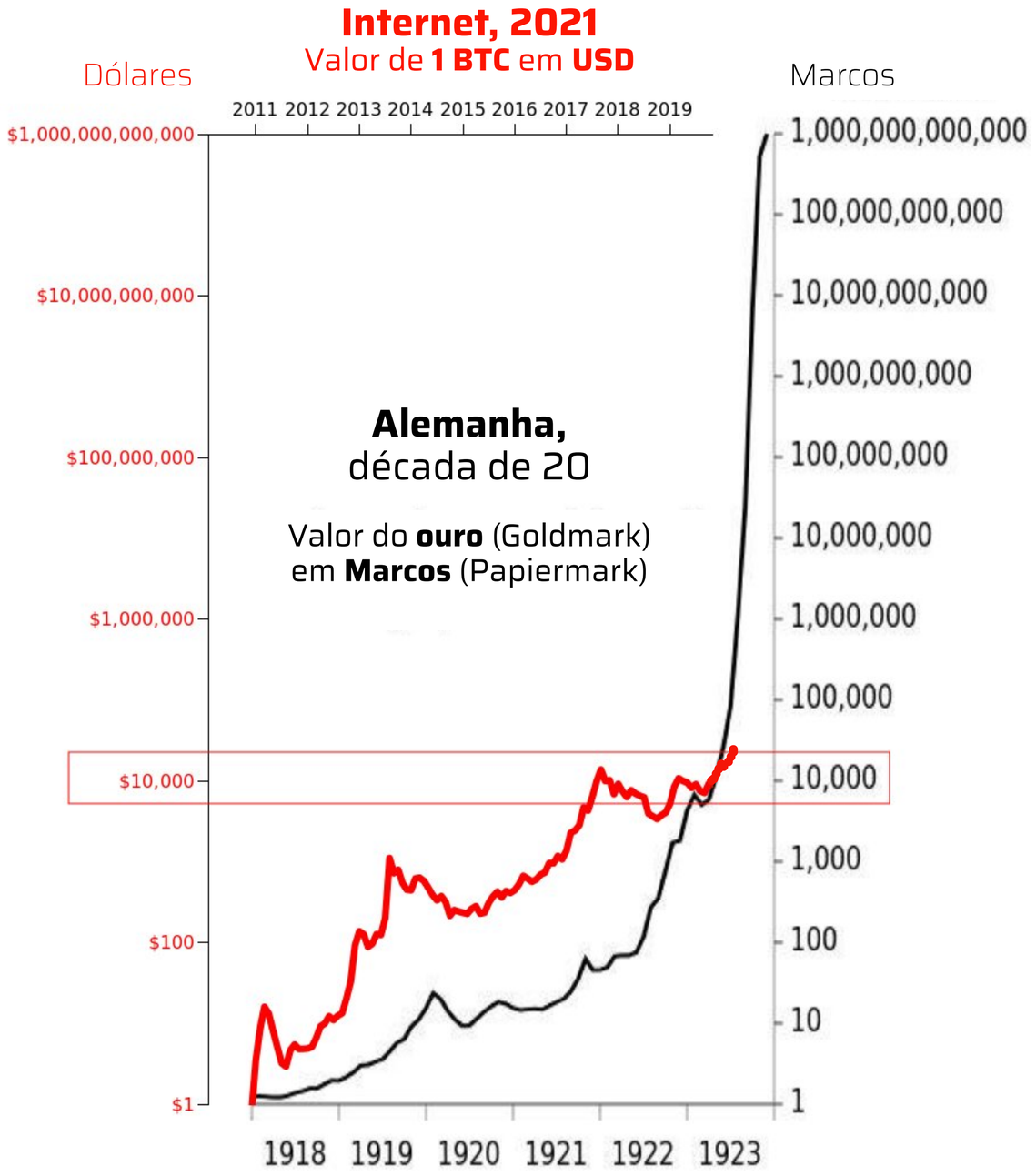
"OS EUA VÃO ENTENDER RÁPIDO O PERIGO DE SE DEIXAR A CHINA DOMINAR A INDÚSTRIA DAS CRIPTOMOEDAS"

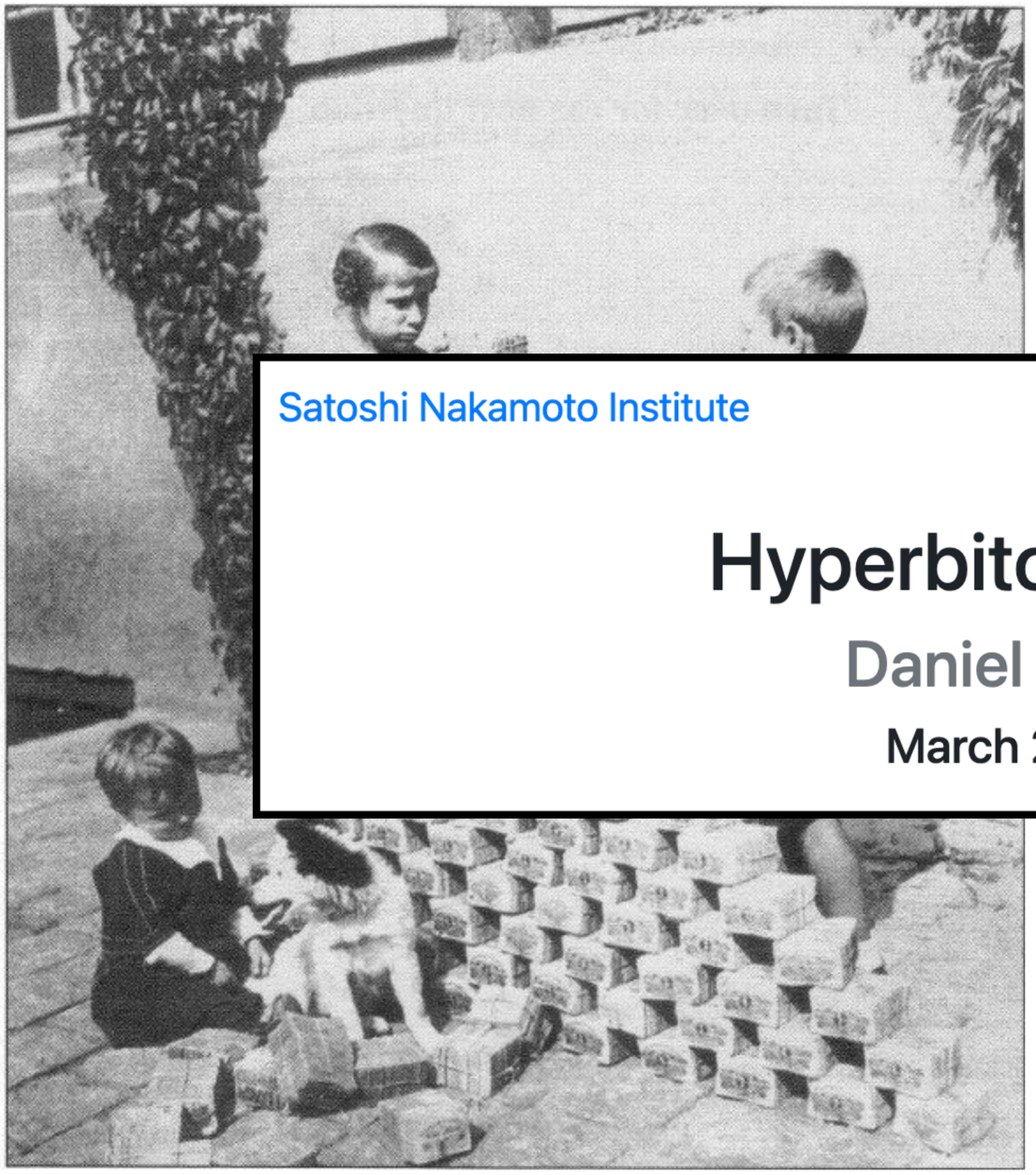


CYNTHIA LUMMIS, SENADORA AMERICANA

RIQUEZA ESTIMADA (EM **BILHÕES DE U$**) DE BILIONÁRIOS QUE ABRAÇARAM A MOEDA EM 2020-21




Internet, 2021
Valor de 1 BTC em USD
Dólares
Marcos
2011 2012 2013 2014 2015 2016 2017 2018 2019
$1,000,000,000,000
$10,000,000,000
$100,000,000
$1,000,000
$10,000
$100
$1
1,000,000,000,000
100,000,000,000
10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
Alemanha,
década de 20
Valor do ouro (Goldmark)
em Marcos (Papiermark)
1918 1919 1920 1921 1922 1923



Satoshi Nakamoto Institute

The Complete Satoshi Literature Research Mempool

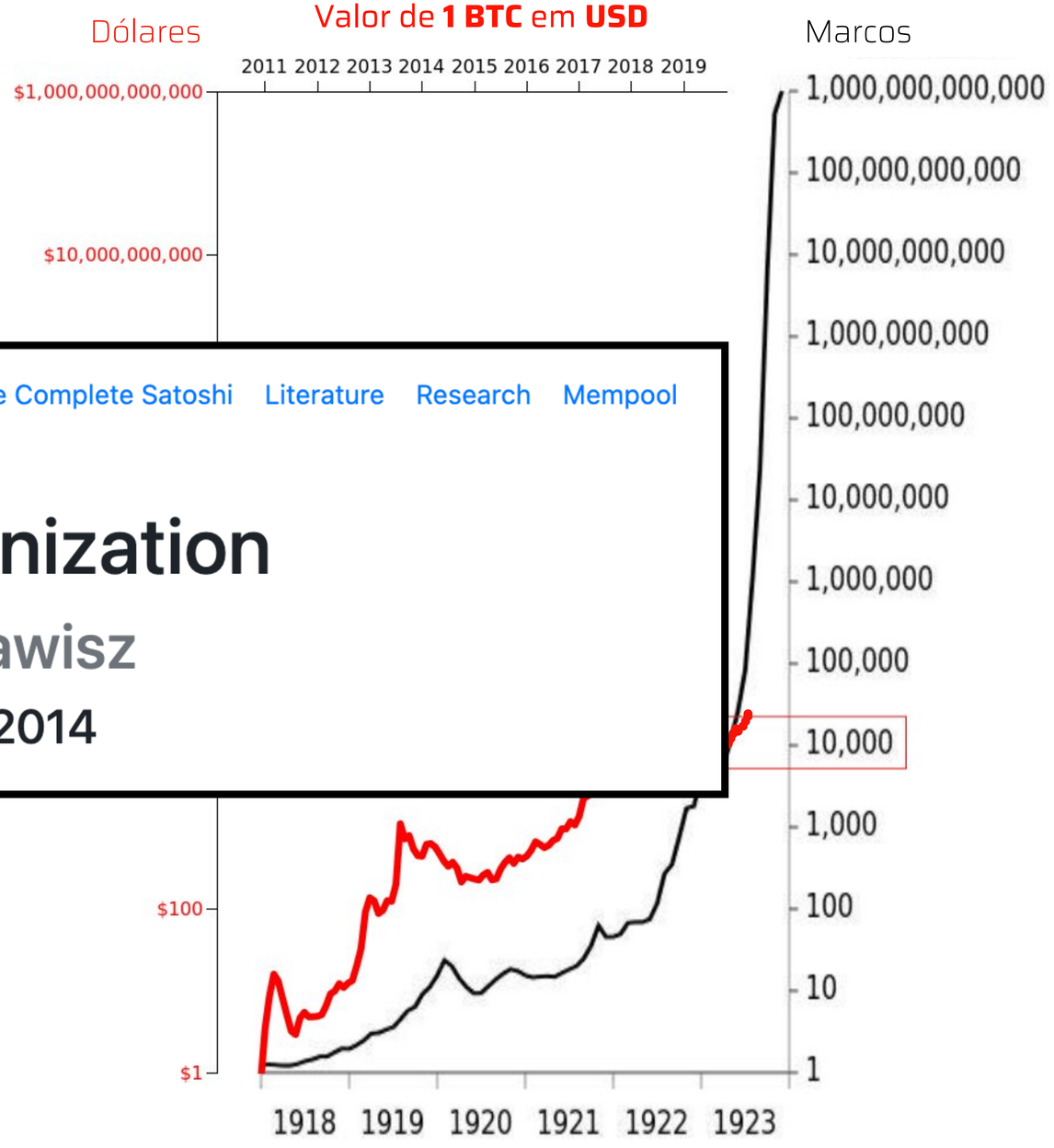
Hyperbitcoinization

Daniel Krawisz

March 29, 2014

Internet, 2021

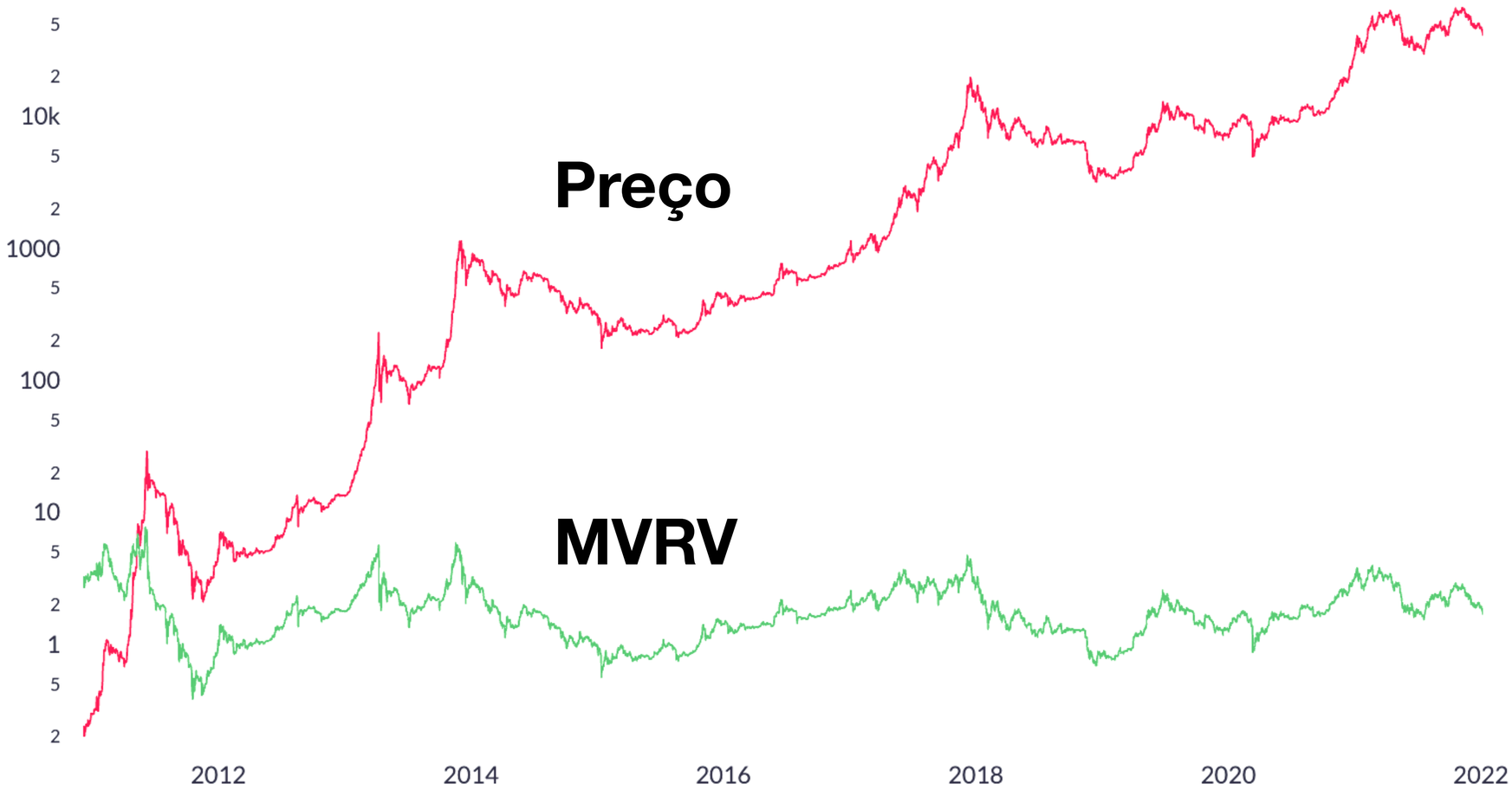
Valor de **1 BTC** em **USD**



Um Indicador Simples:

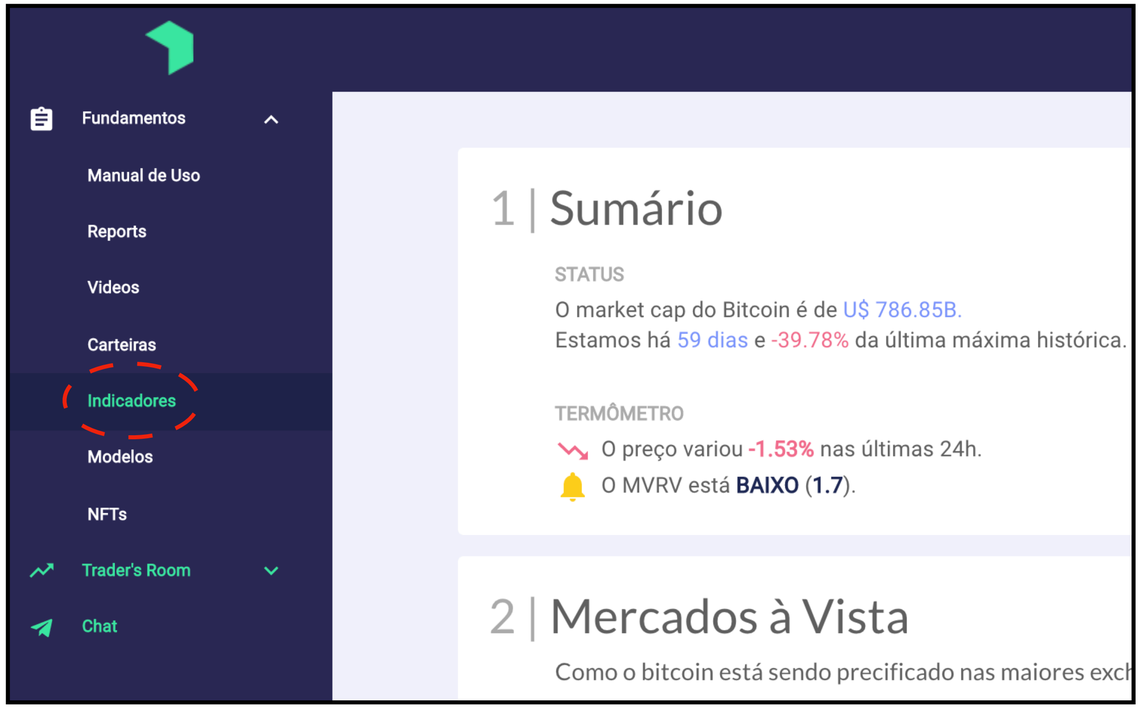
Qual a Melhor Hora de Comprar?

MVRV
(Market Value / Realized Value)



Comprar **abaixo de 1**; reduzir risco **acima de 3.5**


6
4
2
0
50k
0
2012
2014
2016
2018
2020
2022



MVRV: Medindo Euforia e Pânico nos Mercados

Identificando pânico e euforia no Bitcoin - um indicador simples para facilitar sua tomada de decisão.

post.paradigma.education

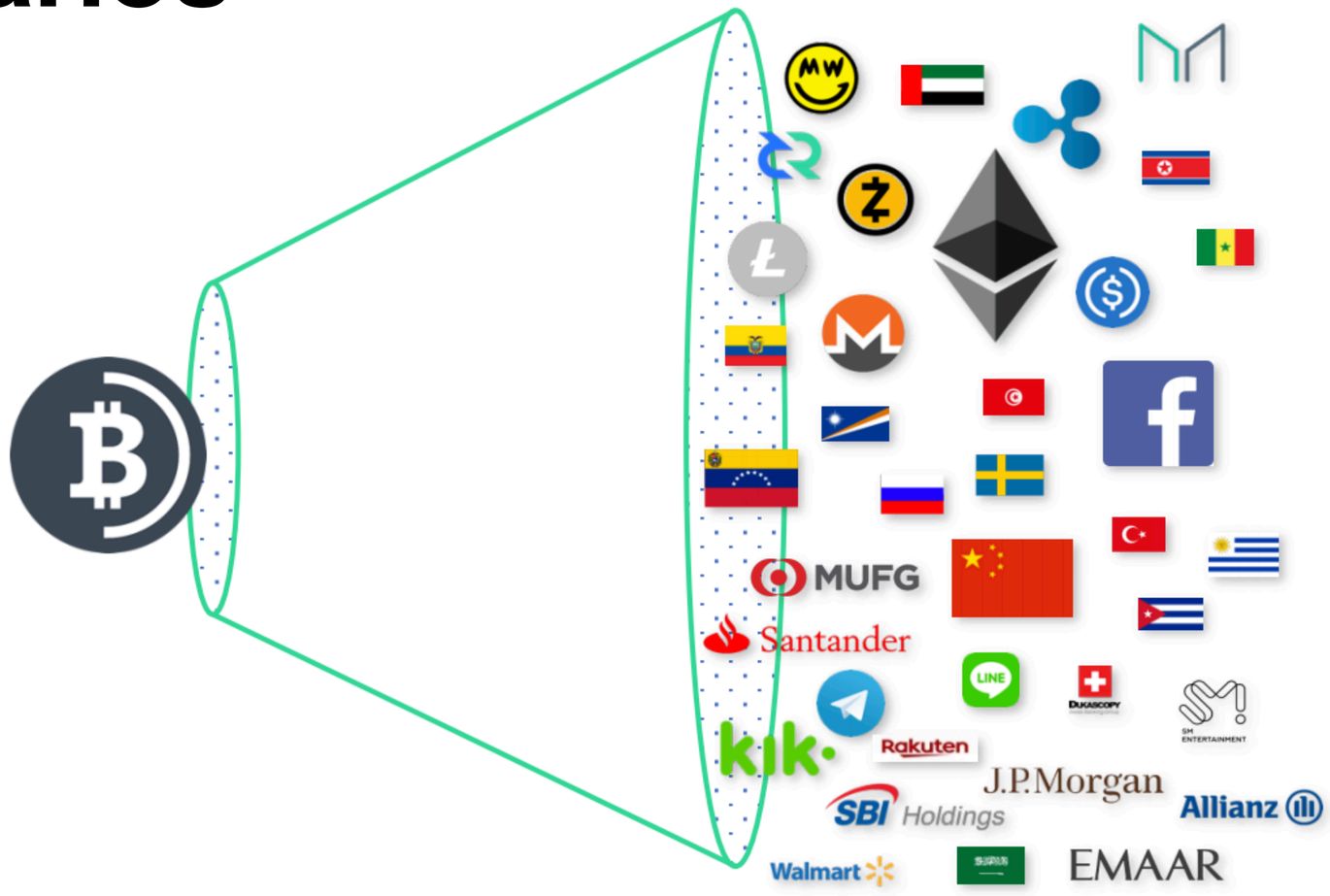
Parte 5

A Origem das Altcoins

E os “*trade-offs*” de Cada Moeda

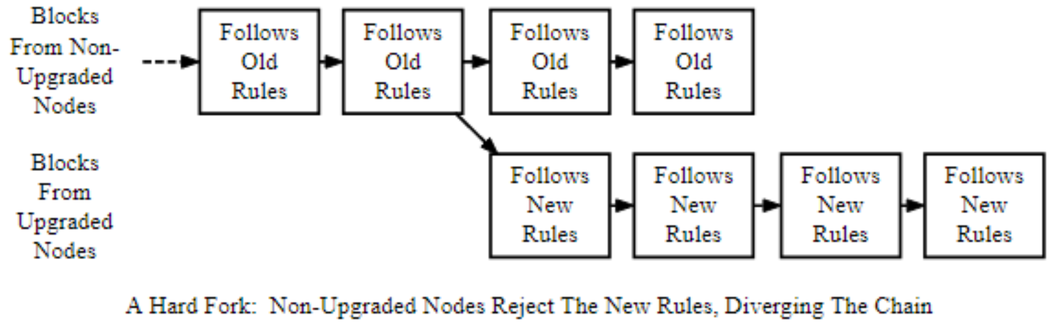
Uma **Explosão Cambriana** de **Sistemas Monetários**

Ligação Inextricável entre o **Estado** e o **Dinheiro**	O **Dinheiro** como **Iniciativa Privada**
A Ausência de um **Livre Mercado** Para **“Dinheiros"**	**Sistemas Monetários Digitalmente Nativos** e **“Soberanos sem Nação”**
Exploração Estatal das **Limitações** de **Formas Apolíticas** de Se **Guardar Valor** (ex: **ouro**)	Alternativas de **Auto-Custódia** e **Propriedade Digital** Permitidas por **Criptografia Assimétrica**

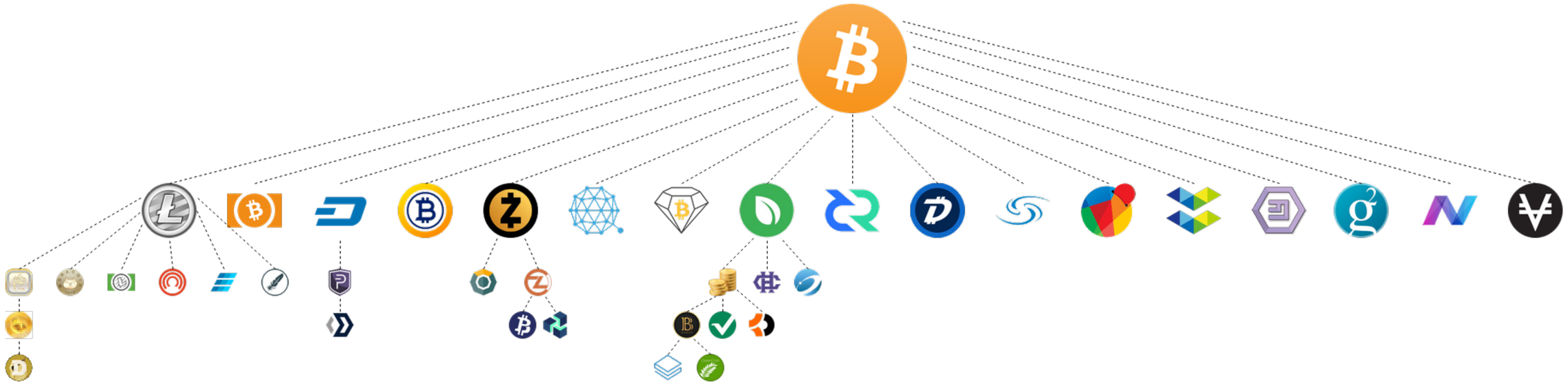


Fonte: ARK LLC, 2019

Forks: bifurcações



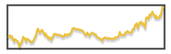
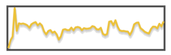
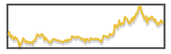
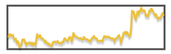
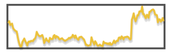
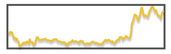
A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain



Fonte: Coursera.

Top 10 moedas em **capitalização de mercado**

Dez/2013

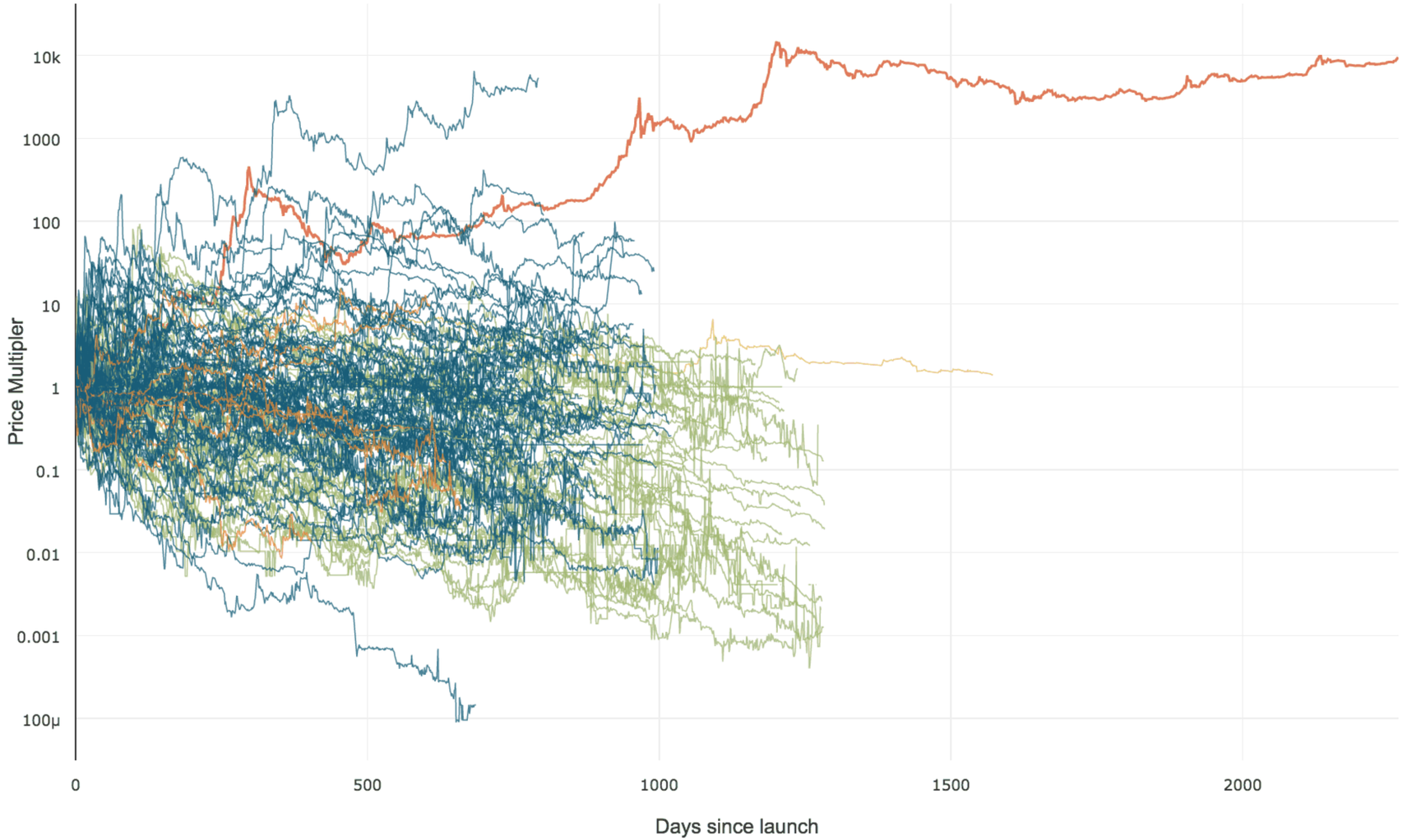
1	Bitcoin	$ 8,855,864,420	$ 726.89	12,183,225 BTC	$ 46,076,750	-4.94 %	
2	Ripple	$ 2,690,298,053	$ 0.027	99,999,998,252 XRP	$ 175,159	+9.26 %	
3	Litecoin	$ 551,369,874	$ 22.66	24,327,542 LTC	$ 30,220,812	-8.57 %	
4	MasterCoin	$ 109,379,395	$ 194.22	563,162 MSC	$ 235,369	+0.62 %	
5	Peercoin	$ 78,361,173	$ 3.74	20,973,413 PPC	$ 494,620	-4.78 %	
6	Namecoin	$ 35,990,073	$ 4.73	7,605,592 NMC	$ 1,445,386	-8.79 %	
7	Quark	$ 28,284,018	$ 0.11	246,850,233 QRK	$ 96,909	-4.66 %	
8	ProtoShares	$ 24,025,818	$ 19.89	1,208,072 PTS	$ 46,878	-3.60 %	
9	WorldCoin	$ 18,442,927	$ 0.49	37,365,620 WDC	$ 162,928	-10.24 %	
10	Megacoin	$ 17,671,960	$ 0.82	21,469,025 MEC	$ 54,401	-9.51 %	

Jan/2022

1	Bitcoin BTC Buy	$41,643.23	1.09%	12.10%	$787,263,746,313	$27,786,790,833 667,930 BTC	18,924,006 BTC	
2	Ethereum ETH Buy	$3,113.24	3.72%	17.15%	$369,894,612,778	$16,349,449,836 5,263,633 ETH	119,085,934 ETH	
3	Tether USDT Buy	$1.00	0.02%	0.04%	$78,311,025,495	$62,571,209,895 62,556,538,471 USDT	78,292,663,468 USDT	
4	Binance Coin BNB Buy	$431.54	5.80%	17.52%	$71,823,853,457	$4,040,351,432 9,383,168 BNB	166,801,148 BNB	
5	USD Coin USDC	$1.00	0.00%	0.04%	$43,607,586,236	$4,120,493,400 4,117,891,184 USDC	43,580,046,735 USDC	
6	Solana SOL Buy	$139.40	4.97%	20.80%	$43,255,788,486	$2,639,863,012 19,000,949 SOL	311,342,303 SOL	
7	Cardano ADA	$1.17	6.86%	14.42%	$39,000,554,212	$1,537,457,340 1,320,596,341 ADA	33,499,459,048 ADA	
8	XRP XRP	$0.7464	3.26%	11.95%	$35,484,205,996	$1,712,125,483 2,295,616,622 XRP	47,577,198,013 XRP	
9	Terra LUNA Buy	$70.84	0.99%	21.59%	$25,118,548,216	$2,485,144,923 35,461,329 LUNA	358,424,609 LUNA	
10	Polkadot DOT	$23.95	5.51%	16.99%	$23,611,840,420	$1,552,411,797 64,930,550 DOT	987,579,315 DOT	

Fonte: CoinMarketCap

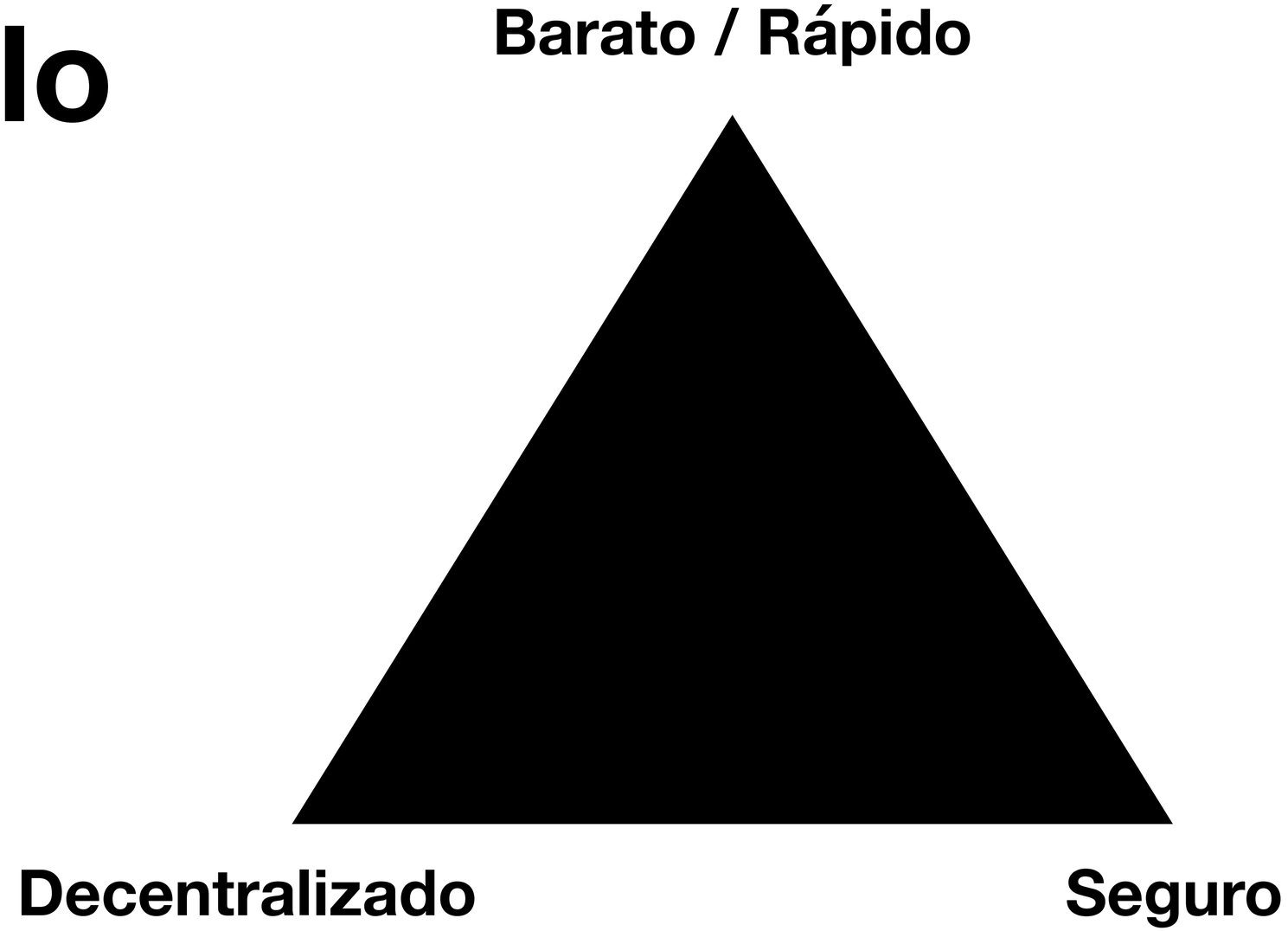
118 moedas (>U$250k mcap) **entre 2011 e 2016**



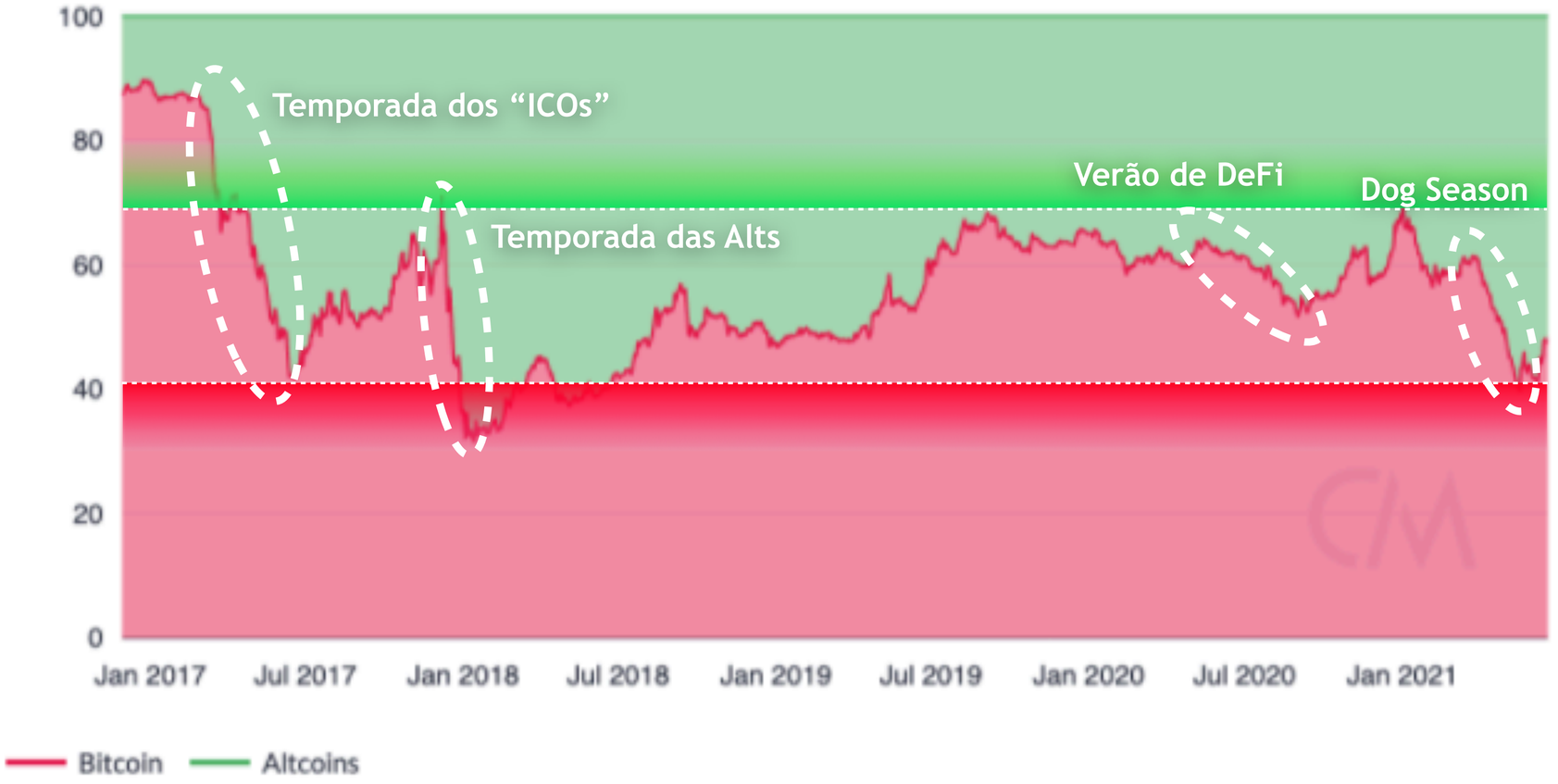
Fonte: https://woobull.com/data-visualisation-118-coins-plotted-over-time-this-is-why-hodl-alt-coin-indexes-dont-work/s/

O **Triângulo** de **Zooko**

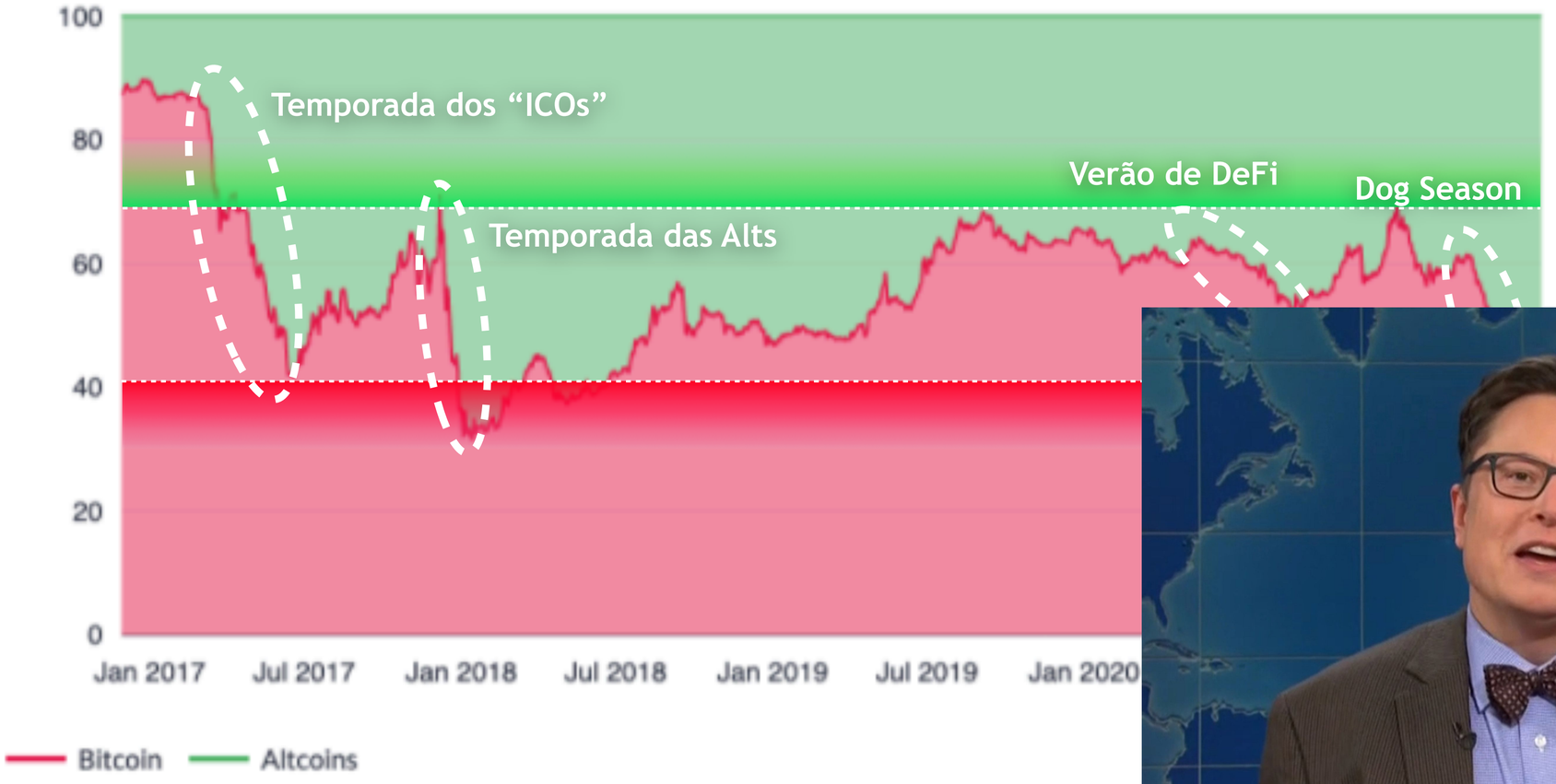
Um **trilema** em que se pode ter **2** de **3 atributos**



A “**Dominância** do **Bitcoin**”



A “**Dominância** do **Bitcoin**”



Vitalik Buterin

(criou a Ethereum aos 19 anos)

Vitalik Buterin

Conheceu o BTC pelo pai

Fundou a Bitcoin Magazine

Trabalhou na Mastercoin
(uma das primeiras altcoins)

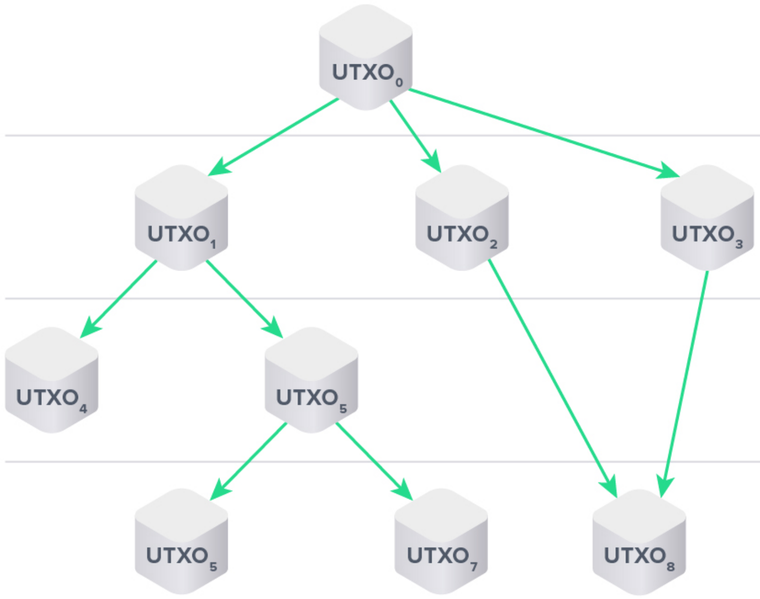
O Bitcoin não tem um conceito de “endereços” ou programas.

A “base de dados” só guarda um registro de todas as “entradas”, junto com condições para que cada uma possa ser “movida” (gasta) . Normalmente, essa condição especifica uma “pessoa” que pode gastar as moedas de cada “entrada”.

Já a Ethereum tem endereços, “programas” e interações arbitrárias entre eles.

Na “***planilha da Ethereum***”, dá pra escrever **programas** - além de meros **valores**

Modelo do Bitcoin



Directed graph of assets (UTXOs) moving between users

Modelo da Ethereum

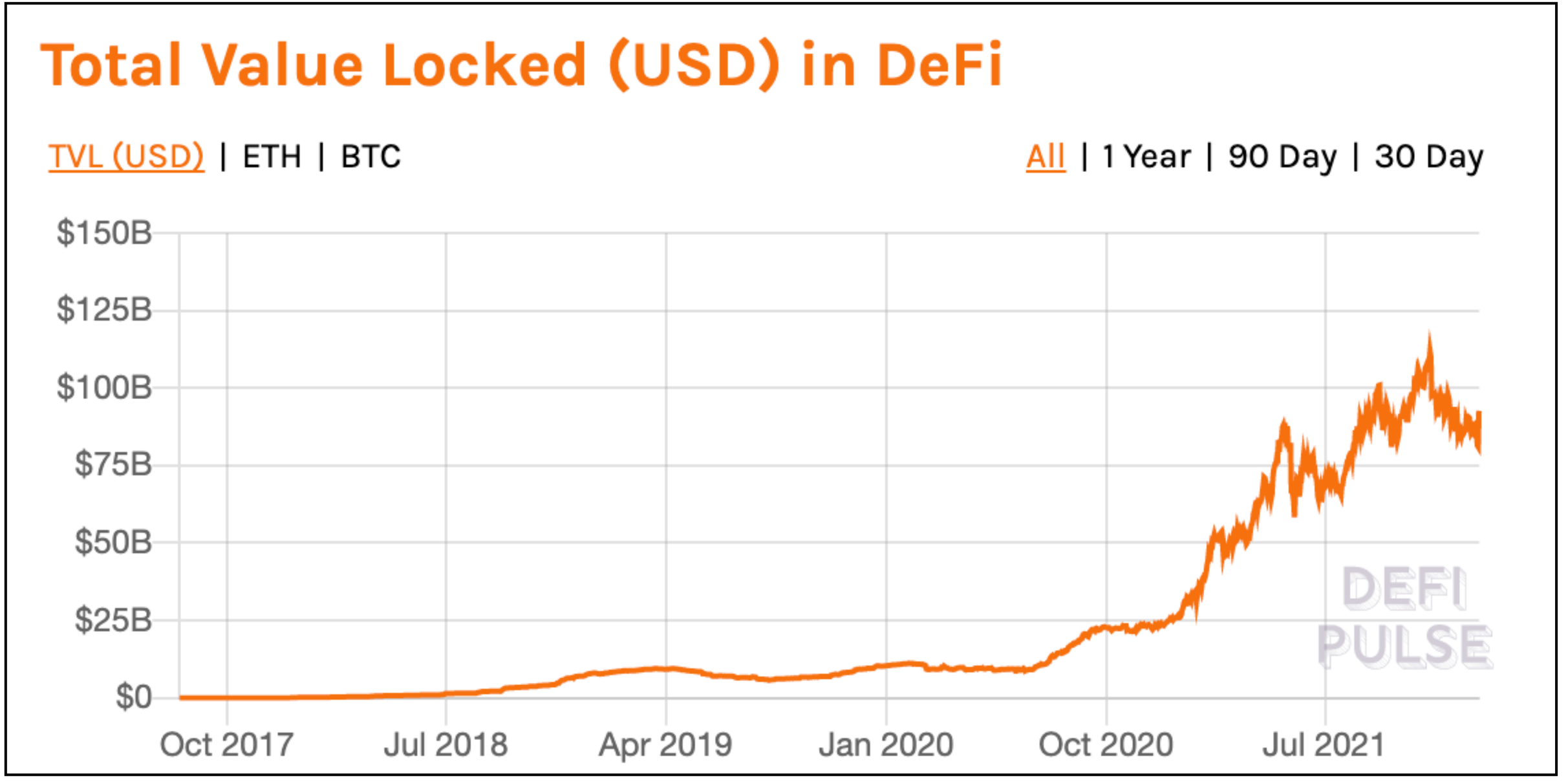
Database of network states

UM CHOQUE *de* CULTURA

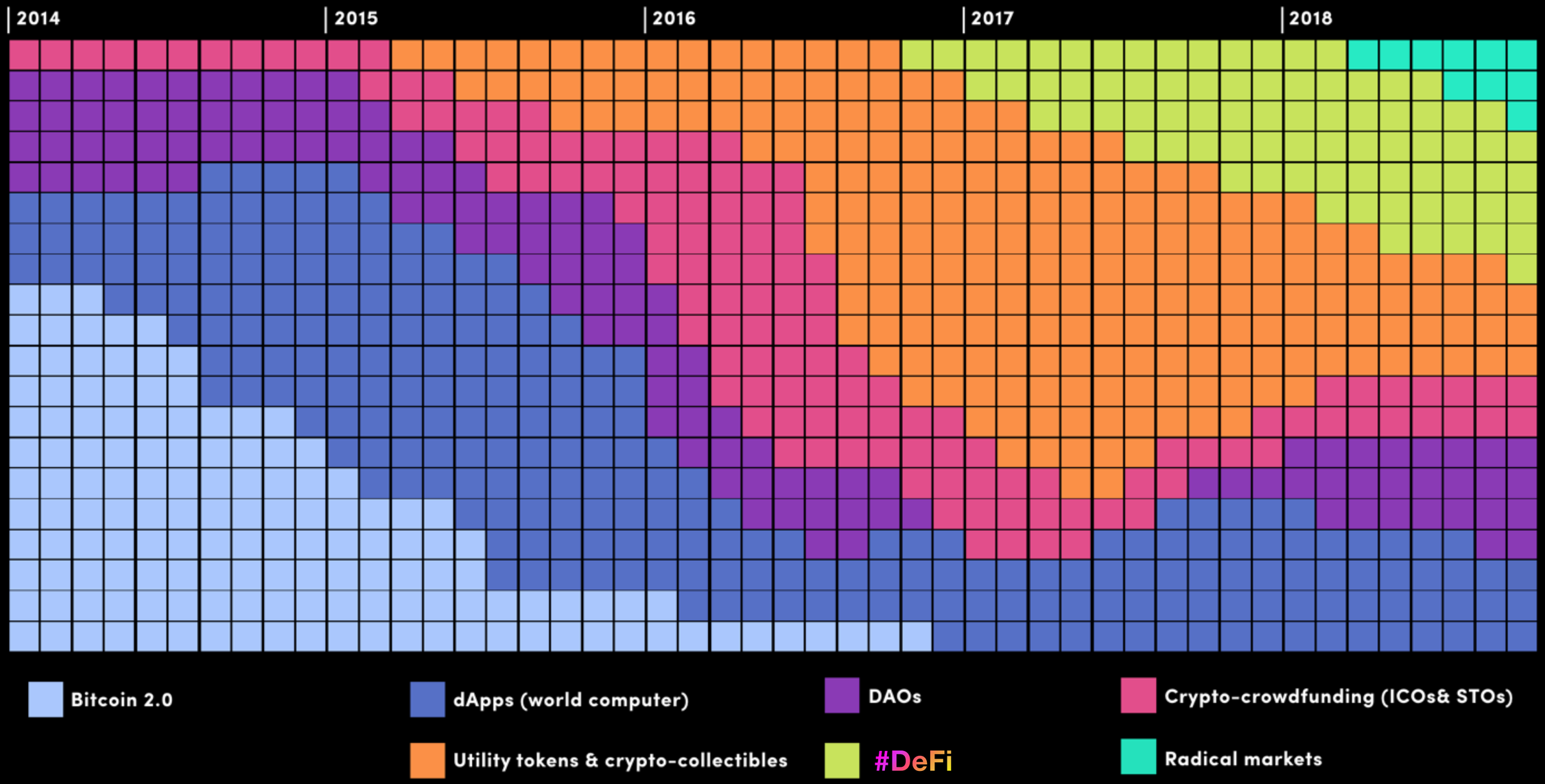
CONSERVADORISMO
MONOTÔNICO
UM PROJETO “PRONTO"
SEM LÍDERES

“MOVE FAST, BREAK THINGS”
COMPLEXO
UM PROJETO EM ANDAMENTO
COM LÍDERES

Total Value Locked (USD) in DeFi



Narrativas da Ethereum ao Longo do Tempo

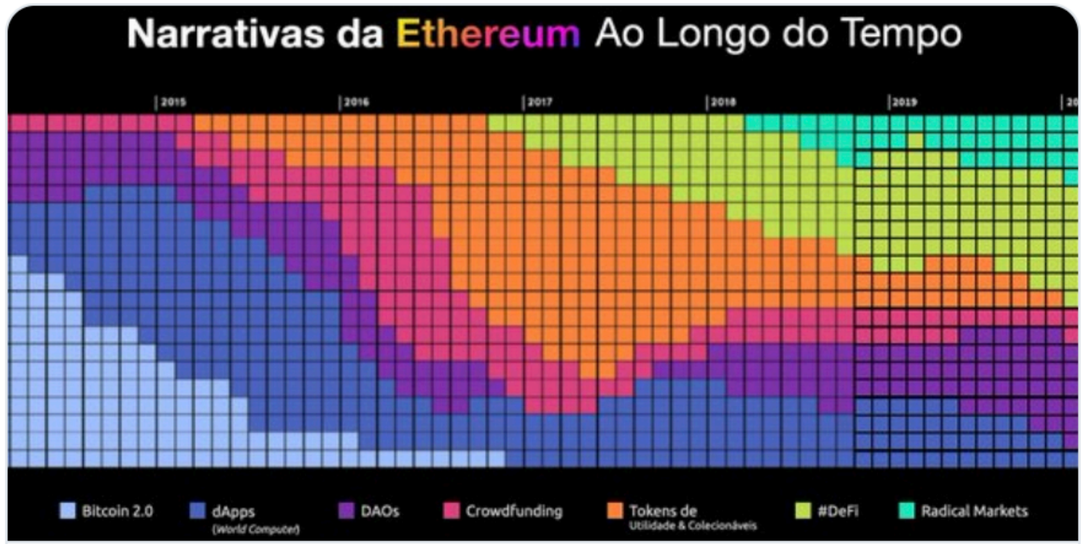


Guardemos este **assunto**…

MÓDULO
03

DEFI (FINANÇAS DESCENTRALIZADAS), STAKING

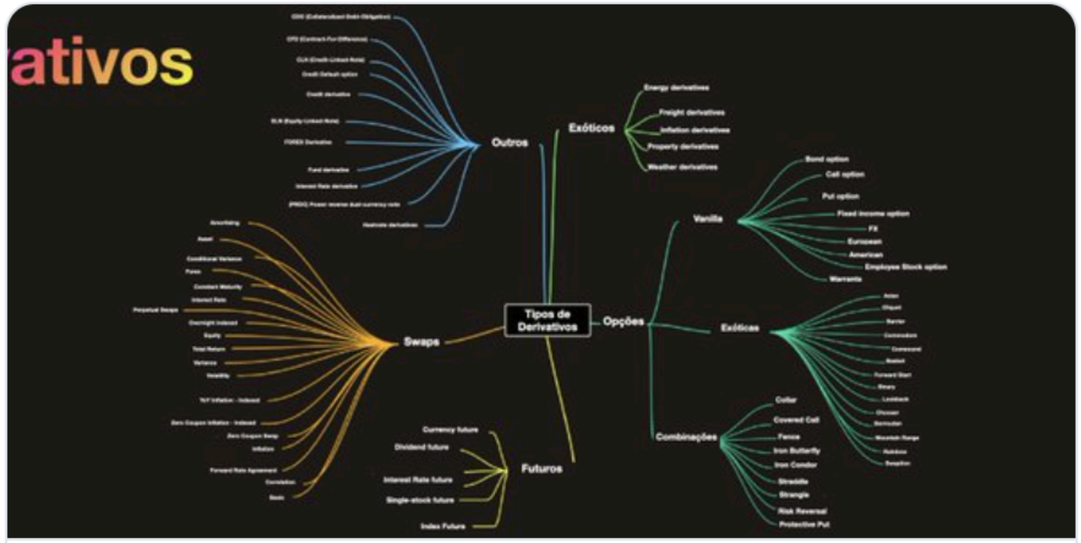
Como ganhar 10% ao ano em criptodólares



🔷 **Uma Breve História da Ethereum**

Como as narrativas da Ethereum (e do ETH) evoluíram ao longo do tempo.

post.paradigma.education



👶🏽 **DeFi pt.1: Explique Como Se Eu Tivesse 5 Anos**

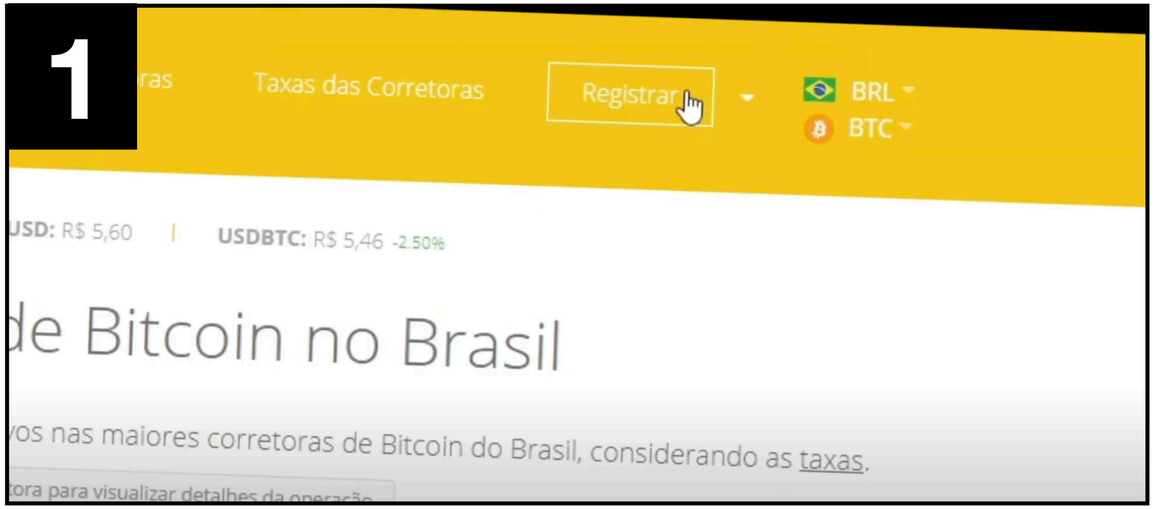
O que é #DeFi, afinal? Quais avanços trazem em relação a instrumentos financeiros legados?

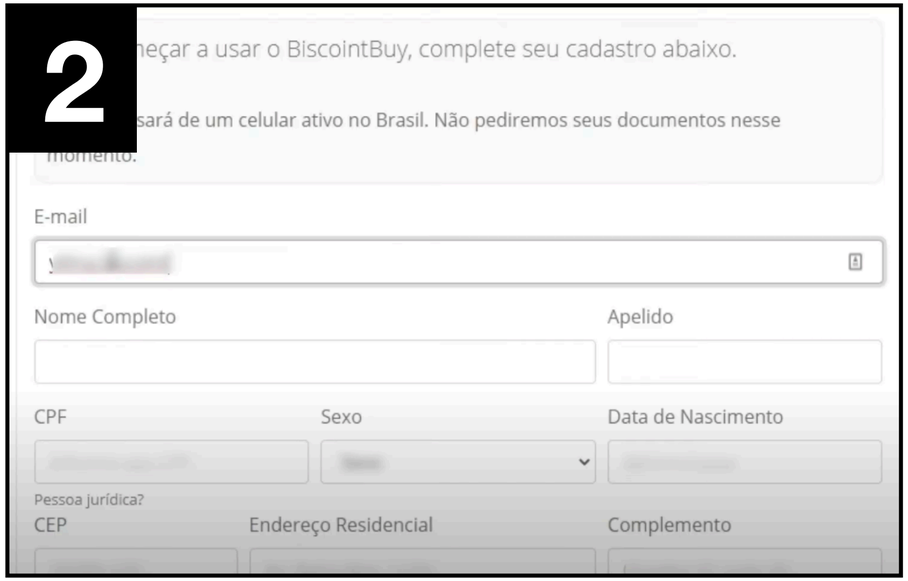
post.paradigma.education

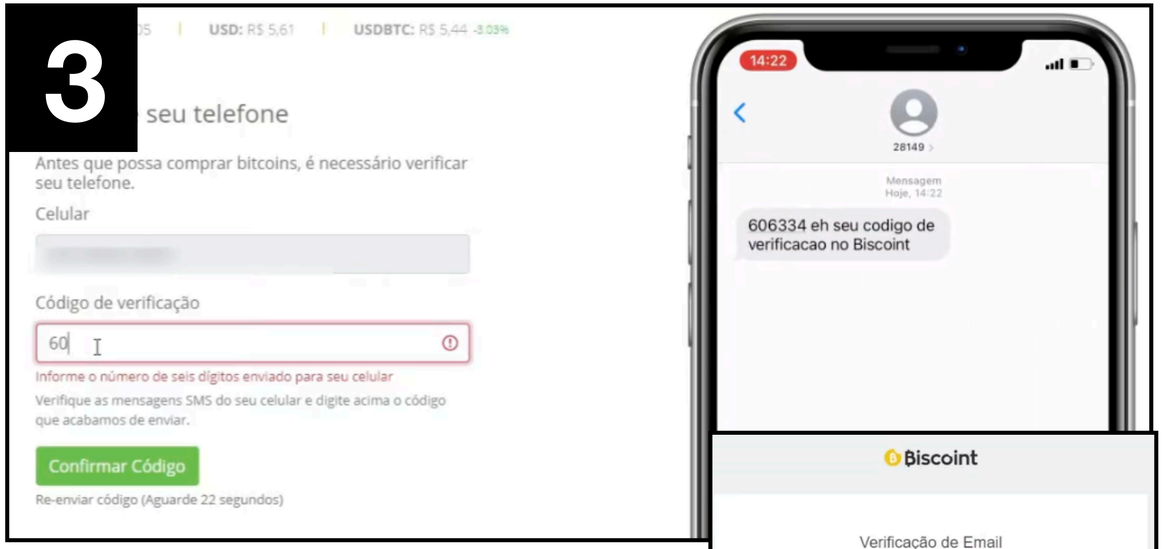
Prática

Abrindo uma Conta em *Exchange*

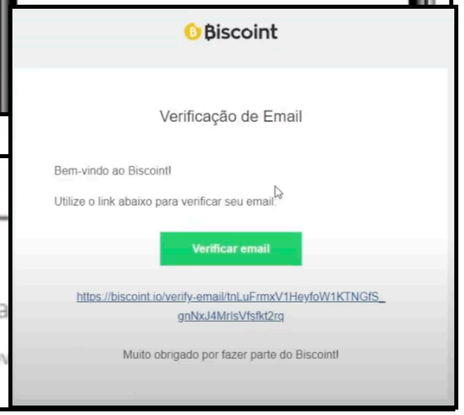
Biscoint e MercadoBitcoin


1
Taxas das Corretoras
Registrar
BRL
BTC
USD: R$ 5,60
USDBTC: R$ 5,46 -2.50%
de Bitcoin no Brasil
os nas maiores corretoras de Bitcoin do Brasil, considerando as taxas.

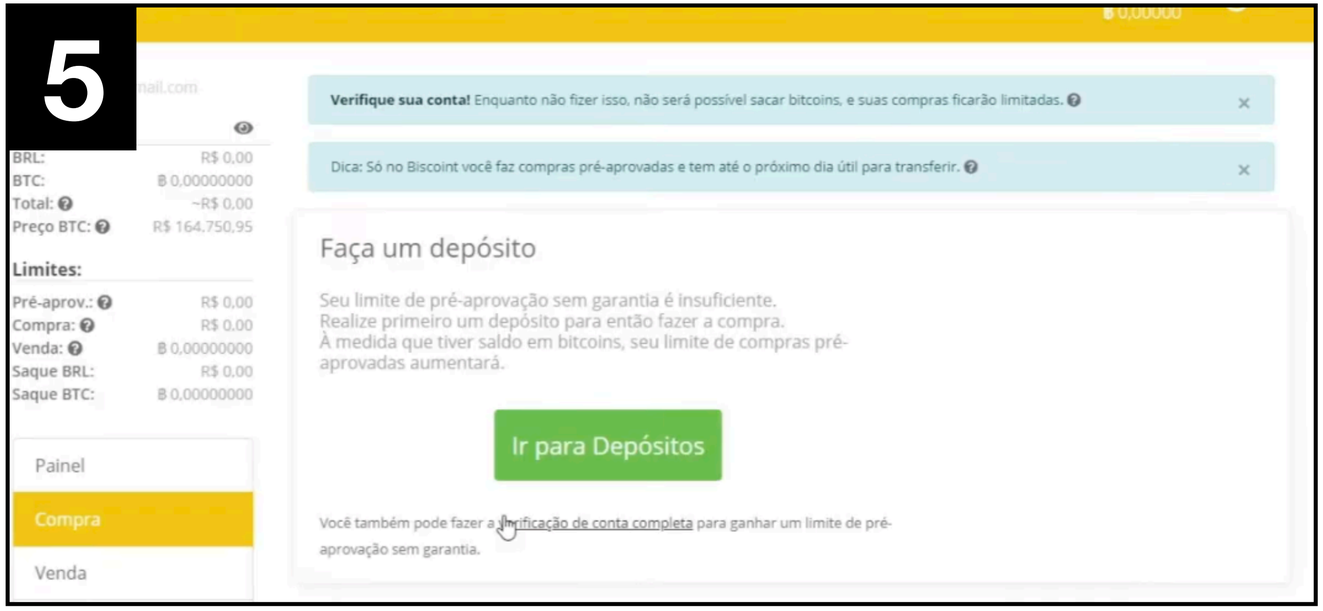

2
neçar a usar o BiscointBuy, complete seu cadastro abaixo.
sará de um celular ativo no Brasil. Não pediremos seus documentos nesse momento.
E-mail
Nome Completo
Apelido
CPF
Sexo
Data de Nascimento
Pessoa jurídica?
CEP
Endereço Residencial
Complemento


3
USD: R$ 5,61
USDBTC: R$ 5,44 -3.03%
seu telefone
Antes que possa comprar bitcoins, é necessário verificar seu telefone.
Celular
Código de verificação
60
Informe o número de seis dígitos enviado para seu celular
Verifique as mensagens SMS do seu celular e digite acima o código que acabamos de enviar.
Confirmar Código
Re-enviar código (Aguarde 22 segundos)

14:22
28149
Mensagem
Hoje, 14:22
606334 eh seu codigo de verificacao no Biscoint


Biscoint
Verificação de Email
Bem-vindo ao Biscoint!
Utilize o link abaixo para verificar seu email.
Verificar email
https://biscoint.io/verify-email/tnLuFrmxV1HeyfoW1KTNGfS_gnNxJ4MrIsVfsfkt2rg
Muito obrigado por fazer parte do Biscoint!

4
Cheque seu e-
Precisamos confirmar seu e-mail. Por favor, acesse a sua ca
Não recebeu o e-mail? Clique aqui para receber um nov


5
Verifique sua conta! Enquanto não fizer isso, não será possível sacar bitcoins, e suas compras ficarão limitadas.
Dica: Só no Biscoint você faz compras pré-aprovadas e tem até o próximo dia útil para transferir.
BRL: R$ 0,00
BTC: ฿ 0,00000000
Total: ~R$ 0,00
Preço BTC: R$ 164.750,95
Limites:
Pré-aprov.: R$ 0,00
Compra: R$ 0,00
Venda: ฿ 0,00000000
Saque BRL: R$ 0,00
Saque BTC: ฿ 0,00000000
Painel
Compra
Venda
Faça um depósito
Seu limite de pré-aprovação sem garantia é insuficiente.
Realize primeiro um depósito para então fazer a compra.
À medida que tiver saldo em bitcoins, seu limite de compras pré-aprovadas aumentará.
Ir para Depósitos
Você também pode fazer a verificação de conta completa para ganhar um limite de pré-aprovação sem garantia.

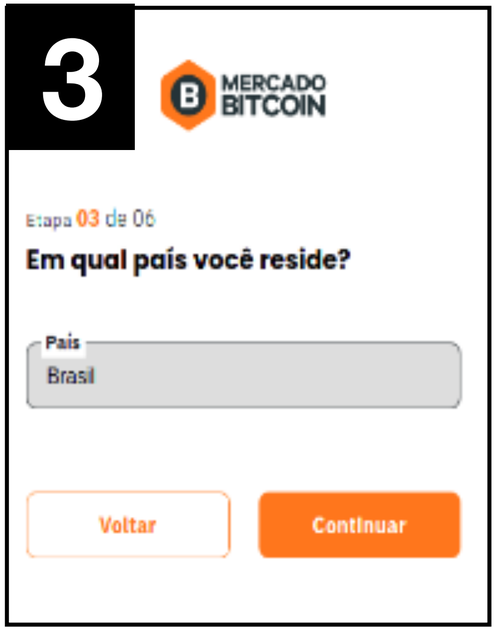
1


MERCADO BITCOIN
Etapa 01 de 06
Seja bem vindo(a)
Qual é o seu e-mail
Crie sua senha de acesso
Pelo menos 8 caracteres, sendo 1 caractere especial, uma letra maiúscula, uma letra minúscula e um número
Continuar
Já tem conta? Acesse sua conta

2


MERCADO BITCOIN
Etapa 02 de 06
Dados pessoais
Qual é o seu CPF ou CNPJ?
E sua data de nascimento
Voltar
Continuar

3


MERCADO BITCOIN
Etapa 03 de 06
Em qual país você reside?
País
Brasil
Voltar
Continuar

4


MERCADO BITCOIN
Etapa 04 de 06
Qual é o seu celular
Celular
Voltar
Continuar

5


MERCADO BITCOIN
Etapa 05 de 06
Qual é o seu CEP?
CEP
Não sei meu CEP
Voltar
Continuar

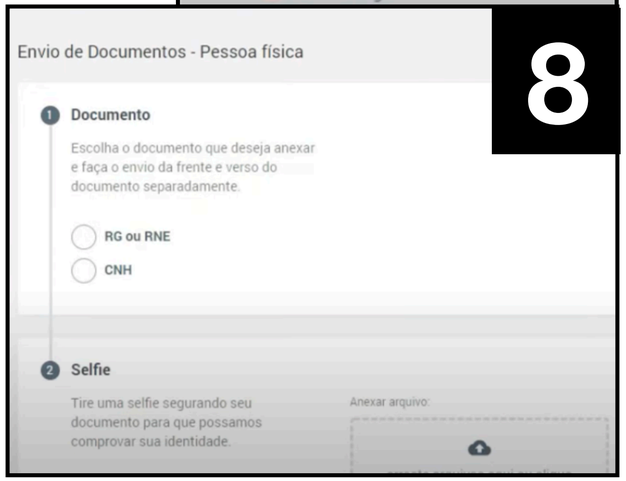
6


Endereço
Nº
Não tenho número
Bairro (opcional)
Complemento (opcional)
Voltar
Continuar

7


MERCADO BITCOIN
« voltar para home
Configurações
Cadastro
Atualização Cadastral
Alterar Perfil
Alterar E-mail
Documento e Selfie
Validar CPF/CNPJ
Segurança
Checklist de segurança
Alterar Senha
Verificação em Duas Etapas (2FA)
Computadores memorizados
Palavra segura

8


Envio de Documentos - Pessoa física
Documento
Escolha o documento que deseja anexar e faça o envio da frente e verso do documento separadamente.
RG ou RNE
CNH
Selfie
Tire uma selfie segurando seu documento para que possamos comprovar sua identidade.
Anexar arquivo:

Leitura Complementar

O *Whitepaper*

Os ***Principais*** *Conceitos*

Relações Entre os Agentes na ***Rede***

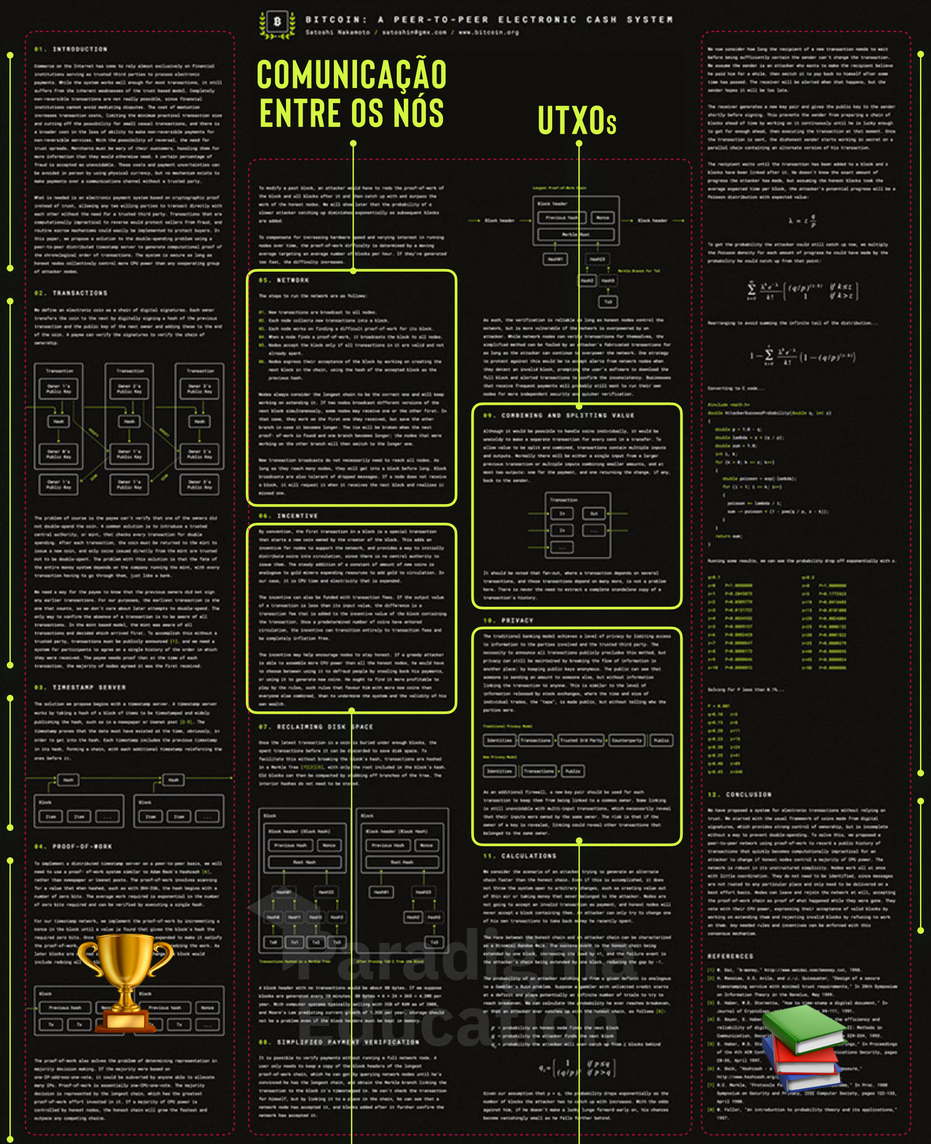
Algumas ***contas…*** *& a* ***conclusão***

INTRODUÇÃO: A INTERNET PRECISA DE UM DINHEIRO APOLÍTICO

O "ESTADO ECONÔMICO" DA REDE É DEFINIDO COMO UMA CADEIA DE ASSINATURAS CRIPTOGRÁFICAS

UMA CORRENTE IRREVERSÍVEL DE CARIMBOS TEMPORAIS (TIME-STAMPING)

O PROOF OF WORK (NISPIRADO NO HASHCASH), GARANTIA DE FINALIDADE E O AJUSTE DE DIFICULDADE



COMUNICAÇÃO ENTRE OS NÓS

UTXOs

DEFININDO INCENTIVOS (RECOMPENSAS POR BLOCO)

PRIVACIDADE VS. ANONIMIDADE

MEDINDO VETORES DE ATAQUE E CALCULANDO A SEGURANÇA DA REDE

CONCLUSÃO: "A REDE É ROBUSTA NA SUA SIMPLICIDADE"