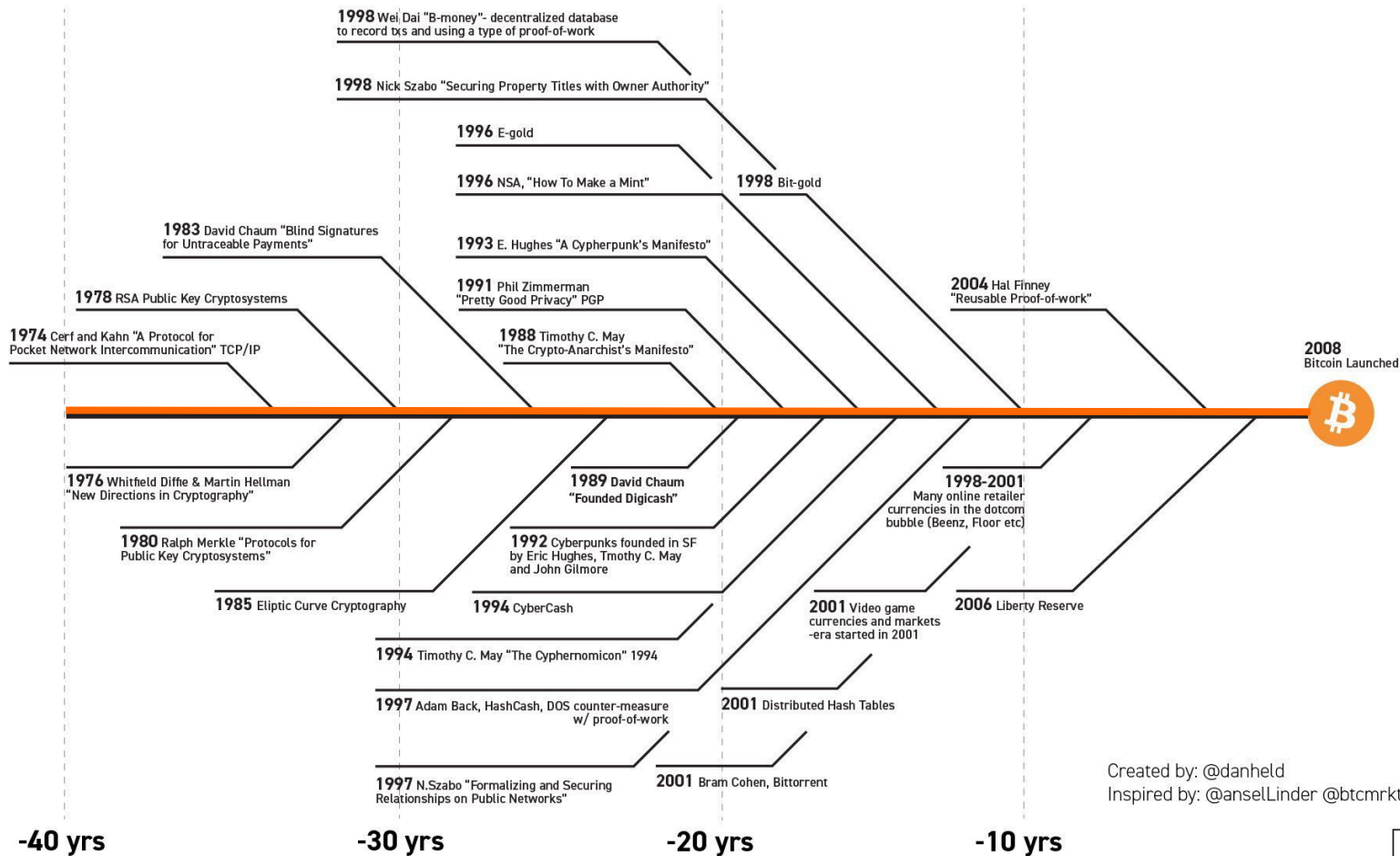


BITCOIN: DINHEIRO DIGITAL SEM BANCOS E SEM GOVERNOS





Created by: @danheld
Inspired by: @ansellinder @btcmrkt



O EMAIL QUE MUDOU O MUNDO

Bitcoin P2P e-cash paper

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@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.



Bitcoin4all

A bronze statue of a hooded figure, resembling the Bitcoin logo, set against a blurred background of trees and a clear sky. The statue is highly reflective, showing highlights and shadows that emphasize its form. The hood is pulled up, covering the head, and the figure's face is smooth and featureless except for the eyes and mouth. The statue is positioned in the center of the frame, with a soft-focus background of autumn-colored trees and a clear blue sky. The lighting is bright, suggesting a sunny day, and the overall composition is centered and balanced.

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.

3. Introduction

early for implementation
a solution to the pro-

Figure 1 illustrates three scenarios of branch merging. Each scenario shows a main line and a branch. In the first scenario, a branch merges into the main line. In the second scenario, a branch merges into the main line, and a note indicates that one or the other key in that case, they work on the first one they required, but once the other branch is done it becomes larger. The one will be better when the next growth work is found. In the third scenario, a branch merges into the main line, and a note indicates that the branch becomes larger. The nodes that were working on the other

6. Incentive

The problem of access is the power can't really that any of the leaders did not underestimate the cost. A common solution is to introduce a trusted central authority, or trust, that checks every transaction for double spending. After each transaction, the cost

that is returned to the coin to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the role of the entire currency system depends on the computer running the mint, with every

A transaction having to go through them, just like a bank. We need a way for the pages to know that the previous owners did not sign any earlier transactions, for our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to

completely inflation bias. The incentive may help encourage nodes to stay honest if a greedy miner is able to ascertain more (1%) profits than all the honest nodes, he would have to choose between going it to defend against his rivals, back to his neighbors, or join a

publicly announced [10], and we used a system for participants to agree on a single history of the game in which they were involved. The payoffs were paid out at the time of each transaction; the value of the payoff agreed to was the final amount.

3. Timestamp

Every file's information is processed begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and sends out the hash back out to be timestamped.

to extract the data without printing the tree, then use `to` as a replacement for `dump` (see [14]). The binary format that the data must have entered at the time, ultimately, in order to get into the heap. Each chunky includes the previous chunky in its tail, forming a chain, with each additional element, indicating

4. PROOF-OF-WORK

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [20], rather than timestamps or shared pools. The

quest of weak seedlings occurring for other that when hatched, such as with 90% 10%, the hatch begins with a number of zero life. The average seeds required is exponential in the number of zero life required and can be verified by executing a single hatch. For the

8. **Simplified Payment Verification**
It is possible to verify payments without running a full network

node i can be changed without disturbing work, if new blocks are chosen after i , the work to change the block would include mining all the blocks after i .

Merke doesn't bring the transaction to the block. It's timestamped in, he can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has assigned it a priority, which often is based on whether the network has accepted the sender can't change the transaction. We assume the sender is an outsider who wants to make the network believe he paid for a while, then expects it to pay back to himself after some time has passed. This creates an off-balance system that, however, is

Figure 1. The structure of the study. The diagram shows the flow of participants through the study. It starts with a box labeled 'Study Population' (N=1000). This leads to a box labeled 'Sampled Population' (N=200). From there, it splits into two paths: 'Control Group' (N=100) and 'Intervention Group' (N=100). The 'Control Group' leads to a box labeled 'Post-Intervention' (N=100). The 'Intervention Group' leads to a box labeled 'Pre-Intervention' (N=100), which then leads to a box labeled 'Post-Intervention' (N=100). The 'Post-Intervention' boxes for both groups lead to a final box labeled 'Analysis' (N=200).

The diagram illustrates the process of a transaction being included in a block. A box on the left labeled 'Transaction' has an arrow pointing to a box on the right labeled 'Block'. Inside the 'Block' box, there is a list of transactions, and the specific transaction from the 'Transaction' box is highlighted within this list.

By such, the verification is reliable as long as human studies control

To get the probability the attacker could off catch on time,

evaluating the program directly for each amount of progress he or she has made by the probability he could catch up from that point:

$$E\left[\frac{\partial U^i}{\partial x_i}\right] = E\left[\frac{\partial U^i}{\partial x_i} \mid \frac{\partial U^i}{\partial x_i} \geq \frac{\partial U^i}{\partial x_i}\right]$$

9. **Combining and Splitting Values**

It is possible to make a separate transaction for every cent in a transfer. To allow cents to be split and combined, transactions cannot be split into cents and subcents. Normally there will be either a single transaction from a single previous transaction or multiple back

considering another scenario, and at most two outputs (one for the payment, and one returning the change, if any, back to the sender).

Transaction

Double $g = 1.0$ (1)
 Double $\text{change} = 1 - \text{tx} / g$
 Double $\text{rate} = 1.0$
 (2), 3

$\begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array} \rightarrow \begin{array}{c} \boxed{2} \\ \boxed{1} \\ \boxed{1} \end{array} \rightarrow \begin{array}{c} \bullet \\ \bullet \\ \bullet \end{array}$

```

getenv("HOME")
sort = getenv("X") - getenv("Y", 0)
}
return sort

```

10. Privacy
The traditional banking model achieves a level of privacy by locking access to information to the parties involved and the trusted third party.

prop. The intensity is assumed to vary across publicly available
 this method, but privacy can still be maintained by breaking the
 flow of information in another place by keeping public steps
 anonymous. The public can see that someone is sending an amount

to someone else, but without information leaving the transaction to anyone. This is similar to the kind of information released by stock exchanges, where the time and size of individual trades, the "logs", is made public, but without telling who the parties were.

```

graph LR
    Customer --> Transaction
    Transaction --> TransactionFee[Transaction Fee]
    TransactionFee --> Merchant
    Merchant --> Bank
  
```

In an additional thread, a new key pair should be used for each

becomes computationally impractical to go through to change based rules control a majority of the games. The network robust to be structurally simplicity. Nodes work at all area with little contribution. They do not need to be identified.

11. Calculations

accomplished, it does not show the system open to arbitrary changes, such as creating what out of this or by taking money that never belonged to the attacker. Nodes are not going to accept or build transaction as evidence, and honest nodes will never accept

References

[2] M. Minster, R.S. Wolfe, and J.-J. Quesada, "Design of a very large space structure with internal joint requirements," in 28th Symposium on Astronautical Sciences in the Americas, May 1990.

[3] S. Yoder, W.J. Sawada, "How is free-form a design?"

document," in *Journal of Cryptology*, vol. 3, no. 3, pages 59-71 (1990).

p = probability an honest node finds the next block
 q = probability the attacker finds the next block
 T_0 = probability the attacker will ever catch up from n blocks behind

then we assume that $p = q$, the probability that a randomly chosen block is the attacker's is $1/2^{256}$.

(10) R. Hofen, "The introduction to probability theory and applications," 1997.

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

UNIÃO DE TECNOLOGIAS E CONCEITOS



Timestamps (timechain / blockchain)

Criptografia (SHA 256)

Descentralização (redes P2P)

Prova de trabalho (PoW)

Economia (escassez + psicologia)

Open Source + Teoria dos Jogos



Bitcoin4all

Bitcoin Genesis Block

Raw Hex Version

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E;fíÝz{.²zÇ,>
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.È.Ã^ŠQ2:Ÿ,a
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_IŸŸ...¬+
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1DŸŸŸŸM.ŸŸ..
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksŸŸŸŸ..ð.
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠŸ°pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0..\"Ö"(à9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.aþ¶IÖ¿?Lİ8Ä
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.â.Á.þ\8M+ø..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._¬....

"Chanceler à beira do segundo resgate aos bancos"

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

504

£1.50



Eat Out from £5

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

Start collecting tokens today Pullout 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 airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens. The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets". The Times has learnt. The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury. The bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans. Whitehall sources said that ministers planned to "keep the banks on the ball" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus

on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash. Under one option, a "bad bank" would be created to dispose of bad

debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

99p

Pub chain cuts the price of a pint from £1.60 to \$100 levels Business, page 47



Michael Sheen
Frost, Nixon
and me
Magazine



Working mums
So that's how
she does it
Body&Soul



Detox in style
The best spas
on the planet
Travel



Salmon Rushdie
I Won't Marry
Again
Pages 22, 23



Giant Killing?
Guide to the FA
Cup Third Round
Sport



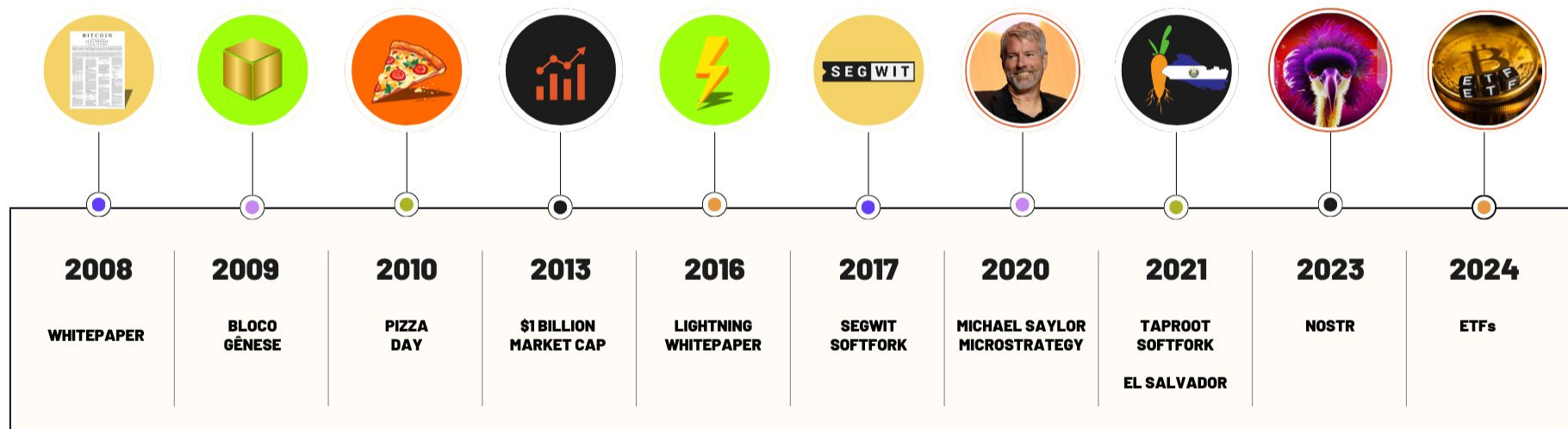
LANÇAMENTO JUSTO

- **Sem pré- mineração.**
- **Whitepaper divulgado 2 meses antes de começar a rodar a rede.**
- **Moedas sem valor por 1,5 anos e circularam livremente.**
- **Crescimento orgânico.**
- **Ao contrário de outros fundadores, Satoshi nunca vendeu.**





MARCOS NA HISTÓRIA DO BITCOIN



SILK ROAD E BITCOIN

A screenshot of the Silk Road anonymous marketplace website. The browser window shows the URL 'silkroadvb5pi3r.onion'. The page has a green header with the Silk Road logo and the text 'anonymous marketplace'. Below the header, there is a navigation bar with links for 'messages(0)', 'orders(0)', 'account(\$0.00)', 'settings', and 'log out'. A search bar and a shopping cart icon with '(0)' are also present. A large banner in the center reads '8 days 2 hrs 51 mins 31 secs until Four Twenty!!!'. On the left, there is a 'Shop by category:' list with various items and their counts. The main content area displays several product listings with images and prices. On the right, there is a 'News:' section with three bullet points.

Firefox - Welcome! | Silk Road - Welcome! | Silk Road
silkroadvb5pi3r.onion

Welcome **Cult Leader!**
messages(0) | orders(0) | account(\$0.00) | settings | log out

search | (0)

8 days 2 hrs 51 mins 31 secs until **Four Twenty!!!**

Shop by category:
Drugs(2679)
Cannabis(741)
Dissociatives(59)
Ecstasy(274)
Opioids(214)
Other(76)
Prescription(515)
Psychedelics(348)
Stimulants(256)
Apparel(22)
Books(283)
Computer equipment(13)
Digital goods(220)
Drug paraphernalia(52)
Electronics(19)
Fireworks(1)
Forgeries(41)
Hardware(3)
Home & Garden(5)
Jewelry(1)

CRANBERRY KUSH & STRAWBERRY...
\$36.82

10pc of Genuine Fake Blu Ray Discs
\$49.50

30mg Oxycodone (Roxie, Roxy) IR...
\$250.00

BITCOINS - NOW THE LOWEST PRICE...
\$0.00

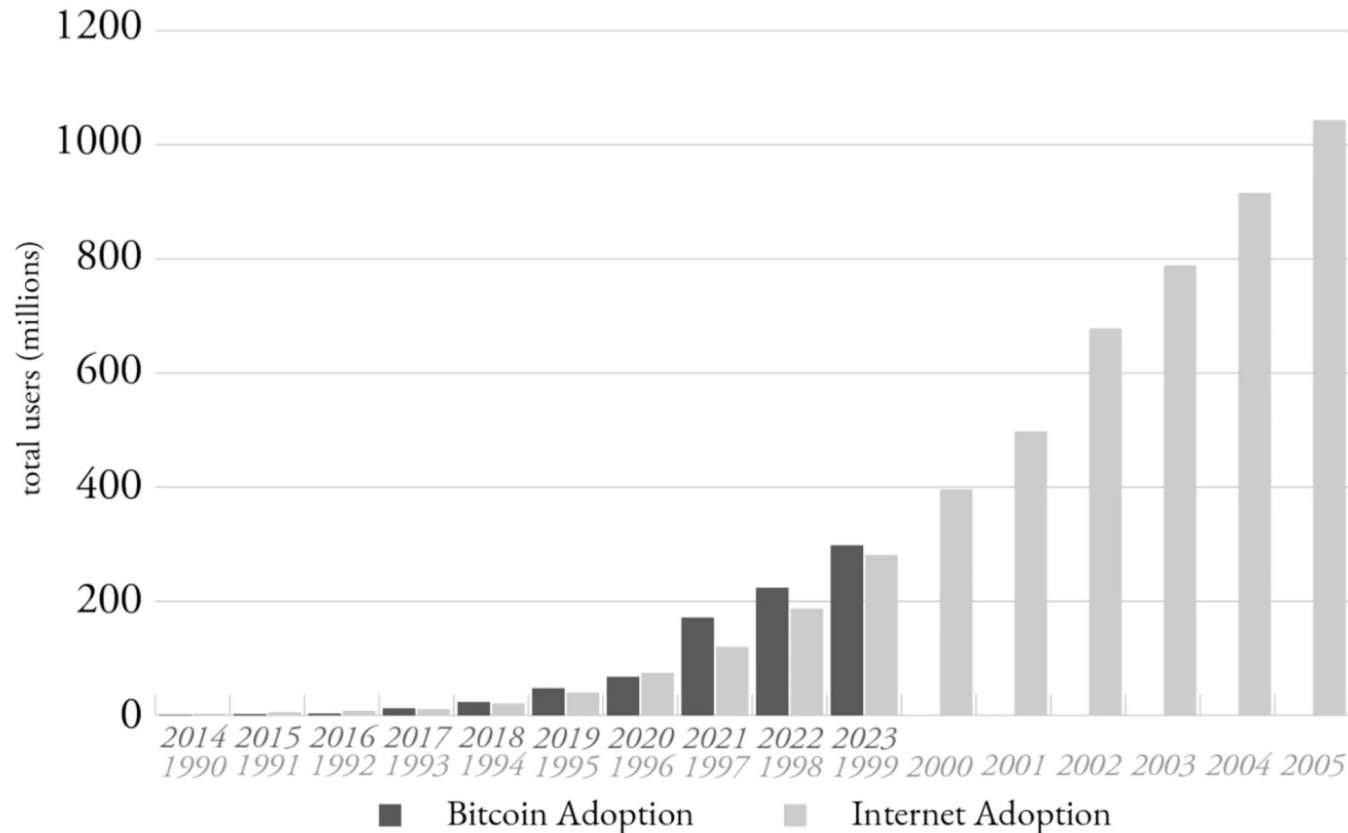
Diazepam (valium) 10mg - 1000...
\$425.50

Anarcho47's Magikally Epic...
\$2.48

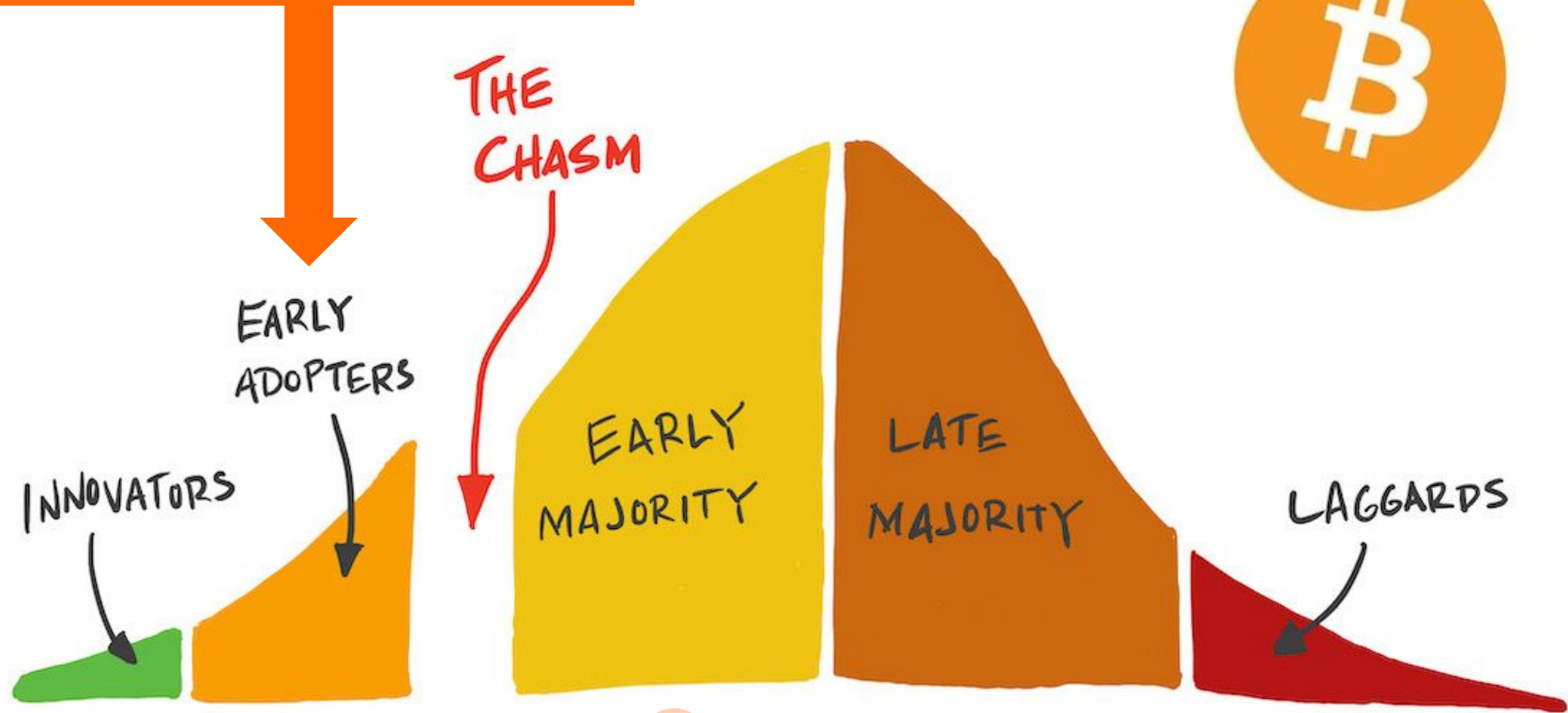
News:

- Who's your **favorite?**
- Acknowledging **Heroes**
- A new anonymous market **The Armory!**
- **State of the Road Address**

ADOÇÃO DO BITCOIN x ADOÇÃO DA INTERNET



ESTAMOS AQUI



Bitcoin4all

Bitcoin:
\$2T

Total global asset value:
\$900T

Gold:
\$16T

Art:
\$18T

**Cars,
collec-
tibles:**
\$6T

Equities:
\$115T

@Croesus_BTC

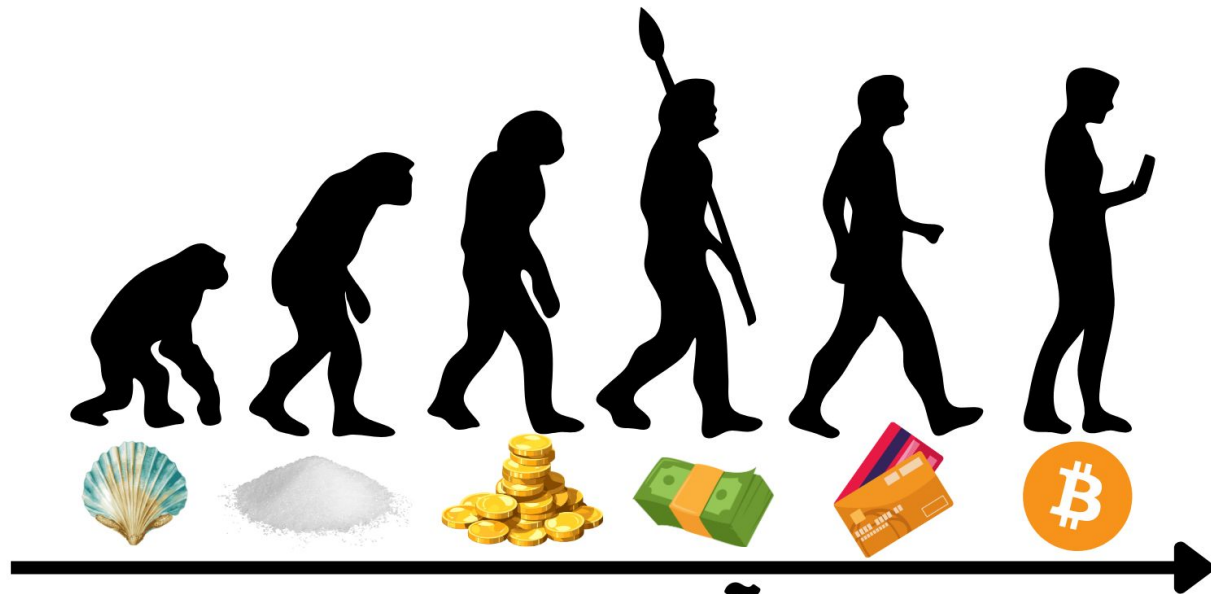
Real estate:
\$330T

Bonds:
\$300T

Money:
\$120T

BITCOIN:UM DINHEIRO MELHOR





A EVOLUÇÃO DO DINHEIRO



Bitcoin4all



**QUAL O PROBLEMA
DO DINHEIRO?**