

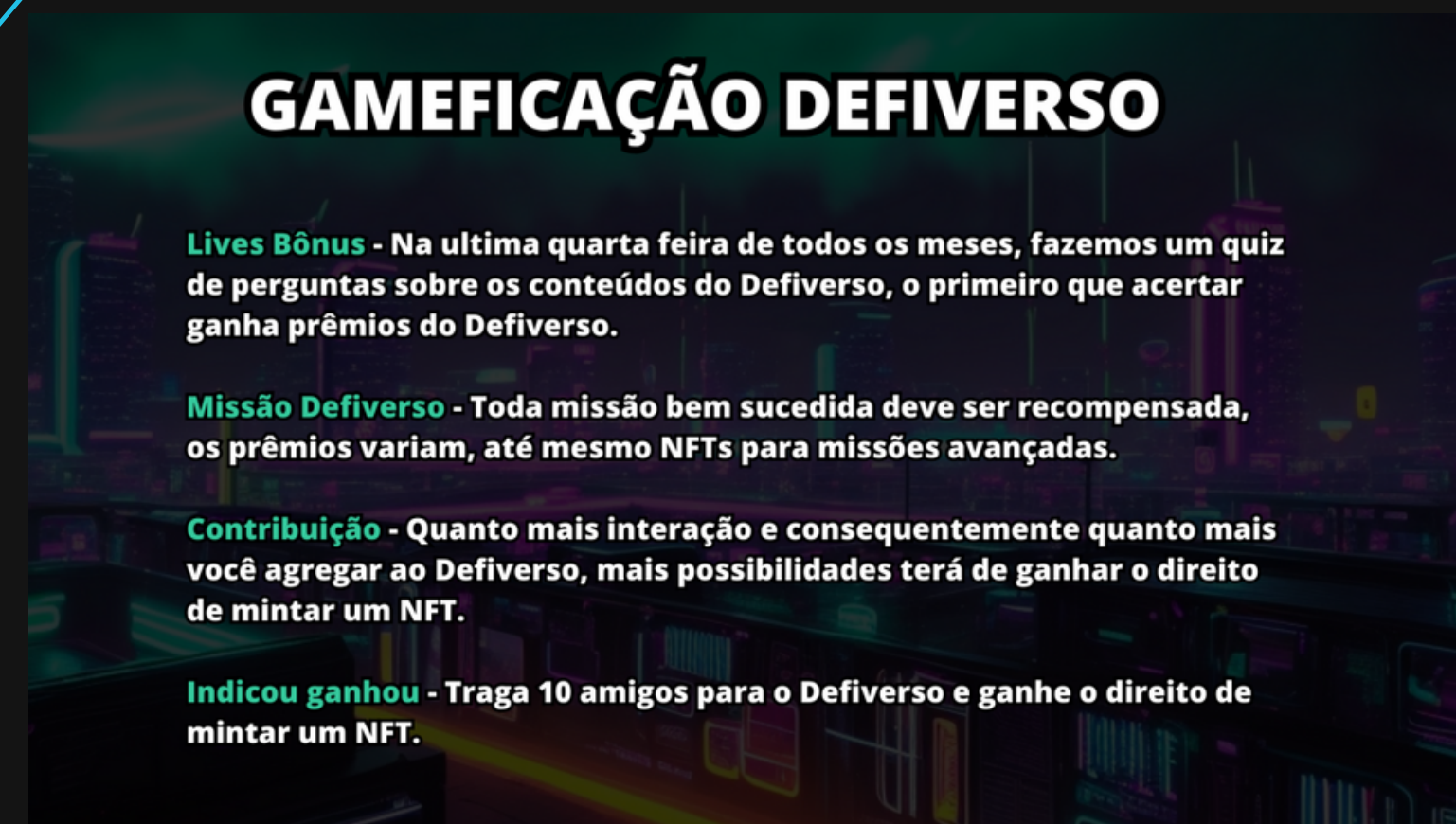
Defiverso

Aqui começa a sua jornada

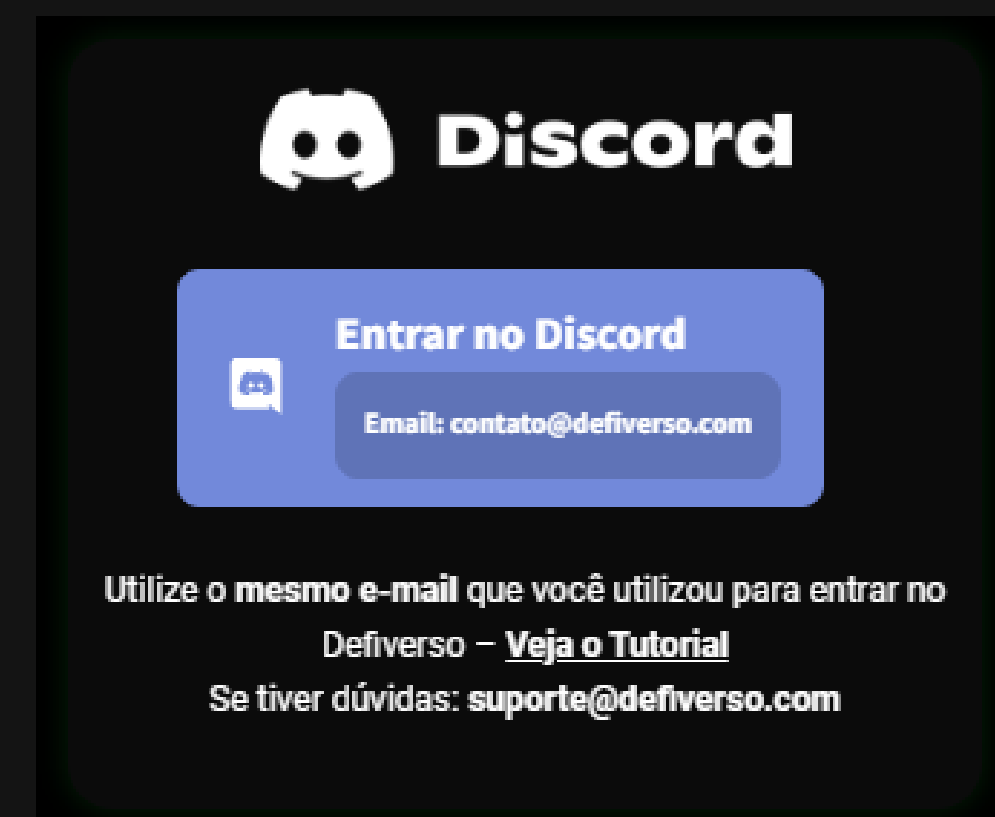




Saudações



- Entre no Discord, com mesmo e-mail utilizado no Defiverso



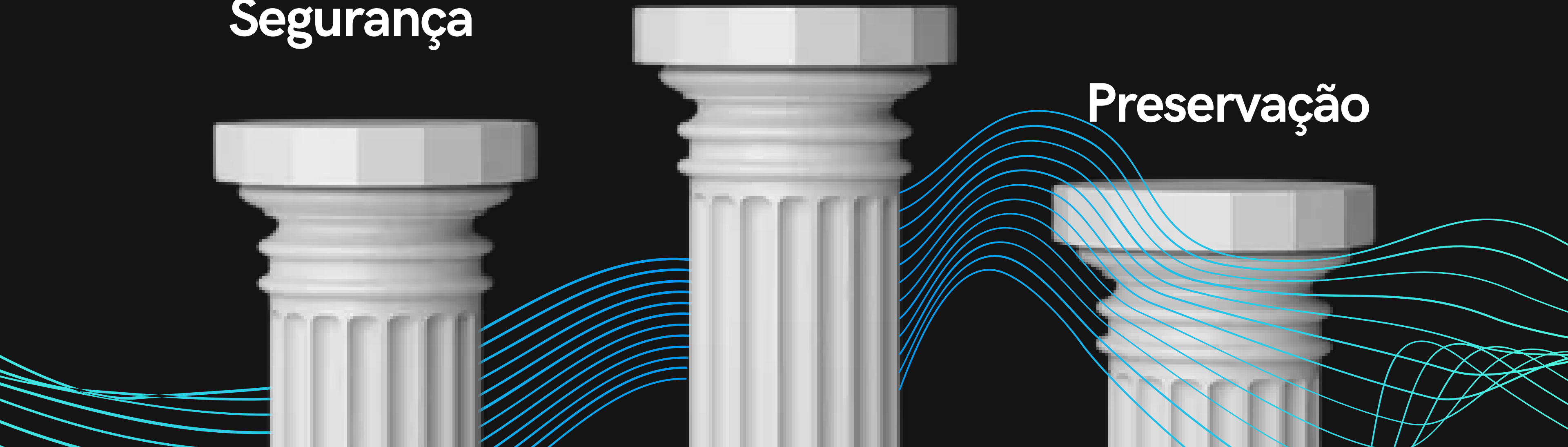
Tutorial do Discord em vídeo na aba de "suporte"

Os 3 Pilares

Ganhar dinheiro

Segurança

Preservação



12 Módulos

É uma jornada que deve ser desfrutada



Filosofia Defiverso



O Dinheiro

Tão antigo, quanto a civilização





- **Unidade de conta**
- **Meio de troca**
- **Reserva de valor**

Mercadoria



- Unidade de conta em um lugar
- Meio de troca
- Reserva de valor

Mercadoria



- Unidade de conta em um lugar
- Meio de troca
- Reserva de valor

Não durável

Metais preciosos



- Unidade de conta em um lugar
- Meio de troca
- Reserva de valor

Metais preciosos



- Unidade de conta em um lugar
 - Meio de troca
 - Reserva de valor
-
- Troco miúdo
 - Grandes volumes
 - Falsificação

Papel moeda



Moeda Fiduciária



- Unidade de conta em um lugar
- Meio de troca
- Reserva de valor

Moeda Fiduciária



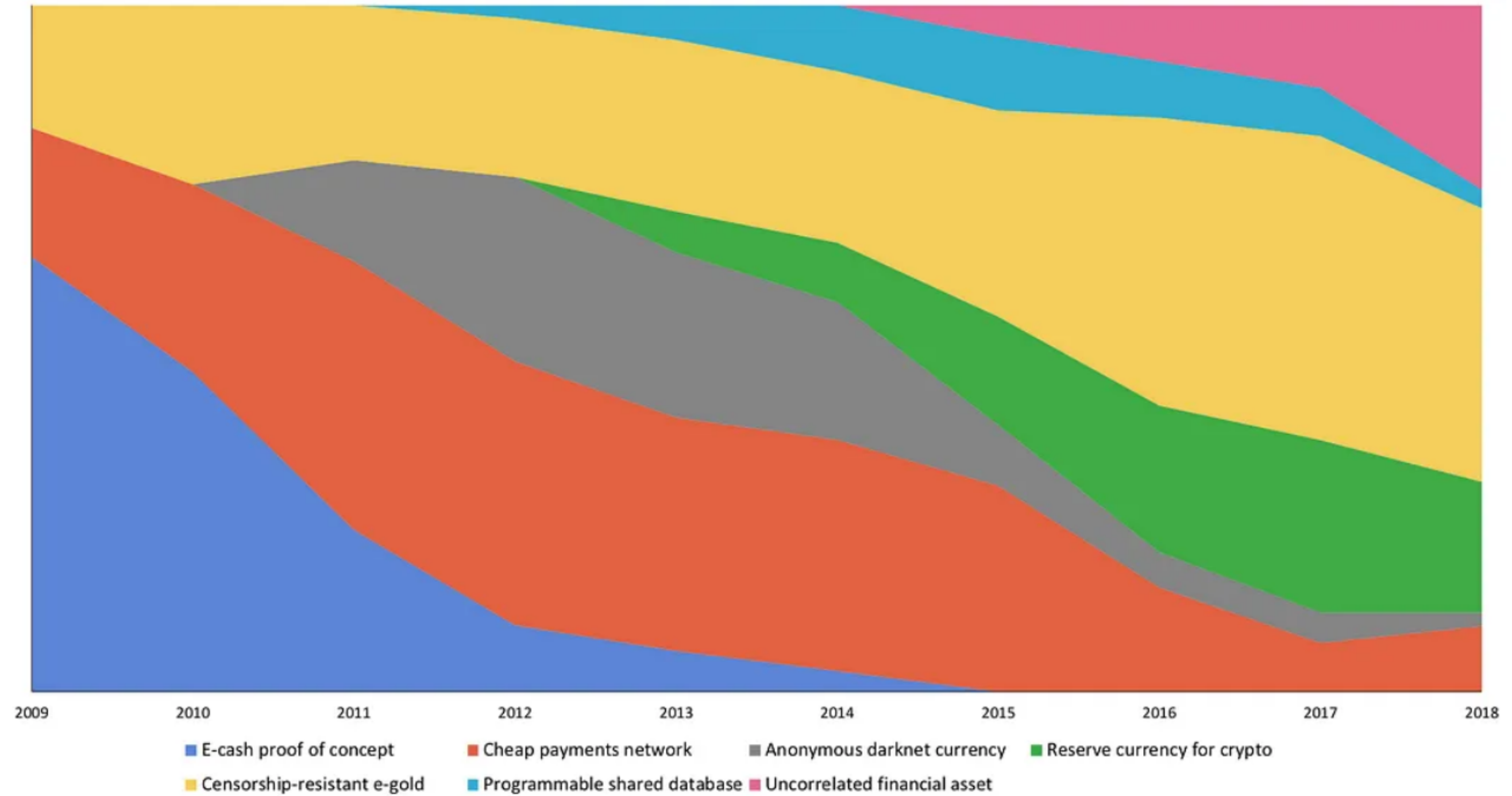
- Unidade de conta em um lugar
- Meio de troca
- Reserva de valor
- Não tem mais escassez

BITCOIN

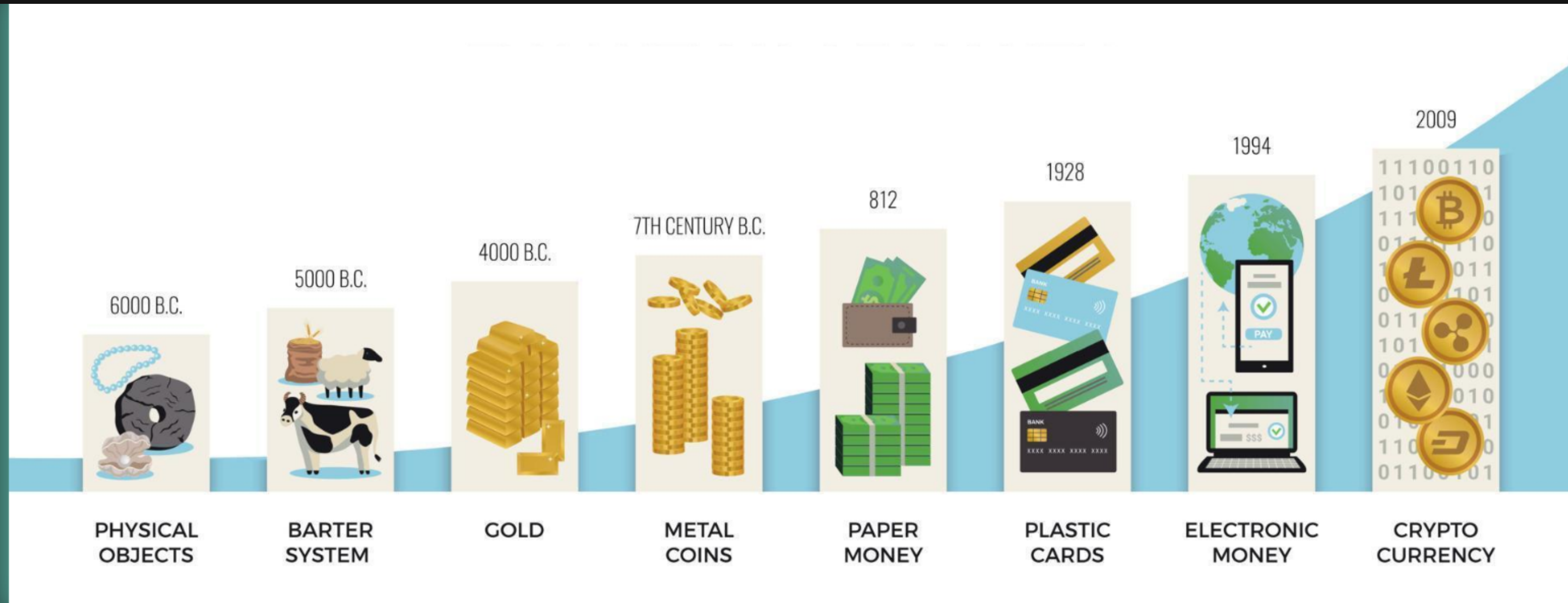


- **Unidade de conta em um lugar**
- **Meio de troca**
- **Reserva de valor**
- **Troco miúdo**
- **Grandes volumes**
- **Falsificação**
- **Não tem mais escassez**

Narrativas Bitcoin



Evolução do Dinheiro



Nascimento do Bitcoin

Bitcoin P2P e-cash paper

James A. Donald [jamesd at echeque.com](mailto:jamesd@echeque.com)

Sun Nov 2 18:46:23 EST 2008

- Previous message: [Who cares about side-channel attacks?](#)
- Next message: [Secrets and cell phones.](#)
- Messages sorted by: [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Satoshi Nakamoto wrote:

> 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 de 2008

Bitcoin v0.1 released

Satoshi Nakamoto | Fri, 09 Jan 2009 17:05:49 -0800

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:

<http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar>

Windows only for now. Open source C++ code is included.

09 de janeiro de 2009



Running bitcoin

1:33 AM · 11 de jan de 2009

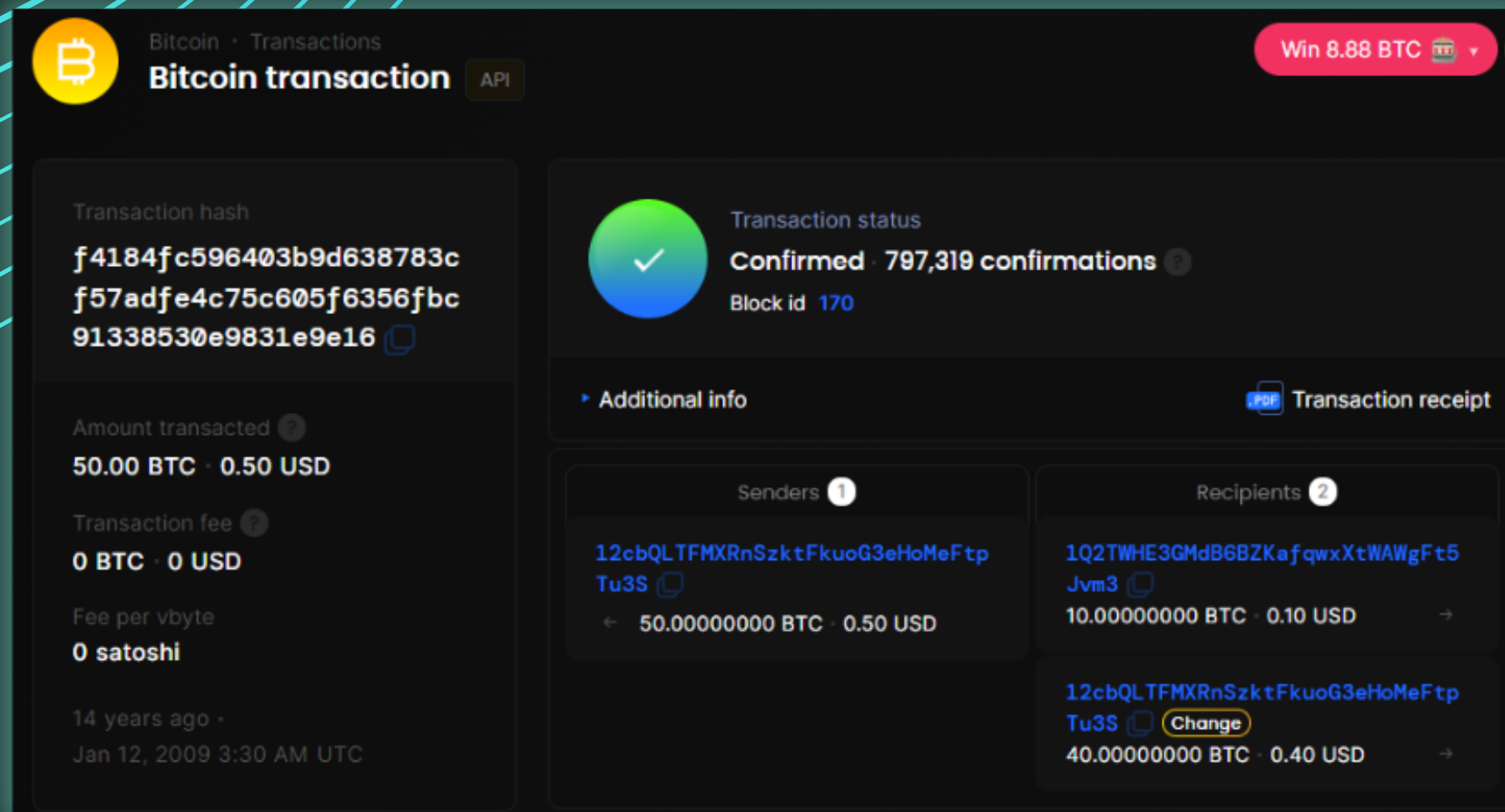
22,5 mil Retweets 7.880 Comentários 70 mil Curtidas 2.896 It



Tweetar sua resposta!

10 de janeiro de 2009

Nascimento do Bitcoin



12 janeiro de 2009



22 de maio de 2010
Lazlo Hanyecz

Nascimento do Bitcoin

Satoshi's Final Email to Gavin Andresen

April 26, 2011 to [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.

References

- [1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [2] H. Massias, X.S. Avila, e J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, Maio 1999.
- [3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, num 2, páginas 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*, páginas 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*, páginas 28-35, Abril 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, páginas 122-133, Abril 1980.
- [8] W. Feller, "An introduction to probability theory and its applications," 1957.

Criptografia

Criptografia vem das palavras gregas :

Kryptos = escondido, oculto

Graphein = Escrita

Escrita escondida – Escrita Oculta

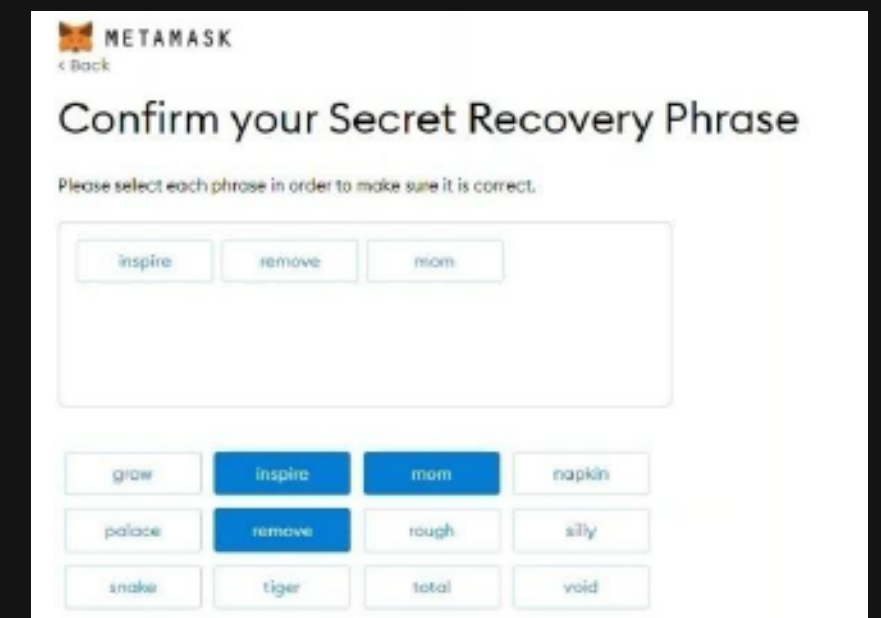
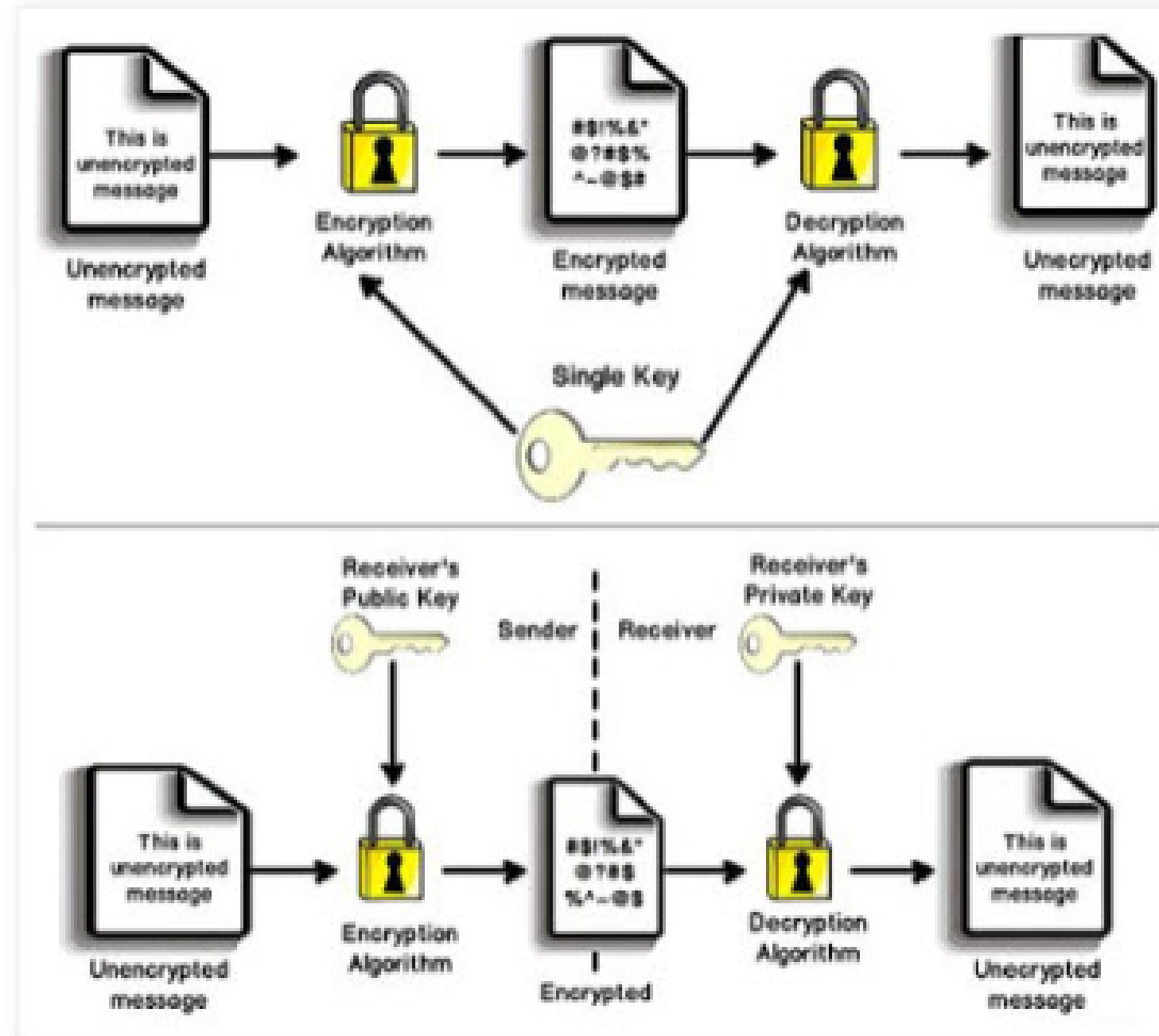


Já por volta dos anos 450 a.C., os militares gregos faziam uso do bastão de Licurgo ou Scytale.

Criptografia

Criptografia simétrica

0478d430274f8c5ec1321338151e9f



Criptografia asimétrica

Criptografia



RELATÓRIOS / O QUE É CRIPTOGRAFIA E COMO CRIPTOGRAFAR UMA MENSAGEM?

O que é Criptografia e Como Criptografar Uma Mensagem?



**" Dizer que Bitcoin é somente
dinheiro digital é como dizer que a
internet é só para envio de e-mails"**





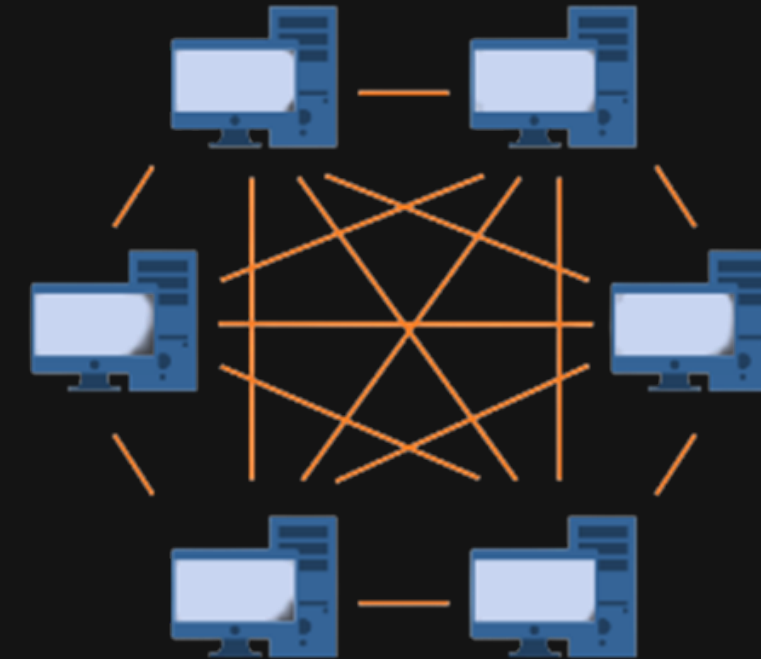
A Blockchain

Base de dados X Peer-to-Peer



Base de dados

- Centralizada
- Participante central
- Ponto de falha



P2P

- Descentralizada
- Compartilhada / Distribuída
- Vários participantes
- Segura

Rede Bitcoin e seus "Nós"

REACHABLE BITCOIN NODES

Updated: Sat Jul 8 11:32:05 2023 -03

16904 NODES

CHARTS

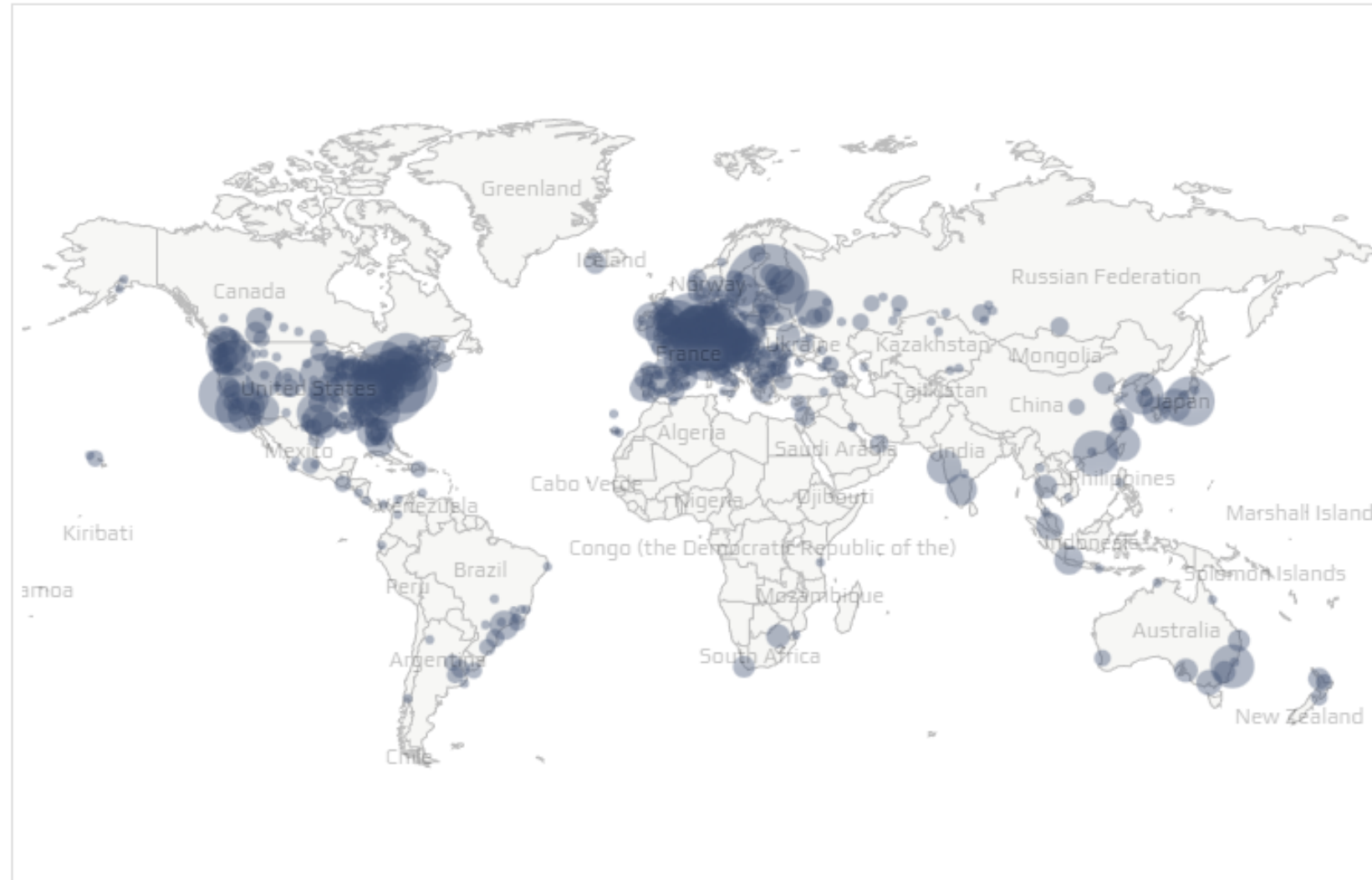
IPv4: -2.2% / IPv6: -0.8% / .onion: -0.7%

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

RANK	COUNTRY	NODES
1	n/a	10357 (61.27%)
2	United States	1662 (9.83%)
3	Germany	1371 (8.11%)
4	France	459 (2.72%)
5	Netherlands	342 (2.02%)
6	Canada	284 (1.68%)
7	Finland	255 (1.51%)
8	United Kingdom	200 (1.18%)
9	Russian Federation	170 (1.01%)
10	Switzerland	154 (0.91%)

[All \(91\) »](#)

NOTE / The data above includes reachable nodes only. [View global nodes here »](#)

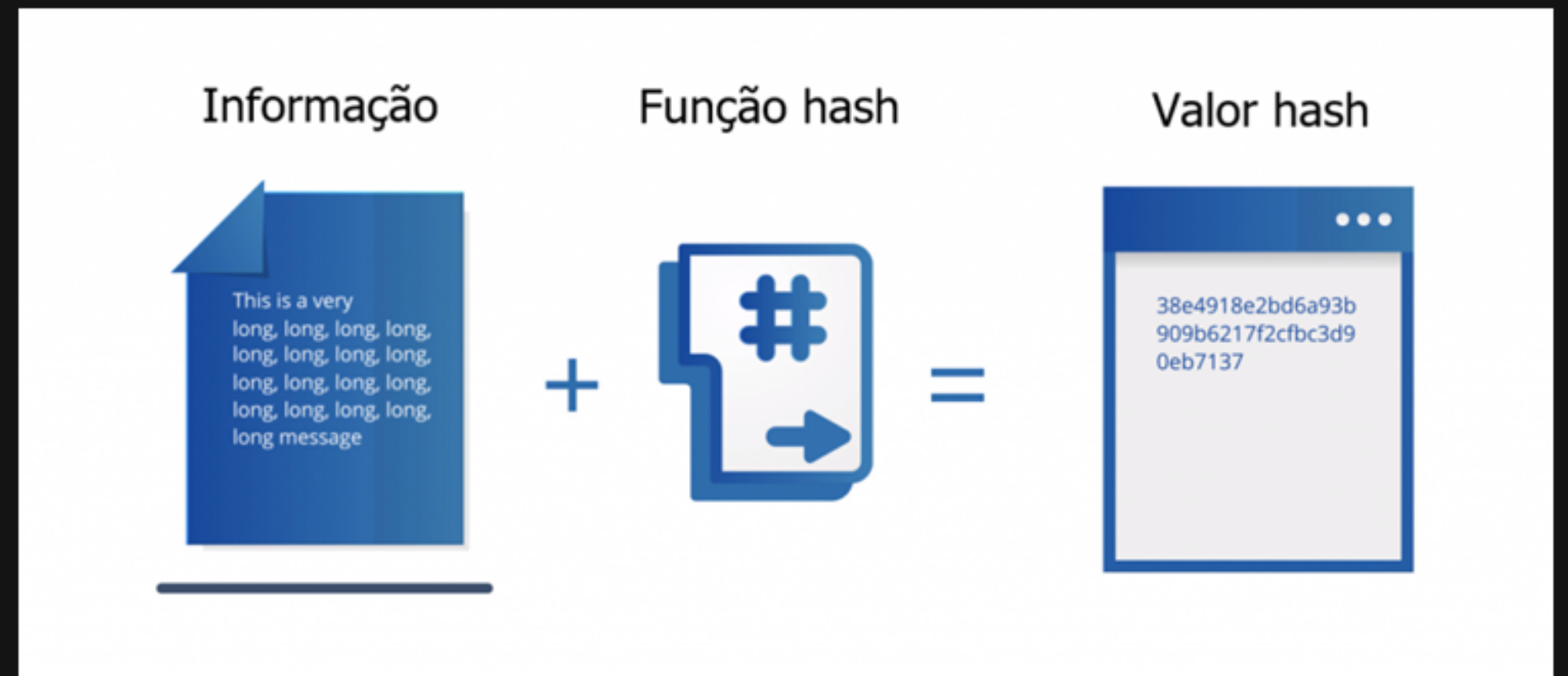


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

[LIVE MAP](#)

Função HASH

É uma função matemática que converte um arquivo de qualquer tamanho em um código de letras e números de tamanho fixo.



Blockchain

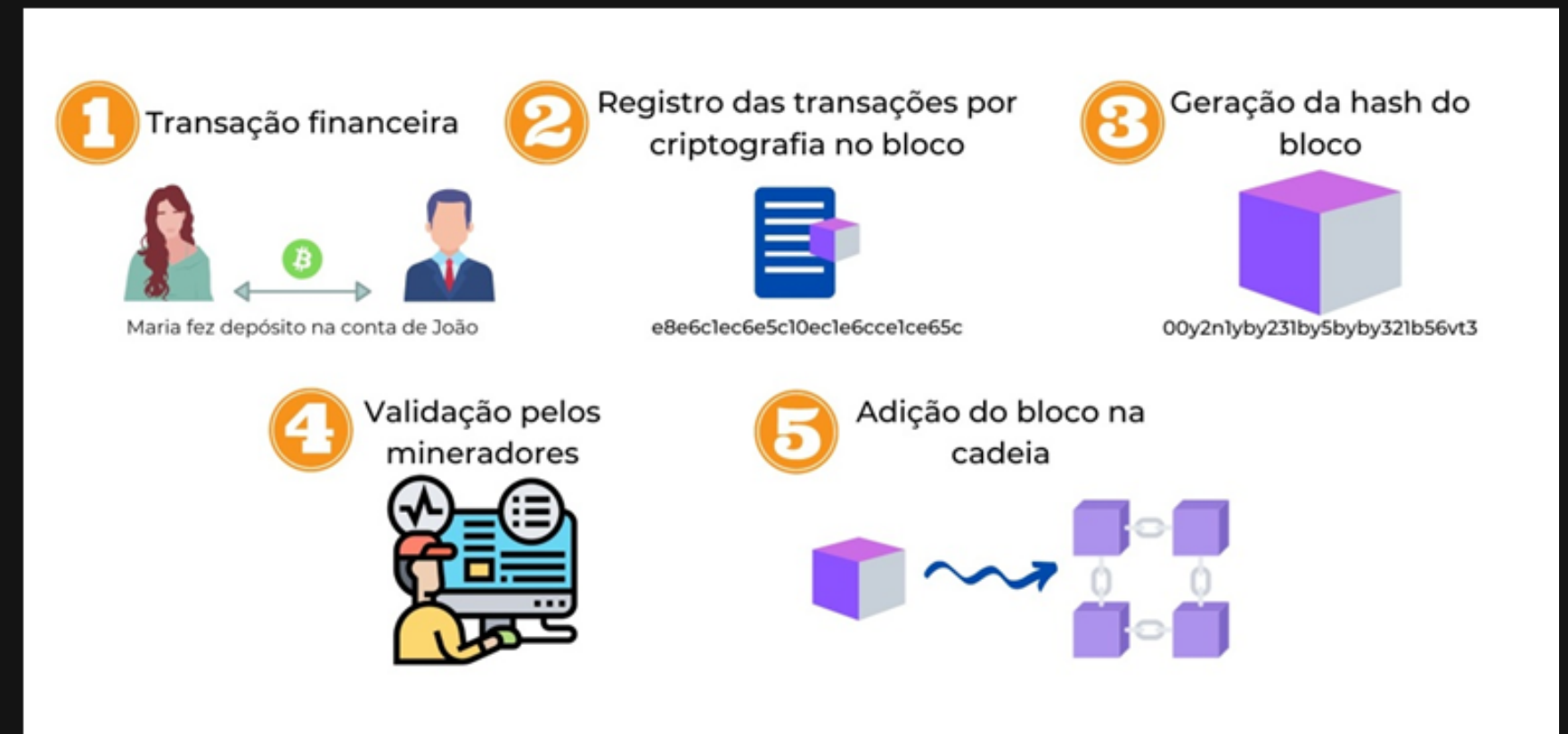
L-P-V-P

L – Livro Razão = Transações

P – Público = Compartilhado/ Distribuído

V – Verificável = Rastreável

P – À prova de adulteração = Segurança



Blockchain



Votação



Moedas digitais



Transferências e pagamentos



Cartório

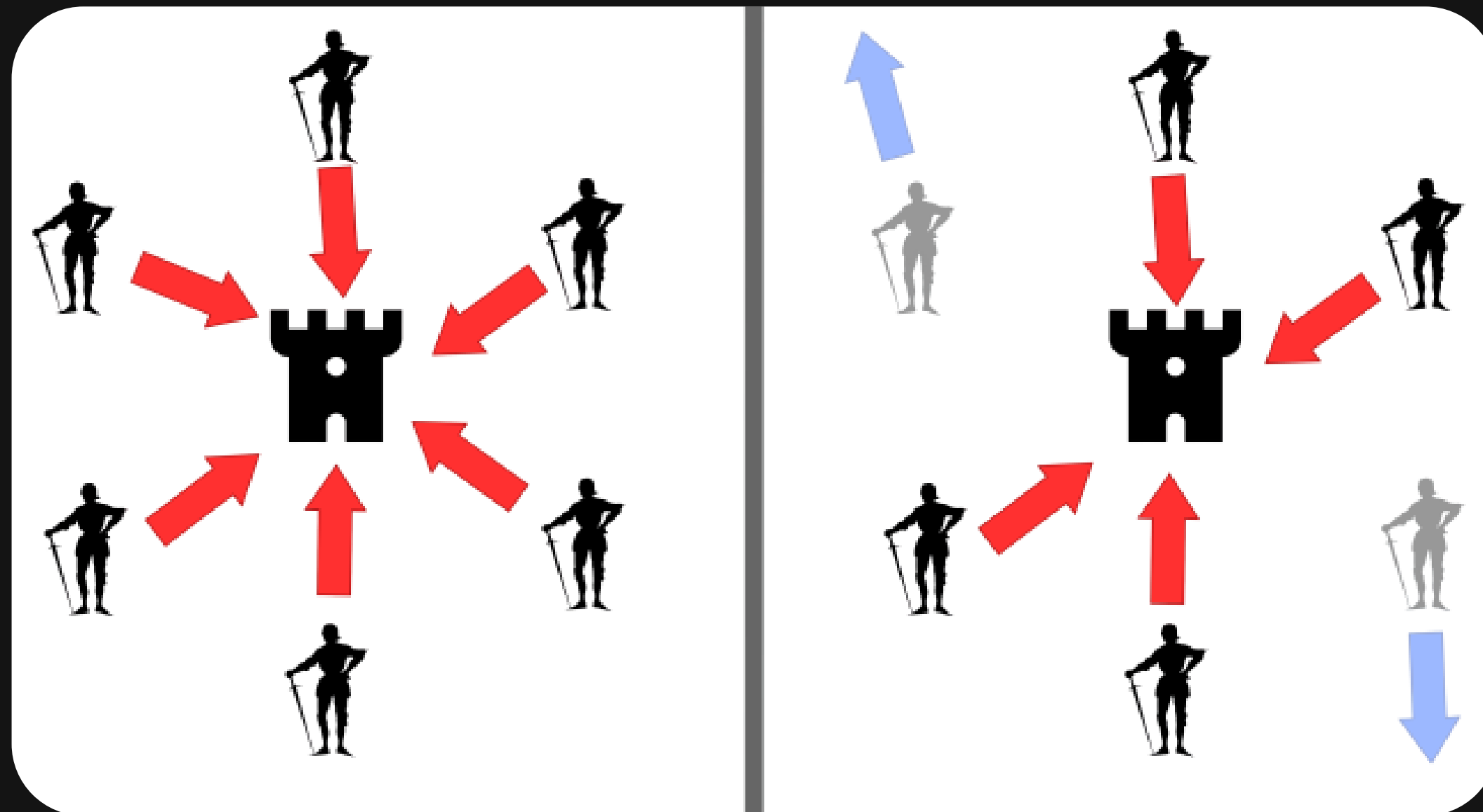


Bancos

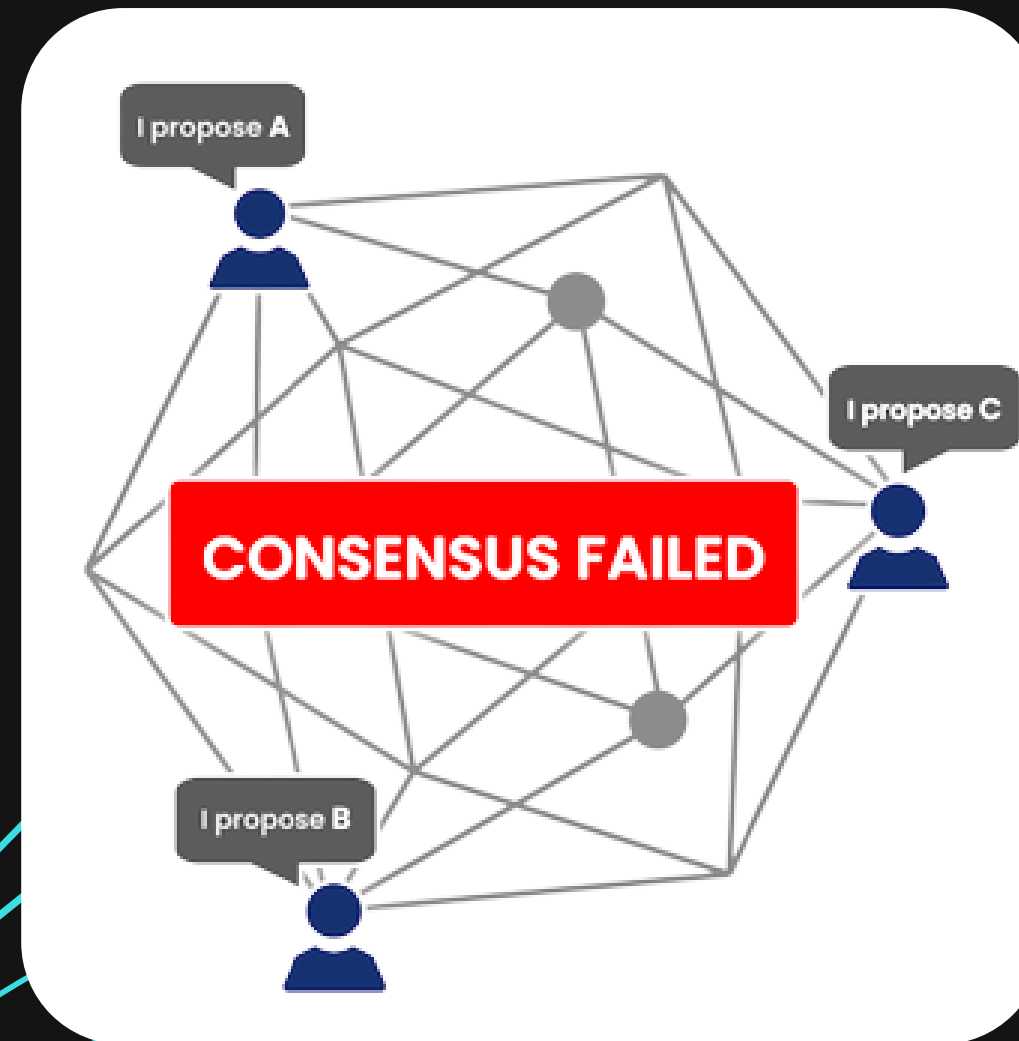


Imóveis

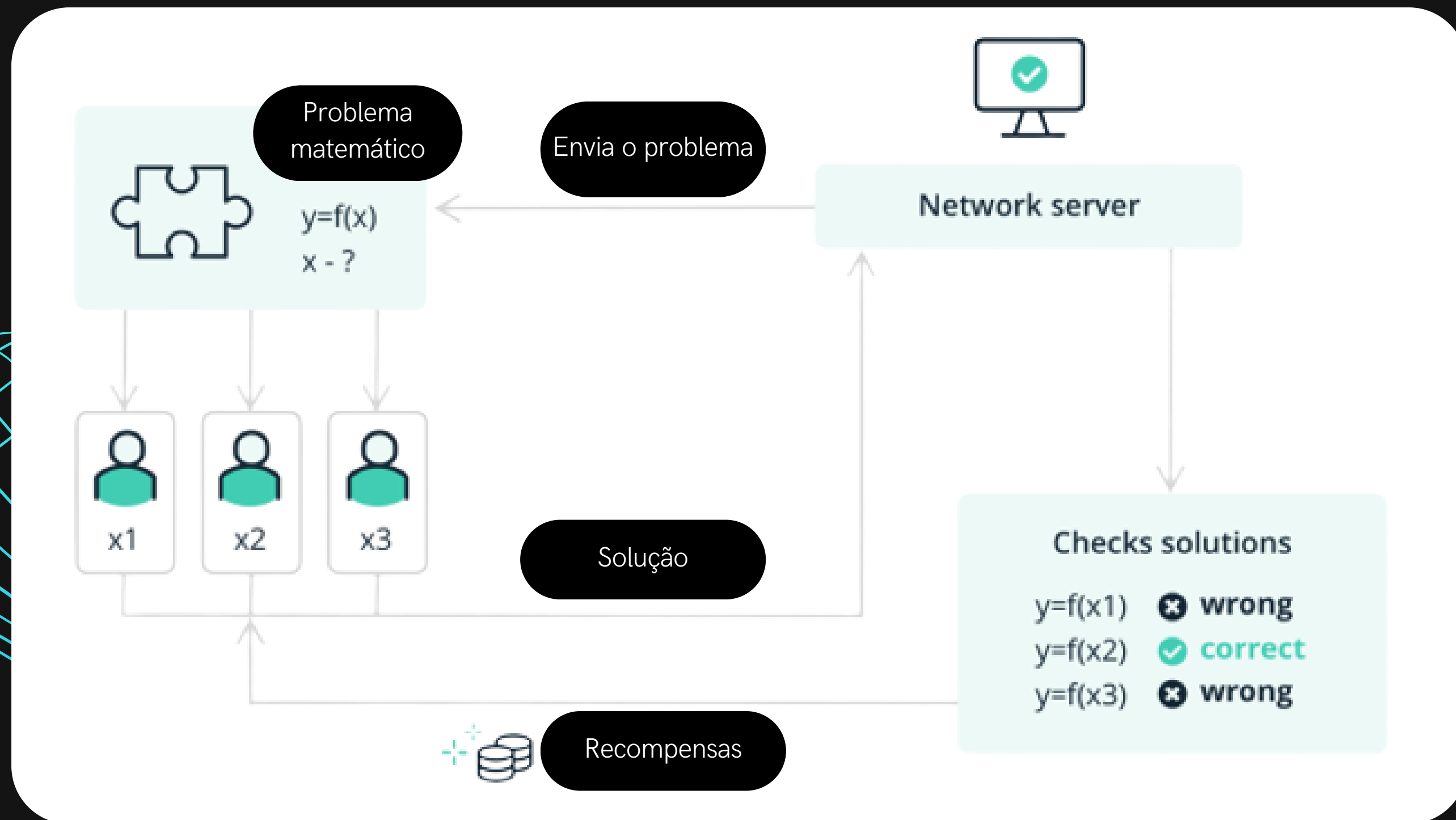
Algoritmo de Consenso



Algoritmo de Consenso



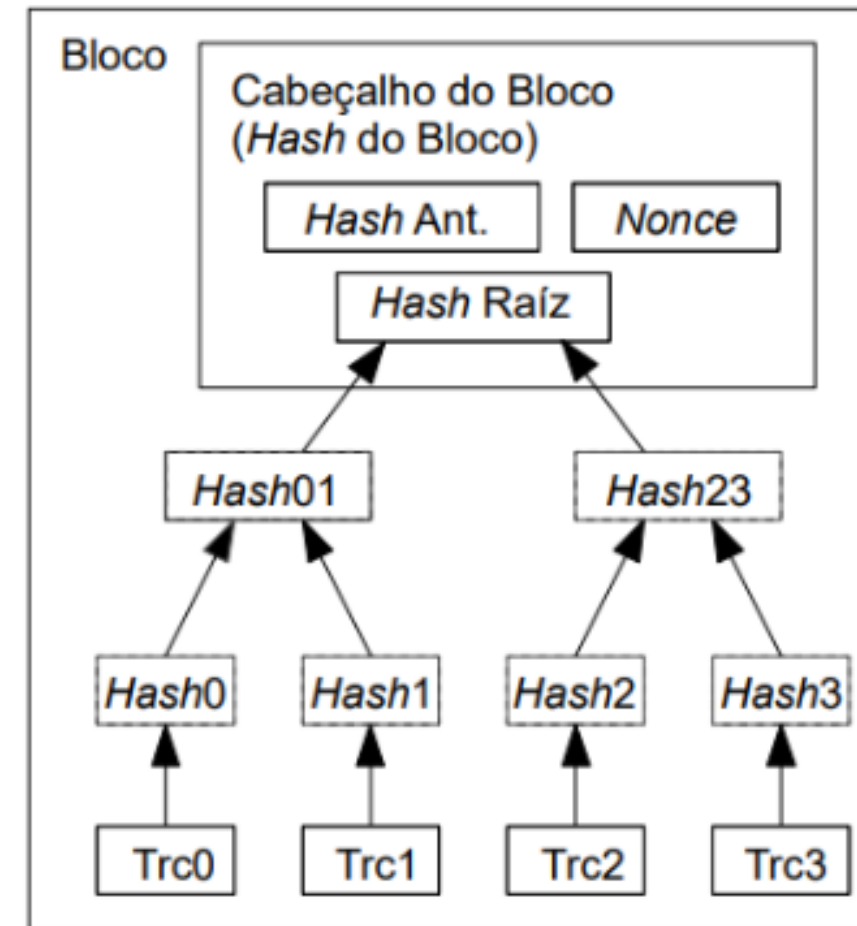
Prova de Trabalho



Prova de Trabalho

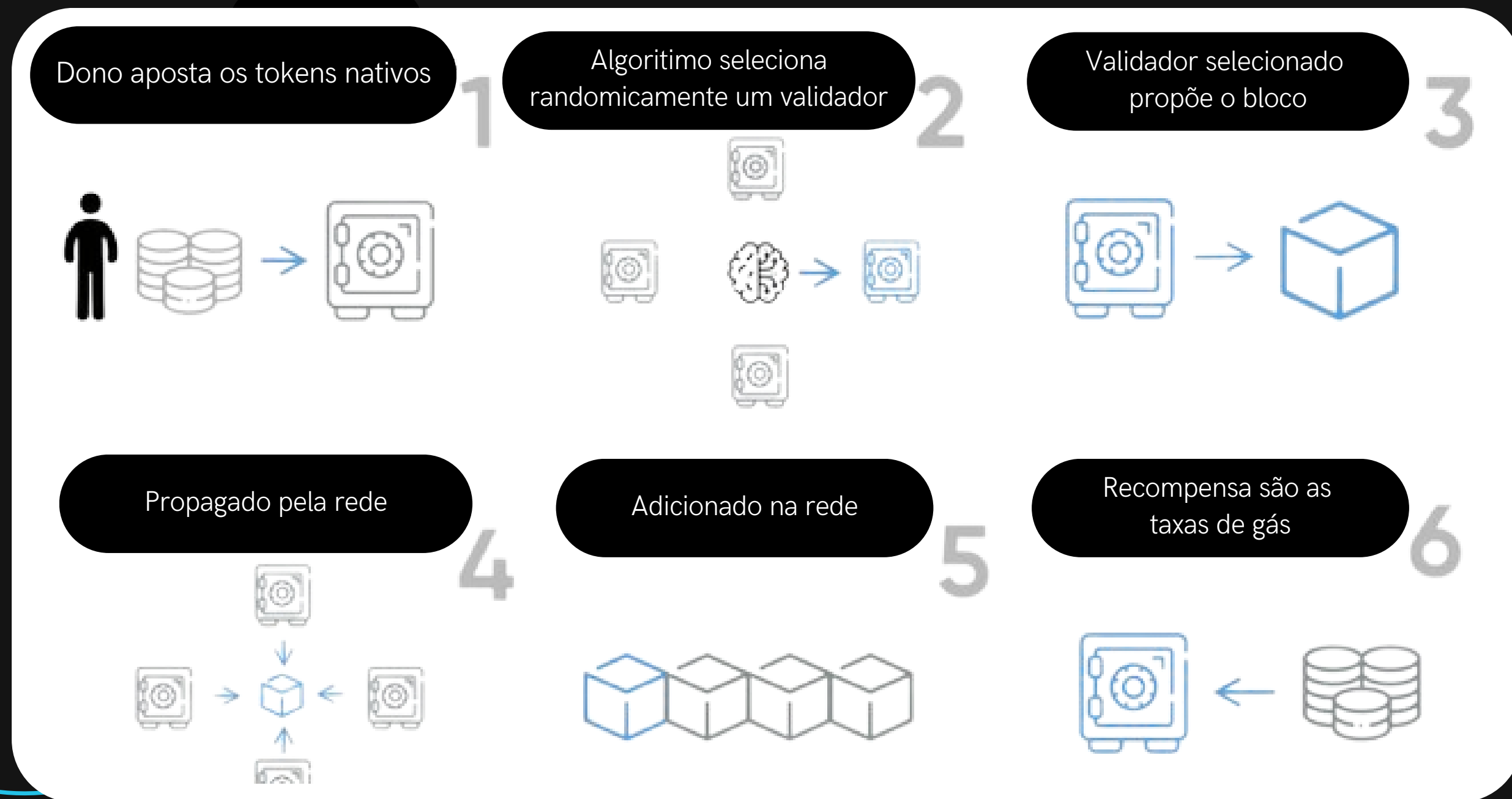


Mineração na prática

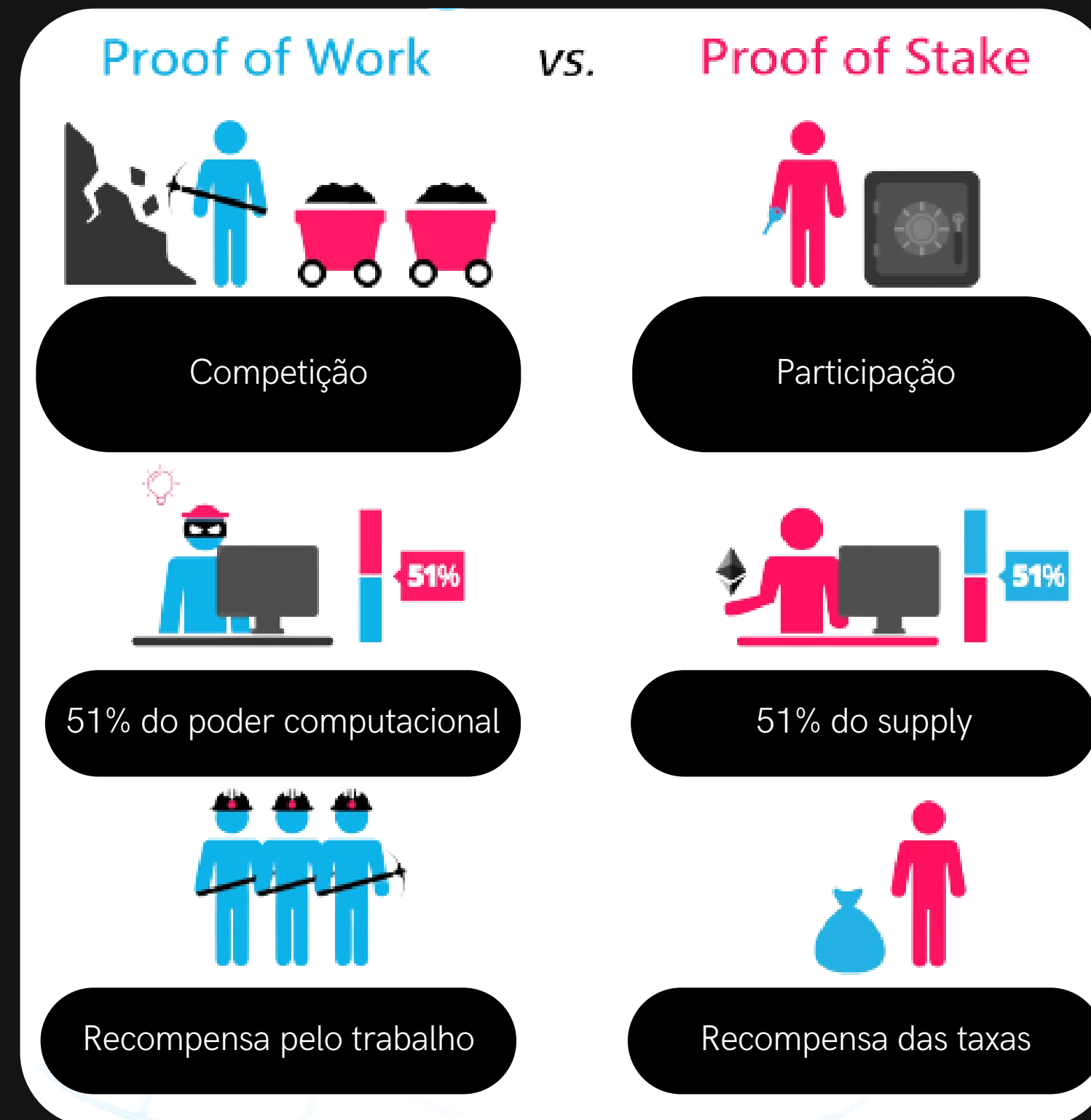


Transações *Hashed* numa árvore Merkle

Prova de Aposta



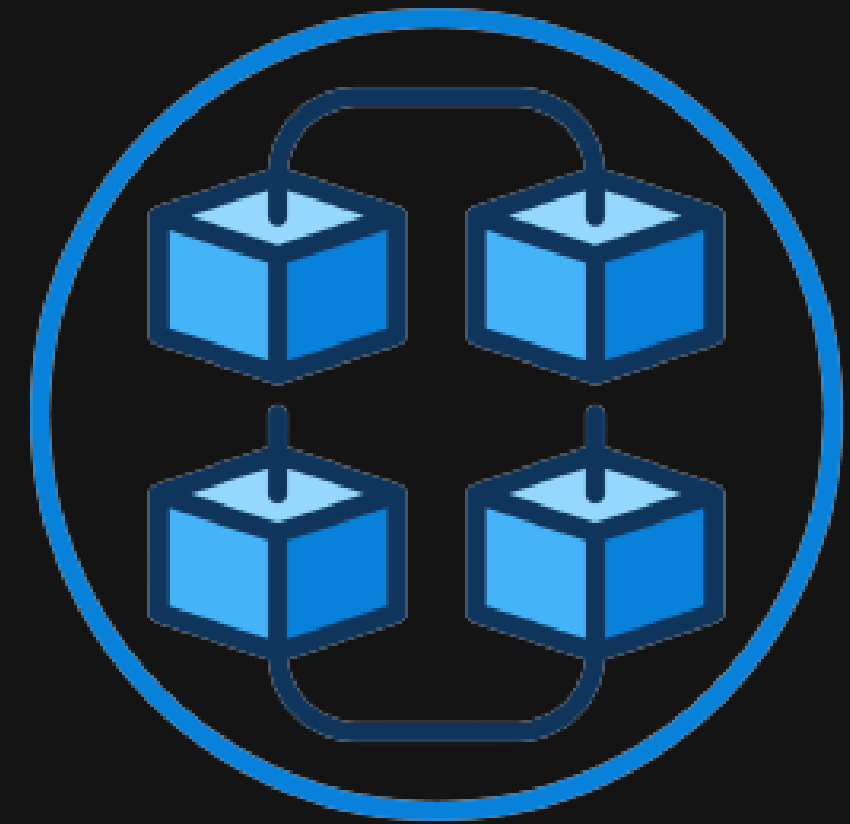
Prova de Trabalho X Prova de Aposta



As transações



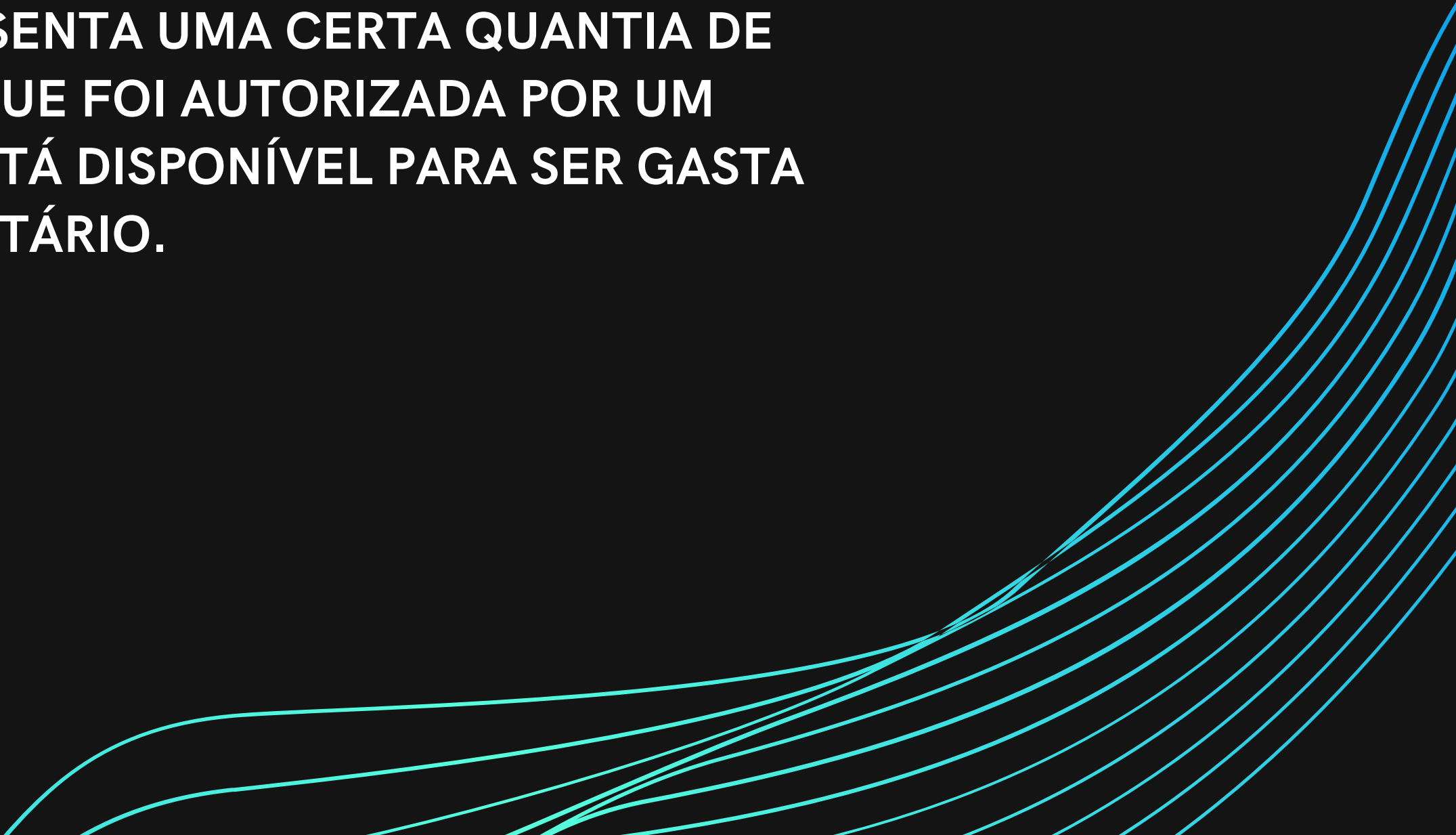
Transação



UTXO

UNSPENT TRANSACTION OUTPUT (TRANSAÇÃO DE SAÍDA NÃO GASTA)

UM **UTXO** REPRESENTA UMA CERTA QUANTIA DE CRIPTOMOEDA QUE FOI AUTORIZADA POR UM REMETENTE E ESTÁ DISPONÍVEL PARA SER GASTA POR UM DESTINATÁRIO.



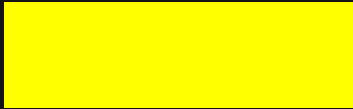
UTXO

GENESIS

	Satoshi
Bloco 1	50 BTC



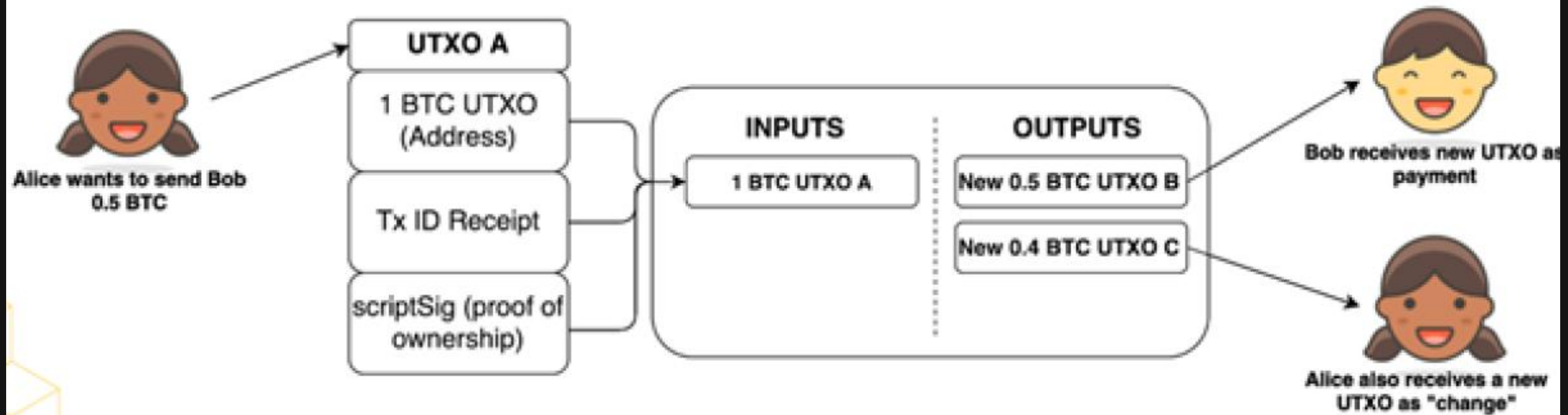
UTXO = Transacionado



UTXO = Minerado

	Satoshi	Maria	João
Bloco 1	50 BTC		
Bloco 2	50 BTC		
Bloco 3	49 BTC	1 BTC	
Bloco 4		0,5 BTC	0,5 BTC
Bloco 5			
Bloco 6			
Bloco 7			

A simplified Overview of Bitcoin UTXOs





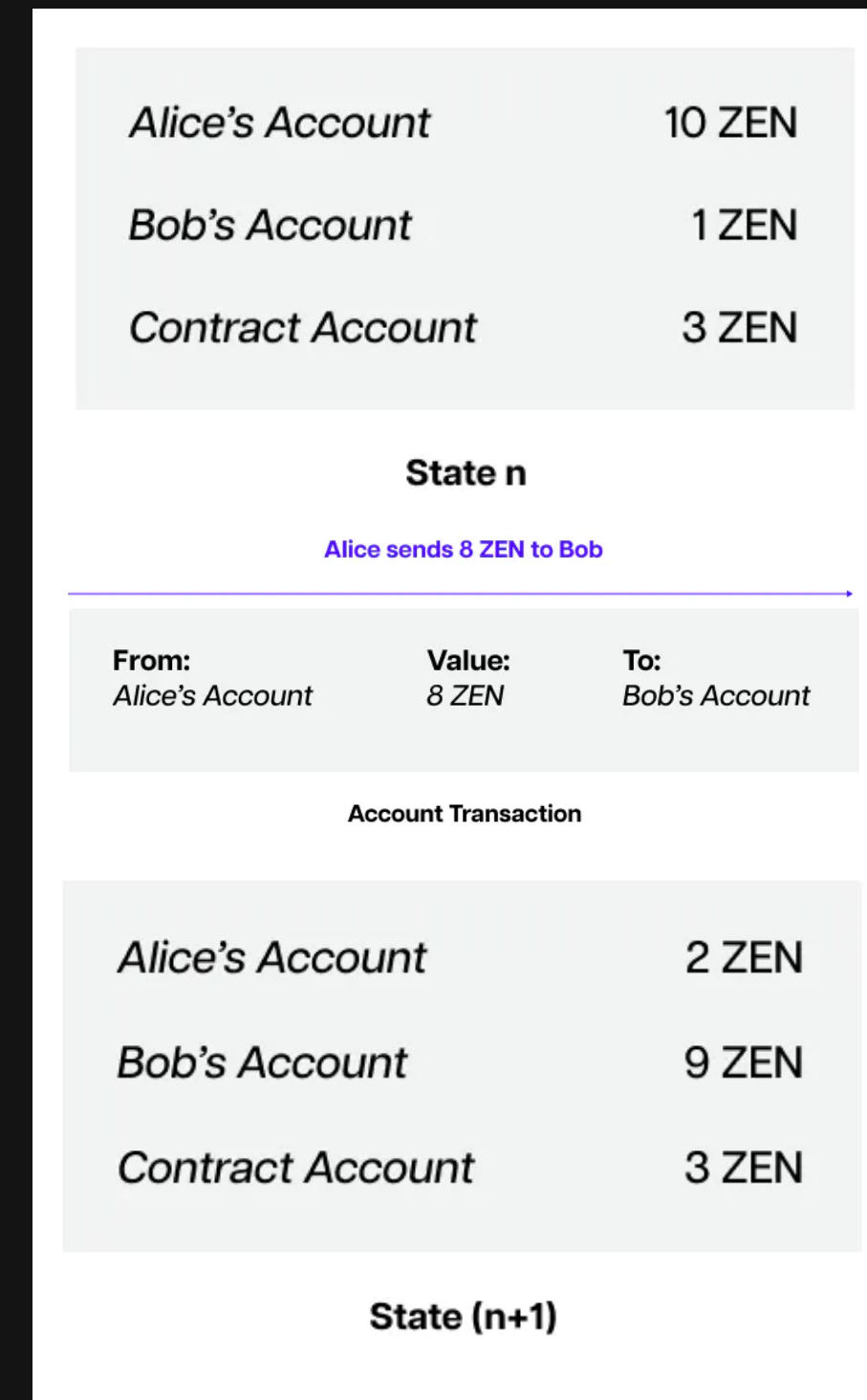
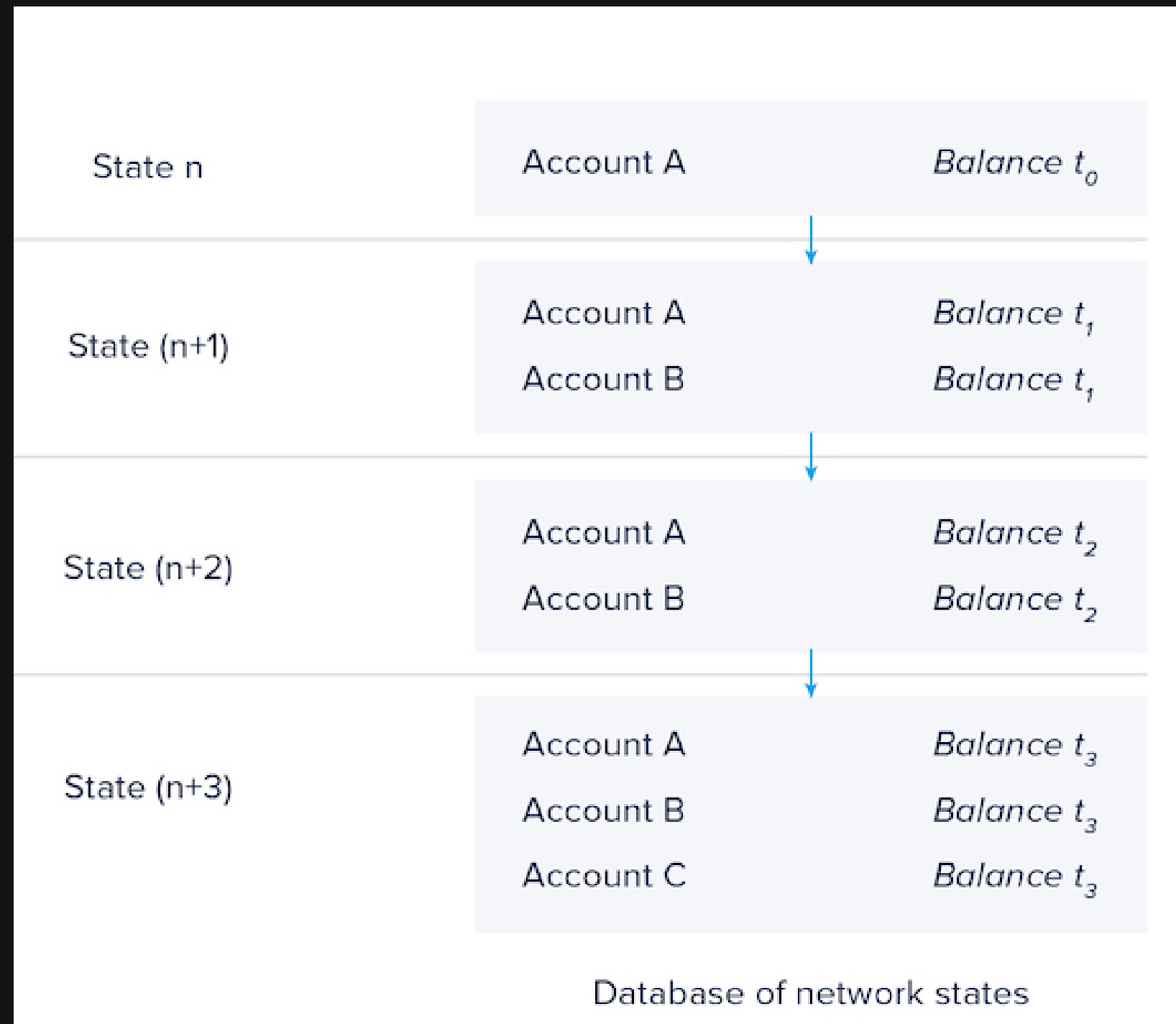
O UTXO É COMO UMA MOEDA QUE
VOCÊ AINDA NÃO USOU.

"Um valor em BTC não gasto"

1 sat = ₮ 0.000000001
10 sats = ₮ 0.00000001
100 sats = ₮ 0.0000001
1.000 sats = ₮ 0.000001
10.000 sats = ₮ 0.00001
100.000 sats = ₮ 0.0001
1.000.000 sats = ₮ 0.001
10.000.000 sats = ₮ 0.01
100.000.000 sats = ₮ 0.1
1.000.000.000 sats = ₮ 1

ACCOUNT BASED

NÃO TEM RASTREAMENTO DE MOEDAS





Leia o Whitepaper do Bitcoin



Compartilhe com 2 pessoas e
responda o formulário.



Vem pra Live na quarta - feira

MOVA-SE,