# *Sistemas Peer-to-Peer*

## *5. Bitcoin*

Francisco Sant'Anna
francisco@ime.uerj.br

# 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.

# Por quê é tão difícil criar um sistema monetário distribuído?

# Sistemas Monetários


- Uso descentralizado
- Emissão centralizada e irrestrita
- Criação difícil / Verificação fácil

```
$ cat 10-reais.txt
Cédula de 10 reais.
```

```
$ vi 10-reais-2.txt
```

```
$ gpg --sign 10-reais.txt
```

```
$ cp 10-reais.txt ...
```

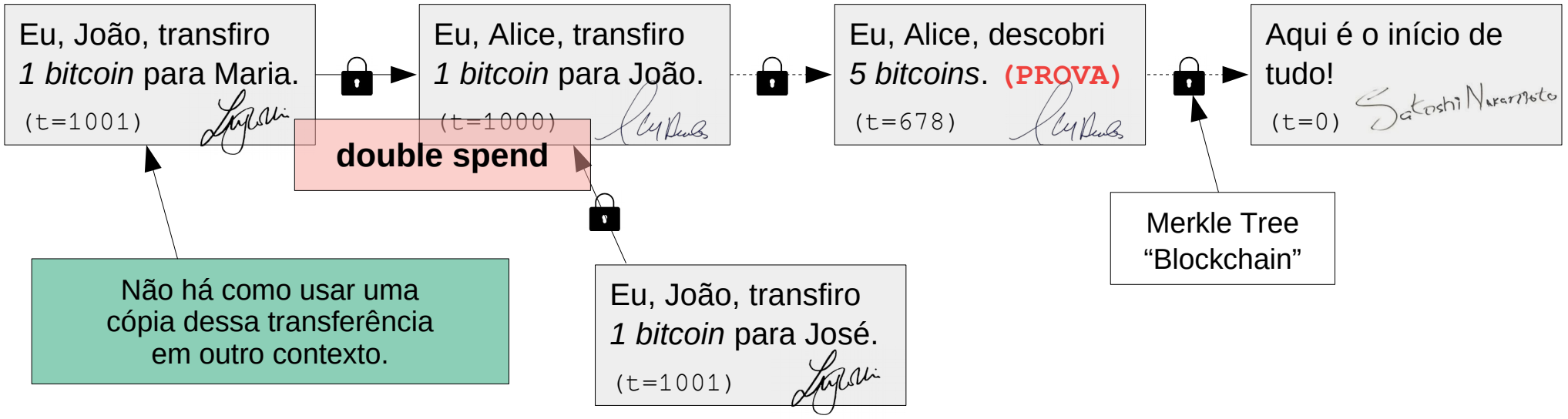
**double spend**

- Uso descentralizado
- Emissão descentralizada e restrita
- Criação difícil / Verificação fácil

**Como criar um recurso digital que seja escasso?**

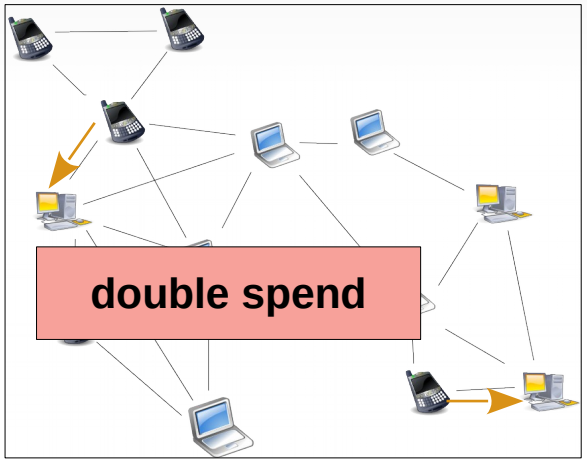
# Bitcoin

- Não há como distinguir cópias de cédulas.
- Em vez de assinar as cédulas em si, assinamos as transferências em uma linha do tempo:



# Double Spend

- O Bitcoin é uma rede P2P não estruturada.
- Não existe um estado único global.




Eu, João, transfiro *1 bitcoin* para Maria. (t=1001)

Eu, João, transfiro *1 bitcoin* para José. (t=1001)

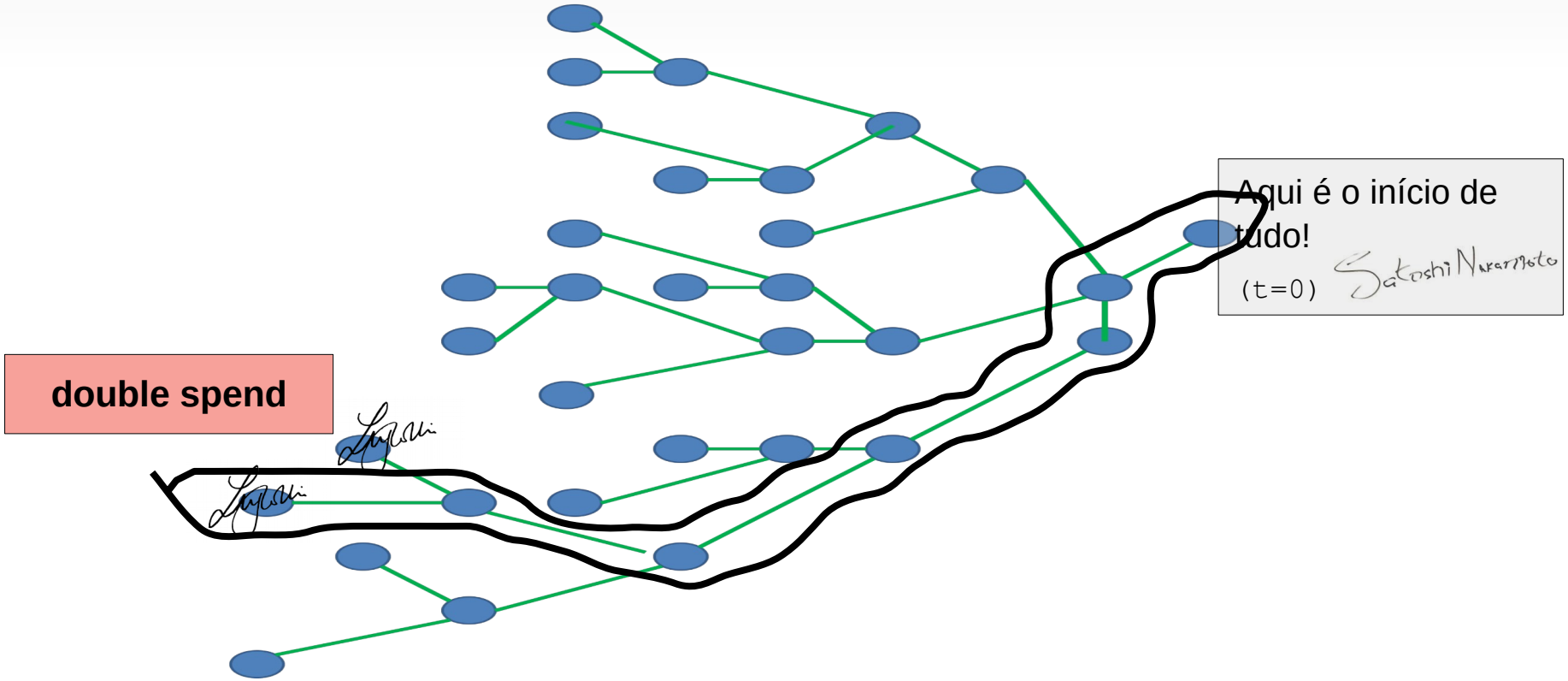
Eu, Alice, transfiro *1 bitcoin* para João. (t=1000)

Eu, Alice, descobri *5 bitcoins*. **(PROVA)** (t=678)

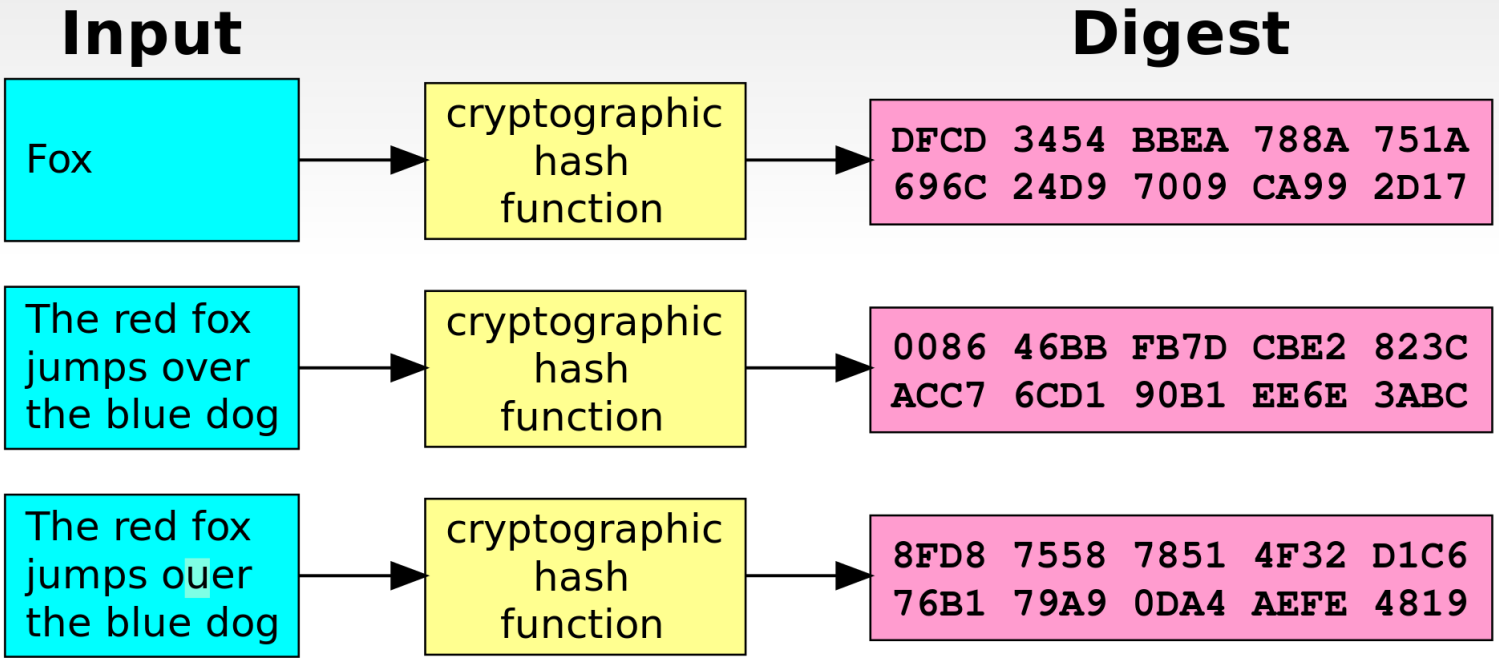
Aqui é o início de tudo! (t=0) Satoshi Nakamoto

# Consenso

- Somente um caminho deve ser válido
- O caminho com mais trabalho associado



# Função Hash Criptográfica



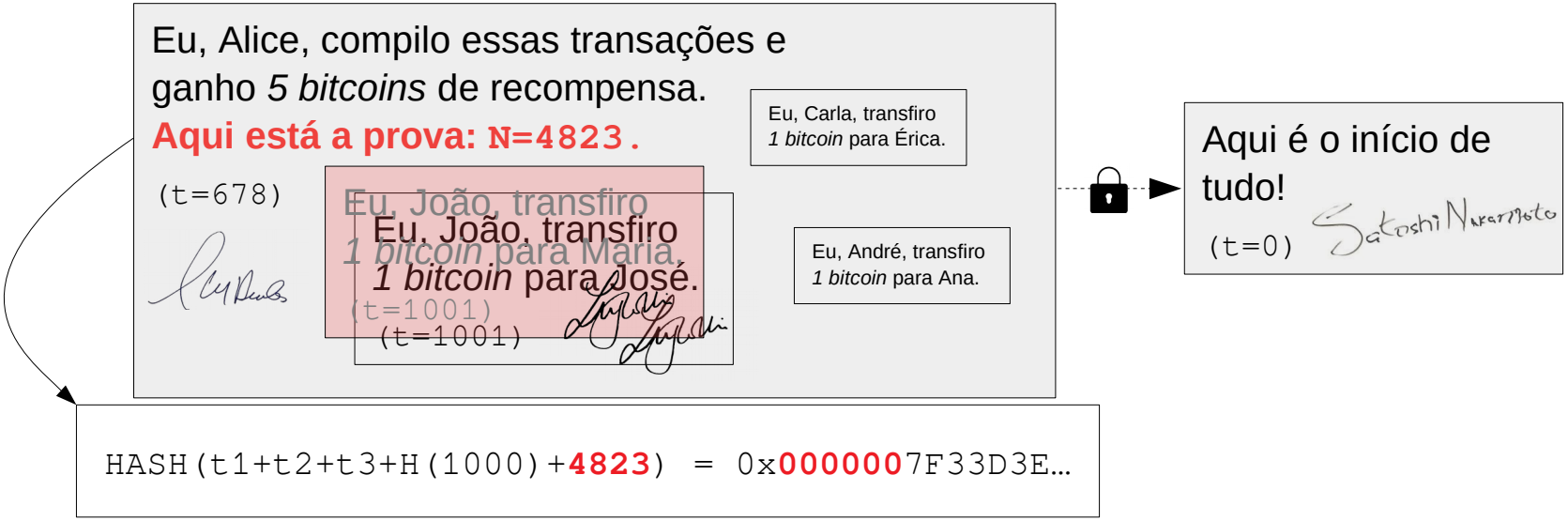
# Função Hash Criptográfica

- Determinística:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
- "One-way" (não inversível):
  - $H^{-1}$`("DFCD BBEA ... CA99 2D17") → ???`
- Sem colisões:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H(~~?????~~) → "DFCD BBEA ... CA99 2D17"`
- Caótica:
  - `H("Fox") → "DFCD BBEA ... CA99 2D17"`
  - `H("Foy") → "1200 C78A ... EF1A D99B"`

# Mineração

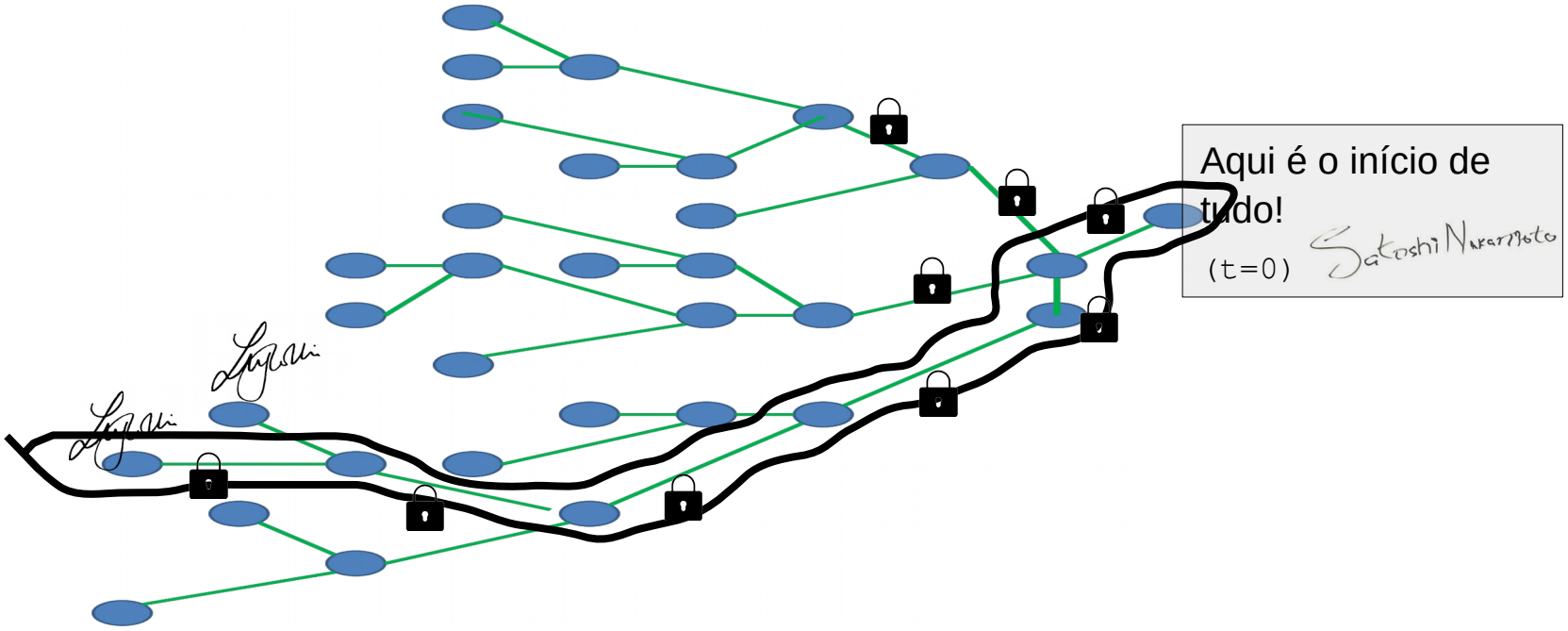
Eu, Alice, descobri *5 bitcoins*. **(PROVA)**
(t=678)

- Custosa:
  - Verifica transações pendentes até o gênesis
  - Realiza um trabalho com dificuldade artificial (e prova!)
- As transações são compiladas em um bloco.



# Consenso

- Somente um caminho deve ser válido
- O caminho com mais trabalho associado
- Trabalho artificial demora ~10 minutos
- Se 51% de CPU da rede for honesta, então a rede é segura



# 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.

# *Sistemas Peer-to-Peer*

## *5. Bitcoin*

Francisco Sant'Anna
francisco@ime.uerj.br