introdução ao protocolo Bitcoin

orientador: André A. Villela

bruno cuconato

EBEF/FGV

o protocolo Bitcoin

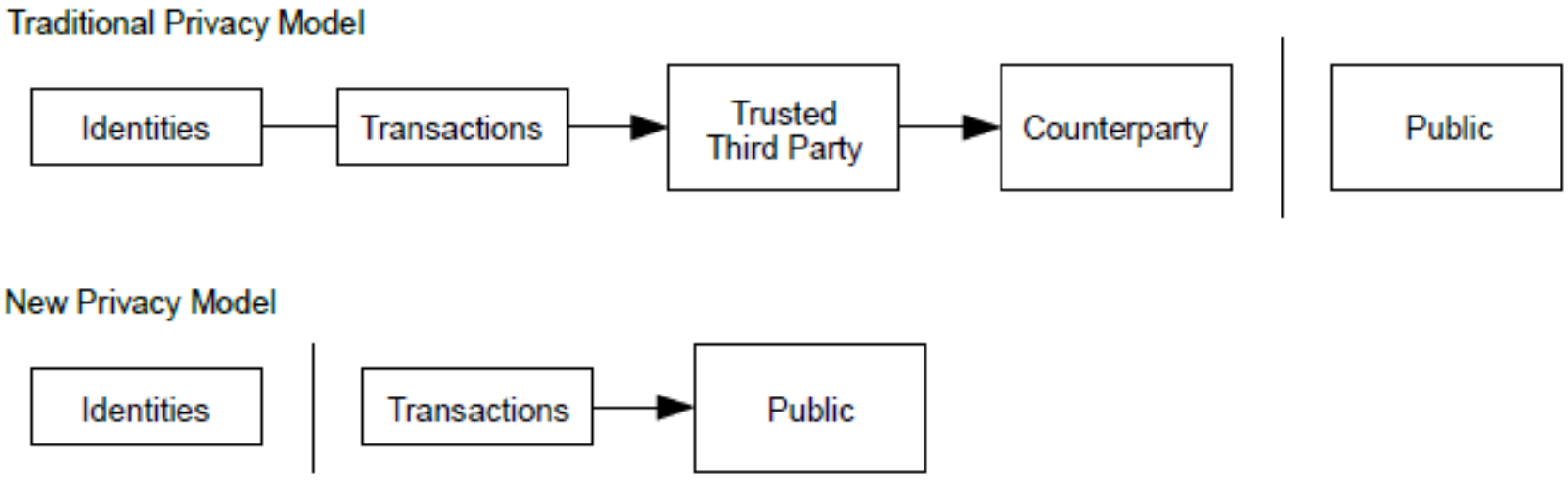

Figura 1: novo modelo de segurança

o protocolo Bitcoin

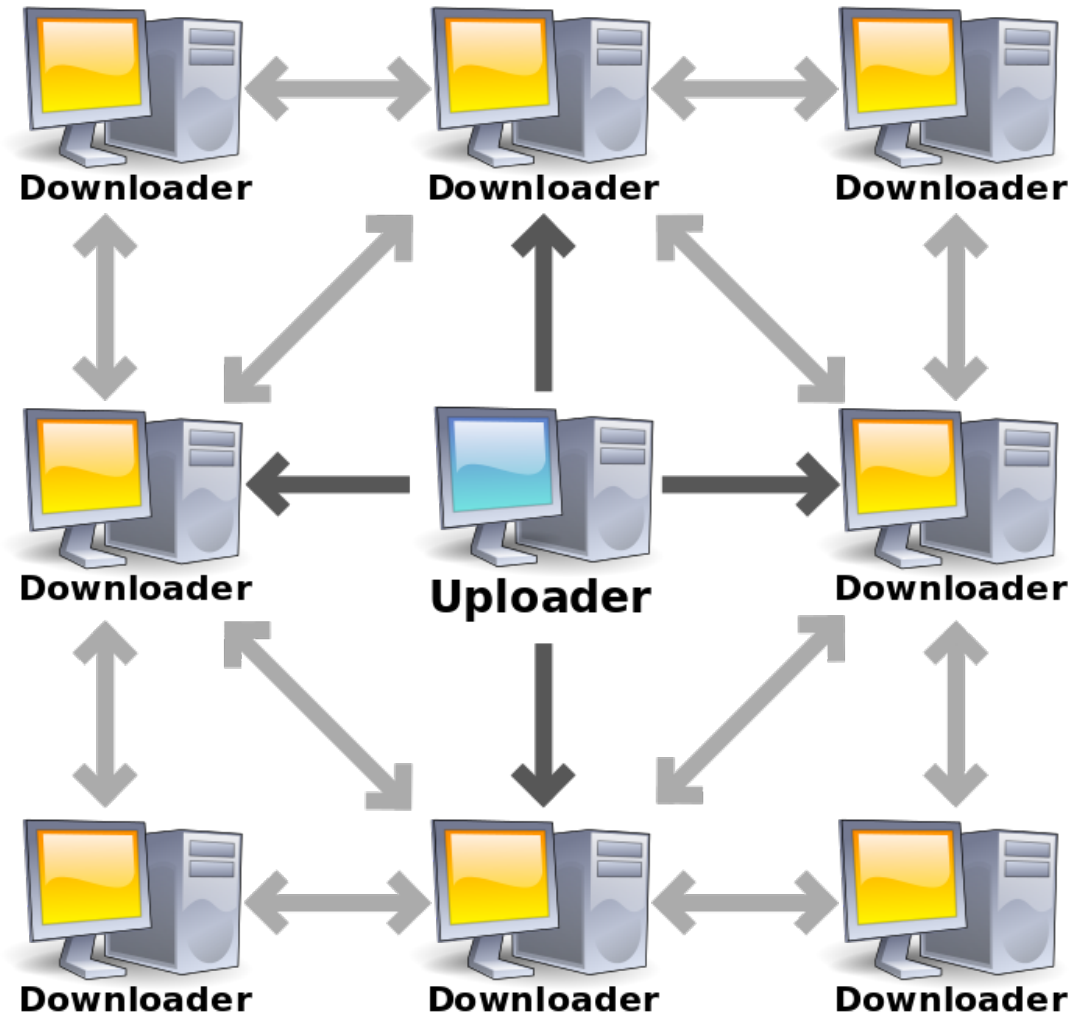

Figura 2: um protocol P2P

o protocolo Bitcoin

"A purely peer-to-peer version of electronic cash"

- mas como?

o protocolo Bitcoin

"A purely peer-to-peer version of electronic cash"

- mas como?
- dois problemas principais

overview de criptografia

assinaturas digitais

- autenticação

assinaturas digitais

- autenticação
- não-repudiação

assinaturas digitais

- autenticação
- não-repudiação
- integridade

criptografia de chave pública

Can the reader say what two numbers multiplied together will produce the number 8616460799? I think it unlikely that anyone but myself will ever know. (William Stanley Jevons, 1874)

- trabalho inovador de Rivest et al.[1]

[1] R.L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. 21 (2): 120–126. (1978)

criptografia de chave pública

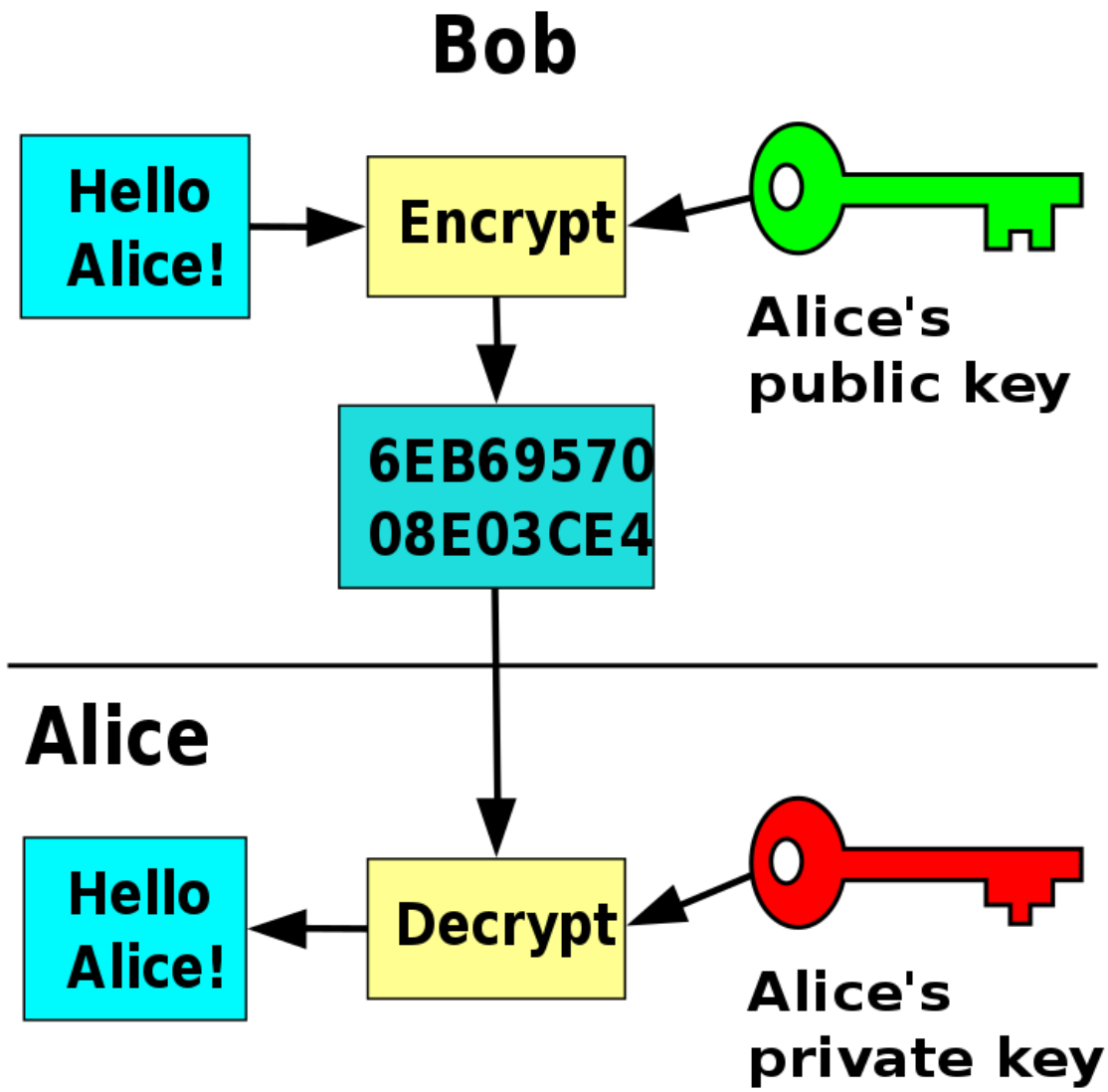

Figura 3: autenticação em criptografia de chave pública

hashing

def: uma função hash é uma função que projeta um valor pertencente a um conjunto (possivelmente infinito) em um conjunto de tamanho fixo (menor do que o do conjunto original).

hashing

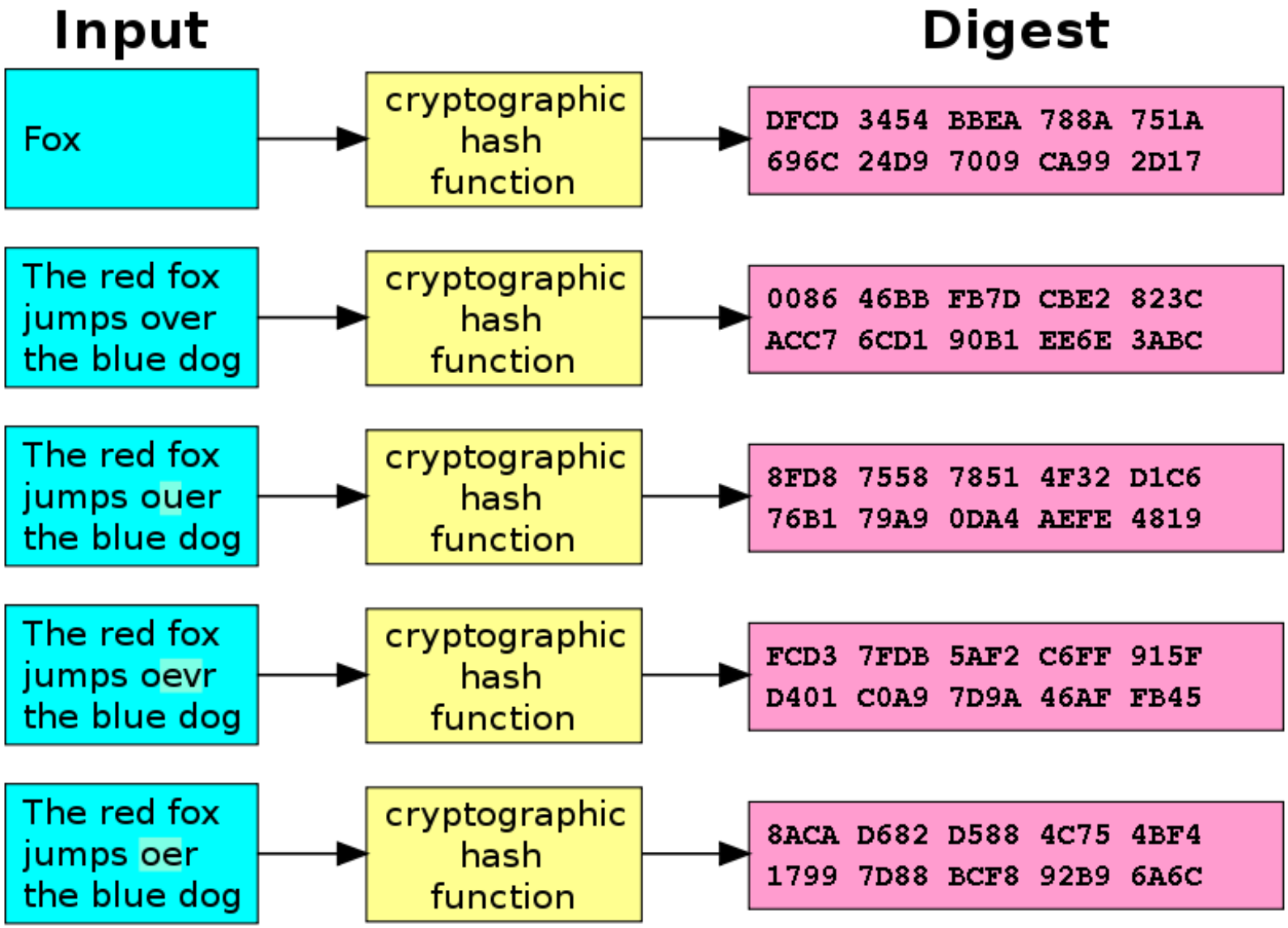

Figura 4: exemplo de output de uma função hash

hashing

- determinística

hashing

- determinística
- eficiente

hashing

- determinística
- eficiente
- irreversível (na prática)

hashing

- determinística
- eficiente
- irreversível (na prática)
- imprevisível

hashing

- determinística
- eficiente
- irreversível (na prática)
- imprevisível
- sem colisões

transações

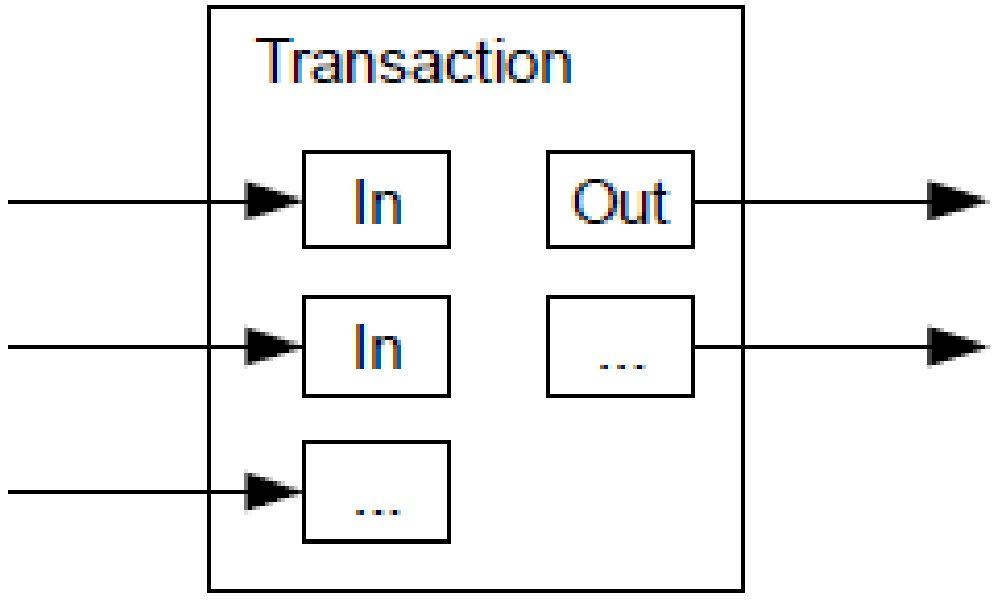

Figura 5: entradas e saídas de uma transação Bitcoin

transações

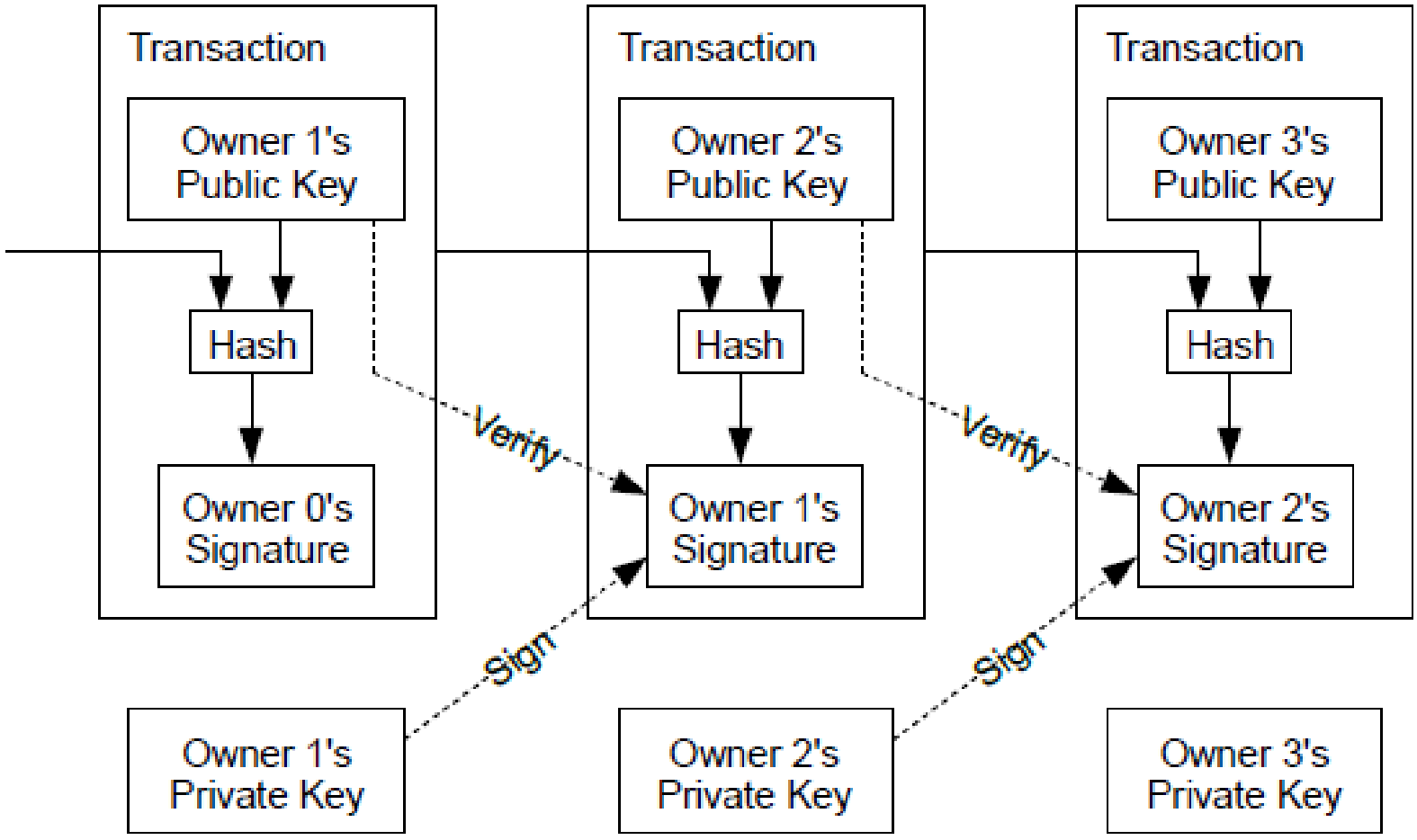

Figura 6: exemplo de transações Bitcoin

transações

- toda transação especifica outras transações como inputs e outputs tal que:

$$\text{input\_txs} \equiv \text{output\_txs} + \text{tx\_fees}$$

transações

- toda transação especifica outras transações como inputs e outputs tal que:

$$\text{input\_txs} \equiv \text{output\_txs} + \text{tx\_fees}$$

- segurança de uma transação

e o gasto duplo?

e se ao mesmo tempo alguém enviar duas transações com os mesmos inputs e outputs diferentes? qual delas vale?

blockchain

- discretização do tempo em blocos

blockchain

- discretização do tempo em blocos
- blocos reunem transações

blockchain

- discretização do tempo em blocos
- blocos reunem transações
- um mesmo bloco tem de ser consistente internamente e com seus predecessores

blockchain

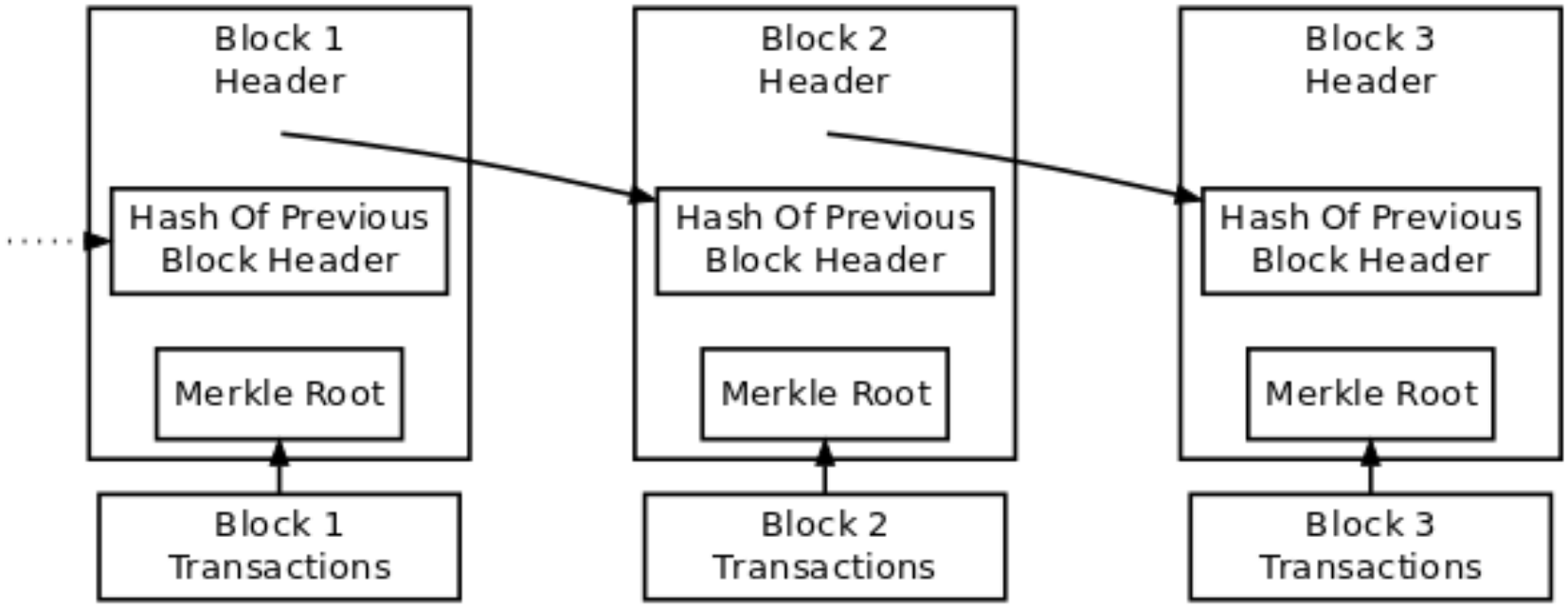

Figura 7: exemplo de blockchain

blockchain

mas qual bloco vale?

proof-of-work (PoW)

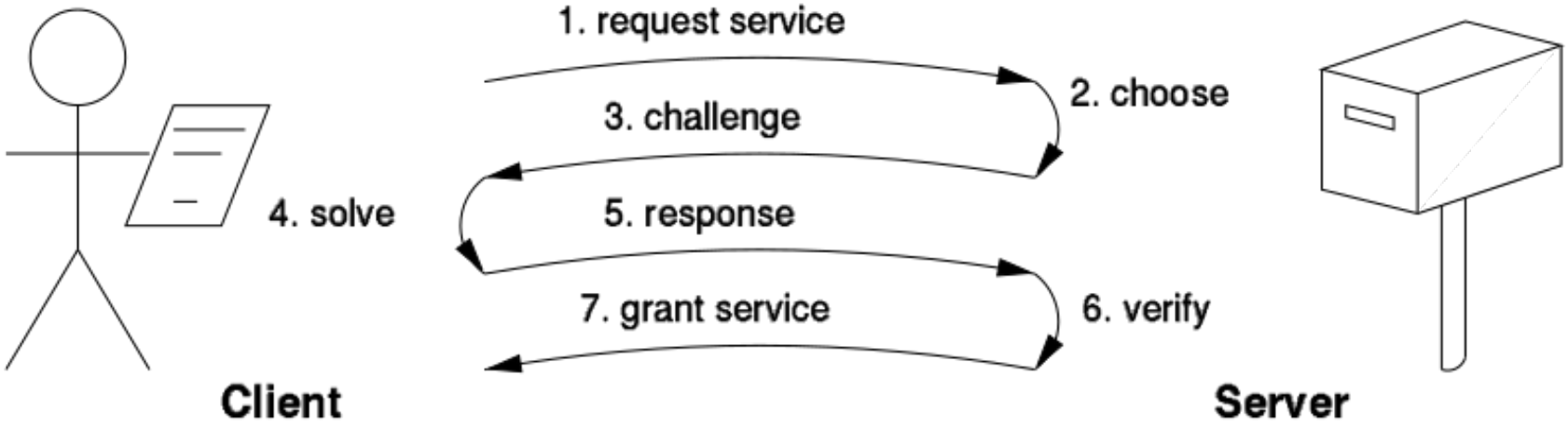

Figura 8: challenge-response PoW

proof-of-work (PoW)

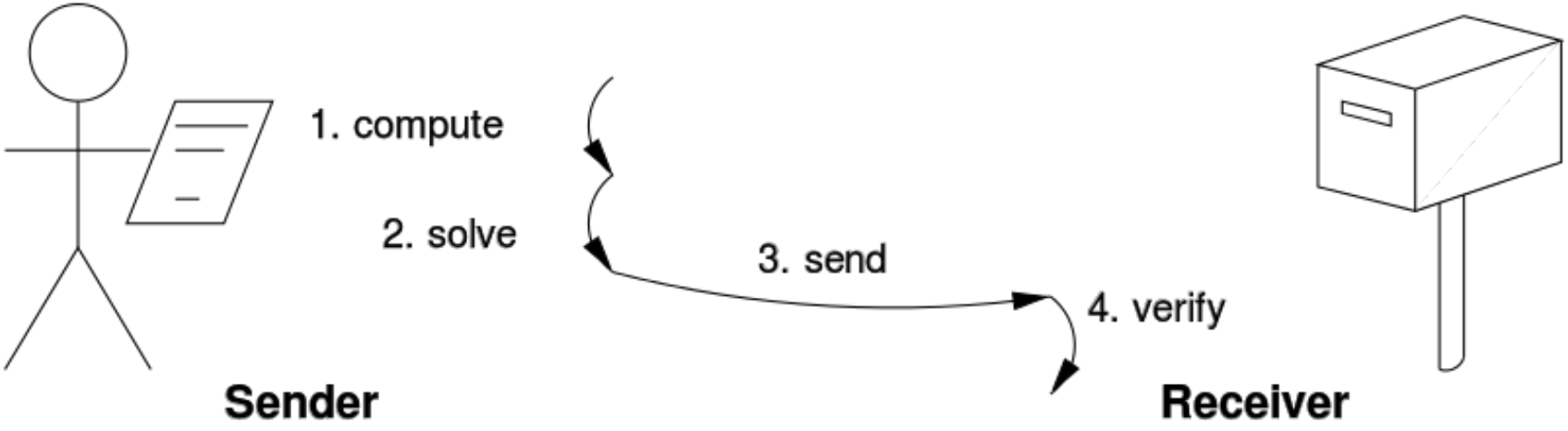

Figura 9: solution-verification PoW

proof-of-work (PoW)

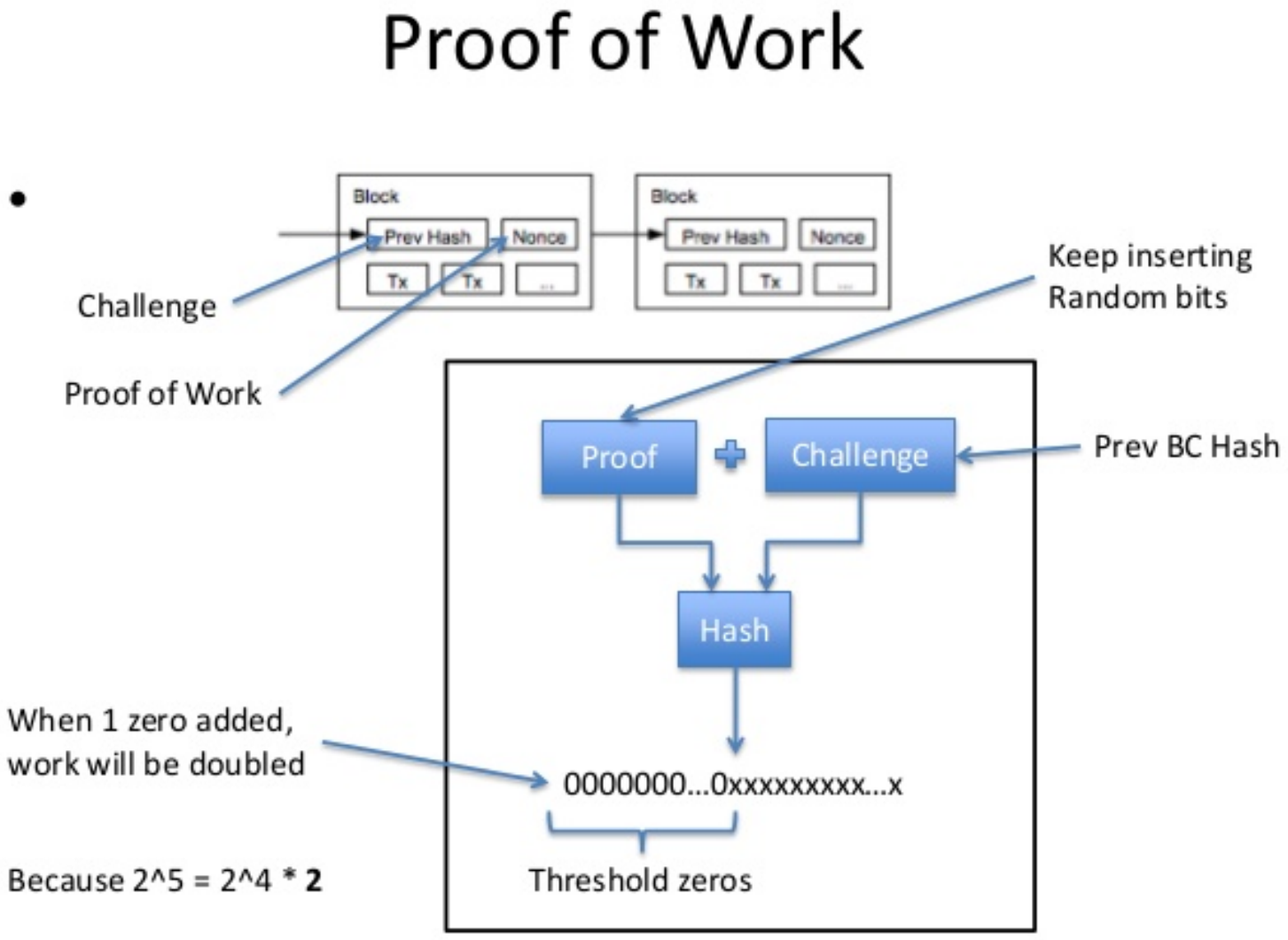

Figura 10: PoW in Bitcoin

proof-of-work (PoW)

```
trying hash input: "cabeçalho de bloco-candidato número 0"
hash digest: 18b34598d215b1103f4cd2313b89a2258e2ee0c[...]
trying again...
trying hash input: "cabeçalho de bloco-candidato número 1"
hash digest: 57cc3a304f9e4eb246a10c82d08840738c126f8[...]
trying again...
trying hash input: "cabeçalho de bloco-candidato número 2"
hash digest: 091519f78f862828d112bc9460ee53dfc324c1e[...]
found!
```

proof-of-work (PoW)

- competição entre mineradores para decidir qual bloco entrará para a blockchain

proof-of-work (PoW)

- competição entre mineradores para decidir qual bloco entrará para a blockchain
- os mineradores são indenizados pelo seu custo computacional por meio da emissão de novas bitcoins e pelas taxas de transação

forking

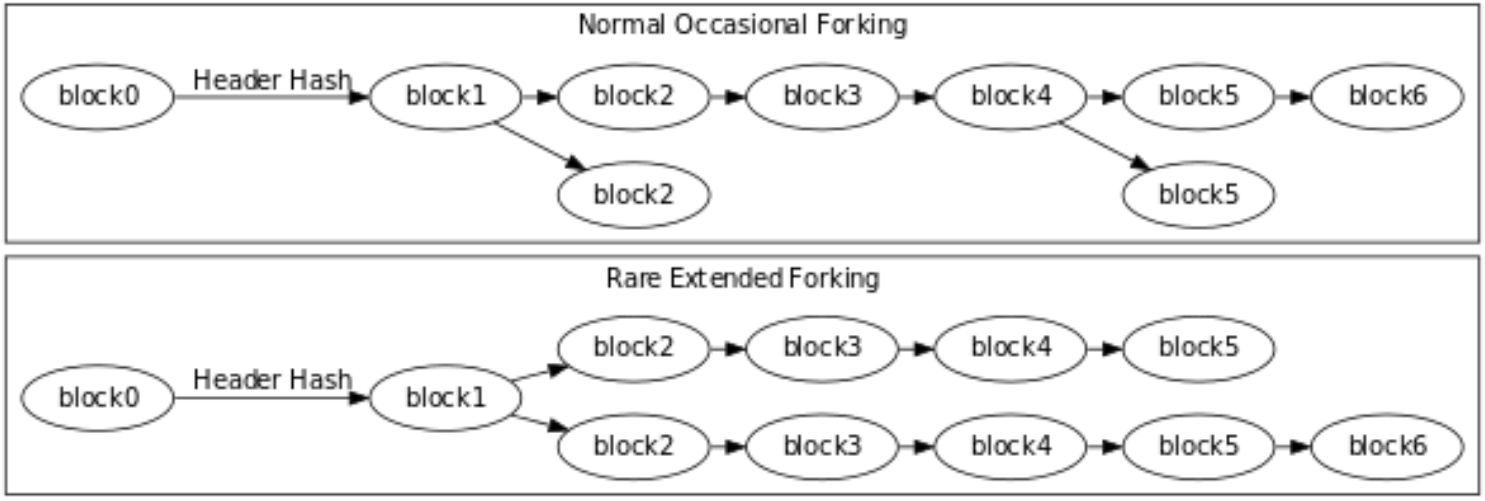

Figura 11: exemplos de fork na blockchain

mineração

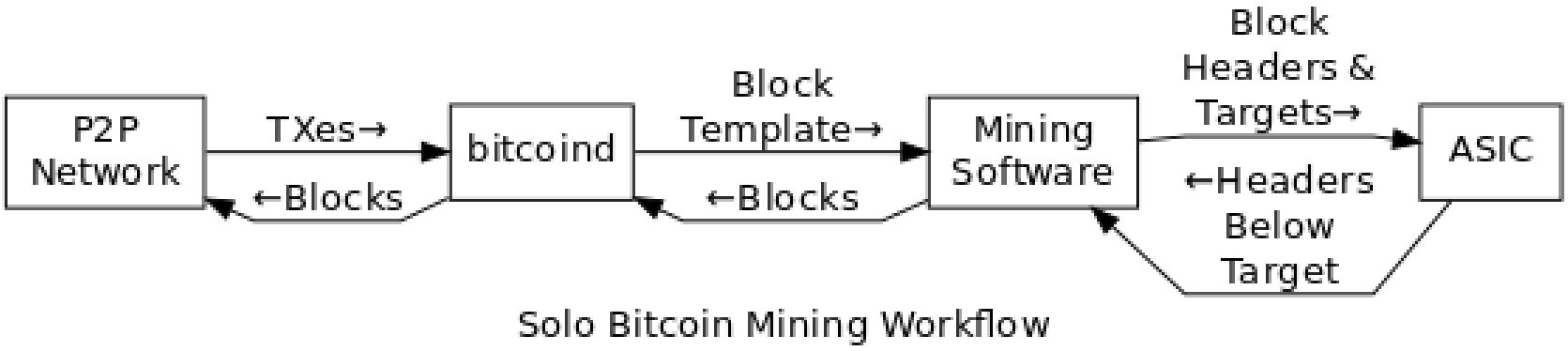

Figura 12: *workflow* de um minerador

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo
- $P_i = f(C_i)$ *hashes* por segundo

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo
- $P_i = f(C_i)$ *hashes* por segundo
- G tentativas esperadas para minerar bloco (depende da dificuldade, constante no modelo)

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo
- $P_i = f(C_i)$ *hashes* por segundo
- G tentativas esperadas para minerar bloco (depende da dificuldade, constante no modelo)
- V dólares pela mineração de um bloco (altamente variável, mas marginalmente constante)

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo
- $P_i = f(C_i)$ *hashes* por segundo
- G tentativas esperadas para minerar bloco (depende da dificuldade, constante no modelo)
- V dólares pela mineração de um bloco (altamente variável, mas marginalmente constante)
- valor esperado de R blocos por segundo (variável aleatória do protocolo)

modelo de mineração

Kroll et al.

- custo para a mineração de bitcoins é de C_i USD por segundo
- $P_i = f(C_i)$ *hashes* por segundo
- G tentativas esperadas para minerar bloco (depende da dificuldade, constante no modelo)
- V dólares pela mineração de um bloco (altamente variável, mas marginalmente constante)
- valor esperado de R blocos por segundo (variável aleatória do protocolo)
- hipótese: tecnologia igual para todos os mineradores

Kroll et al.

conclusão: a mineração é um mercado competitivo sem barreiras à entrada

Kroll et al.

$$\frac{P_i V}{G} \geq C_i \tag{1}$$

com N mineradores competindo, temos $\overline{P} = \sum_{i=1}^{N} P_i$, e

$$G = \frac{\overline{P}}{\overline{R}} \tag{2}$$

Kroll et al.

Unindo as equações 1 e 2, obtém-se a decisão individual entre minerar ou não minerar levando em conta as escolhas dos outros mineradores:

$$\frac{P_i V}{\frac{\overline{P}}{\overline{R}}} \geq C_i \tag{3}$$

Como todos os mineradores tomam a mesma decisão, com $\overline{C} = \sum_{i=1}^{N} C_i$, tem-se:

$$\sum_{i=1}^{N} \frac{P_i V}{\frac{\overline{P}}{\overline{R}}} \geq \sum_{i=1}^{N} C_i$$

$$RV \geq \overline{C} \tag{4}$$

Kroll et al.

problemas

- custo de mineração tem componente fixa grande, além da marginal

Kroll et al.

problemas

- custo de mineração tem componente fixa grande, além da marginal
- a tecnologia pode não ser homogênea entre os mineradores:

Kroll et al.

problemas

- custo de mineração tem componente fixa grande, além da marginal
- a tecnologia pode não ser homogênea entre os mineradores:
  - há mineradores que são fabricantes de *hardware*

Kroll et al.

problemas

- custo de mineração tem componente fixa grande, além da marginal
- a tecnologia pode não ser homogênea entre os mineradores:
  - há mineradores que são fabricantes de *hardware*
  - é possível otimizar os códigos de mineração

Kroll et al.

problemas

- custo de mineração tem componente fixa grande, além da marginal
- a tecnologia pode não ser homogênea entre os mineradores:
  - há mineradores que são fabricantes de *hardware*
  - é possível otimizar os códigos de mineração
- falta levar em conta volatilidade da Bitcoin e a possibilidade de mineração de outras criptomoedas

referências

- SATOSHI, N. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

- Bitcoin core: reference implementation. https://github.com/bitcoin/bitcoin, Acesso em 2016-11-20.

- ANTONOPOULOS, A. M. Mastering bitcoin: unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly Media, Inc., 2014.

- Bitcoin: Developer documentation. https://bitcoin.org/en/developer-documentation, Acesso em 2016-11-20.

- KROLL, J. A.; DAVEY, I. C.; FELTEN, E. W. The economics of bitcoin mining, or bitcoin in the presence of adversaries. Proceedings of WEIS, Washington, D.C., v. 2013, 2013.

contato

material da IC

site pessoal