TÓPICOS AVANÇADOS

MERKLE TREE E CHAMELEON HASH

Prof. Dr. Bruno de Carvalho Albertini
Curso Blockchain Developer

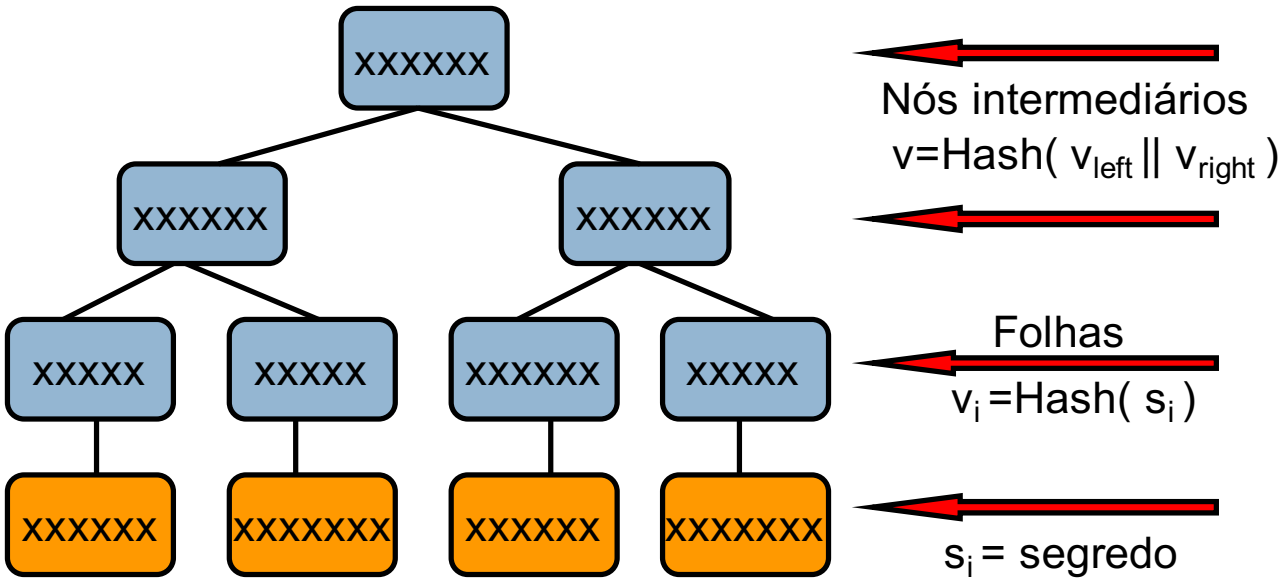
Merkle trees

- Ralph Merkle, 1979
  - Árvore Binária + Hashes
- Utilizada para autenticação
  - Usa somente hashes (função de via única)
  - Não há nenhuma trapdoor

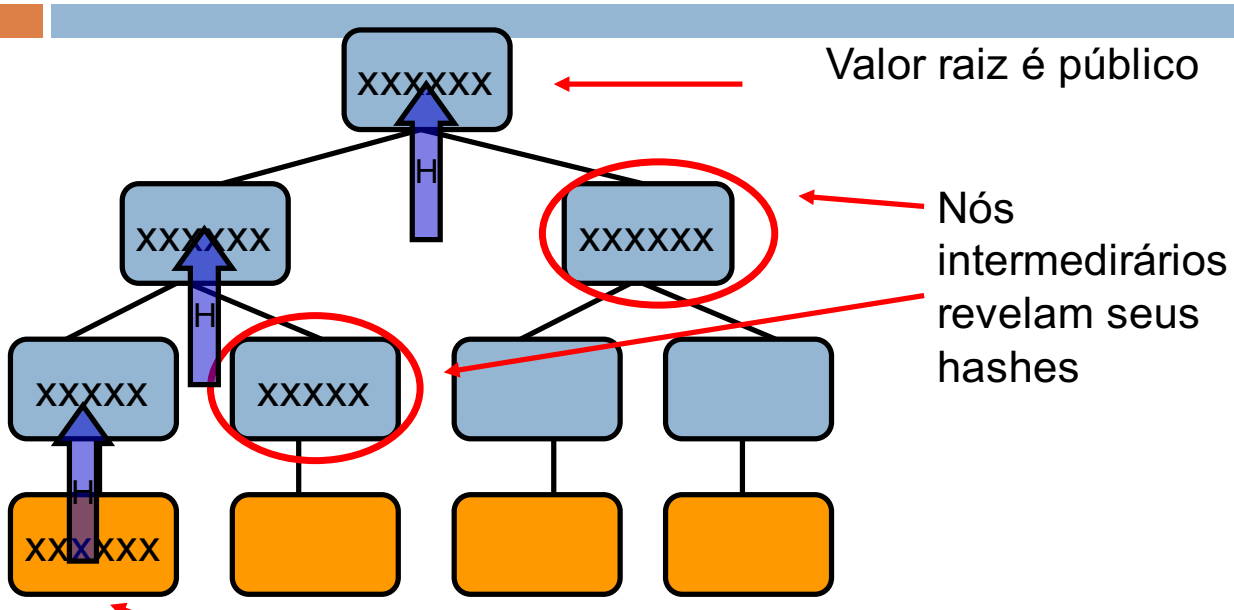
Merkle trees

Árvore binária com nós de 160bits

Folhas tem o valor que deseja-se proteger (segredo)



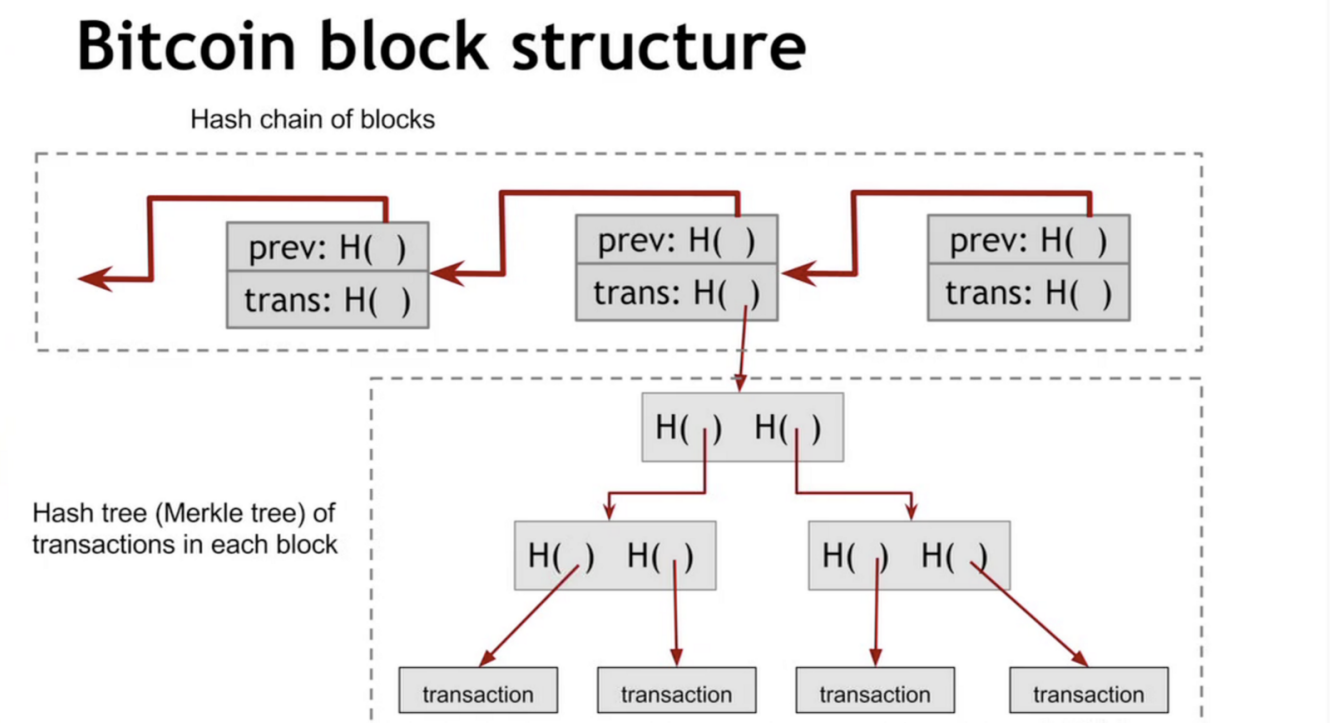
Verificação



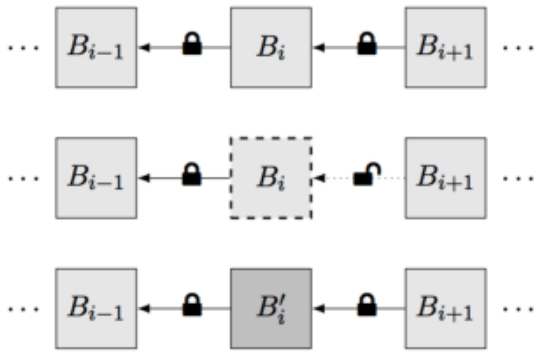
s_0

1. Verifica-se o valor secreto com hashes
2. Aceita-se se o hash final é a raiz

Merkle tree na Blockchain



Blockchain Editável



- Uso de uma chave segura
- Encontrar uma colisão

Chameleon Hash

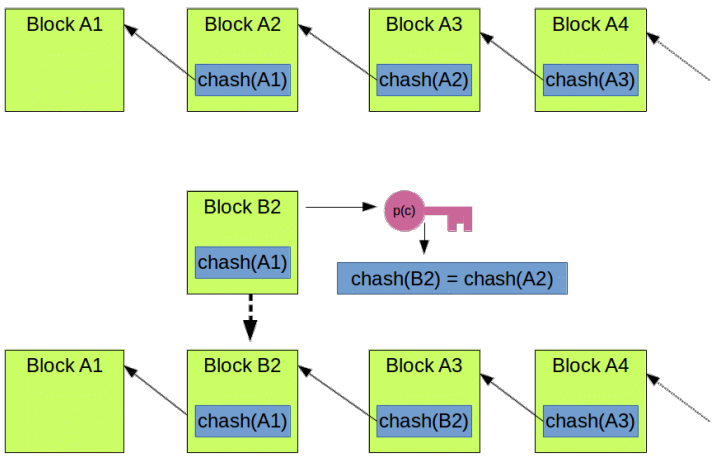
Chameleon Hashing and Signatures

Hugo Krawczyk* Tal Rabin†

October 1997

KRAWCZYK, Hugo; RABIN, Tal. Chameleon hashing and signatures. **Internet--http://www. research. ibm. com/security/projects. html**, 1997.

Chameleon Hash



Blockchain Editável

Redactable Blockchain
– or –
Rewriting History in Bitcoin and Friends*

Giuseppe Ateniese[1], Bernardo Magri[2], Daniele Venturi[3], and Ewerton Andrade[4]

ATENIESE, Giuseppe et al. Redactable blockchain–or–rewriting history in bitcoin and friends. In: **Security and Privacy (EuroS&P), 2017 IEEE European Symposium on**. IEEE, 2017. p. 111-126.