Technology for BlockChain

Hashes, Keys, PKI, Encryption, Signatures

John R Williams, MIT

The FinTech Revolution

jrw@mit.edu

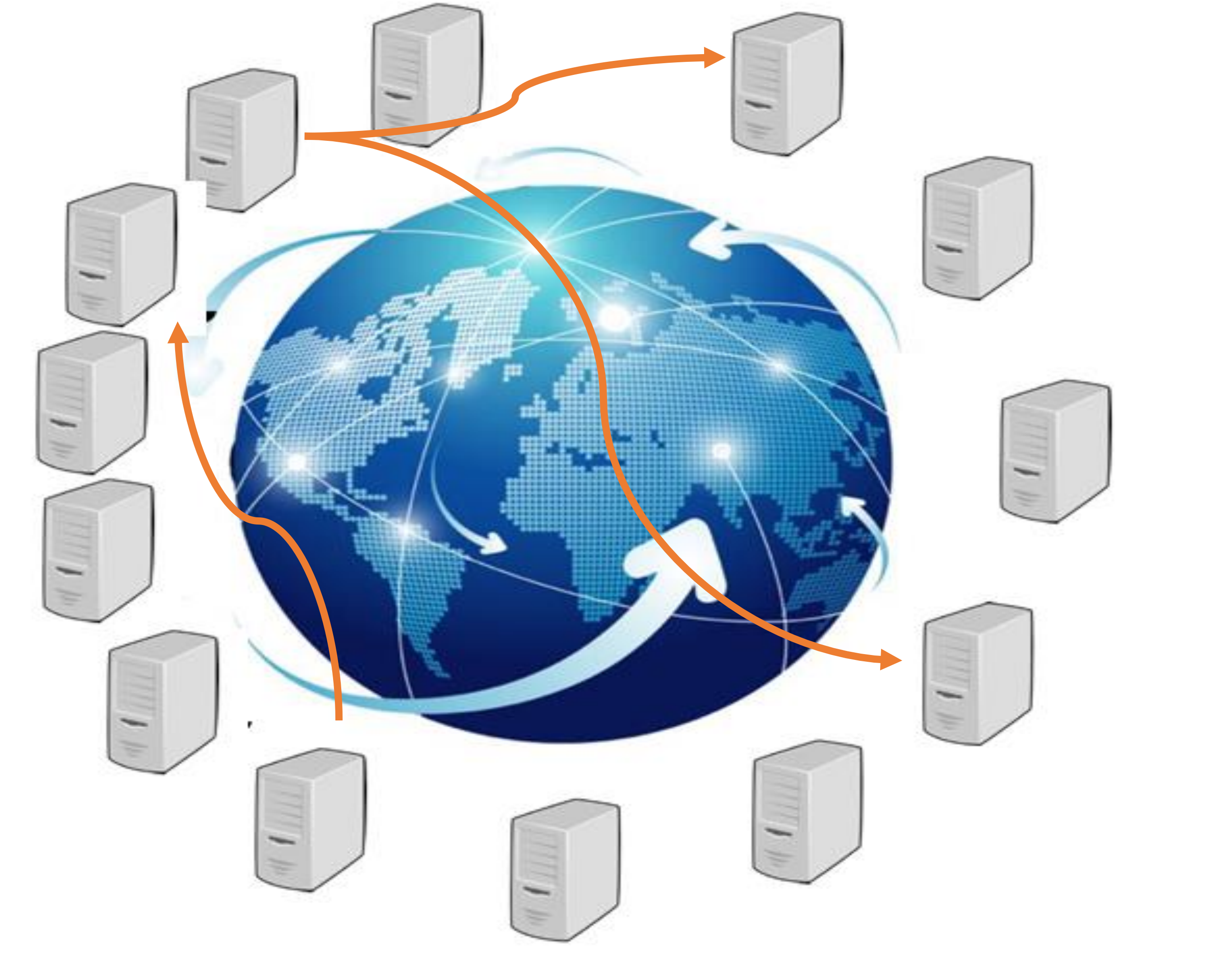
Techno Speak

- Keys, PKI, Hashes, Encryption
- Blockchain, BitCoin, Ethereum, Permissioned, Non-Permissioned, Wallets, Crypto, Hashes, Keys,…

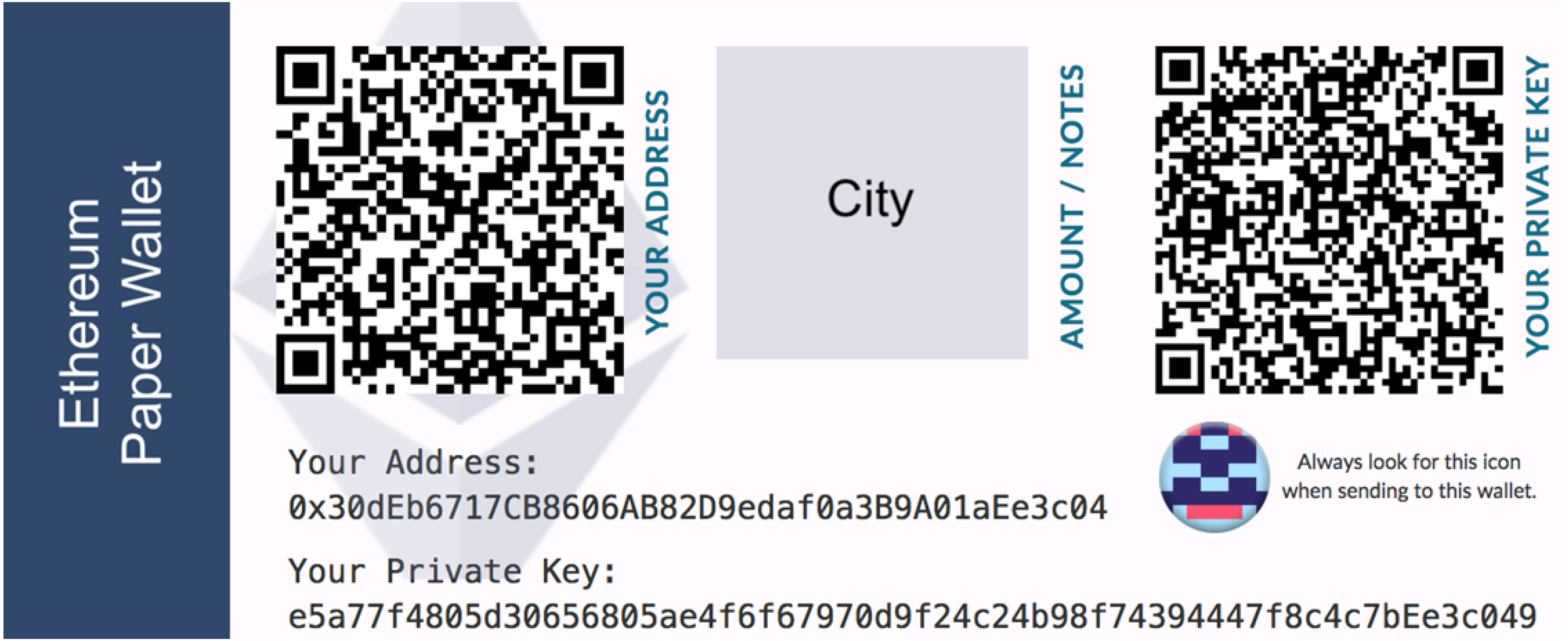
Distributed computing becomes possible with Web.

Challenges

1) Identity
2) Trust
3) Synchronization
4) Messages are asynchronous



Account in Ethereum



Ethereum Paper Wallet

YOUR ADDRESS

City

AMOUNT / NOTES

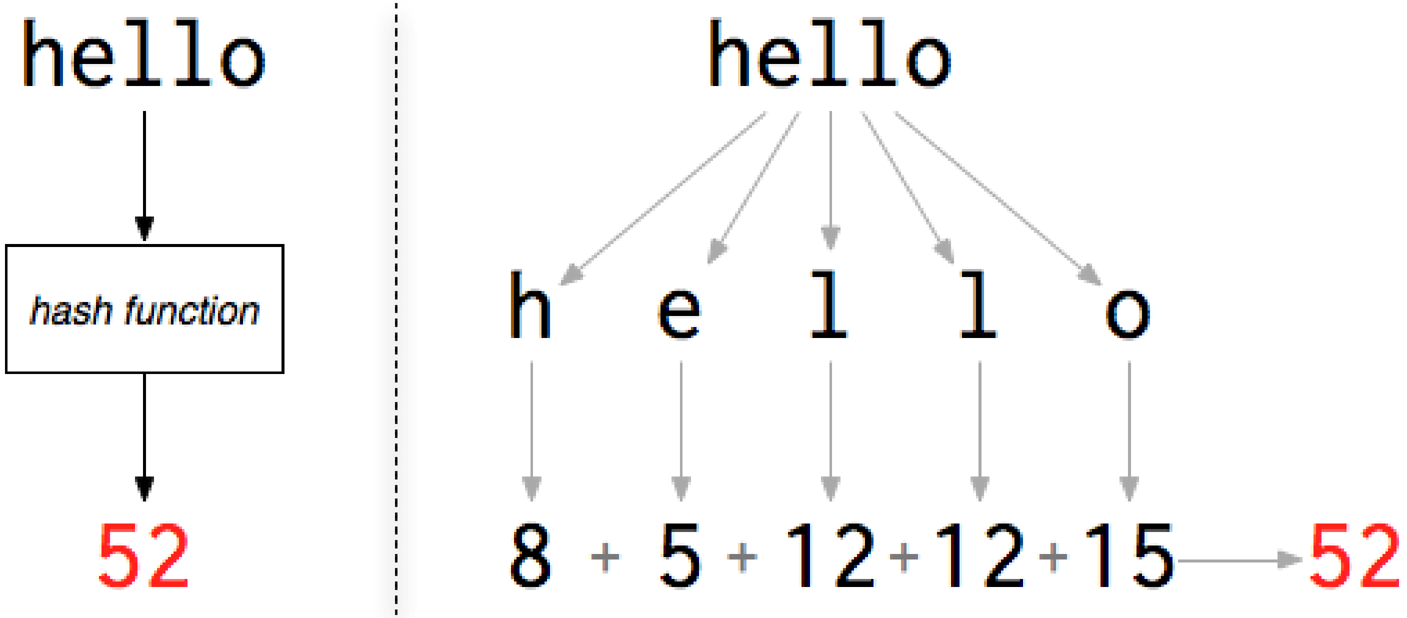
YOUR PRIVATE KEY

Always look for this icon when sending to this wallet.

Your Address:
0x30dEb6717CB8606AB82D9edaf0a3B9A01aEe3c04

Your Private Key:
e5a77f4805d30656805ae4f6f67970d9f24c24b98f74394447f8c4c7bEe3c049

A simple hash?



A hash is like a “finger print” of a document. If anything in the document changes the hash will change. However, given the hash of a document we cannot reconstruct the document ie it only works one way

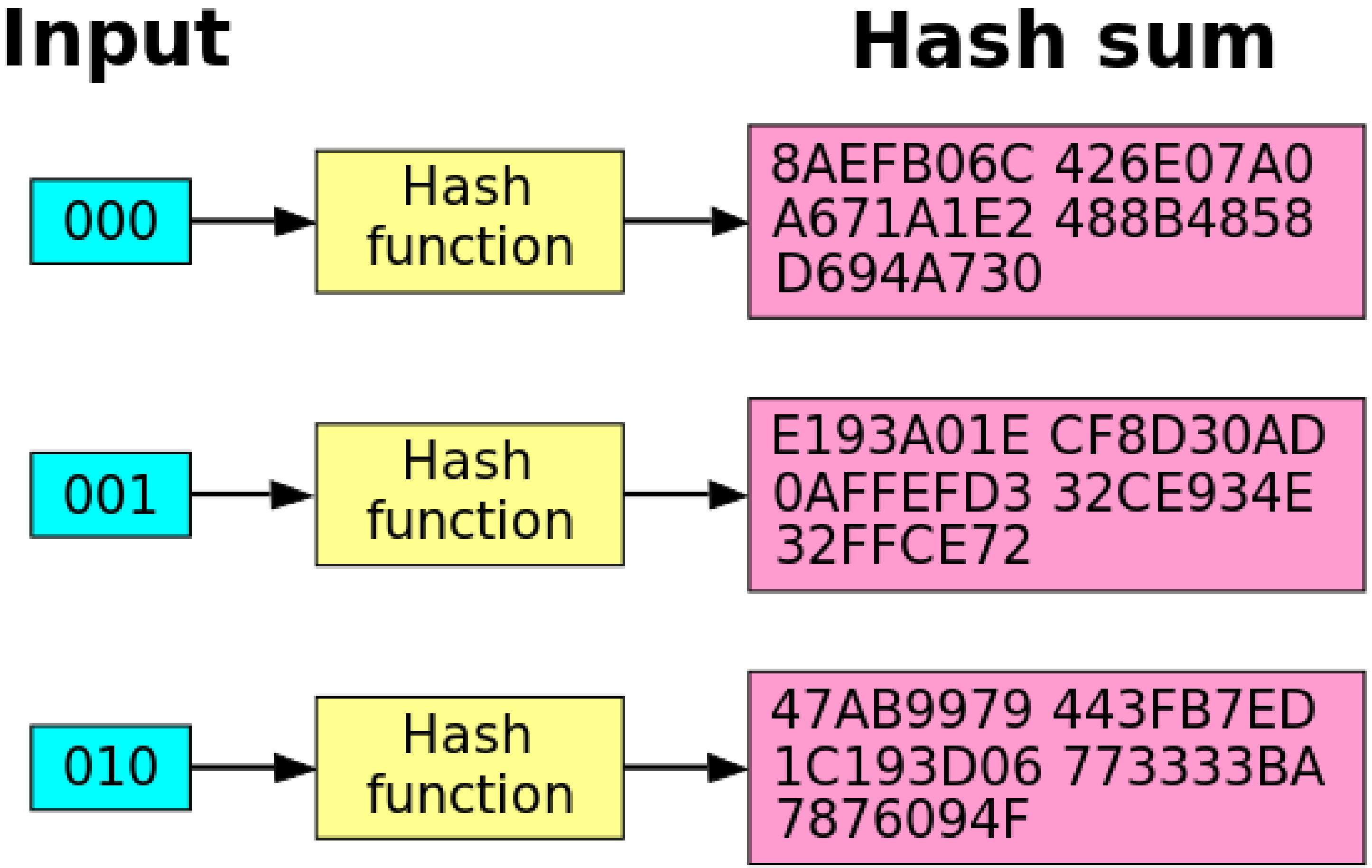
Document → Hash(D)

Demo Hash

Guess a Nonce

Avalanche property

Avalanche property - Small one bit change in input leads to radically different hash sum



Input

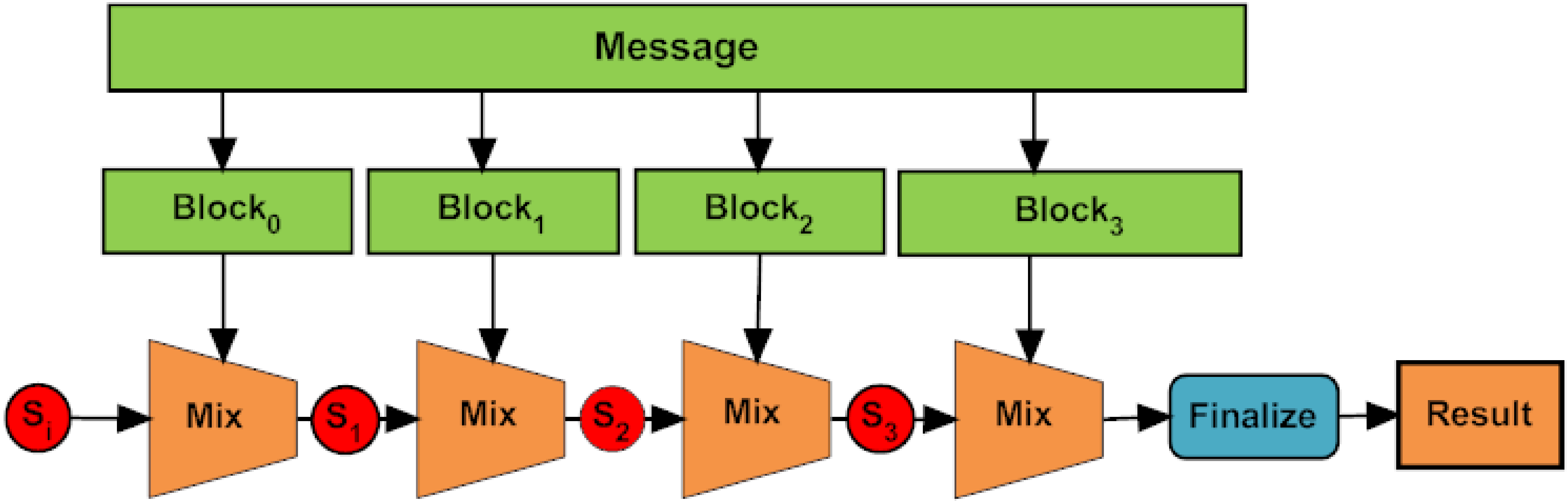
Hash sum

000 → Hash function → 8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730

001 → Hash function → E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72

010 → Hash function → 47AB9979 443FB7ED 1C193D06 773333BA 7876094F

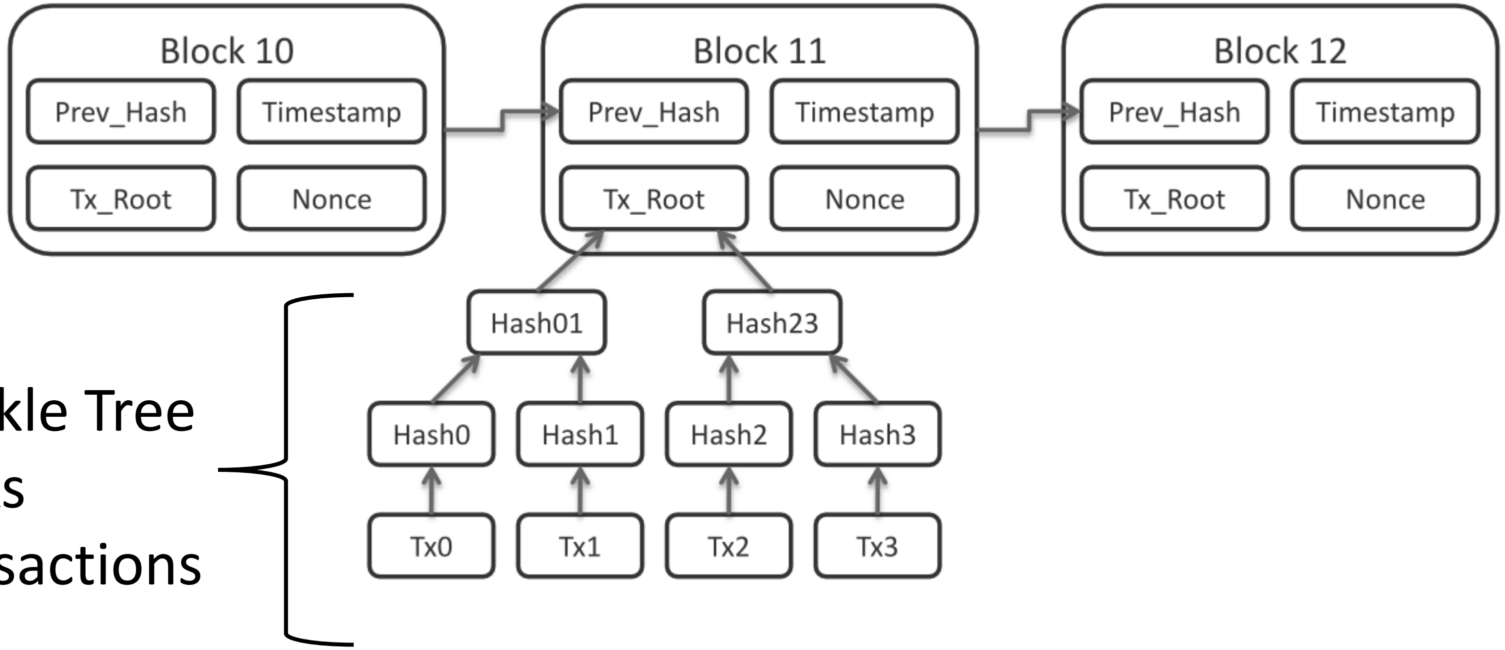
Designing a good hash function



http://www.partow.net/programming/hashfunctions/

Merkle Tree as used in BitCoin

Hash(Prev_Hash + Tx_Root + Nonce) → 000000bc9xxx



Merkle Tree
Locks
transactions

Public Key Infrastructure Keys

Keys come in pairs.

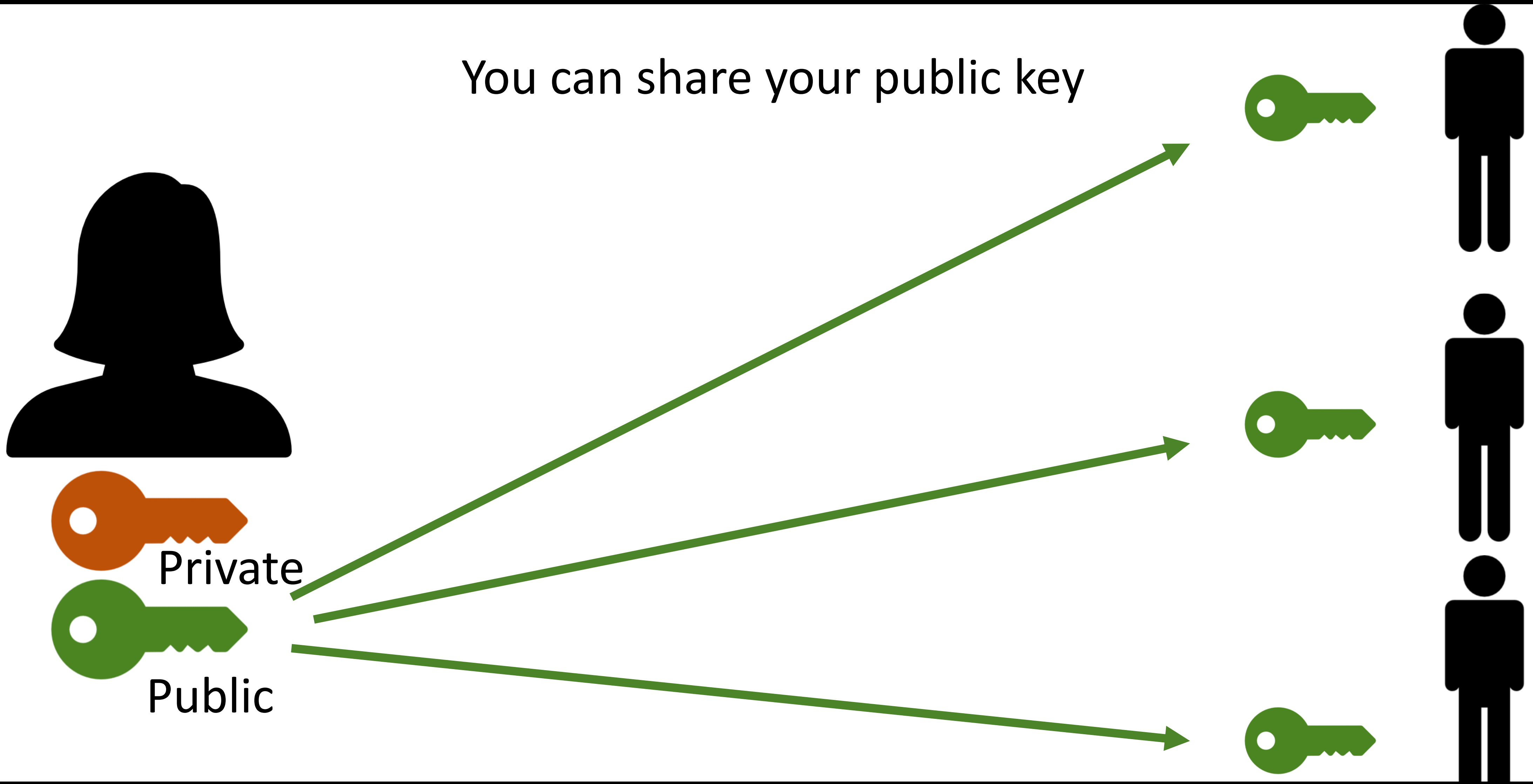
Never share your private key with anyone

Private

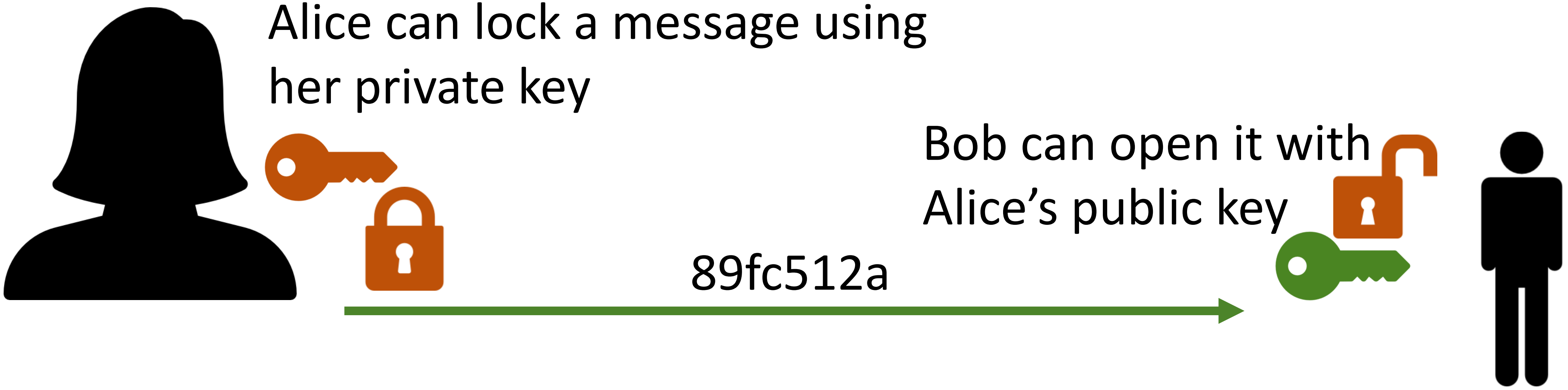
Public

Your Identity is established by your PKI Keys

You can share your public key



Your can Lock or Unlock a Message



Alice

Alice can lock a message using her private key

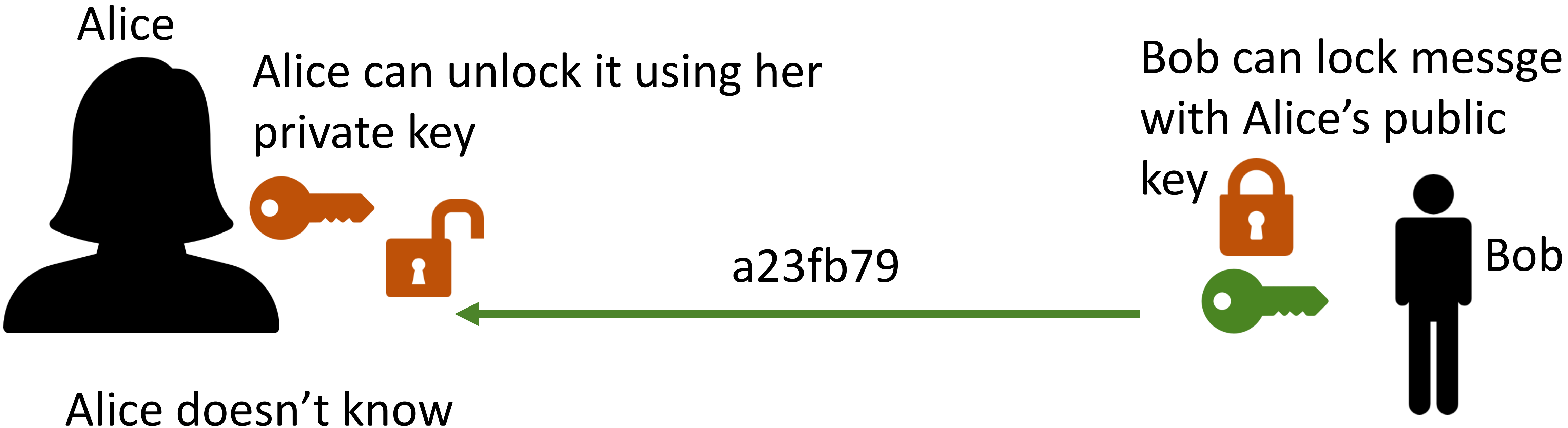
89fc512a

Bob can open it with Alice's public key

Bob

Bob knows the message must have come from Alice

Bob sends a Message to Alice using her public key !!



Alice

Alice can unlock it using her private key

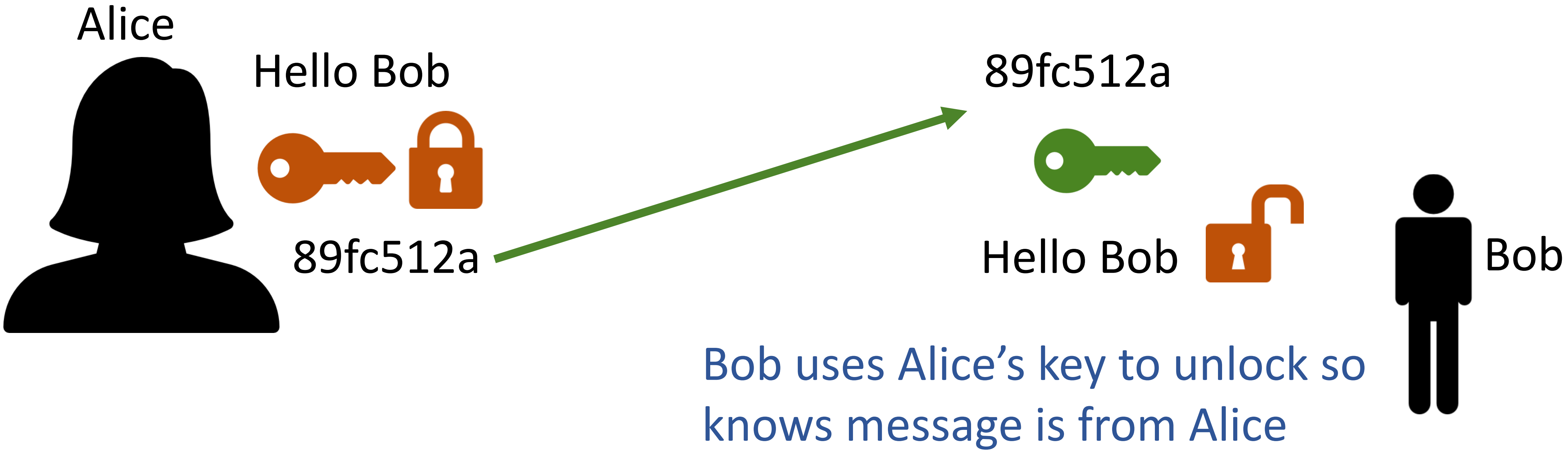
Bob can lock messge with Alice’s public key

a23fb79

Bob

Alice doesn’t know who the message has come from !!

Alice sends Bob Message



Alice

Hello Bob

89fc512a

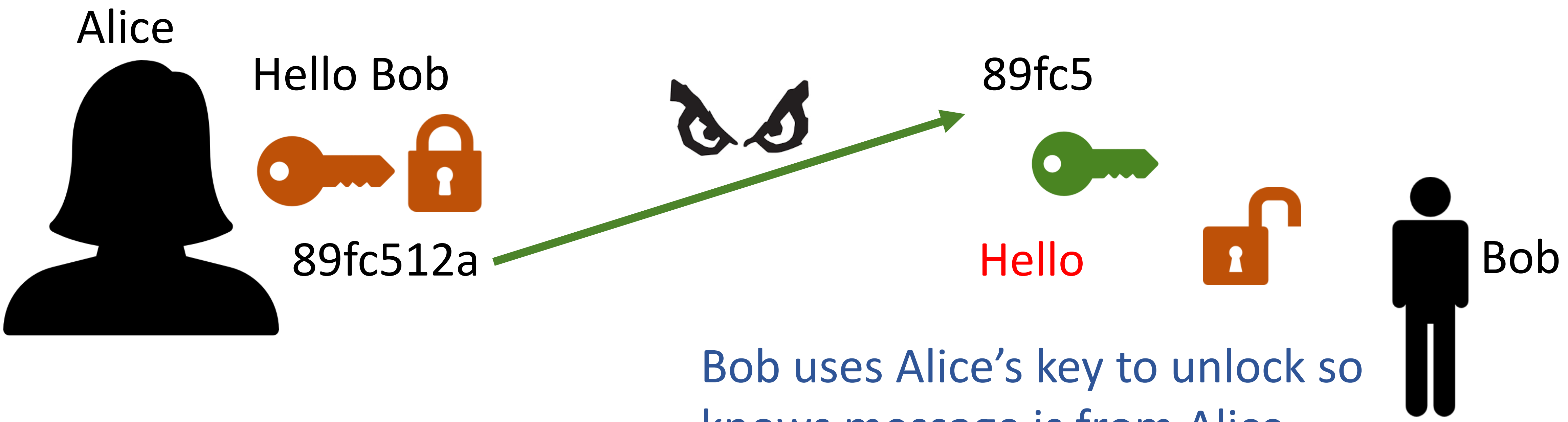
89fc512a

Hello Bob

Bob

Bob uses Alice’s key to unlock so knows message is from Alice

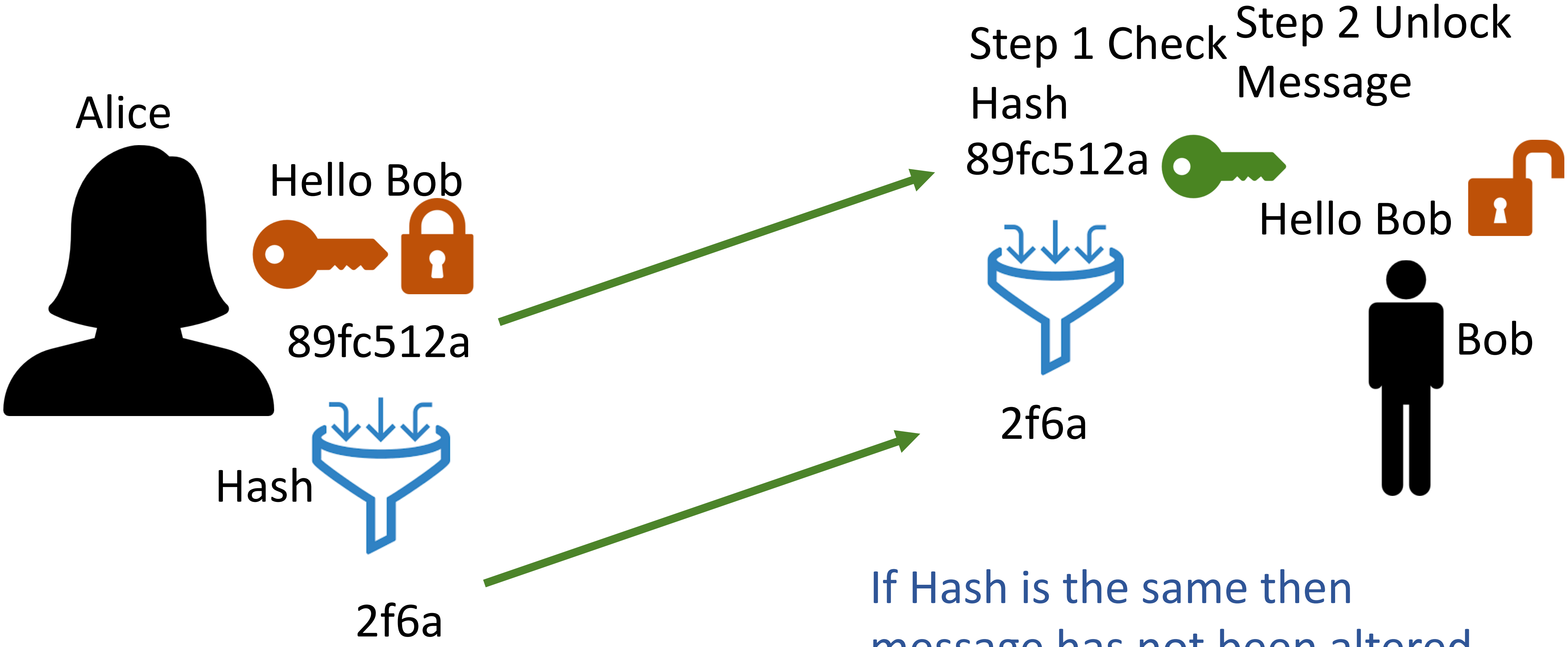
Message tampered with



Bob uses Alice’s key to unlock so knows message is from Alice

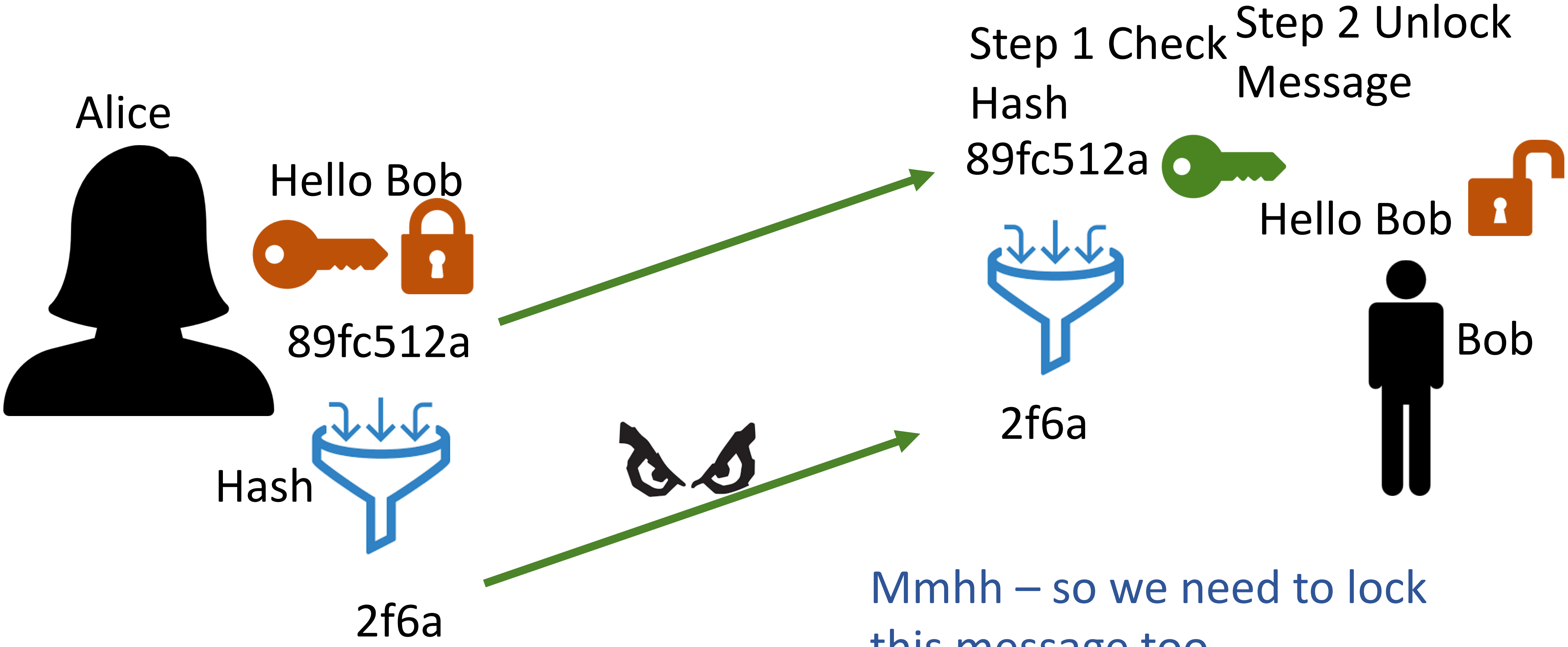
But is this the whole message or did attacker delete part of it

Send Hash of a Message - Fingerprint



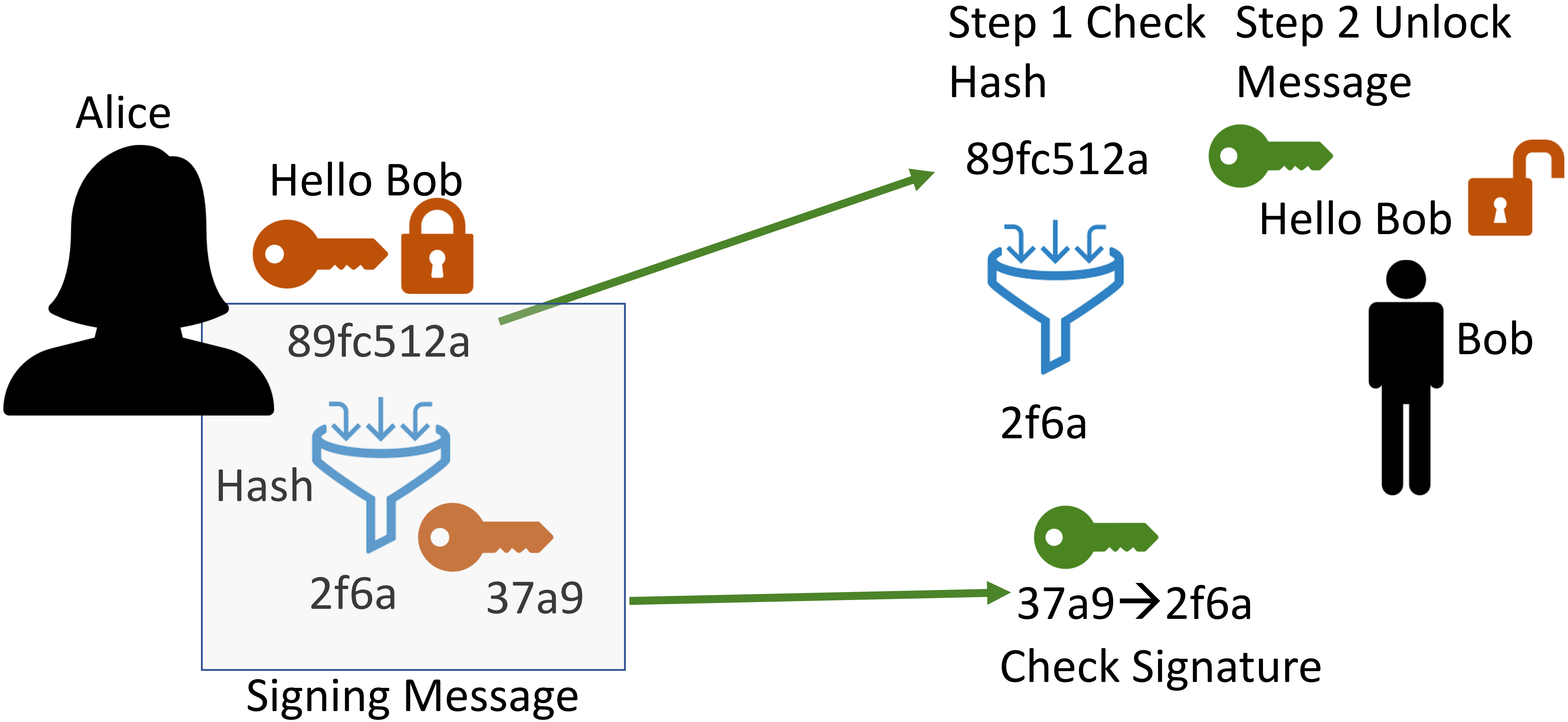
If Hash is the same then message has not been altered

But we haven’t protected the hash

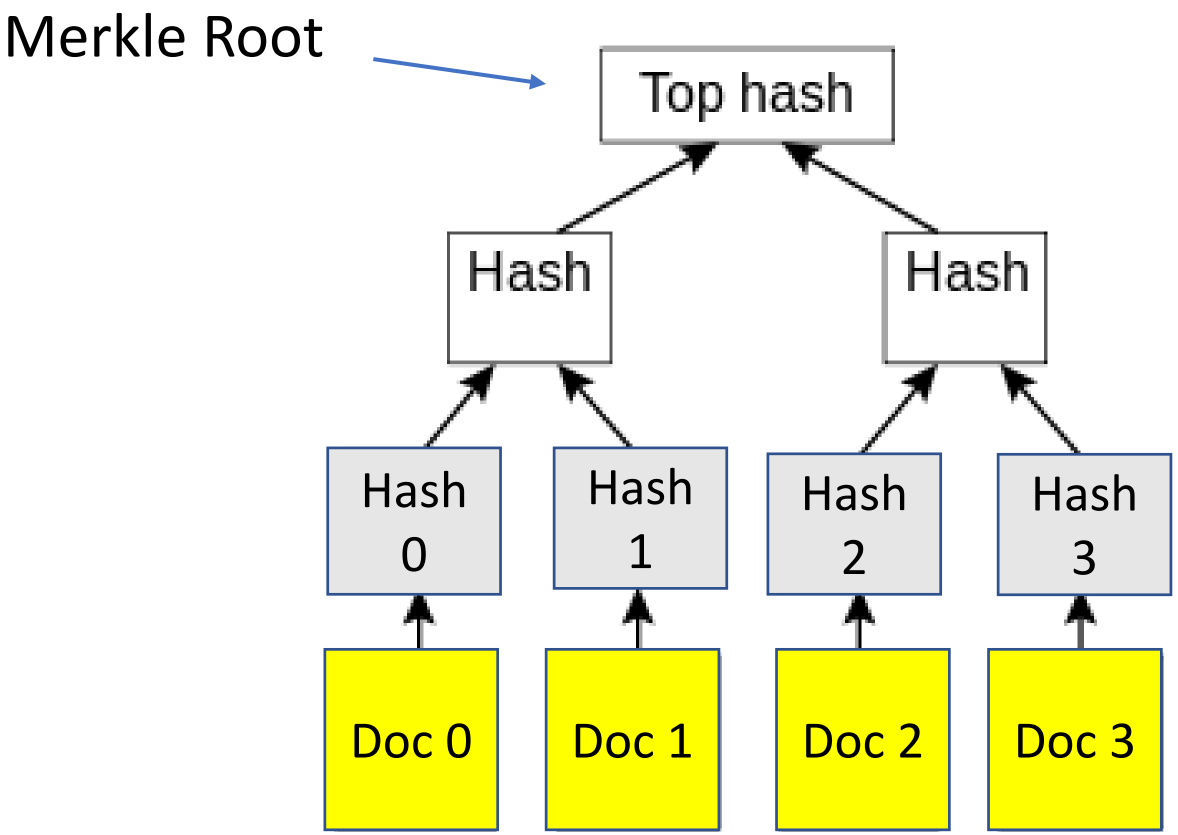


Mmhh – so we need to lock this message too

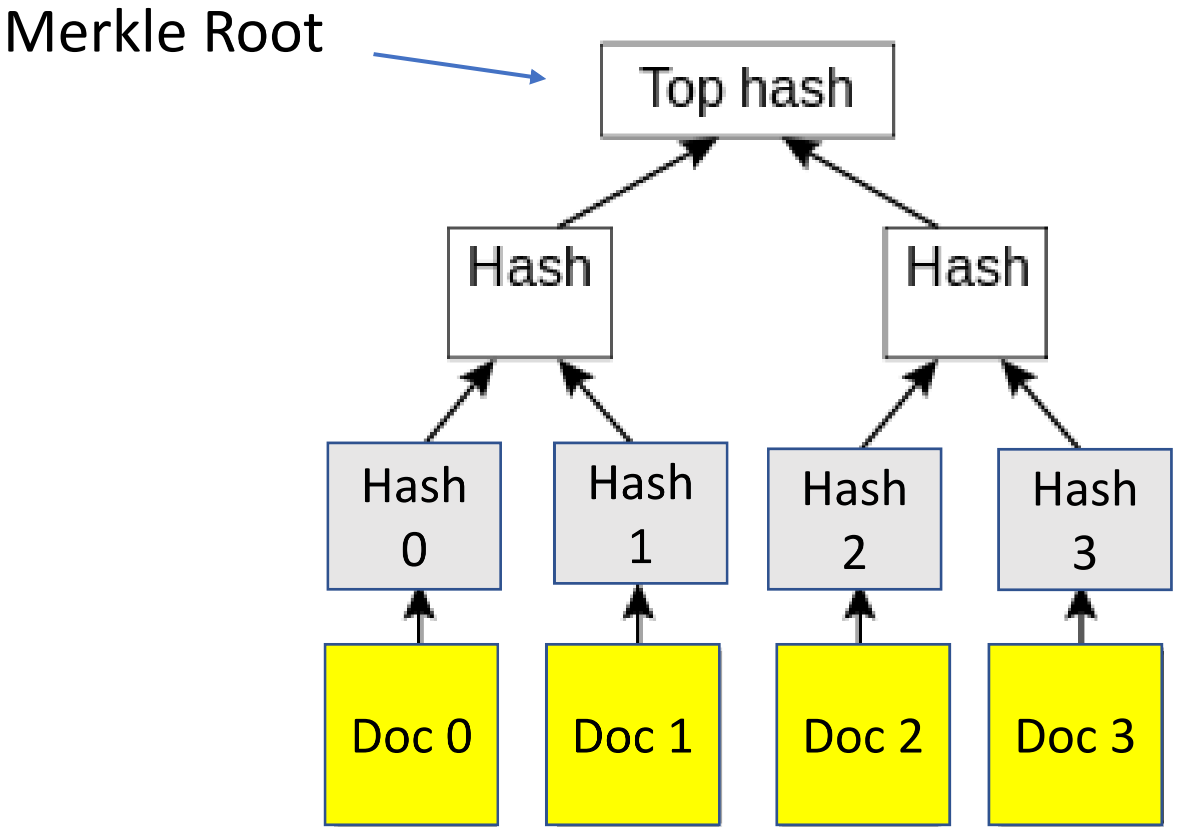
Signing a Message – Encrypt the Hash



Merkle Tree -Locking lots of Documents with 1 Hash

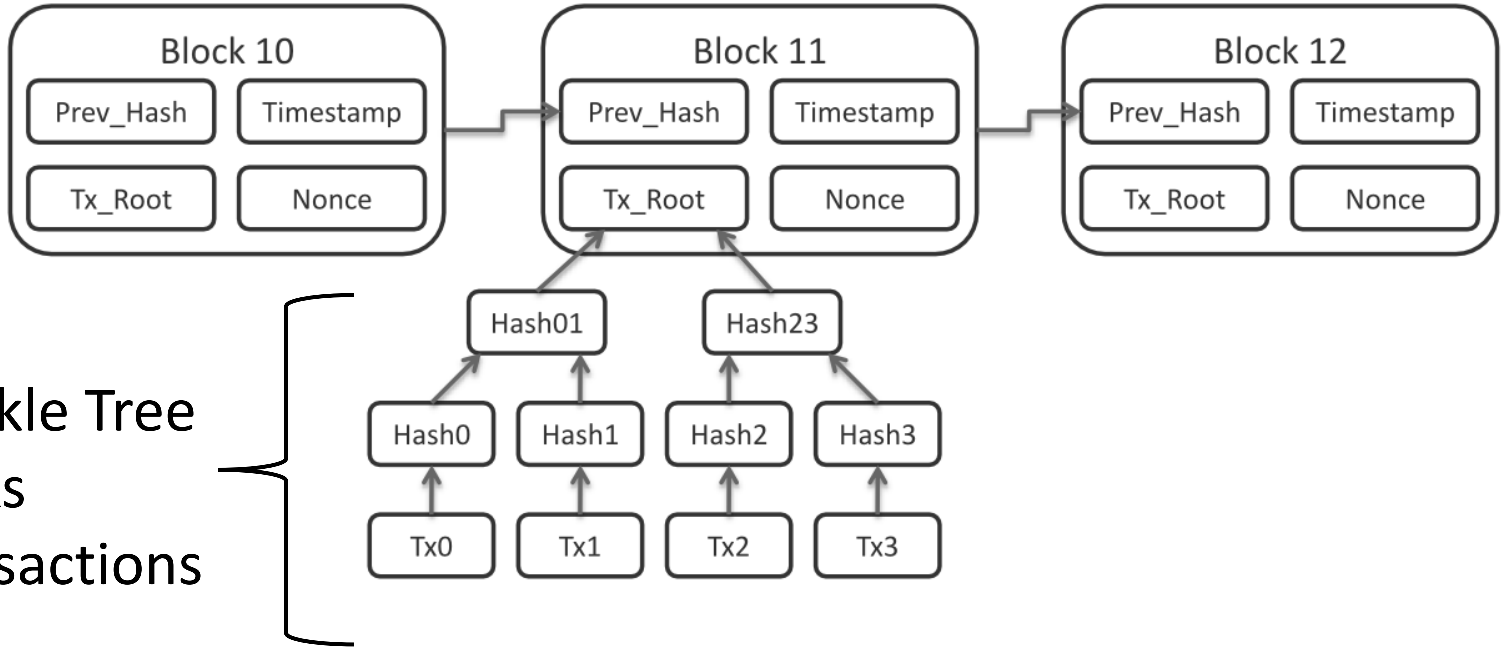


We can lock thousands of documents with one hash



Merkle Tree as used in BitCoin

Hash(Prev_Hash + Tx_Root + Nonce) → 000000bc9xxx



Merkle Tree
Locks
transactions