Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

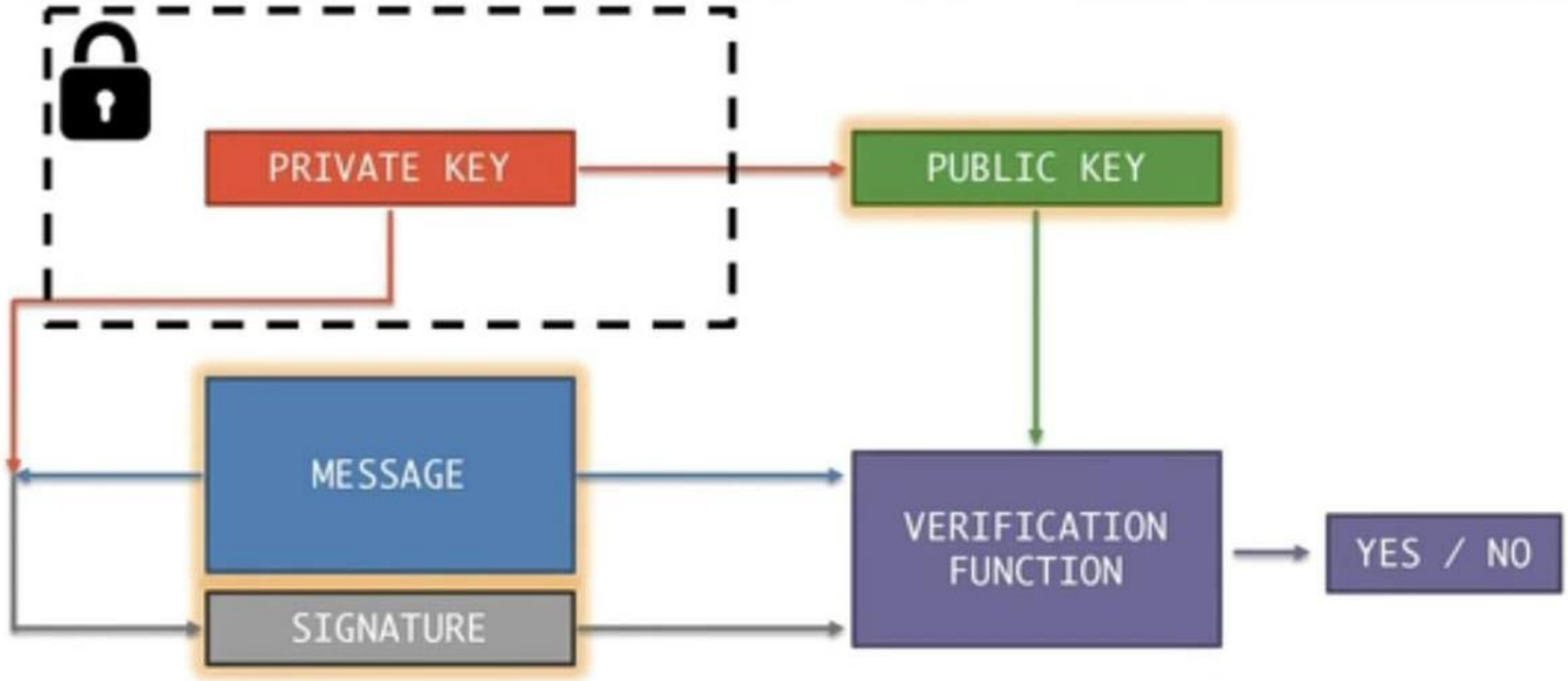
Signatures: Private & Public Keys

What we want from signatures

Only you can sign, but anyone can verify

Signature is tied to a particular document

- can’t be cut-and-pasted to another doc


PRIVATE KEY
PUBLIC KEY
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO

API for digital signatures

(sk, pk) := generateKeys(keysize)

sk: secret signing key

pk: public verification key

sig := sign(sk, message)

can be randomized algorithms

isValid := verify(pk, message, sig)

https://tools.superdatascience.com/blockchain/public-private-keys/keys

Requirements for signatures

“valid signatures verify”

verify(pk, message, sign(sk, message)) == true

“can’t forge signatures”

adversary who:

- knows pk
- gets to see signatures on messages of his choice

can’t produce a verifiable signature on another message

Bitcoin uses ECDSA standard

Elliptic Curve Digital Signature Algorithm

relies on hairy math

will skip the details here --- look it up if you care

good randomness is essential

foul this up in generateKeys() or sign() ?

probably leaked your private key

Decentralized identity management

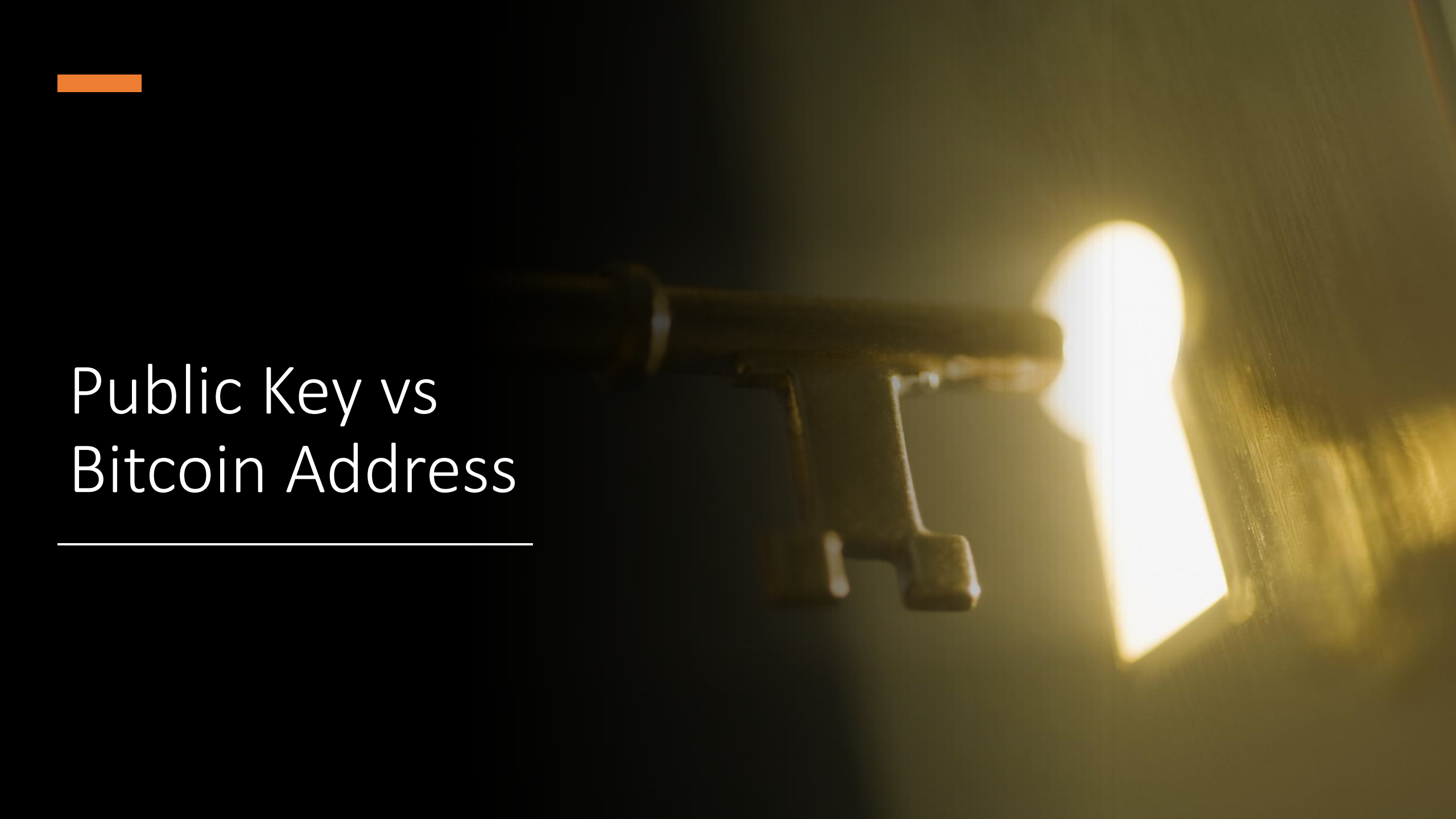
anybody can make a new identity at any time

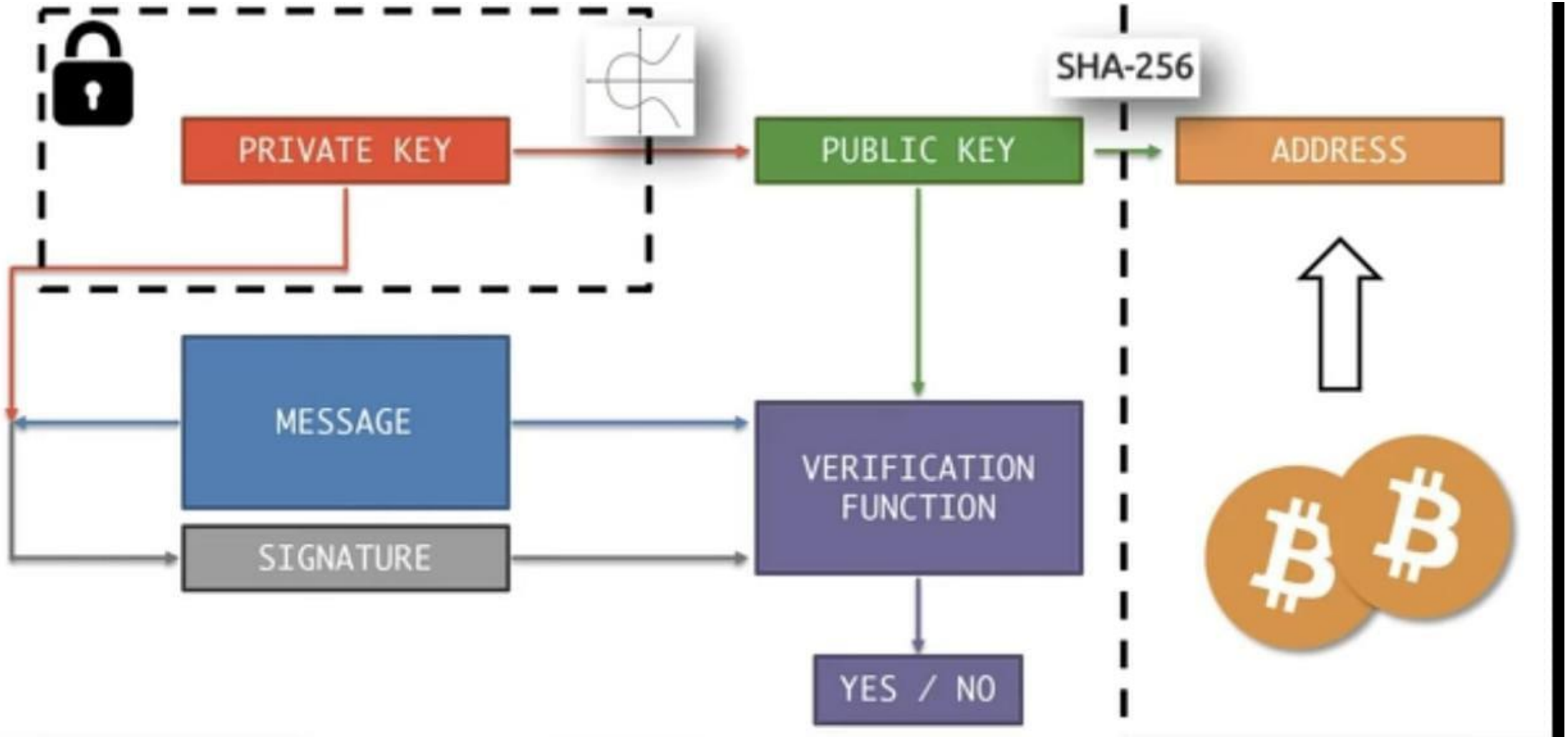
make as many as you want!

no central point of coordination

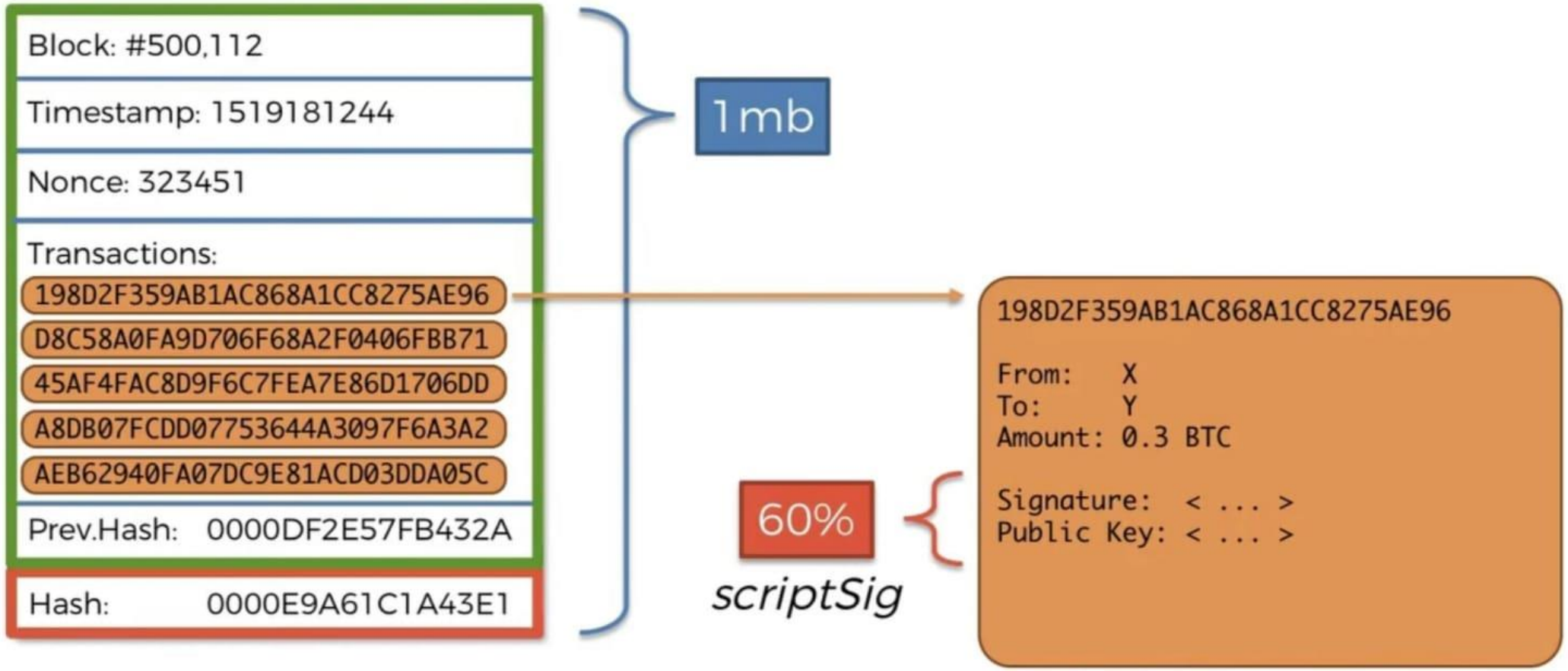
<u>These identities are called “addresses” in Bitcoin.</u>

Public Key vs Bitcoin Address



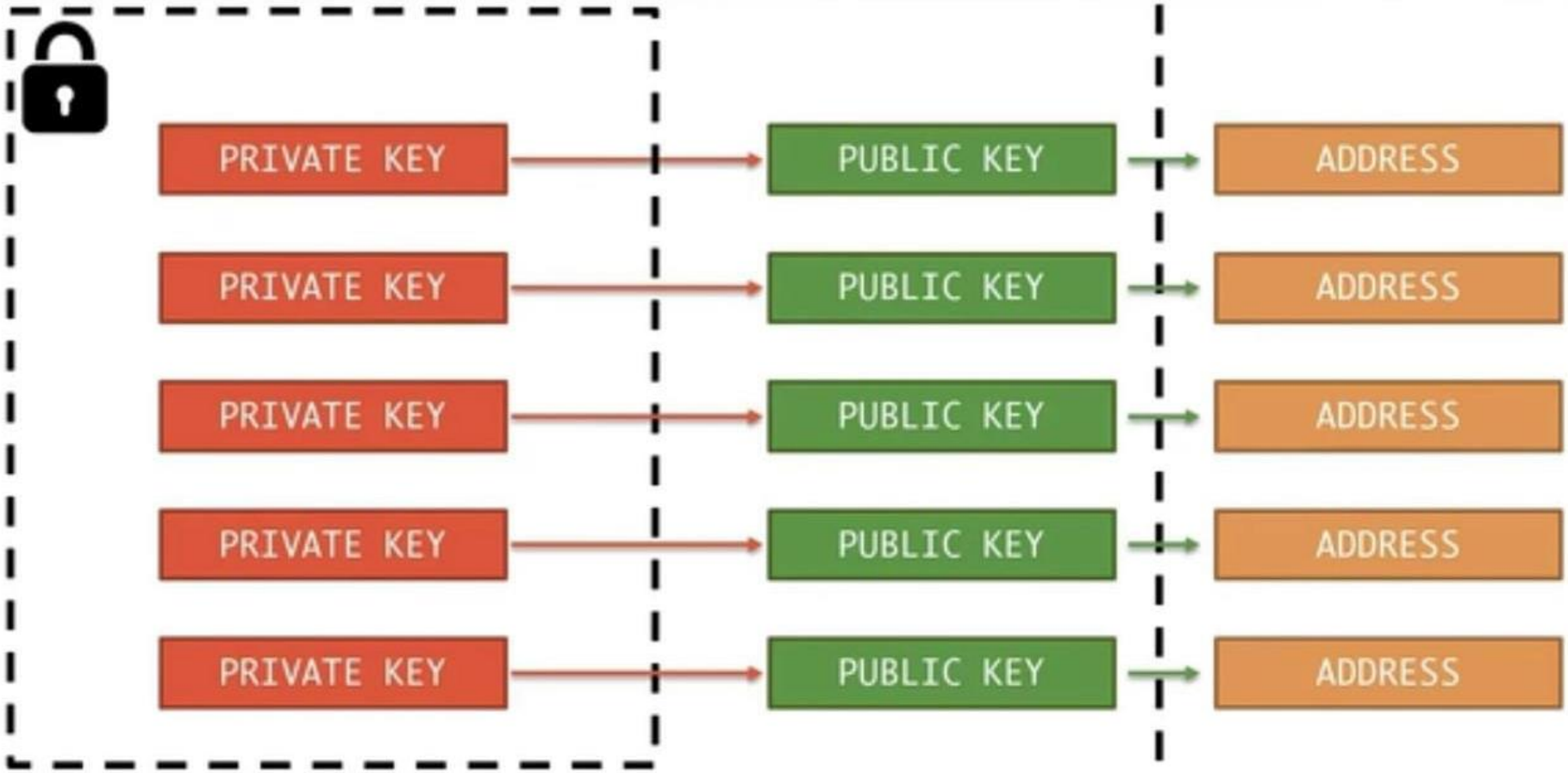

PRIVATE KEY
PUBLIC KEY
SHA-256
ADDRESS
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO

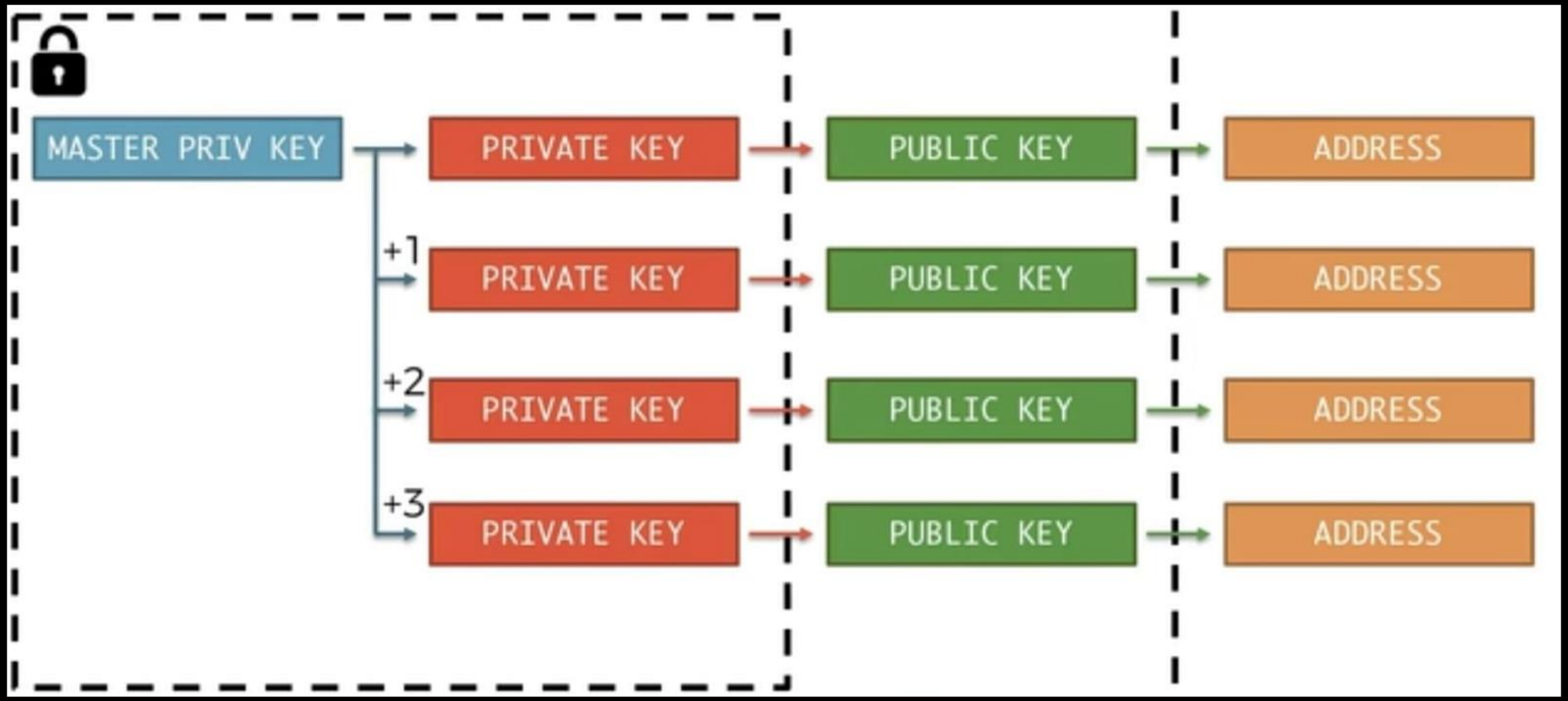
Segregated Witness (SegWit)

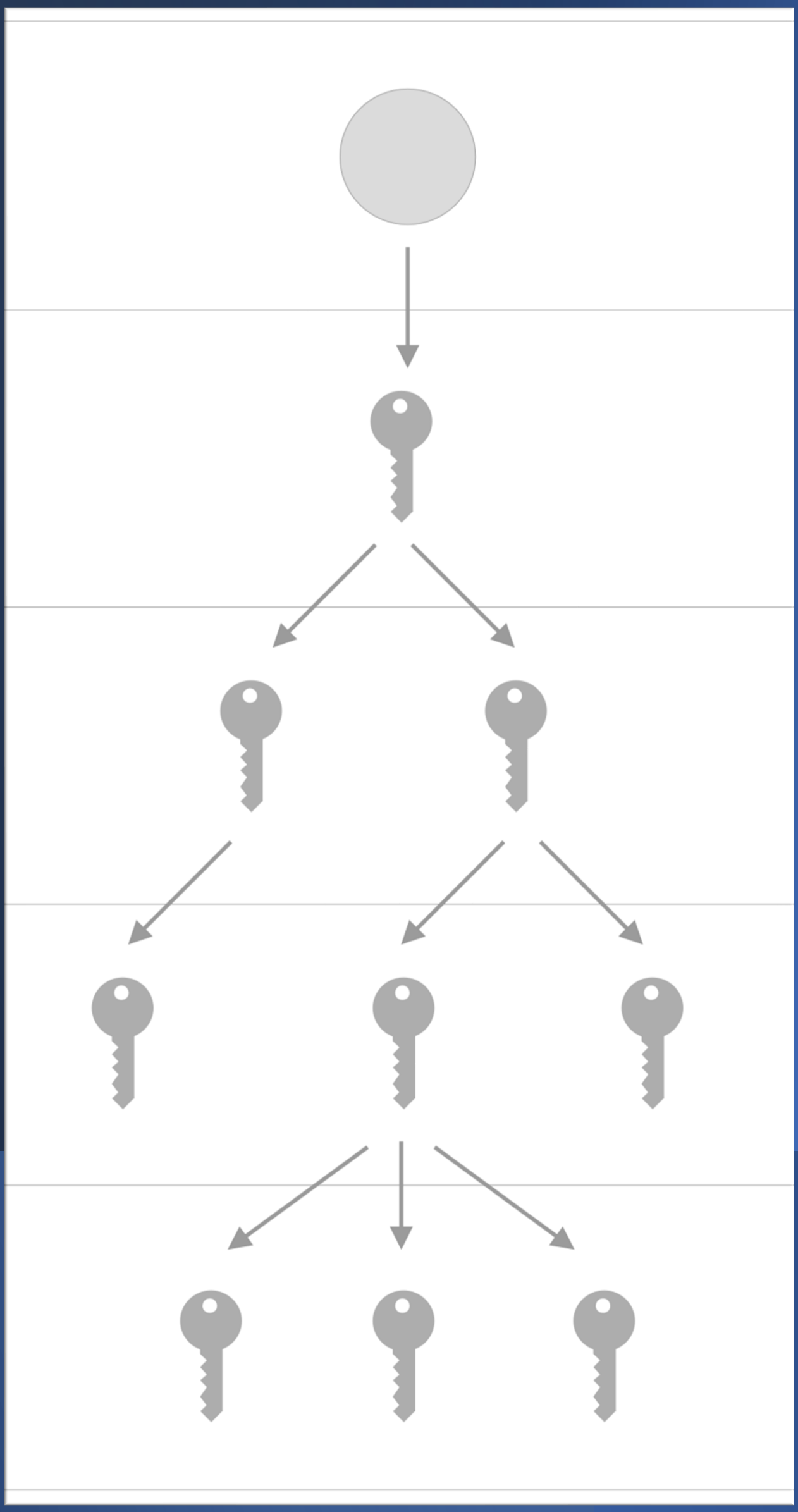

Block: #500,112
Timestamp: 1519181244
Nonce: 323451
Transactions:
198D2F359AB1AC868A1CC8275AE96
D8C58A0FA9D706F68A2F0406FBB71
45AF4FAC8D9F6C7FEA7E86D1706DD
A8DB07FCDD07753644A3097F6A3A2
AEB62940FA07DC9E81ACD03DDA05C
Prev.Hash: 0000DF2E57FB432A
Hash: 0000E9A61C1A43E1
1mb
198D2F359AB1AC868A1CC8275AE96
From: X
To: Y
Amount: 0.3 BTC
Signature: < ... >
Public Key: < ... >
60%
scriptSig

HD(Hierarchically Deterministic) Wallets

Multiple private-public keys for security purpose




MASTER PRIV KEY
+1
+2
+3
PRIVATE KEY
PRIVATE KEY
PRIVATE KEY
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY
PUBLIC KEY
PUBLIC KEY
ADDRESS
ADDRESS
ADDRESS
ADDRESS



Additional Reading

DETERMINISTIC WALLETS, THEIR ADVANTAGES AND THEIR UNDERSTATED FLAWS

https://bitcoinmagazine.com/technical/deterministic-wallets-advantages-flaw-1385450276

Acknowledgement and Source:

- https://www.udemy.com/course/build-your-blockchain-az/