Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari


How Wallets Work

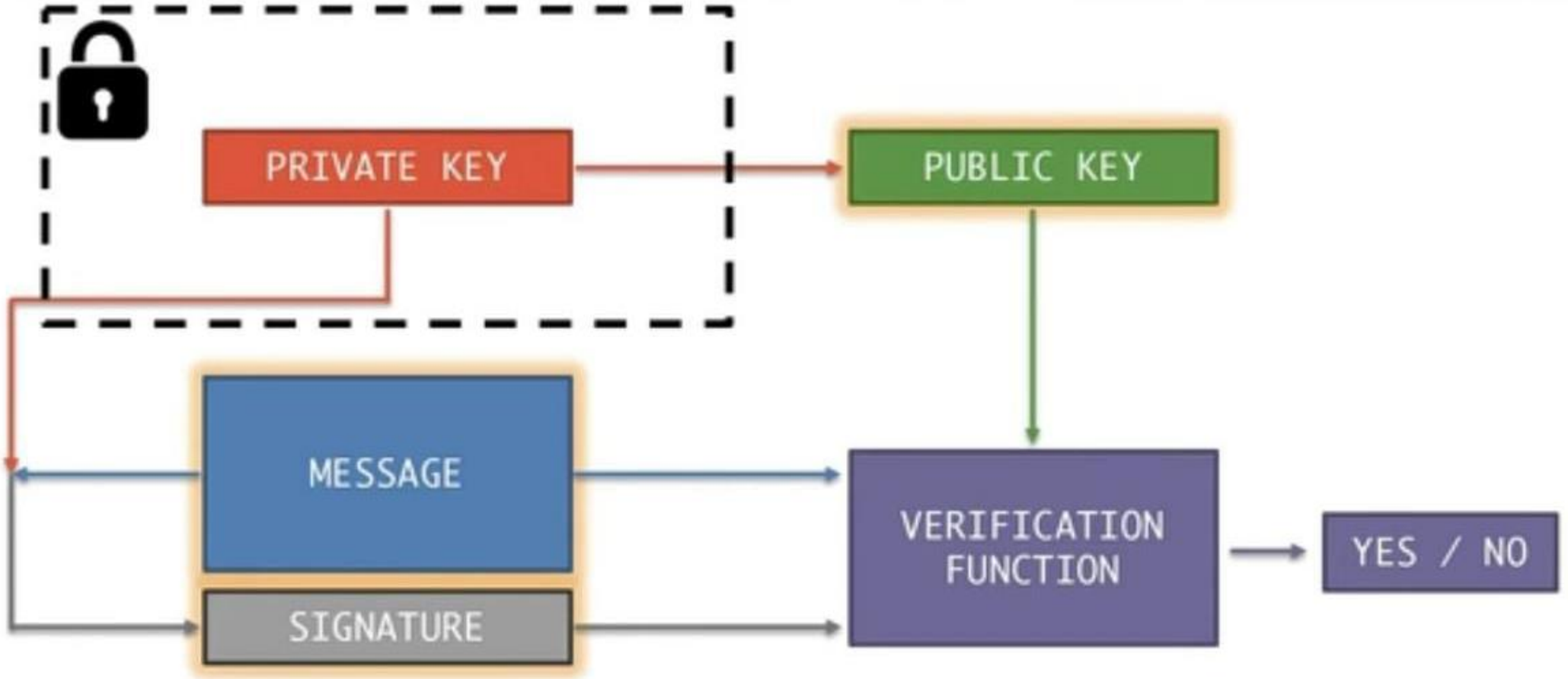
Signatures: Private & Public Keys

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)

isValid := verify(pk, message, sig)

can be randomized algorithms

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

These identities are called “addresses” in Bitcoin.

Acknowledgement and Source:

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