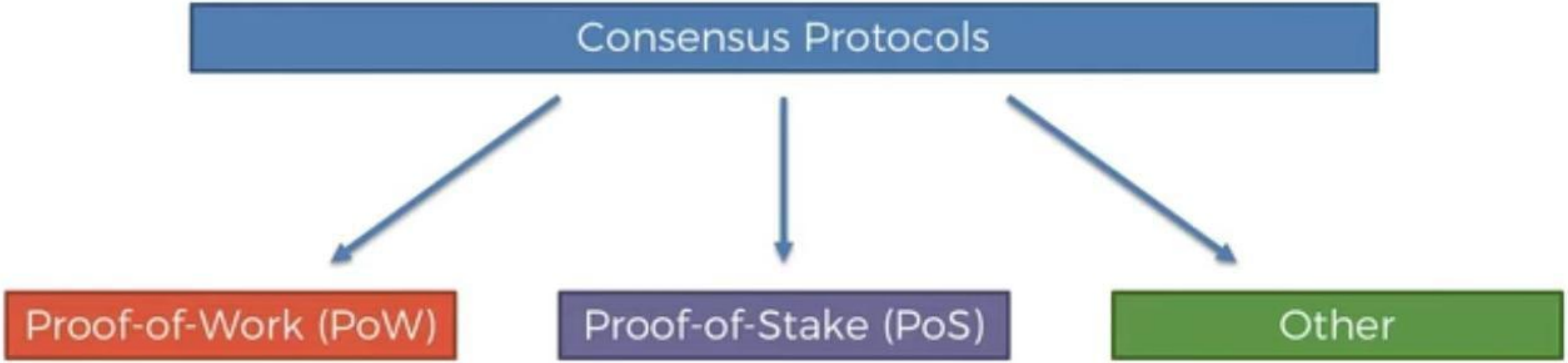
Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari



Consensus Protocols

Proof-of-Work (PoW)

Proof-of-Stake (PoS)

Other

Bitcoin Consensus Algorithm

Consensus algorithm (simplified)

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Incentive for miners

Incentive 1: block reward

Creator of block gets to

- include special coin-creation transaction in the block
- choose recipient address of this transaction

Value is fixed: currently 12.5 BTC, halves every 4 years

Block creator gets to "collect" the reward only if the block ends up on long-term consensus branch!

Incentive 2: transaction fees

Creator of transaction can choose to make output value less than input value

Remainder is a transaction fee and goes to block creator

Purely voluntary, like a tip

Proof of Work

Consensus protocol used by Bitcoin

Equivalent views of proof of work

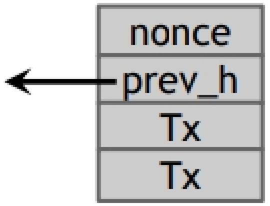
1. Select nodes in proportion to computing power

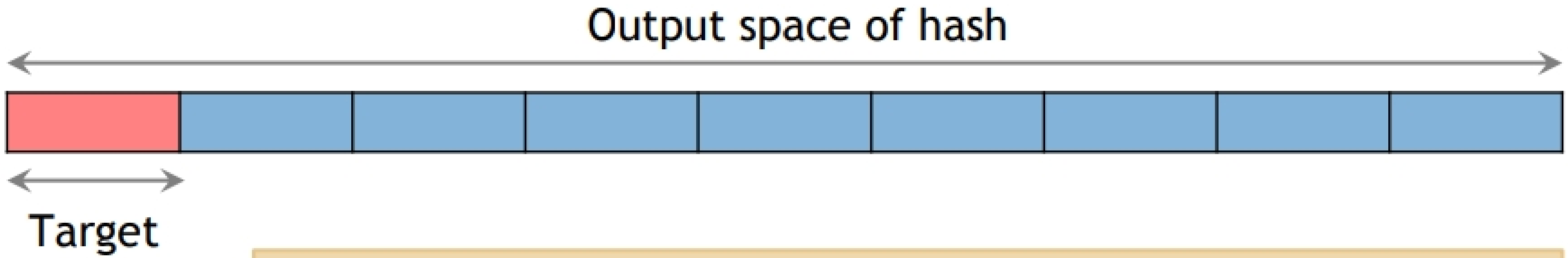
1. Let nodes compete for right to create block

1. Make it moderately hard to create new identities

Hash puzzles

To create block, find nonce s.t.
H(nonce || prev_hash || tx || … || tx) is very small





If hash function is secure:
only way to succeed is to try enough nonces until you get lucky

PoW property 1: difficult to compute

As of Aug 2014: about 10^{20} hashes/block

Only some nodes bother to compete — miners

PoW property 2: parameterizable cost

Nodes automatically re-calculate the target every two weeks

Goal: average time between blocks = 10 minutes

PoW property 3: trivial to verify

Nonce must be published as part of block

Mining economics

If mining reward (block reward + Tx fees)	>	hardware + electricity cost	→	Profit

Complications:

- fixed vs. variable costs
- reward depends on global hash rate

How Wallets Work

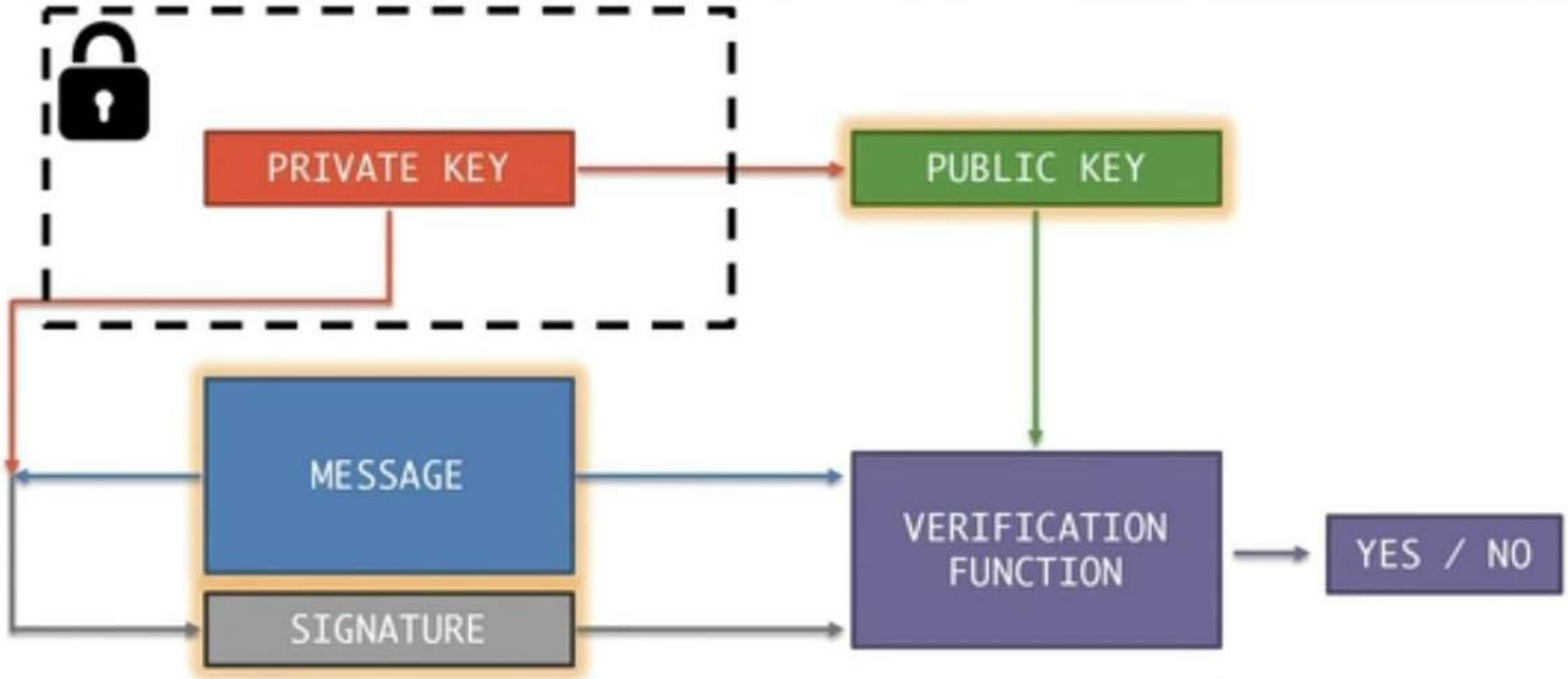
Signatures: Private & Public Keys

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)

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 <u>ECDSA</u> 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

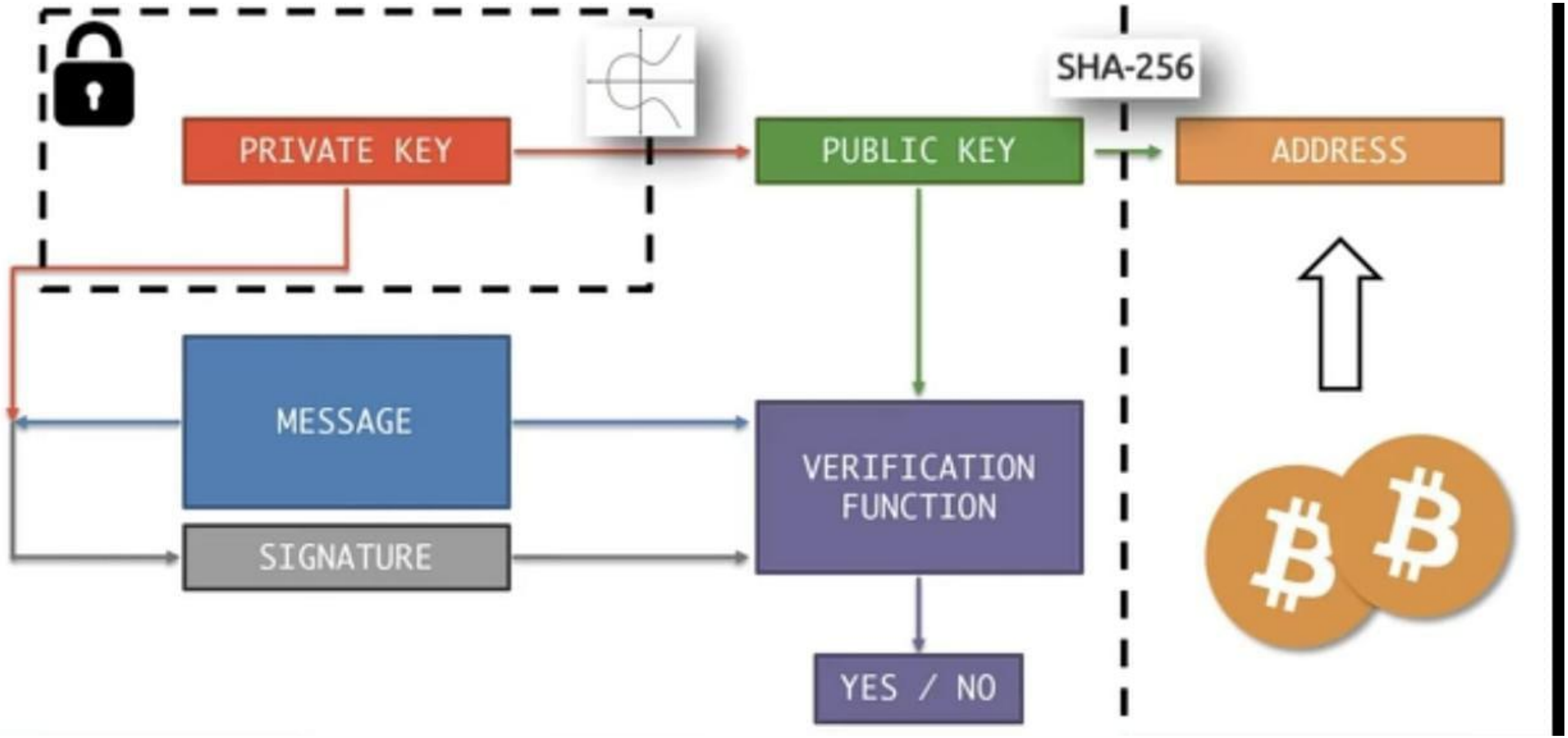
anybody can make a new identity at any time

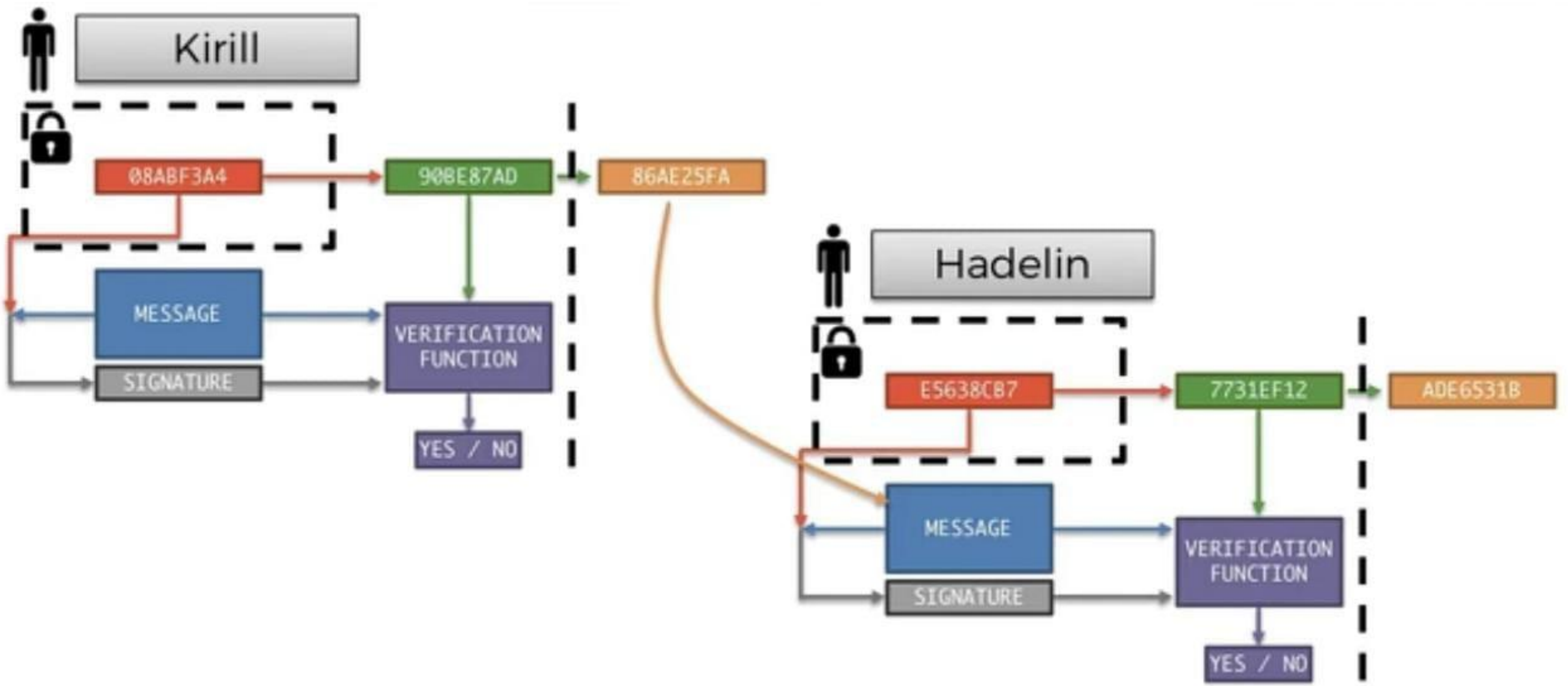
- make as many as you want!

no central point of coordination

These identities are called “addresses” in Bitcoin.

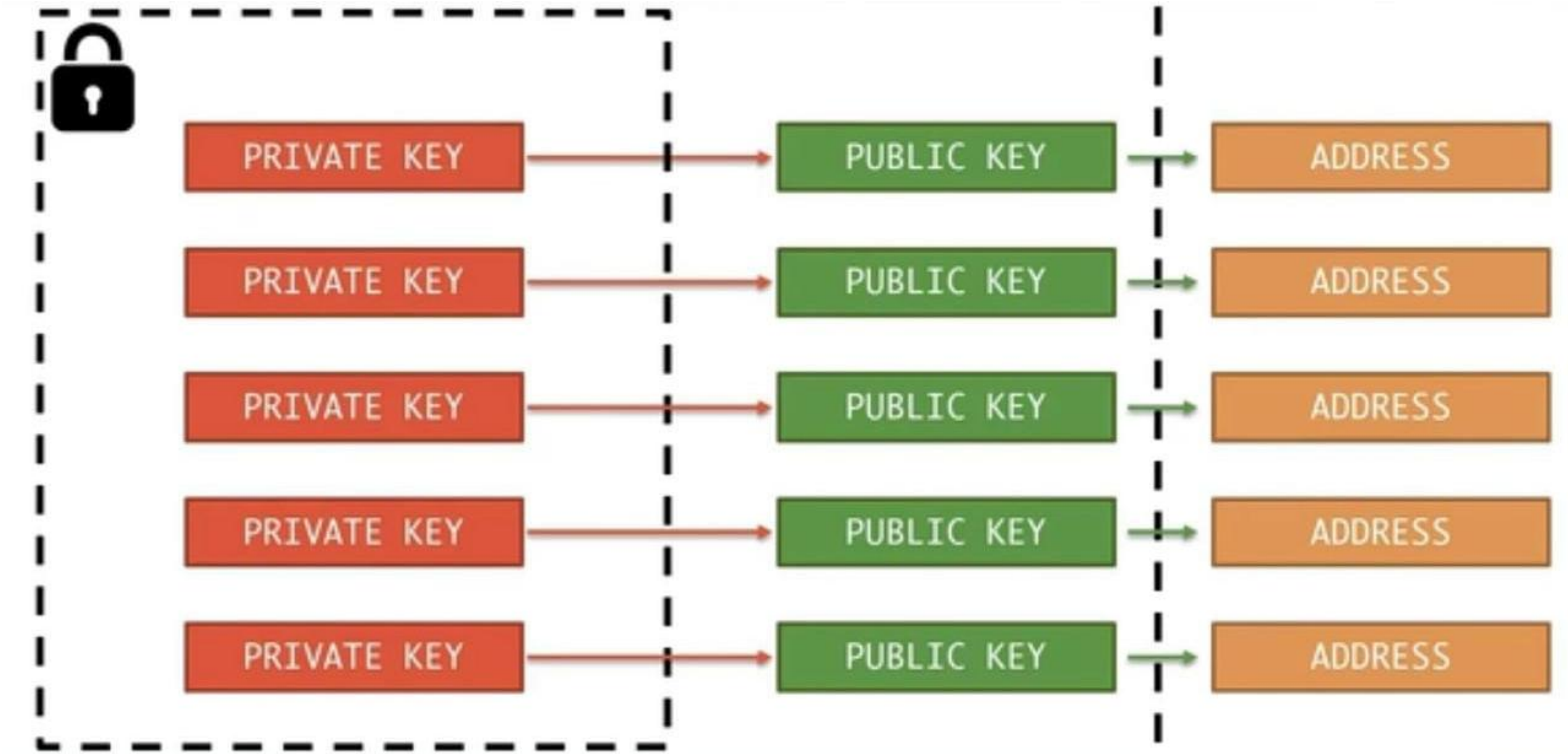
Public Key vs Bitcoin Address

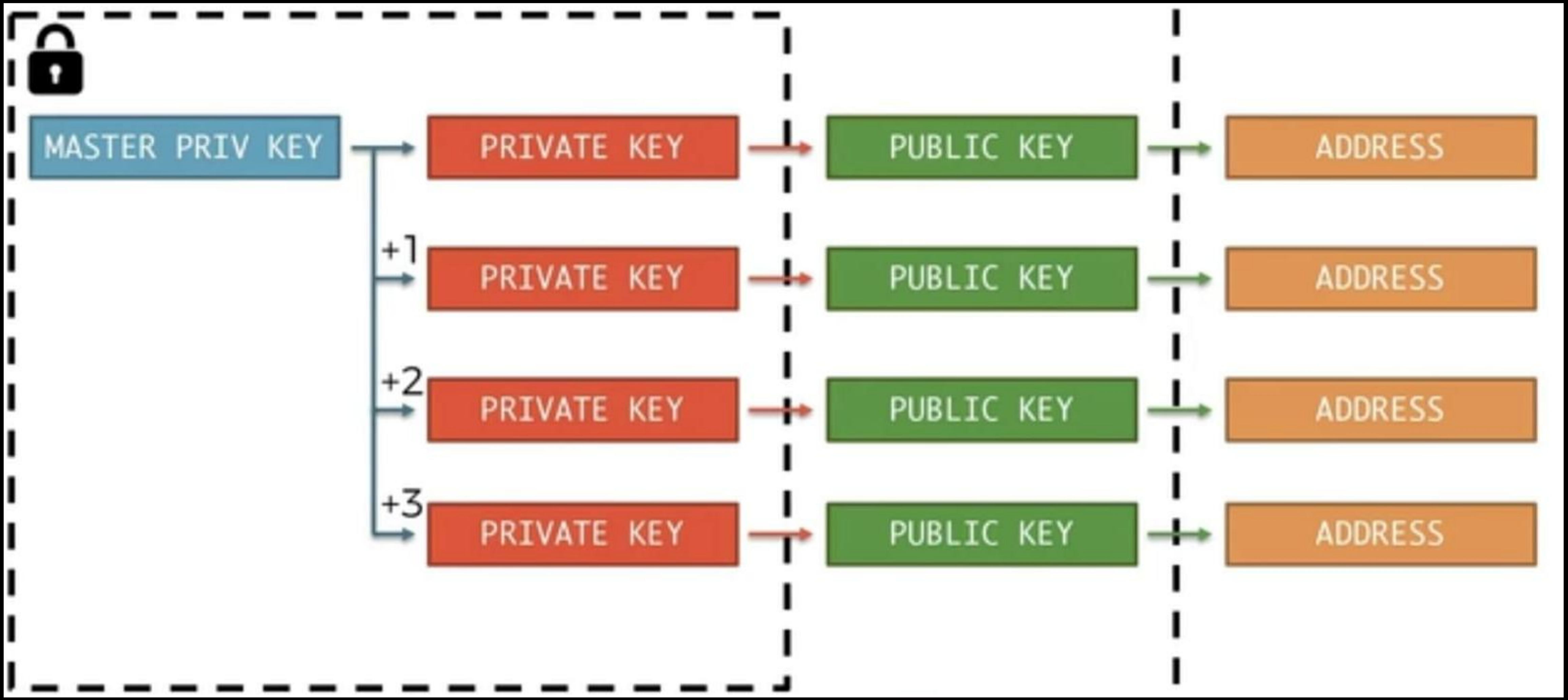

SHA-256
PRIVATE KEY
PUBLIC KEY
ADDRESS
MESSAGE
VERIFICATION FUNCTION
SIGNATURE
YES / NO

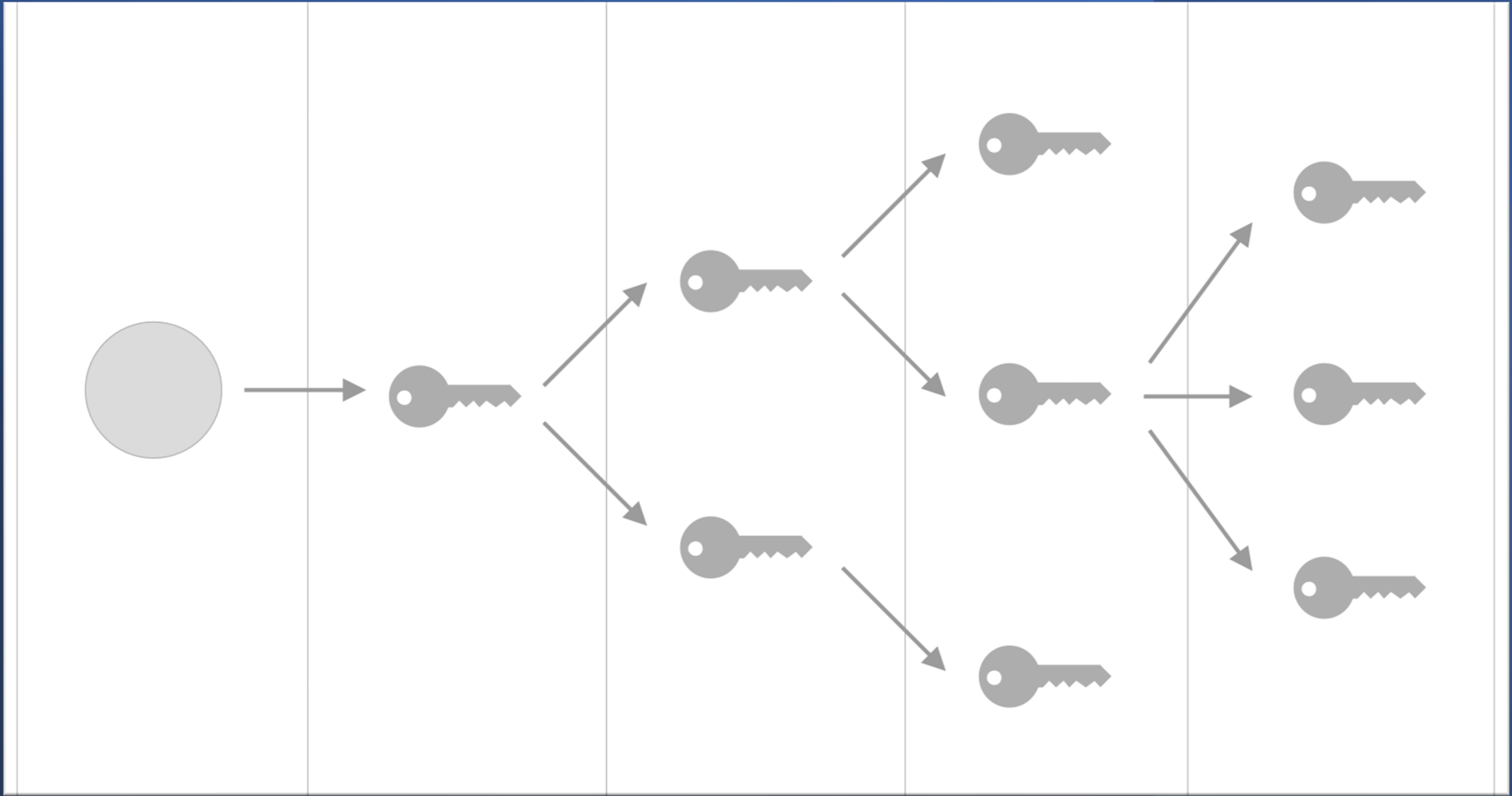

Kirill
08ABF3A4
90BE87AD
86AE25FA
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO
Hadelin
E5638CB7
7731EF12
ADE6531B
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO

HD(Hierarchically Deterministic) Wallets

Multiple private-public keys for security purpose




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