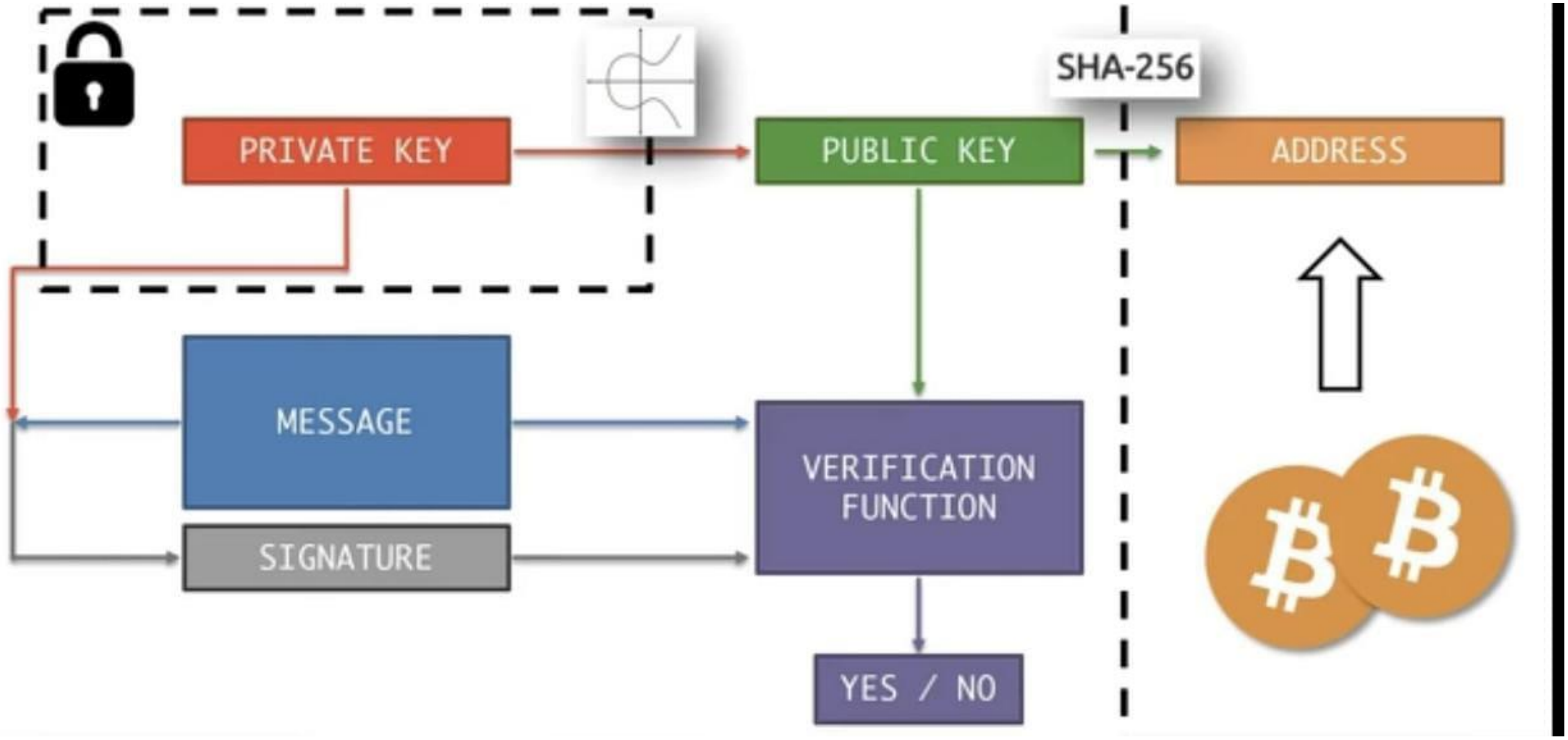
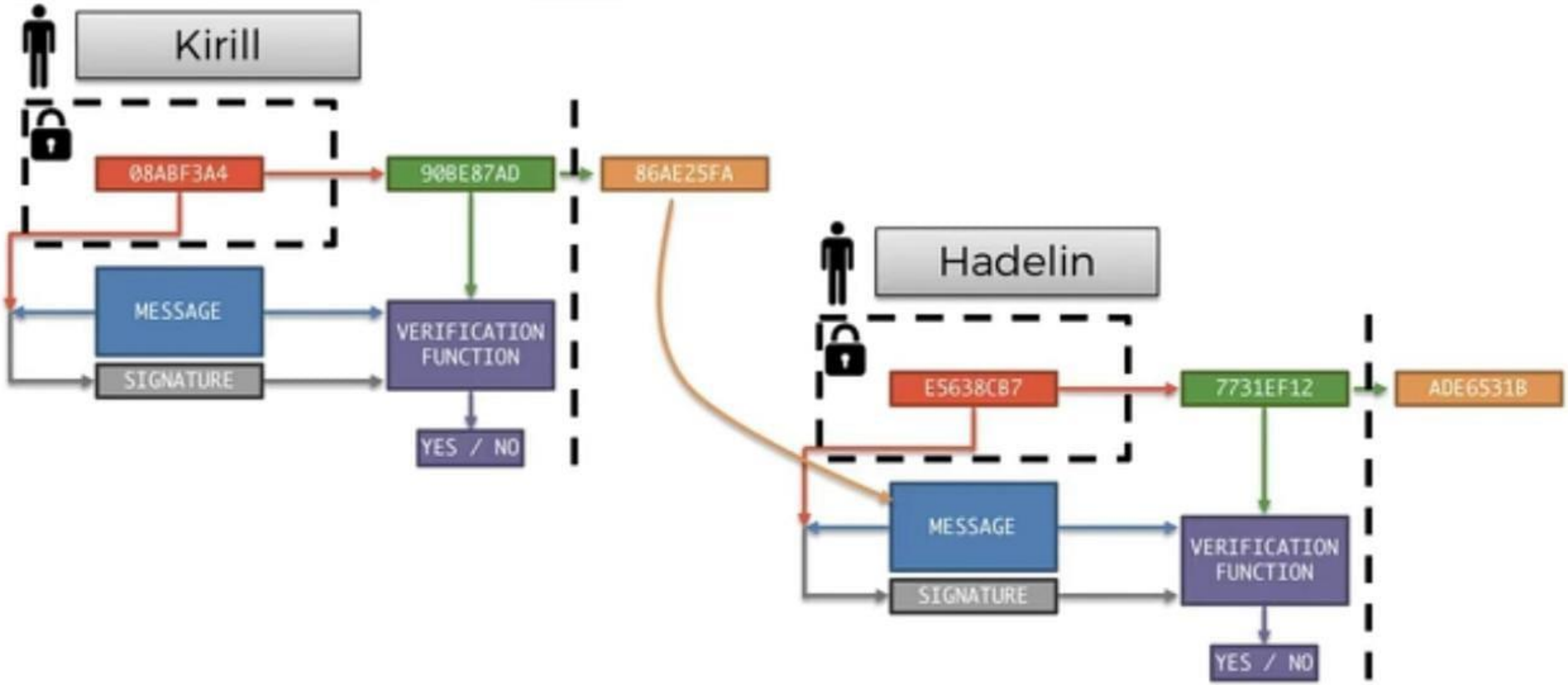
Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

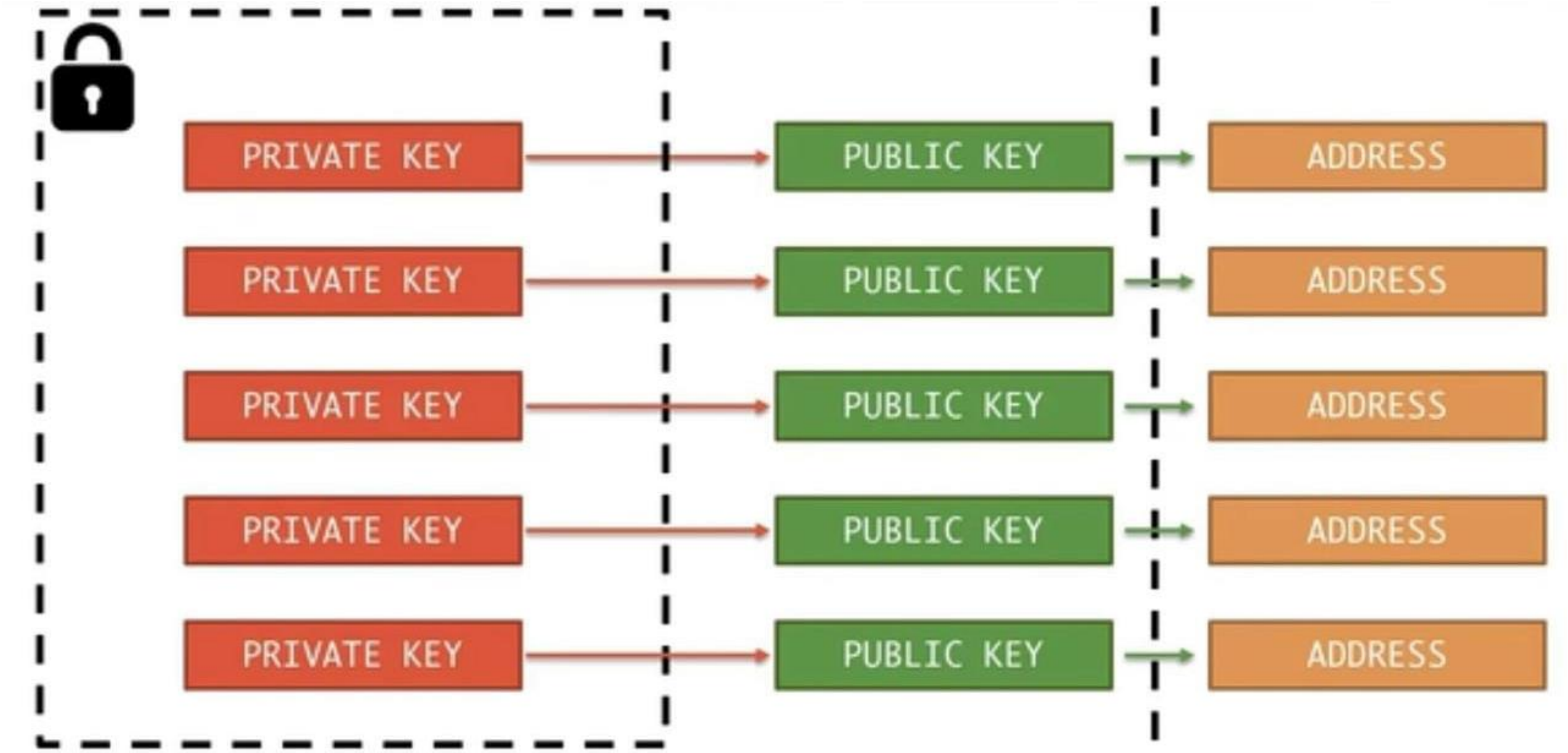
Public Key vs Bitcoin Address

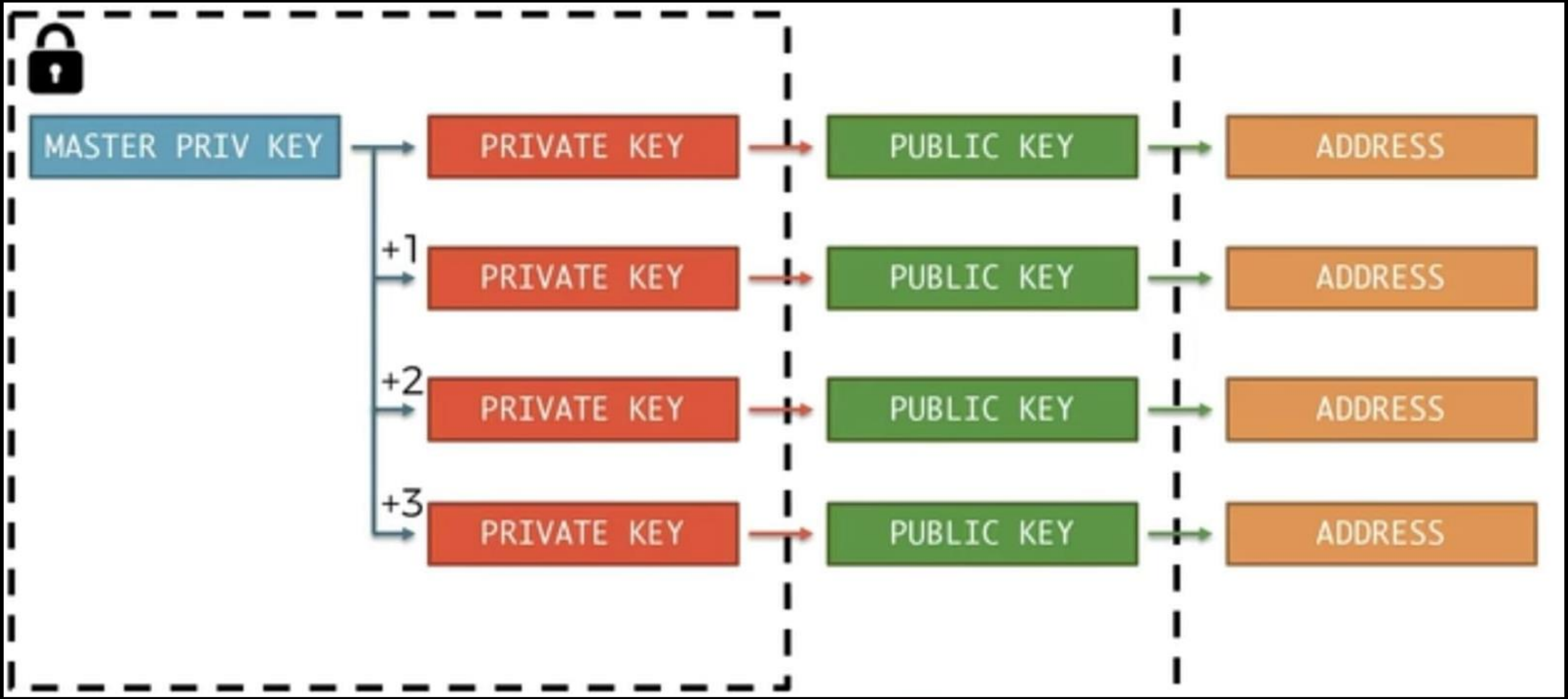

PRIVATE KEY
PUBLIC KEY
SHA-256
ADDRESS
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO

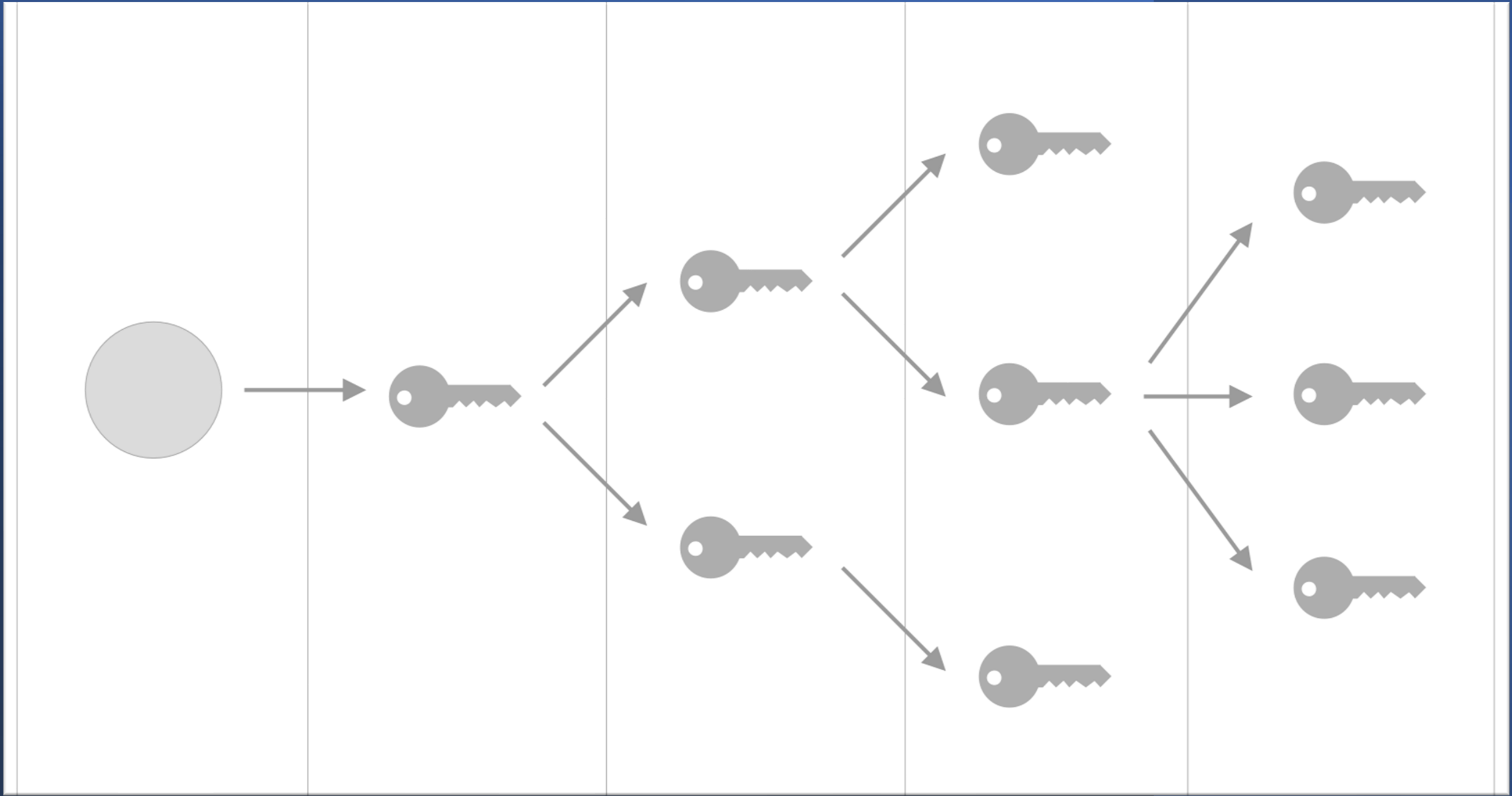

Kirill
08ABF3A4
90BE87AD
86AE25FA
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO
Hadelin
E5638CB7
7731EF12
ADE6531B
MESSAGE
SIGNATURE
VERIFICATION FUNCTION
YES / NO

HD(Hierarchically Deterministic) Wallets

Multiple private-public keys for security purpose




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

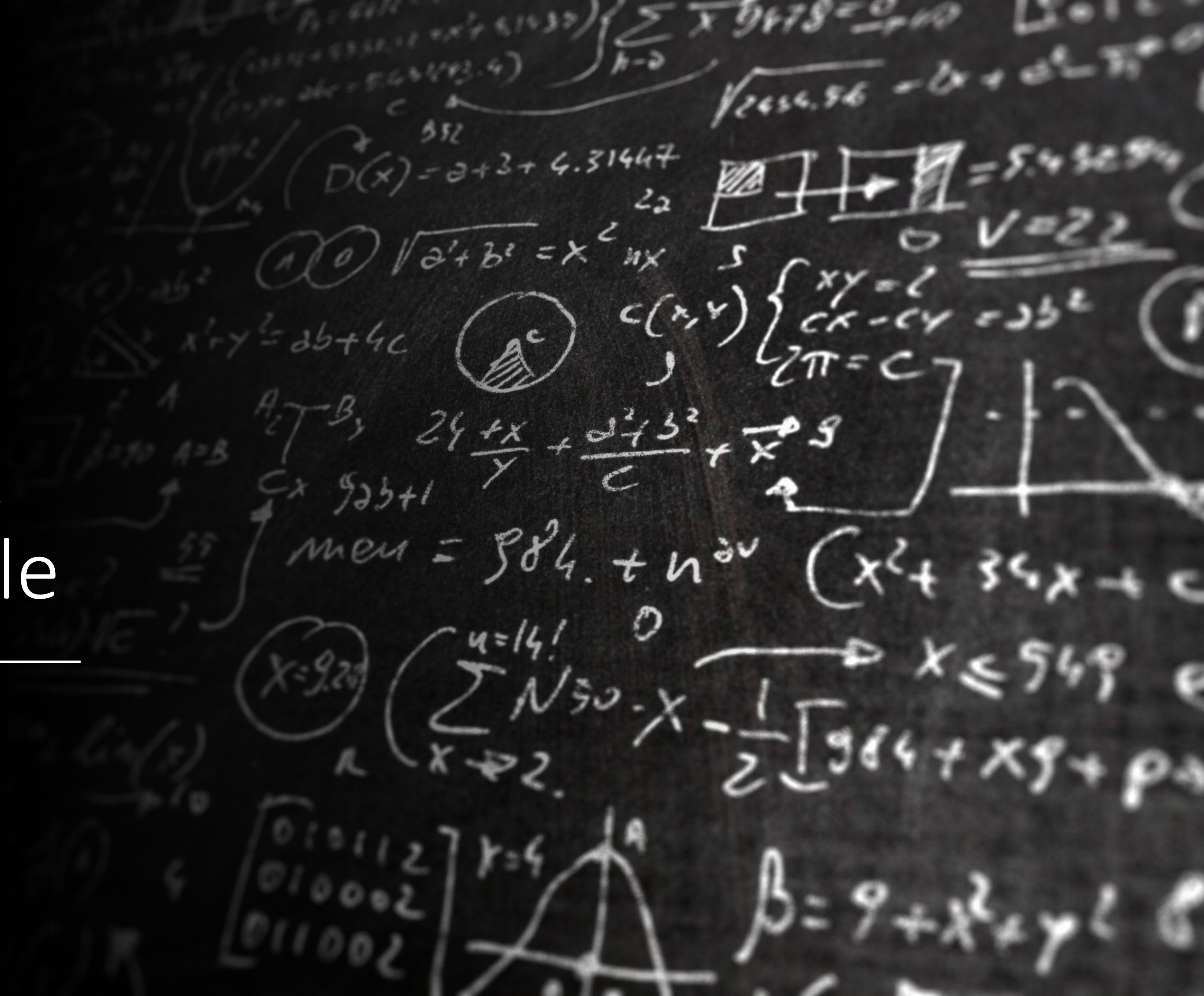


Additional Reading

DETERMINISTIC WALLETS, THEIR ADVANTAGES AND THEIR UNDERSTATED FLAWS

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

Plan of Attack of next Module



- What is Ethereum?
- What is a Smart Contract?
- Decentralized Applications (Dapps)
- Ethereum Virtual Machine & Gas
- Decentralized Autonomous Organizations (DAOs)
- The DAO Attack
- Soft and Hard Forks
- Initial Coin Offerings (ICOs)
- ICO Case Study
- Blockchain Startups: White Papers

What is Ethereum?

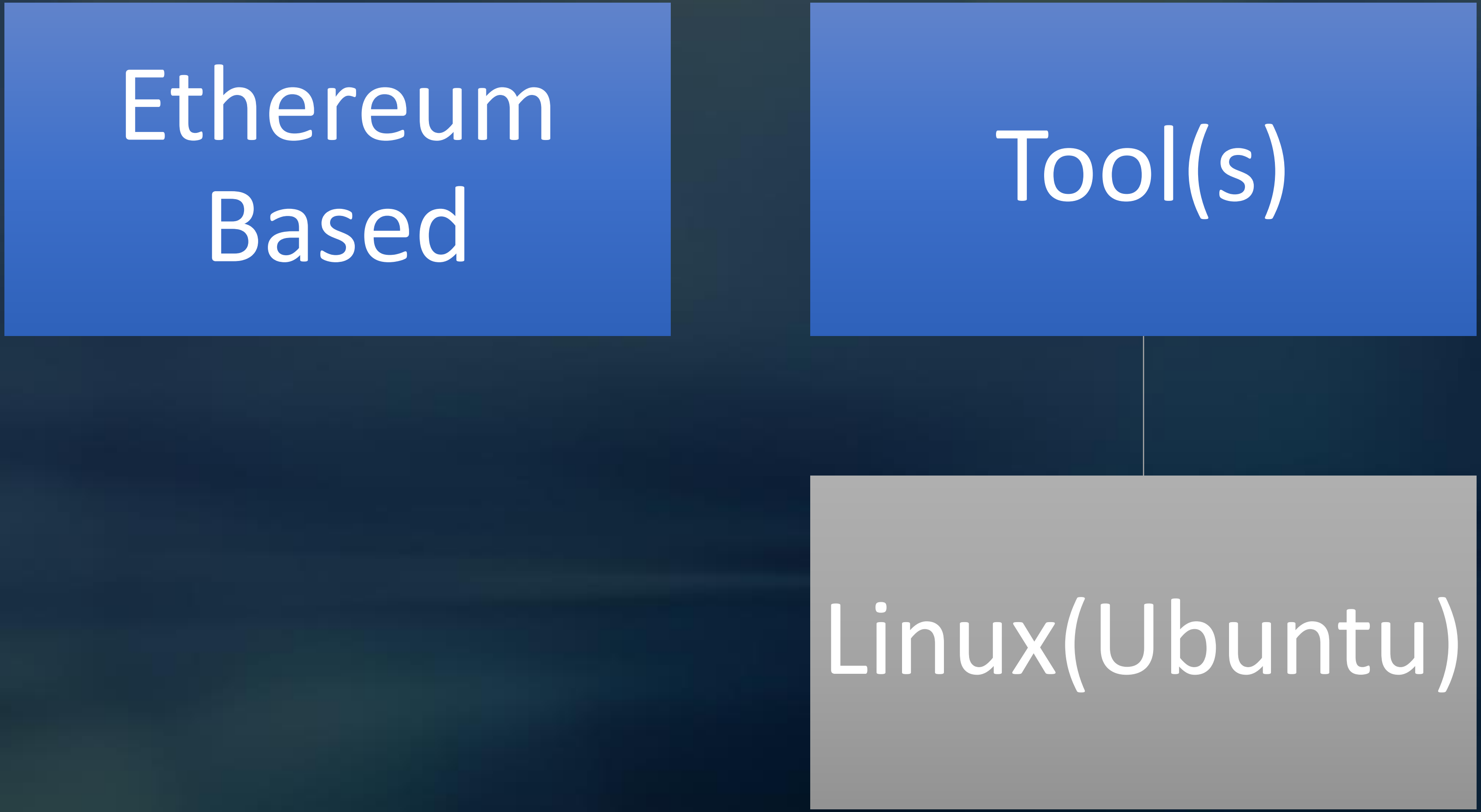
Ethereum: project created by:

Vitalik Buterin

Scripting language used by Ethereum: Solidity

Scripting Language: way to create programs using bitcoin

Regarding Assignment 2:



Ethereum Based

Tool(s)

Linux(Ubuntu)

Acknowledgement and Source:

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