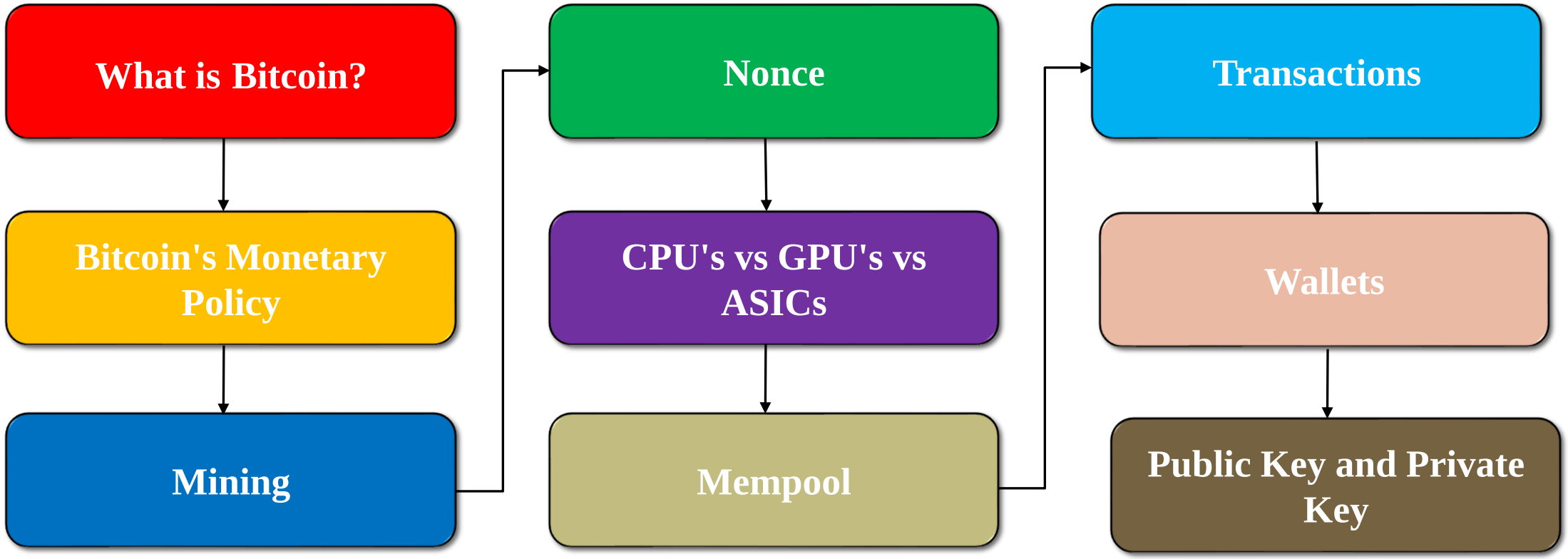
Blockchain

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.

Cryptocurrency

Contents – Module B

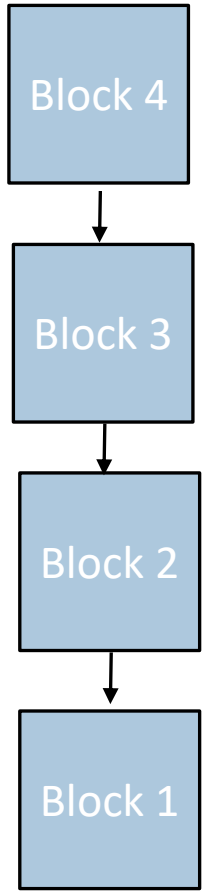


Cryptocurrency Wallet

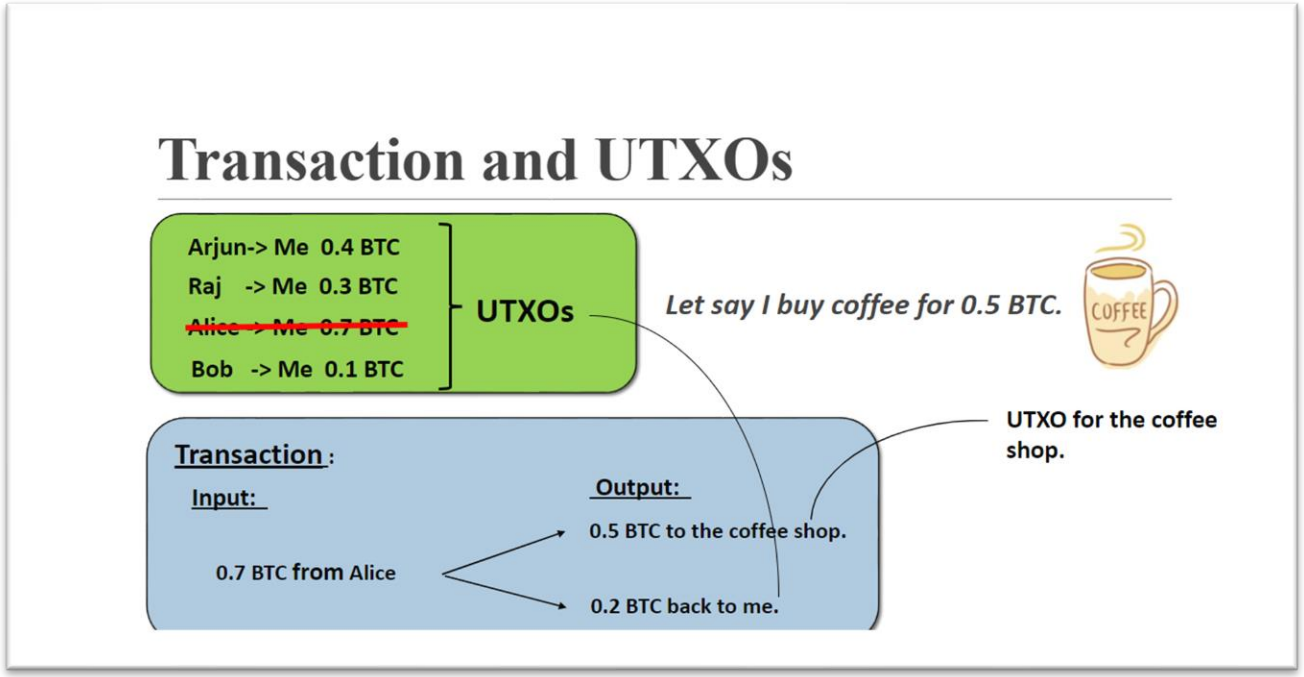
Cryptocurrency Wallets

- A wallet (device or program) stores cryptocurrency keys and allows one to access coins
- Public key is used as a wallet address and for receiving the coins
- Private key is needed to sign transactions and for sending the coins
- Just like Blockchain a wallet is also distributed
- Not storing the balance, computes the balance from the transactions UTXOs
- Wallet note down those transactions that are coming to the wallet, add the transactions' amounts and show it as a balance

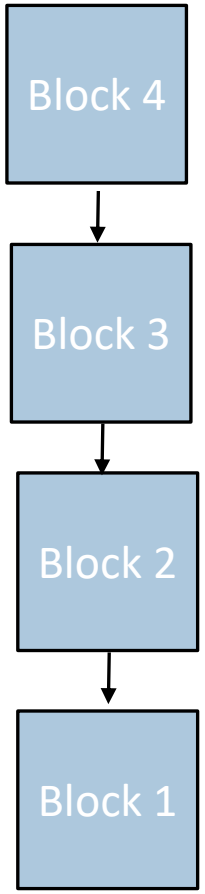
Cryptocurrency Wallets



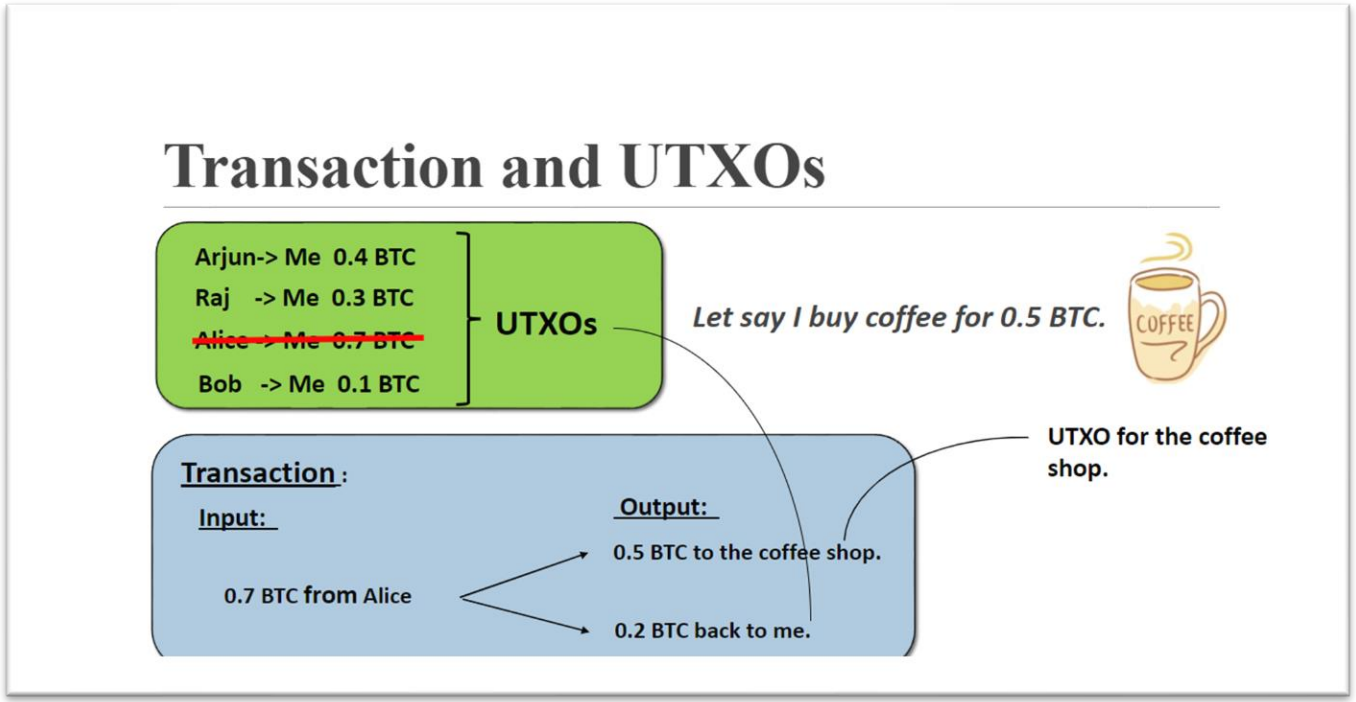
Me->coffee shop	**0.5 BTC**
Me->Me	**0.2 BTC**
Arjun-> Me	**0.4 BTC**
Raj -> Me	**0.3 BTC**
Alice -> Me	**0.7 BTC**
Bob -> Me	**0.1 BTC**



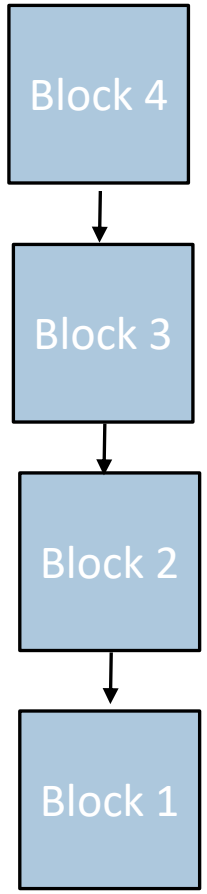
Cryptocurrency Wallets



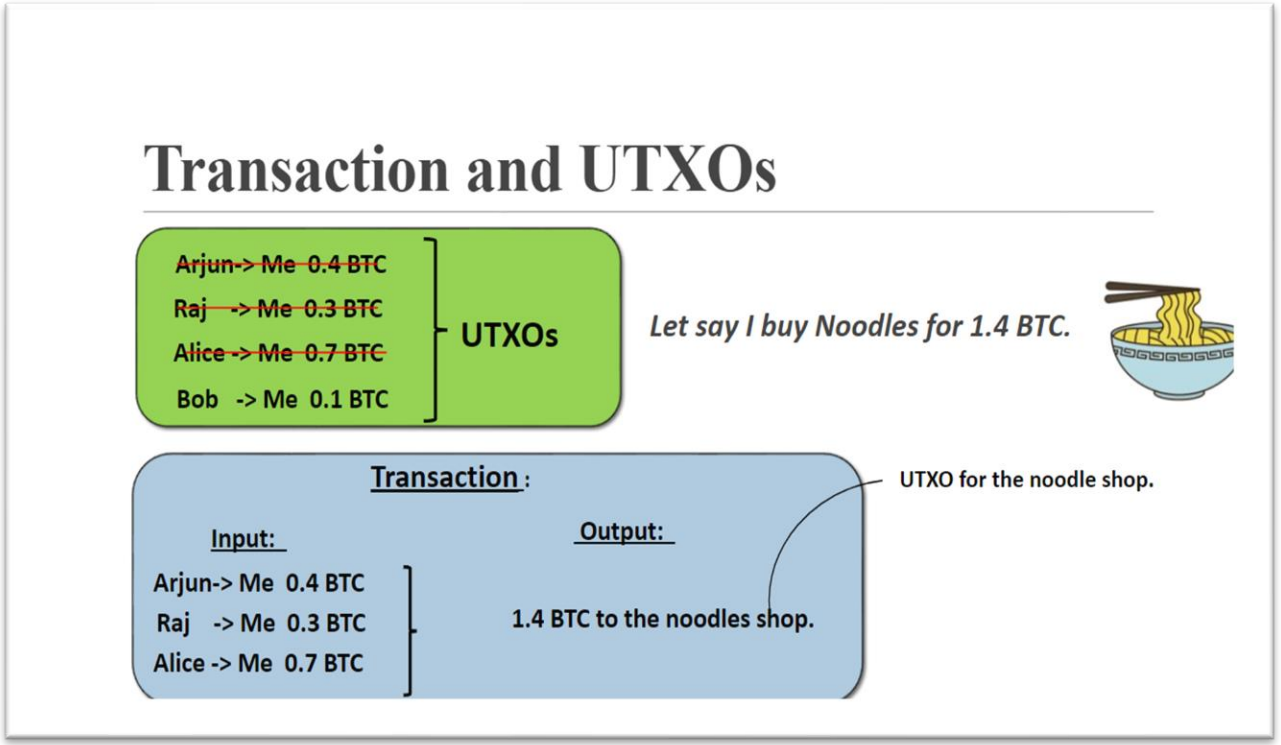
Me->coffee shop	0.5 BTC
Me->Me	0.2 BTC
Arjun-> Me	0.4 BTC
Raj -> Me	0.3 BTC
Alice -> Me	0.7 BTC
Bob -> Me	0.1 BTC



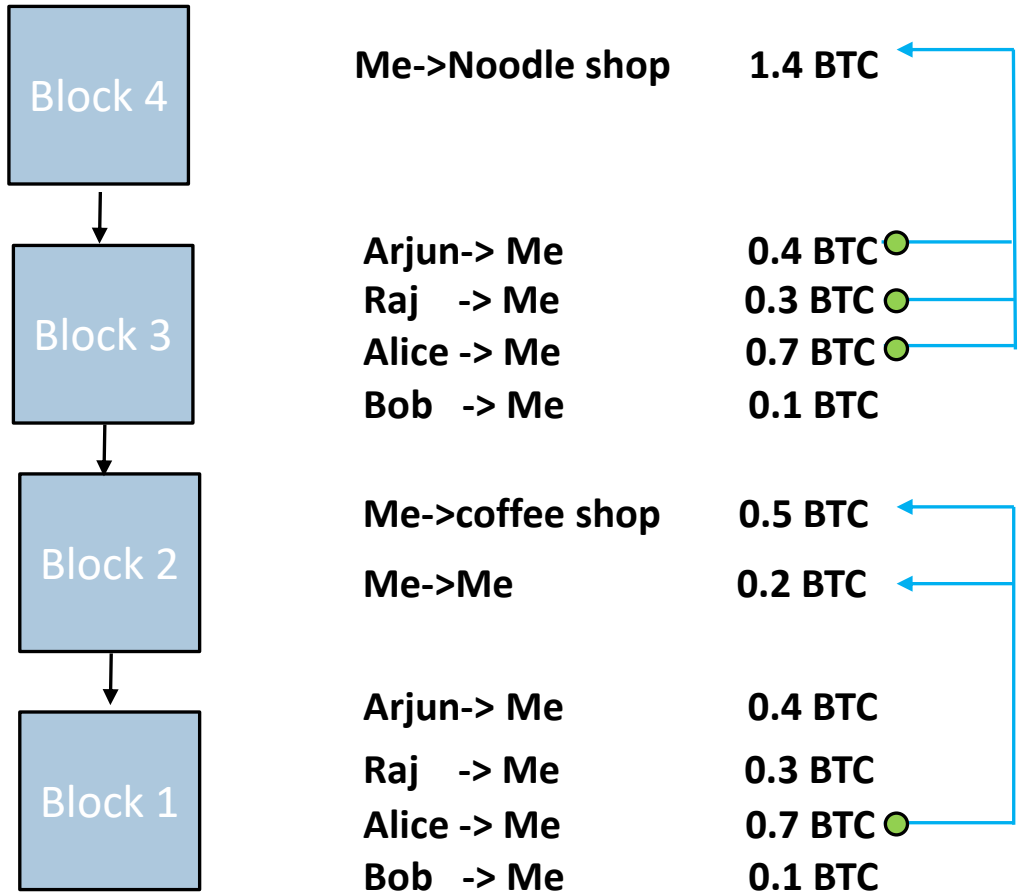
Cryptocurrency Wallets

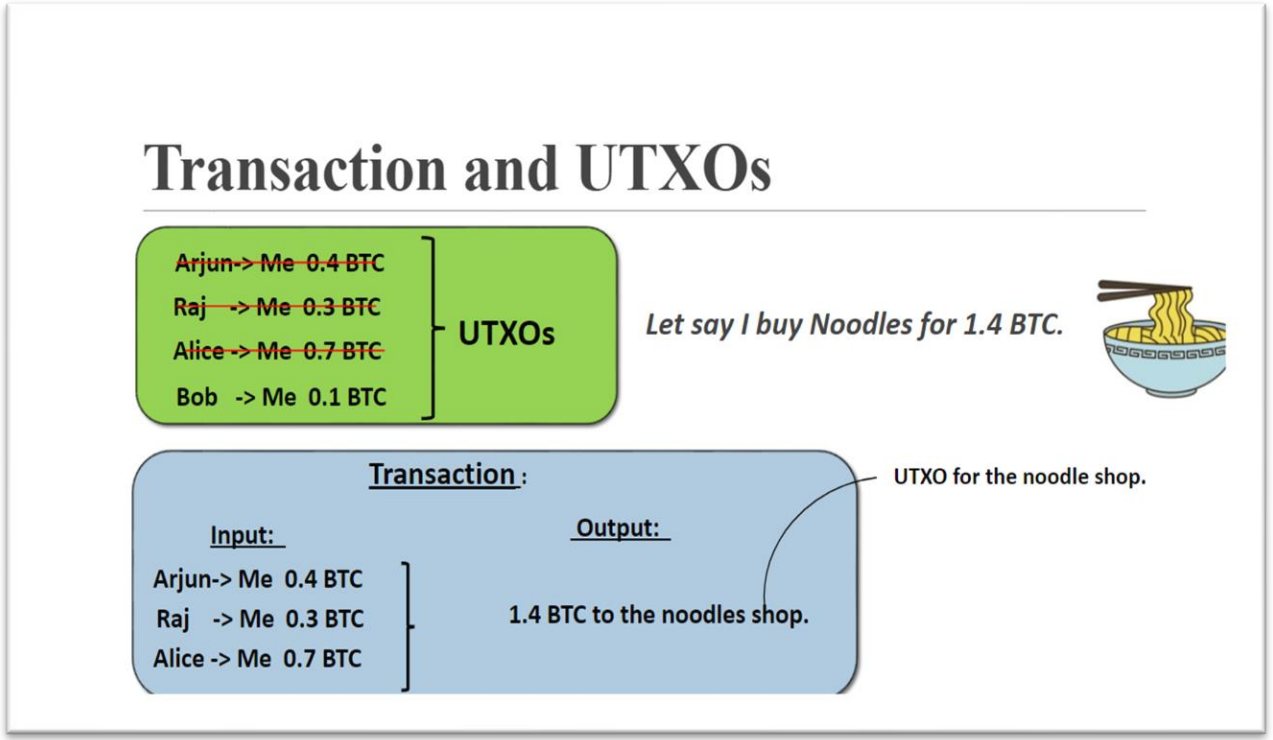


Me->Noodle shop	1.4 BTC
Arjun-> Me	0.4 BTC
Raj -> Me	0.3 BTC
Alice -> Me	0.7 BTC
Bob -> Me	0.1 BTC
Me->coffee shop	0.5 BTC
Me->Me	0.2 BTC
Arjun-> Me	0.4 BTC
Raj -> Me	0.3 BTC
Alice -> Me	0.7 BTC
Bob -> Me	0.1 BTC

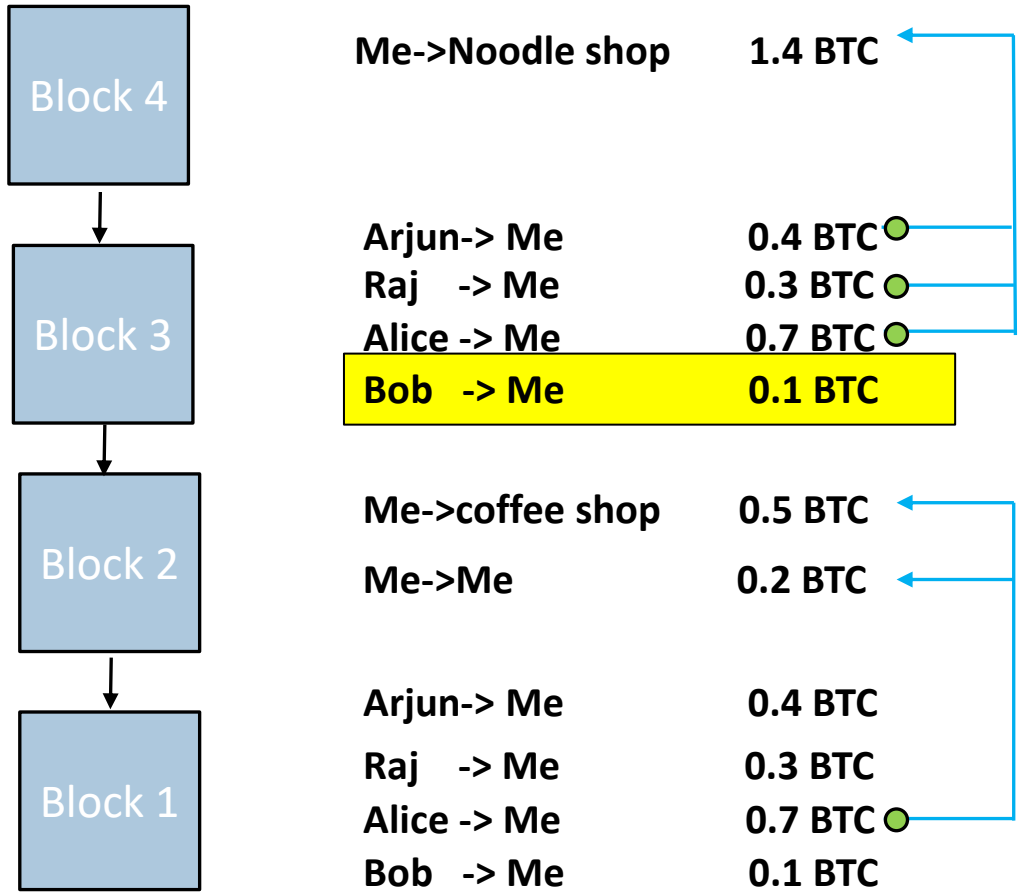


Cryptocurrency Wallets

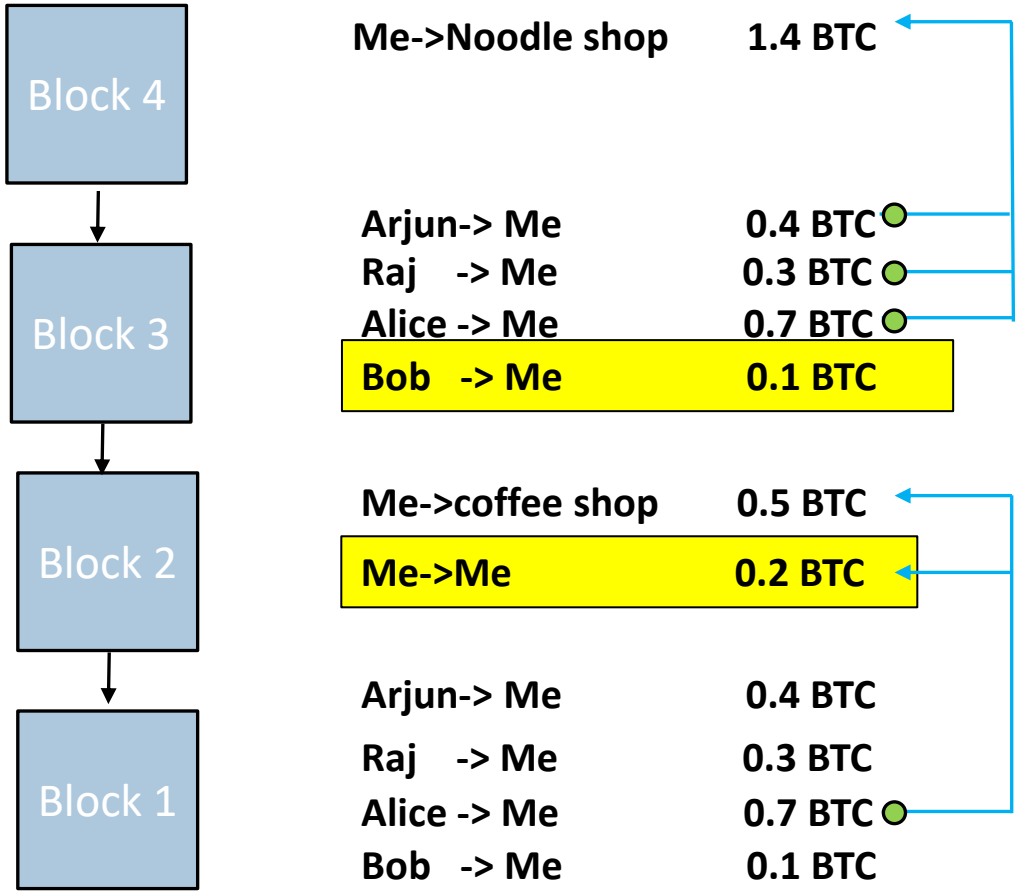




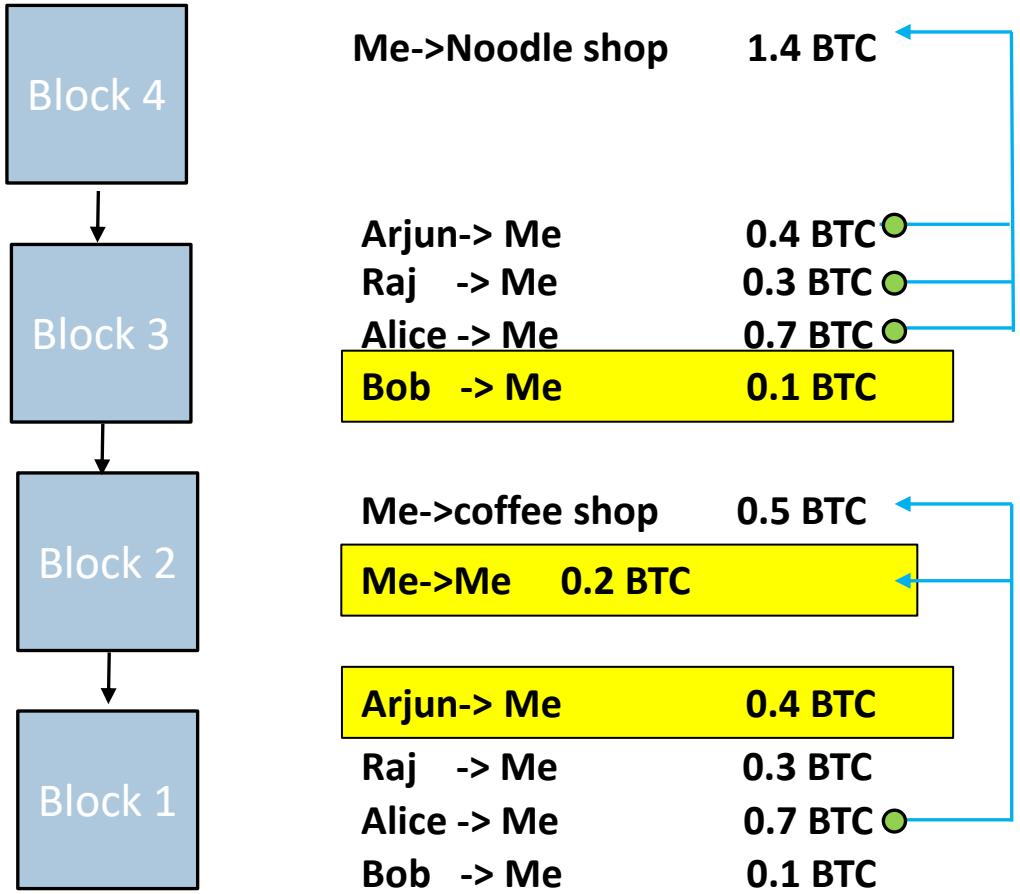
Cryptocurrency Wallets



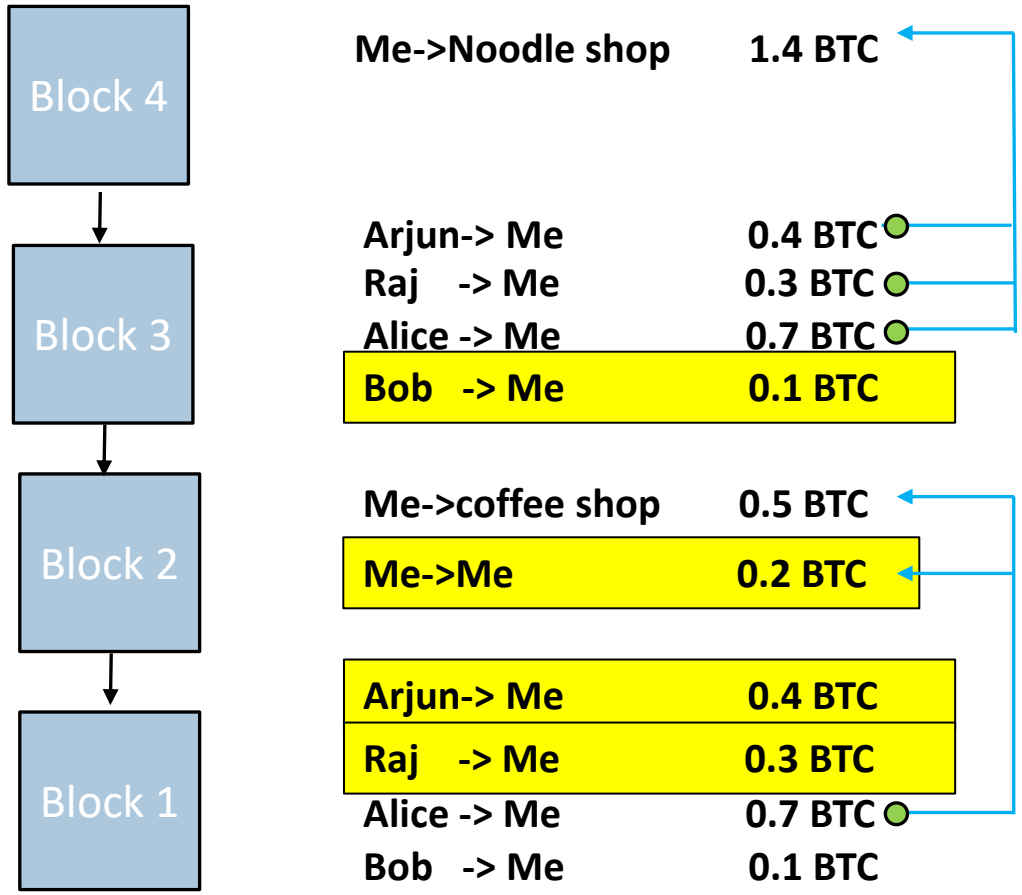
Cryptocurrency Wallets



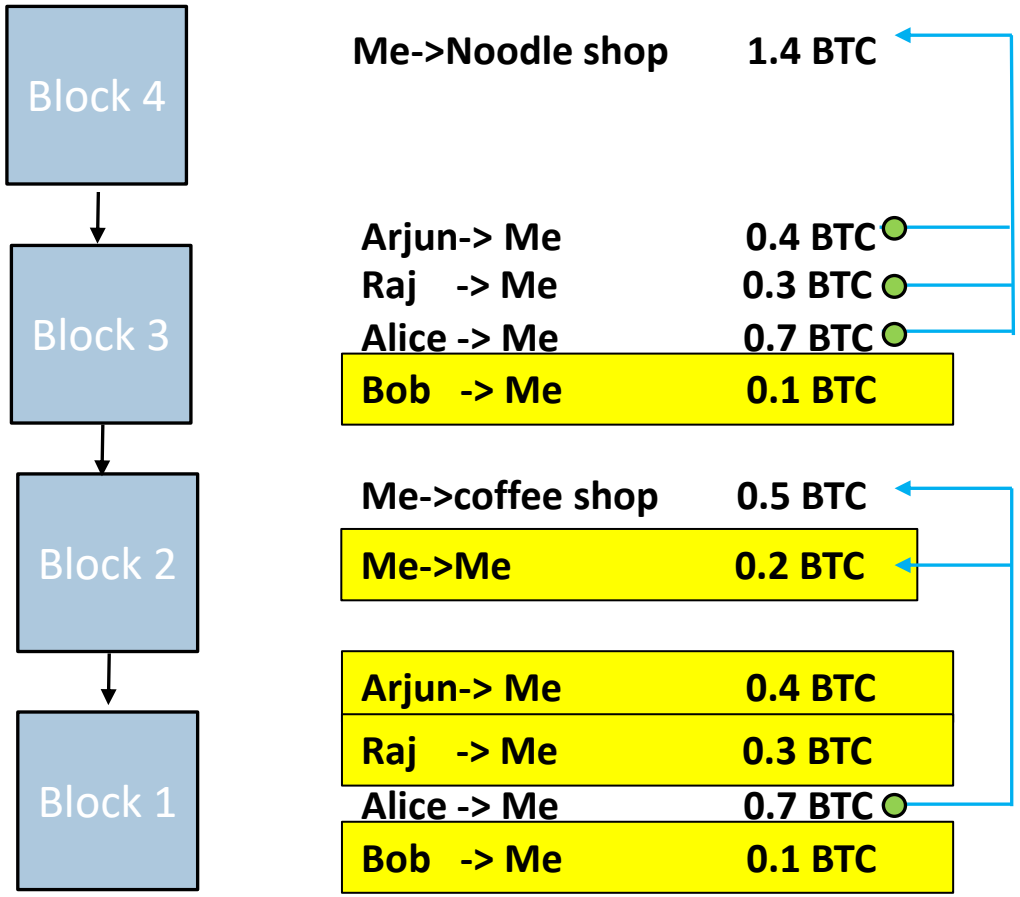
Cryptocurrency Wallets



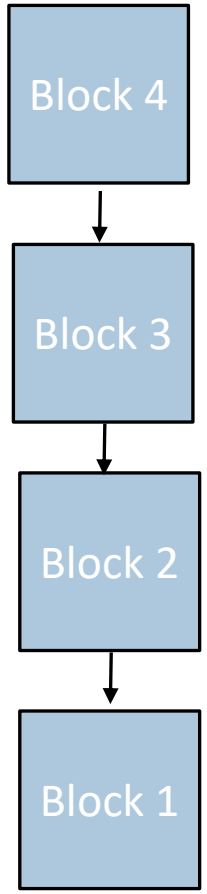
Cryptocurrency Wallets



Cryptocurrency Wallets



Cryptocurrency Wallets



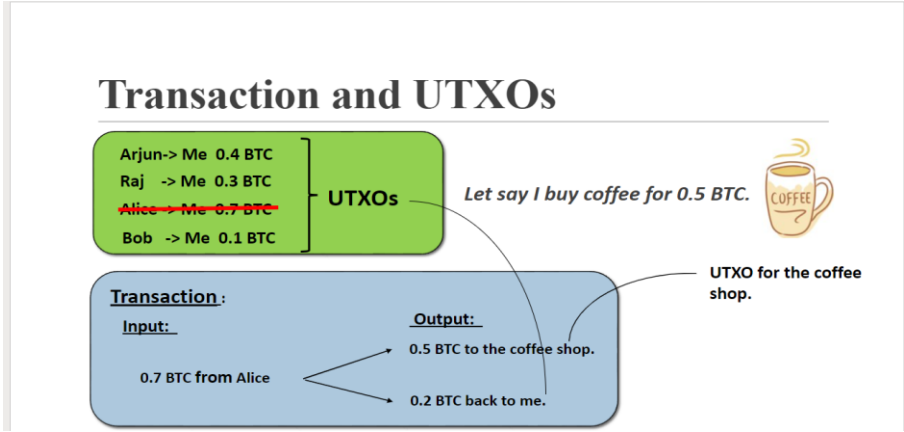
Me->Noodle shop 1.4 BTC

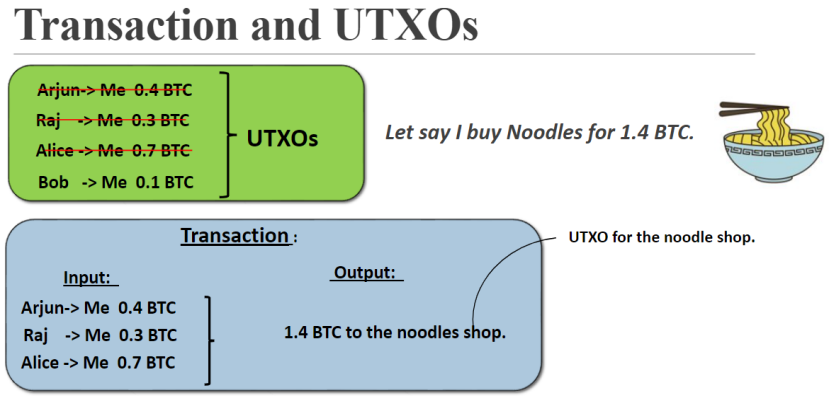
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

Me->coffee shop 0.5 BTC

Me->Me 0.2 BTC

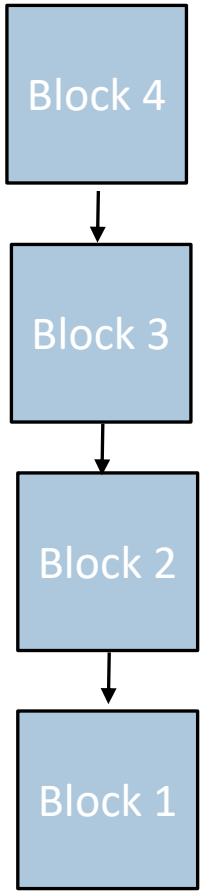
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC





Private and Public Key

Cryptocurrency Wallets



Me->Noodle shop 1.4 BTC

Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

Me->coffee shop 0.5 BTC

Me->Me 0.2 BTC

Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

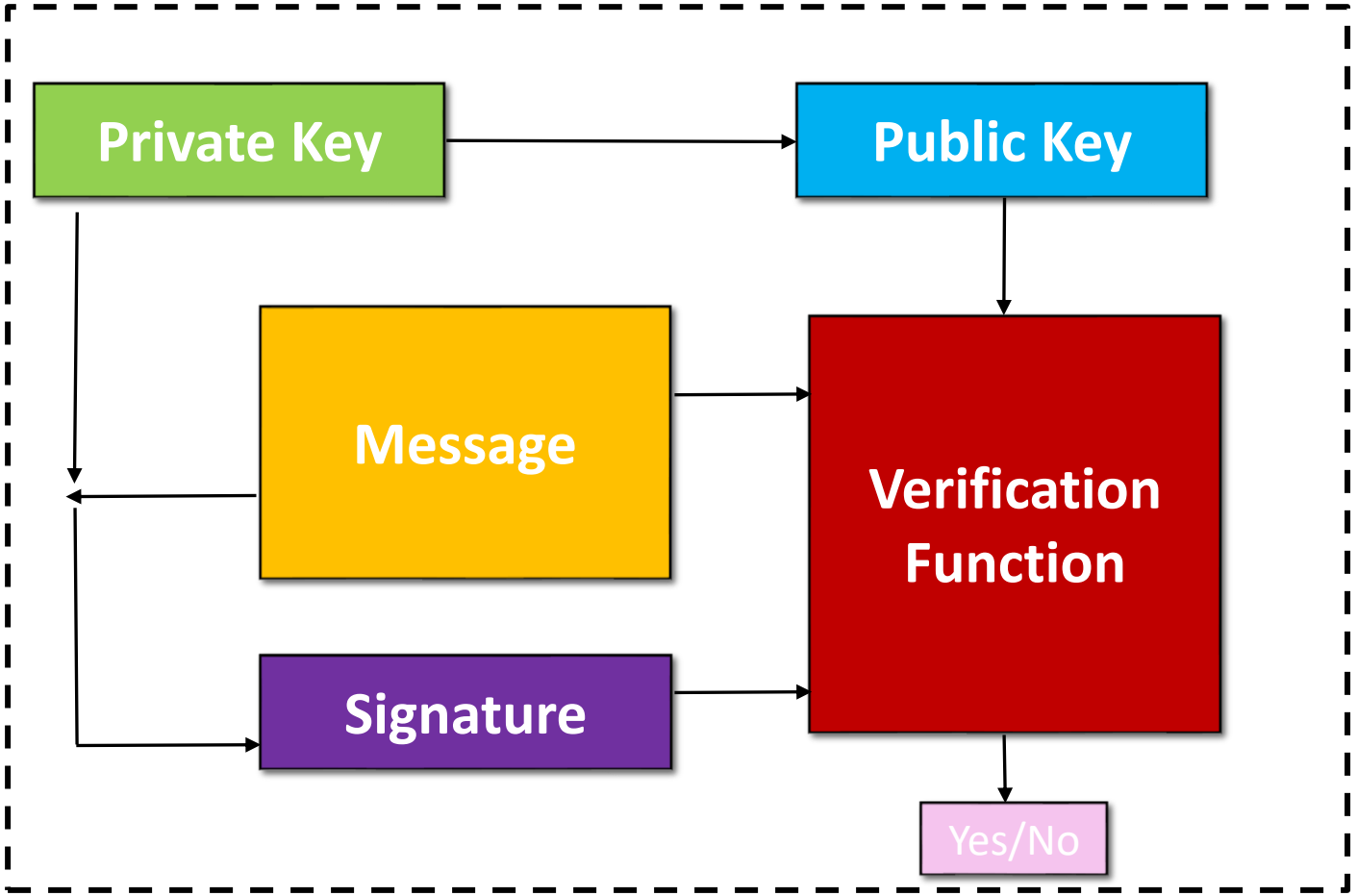
Private and Public Key

- How to check whether the transaction is valid or not, as there is no central authority
- It seems one can write anything in a transaction, so If a hacker adds a fraudulent transaction the transaction will be added to the block. How to check?
- The protocol stops fraudulent transactions using a wallet, and private and public keys
- A wallet is created (software or hardware) and will be used for transactions
- To make a transaction, a signature is created using a private key and a message
- Verification is done using a message, a signature, and a public key

Demonstration of Private and public keys/ Signatures

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

Private and Public Key

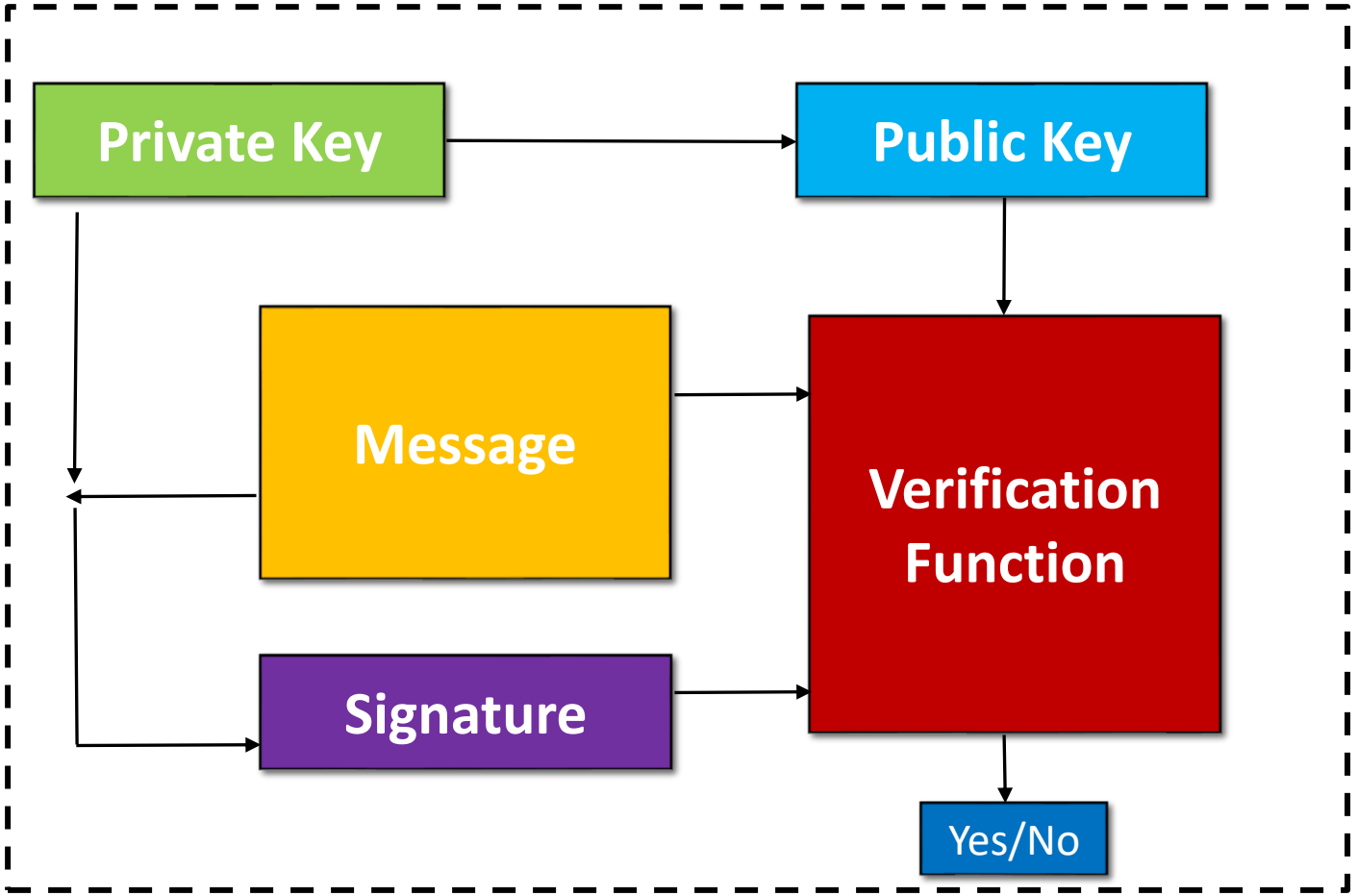


Public Key vs Bitcoin Address

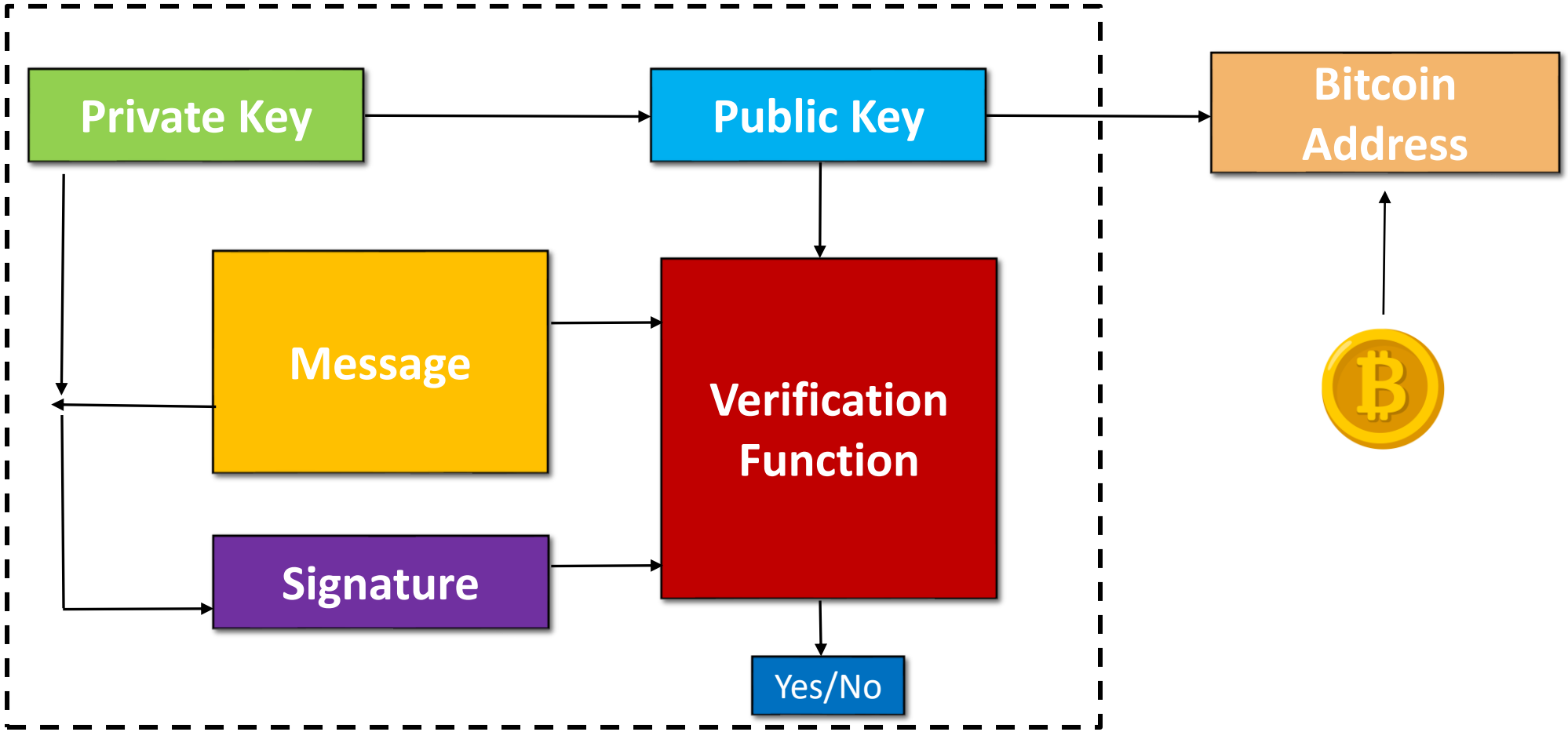
Public Key vs. Bitcoin Address

- Public key and Bitcoin address are not the same
- A transaction is made to others using public, whereas a bitcoin address is used for getting transactions
- To handle a Bitcoin the Bitcoin addresses are used to make it more secure
- An extra layer of security is added to the bitcoin address.
- If a hacker tries to get a private key, he must find out a public key from a Bitcoin address, and then using the public key he will try for the private key.

Private and Public Key



Private and Public Key

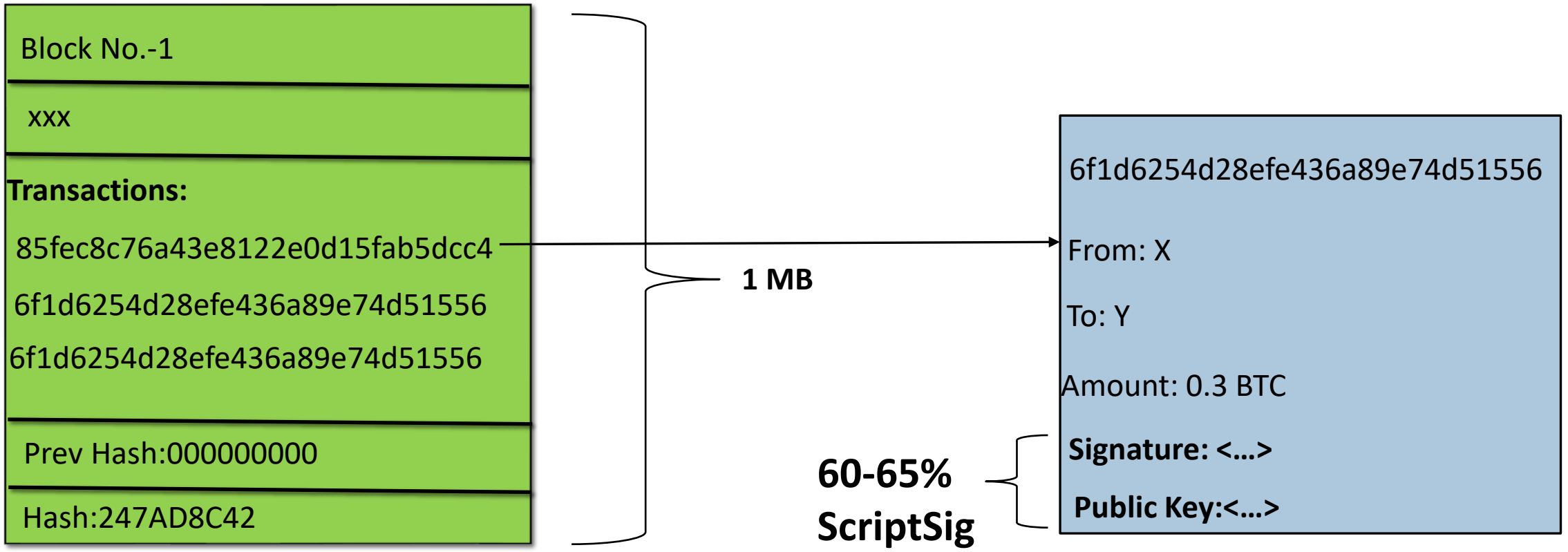


Segregated Witness

Segregated Witness

- The current block size of Bitcoin is 1 MB
- Increasing the block size will decrease the transaction time
- A big block needs more bandwidth, thus, will slow down the blockchain system
- 60-65% of the transaction space is given to signature and public key
- Now as the transactions are increased, 1 MB block size is no more sufficient
- The blockchain community separates the signature and public key from the transaction and will be sent separately.
- Now, 1 MB block can store more transactions, as transactions take less space

Segregated Witness



Hierarchically Deterministic (HD) Wallet

Hierarchically Deterministic Wallet

- If a person does transactions from a specific address i.e., Payment done to or from a specific Bitcoin address multiple time
- This way a pattern is developed, hackers can guess big setups, etc.
- The hackers can track down a person/ company using these patterns.
- Leads to privacy issues, So HD wallets were introduced.

Hierarchically Deterministic Wallet

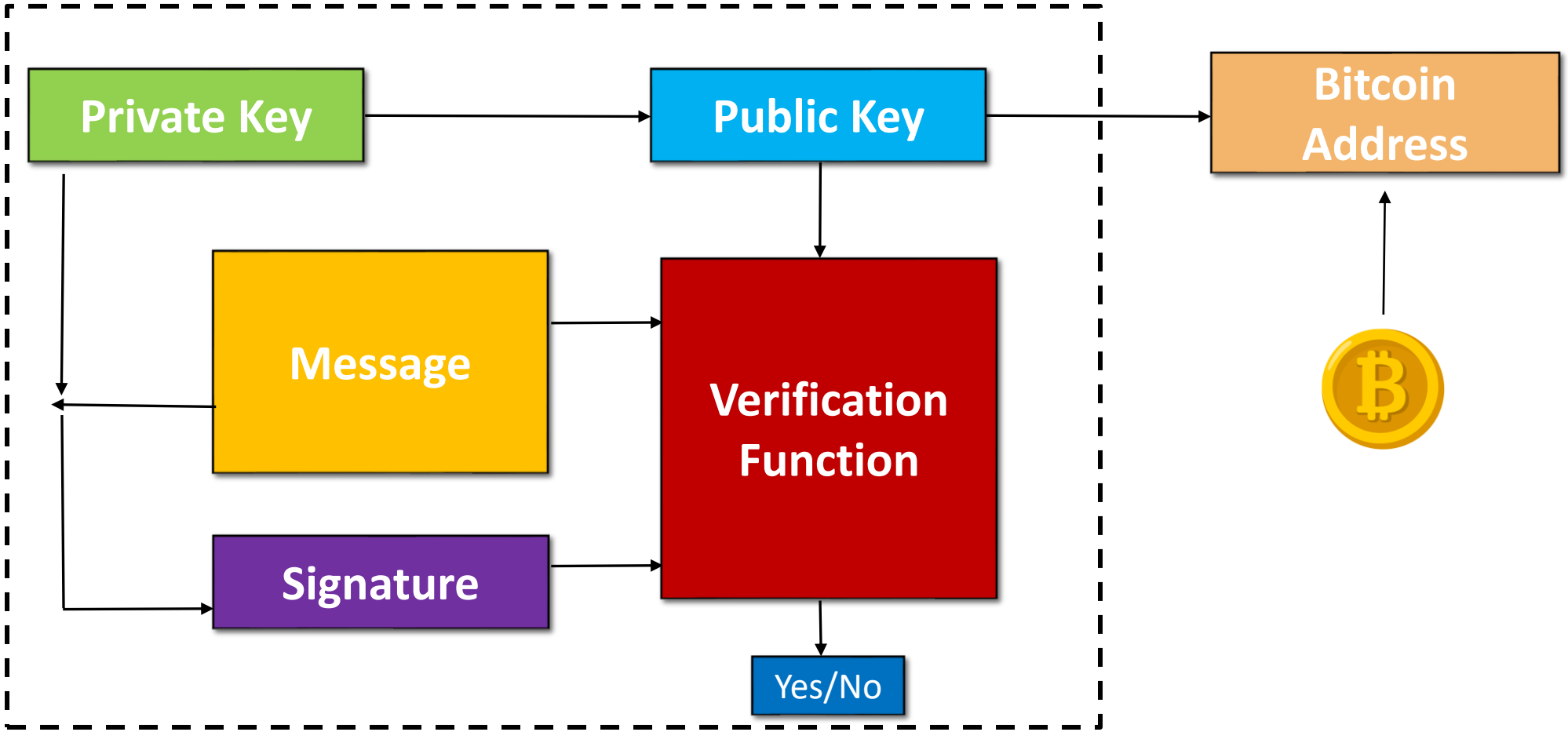
- Keeping multiple private keys is difficult to manage and remember, so HD was introduced
- A master private key is used to generate different private keys
- Private keys are used to generate public keys, which further used to generate different addresses
- Completely different private keys are generated due to the avalanche effect
- **Moreover, do not need to remember them, these keys are easily be generated later**
- Thus, transactions are done using different addresses

Hierarchically Deterministic Wallet

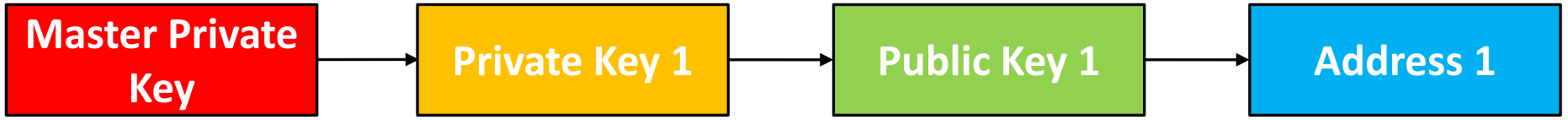
- How Hierarchically Deterministic?
- CEO has a master key, and the subordinates are given the generated private keys.
- CEO can trace all transactions done from generated public keys.

- Usage private key, public key, and Bitcoin address:
- Private key is used to send transactions
- Public key used for transactions' verification
- Address is used for receiving money

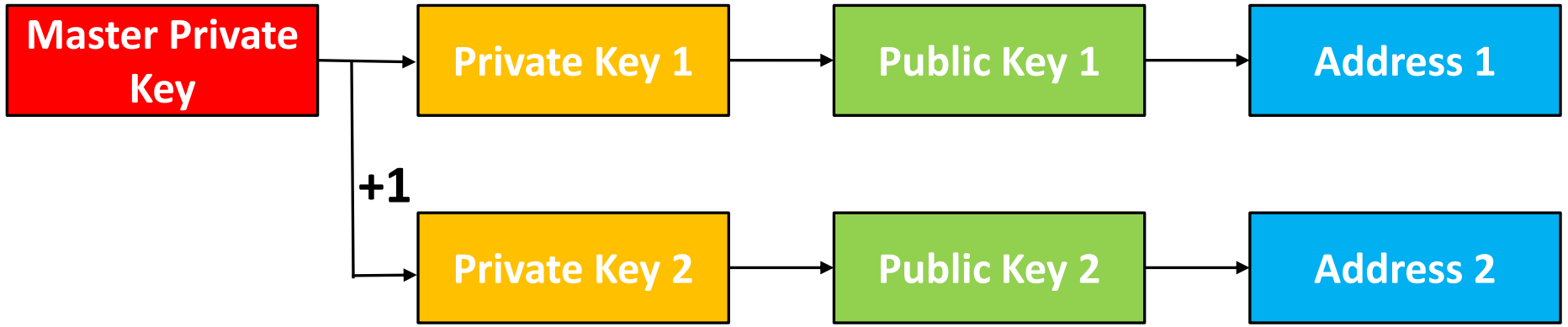
Private and Public Key



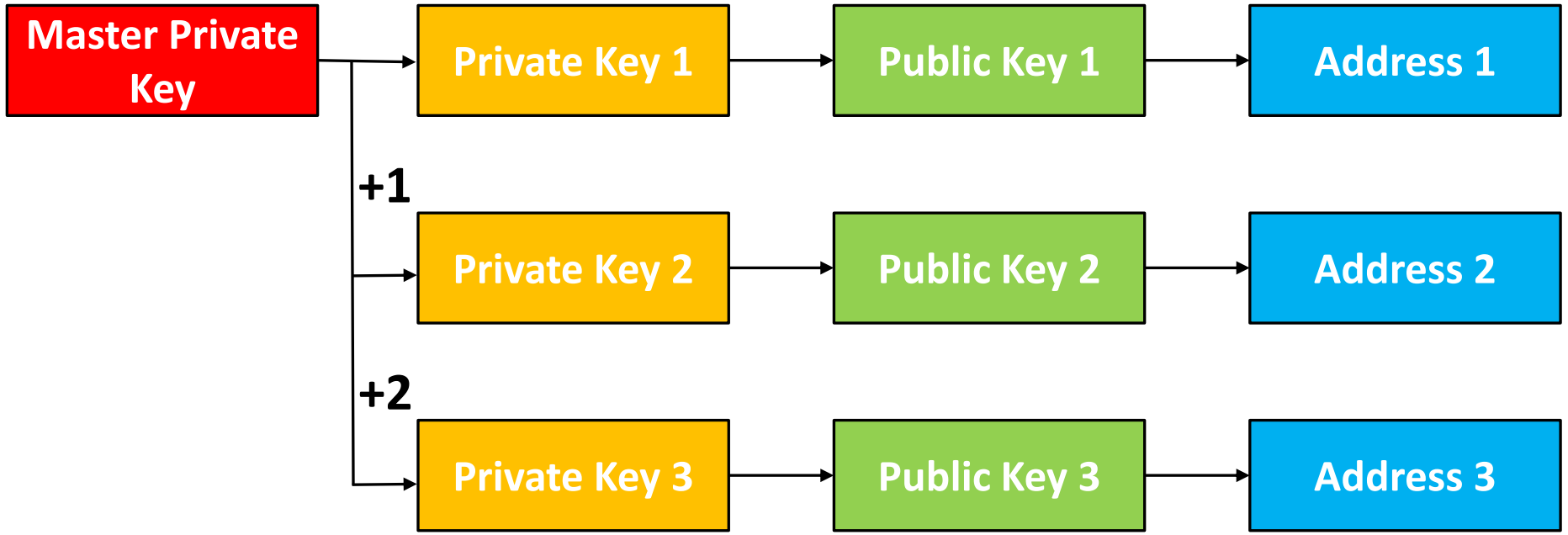
Hierarchically Deterministic (HD) Wallets



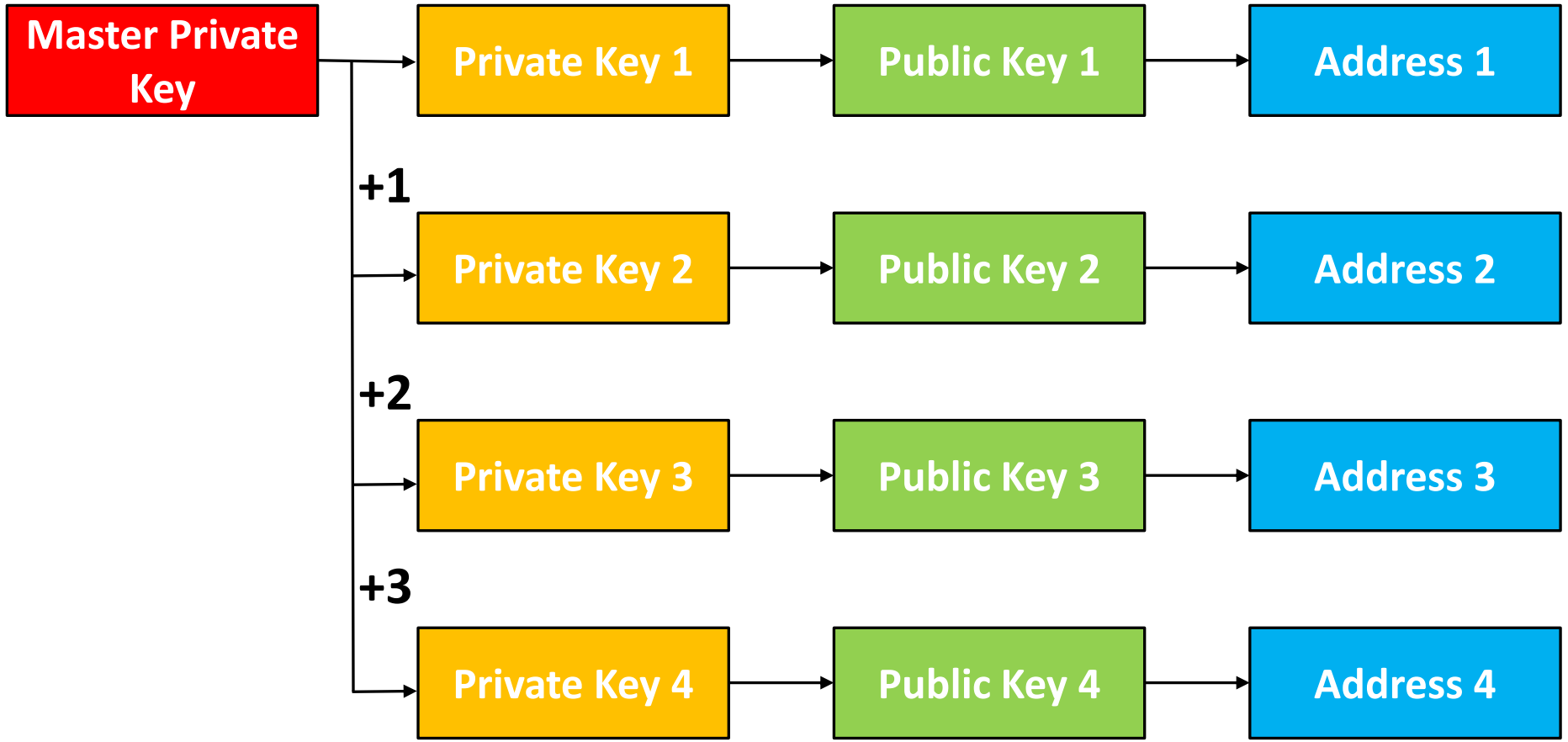
Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets