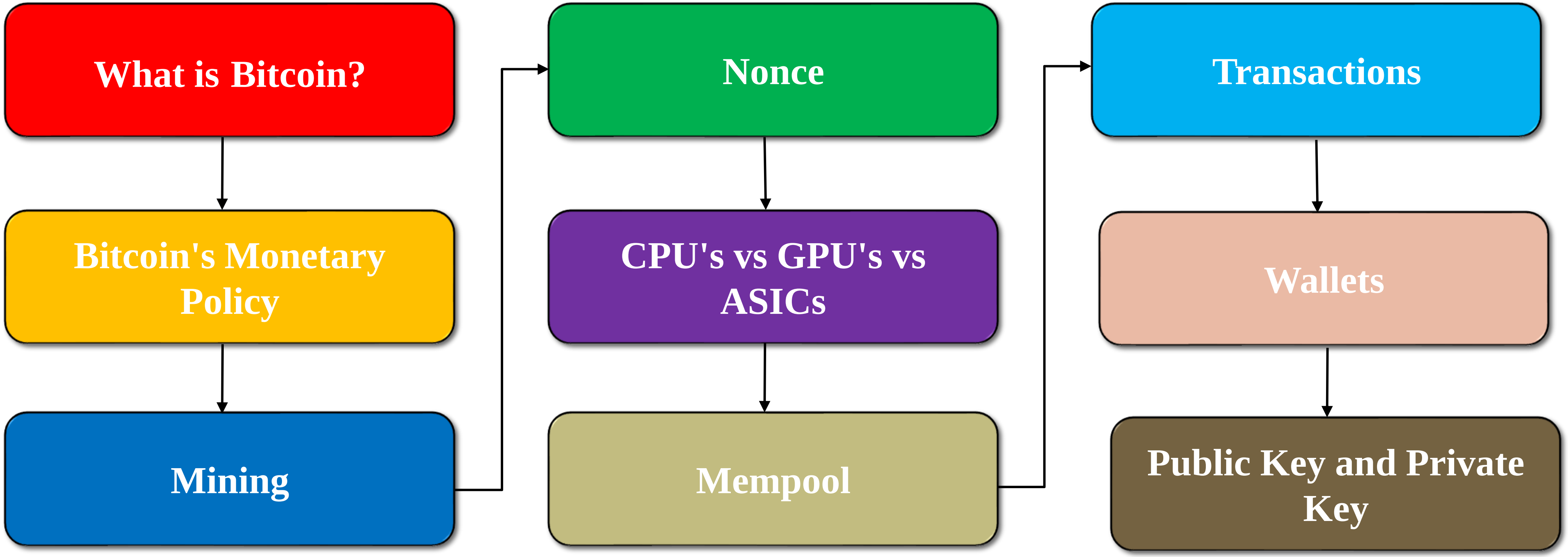
Blockchain

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

Cryptocurrency

Contents – Module B



What is Bitcoin?

Bitcoin's Monetary Policy

Mining

Nonce

CPU's vs GPU's vs ASICs

Mempool

Transactions

Wallets

Public Key and Private Key

Cryptocurrency Wallet

Cryptocurrency Wallets

- A wallet (device/program) stores keys and allows one to access coins
- Public key is used to receive cryptocurrency transactions
- 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

- The primary means of storing and exchanging cryptocurrencies and tokens.
- **Hot wallets:**
  - Internet-enabled and online.
  - It can provide ease of use and a well-designed interface.
- **Cold wallet:**
  - Offline and come in the form of a physical device, such as a USB stick.
  - Offers more security as less possibility to hack
  - Less vulnerable to loss of digital assets.

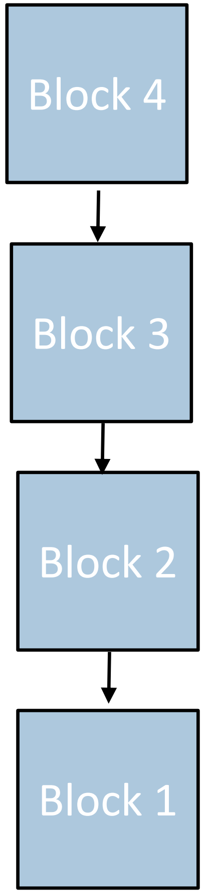
Cryptocurrency Wallets (Hot Wallets)

1. **Exodus:**
   - User-friendly
   - Multi-currency support
   - Available for desktop and mobile platforms.
2. **Electrum:**
   - Lightweight and feature-rich Bitcoin
   - Available for desktop and mobile devices.
3. **Coinbase Wallet:**
   - User-friendly mobile
4. **Trust Wallet:**
   - Trust Wallet is a mobile wallet
   - Providing a secure and user-friendly experience
   - Managing a variety of cryptocurrencies, including Ethereum-based tokens.
5. **Metamask:**
   - A browser extension wallet primarily designed for interacting with Ethereum-based dApps

Cryptocurrency Wallets (Cold Wallets)

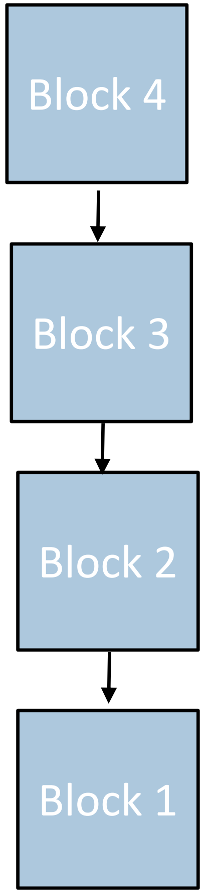
- **Ledger Nano S and Ledger Nano X:**
  - Provide high-security
  - Support for a wide range of cryptocurrencies.
- **Trezor Model T:**
  - Offering advanced security and a touchscreen interface.
- **KeepKey:**
  - Known for its simplicity and ease of use.
  - It provides cold storage for a variety of cryptocurrencies.
- **Coldcard:**
  - Provide advanced security including PIN protection and support for multi-signature wallets.
- **Paper Wallets:**
  - The private and public keys are printed on a physical piece of paper.
  - One of the most secure methods as it's entirely offline.

Cryptocurrency Wallets



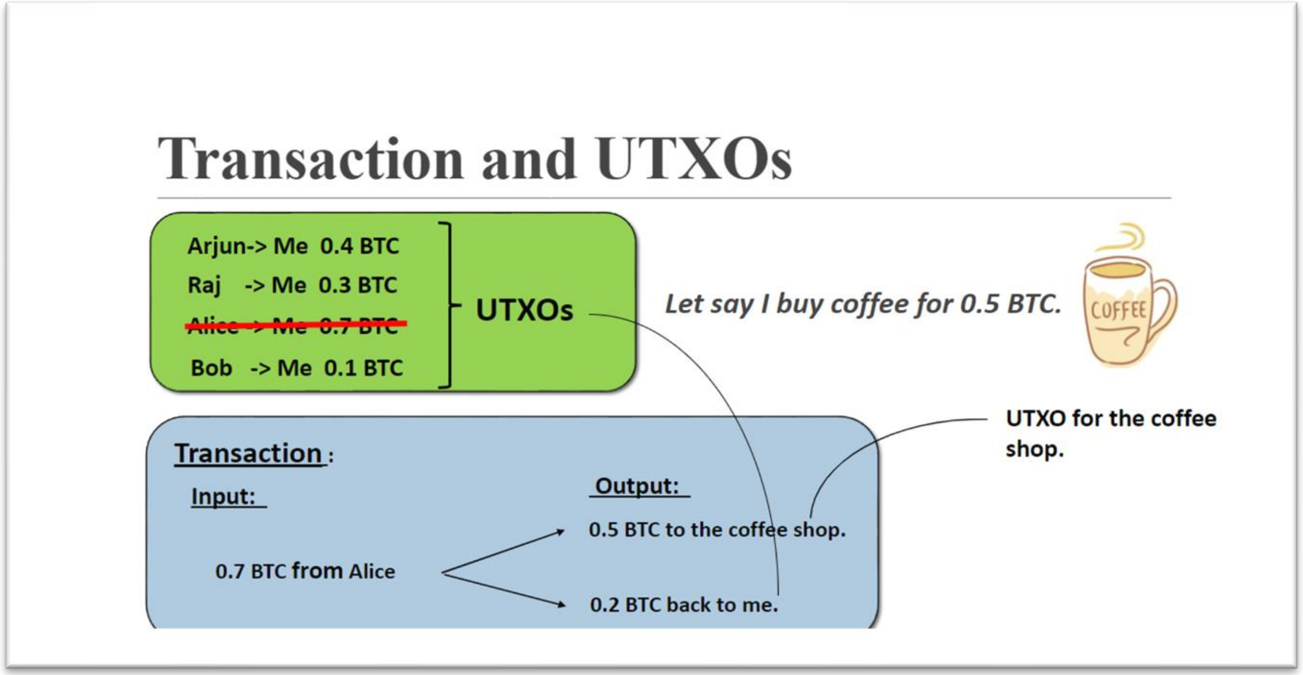
Arjun-> Me	**0.4 BTC**
Raj -> Me	**0.3 BTC**
Alice -> Me	**0.7 BTC**
Bob -> Me	**0.1 BTC**

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



Transaction and UTXOs

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

UTXOs

Let say I buy coffee for 0.5 BTC.

UTXO for the coffee shop.

Transaction :

Input:

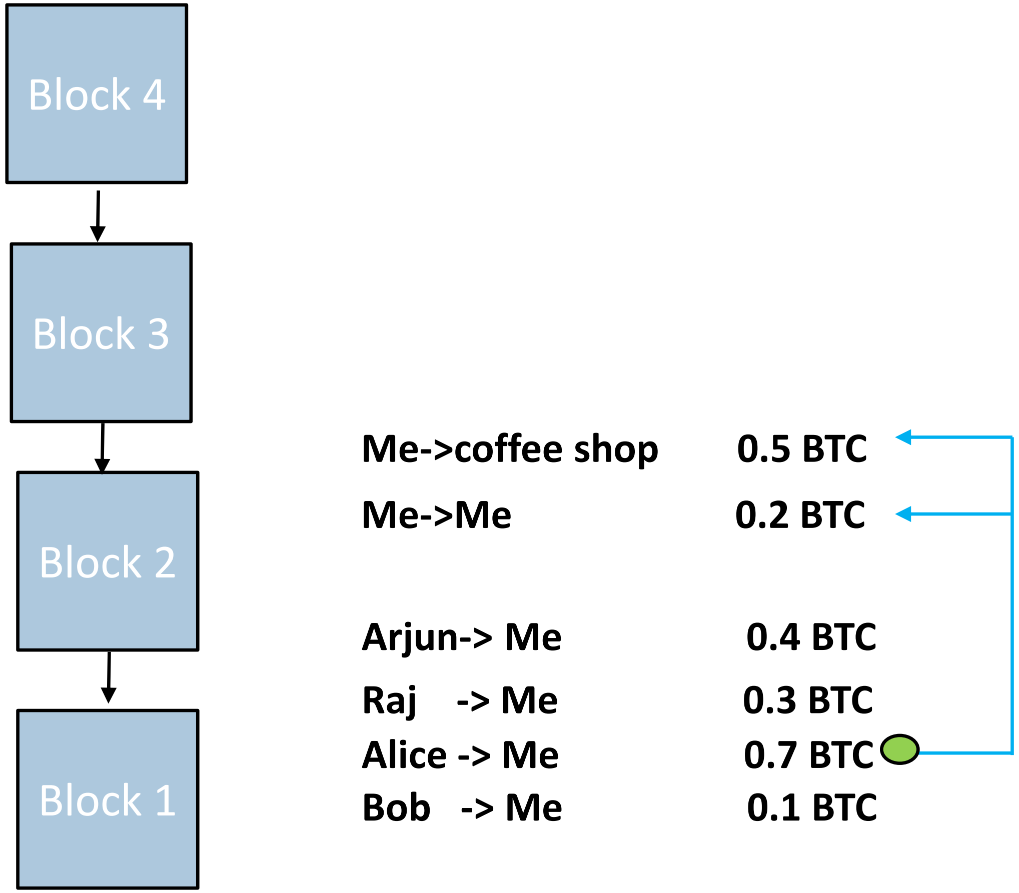
0.7 BTC from Alice

Output:

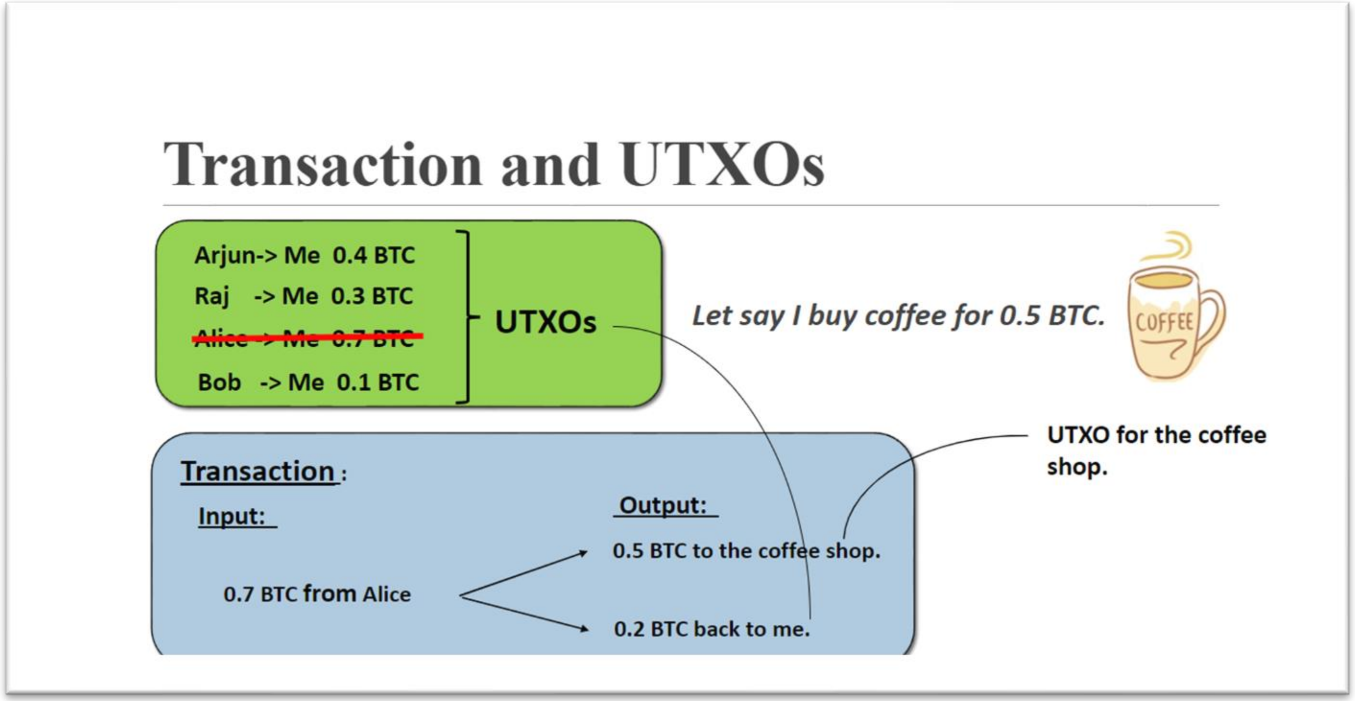
0.5 BTC to the coffee shop.

0.2 BTC back to me.

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



Transaction and UTXOs

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

UTXOs

Let say I buy coffee for 0.5 BTC.

Transaction :

Input:

0.7 BTC from Alice

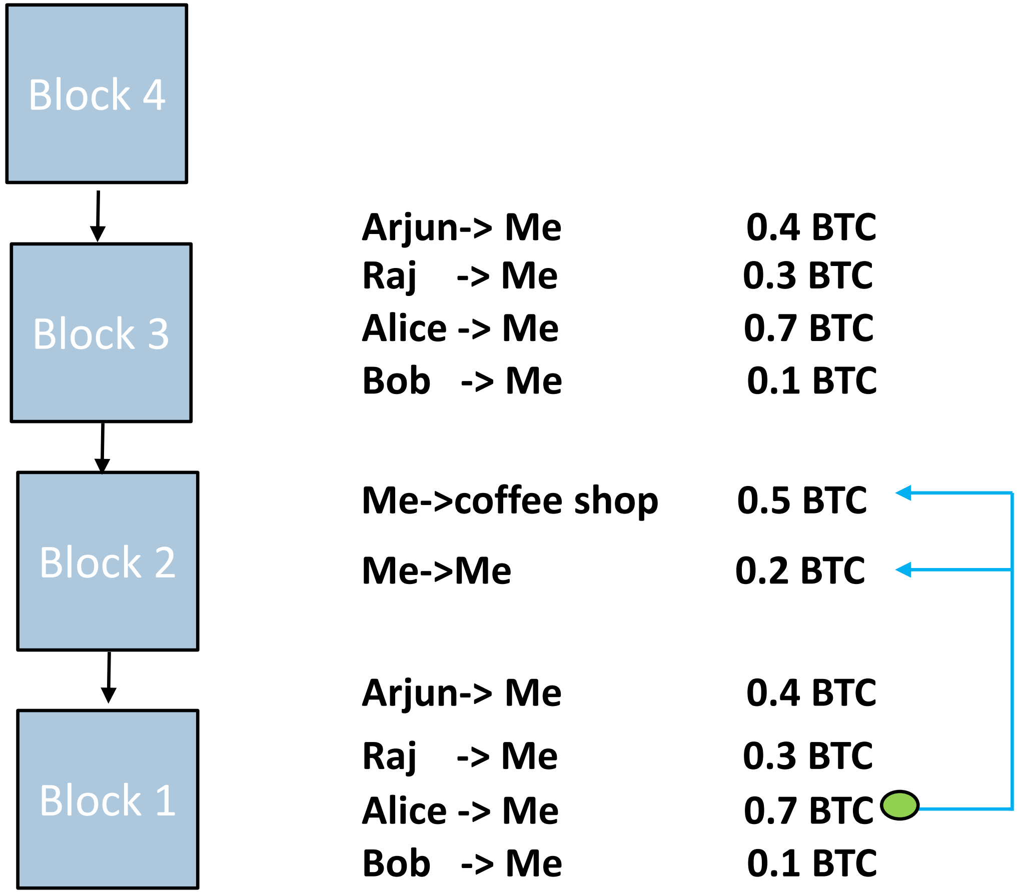
Output:

0.5 BTC to the coffee shop.

0.2 BTC back to me.

UTXO for the coffee shop.

Cryptocurrency Wallets

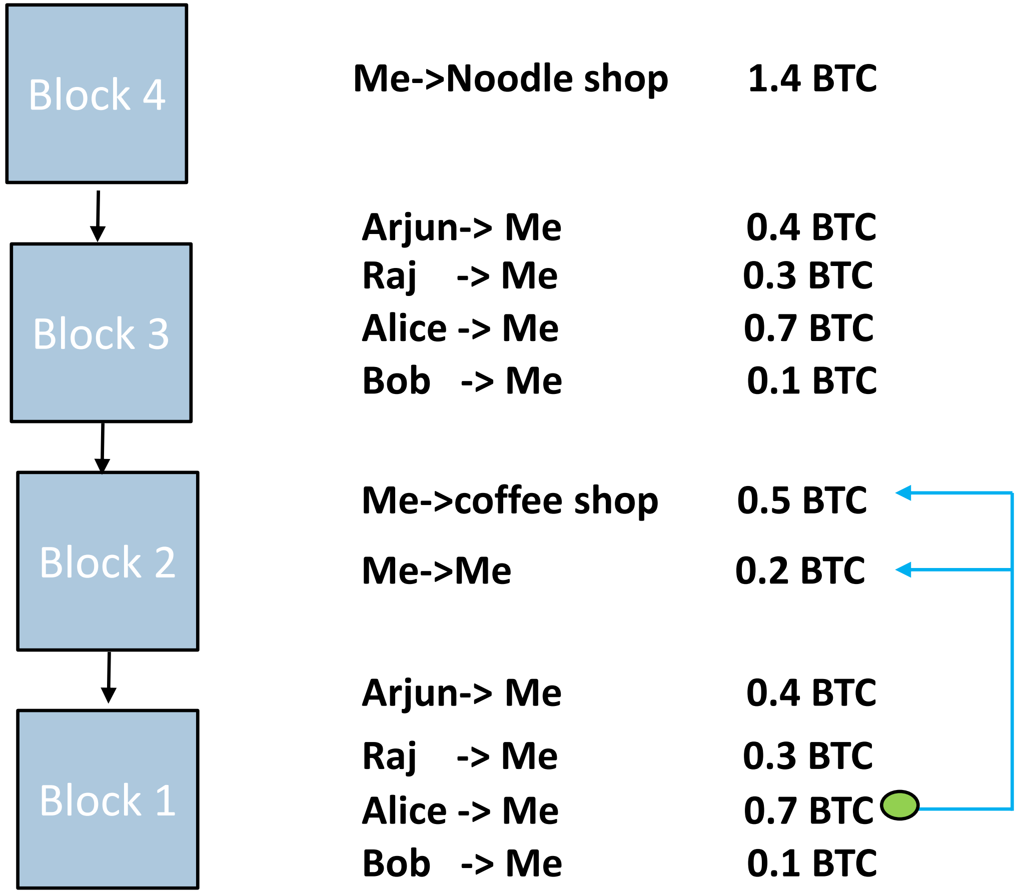


Arjun-> Me	0.4 BTC
Raj -> Me	0.3 BTC
Alice -> Me	0.7 BTC
Bob -> Me	0.1 BTC

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

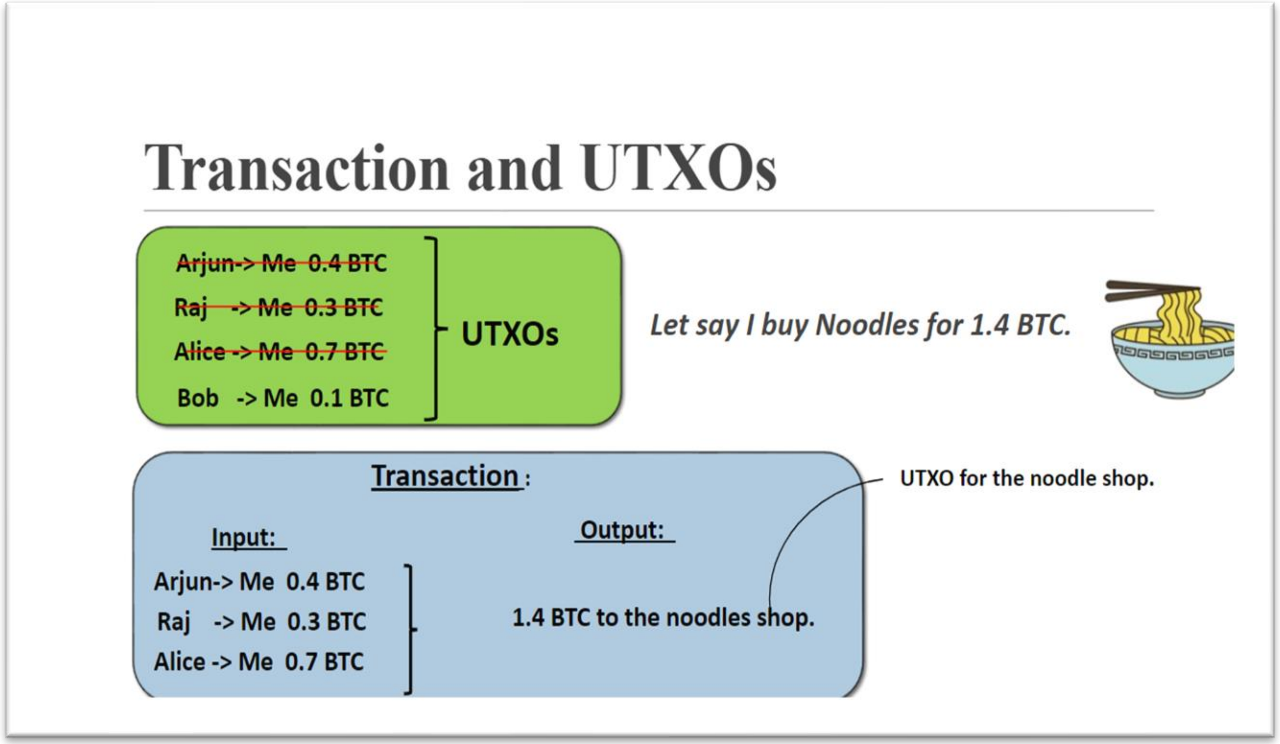


Me->Noodle shop	1.4 BTC

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



Transaction and UTXOs

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

UTXOs

Let say I buy Noodles for 1.4 BTC.

Transaction :

Input:

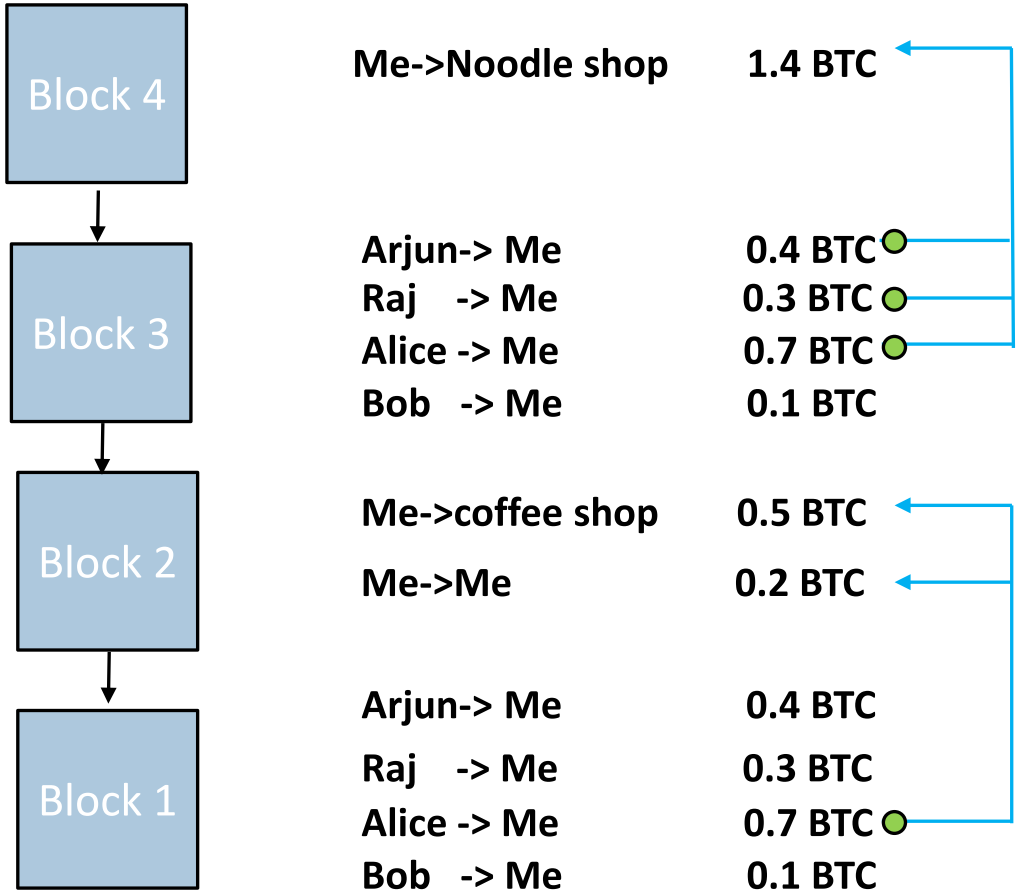
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC

Output:

1.4 BTC to the noodles shop.

UTXO for the noodle shop.

Cryptocurrency Wallets



Block 4

Me->Noodle shop 1.4 BTC

Block 3

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Block 2

Me->coffee shop 0.5 BTC

Me->Me 0.2 BTC

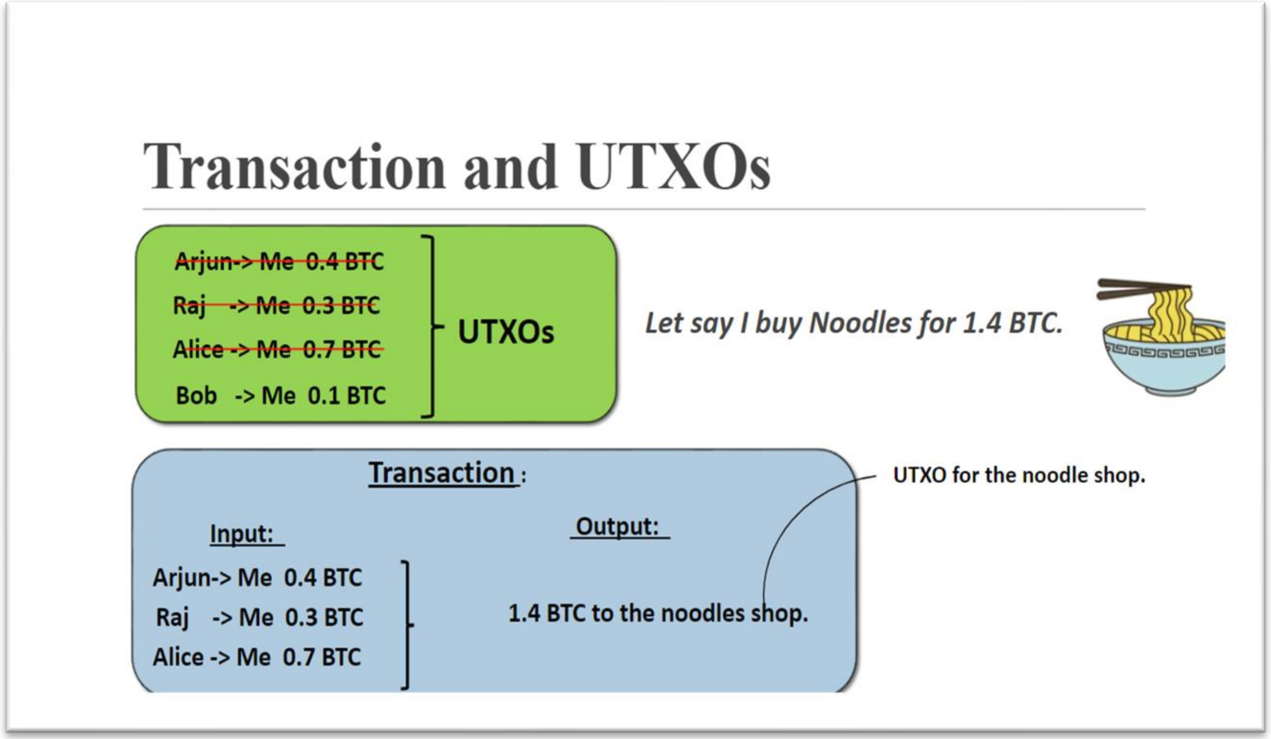
Block 1

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC



Transaction and UTXOs

~~Arjun-> Me 0.4 BTC~~

~~Raj -> Me 0.3 BTC~~

~~Alice -> Me 0.7 BTC~~

Bob -> Me 0.1 BTC

UTXOs

Let say I buy Noodles for 1.4 BTC.

Transaction :

Input:

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

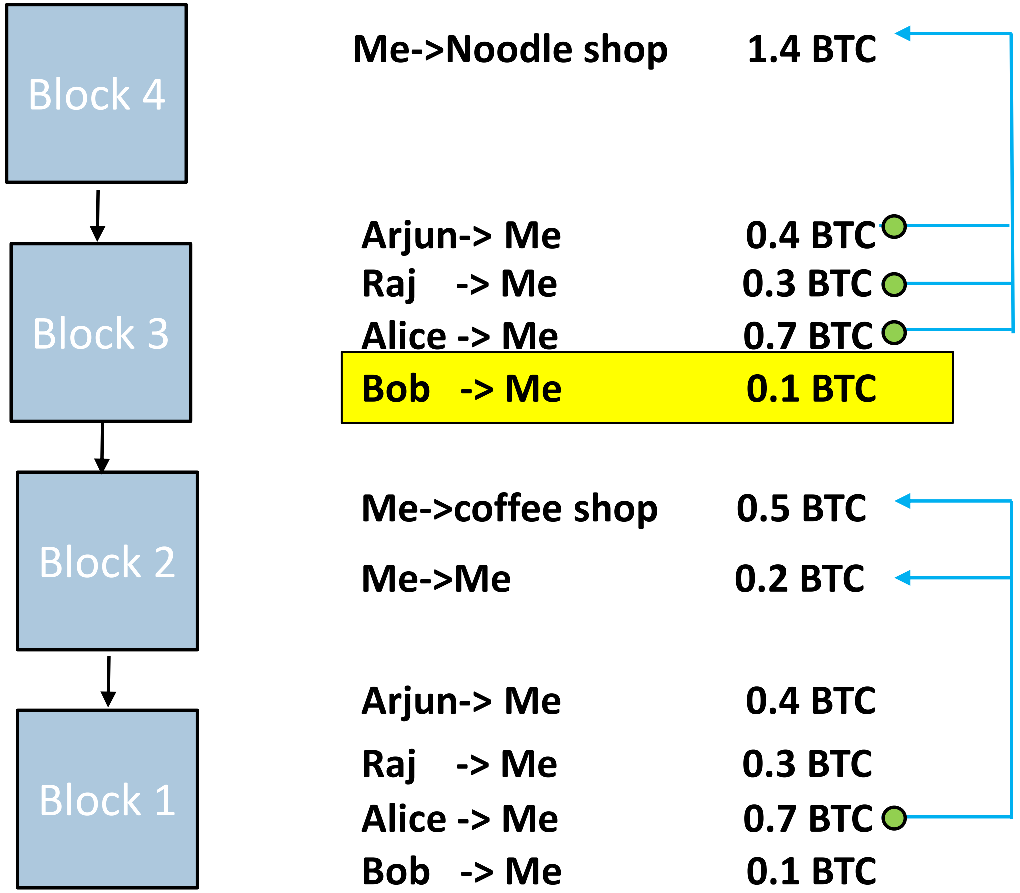
Alice -> Me 0.7 BTC

Output:

1.4 BTC to the noodles shop.

UTXO for the noodle shop.

Cryptocurrency Wallets



Block 4

Me->Noodle shop 1.4 BTC

Block 3

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Block 2

Me->coffee shop 0.5 BTC

Me->Me 0.2 BTC

Block 1

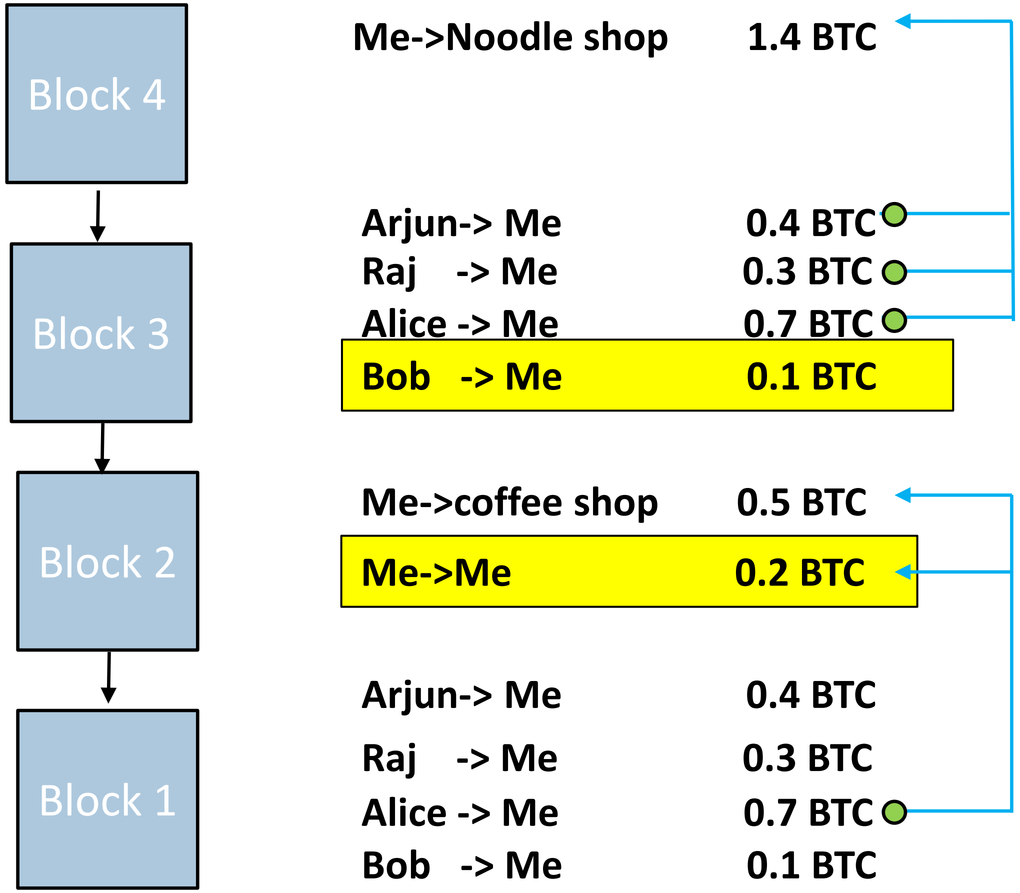
Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Cryptocurrency Wallets



Me->Noodle shop 1.4 BTC

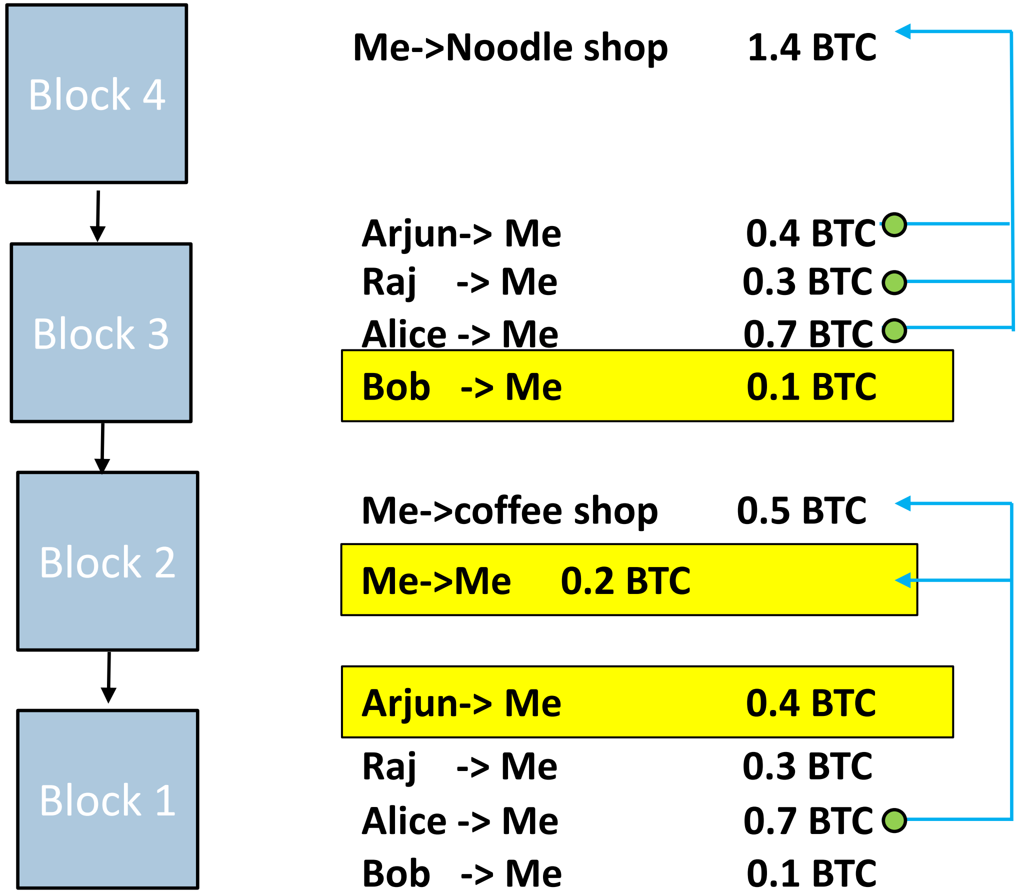
Arjun-> Me 0.4 BTC
Raj -> Me 0.3 BTC
Alice -> Me 0.7 BTC
Bob -> Me 0.1 BTC

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



Block 4

Block 3

Block 2

Block 1

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

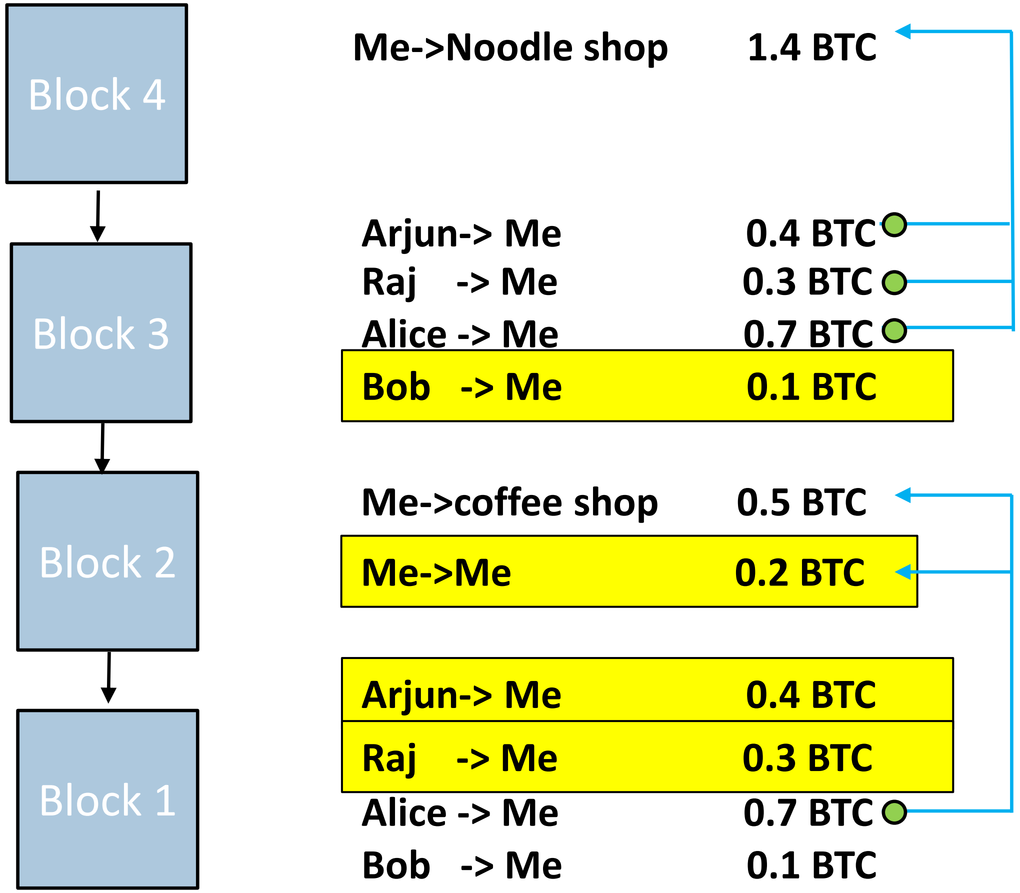
Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Cryptocurrency Wallets



Block 4

Me->Noodle shop 1.4 BTC

Block 3

Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Block 2

Me->coffee shop 0.5 BTC

Me->Me 0.2 BTC

Block 1

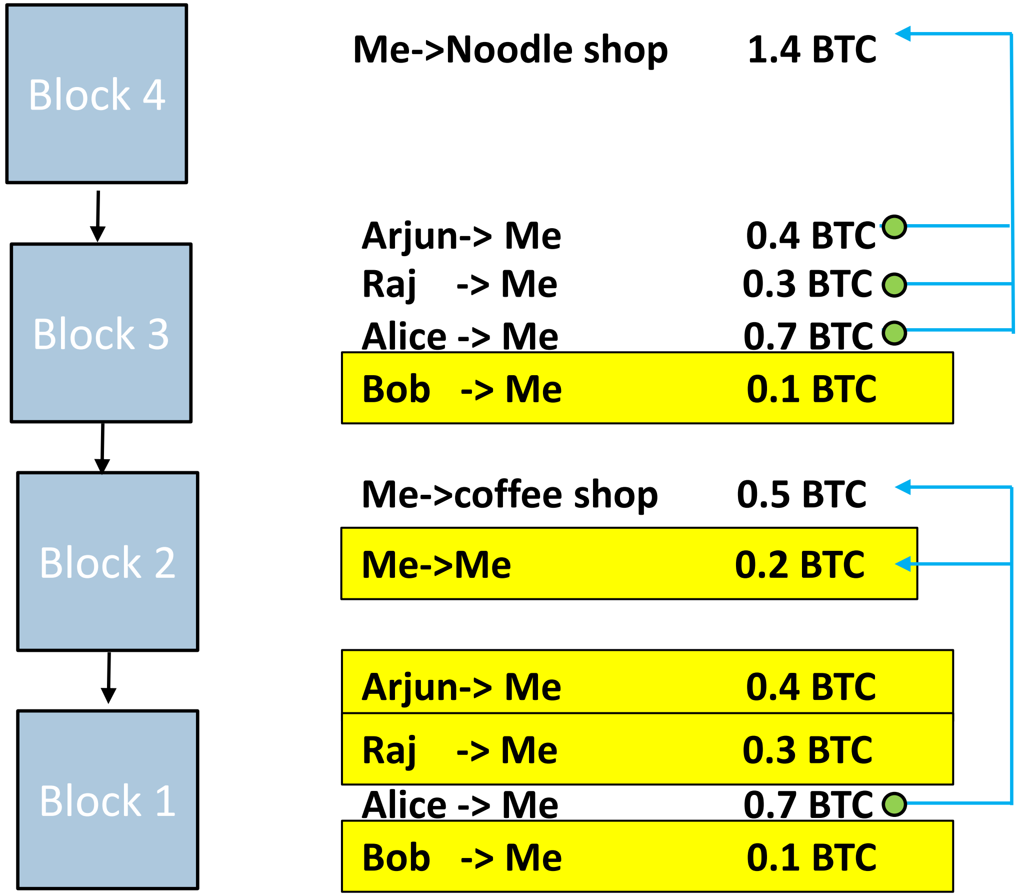
Arjun-> Me 0.4 BTC

Raj -> Me 0.3 BTC

Alice -> Me 0.7 BTC

Bob -> Me 0.1 BTC

Cryptocurrency Wallets



Block 4

Me->Noodle shop 1.4 BTC

Block 3

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

Block 2

Me->coffee shop 0.5 BTC
Me->Me 0.2 BTC

Block 1

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

1.1 BTC

Private and Public Key

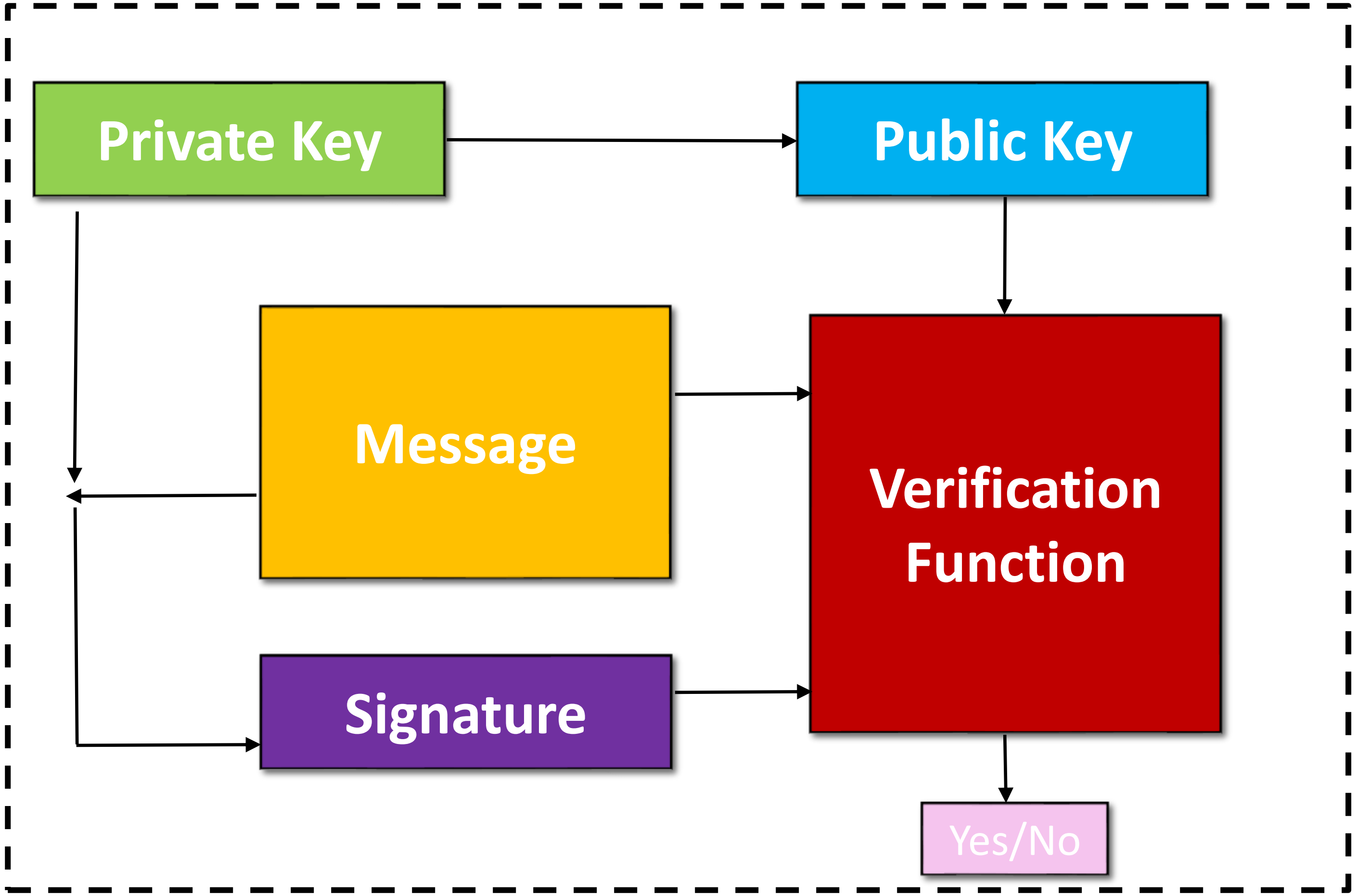
Private and Public Key

- 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

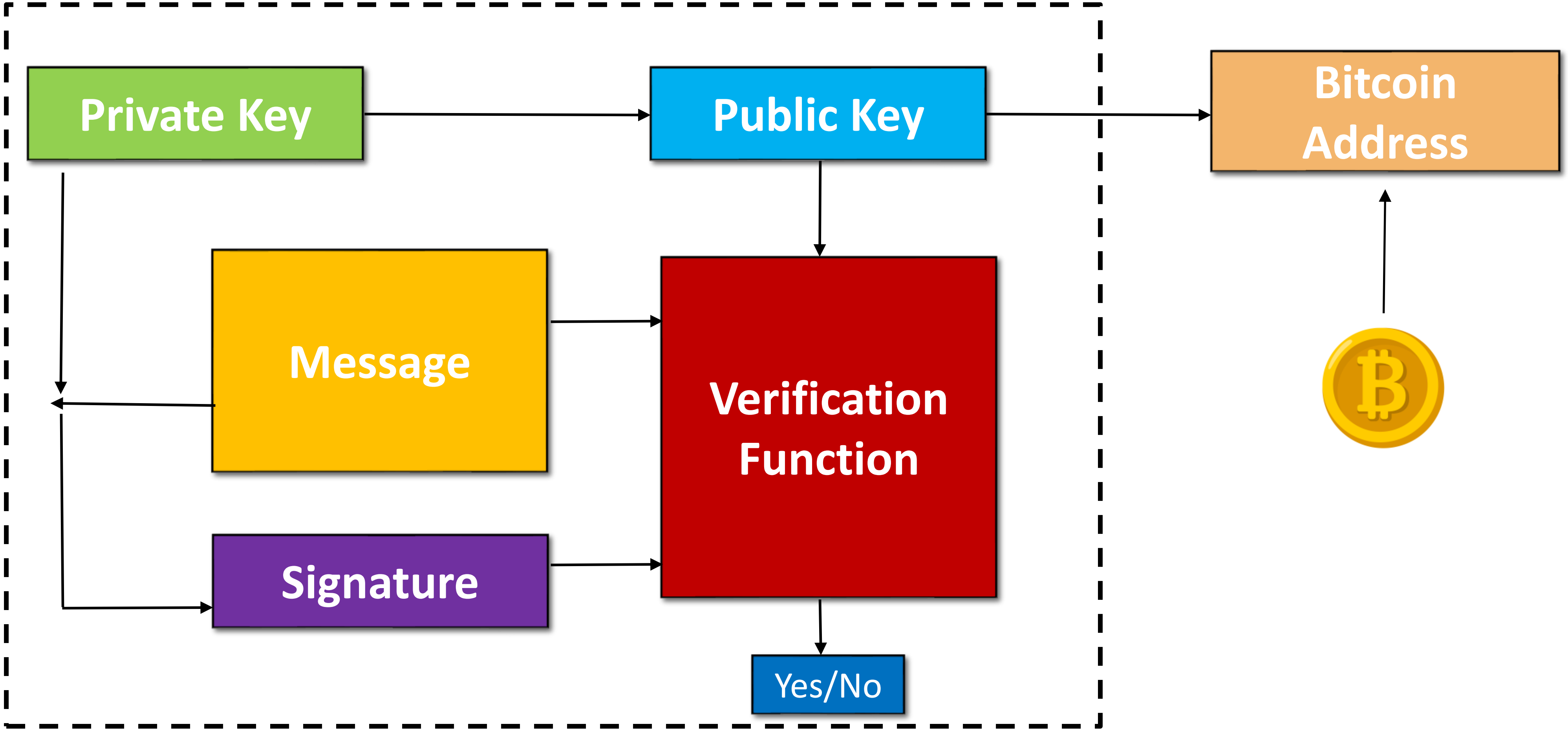
https://tools.superdatascience.com/blockchain/public-private-keys/keys

Private and Public Key



Public Key vs Bitcoin Address

Private and Public Key



Private Key

Public Key

Bitcoin Address

Message

Verification Function

Signature

Yes/No

Public Key vs. Bitcoin Address

- Public key and Bitcoin address are not the same
- 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.

Segregated Witness

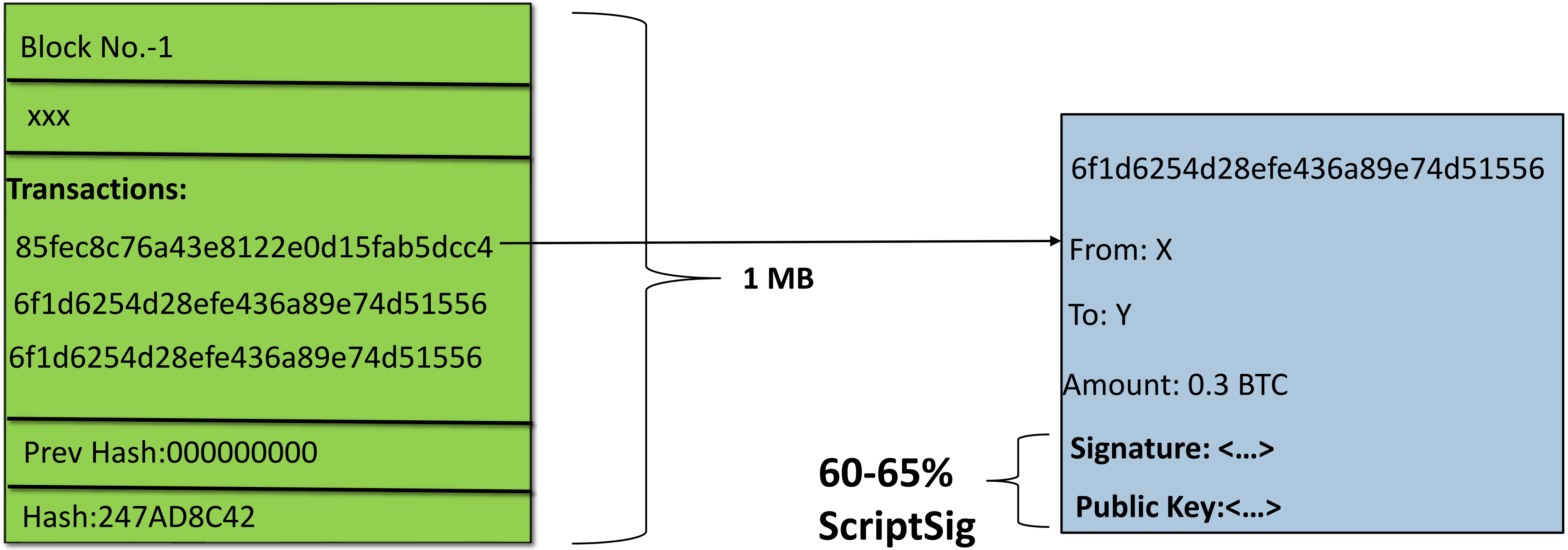
Segregated Witness

- The initial block size in a Bitcoin was 1 MB
- Increasing the block size will decrease the average 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, the 1 MB block size is no more sufficient
- How to resolve this issue?

Segregated Witness

- Segregated Witness (**SegWit**) refers to a change in the transaction format
- To decrease transaction times by increasing the block capacity
- The **SegWit** protocol divides the transaction into **two segments**
- The unlocking signature ("witness" data) is removed from the original
- The original portion holds the sender and receiver data, while the separate structure at the end ("witness" structure) contains scripts and signatures
- Thus, a 1 MB block can store more transactions, as transactions take less space

Segregated Witness



Block No.-1

xxx

Transactions:

85fec8c76a43e8122e0d15fab5dcc4

6f1d6254d28efe436a89e74d51556

6f1d6254d28efe436a89e74d51556

Prev Hash:000000000

Hash:247AD8C42

1 MB

6f1d6254d28efe436a89e74d51556

From: X

To: Y

Amount: 0.3 BTC

Signature: <…>

Public Key:<…>

60-65%
ScriptSig

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

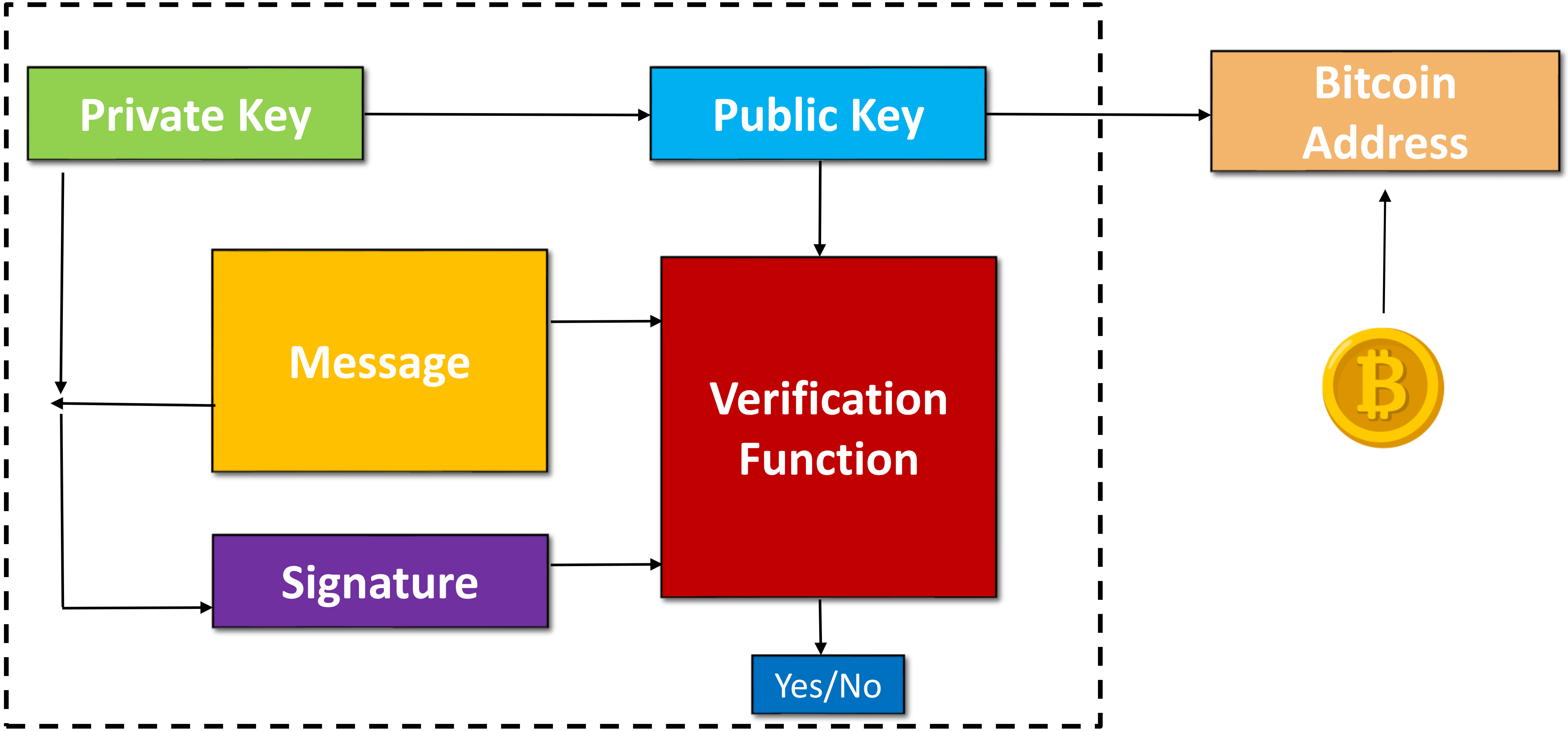
- Keeping multiple private keys is difficult to manage and remember, so HD was introduced
- A master private key is used to generate different private keys
- Private keys are used to generate public keys, which further used to generate different addresses
- Completely different private keys are generated 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

Hierarchically Deterministic (HD) Wallets



Private Key

Public Key

Bitcoin Address

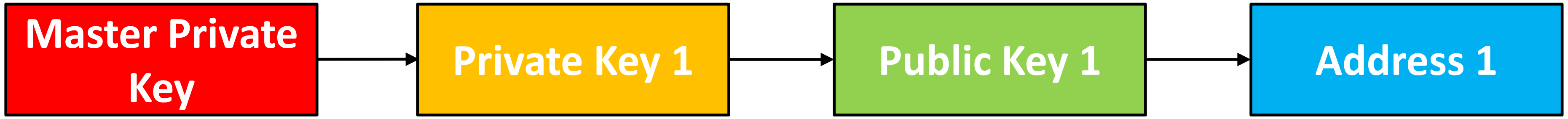
Message

Verification Function

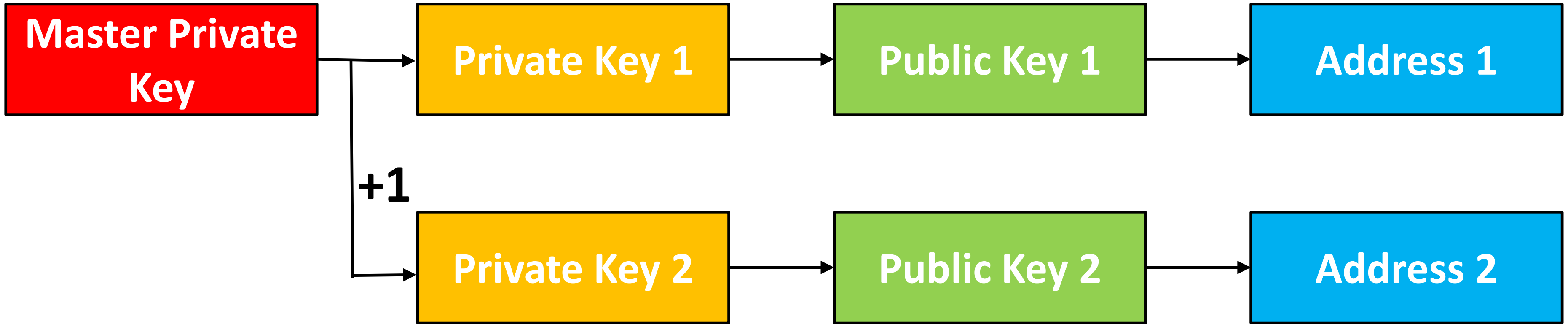
Signature

Yes/No

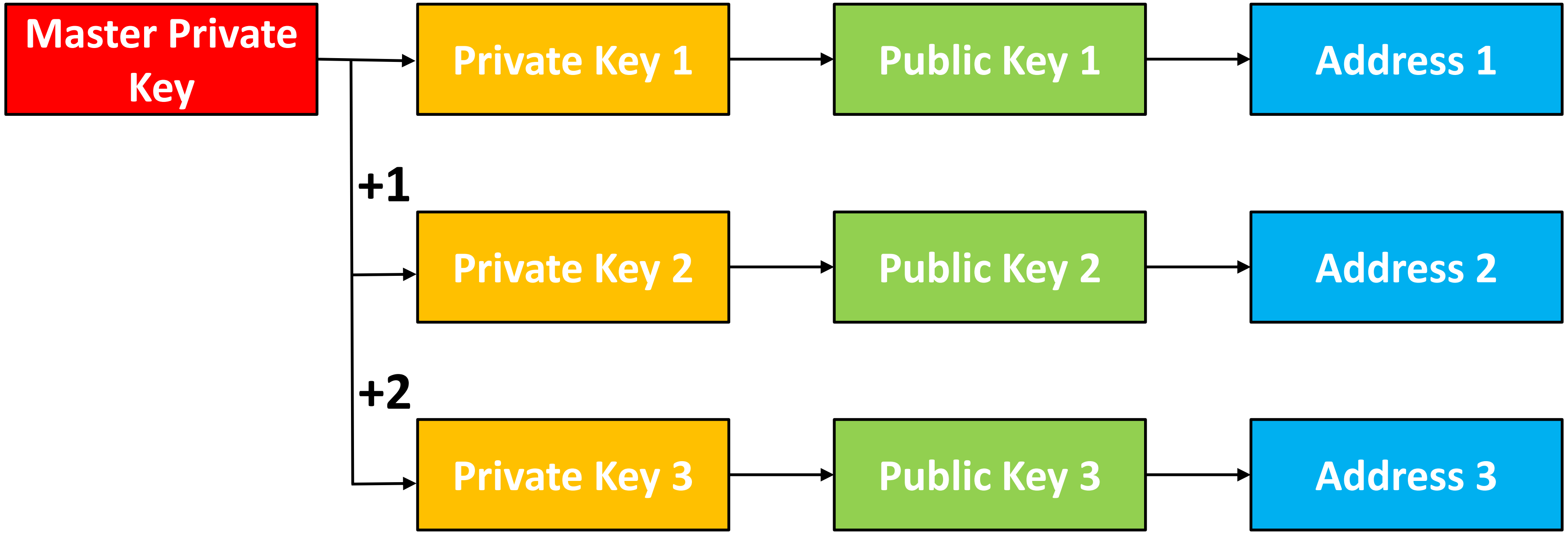
Hierarchically Deterministic (HD) Wallets



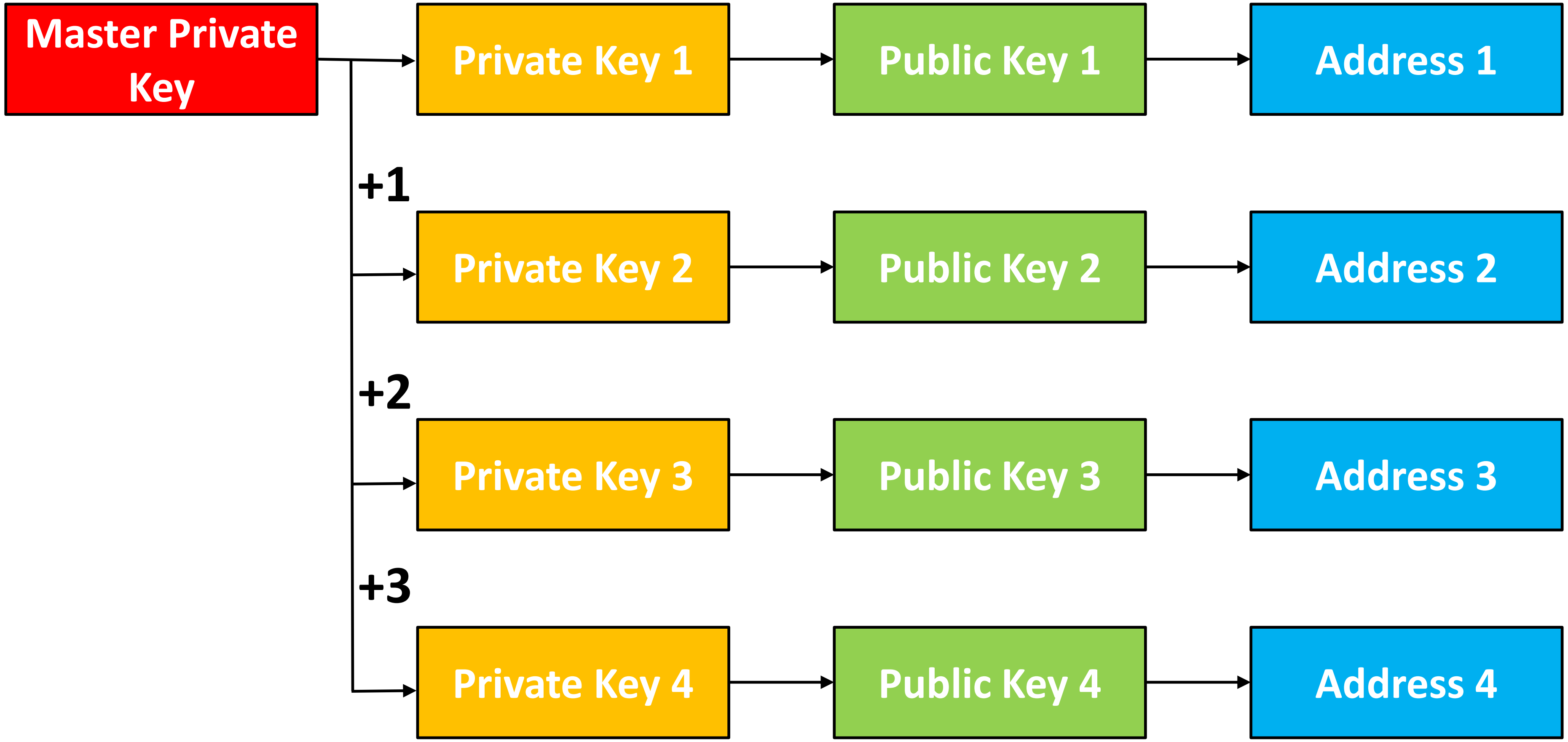
Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets



Hierarchically Deterministic (HD) Wallets



Master Private Key

Private Key 1 → Public Key 1 → Address 1

+1

Private Key 2 → Public Key 2 → Address 2

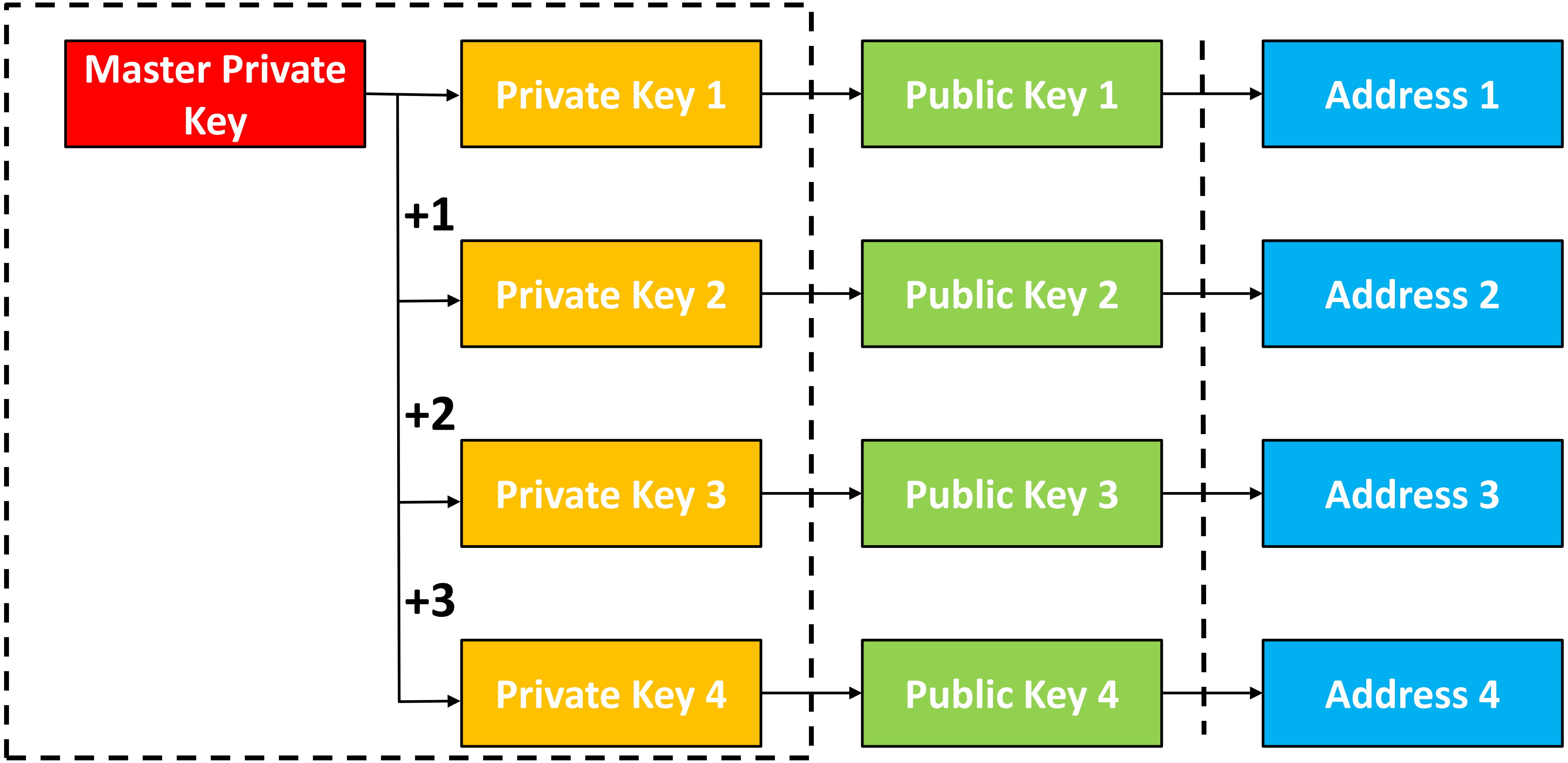
+2

Private Key 3 → Public Key 3 → Address 3

+3

Private Key 4 → Public Key 4 → Address 4

Hierarchically Deterministic (HD) Wallets


Master Private Key
Private Key 1
Public Key 1
Address 1
+1
Private Key 2
Public Key 2
Address 2
+2
Private Key 3
Public Key 3
Address 3
+3
Private Key 4
Public Key 4
Address 4