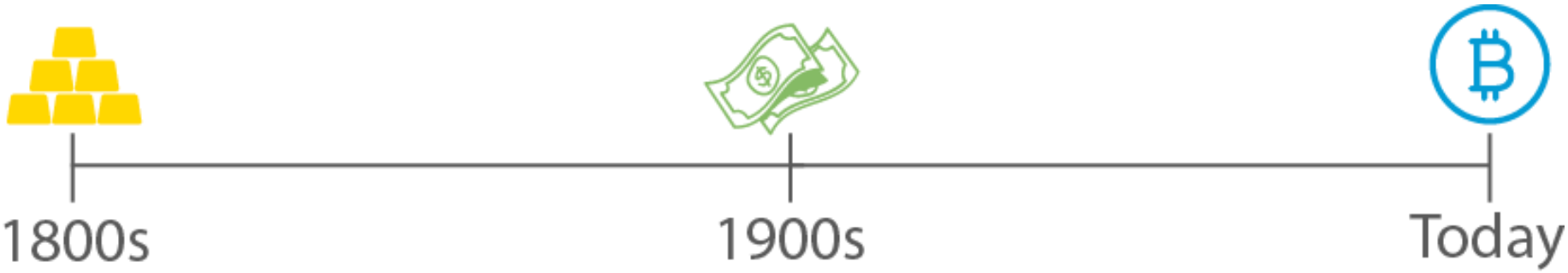
BlockChain Technology – Introduction



Nagendra Kumar Y
Date: 18/05/2017
Mail : ynkumar.nagendra@gmail.com

Agenda

- Basic Terminology in BlockChain
- What is current value of BitCoin?
- How to do Bitcoin transaction?
- What are types of BitCoin Wallets?
- Applications of BlockChain Technology
- Risks in Usage of Blockchain

Basic Terminology

- Block
- Chain
- Bitcoin
- Mining
- Ledger
- Block Reward
- Hashing
- Double spending
- Proof of work (PoW)

Bitcoin Price

-- H 130,371 L 64,996 ₹
₹

3M 1M 1W

Wallets


Electrum


Bitcoin Wallet


Copay


Airbitz


breadwallet


Bither


GreenBits


Mycelium


Green Address


Coinomi

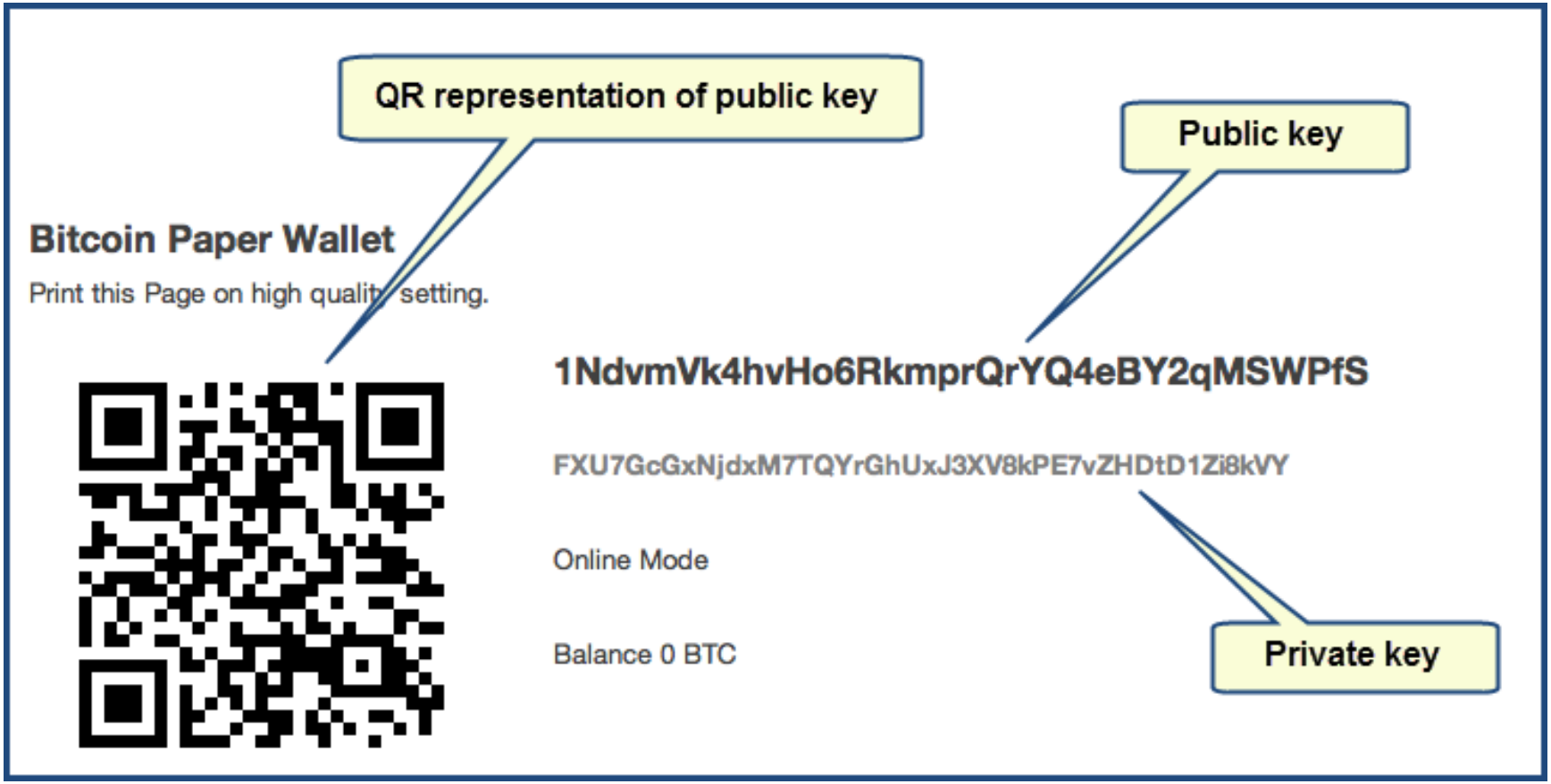

Coin.Space


Simple Bitcoin


ArcBit

BTC.com

Bitcoin – Transactions



Bitcoin– Transactions Contd..

- Each transaction is protected through a digital signature.
- Each transaction is sent to the “public key” of the receiver digitally signed using the “private key” of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the “private key”.
- The entity receiving the digital currency verifies the digital signature –thus ownership of corresponding “private key”--on the transaction using the “public key” of the sender.
- Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification.
- **Verification**
  - 1. Spender owns the cryptocurrency—digital signature verification on the transaction.
  - 2. Spender has sufficient cryptocurrency in his/her account: checking every transaction against spender’s account (“public key”) in the ledger to make sure that he/she has sufficient balance in his/her account.

Hashing

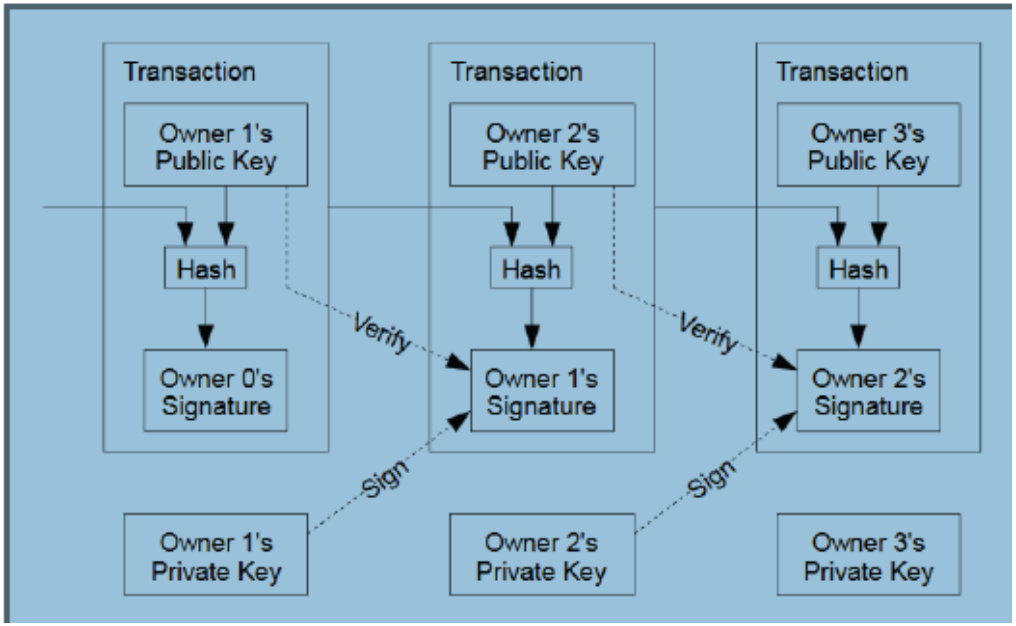
One-Way Computation

The best known cryptographic Hash functions are MD5, SHA1, SHA2.

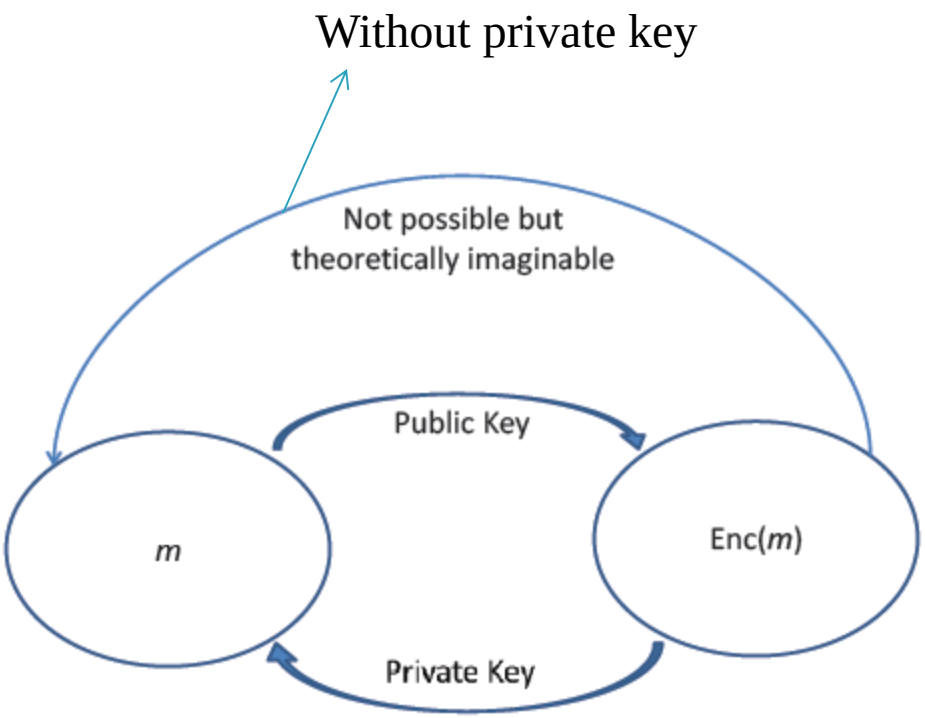
```
MD5("abc") = 900150983cd24fb0d6963f7d28e17f72
```

128- bit string shown in hex format.

Figure 3 (from the original Bitcoin paper of Satoshi Nakamoto)



Public Key Cryptography



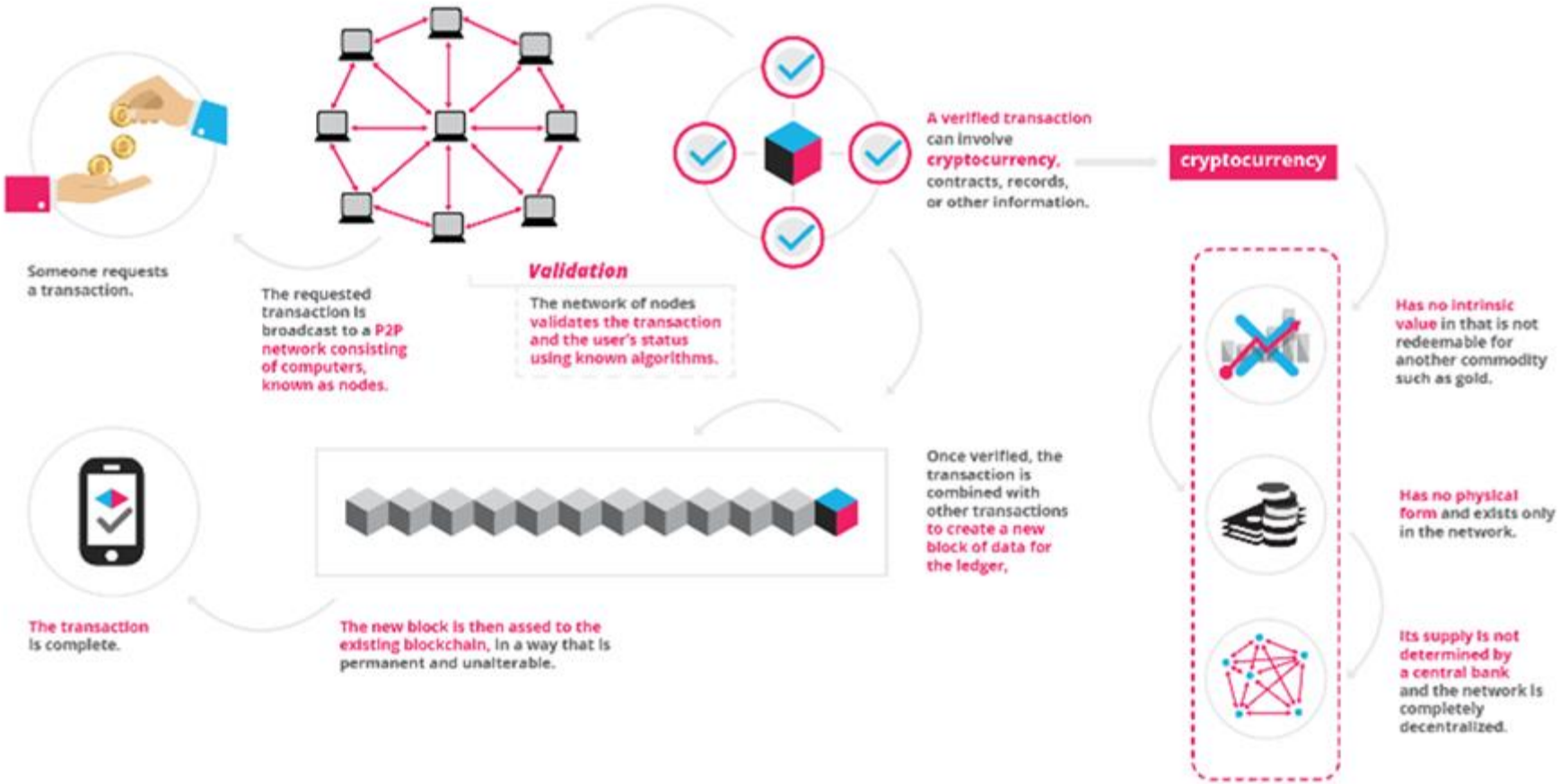
Rules for creating Block

1) Creating a new block requires significant computational effort.

2) Creating a new block is rewarding, so many would make effort to successfully create a new block, and

3) When branching occurs, the longest branch wins.

Transaction – Snapshot



How Blocks are viewd?

LATEST BLOCKS

SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
466928	8 minutes	1904	46,589.17 BTC	F2Pool	999.96
466927	9 minutes	2422	31,161.21 BTC	ViaBTC	999.14
466926	11 minutes	2840	47,784.18 BTC	BTC.com	998.28
466925	14 minutes	2509	59,206.56 BTC	ViaBTC	999.15

This information is available in blockchain.info

Applications

- Financial Applications
  - Coinsetter: New york Bitcoin Exchange.
  - Augur : Decentralized prediction market. (Buy & Sell shares)
  - BitShares: Earn interest on commodities (gold, H)
- Insurance:
  - Everledger: Diamond certifications & transactions
- Notary public:
  - Crypto Public Notary: notarize documents.
- Music Industry:
  - Ujomusic.com – Transparency

Applications contd..

- Data Storage
  - Storj : P2P cloud storage platform
- Internet of Things
  - IBM + Samsung = ADEPT(Autonomous Decentralized Peer-Peer Telemetry)
    - BitTorrent(File Sharing)
    - Ethereum (Smart Contracts)
    - TeleHash(Peer-To-Peer Messaging).
  - Filament – decentralized IOT Software stack
- Anti-Couterfeit
  - BlockVerify (Luxury Items, Diamonds, Certificates)
- Internet Applications – Name Coin – DNS Servers

Risks in BlockChain

- Behavior Change: Visa, MasterCard understanding BlockChain technologies.
- Scaling: Entire set of transactions download
- Bootstrapping: Migration includes lot of changes.
- Government Regulations: adoption of new type of payments.
- Fraudulent Activities: Money trafficking
- Quantum computing: theoretically impossible to decrypt the hash key. – If Possible?

Thank You