Bitcoin
The digital currency

Prepared by Sagar Chand
Supervisor - Professor Dheeraj Sanghi

BITCOIN

- Bitcoin is software-based online payment system described by Satoshi Nakamoto in 2008 and introduced as open-source software in 2009.
- Payments are recorded in a public ledger using its own unit of account (Bitcoin).

BITCOIN (contd..)

- It is a form of digital currency, created and held electronically. It can be used to buy things electronically and in that sense it is no different than conventional dollars.
- Bitcoin is commonly referred to as cryptocurrency and it can be divided into smaller unit called Satoshi (one hundred millionth of a BTC).

WHY?

- Trusted payment
- No 3rd party
- No double spending

INTRODUCTION TO CRYPTO

- SHA 256
- Hash Pointer (key)(hash is collision free)
- Merkle Tree SPV(Simplified Payment Verification)

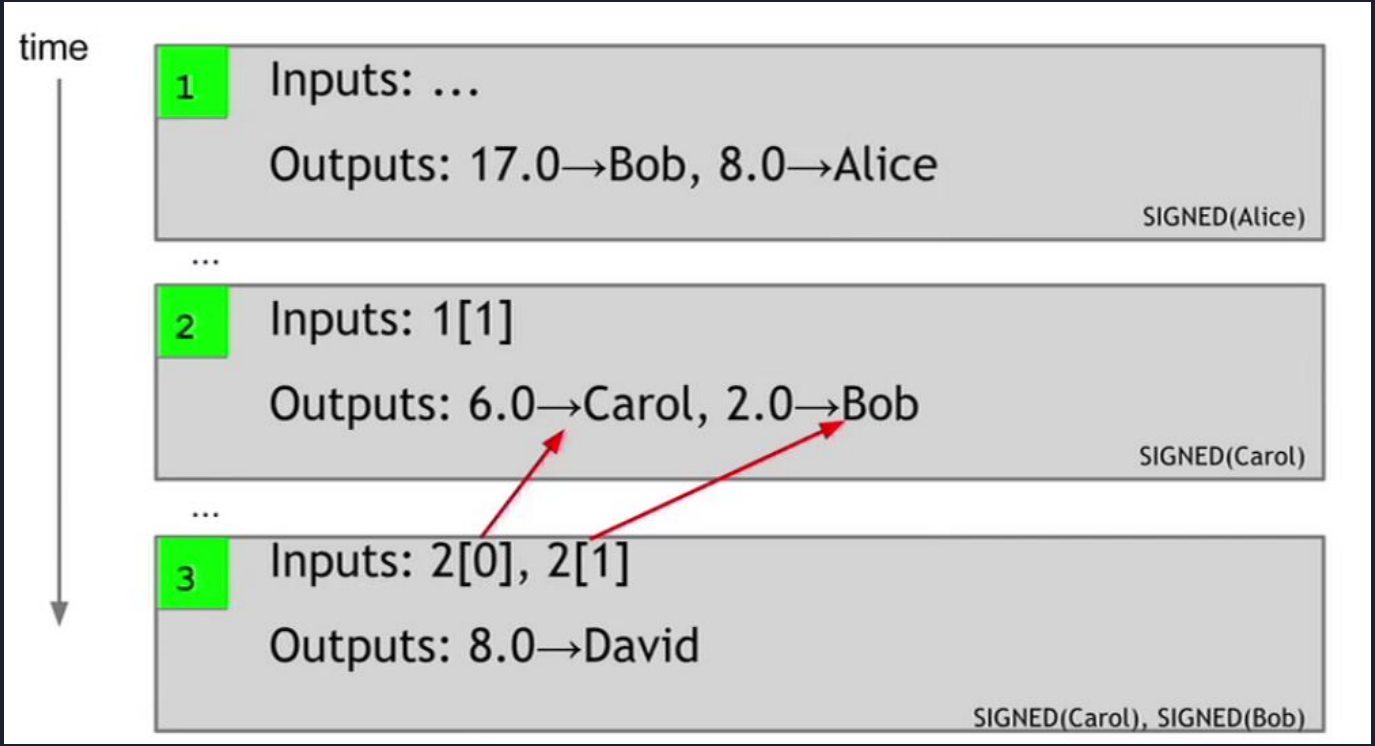
DIGITAL SIGNATURE

- (sk, pk) = generateKeys(keySize)
- sig = sign(sk, message)
- isValid = verify(pk, message, sig)

sk is secret signing key

pk is public verification key

BITCOIN TRANSACTION



time

1

Inputs: ...

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

...

2

Inputs: 1[1]

Outputs: 6.0→Carol, 2.0→Bob

SIGNED(Carol)

...

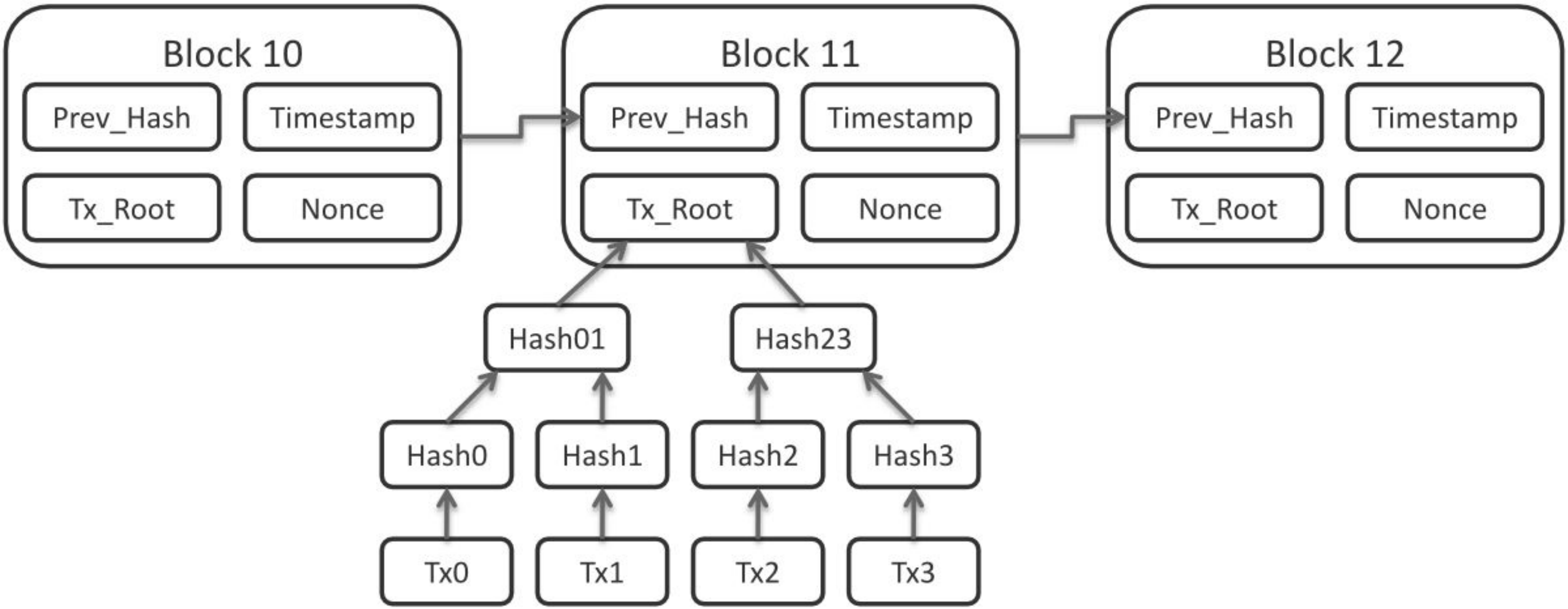
3

Inputs: 2[0], 2[1]

Outputs: 8.0→David

SIGNED(Carol), SIGNED(Bob)

BITCOIN BLOCK



BITCOIN DECENTRALIZATION

- Distributed consensus
- Consensus without identity Algorithm(Block-valid-valid sign and unspent)
- Incentive and proof of work Hash Puzzle 10^20 or 2^67 in 2014

DISTRIBUTED CONSENSUS

- Based on IP
- Nodes have outstanding transactions
- Transaction propagation
- ‘d’ zeros in start of hash
- 40 sec for 95% reach of nodes
- 6 blocks ideal

BITCOIN DECENTRALIZATION

- Distributed consensus
- Consensus without identity Algorithm(Block-valid-valid sign and unspent)
- Incentive and proof of work Hash Puzzle 10^20 or 2^67 in 2014

BITCOIN NETWORK

- P2P Network
- Joining the network
- 5-10K fully validating nodes
- UTO(Unspent Transaction Output)
- Lightweight nodes

P2P NETWORK

- TCP Protocol
- Random Topology
- All nodes are equal
- New nodes can join any time
- Forget non responding nodes after 3h

BITCOIN NETWORK

- P2P Network
- Joining the network
- 5-10K fully validating nodes
- UTO(Unspent Transaction Output)
- Lightweight nodes (~20 MB)

RACE CONDITION

- Default: Accept what you hear first
- Network position matters
- Miners may implement other logic

DETAILS

- $112B in marketcap (April’18)
- 149GB chain size (April’18)
- 3 most transacted crypto currency
- Deflatory
- 21 million in 2140

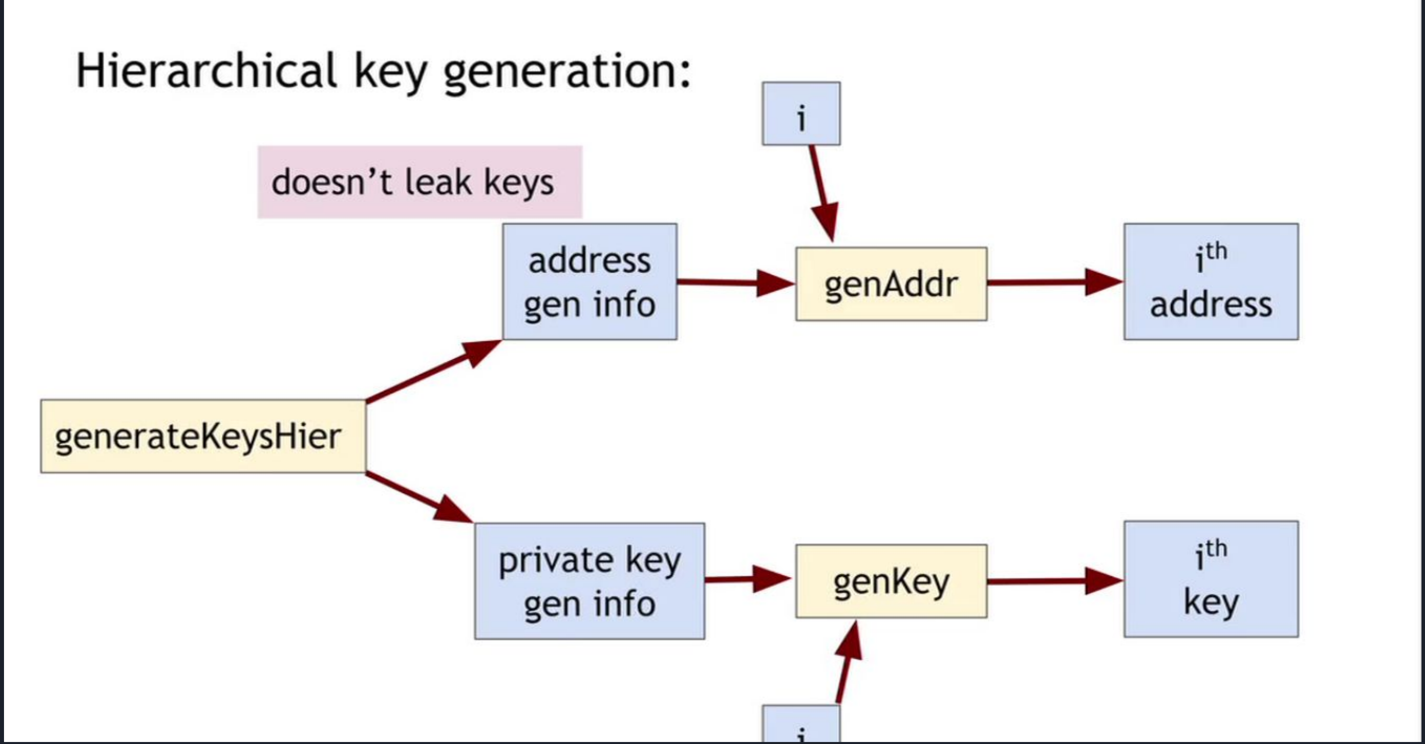
MINING

- Difficulty 2^66 in 2014. Chosen every 2 weeks. Coinbase transactions. 10 min for a block
- Mining pools 1 pool manager. G Hash in 2014 >50%. Reduced to increase trust in system

KEY STORAGE

- Reason
- Offline storage
- Wallet Software
- Split control (k of n)
- Hot and cold storage

HOT and COLD STORAGE



Hierarchical key generation:

ALTCOINS

- New
- Forking

PROBLEMS and SOLUTIONS

- Multiple blocks created at exactly same time
- Attack - Changing a value in a block
- Goldfinger Attack Destroy stability of smaller chains- CoiledCoin by Eligius

LIMITATION and IMPROVEMENT

- 7 transaction/sec
- ECDSA can be broken
- Hard Fork
- Soft Fork

REFERENCES

- Coursera Course by Arvind Narayan - Bitcoin and cryptocurrency technologies
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2008

THANK YOU