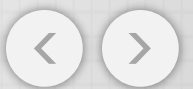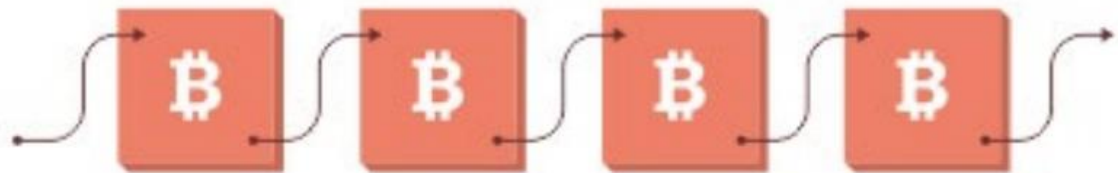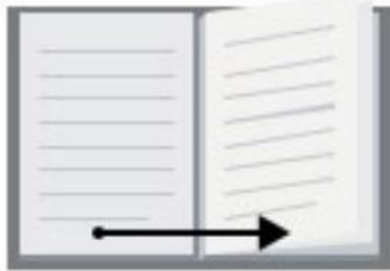# BLOCKCHAIN

WHAT IS BLOCKCHAIN? HOW IT WORKS?

WHAT IS BLOCKCHAIN

- A decentralized ledger tracking digital assets on P2P network
- Any real life example?
  - Records of your sales & purchases of raw material
  - Or may be simply your bank account statement
  - An excel sheets tracking all hospital equipments
  - Simply a large size book

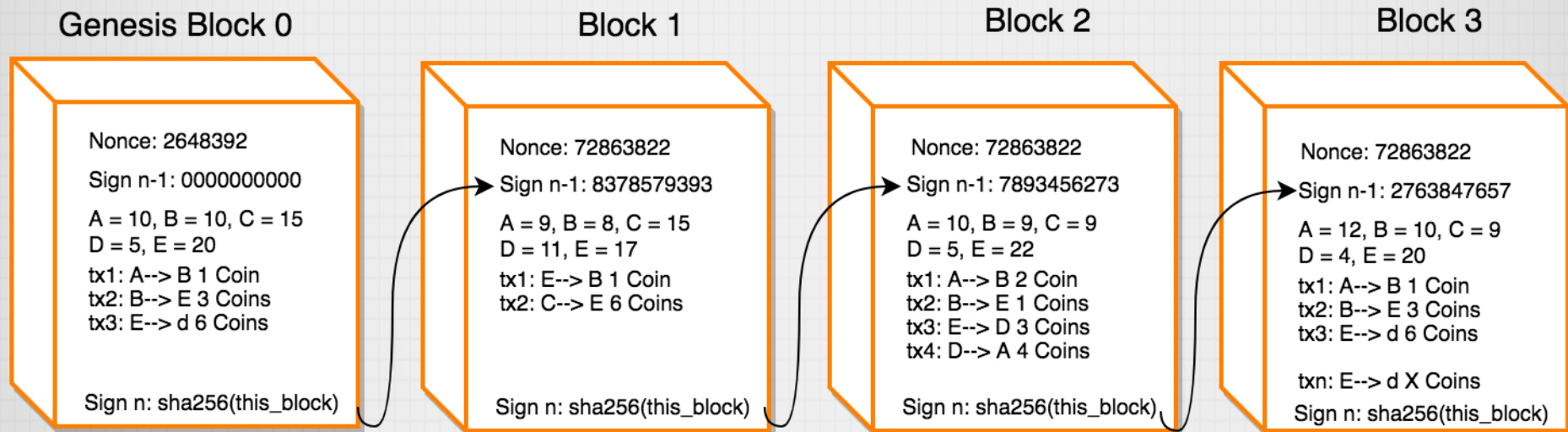*Blocks in a chain refer to previous blocks, like page numbers in a book.*

Ref: bitsonblocks.net

BOOK ANALOGY

- Imagine it as a old time book based ledger where each page reference to the previous page through a page
- Book = Blockchain, Page = Block, an entry in page = blockchain transaction
- Easy to detect if a page/block has been removed or deleted
- Easy to arrange the pages/blocks & identify suspicious activity. That's why page numbers are important in ledger.
- Since the pages/blocks are built tightly on top of each other it is impossible to temper a previous entry in the ledger without someone noticing it.

Ref: bitsonblocks.net

LET'S PEEK INSIDE BLOCKCHAIN

Genesis Block 0

Nonce: 2648392

Sign n-1: 0000000000

A = 10, B = 10, C = 15
D = 5, E = 20
tx1: A--> B 1 Coin
tx2: B--> E 3 Coins
tx3: E--> d 6 Coins

Sign n: sha256(this_block)

Block 1

Nonce: 72863822

Sign n-1: 8378579393

A = 9, B = 8, C = 15
D = 11, E = 17
tx1: E--> B 1 Coin
tx2: C--> E 6 Coins

Sign n: sha256(this_block)

Block 2

Nonce: 72863822

Sign n-1: 7893456273

A = 10, B = 9, C = 9
D = 5, E = 22
tx1: A--> B 2 Coin
tx2: B--> E 1 Coins
tx3: E--> D 3 Coins
tx4: D--> A 4 Coins

Sign n: sha256(this_block)

Block 3

Nonce: 72863822

Sign n-1: 2763847657

A = 12, B = 10, C = 9
D = 4, E = 20
tx1: A--> B 1 Coin
tx2: B--> E 3 Coins
tx3: E--> d 6 Coins

txn: E--> d X Coins
Sign n: sha256(this_block)

TELL ME EVEN MORE

- In case of real Blockchain, each block is built on top of the recent block and use its previous block's content/signature + Nonce (random string).
- Building a block & adding it in the Blockchain is the task of the miner nodes (optional).
- In public Blockchain it is made computationally difficult to add a block to prevent attacks.
- Miners try to guess a number (nonce) in such a way that if it gets crunched with the most recent block's fingerprint then it will create a new fingerprint which will be less than the last/most recent block in the Blockchain.
- It takes time & computational power to add a Block in the Blockchain. Hence there is a reward (12.5 BTC in case of Bitcoin Blockchain, 5 ETH in Ethereum)
- Private Blockchain can chose other methods to add a block as they can trust the miners using a contract etc.

DEFINITION?

- Lets build our own definition
- It's a decentralized database which stores information in the form of transactions
- It can be public or private
- Stored data is Immutable
- Highly secure
- Data gets recorded via consensus based algorithms
- Uses cryptography
- Generally exist over peer-to-peer network

So here is our definition:

"Blockchain is a consensus-based secure decentralized public/private database which stores information immutably over peer-to-peer network"

SUMMARY

- It is a decentralized distributed ledger (data structure) where data is being stored inside blocks in the form of transactions.
- Removes the dependency on the trusted third party for recording the data in Blocks.
- In public Blockchains, more complex algorithms are required to avoid malicious activities.
- Since each block is built on top of the previous Block, the immutability has been achieved.
- Here immutability means, very difficult to fake/alter a block & very very easy to detect the tampering.
- This all exist in the memory of the computers and runs as a computer process.
- Every participant of the Blockchain contains almost same copy of the Blockchain ledger.

OUR CONTACT DETAILS

COMPANY: Blockchain Council

WEBSITE: https://www.blockchain-council.org

EMAIL: training@blockchain-council.org

fb.com/blockchaincouncil

@chaincouncil

THANK YOU FOR YOUR TIME