


Block Chain Technology

Dr. Siddhartha Roy

- 
- Why use block chain technology
 - Basic cryptographic techniques behind block chain technology
 - RSA and Digital Signature
 - Block Chain Architecture
 - Some typical Application of Block chain Technology

Introduction

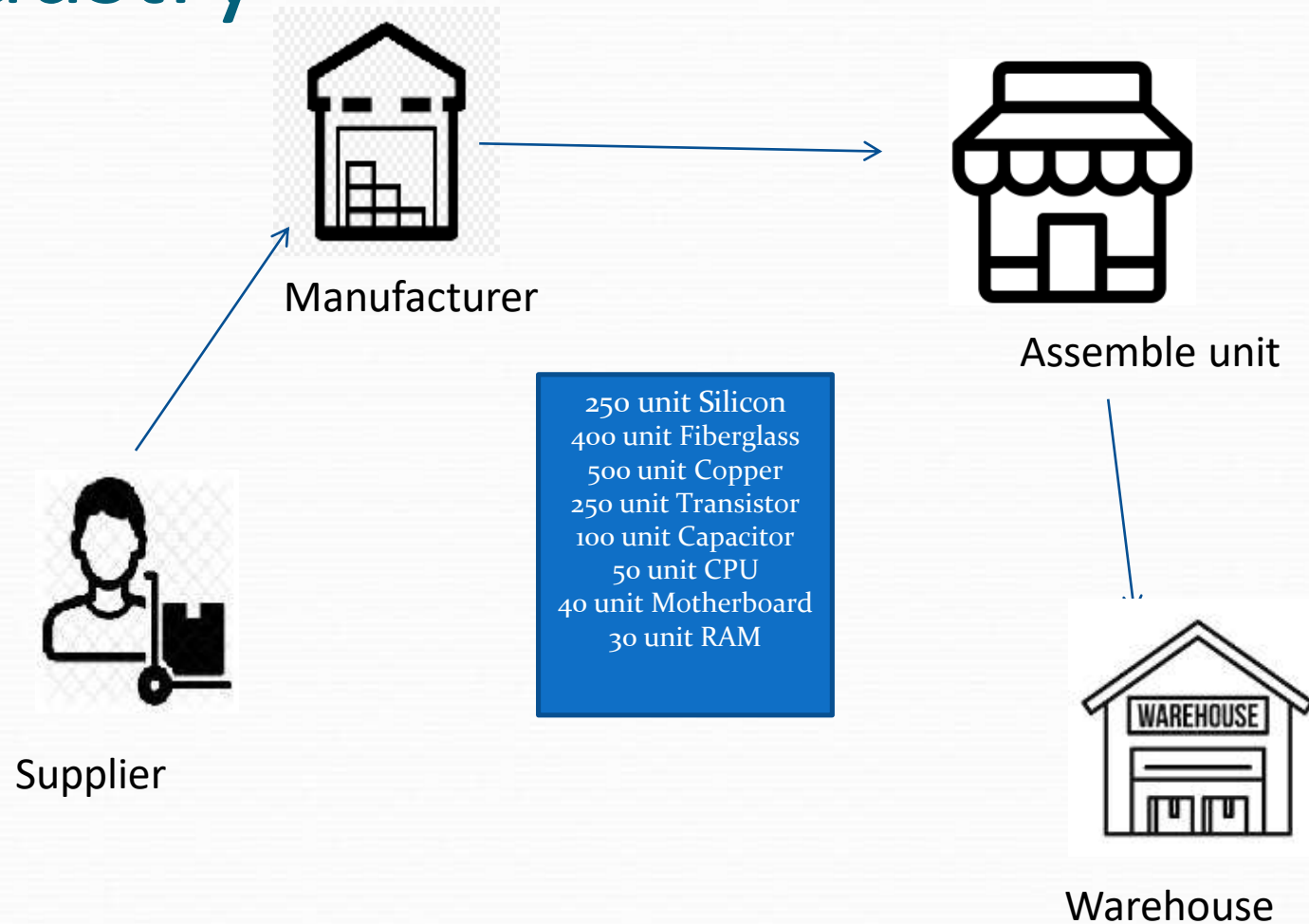
- Blockchain is a system in which the information will be recorded in a way that makes it hard or impossible to modify, hack, or fraud the system. A blockchain is basically a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Blockchain is the backbone Technology of Digital CryptoCurrency(encrypted data string that denotes a unit of currency) such as BitCoin, Ethereum, Litecoin etc.

Successful Supply Chain implementation

- Required Strong coordination among business entities
- Getting Real time information from business entities.
- How to get real time information ? Through Web based portal?
- What is the guarantee that the information submitted is correct?
- If any one denies the information later on?
- We need decentralized solution where no one trust each other but they should cooperate with each other
- Block chain is the solution

- In a business network of different players (businesses, enterprises, Government or Private bodies, or even the individuals)
- Everyone has one objective to fulfill their goal
- They do not trust each other
- . Proper cooperation is required to obtain desired goal
- **Trust less Decentralization = Blockchain**

Typical Scenario of Supply Chain of Computer Industry

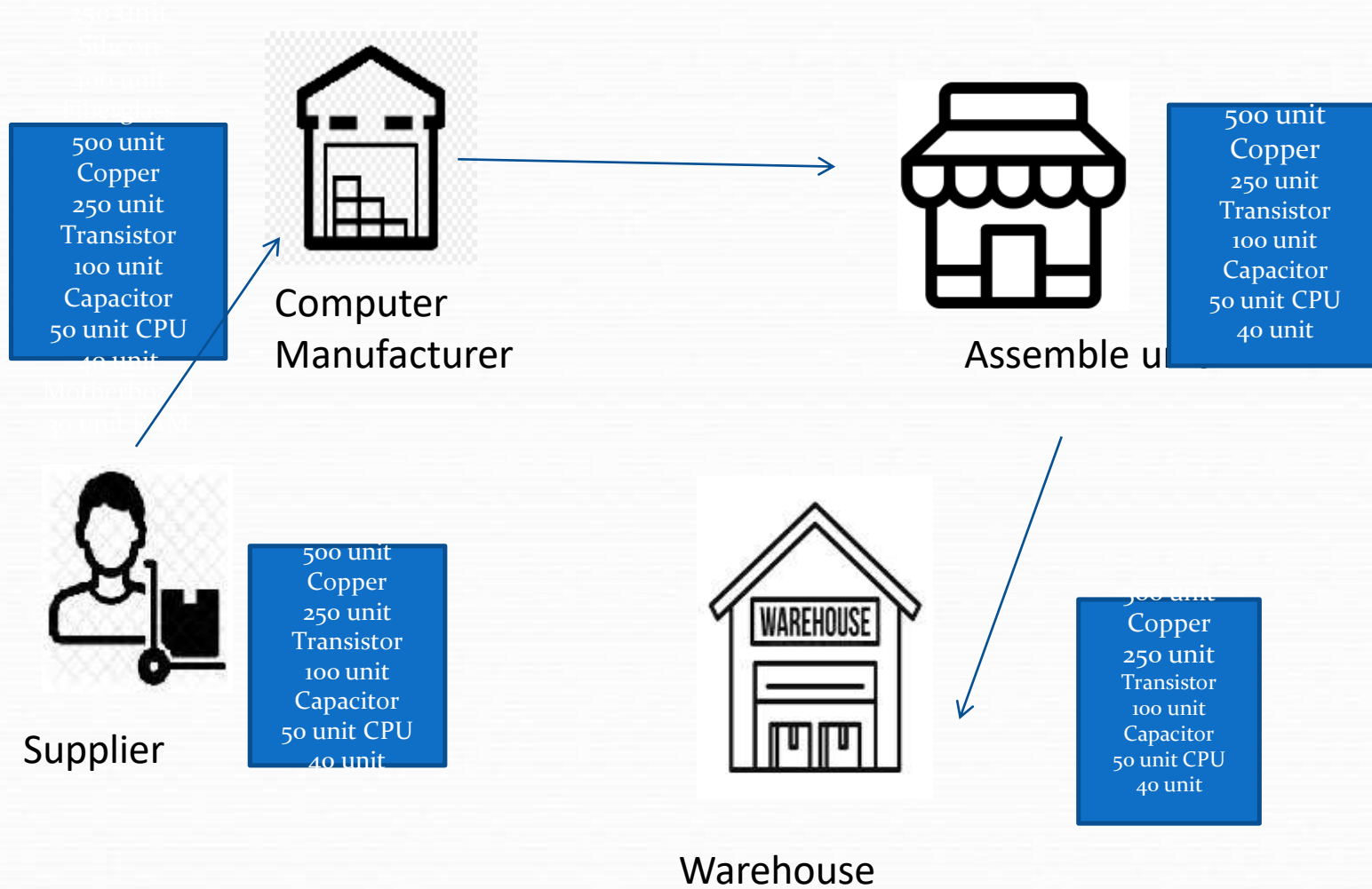


Basic assumptions

- A board is shared with all the business entities
- The board has infinite space, where information can not be deleted
- Everyone can view all the logs and verify
- Any change in information is visible to everyone
- Once the information entered cannot be deny later

Some issues

- Who will maintain this board? Cloud service provider?
- Who will bear the cost ?
- Suppose one of the enterprise maintain private cloud but what is the guarantee it is not fraud?
- Let everyone maintain the same copy of the board individually and independently
- No one is the sole-owner of the data, but everyone has a copy of the data
- There is no central database



- **Everyone holds exactly the same copy of the data at the same instance of the time**
- **An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later**
- **There is no central database to store the chain**
- **Everyone keeps a copy of the chain and processes data locally**
- **New information is added to the chain in the form of new blocks**
- **Blockchain ensures that every party has the same view of the blockchain always**
- **The Information is transparent to everyone –so everyone can verify and validate**
- **A decentralized immutable append-only public ledger**

Definition of Block Chain

- An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later.
- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Basic cryptographic techniques behind blockchain technology

- **Hash Function:** Used to connect the “blocks” in a “chain” in a tamper-proof way
- **Digital Signature:** Digitally sign the data so that no one can “deny” about their own activities. Also, others can check whether it is authentic.

Message Digest

- Message Digest is procedure that maps input data of an arbitrary length to an output of fixed length
- Takes any arbitrarily sized string as input
- Input M: The message
- **Fixed size output** (We typically use 256 bits in Blockchain)
- Output $H(M)$: We call this as the message digest
- **Efficiently computable**

Characteristics of Hash Function

- **Deterministic**
- Always yields an identical hash value for identical input data
- **Collision-Free**
- If two messages are different, then their digests also differ
- **Hiding**
- Hide the original message

More Characteristics on Hash function

- Hash functions are irreversible Given an x , it is easy to find $H(x)$. However, given an $H(x)$, **one cannot find x**
- It is **difficult to find x and y** , where $x \neq y$, but $H(x) = H(y)$
- For a 256 bit hash function, the attacker needs to compute 2^{128} hash operations –this is significantly time-consuming
- If every hash computation takes only **1 microsecond**, it will need $\sim 10^{25}$ years

- If $H(x)=H(y)$, $\Rightarrow x=y$
- We need to remember just the hash value rather than the entire message – we call this as the **message digest**
- To check if two messages x and y are same, i.e., whether $x=y$, simply check if $H(x)=H(y)$
- This is efficient because the **size of the digest is significantly less than the size of the original messages**
- SHA256 is used in Bitcoin mining –to construct the Bitcoin blockchain

Basic concept of Cryptography

- **Symmetric Key Cryptography**
 - Same key used for encryption and decryption
 - How to share the key securely
- **Public Key Cryptography**
 - One key for encryption, one for decryption
 - Handles several requirements like those in blockchain

Public Key Cryptography

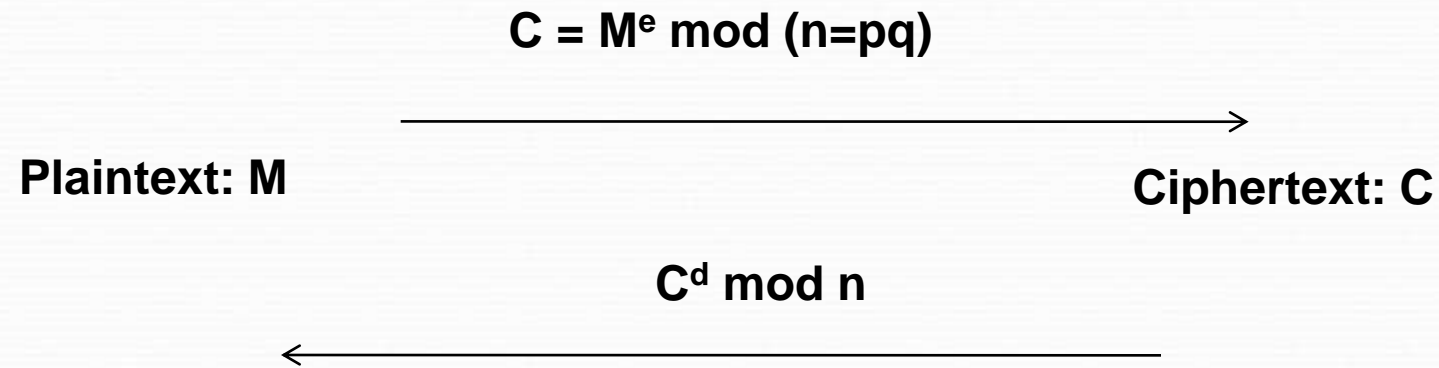
- The key should be of sufficient length –increasing the length makes the key difficult to guess
- The key should contain sufficient entropy, all the bits in the key should be equally random
- **Encryption:** The key is used to convert a plain-text to a cypher-text;
 $M' = E(M, k)$
- **Decryption:** The key is used to convert the cypher-text to the original plain text; $M = D(M', k)$

Public Key Encryption –RSA

- Invented in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman
- The encryption key is public and decryption key is kept secret (private key)
- Anyone can encrypt the data
- Only the intended receiver can decrypt the data

RSA Key Generation and Distribution

- Chose two distinct prime integers p and q
- p and q should be chosen at random to ensure tight security
- Compute $n=pq$; n is used as the modulus, the length of n is called the key length
- Compute $\phi(n)=(p-1)(q-1)$ (*Euler function*)
- Choose an integer such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; e and $\phi(n)$ are co-prime
- Determine $d \equiv e^{-1} \pmod{\phi(n)}$: d is the *modular multiplicative inverse* of $e \pmod{\phi(n)}$
- [Note $d.e \equiv 1 \pmod{\phi(n)}$]



From n , difficult to figure out p,q
From (n,e) , difficult to figure d .
From (n,e) and C , difficult to figure out M s.t. $C = M^e$

Source: Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)

Example

- $p = 11, q = 7, n = 77, \Phi(n) = 60$
- $d = 13, e = 37$ ($ed = 481; ed \bmod 60 = 1$)
- Let $M = 15$. Then $C \equiv M^e \bmod n$
 - $C \equiv 15^{37} \bmod 77 = 71$
- $M \equiv C^d \bmod n$
 - $M \equiv 71^{13} \bmod 77 = 15$

Digital Signature

- A **digital signature** is used to authenticate an electronically transmitted document
- **Purpose of Digital Signature**
- Only the **signing authority** can sign a document, but everyone can verify the signature
- Signature is **associated with** the particular document
- Prevent *non-repudiation* –sender will not be able to deny about the origin of the document

Evolution of Crypto currency

- 2011: Litecoin got introduced
- 2015: Ethereum network went live
- Sometime around 2016: Term "Blockchain" got popular
- 3rd January 2009: Nakamoto mined the first block of the Bitcoin network(called the genesis block)
- 2013: Coinbase reported selling US\$1 Million worth of Bitcoin
- But, why should someone solve the puzzle?

Mining a block in bitcoin network

- Consider an open network where all nodes are connected and don't trust each other.
- There are special nodes, called the Miners
- Miners propose new blocks –solve the puzzle (find the nonce corresponding to a target block hash), and add the solution as a proof of solving the challenge to be the leader
- Why someone would want to be the leader?
- Earn money (bitcoin) by solving the puzzle!
- Mining a Block: The Reward

- Encourage the community to participate in the mining through incentives
- Produces new Bitcoins in the System
- The Bitcoin network works like a Reserve Bank to regulate the flow of Money (Bitcoin) in the market, but without governance intervention or monitoring
- The miner who is able to solve the puzzle becomes the leader
- The block from the leader is appended in the blockchain

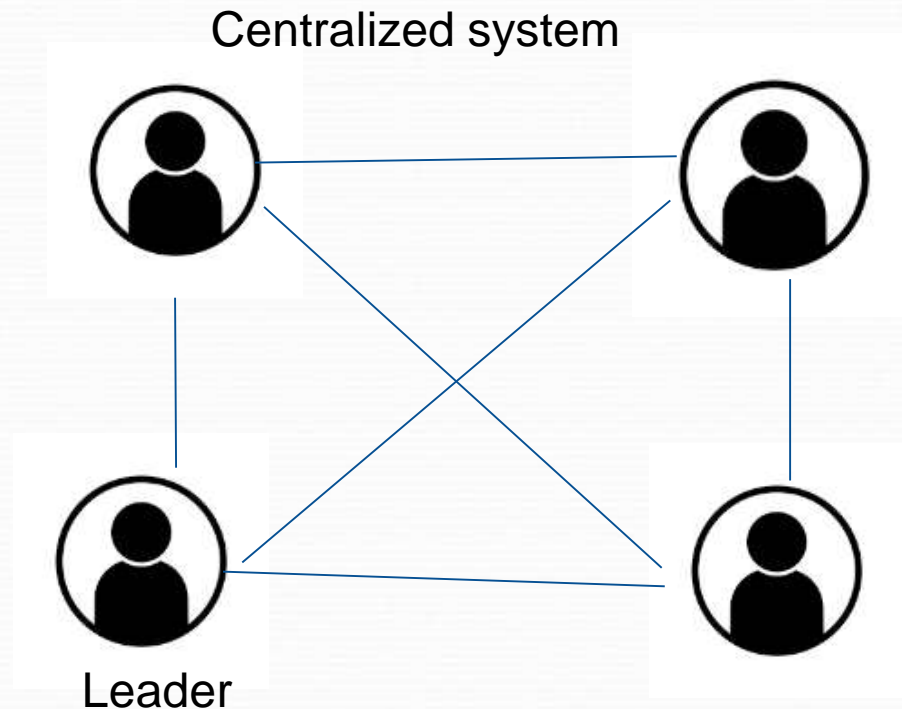
Role of miners

- The network is open
- But nobody knows each other
- A Puzzle will be generated from the system
- Everyone tries to solve it
- One who gives the solution first becomes the leader
- Whatever the leader says, everyone agrees to that

Consensus mechanism in block chain

- Every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

Consensus mechanism in block chain



All the decisions are taken by the leader or a board of decision makers.

This isn't possible in a block chain because a block chain has no "leader". For the block chain to make decisions, they need to come to a consensus using "consensus mechanisms".

- *Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the “favourite” of each individual. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment.”*
- [Source:Wikipedia](#)

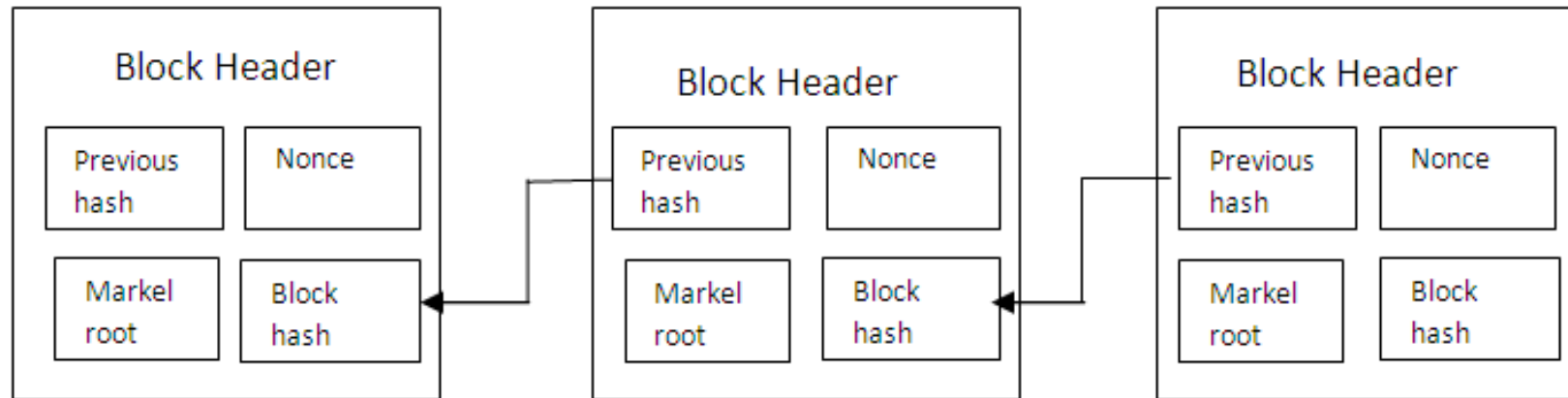
Block Chain Architecture

- Basic assumption
- Multiple organizations or individuals spanned over who may not **trust** each other
- An append-only shared ledger of digitally signed and encrypted transactions replicated across a network of peer nodes
- Digitally signed and encrypted transactions “verified” by each peers

Structure of a Block

- A block is a **container data structure** that contains a series of transactions
- **In Bitcoin:** A block may contain more than 500 transactions on average, the average size of a block is around 1 MB (an upper bound proposed by Satoshi Nakamoto in 2010)
- May grow up to 8 MB or sometime higher
- Larger blocks can help in processing large number of transactions in one go.
- But longer time for verification and propagation
- Two components:
 - **Block Header**
 - **List of Transactions**

Block chain

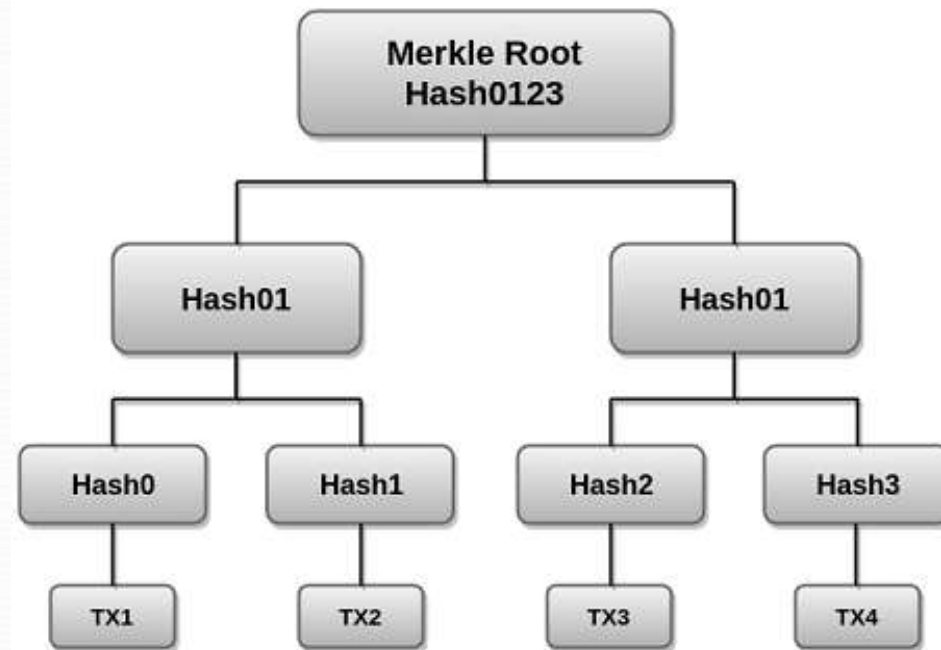


- Block hash
- Previous block hash: Every block inherits from the previous block –we use previous block's hash to create the new block's hash –make the blockchain **tamper proof**
- Merkle tree root
- Nonce

Merkle tree

- Merkle tree is a **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as **Hash Tree**.

Construction of Markle Tree



Source: <https://www.javatpoint.com/blockchain-merkle-tree>

Nonce

- Nonce is the central part of this Proof of Work. Nonce, short for “number used once”, is a random number that can only be used one time. Nonces are generated for a specific use, most often to modify the result of a function in a cryptographic communication.
- Typically, a nonce is a number that varies with time, in order to ensure that some values cannot be reused. It can be a timestamp or a special marker intended to prevent unauthorized reproductions of a file.

Some typical Application of Block chain Technology

Investment Management

Digital IDs (Passports, Personal IDs, Marriage Certificates)

Digitizing the land and property records

Supply Chain Management

Conclusion

- Blockchain is not a Bitcoin (or any other cryptocurrencies)
- Here we discuss the technology and its applications not the legal issues of
- Cryptocurrencies
- Anything in the world cannot be solved using a Blockchain . Blockchain is good but it is not one and only solution to change the society
- Block chain technology can be used for fraud prevention but there are better technology to solve that problem
- Blockchain is not a distributed database.
- A lack of awareness of the blockchain technology and understanding of how it works , especially in all other sectors other than banking

References

- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)
- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Blockchain: Blueprint for a New Economy Paperback(2015) by Melanie Swa
- <https://btc.com/btc/blocks>
- <https://www.businessinsider.com/blockchain-technology-applications-use-cases>
-



● Thank you