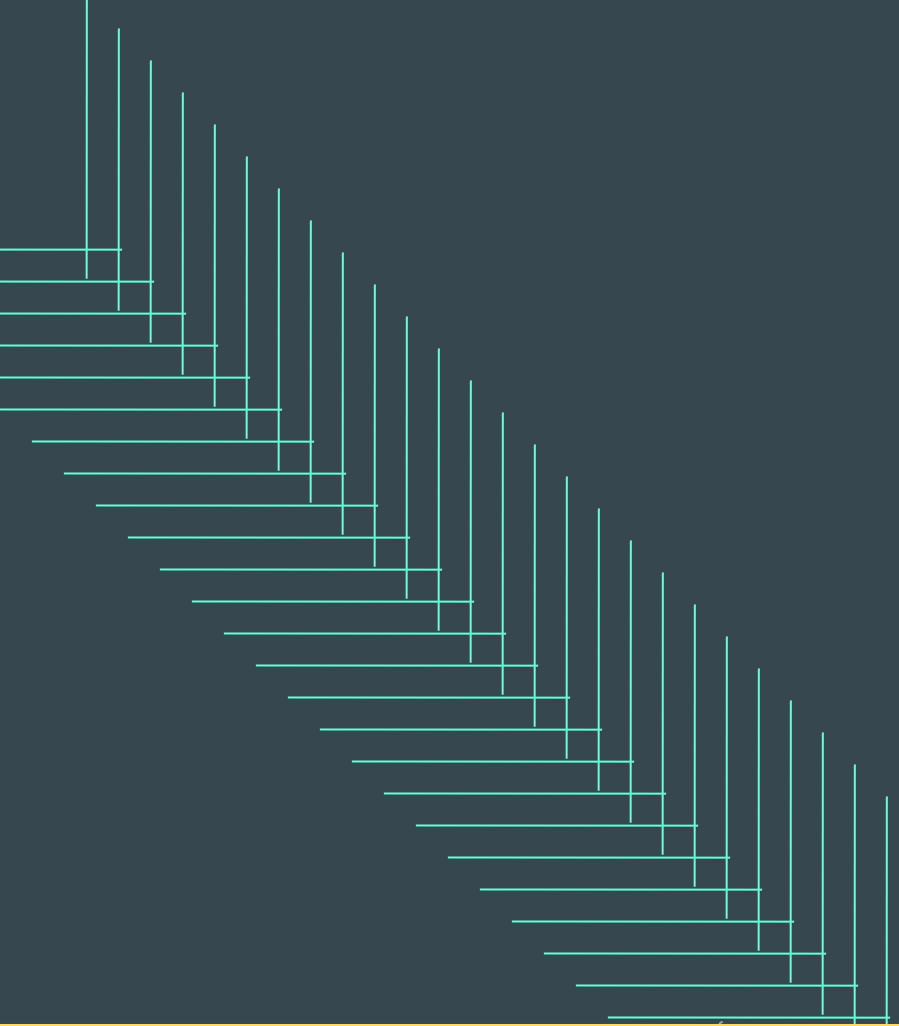


TELCOMA
AN ISO CERTIFIED COMPANY

Blockchain

Full course at
https://telcomaglobal.com

TELCOMA

Blockchain

Blockchain History :

- The very primitive form of the blockchain was Hash tree also known as Merkle tree.
- It performs validation of data in peer-to-peer network of computers.
- It was used to maintain and prove the integrity of data being shared.
- This became the backbone of Bitcoin.

Blockchain technology :

- It is a growing list of records , called blocks which are linked using cryptography.
- Blockchain technology created the backbone of new type of internet.

Blockchain types

Blockchain types :

- Public blockchain
- Private blockchain

Public blockchain

Public blockchain :

- These blockchains are open to the public and anyone can participate as a node in the decision making process.
- These blockchains are also known as permission less ledgers.
- Public blockchain is the model of Bitcoin , Ethereum and Litecoin and is essentially considered to be the original distributed ledger structure.

Public blockchain :

- This type of blockchain is completely open and anyone can join and participate in the network.
- It can send and receive transactions from anybody in the world, and can be audited by anyone who is in the system.
- Each node has as much transmission and power as any other, making public blockchains not only decentralized, but fully distributed as well.

Private Blockchain

Private Blockchain :

- Private blockchains are for the originator but are deployed in what is called a permissioned manner.
- Once the invitation is accepted, the new entity can contribute to the maintenance of the blockchain in the customary manner.
- A typical way for enterprises to use private blockchains is intrabusiness, ensuring that only company members have access.

Private Blockchain ：

- This sort of structure may not be entirely different from older digital structures as the public blockchain is, the technology is still highly powerful and the strong cryptography and auditability offers more security than traditional protocols.

How does Blockchain work..?

Working :

- Blockchain keeps a record of all data exchanges.
- It utilizes a distributed system to verify each transaction.
- Once signed and verified, the new transaction is added to the blockchain and can not be altered.

Working :

- Your keys are the private and public key and together they are combined to give you a digital signature.
- Your public key is how others are able to identify you.
- Your private key gives you the power to digitally sign and authorize different actions on behalf of this digital identify when used with your public key.

Working :

- Everytime a transaction occurs, that transaction is signed by whoever is authorizing it.
- Each transaction gets added to the ledger of the blockchain which includes a time stamp and a unique ID number.

Working :

- When this transaction occurs, it is broadcasted to a peer -to-peer network of nodes - basically other digital entities that acknowledge that this transaction has occurred and adds it to the ledger.
- Each transaction in that ledger will have the same data : a digital signature , a public key , a time stamp and a unique ID.

Working :

- The public key is a randomized sequence of numbers and letters.
- We are free to generate as many key pairs as you want and have multiple cryptocurrency wallets.

CAP theorem and Blockchain :

- C : Consistency
- P : Partition tolerance
- A : Availability

Eventual consistency , where consistency is achieved as a result of validation from multiple nodes over time.
Consensus algorithm called PoW in Bitcoin.

Decentralization in Blockchain

Decentralization :

- It uses a peer-to-peer network , copies of the ledger are stored in many different locations and unless you manage to track down every single of them , you can't destroy it.
- One of the most exciting aspects of blockchain technology is that it is entirely decentralized, rather than stored in one central point.

Decentralization :

- The decentralization nature of blockchain means that it doesn't rely on a central point of control.
- Rather than relying on central authority to securely transact with other users, blockchain utilizes innovative consensus protocol across a network to nodes to validate transactions and record data in a manner that is incorruptible.

Consensus protocol :

- It is a set of rules that describe how the communication and transmission of data between electronic devices such as nodes, work.
- Consensus protocols are the governing rules that allow devices that are scattered across the world to factually come to an agreement , allowing a blockchain network to function without being corrupted.

Decentralization :

- Cryptographic hash functions are used in this.
- The data is made even more secure by the fact that there is no reliance on a central point of storage, reducing the risk of it being lost or destroyed.
-

Benefits

Benefits :

- Greater transparency
- Enhanced security
- Improved traceability
- Increased efficiency and speed
- Reduced costs

Block structure

Block :

- A block is a container data structure.
- A block contains more than 500 transactions on average.
- It is composed of a header and a long list of transactions.

Block header :

The header contains metadata about a block.

- The previous blockhash .
- Mining competition .
- Merkle tree root

Block identifiers :

- To identify a block, you have a cryptographic hash, a digital signature.
- This is created by hashing the block header twice with the SHA256 algorithm.
- The block hash is a unique identifier.

Merkle trees :

- The transactions in a block are contained in a structure called a merkle tree or binary hash tree.
- A merkle tree is constructed by recursively hashing pair of nodes , until there is only one hash, called the root or merkle root.

Ledgers in blockchain

Ledgers :

- A distributed ledger is a database held and updated independently by each participant in a large network .
- The distribution is unique.
- Every single node on the network processes every transaction, coming to its own conclusions and then voting on those conclusions to make certain the majority agree with the conclusions.

ledgers :

- Distributed ledgers are a dynamic form of media and have properties and capabilities that go far beyond static paper based ledgers.
- The invention of distributed ledgers represents a revolution in how information is gathered and communicated.

Distributed ledger technology

Distributed Ledger :

- Blockchain organizes data into blocks , which are chained together in an append only mode.
- DLT could fundamentally change the financial sector, making it more efficient, resilient and reliable.

Distributed Ledger technology :

- This could address persistent challenges in the financial sector and change roles of financial sector stakeholders.
- It requires resolving consumer protection issues, financial integrity concerns , speed of transactions , environmental footprint, legal regulatory and technological issues.

Consensus protocol

Consensus protocol ：

- Consensus algorithm are designed to achieve reliability in a network involving multiple unreliable nodes.
- Consensus algorithm necessarily assume that some processes and systems will be available and that some communications will be lost.

Applications of consensus algorithm :

- Deciding whether to commit a distributed transaction to a database.
- Designating node as a leader for some distributed task.
- Synchronizing state machine replicas and ensuring consistency among them.

Consensus algorithm :

- It supports many real world systems including Google's page rank, load balancing, smart grid , clock synchronization and drone control.
- A blockchain can be thought of as a decentralized database that is managed by distributed computers on a P2P (peer-to-peer) network.

Consensus algorithm :

- The block is an encrypted hash proof of work that is created in a compute-intensive process.
- Other algorithms are PoW, PBFT, PoS and DPoS.

Blockchain Components

Components :

- A node application
- A shared ledger
- A consensus algorithm
- A virtual machine

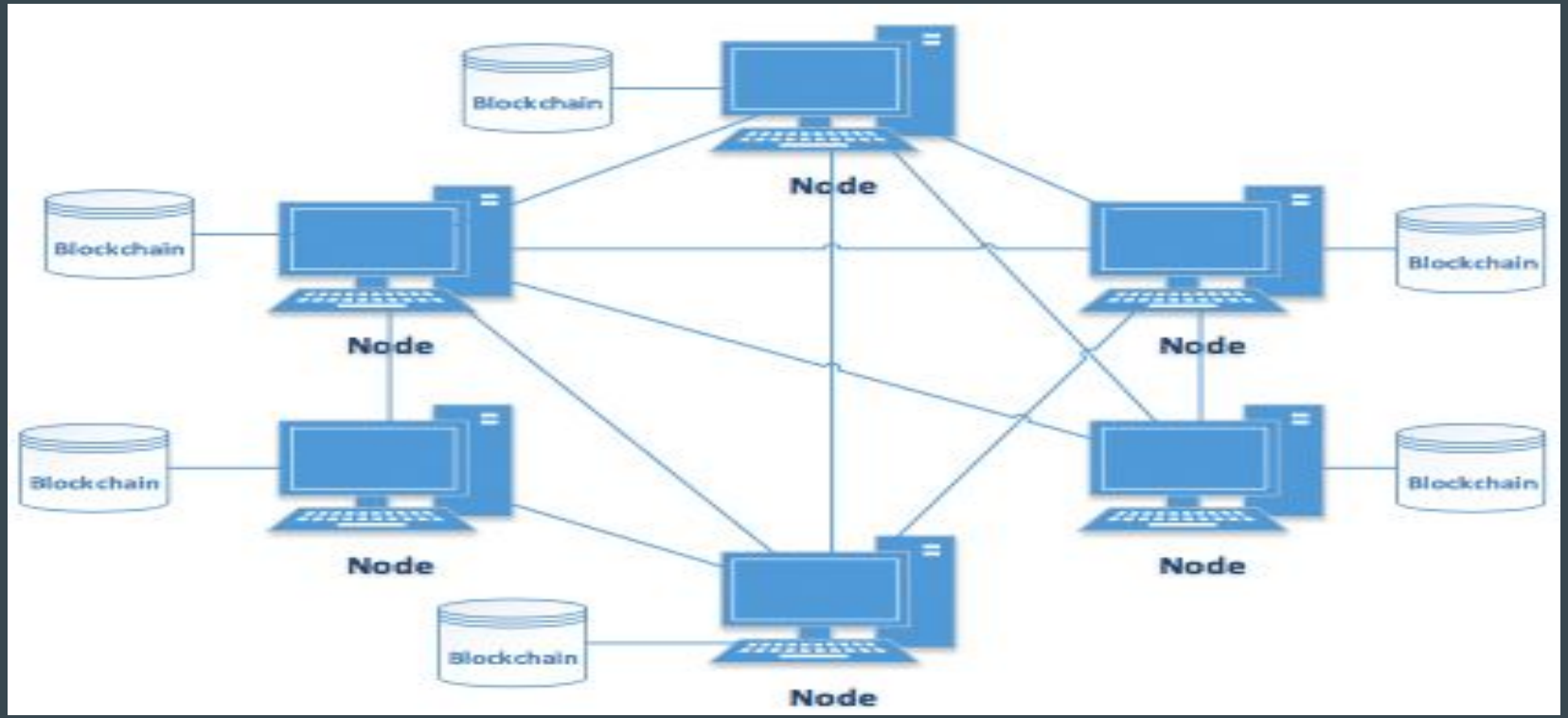
Node application :

- Each internet connected computer needs to install and run a computer application specific to the ecosystem they wish to participate in.

Node :

- A node can be any active electronic device, including a computer, phone or printer , as long as it is connected to the internet and has IP address.
- The role of a node is to support the network by maintaining a copy of a blockchain and in some cases to process transactions.

Node :



Shared Ledger

Shared ledger :

- A distributed ledger is a type of database that is shared, replicated and synchronized among the members of a decentralized network.
- The distributed ledger records the transactions , such as the exchange of assets or data , among the participants in the network.

Shared ledger :

- Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable , immutable history of all transactions in the network.

Role of business ledgers :

- Asset ownership and transfers are the transactions that create value in a business network.
- Business agreements and contracts are recorded in ledgers.

Blockchain application platforms

Platforms :

- Ethereum
- Hyperledger fabric
- R3 corda
- Ripple
- Quorum

Hashing

Hashing :

- It is the process of taking input of any length and turning it into a cryptographic fixed output through a mathematical algorithm.
- Inputs can include a short piece of information.

Securing data with hashing :

- Hashing drastically increases the security of data.
- A cryptographic hash function needs to have several critical qualities which are important to consider :

1. Impossible to produce the same hash value for different inputs.
2. This same message will always produce the same hash value.
3. Quick to produce a hash for any given message.
4. This is one of the foremost aspects and qualities of hashing and securing data.

Hashing :

- Hashing secures data by providing certainty that it hasn't been tampered with before being seen by the intended recipient.
- If the hashes don't match , you can be certain that the file was altered before you received it.

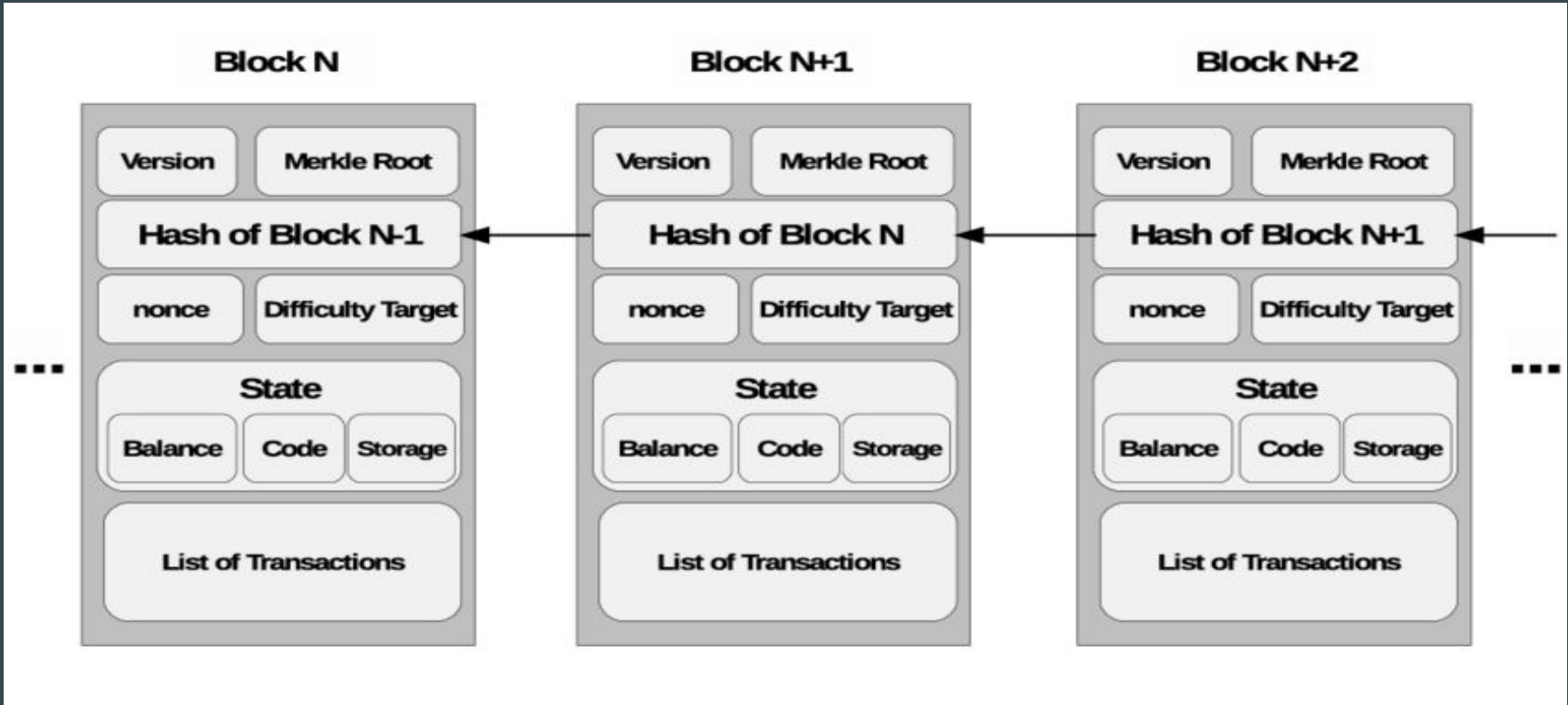
Blockchain hashing :

- In Blockchain, hashes are used to represent the current state of the world, the state of a blockchain.
- The slightest change to any part of the input results in a huge change to the output, in this lie the irrefutable security of blockchain technology.

Blockchain hashing :

- The first block of a blockchain, known as genesis block.
- Genesis block contains its transactions that , when combined and validated , produce a unique hash.
- This hash and all the new transactions that are being processed are the used as input to create a brand new hash that is used in the next block in the chain.

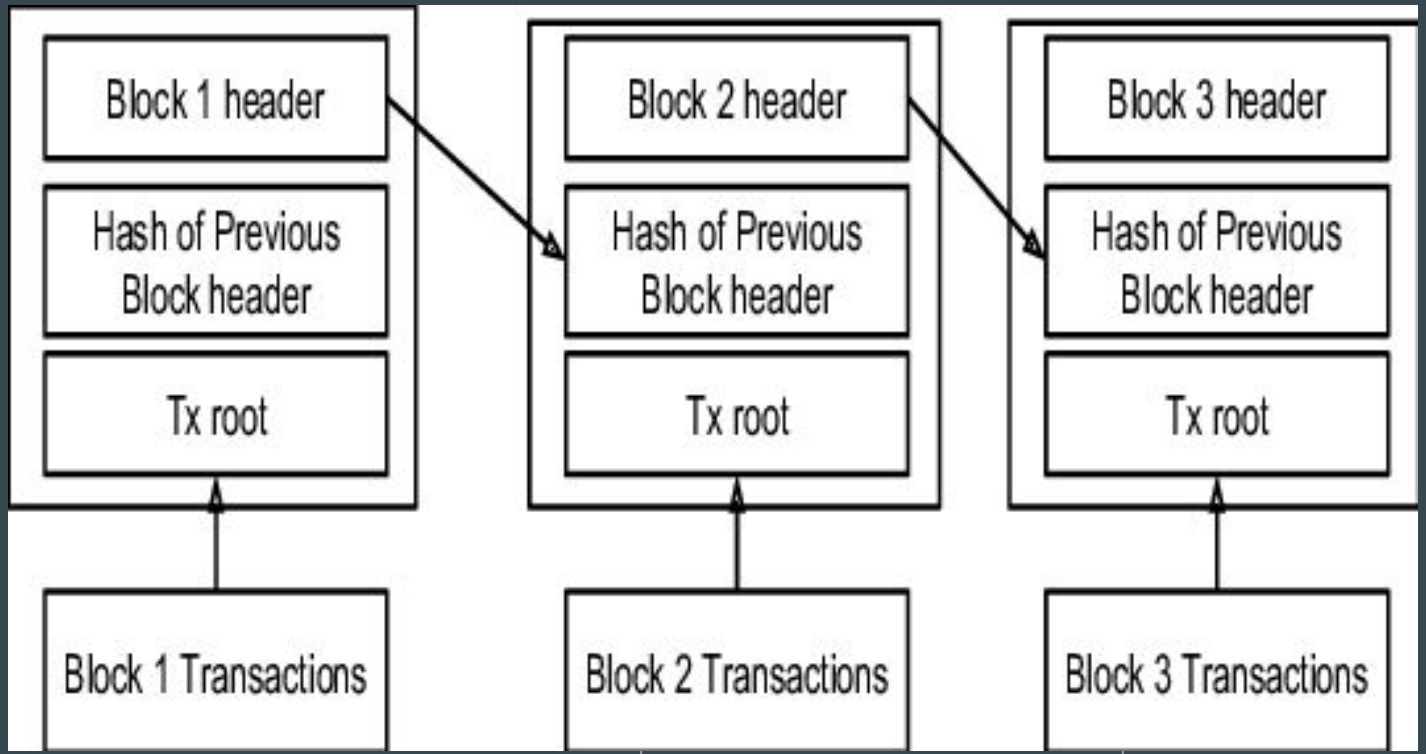
Structure of Blockchain :



Data structures :

- Data structures are a specialized way of storing data.
- Pointer store addresses via variables and as such point of the locations of other variables.
- Linked lists are a sequence of blocks connected to one another through pointers.
- A blockchain is simply a linked list of recorded transactions pointing back to one another through hash pointers.

Data structures :



TXID :

- A TXID is a transaction ID, produced by hashing transaction data and appearing in a string of numbers and letters , that can be used to identify and confirm a transaction has happened.

Merkle trees

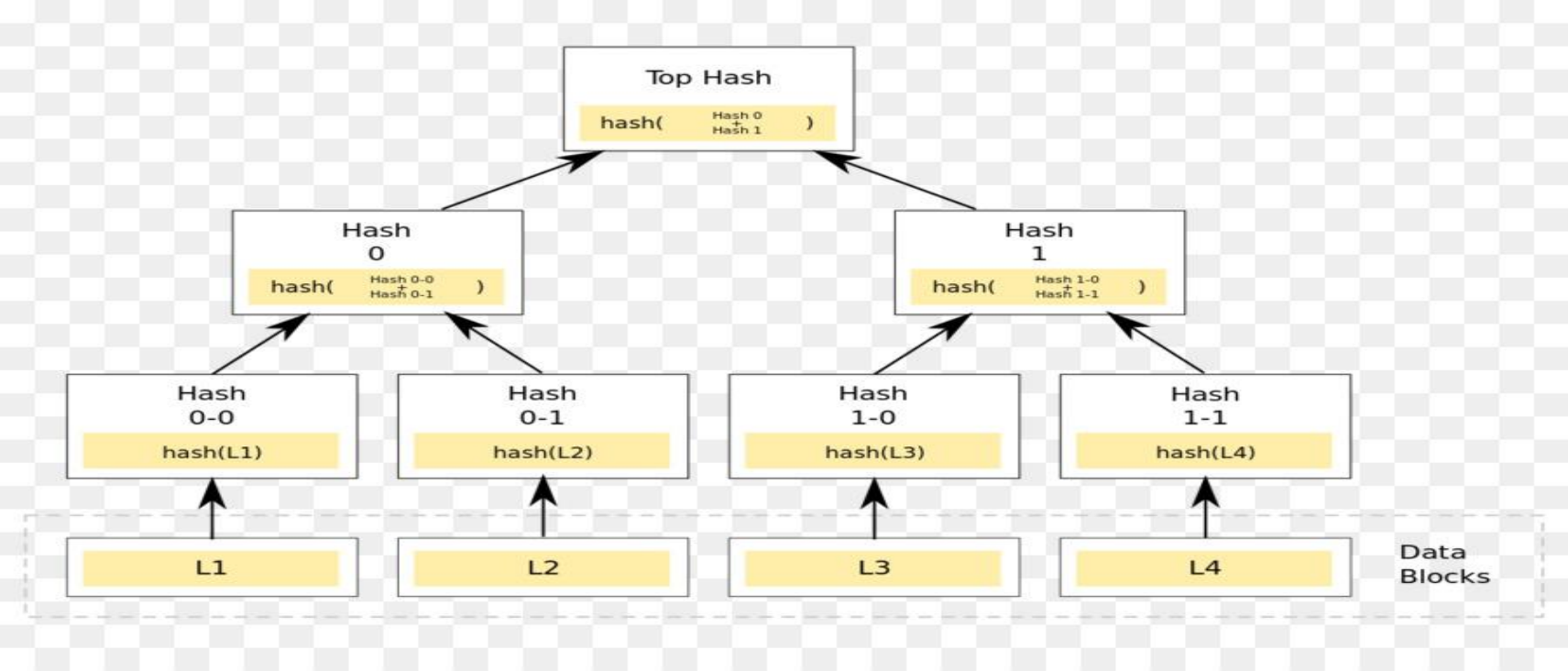
Merkle trees :

- A merkle tree also known as hash tree is a data structure of hashes used to record data onto a blockchain in a secure and efficient manner.
- The system works by running a block of transactions through an algorithm to generate a hash as a means of verifying the validity of that data based on the original transactions.

Merkle tree :

- An entire block of transactions is not run through a hash function at once, but rather each transaction is hashed, with those transactions being linked and hashed together .
- One hash for the entire block.

Merkle tree :



Merkle tree :

- Hashes on the bottom row are known as leaves.
- Middle hashes are reflected to as branches.
- Hash at the top referred as root.

Merkle tree :

- The hash of the merkle root is normally contained in a block header along with :

1. Hash of the previous block
2. Timestamp
3. Nonce
4. The block version number
5. The current difficulty target

Merkle tree

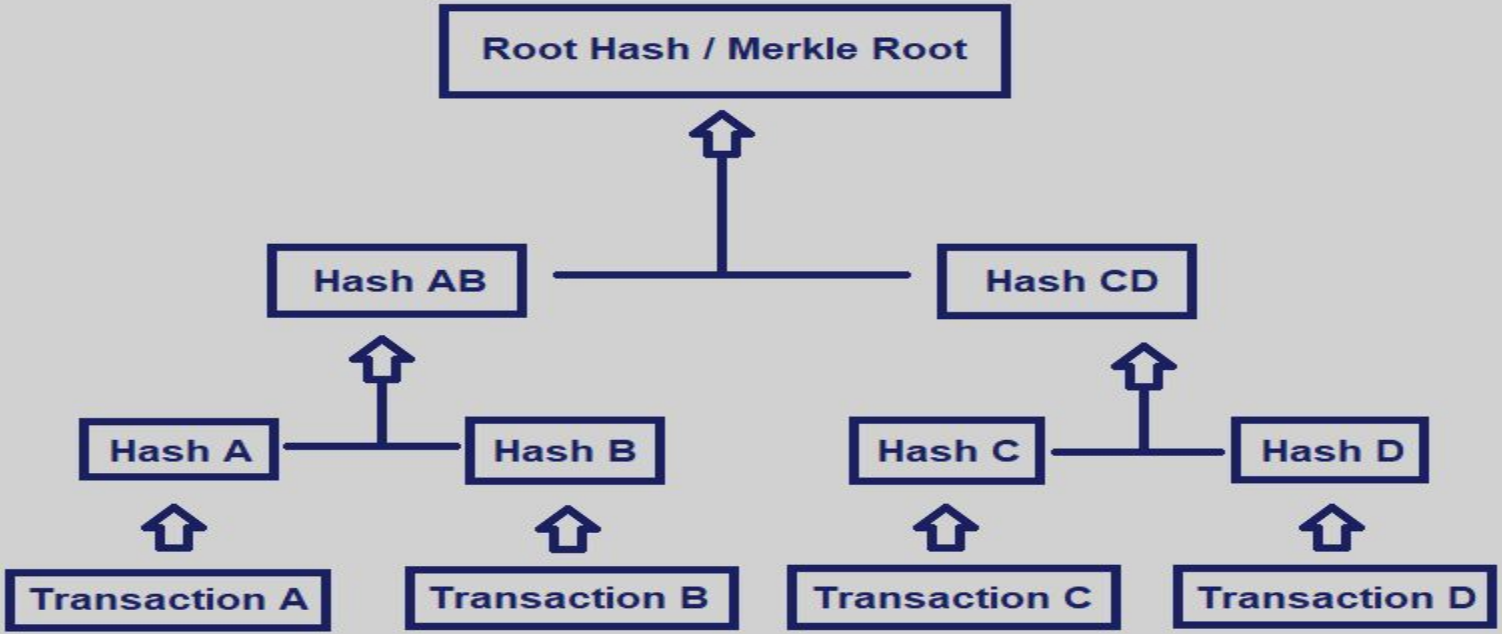
How do Merkle tree work ? :

- A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions , thereby enabling a user to verify whether or not a transaction is included in a block.
- They are constructed from the bottom up, from hashes of individual transactions (known as transaction IDs).

How does Merkle tree work ? :

- Each leaf node is a hash of transactional data, and each non-leaf node is a hash of its previous hashes.
- If the number of transactions is odd, the last hash will be duplicated once to create an even no. of leaf nodes.

How does Merkle tree works ：



How does Merkle tree work ? :

- Hashing Hash A and Hash B resulting in Hash AB and separately hashing Hash C and Hash D resulting in Hash CD.
- The two hashes are then hashed again to produce the Root hash.
- Hashing is usually conducted using the SHA-2 cryptographic hash function, though other functions can also be used.

How does Merkle tree works ? :

- The Merkle root summarizes all of the data in the related transactions, and is stored in the block header.
- Using a Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Merkle tree uses

Uses :

- They provide a means to prove the integrity and validity of data.
- They require little memory or disk space as the proofs are computationally easy and fast.
- Their proofs and management only require tiny amounts of information to be transmitted across networks.

Uses :

- Merkle tree benefits miners and users on the blockchain .
- A miner can calculate hashes progressively , as the miners receives transactions from peers.
- A user can verify parts of blocks individually and can check individual transactions using hashes of other branches of the tree.

SPV :

- It is a method of verifying if particular transactions are included in a block without downloading the entire block.
- Merkle trees are used extensively by SPV nodes.
- SPV only download block headers.

Cryptographic Hash functions

Cryptographic hash functions :

- Hash function : a hash function H takes a message x of arbitrary but finite size and outputs a fixed size hash h.
- Cryptographic hash function properties :

1. Easy to generate
2. Irreversible
3. Commitment
4. Collision free

Cryptographic hashing in blockchains :

- Cryptographic hash functions are simple mathematical algorithms which take the input of variable size and process it into an output of fixed size, known as hash which is entirely different from input.
- Every output value generated for a particular input value should be unique to avoid collision.

Hashing :

- Hashing algorithm thus ensure that all the blocks are well formed and tamper free, and thus blockchain will remain secure and virtually un - breakable.

Role of Nodes in Blockchains

Role of nodes :

- A computer can become the node of a blockchain network or can join the groups known as mining pools which forms the nodes.
- The smart contract powered machines can also act as node in programmable blockchains.

Role of nodes :

- Each node in the blockchain network holds a copy of the entire public ledger similar to a local database.
- The transactions to be added to the chain must be entered through the nodes with the public/private key pair of the participating individuals.
- Use of asymmetric key cryptography for authentication ensures integrity and non-repudiation across the blockchain network .

Cryptographgy

Cryptography :

- It includes techniques for electronic commerce, chip based payment cards , digital signatures , interactive proofs and secure computation etc.
- There are two kinds of crypto systems : symmetric and symmetric.

Symmetric cryptographic ：

- Two parties agree on a secret key and use the same key for encryption and decryption.

Asymmetric cryptography :

Public key cryptography

- It uses a public key to encrypt a message and private key to decrypt it.
- Use of asymmetric systems enhances the security of communication.
- Each party generates their own public-private key-pair.

Digital signature :

- Any message encrypted with a private key can only be decrypted with the corresponding public key.

Public key cryptography :

- Case of padlock

Brute force attack :

- A private key has minimum requirements as : it has to be a randomly generated number , it has to be a very large number, it has to use a secure algorithm for the generation.
- Every number could be guessed with enough computing power.

Consensus mechanisms

Consensus mechanisms :

- These are protocols that make sure all nodes are synchronised with each other and agree on which transactions are legitimate and are added to the blockchain.
- They make sure everyone uses the same blockchain.
- Without a good consensus mechanisms, blockchains are at risk of various attacks.

Types of consensus mechanisms :

- PoW
- POS
- DPOS

PoW :

- It is known as mining and nodes are known as miners.
- Miners solve complex mathematical puzzles which require a lot computational power.

POS :

- POS makes use of the premise that those who own most coins in a network and have a vested interested in keeping the network maintained and the value of it's coins high.
- Users can stake their tokens to become a validator , which means they lock their tokens up for a certain time.

DPOS :

- It is very fast consensus mechanism.
- In this, users can stake their coins to vote for a certain amount of delegates.

Consortium blockchains

Consortium blockchains :

- It is partly private.
- A consortium platform provides many of the same benefits affiliated with private blockchain - efficiency and transaction privacy e.g without consolidating power with only one company.
- Consortium blockchain operate under the leadership of a group instead of a single entity.

Blockchain interoperability

Blockchain interoperability :

- It is the ability to freely share information across blockchain systems.
- Projects that want to implement interoperability in their system aim to create a platform that will enable various different blockchains to communicate easily with each other, without the need for an outside intermediary.

Blockchain interoperability :

- The blockchain concept is characterized by :

1. Interaction
2. Exchange
3. Integration
4. Decentralization

Blockchain interoperability :

- # MetaHash aims to provide blockchain interoperability via #Metachains.
- Interoperability solutions are as complicated as they come in the cryptocurrency realm, we can categorize as : open protocols , multi - chain frameworks.

Open protocols :

- The most well-known open protocol for interoperability of blockchains is the atomic swap.
- Atomic swaps are cross-chain , decentralized services where there is no intermediary or trust needed.
- Interledger is an open-source , cross- chain atomic swap protocol that function as “ atomic swaps on steroids”.

Multi-chain frameworks :

- These are in essence, environments that help to facilitate open communication and transfer of both value and data between multiple blockchains, as part of a more extensive network.

Polkadot :

- It is a multi-chain framework of sub-chains to interact with each other seamlessly.
- The design of Polkadot falls into 3 tiers : Relay chain , Parachain , Bridges.

Cosmos ：

- It focuses on facilitating transactions between blockchains rather than smart contract data too.
- Cosmos is a decentralized network of blockchains powered by Tendermint.

When to use a Blockchain

When to use Blockchain :

- It offers new tools for authentication and authorization in the digital world that preclude the need for many centralized administrators.
- It enables the creation of new digital relationships.
- By formalizing and securing new digital relationships , the blockchain revolution is posed to create the backbone of a layer of the internet for transactions.

When to use blockchain :

- If the data and its history are important to the digital relationships they are helping to establish , then blockchains offer a flexible capacity by enabling many parties to write new entries into a system of record that is also held by many custodians.

When to use blockchain :

- A certain percentage of fraud is accepted as unavoidable.
- Private key cryptography enables push transactions , which don't require centralized systems and the elaborate accounts used to establish digital relationships.
- If this database requires millions of dollars to secure lightweight financial transactions , then there's a chance blockchains are the solution.

When to use blockchain :

- Speed of transaction the most important consideration

Multi-chain technology

Multi-chain technology :

- It is a platform that helps users to establish a certain private blockchains that can be used by the organizations for financial transactions.
- API and CLI helps to preserve and setup the chain.

Objectives of Multi-chain ：

- The Blockchain’s visibility should always be actively kept within the chosen participants to avoid confusions so as to ensure stability and control over which transaction exist.
- This blockchain model whereas only transacts the accounts validated to the participants of this chain.

The hand-shaking process :

- The process of hand shaking in Multichain occurs when the nodes in the blockchain connect with each other.
- The identity of each node represents itself with an address with a list of permissions.

Configuration :

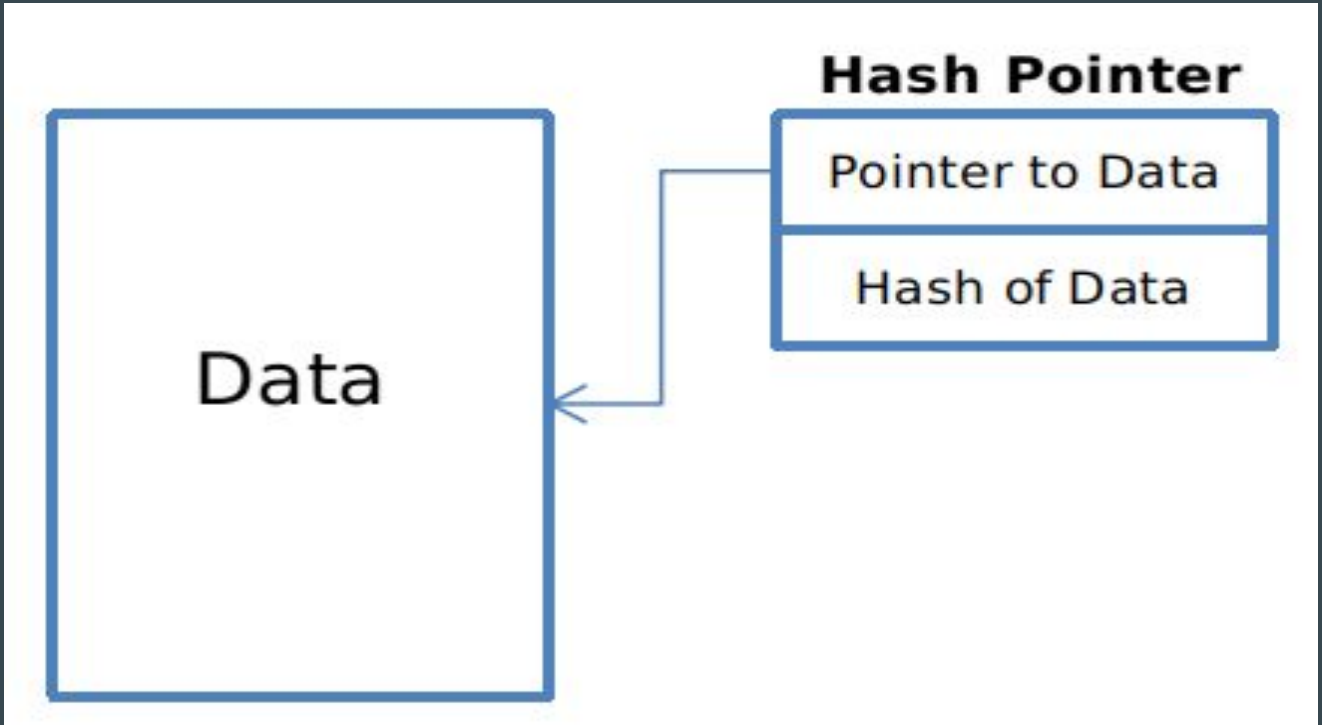
- The protocol of the chain
- Target time for the block
- Active permission type
- Mining diversity
- Mining incentive
- Approved type of transaction
- Maximum block size
- Maximum meta data per transaction

Hash pointer

Hash pointer ：

- It is basically a pointer to the place where some information is stored.
- It also stores the hash of the value that this data had when we last saw it.

Hash pointer ：



Use hash pointer to build data structure

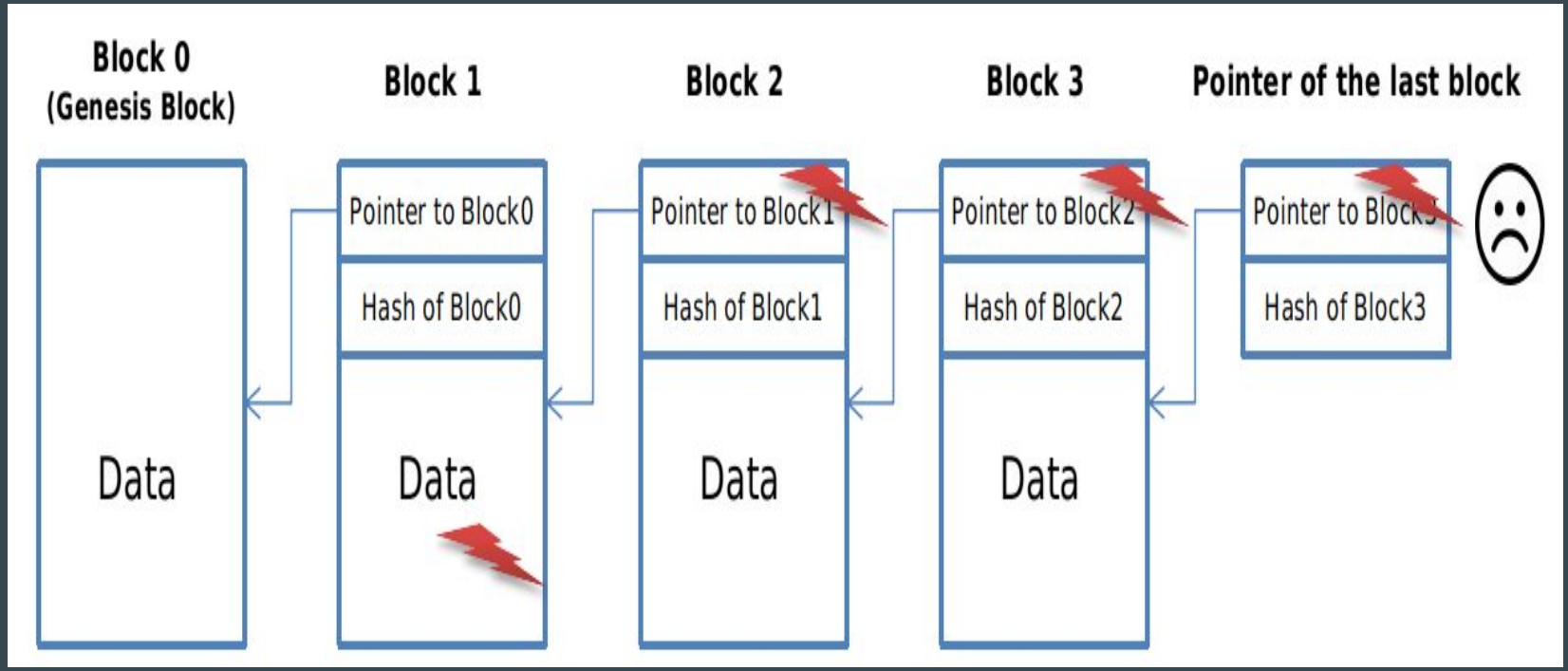
Use hash pointer :

- Take any data structure, link lists, binary search tree and implement it with hash pointers instead of pointers.
- Blockchain is like a regular linked list where you have a series of blocks containing data and a pointer to the previous block in the list.

Tamper evidence :

- If we want to build a log data structure that stores a bunch of data , so that we can add data at the end of the log and detect if somebody tries to mess up with data already present in the same block of log, it is tamper evidence.

Tamper evidence :



Ethereum

Ethereum ：

- It is a programmable blockchain.
- It is based on a peer-to-peer network protocol consisting of many computers worldwide.
- It allows its users to run pretty much any code they want.
- In ethereum, they also run the EVM.

Smart contracts :

- It allows people to deploy smart contracts on the blockchain.
- In ethereum, smart contracts can be written in solidity, an Ethereum specific programming language.
- Self execution results in that counterparty risks and moral hazards are essentially eliminated from the equation, as the control enforces its own provisions.

Tokens :

- A token is a new sort of digital property, the value of which is determined by supply and demand.
- A token grants a set of rights to its owner, in relation to the decentralized application it was created for.

Use cases and the “internet of value” :

- Anything can be coded and secured on its blockchain, other intermediary actors that provide trust could potentially be replaced.
- The internet distributed information in a manner that was not conceivable before the rise of technology.
- Ethereum is the biggest protocol that allows the creation of smart contract, DAo’s and DApps and could be the backbone of new internet.

Ethereum uses

Ethereum uses :

- It enables developers to build and deploy decentralized applications.
- It is a dapp that provides its users peer to peer electronic cash system that enables online Bitcoin payments.
- Decentralized apps are made up of code that runs on a blockchain network, they are not controlled by any individual or central entity.

Ethereum uses :

- It can also be used to build DAO (decentralized autonomous organizations).
- A DAO is fully autonomous, decentralized organization with no single leader.
- DAO's are run by programming code, on a collection of smart contracts written on the Ethereum blockchain.

Ethereum uses :

- It is also being used as a platform to launch other cryptocurrencies.
- Recently created a new standard called ERC721 token for tracking unique digital assets.

Benefits of decentralized ethereum platform :

- Immutability
- Corruption & tamper proof
- Secure
- Zero downtime

Ethereum ecosystem

DApp, iDApp & DAO

DApp :

- The application must be completely open source, it must operate autonomously and with no entity controlling the majority of its tokens.
- The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by consensus of its users.

DApp :

- The application must use a cryptographic token which is necessary for access to the application and any contribution of value should be rewarded in the application's tokens.

DAO :

- DAO concept evolved from DAC (Decentralized autonomous corporation) which is mainly for translating the human corporation organisation into autonomous computer org.
- It is an entity that lives on the internet and exists autonomously , but also heavily relies on hiring individuals to perform certain tasks that the automation itself do.

iDApp :

- It is intelligent DApp
- With the advancement of AI research, the autonomous driving is getting into level 3 or 4, so the new concept calling iDApp is proposed to fill the gap between DApp and DAO.
- iDApp uses blockchains instead of relying on blockchains.
- Public, consortium and private doesn't matter anymore.

Prospectus of Blockchain

Blockchain in banking & finance

Blockchain in banking & finance :

- The blockchain could potentially save banks billions in cash by dramatically reducing processing costs.
- Implementing blockchain would be a step to making banks increasingly profitable & valuable.
- All major banks are trying out blockchain which could be used for money transfers , record keeping and other back-end functions.

Benefits :

- Fraud reduction : most banking systems in the world, built on a centralized database, are more vulnerable to cyber attack because once attackers attack the one system they get full access . this technology would get rid of some of the current crimes committed online.
- KYC : blockchain would allow an organization to access the verification details of a client by another organization , thus avoiding repetition of the KYC process.

Benefits :

- Smart contracts : blockchains facilitate smart contracts as they facilitate storage of any kind of digital information, including computer code that can be executed once two or more parties enter their keys.
- Clearing & settlement
- Trade finance
- Payments
- Trading platforms

Blockchain in telecom

Blockchain in telecom :

- Telecom industry has the most complex operations framework, involving many partners, vendors, customers, distributors, network providers and VAS providers.
- There are a lot of trust issues and transparency challenges due to the involvement of multiple entities.

Use cases :

- Internal processes : OSS and BSS can be streamlined using blockchain.
- Roaming : blockchain can enable complex datasets across multiple parties, in real time with high trust and security, particularly for establishing subscriber identity.
- Smart connection : it helps with automatic generation of billing amounts and payments.

Use cases :

- Smart transactions
- Mobile money
- Identity management
- Way forward

Blockchain in Supply chain

Blockchain in supply chain :

- Blockchain creates solutions that impact all facets of the supply chain, with a particular focus on logistics.
- Traceability and traceability are some of the most important foundations of logistics.

Blockchain in supply chain :

This technology could improve the following tasks :

- Recording
- Tracking
- Assigning
- Linking
- Sharing

xChain2 :

- Blockchain technology is considered to be a game changer for decentralizing infrastructure and building a trust layer for business logic.
- It is envisioned to be a technology that could propel us into the next industrial revolution.

Benefits :

- Enhanced transparency
- Greater scalability
- Better security
- Increased innovation

Blockchain in Health care

Blockchain in Health care ：

- Drug traceability : the main characteristic of blockchain technology that is useful in drug traceability is security. To ensure the authenticity and traceability of drugs, the companies that register a product on the blockchain have to be trustworthy.
- The pharmaceutical companies decide which actors of the supply chain act as miners.

Blockchain in Health care ：

- Clinical trials : blockchain can provide proof-of-existence for any document and allow anyone to verify the authenticity of doc.
- Using bitcoin wallet, public and private key .
- The public key proves that a certain document was registered on the blockchain at a certain time.

Blockchain in Health care ：

- Patient Data management : blockchain can provide a structure for data sharing as well as security.
- The data is stored in organisation's existing database and/or on cloud computing systems.
- Smart contracts are used to manage patient data access.

Blockchain in Energy

Blockchain in Energy :

Problems with our current infrastructure :

- Energy inefficiencies
- Energy and our environment
- Energy inequalities

Blockchain in Energy :

Energy innovations and Blockchain

- Wholesale electricity distribution : A Blockchain startup , Grid+
- Peer to peer energy

Bitcoin

Bitcoin :

- It is not just a cryptocurrency , but also a new financial system comprised of many components.
- It relies on peer to peer network.
- It is a digital currency.

Bitcoin :

- It is a type of cryptocurrency.
- You can make transactions by check, wiring or cash.
- The purchaser decodes the code with his smartphone to get your cryptocurrency.

Bitcoin transactional properties :

- Irreversible
- Pseudonymous
- Fast and global
- Secure
- Permission less

Bitcoin Mining :

- Bitcoin mining requires a computer and a special program.
- Miners will use this program and a lot of computer resources to compete with other miners in solving complicated mathematical problems .
- About every 10 mins, they will try to solve a block that has the latest transaction data in it , using cryptographic hash function.

Bitcoin Miners :

- Initially Bitcoin miners were just cryptography enthusiastics.
- As the value of bitcoin has grown up , more people have seen mining as a potential business, investing in warehouses and hardware to mine as many bitcoin as possible.

Bitcoin

Balances- Blockchain :

- The blockchain is a shared public ledger on which the Bitcoin network relies.
- All confirmed transactions are included in the blockchain.
- It allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring they are actually owned by the spender.

Bitcoin :

- Bitcoin is made up of bit and coin.
- Coins are stored in computer.
- The creator of Bitcoin made three main concepts for Bitcoin that are essential in understanding how does Bitcoin work : cryptography , supply and demand and decentralized networks.

Bitcoin :

How do transactions happen :

- To record transactions, we need to put them in a database.
- Bitcoin uses a decentralized network, because the Bitcoin database is shared.

Bitcoin :

- When you create a Bitcoin wallet , you receive a public key and a private key.

Bitcoin Advantages & Disadvantages

Bitcoin Advantages :

- International payments are a lot faster than banks.
- Fees are low
- Blockchain - near impossible to hack
- Decentralized - can't be shut down at a single point.
- Transparent - you don't have to trust anyone.
- Anonymous - you don't need to use your name.
- No verification for new users.

Bitcoin disadvantages :

- Mining uses lots of electricity
- Not as fast as other cryptocurrencies
- Fees change a lot
- Anonymous - used for crime
- Difficult to use - private, public etc

Bitcoin values & Regulations

Bitcoin values & regulations :

- A single Bitcoin varies value in daily.
- Bitcoin currency is completely unregulated and completely decentralized.
- The value of each bitcoin resides within the bitcoin itself.

How Bitcoins are tracked ? :

- A bitcoin holds a simple data ledger file called a blockchain.
- Each blockchain s unique to each user and his or her personal bitcoin wallet.
- All bitcoin transactions are logged and made available in public ledger, helping ensure their authenticity and preventing fraud.

Banking & other fees to use Bitcoins :

- Three groups of bitcoin services : the servers (nodes) who support the network of miners, the online exchanges that convert your bitcoins into dollars, and the mining pools you join.
- The owners of some server nodes charge one time transaction fees of a few cents every time you send money across their nodes.

Bitcoin production facts :

- Bitcoin mining involves commanding your home computer to work around the clock to solve “ proof of work” problems.
- Each bitcoin math problem has a set of possible 64 digit solutions.
- Bitcoin mining is only profitable if you run multiple computers and join a group of miners to combine your hardware power.

Bitcoin security :

- People who take reasonable precautions are safe from having their personal bitcoin caches stolen by hackers.
- More than hacker intrusion, the real loss risk with bitcoins revolves around not backing up your wallet with a fail-safe copy.
- .dat file that is updated every time you receive or send bitcoins , so that .dat file should be copied and stored as a duplicate backup every day you do bitcoin transactions.