Page :
Date :

Blockchain Technology

* Introduction to Blockchain

* Cryptocurrency

* Programming in Blockchain

1. Introduction to BlockChain

What is Blockchain?

- A blockchain is append-only, cryptographically secured, distributed and replicated store of records.

In other words we can say that Blockchain is a decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other, to co-operate, co-ordinate and collaborate in a rational decision making.

The working of BlockChain

ASR for a Transaction

↓

The transaction is presented to all nodes in the network

↓

Nodes verify the transaction & details related to it using few techniques

↓

A validated transaction can involve anything like cryptocurrency, records etc.

↓

After Varification, a transaction is joined with other transactions to produce a new block of data for ledger

↓

The current Blockchain receives the new block as an addition

↓

The transaction is done

Page :
Date :

Write a short note on components of Blockchain

Terms or elemements used in or during the functionality of Blockchain are called as components of blockchain

1. Node: Computer, mobile or a hardware devile which is connected to blockchain network is called as a node.

Nodes are of two types:

i) Full Node: It maintain full copy of all transactions. Also it is able to validate, acapt & reject the transactions.

ii) Partial Node: It has only partial copy of a blockchain and generally used when user do not have enough space for full blockchain.

It connect to full nodes and use bloom filters to reciev only required data.

2. Ledger:
A ledger of all transactions is being maintained by every node in the blockchain network and the state of data that is being stored on the blockchain is maintained in the transaction. The ledger is replicated amongst all nodes in the network.

3. Wallet:
- It is a digital wallet which allows users to store native units of data (coins)
- Every node in blockchain has a wallet
- Privacy of a wallet is maintained using public/private key pairs.
- There are different types of wallets
  i) Hot Wallet: These wallets are connected to internet and are used frequently, almost daily. It has a high risk as hacker can attack over the internet.
  ii) Cold Wallet:
  These are not connected to internet and have low risk.

4. Nonce: It is a random number which is generated randomly and it can be used while adding the block. It acts as an important element or a key for creating block in block chain.

5. Hash:
A hash function can process data of any size and return a fixed size 'hash' of the original data after the operation. It has the following features:
1. Data is generated with a special hash
2. Because it is one dimension, we cannot recreate the data from its hash
3. A tiny change in the data results in a different hash.
4. It keeps the database small.

6. Mining:
It is a process by which forgers or miners verify new transactions and add them to the blockchain ledger
- To verify blocks of transactions that are updated on the decentralised blockchain ledger, complex cryptographic has puzzles must be solved.
- These puzzles require sophisticated tools and powerful computing power to solve. Bitcoins are given to miners as payment in return.

7. Consensus Protocol:

Blockchain consensus is the process by which the networks peers come to an understanding regarding the current state of the data.
This generates reliability and trust in the blockchain network
For example: Proof of work.

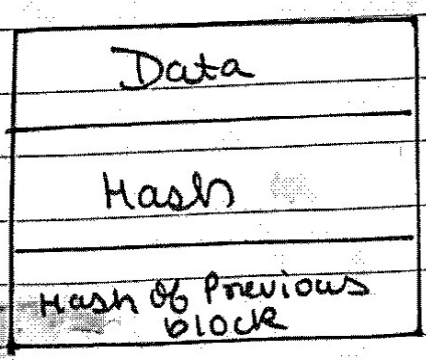
Page :
Date :

Block in Blockchain

- Block contain transactions which are digitally signed and encrypted and they are verified by the nodes.

- There can be multiple such transactions in a block. Now because they are encrypted and digitally signed this ensure that participants can view the information on the ledger that they are allowed / authorized to see.

- The header of the block is divided into or consists of six elements which are:
  a) The nonce
  b) The time in seconds
  c) The version number of the software
  d) The goal of the current difficulty
  e) the hash of previous block
  f) the root hash of market tree



Types of Blockchain

1. Public Blockchain

- In this, anyone with the internet can download entire blockchain, ledger, code also run a code.
- It is fully decentralized, distributed.
- No permission required to read transactions, initiate transactions, participate in consensus
- Nodes can remain anonymous using cryptographic protocols.
- Anonymity, transparency & immutability are valued over efficiency
- Standard consensus algorithm is Proof of work (PoW)
- No single point of failure because validation is done by all nodes

• Disadvantages

- Low transaction processing speed
- Mining & consensus required immense amount of energy
- 51% risk

Page : 8
Date :

2. Private Blockchain

- It is not open to public.
- Participants are known to each other
- Participants are pre approved by some organization.
- Owner / organisation controls the authority to write, read or audit.
- Transactions speeds very high
- Low energy consumption.

Challenges of private blockchain:

- Not decentralized.
- May prefer the traditional database if only trusted nodes are hosting
- Single point of failure.
- Many people dont consider it as blockchain.

3. Consortium Blockchain

- It is assumed or seen as a hybrid between public and private blockchain.
- Its a ledger which is distributed and anyone can download it or acess it and the consensus process is not controlled by one company but by the ~~pre~~ predetermined consortium of companies or ~~representative~~ representative intividuals.

Features:

- As compared to public blockchain they are faster
- They arent completely decontralized

Limitations of Blockchain

- Inability to process large amount of transactions within the own blockchain network
- No incentives for being a non mining full node. Growth of ledger makes it difficult and expensive for them to maintain full node.
- Although of being popular, invester still find it difficult to grasp the entire technology
- Lack of proper documentation.
- Educational institute needs time to develop proper curriculum.
- Lack of experienced developers.
- Security ~~to~~ Vulnerabilities arises due to bugs.

Advantages & disadvantages of blockchain

Advantages :

1. Because it is open to all, anyone can participate in the development of blockchain technology, no one permission is needed to join the distributed network

2. Cost reduction is an advantage because blockchain dosent need any third man so it reduces the cost for the business people and also gives trust

3. Blockchain eliminates any third party interference in transactions and eliminates errors, making the system more effictive and quick. Settlement is facilitated and made easy.

4. Each transaction is stored on a block connected to the others using hashing techniques, which gives blockchain a tighter securits. It stores transactions using the SHA256 hashing algorithm.

5. Blockchain technologies decentralised structure makes it impossible to tamper with data, any change will be reflected across all nodes, making it impossible to commit fraud. As a result transactions can be said to be tamper proof.

Disadvantages :

- There are issues in blockchain in some financial institutions. To adapt blockchain more widely, other technological facets will be necessary.

- The fact that blockchain databases are kept on every node of the network creates a storage problem, as the volume of transactions rises, more storage space will be needed

- Due to some environmental concerns, some nations have outlawed the use of blockchain technology applications like cryptocurrency.. These nations do not encourage the use of blockchain technology in the commercial sector.

2. Crypto Currency

Transactions in Blockchain

The Proces of blockchain transaction goes in this way:

- A wallallet is used by a node in the blockchain to request a transaction
- All network nodes recive a broadcast of the transaction
- The network validates or verifies the transaction using consensus algorithms, or pre established guidelines established by the particular blockchain.
- Either the transaction is approved or denied. If the transaction is approved, it is then sealed and added to the block of data in chronological order with other transactions. ~~which is~~
- The transaction has now been permanently recorded on the blockchain and cannot be changed.

Page :
Date :

Two times Spending problem (Double Spending problem)

- This issue, which is a problem Specific to digital currencies. Spending money twice is known as twice Spending.
- It is possible to dublicate a crypto coin or token and reuse it, just like it is possible to copy a digital file and send it to numerous recipients.
- If this happens in the blockchain network, it could undermine the idea of a trusted disributed ledger and cause inflation by introducing fake, duplicate curriencies in the System.
- Blockchain uses its consensus mechanism to get around this issue.
- It is nearly impossible to twice spend a transaction once it has been confirmed.
- The 51 %. attack can accomplish this though it is very uncommon.

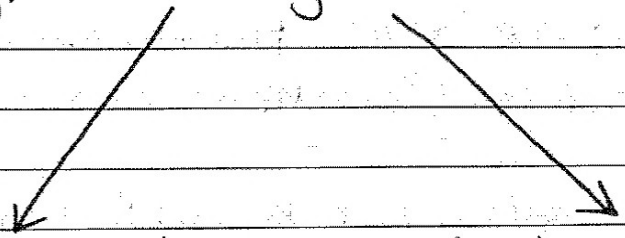
Steps taken to handle this issue:

- Lets say two different miners choose both transactions at the same time and begin building a block.
- Both participants A and B will now wait for confirmation of their transaction after the block has been confirmed.
- A new transaction will be retrieved from the network after the transaction with the most confirmations has been validated.
- Now imagine that A and B started a race when both of them received the initial confirmation at same time.
- The transaction that receives the most network confirmations will be added to the blockchain, and the other transaction will be dropped

Cryptocurrency Wallets

The Storage Space where a user can store his cryptocurrencies is called as Crypto-currency wallet. Every cryptocurrency wallet has a public & private key which is used in case if the user wants any cryptocurrency transaction to be done.

There are ~~two~~ ~~some~~ different types of cryptocurrency wallets:



° Hot wallet °

1. It is designed for online daily transac-tions
2. Most of the time it is connected to the internet and thats why it is strong target for hackers
3. It is advisable to use hot wallet for short term storage
4. Hot wallet is free of charge
5. Eg: Desktop ~~Mob~~ wallet, Mobile Wallet & Online wallet.

Camlin

- Desktop wallet :
1. It is downloaded in laptop or desktop. And they are in a complete control of the person who owns the laptop or desktop.

2. If the laptop or desktop has a virus or is infected there are chances that the desktop wallet inside it ~~is~~ can get hacked

3. Examples: Electrum, Exodus, Bitcoincore

- Mobile wallet :
1. They are Built to operate on the mobile
2. Where ever the Mobile owner goes with his mobile he can carry Mobile wallet with his location
3. As compared to desktop wallet Mobile wallet is more vulnerable to virus.
4. Examples: Coinbase wallet, Mycelium, Trust wallet.

- Online wallets Or web wallets
1. Online wallet run on cloud and thats why the user dont have to download any application in their mobile

2. They are location free
3. Examples: Myetherwallet, Meta Mask, And green address.

- Cold wallet:
  1. Cold wallet is never connected to Internet
  2. User has to pay if he wants to use Cold wallet.
  3. Cold wallets are more secured and suggested to be used for long term cryptocurrency storage
  4. Examples: paper and hardware wallet.

- Hardware wallet:

Hardware wallet are electrical & physical devices. They are connected to internet when sending & receiving a transaction and after the transaction they are disconnected from internet.
Examples: Trezor & ledger.

- Paper wallet:

- Its a piece of paper with crypto address & the private key printed in form of QR code.

- Paper wallets cant be hacked easily

~~Exceptions~~

- We need to keep paper wallet safe from water, fire.

Altcoin

- Cryptocurrencies other than Bitcoin are called as altcoin.
- There are thousands of altcoins in the Market right now
- There are many types of altcoins based on what they were designed for.
- No one can predict the future value of altcoin
- Mostly altcoins arive from a forR of wellknown and durable cryptocurrencies foreg Bitcoin, Etherium etc
- also many altcoins are kind of there predecessors, they try to improve or set themself apart by adding additional features or Securioty
- These digital currencies are peer to peer transactions that require mining.

Tokens

- They are used for fundraising public sales. The most popular token platform is Ethereum.
- Most of the time with decentralized applications tokens are used.

There are two types of tokens

1. Security tokens:

Most of the tokens released by ICOs are security tokens. They are also known as Equity tokens, because they stand in for ownership stakes in the corporation issuing the tokens.

2. Utility tokens:

Acess to a servie or a product is made possible through utility tokens & Due to their scarcity these tokens are valuable

Proof of work : (from 5 marks point of view)

Proof of work is an algorithm used to secure the transaction and establish a new block in a blockchain.

Here miners who can mine compete with each other this process is called as mining.

They have to solve a cryptographic puzzle for which all the competition is for. Also they have to find the value of nonce which they find through trial and error bases.

Whichever miner gets the value of nonce proceeds forward in the process of adding block in a blockchain.

Some of the cryptocurrencies that uses Proof of work are Bitcoin, Litecoin etc.

Advantage :

There is a high level of protection for transaction approach it provides a decentralized approach

In exchange of efforts it allows miners to earn reward.

Page :
Date :

Disadvantages:

- It is inefficient because of slow transaction speeds and high fees.
- The energy consumption is high
- Mining requires costly hardware.

Proof of Stake:

- In the case of Proof of Stake all the miners in the Blockchain network have do Stake an amount.
- The miner who stakes the most amount proceeds a head in the process of adding block in blockchain
- The age of the coins which are been stake should be also high.
- Coin age is, more the time by which you have store coins with you more would be the coin age.
- It is important do know that same coins cant be staked more than once.
- Advantages:
- Energy is conserved as there is no competition between the nodes do be the first to add a new block in the blockchain.
- In Proof of stake the rewards are proportional to amount of stake. So there is less benefit in joining mining pool. This promots decentralization

- If a node wants to attack a network he will have to one more than 50% of stake. This makes the network secured.

Disadvantages:

1. Proof of stake is a new technology thats why research is on going to find flaws, fix them and make it good for current network for transaction

Proof of Elapsed Time

- Proof of Elapsed Time can be assumed as a game of chance which means a lucky miner would get do add block in the blockchain and other miners wont.

- In Proof of Elapsed Time a wait time is given to every miner this wait time is completely random and randomly distributed.

- Miner can't actively work for the waiting time he is alloted And thats the reason why that miner who is been alloted least waiting time can ~~activate his~~ start actively working first and he gets the power to add block in the blockchain.

- few points to know about Proof of Elapsed time

1. after the miner adds block in blockchain mostly of the time miner dont get reward.

2. Proof of Elapsed time is not that secured as compared to Proof of Stake & Proof of work.

Page : 26
Date :

Proof of Burn :

- Miners who wants to add block in the blockchain send a particular amount to a wallet from which that amount cant be taken back & this process is called as burning.

- The miner who sends the largest amount as compared to other miners gets to add block in the blockchain.

- In other words we can say that the miner who burns most of his coins as compared to other miners win and he gets to add block in the block chain.

Advantages :

- Proof of Burn is more secure than other mechanisms.

- There is very low barries to enter

Disadvantages :

- There is a risk of hoarding. This scarce the current supply and this leeds to increase of value. This is good for those people who are holding coins but not good for overall health of coin.

Difference Between Proof of work & Proof of Stake.

	Proof of Work	Proof of Stake
1.	Need to do some work to mine a block	Need Sufficient Stake to mine a block
2.	Consumes Physical resources like CPU Power & time	No external resources are used
3.	Process is Power consuming	Process is Power efficient
4.	To add each block miners compete with each other to solve a puzzle	There is no such competition as one block creator is chosen by algorithm which is based on stake
5.	Initial investment is needed to buy hardware.	Initial investment is needed to buy stake & build reputation

Difference Between Hot & Cold Wallet

	Hot Wallet	Cold Wallet
1. Reason	Used mostly for Short term storage. Good for everyday transaction	Normally used for long term storage
2. Storage	online storage & requires internet	Offline storage & dosent require internet.
3. Price	It is free of cost	User has to pay if he wants to use cold wallet.
4. accessibility	Easy to access	Difficult to access
5. Categories	Desktop wallet Mobile wallet online wallet	Paper wallet Hardware wallet.

Page : 29
Date :

Mining Pool

- It is a fair competition to win a prize when all the nodes are of uniform size, power and opportunity. However some nodes engage in industrial scale mining by connecting to a sizable cluster of computers, utilising sophisticated software, and consuming a lot of electricity.

- Individual miners won't be able to compete with them well.

- Some miners join forces in mining pools to combine their mining capabilities for greater efficiency and cost savings in order to counter the significant time and energy consumption required in transaction validation. They split the processing and mining power.

- In order to prevent double labour and time wastage, mining pools offer the service, they divide it among the individual miners. The various miners within the pool are distributed Nonce values (cryptographic puzzles)

- The mining pool with the matching nonce wins the blocks reward when one of them discovers the nonce. Based on the individual miner's processing power they divide or share the reward.

Camlin

- However mining Pools may violate the fundamental tenet of disributed ledgers because they give anyone or any group the ability to control the validation process through a 51% attack, which is when one party or group gains control of more than 50% of the networkes computing power.

- The 51% attack is not intended to affect the blockchain in any way. The hacker must alter every block in the blockchains subsequent sequence in order to attack a block within it.

Mining Pool Methods:

1. Pay Per Share: An instant and guaranteed payout to a miner is represented by Pay per share, here miners are paid from pools existing balance.

Mostly share of a miner is
$R = B \times P$.

Most of the time miners get almost equal payment but still danger because risk lies in hands of the operator.

2. proportional : Until the pool finds a block miners earn share. Once a pool finds out a block payments are made.

3. Pay per last N Share : It is very similar to proportional - On the bases of N last share miners reward is calculated. for a short fund miner get more profit here.

Advantages :

1. Small size miners can take a chance
2. There is Predictable mining

Disadvantage.

1. This leads to centralization
2. It demotivates most miners for carrying a complete mining process.

Page :
Date : 31

Merkle Tree

- Binary hash trees, sometimes refered to as merkle trees, are a common type of data structure in computer Science.

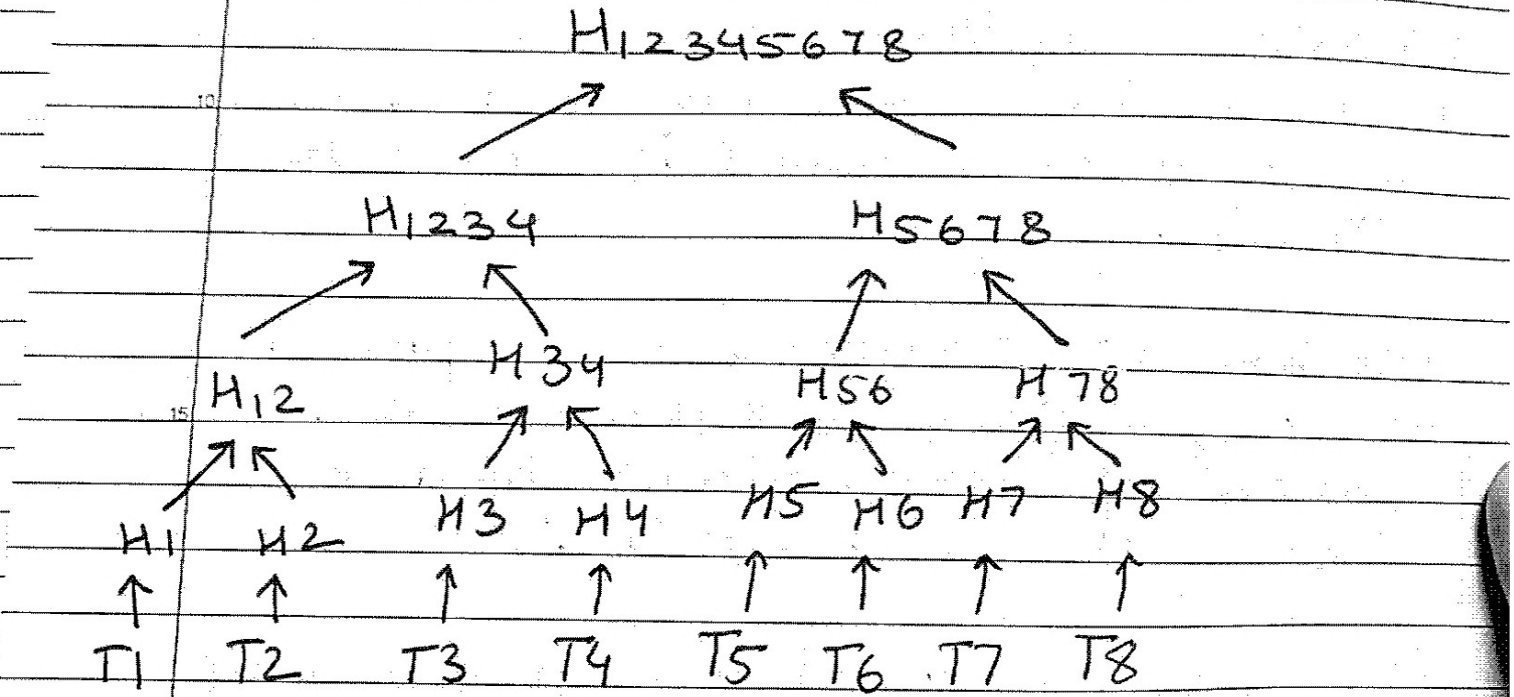
- Merkle true structure is responsible for organizing all transactions. Varifi-cations of all the transaction is the root of the merkle tree.

- They are employed in bitcoin and other crypto currencies to more effectively and securely encrypt blockchain data.

- There exist a hash of the transactions in the merkle tree at the leaf node. Hash of the combined hash value is contained by every intermediate node.

- It is a hash based mathematical data structure that compiles the summaries of all the transactions in a block.

- Additionally it permits rapid and safe content verification across large data sets and checks the accuracy and content of the information.



3. Programming in Blockchain

Introduction to Smart Contracts.

- In 1996 an computer scientiest and cryptographer Nick Szabo coined the term called as Smart contracts

- Smart contract is an condition oriented program which can be coaded or written by a programmer through various programming languages like python, Solidity etc.

- We can also say that if we wish to program inside blockchain we use Smart contracts which are placed in a particular block in the blockchain

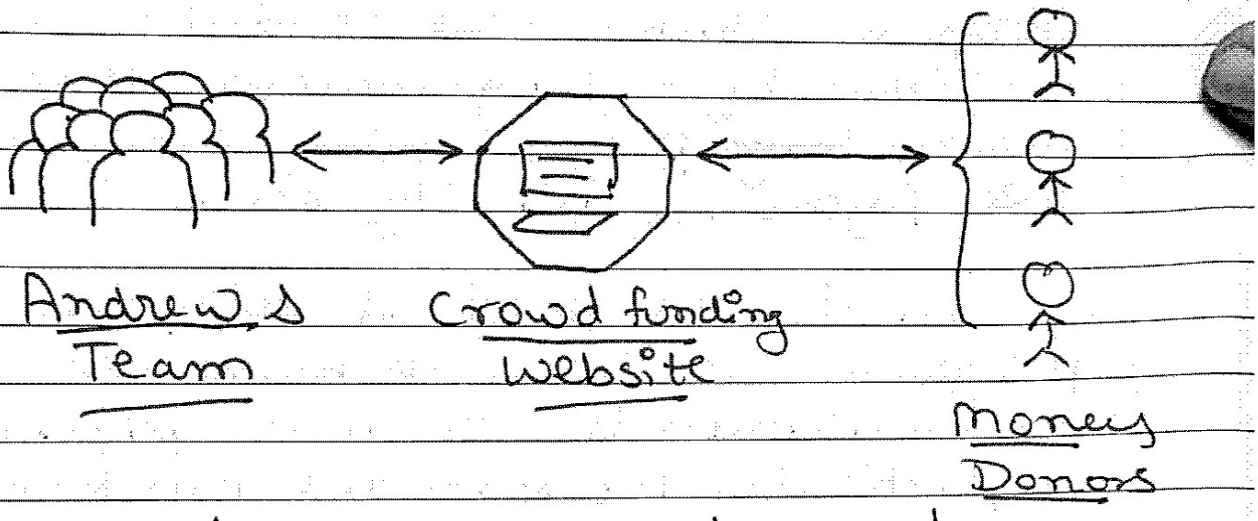
*Example

- Imagine Andrew with his team wants to set up a business but the problem is he dosent have enough money.

- On the other hand there is a Crowd funding website which has contacts to various different money donors who are happy to donate money to businesses like Andrew's.

- In this case Andrew contact the Crowd funding Websidt and shares about his problem and this websidt decides to help Andrew with the support of donors.

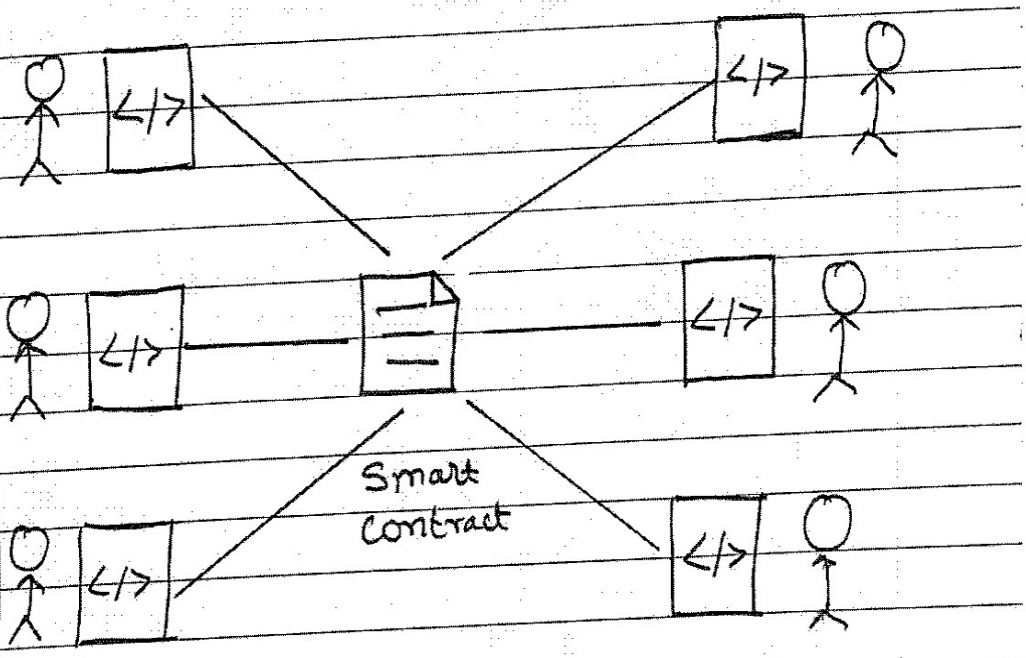
- Now it is the responsibility of the website to take donations and provide some amount initially to andrew to start his business.



- It is also responsible to provide a perticular amount of money to andrew at the time when he reaches perticular milestones also if Andrew decides to scrap his business then in this case the website shall return the remaining amount back to the Money donors.

- Now hear there are two major disadvantages the first one being that there is crowd funding website as an ~~d~~ middleman who charges cummision and Second being that the middleman can always might be a frawdster.

- Smart contract can be a replacement. In the Smart contract case a contract is made with the help of programming language between Andrew and money donors and the copy of contract is available with each involved members.



- Here there are less chances of frawd because if one member tries to change the smart contract he can be easily identified as his copy would be different from others.

- Here things would be carried out automatically, Andrew would get his money whenever it ... he has to get them and whenever the time is write ... automatically because it is mentioned in the contract.

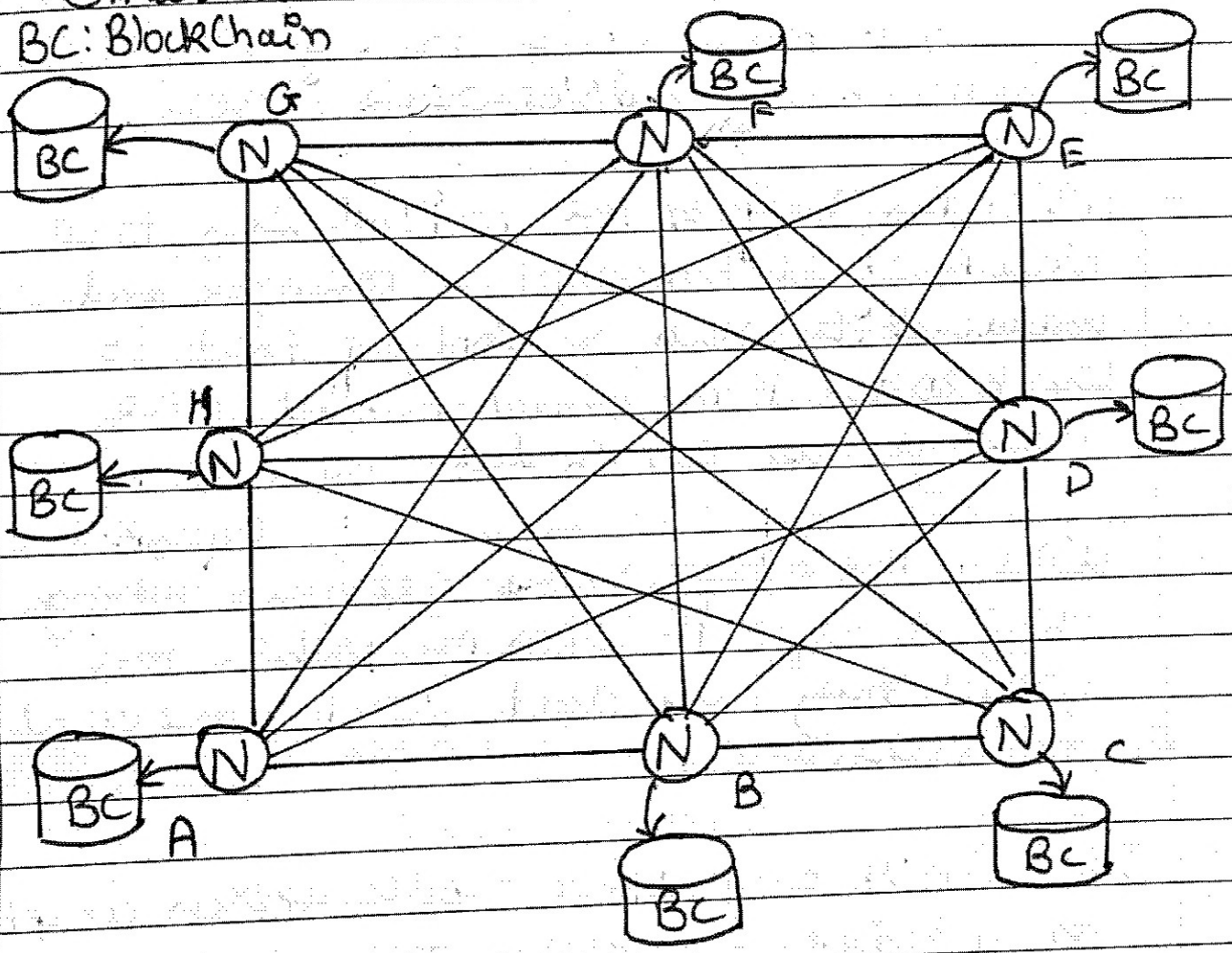
- Moreover there is no middleman so the cost of commission would be very lesser.

Page : 32
Date :

Structure of Smart Contract.

- Smart Contract can get activated by either time or situation.

- Time is when there is a time slot set for the smart contract to get activated and Situation resembles to a particular action taken by a user to activate the Smart contract.



The Structure: What if a user wants to activate the smart Contract. Well there is a process for it.

- Let's assume that Node A wants to activate the smart contract, in this case it broadcasts its public key in the Blockchain network which symbolises that it wants to activate the smart Contract.

- After this initiation the Blockchain network handovers the private key to the smart contract to the Node A Also a public key of the same smart contract would be given to other nodes in the Blockchain network by that Network itself.

- With the help of the private key the Node A would encrypt a message and broadcast it which symbolyses that it wants to execute the smart contract, the message has all the data required.

- When the other nodes get this encrypted message they decrypt it with the public key which they have and verify and validate the message.

- If 50% and abbove nodes approx accepts or validates the message then the Smart contract is activated and its impacts would be reflected to entire Blockchain Network.

Page : 10
Date :

Types of Smart Contracts

1. Smart Legal Contracts: They are Standard legal contracts between two parties.

2. DApp (Decentralized App)

- DApps are blockchain based applications that let users engage with smart contracts that have been set up on the blockchain

- Unlike smart contract they need not necessarily run on top of the blockchain network.

- It is a decentralised network based application that combines a frontend user interface and a smart contract.

- Dapps are blockchain enabled websites, also near Smart contracts are used as API connectors that connect Apps with blockchain

3. Distributed Autonomous Organization (DAO)

- The logic of a decentralized autonomous organisation is expressed by a clear program with stakeholder control and no influence from a centralized authority.

- To track financial transactions over the internet, DAOs employ blockchain technology to keek a secure advanced record in the form of a Digital Ledger (DL)

- Organization management is decentralised and decision logic are maintained on blockchain.

Introduction to Solidity Programming

- There are several programming languages with the help of which smart contracts can be written like python, go Solidity etc

- With the help of solidity a programmer can program smart contracts in a high level, object oriented language.

- programming in solidity is very same as to the javascript.

- Despite of being an OOP language it supports very limited features.

- There is a condition which is that variable name and the function name must be written in a same manner as for perfect execution

Components of Solidity

1. Pragma :

Pragram is the primary line of code which is normally written in the Solidity file. It denotes that what version of compiler can be implemented with the current Solidity file.

2. Comments :

- It is an option from solidity to add single or multiple line comments, just like other programming language.

3. Import.

With the help of this option we are able to import other Solidity files. It also helps in fetching other solidity files code in the current Solidity file.

- Solidity Programming aims to write smart contract for Ethereum and smart contracts are the most simple & basic elements of execution & deployment for Ethereum virtual machines (EVMs)

Page : 4 4
Date :

- Variables and functions are the two main elements ~~of~~ which Smart contract consist of.

o State variable

- A variable which isnt in any function and is declared in a contract is a state variable

- It is used to store the present address of the contract, while the contract is in effect the state variables allotted memory cannot be changed

- Internal, private, public and constant are the qualifiers that can be possessed by the state variable.

Constant: It makes the state variable unalterable

Internal: By default a State variable is internal if no identity is given to it. This means that ~~in~~ in inside the current contract variable can be accessed and not from ~~the~~ outside, but variable can be viewed from Outside.

Private: this is as same kind of to Internal but Stringent. It cannot be used in derived contracts

public: State variables can be accessed instantly and rightaway with no barrier

- Functions

- As same of other programming languages solidity programming also has functions

- In reaction to incoming transactions, functions have the ability to get or set information

- There are two types of function calls:
  1. External
  2. Internal

- External functions can be called from other contracts and via transactions

- Internal functions can only be accessed from in the current contract

- Properties of function
  - There is no arguments or name
  - It dosent return anything
  - Its required to mark it external

- Public functions:
  Here the function can be accessed externally and within too

- private functions:
  for this the contract must be declared private, They arent a chunk of smart contract and cannot be used within derived contracts, they can only be used internally.

- Enums: It is used to designate an integral constant and to generate user defined data types. Unsigned integer numbers begining at 0 can be used to represent the options of enums

Error Handling

- These are two methods used for error handling

1. revert(): This method terminates the Execution and undoes any state changes.

2. assert(bool condition):
If the condition is not met, the method call results in an invalid opcode, and all state changes are undone. This technique is to be used for internal error only.

3. require (bool condition): the method call reverts to the original state if the condition is not met.
The method is generally utilised for errors in external components & inputs.

4. Revert (String memory): This method terminates the execution and undoes any state changes. It offers the choice of sending a personalised message.

Note: For Solidity programming topics we recommend you to watch our lectures on the YouTube

4. Public Blockchain

Introduction

Firstly we need to understand that Etherium is a public blockchain just like Bitcoin. There are few flaws in Bitcoin so Etherium was made for example bitcoin can be used only for financial transaction but Etherium can be used for financial as well as for other type of transactions as well with various accessibilities.

There are few elements we need to understand in Etherium:

1. Miner & Mining Node:

Writing an transaction in Etherium is the miners responsibility which results into miner getting reward if the transaction adds to ledger.

There are two types of rewards to be recived by the miners in is the price for block which is ~~3 Ether~~ 3 Ethers approxx and other is the Gas price.

There are two types of mining nodes first is the miner whose work is to create a block and add in the blockchain. Also he checks wether a block which is being generated is valid or not after the generation process is complete if valid then Approving it.

- Second type of Mining node is EVM (Etherium Virtual Machine)

Etherium Virtual Machine (EVM)

- EVM isn't a mining node it dosent add blocks insted it is a node which includes / has smart contract in it and can execute it.

- It is not necessary that EVM should have an entire copy of Blockchain but it has the data about the current transaction

- EVMs are primarily responsible for providing a runtime that may execute code generated from Smart Contracts.

Although it dosent require acces to the ledger, it only has a limited amount of data on the current transaction.

What is Gas?

- Primararily you need to understand what is Ether. Ether is an crypto currency of Etherium ~~is~~ in other words we can say that if we want to execute any financial transaction in cryptocurrency then in that case we use Ethers.

- When a miner adds block in a block-chain he gets a reward which is few ethers

- Gas is the fee required for every transaction Gas is a Sub or mini version of Ether. It has a very less value but its need to be spent while the transac-tion

- The Reason behind this is if there is no transaction fees the users would have a number of transactions which would be a problem. On the other hand if there is a Gas fee there would be limited no. of transactions

- So Some gas needs to be spent for every transaction

- The Transaction cannot be done unless and untill the gas price is paid.
- There is a specific gas price for every transaction.
- To ensure that there is no depletion of gas a gas limit can be set.
- Ethers is the unit with the use of which gas fees is paid.

Transactions and Accounts

- Transaction is the information which can be stored in the block

- Transaction is an interaction ~~which~~ and whenever and transaction is added in the block it is permonant.

- In other words we can also say that transactions are stored in Blocks in Etherium.

- An exchange of assets, goods, or services would take the role of ~~mo~~ money, cryptocurrencies, or any other asset, either now or in the future. A transaction is just a set of agreements between participants.

- There are two types of accounts in Etherium:
  1. Externally controlled Account
  2. Contract Account.

- User owns an externally controlled account and Ether balance is stored in it.

- Transferring Ethers from one externally owned ocunt to other externally owned account is possible.

- There is a contract account with every smart contract which has address which is similar to externally controlled account.

- But we need to understand that the contract account dose not refer to an externally controled account but it refers to smart contract.

- Ethers can be sent from one account to other for the transactions to have both contract aciount and Externally controlled account as well.

Etherium Architecture

- There are total six layers in etherium architecture which are red from bottom to up.

- Layer Zero (Consensus Layer): Consensus is approval. Taking approval for the current state of the blockchain is called Consensus.
- Inconcensus: all the nodes agree with a state but if they find any error they wont give consensus.

- Layer One (Economic Layer): Economic layer is about Incentives which are given by Etherium.

- In etherium whenever a miner adds block in the blockchain, for adding the block he gets incentives which is under Economic layer. affairs related to Gas are also a part of Economic Layer.

- Layer Two (Blockchain Service): Blockchain Service deals with actual Blockchain, the place where data and transactions are stored in decentralized manner.

In Etherium data is Stored in Inter Planatory File System (IPFS) form.

Layer Three (Inter Opparability):
Whenever we use a decentralized system it might happen that the tokens in blockchain are different. Inter opparability provides a comman platform for tokens. It dosent let a big difference in the prices of for example bitcoin & etherium as it also acts like a regulatory body.

Layer four (Browsers): or distributed applications
With the help of Browser a user can interact with the blockchain. Browser is kind of a UI or front end. Best Browser is mist.

Layer five (Distributed Applications):
With the help of distributed Application a user can perform operations on blockchain.

Dapps
Browsers
Inter OPERability
Blockchain Services
Economic Layer
Consensus Layer

Page : 56
Date :

Difference between Bitcoin and Etherium

	Bitcoin	Etherium
1.	Founder is Satoshi Nakamoto	Founder is vitalik Buterin and more
2.	Release date is 2009 January	Release date is July 2015
3.	Average block time is 10 mins	Average block time is 15 seconds.
4.	Coin Symbol is BTC	Coin Symbol is ETH
5.	Tokens aren't available	Tokens are available
6.	Block limitations is 1MB per block	There is no Block limitation.

Etherscan.IO

Etherscan.Io is an website with the help of which you can access individual wallet. Etherscan.Io is One amongst many websites to access Etherium blockchain.

- Every transaction details can be viewed with the help of this website the details consists of transaction hash, Status of transaction, block number current gas price the network is following etc.

- Sometimes the transactions is account to account and sometimes the (smart contract) transaction is account to contract which is again mentioned as a detail

- All the crypto accts can be viewed ie the number of transactions, fees, number of ethers transfered etc here in this webside

- Transactions performed on the Etherium blockchain can be viewed almost live

following are the things which can be done by Etherscan.Io

1. Smart contracts can be verified
2. View the cryptocurrency assets contained in or connected to a public wallet address.
3. Findout which smart contracts have a Security audit and validated Source code.
4. Count the number of smart contracts that a user has approved using their wallet.
5. Access to wallet for any application which is decentralized for eg DApp can be taken back or reviewed.

5. Private Blockchain

Introduction

- Till now we have studied all the public blockchains where any external entity can participate in your blockchain there is no permission required. Example of public blockchain are bitcoin and Etherium.

Now, If a blockchain is made for a specific group or a close circuit of people then that blockchain is a private blockchain

- for example if a blockchain is made for a particular firm lets call it firm x So that firm wont want that any Other outside person shall interrupt or participate into their blockchain other than the people who are involved already. Such blockchain is a private Blockchain.

- Private Blockchain is centralized which means that the authorized or chosen node would decide the accessibility of other nodes or basically the entire blockchain network.
  → Can manipulate the controls of

- There can be multiple nodes who has the power to change different controls in a private blockchain but the central node is the one which gives power to those nodes and decide which controls shall be given to which node.

Page :
Date :

Characteristics of Blockchain

1. Scalability : Because there is not any requirement of computational power and Storage (more) there is a finer scalability

2. Energy consumption : Energy consump-tion is low.

3. Access : Access is completely restricted.

4. Security : Security depends on which blockchain architecture is adopted.

5. Operation : Transactions can be red or initiated by pre approved participants.

6. Users : Only users who are known and trusted.

7. Verification : To create a block there's single validator node / central authority.

Page: 6
Date:

Need of Private Blockchain

- Firstly we need to understand that private Blockchain is similar to public Blockchain in many ways

- ~~Private Blockchain is also called as permissioned Blockchain~~

- In the private Blockchain the central node controls and rules over other nodes, the entire authority is with this central authority

- Central node has to power to choose nodes and allot them certain powers also it can choose what powers shall be given to what nodes. It has right to change or influence the accessibility of any node as anyone randomly cant participate this network.

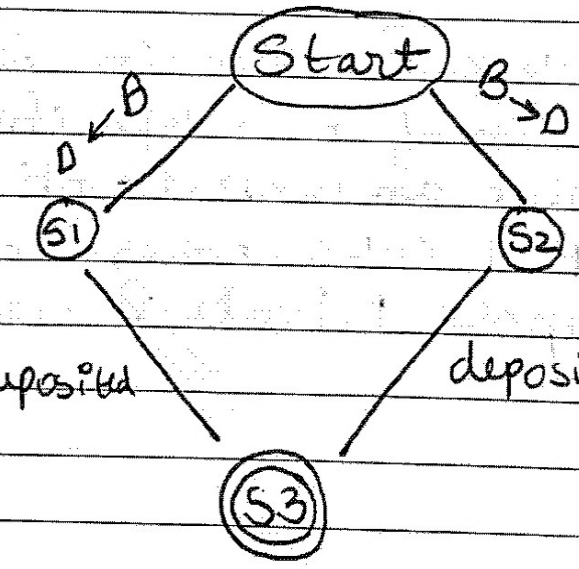
- Because Private Blockchain is limited or it limits itself to a specific group of people so that an central entity could have its control over other nodes for this purpose Private Blockchain is used.

State Machine Replication

- Firstly we need to understand that what is a state diagram. Whenever there is a change it is a change in state. Every machine has a start state.

- Suppose B transfers a certain amount to D as the transfer happens the state changes, Now lets say B also transfers amount to D again at the same time so for this transaction a new state shall be created. When both the transactions are deposited for that a new state is created which shall be the final state.

- Now State Machine Replication says that each and every state shall be synchronized.



- Such System is known as State machine replication.

- In the case if there is any problem in order or any node fails in that case these problems can be fixed in State Machine Replication

- For this we need to have a consensus algorithm so that things are synchronized and there are comparitively less problem

- Why do we employ a consensus approach based on state machine replication? The first is that every node is acquainted with one another in a closed network. State replication is therefore achievable between the known nodes.

- The State machine replication-based scenario avoids the mining overhead, which is the second justification

Page : 65
Date :

Consensus Algorithms

- Consensus Algorithms are the one because of which every node in a blockchain aggrees to one decision.

- We require consensus in the Blockchain during any activity or when a certainly new activity is initiated.

- There are few consensus Algorithms which are being shared:
  1. PAXOS
  2. RAFT
  3. Byzantine Fault Tauleranb.

PAXOS

- Leslie Lamport proposed Paxos as a Consensus algorithm in 1989. It was the first consensus algorithm.

- The main objective of Paxos was to select one value under a crash or network fault

- In other words we can also say that, as asynchronous network connects a distributed group of computers, So Paxos is the technique used to reach Consensus among them.

- Paxos merely chooses a single value from one or more values that are suggested to it and announces that value to everyone.

- The Paxos protocol is executed and a single proposed value is chosen.

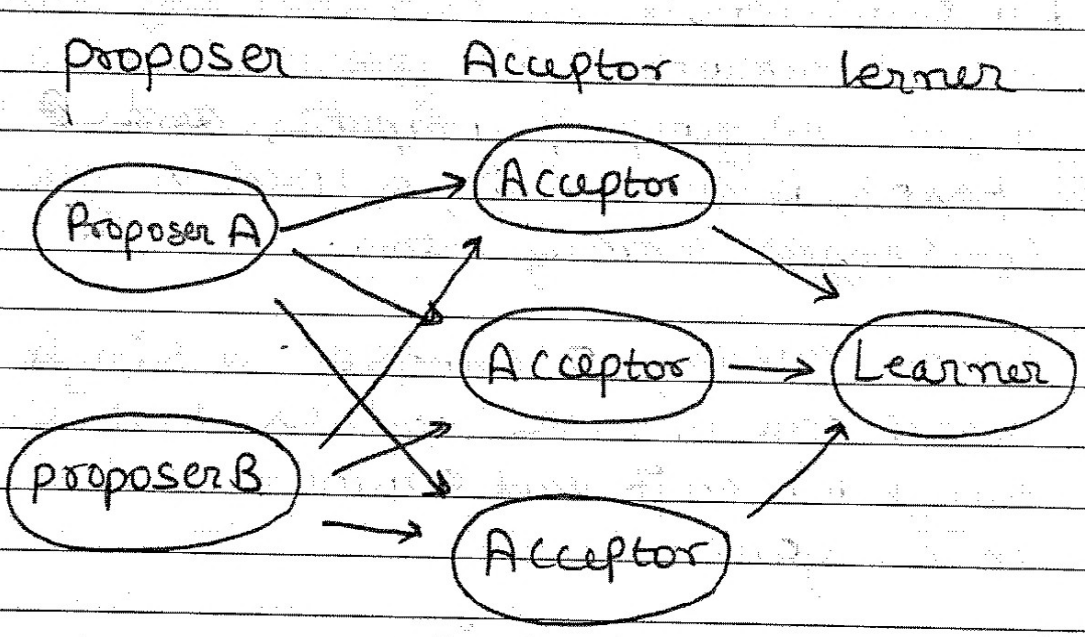
These are the type of nodes in Paxos

1. Proposer: Values that should be chosen by the consensus are proposed by proposer.

- Acceptor: The formation of consensus and acceptance of value these things are done by acceptor

They either rejects or accepts proposals when they hear them from the acceptor.

- Learner: A learner would accept a specific value after learning which value was selected by every acceptor.



- When the network learns about what the majority decisions is everyone in it is a learner. In the beginning, the proposer ~~[illegible]~~ proposes a proposal number.

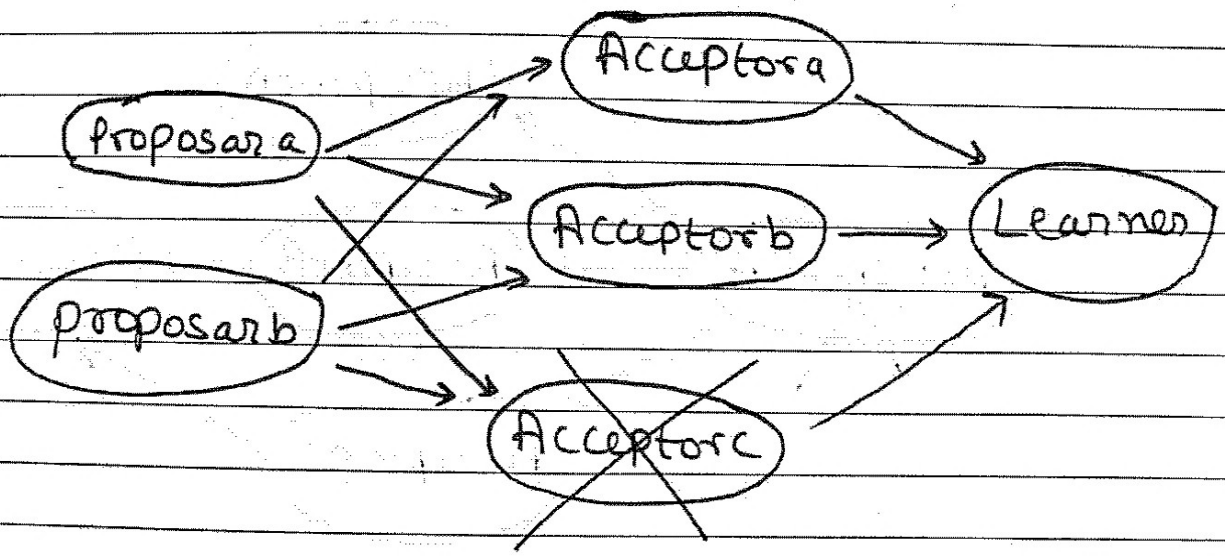
- The proposal number must be worthy of acceptance and it is created by the proposer and sent to the acceptor.

- Cronology is used to determine the ~~prepare~~ proposal number, with the highest number being regarded as current.

o Handeling failures

Q: Acceptor failure

- Few acceptors can fail ~~then~~ while the prepare phase. If this is the case then there is no problem the reason being that other acceptors can hear the proposal and vote against the proposal or for the proposal.

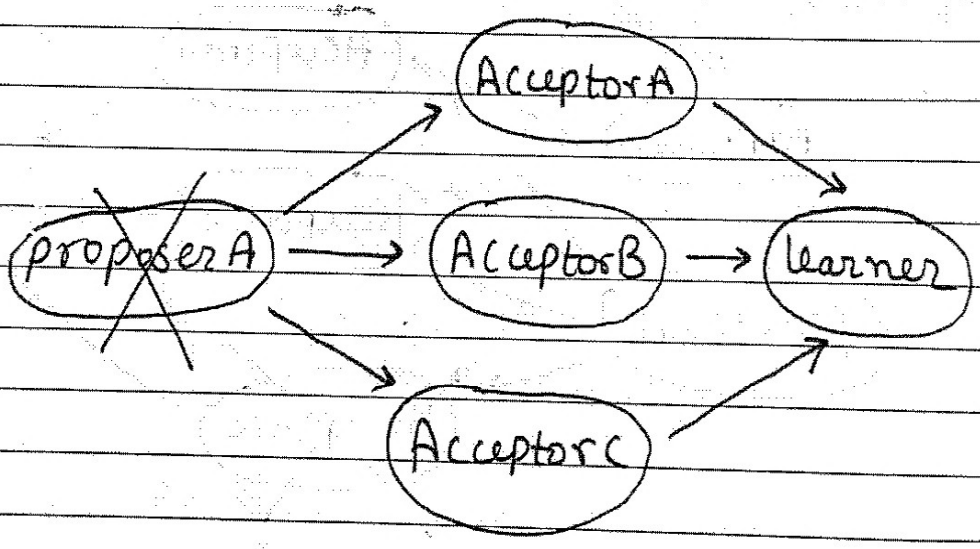


During the accept phase there is a possibility that the the acelpoor fails even in this case there is no problem because other acceptors can vote for the proposal.

- When $\frac{N}{2} - 1$ acceptors fail in that case proposers dont reply and there is no value to be accepted and consensus can't be achieved.

b. Proposer fails

- During the prepare phase if the proposer fails, then in this case there is a certain waiting time for the acceptors and after that time one of the acceptors becomes a proposer



- What if the proposer fails during the accept phase. Well in this case you need to understand that the acceptors have concluded on whether to select or reject the scheme based on majority of the vote.

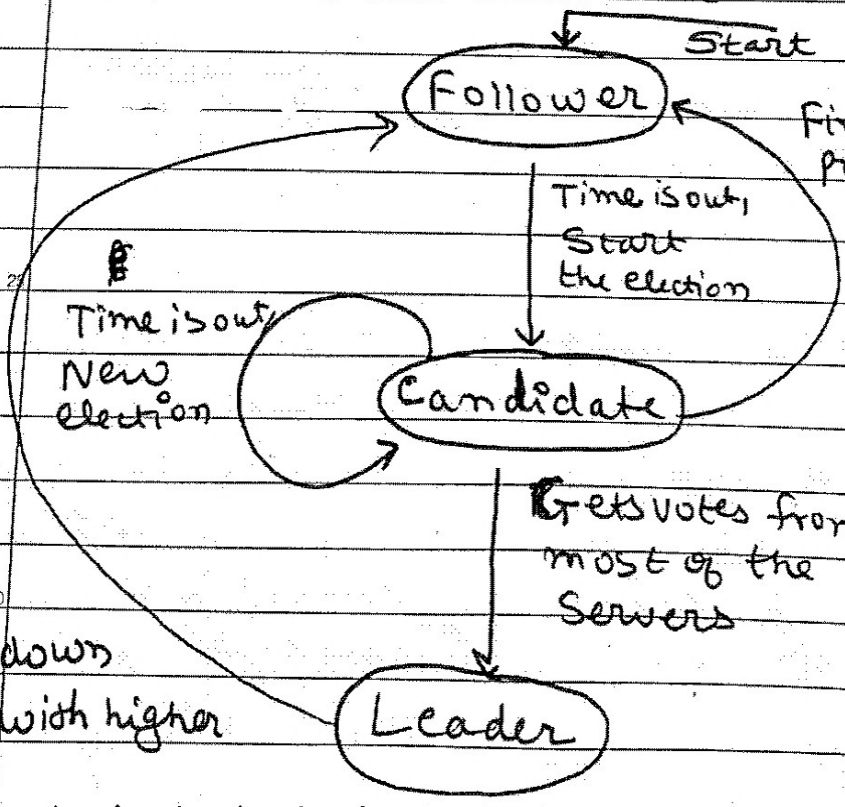
- So most of the votes are shared by the acceptors amongst themselves and in this way acceptors are able to figure out whether proposal has been accepted or rejected.

RAFT

There are two type of nodes in raft one is leader who rules and the other node is the followers who obeys the rules of the leader

In order to choose a leader an election process is being followed. In the Initial stage of election process where there is no leader because he is yet to be chosen in this scenario other followers are the candidates. (followers who are interested)

After the election process that node would be chosen as a leader node. After this except the leader all the other nodes shall become candidate.

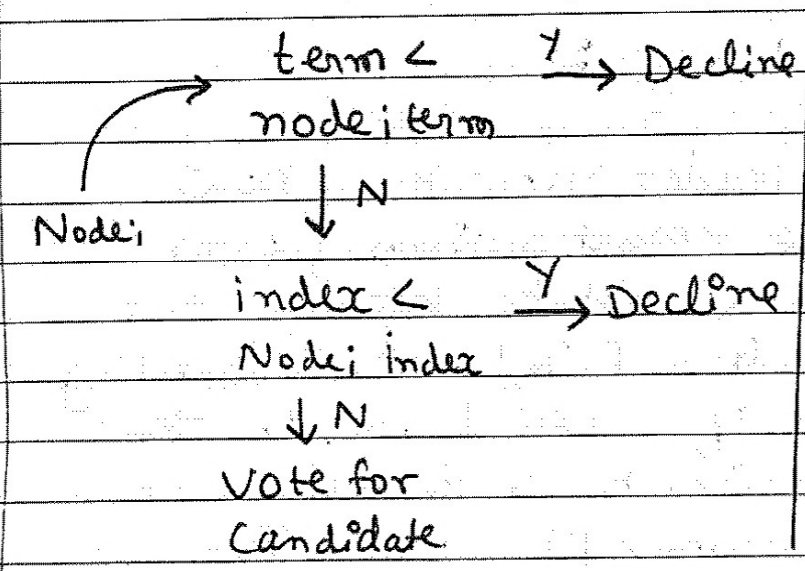


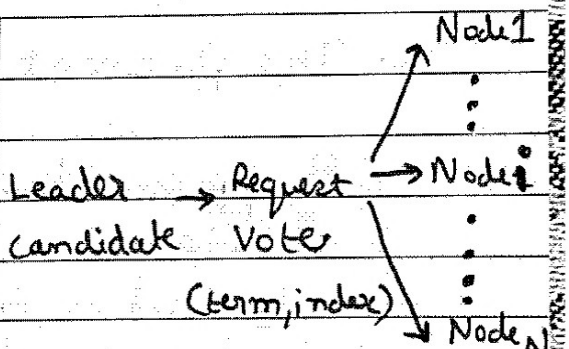
- When a system starts there are some follower nodes who looks whether there is a leader or not. If time out occures it symbolizes that there is no leader and the process of election begins

- When there is a change, leader shall broadcast the change and the followers shall follow the leader and act upon those changes positively

- Each node in a replicated state machine can remain in any one of the three state, namely leader, candidate or follower.

-





Any requests to the follower node are forwarded to the leader node, which is the only node that can interact with the client. To become the leader, a candidate may solicit votes. Only the candidate or the leader receives input from a follower.

- The RAFT algorithm divides time into short terms of arbitrary length to retain these server statuses. A term parameter, or monotonically growing number, is used to identify each term. The second argument, index, stands for the last transaction number.

- Requests from the leader with lower term parameters and index parameters won't be accepted by a server node.

- RAFT is an alternative to PAXOS.

Handling failures

a. The present Leader:

Suppose the leader now has now failed. We must switch from round a to round b because the leader node has failed. necessitating the election of a new leader for the new term, which is equal to the old term number plus one. The following vote for a new leader.

Page : 7.5
Date :

Scenario A :
The message from the new leader reaches the old leader, who makes a full recovery. As a result, the previous leader learns that a new leader, who will serve as the system's leader for the following term, has taken over. As a result, the system has already begun the new term or round. The ageing leader thus transitions from being a leader to follower.

Scenario B :
A different situation occurs when two nodes simultaniously send message requesting votes. Currently the entire system remains in term 10. There are two leaders candidates at the term 10 who have sent a request to vote in round 11. The node that receives the most votes sends a heartbeat message, a special message in which the leader declares that he has recieved most votes. The other leader candidate concedes to a follower majority vote after hearing the winners heartbeat message.

8. Followers
If a follower fails, failure of N/2 - 1 nodes can be acceptable. The system rely on voting of majority of nodes so it dosent really matter

Hyperledger

Hyperledger is a private blockchain. If we want to implement any private blockchain then in that case Hyperledger is used.

: Hyperledger is developed under the flagship of Linux foundation in 2015.

An Hyperledger project has the following properties.

1. Modular:
Modular and extensible frameworks with mutual building blocks which can be reused are developed by hyperledger

2. Easy to use:

Easy to use APIs are provided by one hyperledger and these APIs support interoperability with other systems

Hyperledger attracts and connects developers, users, problem solvers and incubates new ideas and support each other with useful requirements.

3. Interoperable :

- In the upcoming years, there would be communication and exchange of data between different blockchain networks to form Strong networks

- Smart contracts and use must be transportable amongst several different blockchain networks is ensured by hyperledger programms. This maximises the possibilities of adaption of this mechanism.

9. Cryptocurrency agnostic :

Hyperledger does not manage any coin, it exists to provide blockchain Software for businesses. The projects are important and un concerned with any alternate cryptocurrencies or tokens.

While hyperledger might develop a token used to control digital things, it wont produce its own coin.

Page : 77
Date :

5. Secure

- There is an involvement of valuable transactions and/or useful or private data which makes security very important.

Hyperledger Framework

1. Hyperledger Fabric :

Hyperledger Fabric has multiple users and Every user has a particular task. Hyperledger Fabric is also called modular blockchain

There is Endorser, committer and ledger.

Endorser checks and confirms wether a transaction is valid or not. Whenever the Endorser approves a block committer adds the block in the blockchain

After this one blockchain is updated as per the new update.

A Platform for creating distributed ledger systems, Hyperledger Fabric has a modular architecture and offers high levels of security, adaptability, resilience, and stability.

The Fabric Offers plug and play components including consensus and membership Services. It has container technology to host smart contracts often known as 'Chain code' which contain the System's business rules. Pluggable components are supported by fabric by design.

2. Hyper ledger Indy:

The Storage of digital Identity is done by Hyperledger Indy. This Concept is used in the industries like art, creativity etc.

In a decentralised setting, INDY is renowned for offering digital IDs. For the establishment of digital IDs, INDY offers tools, libraries and reusable parts.

Page :
Date :

3. Hyperledger Sawtooth:

There is not much of a difference between hyperledger sawtooth and hyperledger fabric the only difference is the smart contract in hyperledger sawtooth are easy to make it is made with help of Solidity language.

A platform for creating, implementing and ~~deploying~~ operating distributed ledgers is offered by hyperledger sawtooth. A digital record is offered by distributed ledger (eg. asset ownership)

The records are kept without the use of a central organisation or system. Sawtooth seeks to make it easier for businesses to implement smart contracts while maintaining distributed ledgers dispersed rather than storing them on a single server.

Sawtooth is very modular, allowing businesses and consortiums to choose their own blockchain applications.

Scalability, security, privercy and modular design are all features of Sawtooth. Scalability is enhanced by the PoET consensus mechanisms and transaction families broaden the applicability of smart contracts while lowering the attack surface. Additionally supported by sawtooth are trusted execution environments and the functions they play in private transactions.

4. Hyperledger Iroha:

- It is a blockchain framework which is easy to implement in projects.

- It is developed by soramitsu in Japan and Soramitsu, NTT Data, CDLV and Hitachi proposed it to hyperledger.

- The structure is nt complicated, the consensus algorithm is chain based and it Emphasis on mobile app development.

- Iroha issues attributes which are super helpful for making applications for end customers.

5. Hyperledger Burrow

- Monax developed Hyperledger Burrow which is a permissioned Smart contract machine.

- If offers a blockchain client that is modular and has a smart contract interpreter that was partially created in accordance with EVM requirements. Burrow offers a blockchain architecture that is strongly predictable and focusses on Smart contracts.

6. Tools and Applications of Blockchain.

CORDA

- CORDA is used in the private blockchain CORDA can be also considered as an alternative to hyperledger fabric.

- CORDA was developed by R3 organization. CORDA is specifically used in transactions which are financial in nature.

- In CORDA instead of blocks transactions are connected with each other. Here every transaction has the hash value of its previous transaction.

- An approval is not needed from other nodes for an transaction to happen. The benefit is more time is saved.

Advantages of CORDA:

1. When it comes to private transactions, corda is quite accommodating. Depending on the established business regulations, you can give various transactions either a public or private status.

2. The operational speed is very fast

3. The efficiency and cost of inner company co-operation is optimized.

Ripple

Ripple is also used for transaction which are financial in nature. The speciality of ripple is it has its own cryptocurrency named as XRP.

- With the help of Ripple a public as well as private blockchain can be made.
- No heavy algorithm is used in ripple for consensus and thats why Ripple is better than other cryptocurrency
- There are two groups of users in Ripple network which are ripple network users and network members. The primary users of ripple network are payment making institutes like banks etc.
- Network members includes payment providers which are the foundation of the ripple network because they work on processing the payments and liquidity.

- Bitcoin transactions consume more energy, take longer to confirm and have higher transaction costs, whereas ripple transactions use less energy, complete faster and have far lower transaction cost.

By market capitalization, Ripple (XRP) is one of the most valuable blockchain based asset.

Page : 27
Date :

Blockchain for Decentralized Finance (DEFI)

- Decentralized finance or DEFi eliminates third party / parties and centralised institutions from financial transactions by using developing technologies.

- Stable coins, software and hardware that supports application development are the elements of Defi.

Features of DEFI:

1. It eliminates third party, middleman things like that which gives users ownership of their capital

2. on the blockchain network, third partys are typically eliminated via indisputable logic code rather than human intervention. Smart contracts often assist Defi.

3. It promotes cost cutting.

There are three major benefits of DEFI

a. High programmability smart contracts automates execution and make it possible to create new digital assets and financial instructions.

b. Data co-ordination across a blockchain's decentralised architecture that is tamper-proof improves security and auditability.

c. DeFi market players engage with permissionless financial applications and protocols via web 3 wallets like Metamask to keep custody of their money and control over their personal data.