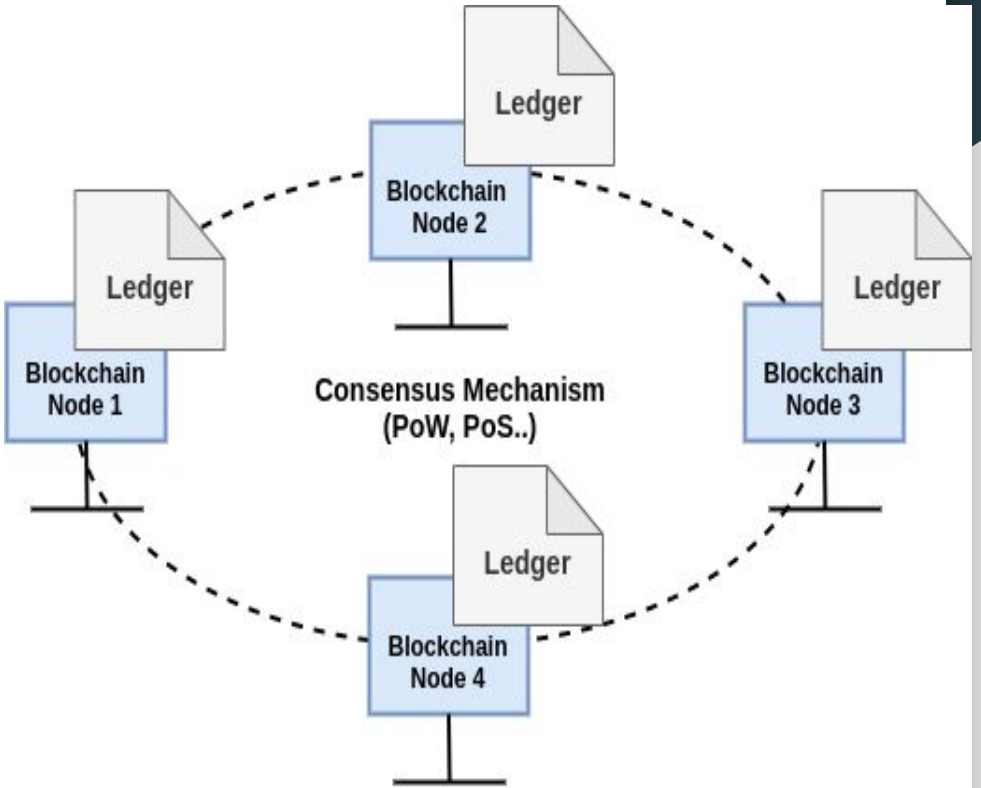
Blockchain Scalability & Decentralized Finance (DeFi)

Dr. Prashanth PVN
Assistant Professor
VNIT-Nagpur

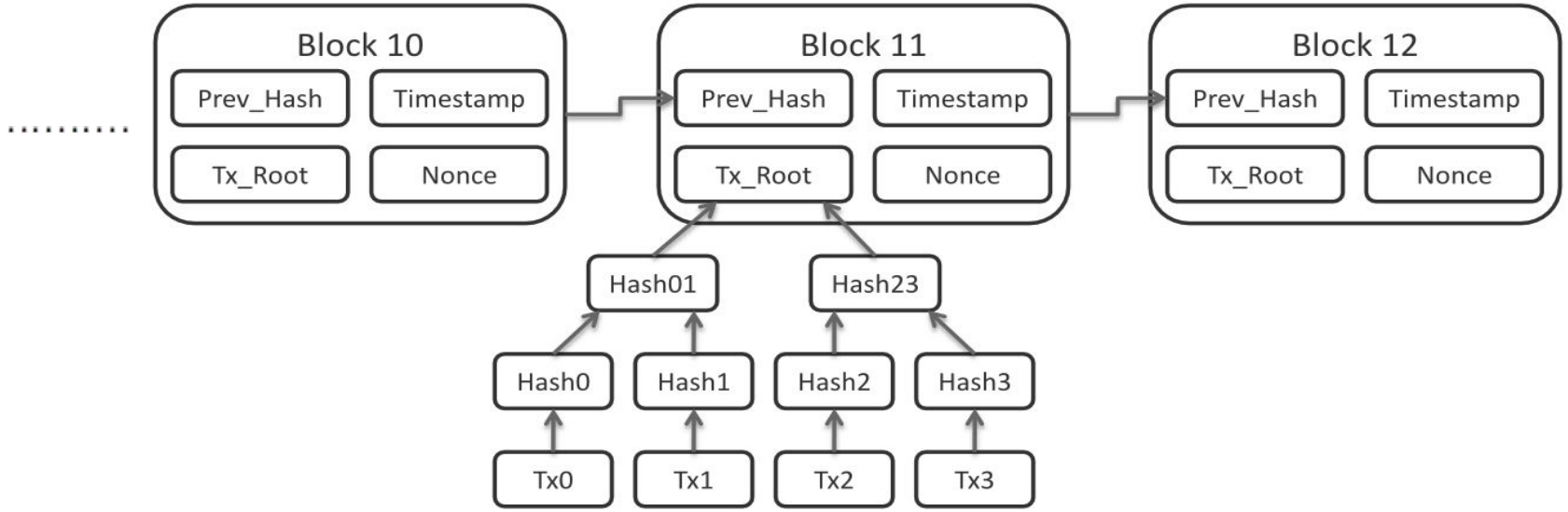
Table of Contents

Blockchain Overview

- **Blockchain:** A global and append only digital ledger (of transactions) shared among **un-trusted entities/domains** in a distributed environment.
- Transactions (signed) from each node are broadcasted to the Blockchain network.
- Transactions are validated using consensus mechanisms (without any centralized party).
  - **Prevents double spending**.
- Every node maintains the **same copy** of the ledger.



Blockchain Overview cont..



- Transactions are maintained in a (linear) chain of blocks.
- Each block carries the hash to its previous block.
  - Change in any intermediate block changes the state of all the following blocks until the end of the chain.

What Blockchain offers ?

- Immutability
- Traceability
- Replicated data storage
- Elimination of a centralized third party
- Provides a decentralized platform among multiple untrusted stakeholders for sharing and verifying tamper-proof assets/resource information.

Use cases :

In Jan 2021, The Ministry of Electronics and Information Technology (MeitY), Government of India, identified 17 different uses of national importance for Blockchain technology.

Examples : Transfer of land records, digital certificate management, pharmaceutical supply chain, e-voting, chit fund administration, etc.

Practical Example:

- Farmers (Sells 20 per kg)⟶ Distributors (Sells 50 per kg) ⟶ Grocery Shops
- How do grocery shops validate the information.
- Solution - Maintain Digital Dashboard (all stakeholders update their service cost)
- Who will host and validate the information (Centralized)

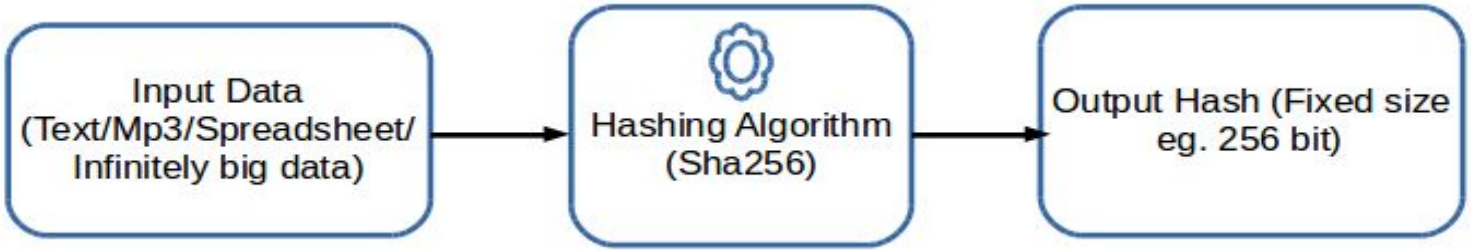
Cryptography behind Blockchains

Two main cryptographic concepts that underpin Blockchain technology:

1. Hashing, and
2. Digital Signatures.

Hashing

- A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length output called as hash value or simply hash.
- The output can vary (128-bit or 256-bit) depending on the hash algorithm
- Hash algorithm produces unique output for each input.



Hashing Properties

Property 1: Deterministic - Hash function gives same result no matter how many times you pass a particular input.

Property 2 : Quick Computation

Property 3: Pre-Image Resistance - Given H(A), it is infeasible to determine A, where A is the input and H(A) is the output hash.

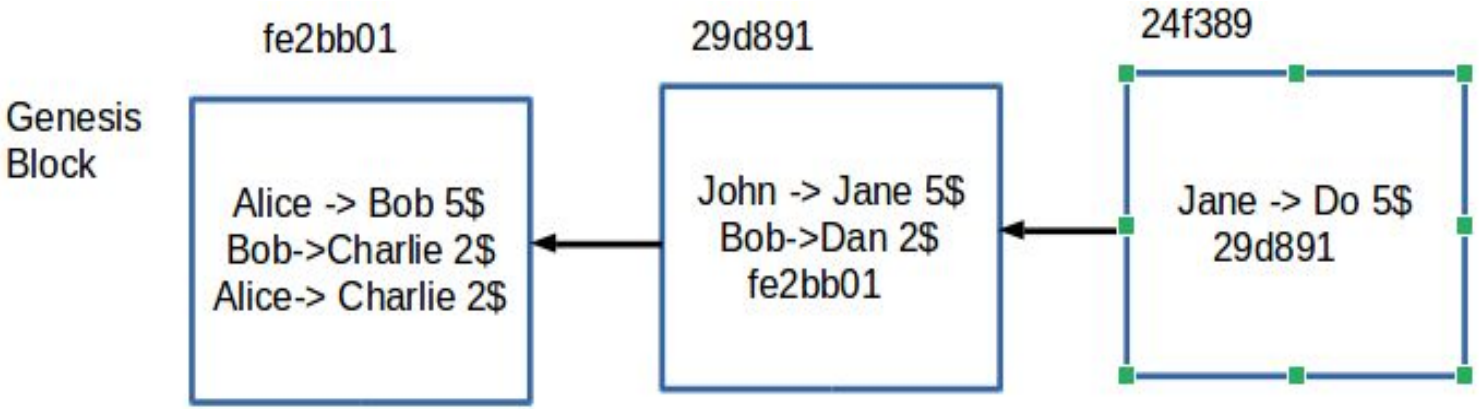
Property 4: Small changes in input changes the total hash value.

Property 5: Collision Resistant - Given two different inputs A, B and H(A) and H(B) are hashes, H(A) and H(B) will not be equal

How hashes are used in Blockchains ?

- For every block of the blockchain, a hash value is calculated by combining the hash of the previous block and the contents of the current block.
  - Thus maintaining a chain property of all the blocks.
- Hashes represent the current state of the entire chain.
- Input – Entire state of blockchain i.e all transactions taken place so far + Pending transactions (that are to be added to blockchain in a new block)
- Output – Current state of blockchain.

Chain of blocks and hashes



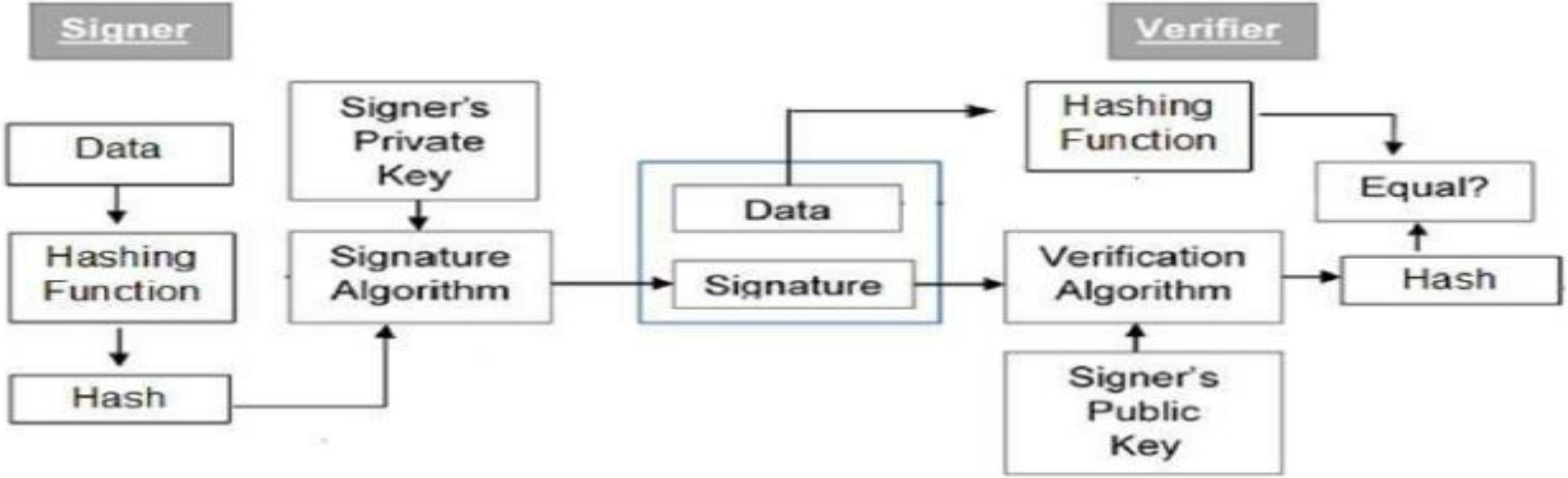
- This system guarantees that no transaction in the history can be tampered because if any single part of the transaction changes, the hash of the block to which it belongs also changes, and any following blocks' hashes.
- Everyone on the blockchain only needs to agree on 256 bits(Hash) to represent the potentially infinite state of the blockchain

Why Digital Signatures ?

- A digital signature is a type of electronic signature used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document).
- Digital signatures create a virtual fingerprint that is unique to a person or entity.
- Digital Signatures are used to identify users and protect information in digital messages or documents.

*A valid **digital signature** gives a recipient reason to believe that the message was created by a known sender (**authentication**), that the sender cannot deny having sent the message (**non-repudiation**), and that the message was not altered in transit (**in***

Digital Signature Generation and Verification



Img Src: https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

Signature Generation

- Every entity generating a Digital Signature (DS) has a public-private key pair.
- The private key is used for signing and the public key is used for verification.
- Signer feeds data to the hash function and generates hash of data.
- The Hash value and signature key(private key) are then fed to the signature algorithm which produces the digital signature on given hash.
- Signature is appended to the data and then both are sent to the verifier.

Signature Verification

- On receiver side, the verification algorithm takes the digital signature and public key algorithm as inputs and produces an the output.
- Verifier also runs same hash function on received data to generate hash value.
- If the hash value and output of verification algorithm are same digital signature is valid.
- Since digital signature is created by ‘private’ key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

- Message authentication
    a. verifier validates the digital signature using public key of a sender;
    b. Sender only has the corresponding secret private key.

- Data Integrity
    a. If data is modified, the digital signature verification at receiver end fails.
    b. The hash of modified data and the output of verification algorithm will not match.

- Non-repudiation
    a. Only the signer has the knowledge of the private key, he can only create unique signature on a given data.
    b. Receiver can present data and the digital signature to a third party as evidence to prove that the sender has actually sent the data.

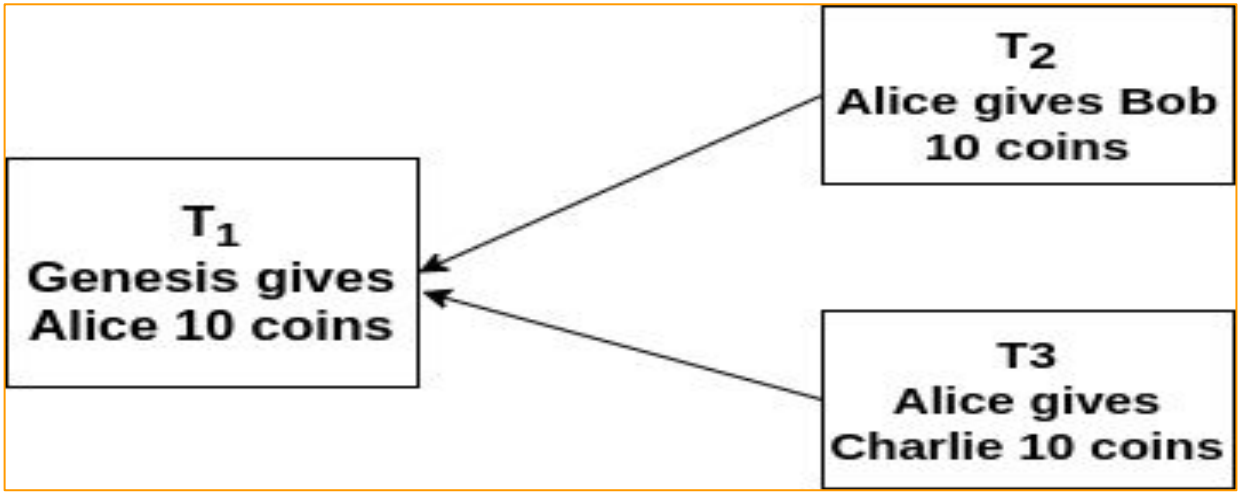
Digital Signatures in Blockchain:

- Digital Signatures are primarily used to verify the authenticity of transactions.
- Every transaction that is executed on the blockchain is digitally signed by the sender using their private key.
- Every node that receives the transaction verifies the signature to confirm the validity of the transaction.
- This signature ensures that only the owner of the account can move money/data out of the account.

Example of signing a transaction.

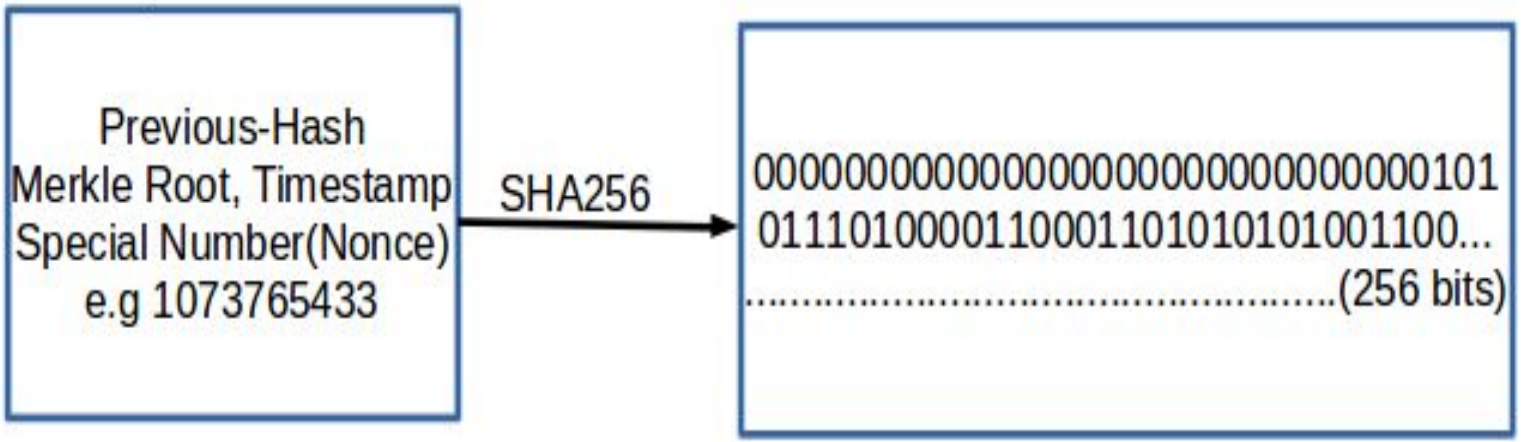
- If Alice wants to send 1 BTC to Bob, she must **sign a transaction spending 1 BTC of inputs** using her private key and send it to nodes on the network.
- The miners, who have knowledge of her public key, will then **check the conditions of the transaction and validate the authenticity of the signature**.
- Once validity is confirmed, the block containing that transaction will be then ready for finalization by a validator/miner.

Blockchain Consensus



Mining in Blockchain

- Miners verify the pending transactions in blockchain and find a new block to add to the blockchain.
- Miners compete to solve a puzzle - Find a special number called nonce and hashes the transaction content including this special number such that the hash value start with fixed number of 0’s. - Proof of Work
- Verification is easy but finding nonce is computationally expensive.


Previous-Hash
Merkle Root, Timestamp
Special Number(Nonce)
e.g 1073765433
SHA256
00000000000000000000000000000101
01110100001100011010101001100...
.....(256 bits)

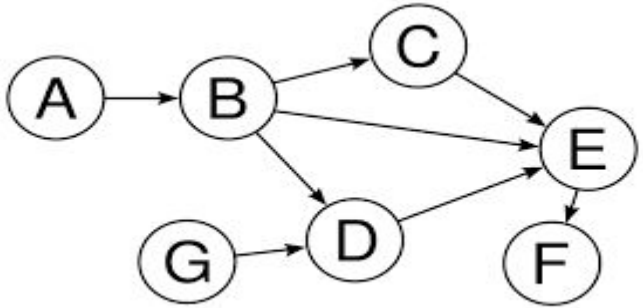
- Wasting resources - Large DCs to compute the nonce.
- Other techniques
  - PoA, Sharding, Sidechains, Hybrid consensus algorithms
  - Also add blocks linearly.
  - Design - competitive mining, wasted computational effort.
- VISA processes ~ 2,000 transactions per second.
- IoT network ~ 50 billion devices could produce several times that.

Directed Acyclic Graphs based Distributed Ledger

Directed Acyclic Graph

In graph theory, a directed acyclic graph means that the graph is directed and there are no cycles.

Each edge is directed from an earlier edge to a later edge. This is also known as a topological ordering of a graph.

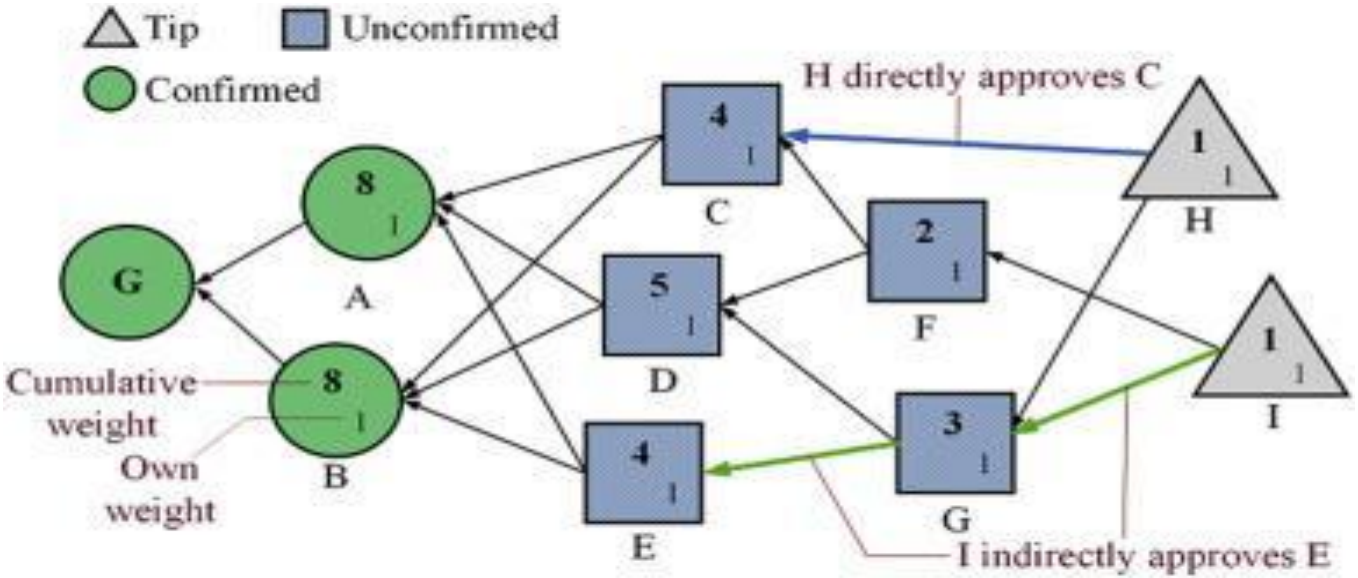


DAG based distributed ledger

- DAGs are another form of distributed ledger technologies.
- DAG is a network of individual transactions linked to other transactions.
- Blockchain is a linked list – while DAG is a tree branching out from transaction to another and so on.
- The vertices are transactions and the edges are references of transactions to its previous transactions.

Referencing previous transactions

- In blockchain a new block references previous block and hence forms a chain.
- In DAG, whenever a new transaction is created, a tip selection algorithm is run to select previous transactions called tips.
- The new transaction now becomes the tip and the process repeats.



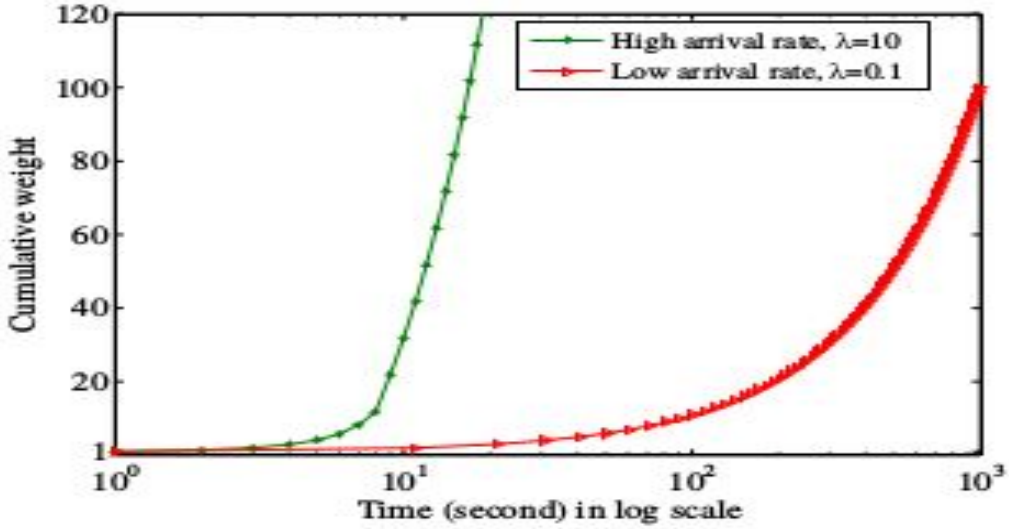
DAG Consensus:

- In Blockchain, consensus mechanism such as PoW , PoS are used where miners validate a set of transactions.
- Here, in DAGs, the new transaction validates the previous two transactions and performs a small proof of work.
- Network users are validators although they cannot validate their own transactions.
- Zero fee – Contribute to validations and get your transactions processed.
- Enables parallel processing.

DAG over linear blockchain

- Suitable for IOT devices
- High Throughput
- Highly scalable
- Faster transaction confirmation time

Consensus of a new transaction depending on arrival rate of transactions

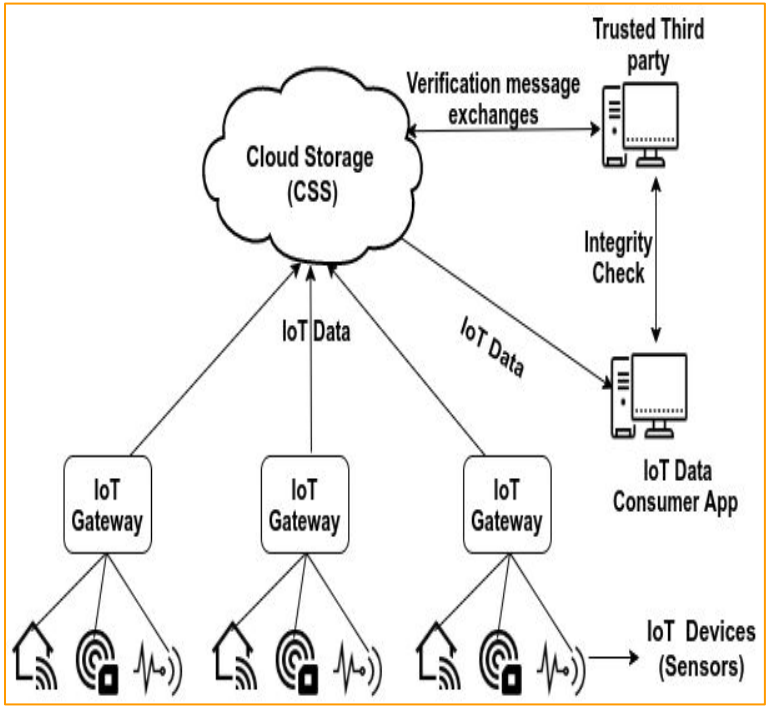


Ref: Yixin et al, Direct Acyclic Graph-based Blockchain for Internet of Things: Performance and Security Analysis.

'Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity'
Presented in 35th International Conference on Information Networking (ICOIN), South Korea

IoT Data Integrity Verification

- IoT applications use Cloud Storage Services (CSS) to store and process data on the Cloud
  - Eliminates local storage and management issues of massive scale data.
- Integrity of IoT data is crucial for building reliable consumer applications.
  - Smart meter data used for billing purposes may be tampered, resulting in higher charges to the customers.



Typical IoT architecture[1]

1. Qian Zhu, Ruicong Wang, Qi Chen, Yan Liu, and Weijun Qin. Iot gateway: Bridging wireless sensor networks into internet of things. In 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,

- Existing works mostly rely on trusted third party auditors.
- Risk and Operational cost by centralization.
- Existing Works on DAG ledgers
  - Stores entire ledger on each node in the P2P network locally- Not Suitable for IoT Environments.
    - Local storage and management issues

1. B. Liu, X. L. Yu, S. Chen, X. Xu and L. Zhu, ”Blockchain Based Data Integrity Service Framework for IoT Data,” 2017 IEEE International Conference on Web Services (ICWS),

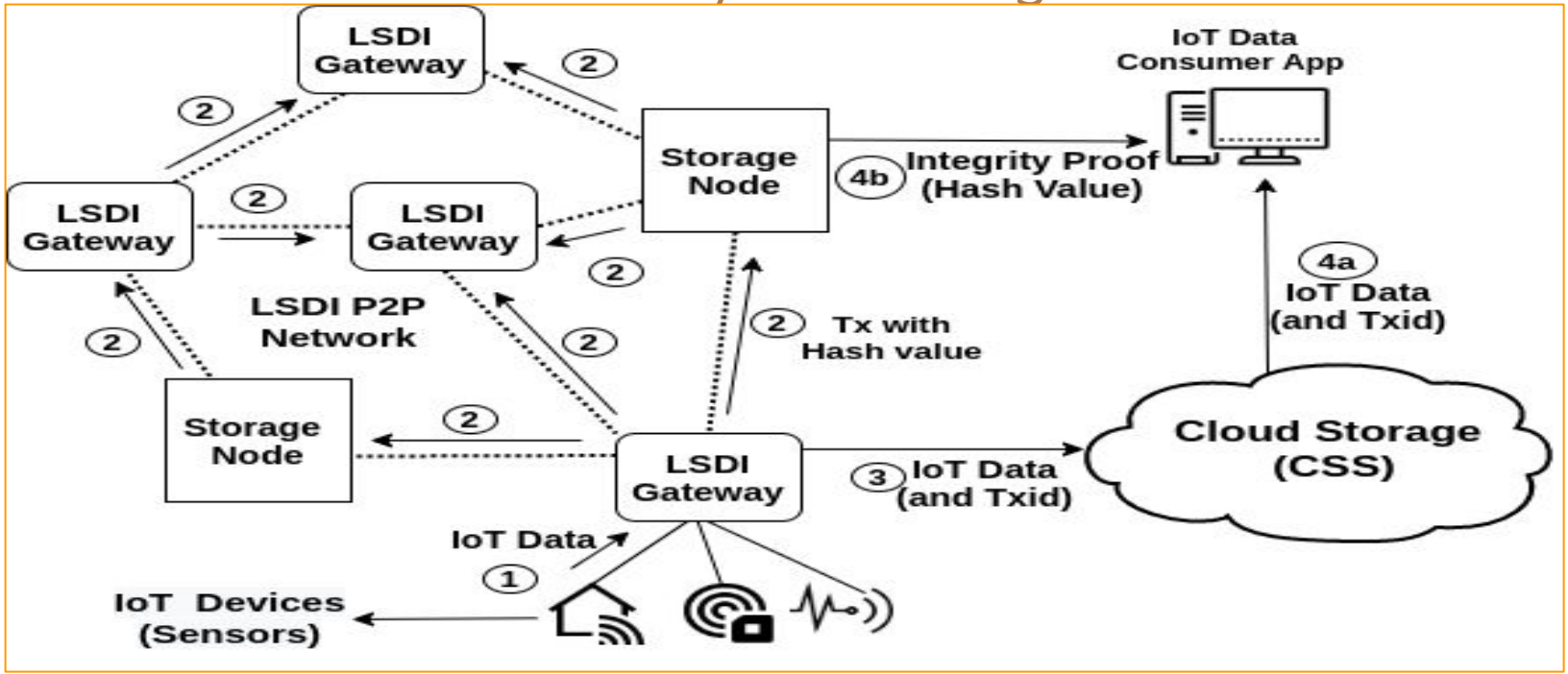
- Participation of IoT devices to P2P network is necessary to prevent potential abuse and attacks.
  - Light node vulnerability - IoT devices (light nodes) must rely on high capacity entities to generate transactions.
- Integrating IoT GWs as part of P2P ledger network is challenging -
  - Limited Storage and processing capacity.
- Solution: LSDI - Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity

System design

- LSDI P2P network comprises of three main entities: Gateways (GWs), Storage Nodes (SNs) and Discovery Nodes (DNs)
- **GateWays**
  - Collect IoT data from a group of end devices (sensors and actuators)
  - Generate **integrity proofs of the IoT data, includes them into the transactions and broadcast them** to the LSDI P2P network, and
  - **Forward the IoT data to the CSS** after appending Transaction IDs (Txid) to IoT data.
  - Performs Pruning and Network partitioning processes (explained later)

- **Storage Nodes** (SNs) are high storage capacity nodes
  - Store copy of the entire ledger
  - **Do not generate transactions**; contribute to the connectivity of the P2P network
  - Primary source of data (integrity proof) retrieval from LSDI.
- Discovery Nodes: Similar to Bootstrapping nodes in Bitcoin Blockchain
  - Newly joined GW nodes connect to the Discovery nodes and asks for peer (GW) information
  - Initiates the Network Clustering algorithm

LSDI System Design



- IoT consumer applications
  - a) obtain IoT data from CSS, compute its hash
  - b) compare it with integrity proofs of the corresponding IoT data from LSDI (using TXID of IoT data)

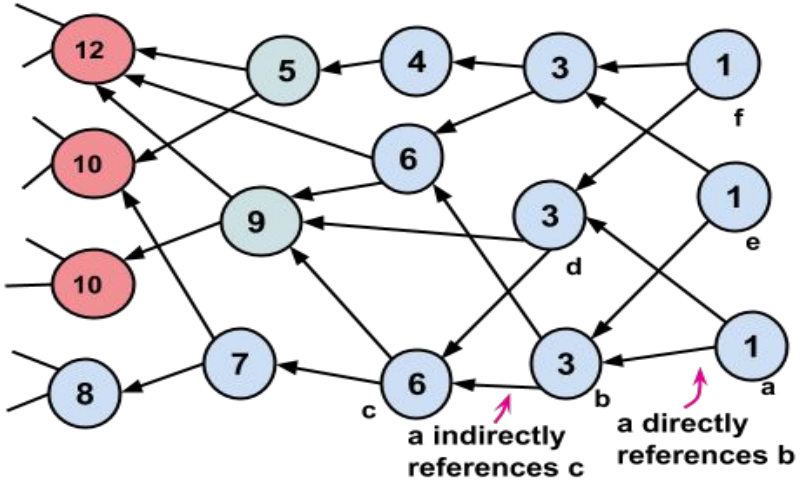
Transaction Structure (Customized to LSDI)

Transaction Field	Details
Left Tip	Tx_ID (SHA256 of left tip transaction)
Right Tip	Tx_ID (SHA256 of right tip transaction)
Integrity Proof	Hash of data
Public Key	Public key of GW
TimeStamp	Unix Timestamp
PoA	Signature of GW
PoW Nonce	Integer (used for rate control)

- Once the PoA & PoW of transaction are validated by a node (GW or SN), Tx is confirmed and added to ledger.
- **No concept of double spending in LSDI as all the transactions are non financial and carry only IoT data.**

Pruning

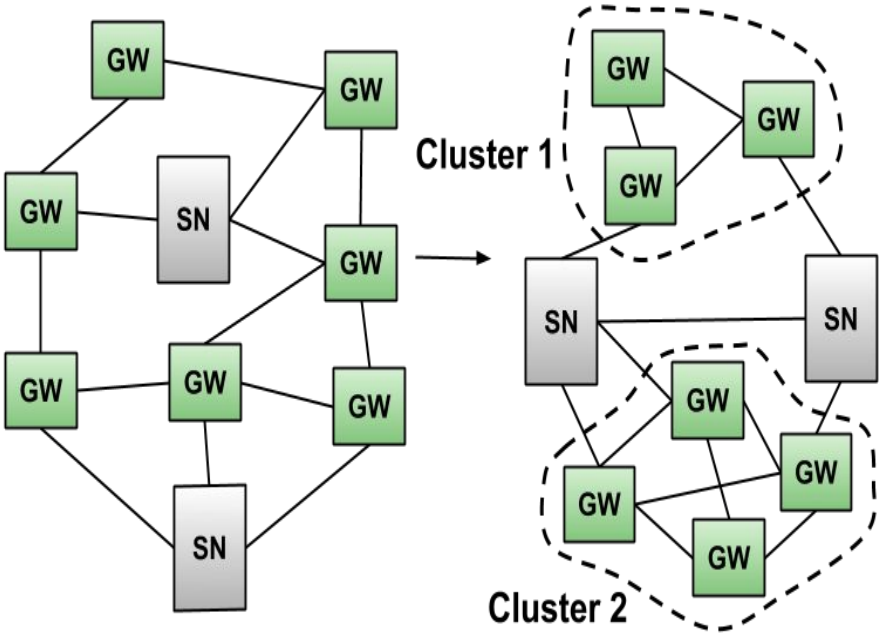
- GWs perform pruning to minimize storage consumption.
- Remove older transactions from DAG based on transaction weight.
- Reduces memory consumption in GWs.
- Storage nodes does not perform pruning.



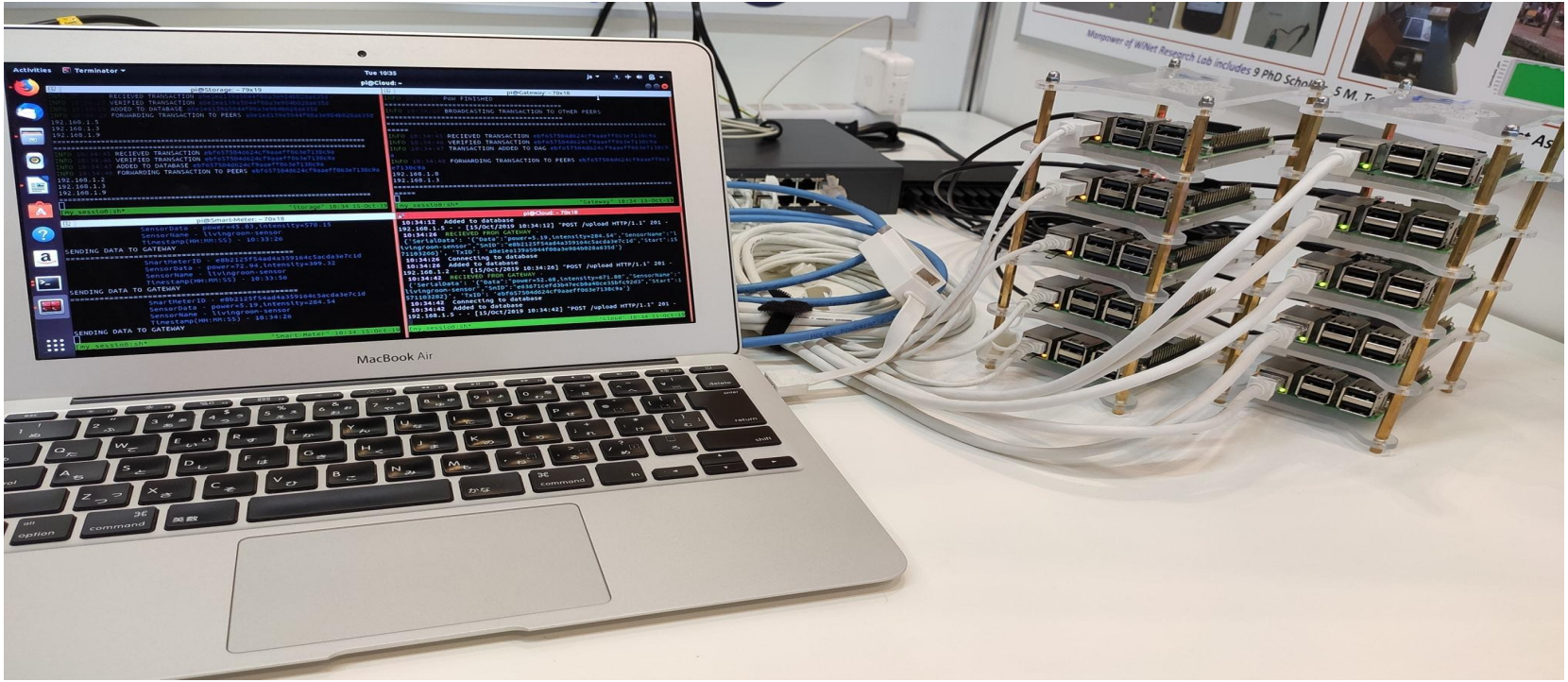
Cumulative weight of c, W_c = 2 (Direct References:b,d) + 3 (Indirect references: a,e,f) + 1 (own weight).

Network Partitioning

- Divides a large cluster of network into two small cluster networks.
- Minimize processing overhead of GWs.
- Discovery node triggers clustering process as the network gets big(than threshold).
- Each GW of a cluster carries out a set of actions (in distributed manner) to computes the Index number I_n (value of 0 or 1)



Experimental Setup (using Raspberry Pi's)

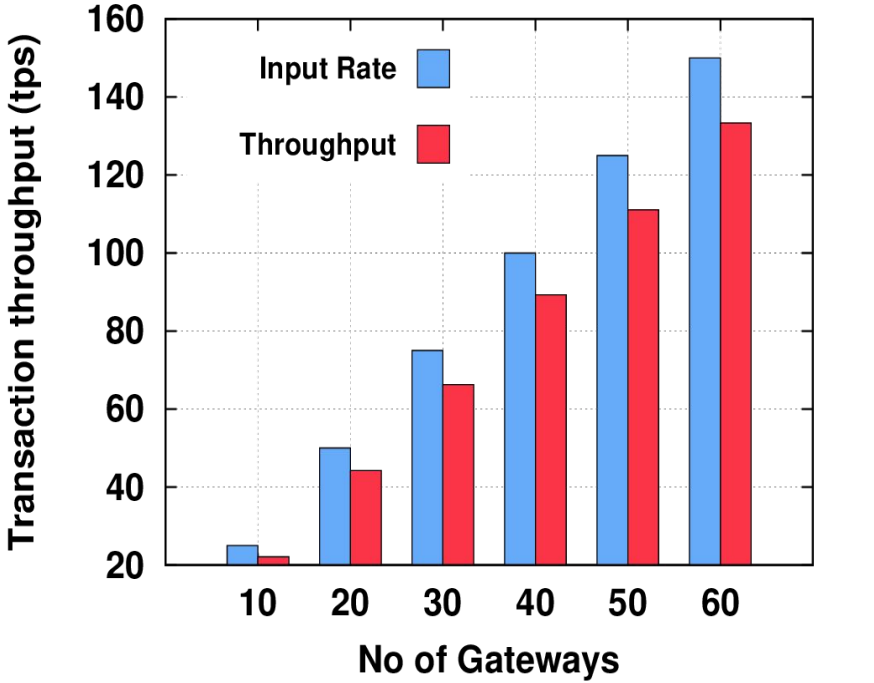


Experimental Setup using Docker containers

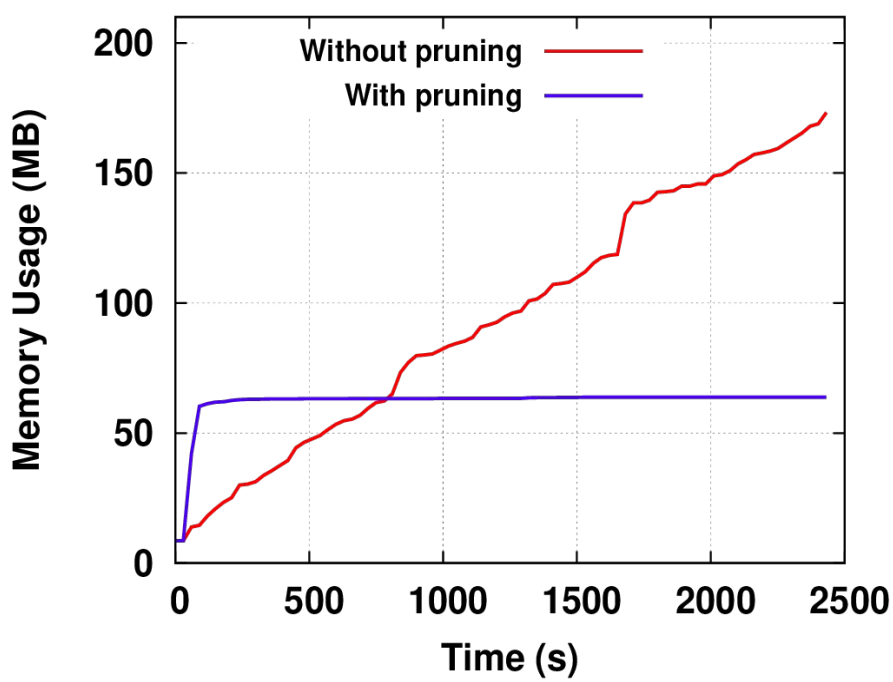
- We used 3 connected linux servers (Intel Xeon Processors, 16 cores, 32 GB RAM). Each node (GW, SN) is run as a docker container.

Total Number of SNs	**4**
Total Number of GWs	**10, 20,30,40,50,60**
Input transaction rate	**2.5 tps per GW (Inter-transaction delay of 400ms)**
Clustering Threshold	**10**
Pruning Threshold	**2000**

Tx Throughput, Memory consumption

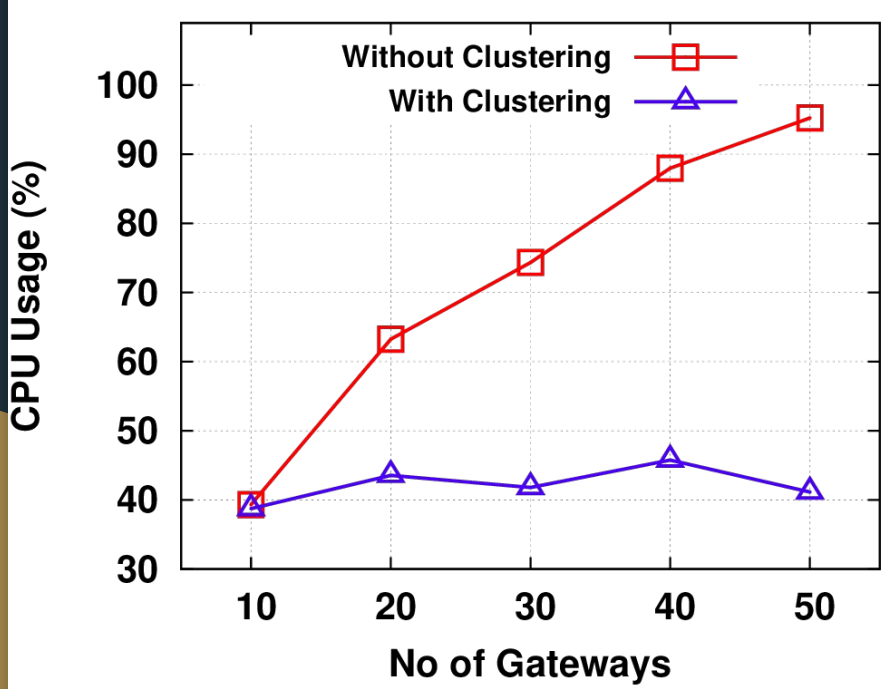


Avg Tx Throughput- rate at which tx are added to ledger

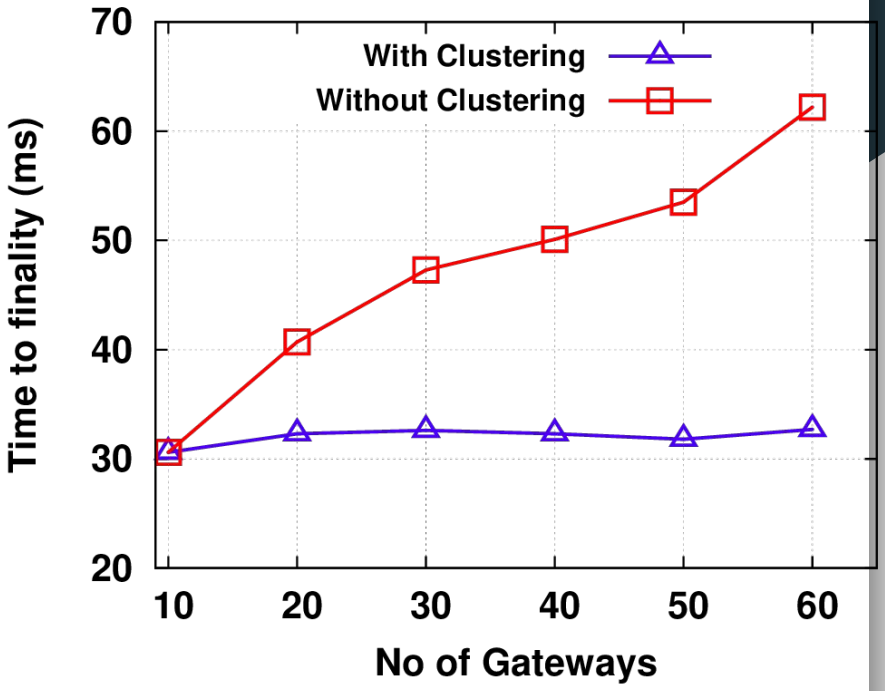


Avg Memory usage of a GW (in MB) in an LSDI P2P network with 30 GWs, with and without applying Pruning.

CPU utilization, Finality time



Average CPU usage



Finality time as Gateways increase.

Blockchain Scalable Solutions

Typically the solutions related to blockchain scalability fall into one of the following categories.

- Layer 1 solutions- are implemented at the base layer of a blockchain network - enhance the capacity and performance of the underlying blockchain protocol itself.
- Layer 2 solutions - aim to increase scalability by processing transactions off-chain or on secondary chains that are connected to the main blockchain.
- Consensus algorithm based solutions
- Blockchain Interoperability
- DAG based ledgers

Layer 1 solutions

Sharding: Sharding partitions the blockchain network into smaller shards, each capable of processing transactions and storing data independently. This allows for parallel processing and improves the scalability of the network.

SEGWIT is basically a protocol improvement in the Bitcoin blockchain network. It removes the signature data associated with each transaction, thereby opening up more capacity and space for storing transactions.

Blockchain Forks: Forking a blockchain can be a way to introduce scalability improvements. Hard forks, such as Bitcoin Cash (BCH) and Ethereum Classic (ETC), have been created to increase the block size or modify other parameters to enhance scalability. However, forks can result in network fragmentation and compatibility issues.

Layer 2 solutions

Off-chain Payment Channels: Payment channels like the Lightning Network (for Bitcoin) and Raiden Network (for Ethereum) enable faster and cheaper off-chain transactions between participating parties.

Sidechains: Sidechains are separate chains that are interoperable with the main blockchain. They can handle a large volume of transactions and settle periodically on the main chain. Examples include the Liquid sidechain for Bitcoin and Polygon for Ethereum.

Blockchain Interoperability: Interoperability solutions enable different blockchain networks to communicate and share data, expanding the overall network capacity and scalability. Projects like Polkadot, Cosmos, and Aion focus on achieving interoperability between multiple blockchains.

DAG-based Ledgers: Directed Acyclic Graph (DAG) structures, used by projects like IOTA and Nano, provide an alternative to traditional blockchain structures. DAG-based ledgers can process multiple transactions concurrently, potentially leading to higher scalability.

Consensus Algorithm Enhancements: Alternative consensus algorithms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) require less computational power and can process transactions more efficiently. Ethereum 2.0 is transitioning to a PoS consensus. Solana which utilizes a Proof of History (PoH) mechanism for parallel processing.

Decentralized Finance

- Decentralized finance (DeFi) is a financial technology based on distributed ledger technology.
- Financial institutions like banks and brokerages are bound by the rules of Government institutions (For example, In the U.S., the Federal Reserve and Securities and Exchange Commission (SEC) are the regulating bodies).
- Consumers rely on these centralized financial institutions to access capital and financial services directly.
- DeFi challenges this centralized financial system by empowering individuals with peer-to-peer digital exchanges.

Centralized Finance (CeFi) in the context of Cryptos

- Examples - Coinbase, Binance, Gemini etc.
- CeFi companies store your cash in custodial wallets and the private keys of users are stored in these crypto wallets.
- These companies offer a variety of services to customers - Ex: Cryptocurrency trading, borrowing, lending, margin trading, and more.
- Disadvantage with CeFi is the risk of being hacked.
- Users' funds would no longer be secure if the custodian's wallets are breached with no compensation by the company.
- The Binance hack in 2019, which resulted in the theft of more than $40 million in cryptocurrency, is one of the most famous examples.

Issues with Centralized Finance

- Government policy and Banks (RBI in case of India) controls the transfer of money.
- They can restrict the movement of currency from one individual/organization to another, regulate the charges and if required can stop you from accessing your money.
- For example if you are running a business and making money, the govt can tell you not to bring your money to the bank - can’t deposit, invest, or safely keep them.
- Impose higher interest rates.

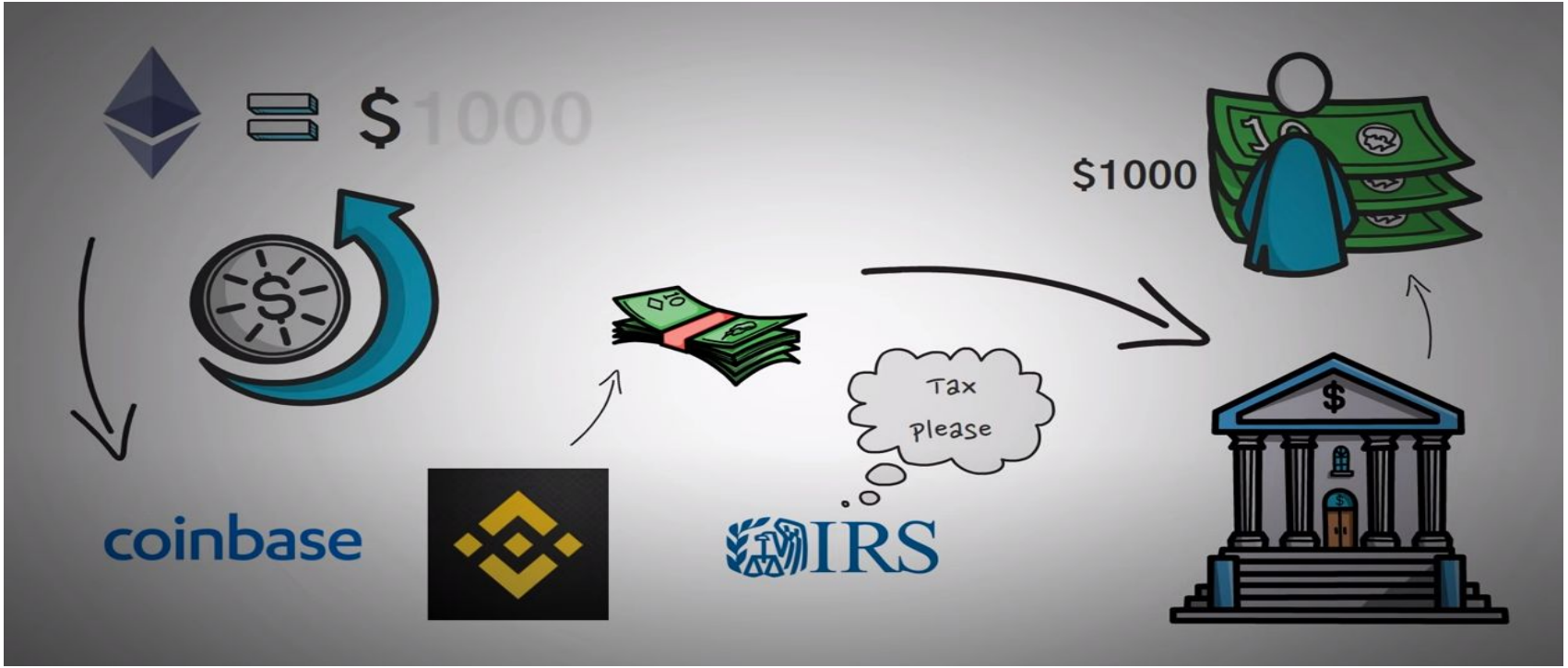
Alternative - Decentralized Finance

- No centralized banks/exchanges - only pieces of code (smart contracts) that run as a bank and open to any one.
- They are immutable, can be trusted- you can view and verify the rules and regulations.
- DeFi eliminates the fees that banks and other financial companies charge for using their services and makes the transaction processing faster.
- Individuals hold money in a secure digital wallet, can transfer funds in minutes, and anyone with an internet connection can use DeFi.
- DeFi is based on Cryptography, Blockchain and Smart Contracts.

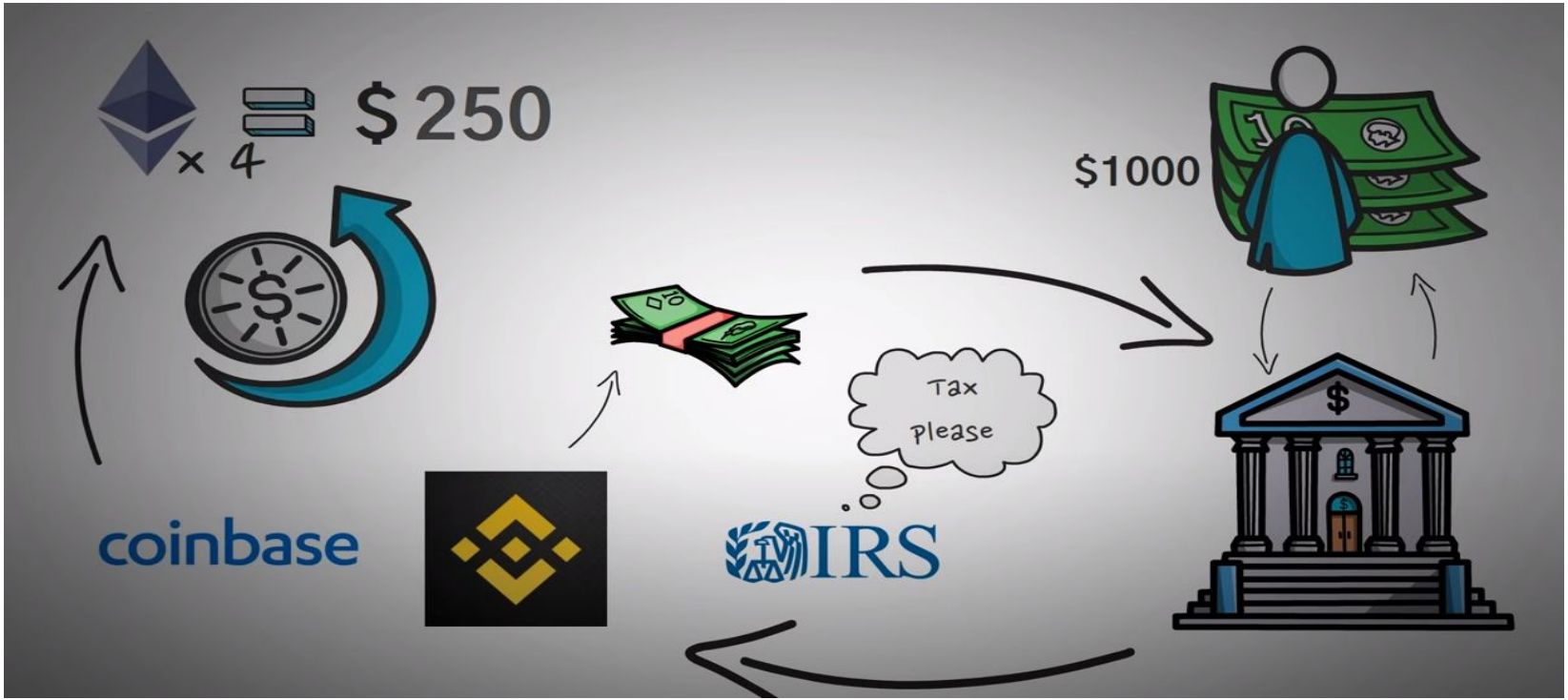
Fundamental pillars of DeFi
Stablecoins

- DIA, Tether, USDCoins are all stablecoins.
- Their price is tied to a real currency - USD
- Without USDCoin you have to trade using a centralized exchange - for example - Coinbase (a centralized cryptocurrency platform CeFi)
- Let us understand this with an example.
- Let say you have some ether worth $500 and it became $1000.

Want $ for ether - Price increased from 500 to 1000



You want to buy back when ether price has gone down to 250.



- Then again sell when Ether price has gone up to 500$.
- Lot of fee, taxes, waiting time to get your money to bank from Coinbase and then withdrawal of the USD.

- Use **Decentralized Autonomous Organization** (DeFi application- Code) actually solves this through stablecoins.
- Convert ether to Stablecoin and trade using stablecoins.
- Less fee (1%), fewer mins to buy and sell.
- DeFi application- Code- trusted- transparent.

Lending and Borrowing

- Current financial systems are mostly used for lending and borrowing money.
- Individuals need to put something down as collateral to lend or borrow money from the banks - Interest rate can be terribly high, sometimes going up to 20%-25%.
- In DeFi space, users are able to work with others by allowing them to use their funds without giving away their custody (collateral).
- This is all possible with the use of smart contracts.

- If a person wants to earn some interest on his crypto holdings, they can simply go to **AAVE** - the biggest crypto lending platform - and deposit their funds into a smart contract.
- In return, they get specific tokens that are equivalent to their original deposit, plus the interest.
- This procedure involves no individual or organization to calculate or complete the transaction; the automated code does it all!
- Hence, there is no such thing as the monopoly of a centralized entity in the system.

Decentralized Exchanges

- Decentralized exchanges, or simply DEX allow the users to trade different assets, such as NFTs and cryptocurrencies, at incredibly low fees.
- For example Forex exchanges (conversion of one fiat currency to another) charge their customers an exchange fee.
- Fee rate is dependent on federal taxes and the personal interest of the exchange owners.
- A DEX is not owned or governed by a single entity - smart contract code regulates every aspect of it - trading fee is predetermined- put into smart contract - can exchange at incredibly lower rates.

Insurances

- Crypto insurance works same way as real-world insurance policies.
- They help you recover your losses by offering you monetary compensation, and in return, you pay them a fee.
- But the difference is, unlike regular insurance firms where people calculate and assess the risk, everything is done by the blockchain code for DeFi insurance.

Thank You.. Queries...?

References

https://www.youtube.com/watch?v=17QRFlml4pA

https://originstamp.com/blog/defi-vs-bitcoin-whats-the-difference/

Youtube Channel - Whiteboard Crypto