Report for SoS’24

Blockchain

Quraishi Abdur Rahman

(23b2471)

Mentor: Pratiksha Deka

Blockchain technology is changing industries in ways we never thought possible. It's not just about cryptocurrencies anymore. In this report, I'll be exploring what blockchain is, how it came to be, and why it's such a big deal in the digital world where everyone wants to grow.

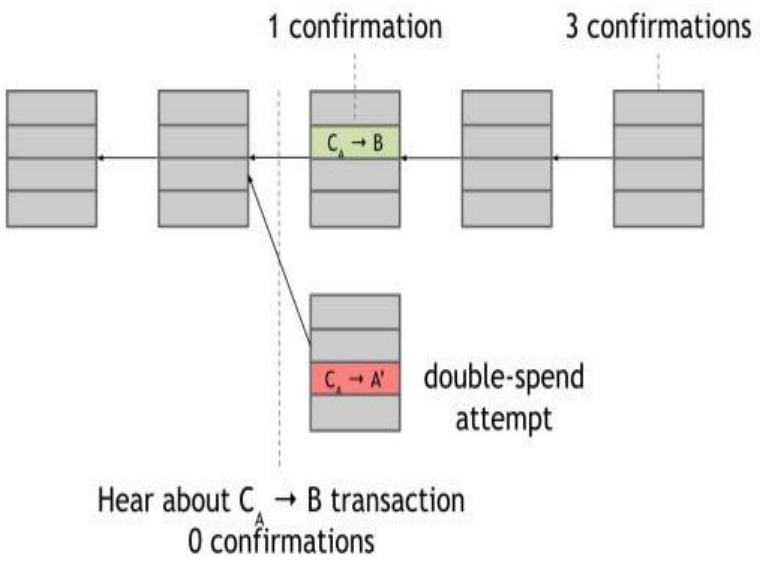
So, what is Blockchain?

A blockchain is a decentralized, distributed ledger that stores records of ownership and transactions.
Unlike those traditional databases which many people use in this world and rely on central authorities, blockchain operate across a network of nodes.
I'm including some features of the same which I've explored through the given references. Some of them are:

1. Decentralization: No single entity controls the entire blockchain. Instead, all participants collectively maintain it.
2. Immutability: Once data is recorded on a blockchain, it becomes irreversible. This immutability ensures trust and security.
3. Transaction Transparency: All transactions are publicly visible which in turns enhances transparency in transaction.
4. Genesis Block and Info-Bitstring: The first block also known as the genesis block initializes the chain and further each subsequent block contains an info-bitstring linking it to the previous one.

Bitcoin and the evolution of the Blockchain technology

- Bitcoin (2009): The first successful implementation of blockchain technology was in Bitcoin, created by the mysterious figure Satoshi Nakamoto. Bitcoin introduced the concept of a decentralized digital currency.
- Demand and Supply: Bitcoin's limited supply which is around 21 million coins drives demand which in turns make it a unique class of asset.
- Double spend Problem: This was the major problem before but blockchain solves the double spend problem by ensuring that each unit of cryptocurrency can only be spent once.



Key Components of Blockchain

1. Private and Public keys:
    a) Users interact with the blockchain using cryptographic keys.
    b) Public keys serve as addresses for receiving funds.
    c) Private keys grant access to control and transfer those funds.
2. Hash Functions:
    a) Hashing ensures data integrity.
    b) Each block contains a hash of the previous block, creating an unbreakable chain.

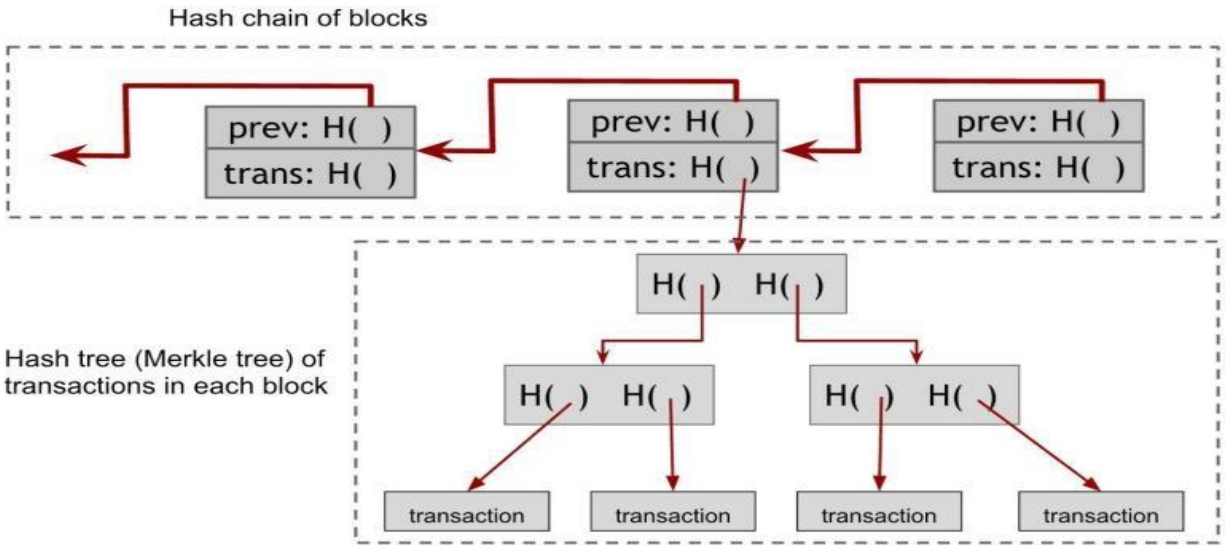


Figure 3.8. The Bitcoin block chain contains two different hash structures. The first is a hash chain of blocks that links the different blocks to one another. The second is internal to each block and is a Merkle Tree of transactions within the blocks.

(Figure is from Arvind Narayanan's Bitcoin and Cryptocurrency Technologies)

3. Proof of Work:
    a) Proof of Work consensus mechanism validates transactions. Although it has some issues as if a controlling entity owns 51% or more nodes in the network than the entity can corrupt the blockchain as it has a majority of the network.
    b) Miners compete to solve complex mathematical puzzles, securing the network.

4. Anonymity:
    a) As we know that transactions are transparent, but users' identities remain confidential
    b) Privacy is one of the major and crucial aspect of adoption of blockchain technology nowadays.

5. Ownership and Common Database:
    a) Ownership is established through cryptographic keys.
    b) The common database (the blockchain itself) maintains a secure record of all transactions.

Applications Beyond Cryptocurrencies

1. Decentralized Finance (DeFi):
    a) Smart contracts enable automated financial services without intermediaries.
    b) Lending, borrowing, and yield farming are popular DeFi applications which are used nowadays.
2. Non-Fungible Tokens (NFTs):
    a) NFTs represent unique digital assets on the blockchain technology.
    b) They prove the ownership and authenticity of the user.

Applications of Blockchain:

1. Governance and Identity:
    a) Land records, e-health records, and transportation data benefit from blockchain's transparency and security.
    b) Virtual currencies, passports, and identification can be securely managed.
2. Commercial:
    a) Supply chains gain transparency and traceability.
    b) Auctions, gaming and inter-bank transfer benefit from decentralized trust.

c) Everledger uses blockchain for diamond provenance which in turns enables customer and industry professionals to verify the authenticity and the history of a diamond.

3. Disruptive Potential:
    a) Cryptocurrencies (Bitcoin) challenge traditional finance.
    b) Initial coin offerings (Ethereum) redefine fundraising.

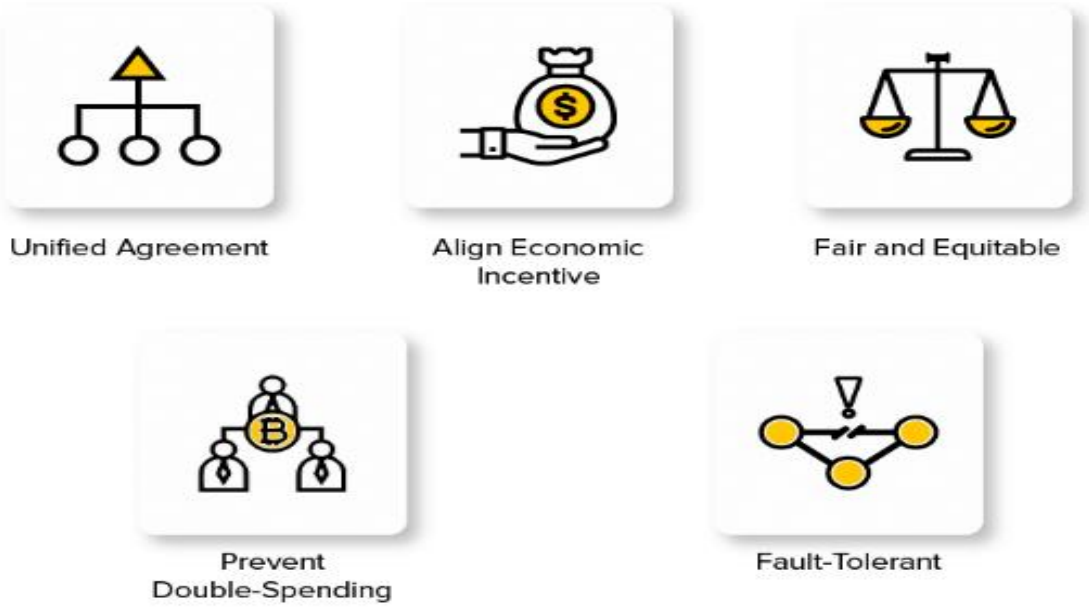
Decentralization and Consensus:

1. Bank Transfers vs. Blockchain:
    a) Traditional bank transfers involve intermediaries and takes time.
    b) Blockchain eliminates middlemen, in turn ensuring faster and direct transaction.
2. Blockchain in Fintech:
    a) Decentralized finance (DeFi) leverages blockchain for lending, borrowing, and for much more.
    b) Legacy system will certainly face disruption.
3. Shared Blockchains:
    a) Multiple in fact almost all banks maintaining a single blockchain enhances efficiency and reduces time for transactions.
    b) Consensus mechanisms validate transaction.

From this all we conclude that blockchain technology will continues to evolve, in turn promising a future of technology where it guarantees trust, transparency, and decentralization which redefine how we interact with digital systems. As we will go further and explore more, we will be able to see the impact of blockchain extends far beyond its origins in Bitcoin.

"Bitcoin is a secure and anonymous digital currency"

— WikiLeaks donations page



Bitcoin: Decentralized Cryptocurrency

1. Bitcoin Basics:
    a) Bitcoin Address: When you install a Bitcoin wallet, it generates your own unique address known as Bitcoin address similarly as an email address. You can share this address with others to receive payments.
    b) Blockchain: As I've described it before that blockchain is based on shared public ledger so for the same Bitcoin transactions are recorded on blockchain.
2. Transactions and Private Keys:
    a) Transactions: When you send Bitcoin to someone, it's a transfer of value between wallets. These transactions are verified by network nodes and added to the blockchain.
    b) Private Key: Your Bitcoin wallet holds a secret piece of data called a private key. It's used to sign transactions which proves your ownership. Once we signed, a transaction cannot be altered mainly to ensure atomic transactions.

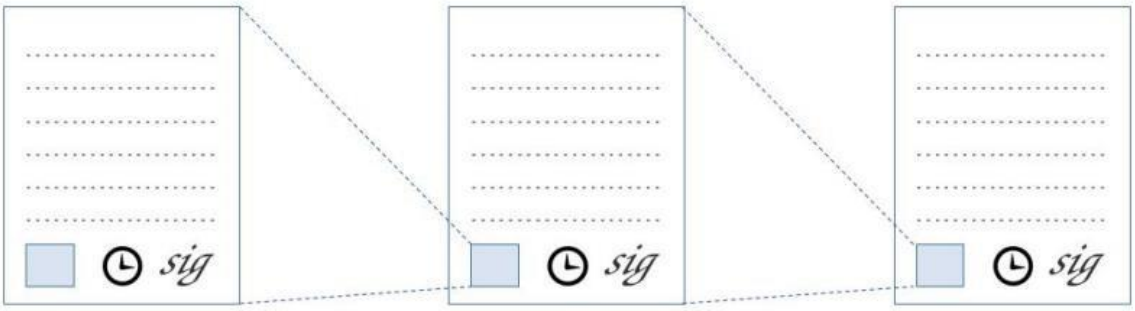


Figure 4: linked timestamping. To create a certificate for a document, the timestamp server includes a hash pointer to the previous document's certificate, the current time, and signs these three data elements together.

3. Mining and Consensus:
    a) Mining: Mining is the process of confirming pending transactions. Miners compete to solve complex mathematical puzzles, creating new blocks. These blocks are added to the blockchain, and once added cannot be removed.
    b) Proof of Work: Miners validate transactions by solving proof of work puzzles. This ensures the integrity of the blockchain and prevents tampering.
4. Decentralization and Trust:
    a) No Middlemen: Bitcoin transaction happen directly between the users, without any intermediaries like banks. As it direct so enhances efficiency and reduces time for transaction.
    b) Immutable Ledger: Once a transaction is confirmed, it's permanent. No one can alter it, ensuring trust.

Understanding Transactions in Blockchain

1. The Digital Ledger: Decentralized and Immutable ○ Let's imagine a global spreadsheet shared among thousands of computers across the globe, this is the blockchain. Whenever you in initiate a transaction (let's say sending bitcoin), it's like adding a new row to this spreadsheet. But here is a twist in it that no single entity controls it, instead nodes(computers) across the world maintain it collectively.
    - Transaction Flow: Suppose you decide to transfer some Bitcoin to your friend. Then you broadcast this transaction to the network. Nodes verify it by checking your balance which ensures that you have enough Bitcoin and they validate your cryptographic signature.
      Once verified, the transaction is bundled into a block.

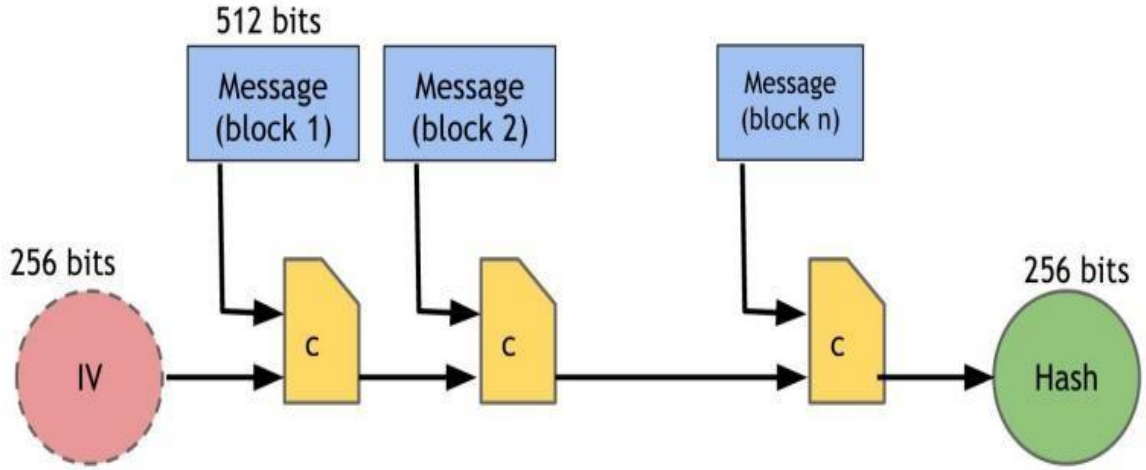
2. Blocks and Chains: The Building Blocks of Trust ○ Blocks: Each block contains a batch of verified transactions. Think of it as a page in a ledger.

   Crucially, each block points back to the previous one. This linking creates a chronological chain – the blockchain.

   Tampering with any block would require recalculating all subsequent blocks' hashes – practically impossible.

   - Immutability: Once a block is added, it's etched in digital stone. No one can alter it.

     This immutability ensures trust. Imagine a land registry where records can't be erased or forged – that's blockchain.



Cryptocurrency Creation: The Role of Mining

1. Proof of Work: Unleashing Digital Gold
   - Mining Process:
     - Miners are like the digital gold prospectors. They compete to solve complex puzzles, which in turn allows them to create a new block, it is similar to like discovering a gold nugget.
     - The first miner to find the solution broadcasts it to the network.
   - Block Reward:
     - As a reward for their computational efforts the successful miners receive freshly minted cryptocurrency (e.g., Bitcoin).
   - Halving Events: Bitcoin's issuance is predictable and roughly after every four years, the block reward is halved.

2. Decentralization and Trust: The Heart of Blockchain

- Decentralization:
    - No central authority. No gatekeepers. Just nodes working together.
    - Trust anyhow emerges from this collective agreement.
- Immutable Records:
    - Once recorded, a transaction becomes part of history.
    - Trust isn't placed in a bank or government; it's woven into the fabric of math and code.

Blockchain isn't just about money; it's about rewriting the rules of trust.
As exploring blockchain this digital frontier, we glimpse a future where we meet with transparency, security, and empowerment converge.

"Bitcoin won't hide you from the NSA's prying eyes"
— Wired UK

How cryptocurrencies operate under different protocols:

Let's imagine a bustling marketplace where all sorts of vendors hawk their wares, but instead of gold coins or other coins, they trade with some shiny new tokens.

These tokens are to be assumed to be cryptocurrencies, and the marketplace itself is run on some set of rules, kind of like a constitution for this digital society.

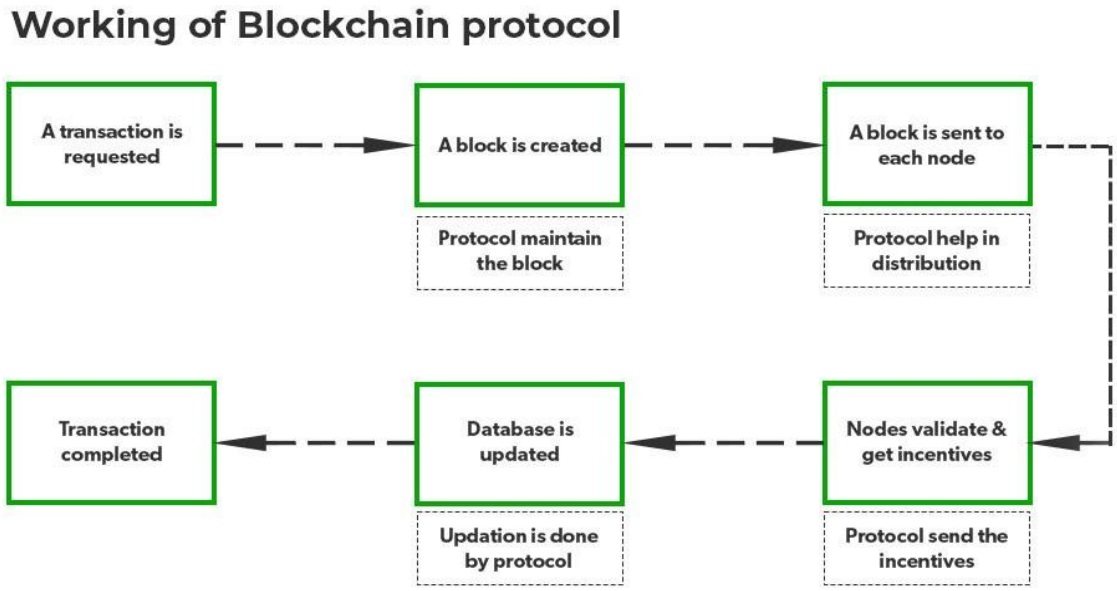
These rules are called protocols, and they only determine how everything will work.

Why protocols matter so much?

1. The Power of Decentralization: Many cryptocurrencies in fact almost are all about ditching the middlemen. Unlike these traditional banks, there is no central authority governing the flow and control of money.
   The protocol ensures everyone on the network plays by the same rules keeping the things fair and transparent.
2. Keeping Things Secure: Security is paramount in this digital marketplace. The protocol dictates how new tokens are created and how transactions are verified, and how the entire system is protected from fraudsters trying to steal or copy tokens. Different protocols use different mechanisms to achieve this, like Proof of Work thing in the similar manner that of miners solving complex puzzles/problems.
3. Shaping the Currency's Character: Think of a protocol as the DNA of a cryptocurrency. It defines things like how many tokens will ever exist, how fast the transactions will happen which is the speed of it, and even what the tokens can be used for Bitcoin, for eg. it is known for its limited supply and secure transactions,

whereas Ethereum is designed for running smart contracts also known for self executing agreements.

4. Evolution and Innovation: The main beauty of protocols is that they can be constantly improved depending on the need. Developers can create new protocols or modify the existing ones to address specific needs. This allows for innovation in the cryptocurrency space, leading to the creation of new and exciting applications.



So, whenever we read or hear about any cryptocurrency, it's not just about the shiny new token. It's all about the intricate protocol that forms the foundation of this digital marketplace, shaping it how it operates and what it can achieve.

In today's world Blockchain technology has revolutionized the way we think about the digital transactions and data security.

In this post mid-term report we will explore specific aspects of blockchain, including the Slasher rule, anonymity, mixing, raft, Byzantine Fault Tolerance, PBFT, payment channel network, and HTLC, to understand how they contribute to the overall robustness and privacy of blockchain networks.

Slasher Rule

The slasher rule is a concept which is specially designed to enhance the security of the blockchain networks, particularly those using PoS consensus mechanisms.

It aims to prevent the malicious behaviour by penalizing the validators who act dishonestly.

How It Works?

1. Double Signing: If a validator attempts to validate multiple conflicting blocks which is commonly called by us as double signing than the Slasher rule comes into the play. Double signing is a form of attack where a validator tries to create

two different versions of the blockchain, which can further lead to a fork and can undermine the networks integrity.

2. Validators and Stakes: In a PoS system, validators are chosen to create new blocks based on their amount of cryptocurrency they hold and are willingly to stake as collateral. This stake acts as a security deposit that can be confiscated if the validator behaves maliciously.
3. Penalties: The Slasher rule penalizes validators who double sign by confiscating/seize a portion of staked cryptocurrency.
   This economic disincentive ensures that validators act honestly, as this cost of malicious behaviour override the potential benefits. The confiscated stake can be redistributed to honest validators or can be destroyed to reduce the total supply of cryptocurrency.

Impact on Security

1. Deterrence: By imposing financial penalties, the Slasher rule deters validators from attempting to compromise with the network.
   The risk of losing their staked assets and their position as validators makes them more likely to follow the rules.
2. Network Integrity: It helps to maintain the integrity and trustworthiness of the blockchain which in turn ensures that all participants adhere to the consensus rules. This mechanism is very much crucial for the stability and security of PoS based blockchains.

Anonymity

Importance of Anonymity:

Anonymity is one of the crucial aspects of blockchain technology, particularly for the cryptocurrencies like Bitcoin. It ensures that users can transact without revealing their actual identities which in turn protect their privacy. Anonymity is essential for maintaining user confidentiality and preventing unwanted surveillance by everyone.

How Anonymity is Achieved?

1. Pseudonymous Addresses: Users interact with the blockchain using pseudonymous addresses, which are not directly linked to their real world identities. Each transaction is associated with a unique address, making it difficult to trace the transaction back to the user.
2. Cryptographic Techniques: Advanced cryptographic techniques, such as zero-knowledge proofs, enable transactions to be verified without revealing

their sensitive information. Zero knowledge proofs allows one party to prove to another that a statement is true without conveying any additional information.

3. Mixing Services: These services further enhance anonymity by pooling and redistributing transactions, making it difficult to trace the origin and destination of funds. In actual we can say these services breaks the link between the sender and receiver which in turn ensures that transaction histories are kept confidential.

Benefits of Anonymity:

1. Privacy Protection: Users can conduct transactions without any fear of surveillance or tracking. This protection is very much important in regions having strict financial regulations or we can say where privacy is highly valued for user.
2. Security: Anonymity reduces the risk of targeted attacks, such as phishing or identity theft. By keeping user identities hidden, it becomes more challenging for many malicious actors/people to target specific user.

Mixing

Overview:

Mixing is a process which is used to enhance the privacy of blockchain transactions. It basically involves combining multiple transactions to hide the path of the funds, which in turn makes difficult to trace individual transactions.
It is an essential tool for users who wants to prioritize privacy and confidentiality in their financial activities.

How It works?

1. Transaction Pooling: Users send their cryptocurrency to a mixing service which in turn pools the funds with those of other users. Which creates a large pool of mixed transactions which makes it difficult to trace the origin of any single transaction.
2. Redistribution: The mixing service then redistributes the funds to the intended recipients in turn breaking the link between the sender and receiver. This process will ensure that the transaction history is confidential which enhances privacy.
3. Enhanced Privacy: By mixing transactions the service ensures that the transaction history is kept confidential which in turn makes it challenging for the third parties to trace the flow of funds. This is particularly useful for those users

who want to keep their financial activities private and confidential from the world.

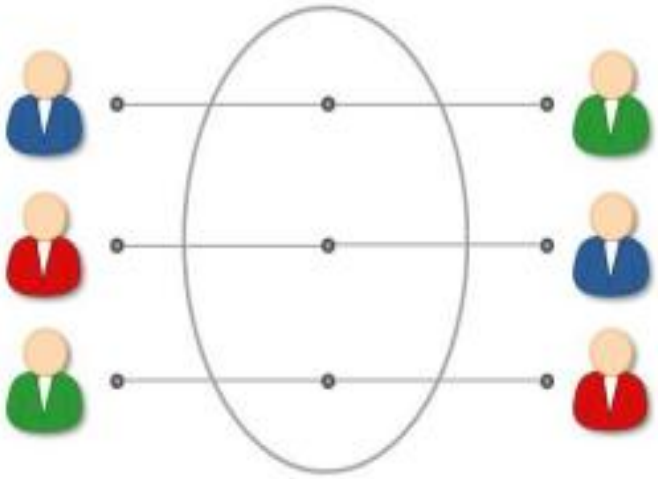


Figure 6.7 : Mixing. Users send coins to an intermediary and get back coins that were deposited by other users. This makes it harder to trace a user's coins on the block chain.

Applications of Mixing

1. Cryptocurrency Transactions: Mixing is commonly used in cryptocurrency transactions nowadays to protect users privacy. In short it helps users maintain anonymity and confidentiality in their financial dealings.
2. Financial Privacy: It can also be applied and can be used in other financial contexts where privacy is important for users. For example, businesses around the globe may use mixing services to protect sensitive financial information from competitors.

In all this blockchain technology, with its innovative concepts like the Slasher rule, anonymity, and mixing, offers solutions for enhancing security and privacy.
This mechanism ensures the user that this technology remains trustworthy and that users can transact easily with confidence knowing their privacy is protected.
As this technology is evolving these features will play a crucial role in its widespread adoption and also its acceptance.

Raft Consensus Algorithm

Overview:

Raft is a consensus algorithm which is been designed to be understandable and easy to implement. It is basically used for managing a replicated log in distributed systems in turn ensures that all nodes in the network agree on the same sequence of transactions.

How It Works?

- Leader Election:
  1. Process: Raft operates by electing a leader among the nodes only. Basically the leader is responsible for managing the log replication and ensuring consistency. If the leader fails than a new leader is elected through a consensus process.
  2. Term: Each term begins with an election. Nodes vote for a candidate, and the candidate with a majority of votes becomes the leader. It is kind of similar like our Indian election which held after every term of 5 years.
  3. Heartbeat Messages: The leader sends periodic heartbeat messages to followers to maintain authority and prevent new elections.

- Log Replication:
  1. Client Requests: The leader receives client requests and adds them to its log.
  2. Replication: The leader replicates these log entries to follower nodes. Followers add the entries to their logs.
  3. Acknowledgment: Followers than acknowledge the receipt of log entries. Once the majority of followers acknowledge the entries, the leader commits it.

- Commitment:
  1. Commit Index: The leader has to maintain a commit index which than indicates the highest log entry known to be committed.
  2. Durability: Committed entries are durable and replicated across the network which in turn ensures consistency.

- Safety and Simplicity:
  1. Separation of Phases: Raft separates the consensus process into distinct phases (leader election, log replication, and safety), which makes it easier to understand and implement compared to other consensus algorithms like Paxos.
  2. Conflict Resolution: Raft than handles conflicts by ensuring that the leader's log is always the authoritative source. If a follower's log diverges, it is than brought in line with the leader's log.

Applications:

Raft is commonly utilized in distributed systems where simplicity and reliability are crucial. It is particularly effective in environments where nodes may crash but are not expected to behave maliciously. Examples of its use include distributed databases, configuration management systems, and replicated state machines.

Byzantine Fault Tolerance (BFT)

Overview:

Byzantine Fault Tolerance is a property of a system that can continue to operate correctly even if some of its nodes behave maliciously or we can say not as usual. BFT is very much crucial for ensuring the reliability of distributed systems even when facing arbitrary faults.

How It Works:

- Fault Tolerance:
    1. Byzantine Faults: BFT systems are designed in such a way that they can tolerate a certain number of faulty nodes or we can say up to one-third of the total nodes. These faults can include software bugs, hardware failures, or the malicious attacks.
    2. Redundancy: BFT systems basically use redundancy to ensure that the system can continue to operate even if some nodes fail or if they act maliciously.

- Consensus Mechanism:
    1. Voting Rounds: BFT algorithms usually use a consensus mechanism that requires nodes to agree on the state of the system. This agreement is achieved through multiple rounds of voting and message exchanges.
    2. Majority Agreement: A supermajority which is typically around two-third of total of nodes must agree on any state change for it to be accepted.

- Cryptographic Techniques:
    1. Message Authentication: BFT systems usually or we can say often employ cryptographic techniques to ensure the authenticity and integrity of messages exchanged between nodes. In this case digital signatures and hash functions are commonly used.
    2. Quorum Systems: Quorum systems ensures that a sufficient number of nodes participates in the consensus process to maintain security and reliability.

Applications:

BFT is essential in environments where security and reliability are very much critical, such as we can say in financial systems, military applications, and blockchain networks. It also ensures that the system remains operational even in the presence of malicious actors. Examples can include permissioned blockchains, distributed databases, and critical infrastructure systems.

Practical Byzantine Fault Tolerance (PBFT)

Overview:

Practical Byzantine Fault Tolerance (PBFT) is an optimized version of BFT which is designed to improve performance and scalability of the network. PBFT is particularly we can say well suited for real world applications where high through put and low latency are required.

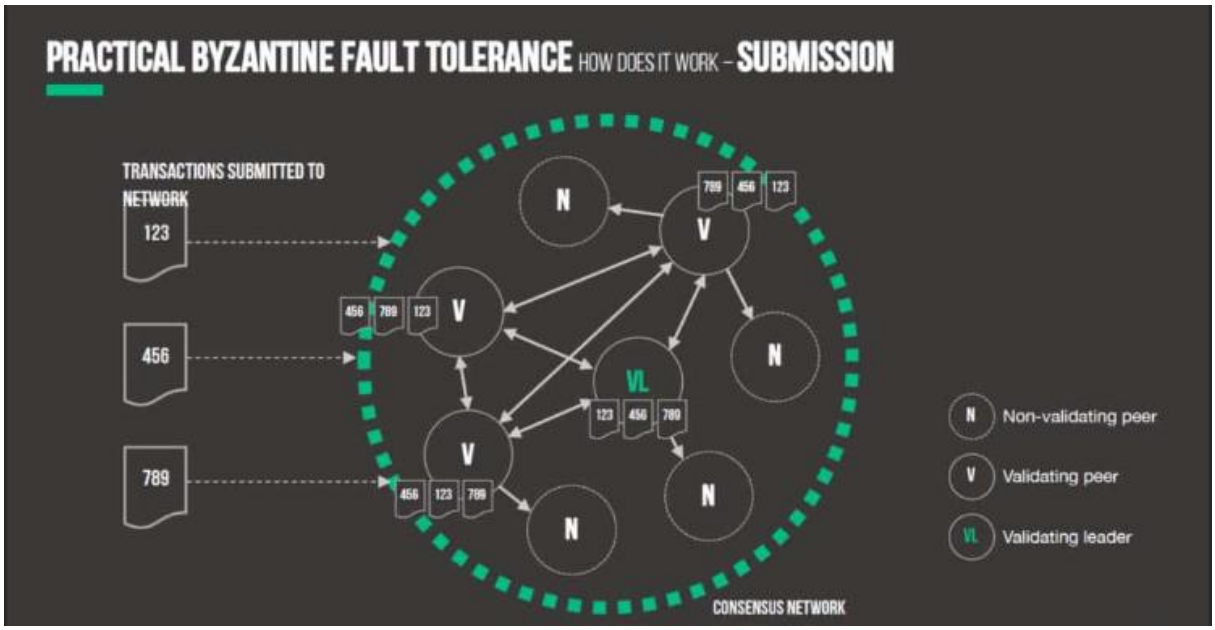
How It Works?

- Primary and Replicas:
    1. Primary Node: PBFT operates with a primary node and also with multiple replica nodes. The primary node first proposes a state change, and the replicas validate and agree on the proposal.
    2. View Changes: If the primary node fails or let's say it acts maliciously than the system can initiate a view change to elect a new primary.

- Three-Phase Protocol:
    1. Pre-Prepare Phase: The primary node sends a pre-prepare message to all replicas in which proposing a state change.
    2. Prepare Phase: Replicas validate the proposal and send the prepared messages to each other. If a replica receives prepare messages from a super majority of the nodes than it moves to the commit phase.
    3. Commit Phase: Replicas than send commit messages to each other. Once a replica receives commit messages from super majority of the nodes than it proceeds to commits the state change.

- Fault Tolerance:
    1. Supermajority Agreement: PBFT can tolerate up to one third of the faulty from the total nodes which is kind of similar of BFT. It also achieves this by requiring a majority which is around two-third of the total nodes to agree on any of the state change.

2. Efficiency: PBFT is designed in such a way that is to be efficient, minimizing the number of messages exchanges which is required to reach consensus.



Applications:

PBFT is nowadays used in various blockchain platforms and distributed systems where performance and fault tolerance are very much critical. It is particularly effective in permissioned blockchain networks, where nodes are known and trusted to some extent. Examples of this can include enterprise blockchains, financial systems, and supply chain management.

From this all we can conclude and say that understanding the consensus mechanisms like Raft, BFT, and PBFT is very much essential for the trust worthiness and also the reliability of the blockchain technology. These typical algorithms ensures that blockchain networks can operate very much securely and efficiently, even in the presence of the faults and malicious actors.
As this great technology continues to get evolve across the globe, these mechanisms will play a very crucial or we can say vital role in its widespread adoption and its success.

Blockchain technology has revolutionized in such a way that we can't even think that the way it handles digital transactions, offering such high levels of security and transparency. However, scalability and transaction speed remain significant challenges. In the following report I will elaborate how Payment Channel Networks and Hashed Timeclock Contracts (HTLC) address these issues which in turn enhances the efficiency and security of blockchain networks.

Payment Channel Networks

Overview:

These networks are an innovative solution which are specially designed to improve the scalability of the blockchain networks. They enable multiple transactions to occur off-chain which in turn reduces the load on the main blockchain and which increases transaction speed.

How these Network Work:

- Opening a Channel:
    1. Two parties (e.g., Alice and Bob) let's say open a payment channel by creating a multi signature address on the blockchain. Then this address requires signatures from both parties which is to authorize transactions.
    2. They deposit a certain x amount of cryptocurrency into this address, which acts as collateral for their transactions.

- Off-Chain Transactions:
    1. Once the channel is open, Alice and Bob can conduct an unlimited number of transactions off-chain. Then these transactions are recorded locally by both parties but they are not immediately broadcast to the blockchain.
    2. Each transaction updates the balance of the channel which then reflects the new distribution of funds between Alice and Bob.

- Closing the Channel:
    1. When Alice and Bob decide to close the channel, they then broadcast the final balance to the blockchain. The blockchain then updates the ledger to reflect the final distribution of funds.
    2. This process ensures that only two on-chain transactions are required (opening and closing the channel) which in turn significantly reduces the load on the blockchain.

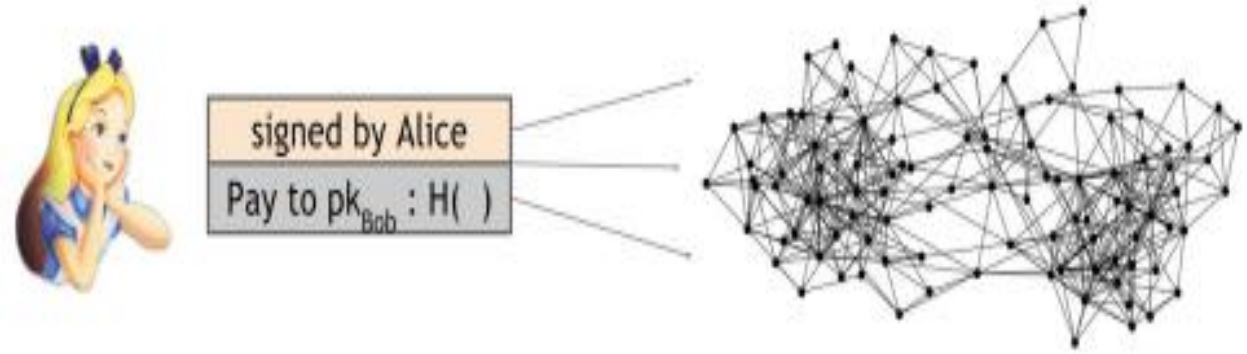


Figure 2.1 Broadcasting a transaction In order to pay Bob, Alice broadcasts the transaction to the entire Bitcoin peer-to-peer network.

Benefits of Payment Channel Networks

- Scalability: By conducting multiple transactions off-chain, Payment Channel Networks significantly increases the scalability of blockchain networks.
- Speed: Off-chain transactions are nearly instantaneous as they do not require confirmation from the entire network.
- Cost Efficiency: Reducing the number of on-chain transactions in turn lowers transaction fees which makes micro transactions feasible.

Hashed Timeclock Contracts (HTLC)

Overview:

Hashed Timeclock Contracts (HTLC) are a very crucial component of Payment Channel Networks, which provides a secure mechanism for conditional payments. HTLCs ensures that transactions are completed only if specific conditions are met which in turn enhances the security and reliability of off-chain transactions.

How HTLCs Work?

- Hashlock:
    1. A hashlock is a cryptographic condition which requires the recipient to provide a preimage which can be called a secret piece of data to claim the funds.
    2. The sender then generates a hash of the preimage and includes it in the HTLC. The recipient must reveal the preimage to unlock the funds.
- Timeclock:

1. A timeclock is a condition that sets a deadline for the transactions. Suppose if the recipient does not claim the funds within a specified timeline, then the funds are returned to the sender.
2. Timeclocks ensure that the funds are not locked indefinitely which provides a fallback mechanism for unclaimed transactions.

Example of HTLC in Action

- Scenario:
    a) Alice wants to send 1 Bitcoin to Carol through Bob, but unfortunately Alice and Carol do not have a direct payment channel.
    b) Alice then creates an HTLC with Bob, specifying that Bob can claim the 1 Bitcoin only if he provides the preimage within a certain timeline.
    c) Bob in turn creates an HTLC with Carol, using the same preimage condition.
    d) Carol provides the preimage to Bob, who then provides it to Alice which in turn completes the transaction.

Applications of HTLC

- Lightning Network:
  HTLCs are a fundamental component of the Lighting Network which enables secure multi hop transactions across interconnected payment channels.

- Cross-Chain Atomic Swaps:
  HTLCs facilitate atomic swaps between different cryptocurrencies which in turn allows users to exchange assets without relying on a centralized exchange.

- Escrow Services:
  HTLCs can be used in escrow services to ensure that the funds are released only when specific conditions and requirements are met.

Payment Channel Network and Hashed Timeclock Contracts (HTLC) are very much powerful tools which enhances the scalability, speed, and security of blockchain networks. By enabling off-chain transactions and conditional payments, these technologies address some of the most significant challenges facing blockchain today.
As this advanced blockchain technology continues to evolve, innovations like these all will play very vital and crucial role in its widespread adoption and success.

References

- Arvind Narayanan’s Bitcoin and Cryptocurrency Technologies
- Saravanan Vijayakumaran’s An Introduction to Bitcoin
- Satoshi Nakamoto’s white paper
- Prof. Vinay Ribeiro YouTube playlist.