



Islamic University of Technology (IUT)

Department of Computer Science and Engineering (CSE)

A Hybrid Blockchain Architecture for Cross-Platform Transactions

Authors

Jarin Tanzim Meem - 170042012

Khan Silvi Yasmin - 170042053

Rokeya Samanta Ruhee - 170042064

Supervisors

Dr. Md Moniruzzaman

Assistant Professor

Department of CSE

Faisal Hussain

Lecturer

Department of CSE

**A thesis submitted to the Department of CSE
in partial fulfillment of the requirements for the degree of**

B.Sc. in Software Engineering

Academic Year: 2020-21

April - 2022

Declaration of Authorship

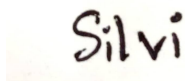
This is to certify that the work presented in this thesis titled as “**A Hybrid Blockchain Architecture for Cross-Platform Transactions**” is the outcome of the research and analysis carried out by Jarin Tanzim Meem, Khan Silvi Yasmin and Rokeya Samantha Ruhee under the supervision of Dr. Md Moniruzzaman, Assistantant Professor and Faisal Hussaain, Lecturer, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT), Dhaka, Bangladesh. It is also declared that neither of this thesis nor any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Authors:



Jarin Tanzim Meem

Student ID - 170042012



Khan Silvi Yasmin

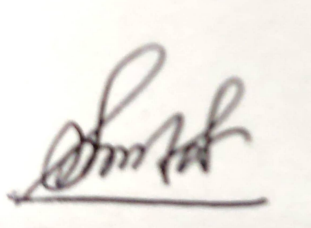
Student ID - 170042053

Rokeya

Rokeya Samantha Ruhee

Student ID - 170042064

Supervisors:




Dr. Md Moniruzzaman

Assistant Professor

Department of Computer Science and Engineering

Islamic University of Technology (IUT)



Faisal Hussain

Lecturer

Department of Computer Science and Engineering

Islamic University of Technology (IUT)

Acknowledgement

At the beginning, we want to express our heartfelt gratitude to Almighty Allah for his blessings to bestow upon us which made it possible to complete this thesis research successfully. Without the mercy of Allah, we wouldn't be where we are right now. All thanks and praises be to Allah.

We would like to express our grateful appreciation for **Dr. Md Moniruzzaman and Faisal Hussain**, Department of Computer Science & Engineering, IUT for being our adviser and mentor. Their motivation, suggestions and insights for this research have been invaluable. Without their support and proper guidance this research would never have been possible. Their valuable opinion, time and input provided throughout to the thesis work, from the very first phase of the thesis starting from topic selection, proposing hybrid architecture, modification to the analysis and finalization which helped us to do our thesis work in proper way.

Lastly, we are deeply grateful to our friends and family for their unconditional support. This work would have never been completed without the consistent support and encouragement from them throughout the program.

Abstract

Blockchain has emerged as one of the most significant technological breakthroughs in software design and technology over the past ten years. Existing blockchain architectures have two major limitations: first, the blockchain itself is vulnerable to attacks such as double spending, selfish mining and IoT smart devices, and distributed denial of service attacks, are also vulnerable once hackers successfully infiltrate blockchain systems; second, because IoT devices are heterogeneous and have resource limitations, implementation of current blockchain systems in the IoT scenario cannot reflect strong adaptability and meet IoT s requirements; and third, because IoT devices are heterogeneous and have resource constraints Our research focuses on the development of a hybrid architecture that facilitates the exchange of assets across multiple blockchains while also improving the privacy of the current blockchain by ensuring data integrity and data integrity fidelity.

Keywords

Blockchain, Consensus mechanism, Miners, Sidechain, Spacechain, Parallel mining, Scalability, Data security.

Contents

1	Introduction	4
2	Literature Review	8
2.1	Glimpse of traditional blockchain technology	10
2.1.1	Types of blockchain	10
2.1.2	Properties of Blockchain	11
2.1.3	Data Block	14
2.1.4	Digital Signature	15
2.1.5	Consensus Protocol	16
2.2	Proof of Work (PoW)	17
2.2.1	Applications	19
2.2.2	Advantages	20
2.2.3	Disadvantages	21
2.3	Proof of stake(PoS)	21
2.3.1	Applications	23
2.3.2	Advantages	23
2.3.3	Disadvantages	24
2.4	Direct Acyclic Graph (DAG)	24
2.5	Comparison among different consensus methods	25
2.6	Sidechain	26
2.6.1	Blockchain Locking	27
2.6.2	How does a two-way peg work?	28
2.7	Spacechain	31
3	Proposed Approach	33
3.1	Research Challenges	33
3.1.1	Lack of research support	33
3.1.2	No Universal Implementation	34
3.2	Methodology	35

4	Experimental Setup	37
4.1	Implementation	37
5	Conclusion	40

List of Figures

1	How blockchain technology works	9
2	Layers of blockchain technology	11
3	Single data block	14
4	Digital signature	15
5	Direct Acyclic Graph	25
6	Comparisons of consensus methods based on PoW, PoS, and DAG .	26
7	Crosschain/sidechain Transaction Call Graph	28
8	How a two-way-peg mechanism works	30
9	Data Structure for Spacechain	32
10	Hybrid Blockchain Architecture	35
11	Assets in the main chain	38
12	Assets in the side chain	39
13	Transaction Dashboard	39

1 Introduction

Blockchains have come a long way since its initial inception in 2008 as the foundation of the Bitcoin cryptocurrency. Blockchains, like the Internet, are intended to be structurally and politically decentralized. However, in recent years, blockchain-based systems have encountered roadblocks in the form of scalability, privacy, security, and other issues. To address these issues, the scientific and professional groups have proposed a number of novel approaches. And, here we are with a proposal of a hybrid architecture with spacechain that uses a Three-Dimensional Greedy Heaviest-Observed Sub-Tree (3D-GHOST) consensus mechanism to improve the security and network performance of traditional blockchains, along with the sidechain in which a secondary blockchain is connected to the main blockchain via a two-way peg that allows the main blockchain to add new functionalities.

As a transparent, reliable, and decentralized ledger on a peer-to-peer network, blockchain is most often linked with the virtual Bitcoin cryptocurrency, which was established in 2008 by Satoshi Nakamoto, and is recognized as the technology involved of the cryptocurrency. A transaction is the compact discs unit on the blockchain, while a Block is a collection of a particular number of transactions that have been grouped together. With all validated Blocks, a decentralized ledger is generated and maintained. The cryptographic hash code of a Blocks inside the distributed ledger is used to connect it to a previously authorized Blocks in the distributed ledger. In fact, this nascent technologies have already been extensively investigated for the development of a variety of applications that go beyond digital coins. In a distributed peer-to-peer network, every member has the ability to see and verify the behavior of other users in the system, and also create, verify, and approve a new transaction to be stored in the blockchain. This infrastructure ensures that blockchain operations are reliable and efficient, while also providing the advantages of tamper resistance and reducing single point of failure vulnerabilities (SPOFs).

Some of the core components of blockchain are as follows:

Node: Individual participant or computer operating within the blockchain.

Transaction: The core component at the most basic level of a blockchain system.

Block: A distributed data structure used to store a set of transactions across all network nodes.

Chain: A series of blocks arranged in a particular pattern.

Miners: Block verification is carried out by a specific set of nodes.

Consensus: A collection of rules and procedures for conducting blockchain operations.

Bitcoin (BTC) was the first and most widely used cryptocurrency, created by Satoshi Nakamoto in 2008. Mining (solving the PoW problem) earns BTCs, which may be transferred between Bitcoin accounts. Each transaction is saved in a block on the BC. The Bitcoin BC is duplicated among all connected nodes. Block leaders are chosen among nodes that successfully compute the PoW and construct, broadcast, and attach new blocks to the BC. Additional nodes will embrace the new block and include it in their own edition of the BC if all transactions included inside it are genuine. For receiving and transmitting bitcoin, digital wallets are used to ease transactions and maintain key pairs. The primary function of a Bitcoin wallet is to hold the private key that is needed to redeem bitcoins and to generate public addresses. BTCs themselves are not physically held in the wallet from a technical perspective. Instead, they are stored on the BC and may only be accessed by individuals who have the appropriate private keys. To "sign" transactions, private keys are also utilized.

Free Bitcoin and other cryptocurrencies are available for all major applications and operating systems, and are intended to meet a range of customer requirements. Various platforms provide a wide range of wallets to choose from. While they all have certain elements in common, each wallet has its own set of features. A shared wallet, also known as a multi-signature wallet or multisig wallet, is one of the most useful features. A multisig wallet has two or more keys, and a BTC transaction needs at least one of them to be authorized. Apart from conventional

transactions signed by a single owner of a private key, the funds must be signed by numerous persons before they can be transferred. It's safer since it limits BTC transactions. If one of the wallets is hacked, the hacker will be unable to spend BTC from the common wallet without the permission of the other wallet owners. Furthermore, by obtaining the transaction history of a particular wallet, it removes buying power from third-party hands in a community and allows participants to be tracked.

Ethereum is a network of autonomous computers that operate together and as one super computer, not merely a cryptocurrency network. It is flexible, enabling transactions to be conducted across either permissionless or permissioned networks. It is a B.c.e platform for implementing smart contracts, therefore it offers more than simply bitcoin transactions. The Ethereum Virtual Machine is the name of this platform (EVM). To deploy on the EVM, all smart contracts are compiled into appropriate bytecode. A smart contract may define any sort of rule or functionality since the Ethereum platform is Turing-complete. Externally owned accounts (EOA) and contract accounts are the two basic kinds of accounts in Ethereum (CA). CAs have related code (known as smart contracts) and data storage, but EOAs are governed.

Regardless of the fact that blockchain technology has a lot of untapped potential and could possibly replace a lot of the existing digital platforms, it still has significant technical limitations in terms of how well it performs, how scalable it is, and how much energy it uses.

Our thesis takes a dive into the shortcomings of the traditional blockchain proposing a new architecture with the hybridization of sidechain and spacechain. Sidechain enables cross platform transactions among different chains thus adds diversity to the existing system, whereas spacechain provides a 3D architecture that ensures data security in the newly proposed architecture.

Chapter 2 provides a literature review of basics of blockchain along with the two diverse architectures of the blockchain. It provides an overview of all the architectures starting from the consensus protocol followed to the drawbacks of each architecture. Section 3 of the paper shows a graphical representation of the hybrid architecture. Section 4 and section 5 discuss about the experimental setup and implementation of the proposed framework. The challenges those are faced throughout the entire process are mentioned in the section 6. Lastly, conclusion and future prospects of our work are mentioned in the section 7 and section 8 respectively.

2 Literature Review

Blockchain is the technology that underpins a variety of digital cryptocurrencies, including Bitcoin and Ethereum, among others. The term "blockchain" refers to a series of blocks that are used to access data using digital signatures in a distributed and decentralized network. It is the characteristics of blockchain, such as its decentralization, immutability, transparency, and auditability, that have made it a popular topic of conversation in today's globe. It assures transactions are more secure and tamper-proof than any centralized system available. Blockchain technology, in addition to bitcoin, may be used to a variety of industries, including risk management, healthcare facilities, financial social services, and so on. Blockchain technology has the potential to become the foundation of global record-keeping systems, despite the fact that it was only introduced ten years ago.

Satoshi Nakamoto, a person (or group of persons) who went by the moniker Satoshi Nakamoto, created the cryptocurrency bitcoin in 2008 to serve as a public transaction log for the cryptocurrency. In contrast to previous techniques, blockchain allows for the movement of digital assets from one person to another without the need for an intermediary. A decentralized ecosystem is enabled by the inclusion of numerous essential techniques, such as cryptographic hashes, digital signatures and distributed consensus procedures. It functions in this context.

The blockchain is accessible to all participants, but it is not governed by any network authority at this point. This idea is achieved by the imposition of stringent rules and the mutual consent of edge devices, which is referred to as the consensus method in computer science. As the name implies, this consensus mechanism refers to the process through which the decentralised ledger is synchronized across all nodes in the blockchain network.

Specifically, the superscript before the bullet points corresponds to the various processes shown in the Figure 1.

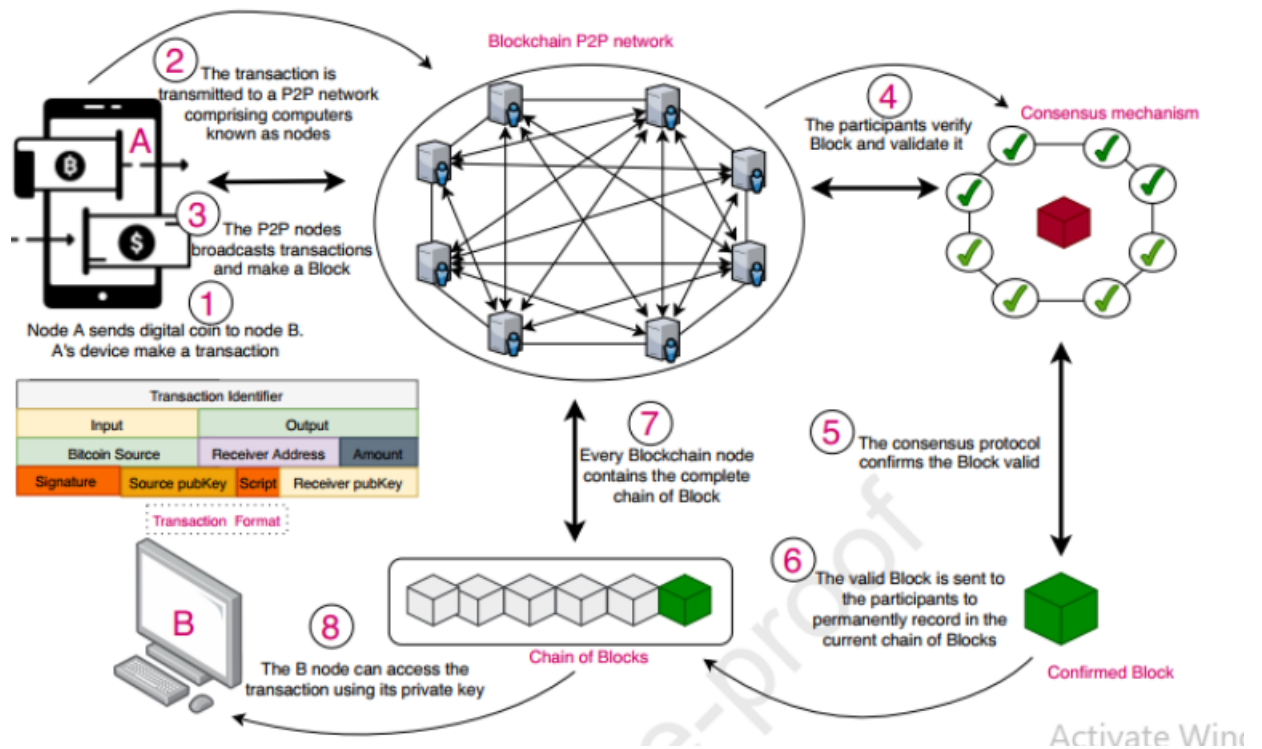


Figure 1: How blockchain technology works

- A participant A sends a certain quantity of digital currency to a participant B. A transaction is started by A's device. Participants may generally conduct transactions using their mobile devices, such as a smartphone, laptop, or low-processing PC. The transactions are authenticated using A's private key, and the contents of the transactions are encrypted using B's public key if required.
- The transaction is sent from A's device to a peer-to-peer network, which is made up of high-processing devices, which are referred to as nodes. This network is used to implement the Blockchain protocols.
- The transaction is replicated and disseminated across the network via the nodes of the Blockchain network. A specific amount of transactions were compressed into a Block by the nodes. Figure 1 illustrates the general structure of the proposed Block of code.
- Every participant adds the Block to the current chain of verified Blocks

when a specified hash code is generated by solving a rigorous mathematical challenge defined as Proof of Work, and only then does the Block become part of the chain. The computing expense and turn-around time for this procedure, which is known as the consensus method, are variable. In the next part, we will look at some of the most prevalent consensus procedures.

- The transaction as from approved Block may be accessed by B's device via the use of its private key.

2.1 Glimpse of traditional blockchain technology

Several research publications classified Blockchain technology into layers that might be further subdivided. The chapter discussed the five levels of a Blockchain technology, as well as an inquiry into the key qualities of Blockchain technology, which include, privacy, integrity, immutability. The structure of the BC, as represented in Figure 2, will be examined in further detail later

2.1.1 Types of blockchain

The material stored in transactions and the actions taken by members in the blockchain network are transparent and adjustable depending on how the blockchain is configured and expected to function. Based on this, we may classify the blockchain network into three categories.

1. **Public Blockchain:** Public blockchain is an open, permissionless network where anybody can join and see, write, and read data in a block, contributing this to blockchain. The information saved here are public. These blockchains are fully decentralized and devoid of authority.
2. **Private Blockchain:** In a private blockchain (also known as a consortium blockchain), only authenticated parties may enter. It is primarily used for private companies. A private blockchain is a distributed ledger that acts as a personal, centralised database based on cryptographic principles.

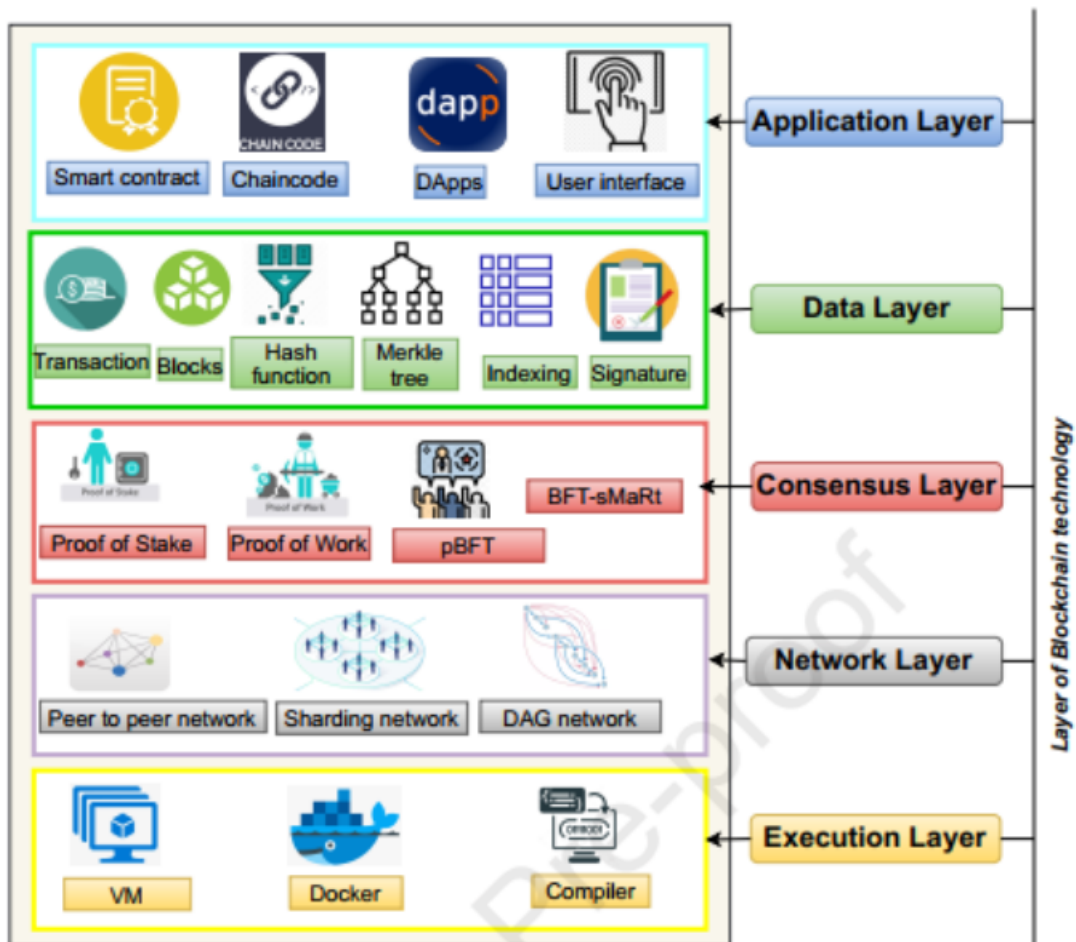


Figure 2: Layers of blockchain technology

3. **Permissioned Blockchain:** In between the blockchain networks(private and public), the permissioned blockchain allows for a lot of customisation choices, such as enabling anybody to join after proper identification verification. These network users are then granted specific rights to execute certain tasks just on a permissioned system.

2.1.2 Properties of Blockchain

Decentralization: With some of its decentralized character, blockchain is a viable solution for successfully tackling bottleneck and one-point failure concerns in the IoT network by removing the requirement for a trusted third party. The functionality of the BCIoT network is unaffected by the failure of a Blockchain

node. The data on a blockchain is often kept in numerous nodes on a peer-to-peer network, and the technology is extremely resistant to technical failures and malevolent assaults. Even if any of the nodes fall down, the network's availability or security cannot be jeopardized. Traditional databases, on the other hand, depend solely on a single or maybe more servers and are more vulnerable to cyber-attacks and technical failure. Moreover, Blockchain's peer-to-peer design gives all network participants equitable validation rights to evaluate the accuracy of IoT data and ensure immutability.

Enhanced Security: In numerous ways, blockchain is more dependable and secure than conventional record-keeping systems. Prior to being recorded by the network members, transactions must be decided upon. When a transaction is approved, it is encrypted and connected to the preceding transaction. Furthermore, instead of storing information about a single server, information is distributed throughout a network of computers, preventing hackers from gaining access to transaction data. The use of PKI (private/public key infrastructure) is the most important aspect of security in Blockchains. Blockchain systems employ asymmetric cryptography to safeguard transactions between members. These keys are produced using random numbers and strings, making it impossible to calculate the private key from the public key. This prevents future assaults on Blockchain documents, minimizes data leakage issues, and improves the privacy of such a Blockchain network.

Improved Traceability: In other systems, goods traded in a complex supply chain can't be controlled back to their origin point as quickly as they can in Blockchain. The use of past transaction data in Blockchain may aid in the verification of asset validity and the avoidance of fraudulent operations. Similarly, the Blockchain may be used to store and monitor a patient's prior data that are critical to their treatment.

Greater Transparency: Because all network users have access to the transaction records in Blockchain, they are more transparent. In contrast to individual copies in a traditional network, blockchain is a decentralized network in which all

members share the same documents. The shared document may only be changed by agreement, which implies that everyone must agree. To put it another way, the identical copy of Blockchain data is distributed throughout a wide network for public validation. As a result, all Blockchain participants have equal access to the network, allowing them to verify, trace and connect, transaction activity. To change a solitary transaction history, all future records would have to be changed as well, necessitating network-wide collusion. As a result, information on a Blockchain network is more accurate, reliable, and transparent than data on a traditional network. By decreasing the risk of illegal data changes, such openness also helps to safeguard the credibility of Blockchain-based systems.

Data Privacy: Storage solutions on the Blockchain are particularly effective in protecting IoT data from change, thanks to Blockchain's immutable and trustworthy features. By using immutable hash chains and digital signatures, blockchain stores information transactions and events in a way that ensures their integrity and validity. Essentially, the Blockchain enables users to keep track of transactions over a network while maintaining computer and data rights.

Reduced Cost: Many firms have cost-cutting as one of their primary goals. Blockchain eliminates the need for third parties or middlemen, as well as the need of infrastructure setup for public BC, lowering the cost of doing business. Because each participant having access to a particular, unchanging ledger, blockchain participants would not need to check a lot of documentation to conduct a transaction. While BC can avoid the costs of third-party services, this will need a significant investment in dedicated infrastructure for consortium and private use. For transaction processing, public BC and blockchain still charge a fee.

Immutability: The Blockchain's transaction data is irreversible in the long run. Technically, after being verified by the Blockchain system, transactions are timestamped and then put into a Block that is cryptographically secured using a hashing mechanism. Blocks are linked together using hash methods, which create a sequential chain. The hash value of information from the preceding Block is always stored in one field of a new Block's header, making the chain highly im-

mutable. After it has been confirmed and stored in the Blockchain, its Block information can no longer be updated, edited, or erased. Any efforts to change or modify transactions will be thwarted by the cryptographic connection between succeeding Blocks. Even though a transaction changes, it will be obvious.

2.1.3 Data Block

Blockchain is basically a chain of blocks, which is a function adds that begins with the creation of the first block, known as the genesis block, and progresses with each subsequent verified Block that is attached to that chain. So every Block consists of numerous operations and contains a field carrying the hashtag of the Block directly before it, which serves to bind the transactions together. This means that any change or alteration to any block's contents is not possible and that all verified blocks in the chain could be tracked back using cryptographic hash codes.

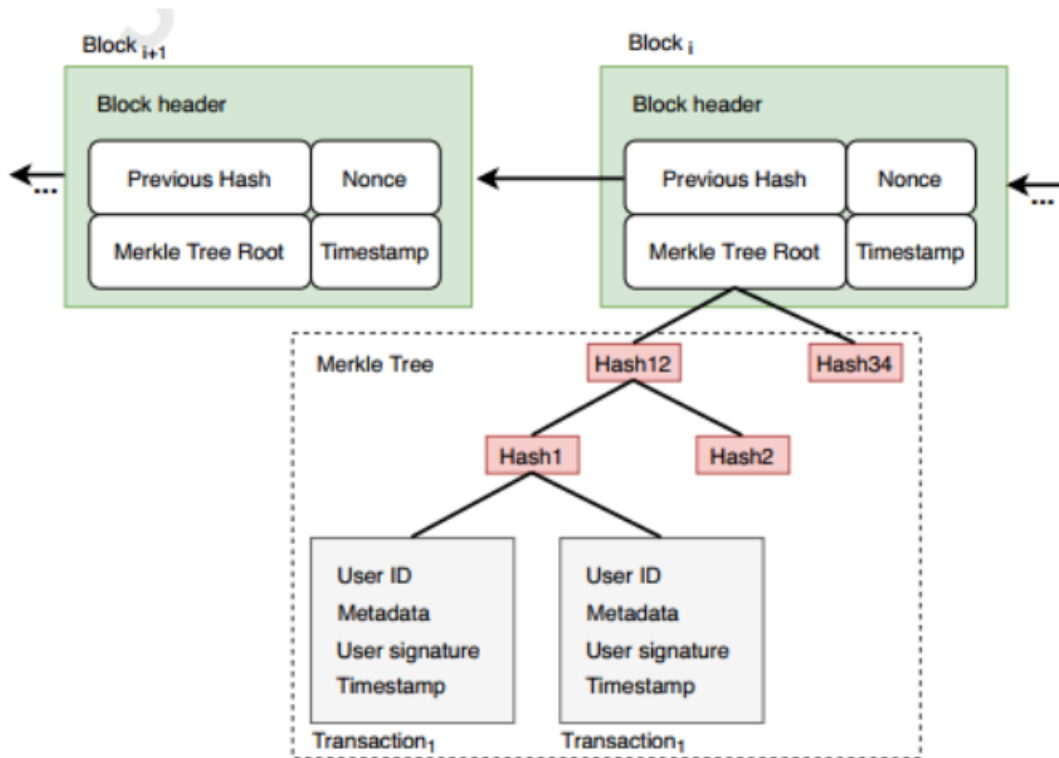


Figure 3: Single data block

Here, Figure 3 shows that a data block is split into two parts: header (or introduction) and transaction record where the previous hash values along with the nonce and timestamps are stored.

2.1.4 Digital Signature

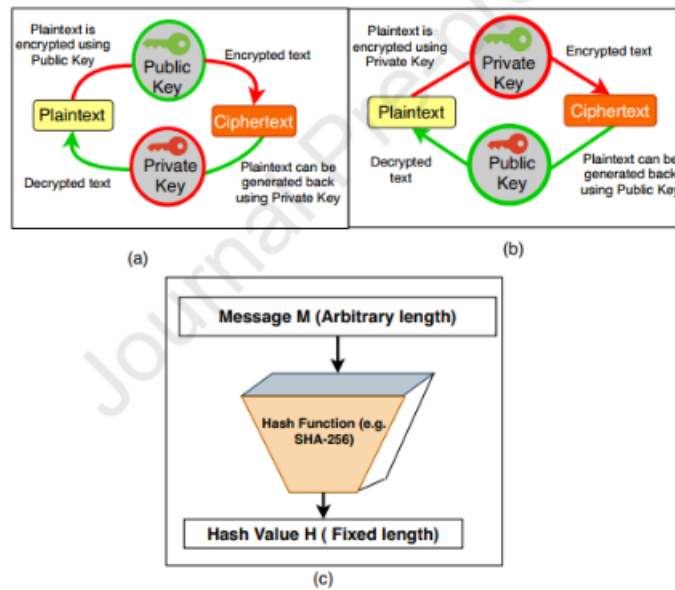


figure 04

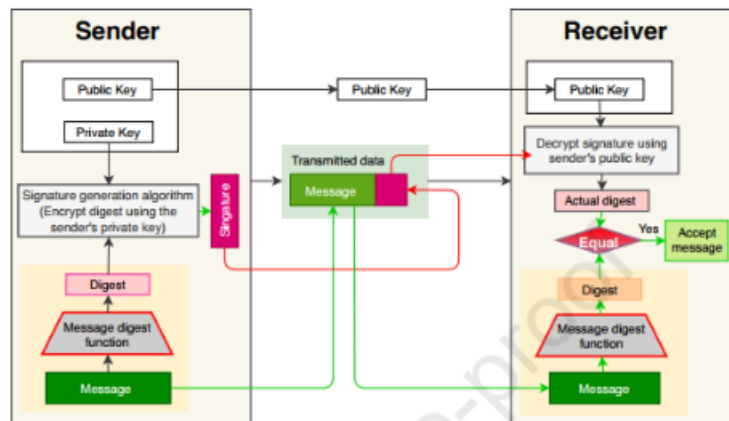


Figure 4: Digital signature

A digital signature (DS) is a cryptographic method for authenticating and ensuring the integrity of digital material. A public-key cryptography (PKI) mechanism is used by DS. The public and private keys in public-key cryptography (PKI) are

coupled together but asymmetrically. The publicly key in the pair is normally shared with authorised entities, while the private key is kept secret by the owner of the key pair. Either of the keys may be used to encrypt a message; the reverse key from the pair that isn't used to encrypt the message is used to decode it. Figure 4 (a) shows how a signal is encrypted using a public key and then decrypted using a private key. Figure 4 (b) demonstrates that the message's ciphertext is created using the private key, while the plaintext is generated by using public key.

In BC technologies like Bitcoin and Ethereum, a user's public key is referred to that as his address, similar to a bank account. Anyone may transmit digital currencies to just a user's address (Public Key), but only the user has access to the currencies using the PKI's private key. In the Bitcoin BC, Figure 7 shows how to sign a message with private key and authenticate it with the public key.

2.1.5 Consensus Protocol

In a blockchain network, nodes either mine new blocks or sign them digitally. New transactions and information must be saved in blocks and uploaded to the blockchain.

However, to produce a block on a blockchain, the procedures are as follows:

1. A transaction needs to occur, i.e., information must always be transmitted.
2. These transactions must be validated.

The functionality of this network differs based on the application. The fundamental methods required in introducing a new block to the blockchain have already been described and analyzed below, using the bitcoin cryptocurrency as an example. A transaction among 2 blockchain users being added to an unconfirmed transaction pool. All of the unconfirmed transactions then are telecasted to all of the network participants within the blockchain network to be validated and checked against the creators' codes. However, on the bitcoin blockchain, only mining nodes execute transaction verification. The miners then put the validated

transactions into a block and hash it. The SHA-256 strong cryptographic technique converts the block contents into a 256-bit integer. The bitcoin producers hash the block's transaction information with the preceding block's hash to create a 256-bit integer that uniquely defines that block (as depicted in Figure 2). Furthermore, a bitcoin miner cannot simply produce random hash for something like the block and upload that one to blockchain network; the hash needs to be match with the particular parameters. Every blockchain network must decide whichever node will add the very next block to the blockchain. This decision is made by consensus.

To add a new block to a bitcoin network, a miner must solve a hard mathematical problem. In a math problem, miners must provide a hash with a. Blockchain is a decentralized system where each node acts as both a host and a server and has to distribute information among other nodes to obtain agreement. No permissions are necessary to join or contribute to a public blockchain network, therefore anybody may be a node and stay anonymous. So a node may edit transactions and re-block them. +us, the blockchain may fork. A chain fork may include solely legitimate transactions, whereas another may have altered transactions. To keep the network decentralized, public blockchain protocols must deal with this problem separately. A single person cannot pronounce a transaction legitimate or invalid. Various consensus methods are employed to prevent forks and to temper blocks so that everyone agrees on the truth. Distinct blockchains have different use cases. Thus, the consensus methods used by blockchain must be acceptable for the application.

In the following sections, we will examine several consensus mechanisms and their blockchain applications.

2.2 Proof of Work (PoW)

POW is a consensus technique used in the blockchain networks such as bitcoin and Ethereum. It defines a system that makes the service requester undertake difficult labor in order to avoid malicious use of computer resources, denial-of-service attacks, as well as other system abuses like spamming. The PoW consensus process

in a blockchain network needs network processing operators to verify that their activity qualifies them to add new contracts including blocks to the blockchain. In Proof of Work, the nodes that will contribute the next block to the blockchain are chosen based on their computational capacity.

As previously stated, miners on the blockchain network produce blocks by computing the answer to a complicated mathematical challenge, and the only method to solve this issue is by expensive guessing, i.e., Proof of Work. Because miners may easily join and exit the network, the difficulty of this challenge is modified per 2,016 blocks to guarantee a 10-minute delay between blocks mined by the same miner. The system automatically adjusts the target hash depending on the amount of miners. Thus, in a distributed consensus based on Proof of Work, miners use a lot of energy and spend so much money on hardware and power.

Two mining nodes may create blocks at the very same moment. This happens because the blockchain network's block acceptance procedure is not immediate. Because of this, another miner may locate the proper hash for such a block at around the same height on the blockchain, resulting in a short-term split. In such a case, nodes must choose between the two newly recognized blocks within two forks. Because it has more Proof - Of - work (POW) therefore more confirmations, the lengthier of both the 2 forks is considered genuine by the blockchain system. Orphan blocks are blocks found on the opposite fork.

A hacker with enough processing power to control the network may also cause a fork. tries to reverse certain transactions or double invest a coin. PoW is an effective way to deal with double-spending. Assume two transactions are executed to spend every single coin, both of which enter the unconfirmed pool. Assume the miners verified the first transaction block before the second transaction block. In this instance, the second transaction is rejected by the miners as invalid and is removed from the network. But what if the miners accept both transactions simultaneously? In this situation, the blockchain gets forked by adding blocks containing both transactions. To get enough conformations on the fraudulent fork,

the adversary would go reverse and back transactions in all of the blocks generated after the fraudulent block, which would take a lot of time and effort. Because every block in blockchain includes a reference to the previous block, if miners try to modify the blockchain or manipulate the mining process, they risk damaging bitcoin's credibility. Changes to the Proof - Of - work consensus-based blockchain are difficult to implement since they need reminding of all the subsequent blocks. PoW also makes it difficult to monopolize the network's computational power by a person or group of users since generating hash needs costly gear and energy.

2.2.1 Applications

The Proof of Work algorithm is commonly used in cryptocurrencies and other blockchain systems. We've previously seen the use of and PoW in bitcoin above. A few more PoW-based blockchain cryptocurrencies have been mentioned below:

- **Litecoin:** Litecoin ,that is a cryptocurrency that allows for quick, low-cost global transactions. Litecoin was created to be a better alternative to bitcoin. Despite the fact that both Litecoin and bitcoin employ the Proof of Work idea for mining, their algorithms are fundamentally different. Scrypt, a memory-intensive algorithm, is used by Litecoin. The major goal of employing this technique was to guarantee that anybody could participate in network mining by eliminating the need for high processing resources like those used in bitcoin as well as replacing them with memory-intensive CPUs.

Litecoin also decreases the time it takes to complete a new transaction from 10 minutes to 2.5 minutes, allowing it to handle larger transaction volumes than bitcoin. However, since Litecoin has a limited quantity, only 84 ,000,000 of them will ever be in circulation.

Ethereum: The mining process for the Ethereum cryptocurrency is almost identical to that of bitcoin. However, the Ethereum frontier network's PoW algorithm, termed Ethash, is kind of different from bitcoin's and was built particularly for Ethereum. The primary motivation for creating a new Proof

of Work algorithm instead of adopting an existing one was to solve the issue of mining centralization induced by hardware resource dependence and to construct a mining systems that could be readily implemented on ordinary hardware.

Technically, the goal with Ethash was to create a network that was resilient to application-specific integrated circuits (ASICs), which are specialized chips that outperform standard computer hardware by many magnitudes in hashing performance and are currently the only beneficial thing to mine bitcoin blocks . Ethash does this by giving a PoW algorithm whereby the commodity hardware used by miners is already well tuned, thus adding an ASIC to it will provide very little benefit over merely utilizing the most recent commodity hardware. Memory hardness is one of the features that such hardware is supposed to attain. Memory hardness refers to a computer system's ability to move information around like that in memory instead of how quickly and efficiently it performs computation processes. Mining hardware is often provided by graphics processing units (GPUs). Performance. PoW consensus offers a number of benefits and drawbacks that have been described in next part.

2.2.2 Advantages

1. **Most battle-tested:** becoming the oldest and used in the initial cryptocurrency, its consensus mechanism has faced several security and stability difficulties. Other processes may be preferable in principle, but they have a drawback in that they just haven't been in active use long enough to develop it.
2. **Quickly achieves consensus:** A crucial feature of PoW is that it is difficult to discover a solution towards the hard arithmetic issue but relatively simple to verify. As a result, when one hash is established, it can be readily validated, and a consensus may be obtained rapidly.

3. **Discourage spammers:** Because PoW demands a significant amount of effort for each procedure, such as emailing, most spammers will lack the computing capacity to send a large number of unwanted emails. Even though a spammer has sufficient computer capability, the expense of doing so is likely to outweigh the profit generated by spamming.

2.2.3 Disadvantages

1. **Electricity reliance and waste:** PoW necessitates a lot of computational power, and a lot of electricity is squandered in the procedure like all mining nodes try to solve the complicated issue, yet only one can mine a block. Furthermore, access to energy is not universal across the country, enabling miners in areas with cheaper electricity to dominate the business.
2. **Centralization:** The Proof of Work consensus is centralized because of its reliance on the power and mining gear. This mechanism is moving in the direction of centralization. The hash rate of the PoW network is largely focused on hydroelectric power, which is cheap and abundant in these places, and mining equipment is available from local providers. This puts the PoW network including all of its data on it at danger.
3. **Less secured for small networks:** Only if there are a large number of participants in a PoW-based blockchain, then only it can guarantee appropriate security.

The blockchain network has a huge number of miners fighting to mine the next block. However, if the network is tiny, there is a greater chance that a hacker will achieve a simple majority of the network's processing power and mine a fake block.

2.3 Proof of stake(PoS)

Proof of Stake (PoS) is a more energy-efficient alternative to Proof of Work (PoW). While the goal of both is the same, i.e. to attain agreement inside the blockchain,

the methods for doing so are vastly different. To choose the validator of the next block from the existing nodes, the Proof of Stake consensus algorithm employs a pseudorandom selection process. staking and Randomization age along the node's wealth are among the things that go into the procedure. Blocks are referred to as "forged" rather than "mined" in the Proof of Stake consensus procedure. While in PoW, the block that solves the most challenging challenge first mines the next block and is rewarded, in PoS, the individual node that makes the next block is chosen based on how much they have "staked" in relation to other rivals' nodes. The stake is often determined by the quantity of coins held by the network node for the blockchain it is trying to mine.

The transaction rate is generally the incentive in these systems, and users who wish to be part of the forging process must lock their stake (a fixed quantity of coins) in a system. The likelihood of a node being chosen to create the next block as even the validator is proportional to the amount of its stake, so that the node's chances of winning the next block rise as its stake grows. However, since the network would be controlled by the one node with the highest stake, those selection processes are skewed. More ways are introduced to the selection procedure to address this problem, two of which are "randomized block selection" and "coin age selection."

- The next forger is chosen using a combination of stake hash value, and the node with the highest stake and lowest hash value is chosen using the randomized block selection process.
- The coin age selection method selects the next forger depending on how long it has carried the stake and the amount of the stake. It is determined by multiplying the quantity of stacked coins by the number of days staked.

After the node has forged a block, its coin age is reset to zero. To prevent huge stake nodes from dominating the blockchain, a node must wait a certain amount of time after generating a block before attempting to generate another.

2.3.1 Applications

Two of the most significant Proof of Stake systems are mentioned below:

1. **Peercoin**, introduced in 2012 and officially based on bitcoin technology, has been the first hybrids blockchain that uses PoS for network security and PoW for coin distribution. With increasing difficulty and decreasing return, mining begins to move towards centralization.
2. **ETH 2.0 Ethereum**, the second-largest blockchain platform after bitcoin, plans to switch from Proof of Work (PoW) to Proof of Stake (PoS) because PoS is more secure and energy-efficient than PoW. In order to operate a validator node on the network, validators must stake 32 ether coins and deposit them to the Ethereum 2.0 deposit contract.

2.3.2 Advantages

1. **Lower power consumption:** Because the PoS system eliminates the need for users to solve sophisticated energy-intensive algorithms, it lowers electricity usage by 99 percent, as stated in 1. Furthermore, network validators do not have to worry about finding a cheap power source since they may use the energy source from anywhere, broadening the validation area.
2. **Makes staking simple:** Proof of Stake fosters widespread involvement and decreases network member stress, making staking simple. The need for a mining rig is avoided since it does not create undue expectations on stackers for hardware. The rate of participation rises due to lesser demand and less pressure on stackers. As a consequence, the network becomes much more decentralized and adaptable.
3. **Environmentally friendly:** Because the PoS mechanism's design is basic, the amount of resources required to strain the environment is minimal. Furthermore, mining farms are not necessary for the network to operate and issue new currencies, making it more ecologically friendly.

4. **Decentralization:** Proof of Stake partially overcomes the centralization issue of Proof of Work by using very little power and requiring very little hardware.

Furthermore, as a result of the aforementioned factors, it becomes more accessible and ecologically beneficial.

2.3.3 Disadvantages

1. In the PoS system, people with a high number of coins may affect the network.
2. It has yet to be established in terms of the long viability, given none of the top three cryptocurrencies presently employ PoS.
3. A cold wallet that cannot be picked as the next block maker in the PoS method since it needs users to synchronize their wallets to establish ownership.

2.4 Direct Acyclic Graph (DAG)

The DAG architecture and its consensus mechanism are presented as a solution to the inadequacies of existing consensus mechanisms in the Internet of Things. Users may put their nodes into the blockchain anywhere at a time using a DAG-based consensus method, as long as they have completed the transactions that came before them in the DAG. Many branches would've been formed at the same time in this manner, which is known as forking. Due to the possibility of "double-spending," this phenomenon is often seen as a concern in many conventional consensus procedures. Specifically, Although the DAG-based consensus method is designed to solve the double-spending issue, it also allows any new arriving transactional access to the blockchain system in a forking topology, which is a significant improvement over the previous consensus process. Figure 5 shows how voting is cast by different users in each round.

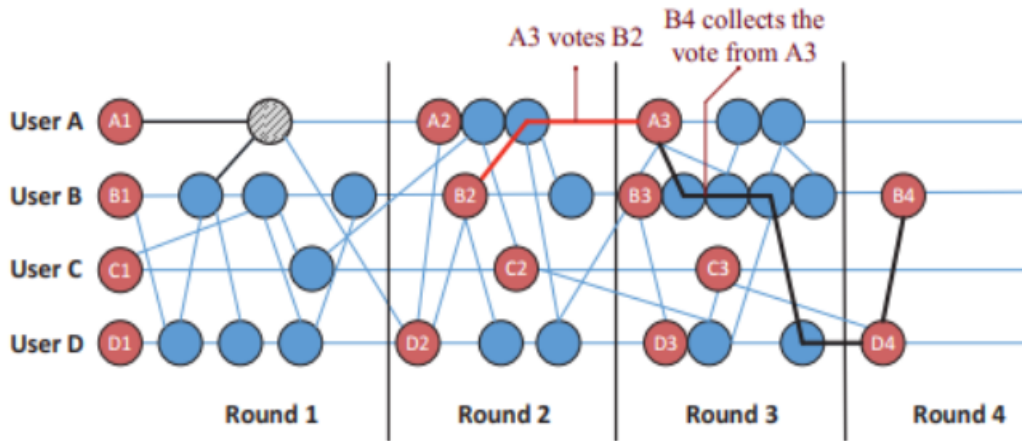


Figure 5: Direct Acyclic Graph

As a consequence, the verification rate and the total number of confirmations would no longer be restricted. Furthermore, since the data contained in DAG is safeguarded by enormous forking blocks, the resource usage for a specific user to generate a new block may be very minimal. As a result, the professional miner is no longer necessary, and minimal or no trading fees are conceivable, which is key to the IoT ecosystem's success.

2.5 Comparison among different consensus methods

In order to show the benefits and drawbacks of DAG-based consensus for the Internet of Things, we compare their efficiency with two standard consensus mechanisms in Figure 6. It is clear from these studies that DAG-based consensus algorithms are better appropriate for large-scale IoT deployments than both PoW and PoS. In particular, DAG-based consensus has the lowest transaction price and resource utilization, and it may achieve a much greater transaction throughput than other types of consensus. Despite this, several drawbacks in DAG-based consensus techniques still exist, such as worries about centralization in the Tangle consensus mechanism. It would have an impact on the confirmation latency of the DAG consensus.

	Bitcoin [1]	Nxt [11]	Tangle [12]	Hashgraph [13]
Byzantine fault tolerance	< 51% of all computing resources	< 1/3 of total assets	< 51% of all computing resources using MCMC tips selection	Dishonest participants < 1/3
Transaction fee	0.0001 BTC	1 Nxt	Zero	Zero
Resource requirements	Enormous computing power	Coinage	Low computing power	Low computing power and bandwidth
Throughput	7 TPS	4 TPS	No technical up bound	2.5 x 10 ⁵ TPS
Confirmation delay	60 mins	10 mins	Depends on transaction arrival rate	Subject to communication frequency
Finality	Six cumulative blocks at least	Ten cumulative blocks at least	Cumulative weight reaches confirmation threshold	Seen by all the famous witnesses in a later round
Unique features	<ul style="list-style-type: none"> • Competition for mining • PoW 	<ul style="list-style-type: none"> • The miner of the next block is predictable • PoS 	<ul style="list-style-type: none"> • Offline transactions • Quantum Immune • DAG 	<ul style="list-style-type: none"> • Proof of asynchronous Byzantine fault tolerance • Gossip to gossip and virtual voting • DAG
Major drawback	High resource consumption (hash complexity)	Centralization concern (coinage)	<ul style="list-style-type: none"> • Large confirmation delay in low trading traffic load • Centralization concern (when coordinator is involved) 	Large confirmation delay caused by low communication frequency (gossip protocol)

Figure 6: Comparisons of consensus methods based on PoW, PoS, and DAG

2.6 Sidechain

A sidechain is a distinct Blockchain that operates concurrently with the main chain and is connected to it by a two-way peg. This allows the sidechain to interact with the main chain in both directions. All successive chains are referred to as side chains, whereas the parent chain is known as the original or main chain. Figure 9 depicts a bidirectional transfer mechanism that allows users to move digital assets from the main Blockchain to the side chain and vice versa. A participant on the main chain must transmit a specific amount of digital currency to the outer address of a Federations system. The Federation distributes equal cash on the sidechain when a defined length of time has elapsed after the transaction has been confirmed. The user can access and spend digital currency on the sidechain. When moving from a sidechain to the main chain, the reverse occurs. A federation is an intermediary that determines when digital money between the main chain and

subsidiary chains are locked and unlocked. Federation provides an additional layer between the main chain and the sidechain. Developers of the sidechain may select members of the federation. A sidechain with its own protocols and implementation can operate separately from the main chain and is completely isolated from it. As a result, if the main chain is hacked or penetrated, the sidechain will continue to function correctly; cyberattacks on the sidechain will not affect the functionality of the main chain.

Here, it shows the communication flow diagram between the Mainchain, Federation, and Sidechain.

1. A user transmits Five main coins to the federation, which locks the currency for sidechain transfer.
2. After conducting verification, the federation's entities sign the transaction. The Five main coins are sent to a user supplying a sidechain address if a sufficient number of entities authorize the transaction.
3. The user may play the rock, scissor, paper game with some other user with Five sidecoins and get Ten sidecoins if he wins; alternatively, if the game is a draw, each user receives Five sidecoins.

2.6.1 Blockchain Locking

The above-mentioned Cross-Shard Contract Yanking process may be thought of as a mechanism for securing an agreement. As previously stated, this approach is not suitable for consortium chains since the shared data secrecy is not maintained. Max C, an Ethereum researcher, presents a two-phase commit locking technique. Locks must be committed to shards where atomically modified data is stored, and Merkle Proofs demonstrating the state modification, which includes the lock, must be sent to the shard that will perform the transaction on the information. To verify the Merkle Proofs, this system needs to know the block hash of the shard on which the information is stored, as well as the shard on which the transaction will be executed.

In the proposed approach, block hashes from one sidechain will not be viewable on some other sidechains. There's also the possibility that releasing a sidechain's block hashes may expose data about the sidechain, jeopardizing the anonymity of the other sidechain. In Cross-Shard Locking, a strategy for resolving deadlocks has been presented . Such an approach necessitates the use of a start block number for all crossshard transactions. When there is lock contention, the cross-shard transaction with both the earlier start block number wins. When two competing operations have the same start block number, the approach fails to address the situation.

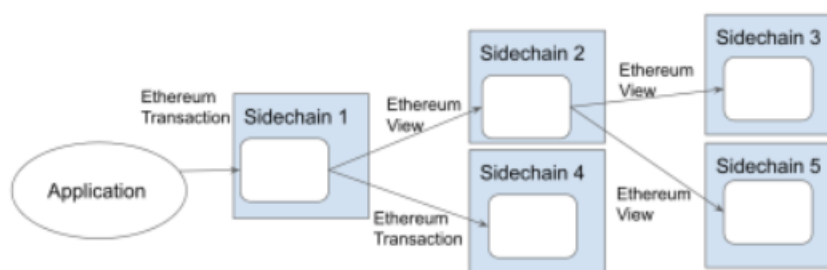


Figure 7: Crosschain/sidechain Transaction Call Graph

Figure 7 represents an application that supports ethereum transaction and the transactions take place in multiple sidechains which are managed by the call graph.

2.6.2 How does a two-way peg work?

In this part, we'll go through the foundations and design considerations for constructing a two-way peg supported sidechain using a simple example. Assume a two-way peg connects a sidechain to a permissionless and public core blockchain.

Due to the lack of a Turing complete Virtual Machine, the principal blockchain: 1) runs a cryptocurrency called MainCoin; and 2) cannot perform non-trivial smart contracts.

The sidechain: 1) has its own cryptocurrency, SideCoin; 2) can execute non-trivial smart contracts; and 3) has a much greater transaction rate than mainchain.

In a multi-blockchain setting, the major blockchain is referred to as the parent blockchain (or mainchain), while the sidechain connecting to it is referred to as the secondary chain. A two-way peg, in our example, enables MainCoins to be transferred from mainchain towards the sidechain and back at a set rate of 1 MainCoin equals 1 SideCoin. If an user wanted to transfer 5 MainCoins from the mainchain towards the sidechain in order to play a rock, paper, and scissors game with some other sample user based on a smart contract (where the winner gets all and a draw outcomes in no swap of coins) implemented on the sidechain, the system could operate in the following abstract manner:

1. The user transmits 5 MainCoins to a particular address (known as lockbox), which locks the coins and can only be opened after money on the sidechain have been locked and later transferred to the mainchain.
2. On the sidechain, 5 SideCoins are produced after the money are locked on the mainchain.
3. The user may now use these SideCoins to play rock, paper, scissors with another randomized user who is prepared to wage the same number of SideCoins.
4. Based on the game's conclusion, either 10 SideCoins are awarded to the champion or Five SideCoins are returned to their owner (if it is a draw).
5. After the SideCoins are destroyed on the sidechain, the user(s) can transfer there own funds back to a mainchain, which basically means that the SideCoins would be locked/destroyed on the sidechain, as well as a comparable number of MainCoins would be unlocked on the mainchain from lock-box (in step 1) just after SideCoins are destroyed on the sidechain.

The aforementioned processes are presented in Figure 8 and may vary depending on how a two-way peg for the sidechain is implemented. This architecture preserves the overall amount of MainCoins in the mainchain ecosystem while introducing additional features, such as non-trivial smart contract execution and

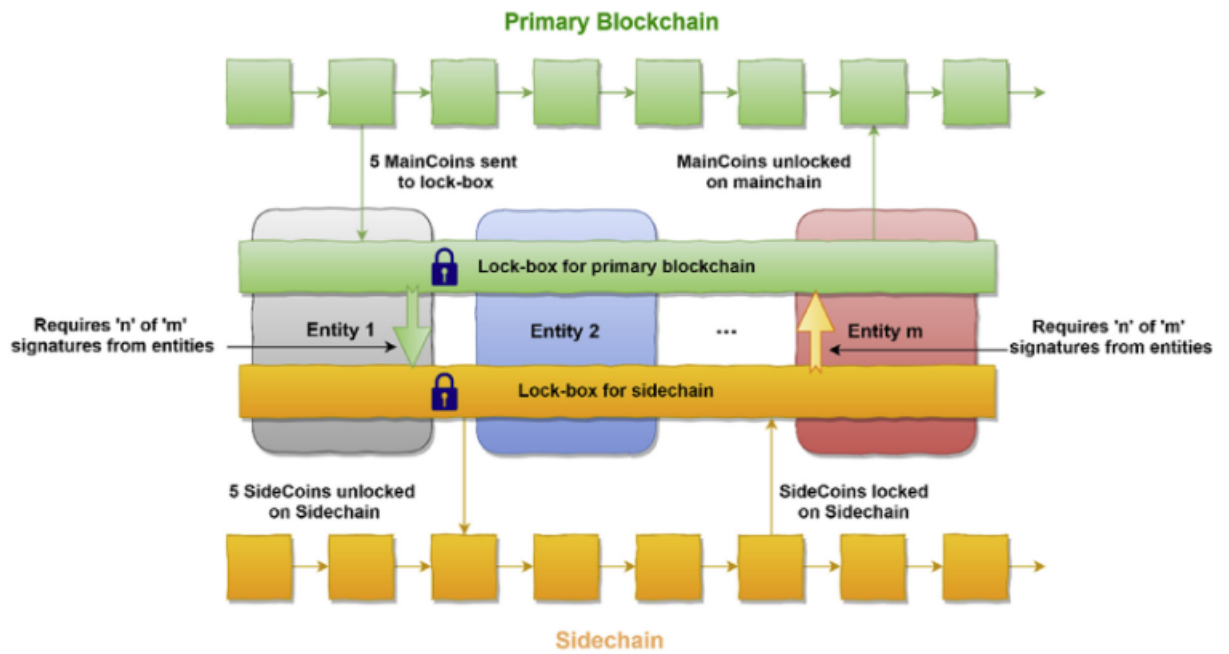


Figure 8: How a two-way-peg mechanism works

quicker transaction speeds. Furthermore, implementing these additional capabilities via sidechains does not need any fundamental changes to the mainchain's core functionality or consensus mechanism.

2.7 Spacechain

Spacechain is a three-dimensional blockchain architecture for IOT. They go through all the design ideas in terms of ledger architecture, data structures, and parallel operations in particular. From the standpoint of ledger design, previous blockchains (such as Bitcoin and Ethereum) used two-dimensional architectures, with the ledger consisting of just one kind of block. The new blocks are linked to numerous (in Ethereum) parent blocks or one (in Bitcoin) producing a linear or pictorial ledger. We introduce the notion of a three-dimensional ledger made of two types of blocks, macroblock and microblock, to improve scalability. We start by employing macroblocks to build a directed acyclic graph (DAG) foundation. The third dimension is formed by connecting multiple microblocks to the DAG base. The simultaneous operations are well accommodated with such a three-dimensional ledger design, which increases network scalability and eliminates the significant heterogeneity in IoT.

The DAG foundation comprises the following essential pieces, as depicted below:

- **Vertex:** Macroblocks are termed vertices, and Genesis is the origin of these vertices. Furthermore, the tip denotes the vertex of whom in-degree is 0
- **Edge:** An edge is a line that connects two vertices. Miners will use the Ref hash to link to prior vertices while creating a pending macroblock, where Ref hash belongs to a list for keeping the hash values of earlier macroblocks.
- **Acknowledgement edge (ackedge):** The acknowledgement edge (ackedge) is the physical manifestation of the voting connection. When one vertex links to another through an ack-edge, the other vertex recognizes the legitimacy of the connection. The ack-edge is the very first element in Ref hash.

The reference edge (ref-edge) is a representation of a temporal connection. The newly generated macroblock will link with the remaining tips through refedge and further populate the Ref hash after determining the ack-edge.

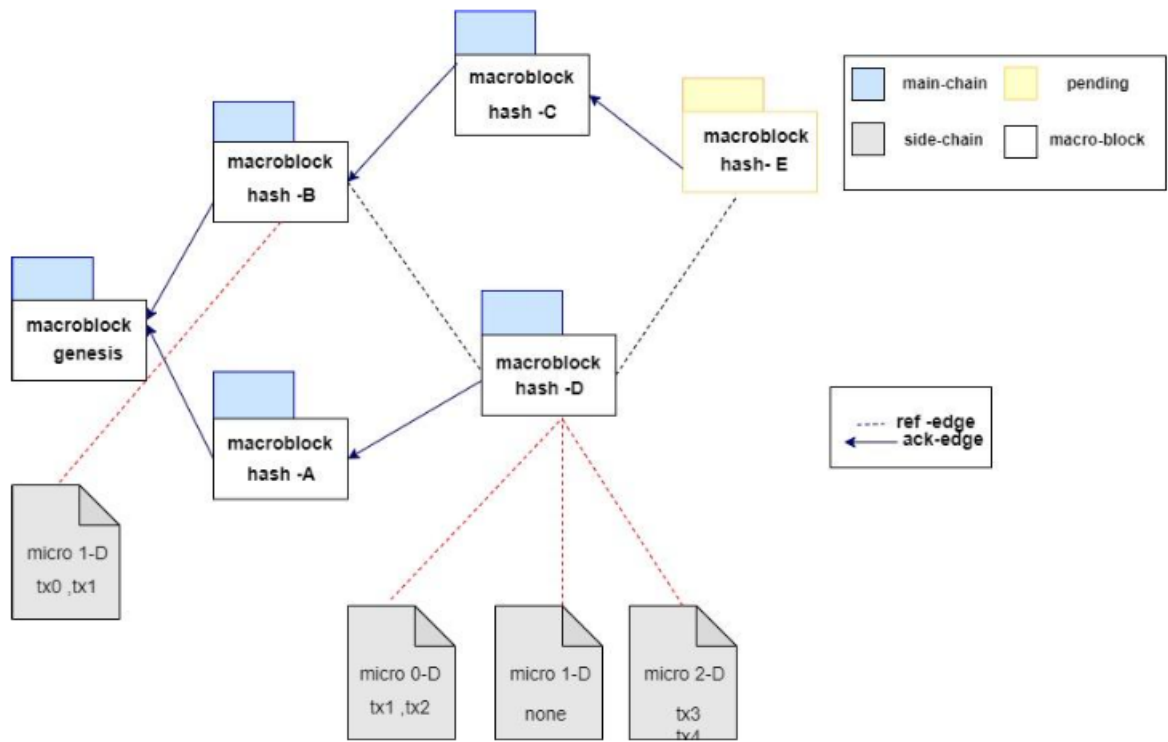


Figure 9: Data Structure for Spacechain

Figure 9 depicts a graphical representation of how macroblocks and microblocks are connected through the ref-edge and ack-edge. All the microblocks connected to each vertex of the DAG are conditionally independent, for example, 2-D, 0-D, and 1-D belonging to D. Furthermore, the number of linked microblocks indicates the weight of a single vertex in the three-dimensional ledger, which really is critical for the proposed 3D-GHOST system.

3 Proposed Approach

3.1 Research Challenges

3.1.1 Lack of research support

Due to the fact that the sidechain arena is still in its infancy, the majority of the most cutting-edge sidechain technologies are still in the research or bounty hunting stages. Because developers do not give entry to all consumers on their platforms at present moment, registering or uploading DApps on some of the platforms (e.g., Liquid and RSK) listed in the preceding section is exceedingly difficult and selective, according to the authors' testing experiences. Some of these sites are not yet interconnected with Ethereum or Bitcoin test-nets, which further complicates the situation (e.g. Liquid). This makes conducting empirical studies on these platforms by academics or practitioners exceedingly difficult and costly owing to the market price of ether and bitcoin crypto-currencies, which are both quite popular today. Empirical research is an essential technique in software engineering because it may reveal hidden tendencies, structures, anomalies, and limits in a software system. Empirical research can be used to discover hidden trends, patterns, anomalies, and limitations in a software system. As a result, we highly recommend the following:

- The incorporation of these platforms into the test-nets of their parent chain. Performance, security, and privacy are among the features that scholars in the community may analyze and evaluate. This will aid in the acceleration of the development process and also the improvement of sidechain Technology as a whole.
- As during the bounty hunting phase, developers of sidechain platforms should make it possible for researchers to do research on their platforms. When it comes to empirical research and benchmarking data, this would be quite beneficial for a platform that is currently being created.

3.1.2 No Universal Implementation

As sidechain is a comparatively new field there are yet no fixed stable implementation, for which we had to try a lot of ways and find out which works best for us. At present, the cross-chain mechanism does not have any universal applicability. That is, no practical implementation so far. That is why, we faced a lot of difficulties in forming a stable system, since its research is still in the initial stage of exploration

3.2 Methodology

A hybrid framework that makes the exchange of values among different blockchains easier and improves privacy of the existing blockchain by maintaining data integrity.

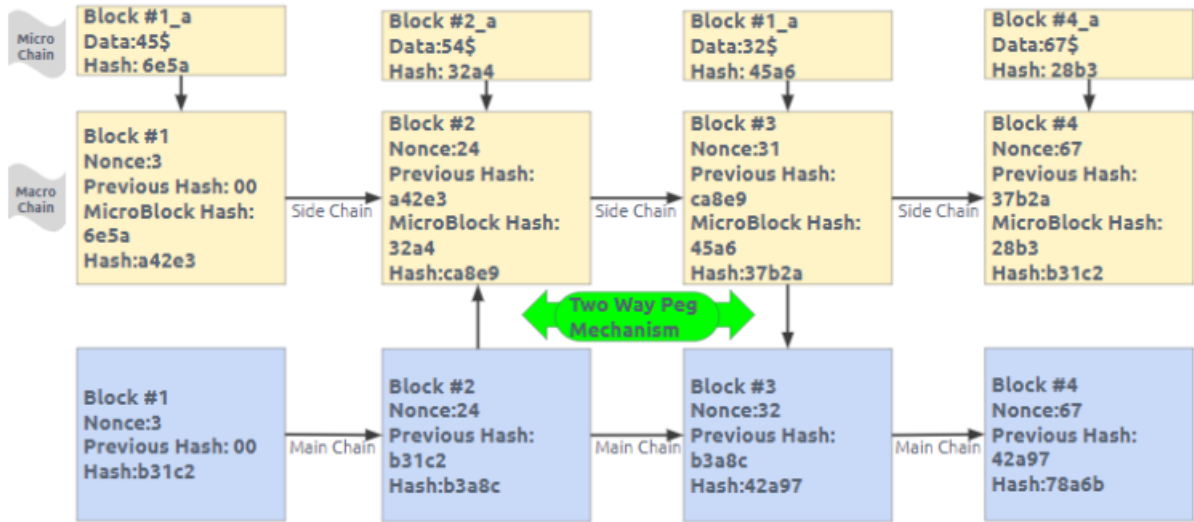


Figure 10: Hybrid Blockchain Architecture

In this Figure 10 there are two chains continuing parallelly. The blue chain, which can be found at the bottom, serves as our primary blockchain. We use a device called a two-way peg to connect the primary chain's second node with the yellow-colored secondary chain. This connection is made at the primary chain's second node. The asset that we wish to convert is kept safe inside the lock box thanks to this particular peg mechanism. When this is complete, we will proceed to do the necessary transactions in the secondary chain. Once the condition in the secondary chain has been satisfied, we will either be able to keep the tokens on the sidechain and make use of them in the future or we will be able to convert them back to our primary chain using the lockbox. In the event that the tokens are converted back, we will collect the previously locked tokens according to the requirements and trash the remaining tokens. Using this method, we are able to construct a system that is interoperable by moving back and forth through the

two way peg mechanism.

There is a chance that sensitive data could be compromised due to the fact that we are collaborating with two distinct chains and running our token exchange on sidechains. Along with the sidechain design, we came up with the concept of space chains in order to address the privacy concerns raised by these transactions. Each of the blocks in the sidechain can be broken down into one of two distinct sections: the macro-block or the micro-block. The micro-block of the side chain is where all of our data, account details, and other sensitive information will be saved. The only information that will be displayed in the macro-block that will have a direct connection to the primary chain will be the hashes and a predetermined amount of data. This spacechain idea is not restricted to the use of the sidechain; rather, it is applicable to the use of the primary chain as well. Since the primary chain will also be susceptible to the loss of data in this scenario. In this scenario, all of our data, account information, and other sensitive data will be saved in the micro-block, and the macro-block will be composed of the data that was previously defined as well as the hashes. Only the hashes will be stored in the macroblock because those hashes are secure enough to prevent anyone from decrypting the information contained therein. Additionally, because it is a distributed ledger network, no chain can be manipulated in any way. If we continue in this manner, not only will the data's confidentiality be protected, but we will also be able to create an architecture that is interoperable.

4 Experimental Setup

At first we had to decide on which platform and language we will be using. Next we fixed our environment and installed Python, Anaconda, Postman and other necessary platforms, tools, and libraries. We followed some guidelines to help us understand the architecture better and built a base architecture where we can build blocks and form a chain like structure by sending messages through API.

4.1 Implementation

The purpose of this documentation is to keep records of how we have prepared our work environment and written smart contracts. We have written all our codes in Visual Studio Code using Solidity language. At first, we built our basic dapp. For that we had to install Node.js, Hardhat, Metamask extension, Truffle, Brownie and other required libraries and extensions. We also installed the solidity, react and setuptools extensions in VSCode for better interface.

We collected our interface components from bootstrap. And built the UI for the Dashboard first. We then connected it with our metamask account which we had previously installed. We also collected some testing tokens for different accounts and created different accounts in our Metamask Wallet beforehand. After that we ran the Dashboard which shows all the transactions and their details in a tabular form. Here everything about the account is given in detail. The dashboard also shows balances for different tokens of the user account. It also shows the NFT's that are available.

Then we went for our side chain contracts which allows the tokens from the main chain to be burned and sent to the side chain. We also built contracts for the tokens in the side chain to be burned and returned to the main chain. This ensures that one can invest in the side chain and come back to their main chain once the need in the side chain is fulfilled.

In order to build this side chain, we at first built a basic project in truffle and then added the contracts to it. We then deployed the contracts by connecting with the

metamask instance. We also built an UI, where we can input our amount of token to be burned and once the tokens are burnt we can also see how much token was burnt and with which account the transaction was done. There is also an UI for the return of tokens, where the amount of tokens to be exchanged is given and then it returns those tokens to our main chain.

The interface for the token transfer bridge looks like the following:

Here, Rinkeby Test Network has been used as the mainchain and Mumbai Polygon Testnet as the sidechain, the Ethereum protocol is being utilized by both of these test networks. In this particular instance, we demonstrated our sidechain in a separate network.

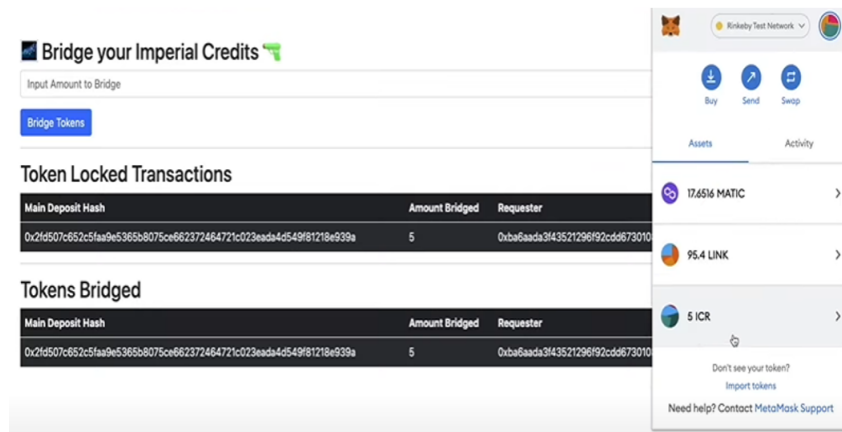


Figure 11: Assets in the main chain

Figure 11 shows an interface through which we can transfer our mainchain token to sidechain token. It shows the amount of the transaction and also the account where the conversion is done.

In Figure 12 it shows an interface for moving sidechain tokens to the mainchain. It displays the transaction total and conversion account.

Both Rinkeby Test Network and Mumbai Polygon Testnet employ the Ethereum protocol. We demonstrated sidechain in a separate network.

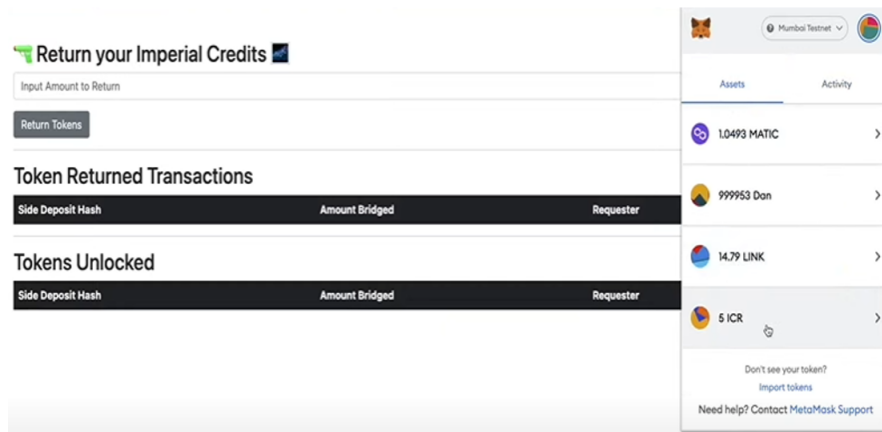


Figure 12: Assets in the side chain

All these transaction records are shown in our dashboard in Figure 13. Here in

Transactions	Block Number	Age	Chain	Type	Fee
0c564411c179ee125fc37cc98c2a0273209a20b3041f647a03da4c00312d88	10566027	42 minute(s) ago	Bridge to sidechain	Outgoing	0.00004070709835712 ETH
0d347b2c0170cac1f62a1142b8ee2acc03d9b1aaa07b638f27e6514710db1bd08	10565995	50 minute(s) ago	Bridge to sidechain	Outgoing	0.000036037700954112 ETH
0a0000dc9ccac4276e5d906a735ef43ef740d44157a07234dc5384aac331e2538	10563335	11 hour(s) ago	Bridge to sidechain	Outgoing	0.000032448000194688 ETH
06a6db389f2aac279c7a09c33ac1ac0875616f6c86d4de153079b25445c932d3	10563320	12 hour(s) ago	Bridge to sidechain	Outgoing	0.00003243000019458 ETH
0x91c289c203c39ef58db106d5c743f25e88bceccccc2cc397bcac87ba0b4a7c	10561146	21 hour(s) ago	Mainchain transaction	Incoming	0.0001500000006 ETH
0xe8116f0d0a400eeba975346d5bcc58a77ac5d0edfae11089b4e4d42219acfd4	10560631	23 hour(s) ago	Mainchain transaction	Incoming	0.0001500000006 ETH
0e4e9e0363807baa137a24a2fd6d679cc03713db2d3a830be75b8ebbd5c7663a09b	10559430	1 day(s) ago	Mainchain transaction	Outgoing	0.0000315000000462 ETH
0x8a90483736e5f58e530e5200dcd5fb549e3d40aaf0ced926e13b9e4819c5bd656	10556656	1 day(s) ago	Mainchain transaction	Incoming	0.00015000000048 ETH
0xed3c1c79db2c508e4d758658090349977520007290988299d82aba44b7b4a	10556655	1 day(s) ago	Mainchain transaction	Incoming	0.00015000000048 ETH
0x09b74b71bd451cc8ec1ca7e428d4a7c1a59505a809964a3a864415c0408cc93f	10556653	1 day(s) ago	Mainchain transaction	Incoming	0.00015000000048 ETH
0xc5db5f12a00c7955ef585aa9f946ce493a78013b5bced803d97c752e11b5e54b	10556650	1 day(s) ago	Mainchain transaction	Incoming	0.00015000000048 ETH
0xc8b1cf9535601442e87119489491c506529431d2626289eb71dc0826b5d277	10550297	2 day(s) ago	Mainchain transaction	Incoming	0.0001500000006 ETH
0x064783a7d073e809624446623b0e1eeb736201d9c4862b401bef33eb33731	10550252	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000054 ETH
0xf0f87366151f89d6b1d7cd39a7d50ce65b0e64b2b045421916fc113c327da	10550234	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000054 ETH
0xea71bc497b984764e31623775c583d963336e98f1b6f115d4d117a7b036a	10550207	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000066 ETH
0x32a39e662997e087326671261046a2b1395ad5d4b18b529599dc5a4b387ed	10550199	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000066 ETH
0xc852c4cd07b549760907029651c4e4c1c4f13e451b19cfd94b604d4d46bd0	10550197	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000072 ETH
0x12ba642347e8c3d42055db0a0a0d8c149efdc73ab94ae9472cd885f66b0	10550191	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000084 ETH
0x794c66091354097d19910600cdcbca864412066bbed101603623abd58073b81	10550187	2 day(s) ago	Mainchain transaction	Incoming	0.00015000000078 ETH
0x3eed72ba46f930ac0420be42f533c5544614457c0ecf9acfb089e128ce6f6	10550182	2 day(s) ago	Mainchain transaction	Incoming	0.001479744014784 ETH

Figure 13: Transaction Dashboard

the Figure 13 the transactions column contains all transaction data, and each transaction's hash provides extra details. Transactions are kept in blocks. The transaction's age is given. The chain shows the current chain. The chain column indicates primary-to-main or main-to-primary token conversions. Column displays if the transaction came from the selected chain or received a token.

In this way we built our side chain and checked with our dashboard whether the bridging is done correctly.

5 Conclusion

“Blockchain interoperability” is a term that describes the capability of numerous blockchain networks to share and utilize data as well as transfer various types of digital assets between their own blockchains. This ability is referred to as “blockchain interoperability.” However, the typical blockchain does not fulfill the requirements of this word in its current form. Sidechain is a solution to this problem; nevertheless, it comes with its own unique set of restrictions. Despite the fact that sidechain makes it easier to conduct cross-platform transactions between different chains, it does so at the expense of adding additional difficulties that could compromise data integrity. Because of this, it is important to take into account the 3-dimensional architecture of the blockchain, which boosts the data’s level of security by preventing it from being exposed in macroblocks.

As a consequence of the limitations of the existing architecture as discussed previously, in this paper, we put forward a substantial solution to the interoperability issue that plagues the blockchain. This solution involves the combination of two new blockchain architectures, known as sidechain and spacechain, in such a way that it enhances the network security provided by the conventional blockchain by making the system more scalable.

There are a lot of scopes for future improvements here, such that-

- Incorporation of complete 3D architecture within the framework.
- Performance evaluation in a practical setting of the hybrid architecture.
- Finally, we will optimize the performance of the framework that has been described.

References

- [1] Monrat, A.A., Schelén, O. and Andersson, K., 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7, pp.117134-117151.
- [2] Wang, X., Zha, X., Ni, W., Liu, R.P., Guo, Y.J., Niu, X. and Zheng, K., 2019. Survey on blockchain for Internet of Things. *Computer Communications*, 136, pp.10-29.
- [3] Ghosh, A., Gupta, S., Dua, A. and Kumar, N., 2020. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *Journal of Network and Computer Applications*, 163, p.102635.
- [4] Du, M., Wang, K., Liu, Y., Qian, K., Sun, Y., Xu, W. and Guo, S., 2020. Spacechain: a three-dimensional blockchain architecture for IoT security. *IEEE Wireless Communications*, 27(3), pp.38-45.
- [5] Singh, A., Click, K., Parizi, R.M., Zhang, Q., Dehghantanha, A. and Choo, K.K.R., 2020. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149, p.102471.
- [6] Lin, S., Kong, Y. and Nie, S., 2021, January. Overview of Block Chain Cross Chain Technology. In *2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)* (pp. 357-360). IEEE.
- [7] Lacity, M.C., 2018. Addressing key challenges to making enterprise blockchain applications a reality. *MIS Quarterly Executive*, 17(3).
- [8] Liu, Y., Wang, K., Lin, Y. and Xu, W., 2019. **LightChain**: a lightweight blockchain system for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 15(6), pp.3571-3581.

- [9] Liu, Y., Wang, K., Qian, K., Du, M. and Guo, S., 2019. Tornado: Enabling blockchain in heterogeneous Internet of Things through a space-structured approach. *IEEE Internet of Things Journal*, 7(2), pp.1273-1286.
- [10] Robinson, P., Ramesh, R. and Johnson, S., 2022. Atomic crosschain transactions for ethereum private sidechains. *Blockchain: Research and Applications*, 3(1), p.100030.
- [11] Kan, J., Chen, S. and Huang, X., 2018, August. Improve blockchain performance using graph data structure and parallel mining. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 173-178). IEEE.
- [12] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P., 2014. Enabling blockchain innovations with pegged sidechains. URL: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>, 72.
- [13] Buterin, V., 2014. A next-generation smart contract and decentralized application platform. white paper, 3(37), pp.2-1.
- [14] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. and Rong, C., 2019. A comprehensive survey of blockchain: From theory to IoT applications and beyond. *IEEE Internet of Things Journal*, 6(5), pp.8114-8154.
- [15] Yu, Y., Li, Y., Tian, J. and Liu, J., 2018. Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, 25(6), pp.12-18.
- [16] Xu, C., Wang, K., Li, P., Guo, S., Luo, J., Ye, B. and Guo, M., 2018. Making big data open in edges: A resource-efficient blockchain-based approach. *IEEE Transactions on Parallel and Distributed Systems*, 30(4), pp.870-882.
- [17] Xu, C., Wang, K. and Guo, M., 2017. Intelligent resource management in blockchain-based cloud datacenters. *IEEE Cloud Computing*, 4(6), pp.50-59.

- [18] Eyal, I. and Sirer, E.G., 2014, March. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security (pp. 436-454). Springer, Berlin, Heidelberg.
- [19] Vukolić, M., 2015, October. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International workshop on open problems in network security (pp. 112-125). Springer, Cham.
- [20] Singh, M., Singh, A. and Kim, S., 2018, February. Blockchain: A game changer for securing IoT data. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 51-55). IEEE.