International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 10 | Oct 2022 www.irjet.net p-ISSN: 2395-0072

Blockchain Technology Overview

Siddhant Shivdikar[1]

[1] *Electronics Department, Fr. Conceicao Rodrigues College of Engineering, Bandra, India*

Abstract - *Blockchains are distributed (i.e., without a central repository) and typically decentralized (i.e., not controlled by a bank, enterprise, or government) tamper-evident and tamper-resistant digital ledgers. At their most basic level, they allow a group of users to log transactions in a shared ledger such that, as long as the blockchain network is functioning normally, no transaction can be modified once it has been recorded. An exhaustive summary of blockchain technology is presented in this article.*

Key Words: **Blockchain, Ledger, Public blockchain networks, Permissioned blockchain networks, Cryptocurrency, Cryptography, etc**.

1. INTRODUCTION

Blockchains are distributed (i.e., without a central repository) and typically decentralized (i.e., not controlled by a bank, enterprise, or government) tamper-evident and tamper-resistant digital ledgers. At their most basic level, they allow a group of users to log transactions in a shared ledger such that, as long as the blockchain network is functioning normally, no transaction can be modified once it has been recorded.

In the late 1980s and early 1990s, the fundamental concepts behind blockchain technology first surfaced. Leslie Lamport created the Paxos protocol in 1989, and in 1990 he submitted his work The PartTime Parliament [1] to the ACM Transactions on Computer Systems, which eventually led to its publication in a 1998 edition. The article outlines a consensus approach for determining a result in a computer network when the machines or network may not be dependable in and of themselves. In order to prove that none of the signed papers in the collection had been altered, a signed chain of information was utilized in 1991 as an electronic ledger for digitally signing documents [2]. The Bitcoin cryptocurrency blockchain network was created in 2009 using the principles that were merged and applied to electronic cash in the article Bitcoin: A Peer to Peer Electronic Cash System [3], which was released under the pseudonym Satoshi Nakamoto. The design for the majority of contemporary cryptocurrency schemes was published in Nakamoto's article (although with variations and modifications).

Modern cryptocurrencies were developed in 2008 using the blockchain concept in conjunction with a number of other technologies and computing ideas. These digital currencies are secured by cryptographic processes rather than a central repository or authority. Bitcoin was the first such blockchain-based cryptocurrency. Before Bitcoin, there were other electronic cash systems (such ecash and NetCash), but none of them became widely used. Bitcoin's adoption was encouraged by the use of a blockchain, which made it possible to deploy electronic money in a distributed manner without a single user having control over it or a single point of failure. Its main advantage was the ability to conduct direct transactions between users without the use of a reliable intermediary. It also made it possible to issue fresh bitcoin in a specified way to users who are able to create new blocks and keep copies of the ledger; in the context of Bitcoin, these users are known as miners. The system's dispersed management was made possible without the need for organization because to the miners' automatic payments.

The blockchain of Bitcoin made it possible for users to employ pseudonyms. Users are therefore anonymous, but account identities are not; in addition, all transactions are open to the public. Because accounts can be created without going through any identification or authorisation procedures (which are normally mandated by Know-Your-Customer (KYC) requirements), Bitcoin is now effectively able to offer pseudo-anonymity.

1.1 KEY ELEMENTS OF BLOCKCHAIN

Since Bitcoin users could only be recognized by their pseudonyms, it was crucial to have procedures in place to foster confidence. This trust was normally given before the adoption of blockchain technology by middlemen who were trusted by both sides. Without trusted intermediates, the four main properties of blockchain technology, which are outlined below, provide the required trust inside a blockchain network:

1. Ledger

   Similar to a database, a blockchain is a distributed ledger, but instead of being managed by a single entity (a MNC, a small business, or an individual), the ledger is spread across numerous computers that are accessible from anywhere in the world and can be operated by anyone with an Internet connection. A blockchain, at its heart, is a ledger where data is continuously added to and updated thanks to the network's various nodes' consensus.

However, unlike a database, once the data is put to the ledger, it cannot be changed or withdrawn. This is a result of how blockchains are made in general.

2. Secure

Once a transaction has been added to the shared ledger, no participant is permitted to alter or interfere with it. A fresh transaction must be entered to undo a mistake in a transaction record before both transactions are displayed.

3. Shared

A sort of database that is shared, copied, and synced across the participants in a decentralized network is known as a distributed ledger. The distributed ledger keeps track of all interactions between network users, such as the trading of goods or information. The ledger's entries are updated by consensus among network participants, who also regulate the system. There isn't any involvement from a centralized authority or a neutral third party, such a clearinghouse or financial institution. Every entry in the distributed ledger has its own cryptographic signature and timestamp.

4. Distributed

Consider, as a mental exercise, an Ethereum network with only one participating entity. Does trust exist? What about when there are three equally influential entities? How many equally influential entities do we have to have participating before that trust actually has value? These types of questions, ones related to nonlinearity and tipping points, are the ones that are typically the drivers of modeling emergent phenomena [4]. Distributing the blockchain is possible. This makes it possible to scale the number of nodes in a blockchain network, increasing its resistance to attacks from malicious parties. A malicious actor's capacity to influence the blockchain's consensus mechanism is diminished by increasing the number of nodes.

2. CLASSIFICATION OF BLOCKCHAIN NETWORKS

Based on their permission mechanism, which governs who may maintain them, blockchain networks can be divided into several categories. The system is permissionless if anybody may publish a new block. It is permissioned if certain users are the only ones who may post blocks. A permissioned blockchain network is analogous to a managed business intranet, whereas a permissionless blockchain network is comparable to the open internet and is accessible to everyone. For a collection of businesses and individuals, referred to as a consortium, permissioned blockchain networks are frequently implemented. Understanding this distinction is essential since it has an effect on several of the blockchain components.

2.1 PUBLIC BLOCKCHAIN NETWORKS

Blockchain networks with no requirement for authorization from any authority are decentralized ledger systems where anybody may publish blocks. Blockchain solutions that don't require permission are frequently free to download and distributed as open source software. Anyone has the ability to publish blocks, which leads in the ability for anyone to read the blockchain and execute transactions on it. A permissionless blockchain network allows any user to view and write to the ledger. Since everyone may participate in permissionless blockchain networks, malevolent users may try to publish blocks in a way that undermines the system. In order to avoid this, permissionless blockchain networks frequently make use of a multiparty agreement mechanism, sometimes known as a "consensus" system (Section 4), which necessitates users to spend or retain resources in order to publish blocks. This makes it difficult for malicious people to compromise the system. Proof of work (Section 4.1) and proof of stake (Section 4.2) procedures are examples of such consensus models. Consensus systems in permissionless blockchain networks often encourage ethical conduct by rewarding protocol-compliant block publishers with a native coin.

2.2 PERMISSIONED BLOCKCHAIN NETWORKS

Blockchain networks that need authorization from a third party for users to publish blocks are known as permissioned networks (centralized/decentralized). You can limit read access and who may issue transactions because only authorized users are maintaining the blockchain. Thus, permissioned blockchain networks may either let everyone access to read the blockchain or they can limit read access to vetted users. Additionally, they may permit anybody to submit transactions for inclusion in the blockchain or, once more, they may restrict access to this information to those who have been given permission. Using open source or closed source software, permissioned blockchain networks may be created and managed.

In addition to having the same distributed, robust, and redundant data storage mechanism as permissionless blockchain networks, permissioned blockchain networks can also have the same traceability of digital assets as they move across the blockchain. For publishing blocks, they too employ consensus models, however these techniques frequently do not necessitate the expenditure or upkeep of

resources, as is the case with contemporary permissionless blockchain networks. This is due to the fact that establishing one's identity is necessary to participate in the permissioned blockchain network; those who maintain the blockchain have a degree of trust in one another because they were all given permission to publish blocks and because that permission can be revoked if they act inappropriately. Based on a blockchain network user's identification or credentials, certain permissioned blockchain networks enable the ability to selectively expose transaction details. A certain level of transactional privacy may be attained with the help of this feature. A transaction between two users of a blockchain network could be recorded on the blockchain, but the actual details of the transaction might only be visible to the persons involved.

So, in permissioned blockchain networks, consensus mechanisms are typically quicker and less computationally costly.

3. ASPECTS OF BLOCKCHAIN

Blockchain technology might appear complicated, but by dissecting each part, it can be made simpler. Blockchain technology, at its most basic level, combines notions from record keeping with well-known computer science methods and cryptographic primitives (cryptographic hash functions, digital signatures, and asymmetric-key cryptography). Each major component is covered in detail in this part, including transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and chaining of blocks.

3.1 CRYPTOGRAPHIC HASH FUNCTIONS

The widespread application of cryptographic hash functions is a key aspect of blockchain technology. Applying a cryptographic hash function to data via hashing produces a comparatively unique result (referred to as a message digest, or simply digest), given an input of almost any size (e.g., a file, text, or image). It enables users to independently take input data, hash that data, and arrive at the same conclusion - demonstrating that the data was unchanged. A single bit changed in the input, for example, might have a huge difference in the output digest. Simple instances of this may be seen in Table 1. These crucial security characteristics apply to cryptographic hash functions:

1. They can withstand preimages. As a result, they are one-way; for example, given a digest, locate x such that hash(x) = digest. It is computationally impossible to determine the proper input value given some output value.

2. They can withstand second preimages. This indicates that it is impossible to discover an input that hashes to a certain output. More specifically, cryptographic hash functions are created in a way that makes it computationally impossible to discover a different input that yields the same output given a specified input (for example, given x, find y such that hash(x) = hash(y)). The sole option is to thoroughly examine the input space, however this is computationally impractical to attempt with any degree of probability.

3. They can withstand collisions. Because of this, it is impossible to discover two inputs that hash to the same output. Finding any two inputs that give the same digest, for example, finding an x and y where hash(x) = hash(y), is computationally impossible.

The Secure Hash Algorithm (SHA), which has an output size of 256 bits, is a particular cryptographic hash function utilized in several blockchain implementations (SHA-256). This technique is hardware supported on many systems, which speeds up computation. A 64-character hexadecimal string is typically shown as the output of SHA-256, which has an output of 32 bytes (1 byte = 8 bits, 32 bytes = 256 bits) (see Table 1 below). Thus, the number of potential digest values is $2^{256} \approx 10^{77}$, or 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665, 640,564,039,457,584,007,913,129,639,936. The algorithm for SHA-256, as well as others, is specified in Federal Information Processing Standard (FIPS) 180-4 [5]. The NIST Secure Hashing website [6] contains FIPS specifications for all NIST-approved hashing algorithms.

Input	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Hello	0x185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
World	0x78ae647dc5544d227130a0682a51e30bc7777fbb6d8a8f17007463a3ecd1d524

Hash(x) = Hash(y) (i.e., the hash of two separate inputs generates the same digest) is feasible but extremely rare because there are an unlimited number of potential input values and a finite number of possible output highest values. Since it would take an average of 2128 executions of the algorithm—340 undecillions, or more exactly 340,282,366,920,938,463,463,374,607,431,768,211,456—to detect a collision in SHA-256, it is considered to be collision-resistant.

3.1.1 NONCE

A nonce is a number that is created at random or almost random for a specified purpose. The phrase, which means "number used once" or "number once," is also known as a

cryptographic nonce. A nonce is often a value that changes over time to ensure that certain values are not repeated. A nonce is a particular marker used to restrict or prohibit the illegal playback or duplication of a file. It can be a date, a visit counter on a website, or a special marker.

hash (data + nonce) = digest

There is a way to get various digest results while preserving the same data by only altering the nonce value. This method is applied in the consensus proof of work model.

3.2 TRANSACTIONS

An interaction between parties is represented by a transaction. When it comes to cryptocurrencies, for instance, a transaction is the transfer of a coin between users of the blockchain network. A transaction might be a technique of documenting activities taking place on physical or digital assets in business-to-business contexts. A hypothetical example of a bitcoin transaction is shown in Figure 1. A blockchain can have zero or more transactions in each block. A continuous flow of new blocks, even those with no transactions, is necessary for various blockchain implementations in order to ensure the network's security. This is because it prevents unscrupulous users from ever "catching up" and creating a longer, modified blockchain.

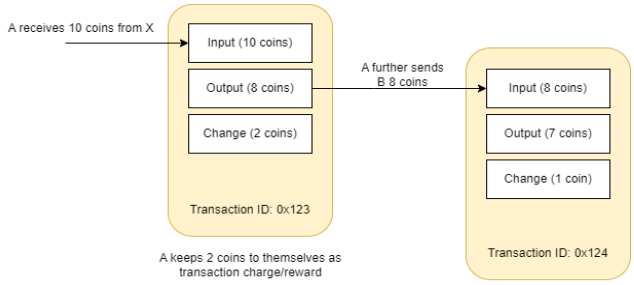

Fig – 1: Hypothetical Example of Bitcoin Transaction

The following information must normally be included in a single cryptocurrency transaction, however it may contain more:

- Input - A list of the digital assets to be transferred often serves as the input. A transaction will make a reference to the origin event for new digital assets or the prior transaction where it was delivered to the sender in order to provide provenance. The digital assets remain unchanged since the input to the transaction is a reference to earlier occurrences. This means that existing digital assets in the case of cryptocurrencies cannot have value added to them or subtracted from them. Instead, a single digital asset can be divided into several new ones, each with a lower value, or several digital assets might be merged to create fewer new ones (with a correspondingly greater value). The transaction output will specify the splitting or joining of assets. The sender must additionally demonstrate that they have access to the inputs they are referencing, often by digitally signing the transaction to demonstrate their control over the private key.

- Output - The accounts that will get the digital assets, along with the quantity they will receive, are typically the outputs. The amount of digital assets to be transferred to the new owner(s), their identification, and the requirements they must satisfy in order to use that value are all specified in each output. The additional money must be explicitly handed back to the sender if the digital assets delivered are greater than what is needed (this is a way to "make change").

3.3 Public Key Cryptography

Public key cryptography, also known as asymmetric key cryptography, is used by blockchain technology. A pair of keys—a public key and a private key—that are mathematically connected to one another are used in asymmetric-key cryptography. Without jeopardizing the process' security, the public key is made available, but the private key must be kept a secret if the data is to continue to be encrypted. Despite the fact that there is a connection between the two keys, figuring out the private key using the public key alone is inefficient. A private key can be used to encrypt data, while a public key may be used to decode it. Another option is to use a public key to encrypt and a private key to decode. Public key cryptography, also known as asymmetric key cryptography, is used by blockchain technology. A pair of keys—a public key and a private key—that are mathematically connected to one another are used in asymmetric-key cryptography. Without jeopardizing the process' security, the public key is made available, but the private key must be kept a secret if the data is to continue to be encrypted. Despite the fact that there is a connection between the two keys, figuring out the private key using the public key alone is inefficient. A private key can be used to encrypt data, while a public key may be used to decode it. Another option is to use a public key to encrypt and a private key to decode. Asymmetric-key cryptography has the downside of being computationally time-consuming.

This is in contrast to symmetric-key cryptography, which encrypts and decrypts data using the same secret key. Users using symmetric-key cryptography must already be in a mutually trusting relationship in order to exchange the pre-shared key. In a symmetric system, any encrypted data that can be decrypted with the pre-shared key verifies it was supplied by another user who also has

access to the key; no user who does not have access to the pre-shared key will be able to read the decrypted data. Symmetric-key cryptography is extremely quick to compute in comparison to asymmetric-key encryption. Due to this, when someone says they are encrypting anything using asymmetric-key cryptography, the material is frequently first encrypted using symmetric-key cryptography before the symmetric-key is encrypted using the asymmetric-key. Asymmetric-key cryptography can be significantly sped up with this "hack". FIPS Publication 186-4, Digital Signature Standard [7] specifies a common algorithm for digital signing used in blockchain technologies: Elliptic Curve Digital Signature Algorithm (ECDSA).

3.4 Addresses

Some blockchain networks utilize an address, which is a brief string of alphanumeric characters created from the user's public key on the blockchain network using a cryptographic hash function, coupled with some other information (e.g., version number, checksums). Addresses are often used as the "to" and "from" endpoints in a transaction in blockchain systems. Addresses are not private and are shorter than public keys. A public key can be created, subjected to a cryptographic hash algorithm, and then converted to text to produce an address:

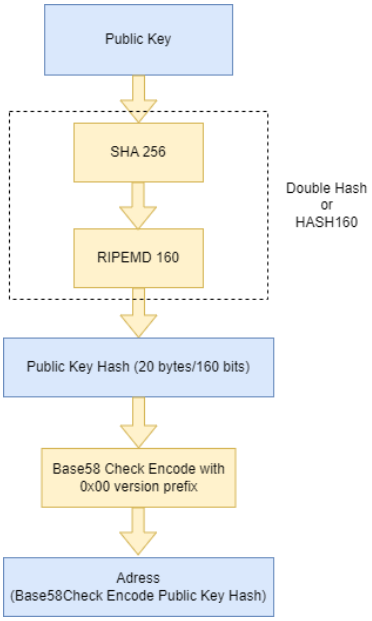

Fig – 2: Hashing public key for generating address

Different methods for calculating addresses may be used in different blockchain implementations. A blockchain network user can create as many asymmetric-key pairs and consequently addresses as desired on permissionless blockchain networks, which enable the establishment of anonymous accounts and offer variable levels of pseudo-anonymity. For ease of usage with mobile devices, addresses are frequently turned into QR codes (Quick Response Code, a 2-dimensional bar code that may store arbitrary data). Addresses can serve as a user's public-facing identify in a blockchain network.

3.4.1 Private Key Storage and Wallet

Users might have to maintain and safely keep their own private keys on some blockchain networks (particularly permissionless blockchain networks). They frequently utilize software to safely save them instead of physically storing them. This program is frequently called a wallet. Private keys, public keys, and related addresses can all be kept in the wallet. It could also carry out additional tasks, such figuring out how many digital assets a person has in total.

Any digital asset linked to a user's lost private key is also lost since it is computationally impossible to produce a new copy of that private key. If a private key is taken, the attacker gains complete control of any digital assets that private key is used to access. Private key security is so crucial that many users keep their private keys on specialized safe hardware; alternatively, users can benefit from a growing market for private key escrow services. In addition to safeguarding private keys, these key escrow services may also abide with KYC regulations as users are required to present identification documentation when opening an account.

Blockchain usage requires the use of cryptocurrency wallets, or "crypto-wallets". Each user must have a cryptocurrency wallet if they plan to utilize the blockchain platform for any type of transaction. Cryptocurrencies are not kept in crypto-wallets, in contrast to conventional pocket wallets. In actuality, cryptocurrencies exist as data of transactions kept on blockchain and do not reside somewhere in a physical form or in a single location. Wallets make it easier for users to create accounts, which consist of a set of private and public keys that are stored in a wallet program. A user must authenticate his ownership of the coins to his wallet's address in order to complete any transaction on the blockchain. By utilizing the wallet's keys to unlock the money, the user may spend coins. Different types of crypto-wallets are used to manage cryptocurrencies, as stated below:

Desktop Wallet: On a PC or laptop, it is software that can be downloaded and set up [8]–[10]. From a single computer where it is installed, it is simple to utilize. One of the highest levels of security are provided by desktop wallets. However, there is a chance of losing keys and therefore money if a computer is hacked or infected.

Online Wallet: It is a piece of software that functions on the cloud and should be simple to use from anywhere [11]-[13]. Such wallets are controlled by a third party and store your private and public keys online, despite being

convenient to access, it exposes users to the danger of third parties being compromised or hacked online.

Mobile wallet: It is software that runs on your phone as a mobile application [14]–[17]. For transactions and payments, it is more user-friendly and convenient to use than retail establishments. Unlike desktop wallets, mobile wallet software provides a straightforward user interface.

Hardware wallet: Hardware wallets vary from software wallets in terms of managing and storing keys since keys are kept on a device like a USB [18], [19]. Public and private keys are maintained offline even if hardware wallets conduct transactions online. As a result, it provides excessive security. The user's public and private keys are unquestionably a physical copy or hardcopy, [20], [21]. It also describes a piece of software that is used to create several keys safely and then prints them out on paper. When compared to the other wallets, using a paper wallet offers the best level of protection and is generally reliable. However, there is still a danger of paper wallet compromise or loss.

3.5 Ledgers

In bookkeeping, a general ledger, is a bookkeeping ledger in which accounting data is posted from journals and aggregated from sub ledgers, such as accounts payable, accounts receivable, cash management, fixed assets, purchasing and projects [22]. The commercial ledgers now in use have significant shortcomings. They are expensive, ineffective, and prone to manipulation and misuse. Conflicts result from a lack of openness as well as vulnerability to fraud and corruption. It is expensive to have to settle disagreements, maybe reverse transactions, or offer transaction insurance. Missed business opportunities are a result of these risks and uncertainties. Furthermore, erroneous business judgments based on shaky, inaccurate data are caused by out-of-sync copies of business ledgers on each network participant's own systems. At best, the process of reconciling several ledger copies delays the capacity to make a fully informed choice.

Modern ledgers are kept digitally, sometimes in sizable databases that are managed by a centralized trustworthy third party (the owner of the ledger) on behalf of a user community. These centralized ownership ledgers can be deployed either centralized or decentralized (i.e., just one server or a coordinating cluster of servers). Such a strategy is made possible by blockchain technology employing a distributed physical architecture as well as distributed ownership. Blockchain networks' distributed physical architecture sometimes uses a substantially greater number of machines than is common for a distributed physical architecture that is centrally managed. Given potential issues about the trustworthiness, security, and dependability of ledgers with centralized ownership, there is rising interest in distributed ownership of ledgers.

Centralised Ledger	Distributed Ledger
Users must have faith that the owner is adequately backing up the system since centrally owned ledgers might be lost or destroyed.	By design, a blockchain network is dispersed, with several backup copies of the same ledger data being created and synced between peers. The ability for each user to retain their own copy of the ledger is a significant advantage of blockchain technology. It is harder to lose or destroy the blockchain network's ledger because whenever new full nodes join it, they seek out other full nodes and ask for a complete copy of it.
In a homogenous network, all software, hardware, and network infrastructure may be the same, and centrally held ledgers may be connected to it. This trait may weaken the overall system resilience since an assault on one area of the network would affect the entire system.	A blockchain network is an example of a heterogeneous network, where the network architecture, hardware, and software are all diverse. An assault on one node on the blockchain network may not be successful against other nodes due to the numerous variances between the nodes.
A user must have faith that the owner is not changing previous transactions since the transaction data on a centrally maintained ledger may have been changed.	To create tamper-evident and tamper-resistant ledgers, a blockchain network makes use of cryptographic processes like digital signatures and cryptographic hash functions.
A user must have faith that the owner is recording all received legitimate transactions even though the ledger's transaction list may not be comprehensive.	All approved transactions are stored on a blockchain network's distributed ledger. Building on top of a prior block necessitates making a reference to the earlier block in order to construct a new one. Other nodes would reject a publishing node's request if it lacked a reference to the most recent block.

3.6 Blocks and Blockchain

Blockchain network users utilize software to propose potential transactions to the blockchain network via desktop applications, smartphone applications, digital wallets, web services, etc. These transactions are sent by the program to a node or nodes in the blockchain network. Both publishing and non-publishing complete nodes may be selected as nodes. The submitted transactions are subsequently sent to the rest of the network's nodes, but this does not automatically add the transaction to the blockchain. A pending transaction must wait in a queue for many blockchain implementations after it has been disseminated to nodes before being published to the blockchain by a publishing node. When a publishing node publishes a block, transactions are added to the blockchain. Blocks are made up of block data and block header.

Genesis Block refers to the initial block that was produced. It includes information and a special hash. All blocks in a chain of blocks, with the exception of the Genesis block, use the previous block's hash to generate their own hash value, along with a timestamp and transactional information. For instance, if block 2 in a chain of 5 blocks is altered, the altered block's hash value invalidates the whole chain because the subsequent blocks no longer have valid hash values. As mentioned in section 3.1 blocks are hashed using the secure hashing algorithm-256 (SHA-256). Every time a new transaction is made or when it is necessary, miners will add new blocks to the chain.

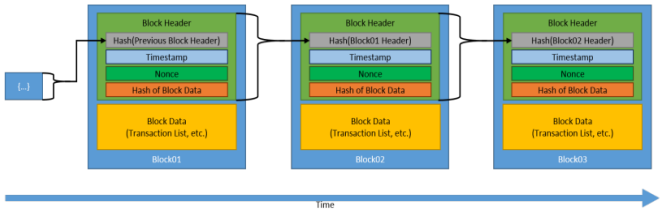

Fig – 3: Generic Chain of Blocks

4. Consensus Models

The selection of which user will publish the following block is a crucial component of blockchain technology. Implementing one of the numerous potential consensus models resolves this. There are typically numerous publishing nodes vying at once to publish the next block in permissionless blockchain networks. Typically, they engage in this behaviour to gain cryptocurrencies/transaction fees. They are often distrusting users who may only be acquainted through public addresses. Each publishing node is probably driven by the desire to make money, not by concern for the welfare of other publishing nodes or even the network as a whole. To settle disputes when many nodes publish a block at almost the same time, blockchain technologies employ consensus methods to allow a group of people that distrust one another to cooperate.

4.1 Proof of Work

The initial cryptographic consensus process, introduced by Bitcoin, is proof of work. Mining and proof of work are concepts that are connected. The network needs a lot of computing power, which is why it's dubbed "proof of work." By competing to be the first to solve a mathematical puzzle, virtual miners from all over the world protect and verify proof-of-work blockchains. The network rewards the winner with a fixed amount of cryptocurrency and allows them to update the blockchain with the most recent confirmed transactions.

Particularly for a very basic but extremely valuable cryptocurrency like Bitcoin, proof of work has several significant advantages (learn more about how Bitcoin works). It's a tried-and-true method for keeping a decentralized blockchain safe. As a cryptocurrency's value rises, more miners are motivated to join the network, boosting its strength and security. It becomes impossible for any person or organization to interfere with the blockchain of a valued cryptocurrency because to the amount of computing power required.

On the other hand, it's a resource-intensive process that would have difficulties scaling to handle the enormous volume of transactions that blockchains that support smart contracts, like Ethereum, can produce. Alternatives have been created as a result, with proof of stake being the most well-liked.

4.2 Proof of Stake

As Ethereum-powered decentralized finance (or DeFi) protocols have grown in popularity, the blockchain has found it difficult to keep up, which has resulted in fees increasing. This is because proof of work has scalability constraints that will ultimately need to be solved. The Ethereum blockchain also has to process a wide range of DeFi transactions, stablecoin smart contracts, NFT minting and sales, and whatever innovations developers come up with in the future, in contrast to the Bitcoin blockchain, which primarily just has to process incoming and outgoing bitcoin transactions, similar to a massive checkbook.

Staking in a proof of stake system performs a similar role to mining in a proof of work system, in that it selects a network participant to add the most recent batch of transactions to the blockchain and get cryptocurrency in return. The specifics vary depending on the project, but generally speaking proof of stake blockchains use a network of "validators" who donate — or "stake" — their own cryptocurrency in return for the opportunity to potentially verify new transactions, update the blockchain, and profit.

- The most invested players are practically rewarded since the network chooses a winner based on the amount of cryptocurrency each validator has in the pool and how long they have kept it there.

- Other validators can vouch for the accuracy of the most recent block of transactions after the winner has confirmed it. The blockchain is updated by the network once a predetermined amount of attestations have been made.

- A reward in the native cryptocurrency is given to all participating validators, and it is typically dispersed by the network in proportion to each validator's stake.

4.3 Round Robin

Some permissioned blockchain networks employ the round robin consensus approach. Nodes create blocks in this consensus model alternately. The history of Round Robin Consensus is rooted in distributed system architecture. These systems may incorporate a time restriction to allow available nodes to publish blocks so that unavailable nodes won't stop block publication in cases when a publishing node is not accessible to publish a block on its turn. With this architecture, it is made sure that no single node produces the bulk of the blocks. It offers the advantages of simplicity, absence of cryptographic difficulties, and low power consumption. Round robin does not function effectively on the permissionless blockchain networks used by the majority of cryptocurrencies since there has to be trust among nodes. This is due to the possibility that rogue nodes might constantly add new nodes to maximize their likelihood of publishing fresh blocks. In the worst case scenario, they may utilize this to obstruct the blockchain network's proper functioning.

4.4 Proof of Identity Consensus Model

The proof of identity model, also known as evidence of authority consensus approach, depends on publishing nodes' partial confidence due to their recognized connection to identities in the actual world. By way of identifying papers that have been authenticated, notarized, and added to the blockchain, publishing nodes must have their identities established and provable inside the blockchain network. The concept is that in order to publish new blocks, the publishing node must stake its reputation and identity. A publishing node's reputation is directly influenced by blockchain network users based on how that node behaves. Publishing nodes can win reputation by operating in a way that the users of the blockchain network agree with, but they can also lose reputation by doing the opposite. The chance of being able to publish a block decreases with reputation. Therefore, a publishing node has a stake in preserving its stellar reputation. Only permissioned blockchain networks with high degrees of trust are compatible with this algorithm.

4.5 Proof of Elapsed Time

Each publishing node in the proof of elapsed time (PoET) consensus architecture asks their computer system's secure hardware time source for a wait time. The publishing node software will get a random wait time that was generated by the secure hardware time source. The random time that publishing nodes are allotted is used during which they are idle. Any publishing node that is still dormant will cease waiting, the process will restart, and so on. When a publishing node awakens from its dormant condition, it generates and publishes a block to the blockchain network, informing the other nodes about the new block. Using this paradigm also necessitates confirming that the publishing node actually waited and did not begin early. Software running in a trusted execution environment, which is present on some computer processors, satisfies these conditions.

5. Forking

Even in the best of circumstances, making adjustments and updating technology may be challenging. It becomes very challenging for permissionless blockchain networks that have a large user base, are dispersed around the globe, and are regulated by user consensus. Forks are modifications to the protocol and data structures of a blockchain network. There are two types of them: soft forks and hard forks. These modifications for a soft fork are backwards compatible with nodes that have not received an upgrade. These modifications are not backwards compatible for a hard fork as non-updated nodes will not accept the modified blocks. As a result, the blockchain network may divide, resulting in numerous iterations of the same blockchain.

6. Conclusion

An existing network, cryptography, and recordkeeping technology is used in a novel way by a blockchain. It will be crucial for businesses to be able to evaluate technology and the benefits and drawbacks of utilizing them. When a blockchain is launched and extensively used, it could be challenging to update it. Even if a mistake is made, once data is entered into a blockchain, it often remains there indefinitely. By having newer blocks and transactions act as updates or modifications to previous blocks and transactions, applications that use the blockchain as a data layer get around the fact that the real blockchain data cannot be changed. Working data may be modified using this software abstraction, which also provides a complete history of changes. These characteristics are beneficial for some organizations. These can be deal-breakers for

certain people, hindering the adoption of blockchain technology. Blockchain technology is still in its infancy, therefore businesses should employ it only when necessary, just like they would any other technical option at their disposal.

REFERENCES

[1] Lamport, Leslie. "The Part-Time Parliament." ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998,pp.133–169. https://dl.acm.org/citation.cfm?doid=279227.279229

[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfed e, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[3] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

[4] M. D. Norman, M. T. Koehler, and R. Pitsko, "Applied complexity science: Enabling emergence through heuristics and simulations," Emergent Behavior in Complex Systems Engineering: A Modeling and Simulation Approach, pp. 201–226, 2018.

[5] National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[6] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions

[7] National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4

[8] 'Exodus', 2020. https://www.fxempire.com/crypto/wallets/exodus.

[9] 'Eidoo', 2017. https://www.cryptowisser.com/wallet/eidoo/

[10] 'Atomic Wallet Review', 2019. https://www.finder.com/in/atomicwallet-review

[11] Coinbase Exchange Review',2018. https://www.finder.com/in/coinbase-exchange-review.

[12] 'Gatehub', 2019. https://en.bitcoinwiki.org/wiki/GateHub

[13] Blockchain Wallet Review,2020. https://www.bestbitcoinexchange.io/wallets/blockchain/

[14] 'Edge Wallet Review', 2018. https://www.finder.com/edge-walletreview

[15] 'Coinomi Wallet Review', 2018. https://www.finder.com/in/coinomiwallet-review

[16] 'Enjin Smart Wallet', 2020. https://www.finder.com/enjin-smartwallet

[17] 'Abra Cryptocurrency Wallet', 2019. https://www.finder.com/abracryptocurrency-app.

[18] 'Keepkey Wallet Review', 2018. https://www.finder.com/in/keepkeywallet-review.

[19] Ledger Nano X', 2019. https://www.finder.com/ledger-nano-x.

[20] Cryptocurrency Wallet Types, 2017. https://www.binance.vision/blockchain/crypto-wallet-typesexplained

[21] 'Cryptocurrency Wallets', 2020. https://www.finder.com/in/cryptocurrency/wallets.

[22] Wikipedia contributors. (2022, July 21). General ledger. In Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=General_ledger&oldid=1099657994