***SINDH MADRESSATUL ISLAM UNIVERSITY***

Logo

Description automatically generated

***DEPARMENT: SOFTWARE ENGINEERING***

***SEMESTER/SECTION: 2(B)***

***ID: BSE-22S-084***

***SUBJECT: SOFTWARE ENGINEERING***

***COURSE CODE: SEN-102***

***SUBMIT TO: MS. WAJEEHA NAIM***

***SUBMIT BY: MUHAMMAD MUBASHIR***

**INTRODUCTION**

Blockchains are distributed digital ledgers that are impenetrable and immune to tampering, generally operating without a central repository or authority (i.e., a bank, company or government). At their most basic level, they allow a user community to record transactions in a shared ledger inside that user community, ensuring that no transaction can be modified after it has been published under standard blockchain network operation. Modern cryptocurrencies, or electronic cash secured by cryptographic processes rather than a central repository or authority, were developed in 2008 by combining the blockchain concept with a number of other technologies and computer ideas..

With the introduction of the first of several contemporary cryptocurrencies, the Bitcoin network, this technology gained widespread recognition in 2009. The transfer of digital data that serves as electronic cash occurs in a distributed system in Bitcoin and other systems comparable to it. Users of Bitcoin may digitally sign and transfer their ownership of that information to another user, and the Bitcoin blockchain publicly records this transfer, enabling all users of the network to independently confirm the transactions' legitimacy. A dispersed network of people independently maintains and manages the Bitcoin blockchain.Because of this and cryptographic procedures, the blockchain is resistant to later efforts to change the ledger (modifying blocks or forging transactions). Bitcoin and Ethereum are only two of the cryptocurrency systems that have been made possible by blockchain technology1. Blockchain technology is frequently thought of as being tied to Bitcoin or maybe cryptocurrency solutions in general as a result. However, the technology has a wider range of uses and is being researched for a number of industries.

The numerous components of blockchain technology along with its reliance on cryptographic primitives and distributed systems can make it challenging to understand. However, each component can be described simply and used as a building block to understand the larger complex system. Blockchains can be informally defined as:

Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance).

It can be difficult to comprehend blockchain technology due to its complexity, reliance on distributed networks, and use of cryptographic primitives. However, it is possible to grasp the more intricate overall system by using a straightforward description of each component. Informally, blockchains may be described as:

Blockchains are decentralised digital ledgers that include blocks of cryptographically signed transactions. Following validation and a consensus decision, each block is cryptographically connected to the preceding one (making it tamper obvious). Older blocks become increasingly challenging to change when new blocks are added (creating tamper resistance).The network's copies of the ledger are updated with the latest blocks, and any disputes are automatically handled according to predetermined rules.

**Purpose and Scope**

A high-level technical overview of blockchain technology is given in this document. It examines many subcategories of implementation strategies. It goes over the elements of blockchain technology and, when appropriate, includes illustrations and examples. A few of the consensus models utilised in blockchain networks are briefly discussed. It also gives a general understanding of how forking, or modifications to blockchain technology, effect the blockchain network. It gives information on how the attestable application procedures known as smart contracts were added to the blockchain technology beyond attestable transactions. It also discusses some of the restrictions and myths related to the technology.Finally, this article lists a number of factors that businesses should think about while researching blockchain technology. Its goal is to make readers more knowledgeable about the technologies that make up blockchain networks.

**Notes on Terms**

Blockchain terminology differs from implementation to implementation, hence while discussing the technology, general phrases will be utilised. The following terminology will be used in this document:**Blockchain – the actual**

**Ledger**

Blockchain technology is the most general word used to describe the technology.

The network in which a blockchain is utilised is known as the blockchain network.

implementation of a certain blockchain

A user of the blockchain network is anybody who makes use of it, including individuals, businesses, governments, and other entities.

A node is a single system that is part of a blockchain network.

The term "full node" refers to a node that holds the whole blockchain and verifies transactions.

A complete node that additionally publishes new blocks is a publishing node.

A lightweight node is a node that must pass transactions but does not keep or maintain a copy of the blockchain.to full.

**Blockchain Components**

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) (such as append only ledgers). Each major component is covered in detail in this part, including transactions, asymmetric-key cryptography, addresses, ledgers, blocks, and chaining of blocks.

**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.

**Cryptographic hash functions have these important security properties:**

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.

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 only method that works is to thoroughly search the inputHowever, doing it computationally in a way that has any chance of success is impossible.

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 utilised in several blockchain implementations (SHA-256). This technique is hardware supported on many systems, which speeds up computation.The result of SHA-256 is 32 bytes (1 byte equals 8 bits, 32 bytes equal 256 bits), which is often shown as a 64-character hexadecimal string.

**Asymmetric-Key Cryptography**

BAsymmetric-key cryptography is used by lockchain technology (also referred to as public key cryptography). 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 jeopardising 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.

In order to establish a trust relationship between users who do not already know or trust one another, asymmetric-key cryptography offers a way to check the authenticity and integrity of transactions while still enabling them to be made public. The transactions are "digitally signed" to do this. This implies that a transaction is encrypted using a private key so that it can be decrypted by anybody who has access to the public key. Encrypting the transaction using the private key demonstrates that the transaction's signer has access to the private key because the public key is publicly accessible A user's public key can also be used to encrypt data, making it so that only anyone with access to the user's private key can decode it. 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. Therefore, when one declares to be When encrypting anything with asymmetric-key cryptography, the data is frequently first encrypted with symmetric-key cryptography before the symmetric-key is encrypted. Asymmetric-key cryptography can be significantly sped up with this "trick."

The application of asymmetric-key cryptography in various blockchain networks is summarised as follows:

Transactions are digitally signed using private keys.

Addresses are derived using public keys.

Signatures created using private keys are verified using public keys.

Asymmetric-key cryptography makes it possible to confirm that the user sending money to another user actually has the private key required to sign the transaction.

**Private Key Storage**

Users may need to maintain and safely keep their own private keys on some blockchain networks (particularly permissionless blockchain networks). They frequently utilise software to safely save them instead of physically storing them. This programme 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 specialised 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 can also comply with KYC regulations.users Users who want to create an account must present identification documentation.

Blockchain technology's private key storage is a crucial component. When "Cryptocurrency XYZ was stolen from..." is mentioned in the press, it almost usually refers to certain private keys that were discovered and used to sign a transaction transferring the funds to a new account, rather than a security breach affecting the blockchain network as a whole. It should be noted that because blockchain data is often immutable, a criminal operation that involves stealing a private key and publicly transferring the corresponding cash to another account is typically irreversible.

**Ledgers**

An assortment of transactions make up a ledger. Pen and paper ledgers have been used to record the transaction of commodities and services throughout history. Modern ledgers are kept digitally, sometimes in sizable databases that are managed by a centralised trustworthy third party (the owner of the ledger) on behalf of a user community. These centralised ownership ledgers can be deployed either centralised or decentralised (i.e., just one server or a coordinating cluster of servers).

Exploring distributed ownership of the ledger is becoming more popular. 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 centralised ownership, there is rising interest in distributed ownership of ledgers.

Users must have faith that the owner is adequately backing up the system since centrally owned ledgers might be lost or destroyed.

A blockchain network is distributed by design, producing several backup copies of the same ledger data that are updated and synced across peers. A fundamental benefit to blockchain technology is that every user may retain their own copy of the ledger. It is challenging 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.

Note that certain blockchain implementations have the capacity to handle ideas like private channels or transactions. Only the nodes involved in the transaction can get information thanks to private transactions, not the entire network.

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.

Centrally held ledgers may be wholly located in a particular region (e.g., all in one country). The ledger and any services that rely on it could not be available if there were network issues there.

A blockchain network can be made up of nodes spread around the globe that are geographically varied. The blockchain network is robust to the loss of any node, or even an entire region of nodes, as a result of this and the peer-to-peer nature of how it operates.

On a centrally held ledger, transactions are not created publicly and may not be authentic; a user must have faith that the owner is authenticating each transaction they receive.

In order to prevent invalid transactions from spreading throughout the blockchain network, a blockchain network must verify that all transactions are genuine. If a malicious node were to send erroneous entries, the others would notice and reject them.

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.

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 uses cryptographic techniques including digital signatures and cryptographic hash functions.

A user must believe that the related computer systems and networks have applied best practises for security and are getting important security fixes even when the centrally owned system may not be safe. Due to security flaws, the system may have been hacked and user information taken.Due to its distributed architecture, a blockchain network does not offer a single point of attack. In general, data on a blockchain network may be viewed by anybody and presents no opportunities for theft. to undermine blockchain

An attacker would have to specifically target each network user. The system's honest nodes would fight back against attempts to attack the blockchain itself. If a certain node was not patched, it would only have an impact on that node and not the entire system.

Blockchain network users utilise software to propose potential transactions to the blockchain network (desktop applications, smartphone applications, digital wallets, web services, etc.). These transactions are sent by the programme to a node or nodes in the blockchain network. Both publishing and non-publishing complete nodes may be selected as nodes. The sent transactions are subsequently transmitted to the rest of the network's nodes, although this does not, by itself, add the transaction to the blockchain. Once a pending transaction has been transmitted to nodes for various blockchain implementations, it must then wait in a queue until it is added 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. Metadata for this block is contained in the block header. A list of verified and genuine transactions that have been uploaded to the blockchain network may be seen in the block data. By ensuring that the transaction is constructed appropriately and that all suppliers of digital assets (specified in the transaction's "input" values) have cryptographically signed the transaction, validity and authenticity are guaranteed.This demonstrates that the individuals who provided the digital assets for a transaction had access to the private key that could sign the assets that were made accessible. All transactions in a published block will be examined for authenticity and validity by the other full nodes, and any blocks with invalid transactions will not be accepted.

Although each blockchain implementation is free to create its own data fields, many of them use data fields like the ones listed below:

**Block Header**

In certain blockchain networks, the block number is also referred to as the block height.

The hash value of the preceding block header.

a hash representation of the block data (this may be done using a number of various techniques, such as creating a Merkle tree and saving the root hash or using a hash of all the combined block data; see Appendix B for further information).

an epoch.

the block's dimensions.

the worth of a nonce. This is a number that is changed by the publishing node in blockchain networks that use mining to solve the hash problem. There may or may not be further blockchain networks that it or apply it to something other than a hash problem.

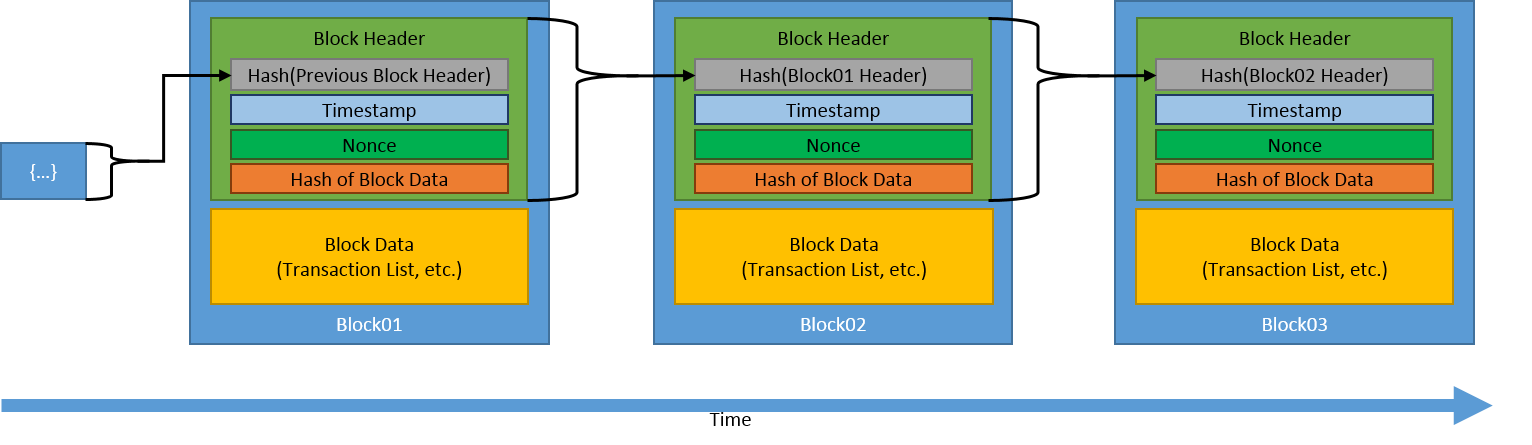
**Block Data**

a rundown of the block's transactions and ledger events.

There could be further data.

**Chaining Blocks**

The blockchain is created by chaining together blocks and storing the hash digest of each block's header in the subsequent block. A previously published block would have a different hash if it were altered. Due to the fact that all following blocks contain the hash of the preceding block, this would result in all consecutive blocks having different hashes. This enables quick detection and rejection of changed blocks. A general chain of blocks is shown Figure



**Generic Chain of Blocks**

**Ledger Conflicts and Resolutions**

As was previously mentioned, it is conceivable for some blockchain networks for several blocks to be broadcast at or around the same time. This might result in different blockchains existing at any given time; these issues need to be rapidly handled to maintain consistency throughout the blockchain network. We go through how these problems are often addressed in this section.

Any dispersed network will have some systems that are behind on information or have different information. Network latency between nodes and the closeness of node groups have a role in this. Due to its openness and abundance of competing publishing nodes, permissionless blockchain networks are more likely to have disputes. Solving data conflicts is a key component of reaching consensus on the status of the blockchain network.

For example:

Block n(A) is created by node A using transactions #1, #2, and #3 before being distributed to some nodes.

Block n(B) is created by node B using transactions #1, #2, and #4 before being sent to some nodes.

There is a disagreement.

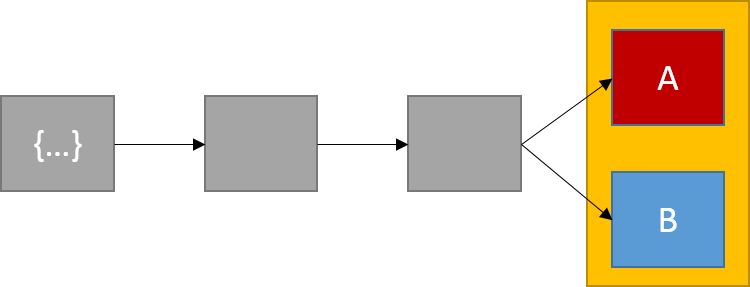
There will be variations in block n across the network.

Transaction #4 is absent from block n(A), while transaction #3 is there.

Transaction #3 is absent from block n(B), yet transaction #4 is there.

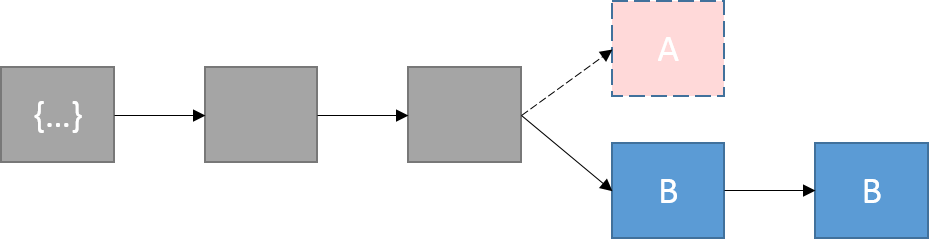
Conflicts momentarily result in several blockchain versions, as shown in Figure.

These many versions were produced using the information that was accessible to each node, not because they are "wrong." People who have block n(A) may observe transfers of digital assets that are absent from block n because the competing blocks are likely to include different transactions (B). Depending on whatever version of the blockchain is being examined, some bitcoin may be both spent and unspent if the blockchain network interacts with cryptocurrencies.



**Ledger in Conflict**

Conflicts are often settled swiftly. The majority of blockchain networks will embrace the "longer blockchain" by waiting until the following block is published and using that chain as the "official" blockchain. Because it received the next legitimate block, as shown in Figure 5, the blockchain containing block n(B) becomes the "official" chain. Any transaction that was a part of the orphaned block block n(A) but not the chain block n(B) is returned to the pending transaction pool (which is where all transactions which have not been included within a block reside). Keep in mind that each node maintains this list of pending transactions locally as The design lacks a central server.



The chain with block n(A) becomes orphaned when the chain with block n(B) adds the subsequent block.

A transaction is often not regarded as confirmed until many more blocks have been constructed on top of the block containing the relevant transaction due to the danger of blocks being overwritten. Since blocks can be replaced, the acceptance of a block is frequently probabilistic rather than deterministic. The likelihood that the first block won't be overwritten increases with the number of blocks that have been added on top of a published block.

Theoretically, a node in a proof of work blockchain network might start at the genesis block and generate a chain that is longer than the one that already exists, wiping away the whole blockchain history. Due of the excessively high number of resources needed, this does not really occur. In order to prevent this from ever happening, some blockchain implementations lock down select older blocks inside the blockchain software..

**CONCLUSION**

A new tool with significant uses for businesses is blockchain technology, which enables safe transactions without the need for a centralised authority. There have been a rising number of blockchain technology-based solutions since Bitcoin first used it in 200913.

The initial uses were electronic currency systems that disseminated a worldwide ledger of all transactions. These transactions are protected by cryptographic hashes, and asymmetric-key pairs are used to sign and validate transactions. A series of events are effectively and securely recorded in the transaction history in a way that Any effort to modify or alter a previous transaction necessitates recalculating all succeeding blocks of transactions as well.

Although it is still in its infancy, blockchain technology is based on strong and widely accepted cryptographic concepts. The technology is now the subject of a lot of excitement and has several potential applications. The euphoria around blockchain technology is expected to fade in the future, making it simply another tool available for usage.

A blockchain depends on already-existing network, cryptography, and recordkeeping technology but employs them in a novel way, as explained throughout this article. It will be crucial for businesses to be able to evaluate technology and the benefits and drawbacks of utilising them. When a blockchain ais 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. Blockchain-based applications that act as a data layer circumvent the inability of later blocks and transactions to update or modify older blocks and transactions so that the real blockchain data cannot be changed. This software abstraction provides a complete history of changes while allowing alterations to working data. These qualities are appealing to certain organisations. Others could view these as deal-breakers that hinder the use of blockchain technology.

Blockchain technology is still in its infancy, so businesses should handle it like they would any other technical tool at their disposal and only apply it where it is necessary.

# *THANK YO*