Impregnable Communication Ideology Based on Blockchain and Cryptanalysis

Sarvesh Sutej Labdhe[1], Sneha.R[2], Sumaiya[3] , Shivani Kamboj[4]

[123] Bachelor of Engineering, Department of Computer Science and Engineering & Brindavan College Of Engineering, Bengaluru, Karnataka, India
[4] Professor, Department of Computer Science and Engineering & Brindavan College Of Engineering, Bengaluru, Karnataka, India

---***---

Abstract - By overcoming these risks and enabling decentralization of critical activities while maintaining a high level of security, the blockchain is a cutting-edge technology. It does away with the necessity for reliable middlemen. Our project's objective is to suggest a blockchain-based secure communications solution. In this project, we discuss how blockchain technology could increase the security of communications while maintaining messaging performance and security, utilizing a smart contract to confirm identities and their associated public keys, and validating the user's certificate using digital signatures and blockchain technology. The system is a complete amalgamation of blockchain technology with cryptography for message verification using a variety of cryptographic techniques.

Key Words: Blockchain, Cryptography, RSA, Hashlib, ECDSA, Signing key, Verifying key, Secp256k1.

1.INTRODUCTION

Blockchain is a distributed database with qualities such as decentralization, traceability, immutability, security, and dependability. Peer-to-peer (P2P) technology, digital encryption technology, consensus technology, smart contracts, and other technologies are all integrated into it. abandoning the conventional central node's maintenance mode and switching to a system of mutual upkeep between users in order to achieve information supervision among numerous parties and protect the accuracy and integrity of the data. Public chain, private chain, and alliance chain are three subcategories of the blockchain platform. The most popular use of blockchain is with Bitcoin, which was first introduced by Nakamoto in 2008 and is also the most successful example of a digital money. Additionally, the blockchain has demonstrated its ability to change the world and increased the value of its unique applications in many areas. It is clear that the blockchain places the most emphasis on cryptographic technologies. It is obvious that the blockchain gives cryptography technology the greatest attention.

Cryptography technology is primarily employed in blockchain to safeguard data integrity, user privacy, and transaction information. The hash algorithm, asymmetric encryption algorithm, and digital signature are a few of the cryptographic techniques that are briefly introduced in this paper. It also elaborates on the blockchain infrastructure, the blockchain structure, bitcoin addresses, digital currency trading, and other blockchain technologies, and it explains in detail how cryptography technology protects privacy and transaction maintenance in the blockchain. To maintain the integrity of data storage, the data layer mostly employs the block data structure. Each node in the network stores the data transactions it has received over time in a block of time-stamped data that is linked to the longest primary blockchain at the moment.

In order to prevent a third party from accessing and learning the information from the private messages sent during a communication process, cryptography is a means of building procedures and protocols. Kryptos and Graphene, two words from ancient Greek that originally meant "to write" and "hide," respectively, also make up the name "cryptography." By definition, it is a strategy for creating protocols and rules to prohibit a third party from accessing and learning the information from the private communications while a conversation is taking place. These are some of the terms that are connected to cryptography:

Encryption: Encryption is the conversion of plaintext (regular text) into ciphertext (random bits).

Key: The cryptographic algorithm's result can be induced with a minimal quantity of information.

Decryption: Decryption is the process of turning plaintext into ciphertext, which is the opposite of encryption.

Cipher: A cryptographic technique or mathematical function that transforms plaintext into ciphertext.

The blockchain benefits from cryptographic hash functions in the following ways: A little modification in the data might produce a noticeably different outcome, which is known as the "avalanche effect."

Uniqueness - i.e., each input results in a different outcome.

Deterministic - meaning that if the same hash function is used on any input, the result will always be the same.

Rapidity – The production may be produced in a relatively little period of time.

It is not feasible to reverse engineer, meaning that we cannot create the input from the output and hash function.

1.1 Blockchain Framework

Blockchain technology, according to Melanie Swan, founder of the Blockchain Science Institute, has gone through two stages. The first is the blockchain 1.0 phase, which is represented by Bitcoin and is a multi-technology portfolio innovation. The second is the blockchain 2.0 phase, which is represented by Ethereum and is a transfer of digital assets. Blockchain technology is typically used for things like Bitcoin, Ethereum, Hyper Ledgers, etc. The underlying design shares a lot of similarities even though the implementations vary. To maintain the integrity of data storage, the data layer mostly employs the block data structure. Each node in the network stores the data transactions it has received over time in a block of time-stamped data that is linked to the longest primary blockchain at the moment.

The primary component of the consensus layer is a consensus mechanism that enables every node in the decentralized system to agree on the veracity of block data. Pow, Pos, PBFT, and SBFT make up the majority of the consensus process. The foundation of the blockchain programmable feature is the smart contract, which is primarily present in the contract layer. The blockchain stores code and data sets that make up the computer programme that can automatically carry out the conditions of the contract. Blockchain nodes spread the distributed execution of smart contracts that are triggered by time or events. Signatures or other external data messages activate the coding, automated settlement, and triggering of all pertinent clauses. Different data transmission protocols and verification techniques are included in the network layer. The blockchain's P2P protocol is primarily used to transfer data between nodes. The major components of the application layer are Hyperledger, Ethereum, and Bitcoin. Bitcoin is mostly used for digital money exchanges. Decentralized apps based on digital money are added by Ethereum. Transactions involving digital currencies, primarily enterprise-level blockchain applications, are not supported by Hyperledger.

1.2 Hash and block structure structure

The hash algorithm is a function that reduces a string of any length messages to a shorter fixed-length value. It is characterized by susceptibility, unidirectionality, collision resistance, and high sensitivity. Hash is typically used to ensure data integrity, or to confirm that the data has not been improperly altered. The hash value of the tested data adjusts as the data changes. As a result, even in a dangerous setting, the integrity of the data may be determined using its hash value. The National Institute of Standards and Technology (NIST) released the cryptographic hash function known as SHA, which possesses the fundamental properties of a cryptographic hash function. A subset of the SHA-2 algorithm cluster is the SHA256 algorithm. The two steps of the algorithm's computation procedure are the main loop and message pre-processing. The information of any length is subjected to binary bit filling and message length filling during the message pre-processing step, and the filled message is then separated into several 512-bit message blocks. Each message block is handled by a compression function during the main loop phase. The output of the previous compression function serves as the input for the current compression process, while the original message's hash value serves as the output of the previous compression function. The COSI research team at the University of Leuven in Belgium created the hash function algorithm known as RIEPEMD, which is a summary of the RACE original integrity check message. The most often used RIPEMD variant is RIPEMD-160. Message complement is the initial stage of the algorithm, and the complement technique is the same as the SHA series algorithm. The compression function, which is a loop with 16 step functions inside each loop, forms the basis of the processing algorithm. The processing of the method is split into two separate instances using different original logic functions in each loop, with five of the two original logic functions executing in reverse order. Once the 512-bit packet processing is finished, the original message's hash value is produced as a 160-bit output. Hash functions may be used for blockchain to perform block and transaction integrity checks. Any user may compare the computed hash value with the stored hash value in the blockchain since the hash value of the data from the previous block is stored in the header of each block. The information in the previous block is then checked for integrity. Public-private key pairs can also be created using the hash function.

1.3 Digital Content Protection

Wu et al. suggested a method that ensures the validity and non-repudiation of digital material in order to protect the privacy for traceable encryption in blockchain. The issue addressed by the authors is the user's private key, which, when shared with other entities, does not hold the user's particular information. It is challenging to determine the origin of the secPret key in the event that the shared key is damaged or misused. Moreover, a bottleneck for current systems is the leakage of private data in access control. In order to safeguard the secret keys, writers have implemented the privacy protection method such as attribute-based encryption (ABE). The decryption process, however, does not demonstrate increased effectiveness. Trust and decentralization. The decryption process, however, does not demonstrate increased effectiveness. To ensure digital data protection, management of data rights is a crucial prerequisite. Transparency, decentralization, and trust are lacking in currently used data rights strategies. Zhang and Zhao presented decentralized blockchain based solutions to the aforementioned issues. Everyone has access to information on the usage of digital content, including transaction and license details. Smart contracts are made to automatically assign licenses. The owner can decide the rates for selling the license to other consumers under this system. However, in order to perform key acquisition, network peers must have powerful computers.

2. LITERATURE SURVEY

2.1 Blockchain-enabled wireless communications: a new paradigm towards 6G

Blockchain is a distributed ledger that is a chain of linked blocks, with each block containing aggregated data that records a list of digital activities (such as transactions or smart contracts) over time. Blockchain is a public database that is maintained by all active nodes in a peer-to-peer (P2P) network. Each block is recognised by a hash value, and each block is connected to the previous block by a hash pointer, meaning that each block holds the preceding block's hash. Any alteration to the data in a block destroys the links created by the hash pointers due to a mathematical property of hash functions. As a result, every new block that is produced secures its predecessors as a confirmation. A block with more confirmations is typically more difficult to undermine. Blockchain miners, sometimes referred to as “mining,” are responsible for validating digital transactions and assembling them into blocks at the top of the chain. Blockchains may be categorized in two ways, according to data management strategies: public/private and permissionless/permissioned. The authentication process, or who has access to the blockchain, is the primary distinction between public and private blockchains .In general, anybody may join a public blockchain, but access to a private blockchain is controlled by the blockchain's owners. On the other hand, who is authorised to alter the blockchain is where the primary distinction between permissioned and permissionless blockchains lies. In contrast to authorised users, anyone can typically update data in a blockchain with permissionless technology.

2.2 A Study of Blockchain-Based Cryptosystems with and without a Software Defined Network

Blockchain draws a broad variety of APIs since it is a foundational technology, which helps to ensure safe data hand over throughout the network. The research covers a variety of topics, including how to use block chains to avoid abuse and corruption in the interchange of huge volumes of data produced by databases for commercial software, safety, and law. The suggested system offers dependability and trust in data exchange across communication channels by using the block chain and the RSA digital signature technique. The study done for this essay indicates that the most important problems in the modern world are data visibility and consistency. Reputation systems are the most effective solution to this enormous problem. In certain systems, automation and granularity are both absent. The trust chain is a three-layered architecture that employs consortium blockchain standards to log transactions, as detailed in this article. Scores on reputation are also crucial for improved performance. In this work, resource tracing was investigated on both a permissioned and a permissionless blockchain. On the permissioned blockchain, they define and elucidate the provenance of goods. We make an effort to provide a thorough analysis of all recent research trends that have been carried out to assess the effectiveness of blockchain technology when combined with different cryptosystem standards in the network area and other models. suggests that identity, privacy, and exchange security are the three main issues with information security. Block-chain technology's key characteristics are data openness, intensification of change, and fine-grained access to data information. This technology is intended for data-operational enterprises that deal with enormous volumes of sensitive data and are frequently targeted by hackers.

2.3 Secure Peer-to-Peer communication based on Blockchain

The objective is to protect network entities' communications. The goal is to utilize the blockchain to verify each user's identity and maintain user trust so that communications may be sent with the highest level of security possible. Each user must only engage with other users whose identities have been verified by a smart contract and must see all other interactions as harmful .Each user who wishes to communicate with others through the system must register their identity and public key and store it on the blockchain. We can utilise the smart contract-enabled Ethereum public blockchain to create such a system. Up to 200,000 people are currently working on the Ethereum network's protocol and related projects, ensuring that the protocol is secure and keeps up with technological advances. In our approach, the most popular notations are listed. The smart contract can begin to function as planned after the code conditions have been verified. In order to carry out this execution, a certain transaction must be sent to the blockchain, which triggers the smart contract to be executed. A blockchain is simply a distributed database that can withstand errors that contains information from a public ledger of all transactions that have been carried out and disseminated among involved parties.A majority of the system's users agree to confirm each transaction in the public ledger. By combining cryptography and consensus, blockchain offers a mechanism for improving data integrity. As a result, there is no single point of control for all servers. The data is organized into blocks, each of which is encrypted and contains transactions, a timestamp, and a link to the block before it. The history of each transaction done in the past is the shared data in blockchain. On a network of computers, referred to as nodes, the ledger is kept in many copies. The nodes verify whether a transaction is legitimate each time it is sent to the ledger. A new timestamp will be recorded when the transaction is produced in the chained data structure of blockchain, and any modifications to previously created data will no longer be permitted.

2.4 Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher

A new method has been Introduced in this paper as Vigenère Cypher, it uses punctuation such as colons, commas, semicolons, question marks, underlines, full stops, and brackets as the key rather than individual characters to make it harder for attacks and assaults, both active and passive. Literate people who are familiar with the fundamentals of cryptography can decipher the message. Due to its vast user base and open architecture, the internet is mentioned as one of the riskiest communication channels. One of the fundamental parametric requirements is data assurance. Various security algorithms are currently being proposed to achieve security during communication. Each of them has some true claims and some false ones that they are trying to make in order to achieve security during communication. The systematic method of using cryptography to conceal data and information through a communication channel. To conceal the info from outsiders takes skill. The requirement for data security over the communication channel increases significantly as innovation progresses. The process of systematically converting plain message text into ciphertext is known as encryption. To convert plain message text into cypher, encryption requires a key and any specified encryption method. The message sender side of the cryptography system is where encryption is executed. Prior to being sent to the recipient, the message is encrypted at the sender's end. . The systematic opposite of encryption is decryption. It converts the message's plaintext from the encrypted ciphertext. In cryptography, the receiver side is where the decryption process is carried out. A key and a decryption algorithm are two steps needed in the decryption algorithm process. Asymmetric and symmetric key encryption are two options. A same key is used for both encryption and decryption in symmetric key encryption.

2.5 Research on the Application of Cryptography on the Blockchain

Blockchain is a distributed database with characteristics like decentralization, traceability, immutability, security, and dependability. Peer-to-peer (P2P) technology, digital encryption technology, consensus technology, smart contracts, and other technologies are all integrated into it. Blockchain technology has been divided two stages. The first is the blockchain 1.0 phase, which is represented by Bitcoin and is a multi-technology portfolio innovation. The second is the blockchain 2.0 phase, which is represented by Ethereum and is transmitted by digital assets. Known for its susceptibility, unidirectionality, collision resistance, and high sensitivity, the hash algorithm is a function that reduces a string of messages of arbitrary length to a shorter fixed-length value. Hash is typically used to ensure data integrity, or to confirm that the data has not been improperly altered. The hash value of the tested data adjusts as the data changes. Therefore, based on the data's hash value, the integrity of the data can be determined even when it is in a risky environment. The National Institute of Standards and Technology (NIST) released the cryptographic hash function known as SHA, which possesses the fundamental properties of a cryptographic hash function. The SHA256 algorithm creates 256-bit messages and is a subset of the SHA-2 algorithm cluster. Symmetric encryption and asymmetric encryption are two of the fundamental cryptographic techniques. The issue of early key distribution in symmetric encryption can be effectively resolved by asymmetric encryption, often known as public key encryption. The encryption key and the decryption key in an asymmetric encryption technique are distinct and are referred to as a public key and a private key, respectively. The public key is calculated using an irreversible process, whereas the private key is often obtained using a random number technique. Separate public and private keys are an advantage of the asymmetric encryption algorithm.

2.6 Provably Secure Covert Communication on Blockchain

Covert channels of communication are intended to safeguard the relationship between the transmitter and the receiver by disguising the fact that secret communication is even occurring. Steganography and cryptography can be used in conjunction to provide secure covert communication. While steganography is used to conceal the fact that there is encrypted communication, cryptography ensures that the message being communicated remains private. Steganography, however, needs a medium. It is necessary that both the transmitter and the receiver have access to a channel where harmless communication is occurring. The channel must also be dependable for the recipient to receive the broadcast message with a high degree of probability and without any manipulation. In this work, we offer a technique. method transmitting secret communications via a blockchain regarded as a payment platform. The sender's ability to embed into the blockchain is constrained by its immutability. We use those payments to send encrypted messages to a receiver, while everyone is allowed to add payments to the chain. We begin by offering a simplified ideal blockchain model for the blockchain that abstracts away unimportant technological aspects. Following this model, we then developed BLOCCE, a method for reliably embedding and extracting data into a blockchain. By submitting payments, we demonstrate the reliability of the method and demonstrate that it runs in expected polynomial time, excluding the time required to wait for new blocks to join the chain. We next provide a notion of safe covert communication on a blockchain based on the difficulty of differentiating the payload containing payments from random payments, based on the proved security of Steg systems. Finally, we demonstrate that our approach adheres to this definition. The blockchain technology was created to increase the reliability of the transaction.

3. PROPOSED SYSTEM

3.1 Objective

All of the user data is kept in our application on a block that is linked to other blocks to build a chain. A decentralized application lacks a centralized server, as the name indicates. Essentially, it is a peer-to-peer network. Additionally, due to the use of a 256-bit hashing function and a very secure encryption, it is nearly impossible to view the data that is stored in a block. Additionally, if a hacker tries to change the data in a block, he or she will need to change all of the copies of that block across the entire blockchain network, which can be very difficult. Despite being on all nodes, the information in the block cannot be accessed by anyone other than the person for whom it is intended.

3.2 Methodology

Initially, we are going to use blockchain to generate the hash key and block no for each of the block and then the user enters the message here simultaneously we are going to use cryptography algorithm and encrypt the message given by the user and then we append earlier generated hash key with the encrypted message and then we send It to recipient, in order to get the message, the recipient need to decrypt the message using key and after than we get original message. And later we compare the message on the both end (user message with the Recipient message) whether they are matched or not, if the message is matched it will display a text as Message Matched else Message is not matched this process ins call digital signature.

3.3 Hashlib

A unified interface to several secure hash and message digest methods is implemented by this module. Included are the RSA MD5 algorithm (described in internet RFC 1321) and the FIPS secure hash algorithms SHA1, SHA224, SHA256, SHA384, and SHA512 (specified in FIPS 180-2). The words "message digest" and "secure hash" are equivalent. Message digests were the name given to older algorithms. Secure hash is the current phrase. Each type of hash has a designated constructor method. All of them provide a hash object with a straightforward interface. For instance, use the sha256() function to create a SHA-256 hash object.. The update () function now allows you to supply this object with bytes-like objects (often bytes). You may use the digest () or hex digest () methods to ask it for the digest of the concatenation of the data you have already given it.

3.4 RSA

Asymmetric cryptography uses the RSA algorithm. Asymmetric actually refers to the fact that it use both a public key and a private key. The private key is kept secret, as suggested by the name, whereas the public key is made available to everyone.The concept of RSA is based on the fact that big integers are hard to factor. The public key is made up of two numbers, one of which is the product of two enormous prime numbers. The same two prime numbers are also used to create the private key. Therefore, the private key is compromised if someone is able to factories the large number. Therefore, the key size completely determines encryption strength, and doubling or tripling the key size significantly boosts encryption strength. RSA keys are frequently 1024 or 2048 bits large, however experts predict that 1024-bit keys will soon be broken. But as of right now, it appears to be an impossible task. As a result, the key size completely determines how strong an encryption is, and if we double or treble the key size, the strength of encryption improves dramatically. RSA keys may normally be 1024 or 2048 bits long, but experts think that 1024-bit keys may soon be cracked. However, it appears to be an impossible task at this time.

3.5 ECDSA

Elliptic curve cryptography keys are used by the Elliptic Curve Digital Signature Algorithm, a Digital Signature Algorithm (DSA). It is a very effective equation that is based on public-key cryptography. ECDSA is the cornerstone of Bitcoin security (with Bitcoin "addresses" acting as public keys), is used in several security systems, and is widely used in encrypted messaging apps. With the use of a digital signature, which serves as the handwritten signature's electronic equivalent, a recipient can persuade a third party that a message was in fact sent by the intended recipient. Compared to digital signatures, handwritten signatures are much less secure. ECDSA is the foundation of Bitcoin security (with Bitcoin "addresses" acting as public keys), is widely utilized in encrypted messaging apps, and is used in many other security systems. Also employed for Transport Layer is ECDSA. A digital signature cannot in any manner be faked. The fact that they apply to the entire message gives digital signatures another benefit over handwritten ones. The signature key has an impact on every aspect of the digital communication. The application of a handwritten signature to the bottom of a paper document. Nothing prevents the text that appears above the scribbled signature from being changed as long as the signature itself stays the same. Such modifications are not permitted with digital signatures. A mathematical problem that is the basis of their security may be used to categories the various digital signature techniques used today.

3.6 Signing Key

The private key utilized in a digital signature is known as the signing key. As opposed to the verification key. See also public key cryptography and digital signatures.

3.7 Verifying Key

The public key utilized in a digital signature is the verification key. Unlike the signing key. see public key cryptography and digital signatures.

3.8 Secp256k1

The elliptic curve used by Bitcoin to achieve its public key cryptography is known as Secp256k1. Valid Bitcoin public keys can be found at any point on this curve. A user multiplies their private key, which is a huge number, by the Generator Point, which is a predetermined point on the secp256k1 curve, in order to produce a public key using their private key. A public key cannot be converted to a private key by dividing it by the Generator Point due to the Discrete Log Problem. Every elliptic curve is an equation that follows the same template: y2 = x3 + axe + b. Specifically for secp256k1, a = 0 and b = 7, resulting in the equation y2 = x3 + 7. Secp256k1 is symmetric across the x-axis because the y component of the equation is squared, and for any value of x, there are two values of y, one of which is odd and the other is even. This reduces the amount of data needed to identify public keys on the blockchain to only the x-coordinate and the parity of the y-coordinate.

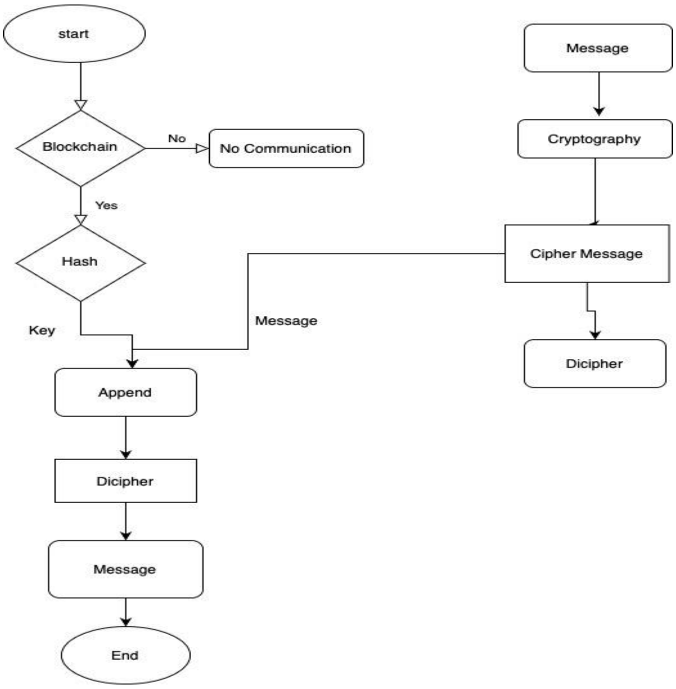
3.9 System Architecture

A system's structure, behaviour, and other aspects are all defined by its conceptual model, or system architecture. A formal description and representation of a system that is set up to facilitate analysis of its structures and behaviour is called an architectural description. A system architecture can be made up of designed subsystems and system components that will cooperate to construct the whole system. The architectural description languages (ADLs) collectively refer to efforts to formalize languages that describe system architecture.

Hash Value: Hash values may be compared to file fingerprints. A cryptographic technique is used to process a file's contents, and the result is a hash value that uniquely identifies the file's contents.

Cipher : The value is data that has been encrypted. A child element of the "Cypher Data" element may be either a "Cypher Reference" or "Cypher Value," but not both. In the event when both are assigned to a Cypher Data object, a Cryptographic Exception is raised.

Decipher: If something can be understood, it can be understood. Your father's message can be read even if his handwriting is horrible with a little effort. Deciphering them is necessary when you need to sort through jumbled information or comprehend enigmatic messages.



To increase the security of the communication, we will combine the hash key and encrypted message. To do this, we will first use the blockchain process to generate the hash key for each block. Next, we will use a cryptography algorithm to encrypt the message provided by the user. Finally, we will add the previously generated hash key to the encrypted message and send it to the user. As soon as this project is complete, we will make an effort to contact network operating companies so they may use this technology and improve the communication security of their network. which demonstrate the integration of blockchain technology, and once we obtain the cypher message, we must decipher it in order to understand it. From this, we can conclude that the message is secured by end-to-end encryption utilizing both blockchain technology and cryptography.

3.9.1. Hash Generation

The hash value for the message the user supplied will be generated throughout this procedure. Utilising hashlib, the generated hash value is distinct and will be generated for each and every character. The common interface to several secure hash and message digest algorithms is implemented by this module. Included are the RSA's MD5 method (described in internet RFC 1321) and the FIPS secure hash algorithms SHA1, SHA224, SHA256, SHA384, and SHA512. In specifically, we are employing the sha256 module and will convert it to hex digest

3.9.2 Block Data Generation

In this procedure, block hashes, block numbers, block data, hashes, and other

Block No: Every block is given a unique number that is allocated as its block number.

Block data: Blockdata gives you access to verifiable information about more than 10.000 blockchain and DLT companies and adopters, as well as unique insights.

Next Hash: This field will indicate the next block hash to which this block is attavhed.

Previous Hash: A blockchain system uses hashes in a number of different places. As new blocks are added, each block's header contains the hash of the previous block, ensuring that nothing has been altered. Blockchains for cryptocurrencies employ hashes to safeguard data and create an immutable record.

Hash : A hash is a deterministic hexadecimal number that appears on a blockchain for a coin. Accordingly, the hash will always contain the same number of characters, regardless of how many characters are present in the input. As an illustration, the hashes for Bitcoin are always 64 digits.

Timestamp: The timestamp, also known as a timestamp, is a short piece of information that is uniquely kept in each block and serves as a way for the blockchain network to track when a block was mined and confirmed.

3.9.3 Cryptographic Encryption Process

In this procedure, we truly go through the ENCRYPTION process' primary phases. In the first step, we define a function called encrypt that uses the message and key as parameters and encrypts each character in the message, where encryption is the process by which we transform plain text into cypher text (scrambled message). In this process, we are using the 26 lower case characters of the English language. The user input message is really encrypted using the main method's lower key value, resulting in a cypher text that is also referred to as a scrambled message.

3.9.4 Appending the hash and Encrypted Message

During this procedure, we actually append the encrypted message, the other 64-bit block hash, and the block hash from the previous step.

3.9.5 Cryptographic Decryption Process

We really go through the decryption procedure in this method. The process of decryption, which transforms scrambled material into plain language that can be understood, is often known as the opposite of encryption .Even though we really decrypt the message character by character during the decryption process, we write a decrypt function that takes message and key as parameters. However, in order to obtain the right encrypted message, we must input the same key that was used for encryption.

3.9.6 Encryption the message using public key and private key

Here, the user enters a message that has been UTF-8 encoded before using the public key generated by RSA, which is 256 bits, to encrypt it. The message is then encrypted using the public key, and we will decrypt it using the private key, which is also 256 bits generated by RSA.

3.9.7 Decryption the message using public key and private key

We are now utilising the private key to decode the message, which was previously encrypted using the public key.

3.9.8 Digital Signature Verification

ECDSA - The Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) that employs keys obtained from elliptic curve cryptography (ECC). Initially, we install ecdsa from the pip module. It is a public key cryptography (PKC)-based equation that is extremely effective.

Digital Signature: A cryptographic hash is produced for the document when a signer digitally authenticates it. The sender's private key, which is kept in a safe HSM box, is subsequently used to encrypt that cryptographic hash.A tangible object that offers additional security for sensitive data is known as a hardware security module (HSM). The document is then transmitted to the recipients with the attachment attached and the sender's public key included.

Message Digest Function: A message digest is a hash function- generated, fixed-size numerical representation of a communication's contents.

Digest: The result of a hash function, such as hash(data) = digest. Also referred to as a harsh value, digest, or message digest.

Signature : A digital signature is a cryptographic output that is used to confirm the accuracy of data.

A digital certificate identifies the identity associated with the key and includes the public key needed for a digital signature. Digital certificates are often provided by reputable organisations and are good for a set amount of time. The certificate authority will serve as the process's guarantee.

4.0 Data Flow Diagram

An information flow diagram (DFD) depicts the movement of data through any system or procedure. It uses preset symbols like rectangles, circles, and arrows as well as brief written explanations to indicate data inputs, outputs, storage places, and paths between each destination. Data flow diagrams can range in complexity from simple, multi-level DFDs that gradually dive deeper into the data handling process to more complicated, hand-drawn process overviews. They can be used to assess an existing system or model a new one. Like the best charts and diagrams, a DFD can frequently "say" things graphically that are hard to explain orally. From developers to CEOs, they are suitable for both technical and nontechnical audiences. That clarifies why DFDs are still in use so frequently today. Even though they still work well for data flow software and systems, they are less useful these days for visualising interactive, real-time, or database-oriented software or systems.

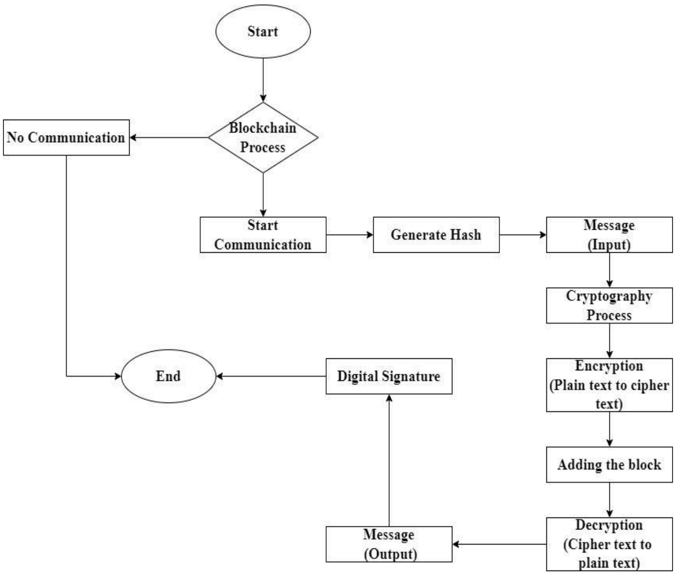


Fig -2 Data Flow Diagram

4.1 Sequence Diagram

In a sequence diagram, object interactions are arranged in temporal order. The objects of the scenario are displayed, as well as the sequence of messages that must be sent and received for the scenario to function properly. Sequence diagrams are also known as event diagrams and event scenarios**.**

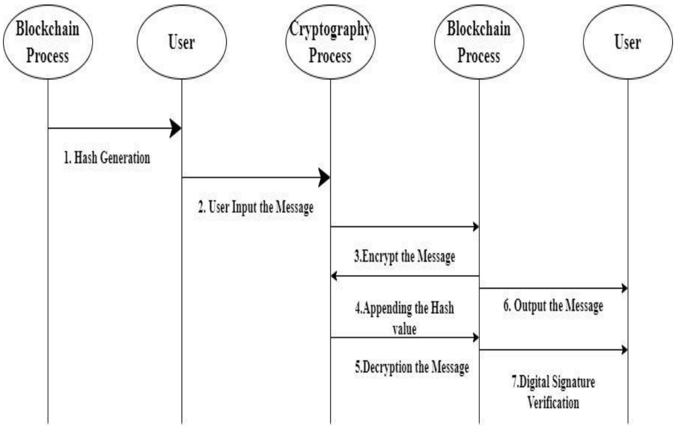


Fig - 3 Sequence Diagram

4.2 Class Diagram of Digital Signtaure

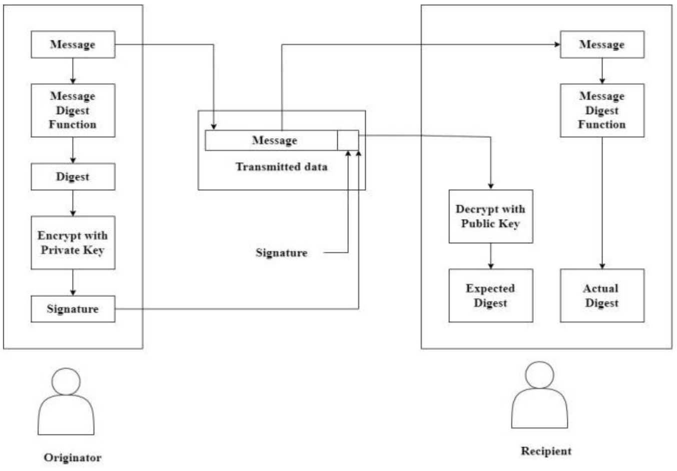


Fig- 4 Class Diagram OF Digital Signature

Message digest: It is a fixed-size numerical representation of a message's contents that is generated using a hash function. A digital signature can be created by encrypting a message digest. The size of messages varies naturally. A message digest is a static numerical representation of a communication's contents.

Data: Public key cryptography's two mutually authenticating cryptographic keys are how digital signatures operate. Data related to the digital signature is encrypted using a private key by the person who creates it, and can only be decrypted using the signer's public key.

Encrypt with Private Key: Encrypt data using a private key: In cryptography, data is encrypted and decrypted using an algorithm and a private key, also known as a secret key. Secret keys should only be accessible to those who are authorised to decrypt the data.

Decrypt with Public Key: In cryptography, a private key, often referred to as a secret key, is a variable that works with an algorithm to encrypt and decode data. Only those parties with permission to decode the data should have access to secret keys.

4.CONCLUSION

All multinational corporations have made the development of blockchain technology a top priority, and over the past few years, a sizable number of startups have appeared in this space. The main applications of cryptography in the blockchain are described in this study, which also looks at current problems. The infrastructure of the blockchain technology is first explained. By using cryptography technology, the blockchain is further improved. The existing security vulnerabilities with the blockchain are then examined. It shows that the primary technology of the blockchain system, digital encryption, is utilised across the whole system. The communication system's message will be transmitted using blockchain and cryptography techniques for extremely high security. Blockchain technology may be extremely beneficial in a society with both centralised and decentralised structures in the future. A wider ecosystem that incorporates the old method of doing things with the new innovation may eventually flourish as a result of the blockchain idea, which, like any new technology, first creates upheaval. History offers several instances, such as how the advent of the radio boosted record sales and how readers like the Kindle have boosted book sales. We now get our news from a variety of sources, including blogs, Twitter, the New York Times, and personalised drone feeds. We watch videos from well-known entertainment studios as well as those on YouTube. Therefore, it's possible that blockchain technology will eventually be a part of a larger ecosystem that employs both centralised and decentralised methods.

REFERENCES

1.Blockchain-enabled wireless communications: a new paradigm towards 6G (National Science Review 8: nwab069, 2021 https://doi.org/10.1093/nsr/nwab069 Advance access publication 26 April 2021)

2.A Study of Blockchain-Based Cryptosystems with and without a Software Defined Network.(IRJET e-ISSN: 2395-0056, p-ISSN: 2395-0072)

3.Secure Peer-to-Peer communication based on Blockchain.(33rd International Conference on Advanced Information Networking and Applications (AINA-2019), Mar 2019, Matsue, Japan. pp.662-672, ff10.1007/978-3-030-15035-8_64ff. ffhal-02180329v2f)

4.Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher (Conference Paper · July 2020 DOI: 10.1109/ComPE49325.2020.9199997)

5.Research on the Application of Cryptography on the Blockchain (IOP Conf. Series: Journal of Physics: Conf. Series 1168 (2019) 032077 doi:10.1088/1742-6596/1168/3/032077)

6. Provably Secure Covert Communication on Blockchain (Physiological Signal Analysis Team, Center for Machine Vision and Signal Analysis, University of Oulu, P.O. Box 5000, FI-90014 Oulu, Finland; juha.partala@oulu.f)

7. Communications cryptography (conference Paper · November2004DOI:10.1109/RFM.2004.1411111 · Source: IEEE Xplore)

BIOGRAPHIES

	SARVESH SUTEJ LABDHE, Bachelor of Engineering in computer Science and Engineering, Brindavan College Of Engineering, affiliated to VTU, Bangaluru, Karnataka, India
	SNEHA.R, Bachelor of Engineering in computer Science and Engineering, Brindavan College Of Engineering, affiliated to VTU, Bangaluru, Karnataka, India
	SUMAIYA, Bachelor of Engineering in computer Science and Engineering, Brindavan College Of Engineering, affiliated to VTU, Bangaluru, Karnataka, India
	Shivani Kamboj, Professor, Department of Computer Science and Engineering, Brindavan College Of Engineering, affiliated to VTU, Bangaluru, Karnataka, India