Blockchain and Cryptography Communication System

Sujata Kullur
Assistant Professor
Usha Mittal Institute of TechnologyMumbai, Maharashtra

Anushka Jain
Information technology
Usha Mittal Institute of TechnologyMumbai, Maharashtra

Kinjal Vyas
Information technology
Usha Mittal Institute of TechnologyMumbai, Maharashtra

Sanika Sawal
Information technology
Usha Mittal Institute of TechnologyMumbai, Maharashtra

***Abstract*—With the increasing use of technologies today across the globe and an increase in data breaches over chat applications, the concern over security has grown into a significant problem. Technology advancements and growth in data flow rates are making it more challenging to protect user data since they are more susceptible to cyber-attacks. This brings in the need for a secure communication system for the smooth streamlining of emerging technologies. Blockchain technology and cryptography are currently the two most important security principles. By combining both, the goal is to offer a double layer of security through the use of asymmetric key algorithms, hash functions, and digital signatures, which ensure the process's integrity. The entire communication system is a hybrid of blockchain and cryptography.**

The aim is to advance security by offering a blockchain-based secure communications solution.

***Index Terms*—Hash Functions, SHA-256, RIPEMD-160, Public- Key, Digital Signature, ECDSA Algorithm**

I. INTRODUCTION

In recent decades, there has been a remarkable increase in wireless devices as well as an exponential rise in the variety of wireless traffic. As a result of everything, a tremendous amount of information has been flowing in, and the communication links are now open for hacking. The concern over cyber attacks and security has become a serious issue with the rising use of the internet today around the globe and an increase in data breaches. Businesses have been using communication networks more and more in recent years. Shareable information and consequently sensitive data are present in communications networks that are interconnected globally. The vulnerability of organisational assets has grown due to this dedication to data communication. Many people think that communications security only refers to preventing unauthorised access to a network. Security is beyond that. The need to strengthen security measures to safeguard digital data grows significantly as our reliance on technology and data grows. This highlights the requirement for a secure communication system to ensure the efficient alignment of new technologies. Blockchain is a particularly revolutionary and promising technology because it can scale transparency while lowering security risks and eradicating fraud. Blockchain technology is currently used to secure healthcare data, provide transparency for the food supply chain, and fundamentally alter how we manage data and ownership. In the upcoming cyberwars, blockchain is more equivalent to a shield than a weapon. Blockchain's most important component is the cryptography technology which uses encryption primarily to maintain data consistency, safeguard user privacy, and preserve information. In this paper, we discuss how combining blockchain technology with cryptography will increase the security of communications and suggest a paradigm for blockchain-based messaging that keeps the performance and security of data stored on the blockchain. The entire system is a combination of blockchain and cryptography along with the implementation of digital signatures. Our project's objective is to suggest a blockchain-based secure communications solution. It can also be deployed on a chat system for secure communication.

II. STUDY AREA

Blockchain technology and cryptography are currently the two most important security principles. The potential benefits of the Blockchain, contrary to what is usually thought, are more than just financial: they extend into plenty of domains such as IoT, digital applications, government, healthcare, retail, manufacturing, energy, supply chain, and education. The blockchain was developed using a variety of different cryptographic techniques. Over the years, organisations have implemented blockchain in multiple web apps for security. Numerous cryptographic algorithms have been used to implement a number of security measures. Namecoin was the first system to build a decentralised naming system using blockchain.A digital signature is an output from cryptography that is used to confirm the validity of data. A digital signature algorithm allows for two different operations: a signing operation, which employs a signing key to form a signature over raw data and a verification operation, where the signature can be checked by a party that has no knowledge of the signing key. A digital signature serves the following key purposes:

1) verification of the signed data's integrity

2) non-repudiation if the signer claims the signature is not authentic

Data legitimacy, concealment, authentication, and identification can all be improved by combining encryption methods with a consensus algorithm with associated hash values. Using these two algorithm standards helps to keep data safe and secure while also protecting it from intruders and predators.
Based on the study area, we found out that till now, there are not many suggestions that use cryptography in blockchain to implement provably secure covert channels further using a digital signature. We attempt to provide a thorough analysis of all recent research trends that have been carried out to assess the effectiveness of blockchain technology in conjunction with different cryptosystem standards in the network sector. It basically makes use of two things i.e Hash functions and Asymmetric-key algorithms. For blockchain, hash functions can be used to perform block integrity verification which makes use of SHA hashing algorithms as its hash function. The blockchain benefits from using cryptographic hash functions in the following ways:
Avalanche effect, where a small change in the input can have a big impact on the output.
Uniqueness i.e., every input has a unique output.
Deterministic i.e., any input will always have the same output if passed through the same hash function.
Public-key cryptography, also known as asymmetric-key encryption, uses various keys for encryption and decryption operations.

III. METHODOLOGY

Blockchain is a distributed database with features like decentralisation, 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 lacks a central node. It has high requirements for its security performance because it maintains all user transaction information. As a result, in order to maintain transaction integrity, blockchain transactions must also guarantee the security of data exchanged over unsafe connections. Since blockchain's data cannot be altered naturally, it is a true disruptor in fields including transactions, information security, and medicine. Blockchain is a superior, secure visual depiction of events that keeps authorised users informed while also preserving the past. The content cannot be changed or accidentally deleted because we receive a statistical data trace and a quickly updated record. Peer-to-peer (P2P) systems in blockchain enable them to solve a number of challenges that are not easily solved by client-server methods. Cryptography technology occupies the most central position in the blockchain. It is the study of methods for encrypting communications such that only the sender and the recipient can read the contents of a message. The most common application of cryptography when sending electronic data is encrypting and decrypting messages. The main goals of cryptosystems, which includes two parts: encoding and decoding, are verification, information validation such as privacy and integrity, non-repudiation of validity, and anonymity. Hash function encryption, public-key encryption, and secret-key encryption are the three types of cryptographic algorithms. The technological stack impacts several aspects of development, including project duration, scalability, quality, and level of security. Visual Studio Code and Jupyter Notebook are the tools used in this project. Python 3.7.0 is the most appropriate version for this project.

A. Hash Functions

The hash algorithm is a mapping function that reduces a series of messages of arbitrary length to a shorter fixed-length value. Its characteristics include susceptibility, unidirectionality, collision resistance, and high sensitivity. Hash is typically used to ensure data integrity or to make sure the data hasn't been wrongly altered. The hash value of the data under test adjusts as the data does. Hence, depending on the data's hash value, the integrity of the data may be determined. Moreover, the SHA-256 and RIPEMD-160 hashing algorithms are typically used by blockchains as their hash function.
Hash functions can be used for blockchain to perform block integrity checks. Any user can compare the calculated 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 every block. The information in the previous block is then checked for integrity. Public-private key pairs can also be created using the hash function. In addition to the standard pointers, the hash pointer is a data structure that also includes certain data information and password hashes linked to that information. When retrieving data, a regular pointer is utilised, and when determining whether the data has been altered, a hash pointer is used. The blockchain is a collection of hash pointers that are linked together by a common hash value. The integrity of the block information is ensured by checking the hash value to see if the data inside the block has been altered.

1) SHA: Secure Hash Algorithm, popularly known by its abbreviation SHA, is used to hash data and certificate files. 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 a 256-bit message digest and is a class of the SHA-2 algorithm cluster. The two steps of the algorithm's computation process are the main loop and message preparation. Binary bit filling and message length filling are carried out on data of any length during the message preprocessing stage, and the filled message is then divided into multiple 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, and the original message's hash value serves as the output of the previous compression function.

2) RIEPEMD: A family of cryptographic hash functions is called RIPEMD (RIPE Message Digest). There are five func-

tions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, with RIPEMD-160 being the most prevalent. The COSI research team at the University of Leuven in Belgium produced the hash function algorithm known as RIEPEMD, which is a summary of the RACE original integrity check message. Message complement is the initial step of the algorithm, and the complement method 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 different cases using different original logic functions in each loop, with five of the two original logic functions running in reverse order. The hash value of the original message is produced as a 160-bit output following the completion of all 512-bit packet processing.

B. Asymmetric-Key Cryptography

Asymmetric cryptography, commonly referred to as public-key cryptography, is a method for encrypting and decrypting messages and safeguarding them from unauthorised access or use. It employs a pair of linked keys—a public key and a private key. The issue of early key distribution in symmetric encryption can be effectively solved by asymmetric encryption as the encryption key and the decryption key in an asymmetric encryption technique are different and are referred to as a public key and a private key, respectively. A random number algorithm is typically required to generate the private key, while an irreversible technique is used to derive the public key. The advantages of the asymmetric encryption technique include distinct public and private keys that can be sent through insecure networks.

1) Public- Key: Asymmetric-key encryption is the second encryption technique that plays a significant part in the applications of cryptography on the blockchain. Public-key cryptography, also known as asymmetric-key encryption, uses various keys for encryption and decryption operations. Anyone with access to a public key can encrypt a message in a public-key encryption system, creating a ciphertext. However, only those who have access to the associated private key can decrypt the ciphertext to reveal the original message. Modern cryptosystems, comprising applications and protocols that provide assurance of the confidentiality, authenticity, and non-reliability of electronic communications and data storage, use public key algorithms as essential security primitives.

2) Private-Key: The Private key uses the same secret key for both encryption and decryption. This key is symmetric since it is copied or shared by another party in order to decrypt the ciphertext. It moves more quickly than public-key cryptography. Smaller, simpler-to-compute keys are used in private key encryption, also known as symmetric encryption. They still offer sufficient computational toughness but require fewer client and server resources. This is the main benefit of symmetric encryption and is crucial, especially at scale.

C. Digital Signature

The presence of a digital signature guarantees that the intended message won't be tampered with while in transit. The user adds a one-way hash (encryption) of the authentication tokens using the secret key each time the service securely signs the document. Biometrics demonstrates that an electronic document or file that has been signed, whether deliberately or accidentally, has not been altered. In order to accomplish this, digital signatures create a unique response message or piece of material and encrypt it using the recipient's master password. A signature algorithm and a verification algorithm often make up the digital signature system. A digital signature is created using a signature algorithm, which is usually controlled by a signature key. Both the signature algorithm and the signature key are kept private and are within the signer's control. The message's digital signature can be efficiently validated using the verification method, and the message may also be checked independently of the signature. The verification method is often managed by the verification key, but both the algorithm and the key are available to the public, making it simple for the person who has to validate the signature to do so.

1) ECDSA Algorithm: One of the more complex public key cryptography encryption systems is called the Elliptic Curve Digital Signature Algorithm, or ECDSA. Elliptic curve cryptography produces keys that are generally smaller than those produced by digital signing algorithms. Elliptic curve cryptography is a public key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curve cryptography is mostly used to generate digital signatures and pseudorandom numbers, among other things. ECDSA is more effective at accomplishing the same task than any other digital signing signature. ECDSA employs smaller keys in order to attain the same level of security as every other digital signature method.

The fact that ECDSA is more recent than other public key cryptography is a plus. Compared to the most widely used public key encryption method, RSA, which was standardised in 1995, ECDSA was just standardised in 2005. Hackers haven't had as much time to study how to break ECDSA since it's been around for such a short time. Switching to ECDSA appears increasingly appealing every year as a result of this and its complexity.

D. Flow

Firstly, starting from the blockchain infrastructure, blockchain technology is simplified. Secondly, cryptography technology has been introduced to elaborate the blockchain. Finally, the existing security problems in the blockchain have been analysed. The Communication system as a message has gone through the cryptography and blockchain process for high-level security.

Libraries that were needed have been imported along with the construction of blocks. Cryptography algorithms have been applied and put into practice for message encryption. Blockchain and cryptography algorithms have been combined. Reverse algorithms have been employed for decryption, and the output is produced as the original message.

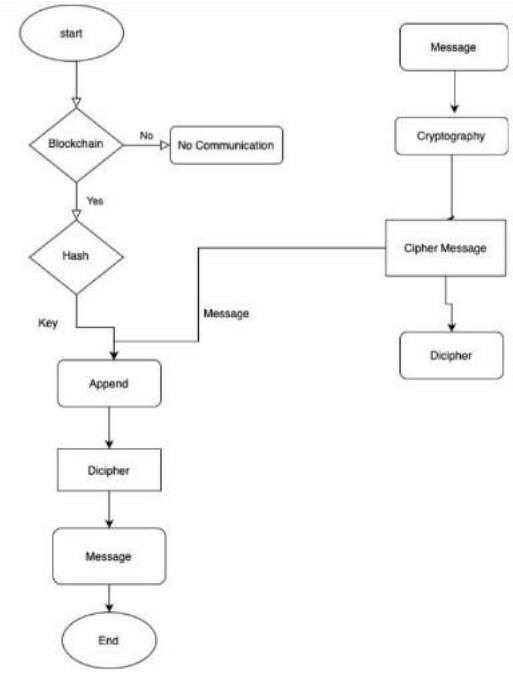

Fig. 1. Flowchart

E. Flowchart

Cryptography algorithms and blockchain technology have both been used. Prior to the cypher message, the hash value is generated. Once we have these two, we combine blockchain technology with cryptography by appending them to one another. The ciphertext needs to be deciphered in order to get the original message. This ensures that the message is encrypted end-to-end using cryptography and the blockchain for security.

IV. Result & Discussion

This project imports various python libraries like hashlib to securely hash the data and generate SHA-256 hashes of messages. In the sha256_hash function, the input message is encoded as a byte string and then passed to hashlib.sha256 function to generate a hash object. The hash values are unique and deterministic for each message which ensures data integrity and detects tampering. The next stage is an implementation of a simple substitution cipher that uses a fixed key to encrypt and decrypt messages. The input message and the key value taken by the encrypt function are iterated within the function to create an encrypted string. The decrypt function works similarly to encrypting but subtracts the key from the index of each character in the message to recover the original letter. The main function prompts the user for input and then calls the appropriate function based on the user's choice. The hashlib and RSA modules are imported to provide hash functions and RSA key generation and encryption/decryption capabilities. The rsa.newkeys function generates a new public-private key pair of 256 bits. The public key is used to encrypt the message, while the private key is used to decrypt it.

The next part demonstrates the use of digital signatures to sign and verify the authenticity of a message using the ECDSA algorithm. The hashlib and ECDSA modules are imported to provide hash functions and ECDSA key generation and signing/verification capabilities. The privateKey.sign function is used to generate a digital signature of the hash using the generated private key. The publicKey.verify function is used to verify the digital signature of the hash using the corresponding public key. If the verification succeeds, the message is considered authentic and its origin is verified by the public/private key pair.

Currently, this system encrypts and decrypts the messages and secures them with a digital signature. Therefore, this system can be built in a working interface instance as a chat application. This system can also be integrated with today's real-time applications like Whatsapp, Instagram, etc for enhanced security.

V. Conclusion

This paper presents the combination of two emerging technologies i.e blockchain with cryptography along with the implementation of digital signatures that have helped in increasing the security of communications.

The major use of cryptography in the blockchain is introduced in this study, which also analyses the current issues. It provides a brief introduction to cryptographic techniques such as hash algorithms, asymmetric encryption algorithms, and digital signatures. It further elaborates on the blockchain's structure and explains in detail how cryptography technology protects users' privacy.

The architecture for a secure mobile chat application has helped provide confidentiality and integrity to users who want to communicate through text messages. Customers can feel safe knowing that no one, not even the service provider, can read their messages.

use section* for acknowledgment

Acknowledgment

It is indeed a great pleasure and proud opportunity for us to present this paper for our final year degree at 'Usha Mittal Institute of Technology. The success of this project has throughout depended upon a combination of hard work and unending cooperation and guidance provided to us by our project guide. Ultimately no words could describe the deep sense of cooperation and ready nature to help us. We would like to thank, Dr. SHIKHA NEMA (Principal), Dr. Sanjay Shitole (H.O.D. of IT Department), and Prof. Sujata Kullur (Project Guide), who made very valuable guidance and cooperation during our project. Further, we are thankful to all the teaching and non-teaching staff of the Information Technology Department for their cooperation during the project work. We are very grateful to those who in the form of books had conveyed guidance in this project work.

REFERENCES

[1] Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma,"Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher," July 2020.
[2] Juha Partala, "Provably Secure Covert Communication on Blockchain", August 2018.
[3] Prof. Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali, May 2020.
[4] Myron Dsilva, "Complete Guide to a Decentralized Exchange", September 2020
[5] Kathleen Richards, Cryptography, September 2021