Original Research Article

BLOCK CHAIN AND CRYPTOGRAPHY BASED SECURE COMMUNICATION SYSTEM

Abstract- The blockchain is a cutting-edge technology that reduces these risks by allowing vital tasks to be decentralized while retaining a high level of security. It eliminates the need for dependable intermediaries. The blockchain, which records all past transactions, is accessible to all network nodes. The goal of our project is to create a blockchain-based secure communication system. We explain why blockchain would improve communication security and propose a model design for blockchain-based messaging that focuses on training the performance and security of data recorded on the blockchain, as well as using a smart contract to verify identities and their associated public keys, as well as validating the users certificate.

Keywords: Block Chain, Security, Validation,Public Keys

1. INTRODUCTION

Blockchain is a decentralized, traceable, non-tamper able, secure, and trustworthy distributed database. This project integrates the P2P protocol, digital encryption technology, a consensus method, a smart contract, and other technologies. Instead of the conventional central node maintenance method, a strategy of mutual maintenance by diverse users is used to establish information supervision among numerous parties, ensuring the data's credibility and integrity. Blockchain systems are classified into three types: public chains, private chains, and alliance chains. The public chain allows any node to join or leave at any moment, while the private chain has tight requirements for participating nodes and the alliance chain is administered collaboratively by multiple partnering institutions.

As a representation of distributed databases, all user transaction information is recorded on the blockchain, which has strict security standards. Blockchain is a peer-to-peer network that is decentralized. There is no need for nodes to trust one another, and there is no central node. As a result, transactions on the blockchain must maintain the confidentiality of transaction

information while preserving transaction integrity over insecure connections. As can be seen, cryptography is the most important blockchain technology.

As a representation of distributed databases, all user transaction information is recorded on the block chain, which has strict security standards. Block chain is a peer-to-peer network that is decentralized. There is no need for nodes to trust one another, and there is no central node. As a result, transactions on the block chain must maintain the confidentiality of transaction information while preserving transaction integrity over insecure connections. As can be seen, cryptography is the most important block chain technology. Cryptography is widely utilized in blockchain to safeguard user privacy and transaction information, as well as to assure data integrity.

The hash algorithm is a function that turns a series of messages of variable lengths into a single shorter value. Some of its properties are susceptibility, unidirectionality, collision resistance, and high sensitivity. Hash is typically used to check data integrity or to confirm that data has not been tampered with incorrectly. When the data being tested changes, so does the hash value. As a result, even if the data is in a dangerous environment, the hash value may be utilized to determine the data's integrity.

Wu et al. proposed a method for ensuring the authenticity and non-repudiation of digital material while maintaining privacy for traceable encryption in blockchain. The authors address the issue of the user's private key, which, when shared with other entities, does not contain the user's specific information. If the shared key is damaged or misused, it is difficult to determine where the secret key came from. Furthermore, access control leakage of sensitive information is a barrier to current solutions. The authors devised a privacy protection approach, such as attribute-based encryption, to safeguard the private keys (ABE). However, the decryption approach does not appear to be more efficient.

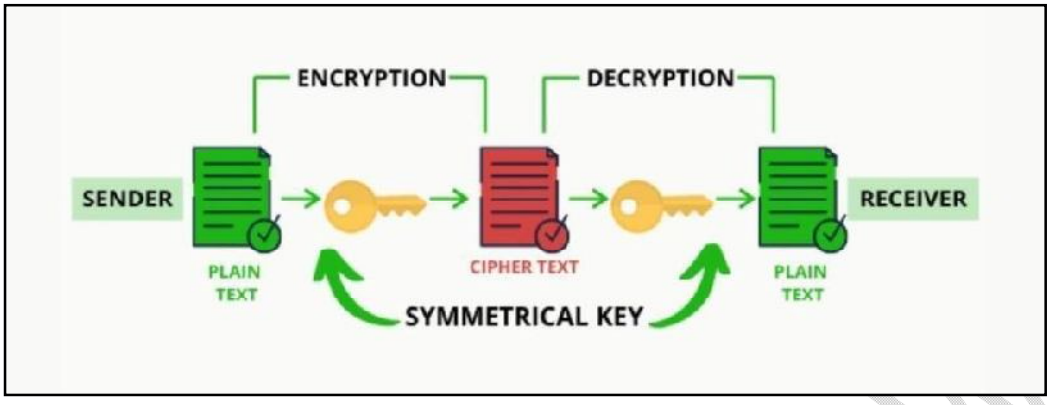


Figure 1: B and C Example

2. METHODOLOGY

Python language is used to write the code. Python provides a wide variety of libraries for scientific and computational usage. Libraries such as hashlib, rsa.

Consider the probability distribution D. V D denotes a random variable V that is distributed according to D. We indicate u D if an element u is sampled from a probability distribution of D. U denotes the uniform probability distribution on a set X. (X). We use standard nomenclature for probabilistic algorithms. When an algorithm A is run with the input x and produces the result y, we call it y A. (x). Oracles can be made available to algorithms. Oracles are "black boxes" that can compute things like functions and other methods. AO denotes an algorithm A with oracle access to an oracle O. The time complexity of calling an oracle and obtaining an answer is assumed to be constant time O*(1)

Algorithm 1: Pseudorandom Cipher text Experiment

Algorithm 1 Pseudorandom Ciphertext Experiment

procedure $\mathrm{PRC\_EXP}^{\mathrm{SE}}_{\mathrm{A}}(1^s)$
  $k \leftarrow \mathrm{Gen}(1^s)$
  $(m, S) \leftarrow \mathrm{A}_1^{\mathrm{Enc}_k}(1^s)$ ▷ S is internal state information of A
  $b \leftarrow U(\{0,1\})$
  if $b = 1$ **then**
    $c \leftarrow \mathrm{Enc}(k, m)$ ▷ Use the actual encryption
  else
    $c \leftarrow U(\{0,1\}^{|\mathrm{Enc}(k,m)|})$ ▷ Use a random string
  end if
  $b' \leftarrow \mathrm{A}_2^{\mathrm{Enc}_k}(c, S)$
  if $b = b'$ **then**
    return 1 ▷ A guessed correctly
  else
    return 0 ▷ A did not guess correctly
  end if
end procedure

Algorithm 2: Embedding Algorithm

Algorithm 2 Embedding Algorithm

procedure Embed($(k, \lambda), m, \mathcal{B}$)
  $c \leftarrow \mathsf{Enc}(k, m)$
  Concatenate $c' = \lambda || c$
  Set $N = |c'|$
  Interpret c' as a bit representation $c'_1 c'_2 \dots c'_N \in \{0,1\}^N$
  $i = 1$
  while $i \leq N$ **do**
    Generate unseen $(s_k, p_k) \leftarrow \mathsf{Gen}_\Sigma(1^s)$
    $a \leftarrow H(p_k^{(i)})$
    Interpret a as a bit representation $a_1 a_2 \dots a_n \in \{0,1\}^n$
    if $a_n = c'_i$ **then**
      $\mu \leftarrow \mathcal{M}_\mathcal{H}$
      Generate a unique identifier t for the payment
      $\sigma \leftarrow \mathsf{Sign}(s_k^{(A)}, (p_k^{(A)}, a, \mu, t))$
      $\mathsf{Submit}(p_k^{(A)}, a, \mu, t, \sigma)$
      Wait for the blockchain to publish a new block
      Update $\mathcal{H}$
      $i \leftarrow i + 1$
    end if
  end while
end procedure

Algorithm 3: Extraction Algorithm

Algorithm 3 Extraction Algorithm

procedure Extract($(\lambda, k), \mathcal{B}$)
  $i = 1$
  $j = 1$
  while have not found λ yet **do** ▷ Scan for λ
    $C = \mathsf{Read}(j)$
    if $C = \perp$ **then**
      Wait until a block appears and read it: $C = \mathsf{Read}(j)$
    end if
    for any payment $P \in C$ **do**
      if P is from $p_k^{(A)}$ **then**
        Extract address a from P and get the LSB a_n
        Scan if we have found the entire $\lambda \in \{0,1\}^n$
      end if
    end for
    $j \leftarrow j + 1$
  end while
  $i = 1$ ▷ Now reading the encrypted hidden message
  while $i \leq N - n_\lambda$ **do**
    $C = \mathsf{Read}(j)$
    if $C = \perp$ **then**
      Wait until a block appears and read it: $C = \mathsf{Read}(j)$
    end if
    for any payment $P \in C$ **do**
      if P is from $p_k^{(A)}$ **then**
        Extract address a from P and get the LSB a_n
        $c_i \leftarrow a_n$
        $i \leftarrow i + 1$
      end if
    end for
    $j \leftarrow j + 1$
  end while
  Compile $c = c_1 c_2 \dots c_{N - n_\lambda}$
  $m \leftarrow \mathsf{Dec}(k, c)$
  output m
end procedure

Algorithm4: Payment Extinguishing Algorithm

Algorithm 4 Payment Distinguishing Experiment

procedure $\text{PAY\_DIST\_EXP}_{A}^{\Pi,\mathcal{B}}(1^s)$
  $(s_k, p_k) \leftarrow \text{Gen}_{\Sigma}(1^s)$
  $(m, S) \leftarrow A_1^{\text{Read,Submit}}(p_k)$ ▷ S is internal state information of the adversary that can be passed to the second stage
  $(\lambda, k) \leftarrow \text{Gen}_{\Pi}(1^s)$
  $b \leftarrow U(\{0,1\})$
  if $b = 1$ **then** ▷ Actual message is sent to the blockchain
    $\text{Embed}((\lambda, k), m, \mathcal{B})$
  else ▷ Random payments are sent to the blockchain
    $n_\lambda \leftarrow |\lambda|$
    $N \leftarrow |\text{Enc}(k, m)| + n_\lambda$ ▷ Enc is the encryption scheme used by Π
    Generate N random addresses a_i for $i \in \{1, 2, \ldots, N\}$
    Simulate Embed to generate payments to a_i
    Submit payments to blockchain one-by-one as Embed does
  end if
  $b' \leftarrow A_2^{\text{Read,Submit}}(p_k, S)$
  if $b = b'$ **then**
    return 1 ▷ A guessed correctly
  else
    return 0 ▷ A did not guess correctly
  end if
end procedure

Algorithm 5 First Stage of Adversary A'

Algorithm 5 First Stage of the Adversary A'

procedure $A_1'^{\text{Enc}_\lambda}(1^s)$
  Initialize a blockchain $\mathcal{B}$
  $(s_k, p_k) \leftarrow \text{Gen}_{\Sigma}(1^s)$
  $(m, S) \leftarrow A_1^{\text{Read,Submit}}(p_k)$ ▷ Answers the queries according to the specification of $\mathcal{B}$
  $S' \leftarrow$ state and internal information of $\mathcal{B}$
  output $(m, (S, S', p_k, s_k))$
end procedure

Algorithm 6 Second Stage of Adversary A'

Algorithm 6 Second Stage of the Adversary A'

1: **procedure** $A'^{Enc_k}_2(c, (S, S', p_k, s_k))$
2: Initialize a blockchain $\mathcal{B}$ according to the state S'
3: $(\lambda, k) \leftarrow Gen_{BLOCCE}(1^s)$
4: Embed $\lambda || c$ into $\mathcal{B}$ by simulating Embed
5: $b' \leftarrow A_2^{Read,Submit}(p_k, S)$
6: **output** b'
7: **end procedure**

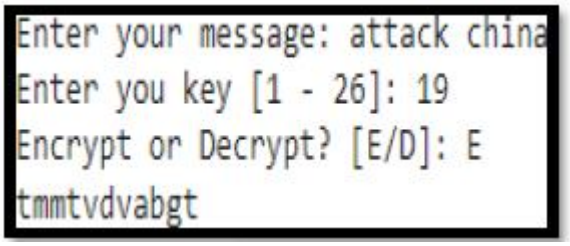
3. RESULTS AND ANALYSIS

As a representation of distributed databases, all user transaction information is recorded on the blockchain, which has strict security standards. Blockchain is a peer-to-peer network that is decentralized. There is no need for nodes to trust one another, and there is no central node. As a result, transactions on the blockchain must maintain the confidentiality of transaction information while preserving transaction integrity over insecure connections. As can be seen, each message while entered allocates and display's a block number, Data and Hash value for the block.

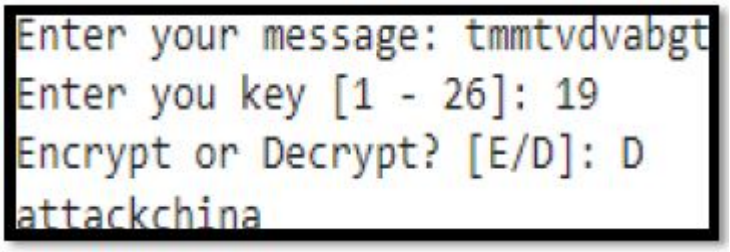
```
Block Hash: b843dd2f3cfa492d4fb4260a4c28968d7615492f9906b0ad6e2d7bbc5c69d7dc
BlockNo: 1
Block Data: Block 1
Hashes: 1013952
--------------
Block Hash: 6156c9f7df237e11aab86dcd1e605fb69150c724a7e6da452939dd964d0d2973
BlockNo: 0
Block Data: Genesis
Hashes: 0
--------------
Block Hash: b843dd2f3cfa492d4fb4260a4c28968d7615492f9906b0ad6e2d7bbc5c69d7dc
BlockNo: 1
Block Data: Block 1
Hashes: 1013952
```

The two types of cryptographic algorithms utilized in block chains are asymmetric-key algorithms and hash functions. Hash functions are used to provide each participant with a unified picture of the block chain. In block chains, the SHA-256 hashing algorithm is often employed as

the hash function. As seen below, while we enter a message, it asks for Encryption or Decryption and converts respectively.



The SHA-256 hashing method is frequently used as the hash function in blockchains. While entering a message, it asks for Encryption or Decryption and transforms accordingly, as shown below.



4. Conclusion and Future Scope

Block chain technology has emerged as a critical focus area for all multinational organizations' development in recent years, with a great number of startups emerging in this industry. This study covers current block chain challenges and presents cryptography's major uses. To begin, the block chain technology, starting with the block chain infrastructure, is simplified. Second, to better understand the block chain, cryptography technology is offered. Finally, the block chain's current security weaknesses are evaluated. It demonstrates that digital encryption is employed throughout the block chain system and is a necessary component. For maximum security, the communication system's message will be transmitted via encryption and the block chain protocol Future plans include developing and deploying social media tools, particularly for communication. Encryption techniques are now used in every system. As a result, in the future, block chain and encryption will combine for more privacy.

References

[1] Nakamoto, S.(2008) Bitcoin:Apeer-to- peer electronic cash system. Consulted. 165:55-61.

[2] Zhu,Y.,Gan,G.H.,Deng,D.(2016)Security Research in Key Technologies of Blockchain.Information Security Research., 12:1090-1097.
[3] Liu,X.F.(2017)Research on block chain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization. Zhejiang University.
[4] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MDand RIPEMD.AdvancesinEurocrypt.,3494:1-18.
[5] Shen, Y., Wang, G. (2017) Improved preimageattacksonRIPEMD- 160andSHA-160.KsiiTransactions on Internet & Information Systems., 12:727-746.
[6] Wang,H.Q.,Wu,T.(2017) Cryptography in Blockchain. Journal of Nanjing University of Posts