Research on Multi-carrier Hybrid Encrypted Communication Technology Based on Blockchain

Xinyi Chen
School of Optoelectronics and Information Engineering, Fujian Normal University, Fuzhou, China

Abstract: As there is a third party intervention in network communication, in the context of big data era, the intervention of the third party platform may obtain the content of the private session, and also may tamper with the content, and the network communication becomes no longer secure, so this paper establishes a multi-carrier hybrid encryption system to ensure the privacy of the communication session. In this paper, an MCHE model is constructed to embed the secret information of communication on the blockchain on the basis of ring signature, using the mechanism of multi-carrier hybrid encryption, which not only improves the anonymity of the two parties of communication, but also improves the security of the content of the communication, and at the same time and proposes to complete the highly efficient encrypted communication based on the blockchain in which each leader leads multiple blocks. Compared with traditional network communication, blockchain communication takes advantage of the blockchain to effectively prevent eavesdroppers and attackers from listening to and tampering with encrypted information. The model can prevent third-party regulation and play the role of a private dialogue space for individuals; for industries, it can prevent competitors from obtaining important information through illegal bribes and other means; for countries, it can be used in the military to prevent enemy countries from intercepting and monitoring the acquisition of intelligence, and to protect their own national security interests.

Keywords: Network Communication; Encryption Technology; Blockchain; Ring Signature

1. Introduction

In today's era of big data, network communication has become an integral part of people's daily lives. However, in traditional network communication, the means of communication is often a third-party platform. With the wide access to third-party platforms and the massive accumulation of data, there is a hidden danger of privacy and security lurking behind this convenience. Third-party service providers sometimes access users‘ personal information without their consent, and even steal or tamper with these private conversations, thus violating users’ privacy rights.

The maturity of blockchain technology and its unique advantages of decentralization, tampering, transparency and encryption, on the other hand, provide a new approach in the field of network communication. Introducing blockchain technology into network communication can achieve direct peer-to-peer communication, and even encryption algorithms can be used to encrypt the content of the communication and improve the security and reliability of the communication. Combining various types of algorithms as well as encryption technology can effectively prevent data tampering, man-in-the-middle attacks, and other network security threats. Therefore, this paper designs a multi-carrier hybrid encryption (MCHE) model based on blockchain to study the security of encrypted communication and the efficiency of encrypted communication.

2. Literature Review

For the research of blockchain covert communication, there have been some attempts made by some scholars at home and abroad.

The first one is the blockchain covert communication scheme under the cover of normal transactions proposed by Jiang Pengkun et al [1]. This method is actually an early strategy used for cryptographic communication. In the Bitcoin system, the user's private key is not directly exposed to the network, but is generated by the user himself through a random number generator. This key is then converted

 Copyright @ STEMM Institute Press

into a public key that is mathematically mapped to a specific address. The sender uses the pre-shared key to generate the sending address, which is the basis for constructing the transaction. When receivers try to access these transactions, they perform elliptic curve multiplication using the sender's public key and the pre-shared key. In this way, the receiver is able to continually deduce the true location of the sending address. In this way, even if the content of the transaction carries sensitive information, the receiver is able to quickly identify and decrypt the secret content contained therein through this transaction data provided by the address. Further, through a series of complex hashing operations, receiving addresses can be created that meet specific requirements. The combination of these receiving addresses constitutes a transmission-free cryptographic table, which greatly reduces the number of key negotiations performed under the blockchain network, thus increasing efficiency. Moreover, this approach achieves full address availability without changing the form of any address, and allows addresses to be embedded in the normal course of transactions without attracting any noticeable attention or traceability. Through this clever design, blockchain technology provides a secure, efficient and reliable route for covert communication.

Partala and his team put forth the BLOCCE scheme, which endeavors to establish a provably secure covert communication mechanism within the blockchain system [2]. In the BLOCCE scheme, the communicating parties transmit secret messages through the use of Bitcoin addresses in a way that draws on information hiding methods from traditional information hiding techniques. In particular, the scheme employs the least significant bit of the address to store the secret message to be concealed. The sender, Alice, generates a set of randomly selected Bitcoin addresses and then selects and sorts the addresses that correspond to the secret message. Alice and Bob then negotiate in advance a fixed address that will be used as the input address for the transaction. Alice uses this fixed address as the input address to transfer money to the selected addresses, thus creating three transactions. These transactions are then broadcast in blocks to the blockchain network. Conversely, Bob is only required to query the transactions associated with the fixed address, obtain the least significant bit of the address in turn, and then retrieve the secret information through the reverse encoding and decryption algorithm. Nevertheless, the BLOCCE scheme is not without its own set of limitations. As each block is permitted to contain up to one bit of data, this results in an extremely low channel utilisation. Furthermore, in order to guarantee the confidentiality of communication, it is necessary to negotiate a message start identifier in advance for each communication process. This undoubtedly results in additional communication overhead.

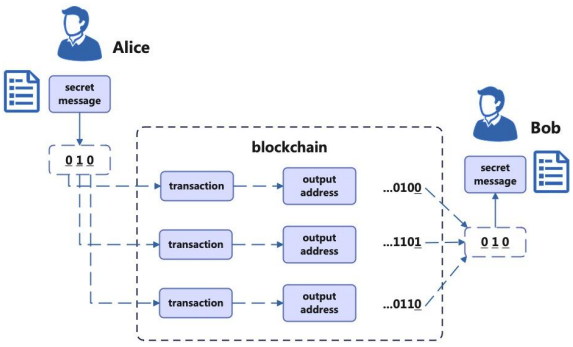

Figure 1. Schematic Diagram of the BLOCCE Programme

Song Shang and Peng Wei put forth an innovative and enhanced scheme [3], BLOCCE+, which integrates the strengths and limitations of the existing BLOCCE scheme. The scheme introduces a novel negotiation process, designated as the subsequent MSI (Multi-Signing Identity) negotiation process. This process guarantees the secure and efficient exchange of messages between participants in subsequent communications. The MSI is constructed in two distinct parts when a message is transmitted. The initial component comprises the initial signature and the acknowledgement code of the message, whereas the subsequent element serves to indicate the commencement of the subsequent message. This structure enables each message to possess a distinctive identity, thereby guaranteeing the singularity and integrity of the communication and reducing superfluous waiting periods. Concurrently, the BLOCCE+ scheme augments security by augmenting the number of embedded bits per transaction and the number of transactions that can be submitted in each block. This approach not only reduces the number of redundant data transfers, but also significantly reduces the burden on the network, thereby improving the overall communication efficiency of the system.

In conclusion, Shan-Yun Huang put forth a semi-constructive covert communication model

that incorporates multi-carrier collaboration [4]. The specific steps are as follows: in the initial stage, the communicating parties engage in negotiations regarding the key, public key, and related algorithms that are necessary for communication. In the subsequent stage, the sender generates the crypto-containing carrier and constructs the transaction that is to be sent to the blockchain network. This is achieved through the utilisation of the semi-constructive message hiding method in conjunction with the formulated rules. In the third stage, the recipient validates the encrypted transaction with the public key and extracts it. In the fourth stage, the communicating parties update the address using the ECDH algorithm (Elliptic Curve Diffie-Hellman Key Exchange Algorithm) to update the address. The proposal is to embed six carriers in each transaction for communication, which will undoubtedly result in a greater quantity of effective information being conveyed in a single communication.

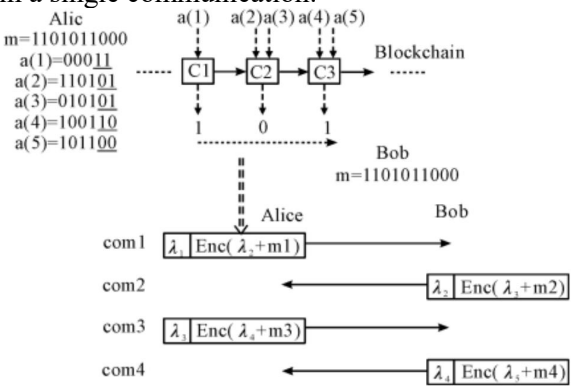

Figure 2. Schematic Diagram of the BLOCCE+ Programme [3]

This paper presents an improvement to the process of transaction address embedding on the BLOCCE scheme. It incorporates the advantages of existing research and proposes a multi-carrier hybrid encryption (MCHE) model to ensure the efficiency and security of communication. Concurrently, to guarantee the confidentiality of the sender, the ring signature methodology is proposed as a means of safeguarding the sender's privacy and security during the communication process. Given that the communication is based on blockchain technology, the efficiency of the communication is contingent upon the speed of blockchain generation. It is therefore proposed that communication be conducted based on a leader leading multiple blocks, with the aim of improving the efficiency of the communication by increasing the speed of blockchain generation.

The MCHE model is a blockchain-based cryptographic communication model that proposes a novel cryptographic communication process based on the recently developed blockchain mechanism of ring signature and single leader for multiple blocks. Prior to initiating communication, the participating parties must first negotiate the use of a pre-shared key (PSK), a message start identifier (MSI), and a fixed address. The sender, Alice, incorporates the pre-negotiated MSI, encrypted data, public key hash, transaction timestamp, transaction amount, transaction fee, transaction signature, and MSI into the transaction address. Subsequently, the recipient, designated as "Bob," decodes the encrypted information using his private key and the pre-negotiated PSK. Subsequently, Bob is able to utilise the subsequent MSI embedded in the address by Alice in order to facilitate further communication with the sender.

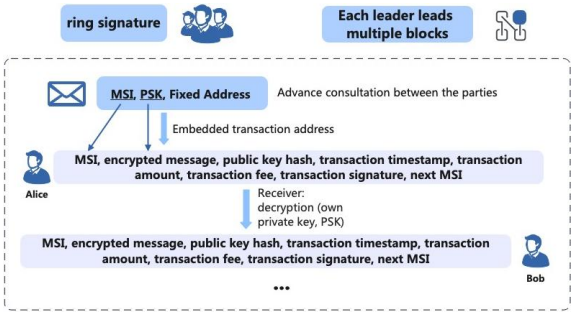

Figure 3. MCHE Model

3. Based on Multi-Carrier Hybrid Encrypted Communication Technology

3.1 Hybrid Encryption

The hybrid encryption technique employed in this model is based on RSA and AES. The process entails the server generating RSA public-private key pairs. The public key is then used to encrypt the AES key, while the private key is employed to decrypt the AES key. The client generates a random AES key to encrypt the data, thereby obtaining the ciphertext, and encrypts the AES key with the server's RSA public key. Subsequently, the client transmits the ciphertext to the server, accompanied by the encrypted AES key. Upon receipt of the ciphertext from the client, the server decrypts the AES key with the RSA private key and then uses the decrypted AES key to restore the original data. This encryption process guarantees that even if the transmitted data is intercepted,

 Copyright @ STEMM Institute Press

the AES key is safeguarded by RSA encryption, rendering it inaccessible to an attacker and thus preventing the decryption of the data.

RSA is an asymmetric encryption algorithm whose security is based on the complexity of the large integer decomposition. Therefore, RSA was selected for use in the MCHE model. RSA works by choosing two large primes p and q and computing their product $n = p * q$. Then use the Euler function $\varphi(n) = (p - 1)(q - 1)$. Choose the public key exponent e such that $1 < e < \varphi(n)$ and e is mutually prime with $\varphi(n)$. Finally compute the private key index d such that $d * e \equiv 1 \pmod{\varphi(n)}$.

In comparison to RSA, AES is a symmetric encryption algorithm, with key lengths of 128, 192 and even 256 bits. The utilisation of AES in MCHE can enhance the efficiency of encryption and decryption by expanding the AES key into multiple subkeys, which are employed for each round of encryption. Initially, the first subkey is utilised to perform an XOR operation on the data block. Subsequently, multiple rounds of encryption are conducted, necessitating 10, 12, and 14 rounds for 128-, 192-, and 256-bit keys, respectively. Each round comprises four stages: byte substitution, row shifting, column obfuscation, and round key addition.

In MCHE, RSA employs a 2048-bit key, which is sufficient to defend against the majority of attacks without imposing an undue computational burden. A 2048-bit key can more effectively defend against complex disassembly attacks than a 1024-bit key. Furthermore, the Advanced Encryption Standard (AES) employs 256-bit keys. In comparison to a 1024-bit key, a 2048-bit key is more effective at defending against complex decomposition attacks and provides a more robust level of security over time. The AES algorithm employs a 256-bit key length, and the longer the AES key, the greater the strength of the cryptographic algorithm. The AES-256 key is regarded as highly secure in accordance with the prevailing standards and is deemed suitable for the transmission of highly sensitive data. Compared to AES-128, AES-256 exhibits a marginally elevated computational burden, yet its enhanced security justifies this additional cost. In similar fashion, the computational burden associated with AES-256 is slightly higher than that of AES-128, yet its enhanced security makes it suitable for application scenarios that require a higher level of protection.

3.2 Message Start Identifier

The message identifier is the type and instance number used to identify the OMCI message and contains four bytes. The message start identifier may be employed to indicate the commencement of a multi-carrier embedded address, thus facilitating the receiver's identification of the relevant position. This technique is based on the conversion of encrypted data into a binary bit stream, which is then used as transmission data after applying hybrid encryption. The sender transmits the encrypted data through the P2P network of the blockchain, and the message start identifier is required to inform the receiver of the commencement of the valid field, given that the editable transaction fields in the block structure are combined with a special arrangement to transmit the encrypted information.

In the MCHE model, the message start identifier and the message start identifier for the subsequent communication are embedded within the address. This enables the receiver to identify the pertinent information from a string of addresses by utilising this indicator. The message start identifier to be employed in the subsequent communication is communicated to the receiver in advance, thus enabling the latter to prepare for the next communication. This represents a step towards improving the efficiency of the communication process.

3.3 Multi-Carrier Co-Construction

Among the modifiable fields in the blockchain, the following are embedded in the transaction address: MSI, encryption information, public key hash, transaction timestamp, transaction amount, transaction fee, transaction signature, and MSI of the next communication. The manner in which these eight modifiable fields are embedded in the address greatly improves the efficiency of communication on the blockchain. Once the message start identifier has been applied, the multi-carrier co-constructed information is that which is to be encrypted. As this is a valid field, it should therefore be placed after the message start identifier. Multi-carrier co-construction represents a flexible approach to the transfer of information. Any information required by both parties can be included in the multi-carrier. However, as the number of carriers increases, the potential for risk also rises. Consequently, the MCHE model proposes the

Copyright @ STEMM Institute Press

inclusion of eight carriers in the address.

3.4 Ring Signatures

The concept of ring signatures was initially proposed by Rivest et al. [2]. These are a special kind of group signature that does not rely on a trusted centre or a group establishment process. Instead, they are designed on the idea of replacing the original need for a specific single public key with a collection of public keys. In the context of the ring signature scheme, the signature forms a closed loop. The underlying principle is that the signer is able to utilise their own private key in conjunction with the public keys of other members of the ring, obviating the necessity to obtain consent from third parties for the use of their public keys. Furthermore, the signer is able to employ the public key of any individual. The verifier performs a specific verification process, but is only aware of the signature within the ring and not the identity of the signer. This ensures the signer's anonymity, while the private key held by the user guarantees the security of the blockchain, as only the private key holder is authorised to access the data [3]. The initial stage of the process entails the generation of public-private key pairs for each user. This involves the input of security parameters, which facilitate the generation of public-private key pairs for each user. Subsequently, the signatory selects one or more public keys belonging to other members, thereby establishing a ring. The message is then signed by the sender using their private key, and the resulting signature is combined with the public keys of other members of the ring to generate a ring signature. Subsequently, in order to verify the signature, the ring signature and associated parameters are entered in order to confirm the validity of the signature.

3.5 Single Leader for Multiple Blocks

The Bitcoin-NG protocol introduces a novel trust model that decouples the election of leaders and the order of transactions [4]. The protocol divides time into discrete cycles, during which the leader in each cycle is permitted to add multiple microblocks consecutively until a new leader is elected. In this approach, the cost of sharing is distributed between current and future leaders, and the fork problem is addressed by extending the longest chain that contains all key blocks. This model represents a departure from the traditional blockchain model, in which each block is generated by a single leader. The proposed model is designed to enhance the throughput and processing speed of the blockchain network. The implementation of the MCHE model in a context of a single leader for multiple blocks would result in a significant increase in the speed of cryptographic communication.

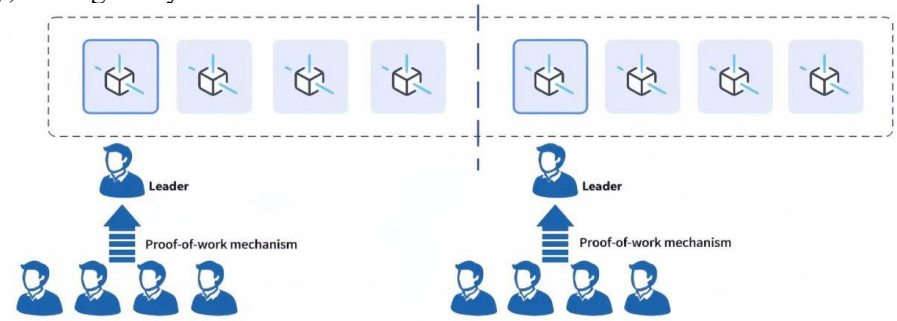

Figure 4. Multi-Block Single Leader Model.

4. Extension of the MCHE model

4.1 MCHE Model Advantages

In light of the findings of the literature review, this paper will proceed to undertake a comparative analysis of several cryptographic communication models, as shown in Table 1.

Table 1.Cryptographic Communication Models

Programme	Technical	Advantages	Disadvantages
Blockchain covert communication solutions	(math.) elliptic curve algorithm	Using Bitcoin's Address Generation Mechanism to Mask Sensitive Information	Single encryption mechanism that relies on address generation rules and pre-shared keys for limited transmission efficiency
BLOCCE	Least Significant Bit	Easy to implement	Low channel utilisation and inefficient communications

 Copyright @ STEMM Institute Press

BLOCCE+	Least Significant Bit and Multi-Signature Identity	Ensure uniqueness and tamperability of messages	Low channel utilisation and inefficient communications
semi-constructive covert communications model	Semi-constructive information hiding and elliptic curve algorithms	Higher volume of information transmission, better communication efficiency and covertness	Complexity of realisation and multi-vector embedding affects concealment
MCHE model	Hybrid RSA+AES encryption, ring signature, multi-block single leader mechanism, multi-signature identity	High encryption and decryption efficiency, high anonymity, fast processing speed, high transmission capacity	Complex implementation, high computing and storage resource requirements

4.2 MCHE Model Scenario Application

The comparison demonstrates that the MCHE model is an optimal choice for scenarios where the necessity for privacy, efficiency, transmission volume, and continuity is exceptionally high.

Firstly, the transmission of confidential information between governments, highly confidential information transmission by multinational enterprises, and the transmission of military instructions and intelligence, amongst other things, requires the most secure encrypted communication. The MCHE model employs RSA+AES hybrid encryption technology to guarantee a high degree of security in the transmission process. Furthermore, the ring-signature mechanism ensures that the content of the communication is anonymous and not easily traceable. Secondly, the MCHE model can be employed in financial or blockchain asset transfer, covert financial transactions and high-frequency fund deployment. This is due to the fact that the model encrypts and protects transaction information and masks user identity, thereby rendering it suitable for covert financial activities involving sensitive assets. Furthermore, the MCHE model can be utilised in a multitude of other contexts, including the Internet of Things (IoT), smart city monitoring, covert device data transmission and distributed smart device control.

5. Conclusion

This study proposes a Multi-Carrier Hybrid Encryption (MCHE) model for the secure communication of data across networks, utilising the capabilities of blockchain technology. The model integrates a number of cryptographic techniques, including hybrid encryption and ring signatures, thereby enhancing security and privacy. The MCHE model facilitates efficient encrypted communication while preventing third-party interference, eavesdropping, and data tampering. Furthermore, the model enhances the efficiency of communication within the blockchain system by utilising the concept of multiple blocks with a single leader. This approach allows individuals, industries and governments to secure data transfers, prevent unauthorised access and protect sensitive information.

Nevertheless, the MCHE model encounters certain constraints in its practical deployment. The first limitation of the model is that it is complex to implement and has high computational resource requirements, which are not compatible with resource-constrained devices or networks. Furthermore, the model results in an increase in transaction costs due to the substantial amount of supplementary information embedded in each transaction. In scenarios involving multiple parties, the process of updating keys may prove challenging.

References

[1] Yang, L. L. & Han, H. L.. (2006). Information security in network communication using hybrid encryption. Science and Technology Intelligence Development and Economy (16), 214-215.

[2] Rivest R L, Shamir A, Tauman Y . How to Leak a Secret[C]// Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Springer, Berlin, Heidelberg, 2001.

[3] Wang, Ruijin, Yu, Suzhe, Li, Yue, Tang, Yucheng & Zhang, Fengli. (2019). Ring signature-based private data sharing model for medical blockchain. Journal of

University of Electronic Science and Technology (06), 886-892.

[4] Eyal, I., Gencer, A. E., Sirer, E. G., & van Renesse, R. (2016). Bitcoin-NG: A scalable blockchain protocol. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 3-18). IEEE. https://doi.org/10.1109/SP.2016.27.

 Copyright @ STEMM Institute Press