Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4618007, 18 pages
https://doi.org/10.1155/2022/4618007

Research Article

The Applications of Blockchain in the Covert Communication

Bangyao Du,[1,2] Debiao He,[3,4,5] Min Luo,[4,6] Cong Peng,[4,7] and Qi Feng[4]

[1]*Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China*
[2]*Hangzhou Innovation Institute, Beihang University, Hangzhou 310052, China*
[3]*Shandong Provincial Key Laboratory of Computer Networks, Qilu University of Technology (Shandong Academy of Sciences), Jinan 250014, China*
[4]*School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China*
[5]*Institute of Network System and Security, Peng Cheng Laboratory, Shenzhen 518000, China*
[6]*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China*
[7]*Shanghai Key Laboratory of Privacy-Preserving Computation, MatrixElements Technologies, Shanghai 201204, China*

Correspondence should be addressed to Debiao He; hedebiao@163.com and Min Luo; mluo@whu.edu.cn

Received 11 January 2022; Revised 3 March 2022; Accepted 5 May 2022; Published 14 June 2022

Academic Editor: Antonio Guerrieri

Covert communication is designed for hiding the subliminal communication which takes place between both of the speakers and their relationship. The traditional covert communication utilizes the centralized channel and the third-party central node or authority to distribute messages which leads to a lack of undetectability, antitraceability, and robustness. In recent years, there have been attempts to apply the blockchain to covert communication solutions, for the characteristics of blockchain such as decentralization, openness, and trustworthiness. In this paper, based on the analysis of the literature and the classification according to the hiding position, we identify four kinds of covert communication: Address Channel, Value Channel, DSA (Digital Signature Algorithm) Channel, and Script Channel, which will help inform future research agenda.

1. Introduction

With the flourishing development of the Internet and computer science, network users communicate more and more on the Internet. The increasingly frequent interactions attract universal attention to the safety problem of information on the network, especially for some important sensitive information. So there is an expectation that covert communication can be realized to protect the safety, integrity, and secrecy in the process of information exchange.

The design goal of covert communication is to hide the relationship and the actual information exchange between the sender and the receiver beneath the superficial phenomenon. Where there is covert communication, there usually exists a subliminal channel. In 1983, Simmons [1] put forward the concept of the covert channel when solving the prisoners' problem that two prisoners want to construct a covert channel to plan an escape in an apparently normal conversation. A covert channel refers to a secret channel established in the digital signature, authentication, and other cryptosystems based on the public key infrastructure. Except for the sender and the designated receiver, no one knows whether there exists covert information in the transmitted cryptographic data content.

Traditional covert communication is served by a centralized channel generally, which results in the vulnerability to the interface of environment and other factors in the process. By monitoring the network and measuring the traffic, a covert channel can be distinguished by the attacker. Once the covert channel is detected by the attacker, participants are under threat of being exposed. In addition, the centralized nodes and devices are too weak to survive the attack, and the worst case may lead to the paralysis of the communication system.

Furthermore, the covert message is usually delivered directly to the receiver. It is sufficiently challenging to find a solution for group covert communication under the circumstance of the traditional method.

As a break of the mainstream mechanism that relies on the third parties in information and trade exchanges, the blockchain [2] is a new technique developing rapidly recently. The blockchain has the characteristics of decentralization, nontampering, nonforgery, openness, and security, which draw the attention of all professions and trades. Not only financial services but also almost every electronic services start exploring the benefits of using the blockchain in their infrastructure. With the entry of the blockchain, new protocols, new applications, and new solutions are published, such as smart contracts, proof of existing services, and covert channels.

For example, the facilities of Bitcoin like Mastercoin [3] and Colored Coins [4] are used in many projects to provide alternative currencies and other financial instruments such as stocks and bonds. All these applications profit from the ability of Bitcoin transactions where additional information can be embedded, so that many scholars manage to apply the blockchain to construct subliminal channels in the field of covert communication.

Compared with traditional covert communication, the applications of the blockchain in covert communication can be highly advantageous. To start with, nodes of a peer-to-peer network in the blockchain flood transactions and blocks. The identity of the receiver will be kept hidden in this mode of communication because there has no specific destination. Under this circumstance, it is more likely to achieve group communication. For another thing, the popularity of Bitcoin continues to grow as shown in Figure 1, so are other cryptocurrencies in the blockchain. As of February 2022, more than 81 million people had created unique Bitcoin wallets on http://Blockchain.com which makes purchasing Bitcoin possible. A huge amount of members lead to tremendous transactions, which provides benefits for covert communication. Thirdly, the blockchain is free of any government or organizational control. Users can send transactions anywhere in the world without banking infrastructure or exchange fees, which fosters the applications of blockchain in covert communication.

1.1. Our Contributions. In this paper we make the following contributions:

(i) We present researches about covert communication with and without blockchain. We concentrate on the blockchain-based covert communication and present some typical work in detail

(ii) According to the secret hiding place, we divide the subliminal channels used in the covert communication schemes on the blockchain into four categories: Address Channel, Value Channel, DSA Channel, and Script Channel. Their definitions and how to embed a secret in each kind of channel are given in Section 5

(iii) We perform an analysis of the proposed channels from three aspects: capacity, concealment, and efficiency. The summary of the related works is analyzed and some suggestions for further research are given in the end

1.2. Organization of This Paper. The remaining of this paper is structured as below. In Section 2, traditional covert communication schemes are briefly explained. In Section 3, we introduce the relevant background materials. The review of some typical schemes is presented in Section 4; then, we classify the existing schemes according to their hiding location and analyze them in Section 5. We discuss the weaknesses of existing protocols and some research directions in Section 6. Finally, we make a conclusion of this paper in Section 7.

2. Traditional Covert Communication

As an application of information hiding technology, covert communication adopts unconventional patterns to break through restrictions of a message and employs steganography or coding permutation as a carrier to transmit the message secretly.

The blockchain appeared in the military field [5] for the first time. Images, audios, and videos are used to build subliminal channels to exchange military information while avoiding the enemy's monitoring. At the military communication conference in 2010, Hijaz and Frost [6] studied the potential of covert communication within an orthogonal frequency division multiplexing (OFDM) waveform and realized secret communication by inserting a covert narrowband signal in a new subcarrier location of OFDM signal. Harvey et al. [7] emphasized the special requirements of specific military local area networks and talked about how higher band millimeter-wave technology can help to achieve high data rate and concealment at the same time.

As the Internet develops, covert communication has been extended to many different fields in which cryptography is taken as a carrier. As public-key cryptography develops, many covert channels are proposed such as DSA-based [8], RSA-based [9, 10], and ECDSA-based [11]. Nevertheless, due to the bandwidth limitation, only a little message can be embedded in these schemes. Hartl et al. [12] proved the existence of a broadband covert channel in the EdDSA signature scheme. In 2001, Rivest et al. [13] formalized the notion of a ring signature and proposed a provably secure ring signature scheme. In 2012, Dong et al. [14] proposed an anonymous covert channel based on RST (Rivest, Shamir, and Taumann) ring signature to keep the signer himself covert anonymous to the covert receiver. In 2019, Wang et al. [15] proposed covert channels in the code-based ring signature scheme in which the designated receiver did not need to know the private key of the signer.

Based on different data carriers, there are three fundamental kinds of covert channels [16] called covert timing channels (CTCs), covert storage channels (CSCs), and covert network channels (CNCs). CTCs mainly use time stamp, the transmission time interval of data packet [17], and

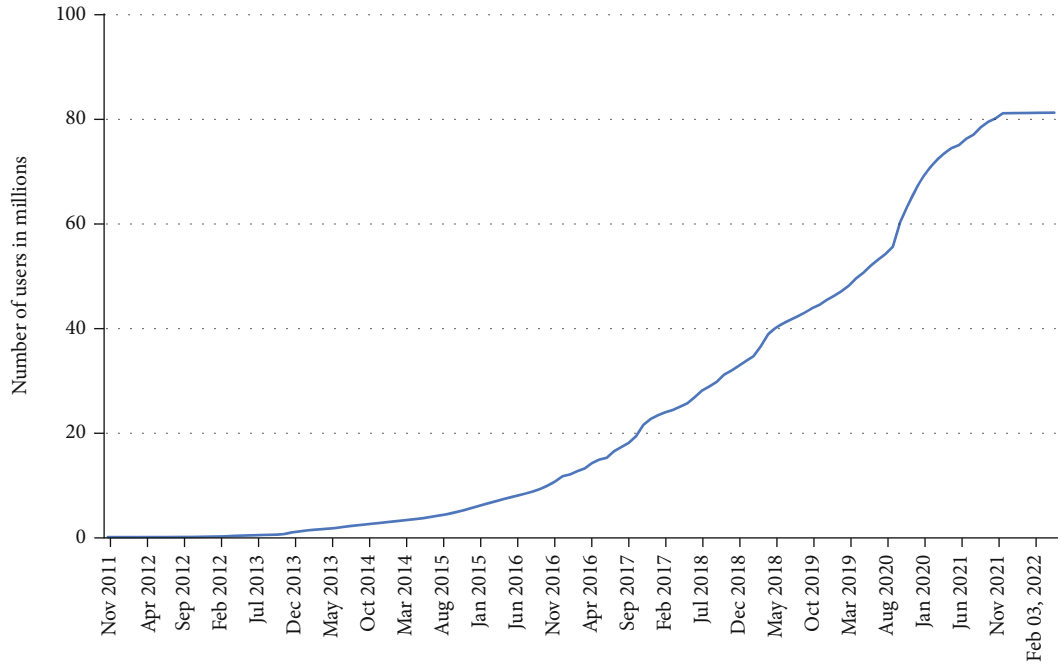

Figure 1: Number of blockchain wallet users worldwide from November 2011 to February 2022.

transmission quantity of data packet in unit time [18] to realize information transmission. Easy to be affected by network delay and jitter, CTCs have weak robustness [19]. And CSCs employ system variables or attributes except for time such as image [20, 21], protocol [22], and biological signal [23] to represent covert information. Different from CTCs, CSCs are not easy to be disturbed by the network environment and have better robustness, higher information embedding rate, and more types of carriers. CNCs include variations of CTCs, CSCs, and the properties of the network over which they operate [24, 25].

3. Preliminaries

In this section, we briefly review covert communication channel and the blockchain technology.

3.1. Covert Communication Channel. As a supplement to the traditional encryption technology, information hiding embeds information covertly into the media or carrier so as to transmit secret information without being noticed. At first, it only used static media like images as carriers to hide information. But in recent years, as communication technology and network media develop, the widespread adoption of information hiding in the field of communication has gradually developed into an emerging technology—covert communication channel.

Unlike the traditional encryption technology to hide the content of the message itself, covert communication is aimed at hiding the existence of a covert message. The information is transmitted secretly and the redundant part of the carrier serves to insert the processed information into communication and media messages. The model of a traditional covert communication channel with an omniscient knowledge of the covert channel is shown in Figure 2.

It is obvious that the covert/overt sender and receiver may not be the same node. So there are some requirements of the established channel to be covert and undetectable by the adversary.

(i) Subsurface; a covert channel ought to be hidden under an overt channel whose operation is not controlled by the adversary. If the overt channel gets closed, the covert channel will no longer exist.

(ii) Nonintervention and reasonable: there exist overt users, while covert users are using the communication channel. So users in the overt channel cannot be bothered or suspected, which requires the establishment of the covert channel to bring no damage to the existing channel.

(iii) Undifferentiated: in the communication channel, the covert data is supposed to be the same as the overt data. It is expected that the observer is not able to find out the difference between covert data and legitimate overt data.

3.2. Blockchain. As a data structure, blockchain consists of many blocks linked in the order of time from back to front which contain transactions submitted to it. The blockchain is also a tamper-resistant unforgeable distributed and decentralized ledger that can store sequential data which can be verified in the system. The addition of a consensus mechanism turns the blockchain into a trusted network. Block can be regarded as a container that aggregates inner transactions' information, whose structure is shown in Figure 3. TX refers to a transaction. It is composed of a block header

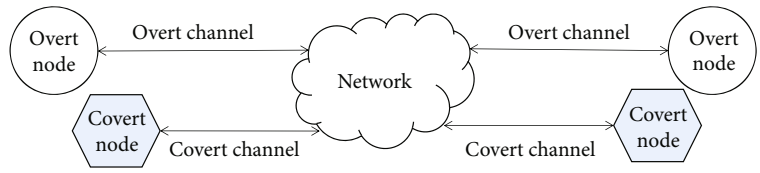

Figure 2: The model of traditional covert communication channel.

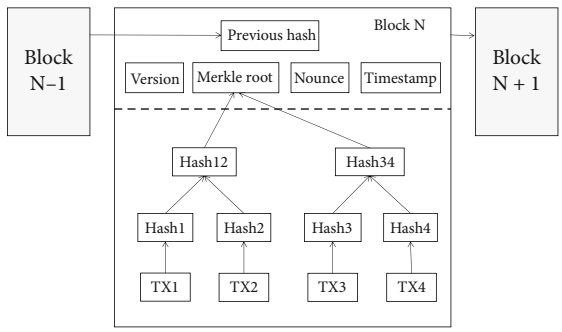

Figure 3: The structure of block.

followed by a series of transactions, which form the main body of the block. It has the following advantages.

3.2.1. Transparency. The openness and transparency of cryptography technology and data guarantee the security of the blockchain system. Anybody is able to join the blockchain as he wishes. Users can better supervise the data in the system and prevent dishonesty, denial, and disputes from happening. Cryptography guarantees that the exchanged message keeps privacy.

3.2.2. Decentralization. There are no intermediaries and trusted third parties in the blockchain. The recording, verification, restoration, and transmission of the blockchain data are all based on the distributed system architecture, rather than the traditional central structure. The whole network will not collapse due to the failure of several nodes or the attack on the central node, and the data will not be leaked due to the trust issues of the central node. So the blockchain has better fault tolerance and antiattack ability.

3.2.3. Traceability. Blockchain shows up as chain-like blocks with a timestamp attached, thus adding the time dimension and making it traceable and verifiable. Each node can track the changes in assets and transaction behavior according to the input and output of the transaction, which ensures the authenticity of data.

3.2.4. Immutability. Due to the special linked structure of blockchain, adjacent blocks keep in touch by means of hash values. Besides, the Merkle tree of each block guarantees that the transaction information cannot be distorted. Once the value of Merkle root is modified, the nonce in that block header is no longer legitimate. If an attacker wants to modify values in an existing block, he will have to modify the corresponding values in the latter block until the end of the chain to meet the needs of validation, which requires such tremendous computing power that it cannot be achieved within the time limit of consensus mechanism.

3.2.5. Collective Maintenance. A specific mechanism is adopted to make sure that all the nodes in the system take part in the validation procedure of data blocks during which a particular node is chosen through a consensus algorithm to append new blocks to the blockchain. All nodes jointly maintain the network while keeping their local ledger.

3.2.6. Anonymity. In the blockchain system, the addresses and accounts are generated by the user himself as long as they are legitimate. From an observer's point of view, the identity of the participants cannot be obtained directly from the transaction information.

3.3. Types of Cryptocurrency. On the basis of the open-resource blockchain technology, any developer has the access to the original source code which contributes to the upper creation. It should be noted that cryptocurrencies such as Bitcoin are built on the blockchain rather than take the place of it. Blockchain is merely used as a way to record purchases, payment information, etc. As is shown in Figure 4, it is estimated by http://statista.com that there are more than 10000 transactions as of the writing.

Although cryptocurrencies are virtual currencies, they can be traded or invested like any other real currencies and are particularly independent of banks and governments. The "crypto" part in cryptocurrencies indicates complex cryptographic algorithms used to deal with the processing of digital currencies and their exchange across decentralized users. There is not one "best" cryptocurrency because each developer's design is focused on a certain point to solve an existed problem.

Here is an overview of some of the most popular digital coins and how each is being used. Table 1 provides the methods of signature used in mainstream cryptocurrencies and their pros and cons. The circulating supply of each cryptocurrency is updated on Feb. 28, 2022. Type refers to whether the cryptocurrency is based on the UTXO model or not. The Signing Alg shows what kind of signing algorithm is adopted, and the elliptic curve used is shown in the column Curve.

Regarded as the first blockchain-based cryptocurrency launched by Satoshi in 2009, Bitcoin is the most popular and the biggest by market capitalization with the elimination of trusted third parties. Ether plays the role of the token on Ethereum to facilitate transactions. Designed on the basis of RippleNet, a digital payment platform, XRP was planned for financial institutions. In Litecoin, central processing

units (CPUs) can help the decoding process. Zero-knowledge proofs (zk-SNARKs) provide users in ZCash absolute privacy with no information leaked during validation. Taking advantage of the ring signature, Monero is able to hide the complete privacy of the sender. Unlike serving as a store of trading, Dash is devoted to becoming a real-life form of payment. In addition to payments, Lumens (XLM) can be used to fight spam.

3.4. Ethereum. Forbes mentioned that Ethereum is the first generic blockchain platform that allows users to create and deploy their decentralized and trustless applications easily. It has created incredible opportunities in the FinTech space. This section will introduce what Ethereum is and the Whisper protocol therein.

Ethereum is a decentralized application platform on the strength of blockchain technology. It allows users to establish and have distributed applications running on this platform in a decentralized manner. This means that applications running on Ethereum are available anywhere and anytime.

Compared with Bitcoin, Ethereum uses the account model rather than UTXO. This brings some advantages. Each transaction in Ethereum has only one input, one output, and one signature, thus saving much space and making it easier to understand. And the simple coding ability is required while there is no need to write complex scripts.

In the Whisper protocol, based on blockchain, Ethereum provides context both for the distributed applications (DAPP) and for the developers. In a DAPP where participants manage to reach an agreement, one-on-one communication between them is of great importance. That also accounts for the reason why Whisper takes a significant part under the circumstance of Ethereum [26]. Serving as the "decentralized communicate" component, Whisper works on a peer-to-peer framework with no server participating throughout the whole process and allows nodes to conceal the correlative information from unrelated parties while securely interacting with each other.

All the messages broadcast on the public network are routed according to the topic specified as shown in Figure 5 until they reach their destinations. Since there is a direct correspondence between every topic and the key to encrypt/decrypt data, that is to say, the covert message is encrypted with the public key of the recipient and is spread afterward. Nodes can apply for interested topics. Then, only messages with these topics will be received, the others will be abandoned.

The envelope acts as the basic data transfer unit in the Whisper protocol [27], whose structure is shown in Figure 6. There are two components in the envelope: enciphered data body and unencrypted metadata utilized for verification and data decryption in the envelope.

RLP (Recursive Length Prefix) encoding format is used while transmitting envelope.

(i) Version: 4 bytes at most (only 1 byte is being used now). During the transmission, if the envelope has a higher version than the node gets, it will not be decrypted and be forwarded only

(ii) Expiry: 4 bytes (UNIX timestamp in seconds) represents expiration time

(iii) TTL: 4 bytes, remaining survival time of the envelope in seconds

(iv) Topic: 4 bytes. The envelope is designed to have only one topic each. Besides, there is a consistent one-to-one match between each topic and the key required in the process of encryption and decryption

(v) AESNounce: 12-byte random digit, valid merely in symmetric encryption

(vi) Data: encrypted data body, whose role is to store message. It mainly consists of two parts. One is payload where the genuine information is located and is often enciphered in advance. The other is padding used to lower the risk of information exposure through the length

(vii) EnvNonce: 8-byte arbitrary data (for PoW calculation)

(viii) PoW: The aim of exploiting PoW is to reduce the quantity of junk mails and lighten network loads

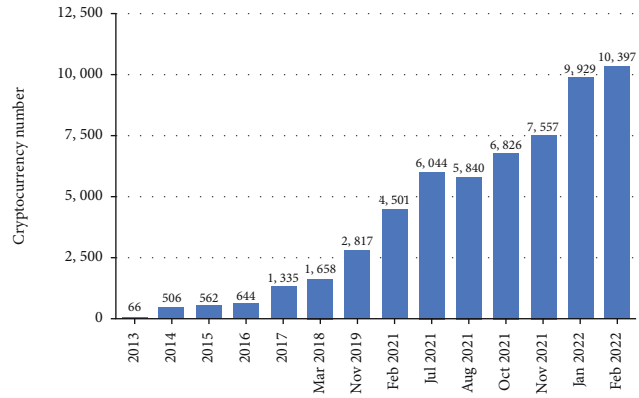

Figure 4: Number of cryptocurrencies worldwide from 2013 to February 2022.

The default rule to set data in version 5 is to keep the data length at multiples of 256 bytes. When obtaining an envelope whose topic is acknowledged, it will be decrypted by the appropriate key to gain the real information. Obviously, the identity of the sender in Whisper cannot be traced, let alone the location of the sender.

In the Whisper protocol, after each peer is connected successfully, two goroutines are generated to receive and broadcast messages.

3.5. Smart Contract. The concept of smart contract was first put forward in 1994. Smart contract was aimed at satisfying general needs, minimizing baleful and abnormal conditions, and lowering dependency on trusted intermediaries. The

Table 1: Mainstream digital currencies on blockchain (updated Feb. 28, 2022).

Name	Symbol	Type	Signing Alg	Curve	Pros	Cons	Circulating supply
Bitcoin	BTC	UTXO	ECDSA	secp256k1	Independence from central authorities; user anonymity and transparency.	No government regulations; limited use.	18,970,150 BTC
Ethereum	ETH	account	ECDSA	secp256k1	Second-biggest cryptocurrency; fast transaction speed.	Uncapped supply leads to inflation.	119,761,811 ETH
Ripple	XRP	account	ECDSA	secp256k1	Lightning fast transaction speed; cheap.	Less secure consensus protocol.	47,949,281,138 XRP
Litecoin	LTC	UTXO	ECDSA	secp256k1	Faster confirmation; cheap transaction fee.	Low market captalisation.	69,734,906 LTC
Zcash	ZEC	UTXO	ECDSA, zk-SNARKs	secp256k1	Prominent level of anonymity; fungible and interchangeable.	Restricted to CPU mining.	13,841,481 ZEC
Monero	XMR	UTXO	ECC, MLSAG	ed25519	Block limit flexibility; well security.	No mobile wallet; weak scalability.	18,085,509 XMR
Dash	DASH	UTXO	ECDSA	secp256k1	Faster confirmation speed; lower transaction fee.	Theoretical traceability.	10,603,264 DASH
Stellar	XLM	account	EdDSA	ed25519	Integrates with banks.	Not widely recognized.	24,943,914,340 XLM

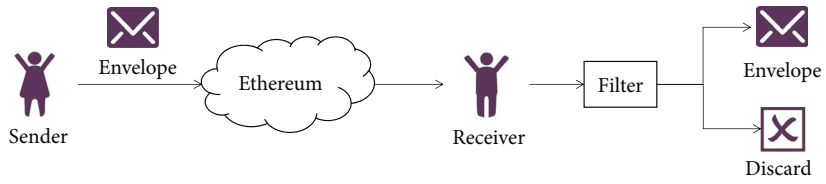

Figure 5: Message transmission in Whisper.

smart contract has been applied in many fields such as identity management [28], IoT [29], and medical privacy [30].

The smart contract makes the blockchain-based applications more convenient and expandable. While the contract is written into the blockchain in a digital form, the written data cannot be deleted but can be added or altered as a result of the characteristics of the blockchain. The whole process is transparent and trackable to ensure historical traceability. Because the behavior will be permanently recorded, the interference of malicious behavior on the normal execution of the contract can be avoided to a great extent. With the influence of centralization factors avoided, the cost efficiency of smart contract improves a lot.

4. Review of Blockchain-Based Covert Communication Protocols

Due to the immutable chain structure and distributed storage schema, a secure channel can be offered by blockchain. It requires extremely high cost that nearly nobody can afford to alter or fabricate the historical blocks. Because the blockchain network is on the basis of the peer-to-peer network, no third-party provider is needed while establishing the communication channel and delivering messages on it, thus making the blockchain-based covert communication protocols invulnerable to any availability attacks.

Version	Expiry	TTL
Topic	AESNounce	
Data	EnvNounce	
PoW		

Figure 6: The structure of envelope.

We investigated a number of recent papers related to blockchain-based covert communication protocols. Here, we make brief illustrations of some typical schemes by supposing a scene in which Alice, the sender, tries to dispatch a message denoted by M secretly to Bob, the receiver.

4.1. BLOCCE. Partala [31] provided an illustration of the method called $B\text{LOCCE} = (\text{Gen}_{\text{BLOCCE}}, \text{Embed}, \text{Extract})$ (Blockchain Covert Channel) in detail.

It is assumed that the latent message is of constant length and known to both Alice and Bob. Before transmission, a pretreatment of M, a symmetric encryption algorithm $\text{SE} = (\text{Gen}_{\text{SE}}, \text{Enc}, \text{Dec})$ whose secret key k is required. The protocol shown in Figure 7 proceeds as follows:

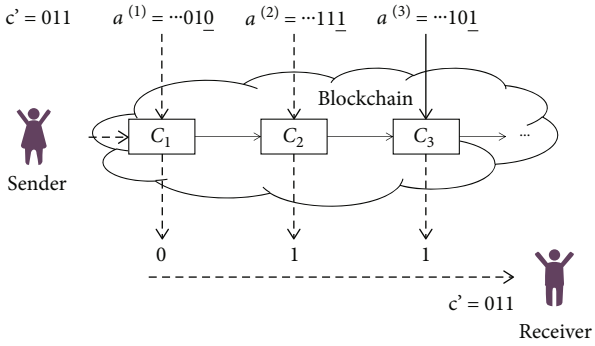

Figure 7: A simplified overview of BLOCCE.

Step 1 ($\text{Gen}_{\text{BLOCCE}}$): Alice produces a lot of private/public key pairs $(s_k^{(1)}, p_k^{(1)}), (s_k^{(2)}, p_k^{(2)}), \cdots, (s_k^{(n)}, p_k^{(n)})$ and calculates the billing addresses $a^{(1)}, a^{(2)}, \cdots, a^{(n)}$ correspondingly

Step 2 (Embed): a small quantity of transfer transactions are generated by Alice from her individual account to the newly generated addresses in the previous step. In advance, according to the secret text $c' \longleftarrow \lambda||c, c \longleftarrow \text{Enc}(k, M)$ of the plaintext M and a random message start indicator λ, Alice orders these addresses to use the least significant bits (LSBs) of the payment addresses to make up c'. Note that both Alice and Bob know n_λ (the length of λ) and $|c|$ (the length of c) denoted by $N = n_\lambda + |c|$, where N is the length of hidden text message c'.

Step 3: Alice submits payments to the blockchain in the correct order and for each block, there is a single payment from Alice, so that the message can be gathered properly.

Step 4 (Extract): after reading the blockchain and filtering out transactions made by Alice, Bob can concat the LSBs of the payment addresses to obtain the hidden text. The first n_λ bits generates λ, while the next $|c|$ generates ciphertext c. Eventually, the plaintext message $M \longleftarrow \text{Dec}(k, c)$ can be extracted.

This protocol is considered the first attempt to combine blockchain with covert communication. The size of data carried in each transaction is so small that it will not be used for real. Although it has extremely low efficiency, it contributes a lot to the following research.

4.2. V-BLOCCE. Improving on the BLOCCE, Lejun et al. [32] proposed the V-BLOCCE, a covert communication method. In this method, the covert message is coded in the form of Base58 and the addresses including embedded data are generated by Vanitygen. Figure 8 shows the integrated procedure of the system.

Step 1: the message M is encrypted into a provisional cipher and then completed with the Base58 encoding to get the ultimate ciphertext.

Step 2: All the different characters appeared in the final ciphertext are stitched into a string which is provided for the Vanitygen software to generate Bitcoin addresses.

Step 3: Alice goes through these addresses looking for matches with the characters of ciphertext. If a match is found, the index of the character in the ciphertext and the index of the addresses are recorded as a tuple in a list. In this way, the information is embedded with the index list generated. Then, the addresses are sorted in order of their hash value and the index lists are encrypted to be filled in the OP_RETURN field.

Step 4: Bob scans the transactions sent by Alice for the transaction information. Next, he picks up the order of the address used and the index information from OP_RETURN which are used to determine every character and its location to restore the ciphertext. It is decoded by Base58 and then decrypted to acquire the real message M.

Based on the protocol in Subsection 4.1, it improves the efficiency of data entry into special transactions. Furthermore, it leads the attention of researchers to the script field in the transaction, which brings more potential application to this domain.

4.3. DLchain. Tian et al. [33] proposed a new blockchain covert channel construction scheme implemented with dynamic labels which are generated on the basis of the distribution of a large amount of real transaction data to guarantee its dynamic and variety. Here, the OP_RETURN script is chosen to carry labels whose fixed length is 23. The scheme process is shown in Figure 9.

Step 1: dynamic labels are produced by both sides in the communication at the same time. So the receiver is able to recognize specific transactions coming from the sender.

Step 2: a prenegotiated key is employed to encrypt the message. Then, the encrypted messages take the place of the private key required in signature generation. At last, the sender signs two transactions with the particular private-key and packages the agreed label into them.

Step 3: after verification, the transactions spread through peer-to-peer connections online and the corresponding record is kept by the blockchain.

Step 4: in the light of the negotiated dynamic label, transactions with information hidden can be identified and filtered.

Step 5: the receiver extracts the secret message.

Taking the DGA algorithm Banjori [34] as a reference, the dynamic label generation algorithm is designed after analyzing the universal distribution of the OP_RETURN scripts in the practical transaction data statistically to make the label indiscernible.

This protocol focuses its attention on the verification phase. It is perceived that many special transactions with the covert message are attached to a fixed label so that receiver can make a distinguishment. This protocol puts forward a dynamic label generation algorithm which is frontline at that time.

4.4. Whispers on Ethereum: Blockchain-Based Covert Data Embedding Schemes. Liu et al. [35] used the VALUE field of a transaction in the Ethereum system to construct a one-bit embedding (OBE) scheme and an HMAC-based multiple-bit embedding (HMAC-based MBE) scheme. Furthermore, a Hash-based multiple-bit embedding (Hash-based MBE) scheme is proposed to enhance the covertness.

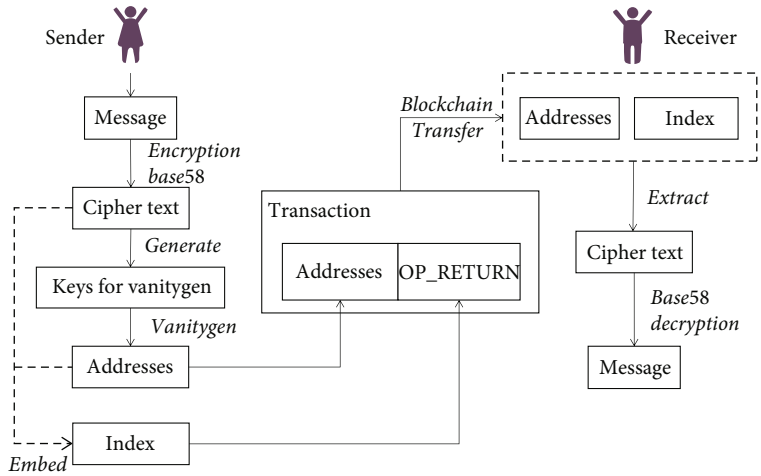

Figure 8: The procedure of the V-BLOCCE method.

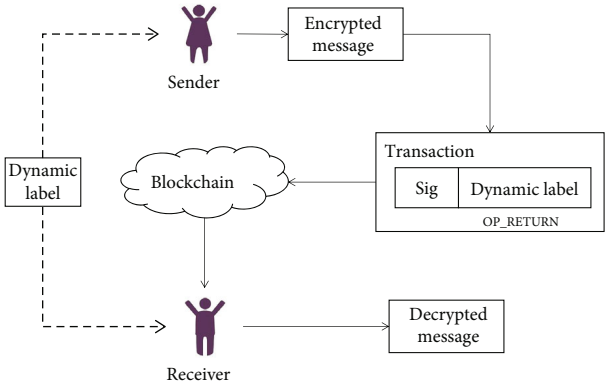

Figure 9: DLchain architecture.

The hidden message in all the proposed schemes is stored directly in the VALUE field.

Liu et al. [36] proposed a novel Monero-based covert communication system which provided higher security to fend off Eclipse attacks [37] and node crawling attacks [38]. The covert data is converted to decimal and then takes the place of the amount field in the transfer transaction. At the same time, the application of Stealth Address implements the anonymity of the receiver, while the application of the ring signature guarantees the privacy of the sender.

In these three schemes mentioned before, the AES encryption scheme is used to encrypt secret data M before it is embedded into the transactions which is defined as $c = r||\mathrm{AES}_{k_1}(r) \oplus M$. Here, c is the cipher text, k_1 is the encryption key and even if the same message M is encrypted for multiple times, the ciphertext will not be the same thanks to the random number r; thus, the chosen plaintext attack can be resisted.

4.4.1. The OBE Scheme. Transactions are constructed for each bit by filling in the VALUE field when traversing the ciphertext c bit-by-bit as is shown in Figure 10. There are two intervals V_0, V_1 representing the result of the HMAC. For every bit in c, if the bit $c[i]$ is 0, calculate a number VALUE to meet the demand that its HMAC result $\mathrm{HMAC}(k_2, \mathrm{VALUE})$ is in the set V_0. k_2 is the HMAC key. And when the bit $c[i]$ is 1, then calculate a number VALUE whose HMAC result $\mathrm{HMAC}(k_2, \mathrm{VALUE})$ stays in the interval V_1. In this scheme, only one bit is loaded in a transaction, which means the embedding rate is 1 bpt (bit per transaction).

Since the OBE scheme has low efficiency in the aspect of the embedding rate, a multiple-bit embedding scheme is further proposed as shown in Figures 11 and 12.

4.4.2. The HMAC-Based MBE Scheme. The first bit of the VALUE of the transaction is supposed to be 1. Then, we traverse the ciphertext c, for each bit $c[i]$, we select a number from 0 to 15 to make the HMAC result in the corresponding interval similarly to the OBE scheme. In this way, every 4 bits generated to represent 1 bit of the ciphertext will be placed in order together with the first bit 1 in the VALUE field of the constructed transaction.

4.4.3. The Hash-Based MBE Scheme. Apart from the covert data, the obfuscation data in this scheme is introduced to confuse the attacker. Before constructing the covert channel, a mixed hash root indicating the index of significant bits in the VALUE field of each transaction needs to be known to both the sender and the recipient. Valid ciphertext is divided into bits which are sequentially stored in the location of bit "1" in the binary representation of the mixed hash. Note that the second bit of VALUE and the first bit of the mixed hash should align. Moreover, the mixed hash of the first embedded transaction hashs from the mixed hash root while the mixed hash of the latter transaction hashs from that of the former transaction.

This protocol uses VALUE field in the transaction, which makes the embedding rate related to the length of value. Nevertheless, the requirements for special value in the special transaction may arise suspicion which needs be considered in the future work.

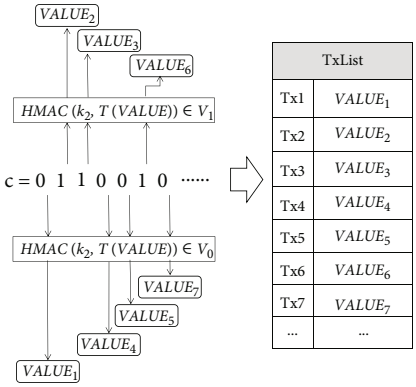

Figure 10: One-bit embedding (OBE) scheme.

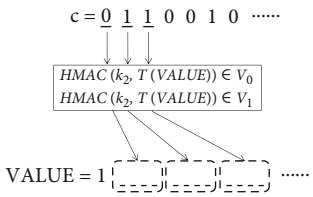

Figure 11: HMAC-based MBE scheme.

4.5. A Covert Communication Model Based on Ethereum's Whisper Protocol. Zhang et al. [39] designed a new covert communication model shown in Figure 13 founded on the Whisper protocol which is applicable to Ethereum.

In the architecture of Whisper network, envelope which consists of enciphered data and unencrypted data is the basic form of data transmission. Each envelope contains a topic introduced to scan for the target envelopes, and there is a one-to-one mapping between each topic and a encrypt/decrypt key. The protocol proceeds as follows:

Step 1: before transmission, each node participating in the covert communication needs to interact with Whisper to obtain the topic and key. Next, the secret message M will be encrypted to C to ensure its concealment.

Step 2: Alice sets the value of payload and padding to establish the envelope which is encrypted with the key obtained in step 1. The payload is either generated randomly or provided by Alice. For each bit of C, Alice compares it with each bit of the payload working as a carrier. If the match is successful, Alice will take down the indexes of the carrier and corresponding encrypted message.

Alice replaces the matched bits in C with * and repeats the former step until the message has only * or the payload does not contain any message characters. In the meanwhile, two index arrays are generated and stitched together as the first part of the padding P_1. Then, Alice sets a splitter R as the second part and a random redundant field P_2 as the last part of the padding. And P_1, R, P_2 are spliced into the padding.

Step 3: some attributes like TTL are packaged with the topic of the envelope set to construct the envelope.

Step 4: with the widespread of envelope, Bob is able to find out the particular envelope with the negotiated topic and obtains the payload and padding. After obtaining padding field, P_1 can be gained by deleting R and P_2 and then be decrypted to obtain the index arrays, according to which the ciphertext C can be restored and then decrypted to the original message M.

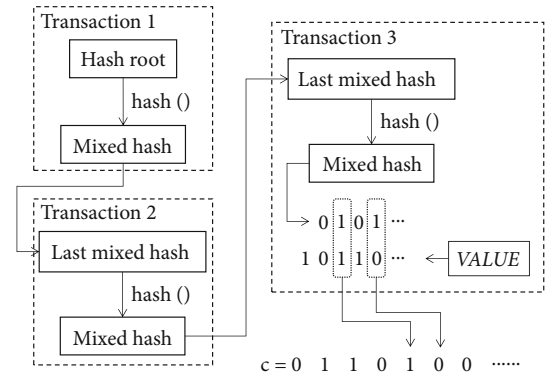

Figure 12: Hash-based MBE scheme.

This protocol takes advantage of Whisper protocol in Ethereum which is unique to other blockchain platforms. Focusing on the specific characteristics of current blockchain products provides innovation and alternative to the further research.

4.6. CCBRSN. Wang and Su [40] proposed a system called Covert Communication based on Bitcoin Regtest Self-built Network (CCBRSN), which takes blockchain as a covert communication channel.

The secret message is embedded into the blockchain's addresses in transmission. DES and Base58 are used to encrypt and code the secret message before embedding the encrypted message into a group of addresses which is employed to conduct a ciphertext-embedded transaction. As is shown in Figure 14, the system works as follows:

Step 1: Alice uses DES to encrypt the secret message M whose encryption key k is prenegotiated to get the result $\mathrm{DES}_k(M)$. Then, Base58 is called to encode $\mathrm{DES}_k(M)$ into $\mathrm{Base58}(b)$.

Step 2: Alice uses ECDSA while generating a private/public key pair $(\mathrm{sk}^{(1)}, \mathrm{pk}^{(1)})$. Then, $\mathrm{pk}^{(1)}$ needs to be computed using SHA256 hash, RIPEMD160 hash, and Base58 step by step to produce a corresponding address $a^{(1)}$.

Step 3: for every bit of $a^{(1)}$, Alice matches it with each bit of $\mathrm{Base58}(b)$. If succeed, Alice will record corresponding indexes of $a^{(1)}$ as set^a and indexes of $\mathrm{Base58}(b)$ as set^M which meet the equality that $a^{(1)}[set_k^a] = Base58(b)[set_k^M]$ (k means an arbitrary but the same place in the set).

Step 4: with the corresponding bits in $\mathrm{Base58}(b)$ replaced by *, $\mathrm{Base58}(b)$ is consequently transformed into $\mathrm{Base58}(b1)$. Then, Alice continues to repeat the same procedure for $\mathrm{Base58}(b1)$ until every bit in $\mathrm{Base58}(b1)$ is replaced.

Step 5: a transaction whose output addresses are $a^{(1)}$, $a^{(2)}, \cdots, a^{(n)}$ is submitted to the blockchain. And the earlier the address is generated, the more the transaction fee will be set to define the sequence. Then, the sets $\{\mathrm{set}^M\}_n$, $\{\mathrm{set}^a\}_n$ and transaction ID TxID are packed into a file *File* for the following extraction.

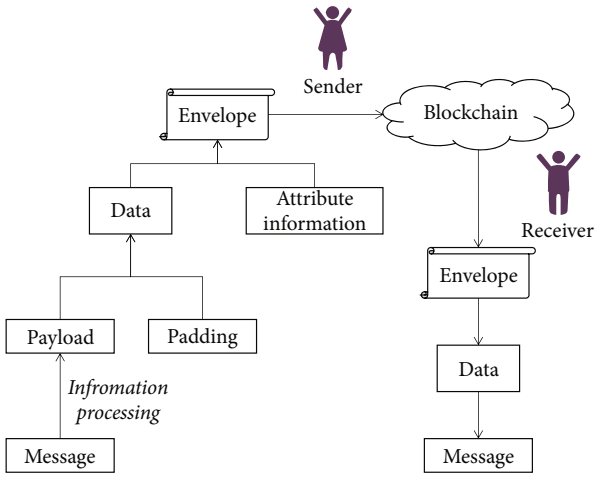

Figure 13: Covert communication model on Whisper.

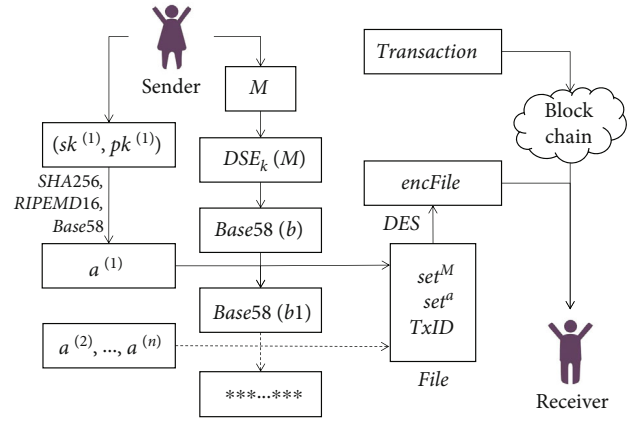

Figure 14: The process of CCBRSN execution.

Step 6: to protect the content of *File*, DES encryption is applied with a negotiated key before encrypting *File* into *encFile*.

Step 7: having received the *encFile*, Bob first decrypts it into *File* to obtain $\{\text{set}^M\}_n$, $\{set^a\}_n$ and TxID. And then, he finds the transaction in line with the TxID, gets the output addresses, and restores the ciphertext according to the correspondence.

Step 8: finally, after decoding with Base58 and decrypting with DES, Bob transforms the ciphertext into plaintext, so-called the secret message M.

With essential data for encryption/decryption recorded in an extra file and encoded data recorded in the addresses, this protocol achieves the cooperation between online transactions and offline transfers. However, when there are a lot of online transactions and offline files delivered to the receiver, it may lead to a mismatch.

4.7. A Covert Communication Model Realized by Using Smart Contracts. Zhang et al. [41] proposed a covert communication model combined with smart contracts to covertly transfer information under the blockchain circumstance. The parameters in the contract are used to carry the secret message, and the covert communication is completed by calling the smart contract.

Supposing that the secret message is encoded in ASCII format after the negotiation between Alice and Bob, a number ranging from 0 to 95 can represent any one of the 95 characters from 32nd to the 126th in the ASCII table. Take the biding contract as an example, the protocol shown in Figure 15 proceeds as follows:

Step 1: before communication, Alice and Bob need to reach a consensus on the effective price range interaction where quotations can be made. When bidding, the two decimal places are regarded as a carrier considering the number of characters used is 95.

Step 2: an actual price and the corresponding address of each bid are generated. Alice invokes the keccak(), a unidirectional cryptographic algorithm to produce an encrypted price of the bid with covert information embedded. Furthermore, the quoted price is exchanged between participants in enciphered form thus improving the tamper-proof ability when bidding.

Step 3: in the quotation announcement period, Alice provides both the special bids and the normal bids to the contract for comparison. If the bid matches the range, it is considered effective in the communication and will be used to restore the covert information.

Step 4: Bob extracts a price sequence from all the effective bids and selects all the prices within the valid price range. The number after the decimal point of the selected prices will be converted into a character according to the mapping relationship mentioned above. Then, the characters are ordered from low to high according to the number before the decimal point to generate the covert information.

Rather than common transfer transactions, this protocol makes use of smart contract where there are more application scenarios. Since the parameters of a customized contract are more flexible, this protocol provides better secrecy.

4.8. MRCC: A Practical Covert Channel over Monero. Guo et al. [42] proposed a practical and secure covert channel with no labels employed.

Before constructing a covert channel, both the sender and receiver have to reach an agreement on the data transfer algorithm and the necessary key information, including a public-key encryption scheme $\text{PKE} = (\text{Gen}, \text{Enc}, \text{Dec})$, a related key pair $(\text{PK}_e, \text{SK}_e)$ to encrypt/decrypt the message, and Bob's address (A, B). In the interest of brevity, let us suppose that both M and its corresponding ciphertext under PKE are of n-bit length. The protocol shown in Figure 16 proceeds as follows:

Step 1: the plaintext M is encrypted by PK_e, and C is the ciphertext.

Step 2: Alice establishes a particular transaction $tx = (PK[n], OTA, v, \sigma)$ which has the same format of common transactions. In the constructed transaction tx, $PK[n]$ is a public key set whose hash values' the least valid bits make up C, OTA is an one-time address of Bob, and σ is a significant ring signature generated by Alice's spending key.

Step 3: Alice submits the transaction tx to Monero's blockchain.

Figure 15: Data transmission method on bidding contract.

Step 4: while going through all of Monero's blockchain, Bob recognizes *tx* from the general transactions with the help of his tracking key.

Step 5: as PK[*n*] can be extracted from *tx* easily, Bob needs to pick up the least significant bit of each public key's hash value to reconstruct *C*. After the decryption of *C* using SK_e, the real message *M* will be the output.

This protocol pays attention to the technical characteristics of the blockchain platform, which makes the application of blockchain in the covert communication more customized than other protocols. However, there are some weaknesses that random value in elliptic curve (ed25519 in this protocol) cannot be replaced by any 256-bit number completely due to the range. So more details should be considered when pursuing research.

5. Comparison and Analysis

In this section, we will give some requirements for the blockchain-based covert communication channel and analysis based on the embedding position of the covert message.

There are some needs for the message embedding.

(i) Message Processing: in different kinds of protocols, the covert information is transformed into different forms depending on the way it splits. And for the concealment of the information, it is usually encrypted into ciphertext before transmission.

(ii) Indistinguishability: here, indistinguishability is defined from two aspects. On the one hand, indistinguishability in behavior is necessary. All the network behavior that happened during the phase of covert communication between the sender and receiver proceeds on the basis of universal blockchain protocols. So it is supposed to be indistinguishable from the behavior of ordinary blockchain users. On the other hand, the content and form of the blocks with a message are required to be indistinguishable. So that the malicious user observing the network will not have the ability to perceive hidden messages until the recognition method is known.

(iii) Compatible: the proposed covert communication system must be compatible with the existing public blockchains. It is not hard to figure out that the concealment of special transactions keeps improving with increasing normal transactions in a blockchain. Therefore, scenarios best suited for concealed data transmission are usually public blockchain. It is a must for the covert communication mechanism to be compatible with popular public blockchains without modifying their protocols

The comparison is shown in Table 2 and Table 3. It is assumed that there are 4 inputs in a Bytecoin transaction and 10 public keys in its ring signature.

5.1. Address Channel. Address Channel is a method using the address field of the blockchain when achieving covert communication. A Bitcoin transaction is a data structure consisting of inputs and outputs in which information of a fund flows from the initial place (inputs) to its destination (outputs). The inputs and outputs of the transaction have nothing to do with accounts or identity. They can be understood as a certain amount of Bitcoins with secret information locked. Only their owner or someone who knows the secret can unlock them. Transactions have multiple data fields as is shown in Table 4.

Blockchain address generation goes through a series of algorithms such as ECDSA, SHA-256, and RIPEMD-160, which means the generated address is random in some way under meeting standards. So as long as the addresses that occurred in the blockchain are legitimate, the address-based covert message will not be censored.

Partala [31] proposed an ideal covert communication protocol based on the blockchain. The protocol used a symmetric encryption scheme to deal with the covert message, attached a random tag to it, converted each character in it into an 8 bits binary number, and then embedded it into the generated address bit-by-bit. There are as many addresses needed as the bits of the processed information, which results in low efficiency.

Lejun et al. [32] chose Base58 rather than binarization to encode the message which directly increases the embedding bytes. With Vanitygen generating addresses which can be reused in information embedding and the OP_RETURN field utilized to save the index lists, the efficiency of information transmission increased greatly.

Wang and Su [40] encrypted and encoded plaintext, then embedded it into Bitcoin's output address. With these addresses as a carrier of the covert message, special transactions were constructed to transmit information. However, due to the size limit of the transaction, the message could be too large to be embedded. Meanwhile, the file for decryption is a necessity for restoration and is very important to the receiver, which requires an extrasecure transmission tunnel in the offline transfer.

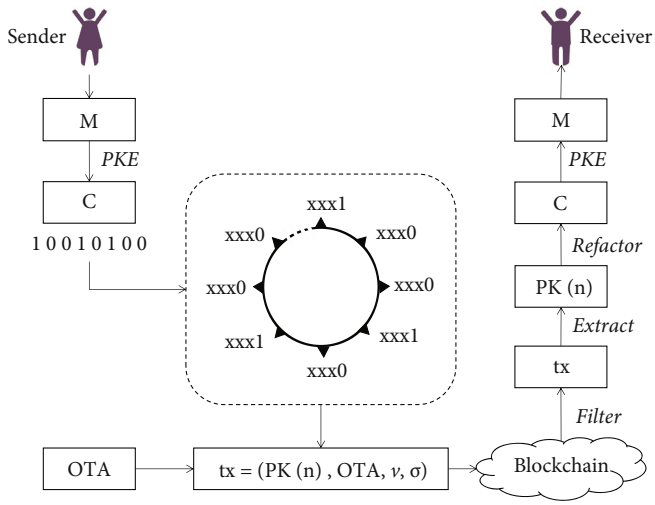

Figure 16: MRCC protocol.

Luo et al. [48] proposed a covert communication method based on Bitcoin transactions which designs the index matrix of the transaction address for the first time. The covert message is embedded in the address interaction relationship combined with the transaction amount. This embedding method decreases the quantity of transactions while increasing the embedding capacity of a single transaction. Besides, a recycled transaction index matrix of address is designed to save the intracorporeal relationship, thus making the address reused.

Minaei et al. [44] proposed R3C3 using the Insight API. It is widely acknowledged that the addresses in the Zcash are of two types: shielded address and unshielded address, the transactions fall into two kinds: minting transaction which creates new coins and pouring transaction which transfers the value of one coin to some new coins. Shielded outputs of a pouring transaction are tuples of the form $(\mathrm{rt}, \mathrm{sn}^{\mathrm{old}}, \mathrm{co}\ \mathrm{m}_1^{\mathrm{new}}, \mathrm{ct}_1, \mathrm{com}_2^{\mathrm{new}}, \mathrm{ct}_2, h, \mathrm{vk}^*, \sigma^*, \pi_{\mathrm{pour}})$, in which rt, sn^{old}, and com_i^{new} are used to complete the zero-knowledge proof π_{pour}, ct_i is used to reconstruct the coin. But since the receiver is in alliance with the sender, ct_i can be reused to carry encrypted data whose portion constitutes 584 bytes.

Cao et al. [51] put forward a chain-based data embedding scheme. Rather than using one address once in the transaction, the proposed scheme uses the derivation from input address to output address to denote 0 or 1. In this way, one bit of binary data is embedded into a transaction.

With low transport volumes, Address Channel is favored when transferring short covert messages. Since each transaction is recorded according to the time sequence, there is no need to worry mess up covert transactions which makes Address Channel suitable for interactive communication.

5.2. Value Channel. Value Channel is a method using the VALUE field of the blockchain when achieving covert communication. It is noted that the VALUE field can be the amount of transfer, the parameters of the smart contract, or other flexible values.

In the Ethereum, its editable fields are described in Table 5 concerning the summary in [35]. Compared with the address field and the input field, the VALUE field is much more flexible. Whatever the value is, it complies with the specifications. So it can be used to store covert messages.

Liu et al. [35] proposed an OBE scheme and two MBE schemes, all of which take advantage of the VALUE field in transactions to construct a subliminal communication channel in Ethereum for the first time. Although the chosen location of the embedded message is exquisite, there lacks a method to recognize special transactions. The receiver has to consider all the transactions delivered from the sender as special transactions, which is bound to increase the processing burden of the receiver.

The smart contract is regarded as a covert communication carrier worth considering due to its diversity, redundancy, and programmability of data. The parameters submitted when calling a contract can be treated as a value.

Zhang et al. [41] proposed the scheme which first encrypted and encoded the data to be transferred in the form of ASCII. To call the smart contract, parameters need to be constructed accordingly. Besides, redundant parameters can be set to enhance the concealment of secret information and to defend against malicious attacks. When using hexadecimal as the format of information and containing eight prices in the bidding contract for each transaction, the loading capacity of a single transaction is 4 bytes.

Basuki et al. [45] proposed the joint use of image steganography and smart contract calling in the Ethereum to achieve a natural transactional model and high volume covert communication. The picture-based steganography is used to supply the scheme with a large storage capacity. By contrast, only the instruction manual is required to be recorded in the transactional steganography to retrieve the stegano-image, thus decreasing the amount of transactions. A smart contract for sensor gateways serves as the experimental platform in the proposed scheme. Pretending as one of the gateways, the sender will update sensor data regularly to the blockchain.

Table 2: Contrast among blockchain-based covert communication channel.

Scheme	Time	Type	Position	Environment	Hiding capacity (bit)/TX
Partala [31]	2018	Address Channel	Input address	Bitcoin	1
Frkat et al. [43]	2018	DSA Channel	Signature	Botnet	256
Minaei et al. [44]	2018	Address Channel	Output shielded address	Zcash	9344
Basuki and Rosiyadi [45]	2019	Value Channel	Contract parameter	Ethereum	29
Recabarren and Carbunar [46]	2019	DSA Channel	Signature	Bitcoin	13200
Alsalami and Zhang [47]	2019	DSA Channel	Signature	Bytecoin	16384
Tian et al. [33]	2019	Script Channel	OP_RETURN	Bitcoin	256
Lejun et al. [32]	2020	Address Channel	Input address	Bitcoin	36
Wang and Su [40]	2020	Address Channel	Output address	Bitcoin	34
Luo et al. [48]	2020	Address Channel	Interaction between address and transaction amount	Bitcoin	Uncertain
		Value Channel	VALUE	Ethereum	OBE:1
Liu et al. [36]	2020	Value Channel	VALUE	Ethereum	HMAC: 0.25* (ValueLength-1)
		Value Channel	VALUE	Ethereum	Hash: 0.5*(ValueLength-1)
Alsalami and Zhang [49]	2020	DSA Channel	Signature	Bytecoin	16384
Zhang et al. [39]	2020	Script Channel	Whisper payload	Ethereum	256
Cao et al. [38]	2020	Address Channel	Public key derivation	Bitcoin	1
Gao et al. [50]	2020	Script Channel	OP_RETURN	Bitcoin	640
Zhang et al. [41]	2021	Value Channel	Contract parameter	Ethereum	41.8
Liu et al. [36]	2022	Value Channel	Amount	Monero	39

Table 3: Comparison of transaction cost (updated Feb. 27, 2022).

Scheme	Time (year)	Environment	Capacity(/TX)	Tx fee(coin)	Price/coin	TX fee($)	Cost($)/1 MB
Minaei et al. [44]	2018	Zcash	1168 byte	0.0001 ZEC	109.64USD	0.011	9.4
Recabarren and Carbunar [46]	2019	Bitcoin	1650 byte	0.0000165 BTC	38763.7USD	0.64	387.89
Gao et al. [50]	2020	Bitcoin	80 byte	0.000039 BTC	38763.7USD	0.1512	1890
Alsalami and Zhang [49]	2020	Bytecoin	2 KB	0.01 BCN	0.00016USD	0.0000016	0.0000931
Liu et al. [36]	2022	Monero	39 bit	0.000009 XMR	155.51USD	0.0014	287

Compared with Address Channel, there is more flexibility in Value Channel. Value Channel is suitable for all blockchain platforms. But long communication which draws attackers' attention is not available, because the value of the special transaction is so intentionally designed that it may be exposed by statistical analysis.

5.3. Digital Signature Algorithm (DSA) Channel. DSA Channel is a method using the signature field of the blockchain when achieving covert communication. It is easy to find out that all the mainstream blockchain cryptocurrencies use original cryptographic primitives, for instance, digital signatures and noninteractive zero-knowledge proofs, so

Table 4: Transaction structure in Bitcoin.

Type	Name	Description	Length
Value	Version	Define the rules for this transaction	4 bytes
Value	Input counter	The number of inputs included	1-9 bytes
UTXO	Input	One or more transaction inputs	Uncertain
Value	Output counter	The number of inputs included	1-9 bytes
UTXO	Output	One or more transaction outputs	Uncertain
Time	Locktime	A block number or UNIX timestamp	4 bytes

Table 5: Transaction structure in Ethereum.

Type	Name	Description	Length
Address	From	The account of sender	Up to 20 bytes
Address	To	The account of receiver. If empty, create a contract.	Up to 20 bytes
Gas	Gas limit	Estimated maximum gas	Up to 32 bytes
Gas	Gas price	The price to cost ether	Up to 32 bytes
Value	VALUE	The amount of ether	Up to 32 bytes
Input	INPUT	An arbitrary message, or a code segment to create a contract, or a function call to a contract	0-about 700 KB

that the uncontrollability of random value in the blockchain can be harnessed under conscious control to complete covert communication.

Alsalami and Zhang [47] demonstrated how to embed covert messages in any subsistent public blockchain where there is enough redundant data. Covert information is embedded in the signatures of the transaction and then broadcast over the blockchain. To isolate and recognize transactions equipped with stegano-text, the receiver has to scan every new transaction appended to the blockchain. If desired transactions are detected, a secret message will be extracted. Otherwise, the receiver keeps searching.

Alsalami and Zhang [49] designed and implemented the first practical covert broadcast communication system which combines steganographic technique with Boneh et al. [52] broadcast encryption scheme. In the CryptoNote protocol, the random numbers in the ring signature are uncontrolled random group elements that can be employed. Considering that the highest significant bit of the random value is not uniformly distributed on 0 and 1, only the least 252 bits of the random number are used to embed covert messages to ensure indistinguishability.

Recabarren and Carbunar [46] introduced a Bitcoin-based framework, called Tithonus, which provides a censorship-resistant communication mechanism. Rather than employing a blockchain consensus mechanism of low speed and high expense, Tithonus makes use of the peer-to-peer gossip protocol in the blockchain as a straightforward agent to exchange covert messages. The encrypted information is embedded in the elliptic curve point generation procedure.

Ali et al. [53] proposed ZombieCoin 2.0 and validated Brenner's discussion [54] that the blockchain technology can be applied to the transmission of C&C instructions secretly. The C&C instruction within 32 bytes can be embedded in the 32-byte ECDSA private key. After the prototype implementation of ZombieCoin 2.0, Ali et al. deployed and controlled the Bitcoin network successfully.

Frkat et al. [43] presented ChanChannels which is a hidden botnet communication in which covert message is injected into the classical Elliptic Curve Digital Signature Algorithm (ECDSA) commonly used in the blockchain. In order to insert a covert message, the randomness in the signature is substituted with the hidden message. Using broadband secret channels, the proposed method could be distributed over multiple blockchains instead of a specific blockchain.

DSA Channel is for use in all scenarios where participants have the capabilities to sign and verify the customized signature. DSA Channel is preferred in the scenario relating to confidential information because outside users can only see on the face of it.

5.4. Script Channel. Script Channel is a method of calling other scripts when achieving covert communication. Bitcoin client calls a verifying script to distinguish transactions. A scriptPubkey is written into UTXO which simultaneously contains a scriptSig written in the same scripting language as the previous script. When a Bitcoin transaction is verified, the scriptSig in each input will be executed at the same time with the corresponding sigPubkey (without mutual interference), so as to check whether the transaction meets the applicable condition.

In the 0.9 version of the Bitcoin client, OP_RETURN operator has been used to compromise a situation that the blockchain is utilized to store data irrelevant to Bitcoin payment. OP_RETURN script allows developers to append nontransactional data of 40 bytes to the output of the transaction and create a remarkable nontransaction output with no need for storage in the UTXO set. The outputs of OP_RETURN are logged on the blockchain, which increases both the disk space consumption and the size of the blockchain. However, since they are not stored in UTXO, they will

not expand UTXO memory, nor will they overburden all nodes at the cost of consuming expensive memory.

Tian et al. [34] proposed DLchain, a mechanism which substitutes the private key with the covert message and presents a dynamic label generation algorithm. It can dynamically create tags that cannot be tracked statistically. Rather than on the stitching of characters in some fixed position, the generation scheme is founded on the statistical analysis of OP_RETURN distribution in plenty of actual transactions.

Gao et al. [50] proposed a mechanism to establish covert channels in public blockchain channels through the kleptography algorithm and OP_RETURN operator. In the submitted special transactions, the signature is dealt with using kleptography algorithm and OP_RETURN field is used to store the encrypted covert message. Then, the receiver can distinguish particular transactions by detecting the signature data.

As a communication protocol for information synchronization, Whisper allows nodes of distributed platforms to interact with each other securely and privately.

Abdulaziz et al. [55] put forward a secure and anonymous decentralized messaging application which can be divided into two phases. One is the temporary Topic and key distribution phase in which Whisper is used to transmit asymmetrically encrypted messages consisting of a random symmetric key for message processing and temporary Topic for message clarification. The other is the communication phase in which the sender constructs an envelope with an encrypted message and prenegotiated Topic. Although the information transferred is encrypted but it is stored directly in the envelope which is somewhat unsafe.

Zhang et al. [39] proposed a new kind of covert communication model for Ethereum. Communication Topic and data-encrypting key are also decided before communication. This paper takes a random string as the objective to refer to while recording the index information at the same time. Rather than transmit the encrypted message directly, it is separated into bytes mapping to another string and needs reorganization after being accepted. Considering that the character string is completely random and only lowercase English letters are contained, the amount of information can be calculated as $\log_2 26$ bits per character (bpc).

Zhang et al. [56] proposed a covert communication model with the Ethereum Whisper model. The payload field of envelope is used as a communicational unit, while the corresponding index information is logged in the padding field. In order to simplify the filtering procedure, this method sets the public key hash value of the recipient for the topic of the envelope.

Script Channel is able to achieve covert communication with high capacity which is suitable for some dense scenarios. With plenty of scripts used in the blockchain, Script Channel can be combined with other covert data transmission technologies. Furthermore, Script Channel is suitable for certain scenarios dedicated to certain blockchain platforms by using their unique scripts, which means the whole process can be customized.

5.5. Findings. As mentioned above, the blockchain-based covert communication channel is divided into four categories, Address Channel, Value Channel, Digital Signature Algorithm (DSA) Channel, and Script Channel. The analysis of the four kinds of channels is shown in Table 6.

Address Channel substitutes the input or output addresses in a transaction for an encoded covert message. The address used as a carrier has to be legitimate, so a covert message needs to go through several steps to the address, resulting in the low capacity and low efficiency of the Address Channel. However, thanks to the commonness of addresses, Address Channel has good invisibility. Address Channel is suitable for intercovert communication with low demand of transport volumes.

Similar to Address Channel, Value Channel replaces the value part of a transaction which also naturally exists in the transaction. It has the characteristic of low capacity. However, as the VALUE field is plain, the covert message may be detected by statistical methods.

Just as its name implies, DSA Channel utilizes mostly the randomness in a transaction to covertly transmit the information, which provides high capacity. Besides, information keeps being processed in the following procedures of the signature algorithm after being inserted, which leads to high concealment.

Script Channel requires extra fields or protocols which is not common or necessary in a transaction. The data fields employed to construct Script Channel may be a plain message or enciphered text. It is so easy to overlook the data fields when dealing with transactions that low concealment is gained. However, in Script Channel, these data fields are always dedicated storage parameters providing high capacity and efficiency.

Among the applications of blockchain in the covert communication, Address Channel and Value Channel are favored in short communication while DSA Channel and Script Channel are favored in long communication. When related to confidential information, DSA Channel is preferred since the ciphertext is not exposed. However, Script Channel is the most suitable for customized demand.

6. Discussion and Future Work

There are pros and cons in the applications of blockchain in the covert communication. On the one hand, the characteristics of high reliability, strong robustness, and decentralization of the blockchain bring about overwhelming change in the traditional covert communication. Blockchain has the capacity to hide both sender's and receiver's identities. With variable ways to embed data, blockchain is a natural alternative where stealth is required. On the other hand, the openness and tamper-resistance of blockchain make it simple for the potential adversary to fetch data which does no good to covertness. There are some drawbacks as follows.

(i) Uncommon flow: the size of data carried in a special transaction is limited. If someone wants to send a long text, so many transactions will be constructed that it is conspicuous in any way. Furthermore, if the amount of an irregular type of transaction soars,

Table 6: Analysis of channels.

Type	Capacity	Concealment	Efficiency
Address Channel	Low	High	Low
Value Channel	Low	Low	Medium
DSA Channel	High	High	Low
Script Channel	High	Low	High

reasonable suspicion exists there emerges covert communication.

(ii) Inefficient screening: in most cases, the receiver needs to scan all the received transactions and execute a recognition algorithm for special transactions, which leads to low efficiency

(iii) Vaporization of covertness. It is out of disputes that covert message stays hidden after the communication at first. But as time goes by, attackers can collect transactions sufficient enough to analyze, which increases the risk of exposure

A satisfactory covert communication protocol is supposed to hide its existence as much as possible while protecting the identities of participants in the communication at the same time especially when it has been detected. As is detailed below, some research directions are recommended in future work.

6.1. One-to-Many Solution. Construct an efficient scheme for one-to-many covert communication, that is, the sender can distribute the same secret message imperceptibly at the same time to many receivers whose communication keys are different. Current covert communication mainly allows people to be in touch one-to-one with the session key negotiated. If there requires one-to-many covert communication, it is more convenient to construct a special multikey protocol rather than embed the same message multiple times for each receiver; then, the receiver can extract the message with their own key. The existence of such a multikey covert communication scheme can be verified in future work.

6.2. Temporariness within Time Slice. Due to the immutability of blockchain, once the covert message is embedded and submitted, the probability of altering or withdrawing it is extremely low. Besides, the integrity guarantees are not supported by any centralized party, but by the consensus of the entire network. The embedding of covert messages is too fragile to stay undetected forever. Once the embedding is detected, the hidden message is supposed not to be extracted successfully. It is inevitable to consider the revocation and variation of covert communication by introducing an effective time slice. Considering that blockchain includes timestamp which provides a temporal feature by nature, how to embed a covert message into blockchain temporarily will become a trend of future work. The existence of such a scheme can be verified in further research for the future.

6.3. Key Compromise Impersonation Resilience. In cryptography, key disclosure is a serious problem. Once the communication key is leaked, the attackers may be able to forge a fake message sent to the legal receiver which disturbs the peace of the covert communication system. However, key-evolution and key-insulated schemes have been put forward to solve the problem mentioned above. Therefore, how to construct a provably secure antikey-disclosure scheme will be the following step of this paper.

7. Conclusion

In this paper, we provide an in-depth review of the applications of blockchain in the covert communication. In recent decades, blockchain technology has attracted a lot of interest in various applications, such as the Internet of Things, identity management, and covert communication. Covert communication uses information hiding techniques to embed secret messages into information carriers during the transmission, which protects the privacy of the secret message. With the underlying technology of cryptocurrencies in blockchain, there are a growing number of researches about covert communication on the blockchain. We investigate these schemes and classify them into certain types according to the hiding position. We also present the difference and comparisons among these types. With the analysis of current protocols, we aim to put forward some new schemes with higher capacity, lower cost, and better efficiency in the future work. With the same underlying architecture of blockchain, analyzing the applications of blockchain in the covert communication contributes to the following research.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The work was supported the National Key Research and Development Program of China (No. 2019QY0800), the Shandong Provincial Key Research and Development Program (Nos. 2020CXGC010107 and 2021CXGC010107), the National Natural Science Foundation of China (Nos. U21A20466, 62172307, 61972294, and 61932016), the Blockchain Core Technology Strategic Research Program of Ministry of Education of China (No. 2020KJ010301), the Special Project on Science and Technology Program of Hubei Province (No. 2020AEA013), the Natural Science Foundation of Hubei Province (No. 2020CFA052), the Wuhan Municipal Science and Technology Project (No. 2020010601012187), the Foundation of Hangzhou Innovation Institute, Beihang University (No. 2020-Y10-A-019), the Peng Cheng Laboratory Project (Grant No. PCL2021A02), and the Foundation of Guangxi Key Laboratory of Trusted Software (No. kx202001).

References

[1] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Crypto*, Plenum Press, New York, 1984.

[2] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[3] J. Willett, M. Hidskes, D. Johnston, R. Gross, and M. Schneider, *Omni protocol specification (formerly mastercoin)*, vol. 28, 2016white paper.

[4] M. Rosenfeld, "Overview of colored coins," in *White paper, bitcoil. co. il*, vol. 41, p. 94, Coinprism, 2012.

[5] R. Roy and S. Changder, "Steganography with projection aided payload dimension reduction and reconstruction for military covert communication," *International Journal of Computer Applications*, vol. 139, no. 3, pp. 32–37, 2016.

[6] Z. Hijaz and V. S. Frost, "Exploiting OFDM systems for covert communication," in *2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, pp. 2149–2155, San Jose, CA, USA, 2010.

[7] J. F. Harvey, M. B. Steer, and T. S. Rappaport, "Exploiting high millimeter wave bands for military communications, applications, and design," *IEEE Access*, vol. 7, pp. 52350–52359, 2019.

[8] G. J. Simmons, "Subliminal communication is easy using the DSA," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 218–232, Springer, 1993.

[9] J.-K. Jan and Y.-M. Tseng, "New digital signature with subliminal channels based on the discrete logarithm problem," in *Proceedings of the 1999 ICPP Workshops on Collaboration and Mobile Computing (CMC'99). Group Communications (IWGC). Internet '99 (IWI'99). Industrial Applications on Network Computing (INDAP). Multime*, pp. 198–203, Aizu-Wakamatsu, Japan, 1999.

[10] J.-M. Bohli and R. Steinwandt, "On subliminal channels in deterministic signature schemes," in *International Conference on Information Security and Cryptology*, pp. 182–194, Springer, 2004.

[11] J.-M. Bohli, M. I. G. Vasco, and R. Steinwandt, "A subliminal-free variant of ECDSA," in *International Workshop on Information Hiding*, pp. 375–387, Springer, 2006.

[12] A. Hartl, R. Annessi, and T. Zseby, "A subliminal channel in EDDSA: information leakage with high-speed signatures," in *Proceedings of the 2017 International Workshop on Managing Insider Security Threats*, pp. 67–78, Dallas, TX, USA, 2017.

[13] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, Springer, 2001.

[14] Q. Dong, X. Li, and Y. Liu, "Two extensions of the ring signature scheme of Rivest-Shamir-Taumann," *Information Sciences*, vol. 188, pp. 338–345, 2012.

[15] B. Wang, Z. Zhang, and F. Zhang, "Subliminal channels in the code-based ring signature scheme," in *2019 14th Asia Joint Conference on Information Security (AsiaJCIS)*, Kobe, Japan, 2019.

[16] J. A. B. Dykstra, *A framework for network covert channel detection*, Iowa State University, 2004, PhD thesis.

[17] C. Wang, Y. Yuan, and L. Huang, "Base communication model of IP covert timing channels," *Frontiers of Computer Science*, vol. 10, no. 6, pp. 1130–1141, 2016.

[18] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: automated modeling and evasion," in *International Workshop on Recent Advances in Intrusion Detection*, pp. 211–230, Springer, 2008.

[19] J. Millen, "20 years of covert channel modeling and analysis," in *Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No. 99CB36344)*, pp. 113-114, Oakland, CA, USA, May 1999.

[20] S. M. R. Farschi and H. Farschi, "A novel chaotic approach for information hiding in image," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1525–1539, 2012.

[21] J. M. Blackledge and A. R. I. Al-Rawi, "Steganography using stochastic diffusion for the covert communication of digital images," *International Journal of Applied Mathematics*, vol. 41, no. 4, 2011.

[22] L. Ji, Y. Fan, and C. Ma, "Covert channel for local area network," in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 316–319, Beijing, 2010.

[23] H. Dol, B. Quesson, and F. Benders, "Covert underwater communication with marine mammal sounds," in *Undersea Defence Technology-UDT Europe 2008*, ACM, Glasgow, UK, 2008.

[24] D. Kundur and K. Ahsan, "Practical internet steganography: data hiding in IP," *Proc. Texas wksp. security of information systems*, 2003.

[25] C. G. Girling, "Covert channels in LAN's," *IEEE Transactions on software engineering*, vol. SE-13, no. 2, pp. 292–296, 1987.

[26] D. Mohanty and D. Mohanty, "Ethereum Architecture," in *Ethereum for Architects and Developers*, Apress, Berkeley, CA, 2018.

[27] *Whisper poc 2 protocol spec*https://eth.wiki/concepts/whisper/poc-2-protocol-spec.

[28] M. Al-Bassam, "Scpki: a smart contract-based PKI and identity system," in *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 35–40, Abu Dhabi United Arab Emirates, 2017.

[29] Y. Zhang and J. Wen, "The IoT electric business model: using blockchain technology for the Internet of Things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[30] J. Cunningham and J. Ainsworth, "Enabling patient control of personal electronic health records through distributed ledger technology," *Studies in Health Technology and Informatics*, vol. 245, pp. 45–48, 2018.

[31] J. Partala, "Provably secure covert communication on blockchain," *Cryptography*, vol. 2, no. 3, p. 18, 2018.

[32] Z. Lejun, Z. Zhijie, W. Weizheng et al., "A covert communication method using special Bitcoin addresses generated by Vanitygen," *Cmc-computers Materials & Continua*, vol. 65, no. 1, pp. 597–616, 2020.

[33] J. Tian, G. Gou, C. Liu, Y. Chen, G. Xiong, and Z. Li, "DLchain: a covert channel over blockchain based on dynamic labels," *ICICS*, Springer, 2020.

[34] P. Barford, "The DGA of Banjori," February 10, 2015, https://blog.51cto.com/rude3knife/2910831.

[35] S. Liu, Z. Fang, F. Gao et al., "Whispers on ethereum: blockchain-based covert data embedding schemes," in *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Taipei, Taiwan, China, 2020.

[36] L. Liu, L. Liu, B. Li, Y. Zhong, S. Liao, and L. Zhang, "MSCCS: a Monero-based security-enhanced covert communication system," *Computer Networks*, vol. 205, article 108759, 2022.

[37] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on fBitcoin'sgf Peer-to-Peerg network," in *24th USENIX Security Symposium (USENIX Security 15)*, pp. 129–144, Washington, D.C., USA, 2015.

[38] T. Cao, J. Yu, J. Decouchant, X. Luo, and P. Verissimo, "Exploring the Monero peer-to-peer network," in *International Conference on Financial Cryptography and Data Security*, pp. 578–594, Springer, 2020.

[39] Z. Zhang, L. Zhang, W. Rasheed et al., "The research on covert communication model based on blockchain: a case study of Ethereum's Whisper Protocol," Springer, Singapore, 2020.

[40] W. Wang and C. Su, "CCBRSN: a system with high embedding capacity for covert communication in Bitcoin," *ICT Systems Security and Privacy Protection*, vol. 580, pp. 324–337, 2020.

[41] L. Zhang, Z. Zhang, W. Wang, Z. Jin, Y. Su, and H. Chen, "Research on a covert communication model realized by using smart contracts in blockchain environment," *IEEE Systems Journal*, pp. 1–12, 2021.

[42] Z. Guo, L. Shi, M. Xu, and H. Yin, "MRCC: a practical covert channel over Monero with provable security," *IEEE Access*, vol. 9, pp. 31816–31825, 2021.

[43] D. Frkat, R. Annessi, and T. Zseby, "Chainchannels: Private botnet communication over public blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1244–1252, Halifax, NS, Canada, 2018.

[44] M. Minaei, P. Moreno-Sanchez, and A. Kate, "R3c3: cryptographically secure censorship resistant rendezvous using cryptocurrencies," *Cryptology ePrint Archive*, , Cryptology ePrint Archivep. 454, 2018.

[45] A. Basuki and D. Rosiyadi, "Joint transaction-image steganography for high capacity covert communication," in *2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, pp. 41–46, Tangerang, Indonesia, 2019.

[46] R. Recabarren and B. Carbunar, "Tithonus: a Bitcoin based censorship resilient system," *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 1, pp. 68–86, 2019.

[47] N. Alsalami and B. Zhang, "Utilizing public blockchains for censorship-circumvention and IoT communication," in *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, Hangzhou, China, 2019.

[48] X. Luo, P. Zhang, M. Zhang, H. Li, and Q. Cheng, "A novel covert communication method based on Bitcoin transaction," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2830–2839, 2021.

[49] N. Alsalami and B. Zhang, "Uncontrolled randomness in blockchains: covert bulletin board for illicit activity," in *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*, Hang Zhou, China, 2020.

[50] F. Gao, L. Zhu, K. Gai, C. Zhang, and S. Liu, "Achieving a covert channel over an open blockchain network," *IEEE Network*, vol. 34, no. 2, pp. 6–13, 2020.

[51] H. Cao, H. Yin, F. Gao et al., "Chain-based covert data embedding schemes in blockchain," *IEEE Internet of Things Journal*, 2020.

[52] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Annual international cryptology conference*, pp. 258–275, Springer, 2005.

[53] S. T. Ali, P. McCorry, P. J. Lee, and F. Hao, "Zombiecoin 2.0: managing next-generation botnets using Bitcoin," *International Journal of Information Security*, vol. 17, no. 4, pp. 411–422, 2018.

[54] M. Brenner, T. Moore, and M. Smith, *Financial Cryptography and Data Security*, Springer, 2014.

[55] M. Abdulaziz, D. Çulha, and A. Yazici, "A decentralized application for secure messaging in a trustless environment," in *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Ankara, Turkey, 2018.

[56] L. Zhang, Z. Zhang, Z. Jin, Y. Su, and Z. Wang, "An approach of covert communication based on the Ethereum whisper protocol in blockchain," *International Journal of Intelligent Systems*, vol. 36, no. 2, pp. 962–996, 2021.