This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2024.3358013

Amount-based Covert Communication over Blockchain

Yang Tian, Xin Liao*, Li Dong, Yang Xu, and Hongbo Jiang

***Abstract*—Recent years have witnessed the booming growth of 5G and 6G technology, which has brought unprecedented massive data transmission, causing severe privacy issues. However, traditional information encryption and multimedia covert communication fail to protect the identities of communication parties and the originality of messages. The emergence of blockchain provides a promising solution to solve these problems. Its anonymity manages to hide the identities of communication parties, and immutability ensures the message is undestroyable. However, the existing blockchain-based covert communication schemes suffer the issues of low embedding capacity and high time cost. In this paper, an amount-based covert communication scheme over the blockchain is proposed, in which a unique coding method is devised for hiding messages into transaction amounts to improve the embedding capacity. Compared with existing address-based methods, the proposed scheme can apply any address and reduce the time of obtaining special addresses. Besides, we innovate the way to prove the concealment by calculating the relative entropy of the transaction amount between Bitcoin and the proposed scheme. The security of our method is demonstrated by comparing the probability of attackers acquiring secret messages under different adversary capabilities. The experimental results verify that the proposed approach outperforms the existing schemes regarding embedding capacity, time costs, number of transactions, concealment, and security.**

***Index Terms*—Covert communication; blockchain; transaction amount; concealment.**

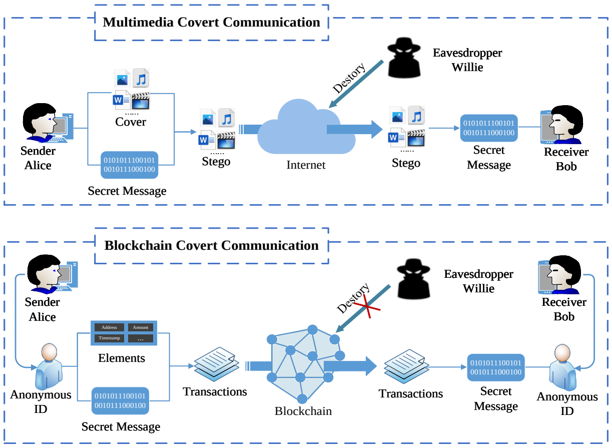


Fig. 1. Comparison between multimedia covert communication and blockchain covert communication. Multimedia covert communication can not protect the identity of the communication parties, and eavesdroppers can destroy the covert communication messages. Blockchain covert communication anonymizes the identities of the communication parties, and the messages on the blockchain are immutable.

I. Introduction

NOWADAYS, with the vigorous promotion of 5G technology, the 5G era has fully arrived. 5G is a brand-new system integrating semiconductors, communications, artificial intelligence, intelligent hardware, new services, and applications. It has brought about the improvement of social competence and efficiency and incurred a profound impact on the traditional operating system and related industries, but it has also led to serious privacy issues [1]. In the era of 5G, the Internet is playing an irreplaceable role in both work and life [2], which enables online communication to be a mainstream and convenient mode of communication between people. Nevertheless, severe privacy problems may occur in the meantime [3]. Online privacy protection primarily relies on encryption and covert communication. The cryptography-based encryption technology [4]-[6] encrypts the plaintext into ciphertext, which, however, may expose the communication parties and process. In contrast, covert communication [7] has been drawing huge attention [8]. The working principle of covert communication is to embed the secret message into public carriers and then transmit it through centralized public channels. Generally, carriers include images, videos, and audio [9]. Channels are chat software or chat websites, such as WhatsApp, Kakaotalk, Instagram, Facebook, and so on. With covert communication messages, the availability of the original carrier can not be destroyed. Meanwhile, the difference between covert and ordinary communication messages cannot be distinguished by humans normally, so as to achieve information hiding. In this case, attackers intending to steal the secret message must know whether both sides have communicated first.

However, covert communication should protect the identities of both parties [10] and the originality of messages while ensuring that the communication is out of awareness. Multimedia covert communication can not protect communication parties. Once the covert communication is discovered, the identities may be revealed. Although covert communication hides communication behavior, the concealment is under severe threat. If attackers deliberately perform traffic analysis or steganalysis, it is possible to detect communication [11]. Currently, there are studies that can extract information from video [12] and many works on steganography detection for different carriers, such as the work [13] in the image steganog-

Y. Tian, X. Liao, Y. Xu, and H. Jiang are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, 410082. (E-mail: {tianyang, xinliao, xuyangcs, hongbojiang}@hnu.edu.cn)

L. Dong is with the Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo, China, 315211. (E-mail: dongli@nbu.edu.cn)

*Corresponding author: Xin Liao.

This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2024.3358013

raphy detection, the work [14] in the field of steganalysis of audio, and the work [15] in the steganalysis of video. These studies show that the data hiding is not absolutely invisible and the existence of covert communication is not completely concealed. Once the communication is detected, the identities of parties in the traditional multimedia covert communication will be exposed. Therefore, it is necessary to use blockchain to ensure anonymity. In addition, in the communication process of multimedia covert communication, attackers can destroy secret messages, which may cause the receiver to receive incorrect messages.

To tackle the above issues, covert communication approaches based on blockchain were proposed, which utilize blockchain as the communication channel and transactions as the carrier [16]. Blockchain, a decentralized public distributed ledger built on a peer-to-peer network [17], can protect the true identities of communicating parties effectively with its anonymization functionality. Even the covert communication behavior can be exposed, malicious intruders cannot access the real identity information of both parties. In addition, the non-tampering characteristics of blockchain ensure that malicious intruders have no way to tamper with transaction messages. Secret messages are camouflaged before they are embedded in the blockchain, thus, despite the blockchain being visible to everyone, non-recipients cannot distinguish between transactions containing secret messages and ordinary transactions. Other than the communication parties, it is impossible to identify transactions containing secret information from the mass of transactions. Furthermore, before the data is transferred to the blockchain, we encrypt it and transform the data form. Hence, adversaries can not get the original data. Fig. 1 depicts the multimedia covert communication and the blockchain covert communication. Multimedia covert communication can not protect communication parties and the eavesdropper has the ability to destroy the message. Once the covert communication is discovered, the identities may be revealed. In blockchain covert communication schemes, Alice and Bob utilize anonymous IDs, and Alice embeds the secret message in the transaction and sends it to the blockchain. During this process, eavesdroppers cannot destroy the message.

At present, blockchain covert communication has been studied by researchers [18]. In 2018, Partala proposed a blockchain covert communication approach called BLOCCE [16], which was regarded as the first attempt to combine blockchain and covert communication. Afterward, many researchers designed various covert communication schemes based on blockchain. The OP_RETURN is used for covert communication, easy to expose the communication [19], [20]. The transaction sequence is adopted to embed information, which can hide communication behavior but has high risk [21], [22]. Then, the signature is utilized to hide information, which has low risk but a relatively single way [24], [25]. Ref. [16], [26]-[31] embed secret information in transaction addresses. It has various forms, low risk, and good concealing, but it suffers the disadvantages of low embedding capacity and large time costs.

In this paper, we make attempts to solve two main issues of existing covert communication approaches based on blockchain: (1) low embedding capacity, and (2) high time costs. If the capacity is too low, the system cost is too high to be used. Too much time cost will affect the immediacy of communication. An amount-based covert communication scheme over the blockchain is proposed, which devises a unique $\underline{\text{am}}$ount $\underline{\text{ASC}}$II (AMASC) code encoding strategy to transform secret messages into transaction amounts. By changing the embedding position, the embedding capacity of each address amount pair is greatly enlarged. Additionally, the Unspent Transaction Output (UTXO) structure and the change address of Bitcoin are employed skillfully to resolve time costs and identifier problems. Our scheme utilizes a particular embedding manner to improve security and constructs a mapping function to enhance concealment. To the best of our knowledge, this paper is the first to use information theory to prove the security and concealment of blockchain covert communication. The main contributions of this paper are as follows.

- We propose an amount-based covert communication scheme over the blockchain. The scheme designs a unique AMASC code coding way to embed ciphertext into transaction amounts and improve the embedding capacity. Compared with address-based methods, the proposed approach changes the embedding position and can adopt any address without generating a specific type of address, improving the embedding capacity and efficiency simultaneously.
- We calculate the relative entropy between the transaction amount of Bitcoin and the proposed scheme and formulate a threat model to compare the probability of acquiring secret information with the existing methods under different adversary capabilities, verifying the concealment and security performance of the approach.
- We implement the proposed scheme on Bitcoin Testnet and compare it with existing blockchain covert communication methods. Experimental results demonstrate that the proposed scheme increases embedding capacity eightfold in each address-amount pair, and achieves superior performance in terms of time costs, number of transactions, concealment, security, and transaction fees.

The remainder of the paper is organized as follows. Section II provides preliminary knowledge and related works. Section III illustrates the motivation. Section IV provides the overview of the proposed scheme and design goals. Section V describes the proposed scheme in detail. Section VI shows the theoretical analysis and proof. Section VII presents experiment results. Finally, the conclusion part is given in Section VIII.

II. Related Work

In this section, we first give a brief review of covert communication and blockchain, respectively. Then, related works on blockchain covert communication are surveyed.

A. Covert Communication

Unlike traditional encryption technology, which hides the content of messages itself, covert communication focuses on the perceptibility of communication. It processes the message to be transmitted covertly and embeds the message into communication and media information for transmission [7] with the redundancy of information. The traditional covert communication scheme can be summarized in five steps: message processing, message embedding, transmission, message extraction, and message restoration. The main parts of the scheme are the message sender, the message receiver, and the communication channel. However, the traditional channel is vulnerable to monitoring and detecting, and participants are easily exposed. Once there is a trust problem in the central node that the communication depends on, the data is easily leaked or even tampered with.

B. Blockchain

As a newly booming technology in recent years, blockchain breaks the mainstream mechanism that relies on third-party institutions for information exchange or trade transfer. Each node acts as an individual server and keeps an independent ledger distributed. Data such as transaction information is stored in an encrypted blockchain structure. Each block consists of a block header and body with its unique hash value corresponding to the block address, and adjacent blocks are linked via the unique hash value. The block header contains the previous block's hash value and the Merkle root value of this block. When a transaction is recorded in the block, everyone can query the transaction record and verify the transaction. Once a transaction is maliciously altered, the hash of the Merkle root changes. The blockchain uses the hash value of the public key as the account address, isolating the relationship between the user's real identity and that of the trader, which enables anonymity.

As one of the most popular cryptocurrencies, Bitcoin [17] is a P2P form of virtual cryptocurrency proposed by Satoshi Nakamoto. It adopts the UTXO structure where each transaction can have multiple inputs and outputs and the PoW (Proof of Work) consensus mechanism that solves the problem of accounting rights. During this period of time, blockchain technology is no longer limited to the field of cryptocurrency. In addition to the field of covert communication mentioned in this paper, it also finds many application scenarios, such as the Internet of Vehicles [32], [33], Internet of Things [34], [35], financial trade [36], [37] and medical field [38].

C. Bitcoin-based Covert Communication Schemes

The current Bitcoin-based covert communication schemes can be roughly divided into the following four categories.

The first approach is utilizing the OP_RETURN output script [39] for information embedding, which is the most direct and effective way to embed information in Bitcoin. In version 0.12.0 [40], the default limit for OP_RETURN output size is 83 bytes. In [19], fixed labels in communication were transformed into dynamic labels and hidden in OP_RETURN. Both sides of a transaction apply the same rule to generate dynamic labels simultaneously for transaction recognition. Based on BLOCCE [16], the work [20] came up with V-BLOCCE, which adopted Vanitygen to generate the address of bytes containing the encrypted message. V-BLOCCE embedded the corresponding index of the transaction address and bytes position having the encrypted message into the OP_RETURN. Although this way is simple, effective, and high-capacity, it has the risk of transaction behavior exposure in covert communication. In other words, once the output of the transaction includes OP_RETURN, attackers would suspect that there is some information hidden in the transaction.

The order of transactions is the second approach for covert communication. Fionov [21] proposed that the order of transactions could be applied in Bitcoin for covert communication. Xu *et al.* [22] took miners as embedders. Miners packaged transactions in order, with different orders representing different messages. However, this is a risky manner, as the accounting right is contested, and the miner may not necessarily get accounting rights in Bitcoin. Hence, the order would change, which prevents the receiver from restoring the secret message.

The ECDSA signature can be applied as the third approach for covert communication. In 2018, in order to hide botnet, Frkat *et al.* [23] exploited the digital signatures used in blockchains to inject subliminal messages. In 2020 and 2021, Alsalami *et al.* [24] and Tiemann *et al.* [25] made use of the nonce of ECDSA signature to embed secret messages in Bitcoin. This method is delicately devised, but it can only use the nonce of ECDSA for embedding, which is too one-dimensional.

The last way is address-based covert communication. Partala put forward for the first time that blockchain could be used for covert communication and came up with BLOCCE which exploited the least significant bit (LSB) of the sending address to carry secret messages in 2018 [16]. In BLOCCE, one address can embed one bit, and one block contains one embedded address. Hence, the embedding capacity of this manner is insufficient, and the time cost is enormous. In 2020, Wang *et al.* came up with CCBRSN [26], which generated many addresses to match secret messages. However, the scheme needs to have an index file and send it to the receiver, increasing the communication between the two parties. In 2021, two Bitcoin-based covert communication schemes were put forward by Troki *et al.* [27]. The high-capacity scheme was populated with the encrypted message and disguised as the output address to conduct the transaction, which consumed the coin in the transaction, and the output coin could not be recovered or reused either, making it impractical. The lower capacity scheme was embedded in part of the address, which required the index file to find the message. How to transfer the index file is also a crucial issue. In 2021, Qin *et al.* [28] used the parity of transaction addresses to carry out covert communication. The scheme is clever but too expensive and has low embedding capacity. Zheng *et al.* [29] defined a mapping rule between different public keys and different bitstrings in a codebook. Then, these public keys were utilized as addresses. This scheme will cause address reuse, and once the password book (mapping relationship) is lost, anyone can extract secret information, which is not secure enough. Huang *et al.* [30] embedded secret information in the public key hash field. This scheme can update the communication address and key automatically. However, double-spend attacks need to be

TABLE I
Comparison of Our Scheme with the Existing Schemes in terms of Embedding Location, Sustainable Communication, Security, Embed Way, Extract Correct, and Concealment.

Schemes	Embedding Location	Sustainable Communication	Security	Embed Way	Extract Correct	Concealment
[19], [20]	OP_RETURN	✗	low	diverse	✓	✗
[21], [22]	transaction order	✗	medium	single	✗	✓
[23]-[25]	ECDSA	✗	high	single	✓	✓
[31]	address	✓	medium	diverse	✓	✓
[16], [26]-[30]	address	✗	medium	diverse	✓	✓
Ours	amount	✓	high	diverse	✓	✓

created to recover unspent bitcoins. Therefore, double-spend attacks need to be created to recover unspent bitcoins. Hence, the recipient must accept the message in a short time, and the transaction fee is high. In 2022, Cao *et al.* [31] proposed HC-CDE, which first defined the PSK corresponding bits 0 and 1, and then generated the corresponding addresses according to the secret message. In this way, the labeling and sorting of embedding transactions are worked out. Compared with BLOCCE [16], HC-CDE increases the system cost and time cost. Nevertheless, its capacity and time costs still cannot satisfy the demand. Therefore, the aforementioned approaches still need to improve.

III. Motivation

In this section, the motivation of the proposed method is presented by comparing it with multimedia covert communication and existing blockchain-based covert communication.

A. Comparison with Multimedia Covert Communication

At present, the vast majority of covert communication research is based on multimedia. It is undeniable that multimedia covert communication is convenient and has a large capacity. However, for some scenarios with higher privacy, such as national defense, military industry, or some situations that want complete privacy, it is necessary to ensure that the real identities of the two sides of the communicator cannot be determined and the information transmitted is completely accurate, which cannot be achieved by multimedia covert communication. At this time, the technical advantages of blockchain become apparent. Here are two main advantages of blockchain for covert communication.

Identity protection. Blockchain is anonymous. As shown in Fig. 1, blockchain covert communication can anonymize the communication parties. Therefore, the IDs of the communication parties do not contain any personally identifiable information about them. Additionally, due to the UTXO structure of the blockchain, the user's address is constantly changing, which gives it a higher level of privacy. Even if covert communications are detected, the communicator cannot be identified.

Originality of the message. Blockchain is immutable, meaning that attackers cannot destroy the originality of the messages during information transmission. That is, messages received by the receiver are completely correct. The blockchain environment ensures that data is not affected by the network in the transmission process. Moreover, in multimedia covert communication schemes, data are easily lost, and the integrity of the message is more likely destroyed [41] once the network shock is encountered, but blockchain-based schemes are not.

B. Comparison with Related Work

At present, blockchain covert communication typically employs two carriers, Bitcoin [16], [19]-[31] and Ethereum [42]-[44]. There are a lot of smart contracts on Ethereum, which has some advantages for covert. Instead, Ethereum uses an account model, which makes it easy for the involved parties to be tracked. However, every transaction of Bitcoin is a new address, which makes it more concealable. Therefore, we in this work employ Bitcoin as the carrier. More specifically, we investigate existing blockchain covert communication solutions. As shown in Table I, the first three types of models suffer drawbacks: the first type is insufficient concealment, the second type cannot guarantee that receivers receive the correct information, and the third type has a single-way of embedding. The fourth and fifth types are extensively studied at present. The fifth type can not realize sustainable communication. Hence, the fourth type paper [31] is an article with a good comprehensive performance at present. But the use of transaction address embedding can incur a low capacity of embedding, and then lead to a huge system cost and time cost. Therefore, this paper aims to increase the embedding capacity and reduce the time cost by changing the embedding location of information while ensuring security and concealment.

IV. Models and Design Goals

In this section, an overview and threat model of the proposed scheme are given first. Then, the design goals of the proposed scheme are summarized.

A. Overview and Threat Model

We show the overall architecture of the amount-based covert communication scheme in Fig. 2, which consists of two components: (1) the embedding process, and (2) the extraction process. Both processes contain two entities: a sender, and a receiver. In addition, there are adversaries to steal the message in this process. Due to the immutable property of the blockchain, attackers cannot destroy the embedded secret information, so the aim of attackers is to steal secret information from the blockchain. In the next, we summarize the goals of the three entities and formulate a threat model.

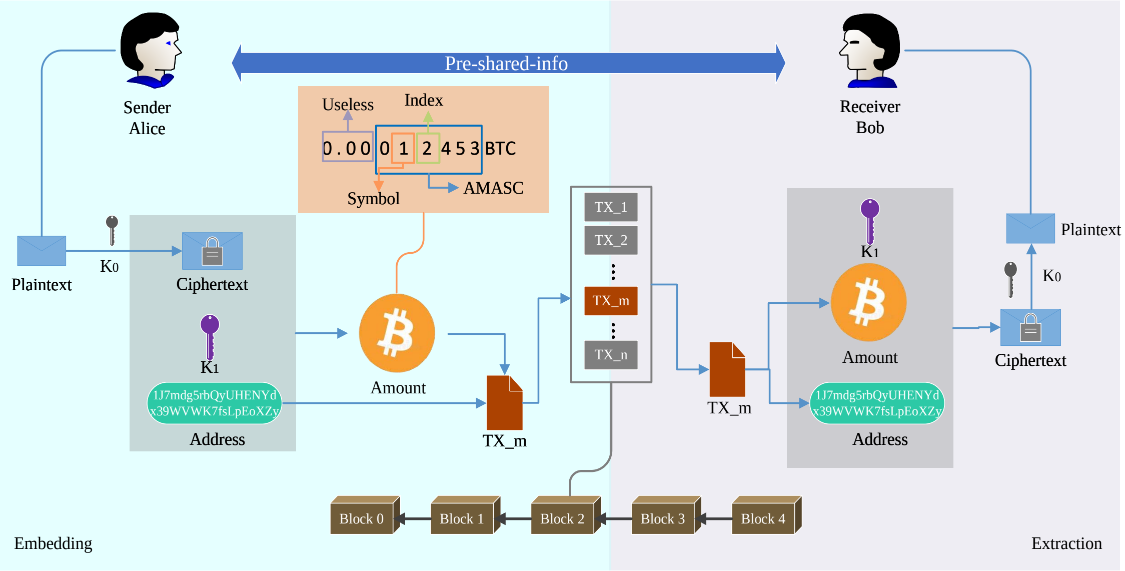


Fig. 2. The overall architecture of the proposed scheme. Alice hides the message in the transaction and sends it to Bitcoin. Bob queries the transaction and extracts the message from it. The secret message is hidden in the transaction amount, and the amount is calculated by the address, ciphertext, $Fmap(x)$, and K_1. The box over the amount is the amount design rule.

Sender. During the embedding process, the sender first converts plaintext to ciphertext, then utilizes the ciphertext, K_1, and addresses to calculate amounts and constructs transactions with addresses and amounts. In the end, the transactions are sent to the blockchain.

Receiver. In the procedure of extraction, the receiver queries transactions from the blockchain and obtains information with transactions, so as extracting the ciphertext with the information and converting the ciphertext to plaintext.

Adversary. Adversaries constantly monitor the blockchain in an attempt to steal plaintext secret information.

As shown in the box above the amount in Fig. 2, the integer and two decimal places of the amount can be any value, and the rest is the AMASC code digit. The fourth decimal digit is the symbol digit, and the fifth decimal digit is the index digit. In this paper, the AMASC code digits of the transaction amount are selected as effective digits for the convenience of the experiment, in case the amount to be raised through faucets is too large.

To better understand the proposed model, Fig. 3 shows the workflow of the model. As shown in Fig. 3, both the embedding and extraction processes consist of four steps, which are described in detail in Section V.

In this paper, the sender and receiver are assumed as honest-and-credible parties, which will follow our scheme honestly and manage the secret key properly. Therefore, it should be ensured that secret information is not cracked.

In our threat model, adversaries try to recover secret messages. To better evaluate the security property of the proposed scheme, we classify the ability of adversaries into four levels as follows according to the availability of the prior information on the system.

Level 1. The adversary only knows the rules of message embedding.

Level 2. The adversary only has the identification of embedded transactions.

Level 3. Apart from the ability in Level 1, the adversary has the ability in Level 2.

Level 4. Apart from the ability in Level 3, the adversary knows one key of schemes.

B. Design Goals

Besides making covert communication come true, achieving higher embedding capacity and lower time costs while ensuring security are the design objectives of the schemes. For the sake of further improving embedding capacity, the unique AMASC code embedding is designed, which enhances the embedding capacity to eight bits per address-amount pair. AMASC code is the value obtained by a series of transformations of the ciphertext. As shown in the box over the amount in Fig. 2, the AMASC code is the amount in the third to eighth decimal places. The amount-based approach can reduce time costs and the number of addresses compared with address-based methods. For example, when embedding eight bits, the address-based way requires eight addresses while the amount-based embedding approach requires only one address. Bitcoin employs the UTXO structure in which one transaction can have n input (s) and m output (s). In Bitcoin, any number of transaction addresses is normal. To cut down the count of transactions and time costs, the proposed scheme sets every transaction as one input and seven outputs (one for change and six for embedding).

V. The Proposed Amount-based Covert Communication Scheme

In this section, the amount-based covert communication scheme over the blockchain is introduced in detail in three parts: data embedding, data extraction, and mapping function.

This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2024.3358013

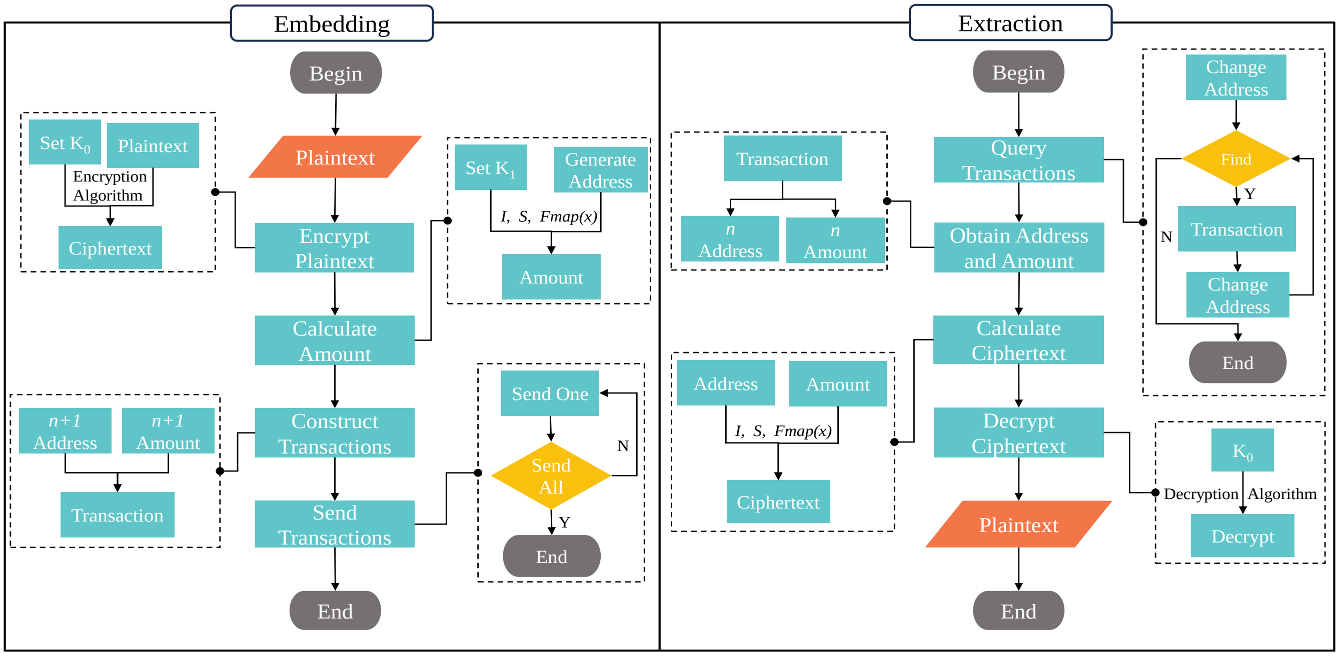


Fig. 3. A flow chart for the proposed framework. Both the embedding and extraction processes can be divided into four steps.

A. Data Embedding

Pre-shared-info: Refers to the shared secret information that is previously shared between the sender and receiver before the covert communication. It includes the embedding function, the first communication address $addr_0$, the AES [45] encryption key K_0, and the amount calculation key K_1. Both the sender and receiver shall keep these keys secret.

The embedding process is described in four steps according to the flow chart shown in Fig. 3.

Step 1. Eq. (1) is used by the sender to produce 32 bits Bitcoin address randomly as AES encryption key K_0 for our scheme. Note that the AES secret key can be generated utilizing any secure method, and the Bitcoin address is adopted instead for the sake of the experiment. In addition, plaintext encryption does not have to choose AES encryption, and the sender is allowed to choose their own encryption method. Although the scheme proposed in this paper uses symmetric encryption, it does not embed the key into Bitcoin but uses it as a parameter to participate in the calculation of the transaction amount. Therefore, it is impossible for attackers to extract the key from the transaction. In addition, considering that secret information is stored permanently on the blockchain, the key of AES needs to be changed regularly.

$$K_0 \leftarrow [[BIT.AddrGen(1)]]_0^{31}, \tag{1}$$

where $[[a]]_m^n$ means to take the $m-th$ position to the $n-th$ position of a, $BIT.AddrGen(a)$ means that generating a different addresses randomly. Then, the plaintext secret message M is encrypted according to the pre-shared AES encryption key K_0 to obtain the ciphertext P.

Step 2. In this step, the key, the random address, the mapping function $Fmap(x)$, and the secret message are utilized to get the AMASC code A_m.

Algorithm 1: AMASC code value calculation and the message embedding.

```
Input:
    The transaction address: $D$.
    The secret message(one): $M$.
    The AES secret key: $K_0$.
    The amount calculation secret key: $K_1$.
Output:
    Transaction amount at this address: $A$.
ciphertext $P \leftarrow AES.Enc(K_0, M)$
key values $K_{value} \leftarrow AderssToValue(K_1)$
address values $D_{value} \leftarrow AderssToValue(D) + K_{value}$
ciphertext ASCII $M_{asc} \leftarrow Ord(P)$
$B \leftarrow Fmap(D_{value} - M_{asc})$
AMASC code $A_m \leftarrow Abs(B * 10^{-8})$
mapping $A_m \leftarrow Fmap(A_m)$
if $B > 0$ then
    symbol $S = Random([0,1,2,3,4])$
else
    symbol $S = Random([5,6,7,8,9])$
end if
$A_m \leftarrow A_m + S$
index $I \leftarrow Random(1,9)$
$A_m \leftarrow A_m + I$
$A \leftarrow A_m$
```

Firstly, l embedded addresses and l/n change addresses are randomly generated on the basis of the ciphertext length l.

$$addr_0^{l+\frac{l}{n}} \leftarrow BIT.AddrGen(l + \frac{l}{n}), \tag{2}$$

where n is the number of embedded addresses in a transaction.

Algorithm 2: Recover a ciphertext message from one transaction address-amount pair.

```
Input:
    The transaction address: $D$.
    The transaction amount(one): $A$.
    The AES secret key: $K_0$.
    The amount calculation secret key: $K_1$.
Output:
    The secret message(one): $M$.
key values $K_{value} \leftarrow AdderssToValue(K_1)$
address values $D_{value} \leftarrow AdderssToValue(D) + K_{value}$
AMASC code $A_m \leftarrow A$
$A_m \leftarrow Fmap(A_m)$
$AI \leftarrow A_m \% I * 10^8$
if $C \leq S * 5 * 10^8$ then
    $A_m \leftarrow Fmap(D_{value} - AI)$
else
    $A_m \leftarrow Fmap(D_{value} + AI)$
end if
$A_m \leftarrow (C - S * 10^8)//(I * 10^8)$
ciphertext $P \leftarrow$Chr$(A_m)$
$M \leftarrow AES.Dec(K_0, P)$
```

Secondly, generating K_1 using Eq. (3) and calculating K_{value} with $AddressToValue()$ function.

$$K_1 \leftarrow BIT.AddrGen(1). \tag{3}$$

The $AddressToValue()$ function adopts the ASCII code of each digit of K_1 and adds them up according to the rule that odd digits are positive and even digits are negative.

Thirdly, $AddressToValue()$ and K_{value} are employed to calculate address value D_{value}.

Finally, the symbol digit S and the index digit I are inserted in accordance with the amount design rule in Fig. 2. Then, the mapping function $Fmap(x)$ is utilized to make the amount of the proposed scheme evenly cover all the value space of Bitcoin. $Fmap(x)$ is described in detail in Section III.D. Subsequently, the AMASC code A_m and amount A are able to get with

$$A \leftarrow A_m \leftarrow (D_{value}, M_{asc}, I, S, Fmap(x)), \tag{4}$$

The transaction amounts calculation process includes the **Step 1** and **Step 2**, and the process of a single amount is shown in the Algorithm 1 in detail.

Step 3. The corresponding address-amount pairs are packed into transactions. Each transaction contains 1 input and $n + 1$ outputs (n can be customized). The transaction amount of the sending address should be greater than 0.01 BTC to distinguish the change address easily. This paper does not compare with other schemes in this aspect, mainly for two reasons. First of all, the transaction requires a commission. Take Bitcoin Core for example, its default transaction commission is 0.00001BTC/KB, thus, the capital should not be too small. Secondly, in this paper, there is no other capital loss in the communication process except the loss of transaction fees, and other addresses generated in the transaction are owned by both sides of the transaction. Therefore, it is reasonable to have more initial capital. The input address of the latter transaction is the change address of the previous transaction. For instance, in Fig. 4, the output address $addr\_i$ of the previous transaction TX_0 is the input address of the next transaction TX_1.

Step 4. The transactions packaged in **Step 3** are sent to the blockchain via Bitcoin Core [46]. It is unnecessary for a sender to send transactions in the message embedding order, but ensure that all the transactions are sent.

B. Data Extraction

The extraction process is introduced in four steps on the basis of the flow chart shown in Fig. 3 as well.

Step 1. Transactions embedded with secret information are queried by recipients based on the starting address. Then, the change address in the transaction output is identified according to the rules. The next transaction information is captured in accordance with the change address until this change address fails to retrieve the transaction information as the input address.

Step 2. The transaction address and amount are extracted from each transaction found in **Step 1**. One shall be careful not to store address-amount pairs for each transaction together or combine address-amount pairs for different transactions.

Step 3. In this step, the ciphertext P is calculated by the receiver according to the inverse process of the amount generation process. In the Algorithm 2, the process of recovering the message of a single address is shown. First, compute K_{value} and D_{value}, and covert A to A_m. Second, the inverse process of $Fmap(x)$ is used to get the A_m before mapping. Then, the ciphertext information value is calculated, and the index and symbol are extracted. Finally, sorting the message according to the index value to get the ciphertext P.

$$P \leftarrow (D_{value}, I, S, A_m, Fmap(x)). \tag{5}$$

Step 4. The ciphertext P obtained in **Step 3** is decrypted utilizing the pre-shared AES encryption key K_0 to acquire the plaintext secret message M.

$$M = AES.Dec(K_0, P). \tag{6}$$

The **Step 3** and **Step 4** are the processes of recovering messages, and recovering the message course of a single address is shown in the Algorithm 2.

C. Mapping Function $Fmap(x)$

Due to the limitation of ASCII code, the values of the third, sixth, seventh, and eighth decimal places of the proposed scheme amount are randomly distributed between $[0, 2638]$, whereas in normal Bitcoin transactions, the values should be randomly distributed between $[0, 9999]$. The other bits of the amount are generated by random functions without scope limitation and need not be mapped. Therefore, to balance distribution and improve concealing, a mapping function $Fmap(x)$ is designed to map the value evenly to $[0, 9999]$. The specific design is as follows.

For the convenience of expression, the 3rd, 6th, 7th, and 8th digits of the amount of our scheme after the decimal point

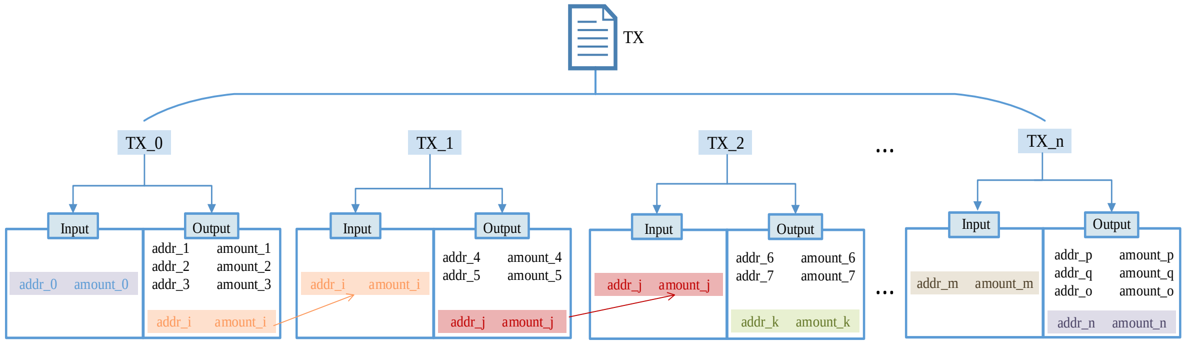


Fig. 4. The transaction address rule of the proposed approach. The output address $addr\_i$ of the previous transaction TX_0 is the input address of the next transaction TX_1.

are denoted as RA, and the corresponding four digits of the Bitcoin amount are denoted as BA. Therefore, $RA \in [0, 2638]$, $BA \in [0, 9999]$, there are 2639 possible values of RA and 10000 possible values of RB.

$Fmap(x)$ firstly subtracts 2361 when computing B in the Algorithm 1, then, $RA \in [0, 4999]$.

In the next step, $Fmap(x)$ designs a proportion of BA value corresponding to RA is $1 : 2$. Each RA maps to two BA.

After each RA value is calculated, one of the corresponding 2 BA values is randomly selected as the third, sixth, seventh, and eighth decimal places of the final amount.

VI. Theoretical Analysis and Proof

In this section, the concealment and security of the proposed method are analyzed first. In the concealment analysis, we calculate the relative entropy of our scheme and Bitcoin to compare the similarity between them. Then, the security is verified from two perspectives anti-tampering characteristics and crack probability. The anti-tampering characteristic of the proposed model is analyzed from the perspective of temper probability. The crack probability of our approach is analyzed under four different conditions from the probabilistic perspective, and the probability that the message is decrypted in our scheme, BLOCCE [16], and HC-CDE [31] is calculated. Then, the proposed method is analyzed from four aspects: computational costs, scalability, embedding capacity, and sustainable communication.

A. Concealment Analysis

For the purpose of explaining the concealment of the proposed manner, this paper firstly carries out a theoretical analysis from four aspects and then calculates the relative entropy of our scheme and Bitcoin to compare the similarity among them.

Firstly, the concealment of the proposed scheme is analyzed from four aspects. First of all, our method does not add any additional content and utilizes things that exist in normal transactions. Then, from the transaction structure and size perspective, our communication transactions are the same as ordinary transactions. Next, the proposed manner utilizes a random address to generate the amount, which brings more difficulties for attackers to identify the transaction. Then, Bitcoin Core is adopted to send transactions. We do not apply APIs developed by third-party platforms to send transactions but employ the official Bitcoin Core to send transactions, increasing the concealment.

Secondly, the mapping function $Fmap(x)$ makes the amount generated by our scheme have the same distribution interval as the amount of normal Bitcoin transactions and conform to the random distribution. Therefore, the amounts of the proposed scheme and Bitcoin are indistinguishable. The detailed proof is provided as follows.

1) In RA, each value appears randomly. After each RA value is calculated, one of the corresponding two BA values is gotten randomly, so,

$$P = \frac{1}{5000} \cdot \frac{1}{2} = \frac{1}{10000}. \tag{7}$$

2) Hence, the amount of our scheme is distributed evenly in the same range as the amount of Bitcoin.
3) According to the relative entropy formula of Eq. 8,

$$D(p \,\|\, q) = \sum_{i=1}^{n} p(x_i) \log \frac{p(x_i)}{q(x_i)} \tag{8}$$

it can be calculated as

$$p(x_i) = q(x_i) = \frac{1}{10000}, \quad D(Ours \,\|\, Bitcoin) = 0. \tag{9}$$

The relative entropy of our transaction and Bitcoin transaction is equal to 0, that is to say, the two are indistinguishable. Thus, the proposed scheme has favorable concealment.

B. Security Analysis

In this subsection, the anti-tampering characteristic of the proposed model is analyzed from the perspective of temper probability. In addition, this paper compares the possibility of secret information decryption between the proposed method and the other two schemes under different adversary capabilities. This paper chooses to analyze the probability of decryption, because, under the premise of certain concealment, the ultimate goal of adversaries must be the decryption of information, not just the discovery of communication. Therefore, this paper aims to analyze the security of the proposed approach through cracking probability.

1) Anti-tampering: To implement an attack, attackers need to program the longest chain of the attack chain, thus, we shall calculate the probability of programming the longest chain of the attack chain. Suppose that the probability of the honest chain generating a new block is h, and the probability of the attacking chain generating a new block is f ($f = 1-h$). In the case that the honesty chain extends z blocks and the attack chain extends k blocks, the probability of the attack chain successfully catching up with the honesty chain to become the longest chain is

$$Pr_{k=z} = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left(1 - \frac{f}{h^{z-k}}\right). \tag{10}$$

The attack chain produces k blocks, and k can be any integer greater than or equal to zero, thus, the probability of values of k follows the Poisson Distribution. Since values of k are uncertain, the probability of k occurring between zero and infinity is

$$Pr_k = \frac{\lambda^k e^{-\lambda}}{k!}, \tag{11}$$

where λ is the mean of k, and λ and z satisfy the proportional relationship in Eq. (12).

$$\lambda = z\frac{f}{h}. \tag{12}$$

Bitcoin transactions require six confirmations [17], thus, for attacks to succeed, z needs to be at least five. According to Eq. (10), when $z = 5$, $Pr_{k=z}$ is 0.001, indicating that our scheme is immutable.

2) Crack Probability: Intuitively, the security of our scheme depends on two keys, K_0 and K_1. If an adversary gets two keys, the hidden message can be decrypted. However, since the adversary does not have the private key of the address, and it is almost impossible to get the private key from the Bitcoin address, covert communication messages cannot be forged by the adversary.

To illustrate the security of the proposed method, a comparative analysis with BLOCCE [16] and HC-CDE [31] from the probabilistic perspective is done. When people carry out covert communication, one must protect the key. The pre-shared key of HC-CDE is represented by S_0 and S_1. To the best of our knowledge, we are the first ones to prove security from the probabilistic perspective.

Let B be an adversary. An adversary power function $L(n)$ is defined to show the information that B has. $L(n)$ could be defined as follows.

Definition 1. An adversary power $L(n) = n_0 + n_1 + \cdots + n_i$, $i \in [0,5]$, $n_i \in \{R, ID, K_0, K_1, S_0, S_1\}$. The more n_i terms, the more power B has.

- R is the rule of message embedding. B can know how the scheme realizes covert communication with R.
- ID is the identification of embedded transactions. Utilizing ID, the target transactions can be recognized.
- The pre-shared key of HC-CDE is represented by S_0 and S_1. $S_0 \to \{0,1\}$, $S_1 \to \{0,1\}$.
- K_0 and K_1 are the AES encryption key and the amount calculation key of the proposed scheme, respectively.

Theorem 1. If $L(n) = R$, the probabilities of B to decode and obtain the secret message M for the three approaches are

$$P(BLOCCE) = P(HC\text{-}CDE) = P(Ours) = 0. \tag{13}$$

Proof: Although B knows R, one cannot identify embedding transactions and cannot know how many embedding transactions are in total. None of these three schemes have obvious transaction signs, thus, they appear to be regular transactions on the surface. Therefore, the secret message cannot be extracted by B. Namely, the three schemes are safe. ■

Theorem 2. If $L(n) = ID$, the probabilities of B to decode and obtain the secret message M for the three methods are

$$P(BLOCCE) = P(HC\text{-}CDE) = P(Ours) = 0. \tag{14}$$

Proof: B is able to use ID to identify covert communication transactions from all transactions. However, considering that B does not know the embedding rules and keys, it cannot obtain the secret messages. It is only possible to decode secret messages if both ID and R are stolen. ■

Theorem 3. If $L(n) = R + ID$, the probabilities of B to decode and get the secret message M for the three schemes are

$$P(BLOCCE) = 1, \quad P(HC\text{-}CDE) = P(Ours) = 0. \tag{15}$$

Proof: The embedded transaction can be identified according to ID, and the embedded message can be directly extracted by R. For example, if B receives eight transactions, the LSB bit of every transaction is extracted and sorted by transaction time. Then, a string of binary numbers such as "01010100" can be obtained. Finally, "01010100" is converted to a secret message "T". For HC-CDE and our scheme, since these two methods have two keys, B cannot extract the secret message M even if he knows R after acquiring the transaction information. HC-CDE uses a hash function that is irreversible and cannot be cracked by B. The proposed approach utilizes AES encryption, meaning that B cannot crack. Therefore, HC-CDE and our scheme have safety under this condition. ■

Theorem 4. If $L(n) = R + ID + S + K$, $S \in \{S_0, S_1\}$ and $K \in \{K_0, K_1\}$, the probabilities of B to get the secret message for the three schemes are $P(BLOCCE) = 1$,

$$\begin{aligned} &\text{I.} \quad P(HC\text{-}CDE) \in [2^{-1}, 1], \\ &\text{II.} \quad P(Ours) \in \{0, 2517^{-1}\}. \end{aligned} \tag{16}$$

Proof for Statement I: For B, having S_0 or having S_1 is equivalent. Suppose the adversary B gets S_0, then, $L(n) = R + ID + S_0 + K$ and he guesses $S_0 \to 0$. The probability that B uses $L(n)$ to acquire the secret message M is shown below.

1) B retrieves public key PSK_i and PSK_{i+1} from the addresses $addr_i$ and $addr_{i+1}$ of transaction tx_i.
2) Private key SK_{i+1} is obtained by B with $Hash(PSK_i, S_0)$.
3) B calculates public key PSK'_{i+1} according to SK_{i+1}.
4) PSK_{i+1} and PSK'_{i+1} are compared. If $PSK_{i+1} = PSK'_{i+1}$, 0 is hidden in tx_i. Otherwise, 1 is hidden in tx_i.
5) Go to the next transaction and repeat the above steps to get the hidden message until all transactions are processed. Then, B can acquire a binary string STR.

6) STR is converted by B to obtain M'.
7) If M' is meaningful, B guesses right. On the contrary, he guesses wrong and $S_0 \rightarrow 1$.
8) The above is the best scenario and $P(HC\text{-}CDE) = 1$ in this time. However, if B just has one communication transaction, then it is likely that M' is meaningful whether he guesses $S_0 \rightarrow 1$ or $S_0 \rightarrow 0$. In this condition, $P(HC\text{-}CDE) = 2^{-1}$. But if B obtains sufficient data,

$$P(HC\text{-}CDE) = 2^{-1} + 2^{-2} + 2^{-3} + \cdots 2^{-n}, n \in N^{+}. \quad (17)$$

Namely, $P(HC\text{-}CDE) \rightarrow 1$ infinitely. Hence, the probability for B to get M is sufficiently large.

■

Proof for Statement II: Suppose the adversary B gets K_0, then, $L(n) = R + ID + K_0$. To acquire the secret message M, B needs to solve: $P = A - K_{value} - D_{value}$ and then decrypt P. Utilizing $L(n)$, $P \rightarrow M$ can be calculated, hence, B need to obtain P. Then, the probability used $L(n)$ to acquire P is as follows.

1) B gets A and D_{value} according to R and ID.
2) Due to $AddressToValue()$, K_{value} is limited in scope and $K_{value} \in [-1258, 1258]$, therefore, K_{value} has 2517 possibilities. Hence, B can only use an exhaustive matching method to solve. Thus, $P(Ours) = 2517^{-1}$.
3) However, there may be more than one correct K_{value} possibility based on a single covert communication transaction. Let m_i represent the number of K_{value} that may be correct in the $i - th$ communication. During this time,

$$P(Ours) = \frac{m_1}{2517} \cdot \frac{m_2}{m_1} \cdot \frac{m_3}{m_2} \cdots \frac{m_i}{m_{i-1}}, m \in N^{+}. \quad (18)$$

Hence, when $i \rightarrow \infty$, and $m_i \rightarrow 1$, $P(Ours) = 2517^{-1}$.

Suppose the adversary B gets K_1, then, $L(n) = R + ID + K_1$. To obtain the secret message M, B needs to solve: $P = A - K_{value} - D_{value}$ and then decrypt P. In this $L(n)$, B acquires P, but he cannot calculate $P \rightarrow M$. In our scheme, AES-256 is adopted, which is almost impossible to crack proverbially. Hence, the probability $P(Ours) = 0$. ■

C. Computational Costs Analysis

The computational cost of the proposed approach is calculated and compared with the existing schemes from the embedding process and extracting process respectively. Assuming that m bytes are embedded in each transaction, a total of N bytes of plaintext message need to be embedded. Due to AES encryption, the length of the message to be embedded is doubled. Namely, the length of the ciphertext is $2N$. Under this assumption, the transaction count that needs to be sent is $2N/m$.

We use q, s, and d to represent the time cost of querying a transaction, sending a transaction, and randomly generating an address respectively. In Bitcoin, since the transaction sending and querying are completed by API, parameters q, s, and d are constants. Meanwhile, the computational cost of the proposed scheme and other methods depends on N, embedding algorithm, and extraction algorithm. Table II illustrates the computational cost of each scheme, reflecting that the computational cost of our approach is similar to that of BLOCCE and HC-CDE. The computational cost of embedding contains three parts: data pre-processing, data embedding, and transaction sending. The computational cost of extraction includes three parts: transaction querying, data extraction, and data conversion. In Table II, each {} denotes one part. According to the following analysis, the computational cost of our scheme is bigger than BLOCCE and smaller than HC-CDE.

In this part, C_{aes} is computational costs of the AES algorithm, C_{al-em} and C_{al-ex} are respectively computational costs of the embedding and extraction algorithm of our scheme, C_{gen} is computational costs of key generation algorithm, C_{p2a} is computational costs of address generation based on the public key, C_{gpk} and C_{mul} are computational costs of public key extraction and elliptic curve multiplication respectively, C_{cmp} and C_{bin} are computational costs of comparison and binary conversion respectively. We use EM_a^i and EX_a^i to represent computational costs of the part i of scheme a in embedding and extraction respectively. EM_a and EX_a are computational costs of a in embedding and extraction process respectively.

Embedding. Under normal conditions, $C_{bin} < C_{aes}$, therefore, $EM_{BLOCCE}^1 = EM_{HC\text{-}CDE}^1 < EM_{Ours}^1$. Because $tn = \frac{2N}{ml} < N$, $EM_{BLOCCE}^3 = EM_{HC\text{-}CDE}^3 > EM_{Ours}^3$. Since the key generation operation of HC-CDE includes the hash operation and elliptic curve operation, and the embedding operation of our scheme is a simple math transformation, It can be inferred that $C_{gen} >> C_{al-em}$. In addition, $C_{p2a} > d$ because the process of generating addresses at random is simpler than according to a public key. So, $EM_{BLOCCE}^2 < EM_{Ours}^2 << EX_{HC\text{-}CDE}^2$. Hence, $EM_{BLOCCE} < EM_{Ours} < EM_{HC\text{-}CDE}$ can be deduced.

Extraction. Similar to analysis on embedding process, $EX_{BLOCCE}^3 = EX_{HC\text{-}CDE}^3 < EX_{Ours}^3$. Since the extraction operation of HC-CDE contains the hash operation and elliptic curve operation, moreover, the extraction operation of our method is a simple math transformation, it is easy to get $(C_{cmp} + C_{mul}) > > C_{al-ex}$. Besides, $tn < N$, so, $0 = EX_{BLOCCE}^2 < EX_{Ours}^2 << EX_{HC\text{-}CDE}^2$ and $EX_{BLOCCE}^1 = EX_{HC\text{-}CDE}^1 > EX_{Ours}^1$. Therefore, it can be concluded that $EX_{BLOCCE} < EX_{Ours} < EX_{HC\text{-}CDE}$.

D. Scalability Analysis

In the analysis and experiment, we define the transaction as one input and seven outputs. Certainly, in practice, the mode of n input (s) and m output (s) can be adopted (n and m are integers). Multiple addresses can be used when the amount of change address is insufficient.

In principle, there is no upper limit to the number of addresses contained in each Bitcoin transaction. However, in practice, there is a certain limit to the number of addresses contained in Bitcoin transactions. For example, Bitcoin generates one block every 10 minutes, each block is currently about 1MB, and one transaction contains input and output addresses that take up a certain capacity. In addition, Bitcoin prescribes standard transactions used to protect and help the entire Bitcoin network. As of Bitcoin Core 0.9.3, standard transactions stipulate that transaction sizes must be less than 100,000 bytes. This is about the size of more than 200 typical single input,

TABLE II
COMPUTATIONAL COSTS OF THE PROPOSED SCHEME AND OTHER BLOCKCHAIN COVERT COMMUNICATION SCHEMES. tn DENOTES THE TRANSACTION COUNT THAT NEEDS TO BE SENT OF THE PROPOSED SCHEME ($tn = \frac{2N}{ml} < N$, ml IS MESSAGE LENGTH EMBEDDED IN EACH TRANSACTION).

Schemes	**Embedding**	**Extraction**
	{Data Pre-processing} + {Data Embedding} + {Transaction Sending}	**{Transaction Querying} + {Data Extraction} + {Data Conversion}**
BLOCCE [16]	$\{C_{bin}\} + \{8 \cdot N \cdot 62 \cdot d\} + \{8 \cdot N \cdot s\}$	$\{8 \cdot N \cdot q\} + \{0\} + \{C_{bin}\}$
HC-CDE [31]	$\{C_{bin}\} + \{8 \cdot N \cdot (C_{gen} + 2 \cdot C_{p2a})\} + \{8 \cdot N \cdot s\}$	$\{8 \cdot N \cdot q\} + \{8 \cdot N \cdot (2 \cdot C_{gpk} + 2 \cdot C_{mul} + C_{cmp})\} + \{C_{bin}\}$
Ours	$\{C_{aes}\} + \{2 \cdot N \cdot C_{al-em} + d \cdot (2 \cdot N + tn)\} + \{tn \cdot s\}$	$\{tn \cdot q\} + \{tn \cdot C_{al-ex}\} + \{C_{aes}\}$

single output P2PKH transactions. Standard transactions also stipulate that the signature script size for each transaction must be less than 1650 bytes. In a P2SH transaction, this is enough to accommodate 15-of-15 multiple signatures using a compressed public key. Therefore, in our scheme, the output address of the transaction cannot be increased indefinitely.

One can freely choose the encryption methods beyond the conventional AES encryption or choose transfer plaintext, affecting embedding capacity and security. The amount calculation method of the proposed scheme can be applied to Ethereum as well. Moreover, the amount setting rules can be customized by users.

E. Embedding Capacity Analysis

To optimize existing covert communication approaches, the embedding capacity of single-time communication must be improved. In our scheme, the bit embedding approach is not adopted because it likely increases security risks. One must embed it in many places in the transaction to increase the embedding capacity if he utilizes the bit embedding way. We design the AMASC code to convert the bytes and embed them in the transaction amount. In this way, one byte can be embedded in an amount increasing the embedding capacity. The AMASC code is obtained by the address and the key through a series of transformations, and the specific transformation process is introduced in the Algorithm 1. Considering that our method is AES encrypted before embedding, the length of the secret message is doubled. Therefore, one byte of plaintext corresponds to two address-amount pairs. That is, one address-amount pair can embed four bits of plaintext messages (eight bits of ciphertext messages). Utilizing the UTXO structure, one transaction in this paper contains six output address-amount pairs that contain secret messages. Hence, the embedding capacity of one transaction is forty-eight bits. namely, one transaction is able to contain twenty-four bits of plaintext messages because of AES encryption. The embedding capacity of our scheme per address pair is eight times that of the traditional approach.

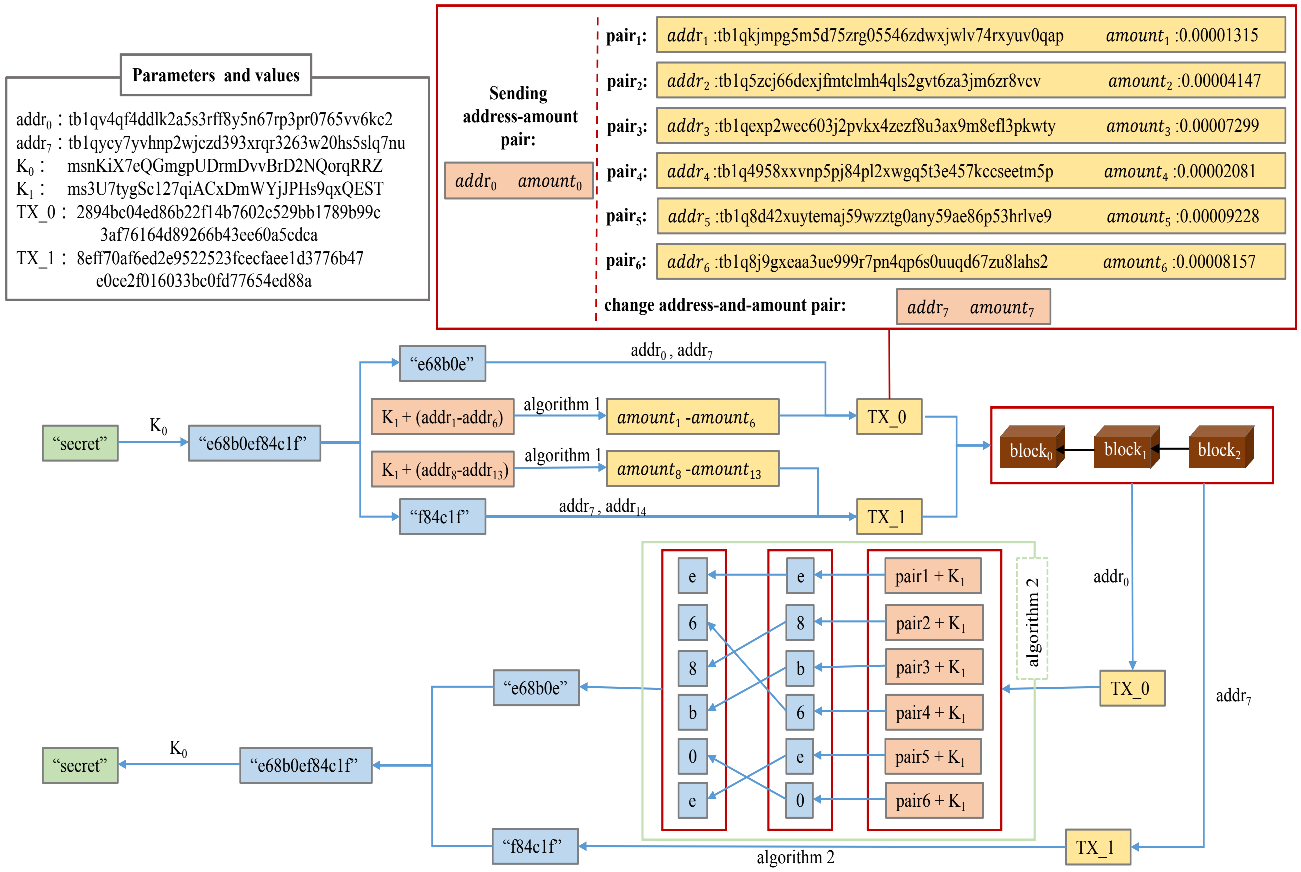
The above analysis of the embedding capacity of the model is limited to the setup of this experiment and the algorithm of the model is now extended to the theoretical case to analyze its embedding capacity. The scheme proposed requires six amount significant digits, but the index digit can be reused. According to the fixed total amount of Bitcoin, one can see that the sum of integer bits and decimal places of Bitcoin amount is sixteen. Thus a maximum of three bytes can be hidden in a Bitcoin amount. Assuming that a transaction has m transaction addresses, a Bitcoin transaction can be embedded with a maximum of $3m$ bytes. In addition, the scheme presented in this paper is not only applicable to Bitcoin but also can be applied to other blockchain frameworks. Assuming that the number of digits of the transaction amount is n, the number of bytes that can be embedded in each transaction amount in this scheme is $[(n-6)/5]+1$, where $[\cdot]$ denotes the rounding operation.

As shown in Table I, in terms of the basic requirements of covert communication, both the existing address-based covert communication schemes and the proposed schemes perform well. Compared with existing address-based schemes, the embedding capacity of one address-amount pair is eight times that of the proposed scheme. However, theoretically, the length of an address in Bitcoin is 32, so it can embed up to 32 bytes of information, which is higher than the hidden communication scheme based on the amount proposed in this paper. However, it can be seen from Section VII.C that the time cost of the current address-based model is already relatively large. If address embedding is carried out in a matching way and concealment is considered, random addresses should be used. Regardless of how the location information is embedded, each additional byte of embedding capacity increases the time cost exponentially. This is also why the embedding capacity of current address-based schemes is Bit-level. This paper designs a covert communication model based on transaction amount, which can increase the embedding capacity of the existing covert communication model while ensuring security, concealment, and time costs.

F. Sustainable Communication Analysis

Instead of inserting an identifier into a transaction to identify particular transactions, the input addresses are utilized to identify transactions. Because of Bitcoin's UTXO structure, the balance of each transaction is transferred to a change address. Our scheme ingeniously exploits the address of change in Bitcoin transactions to achieve sustainable communication. We use the change address of the previous transaction as the input address for the next transaction. The two parties do not have to renegotiate the starting address when starting the second transaction. The recipient only needs to monitor for the change address of the last transaction in the last communication. In this way, not only is sustainable communication between the two sides realized, but also the times of information sharing through other channels are reduced, and security is enlarged.

Although the Bitcoin change address is public, the proposed model still has superior concealment. First, the change address is the fixed structure of Bitcoin, so the presence of a change address in a transaction does not arouse suspicion. Secondly,



Parameters and values

$addr_0$: tb1qv4qf4ddlk2a5s3rff8y5n67rp3pr0765vv6kc2
$addr_7$: tb1qycy7yvhnp2wjczd393xrqr3263w20hs5slq7nu
K_0 : msnKiX7eQGmgpUDrmDvvBrD2NQorqRRZ
K_1 : ms3U7tygSc127qiACxDmWYjJPHs9qxQEST
TX_0 : 2894bc04ed86b22f14b7602c529bb1789b99c3af76164d89266b43ee60a5cdca
TX_1 : 8eff70af6ed2e9522523fcecfaee1d3776b47e0ce2f016033bc0fd77654ed88a

Sending address-amount pair: $addr_0$ $amount_0$

$pair_1$: $addr_1$:tb1qkjmpg5m5d75zrg05546zdwxjwlv74rxyuv0qap $amount_1$:0.00001315
$pair_2$: $addr_2$:tb1q5zcj66dexjfmtclmh4qls2gvt6za3jm6zr8vcv $amount_2$:0.00004147
$pair_3$: $addr_3$:tb1qexp2wec603j2pvkx4zezf8u3ax9m8efl3pkwty $amount_3$:0.00007299
$pair_4$: $addr_4$:tb1q4958xxvnp5pj84pl2xwgq5t3e457kccseetm5p $amount_4$:0.00002081
$pair_5$: $addr_5$:tb1q8d42xuytemaj59wzztg0any59ae86p53hrlve9 $amount_5$:0.00009228
$pair_6$: $addr_6$:tb1q8j9gxeaa3ue999r7pn4qp6s0uuqd67zu8lahs2 $amount_6$:0.00008157

change address-and-amount pair: $addr_7$ $amount_7$

Fig. 5. Details of the example. The secret message is "secret". TX_0 and TX_1 are the embedded transaction. One sending address-amount pair, six embedded address-amount pairs, and one change address-amount pair are contained in TX_0 and TX_1.

in a normal Bitcoin transaction, the sending address of each transaction is the change address of a previous transaction, so it is reasonable for this model to use it as a bridge for sustainable communication. Moreover, the change address in this model can be randomly generated by the system without any special characteristics.

VII. Experimental Results and Analysis

In this section, detailed experimental settings are given. Furthermore, the detailed implementation example of the proposed method on the Bitcoin Testnet is described to verify its feasibility. To evaluate the performance, the proposed scheme is compared with BLOCCE [16] and HC-CDE [31] in terms of time costs, the number of transactions, and transaction fees. In the experimental part, there are two purposes: (1) verifying the implementability of our scheme on Bitcoin, and (2) comparing the proposed approach with BLOCCE and HC-CDE in terms of the number of transactions, time costs, and transaction fees. There are two main reasons for choosing BLOCCE and HC-CDE for comparison: (1) BLOCCE, HC-CDE, and our scheme all use transactions for covert communication, which has certain similarities, and (2) BLOCCE is the first method of blockchain covert communication. HC-CDE has the best effect, the most comprehensive analysis, the highest quality, and the most representative of utilizing transaction addresses for covert communication in blockchain at present.

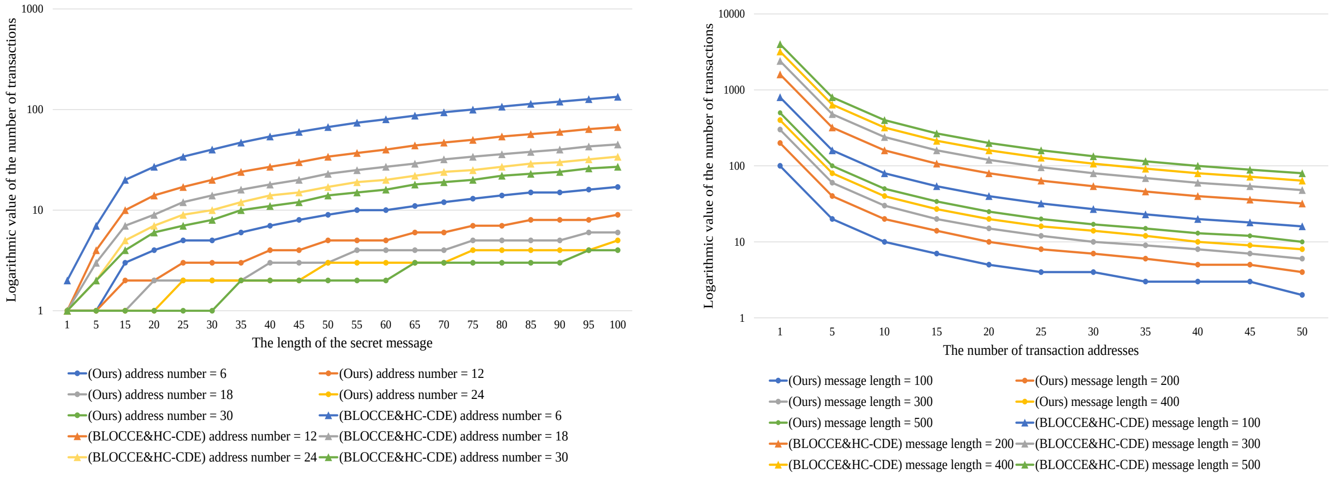
A. Experimental Settings

The proposed scheme is implemented with Python and tested in the Bitcoin Testnet [47]. Bitcoin Core provides the Testnet environment, and transactions can be sent conveniently. On the receiver side, BlockCypher [48] is utilized to query transactions. In the Testnet, coins are able to be obtained through a server called faucet. Mainnet and Testnet are independent of each other, and the coin obtained from the faucet can not be used on the Mainnet. Furthermore, the proof-of-work difficulty of Testnet is lower than Mainnet, which accelerates the block generation process.

B. Case Study of the Proposed Scheme

In this subsection, six bytes message "secret" are embedded on the Bitcoin Testnet using Bitcoin Core. Before the first covert communication, the parties have to share some information, including the AES encryption key K_0, the amount calculation key K_1, and the address of the first communication $addr_0$. Fig. 5 shows the example of our scheme, and one can verify the transactions tabulated. In this example, the symbol bits are simplified to 0 and 1 to reduce fundraising. In addition, $Fmap(x)$ mapping is not performed in the example due to the funding shortage.

Embedding. In this phase, six bytes "secret" need to be embedded in Bitcoin. The first thirty-two bits of a randomly generated address are utilized as K_0, and another randomly



(a) case 1

(b) case 2

Fig. 6. The variation in the number of transactions that need to be sent in case 1 and case 2. Dots and triangular lines represent our model and the contrast model respectively.

generated address as K_1. Firstly, the plaintext "secret" is converted to the ciphertext "e68b0ef84c1f" with AES encryption key K_0. Secondly, Bitcoin Core is adopted to generate fourteen random addresses (two change addresses and twelve embedded addresses). Thirdly, the amount corresponding to each address is calculated with the Algorithm 1. Fourthly, make use of address-amount pairs to construct two transactions TX_0 and TX_1, each including six embedded addresses, one change address, and one sending address. The sending address of the second transaction is the change address of the first transaction. Finally, these transactions are sent to Testnet with Bitcoin Core.

Extraction. In this phase, the secret message "secret" is extracted. First of all, BlockCypher is utilized to query the transaction TX_0 based on pre-shared addresses $addr_0$. Using the change address $addr_7$ of TX_0 to query TX_1. Then, twelve transaction addresses and the corresponding amounts are drawn from the two transactions. Next, the ciphertext is calculated with Algorithm 1. Finally, the ciphertext "e68b0ef84c1f" is converted to plaintext "secret" with AES encryption key K_0.

C. Comparative Experiments

In this subsection, our proposed method is compared with BLOCCE [16] and HC-CDE [31] in terms of the number of transactions, time costs, and transaction fees.

*1) **Comparison of Transactions Number**:* In this part, the variation in the number of transactions that need to be sent is discussed in the following two cases.

Case 1: In the case of a different number of output addresses, the number of transactions required changes with the increase in the length of embedded information. As shown in Fig. 6(a), as the length of secret information increases, the number of transactions required by the proposed scheme increases gradually, and in the case of larger output addresses, the number of transactions required increases more slowly. A comparison between dot lines and triangular lines shows that under the same conditions, the proposed scheme requires far fewer transactions than the existing schemes. In addition, when the number of output addresses of each transaction increases, the length of secret information that can be matched by each transaction becomes longer. This is because, as the number of output addresses increases, the length of secret information that can be embedded in a single transaction increases as well. Although BLOCCE and HC-CDE capacity increase too, the increase is much smaller than the proposed solution. Experimental results show that the proposed scheme is more suitable for large-capacity embedding than existing schemes.

TABLE III
TIME COSTS OF THE MAIN ALGORITHM (48 BITS SECRET MESSAGE). LOWER VALUE INDICATES BETTER PERFORMANCE.

Criteria	Schemes	Max (s)	Min (s)	Mean (s)
MEMA Time	BLOCCE [16]	2.480124	2.418124	2.442924
	HC-CDE [31]	0.255085	0.231584	0.239959
	Ours	**0.016093**	**0.012101**	**0.014108**
MEXA Time	BLOCCE [16]	**0**	**0**	**0**
	HC-CDE [31]	0.411799	0.372619	0.387465
	Ours	0.000970	0.000705	0.000770

Case 2: Changes in the number of transactions required as the number of output addresses increases under different information lengths. As shown in Fig. 6(b), with the increase in the number of output addresses, the number of required transactions shows a downward trend. The larger the length of secret information, the more transactions are consumed. For all cases, the proposed scheme required fewer transactions than BLOCCE and HC-CDE. Experimental results show that the proposed scheme has a great advantage in the required number of transactions.

*2) **Comparison of Time Costs**:* To compare time costs between the proposed approach and other schemes effectively, time costs of the main embedding algorithm (MEMA) and the

TABLE IV
THE COMPARISONS OF TIME COSTS. NUMBERS IN BOLD INDICATE BEST PERFORMANCE.

Schemes	MEMA Time (s)	MEXA Time (s)	Embedding Time (s)	Extraction Time (s)
BLOCCE [16]	2.442924	**0**	$t_1 + 48t$	$28800 + 48t_0$
HC-CDE [31]	0.239959	0.387465	$t_1 + 48t$	$t_2 + 48t_0$
Ours	**0.014108**	0.000770	$t_1 + 2t$	$t_2 + 2t_0$

main extraction algorithm (MEXA) of the three methods are compared first, and then time costs of the total embedding and extraction process are compared.

MEMA and MEXA are different in each scheme. For our approach, MEMA is the address generation algorithm and embedding algorithm, and MEXA is the extraction algorithm. As for BLOCCE, MEMA is an algorithm for generating coincidence addresses, and it does not need MEXA. With regard to HC-CDE, MEMA is the corresponding public key calculation algorithm and address generation algorithm, and MEXA is the public key calculation algorithm and comparison algorithm. In the experiment, the length of the secret message is set to 48 bits, and the MEMA and MEXA time of each scheme are calculated many times. Then, the maximum, minimum, and average values of the results are shown in Table III, which demonstrates that our scheme outperforms HC-CDE in the MEMA and MEXA time and is inferior to BLOCCE in the MEMA time. The MEMA time of the BLOCCE scheme and HC-CDE scheme is about 17 times and 174 times of the proposed scheme respectively, indicating that the proposed scheme embedding algorithm is relatively simple. The MEXA time of the HC-CDE scheme is roughly 500 times that of the proposed scheme, which means that our scheme makes it easy to extract secret information. In terms of MEXA time, the proposed scheme is inferior to the BLOCCE scheme. This is due to the special design of the BLOCCE scheme, which requires almost no extraction. However, due to the huge waiting time for the extraction process, the final extraction time of the BLOCCE scheme is much higher than the proposed scheme.

The average values in Table III are chosen as the MEMA time and MEXA time for the three methods. As shown in Table IV, the expressions of the total embedding time and the total extraction time of the three schemes are calculated. In this experiment, the length of the secret message is set to 48 bits. For BLOCCE, embedding time is $t_1 + 48t$, and extraction time is $28800 + 48t_0$. 28800 is the time of block generation. About HC-CDE, embedding time is also t_1+48t, and extraction time is $t_2 + 48t_0$. With regard to our scheme, embedding time is $t_1 + 2t$, and extraction time is $t_2 + 2t_0$. t_1 is MEMA time, t_2 is MEXA time. Considering different APIs, sending and querying a transaction takes different amounts of time. We utilize t to indicate the time it takes to send a transaction and t_0 to indicate its time to query a transaction. From these expressions, it can be seen that when the secret message of the same length is embedded, the number of transactions needed to be sent by the proposed model is smaller than that of other models.

To test the impact of API response time on schemes, as indicated in Table V, eight different API response times are adopted to show the time cost of the three approaches in the embedding and extraction process with a fixed 48-bits secret message length. Table V demonstrates that the time cost of the proposed scheme is lower than the other two schemes, both in the embedding and extraction process. Furthermore, as the response time of API increases, the advantage of the proposed scheme does not diminish.

In addition to the time cost comparison of the fixed API response time, the time cost of the three schemes for variable-length messages is compared as well. In Table VI, a fixed time of 0.5s and 0.2s are spent to send a transaction and query a transaction, respectively. Then, time costs of the embedding and extraction process at eight different message lengths are calculated. Table VI shows that as the length of the message increases, the time cost of our method, both in the embedding process and the extraction process, grows slowly and has a low value. This is because as the length of the secret message increases, BLOCCE needs to generate more eligible transaction addresses, resulting in increased time required. Furthermore, due to the low volume, the number of transactions required by BLOCCE increases, and the time to send and query transactions increases. In addition, since BLOCCE is sorted by block-out time, it has to wait for block-out, resulting in a time-consuming extraction. HC-CDE does not need to rely on block time sorting, so the extraction time is better than BLOCCE, but its low embedding amount leads to a large number of required transactions, and time-consuming sending and query. On the contrary, the proposed scheme is superior to the existing scheme because it has a large amount of embedding, requires fewer transactions, takes less time to send and query transactions, and does not depend on the sorting of block time. In addition, as the length of secret information increases, the time advantage of the proposed scheme becomes more significant, indicating that our model is more suitable for information embedding with larger secret information length.

The time cost of a blockchain covert communication scheme is composed of two parts: on-chain time and off-chain time. The delay of the proposed scheme in the actual communication process is mainly the off-chain algorithm time, and the on-chain time is almost zero. Considering that the proposed model does not rely on block order to sort, a lot of waiting time for block generation is reduced. In the proposed scheme, after the sender sends the message, the receiver can receive the message immediately. Even if multiple messages are sent at the same time, the immediate reception of the recipient is not affected. Therefore, for the proposed scheme, after the sender sends the message, the receiver can extract the secret information immediately. In contrast, BLOCCE [16] schemes rely on block-out time ordering, which has a huge communication delay. In addition, compared with the existing schemes, the proposed algorithm is relatively simple and the calculation time is short, which can ensure the communication delay is in the acceptable range to a certain extent. It can also be seen from the above experimental data that the proposed scheme has certain advantages in the time cost. Especially in the aspect of extracting time cost, the proposed scheme has

TABLE V
The Comparisons of Time Costs with Fixed Secret Message Length (48 Bits) and Variable API Response Time. Numbers in Bold Indicate Best Performance.

Criteria	**Schemes**	**Response Time of API (s): t, t_0**							
		0.1, 0.1	**0.2, 0.2**	**0.3, 0.3**	**0.4, 0.4**	**0.5, 0.5**	**0.6, 0.6**	**0.7, 0.7**	**0.8, 0.8**
Embedding Time (s)	BLOCCE [16]	7.242924	12.042924	18.842924	21.642924	26.442924	31.242924	36.042923	40.842924
	HC-CDE [31]	5.039959	9.839959	14.639959	19.439959	24.239959	29.039958	33.839958	38.639959
	Ours	**0.214108**	**0.414108**	**0.614108**	**0.814108**	**1.014108**	**1.214108**	**1.414108**	**1.614108**
Extraction Time (s)	BLOCCE [16]	28804.8	28809.6	28814.4	28819.2	28824.0	28828.8	28833.6	28838.4
	HC-CDE [31]	5.187465	9.987465	14.787465	19.587465	24.387465	29.187464	33.987464	38.787465
	Ours	**0.200770**	**0.400770**	**0.600770**	**0.800770**	**1.000770**	**1.200770**	**1.400770**	**1.600770**

TABLE VI
The Comparisons of Time Costs with the Vary Length of Secret Messages and Fixed Response Time of API (t = 0.5s, t_0 = 0.2s). Numbers in Bold Indicate Best Performance.

Criteria	**Schemes**	**Length of Message (byte, bit)**							
		1, 8	**2, 16**	**3, 24**	**6, 48**	**9, 72**	**12, 96**	**15, 120**	**18, 144**
Embedding Time (s)	BLOCCE [16]	4.4340248	8.8060496	13.1780682	26.4181426	39.6582046	52.9602852	66.0763472	79.3164216
	HC-CDE [31]	4.0409306	8.10414	12.1287693	24.2483706	36.3720602	48.5000265	60.63222	72.7251152
	Ours	**0.5021239**	**0.505401**	**0.5064522**	**1.0108174**	**1.5187984**	**2.0315421**	**2.5404643**	**3.0451687**
Extraction Time (s)	BLOCCE [16]	4801.6	9603.2	14404.8	28809.6	43214.4	57619.2	72024	86428.8
	HC-CDE [31]	1.6628569	3.3296497	4.9916075	9.9960633	14.9695682	19.9639273	25.0077112	29.4008638
	Ours	**0.2001189**	**0.2002472**	**0.2004818**	**0.4007762**	**0.6012092**	**0.8015319**	**1.0019036**	**1.2056172**

TABLE VII
Comparisons in Transaction Fees (48 Bits Secret Message). Numbers in Bold Indicate Best Performance.

Schemes	**Embedded Capacity (bit)**	**System Costs (tx)**	**Single Transaction Fee (BTC)**	**Total Fees (BTC)**
BLOCCE [16]	1	48	**0.00000141**	0.00006768
HC-CDE [31]	1	48	**0.00000141**	0.00006768
Ours	**8**	**2**	0.00000296	**0.00000592**

obvious advantages. In the real-world covert communication environment, the time advantage of the scheme can enable the receiver to extract the secret information quickly and reduce the communication delay, which is of great significance for covert communication.

*3) **Comparison of Transaction Fees**:* Transaction fees among the three schemes are evaluated. As in the previous experiment, the secret message length is fixed at forty-eight bits, and Bitcoin Core is utilized to calculate the single transaction fee and system costs. The system cost is the number of transactions to send the secret message. For BLOCCE [16] and HC-CDE [31], the single transaction fee is 0.00000141 BTC, and system costs are forty-eight. For our method, the single transaction fee is 0.00000296 BTC, and system costs are 2. As shown in Table VII, the total fees of the proposed approach are less, which means the cost of our model is lower.

Transaction fees are an integral part of Bitcoin transactions and the most direct cost of blockchain covert communication. As shown in Table VII, compared with the existing schemes, the proposed scheme requires fewer transaction fees to transmit the same information. In blockchain covert communication, we cannot eliminate transaction fees, but can only reduce transaction fees by increasing the embedding capacity and reducing the system cost as much as possible.

VIII. Conclusion

An amount-based covert communication scheme over the blockchain is proposed in this paper. Instead of hiding messages in addresses, the proposed method constructs the A-MASC code embedding strategy, which could hide secret messages into transaction amounts to increase the embedding capacity and can use any randomly generated address. The embedding capacity of our scheme is eight times than that of the traditional approaches. To enhance concealment, this paper designs a mapping function to make the transaction amount of the proposed scheme indistinguishable from the transaction amount of Bitcoin. Besides, the cross entropy between the transaction amount of the proposed scheme and the transaction amount of Bitcoin is zero, which proves the good concealment of the proposed scheme. Additionally, we exploit the UTXO structure and the change address of Bitcoin to solve the time cost and identifier issues. We implement the proposed scheme on Bitcoin Testnet. Everyone can verify and analyze the effectiveness of the proposed scheme by extracting secret information online. The model parameters are publicly available for facilitating further research. Four different adversary abilities are applied to compare the security of the proposed method and other blockchain covert communication schemes from the probabilistic perspective. It can be seen from the experimental results that the cracking probability of the proposed scheme is 2517^{-1} when the information leakage is the highest, which is smaller than the existing scheme. In addition, the concealment analysis shows that the proposed scheme is indistinguishable from Bitcoin. In the same case, the embedding time and extraction time required by the proposed scheme are much smaller than that of the existing scheme. The transaction costs required would be approximately one-tenth of the existing options. The embedding capacity is eight times that of the current scheme and the number of transactions required is one-24th of the current scheme. Experimental results and analysis verify that our approach outperforms state-of-the-art methods regarding embedding capacity, time costs, number of transactions, transaction fees, concealment, and security. This scheme is expected to promote the research on blockchain covert communication and provide a theoretical basis and technical support for covert communication applications in the highly confidential field, which is of great significance to the research on information security in the public Internet environment.

In future work, we would like to focus on exploring more effective concealment detection methods and using blockchain to secretly transfer a large amount of messages. In addition, we will explore other more secure embedding locations with greater capacity on the blockchain.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Nos. U22A2030, 61972142, 61901237, 62171244, 62272154, 62002113), the National Key Research and Development Program of China (No. 2022YFB3103500), the Science and Technology Innovation Program of Hunan Province (No. 2023RC3125), the Science & Technology Talents Lifting Project of Hunan Province (No. 2023TJ-N23), the Training Program for Excellent Young Innovators of Changsha (No. kq2209008).

References

[1] J. An, Z. Wang, X. He, X. Gui, J. Cheng and R. Gui, "Know Where You are: A Practical Privacy-Preserving Semi-Supervised Indoor Positioning via Edge-Crowdsensing," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4875-4887, 2021.

[2] R. Yan, "The Rise of Multimedia for Online Communication Startups," *IEEE MultiMedia*, vol. 22, no. 4, pp. 100-104, 2015.

[3] C. Zhang, J. Sun, X. Zhu and Y. Fang, "Privacy and Security for Online Social Networks: Challenges and Opportunities," *IEEE Network*, vol. 24, no. 4, pp. 13-18, 2010.

[4] Y. Jiang, X. Xu and F. Xiao, "Attribute-Based Encryption With Blockchain Protection Scheme for Electronic Health Records," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3884-3895, 2022.

[5] S. Bai, G. Yang, G. Liu, H. Dai and C. Rong, "NttpFL: Privacy-Preserving Oriented No Trusted Third Party Federated Learning System Based on Blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3750-3763, 2022.

[6] R. D. Garcia, G. S. Ramachandran, R. Jurdak and J. Ueyama, "Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3781-3793, 2022.

[7] H. Xiao, B. Xiao and Y. Huang, "Implementation of Covert Communication Based on Steganography," in *Proc. of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1512-1515, 2008.

[8] J. Tan, X. Liao, J. Liu, Y. Cao and H. Jiang, "Channel Attention Image Steganography with Generative Adversarial Networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 2, pp. 88-903, 2022.

[9] G. Kessler, "An Overview of Steganography for the Computer Forensics Examiner," *Forensic Science Communications*, vol. 6, no. 3, pp. 1-27, 2004.

[10] Z. Cheng, J. Si, Z. Li, L. Guan, Y. Zhao, D. Wang, J. Cheng and N. AI-Dhahir, "Covert Surveillance via Proactive Eavesdropping Under Channel Uncertainty," *IEEE Transactions on Communications*, vol. 69, no. 6, pp. 4024-4037, 2021.

[11] M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama and M. J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1201-1210, 2013.

[12] G. Xu, W. Li, J. Liu. "A Social Emotion Classification Approach Using Multi-model Fusion," *Future Generation Computer Systems*, vol. 102, pp. 347-356, 2020.

[13] J. Ye, J. Ni and Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 11, pp. 2545-2557, 2017.

[14] Y. Ren, D. Liu, C. Liu, Q. Xiong, J. Fu and L. Wang, "A Universal Audio Steganalysis Scheme based on Multiscale Spectrograms and DeepResNet," *IEEE Transactions on Dependable and Secure Computing*, DOI: 10.1109/TDSC.2022.3141121, 2022.

[15] Y. Cao, H. Zhang, X. Zhao and X. He, "Steganalysis of H.264/AVC Videos Exploiting Subtractive Prediction Error Blocks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3326-3338, 2021.

[16] J. Partala, "Provably Secure Covert Communication on Blockchain," *Cryptography*, vol. 2, no. 3, pp. 18, 2018.

[17] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," *Decentralized Business Review*, pp. 21260, 2008.

[18] T. Zhang, B. Li, Y. Zhu, T. Han and Q. Wu. "Covert Channels in Blockchain and Blockchain Based Covert Communication: Overview, State-of-the-art, and Future Directions," *Computer Communications*, DOI: 10.1016/j.comcom.2023. 04.01, 2023.

[19] J. Tian, G. Gou, C. Liu, Y. Chen, G. Xiong and Z. Li, "DLchain: A Covert Channel Over Blockchain Based on Dynamic Labels," in *Proc. of International Conference on Information and Communications Security*, pp. 814-830, 2019.

[20] L. Zhang, Z. Zhang, W. Wang, R. Waqas, C. Zhao, S. Kim and H. Chen. "A Covert Communication Method Using Special Bitcoin Addresses Generated by Vanitygen," *CMC-Comput Mater Contin*, vol. 65, no. 1, pp. 597-616, 2020.

[21] A. Fionov, "Exploring Covert Channels in Bitcoin Transactions," in *Proc. of IEEE International Multi-Conference on Engineering, Computer and Information Sciences*, pp. 59-64, 2019.

[22] M. Xu, H. Wu, G. Feng, X. Zhang and F. Ding, "Broadcasting Steganography in the Blockchain," in *Proc. of International Workshop on Digital Watermarking*, pp. 256-267, 2019.

[23] D. Frkat, R. Annessi and T. Zseby, "ChainChannels: Private Botnet Communication Over Public Blockchains," in *Proc. of IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, pp. 1244-1252, 2018.

[24] N. Alsalami and B. Zhang, "Uncontrolled Randomness in Blockchains: Covert Bulletin Board for Illicit Activity," in *Proc. of IEEE/ACM 28th International Symposium on Quality of Service*, pp. 1-10, 2020.

[25] T. Tiemann, S. Berndt, T. Eisenbarth and M. Liskiewicz, "Act natural: Having a Private Chat on a Public Blockchain," *Cryptology ePrint Archive*, 2021.

[26] W. Wang and C. Su, "CCBRSN: A System with High Embedding Capacity for Covert Communication in Bitcoin," in *Proc. of International Conference on ICT Systems Security and Privacy Protection*, pp. 324-337, 2020.

[27] O. Torki, M. Ashouri-Talouki and M. Mahdavi, "Blockchain for Steganography: Advantages, New Algorithms and Open Challenges," *arXiv preprint*, arXiv: 2101. 03103, 2021.

[28] J. Qin, Y. Luo, X. Xiang and Y. Tan, "A Novel Network Covert Channel Model Based on Blockchain Transaction Parity," in *Proc. of International Conference on Artificial Intelligence and Security*, pp. 54-63, 2021.

[29] S. Zheng, C. Yin and B. Wu, "Keys as Secret Messages: Provably Secure and Efficiency-balanced Steganography on Blockchain," *Proc. of IEEE Intl Conf on Parallel and Distributed Processing with Applications, Big Data and Cloud Computing, Sustainable Computing and Communications, Social Computing and Networking*, PP. 1269-1278, 2021.

[30] S. Huang, W. Zhang, X. Yu, J. Wang, W. Song and B. Li, "Covert communication scheme based on Bitcoin transaction mechanism," *Security and Communication Networks*, pp. 1-17, 2021.

[31] H. Cao, H. Yin, F. Gao, Z. Zhang, B. Khoussainov, S. Xu and L. Zhu, "Chain-based Covert Data Embedding Schemes in Blockchain". *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14699-14707, 2022.

[32] M. Abouyoussef and M. Ismail, "Blockchain-Based Privacy-Preserving Networking Strategy for Dynamic Wireless Charging of EVs," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1203-1215, 2022.

[33] P. Lv, L. Xie, J. Xu, X. Wu and T. Li, "Misbehavior Detection in Vehicular Ad Hoc Networks Based on Privacy-Preserving Federated Learning and Blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3936-3948, 2022.

[34] M. S. Abegaz, H. N. Abishu, Y. H. Yacob, T. A. Ayall, A. Erbad and M. Guizani, "Blockchain-Based Resource Trading in Multi-UAV-Assisted Industrial IoT Networks: A Multi-Agent DRL Approach," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 166-181, 2023.

[35] W. Ren, Y. Sun, H. Luo and M. Guizani, "SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4406-4419, 2021.

[36] C. Lin, D. He, X. Huang, M. K. Khan and K. -K. R. Choo, "DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2440-2452, 2020.

[37] Y. Chen, X. Li, J. Zhang and H. Bi, "Multi-Party Payment Channel Network Based on Smart Contract," *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 4847-4857, 2022.

[38] Y. Liu, W. Yu, Z. Ai, G. Xu, L. Zhao and Z. Tian, "A Blockchain-empowered Federated Learning in Healthcare-based Cyber Physical Systems," *IEEE Transactions on Network Science and Engineering*, DOI: 10.1109/TNSE.2022.3168025, 2022.

[39] M. Bartoletti and L. Pompianu, "An Analysis of Bitcoin OP_RETURN Metadata," in *Proc. of International Conference on Financial Cryptography and Data Security*, pp. 218-230, 2017.

[40] "Bitcoin Core Version 0.12.0 Released," Feb. 2016. [Online]. Available: https://bitcoin.org/en/release/v0.12.0

[41] K. -H. Cho and S. -H. Lee, "Treating Interference as Noise Is Optimal for Covert Communication Over Interference Channels." *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 322-332, 2021.

[42] M. F. Sidiq, F. M. Wibowo, M. Wibowo, A. I. Basuki, I. Setiawan and D. Rosiyadi, "Secret and Trustable Communication Channel over Blockchain Public Ledger," in *Proc. of IEEE International Conference on Communication, Networks and Satellite*, pp. 371-376, 2021.

[43] M. Gimenez-Aguilar, J. M. De Fuentes, L. Gonz¢lez-Manzano and C. Camara, "Zephyrus: An Information Hiding Mechanism Leveraging Ethereum Data Fields," *IEEE Access*, vol. 9, pp. 118553-118570, 2021.

[44] V. Kanth, and B. Hale, "Blockchain-based Authenticated Stego-Channels: A Security Framework and Construction," in *Proc. of IEEE International Conference on Blockchain*, pp. 208-215, 2022.

[45] P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security". *Global Journal of Computer Science and Technology*, 2013.

[46] P. Kaushal, A. Bagga and R. Sobti, "Evolution of Bitcoin and Security Risk in Bitcoin Wallets," in *Proc. of IEEE International Conference on Computer, Communications and Electronics*, pp. 172-177, 2017.

[47] "Testnet," [Online]. Available: https://en.bitcoin.it/Testnet

[48] "BlockCypher," [Online]. Available: https://live.blockcypher.com/zai

Yang Tian received the B.S. degree form the College of Software, Nanchang University, Nanchang, China, in 2020. She is currently working toward the M.S. degree with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. Her current research interests include covert communication and blockchain.

Xin Liao (Senior Member, IEEE) received the B.E. and Ph.D. degrees in information security from Beijing University of Posts and Telecommunications in 2007 and 2012, respectively. He is currently a Professor and a Doctoral Supervisor with Hunan University, China. He worked as a Post-Doctoral Fellow with the Institute of Software, Chinese Academy of Sciences, and also a Research Associate with The University of Hong Kong. From 2016 to 2017, he was a Visiting Scholar with the University of Maryland, College Park, USA. His current research interests include multimedia forensics, covert communication, and watermarking. He is a member of Technical Committee (TC) on Multimedia Security and Forensics of Asia Pacific Signal and Information Processing Association, TC on Cyberspace Security of Chinese Institute of Electronics, TC on Computer Forensics of Chinese Institute of Electronics, and TC on Digital Forensics and Security of China Society of Image and Graphics. He is serving as an Associate Editor for the IEEE Signal Processing Magazine. He is a senior member of the IEEE.

Li Dong received the B.Eng. degree from Chongqing University, in 2012, the M.S. and Ph.D. degree, both from University of Macau, in 2014 and 2018, respectively. He is currently an Associate Professor with the Department of Computer Science, Faculty of Electrical Engineering and Computer Science, Ningbo University. His research interests include statistical image modeling and processing, multimedia security and forensic, and machine learning.

Yang Xu received the Ph.D. degree in Computer Science and Technology from Central South University, China, in 2019. From 2015 to 2017, he was a visiting scholar in the Department of Computer Science and Engineering at Texas A&M University, USA. He is currently an Associate Professor at the College of Computer Science and Electronic Engineering, Hunan University, China. His research interests include distributed computing, cloud computing, blockchain, artificial intelligence, and trustworthy/privacy computing. He has published over 50 articles in international journals and conferences, including IEEE TSC, TII, TCC, TETC, TCBB, TNSE etc. He was the awardee of the Best Paper Award of IEEE International Conference on Internet of People (IoP 2018). He is a member of Blockchain Technical Committee of China Computer Federation (CCF) and China Society for Industrial and Applied Mathematics (CSIAM), and a member of IEEE and ACM.

Hongbo Jiang is now a full professor in the College of Computer Science and Electronic Engineering, Hunan University. He was a professor at Huazhong University of Science and Technology. He received a Ph.D. from Case Western Reserve University in 2008. His research concerns computer networking, especially algorithms and protocols for wireless and mobile networks. He is serving as the editor for IEEE/ACM Transactions on Networking, the associate editor for IEEE Transactions on Mobile Computing, and the associate technical editor for IEEE Communications Magazine. He is a senior member of the IEEE.