

基于正常交易掩盖下的区块链隐蔽通信方案

姜鹏坤¹, 张问银¹, 王九如¹, 黄善云^{1,2}, 宋万水^{1,2}

(1. 临沂大学信息科学与工程学院, 山东 临沂 276000;
2. 山东师范大学信息科学与工程学院, 山东 济南 250358)

摘要: 随着计算机技术的发展, 现代网络攻防形势日益严峻, 秘密信息的安全传输问题亟待解决。隐蔽通信技术将秘密信息嵌入载体中通过隐蔽信道安全地传输, 但传统的隐蔽信道存在数据易受损、易被攻击、易被检测等问题, 无法满足更高的安全需求。区块链作为公共数据平台, 能够在大量交易的掩盖下嵌入秘密信息, 其具有的不易篡改、匿名性、去中心化等特点, 可以很好地解决传统隐蔽信道存在的问题, 实现安全的隐蔽通信, 但现有的区块链隐蔽通信方案存在通信效率较低、安全性较差等问题, 如何安全、高效地进行通信是区块链隐蔽通信的研究重点。提出一种基于正常交易掩盖下的区块链隐蔽通信方案, 利用哈希算法构建免传输密码表在不改变任何交易数据的情况下实现秘密信息的嵌入, 利用椭圆曲线特性可在海量的交易中快速筛选出带有隐藏信息的交易, 从而快速提取秘密信息。所提方案提高了隐蔽通信的安全性、效率, 可迁移性强, 理论分析显示, 攻击者无法区分普通交易和特殊交易, 所提方案具有极高的抗检测性和可扩展性; 比特币测试网的实验结果表明, 所提方案的效率高。

关键词: 区块链; 隐蔽通信; 信息隐藏; 比特币; 哈希算法

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022043

Blockchain covert communication scheme based on the cover of normal transactions

JIANG Pengkun¹, ZHANG Wenyin¹, WANG Jiuru¹, HUANG Shanyun^{1,2}, SONG Wanshui^{1,2}

1. School of Information Science and Engineering, Linyi University, Linyi 276000, China

2. School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China

Abstract: With the development of computer technology, the situation of modern network attack and defense is becoming increasingly severe, and the problem of secure transmission of secret information needs to be solved urgently. Covert communication technology embeds secret information into the carrier and transmits the information safely through the covert channel. However, the traditional covert channels face the challenges of data damaging,

收稿日期: 2022-05-27; 修回日期: 2022-07-07

通信作者: 张问银, zhangwenyin@lyu.edu.cn

基金项目: 山东省自然科学基金 (ZR2020MF058, ZR2020MF029)

Foundation Item: The Natural Science Foundation of Shandong Province (ZR2020MF058, ZR2020MF029)

引用格式: 姜鹏坤, 张问银, 王九如, 等. 基于正常交易掩盖下的区块链隐蔽通信方案[J]. 网络与信息安全学报, 2022, 8(4): 77-86.

Citation Format: JIANG P K, ZHANG W Y, WANG J R, et al. Blockchain covert communication scheme based on the cover of normal transactions[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 77-86.

attack, detection and so on, which cannot meet the higher security requirements. As a public data platform, blockchain can embed secret information under the cover of a large number of transactions. With its tamper proof, anonymity, decentralization and other characteristics, blockchain can well solve the problems of traditional covert channels and achieve secure covert communication. However, the existing blockchain covert communication schemes are limited by low communication efficiency and poor security. How to improve safety and efficiency of covert communication is a research focus of blockchain covert communication. Motivated by this issue, a blockchain covert communication scheme based on the cover of normal transactions was proposed. The hash algorithm was used to build a transmission-free password table to embed secret information without changing any transaction data. Using the elliptic curve feature, transactions with hidden information can be quickly screened out from a large number of transactions, to extract secret information quickly. This scheme improves the security and efficiency of covert communication and has strong portability. Theoretical analysis shows that attackers cannot distinguish between ordinary transactions and special transactions. This scheme has high anti-detection and scalability. Besides, the experimental results of the bitcoin test network show the high efficiency of this scheme.

Keywords: blockchain, covert communication, information hiding, bitcoin, hash algorithm

0 引言

随着计算机软硬件技术的发展,信息传输的安全性越来越受到人们的重视。最开始通常使用密码学技术对明文信息进行加密,以保证除了持有密钥的接收者外其他人无法获得通信内容,然而随着技术进步,很多加密算法变得容易被破解或被干扰,人们开始将视线转向信息隐藏。信息隐藏最早来源于 Simmons 提出的“囚徒”问题^[1],信息隐藏技术是将秘密信息以某种特定方式隐藏在载体数据中而不被其他人发现通信行为或秘密信息的技术。信息隐藏按 Petitcolas 等^[2]的分类方法可以分为隐写术、匿名、隐蔽信道和版权水印 4 类。隐写术是一种将秘密信息隐藏在载体中而不被人怀疑的技术,匿名主要是隐藏通信关系,使攻击者无法辨别通信双方。近年来,基于隐写术和匿名发展而来的隐蔽通信技术获得巨大的发展,隐蔽通信^[3]在 1973 年由 Lampson 提出,指匿名双方传递秘密消息,隐蔽通信模型包含发送者、接收者和隐蔽信道,发送者将秘密信息嵌入隐蔽信道中,接收者从中提取并还原秘密信息,隐蔽信道发挥着重要的作用。最开始学者研究的是本地存储隐蔽信道和时间隐蔽信道,利用本地计算机资源构建信道,之后随着网络技术发展,网络存储和时间隐蔽信道随之出现并逐渐成为研究重点^[4]。此信道通过网络数据包、包时延等构建隐蔽信道,但由于发送者和接收者是点对点通信,

监听者可以通过机器学习、统计分析等方法分析网络中的数据包^[5],秘密信息泄露风险很大,而且会暴露发送者和接收者之间的通信行为,进而通过 IP 等信息与现实身份进行关联,匿名性得不到可靠的保证;攻击者可以通过篡改数据包、添加噪声等方式进行干扰,传输安全性、可靠性得不到保证。

近几年,区块链技术作为比特币的底层支撑技术得到迅速发展,在金融、制造、物联网、医疗、供应链、公证等领域应用广泛^[6-7],已引起政府、企业和市场的高度关注^[8]。区块链技术是一种去中心化、可追溯、不易篡改的分布式共享数据库技术,它具有去中心化、匿名性、安全等特点。

1) 去中心化:区块链是由众多节点组成,通过点对点(P2P, peer to peer)网络进行消息传播,不存在中心化节点或机构。

2) 匿名性:用户通过自行生成地址参与区块链交易活动,用户可以生成多个地址,这些地址不与现实身份产生关联,具有较强的匿名性。

3) 安全:区块链通过非对称加密、签名、哈希等密码学技术来保证安全性,另外每个节点都保存区块链数据,采用的共识算法可以抵御恶意攻击,保证了数据的完整性。

区块链的这些特点天然适合用来构建隐蔽信道进行隐蔽通信^[9],匿名性保障了发送者和接收者的真实身份不会泄露,去中心化和安全使得区

区块链具有其他信道不具备的抗干扰性, 保障了信息的完整传输。

现有区块链隐蔽通信方案大多利用隐写术或交易中的字段实现嵌入, 这些方案容易被机器学习、统计学方法分析, 存在容量较低、安全性较差、效率低的问题, 本文提出一种基于正常交易掩盖下的区块链隐蔽通信方案, 利用哈希算法构建免传输的密码表实现地址到二进制位的匹配, 不向交易中嵌入任何信息。

1 相关工作

利用区块链进行隐蔽通信的研究有很多, 最常见也最简便的方法是利用比特币协议中的 OP_RETURN 字段^[10], OP_RETURN 字段允许用户写进任意内容, 它的容量为 83 byte。Tian 等^[11]将动态标签放入 OP_RETURN 字段, 通过动态标签快速识别特殊交易, 还根据现实情况中常见的 OP_RETURN 字段长度来设计标签, 但由于 OP_RETURN 字段对于任何人都是可见的, 只要 OP_RETURN 字段有内容, 监听者就可以怀疑其中有隐藏信息并进行收集分析, 这增加了隐蔽通信行为暴露和信息泄露的风险。将隐写术应用于区块链是更好的解决办法, Partala^[12]使用最低有效位 (LSB, least significant bit) 嵌入方法将秘密信息嵌入比特币地址中, 并提出一个名为“BLOCCE”的系统, 相比于其他方案, 该方案隐蔽性更高, 但它要求发送方创建的交易按序出现于区块链上, 这意味着一个区块至多有一笔携带秘密信息的交易, 而且一笔交易只能隐藏一比特信息, 容量大且受限。Gao 等^[13]设计了一种利用 Kleptography 将发送者私钥隐藏于签名中的方法, 接收方从签名中获得私钥解密交易中的加密信息, 由于签名的限制, 通信双方须在固定地址上通信, 存在暴露风险。余维等^[14]提出面向纯文本信息隐藏的区块链隐蔽通信模型, 以空格法嵌入秘密信息, 但该方案需要应用的区块链传输大量文本, 不具有普适性。司成祥等^[15]提出一种利用动态标签筛选交易的算法, 以便从海量交易中快速筛选特殊交易。文献^[16]提出派生链的思想, 进一步提高了筛选速度, 以共享密钥匹配 0、1 二进制位并生成接收地址和发送地址,

但所有交易构成一条交易链, 并且提高容量需要协商更多的密钥, 过多的链下通信会大大增加暴露的风险。

为了设计一种能快速识别特殊交易而且不会有明显的特征被对手捕捉、容量大的隐蔽通信方法, 本文提出了一种基于正常交易掩盖下的区块链隐蔽通信方案, 利用椭圆曲线特性快速筛选交易, 自行生成地址构建免协商密码表匹配二进制位, 安全高效。相比 LSB 方案^[12], 进一步提高了容量、安全性和效率; 相比于链方案^[16], 进一步提升了安全性和扩展性, 可以实现高效、安全的隐蔽通信。本文方案对比特币系统进行阐述和验证, 但它完全适用于其他所有使用椭圆曲线算法的区块链, 具有很高的可迁移性。

2 技术背景

2.1 比特币

比特币是最早出现的区块链, 也是最具代表性的区块链^[17], 它由中本聪提出并构建。比特币区块链是一个金融区块链, 它出现的原始目标是代替中心化的银行机构, 现在已发展为全球最大的公有链网络。参与者构造交易发布于网络上, 所有节点都可以打包交易构成区块, 并计算一个满足难度值的随机数, 最先计算出的节点成为新区块的拥有者, 并获得比特币奖励。目前比特币每天诞生 144 个区块, 一天可处理的交易量约为 500 000 笔, 活跃节点数超 10 000 个。

2.2 比特币交易和地址

比特币系统是基于交易的账本, 所有节点共同维护一个未被花费的交易输出的集合 (UTXO), 用户转账需要以集合中的输出作为输入, 并产生新的输出。用户之间的转账操作属于普通交易, 它的具体格式如表 1 所示, 主要包括系统版本号、交易哈希值、由输入组成的数组、由输出组成的数组、交易锁定时间 5 部分。输入由上一笔交易的 hash、在上一笔交易中的位置、包含发送者私钥和接收者公钥的解锁脚本组成, 输出由比特币数量、包含接收者公钥的锁定脚本组成。

表 1 交易格式
Table1 Transaction format

名称	描述
version	比特币系统版本号
hash	交易的哈希值
input	由输入组成的数组
output	由输出组成的数组
locktime	交易锁定时间; 0 表示立即执行, 不为 0 表示在指定高度或时间后执行

比特币地址是由公钥经过多步转换得到的, 过程如图 1 所示。首先对公钥进行加密哈希运算 (SHA256) 得到 256 位哈希值, 对哈希值进行加密运算 (RIPEMD160) 得到 160 位结果, 将版本号和 160 位结果进行双 SHA256 运算, 取前 4 个字节为校验码, 将版本号、RIPEMD160 结果和校验码拼接进行转码 (Base58) 得到地址。

2.3 哈希算法

SHA256 算法在比特币中应用广泛, 它是一种密码哈希函数, 是安全哈希算法 2 分出的一种算法, 由美国国家安全局研发, 它可以将任意长度的输入映射到 256 byte 的输出。它具有确定性、抗碰撞的特点, 对于确定的输入只会产生相同的结果, 对于不同的输入一定产生不同的结果, 它的安全性主要取决于抗碰撞能力, 即攻击者在现有条件下能否找到该函数的一对碰撞, 目前主要的攻击方法包括生日攻击和差

分攻击。哈希值越长抵御生日攻击能力越强, SHA256 使用 256 byte 哈希值, 生日攻击所需代价的数量级为 2^{128} , 差分攻击只可找到 SHA256 的一个部分碰撞, 其复杂度为 2^{66} , 但无法找到一个整体碰撞。由此可见, SHA256 对于生日攻击和差分攻击具有极高的抵御能力, 算法的安全性非常高。

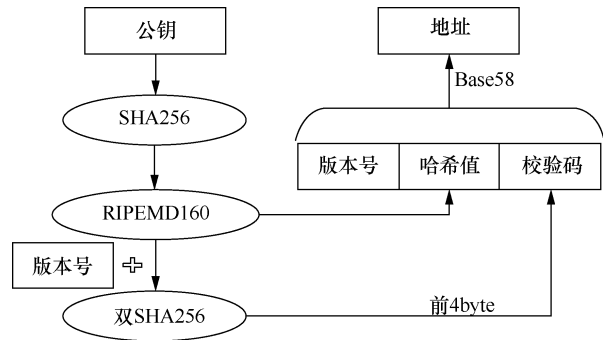


图 1 公钥转换到比特币地址
Figure 1 Convert public key to bitcoin address

3 区块链隐蔽通信模型与方案

3.1 区块链隐蔽通信模型

区块链环境下, 整个区块链数据都是对节点公开的, 因此在设计区块链隐蔽通信模型时除了必须要有发送者、接收者、秘密信息、预共享密钥和区块链信道, 还要假定存在一个全局的监听者, 它具有强大的算力, 可以监听全网数据并进行分析, 模型如图 2 所示。

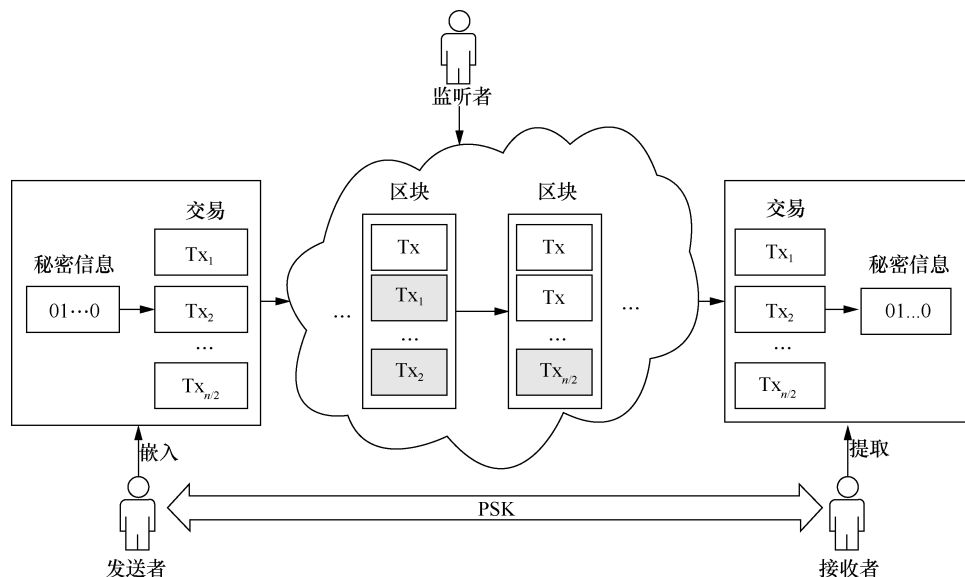


图 2 区块链隐蔽通信模型
Figure 2 Blockchain covert communication model

1) 预共享密钥 (PSK): 发送者和接收者在通信之前先协商好密钥是地址派生、提取函数的关键参数, 发送者和接收者都必须小心保存以免泄露。

2) 秘密信息: 双方要进行隐蔽传输的信息。

3) 发送者: 按照密钥生成算法构造发送地址公私钥对, 负责将秘密信息按预定规则编码, 构造交易发布于区块链上。

4) 接收者: 按筛选算法从区块链网络获取携带秘密信息的交易, 并还原出秘密信息。

5) 监听者: 假定的具备强大算力的节点, 可对区块链系统中网络流量进行监测分析, 检测异常行为。

6) 区块链信道: 以比特币、以太坊等公链为代表的区块链是良好的隐蔽信道。

3.2 区块链隐蔽通信方案

比特币系统具有活跃节点多、交易数据量大、数据包多的特点^[18], 将秘密信息隐藏在交易中是常见的一种隐藏方法, 发送者将编码后的信息嵌入交易中, 接收者从海量交易中筛选出隐藏信息的交易, 之后从中提取并还原秘密信息。如何从海量的交易中快速筛选出带有隐藏信息的交易是制约提取速度的关键, 直接根据确定地址筛选的速度无疑是较快的^[16]。在比特币中, 私钥是由用户随机生成的, 再经椭圆曲线算法产生公钥, 公钥经过变换得到地址, 发送者通过预共享密钥生成发送地址并以这些地址构造交易, 接收者通过发送者公钥和预共享密钥进行椭圆曲线乘法运算不断推演发送地址, 进而通过地址快速获得携带秘密信息的交易, 另外通过哈希运算生成符合要求的接收地址以构建免传输密码表, 大大减少链下密钥协商次数, 并且不改变任何地址的形式, 地址完全可用并实现嵌入。

在上述思路的基础上, 本文以比特币交易地址为载体, 在比特币网络上构建隐蔽信道, 发送者通过预共享密钥生成发送地址, 随机生成接收地址, 根据预共享密钥筛选得到免传输密码表, 将秘密信息拆分, 构造到接收地址的交易, 并将交易发送到区块链网络上, 接收者通过发送地址快速获取交易并提取秘密信息。本文方案包括嵌入和提取两个过程, 过程中所出现的符号如表2所示。

表2 符号及含义
Table2 Symbol and its meaning

符号	含义
*	椭圆曲线乘法
	拼接两个字符串
r	单笔交易嵌入的二进制位数
b_i	分割的秘密信息
n	秘密信息长度
m	秘密信息
a_i	接收地址
A	接收地址集合
tx_i	交易
Tx	交易集合
N	比特币私钥空间
G	比特币所用椭圆曲线基点
sk_i	私钥
pk_i	公钥
addr	地址
mod	模运算
PSK	预共享密钥
SHA256	哈希算法
Genkey	密钥生成算法
Extract	单次提取算法
getAddressInfo	区块链 API, 得到与地址相关的交易
publickeyToAddress	区块链 API, 将公钥转换为地址
privatekeyToAddress	区块链 API, 将私钥转换为地址
getPublicKey	区块链 API, 从交易输入提取公钥
makeTransaction	区块链 API, 构造交易并返回交易哈希

3.2.1 嵌入过程

嵌入过程如图3所示, 双方首先沟通 PSK、发送者地址 $addr_1$ 和单笔交易嵌入的位数 (以两位为例), 发送者将秘密信息 (或编码后) 转化为二进制并按嵌入位数进行分割。发送地址间存在派生关系, 该关系可由算法1所示的密钥生成算法^[16]推演, 发送者计算 $sk_1 \cdot PSK(\text{mod } N)$ 得到第二个发送地址的私钥 sk_2 , 再将私钥 sk_2 转化为公钥 pk_2 , 发送者重复此过程得到后续发送交易的账户; 接收地址由算法2的地址生成算法生成, 随机生成地址, 将 PSK 与地址拼接进行 SHA256 运算, 转换成二进制取最后两位分别与 “00” “01” “10” “11” 匹配, 匹配成功则放入 A , 重复此过程最终得到地址集

合 A ，它类似于密码表，由 2^r (r 为一笔交易嵌入的位数) 个地址构成。算法 3 给出嵌入过程的伪代码，发送者依据转化后的秘密信息构造发送地址到 A 中地址的交易实现秘密信息嵌入。

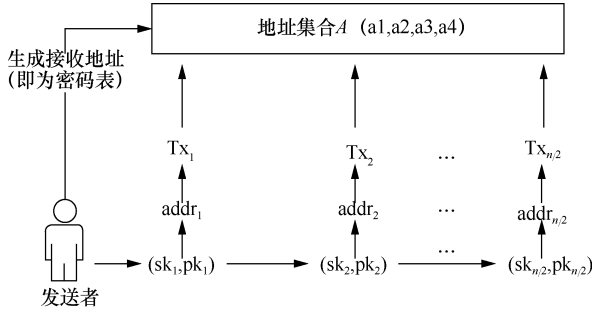


图 3 嵌入过程
Figure 3 Embedding process

算法 1 密钥生成算法

输入 sk_i, PSK

输出 pk_{i+1}, sk_{i+1}

1) $sk_{i+1} \leftarrow sk_i \cdot PSK \% N$

2) $pk_{i+1} \leftarrow sk_{i+1} \cdot G$

3) return(pk_{i+1}, sk_{i+1})

算法 2 地址生成算法

输入 PSK

输出 $A(a_1, a_2, a_3, a_4)$

1) while A not full

2) $S \leftarrow \text{secrets.randbits}(256)$ //随机生成私钥

3) $P \leftarrow G \cdot S$

4) $\text{addr} \leftarrow \text{publickeyToAddress}(P)$ //转换为地址

5) $h \leftarrow \text{SHA256}(PSK || y)$

6) $\text{last} \leftarrow \text{bin}(\text{int}(h[63:]))$ //取末尾转二进制

7) while $a_1 == 0$ & $\text{last}[4:] == '00'$

8) $a_1 = y$

9) while $a_2 == 0$ & $\text{last}[4:] == '01'$

10) $a_2 = y$

11) while $a_3 == 0$ & $\text{last}[4:] == '10'$

12) $a_3 = y$

13) while $a_4 == 0$ & $\text{last}[4:] == '00'$

14) $a_4 = y$

15) return A

算法 3 嵌入算法

输入 $(sk_1, pk_1), m(b_1, b_2, \dots, b_{n/2}), A$

输出 $Tx(tx_1, tx_2, \dots, tx_{n/2})$

1) for $i=1; i \leq n; i++$

2) $sk_{i+1}, pk_{i+1} \leftarrow \text{Genkey}(sk_i, PSK)$ //生成公私钥

3) $\text{addr}_i \leftarrow \text{publickeyToAddress}(pk_i)$ //通过 API 获取地址

4) if $b_i == '00'$

5) $tx_i \leftarrow \text{makeTransaction}(\text{from}=\text{addr}_i, \text{to}=a_1, \text{sk}=sk_i)$ //通过 API 构造交易

6) add tx_i to Tx

7) else if $b_i == '01'$

8) $tx_i \leftarrow \text{makeTransaction}(\text{from}=\text{addr}_i, \text{to}=a_2, \text{sk}=sk_i)$

9) add tx_i to Tx

10) else if $b_i == '10'$

11) $tx_i \leftarrow \text{makeTransaction}(\text{from}=\text{addr}_i, \text{to}=a_3, \text{sk}=sk_i)$

12) add tx_i to Tx

13) else

14) $tx_i \leftarrow \text{makeTransaction}(\text{from}=\text{addr}_i, \text{to}=a_4, \text{sk}=sk_i)$

15) add tx_i to Tx

16) end

17) return Tx

3.2.2 提取过程

提取过程如图 4 所示，本文方案的单次提取算法如算法 4 所示。接收者监听发送者地址发出的交易，并使用区块链 API 获取交易，将 PSK 和交易的接收地址拼接进行 SHA256 运算，将结果最后一位转换为二进制，取上步结果的后两位即可得到该笔交易所隐藏的二进制位。接收者进行发送地址推演只需要将前一笔交易的发送地址对应的公钥与 PSK 进行椭圆曲线乘法运算，即可得到下一笔交易的发送地址对应的公钥，再将公钥转化为地址；之后接收者重复单次提取过程，当某个地址一段时间监听不到交易时即视为传输终止，接收者将所有提取到的二进制位进行拼接，然后转码即可还原秘密信息。算法 5 给出了提取过程的伪代码。整个过程接收者知道的只有发送地址、接收地址和对应的公钥，这属于区块链上公开的数据，所有私钥均由发送者掌握，所以不

会对发送者的资金造成威胁。

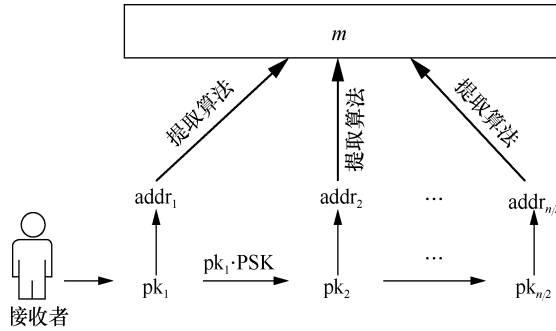


图4 提取过程
Figure 4 Extraction process

算法4 单次提取算法

输入 PSK, $addr_i$

输出 $addr, b$

- 1) $tx \leftarrow \text{getAddressInfo}(addr_i)$ //调用 API 获取交易
- 2) if $addr_i == tx.input$
- 3) $h \leftarrow \text{SHA256}(PSK || tx.output)$ //取哈希
- 4) $last \leftarrow \text{bin}(\text{int}(h[63:]))$
- 5) $b \leftarrow last[4:]$ //取最后两个二进制位
- 6) $pk_i \leftarrow \text{getPublicKey}(addr_i)$
- 7) $raddr = \text{publickeyToAddress}(pk_i \cdot PSK)$ //获取下个发送地址
- 8) return($raddr, b$)
- 9) return (Null, Null) //无下一笔交易, 传输结束

算法5 提取过程

输入 $addr_1, PSK$

输出 m

- 1) init m
- 2) $raddr \leftarrow addr_1$
- 3) while $raddr$ is not NULL //逐笔交易提取
- 4) $raddr, b \leftarrow \text{Extract}(PSK, raddr)$
- 5) add b to m
- 6) return m

4 实验和分析

4.1 实验

本文利用 Python 对整个方案流程进行了实现, 并在比特币测试网上完成测试, 本文所使用的实验设备包括一台便携式计算机, 具体配置为 AMD R7-4800H 2.9GHz 64 位 CPU、16 GB 内存、

1 TB 硬盘、Windows11 操作系统, 使用的区块链 API 为 Blockcypher, 表 3 和表 4 给出了一部分实验数据。

表3 实验数据 1
Table 3 Experiment data1

地址	值
$a_0(00)$	mssMAo1V4WU4e8aud15PYetXzWRKHgig2f
$a_1(01)$	mwZ3J21YRsGxaL6hLndJNpuGcQBqEZEUoj
$a_2(10)$	msGYoaaAMRUy5XFNGdjo5tsDhpah7Zn4U1
$a_3(11)$	n4FfKv4ytC2kEWZgVRh6DQZBcYPrA7Mymv

表4 实验数据 2
Table 4 Experiment data 2

参数	值
PSK	93199655975891431655472996197823976432812287130971275966920133320673197145071
b	011110010110010101110011
pk_1	(14445570168545214914766700056560968305626963274466755636452446931895023971256, 36925227269403861818765288719624287631440161515177762680431976377130310550544)
$addr_1$	mhMbHvFpmaDWNbpq7pXAa5NHmWfktwnfEs
pk_i	(53304206540227669758761895931701099952298339724174380173755615599843126977732, 99534090803506671914426953071409577604391826006150187216348291308197580373978)
$addr_i$	mtvJy4BL43ondxt75WwUzb7cPLZWjdmBYN
tx_1	8d34906fc9340d10ff7b1ededeb36db9d7963c3b141292287ce3852ca45d6494
tx_2	7f2572c8aaf53fa4872e870445dd8dffe9cbe4cd54e272d571f545496f748617

比特币测试网是比特币的一条备用链, 测试网的代币不同于真正比特币, 它没有任何实际价值, 仅用于在测试网进行开发实验使用, 这避免了昂贵的通信成本消耗。另外测试网的计算复杂度远低于比特币网络, 交易可以得到更快的确认。本实验将“yes”作为嵌入信息, 它的二进制表示为“011110010110010101110011”, 共有 24 位二进制数, 需要构造 12 笔交易。从比特币私钥空间选择预共享密钥, 然后将预共享密钥输入地址生成算法得到接收地址 $A = \{a_1, a_2, a_3, a_4\}$, 分别对应 00、01、10、11 的映射, 发送者私钥 s_1 、公钥 p_1 , 对应的地址为 $addr_1$, 派生需要的发送地址, 并根据秘密信息 m 构造到接收地址集合 A 的交易, 接收者再从 $addr_1$ 开始获取交易列表提取秘密信息。

(1) 嵌入过程

首先对地址生成算法进行测试, 分别生成 3 次匹配 1 bit、2 bit、4 bit 信息的地址, 具体实验数据如表 5 所示。可以看到匹配比特数每增加 2 倍, 所用时间约增加 5 倍, 但在匹配比特数未超过 8 bit 时, 所用时间不超过 1 s; 密钥生成过程类似于比特币生成公私钥对的过程, 所用时间可以忽略不计。另外就是调用区块链 API 的响应时间, 表 6 给出以 2 bit 将 “yes” 嵌入的耗时, 可以看到单次嵌入耗时在 1 s 左右浮动, 而生成匹

配 2 bit 秘密信息的地址只需要 0.02 s 左右, 整个嵌入过程主要取决于调用区块链 API 的时间, 将 “yes” 嵌入 12 笔交易的总共用时约为 28.068 s。

表 5 地址生成耗时
Table 5 Address generation time

单位: s				
匹配比特数	第 1 次	第 2 次	第 3 次	平均值
1 bit	0.004 999	0.005 000	0.007 001	0.005 667
2 bit	0.020 435	0.035 006	0.019 002	0.024 814
4 bit	0.117 438	0.138 514	0.095 620	0.117 190

表 6 2 bit 秘密信息嵌入耗时
Table 6 2 bit secret information embedding time

嵌入信息	二进制表示	交易数	最低嵌入时间/s	最高嵌入时间/s	平均嵌入时间/s
y	1111001	4	1.451 340	2.915 667	2.161 076
e	1100101	4	1.564 582	3.271 380	2.249 448
s	1110011	4	1.602 346	3.867 852	2.357 694

(2) 提取过程

提取秘密信息需要的时间同样取决于调用区块链 API 的响应时间, 所需要的时间与秘密信息的长度成正比, 24 bit 秘密信息提取总共耗时约为 30.537 s。

4.2 性能分析

4.2.1 抗检测性

隐蔽通信的安全性主要指通信的抗检测性, 指的是载体信息在嵌入秘密信息前后的统计特征上呈现的一致性, 使攻击者难以检测秘密信息。该一致性可以用相对熵来表示, 设系统的相对熵为 $D(P||Q)$, P 表示嵌入秘密信息之后载体的概率分布, Q 表示未嵌入秘密信息载体的概率分布。相对熵 $D(P||Q)$ 越小, P 和 Q 在统计特征上所呈现的一致性就越高。相对熵公式如下:

$$D(P||Q) = \sum_i p_i \log \frac{p_i}{q_i} \quad (1)$$

若存在一个 ε , 使 $D(P||Q) \leq \varepsilon$, 则该隐蔽通信系统是抗检测的, ε 越小, 抗检测能力越强^[14]。本文方案所用载体为接收地址, 嵌入前后不发生任何更改, 每个字符的概率分布不发生改变, 因此相对熵 $D(P||Q)=0$, 对任意 ε , $D(P||Q) \leq \varepsilon$, 具有极高的抗检测性。

对于通过图方法对交易行为进行数据分析的攻击者, 本文方案的隐蔽通信活动完全类似于社

区组织、集资等活动, 具有极高的抗检测性; 另外, 相比链方案^[16]扩大容量需要链下协商更多的密钥, 本文方案扩大容量不需要进行链下协商, 大大降低了暴露风险。

4.2.2 复杂度

(1) 嵌入过程

地址生成算法和密钥生成算法的时间复杂度分别为 C_{Agen} 、 C_{Kgen} , 调用 `publickey ToAddress` 和 `makeTransaction` 两个区块链 API 的时间复杂度分别用 C_{P2A} 和 C_{MTx} 表示, 那么将 N bit 秘密信息嵌入到比特币区块链中的时间复杂度约为 $O(N/2(C_{Agen}+C_{Kgen}+C_{P2A}+C_{MTx}))$, 取决于 API 调用所用的时间。

(2) 提取过程

调用区块链 API `getAddressInfo` 的时间复杂度用 C_{GA} 表示, C_{GP} 表示从输入获取公钥的 `getPublicKey` 的时间复杂度, 那么单次提取算法的复杂度为 $O(C_{GA}+C_{GP}+C_{P2A})$, 完成提取 N bit 秘密信息的时间复杂度约为 $O(N/2(C_{GA}+C_{GP}+C_{P2A}))$, 同样取决于 API 调用所用的时间。

本文对不同方案发送相同比特秘密信息的嵌入和提取用时进行了对比, 如表 7 所示。文献[12]所提方案的发送地址固定, 只需调用一次区块链 API 即可获得所有交易, 因此它的提取用时短,

但相比于它的嵌入用时，提取过程带来的优势可以忽略。

表7 不同方案的嵌入和提取用时对比
Table 7 Embedding and extraction time comparison of different schemes

方案	嵌入用时	提取用时
文献[12]方案	≥ 4 h	约 2.38 s
文献[16]方案	约 61.57 s	约 62.98 s
本文方案	约 28.07 s	约 30.54 s

4.2.3 可扩展性

本文方案演示的是两位嵌入，即一笔交易嵌入 2 bit 秘密信息，用到 4 个接收地址。相应地可以嵌入 4 bit、8 bit 秘密信息或者字母等，可以获得相应倍数效率的提高，同时使用的接收地址会增多，但本文方案不需要链下协商接收地址，接收者可在提取的过程中获得接收地址集合，这避免了链下协商带来的暴露风险，具有良好的扩展性。当嵌入的位数不是很多时，生成接收地址耗费的时间相对于传输效率的提升可以忽略，发送者与接收者双方可以自行协商使用的嵌入位数。

5 结束语

本文提出一种基于正常交易掩盖下的区块链隐蔽通信方案，与常见的隐写术不同，本文利用哈希算法构建免传输密码表匹配二进制位，不对交易的格式进行任何改动，并在比特币测试网上完成实验仿真。实验表明，本文方案具有极高的安全性、较高的效率和可扩展性，并可应用于各种区块链系统，一台普通便携式计算机就可以通过本文方案进行隐蔽通信。然而本文方案存在一定的局限性，即生成匹配高比特数的地址耗时较高，之后将进一步研究高效地址生成算法，提高效率；并继续研究在其他区块链中构造合适的隐蔽信道的方法。

参考文献：

- [1] SIMMONS G J. The prisoners' problem and the subliminal channel[M]//Advances in Cryptology. Boston, MA: Springer, 1984: 51-67.
- [2] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Information

hiding-a survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062-1078.

- [3] LAMPSON B W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613-615.
- [4] 王翀, 王秀利, 吕荫润, 等. 隐蔽信道新型分类方法与威胁限制策略[J]. 软件学报, 2020, 31(1): 228-245.
WANG C, WANG X L, LYU Y R, et al. Categorization of covert channels and its application in threat restriction techniques[J]. Journal of Software, 2020, 31(1): 228-245.
- [5] SATTOLO T A V. Real-time detection of storage covert channels[D]. Ottawa: Carleton University, 2021.
- [6] ALI O, JARADAT A, KULAKLI A, et al. A comparative study: blockchain technology utilization benefits, challenges and functionalities[J]. IEEE Access, 2021, 9: 12730-12749.
- [7] SANKA A I, IRFAN M, HUANG I, et al. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research[J]. Computer Communications, 2021, 169: 179-201.
- [8] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [9] 李彦峰, 丁丽萍, 吴敬征, 等. 区块链环境下的新型网络隐蔽信道模型研究[J]. 通信学报, 2019, 40(5): 67-78.
LI Y F, DING L P, WU J Z, et al. Research on a new network covert channel model in blockchain environment[J]. Journal on Communications, 2019, 40(5): 67-78.
- [10] BARTOLETTI M, POMPIANU L. An analysis of Bitcoin OP_RETURN metadata[C]//International Conference on Financial Cryptography and Data Security. 2017: 218-230.
- [11] TIAN J, GOU G, LIU C, et al. DLchain: A covert channel over blockchain based on dynamic labels[C]//International Conference on Information and Communications Security. 2019: 814-830.
- [12] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18.
- [13] GAO F, ZHU L H, GAI K K, et al. Achieving a covert channel over an open blockchain network[J]. IEEE Network, 2020, 34(2): 6-13.
- [14] 余维, 霍丽娟, 田钊, 等. 面向纯文本信息隐藏的区块链隐蔽通信模型[J]. 计算机科学, 2022, 49(1): 345-352.
SHE W, HUO L J, TIAN Z, et al. Blockchain covert communication model for plain text information hiding[J]. Computer Science, 2022, 49(1): 345-352.
- [15] 司成祥, 高峰, 祝烈煌, 等. 一种支持动态标签的区块链数据隐蔽传输机制[J]. 西安电子科技大学学报, 2020, 47(5): 94-102.
SI C X, GAO F, ZHU L H, et al. Covert data transmission mechanism based on dynamic label in blockchain[J]. Journal of Xidian University, 2020, 47(5): 94-102.
- [16] CAO H, YIN H, GAO F, et al. Chain-based covert data embedding schemes in blockchain[J]. IEEE Internet of Things Journal, 2020, PP(99):1-1.
- [17] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[R].

2008.

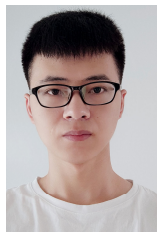
- [18] 张涛, 伍前红, 唐宗勋. 基于比特币区块链的隐蔽信息传输研究[J]. 网络与信息安全学报, 2021, 7(1): 84-92.

ZHANG T, WU Q H, TANG Z X. Bitcoin blockchain based information convert transmission[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 84-92.



王九如(1983-), 男, 山东临沂人, 博士, 临沂大学副教授, 主要研究方向为区块链技术、物联网安全。

[作者简介]



姜鹏坤(1997-), 男, 山东烟台人, 临沂大学硕士生, 主要研究方向为区块链技术、信息隐藏。



黄善云(1997-), 男, 山东济宁人, 山东师范大学硕士生, 主要研究方向为区块链技术、隐蔽通信。



张问银(1972-), 男, 山东临沂人, 博士, 临沂大学教授、博士生导师, 主要研究方向为区块链技术、信息隐藏、图像处理。



宋万水(1997-), 男, 山东济南人, 山东师范大学硕士生, 主要研究方向为区块链技术、数据分析。