基于比特币区块链的隐蔽信息传输研究

张涛，伍前红，唐宗勋
（北京航空航天大学网络空间安全学院，北京 100191）

摘　要：为满足机密信息高效、安全、隐蔽、稳定传输的需求，分析了比特币的交易数据结构及潜在隐蔽信道的位置和容量，提出了一种基于比特币区块链的存储隐蔽信道数据传输模型，可以在不破坏原有交易格式、不增加交易内容特殊性，克服现有网络环境下的隐蔽信道特性缺陷等弊端，保证数据不被检测，同时保护数据隐蔽传输的发送方和接收方。基于区块链的数据传输将成为数据隐蔽传输新的发展方向，对于推动特种应用安全传输技术的发展具有非常重要的意义。

关键词：信息隐藏；区块链；比特币；隐蔽信道；隐蔽信息传输
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096−109x.2021009

Bitcoin blockchain based information convert transmission

ZHANG Tao, WU Qianhong, TANG Zongxun
School of Cyber Science and Technology, Beihang University, Beijing 100191, China

Abstract: To meet efficient, safe, covert and stable transmission of confidential information, the transaction data structures, location and capacity of potential convert channels were analyzed. Then a formal security model of covert transmission in the bitcoin blockchain environment was proposed, which would not break the transaction structures, add special transaction content, can overcome shortcomings of traditional convert channels and protect the anonymity of both sender and receiver. The proposed security model opens a promising avenue of covert transmission, which is of great significance to promote the secure transmission technologies for the national special applications.

Keywords: information hiding, blockchain, bitcoin, convert channel, information covert transmission

收稿日期：2020−01−14；**修回日期：**2020−07−02
通信作者：唐宗勋，tangzongxun@hotmail.com
基金项目：国家重点研发计划（2020YFB10056，2019QY(Y)0602, 2017YFB1400700, 2017YFB0802500）；国家自然科学基金（61932011, 61972019, 61772538, 61532021, 91646203, 61672083）
Foundation Items: The National Key R&D Program of China (2020YFB10056, 2019QY(Y)0602, 2017YFB1400700, 2017YFB0802500), The Natural Science Foundation of China (61932011, 61972019, 61772538, 61532021, 91646203, 61672083)

论文引用格式：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.

1　引言

随着计算机和网络技术的发展，信息的安全传输越来越受到人们的重视。信息以明文形式传输时，很容易遭到敌手拦截和篡改，无法保证信息传输过程中的机密性和完整性。如何安全地进行信息传输成为研究人员面临的一大难题。加密和信息隐藏方法是确保信息传输过程中的机密性和完整性常用的方法。使用加密进行信息传输时，传输的是密文，只有拥有密钥的通信双方才能提取正确的明文信息，这一过程保证了信息的机密性和完整性。传统的隐蔽信息传输方法将隐蔽信息嵌入音频、图片、视频中，利用网络多媒体传输机制实现隐蔽信息传递的目的。但现有信息隐藏方法和网络隐蔽信道存在带宽低、易被检测、易被针对性地阻断等问题，限制了隐蔽信息传输的使用。如何通过公开非专用（秘密）信道安全地传输信息而不被敌手检测到成为困扰科学界的一大难题。

2008 年，Nakamoto[1]提出了比特币区块链的概念。比特币区块链具有去中心化、信息不可篡改、信息广泛传播、信息匿名特性和频繁交易特性，区块链的上述特点为密码技术与信息隐藏技术的融合提供了新的思路与解决手段。

2　相关工作

2.1　信息隐藏

信息隐藏方法可以根据信息隐藏载体的不同分为 3 类：基于文本的信息隐藏、基于音频的信息隐藏、基于图像和视频的信息隐藏。

基于文本的信息隐藏可以分为文本格式信息隐藏和文本内容信息隐藏。基于文本格式的信息隐藏技术主要利用格式在文档内容组织结构和排版等方面的格式信息来进行信息隐藏。Maxemchuk 等提出了一系列的文档标记技术，包括行移编码[2]、字移编码[3]和字符特征编码[4]等方法。Adnan 等[5]利用扩频技术、BCH 差错控制编码的方式调整字间距来嵌入信息。Takizawa 等[6]通过在词素内部插入换行符改变文本起始或结束位置的方式来嵌入信息。基于文本内容的方法主要利用自然语言处理通过修改文字内容来隐藏信息。Wayner 等[7]提出了 Mimic 函数并构建了信息隐藏的理论模型。Topkara 等[8]通过引入错误拼写的词组替换的方式进行数据隐藏；Muhammad 等[9]构建了由两个绝对同义词组成的同义词词库用于数据隐藏。

音频信息隐藏的主要方法是根据待隐藏信息，对人耳听觉不敏感的音频参数进行修改，以达到信息嵌入的目的。最早的音频信息隐藏技术研究是 Bender 等[10]在 1996 年提出的最不重要位置替换法（LSB 算法）。LSB 算法利用程序修改文件中每个字节的最低有效位，通过对最低有效位的编码来隐藏信息。受到 LSB 算法的启发，Mansour 等[11]通过将音频信号在时域上沿时间轴拉伸或压缩的方式来嵌入信息。Boney 等[12]利用人类听觉系统的频域遮掩效应对伪随机序列进行若干级滤波，保证了良好的透明性。Wu 等[13]将信息嵌入数值较大的离散傅里叶变换幅度系数之上。陆陌林等[14]利用量化方法在小波变换域的近似分量和细节分量上分别嵌入信息，实现了信息的高效嵌入和完整性检测。

图像在空间域隐藏算法的起源同样可以追溯到 Bender 等[10]提出的 LSB 算法。刘红翼等[15]提出了高于依赖 LSB 的数字图像信息隐藏算法，根据嵌入数据的大小和载体图像的大小，利用随机函数确定嵌入位置，提高了信息嵌入量。Luo 等[16]提出将 LSB 推广到更大的适用范围的算法，该算法根据嵌入消息的大小以及相邻像素点间的差异能够自适应地选择嵌入区域。Thodi 等[17]首次提出了预测误差扩展算法，挖掘自然图形的相关性，实现更优的嵌入。图像、声音、视频等数字载体由于具有一定的数据冗余度、隐藏容量大等特点[18]，是信息隐藏的主要载体。视频的每一帧都是一副独立的图像，因此基于视频的信息隐藏技术可以将基于图像的隐藏技术直接应用于视频信息隐藏。花广路等[19]在现有视频信息隐藏算法的基础上，结合 H.264/AVC 视频低频域系数的特征，提出了一种基于 H.264/AVC 低频域视频信息隐藏算法。

2.2　隐蔽信道和隐蔽信息传输

1984 年，Simmons[20]利用签名技术提出了通过公开非安全信道秘密地传输信息而不被侦测到

的思路，即将签名密钥分成 2 个不同集合，通过使用不同集合中的密钥签名信息，任何不知道密钥集合的人都无法从签名中获取额外信息，而知道密钥集合信息的人则能够获取签名对应密钥集合的信息，该方法被称为隐蔽信道传输（subliminal channel communication）。随后，Simmons[21]提出在已知密钥前提下，利用数据签名构造隐蔽信道方法。1993 年，Simmons[22]又提出在无须知晓私钥的前提下，利用美国数字签名标准（DSA）来构造增强隐蔽信道的方法。1997 年，Young 等[23]在上述隐蔽信道的研究基础上，提出了一种新型的密码系统信息隐蔽传输方法。在传统密码学算法中嵌入后门，正常的使用者无法根据算法输出分辨是否存在后门，但算法设计者能够通过隐蔽信道获取系统运行的随机数状态，进而得出使用者的系统密钥，达到隐蔽获取敏感信息的目的。在此思想的影响下，出现了针对 DSA、ElGamal 加密、ElGamal 签名以及 Schnorr 签字等的隐蔽信道利用方法[24]。2014 年，Bellare 等[25]探索了此类方法在单钥加密系统中的应用。项世军等[26]提出了一种利用同态公钥加密的信息隐藏方法，可以将信息隐藏在图片中，实现了对加密图像的有效管理和安全保护。

2.3 比特币和区块链

区块链是一种开放的分布式存储系统，具有点对点通信、去中心化、信息不可篡改、信息洪泛传播、匿名性等特性[27-28]。任何人都可以随时加入区块链，成为区块链网络中的节点，网络中的任何节点可以读取、保存和验证区块链账本上的所有数据。比特币[1,29]是一种典型的区块链系统，除了区块链网络的特性外，还有活跃用户量大、交易数据量大、交易数据包多等特点。密码学是区块链技术的基础，在比特币区块链中，比特币地址映射是基于 SHA-256 算法的，签名所用的公钥和私钥是用椭圆曲线签名算法（ECDSA，elliptic curve digital signature algorithm）生成的。

2.4 基于区块链的隐蔽信息传输

比特币区块链技术展现出的去中心化、信息不可篡改、信息广泛传播、信息匿名特性和频繁交易特性符合隐蔽数据传输的需求与应用环境，但目前国内外在基于区块链的隐蔽信息传输方面的研究处于起步阶段。2018 年，Partala[30]提出了一种基于区块链的数据嵌入方法 BLOCCE，可以安全地嵌入隐蔽信息到区块链中。2019 年，宋上[31]对 BLOCCE 系统进行了改进，提高了系统的通信效率和通信过程的可延续性。李彦峰等[32]提出了一种区块链环境下的新型网络隐蔽信道模型，并证明了该模型的抗干扰性、抗篡改性、多线路通信性、接收方匿名性和线路无关性。

3 基于比特币区块链的信息隐蔽传输方法

传统隐蔽信息传输方法大多是定向发送、显式接收的，也就是说信息传输是点对点的，这种隐蔽传输方式易被敌手监听，敌手可以通过监听网络、分析网络流量的方式检测出隐蔽信道。敌手一旦检测出隐蔽信道，参与隐蔽传输的双方身份就容易暴露。而且网络延迟等其他因素可能会导致接收方无法准确地提取出隐蔽信道传输的信息。区块链具有活跃用户量大、交易数据包多的特点，因此具有构建隐蔽信道的天然载体的特点。密码技术与信息隐藏技术的融合提供了新的思路，利用区块链进行信息隐藏和传输具有以下特点：隐蔽信道难以被监听和检测；难以从海量数据交易中提取隐藏的信息，保护数据隐蔽传输的接收方。

如图 1 所示，隐蔽信息传输模型是一个四元组，包括发送方、接收方、共享资源（隐蔽信道）、编码机制。为了保证信息传输的机密性，信息的发送方需要利用编码机制对传输的明文信息进行编码和加密，接收方在接收到信息后需要对接收的信息进行解码和解密以获取明文信息。根据隐蔽信息载体的不同，隐蔽信道可以分为时间隐蔽信道和存储隐蔽信道。存储隐蔽信道以共享资源的内容为隐蔽信息的载体，本文提出隐蔽信息传输模型是基于存储隐蔽信道的，目标是不破坏原有交易格式、不降低交易内容特殊性、确保数据不被检测。

3.1 基于比特币区块链系统的隐蔽信息传输模型

根据 bitinfocharts[33]的数据，截至 2019 年 12 月 30 日，比特币活跃用户地址约 68.8 万个，日均交

易量约 30 万笔。比特币活跃用户量大、交易数据量大、交易数据包多，可以嵌入隐蔽数据的方式多，因此以比特币为代表的区块链是构建隐蔽信道的良好载体。基于比特币区块链的隐蔽信息传输模型如图 2 所示。

图 1　隐蔽信息传输模型
Figure 1　Information convert transmission model

3.2　比特币隐蔽信道分析

比特币具有交易数据量大、数据包多的特点，因此将要传输的信息隐藏在比特币交易数据包的字段中，不会引起敌手的注意。比特币区块链数据结构固定、冗余空间有限的特性与数据隐藏需要独立的冗余存储空间存在冲突。为了保证信息的隐蔽传输，需要对数据进行封装并将其嵌入比特币区块链交易信息上，即“数据隐藏嵌入”。一方面，出于数据保密性需求考虑，嵌入的数据不能暴露本身所涵盖的语义信息，因此需要对嵌入信息进行随机化处理；另一方面，出于信息隐蔽性考虑，嵌入的数据必须满足区块链本身的算法及脚本标准要求，必须保证所嵌入的信息能够被正常纳入比特币区块链，不因数据格式不合法而被抛弃或发现。因此，需要分析比特币交易的数据格式，以确定数据格式中的哪些字段可以用来隐藏信息以及比特币区块链中的存储隐蔽信道。

3.2.1　比特币交易数据结构

一个完整的比特币交易主要包含 4 部分内容：版本号、交易输入、交易输出以及锁定时间。比特币交易数据格式如表 1 所示，其中版本是交易数据结构的版本号，明确一笔交易遵循的规则，一般情况下，版本号是固定不变的。因为交易的输入和输出可能是多个，因此交易数据中由交易输入数量和交易输出数量两个字段来描述交易输入和输出的个数。锁定时间（lock_time）指该交易可被添加到区块链中的最早时间，一般情况下，lock_time 的值为 0；当 0<lock_time<500 000 000 时，lock_time 表示区块高度；当 500 000 000<lock_time 时，lock_time 表示一个 unix 时间戳。

（1）交易输入

一个交易的输入包含 5 部分内容，分别是前一个交易的输出哈希值、前一个交易的索引、解锁脚本长度、解锁脚本和序列号。比特币交易输入数据格式如表 2 所示，其中，解锁脚本的长度是未知的，需要使用一个可变整形来表示解锁脚本的长度；序列号大小为 4 byte，暂未使用。

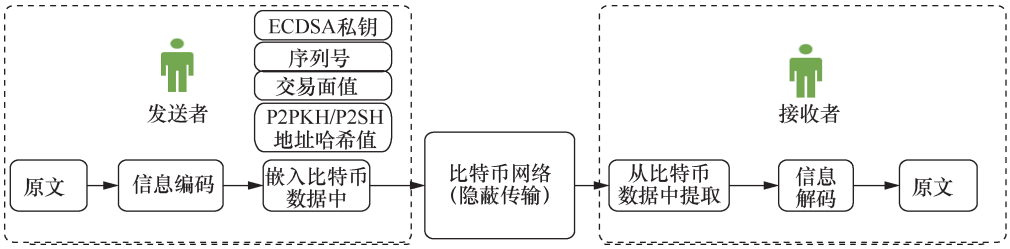


图 2　基于比特币区块链的隐蔽信息传输模型
Figure 2　Bitcoin blockchain based information convert transmission model

表 1　比特币交易数据格式
Table 1　Data structure of Bitcoin transaction format

字段名	字段名（英文）	大小	描述
版本	Version	4 byte	交易数据结构的版本号
交易输入	tx_in	大于 41 byte	输入交易的数组，每个输入大于等于 41 byte
交易输入数量	tx_in count	1~9 byte	输入交易的数量
输出	tx_out	大于 9 byte	输出地址的数组，每个输入大于等于 9 byte
交易输出数量	tx_out count	大于 1 byte	交易输出地址的数量
锁定时间	lock_time	4 byte	一个 unix 时间戳或区块高度

出于安全原因，比特币对脚本类型进行了限制。从 Bitcoin Core 0.9 版本开始，规定了标准公钥脚本类型有 5 种，分别是 P2PKH（Pay To Public Key Hash）、P2SH（Pay To Script Hash）、Multisig、PubKey 和 Null Data[34]。各种类型的公钥脚本格式如表 3 所示，具体如下。

① P2PKH。P2PKH 是最常用的公钥脚本，可以将发送交易到一个或多个比特币地址。签名脚本包含 ECDSA 签名和 ECDSA 公钥，将签名脚本和公钥脚本拼接起来后的形式如下。

<Sig> <PubKey> OP_DUP OP_HASH160 <PubkeyHash> OP_EQUALVERIFY OP_ CHECK-SIG P2SH

P2SH 能够将交易发送至一个脚本的哈希值。具体流程与 P2PKH 类似。

② PubKey。 PubKey 是一个 P2PKH 公钥脚本的简化版本，但是安全性不及 P2PKH，大部分新交易已经不再适用这种脚本。

③ Multisig。在 Multisig 脚本中有两个参数，分别是 m 和 n。其中，n 是公钥的总数，m 是该比特币能够被消费所需要的签名数目。

④ Null Data。 Bitcoin Core 0.9.x 到 0.10.0 版本会默认设置中转和打包 null data 交易类型，支持单次提交数据多达 40 byte。在 Bitcoin Core 0.11.x 版本中，将默认值增加到 80 byte，其他规则保持不变。在 Bitcoin Core 0.12.0 版本中，在不超过总字节限制的情况下，可以支持最多 83 byte。

（2）交易输出

交易输出指出了钱的去向，拥有交易输出值并用私钥解密后，就可以作为其他交易的输入，进行消费。一个交易的输出由交易值、锁定脚本长度和锁定脚本数据 3 部分组成，如表 4 所示。其中，交易值大小为 8 byte，存储了交易的金额；锁定脚本长度为 1~9 的可变整数，该值表示后面的锁定脚本长度。锁定脚本数据定义了支付输出所需条件的脚本，为可变长度。

3.2.2　比特币隐蔽信道分析

从比特币交易数据格式来看，版本、锁定时间交易输入的数量和交易输出的数量无法用于隐藏信息。在比特币交易输入数据格式中，由于交

表 2　比特币交易输入数据格式

Table 2　Data structure of input of Bitcoin transaction format

字段名	字段名（英文）	大小	描述
前一个交易的输出哈希值	Hash	32 byte	关联输出所在的交易 Hash 地址
前一个交易的索引	Index	4 byte	关联输出在其交易输出集合中的索引
解锁脚本长度	scriptLen	1~9 byte（可变整数）	解锁脚本长度
解锁脚本	script bytes	变长	解锁脚本数据
序列号	sequence	4 byte	序列号，暂未使用

表 3　公钥脚本格式

Table 3　Pubkey script format

公钥脚本	公钥脚本格式	签名脚本格式
P2PKH	OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	<sig> <pubkey>
P2SH	OP_HASH160 <Hash160(redeemScript)> OP_EQUAL	<sig> [sig] [sig···] <redeemScript>
Multisig	<m> <A pubkey> [B pubkey] [C pubkey...] <n> OP_CHECKMULTISIG	OP_0 <A sig> [B sig] [C sig···]
Null Data	OP_RETURN <0 to 40 bytes of data>	—

表 4　比特币交易输出数据格式

Table 4　Data structure of Bitcoin output transaction format

字段名	字段名（英文）	大小	描述
交易值	value	8 byte	单位是聪，用聪表示比特币的值
锁定脚本长度	scriptLen	1~9 byte（可变整数）	用 byte 表示后面的锁定脚本长度
锁定脚本数据	script bytes	可变长度	定义了支付输出所需条件的脚本

易的输入值必须要有前一个交易的输出哈希值和前一个交易的索引，因此这两个字段无法修改，也无法用于隐藏数据。如果一个比特币交易能够满足锁定时间小于当前区块链的长度，那么序列号的值可以是任意值。所以，在交易输入数据的序列号字段可以用于隐藏数据，大小为 4 byte（32 bit）。

在比特币交易输入和输出数据格式中，脚本部分都可以用来隐藏数据。在 P2PKH 和 P2SH 脚本中，所有操作符的格式都是固定的，能够被修改的部分只有 20 byte 的哈希值。理论上，在这 20 byte 的哈希值中最多可以嵌入 160 bit 的数据，但这样，其对应的公私钥未知，该交易输出中的比特币将成为无法花费的比特币。因此，如果在这一哈希值嵌入数据，应考虑使用哈希值的部分碰撞。嵌入哈希值中的字节数与生成的 ECDSA 公私钥对数以及与存储账户所需存储空间的对应关系如表 5 所示。

表 5　P2PKH 和 P2SH 脚本中嵌入哈希值
Table 5　Hash embedded into P2PKH and P2SH script

嵌入数据的字节数（比特数）	生成的 ECDSA 公私钥对数	账号存储所需存储空间
1（8 bit）	256	约 20 kB
2（16 bit）	65 536	约 6 MB
3（24 bit）	16 777 216	约 1.5 GB

如果在哈希值集中嵌入 2 byte（16 bit）的数据，可以生成 65 536 个 ECDSA 公钥私钥对，并令这 65 535 个公钥的哈希值的前两个字节的数值分别是 0~65 535。考虑到账号的回收，这 65 536 个账号必须全部被存储在本地的数据库中，占用的硬盘空间约为 6 MB。如果要嵌入 3 byte 数据，那么所需的存储空间约为 1.5GB。综合嵌入的数据和本次保存账户所需存储空间，建议在 P2PKH 和 P2SH 脚本中嵌入数据 2 byte 数据。

在 Nulldata 脚本中，根据比特币系统版本的不同，用户可以嵌入不少于 40 byte（320 bit）的数据。由于比特币交易允许找零，交易的数值的零头中也可以用来隐藏数据。比特币密码算法中使用的椭圆曲线私钥长度为 32 byte，可以通过共享 ECDSA 私钥来嵌入数据。首先对命令进行编码，加入混淆后生成私钥，用此私钥生成公钥和比特币地址；然后使用这个比特币地址创建两个交易，对这两个交易使用相同的随机密钥进行签名（r, s）。接收者需要监听该比特币地址的交易，在发现两个交易公钥中的 r 相同时，保存交易内容，从中计算出私钥，并按预先设置的解码规则解出数据。

比特币隐蔽信道的位置和容量如表 6 所示。在这些隐蔽信道中，共享的 ECDSA 私钥、P2PKH/P2SH 地址的哈希部分碰撞和 Nulldata 脚本这 3 种隐蔽信道的容量较高。在一次交易中，利用共享的 ECDSA 私钥、P2PKH/P2SH 地址的哈希部分碰撞和 Nulldata 脚本这些隐蔽信道可以嵌入不少于 20 byte 的数据，且不会引起比特币区块链上的信息异常，但这几种方法需要大量的本地计算。序列号和交易面值这两种隐蔽信道容量相对来说较小，在一次交易中仅能够嵌入 2~4 byte 的数据，传递的信息量有限。利用 ECDSA 共享私钥的方法可以以任何交易的形式存在，但这种方法存在泄露私钥的风险。在实际应用中建议使用 P2PKH/P2SH 地址的哈希部分碰撞和 Nulldata 脚本这两种隐蔽信道。

3.3　隐蔽消息编码

由于比特币区块链交易数据是公开的，所有

表 6　比特币隐蔽信道位置和容量
Table 6　Position and capacity of convert channel in Bitcoin

隐蔽信道	隐蔽信道位置	容量
共享 ECDSA 私钥	—	32 byte/签名
序列号	—	4 byte/交易输入
交易面值	—	2 byte/交易输出
解锁脚本	P2PKH/P2SH 地址的哈希部分碰撞	20 byte/交易输出
	Nulldata 脚本	不少于 40 byte/交易

参与的节点都可以拥有交易数据的全部副本。为了保证信息传输的机密性，在向比特币交易中嵌入数据前，需要对要传输的信息进行加密，以实现在公开和透明的场景下隐藏数据传输的行为。由于接收方接收到加密的信息后，还需要解密，为了确保信息的高效传输和简化密钥管理，应使用技术成熟的对称密钥加密算法。AES[35]是美国的分组加密标准，分组长度 128 bit，密钥可选 128 bit、192 bit 或 256 bit。出于安全性的考虑，建议采用分组长度为 128 bit、密钥长度为 256 bit 的 AES 算法对明文消息进行编码。

4 区块链隐蔽信息传输的挑战

4.1 传输的效率问题

（1）嵌入隐蔽信息的交易识别效率低。由于区块链交易数据量大，隐蔽信息传输接收方如何从海量交易数据中识别出符合条件的交易数据，并从中提取出传输的隐蔽数据是基于区块链的隐蔽信息传输面临的一大挑战。传统的解决方法是在传输的数据中设置特殊标签。在交易数据中设置特殊标签可以提高识别包含传输信息的交易数据的效率，但在交易数据中设置特殊标签必然会占用隐蔽信道容量，降低隐蔽信息传输的效率，而且包含特殊标签特征的交易相比正常交易很容易被区分，攻击者可以利用特别标签特征来识别这些特殊的交易数据。

（2）交易数据确认耗时长。区块链是一种分布式账本技术，交易需要网络中的节点确认才可以加入链上，但交易数据确认耗时较长。以比特币为例，根据 bitinfocharts[33]的数据，2019 年 12 月 30 日比特币交易确认平均时间为 8.276 min。整个隐蔽信息传输过程耗时比较长，这也是制约区块链隐蔽信息传输效率的一个难题。

（3）交易产生成本高。区块链中采取共识机制来解决分布式网络中的同步问题，常用的共识机制工作量证明有（PoW，proof of work）和权益证明（PoS，proof of stake）。比特币区块链使用 PoW 共识机制，而 PoW 机制需要消耗大量的计算和电力资源，因此，每产生一个待确认的交易会消耗大量的资源。相比 PoW，PoS 有了很大的改进，但本质上仍然是哈希运算竞争获取记账权。因此，从目前情况看，基于区块链的隐蔽信息传输需要大量的计算资源，交易产生的成本高。

4.2 传输的安全性问题

（1）传输的匿名性问题。区块链虽然是匿名的，但最新研究表明通过交易关联分析、地址关联分析等方式仍然可以进行交易信息溯源。加之区块链交易数据的公开性和开放性，使区块链信息传输的匿名性成为基于区块链的隐蔽信息传输安全性的一大挑战。

（2）传输的隐蔽性问题。由于区块链交易数据是开放的，所有节点都可以拥有所有数据的完整副本。在一对一的隐蔽信息传输中，隐蔽信息传输的隐蔽性可能会被隐蔽传输的匿名性、特殊交易数据的特殊性和特殊交易数据的数量等因素影响。在多对多数据传输中，无法指定接收方的账号，因此隐蔽信息传输需要在保证接收方可识别的情况下尽可能与普通交易的一致性，降低特殊性，以防交易数据被攻击者识别和窃听。

（3）传输的安全性问题。区块链具有不可篡改性，经过共识机制存储到区块链上的数据很难被修改，因此通过区块链传输数据可以保证数据的抗篡改性，进而保证数据传输过程中的安全性。同时，区块链具有开放透明的特性，所有参与的节点都可以拥有整个区块链账本的副本。因此，区块链上传输的密文信息是向所用参与用户公开的，要确保传输数据的安全性，必须确保密钥的安全分发和数据传输的隐蔽性。

5 结束语

传统的隐蔽信息传输方法将隐蔽信息嵌入音频、图片、视频中，利用网络多媒体传输机制实现隐蔽信息传递的目的。但传统信息隐藏方法存在带宽、被监控等问题，限制了隐蔽信息传输的使用。比特币活跃用户量大、交易数据量大、交易数据包多，可以嵌入隐蔽数据的方式多，因此以比特币为代表的区块链是构建隐蔽信道的天然载体。本文分析了比特币交易数据格式，分析了其中潜在的隐蔽信道，提出了一种基于比特币区块链的存储隐蔽信道数据传输模型，可以不破坏原有交易格式、不降低交易内容特殊性，克服现有网络环境下隐蔽信道特性缺陷等弊端，保证传

输数据不被检测，同时保护数据隐蔽传输的发送方和接收方。最后，本文分析了基于区块链的隐蔽信息传输存在的传输效率和传输安全性等挑战。

除了比特币区块链的存储隐蔽信道外，还可以利用区块链交易数据包的传输时间间隔作为载体，模拟合法数据流的统计特性，将信息隐蔽编码在数据包的时间特性中。下一步将对比特币区块链的时间隐蔽信道进行研究，并对比特币隐蔽信道传输的效率、成本、接收方和发送方身份的隐蔽性进行研究。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R].

[2] MAXEMCHUK, NICHOLAS F. Electronic document distribution[J]. AT&T Technical Journal, 1994, 73(5): 73-80.

[3] LOW S H, MAXEMCHUK N F, BRASSIL J T, et al. Document marking and identification using both line and word shifting[C]// Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM '95). 1995.

[4] BRASSIL J, LOW S, MAXEMCHUK N, et al. Electronic marking and identification techniques to discourage document copying[C]//13th Proceedings IEEE Networking for Global Communications INFOCOM '94. 1994.

[5] ALATTAR A M, ALATTAR O M. Watermarking electronic text documents containing justified paragraphs and irregular line spacing[J]. Proceedings of SPIE - The International Society for Optical Engineering, 2004, 5306: 685-695.

[6] TAKIZAWA O, MATSUMOTO T, NAKAGAWA H, et al. 3-8 information hiding on digital docu-ments by adjustment of new-line positions[J]. Journal of the National Institute of Information and Communications Technology , 2005, 52(1/2).

[7] WAYNER P. Mimic functions[J]. Cryptologia, 1992, 16(3): 193-214.

[8] TOPKARA M, TOPKARA U, ATALLAH M J. Information hiding through errors: a confusing approach[C]//Security, Steganography, and Watermarking of Multimedia Contents IX. International Society for Optics and Photonics, 2007, 6505: 65050V.

[9] MUHAMMAD H Z, RAHMAN S M S A A, SHAKIL A. Synonym based malay linguistic text steganography[C]//2009 Innovative Technologies in Intelligent Systems and Industrial Applications. 2009: 423-427.

[10] BENDER W, GRUHL D, MORIMOTO N, et al. Techniques for data hiding[J]. IBM Systems Journal, 1996, 35(3.4): 313-336.

[11] MANSOUR M F, TEWFIK A H. Audio watermarking by time-scale modification[C]//2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. 2001: 1353-1356.

[12] BONEY L, TEWFIK A H, HAMDY K N. Digital watermarks for audio signals[C]//Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems. IEEE, 1996: 473-480.

[13] WU C P, SU P C, KUO C C J. Robust and efficient digital audio watermarking using audio content analysis[C]//Security and Watermarking of Multimedia Contents II. International Society for Optics and Photonics. 2000: 382-392.

[14] 陆佰林, 朱艳琴. 基于小波变换的双水印算法[J]. 微电子学与计算机, 2007(8):37-40.
LU B L, ZHU Y Q. An Algorithm of dual watermarking based on wavelet transform[J]. Microelectronics & Computer, 2007(8): 37-40.

[15] 刘红翼, 王继军, 韦月琼, 等. 一种基于 LSB 的数字图像信息隐藏算法[J]. 计算机科学, 2008, 35(1): 100-102.
LIU H Y, WANG J J, WEI Y Q, et al. Department of computer science[J]. Computer Science, 2008, 35(1): 100-102.

[16] LUO W, HUANG F, HUANG J. Edge adaptive image steganography based on LSB matching revisited[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 201-214.

[17] THODI D M, RODRÍGUEZ J J. Expansion embedding techniques for reversible watermarking[J]. IEEE Transactions on Image Processing, 2007, 16(3): 721-730.

[18] 钮心忻, 杨义先, 吴志军. 信息隐藏理论与关键技术研究[J]. 电信科学, 2004, 20(12):28-30.
NIU X X , YANG Y X, WU Z J. Study on the basic theory and technology of information hiding[J]. Telecommunications Science, 2004, 20(12) :28-30.

[19] 花广路, 李芝棠, 冯兵. 基于 H.264/AVC 视频的低频隐写算法[J]. 通信学报, 2013, 34(Z2): 47-50.
HUA G L, LI Z T, FENG B. Low frequency steganography algorithm for H.264/AVC[J]. Journal on Communications, 2013, 34(Z2): 47-50.

[20] SIMMONS G J. The prisones' problem and the subliminal channel[C]//Advances in Cryptology Proc Crypto, 1984.

[21] SIMMONS G J. The subliminal channel and digital signatures[C]// Proc of the EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques. 2007.

[22] SIMMONS G J. The subliminal channels of the US digital signature algorithm (DSA)[C]//Proceedings of the 3rd Symposium on: State and Progress of Research in Cryptography. 1993: 35-54.

[23] YOUNG A, YUNG M. Kleptography: using cryptography against cryptography[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 1997: 62-74.

[24] YOUNG A, YUNG M. The prevalence of kleptographic attacks on discrete-log based cryptosystems[C]//Annual International Cryptology Conference. 1997: 264-276.

[25] BELLARE M, PATERSON K G, ROGAWAY P. Security of symmetric encryption against mass surveillance[C]//Annual Cryptology Conference. 2014: 1-19.

[26] 项世军, 罗欣荣 . 同态公钥加密系统的图像可逆信息隐藏算法[J]. 软件学报, 2016, 27(6): 1592-1601.
XIANG S J, LUO X R. Reversible data hiding in encrypted image based on homomorphic public key cryptosystem[J]. Journal of Software, 2016, 27(6): 1592-1601.

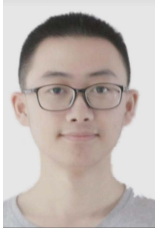
[27] 李佩丽, 徐海霞, 马添军, 等. 可更改区块链技术研究[J]. 密码

学报, 2018, 5(5): 501–509.
LI P L, XU H X, MA T J, et al. Research on fault-correcting blockchain technology[J]. Journal of Cryptologic Research, 2018, 5(5): 501–509.
[28] 秦波, 陈李昌豪, 伍前红, 等. 比特币与法定数字货币[J]. 密码学报, 2017, 4(2): 176–186.
QIN B, CHEN L C H, WU Q H, et al. Bitcoin and digital fiat currency[J]. Journal of Cryptologic Research, 2017, 4(2): 176–186.
[29] YAGA D, MELL P, ROBY N, et al. Blockchain technology overview[J]. arXiv preprint arXiv:1906.11078, 2019.
[30] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18.
[31] 宋上. 基于区块链的隐蔽通信系统 BLOCCE 改进研究[D]. 兰州: 兰州大学, 2019.
SONG S. Research on the improvement of block chain based covert communication system BLOCCE [D]. Lanzhou: Lanzhou University. 2019.
[32] 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.
[33] Bitcoin (BTC) price stats and information[EB].
[34] Bitcoin developer guide[EB].
[35] RIJMEN V, DAEMEN J. Advanced encryption standard[C]// Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology. 2001: 19-22.

[作者简介]

张涛（1991− ），男，甘肃平凉人，北京航空航天大学博士生，主要研究方向为区块链、网络信息安全。

伍前红（1973− ），男，四川资阳人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学、数据安全、密码货币、区块链、云计算安全、智能安全。



唐宗勋（1996− ），男，安徽池州人，北京航空航天大学硕士生，主要研究方向为区块链、网络信息安全。