一种基于区块链的防篡改隐蔽通信系统

谢小龙[1]，黄华军[1,2]，曾帆[1]，

[1](中南林业科技大学 计算机与信息工程学院，长沙 410004)

[2](湖南财政经济学院 信息技术与管理学院，长沙 410205)

摘要：信息在通信过程，存在会被第三方截获，在无法破译信息的情况下，遭第三方篡改，破坏信息安全传递。基于此，结合区块链的不可篡改性，提出一种防篡改隐蔽通信系统。利用区块链 OP_RETURN 脚本附带隐藏的外带数据，经挖矿确认后加入到区块链中，确保信息无法被篡改。系统实现了传递秘密信息的完整性和可用性，保障信息的安全传递。

关键词：隐蔽通信；区块链；外带数据；防篡改

A Tamper-resistant Steganography System based on Block-chain

Xie Xiao-long[1], HUANG Hua-jun[1,2], Zeng Fan[1]

[1](College of computer and information engineering, Central South University of Forestry and Technology, Changsha, 410004, China)

2(School of information Technology and Management, Hunan University of Finance and Economics, Changsha, 410205, China)

Abstract: In the covert communication, the existence of secret information will be intercepted by a third party. In the case of unable to decipher the information, the third party will forcibly tamper with the covert information, destroy the integrity of the covert information, and affect the transmission of covert information. Based on this, combined with the tamper-resistant nature of block-chains, a tamper-resistant steganography system is proposed. Using the block-chain OP_RETURN script with hidden external data, after mining confirmation, it is added to the block chain to ensure that the hidden information cannot be tampered with. The system realizes the integrity and availability of secret information transmission, which is an excellent and reliable method for secret communication.

Key words: Steganography; block-chain; outside data; tamper-resistant

中图法分类号: TP309 **文献标识号**:A **文章编号**:

1 引言

信息的安全传递是信息战及保密通信的核心任务[1]。加密与信息隐藏是保障信息安全传递的两种技术。加密使信息看不懂，而信息隐藏使信息通信看不见，是更高层次的安全通信方式。隐蔽通信作为信息隐藏的分支之一，是指在图像、视频、音频、文本、网页等载体中嵌入一些秘密信息，让第三方在主观上难以察觉秘密信息的存在，对国家安全与信息安全具有重要意义[2]-[4]。

随着个人计算机的普及和互联网上多媒体数据泛滥为隐蔽通信提供了便利条件，使得隐蔽通信得到迅速发展。传统的隐蔽通信都是对载体按照嵌入规则修改以嵌入待隐藏的秘密信

收稿日期:2018-7-28

基金项目:国家自然科学基金资助项目（No.61802444, 61772561,No.61304208）;湖南省普通高校教学改革研究项目（湘教通[2015]291 号）.

作者简介:谢小龙(1995 年生-),男,硕士生，研究方向为区块链,信息隐藏; 黄华军(1978 年生-),男,博士,教授,研究方向为网络安全,金融信息系统安全;曾帆(1994 年生-),男,硕士生，研究方向为区块链,信息隐藏;周千元(1992 年生-),男,硕士生，研究方向为个性化推荐.

通信作者:黄华军,hhj0906@163.com

息，从而不可避免的修改了载体文件。按照载体类型可以分为：图像、视频信息隐藏、音频、文本、软件、数据库和 XML、网页信息隐藏等[5]。但近年来的发展速度有所放缓。究其原因如下：1）隐写分析地发展威胁着信息隐藏的广泛使用；2）主流信息隐藏技术采用修改载体的模式，难有突破性成果；3）信息隐藏理论研究滞后，不能为技术发展提供有力支撑。

为了改变信息隐藏必须修改载体的模式，2014 年 5 月，有关专家提出了“无载体信息隐藏”这一全新的概念。“无载体”并不是指不需要载体，而是与传统的信息隐藏相比，它强调的是不需要其他载体，而是直接以秘密信息为驱动来“生成/获取”含密载体[6]。

隐蔽通信的形态在新的网络环境下将不断发展变化，网络上的各种信息媒介均可作为秘密信息的伪装载体。安全通信不仅限于要隐藏正在发送消息通信这一事实，还要让发送者和接收者对于监听者来说不可检测到，因此也需具备匿名性和隐私性。区块链在去中心化的网络环境作为秘密信息载体有着天然优势：区块链的不可篡改性使得恶意篡改攻击无法实现，同时区块链的匿名交易保障了通信双方的匿名性与隐私性。

针对隐蔽信息在通信过程，存在会被第三方截获，在无法破译信息的情况下，遭第三方强行篡改原本信息，导致信息破坏影响信息准确传递的问题。为此，结合区块链技术的不可篡改性、单链式结构、去信任化、去中心化式等特性，在点对点交易方式的交易过程中附带隐藏的外带数据，经确认后加入到区块中，确保了信息准确传达，这对隐蔽通信而言是一种绝佳的可靠的安全可行的方法。最后对该技术进行了实验实现和分析以及未来的展望。

本文的主要贡献有 3 个方面：1)结合区块链技术的不可篡改等特性，首次提出基于区块链技术实现隐蔽通信；2) 在现有区块链数据中，找到进行了隐蔽通信的交易记录并对这些数据进行了分析，论证了基于区块链的隐蔽通信的可能性；3) 实现了基于区块链的隐蔽通信系统，并进行了实验模拟，进行性能分析。

2 区块链技术原理

区块链首次出现在中本聪发表的《比特币：一种点对点式的电子现金系统》[7]。区块链实现了无需信任基础就能安全可靠的完成点对点交易，这得益于它的去中心化，匿名性，不可篡改性等优势。

为了达到区块链数据的不可篡改性，区块链技术采用 P2P 网络让网络每个节点地位均等，节点生成的交易信息通过广播的方式传达相近的节点，当全网 51%的节点接收通过后，交易信息会被加入到区块中，全网节点进行同步，该区块就会被添加到链上。除了创世区块外，每个区块都包含了前一个区块的哈希散列值且每个区块头都加盖了时间戳确保唯一性，区块通过这种方式联系在一起形成了一条单链，如图 1 所示[8]-[12]。

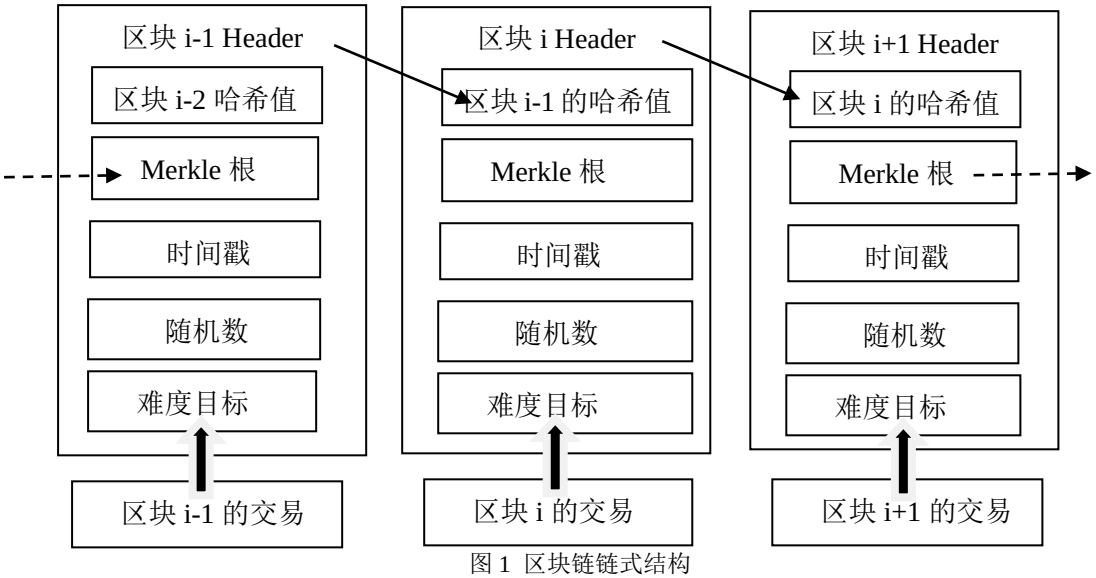

图 1 区块链链式结构

3 基于区块链的隐蔽通信系统

3.1 OP_Return 脚本

基于区块链的隐蔽通信系统一般是通过一对一交易方式，发送方创建一笔正常的代币转账，附带上想要传达的信息，这有点像转账信息备注，交易验证通过后，接收方除了收到代币外，还会有一串外带数据。隐蔽通信实现过程是利用了比特币 OP_Return 脚本。

要想在交易时添加外带数据，比特币脚本起到重要作用。脚本是比特币重要的技术，比特币脚本存在的意义是让每笔交易合法化，这个合法化不是人工审核而是有脚本自动执行校验的。脚本分为锁定脚本和解锁脚本。锁定脚本和交易（UTXO）是对应的，一个 UTXO 中包含一个锁定脚本。当这个 UTXO 要被使用时,比如 Alice 转账给 Bob 需要引用这个 UTXO, 这就产生了一笔交易。这笔交易只有被验证了才可能在比特币的网络中广播，广播被大多数节点验证通后就可以被矿工加入区块链，验证的时候需要的就是解锁脚本。从上述流程可以看出: 锁定脚本和 UTXO 关联，而解锁脚本和某笔交易关联。锁定脚本被叫做 scriptPubKey, 解锁脚本被叫做 ScriptSig。脚本就是一堆命令加参数，如图 2 所示。

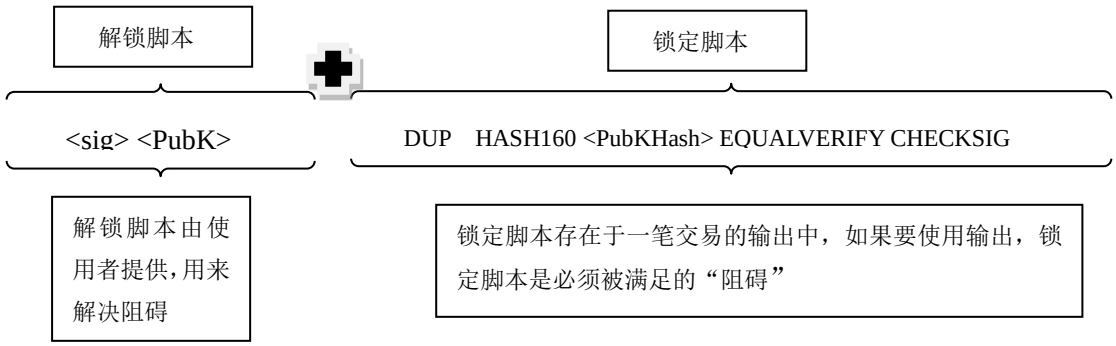

图 2 比特币脚本

从 0.9 版开始的比特币核心客户端上，通过 OP_Return 操作允许开发者在交易输出上增加 40 字节的非交易数据（有扩大到 80 字节，之后又缩小到 40 字节）。OP_Return 脚本的样式：OP_RETURN <data>。它有如下 4 个特点：

1） OP_Return 不是用于支付的解锁脚本，不能使用其输出中锁定的资金，也不会被记录到 UTXO 集中，避免了内存占用，引起 UTXO 内存膨胀问题，但还是会记录在区块链上，导致区块链的规模增加，消耗更大的磁盘空间；

2）OP_Retuen 常为一个金额为 0 的比特币输出，因为任何与该输出相对应的比特币都会消失。

3） 如果以 OP_Return 作为一笔交易的输入，则该笔交易是无效的。

4） 一笔标准交易有一个 OP_Return 输出，但是 OP_Return 可以跟其他类型的输出交易进行组合。

比特币系统允许开发者加入外带数据，这给隐蔽通信提供了方便。RETURN PUSHDATA(35) [some garbage]，这个脚本从“OP_RETURN”开始，被称为空数据输出，用于用户在区块链中存储任意数据。由于这些输出数据不同于代币转账，是不能进行花费的，所以 scripts 脚本不能对他进行有效评估。但其实这样的数据输出大多是伴随着一个正常转账输出出现的。这有点像转账信息备注,用户在做这笔 0.0494 个 BTC 转账的时候，就可以将转账的一些信息写入这笔交易“ Alice send to Bob”. 但是这样的信息是无法进行消费的,所以会永远处于 Unspent 状态,并且出现 Unable to decode output address (无法解析输出地址)这样的情况。当“Alice send to Bob”变成了“OKT□o□□┤R8o□$□U□□;S/E□EeL.□□5L”的时候，隐蔽通信的目的就达到了。

3.2 系统模型

隐蔽通信的模型可以用图3来描述。秘密信息*M*与密钥*K*相结合加密后，通过OP_Return脚本隐藏到比特币交易I中，形成含有隐蔽信息的比特币交易*I'*,*I'*与*I*应非常相似，不会引起他人的怀疑。每个节点维护一个交易池，用来存放临时的未经确认的交易，一般情况下，挖矿节点从交易池中选择一系列交易构成区块，其中会包含*I'* ，等待矿工进行验证确认。当挖矿节点基于自身算力找到一个具有足够难度的工作量证明且所有交易都通过验证后，该区块会添加到链上，然后查询交易记录后，利用密钥K应能正确提取出秘密信息。

具体过程：

Step1：输入秘密信息 M，利用 OP_Return 脚本将 M 添加进交易中；

Step2：创建一笔新的比特币交易；

Step3：该笔交易经签名后广播到整个 P2P 网络，暂时存放在交易池中，等待验证确认；

Step4：节点从交易池中挑选一系列未确认的交易（包含该交易）进行验证构成区块，节点矿工找到一个具有足够难度的工作量证明后，全网广播；

Step5：当这一系列交易都是有效的且交易输入未动用（UTXO），新区块产生，交易完成，交易记录为保存在区块链上；

Step6：查看交易记录，获取秘密信息。

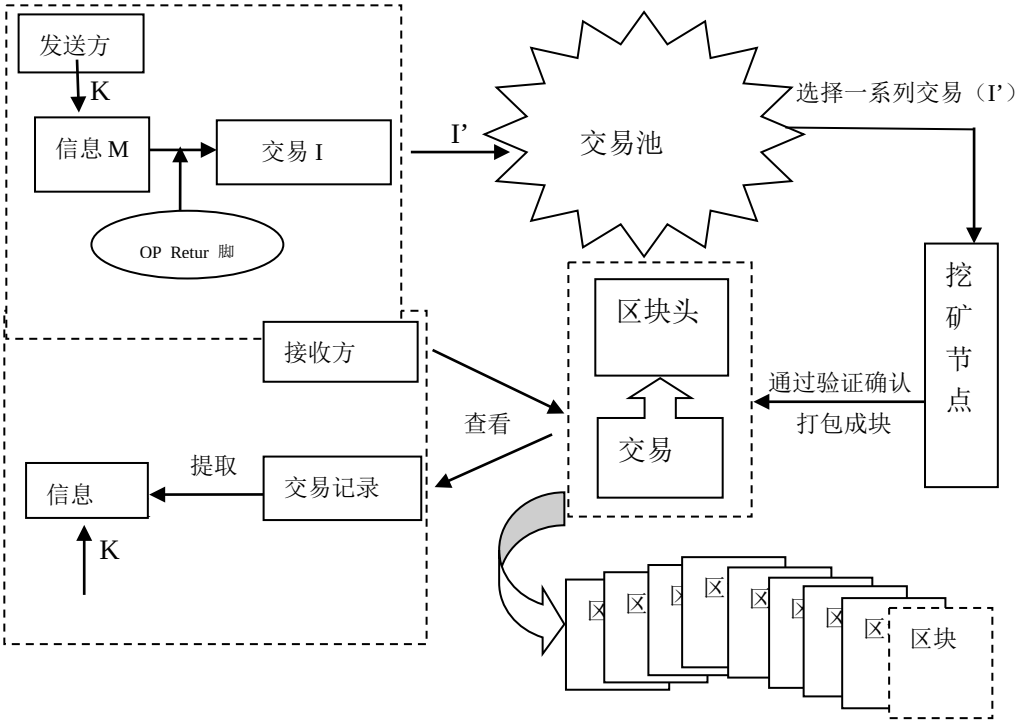

图 3 隐蔽通信系统模型

基于区块链的隐蔽通信系统模块如图 4 所示，主要分为四个模块：

1) 挖矿模块：计算工作量证明 PoW，新增一笔 coinbase 交易，将产生新的区块添加到链中。挖矿模块是让交易能够保证确认通过添加进区块链数据的关键，通过产生的新区块加入链上，我们才能从查看整个区块链上查看所有交易记录和所要传达的信息；

2) 传输模块：隐蔽通信需要以比特币交易形式将进行处理过后的信息附带，所以先创建一笔交易，发送方为 A 地址，接收方为 B 地址，隐蔽信息为；

3) 查看模块：返回最新的整个区块链数据；

4) 提取模块：查看交易记录后，提取通过交易传输过来的秘密信息。

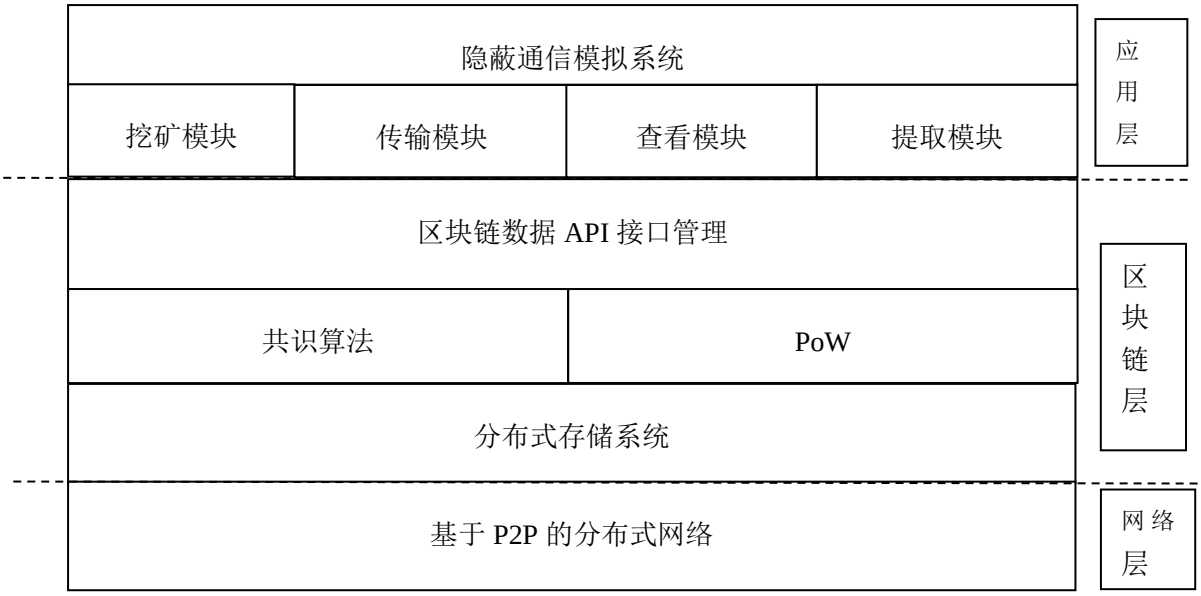

图 4. 基于区块链的隐蔽通信系统模块

通过 API 接口连接到区块链系统设计隐蔽通信传输流程，传输模块负责交易创建，挖矿模块对新发起的交易进行审核并计算 PoW 生成新区块添加到链上，所有的区块链数据可以从查看模块获取，从区块链数据找到包含秘密信息的交易记录后，进行解密提取获得秘密信息。

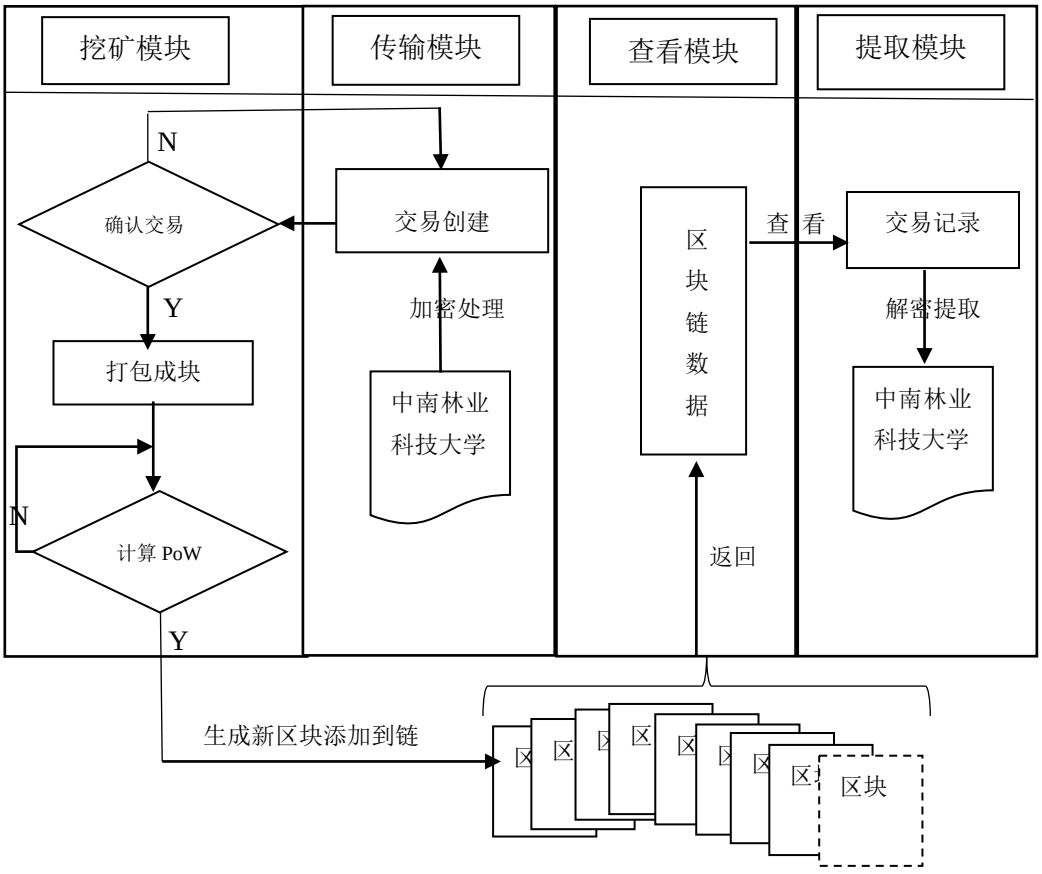

图 5. 系统流程图

系统流程图如图 5 所示，具体包括：

1） 运行区块链系统，通过 API 接口进行交互；

2） 创建一个交易请求,请求 http://localhost:5001/transactions/new（POST），将秘密信息包含到交易中；

3） 通过请求 http://localhost:5001/mine（GET）来进行挖矿，对交易进行确认并生成新区块添加到链上；

4） 通过请求 http://localhost:5000/chain 查看所有区块的信息；

5） 查看整个区块链数据找到包含秘密信息的交易记录，对秘密信息进行解密提取。

4 实验结果与性能分析

4.1 实验结果

为验证区块链中存在隐蔽通信存在，我们对比特币系统中 53 万个区块进行了分析，并发现了两个地址在进行通信的现象，图 6 所示。

地址 A：13XzuQvRnMYqcWde6y1ExwQzCLMDLHZSz4；

地址 B：14jSUj5DtbHe94xxubXD6EsxpPFefUQJmX。

通过比较分析了 A 跟 B 之间近期交易记录，可以发现以下 3 个特点：1）A 跟 B 用来交易的比特币数量是以必要的交易手续费递减的；2）A 跟 B 之间交易频率平均每天两到三次；3）隐藏信息都是以 OKT 三个字母开头。实际上，从 2016 年 5 月 17 日起到 2018 年 7 月 2 日为止，这样的交易记录一共有 12365 条，其中 A 跟 B 的交易记录有 4917 条，在 A 跟 B 进行传递信息之前，B 进行了 7448 次自身交易，如图 7 所示。A 与 B 之间的 2017 年交易次数频繁，在该年 3 月份次数达到 2514 次之多，最后在 2018 年年交易初次数开始有所减少，维持着每天两到三次。所有这些交易包含的秘密信息都以乱码、数字与字符等组合的形式展现，只知道其 16 进制字符串，在不知道信息隐藏的规则以及发送方密钥的情况下，无法得知确切内容。

A 与 B 之间进行如此多次交易都以 0.0001BTC，0.0002BTC，0.0005BTC 或 0.001BTC 数额支付了所必须的交易费，花费了共 5.8551BTC，根据 16 年到 18 年的比特币价格走势图，光交易费也是一笔不小消耗。

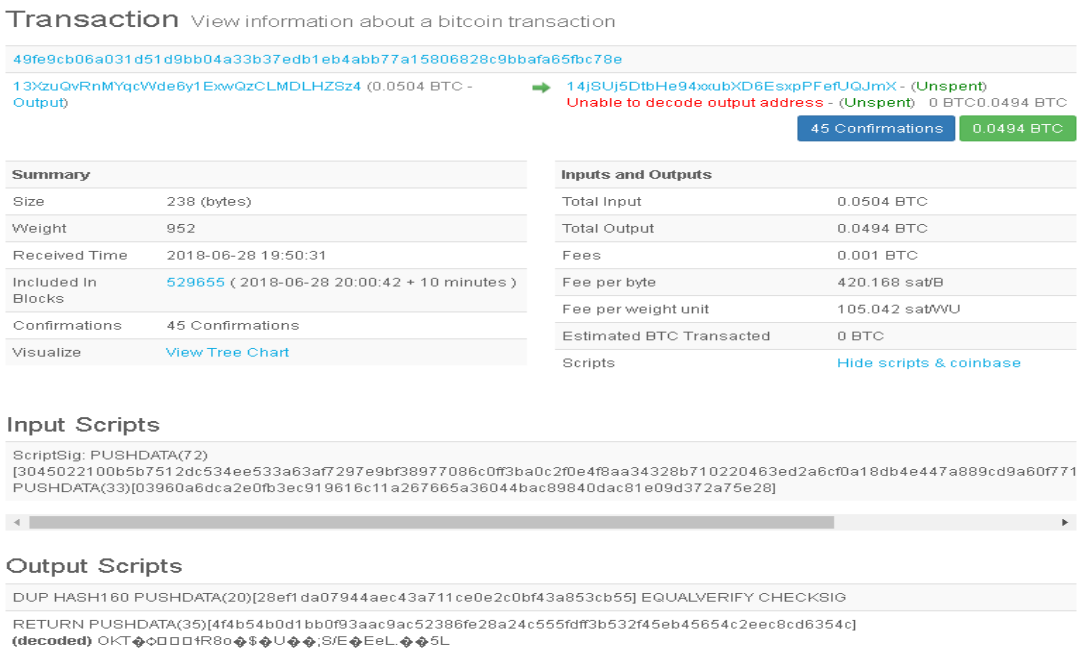

图 6. 地址 A 与地址 B 隐蔽通信交易图

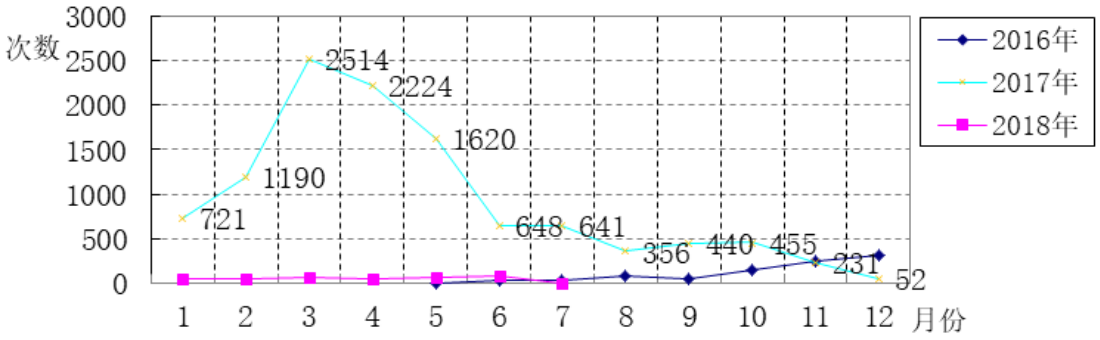

图 7. 地址 A 与地址 B 隐蔽通信次数图

4.2 系统实现

本文使用 CPU 主频 3.2GHz 的主机，在 linux 平台 python 编程环境下进行实验，实现了基于区块链的隐蔽通信系统。系统功能演示主界面如图 8 所示。

图 8 基于区块链的隐蔽通信系统主界面

下面以“中南林业科技大学”作为传递的秘密信息进行一次基于区块链的隐蔽通信模拟实验。

传输模块：首先模拟发送方要创建一笔交易，除了必要的交易信息填写外，加上需要传递的秘密信息“中南林业科学大学”，再对其进行加密处理。图 9 表示交易的创建，图 10 是对信息进行加密处理之后的界面。

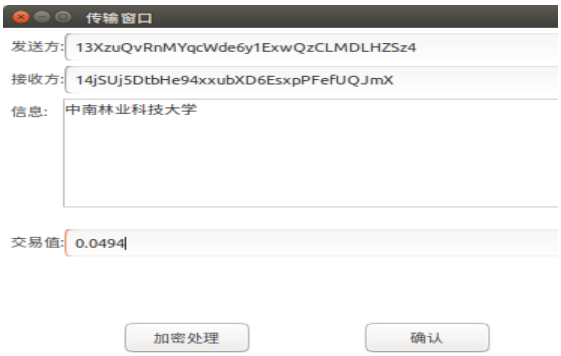

图 9 交易的创建

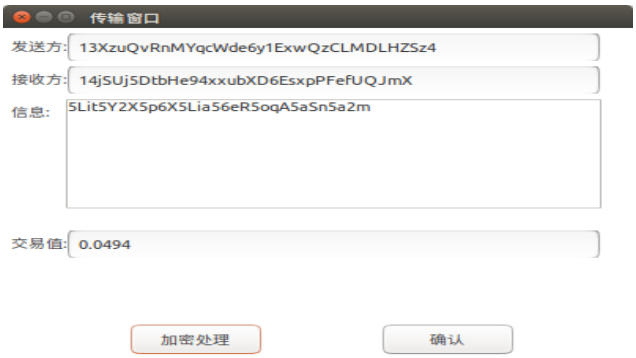

图 10 加密处理

挖矿模块：交易创建完成后，需要等待挖矿模块验证确认对其打包成块，成功产生新区块时，该笔交易就会放进区块链上，秘密信息就永久的存储在区块链上了，无法篡改。图 11 表示挖矿成功。

图 11 挖矿成功

查看模块：为了确认包含秘密信息的交易是否成功添加到链上，可以通过查看模块获取最新的区块链数据，因为区块链具有公开性，所以可以查询到所有的交易记录。图 12 表示区块链数据。

图 12 区块链数据

提取模块：接收方通过查看模块成功找到那条包含秘密信息的交易时，对秘密信息进行提取，隐蔽通信的目的就完成了，图 13 是提取操作。

图 13 提取信息

4.3 性能分析

防篡改性：从 2009 年中本聪挖出创世区块运行到现在 2018 年，区块链已经产生了将近 53 万个区块，并还在以平均每十分钟产生一个新区快，每秒 7 个交易的速度稳定运行中，所有交易信息都保存在区块链当中，区块链的特性让它成为一个天然的可靠的安全的可以进行信息隐藏的场所，如果想要破解区块链系统，只有等到量子计算机，依据当前的密码理论，只有量子计算机才有可能在短时间内破解区块链系统让其崩溃，只要区块链系统不崩溃，交易记录将永久保存且无法进行篡改，隐蔽通信的安全性极高。

隐蔽性：区块链数据是公开的，但由于现有的比特币上的区块已达到 53 万块，而隐蔽通信是在一笔交易上，对于区块链海量的交易笔来说，想要确定出哪一笔交易存在隐蔽通信

在计算上还是困难的。

容量：由于比特币核心开发者认为 OP_RETURN 会导致用户在比特币网络上存储过多的非交易信息，可能影响比特币的正常使用，所以对其所能添加的外带数据大小做了限制（最早是 40 字节，扩大到 80 字节，之后又缩小到 40 字节）。事实上，比特币的交易费是与交易的体积相关的，使用者都会趋向于在实现功能的前提下尽量少地占用空间，过小的强制限制并没有必要。而且 OP_RETURN 交易的总体积只占了整个区块体积的 0.3%，在 2018 年 5 月份的升级中，比特币现金计划将 OP_RETURN 的空间提升到 233 字节，利用区块链上的这更大存储空间，就可以做更多事情了。

即时性：交易的去确认需要时间，一般是 10 分钟左右，所以在即使通信方面，利用区块链的比特币交易进行的隐蔽通信存在缺陷。

5 结束语

信息隐藏的形态在新的网络环境下将不断发展变化，网络上的各种信息媒介均可作为秘密信息的伪装载体。区块链在去中心化的网络环境作为秘密信息载体有着天然优势：区块链的不可篡改性使得恶意篡改攻击无法实现，同时区块链的匿名交易保障了通信双方的匿名性与隐私性。

本文首先探讨了区块链自身特性，并对现存比特币中的区块链数据进行分析发现：有疑似秘密通信的行为存在。接着，论文实现了一套简单的基于外带数据的区块链秘密通信的方案，并进行秘密通信实验，实验结果满足信息隐藏的需要。但是本文采用了最为简单的外带数据，还是存在秘密信息不可见的特性。接下来的工作将考虑采用无载体信息隐藏方法在区块链上实现隐蔽通信的目的。

参考文献

[1] 张新鹏,钱振兴,李晟.信息隐藏研究展望[J].应用科学学报,2016,34(05): 475-489.

[2] Zielińska E, Mazurczyk W, Szczypiorski K. Trends in steganography [J]. Communications of the ACM, 2014, 57(3): 86-95.

[3] Mazurczyk W, Wendzel S. Information Hiding: Challenges for Forensic Experts [J]. Communications of the ACM, 2018, 61(1): 86-94.

[4] 黄殿中,张静飞,张茹,等. 基于大数据环境的多模态信息隐藏新体系[J].电子学报, 2017, 45(02): 477-484.

[5] 张新鹏,殷赵霞. 多媒体信息隐藏技术[J].自然杂志,2017, 39(2): 87-95.

[6] 周志立,曹燚,孙星明. 基于图像Bag-of-Words模型的无载体信息隐藏[J].应用科学学报,2016,34(5): 527-536.

[7] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [J]. 2008.

[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.

[9] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J].计算机学报, 2018,41(5):969-988.

[10] 刘敖迪,杜学绘,王娜,等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报, 2018, 29(7):2092-2115.

[11] 叶聪聪,李国强,蔡鸿明,等. 区块链的安全检测模型[J].软件学报,2018, 29(5): 1-10.

[12] 祝烈煌,高峰,沈蒙,等. 区块链隐私保护研究综述[J].计算机研究与发展, 2017, 54(10): 2170-2186.