多地址的时间型区块链隐蔽通信方法研究

黄冬艳，李琨

（桂林电子科技大学广西无线宽带通信与信号处理重点实验室，广西 桂林 541004）

摘 要：针对现有的区块时间戳间隔隐藏方法所携带信息量低的问题，提出一种多地址的时间型区块链隐蔽通信方法。首先将密文拆分并由不同的地址来传输，地址的区块时间戳间隔表示密文分片的内容；然后接收方读取并统计这些地址所在区块的间隔；最后组合还原出密文。此外，针对时间型区块链隐蔽通信系统缺少隐蔽措施的问题，还提出了一种调整交易发起时间间隔的方法，以降低因隐蔽通信行为而导致地址呈现特殊性的概率。实验结果验证了在有 n 个地址参与情况下，所提方法的传输速率比基础时间型区块链隐蔽通信方法提升了约 n 倍。

关键词：区块链；隐蔽通信；信息隐藏

中图分类号：TP309.2

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023026

Research on multi-address time-based blockchain covert communication method

HUANG Dongyan, LI Kun

Guangxi Key Laboratory of Wireless Wideband Communication and Signal Processing, Guilin University of Electronic Technology, Guilin 541004, China

Abstract: Aiming at the problem of low amount of information carried by the existing block timestamp interval hiding method, a multi-address time-based blockchain covert communication method was proposed. Firstly, the ciphertext was split and transmitted by different addresses. The content of the ciphertext fragment was represented by the block timestamp interval of the address. Then the interval of the blocks was read and counted by the receiver where these addresses were located. Finally, the ciphertext was restored by combination. In addition, in view of the lack of concealment measures in the time-based blockchain covert communication system, a method of adjusting the time interval of transaction initiation was proposed to reduce the probability of address specificity caused by covert communication behavior. The experimental results verify that the transmission rate of the proposed method is about n times higher than that of the time-based blockchain covert communication method when n addresses are involved.

Keywords: blockchain, covert communication, information hiding

0 引言

隐蔽通信利用正常的通信行为传送秘密信息，可大大降低信息在传递过程中受攻击的风险。不同于一般的加密通信，隐蔽通信一般采用公共的信息载体，将隐蔽信息隐藏在主体信息中并随之一起传输。所有用户都可以读取或接收到主体信息，但只有隐蔽通信的目标接收方才有解密隐蔽信息的方法，其他用户无法察觉正在进行的隐蔽通信行为[1]。然而，若攻击者有足够多的时间和计算机资源对存

收稿日期：2022−09−01；**修回日期：**2022−12−29

基金项目：广西重点研发计划基金资助项目（桂科 AB20238026）；广西自然科学青年基金资助项目（No.2022GXNSFBA035645）；国家自然科学基金资助项目（No.6217070229）；桂林电子科技大学研究生创新项目（No.2022YCXS052, No.2021YCXS042）

Foundation Items: Guangxi Key Research and Development Program (No.AB20238026), Guangxi Natural Science Foundation for Youths (No.2022GXNSFBA035645), The National Natural Science Foundation of China (No.6217070229), Innovation Project of GUET Graduate Education (No.2022YCXS052, No.2021YCXS042)

在隐蔽通信行为的通信方进行针对性的检测，就可以区分和检测出隐蔽通道[2]。

区块链特别是公链，以去中心化和难以篡改著称，由大部分节点参与共识形成的去中心化结构提供了匿名环境；区块中的交易内容是随机生成的地址之间的转账过程，而不是实际的账户，因此无法通过交易地址得知账户拥有人；利用 Hash 函数唯一性特点[3]将产生的区块以时间戳顺序串联起来保证区块的内容难以篡改，具有很强的安全性。第三方检测者要想从随机地址的交易环境中找到存在隐蔽通信行为的用户非常困难。因此，区块链平台是实现隐蔽通信理想的信息载体。

比特币[4]和以太坊[5]是目前最活跃、最完善的公链，现有关于区块链隐蔽通信的研究大多基于这 2 种公链。

基于比特币的隐藏方案。Partala[6]提出的 BLOCCE 隐藏结构，在比特币公钥地址的最低有效位（LSB）添加一位数据，通过连续的交易，接收方将地址解析后再组合成密文消息。在此基础上，宋上等[7]提出的 BLOCCE+提高了单次交易的嵌入数据量和单个区块可提取的交易数量，实现信息传输速率的提升，并且通过将下一次隐蔽信息的开始标识符（MSI）包含在密文中以减少链外通信次数。Zhang 等[8]提出的 V-BLOCCE 则将 BLOCCE 原本以二进制嵌入地址换成与比特币地址同样编码的 BASE58，利用比特币地址生成应用 Vanitygen 在地址中映射密文，并将索引表存放在交易的脚本字段，极大地提升了传输速率。但是，以 BLOCCE 为代表的 LSB 交易地址隐藏方法需要维护大量参与隐蔽通信的特殊地址，其改进方案使用更多的交易字段来隐藏数据，这意味着交易的特殊性增加，容易被检测为异常行为。

基于以太坊的隐藏方案。Liu 等[9]使用以太坊交易的 VALUE 字段构造了基于哈希消息认证码（HMAC）的多比特嵌入方法，同时构建哈希链增加隐蔽性，并且增加了模糊数据以提升安全性。Zhang 等[10]利用以太坊 Whispers 通信中的信封和信体机制，将密文和映射表存储到信体中，信封的主题字段存储标志，用于加快收信人的筛选速度，收信人通过筛选信封主题快速收集隐蔽信息。Zhang 等[11]对投票和竞价智能合约提出隐藏方法，接收方根据收到的投票和竞价顺序或地址首字母进行排序，若以选项作为载体，则对地址排序，地址对应的选项序号为隐藏的字符；若以地址作为载体，则以选项顺序对应地址首字母作为隐藏信息。

基于文本或图像的隐藏方案。佘维等[12]通过在交易中发送 txt 文件的最后文本行添加空格表示二进制密文，并且通过双方提前协商建立偏序集来增加隐藏强度。Basuki 等[13]提出了基于加密图像实现隐藏大量信息的方法，首先由发送方在以太坊交易的时间戳、目标地址和交易上限字段中利用最高有效位（MSB）嵌入图像解密的方法数据包，然后接收方获取并解析数据包后得到加密图像的统一资源定位符（URL）和解密方法，最后解密图像即可得到大量的隐藏信息。

上述方案均是基于在地址或字段的特殊位置隐藏的思路开展的研究，可归类为存储型隐蔽通信方案。不同于以上方案，隐蔽通信系统还能以时间为载体进行构建，如调整时间间隔、改变数据速率、改变包排列顺序、触发数据重传等[2]。

区块链系统中的时间戳机制是良好的时间载体，然而目前的研究较少，仅有李彦峰等[14]提出的基于区块链时间戳隐藏方法，该方法不依赖特殊地址，而是对交易时间戳的间隔进行编码以承载隐藏信息，因此具有独特的隐蔽性。但受限于单位时间内有限的信息量，隐蔽通信的传输速率低，且通信的开始和结束标志为连续的码字，也容易被检测为异常行为。

在此研究基础上，本文以提升时间型区块链隐蔽通信的传输速率和增强抗检测性为目的，提出一种多地址时间型区块链隐蔽通信方法，由特殊地址表示隐蔽通信的开始和结束，在一个区块内由多个地址参与隐蔽通信，将隐蔽通信任务拆分到更多地址上，地址的交易时间戳间隔表示密文片段，接收方读取区块并统计这些交易的间隔，最后组合、解密和还原出密文。

本文的主要贡献如下。

1) 提出了多地址的时间型区块链隐蔽通信方法，在一个区块内传输更多的信息量，具有更高的传输速率。

2) 提出了一种调整交易发起时间间隔的方法，降低了因隐蔽通信行为而导致地址呈现特殊性的概率，实现更好的抗检测性能。

3) 以比特币交易数据作为测试数据，评估了所提隐蔽通信方法的传输速率和抗检测性。

1 背景知识

1.1 隐蔽通信系统

基础的隐蔽通信系统主要由构建网络隐蔽信道、嵌入密文和提取密文 3 个过程组成。

1) 网络隐蔽信道可以分为存储型网络隐蔽信道和时间型网络隐蔽信道。存储型网络隐蔽信道使用协议数据单元内部的信息传输隐蔽数据；时间型网络隐蔽信道使用协议数据单元的时间特性传输隐蔽数据。时间型隐蔽通信比存储型隐蔽通信的隐蔽性更好，但传输速率更低[1]。

2) 存储型网络隐蔽信道嵌入密文的方法主要有根据数据包和协议头中未使用的或不会被验证的字段增加数据，例如，在数据包中非关键报文的排列顺序隐藏信息；根据需要编码的字段中嵌入一位有效值，称为 LSB。时间型网络隐蔽信道嵌入密文的方法主要有 2 种，分别为根据不同数据包之间的时间间隔隐藏编码后的信息和根据数据包到达的时间顺序隐藏信息[2]。

3) 密文提取方法由隐蔽通信双方在通信开始前协商，密文的接收一般根据时间顺序依次提取隐藏信息组合，得到的密文由发送方进行加密，接收方根据提前协商的方法解密便可得到信息。

在此基础上，还有一些结合所在网络环境实现隐蔽通信的方案，Taheri 等[15]在 VANET（vehicular ad-hoc network）中开发了一种混合（时间和存储）隐蔽通道，时间方面通过改变服务和控制数据包的时间模式来发送隐蔽消息，存储方面通过控制信道发送周期性消息的一些字段。Wendzel 等[16]使用 TCP/IP 头字段作为隐蔽信道载体，将传输的密文内容分片，同时建立多个传输协议随机发送分片，收集所有分片以还原密文信息。Zhang 等[17]提出了一种双向长期演进语音承载（VoLTE）隐蔽方法，正向通过主动丢弃数据包来调制隐蔽消息，反向通过数据包存储反馈隐蔽信息，通过反馈更改正向传输的参数。这些隐蔽通信实现方法对在区块链中实现更好的隐蔽通信有借鉴意义。

1.2 区块链技术

隐蔽通信中涉及的区块链相关概念如下。

1) 交易的地址。一次交易的发起需要发送方的地址、对应的公钥和签名，以及接收方的地址。用户可以拥有多个地址，只要掌握地址对应的私钥即视为拥有此地址。以比特币为例，地址生成过程如图 1 所示，地址的私钥是随机生成的，私钥经过椭圆曲线计算生成公钥，再通过 SHA256 运算和 RIPEMD160 运算得到 Hash 值，和版本号一起进行双 SHA256 运算，选取前 4 B 作为校验码，一起封装后再经过 BASE58 编码转换成比特币地址。

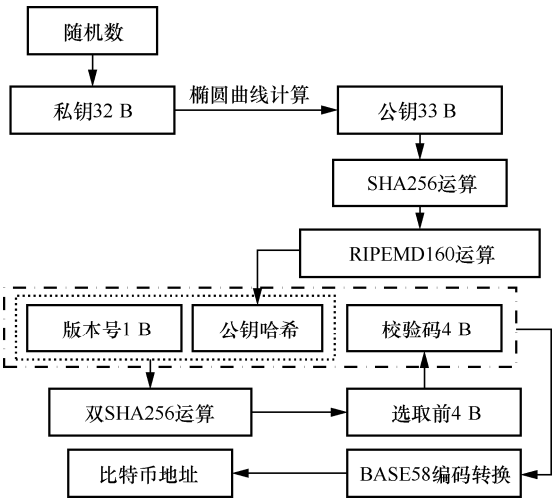


图 1 比特币地址生成过程

2) 交易的时间戳。区块链的时间戳有 2 个作用，一是防止篡改区块哈希值，二是保证区块排列顺序。如图 2 所示，待确认交易的时间是本地用户发起交易的时间，在未被区块验证和打包成块之前所有待确认交易都使用本地时间。对于确认后的交易来说，其时间戳为区块时间戳，即一个区块的所有交易都是同一个确认时间。

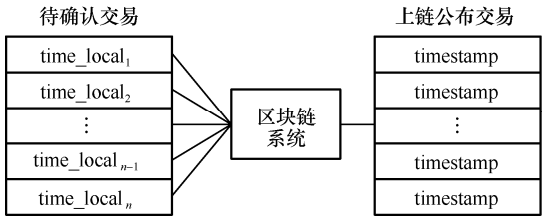


图 2 区块链系统的发起交易时间和确认时间

3) 地址发起交易的间隔。对于区块链系统来说，不同地址发起交易的频率是独立分布的，交易首先进入待确认过程，被系统打包成块后再被赋予时间戳等信息。因此地址发起交易间隔有本地发起交易间隔和区块时间戳间隔两类。如图 3 所示，对于地址 add_2 的连续两次交易，发起时间为 t_1和t_2，对应的区块时间戳为 t_1'和t_2'，交易的确认时间为 Δ_1和Δ_2，发起交易的间隔为 Δt_1，区块时间戳间隔为 $\Delta t_1'$。

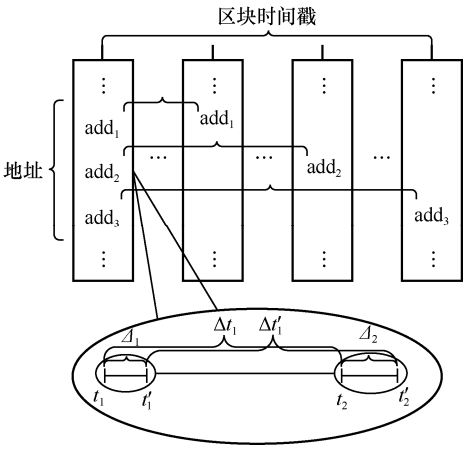


图 3　地址发起交易的间隔

4) 地址发起交易的交易费。区块链系统为了避免恶意发起大量无效交易增加了交易费机制，因此对于打包区块方来说，交易费越高越先进入区块。当等待打包交易的队列过长或者一笔交易的交易费少于绝大部分交易时，交易费低的交易可能一直不会被打包进区块，并且随着拥塞时间的增加被撤销而成为无效交易。

2　多地址区块链隐蔽通信方法设计

公链区块链的地址权限是由掌握对应私钥的用户所使用的，用户实际控制的私钥和地址的数量是可观的，又由于地址对应的私钥不会公开，用户始终是匿名的，因此使用部分地址组成一个地址池参与隐蔽通信在用户角度是完全可行的。

2.1　隐蔽通信流程

多地址区块链隐蔽通信流程如图 4 所示。

1) 隐蔽通信的开始和结束标志仅由发送方用特殊地址 add_s 发给接收方的地址表示，其他地址对应密文 M 的分片 M_i，这些地址组成地址池，特殊地址可以在发送方本身拥有的地址中挑选，也可以使用 Vanitygen 程序生成[8]，对指定地址位规定数值并自动生成地址，只需双方在提前协商过程中达成共识即可。

2) 当收到特殊地址的交易后，接收方开始在下一个区块中遍历发送方所有参与隐蔽通信的地址。这些地址的交易可以指向任意地址而不只是接收方，因此不影响发送方的正常交易。由于区块时间戳不需要额外获取，接收方只需要遍历地址池的地址是否出现在此区块中，因此减少了遍历的开销。

3) 接收方首先根据地址列表筛选，得到每个地址的交易发起分布，再按照交易发起的时间戳排序，直到收到结束标志的地址开始解密。2 个交易之间的间隔表示为隐蔽信息，若以二进制作为密文的调制方式，则可以设定短交易区块时间戳间隔 $\Delta t_1'$ 为“0”，长交易区块时间戳间隔 $\Delta t_2'$ 为“1”，将

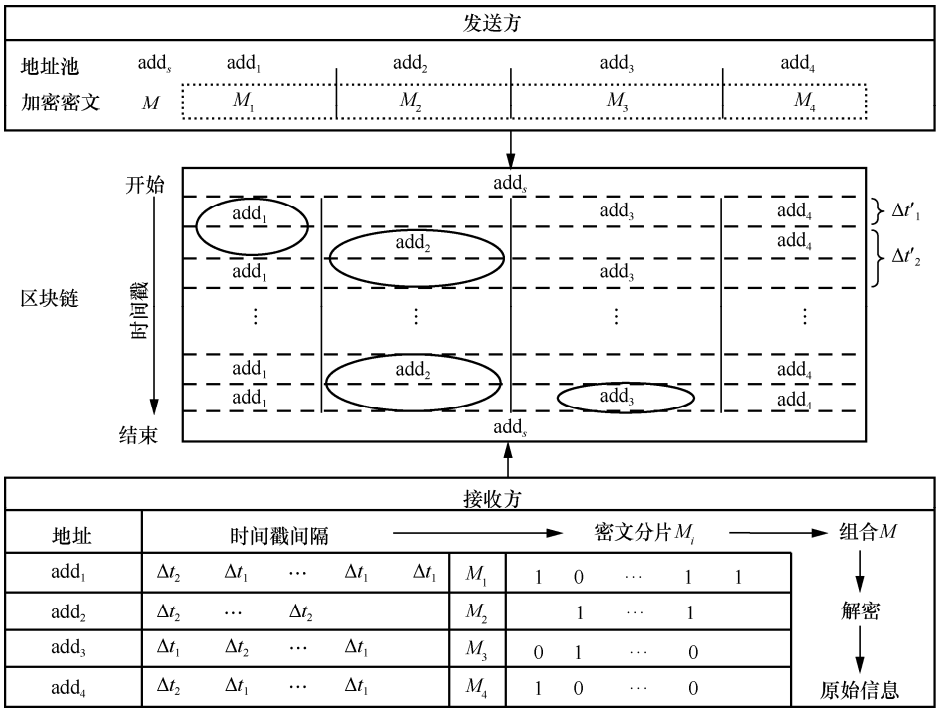


图 4　多地址区块链隐蔽通信流程

所有地址的交易间隔对应的密文分片组合得到完整密文，密文分片的顺序由地址池的顺序保证，地址池的顺序可按照地址的字母排序或双方提前协商的规则。

4) 如果某个交易因为交易费不足或区块链系统拥塞没有被及时打包到对应的区块中，导致最新的区块中读取不到该地址，则发送方在下一个区块中追加一个由特殊地址 add_s 发起的交易表示暂停，本次信息无效，该交易的接收指向接收方地址和被延迟打包的地址，同时暂停被延迟打包的地址发起下一次通信，直到发送方和接收方在新的区块中发现被延迟打包的地址出现在后续的区块，结束暂停。

5) 隐蔽通信开始之前的协商内容如下。① 发送方发起隐蔽通信的地址池包括特殊地址；② 密文对应的信息编码和加密规则。在一次正常的交易中，接收方需要向发送方公布接收地址，协商过程本来就合理存在，因此协商可以顺利完成。

整个隐蔽通信中地址的对应关系如图 5 所示，只有特殊地址 add_s 的交易指向接收方地址，而其他地址的交易指向可以是任意地址，接收地址出现的频率减少，降低了地址交易的特殊性，且不影响发送方本身常规的交易需求。

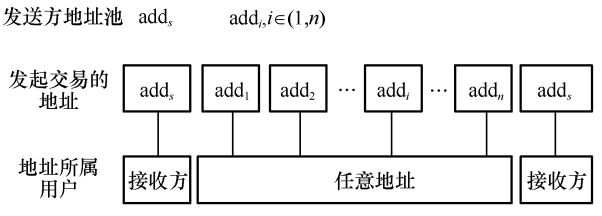


图 5 地址的对应关系

2.2 地址交易间隔分布和传输速率

区块链系统将一个时间段的交易打包并赋予同一个时间戳，而时间型隐蔽通信利用时间间隔作为载体隐藏密文，间隔长短对应不同的码字，因此参与隐蔽通信的地址在一段时间内会间隔着区块时间戳出现在区块中。若以此规律作为检测区块中是否存在特殊地址的判断条件，则会有大量正常样本被计入可疑样本。由于本文方法参与传输密文的地址数量增多，每个地址承担的隐蔽通信任务时间大大缩短，更难以和正常样本区分，故隐蔽性较好；若检测地址发起交易间隔，也就是待确认交易，这个阶段的交易发起行为更加随机化，对于有规律的隐蔽通信行为会变得更特殊、更容易分辨。因此需要对一般的地址交易发起行为进行统计和建模，以优化隐蔽通信地址的交易发起行为。

将整个区块链的交易到达过程视为一个随机过程，这个随机过程可以简化为参数为 λ 的泊松流模型 $P_n(t)=(\lambda t)^n\dfrac{\mathrm{e}^{-\lambda t}}{n!}$，表示在时间区间 t 内 n 个交易到达的概率，参数 λ 表示单位时间内平均到达的交易数量[18]。那么两次交易间隔 T 必定服从指数分布，易证明对任意时间 $t>0$ 和 $s>0$，$P\{T>t+s\,|\,T>s\}=P\{T>t\}$ 具有马尔可夫性，交易到达的间隔与前一次交易无关，交易间隔分布情况由指数分布的分布函数 $1-\mathrm{e}^{-\lambda t}$ 体现。

本文使用的变量和符号释义如表 1 所示。区块链中交易的发起行为由用户决定，且活跃用户的可用地址形成地址池，则在单位时间内，区块链系统平均到达的交易数量 $\lambda=\dfrac{n_\mathrm{T}}{t_\mathrm{B}}$，$t_\mathrm{T}=1-\mathrm{e}^{-\frac{tn_\mathrm{T}}{t_\mathrm{B}}}$；$\alpha n_\mathrm{B}$ 表示单位时间内同地址发起的交易数量，则同地址平均到达的交易数量 $\lambda_\alpha=\dfrac{\alpha n_\mathrm{T}}{t_\mathrm{B}}$，$t_\mathrm{A}=1-\mathrm{e}^{-\frac{t\alpha n_\mathrm{T}}{t_\mathrm{B}}}$。因此，无论是区块链系统的交易间隔分布还是同地址的交易间隔分布，在理论上都是服从指数分布的。

表 1 变量和符号释义

变量	解释
α	单位时间内单个地址发起交易的概率
n_A	参与隐蔽通信的地址数量
n_B	区块链系统当前有效地址的数量
n_T	区块可承载的交易数量
m	密文长度
t_A	同地址发起交易的时间间隔
t_B	区块链系统完成出块的时间
t_T	区块链系统到达的交易间隔

为了得到真实的交易间隔分布，本文收集了比特币一周的交易发起时间数据，对地址的发起交易间隔分析得到发起交易间隔的一般规律，同地址发起交易间隔的分布情况如图 6 所示，发起交易间隔为 0～40 min 的分布情况如图 7 所示。

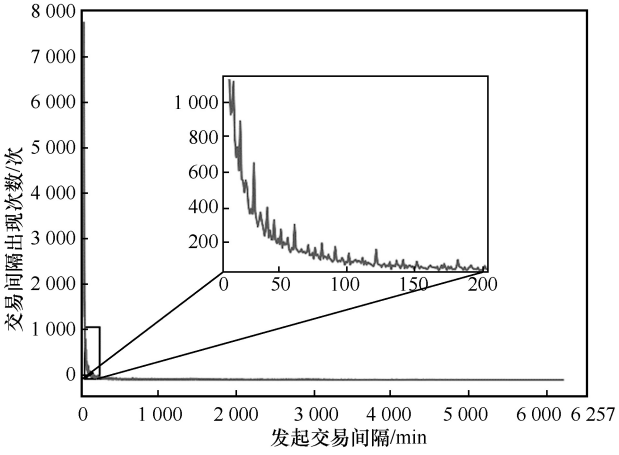


图 6　同地址发起交易间隔的分布情况

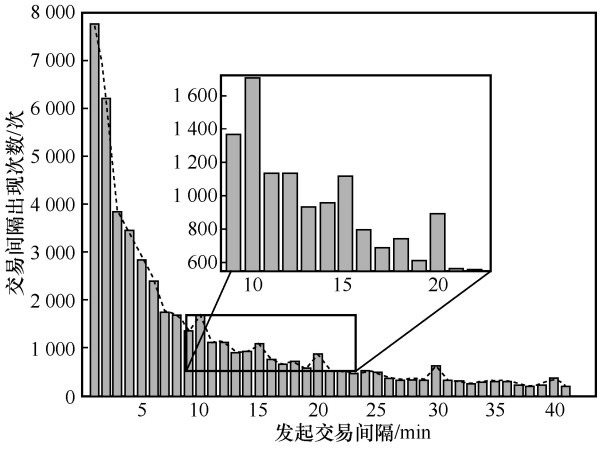


图 7　发起交易间隔为 0～40 min 的分布情况

从图 6 可以看出，同地址发起交易间隔次数的规律近似于指数分布的概率密度函数曲线。

从图 7 可以看出，发起交易间隔出现次数在 10 min、20 min、30 min 都高于邻近时间，这与比特币大约每 10 min 完成一次出块具有很大的关联性，间隔为 10 min 的数量约为 20 min 的 2 倍。

若假设传输的密文以二进制进行调制，短区间（约 10 min）包含一个区块，长区间（约 20 min）包含 2 个区块，由此可以得到隐蔽通信的传输速率。设发送方有 n_{A} 个可以用于隐蔽通信的地址，若密文调制后的“0”“1”码字出现概率为均匀分布，即码字出现的概率相同，可以得到一个地址传输一个码字的平均时间约为 15 min。则拥有 n_{A} 个地址的发送方传输一个码字时间平均约为 $\frac{15}{n_{\mathrm{A}}}$ min，速率为 $\frac{2n_{\mathrm{A}}}{3}$ 比特每区块（bit/block）。发送方传输一个地址私钥随机数为 1 ～ 2^{256}，用二进制表示至多 256 bit，需要经过 $\frac{384}{n_{\mathrm{A}}}$ 个区块传输完成，传输长度为 m 的密文所需区块为 $\frac{3m}{2n_{\mathrm{A}}}$ 个，且 $\frac{3m}{2n_{\mathrm{A}}} \geqslant 2$，即至少有 2 个区块来表示 2 种码字。

同时，地址数量不能超过区块所承载的交易量，大量地址参与会提高交易费，这对区块链系统而言是一种特殊事件，故不可同时发送大量地址。

2.3　地址交易间隔调整

密文码字出现的概率对应时间间隔长短的概率，对于均匀分布的二进制密文，2 个区间包含的交易数量相同，且区间内大部分的交易集中在对应的区块间隔时间上。设长短区间内的不同时间交易发起次数都服从正态分布 $N(\mu,\sigma^2)$，如图 8 所示。从图 8 可知，短区间内服从期望 $\mu=10$ 的正态分布 $N(10,\sigma^2)$，长区间内服从期望 $\mu=20$ 的正态分布 $N(20,\sigma^2)$，15 min 时长短区间的数据重合。

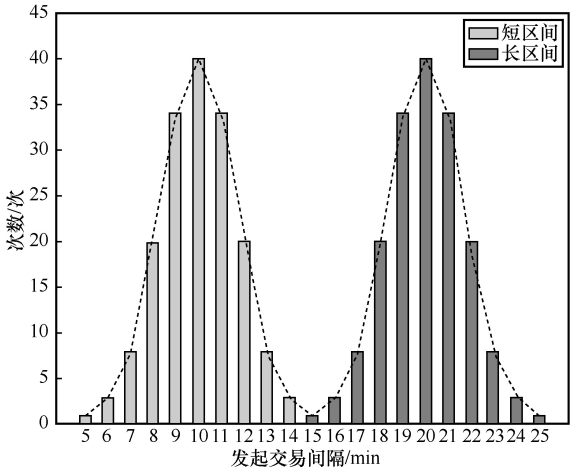


图 8　长短区间内发起交易间隔呈现的正态分布

当这段特殊交易间隔被加入某个地址的交易行为中时，会改变原本指数分布的发起规律，若地址想再次作为隐蔽通信地址，则需要用更多的正常交易来保持正常规律，这不仅影响了隐蔽通信的二次运行效率，还增加了地址的维护开销。

因此可以调整交易间隔分布拟合指数分布，图 9 为交易间隔调整流程，短区间内的发起交易间隔映射在 5～15 min，平均为 10 min；长区间内的发起交易间隔映射在 15～25 min，平均为 20 min。

不同时间间隔出现的次数需要拟合指数分布，若将所有的时间点都分配相应的交易数量，则短区间的交易数量将远超长区间，这不符合密文码字分布。因此在短区间中，可以将交易数量集中在一部分时间点上，使这部分时间点拟合指数分布。

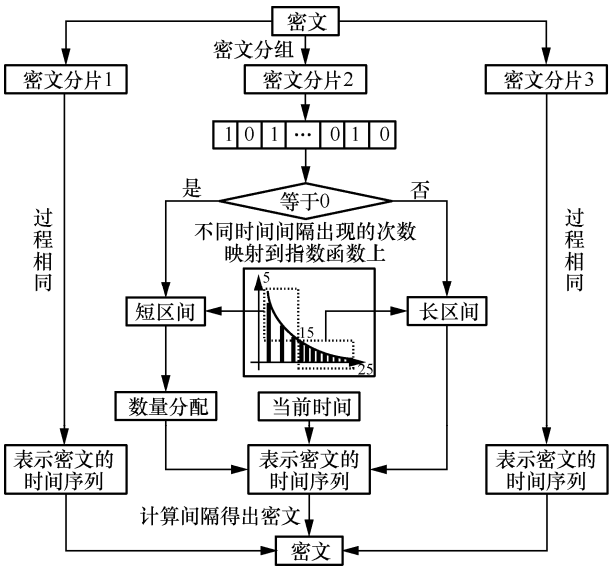


图 9 交易间隔调整流程

调整后的交易间隔分布如图 10 所示，长短 2 个区间内的交易数量相同，长区间内的交易间隔次数服从指数分布，短区间内的交易集中在一些时间点上使整体近似指数分布，当地址完成本次隐蔽通信任务后可以根据发送方要求进入下一次隐蔽通信。而下一次隐蔽通信的序列可以填补上一次短区间空缺的时间点，两次交易间隔都近似指数分布，若统计样本中包含了两次间隔累计次数，则长短区间内交易间隔次数都近似指数分布，地址交易间隔的特殊性进一步降低。

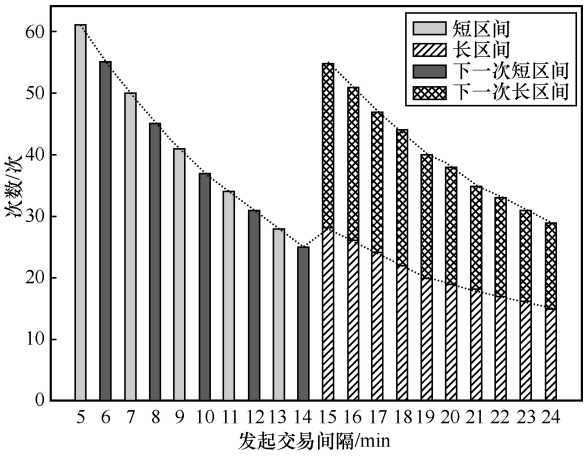


图 10 调整后的交易间隔分布

3 所提隐蔽通信方法的性能分析

3.1 传输速率

不同于文献[19]将隐藏容量定义为每条交易可以嵌入的秘密信息比特数，再根据隐蔽通信时间得到系统效率的对比方式，时间型区块链隐蔽通信方法以区块时间戳间隔为载体，至少需要经过 2 个以上的时间戳间隔才能完成隐蔽通信，因此不适合直接使用上述方式进行对比。

传输速率 C 定义为每个区块中隐藏信息的比特数，单位为比特每区块，若每条交易包含的信息量为 I bit，同时一个区块内可能存在多条参与隐蔽通信的交易，则传输的总信息量为 $I_{\mathrm{C}}=\sum_{t=0}^{t_{\mathrm{B}}} I$ bit。隐蔽通信系统传输一段 m bit 的密文需要 $\frac{m}{I}$ 条交易，故隐蔽通信系统的传输速率表示为

$$C=\frac{m}{\sum_{t=0}^{t_{\mathrm{B}}} I}=I_{\mathrm{C}} \tag{1}$$

BLOCCE 的 LSB 地址隐藏方法一个区块内由一个地址发起一次特殊交易，特殊交易的地址最低有效位嵌入一位字符表示密文，即每个区块时间传输一个包含字符 M 的交易，每条交易的信息量为 $I=\mathrm{lb}M$，其传输速率表示为

$$C=I_{\mathrm{C}}=I=\mathrm{lb}M \tag{2}$$

考虑到在时间型隐蔽通信方法中也可以使用多进制调制密文，但是需要更长的时间间隔来对应码字，其传输效率 $\eta=\frac{1+M}{2\mathrm{lb}M}$，$\frac{1+M}{2}$ 表示传输一个码字的平均区块个数。

如图 11 所示，η 收敛于 $M=4$，为每 1.25 个区块传输 1 bit，二进制传输速率为每 1.5 个区块传输 1 bit，随着编码进制的增加，交易间隔越来越大，传输速率反而下降。因此可以设计一种四进制编码规则以提升速率，限于篇幅，本文采用二进制这种更加普遍的调制方式。

由图 11 可知，本文提出的多地址时间型区块链隐蔽方法二进制调制的密文平均需要 1.5 个区块传输 1 bit，故每条交易的信息量为 $I=\frac{1}{\eta}=\frac{2}{3}$ bit，系统有 n_{A} 个地址，所有地址参与隐蔽通信可视为同一行为，故总信息量为 $I_{\mathrm{C}}=n_{\mathrm{A}}I=\frac{n_{\mathrm{A}}}{\eta}=\frac{2n_{\mathrm{A}}}{3}$ bit。

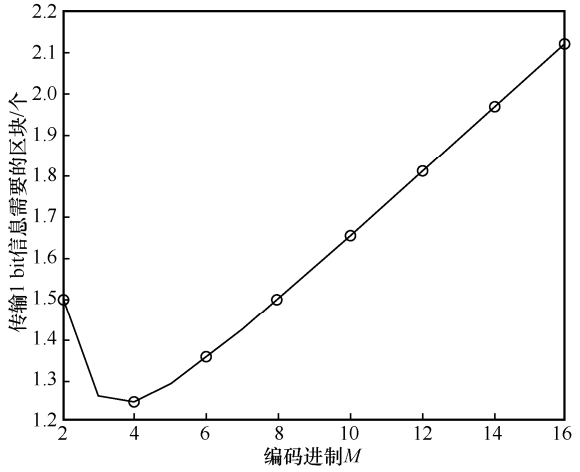


图 11　使用多进制编码的速率曲线

由于时间型隐蔽通信系统开始和结束隐蔽通信需要额外过程，本文方法使用特殊地址尽可能减少这一过程的损耗。为保持开始阶段所有地址同步，开始标志的特殊地址不参与时间间隔计算。考虑到所有地址承载的密文长度不同，结束标志的特殊地址也不参与时间间隔计算，所以整个系统仅多出两次不表示密文的交易。故传输一段 m bit 的密文需要 $\frac{m}{I}+2$ 条交易，其传输速率为 $C=\left(\frac{m}{\frac{3m}{2n_{\mathrm{A}}}+2}\right)$ bit/block，在多进制情况下的传输速率表示为

$$C=\frac{m}{\frac{\eta m}{n_{\mathrm{A}}}+2}=\frac{m}{\frac{m(1+M)}{2n_{\mathrm{A}}\mathrm{lb}M}+2} \tag{3}$$

基础时间间隔隐藏方法，开始和结束标志为连续相同码字，设定为连续的 5 个“0”和“1”，共 10 个间隔作为标志[14]，可由 s 表示开始和结束标志个数，二进制调制下总信息量为 $I_{\mathrm{C}}=I=\frac{2}{3}$ bit，其传输速率为 $C=\left(\frac{m}{\frac{3m}{2}+2s}\right)$ bit/block，在多进制情况下的传输速率表示为

$$C=\frac{m}{\eta m+2s}=\frac{m}{\frac{m(1+M)}{2\mathrm{lb}M}+2s} \tag{4}$$

多地址时间型方法、文献[6]提出的 BLOCCE 的地址 LSB 嵌入型方法和文献[14]提出的基础时间型方法的理论传输速率对比如表 2 所示。其中，M 为编码进制，m 为密文比特数，n_{A} 为用户拥有的可发起的隐蔽通信的地址数，s 为开始和结束标志个数。

表 2　不同隐蔽通信方法的理论传输速率对比

方法	传输速率/(bit·block^{-1})
地址 LSB 嵌入型	$\mathrm{lb}M$
多地址时间型	$\frac{m}{\frac{m(1+M)}{2n_{\mathrm{A}}\mathrm{lb}M}+2}$
基础时间型	$\frac{m}{\frac{m(1+M)}{2\mathrm{lb}M}+2s}$

为了简化对比，接收方从完成出块的区块中遍历隐蔽信息和解码的时间为接收方获密时间，获密时间不计入密文传输时间。

在比特币交易系统中使用同样的编码方式和地址交易发起频率传输同一段密文。设所有隐蔽通信系统都以 10 min 的区块为单位计算隐蔽通信时间，时间型隐蔽通信方法统一使用二进制编码；地址 LSB 嵌入型通信方法中一个区块内包含一次交易，同时传输 256 bit 的密文，不同隐蔽通信方法的传输速率对比如图 12 所示。

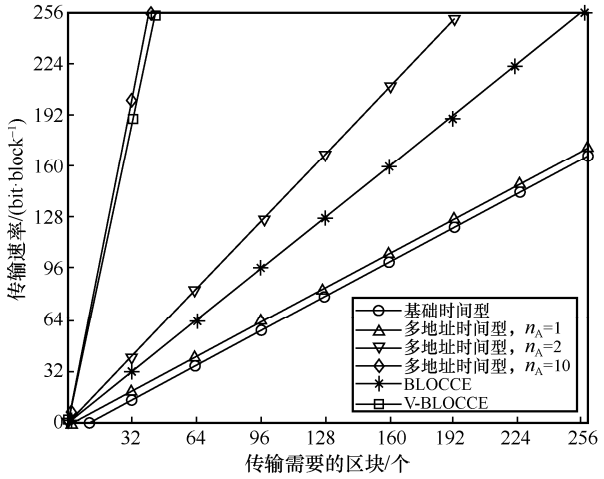


图 12　不同隐蔽通信方法的传输速率对比

当多地址时间型隐蔽通信方法的地址数量 $n_{\mathrm{A}}=1$ 时，信息传输速率略高于基础时间型隐蔽通信方法，这是因为其使用了特殊地址代替发送连续同码字密文作为开始结束标志；当多地址时间型隐蔽通信方法的地址数量 $n_{\mathrm{A}}=2$ 时，信息传输速率高于 LSB 地址隐藏的 BLOCCE；当多地址时间型隐蔽通信方法的地址数量 $n_{\mathrm{A}}=10$ 时，信息传输速率接近直接以 BASE58 编码的 V-BLOCCE[8]。

在包含 2 000 个以上交易的比特币区块中，平均每个区块内仅有 5 次交易参与隐蔽通信，特殊交易占比 0.25%。若将占比小于 1%视为不会引起交易费异常的安全值，在二进制编码下，地址平均每 1.5 个区块出现一次，则极限的地址数量为 $n_{\mathrm{A}}=30$，此时传输速率约为 20 bit/block 。

尽管多地址传输速率比单地址传输速率提升了 n_{A} 倍，可以在更短的时间内完成所有隐藏信息的发送，对于单个地址而言传输时间也相应减少，被检测的可能性也被分散到各个地址中。但用户总体的交易发起次数没有减少，需要同样的交易费，而多进制编码的 BLOCCE 可以在单次交易中隐藏更多的信息从而减少交易发起次数，这是时间型区块链隐蔽通信方法暂时无法做到的。

3.2 抗检测性

抗检测性即隐蔽通信系统的安全性，不同于加密密文提升密文安全性，抗检测的安全性表现为网络隐蔽信道不被发现的能力，是密文安全的第一道防线，一个好的隐蔽通信系统可以不依赖加密密文等方法做到隐蔽传输完成而不被发现，即隐蔽通信系统可以在被检测出来前完成密文传递[20]。

在区块链系统中，隐蔽通信信道的基本单元为地址，本文提出的多地址时间型隐蔽通信方法从 3 个方面降低地址的特殊性：1) 除了作为标志的特殊地址，其余所有地址的交易指向可以是任意地址，使承载密文的地址不泄露接收地址，降低了接收地址的特殊性；2) 使用多地址实现分布式传输密文不仅提升传输速率也均衡了每个地址隐蔽通信量，地址隐蔽通信的持续时间大大减少，降低了发起地址出现次数的特殊性；3) 优化交易的发起时间间隔，拟合正常样本的分布，降低了发起地址的发起时间间隔的特殊性。

针对发起时间，从信息论角度对比加入隐蔽通信过程后的交易间隔分布和正常的交易间隔分布得到抗检测性能。K-L 散度又称相对熵，用于描述 2 个概率分布的差异关系，定义为 $D_{\mathrm{KL}}\left(P\|G\right)=\sum_{x}P(x)\cdot \mathrm{lb}\left(\dfrac{P(x)}{G(x)}\right)$，其中，$P$ 表示真实的概率分布，G 表示拟合的概率分布。在隐蔽通信的抗检测性测试中，P 和 G 可以体现为合法流量和隐蔽流量的概率分布[21]。

基于对比特币正常交易间隔分布的统计结果，设正常样本为指数分布的交易间隔，隐蔽通信交易隔间主要集中在 5～25 min。当前场景下 $x\in[5,25]$，未作处理的正态分布表示为

$$G_{\mathrm{n}}(x)=\begin{cases}\dfrac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x-\mu_1)^2}{2\sigma^2}}, x\in[5,15],\mu_1=10\\ \dfrac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x-\mu_2)^2}{2\sigma^2}}, x\in[16,25],\mu_2=20\end{cases} \tag{5}$$

一次拟合的指数分布表示为

$$G_{\mathrm{e1}}(x)=\begin{cases}\lambda\mathrm{e}^{-\lambda x}, x=2n-1, n\in[3,7]\\ \lambda\mathrm{e}^{-\lambda x}, x=n, n\in[16,25]\end{cases} \tag{6}$$

两次拟合的指数分布表示为

$$G_{\mathrm{e2}}(x)=\begin{cases}\lambda\mathrm{e}^{-\lambda x}, x\in[5,15]\\ 2\lambda\mathrm{e}^{-\lambda x}, x\in[16,25]\end{cases} \tag{7}$$

合法流量的概率分布 $P(x)=\lambda\mathrm{e}^{-\lambda x}, x\in[5,25]$，依次得到的 3 个离散熵分别表示为

$$D_{\mathrm{KLn}}\left(P\|G_{\mathrm{n}}\right)=\sum_{x=5}^{25}\lambda\mathrm{e}^{-\lambda x}\mathrm{lb}\left(\frac{\lambda\mathrm{e}^{-\lambda x}}{G_{\mathrm{n}}(x)}\right) \tag{8}$$

$$D_{\mathrm{KLe1}}\left(P\|G_{\mathrm{e1}}\right)=\sum_{x=5}^{25}\lambda\mathrm{e}^{-\lambda x}\mathrm{lb}\left(\frac{\lambda\mathrm{e}^{-\lambda x}}{G_{\mathrm{e1}}(x)}\right) \tag{9}$$

$$D_{\mathrm{KLe2}}\left(P\|G_{\mathrm{e2}}\right)=\sum_{x=5}^{25}\lambda\mathrm{e}^{-\lambda x}\mathrm{lb}\left(\frac{\lambda\mathrm{e}^{-\lambda x}}{G_{\mathrm{e2}}(x)}\right) \tag{10}$$

将隐蔽流量混入合法流量后中进行评估离散度，由 K-L 散度公式和熵函数可知，合法流量 P 和隐蔽流量 G 的差值越大，相对熵 $\mathrm{D_{KL}}$ 越大，当相对熵达到某个阈值时可以认定为隐蔽流量。

G_{e1}、G_{e2} 和合法流量 P 都为指数分布，相较于正态分布的 G_{n} 会具有更低的离散度，而两次拟合后的指数分布 G_{e2} 相较于一次拟合的 G_{e1} 拟合的时间点更多，离散度将会进一步降低。

假设某地址在一段时间内一共发起 1 000 次交易，其中包含了 100 次隐蔽通信交易，即隐蔽通信样本和正常样本的比例为 1:9。正常交易间隔序列和分别加入正态分布密文、指数分布密文后的序列如图 13 所示，其中指数分布密文序列分为两阶段，第一阶段为加入一次指数分布密文后的分布，如图 13(c)所示；第二阶段为加入两次指数分布密文后的分布，如图 13(d)所示，为了方便对比，比例仍然为 1:9。

表 3 为合法流量 P 和隐蔽流量 G 的概率分布情况，P 为 1 000 次正常交易间隔样本，G 为 900 次

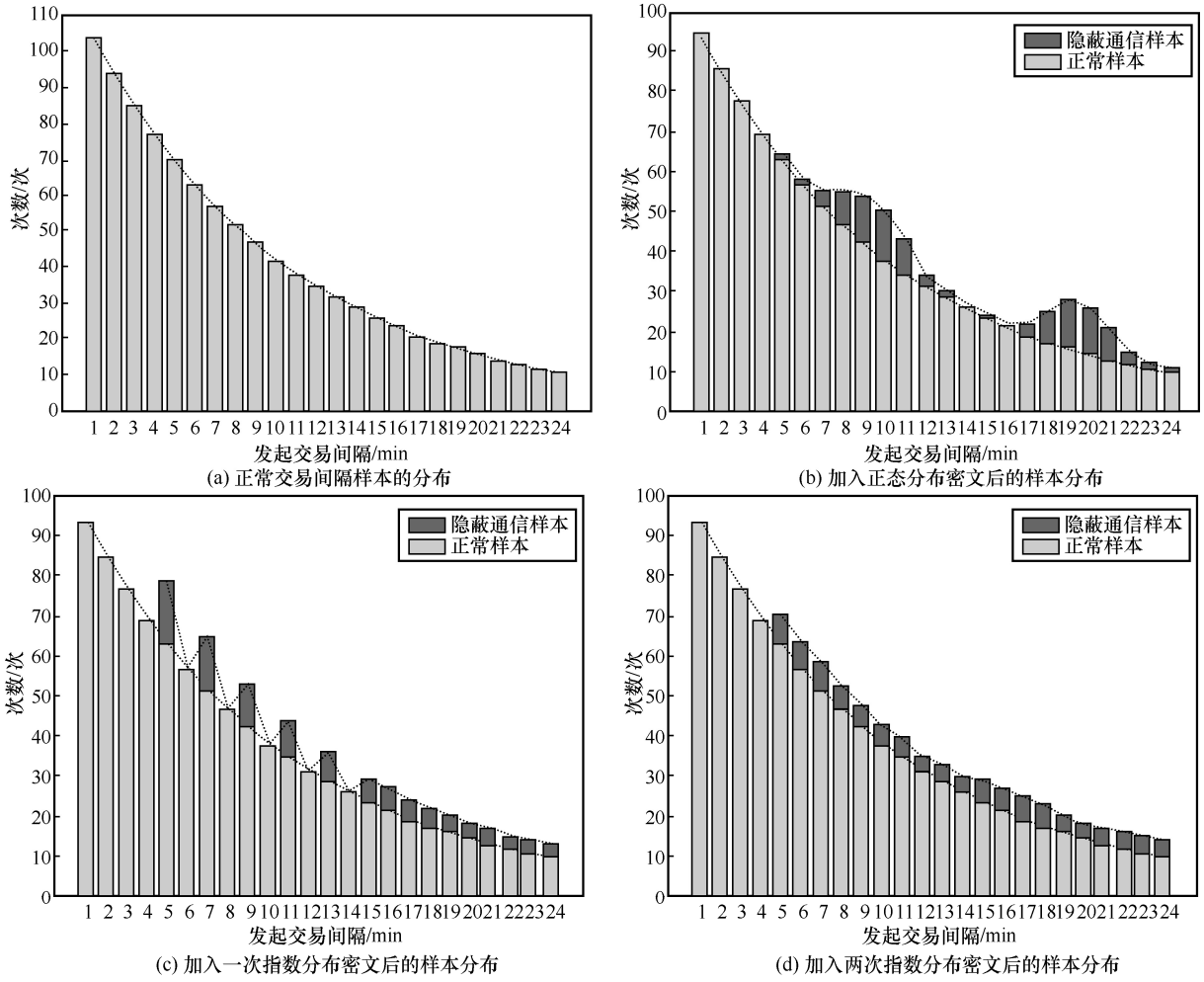


图 13　正常交易间隔样本和隐蔽通信交易间隔样本的分布

表 3　　**合法流量 *P* 和隐蔽流量 *G* 的概率分布情况**

x	$P(x)$	$G_n(x)$	$G_{e1}(x)$	$G_{e2}(x)$	x	$P(x)$	$G_n(x)$	$G_{e1}(x)$	$G_{e2}(x)$
1	0.104	0.094	0.094	0.094	13	0.032	0.030	0.036	0.033
2	0.094	0.085	0.085	0.085	14	0.029	0.027	0.026	0.030
3	0.085	0.077	0.077	0.077	15	0.026	0.024	0.029	0.028
4	0.077	0.069	0.069	0.069	16	0.024	0.022	0.027	0.026
5	0.070	0.064	0.079	0.071	17	0.021	0.022	0.024	0.025
6	0.063	0.055	0.057	0.063	18	0.019	0.025	0.022	0.023
7	0.057	0.055	0.065	0.058	19	0.018	0.028	0.020	0.020
8	0.052	0.055	0.047	0.053	20	0.016	0.026	0.018	0.018
9	0.047	0.054	0.053	0.048	21	0.014	0.021	0.017	0.017
10	0.042	0.050	0.038	0.043	22	0.013	0.015	0.015	0.016
11	0.038	0.043	0.044	0.039	23	0.012	0.012	0.014	0.015
12	0.035	0.034	0.031	0.035	24	0.011	0.011	0.013	0.013

的正常交易样本中加入 100 次隐蔽通信样本，设 G_{n} 为 $\mu_1=10$、$\mu_2=20$、$\sigma=2$ 的正态分布样本，G_{e1} 为一次 $\lambda=0.1$ 的指数分布样本，G_{e2} 为两次 $\lambda=0.1$ 的指数分布样本。

计算密文添加到正常序列后和正常序列的 K-L 散度计算结果如表 4 所示。

表 4　　K-L 散度计算结果

密文分布方式	K-L 散度
正态分布	0.016 4
一次指数分布	0.009 6
两次指数分布	0.005 8

经过调整后的交易间隔序列K-L散度低于常规正态分布的 60%，而加入两次指数分布后的密文序列 K-L 散度为正态分布的 35%，这和理论推导的结果相吻合，可证明调整交易间隔后的时间型隐蔽通信系统可以承受更高的交易间隔检测阈值，具有更好的抗检测性。

又因为使用多个地址来传输隐蔽信息，每个地址分配到一部分密文并且传输密文的长度相近。所以地址的交易间隔是独立同分布的，地址都满足以上的抗检测性能。而特殊地址的发起频率很低，不属于高频交易地址，故被检测的概率极低。

3.3　其他性能

1) 误码率。传统的隐蔽通信系统中因为网络波动或收发双方的误差，误码情况不可避免，因此提出了很多保证密文序列的方法。然而在区块链网络上实现隐蔽通信的方法中，使用的时间都指系统生成的区块时间戳。隐蔽通信的双方都可以读取时间戳信息，只需统计交易是否出现在区块中即可得到时间戳间隔信息，故传统意义上时间波动对区块链网络下的隐蔽通信影响很小，不存在因网络波动而导致密文误码的情况。

对于时间型区块链隐蔽通信而言，出现误码的情况为交易没有及时上链，导致表示密文的时间戳间隔改变，本文在第 2 节的描述中已经提到这种情况并且通过特殊地址暂停隐蔽通信等待重新开始的方法解决误码事件。

2) 获密时间。接收方从完成共识后的区块中获取密文的时间，由于区块的时间戳无须获取，接收方只需要遍历每个区块中地址是否存在，因此遍历的复杂度为 $O(n_{\mathrm{T}}n_{\mathrm{A}})$，其中，$n_{\mathrm{T}}$ 为一个区块包含的交易数量，n_{A} 为参与隐蔽通信的地址数量。地址 LSB 嵌入型利用特殊地址的标签机制[22]加速遍历的收敛，得到的复杂度为 $O(n_{\mathrm{T}}n_{\mathrm{L}})$，$n_{\mathrm{L}}$ 为标签地址的数量，然而地址嵌入型获密过程还包含了地址的解析，因此需要更多的计算资源，故时间型区块链隐蔽通信方法在获密时间上存在一定的优势。

3) 通信成本。在区块链系统中实现隐蔽通信具有更高的安全性但是也需要更多的通信成本，主要体现在交易费中，本文在性能测试中已经提出此问题，即使提高了时间型区块链隐蔽通信方法的传输速率，但是通信所产生的总交易费没有改变，若要减少通信成本只能采用更高效的编码方式，从而使一次交易可以承载更多的信息量。

4　结束语

针对时间型区块链隐蔽通信传输速率低的问题，本文提出了多地址时间型区块链隐蔽通信方法，由多个地址发起交易，这些交易可以指向任意地址，接收方由共识广播获取所有参与隐蔽通信地址的区块时间戳间隔，将间隔对照密文表转换为密文片段，组合后得到完整密文。

本文系统的传输速率随着参与隐蔽通信地址数量增加而提升，并且从交易接收地址、发起地址的出现次数和发起时间间隔 3 个方面降低了地址的特殊性。经统计得出比特币中同一个地址交易发起时间间隔近似为指数分布的规律，根据这个规律提出了一种调整地址发起交易间隔拟合为指数分布的方法，将密文序列对应的交易间隔加入正常交易序列中和正常序列对比，拟合后的序列具有更低的 K-L 散度，说明本文方法具有更好的抗检测性。

在未来工作中，笔者将结合时间型抗检测性强和空间型单次交易传输信息量大的优点实现混合型区块链隐蔽通信方法，在此基础上还可以探索时间和空间双通道的区块链隐蔽通信方法。

参考文献：

[1] 黄永峰, 李松斌. 网络隐蔽通信及其检测技术[M]. 北京: 清华大学出版社, 2016.
HUANG YF, LI S B. Network covert communication and its detection technology[M]. Beijing: Tsinghua University Press, 2016.

[2] 李彦峰, 丁丽萍, 吴敬征, 等. 网络隐蔽信道关键技术研究综述[J]. 软件学报, 2019, 30(8): 2470-2490.
LI Y F, DING L P, WU J Z, et al. Survey on key issues in networks covert channel[J]. Journal of Software, 2019, 30(8): 2470-2490.

[3] 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.
LIU A D, DU X H, WANG N, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[5] BUTERIN V. Ethereum white paper[J]. GitHub repository, 2013, 1: 22-23.

[6] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18.

[7] 宋上, 彭伟. BLOCCE+: 一种改进的基于区块链的隐蔽通信方法[J]. 重庆理工大学学报(自然科学), 2020, 34(9): 238-244.
SONG S, PENG W. BLOCCE +: an improved blockchain-based covert communication approach[J]. Journal of Chongqing University of Technology (Natural Science), 2020, 34(9): 238-244.

[8] ZHANG L J, ZHANG Z J, WANG W Z, et al. A covert communication method using special bitcoin addresses generated by vanitygen[J]. Computers, Materials & Continua, 2020, 65(1): 597-616.

[9] LIU S Y, FANG Z, GAO F, et al. Whispers on ethereum: blockchain-based covert data embedding schemes[C]//Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure. New York: ACM Press, 2020: 171-179.

[10] ZHANG L J, ZHANG Z J, JIN Z L, et al. An approach of covert communication based on the Ethereum whisper protocol in blockchain[J]. International Journal of Intelligent Systems, 2021, 36(2): 962-996.

[11] ZHANG L J, ZHANG Z J, WANG W Z, et al. Research on a covert communication model realized by using smart contracts in blockchain environment[J]. IEEE Systems Journal, 2022, 16(2): 2822-2833.

[12] 佘维, 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.

[13] BASUKI A I, ROSIYADI D. Joint transaction-image steganography for high capacity covert communication[C]//Proceedings of 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA). Piscataway: IEEE Press, 2020: 41-46.

[14] 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.

[15] TAHERI S, MAHDAVI M, MOGHIM N. A dynamic timing-storage covert channel in vehicular ad hoc networks[J]. Telecommunication Systems, 2018, 69(4): 415-429.

[16] WENDZEL S, KELLER J. Low-attention forwarding for mobile network covert channels[C]//Proceedings of the 12th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security. New York: ACM Press, 2011: 122-133.

[17] ZHANG X S, GUO L H, XUE Y, et al. A two-way VoLTE covert channel with feedback adaptive to mobile network environment[J]. IEEE Access, 2019, 7: 122214-122223.

[18] 黄冬艳, 李浪. 基于排队博弈的最优比特币交易费支付策略[J]. 计算机应用, 2020, 40(9): 2646-2649.
HUANG D Y, LI L. Optimal bitcoin transaction fee payment strategy based on queuing game[J]. Journal of Computer Applications, 2020, 40(9): 2646-2649.

[19] 熊礼治, 朱蓉, 付章杰. 基于交易构造和转发机制的区块链网络隐蔽通信方法[J]. 通信学报, 2022, 43(8): 176-187.
XIONG L Z, ZHU R, FU Z J. Covert communication method of blockchain network based on transaction construction and forwarding mechanism[J]. Journal on Communications, 2022, 43(8): 176-187.

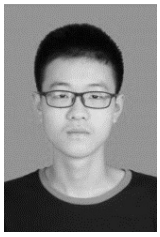
[20] 佘维, 荣欣鹏, 贾骏, 等. 区块链隐蔽通信的构建技术及检测方法研究综述[J]. 郑州大学学报(理学版), 2022, 54(6): 1-11.
SHE W, RONG X P, JIA J, et al. Technology development and research status of blockchain covert communication and detection methods[J]. Journal of Zhengzhou University (Natural Science Edition), 2022, 54(6): 1-11.

[21] 李凤华, 李超洋, 郭超, 等. 泛在网络环境下隐蔽通道关键技术研究综述[J]. 通信学报, 2022, 43(4): 186-201.
LI F H, LI C Y, GUO C, et al. Survey on key technologies of covert channel in ubiquitous network environment[J]. Journal on Communications, 2022, 43(4): 186-201.

[22] 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.

[作者简介]

黄冬艳（1984– ），女，广西南宁人，博士，桂林电子科技大学副教授、硕士生导师，主要研究方向为区块链技术、共识机制等。



李琨（1999– ），男，浙江绍兴人，桂林电子科技大学硕士生，主要研究方向为区块链技术、隐蔽通信等。