区块链网络隐蔽信道研究进展

李雷孝[1,2]，杜金泽[1,2]，林浩[3]，高昊昱[1]，杨艳艳[1]，高静[4]

（1. 内蒙古工业大学数据科学与应用学院，内蒙古 呼和浩特 010080；
2. 内蒙古自治区基于大数据的软件服务工程技术研究中心，内蒙古 呼和浩特 010080；
3. 天津理工大学计算机科学与工程学院，天津 300384；
4. 内蒙古农业大学计算机与信息工程学院，内蒙古 呼和浩特 010011）

摘 要：数字货币伴生的区块链技术具有去中心化、匿名性、强稳健性和抗篡改性等特点，是构建隐蔽通信信道的天然载体。首先介绍了网络隐蔽信道的定义和发展历史，区块链技术的架构，以及传统的网络隐蔽信道并引出了区块链网络隐蔽信道的优势；然后按照交易地址、签名算法、智能合约和 P2P 广播机制对区块链网络隐蔽信道进行分类，并从隐蔽性、传输效率和通信成本 3 个方面分析了其优缺点；最后提出了区块链网络隐蔽信道仍存在的问题并给出了未来研究方向。

关键词：网络隐蔽信道；隐蔽通信；区块链；传输效率；通信成本

中图分类号：TP309.2

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022146

Research progress of blockchain network covert channel

LI Leixiao[1,2], DU Jinze[1,2], LIN Hao[3], GAO Haoyu[1], YANG Yanyan[1], GAO Jing[4]

1. College of Data Science and Application, Inner Mongolia University of Technology, Hohhot 010080, China
2. Inner Mongolia Autonomous Region Software Service Engineering Technology Research Center Based on Big Data, Hohhot 010080, China
3. College of Computer Science and Engineering, Tianjing University of Technology, Tianjin 300384, China
4. College of Computer and Information Engineering, Inner Mongolia Agricultural University, Hohhot 010011, China

Abstract: Characterized by decentration, anonymity, strong robustness and tamper resistance, blockchain accompanied by digital currency is a natural carrier for building the covert communication channel. First, the definition and development history of the network covert channel, the framework of blockchain technology and the traditional network covert channel were introduced and the advantages of the channel in the blockchain were given. Thus, the channel in blockchain was classified on the basis of transaction address, signature algorithm, smart contract and P2P broadcast mechanism. The merits and demerits were analyzed in terms of crypticity, transmission efficiency, and communication costs. Lastly, problems and the future research direction of the network covert channel in blockchain were presented.

Keywords: network covert channel, covert communication, blockchain, transmission efficiency, communication cost

收稿日期：2022−04−02；**修回日期：**2022−06−28

通信作者：杜金泽，865416133@qq.com

基金项目：内蒙古自治区科技成果转化专项资金资助项目（No.2021CG0033, No.2020CG0073）；内蒙古自治区重点研发与成果转化计划基金资助项目（No.2022YFSJ0013）；内蒙古自治区研究生科研创新基金资助项目（No.S20210194Z）；内蒙古自治区高等学校青年科技英才支持计划基金资助项目（No.NJYT22084）

Foundation Items: The Fund Project for Transformation of Scientific and Technological Achievements of Inner Mongolia of China (No.2021CG0033, No.2020CG0073), The Key Research and Development and Transformation of Technological Program of Inner Mongolia of China (No.2022YFSJ0013), Postgraduate Scientific Research Innovation Project of Inner Mongolia of China (No.S20210194Z), Research Program for Young Talents From Inner Mongolia Colleges of China (No.NJYT22084)

0 引言

随着信息技术的发展，其安全传输问题受到广泛关注。虽然日益完善的密码学加密技术可对信息明文加密，避免被攻击者直接破解信息内容。但是对信息安全传输需求最大的群体通常是存在对立关系的群体。只要检测到通信过程的发生，就足以意识到某些信息已经被传递。在此情形下，研究者开始构建隐蔽信道来实现隐蔽通信。隐蔽通信就是把信息嵌入按照常规状态进行传输的公开载体上，使第三方从根本上无法察觉通信的发生。

最初，研究者更侧重于研究本地隐蔽信道，即可用于将数据从同一系统上的高安全级别进程传递到低安全级别进程的隐蔽信道[1]。随着20世纪90年代计算机网络的兴起，大量不同网络协议中附带的数据成为隐蔽信道的高带宽载体，仅一个大型互联网网站每年可作为载体的数据就多达26 GB[1]。但是该类隐蔽信道大多数以分布式计算机网络系统为载体，构建传统网络隐蔽信道的方法存在着很多问题。首先，信息传输载体由一个中心化的第三方机构提供，通信双方所处环境不是完全可信的，无法保证通信双方匿名性；其次，遭到分布式拒绝服务（DDoS, distributed denial of service）攻击时容易造成载体崩溃，中断通信；此外，现有传统网络隐蔽信道的通信双方大多是直接通信，采用的通信信道固定单一，容易被已有探测手段针对性探测。而最初作为比特币底层机制引入的区块链技术[2]具有去中心化、匿名性、不可篡改性和强稳健性等特点，可以被用来解决上述问题，是更好的构建网络隐蔽信道的载体。

目前，国内外学者和研究机构对网络隐蔽信道进行了分类与综述[3-6]，论述了网络隐蔽信道的分类原理与构建过程，并提出了检测隐蔽信道的方法。但是，现有研究缺乏对区块链网络环境下的隐蔽信道的综述分析，对该类型的信道构建尚处在初始阶段。

为提升对区块链网络隐蔽信道的研究，并为学者提供研究思路，本文在已有综述的基础上，首先，概括了区块链技术和网络隐蔽信道的发展，引出了区块链网络隐蔽信道的优点；其次，将区块链网络隐蔽信道按照构建载体的不同，分为交易地址型、签名算法型、智能合约型和P2P广播机制型4类，总结了每种类型的构建方法；再次，将区块链网络隐蔽信道构建过程定义为隐秘信息嵌入、载体混淆传输、特殊载体筛选和隐秘信息解码4个步骤，并分析了其中的关键技术；最后，总结了现有区块链网络隐蔽信道存在的问题并给出了解决方法。

1 网络隐蔽信道相关概念与发展

1.1 区块链技术

区块链技术是利用块链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全性、利用由自动化脚本代码组成的智能合约来操作数据的一种全新分布式基础架构。区块链架构如图1所示。

1.2 网络隐蔽信道定义和历史

隐蔽信道作为信息隐藏技术的一个分支[7]，最初是由Lampson[8]在1973年基于单片机系统的背景下给出的定义，即根本不用于信息传输的通道。相比于隐写术、匿名通信、版权标识这3种信息隐藏技术，隐蔽信道更注重于隐藏信道本身的存在，用来保证隐秘信息的安全传输。1984年，Simmons[9]首次提出囚犯问题来定义隐蔽信道：在看守人Wendy察觉Alice和Bob有越狱想法，且愿意让二人传递消息的环境下，Alice和Bob需要寻找一种在交流中秘密沟通的方式来欺骗Wendy，即众目睽睽之下建立一个“潜意识通道”——隐蔽信道。Craver[10]对囚犯问题进行了拓展，区分了3种不同类型的看守人。积极的看守人被允许在囚犯之间传递信息时进行同义词替换，但不能修改语义内容；消极的看守人能发现隐蔽信道但不能做任何修改；恶意的看守人可以任意修改信息。在此背景下，构建隐蔽信道需考虑更多的因素。Millen[11]在总结和分析后，将应用于网络环境中的隐蔽信道定义为网络隐蔽信道。

隐蔽信道发展过程如图2所示。在加密传输通信的安全性无法满足需求后，研究者将隐蔽信道构建在同一本地系统中，由高安全级别的进程传递到低安全级别的进程。虽然提高了通信的隐蔽性，但是本地隐蔽信道有很大的范围局限性，不能满足远距离传输。之后，Handel等[12]首次将囚犯问题扩展到计算机网络中，构建网络隐蔽信道，成为研究者的主要方向。早期提出的大多为存储型网络隐蔽信道，例如Cauich等[13]利用IP报头构建了隐蔽信道、Girling[14]接连发现了3种局域网上的隐蔽信道、Rowland[15]将IPv4报头和IP报头中未使用的冗余字段作为构建隐蔽信道的载体，但此类型信道在易被使用的同时也易被检测。1989年，Wolf[16]提出了

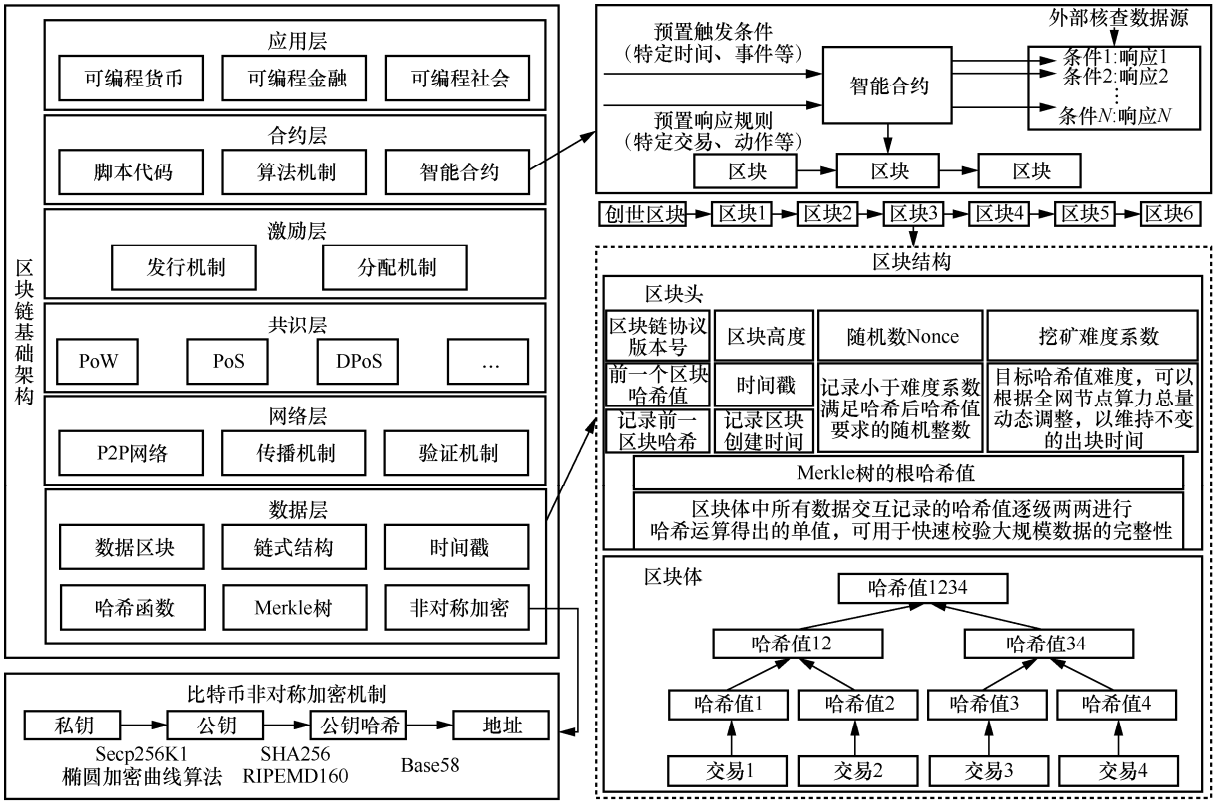

图 1　区块链架构

基于消息确认的时间型网络隐蔽信道，为隐蔽信道的构建提供了一种新思路。虽然此类信道易被噪声干扰，但是也更难被检测和消除。之后为了兼顾信道容量和隐蔽性，研究者构建了将 2 种类型信道结合的混合型新型隐蔽信道[17]。在 2018 年 Partala[18] 首次构建了区块链网络隐蔽信道后，一个规模巨大的新型网络环境被更多研究者关注[19]，隐蔽信道的构建有了更多样化的选择。

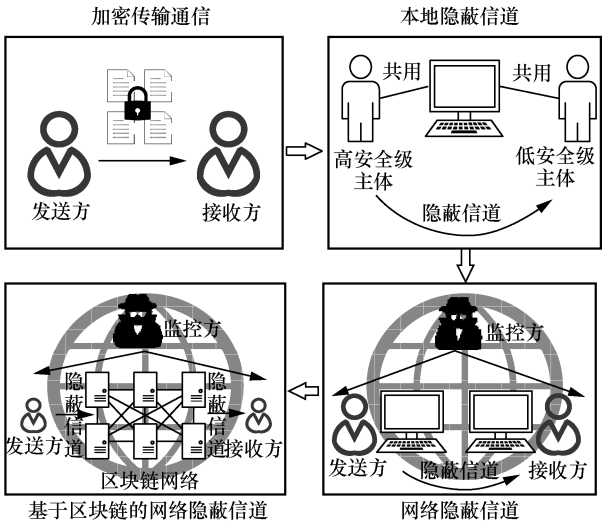

图 2　隐蔽信道发展过程

1.3　传统网络隐蔽信道和新型网络隐蔽信道

目前，国内外将传统网络隐蔽信道按照信息编码方式分为存储型网络隐蔽信道、时间型网络隐蔽信道和混合型网络隐蔽信道三大类[3-4]。

存储型网络隐蔽信道利用头元素或协议数据单元（PDU, protocol data unit）的空间特性，例如通过修改字段长度[20-21]、字段位置[22-23]和字段值[24-26]来编码隐秘信息，或利用冗余字段即在给定头元素或 PDU 中创建用于隐藏数据的空间[27-28]；时间型网络隐蔽信道通过调整数据包的时间特性将隐秘信息编入其中，例如通过发送数据包本身具有的时间差异[29-30]或利用网络环境时延的不同[31-32]来编码隐秘信息；混合型网络隐蔽信道是存储型和时间型网络隐蔽信道方法的结合[17,33-34]，针对存储型网络隐蔽信道不稳定和时间型网络隐蔽信道效率低的问题，混合型网络隐蔽信道在空间和时间特性中都编码隐秘信息，不会被单一的信道检测方法完全检测到，提升了隐蔽性和传输效率。

虽然存储型、时间型和混合型网络隐蔽信道方法越来越完善，但是仍存在着以下弊端。

1) 存储型网络隐蔽信道修改的字段分组长度

不同于正常业务的分组长度，经分析易被检测。并且在传输大量数据的情况下，难以在隐蔽性和传输效率之间保持平衡。

2) 时间型网络隐蔽信道的稳定性较低，通信过程需要保证双方的网络状态同步。而网络环境本身就存在着各种噪声，影响时间间隔，还易受到网络干扰[35]，监控者可发动大量请求破坏通信。

3) 以类似于浏览器的中心化第三方软件作为载体时，攻击者不需要检测信道本身，而是选择直接检测第三方软件，易发现通信过程的存在。

4) 稳健性较低，绝大多数采用通信双方直接通信的方式。出现单点故障的可能性高，针对性的检测也较为容易。在遭遇 DDoS 攻击时容易造成网络拥堵或目标系统服务器停止响应，中断通信。

5) 通信双方的匿名性较难保证，用户的身份标识都是基于第三方认证中心颁发数字证书确认的，通信双方的身份容易泄露。

而作为新型载体的区块链网络隐蔽信道具有以下几个特点，在一定程度上解决了上述问题。

1) 去中心化。区块链所有数据的存储、传输和验证过程均基于分布式的点对点系统架构，不依赖任何一个中心化机构。所有的节点都是单独存在的个体并且遍布全球各地，每个节点都可以作为发送方和接收方，其余所有节点都将是隐蔽通信的掩护者。

2) 匿名性。区块链系统采用公钥编码而成的地址作为用户的身份标识，不需要中心化机构颁发数字证书来确认身份。用户只需要公开可随意变换的地址，不需要公开真实身份。

3) 不可篡改性。区块链的链式存储结构和各种密码学算法保证了其内容的不可篡改性。

4) 强稳健性。区块头中的时间戳技术和区块链的复制状态机特性使区块链网络环境的时间特性不受网络波动的影响，对通信双方的网络环境要求较低。并且，区块链网络天然防止 DDoS 攻击，在实际环境当中，推翻之前的区块数据所需要的算力和时间成本远大于收益。此外，其 P2P 网络的架构也远安全于传统网络环境，破坏任一节点也不会影响整个系统的状态信息，防单点故障的能力强。

5) 开源性。可免费加入开源可编程的区块链网络，数据和程序对所有人公开。其开放性和多样性将使区块链有更多的隐蔽信道构建方式。

2 区块链网络隐蔽信道

本文将区块链网络隐蔽信道定义为利用区块链环境所独有的载体特征，构建无法被检测到的通信信道。将载体特征按照交易地址、签名算法、智能合约和 P2P 广播机制 4 种类型进行分类，依照隐蔽性、传输效率和通信成本 3 种评价指标进行对比分析。此外，总结性地提出了区块链隐蔽信道模型的构建过程。最后，提出了该类型信道存在的问题。

2.1 区块链网络隐蔽信道分类

2.1.1 交易地址型

该类隐蔽信道将区块链中的交易地址作为载体特征。交易地址由唯一的公私钥对编码而成，例如图 1 中比特币的交易地址生成过程。在通信过程中，根据不同的公私钥对生成不同的交易地址来作为隐秘信息的载体编码或传输，其构建过程如下。

将明文 M 按照预共享编码规则 C 编码为可用作传输的密文 M'，如式(1)所示。

$$M \xrightarrow{C} M' = (m_1, m_2, \cdots, m_n) \xrightarrow{C} (m_1', m_2', \cdots, m_n') \tag{1}$$

将密文 M' 编码入交易地址 T_A 经过通信双方预共享的规则 E 重新排序或经过密码学算法 U 重新生成的交易地址 T_A' 中，形成含有隐秘信息的有限地址集合 T_A''，如式(2)和式(3)所示。

$$T_A \xrightarrow[U]{E} T_A' = (T_A^1, T_A^2, \cdots, T_A^n) \xrightarrow[U]{E} (T_A^{1'}, T_A^{2'}, \cdots, T_A^{n'}) \tag{2}$$

$$T_A'' = T_A' + M' = \{(T_A^{1'}, m_1), (T_A^{2'}, m_2), \cdots, (T_A^{n'}, m_n)\} \tag{3}$$

隐蔽通信发送方 S 生成交易地址为 T_A'' 的交易至区块链公链中。接收方 P 利用规则 E 或算法 U 将 T_A'' 从区块链公链中筛选出来，并提取出密文 M'，之后利用规则 C 进行解码，从而得到明文 M，如式(4)和式(5)所示。

$$S \xrightarrow{T_A''} P \rightarrow \text{Blockchain} \tag{4}$$

$$P \xrightarrow[U]{E} T_A'' \rightarrow M' \xrightarrow{C} M \tag{5}$$

利用上述过程，文献[18]提出 BLOCCE 区块链网络隐蔽信道，文献[36]在 BLOCCE 的基础上做出改进，文献[37]利用同样的思路，使用地址生成软件 Vanitygen 的 V-BLOCCE 方法。BLOCCE 系列直接将隐秘信息显示在地址的有效位中，3 种方法对应的流程如图 3 所示，其改进过程与优缺点分析如表 1 所示。

不同于 BLOCCE 系列将隐秘信息直接映射至交易地址，文献[39]直接利用特殊地址生成算法编

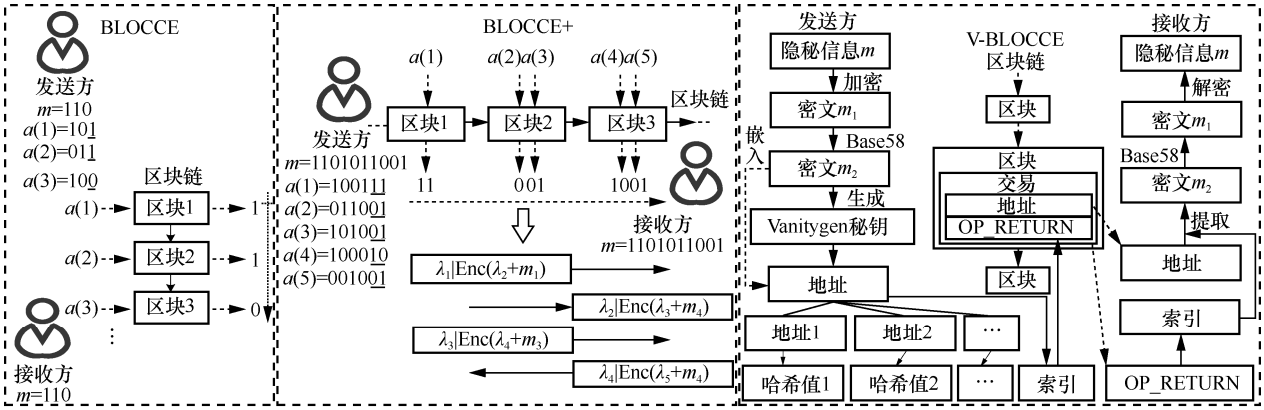

图 3　3 种方法对应的流程

表 1　　**3 种方法改进过程与优缺点分析**

方法名	特点	存在问题
BLOCCE	发送方生成多个支付地址，支付地址的最低有效位（LSB, least significant bit）按顺序与加密后的隐秘信息组合相映射，设定信息开始符作为通信开始的标志，按顺序向区块链广播交易	①发送方随机生成的地址要匹配编码后信息的 LSB 或低 α 位，所用时间成本并未考虑 ②通信开始前节点有意外生成信息开始符的可能，误以为通信开始；并且在网络时延或交易费用大小不同的情况下，交易不一定会按提交顺序被打包到某个特定的区块，接收方接收的隐秘信息可能是混乱的 ③没有提取特殊交易的筛选方法，需要遍历区块中的全部交易，效率极低
BLOCCE+	较之 BLOCCE 每次通信都需要传递信息开始符，该方法将隐秘信息和信息开始符一起编码，前一次通信就传递了下一次的信息开始符，减少了过多的信息传递，提升了隐蔽性；将原有对 LSB 的信息嵌入改为对地址的低 α 位信息嵌入，在同一区块中打包入多笔交易	
V-BLOCCE	Vanitygen 可以随机生成符合要求的地址，并且可以准确搜索特定前缀、后缀或常规匹配的地址，信息嵌入地址中的速度加快；采用 Base58 编码方式代替二进制编码，嵌入的信息量是 BLOCCE 的 lb58 倍；地址序列索引信息加密后写入交易的 OP_RETURN 字段，不需要按交易提交的顺序打包入区块	每笔交易只有一个 OP_RETURN 字段，如果隐秘信息较长，需将索引写入多个 OP_RETURN 字段。而该字段使用率只占比特币交易的极少部分[38]，如果连续多个 OP_RETURN 字段都含有特殊内容，易被检测

码信息。将需要嵌入的二进制隐秘信息与预共享密钥融合产生新的公钥，根据公钥生成交易地址作为载体传输隐秘信息。接收方只需要根据交易地址判断公钥与输出的关系就可以判断是否含有隐秘信息并解码。并且将前一个交易的输出作为下一个交易的输入，不需要遍历所有交易即可筛选出特殊地址，提升了效率。虽然该方法中每个地址只能嵌入 1 bit 信息，但是将隐秘信息直接与交易地址相结合地址的方法提升了隐蔽性。文献[40]按照交易时间的先后生成交易地址索引矩阵，对编码隐秘信息的交易金额进行排序并解码。该方法使用金额编码隐秘信息，增加了单笔交易可嵌入信息的容量，减少了交易数量，提高了传输效率。并且交易地址索引矩阵提供了筛选方法，不需要遍历全部交易，筛选效率更高。但是该方法反复利用一个通信双方都知晓的地址集进行交易，通过交易地址关联分析的方法就能够溯源到通信双方，破坏信道的隐蔽性。

此外，相比于上述基于固定地址的筛选机制，交易地址结合动态标签生成特殊交易地址的设定更好地兼顾了筛选效率和隐蔽性。文献[41]用不断变化的区块高度作为动态标签，与预共享的密钥使用哈希运算消息认证码（HMAC, Hash-based message authentication code）生成新的私钥，并生成含有特殊交易的交易地址，保证了只有持有预共享密钥的通信双方才能提取信息；文献[42]基于 OP_RETURN 字段上真实的交易数据统计分布，结合域生成算法生成含有动态标签的特殊地址；文献[43]则利用前一个区块的区块号和 Nonce 值来生成动态标签。

2.1.2　签名算法型

该类隐蔽信道将区块链中的数字签名算法作为载体特征。在区块链中，每笔交易都会由交易双方对其进行数字签名，来保证数据不被篡改且交易双方身份真实可靠。签名算法型隐蔽信道构建过程如图 4 所示，只有接收方使用私钥才能从修改后的特殊签名算法中得到发送方私钥并提取隐秘信息。另一种则是与交易地址型构建过程类似，将签名算法本身作为隐秘信息的存储载体（如数字签名中的某一有效位）进行传输。

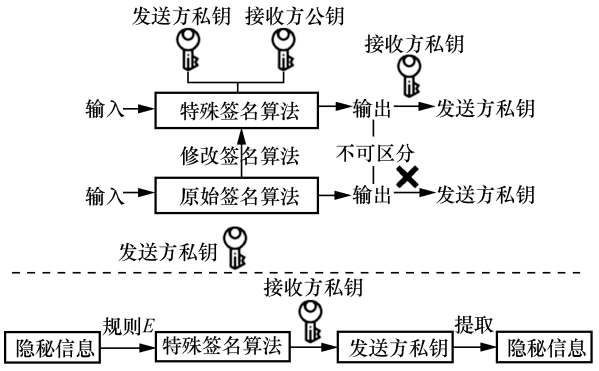

图 4 签名算法型隐蔽信道构建过程

文献[44]最先提出了构建签名算法型隐蔽信道的模型。文献[45]给出了具体的方法，即利用窃密算法修改区块链中原有的签名算法构建信道。利用区块链官方客户端开源代码设计特殊数据发送客户端和特殊数据接收客户端进行信息传输，发送客户端对含有隐秘信息的交易中的签名算法进行修改，接收客户端用窃密算法检测和筛选含有隐秘信息的交易并提取信息。只有知晓窃密算法关键信息的节点才可提取出私钥，并解码隐秘信息。该方法生成每笔交易所用的时间比生成普通交易所用的时间只增加 36 ms，并无显著差异。文献[46]通过修改比特币中交易的椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm），在僵尸网络场景中构建了隐蔽信道。文献[47]和文献[48]结合门罗币环签名技术，利用环签名技术的特性构建隐蔽信道的同时提升了匿名性。

2.1.3 智能合约型

该类隐蔽信道将区块链的智能合约作为载体特征。智能合约种类的丰富性、参数的多样性、数据的冗余性和代码的可编程性等特点，使其成为构建隐蔽信道的优秀载体。智能合约型隐蔽信道构建过程如图 5 所示，发送方将隐秘信息编码入智能合约的预置触发条件和预置响应规则当中，接收方依据不同的响应解码不同的隐秘信息。

文献[49]利用智能合约作为传感器网关并结合图像隐写术实现隐蔽通信。将包含分区号、访问时间和图像地址的说明手册嵌入智能合约事务的时间戳当中，接收方依据预共享信息从合约中进行提取。其中，分区号即多播传递的接收者数量，访问时间即隐写图像的时效性，图像网址即隐写图像位置。该方法利用智能合约作为载体结合图像隐写术，信道容量较高。说明手册中的访问时间使隐秘信息不会永久保存在区块链中，提升了信道的隐蔽性。文献[50]则利用投票合约中选项的不同和投标合约中出价数目的不同映射秘密信息序列，之后调用合约传递信息。投票合约中，增设多项选择和冗余选择，提高了信息编码复杂度的同时也提高了信息传输效率。投标合约中，通过设置单节点有效投标价格范围提高筛选效率，并允许提出含有多个有效投标的集合，减少交易数量，提升传输效率。

2.1.4 P2P 广播机制型

该类隐蔽信道将区块链的 P2P 广播机制作为载体特征，是区块链各节点之间通过泛洪模式迭代转发并经过滤后的区块数据和交易信息体系下的网络隐蔽信道。一方面通过空间特性，利用 P2P 广播机制转发过程，修改数据中的字段或利用冗余字段添加内容来编码隐秘信息构建隐蔽信道的方法。另一方面通过时间特性，利用交易转发的时间间隔以及转发数据的时延编码隐秘信息构建隐蔽信道的方法。

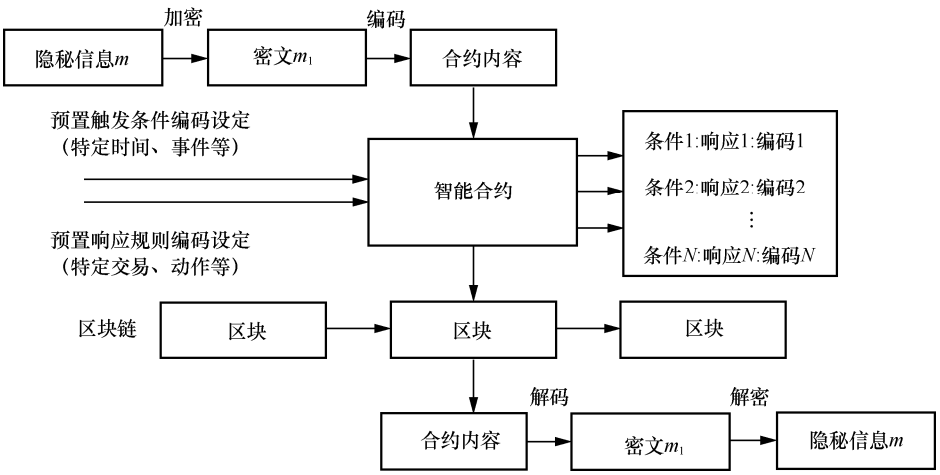

图 5 智能合约型隐蔽信道构建过程

在利用空间特性的方法中，文献[51]基于图 6 的比特币交易广播机制，首先将 A 节点加密后的隐秘信息编码入 coinbase 字段，将其哈希值作为索引，插入 inv 消息和 getdata 消息所共有的清单向量，用于告知其他节点本节点拥有对象或请求数据。B 节点收到 inv 消息后，依据索引搜索节点交易消息中是否存在相等的交易哈希值。若存在，则找到该交易的 coinbase 字段提取并解码信息，然后将过滤后的 getdata 消息返回给 A 节点；若不存在，则将包含索引的 getdata 消息返回给 A 节点，代表未曾完成通信。不过将隐秘信息编码入本身使用率就较低且每 10 min 产生一个的 coinbase 字段，影响了信道的传输效率和隐蔽性。此外，该文献还利用比特币节点之间通过 TCP 三次握手建立连接向邻居节点发送地址广播的机制，依据地址广播的顺序是否正确编码二进制隐秘信息，构建隐蔽信道。

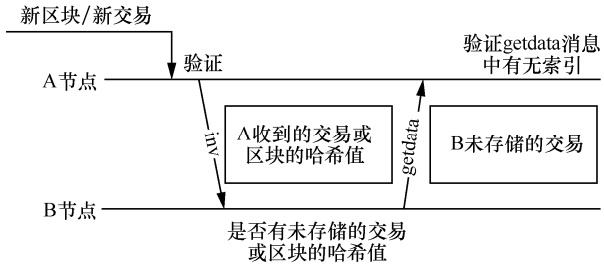

图 6　比特币交易广播机制

文献[52]提出利用以太坊 Whisper 协议构建隐蔽信道的模型，文献[53]和文献[54]在此基础上给出了基于 Whisper 协议的隐蔽信道模型，如图 7 所示。该方法有很多优点：Whisper 协议信件的信封中设有最晚有效时间和存活时间，过期作废不永久保存，提高信道隐蔽性；采用类似于比特币挖矿机制寻找

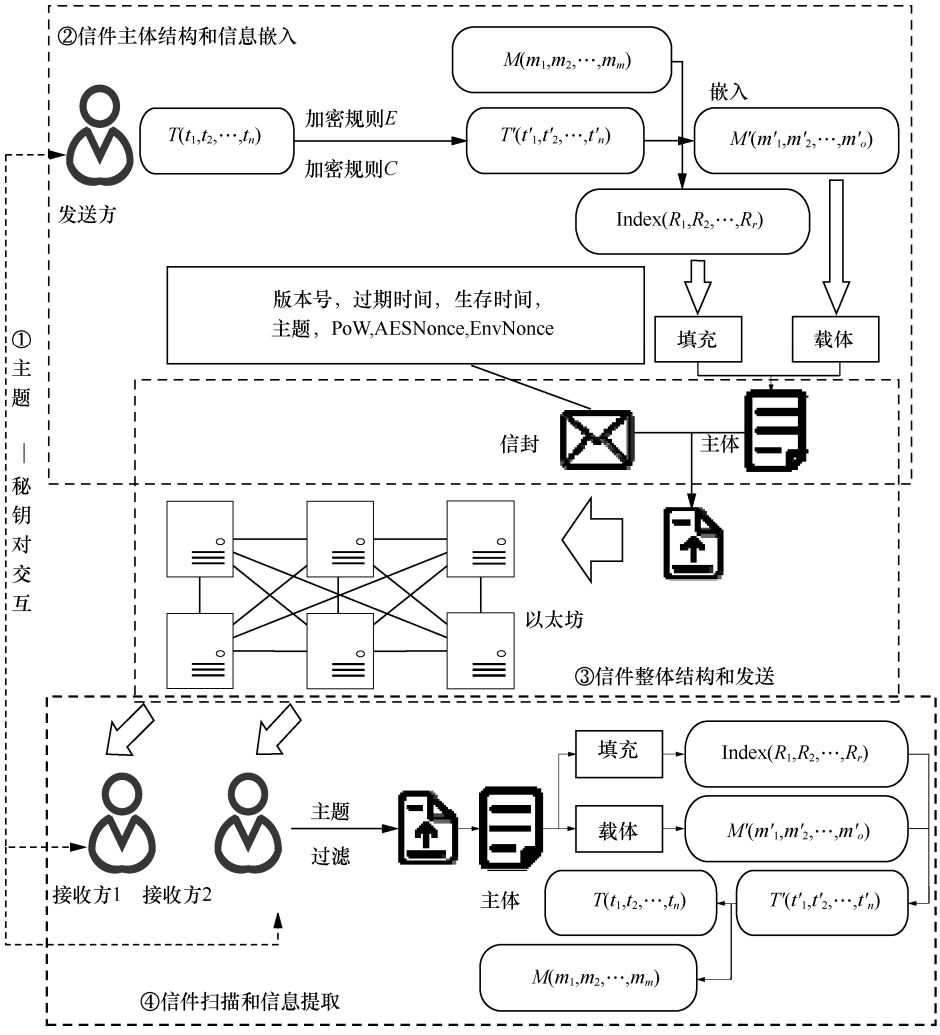

图 7　基于 Whisper 协议的隐蔽信道模型

Nonce 值的方法设定阈值，只有当节点发送消息的阈值超过特定阈值时，才可在以太坊网络中继续转发，还能将连续发送不符合要求的节点列入黑名单，避免了第三方的干扰；利用特殊编码的主题字段过滤无关内容，提升了筛选效率。除了以太坊中的 Whisper 协议之外，文献[55]在比特币中利用同为 P2P 广播机制的 Gossip 协议，通过使用一种基于比特币的审查弹性客户端 Tithonus 构建了隐蔽信道。

文献[56]则利用广播机制中的时间特性，构建了一种基于多节点时间戳共谋的区块链网络隐蔽信道[57]，其模型如图 8 所示。将隐秘信息映射为不同的区块链业务操作的时间间隔，与唯一标识序列构成集合后发送，信息接收方利用预先设定的方法辨别唯一性标识的节点，提取并解码隐秘信息。文献[58]结合具体应用场景，利用区块链业务的时间间隔是否超过阈值来编码授权信息，并用此技术保证智能电网中用户授权有效性。这 2 种利用 P2P 广播机制的时间特性编码隐秘信息的方法因区块链网络的时间戳功能受网络波动的影响较小，故在信道隐蔽性和稳健性方面都优于传统的时间型网络隐蔽信道。

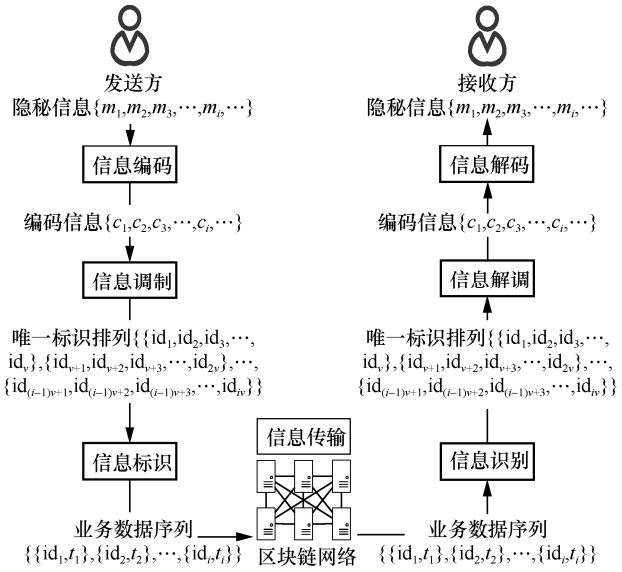

图 8 基于多节点时间戳共谋的隐蔽信道模型

2.2 区块链网络隐蔽信道评价指标和对比分析

结合传统网络隐蔽信道和上述 4 种不同类型的区块链网络隐蔽信道，本文总结了隐蔽性、传输效率和通信成本 3 种评价指标，并依据该评价指标对 4 种不同类型下的不同方法进行对比分析。

2.2.1 隐蔽性

区块链网络隐蔽信道中的隐蔽性一方面是信道的抗检测能力，另一方面是对通信双方匿名性的保护。

对于抗检测能力，可以使用 KL（Kullback-Leibler）距离评定，也叫作相对熵。该指标用于衡量相同事件空间中 2 个概率分布差异情况，即不包含携带隐秘信息的载体时满足的概率分布 $P(x)$ 与含有携带隐秘信息的载体时满足的概率分布 $Q(x)$ 的差异情况，用 $D(P\|Q)$ 表示，计算式如式(6)所示。由式(6)可得，当 2 种概率分布情况相似度越高时，$D(P\|Q)$ 越小，KL 距离越小，抗检测能力越大，隐蔽性越高。

$$D(P\|Q)=\sum_{x\in X}P(x)\mathrm{lb}\frac{P(x)}{Q(x)} \tag{6}$$

区块链网络环境下的隐蔽通信场景虽然对通信双方的匿名性的保护远高于传统网络隐蔽信道，但是仍存在攻击者通过交易关联分析、地址关联分析和身份关联分析来进行身份溯源。经过对区块链网络隐蔽信道构建方法的分析可知，采用固定交易数据的隐蔽信道匿名性低于采用动态交易数据的隐蔽信道匿名性，且交易数据动态变化越多，攻击者分析交易数据的关联性越困难，匿名性越强；固定交易数据的使用次数越多，攻击者分析交易数据的关联性越简单，匿名性越弱。

2.2.2 传输效率

区块链网络隐蔽信道的传输效率 V 指单位时间内传输的最大无错误信息量，单位为 bit/s，如式(7)所示。其中，C 代表最大无错误信息量，t 代表单位时间，单位时间内 C 越大，代表该类隐蔽信道的传输效率越高。

$$V=\frac{C}{t} \tag{7}$$

依据香农定律，当通信速率低于信道容量时，可使误差接近于零，即错误信息量最少。当通信速率无限接近于信道容量时，即传输的最大无错误信息量。因此，传输效率中的 C 可被构建该类隐蔽信道所产生的信道容量代替。通信信道是一个系统，系统的输出信号按概率依赖于输入信号，该系统特征由一个转移概率矩阵 $p(y|x)$ 决定，该矩阵决定在给定输入情况下输出的条件概率分布。对于输入信号 X 即明文，输出信号 Y 即编码对应的用于传输的密文，信道容量 C 定义为

$$C=\max_{p(x)}I(X;Y) \tag{8}$$

其中，$I(X;Y)$为互信息，如式(9)所示，是由另一随机变量导致的原随机变量不确定度（即信息熵）的缩减量，代表 2 个随机变量相互之间独立程度的度量，关于 X 和 Y 对称且永远非负。

$$I(X;Y)=H(X)-H(X\mid Y)=\sum_{x,y}p(x,y)\mathrm{lb}\frac{p(x,y)}{p(x),p(y)} \tag{9}$$

当随机变量 X 的概率密度函数为 $p(x)$ 时，将 X 的熵定义为 $H(X)$，如式(10)所示。其中，$p(i)$ 为第 i 个不同编码字符出现的概率密度分布。

$$H(X)=-\sum_{i}^{x}p(i)\mathrm{lb}p(i) \tag{10}$$

综上，可以计算出区块链网络隐蔽信道的传输速率 V。由上述过程可推得，在编码过程中，可通过增加更多数量的编码字符提高隐秘信息的传输速率，但需要满足编码的期望长度 $L(C)$ 大于或等于熵这一条件，如式(11)所示。其中，$l(x)$ 为对应于 x 的码字长度。

$$L(C)=\sum_{x\in X}p(x)l(x) \tag{11}$$

2.2.3　通信成本

区块链网络隐蔽信道的通信成本一方面是计算成本，另一方面是金钱成本。

对于计算成本，取决于信道构建的时间复杂度 $O(f(n))$，$O(f(n))$ 越高，计算成本就越高，且计算成本高低取决于式(12)。当存在特殊载体生成的过程中，就会产生不同的时间复杂度，例如生成特殊的地址、签名算法、智能合约和广播内容。

$$O(1)<O(\mathrm{lb}n)<O(n)<O(n\mathrm{lb}n)<O(n^2)<O(n^3)<\cdots<O(2^n)<O(n!) \tag{12}$$

在任何一条区块链公有链中构建隐蔽信道的过程中，产生交易数据的同时都会产生数量为 a、价值为 b 的某种币种，如比特币或以太币等。因此，对于金钱成本 S，即单位字节的传输成本，计算方法如式(13)所示。其中，C 表示信道容量。

$$S=\frac{ab}{C} \tag{13}$$

2.2.4　对比分析

对上述 4 种区块链网络隐蔽信道构建方法，依据隐蔽性、传输效率和通信成本 3 种评价指标进行分析，如表 2 所示。经分析可看出，现有基于区块链的网络隐蔽信道很难同时满足隐蔽性、传输效率和传输成本 3 种评价指标，在选择时要根据具体应用场景而定。

2.3　区块链网络隐蔽信道模型

通过对上述区块链网络隐蔽信道的论述并结合具体构建信道的方法，本文将此类型的区块链网络隐蔽信道构建模型定义为隐秘信息嵌入部分、载体混淆传输部分、特殊载体筛选部分和隐秘信息解码部分 4 个步骤，如图 9 所示。

表 2　　**基于区块链的网络隐蔽信道构建方法**

载体类型	文献	简要介绍	评价指标		
			隐蔽性	传输效率	通信成本
交易地址	文献[18]	利用地址的 LSB 编码信息，每次共享信息开始符	低	低	高
	文献[36]	利用地址的低 α 位编码信息并将信息开始符也编码入信息序列中	低	低	高
	文献[37]	base58 编码信息嵌入多个 Vanitygen 生成地址的 LSB，索引写入 OP_RETURN	低	中	中
	文献[39]	将信息直接编码入公钥中生成交易地址	高	低	高
	文献[40]	将交易金额矩阵与交易地址索引矩阵结合	中	中	高
签名算法	文献[45]	设计窃密算法生成特殊签名，只有信息接收方可提取交易	高	中	高
	文献[47]	利用门罗币环签名特性，将信息编码入环签名公钥集中	中	低	低
智能合约	文献[49]	依据图像隐写术编码信息并调用智能合约传递	低	高	低
	文献[50]	依据投票合约选项和投标合约价格的不同编码信息	中	中	低
P2P 广播机制	文献[51]	信息分片写入交易 coinbase 字段，利用交易广播机制建立联系传输交易	低	低	高
	文献[53-54]	利用以太坊 Whisper 协议传输信息	中	高	低
	文献[57]	基于时间间隔与节点唯一性标识符结合编码信息进行通信	高	低	低

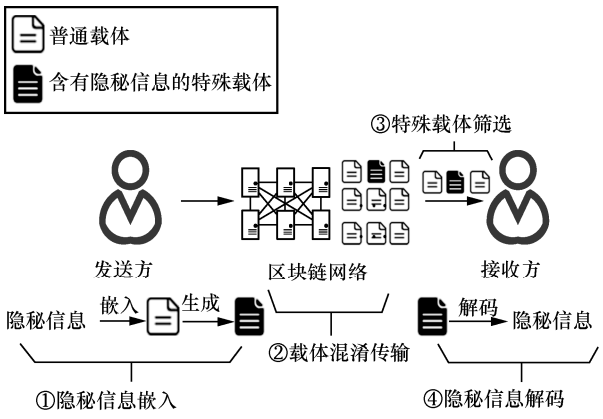

图 9 区块链网络隐蔽信道构建模型

隐秘信息嵌入部分是指发送方将隐秘信息编码并嵌入载体中，生成含有隐秘信息的特殊载体。通过对上述 4 种载体类型的隐蔽信道分析，将隐秘信息嵌入机制定义为显示嵌入和隐示嵌入 2 种，如表 3 所示。显示嵌入是隐秘信息直接嵌入载体的某一字段当中。由于区块链账本公开，第三方有足够的时间对所有数据进行分析，隐蔽性低。而隐示嵌入是通过特定的编码方式编码入载体，隐秘信息字符特征不体现在字段中，隐蔽性高于显示嵌入。

载体混淆传输部分是指发送方将含有隐秘信息的特殊载体按照普通载体的特征构建后混入普通载体当中，使监控方无法区分特殊载体和普通载体，达到隐蔽通信的效果。

特殊载体筛选部分是指接收方从区块链的大量信息中筛选出含有隐秘信息的特殊载体。由于区块链去中心化的特点，所有节点信息全部存储在区块链中，产生的数据量极大，筛选难度极高，因此设定合理的筛选机制十分重要。本文将特殊载体筛选机制分为基于固定标签的筛选和基于动态标签的筛选。基于固定标签地址的筛选效率较高，但是使用次数过多会使信道被发现的风险增加，影响其隐蔽性。而使用基于动态标签的筛选机制不需要反复使用相同内容，隐蔽性高于基于固定标签的筛选方法，但是每次通信接收方都需要重新筛选，传输效率低于基于固定标签的筛选方法，如表 4 所示。

隐秘信息解码部分是指接收方在筛选出特殊载体之后，按照最初信息编码的逆运算解码出原始的隐秘信息，也表示利用区块链网络隐蔽信道实现隐蔽通信的过程结束。在区块链网络隐蔽通信过程中，为使接收方顺利提取隐秘信息，通信双方不可避免地需要预共享一些信息。现有的研究大多是直接预设一个理想情况，即通信双方在绝对安全的环境下，进行有且仅有一次的预共享信息过程。但实际上预共享信息的过程所处环境的安全性也需要被考虑在内。后续的研究也可对预共享部分做严格分析设计，以此提升总体区块链网络隐蔽信道的隐蔽性。

表 3 区块链中隐秘信息嵌入机制

嵌入机制	嵌入机制描述	类型	信道容量	隐蔽性
LSB 方式	利用载体的最低有效位，例如 xxx1、xxx0	显示嵌入	1 bit	低
存储字段	载体本身字段，例如 OP_RETURN、输入输出字段	显示嵌入	80 byte，2 000 byte	低
金额字段	交易中的金额字段	显示嵌入	28 bit	低
直接写入	加密算法加密后直接写入载体，例如 Whisper 协议	显示嵌入	255 bit	低
特殊地址	通过哈希算法等方法生成特殊地址	隐示嵌入	1 bit	高
签名字段	嵌入数字签名算法中的随机数 k	隐示嵌入	255 bit	高
时间间隔	交易广播时间间隔区分隐秘信息	隐示嵌入	1 bit	高

表 4 区块链载体筛选机制

筛选机制	筛选机制描述	类型	传输效率	隐蔽性
固定地址	具体的某一固定地址	固定标签	高	低
固定存储字段	载体固定的字符串字段	固定标签	高	低
地址索引矩阵	预共享的地址索引矩阵	固定标签	高	低
环签名公钥集	门罗币环签名公钥集	固定标签	高	低
特殊地址	根据特殊算法计算而成	动态标签	低	高
动态区块高度	将交易的区块高度作为标签	动态标签	低	高
动态区块号	将交易的区块号作为标签	动态标签	低	高
动态地址链	将交易的输入输出连成链	动态标签	低	高

2.4　区块链网络隐蔽信道存在的问题

尽管区块链网络隐蔽信道有去中心化、匿名性、不可篡改性、强稳健性和开源性等优势[59]，但还是存在以下几点问题。

1）数据多副本。区块链中的数据被永久存储在链上，再加之其去中心化的特点，会被多个节点备份，从而增加隐蔽信道被发现的风险。此外，随着检测技术的不断更新，已完成的通信也会面临被重新检测到的风险。

2）身份易泄露。通信双方的匿名性是构建网络隐蔽信道需要考虑的重要因素。区块链存在假匿名性问题，第三方会利用区块链中完整的交易记录，通过交易关联分析、地址关联分析和身份关联分析三步对通信双方身份进行溯源。

3）信息难筛选。由于区块链中的一些交易可以不明确指定接收方账号，显著增加了接收方的识别难度。并且公链中同一时刻交易众多，遍历全部交易筛选的过程十分困难。

4）性能难兼顾。去中心化、安全和高性能 3 个特征构成了区块链技术的“不可能三角”。同样，区块链网络隐蔽信道构建也存在着隐蔽性、传输效率和通信成本三者的“不可能三角”，如图 10 所示。3 个特征无法同时满足，需要结合实际通信场景进行取舍。

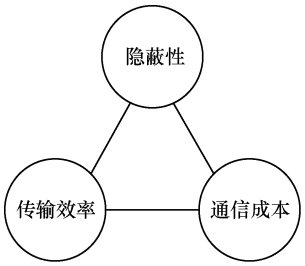

图 10　区块链网络隐蔽信道的“不可能三角”

3　网络隐蔽信道未来研究方向

通过上述论述的内容，对现有区块链网络隐蔽信道构建方法所存在问题，针对性地提出解决方法，给出未来研究思路。

3.1　利用混币技术

针对身份易泄露问题，可以采用混币技术提升通信双方的匿名性，进而提升隐蔽信道的隐蔽性。

最初 Meiklejohn[60]提出了混币方案 CoinJoin，即将金额相等的交易混淆，每个接收地址可以接收任意一个交易输入，提供了外部不可关联性。达世币就是一种基于混币思想[61]以隐私为中心的公有链。利用 PrivateSend 随机选取主节点进行交易混淆，允许前一轮的交易输出作为下一轮的交易输入。通信双方经过多轮混淆交易之后，参与的用户数量呈指数上升，很难再找到联系。此外，达世币不需要等待特定时间来确认区块中的交易，只需要几秒就可以完成一笔交易，且交易无论发送的金额是多少，费用都极低。所以，未来的研究可以将构建隐蔽信道的方法在达世币公有链中应用，以此来保证通信双方的匿名性。

3.2　利用扩容方案

目前，诸如比特币或以太坊等公有链都存在低吞吐量的问题。对于在隐蔽通信过程中对时效性要求较高的场景来说，并不能满足需求。对此，本文按照链下、链上 2 种扩容方法给出了提升传输效率的思路。

3.2.1　链下方案

作为链下方案的一种，比特币侧链技术的发展为隐蔽信道的构建提供了天然载体。其定义是可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。现有侧链技术中的 RSK（rootstock）[62]、闪电网络或者元素链都可以很好地提升传输效率。以元素链为例，其隐蔽性和信息传输效率相比于比特币有很大提高，并且具有以下特点。

1) 私密交易。通过在地址中加入盲化因子，使原有比特币交易地址变成特殊的私密地址，并在金额中加入仅有交易参与者知道的盲化因子隐藏交易金额，为区块链网络隐蔽信道的构建提供了更好的隐蔽性。

2) 签名验证。采用 Schnorr 签名方案，使区块链存储和带宽减少至少 25%，支持批量验证，速度更快，效率更高。

3) 隔离见证。将签名环节从交易中提取出来，减少了交易的大小，使区块中可以打包更多的交易，提升了隐蔽信道传输效率。同时解决了任何已知形式的交易可塑性问题，避免了攻击者在比特币中利用交易可塑性修改交易 ID，替换原有正常交易，破坏隐蔽通信过程。

3.2.2　链上方案

除侧链技术外，还可以利用基于有向无环图（DAG, directed acyclic graph）的链上扩容方案，提升隐蔽信道的传输效率。

同为分布式账本的 IOTA 与区块链技术是 2 种

完全独立的架构，却建立在同一种规则之上。IOTA 拥有如下几个优点，使其成为天然的构建隐蔽通信信道的载体。

1) 不同于区块链的链式结构，IOTA 是一种基于 DAG 的拓扑结构。允许无限的可扩展性，整个系统可以同时验证多笔交易，实现较高吞吐量。单位时间内交易数量增多，可嵌入信息增多，传输效率更高。

2) 区块链中的交易需要被验证并且打包入下一个区块，并且需要支付手续费。而 IOTA 每一个节点都可以发起和确认交易，不需要支付手续费，隐蔽通信成本低。区块链中较为突兀的小额交易在 IOTA 中完全适用，利用金额作为载体构建信道的方法更加可行。

3) IOTA 的全节点会定期删除大部分交易记录，只保留账本中最近发生的事件。节点在通信过后会删除之前用于通信的特殊交易，达到提高信道隐蔽性的目的。

4) IOTA 中交易的发布需要验证 2 个旧的交易，并且可以查询到哪些交易确定了该交易，降低了筛选过程难度，提升了传输效率。

3.3　利用链下信息编码

针对数据多副本问题，可以利用区块链中无法永久存储或无法查询的链下信息作为载体构建信道。

在区块链网络中，不断有新的交易广播，交易顺序是实时变化的，且当下的顺序过期不可见。本文提出发送方通过调制交易广播顺序来编码信息的方法，如图 11 所示。其中的编码规则是多样的，本文将两笔交易划分为一组，按照交易地址最后一位是数字还是字母的方式组合编码。本文提出的模型只是提供一种方向，采用了较简单的编码方式。后续研究可根据信道传输效率，增加参与信息编码地址的位数，提高编码的复杂性。该方案不仅具有数据不永久存储、可抵抗数据分析攻击的特点，而且交易广播时间远小于交易上链时间，通信效率高。

3.4　利用密码学算法特点

区块链技术本就使用了大量的密码学技术，保证账本的完整性、公开性、不可篡改性和隐私保护等特性。在隐蔽信道的构建过程中，可以与密码学算法特性相结合，增加信道的隐蔽性。本文提出基

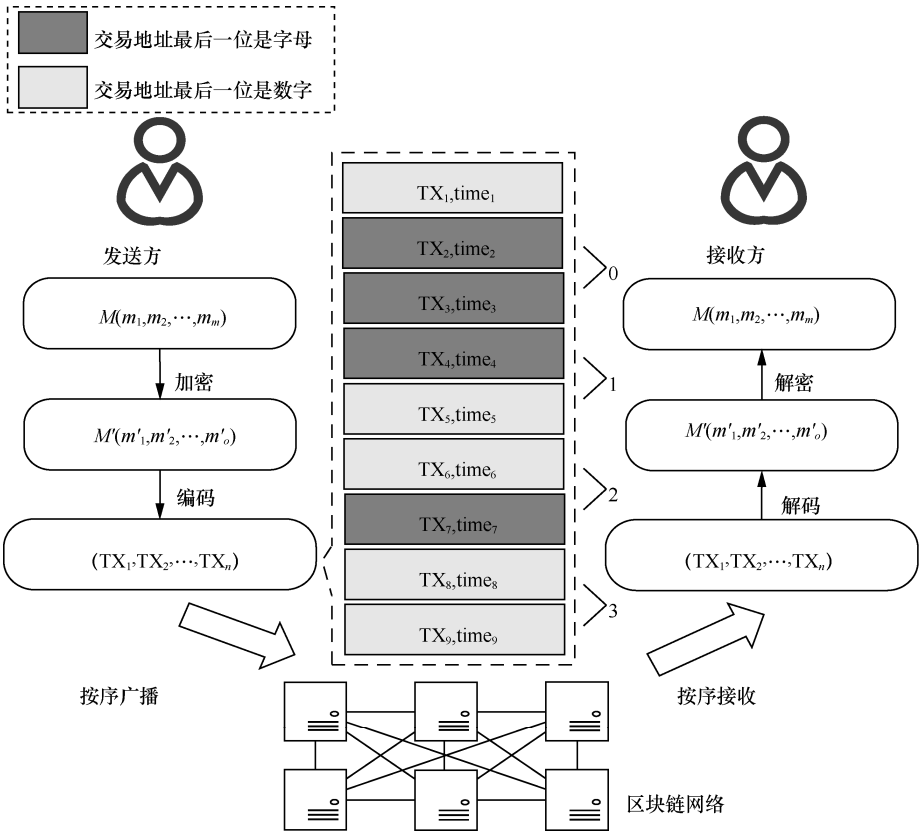

图 11　基于交易广播顺序的隐蔽通信模型

于可验证延迟函数（VDF, verifiable delay function）的一种隐蔽信道构建方法进行举例说明。

VDF 是一类数学函数，接收一个输入和一些安全参数，运行一定时间后，输出一个唯一对应的结果以及证明。验证者会依据输入、参数、输出和证明判断 VDF 是否正确，达到验证目的。经本文实验分析，由不同 CPU 型号运行相同 VDF 时所需时间存在差异。因此，可对运行时间进行阈值设定来编码隐秘信息，是一种隐蔽性非常高的方法。之后，结合上述 4 种类型，选用交易地址、签名算法、智能合约或 P2P 广播机制作为载体构建区块链网络隐蔽信道。

4　结束语

区块链这样一个新型网络环境下构建信道的思路引起了研究者的大量关注，为信息的安全传输提供了更好的方法。本文首先介绍了网络隐蔽信道的定义和发展历史，简单描述了区块链整体架构，通过对传统网络隐蔽信道的分析，引出了新型的区块链网络隐蔽信道；将隐蔽信道按照载体的不同，分为交易地址型、签名算法型、智能合约型和 P2P 广播机制型 4 类；依据隐蔽性、传输效率和通信成本 3 个评价指标，结合各类区块链网络隐蔽信道进行对比和评估，将区块链网络环境下的隐蔽信道模型定义为隐秘信息嵌入、载体混淆传输、特殊载体筛选和隐秘信息解码 4 个步骤；最后提出了现有方法的不足，并提供了解决思路。希望本文为以后网络隐蔽信道的构建提供有益的参考。

参考文献：

[1] ZANDER S, ARMITAGE G, BRANCH P. Covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys and Tutorials, 2007, 45(12): 136-142.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008, 28(1): 21260-21268.

[3] WENDZEL S, ZANDER S, FECHNER B, et al. Pattern-based survey and categorization of network covert channel techniques[J]. ACM Computing Surveys, 2015, 47(3): 50.

[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] 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.

[6] 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.

[7] PETITCOLAS F A P, ANDERSON R J, KUHN M G. Information hiding-a survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062-1078.

[8] LAMPSON B W. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613-615.

[9] SIMMONS G J. The prisoners' problem and the subliminal channel[C]//Proceedings of CRYPTO. Berlin: Spinger, 1984: 51-67.

[10] CRAVER S. On public-key steganography in the presence of an active warden[C]//International Workshop on Information Hiding. Berlin: Spinger, 1998: 355-368.

[11] MILLEN J. 20 years of covert channel modeling and analysis[C]//Proceedings of the 1999 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 1999: 113-114.

[12] HANDEL T G, SANDFORD M T II. Hiding data in the OSI network model[C]//International Workshop on Information Hiding. Berlin: Spinger, 1996: 23-38.

[13] CAUICH E, GOMEZ C R, WATANABE R. Data hiding in identification and offset IP fields[C]//Proceedings of the 5th International School and Symposium. Berlin: Spinger, 2005: 247-261.

[14] GIRLING C G. Covert channels in LAN's[J]. IEEE Transactions on Software Engineering, 1987, 13(2): 292-296.

[15] ROWLAND C H. Covert channels in the TCP/IP protocol suite[J]. First Monday, 1997, 2(5): 1.

[16] WOLF M. Covert channels in LAN protocols[C]//Local Area Network Security. Berlin: Spinger, 1989: 89-101.

[17] WU J Z, WU Y J, YANG M T, et al. POSTER: biTheft: stealing your secrets by bidirectional covert channel communication with zero-permission android application[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1690-1692.

[18] PARTALA J. Provably secure covert communication on blockchain[J]. Cryptography, 2018, 2(3): 18-35.

[19] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27.

[20] EPISHKINA A, KOGOS K. Protection from binary and multi-symbol packet length covert channels[C]//Proceedings of the 8th International Conference on Security of Information and Networks. New York: ACM Press, 2015: 196-202.

[21] MAZURCZYK W, SZCZYPIORSKI K. Evaluation of steganographic methods for oversized IP packets[J]. Telecommunication Systems, 2012, 49(2): 207-217.

[22] RIOS R, ONIEVA J A, LOPEZ J. HIDE_DHCP: covert communications through network configuration messages[C]//Information Secu-

rity and Privacy Research. [S.l.:s.n.], 2012: 162-173.

[23] ZOU X G, LI Q, SUN S H, et al. The research on information hiding based on command sequence of FTP protocol[C]//Knowledge-Based Intelligent Information and Engineering Systems. [S.l.:s.n.], 2005: 1079-1085.

[24] PATUCK R, HERNANDEZ-CASTRO J. Steganography using the extensible messaging and presence protocol (XMPP)[J]. arXiv Preprint, arXiv: 1310.0524, 2013.

[25] WENDZEL S, KAHLER B, RIST T. Covert channels and their prevention in building automation protocols: a prototype exemplified using BACnet[C]//Proceedings of 2012 IEEE International Conference on Green Computing and Communications. Piscataway: IEEE Press, 2012: 731-736.

[26] GIFFIFIN J, GREENSTADT R, LITWACK P, et al. Covert messaging through TCP timestamps[C]//Proceedings of 2002 International Conference on Privacy Enhancing Technologies. Piscataway: IEEE Press, 2020: 194-208.

[27] LUCENA N B, PEASE J, YADOLLAHPOUR P, et al. Syntax and semantics-preserving application-layer protocol steganography[C]// International Workshop on Information Hiding. Berlin: Spinger, 2004: 164-179.

[28] MUCHENE D N, LULI K, SHUE C A. Reporting insider threats via covert channels[C]//Proceedings of 2013 IEEE Security and Privacy Workshops. Piscataway: IEEE Press, 2013: 68-71.

[29] TAHIR R, KHAN M T, GONG X, et al. Sneak-Peek: high speed covert channels in data center networks[C]//Proceedings of the 35th Annual IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2016: 1-9.

[30] EL-ATAWY A, DUAN Q, AL-SHAER E. A novel class of robust covert channels using out-of-order packets[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 14(2): 116-129.

[31] LIU F F, YAROM Y, GE Q, et al. Last-level cache side-channel attacks are practical[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 605-622.

[32] IRAZOQUI G, EISENBARTH T, SUNAR B. Cross processor cache attacks[C]//Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. New York: ACM Press, 2016: 353-364.

[33] MAZURCZYK W. Lost audio packets steganography: the first practical evaluation[J]. Security and Communication Networks, 2012, 5(12): 1394-1403.

[34] TAHMASBI F, MOGHIM N, MAHDAVI M. Code-based timing covert channel in IEEE 802.11[C]//Proceedings of 2015 5th International Conference on Computer and Knowledge Engineering (ICCKE). Piscataway: IEEE Press, 2015: 12-17.

[35] GILES J, HAJEK B. An information-theoretic and game-theoretic study of timing channels[J]. IEEE Transactions on Information Theory, 2002, 48(9): 2455-2477.

[36] 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.

[37] 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.

[38] BARTOLETTI M, POMPIANU L. An analysis of Bitcoin OP_RETURN metadata[J]. Lecture Notes in Computer Science, 2017, 10323: 218-230.

[39] CAO H T, YIN H, GAO F, et al. Chain-based covert data embedding schemes in blockchain[J]. IEEE Internet of Things Journal, 2022, 9(16): 14699-14707.

[40] LUO X Y, ZHANG P, ZHANG M L, et al. A novel covert communication method based on bitcoin transaction[J]. IEEE Transactions on Industrial Informatics, 2022, 18(4): 2830-2839.

[41] 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.

[42] TIAN J, GOU G P, LIU C, et al. DLchain: a covert channel over blockchain based on dynamic labels[C]//International Conference on Information and Communications Security. Piscataway: IEEE Press, 2019: 814-830.

[43] SIDIQ M F, WIBOWO F M, WIBOWO M, et al. Secret and trustable communication channel over blockchain public ledger[C]//Proceedings of 2021 IEEE International Conference on Communication, Networks and Satellite. Piscataway: IEEE Press, 2021: 371-376.

[44] FIONOV A. Exploring covert channels in bitcoin transactions[C]//Proceedings of 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). Piscataway: IEEE Press, 2019: 59-64.

[45] 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.

[46] FRKAT D, ANNESSI R, ZSEBY T. ChainChannels: private botnet communication over public blockchains[C]//Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Piscataway: IEEE Press, 2018: 1244-1252.

[47] GUO Z Z, SHI L C, XU M Z, et al. MRCC: a practical covert channel over monero with provable security[J]. IEEE Access, 2021, 9: 31816-31825.

[48] 蓝怡琴, 张方国, 田海博. 利用门罗币实现隐蔽通信[J]. 西安电子科技大学学报, 2020, 47(5): 19-27.
LAN Y Q, ZHANG F G, TIAN H B. Using Monero to realize covert communication[J]. Journal of Xidian University, 2020, 47(5): 19-27.

[49] 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, 2019: 41-46.

[50] 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.

[51] 吕婧淑, 操晓春. 基于比特币系统的隐蔽通信技术[J]. 信息安全学报, 2021, 6(2): 143-152.
LYU J S, CAO X C. Covert communication technology based on bitcoin[J]. Journal of Cyber Security, 2021, 6(2): 143-152.

[52] ABDULAZIZ M, ÇULHA D, YAZICI A. A decentralized application for secure messaging in a trustless environment[C]//Proceedings of 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT). Piscataway: IEEE Press, 2018: 1-5.

[53] 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.

[54] ZHANG Z J, ZHANG L J, RASHEED W, et al. The research on covert communication model based on blockchain: a case study of Ethereum's whisper protocol[C]//Frontiers in Cyber Security. [S.l.:s.n.], 2020: 215-230.

[55] RECABARREN R, CARBUNAR B. Tithonus: a bitcoin based censorship resilient system[J]. Proceedings on Privacy Enhancing Technologies, 2019, 2019(1): 68-86.

[56] 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.

[57] 李彦峰, 丁丽萍, 吴敬征, 等. 一种基于多节点时间戳共谋的区块链网络隐蔽通信方法: CN111245570B[P]. 2021-06-08.
LI Y F, DING L P, WU J Z, et al. Block chain network covert communication method based on multi-node timestamp collusion: CN111245570B[P]. 2021-06-08.

[58] GAI K K, WU Y L, ZHU L H, et al. Permissioned blockchain and edge computing emPoWered privacy-preserving smart grid networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 7992-8004.

[59] 黄韬, 刘江, 汪硕, 等. 未来网络技术与发展趋势综述[J]. 通信学报, 2021, 42(1): 130-150.
HUANG T, LIU J, WANG S, et al. Survey of the future network technology and trend[J]. Journal on Communications, 2021, 42(1): 130-150.

[60] MEIKLEJOHN S, ORLANDI C. Privacy-enhancing overlays in bitcoin[C]//International Conference on Financial Cryptography and Data Security. Berlin: Spinger, 2015: 127-141.

[61] AVERIN A, SAMARTSEV A, SACHENKO N. Review of methods for ensuring anonymity and de-anonymization in blockchain[C]// Proceedings of 2020 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Piscataway: IEEE Press, 2020: 82-87.

[62] WORLEY C, SKJELLUM A. Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability[C]//Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Piscataway: IEEE Press, 2018: 1582-1587.

[作者简介]

李雷孝（1978− ），男，山东成武人，博士，内蒙古工业大学教授，主要研究方向为网络空间安全、区块链技术、数据分析与数据挖掘等。

杜金泽（1998− ），男，山西太原人，内蒙古工业大学硕士生，主要研究方向为区块链技术、隐蔽信道构建与分析。

林浩（1995− ），男，天津人，天津理工大学博士生，主要研究方向为数据挖掘、人格检测、区块链技术。

高昊昱（1994− ），男，山西太原人，内蒙古工业大学硕士生，主要研究方向为区块链技术、共识算法与可信执行环境。

杨艳艳（1997− ），女，山东菏泽人，内蒙古工业大学硕士生，主要研究方向为计算机视觉、云计算与大数据分析、深度学习与图像处理。

高静（1970− ），女，辽宁沈阳人，博士，内蒙古农业大学教授，主要研究方向为云计算、大数据与农业信息化。