区块链数据隐私保护研究

王宗慧[1]，张胜利[1]，金石[2]，王晖[1]
（1. 深圳大学信息工程学院，广东 深圳 518060；2. 东南大学移动通信国家重点实验室，江苏 南京 210096）

摘　要：区块链是一种具有去中心化、安全可信、防篡改和可编程等特点的分布式账本技术。区块链系统的公开透明特性使用户交易隐私受到严重威胁，针对此问题设计了不同应用场景相应的隐私问题解决方案。首先介绍区块链技术且基本工作原理，并介绍区块链中典型的隐私问题，如交易隐私问题和账户隐私问题；其次，将现有典型的区块链隐私保护方案分为 3 种，即混币方案、密码学方案和安全通道方案，并对这 3 种区块链隐私保护技术方案进行综合而全面的介绍；最后，对区块链数据隐私保护技术进行分析并展望其在物联网安全领域的应用与发展。

关键词：比特币；区块链；隐私保护；密码学；物联网
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096-3750.2018.00066

Survey on privacy preserving techniques for blockchain

WANG Zonghui[1], ZHANG Shengli[1], JIN Shi[2], WANG Hui[1]
1. College of Information Engineering, Shenzhen University, Shenzhen 518060, China
2. National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Abstract: Blockchain is a kind of distributed ledger technology with the characteristics of decentralization, security reliability, tamper-proof and programmable. The open and transparent feature of the blockchain system has seriously threatened the transaction privacy of users, and the corresponding privacy problem solution is designed for different application scenarios. Firstly, the basic working principle of block chain technology was introduced, and typical privacy issues was introduced in blockchain, such as transaction privacy and account privacy. Secondly, the existing typical blockchain privacy protection schemes were divided into three types: mixed-coin technology, cryptography technology and secure channel technology, and presents a comprehensive and comprehensive introduction to this three privacy protection schemes; Finally, the blockchain data privacy protection technology was analyzed, the application and development on IoT security were prospeted.

Key words: bitcoin, blockchain, privacy preserving, cryptography, Internet of things

1　引言

区块链是由数据区块按时间顺序形成链式结构的散列链。区块链是比特币、以太坊等数字加密货币的核心技术，通过运用数据加密、时间戳、分布式共识和激励机制等方式，系统中的节点能在分布式系统中实现去信任的点对点交易，从而解决中心化系统存在的高信任、低效率及数据存储不安全等问题[1]。随着比特币的推广，比特币底层核心技术区块链的研究与应用快速增长，被认为是继移动互联网后的第五代互联网颠覆性技术[2]。

区块链的优良特性使其广泛应用于各领域。在“数字加密货币”领域中，市场上存在 1 498 种“加密货币”，市值达 3 500 多亿美元。目前，比特币的用户数量已超过 1 300 万人，根据 Coinbase 提供的用户增长数据表预测，到 2024 年，比特币的用户

收稿日期：2018-03-15；**修回日期：**2018-05-25
基金项目：国家自然科学基金资助项目（No. 61771315）；深圳市基础研究基金资助项目（No. JCYJ20160226192223251）
Foundation Items: The National Natural Science Foundation of China (No. 61771315), Shenzhen Research Foundation (No. JCYJ20160226192223251)

数量将达到 2 亿人。在金融领域，区块链技术可以改善传统金融系统中对账清算时间长、跨境结算效率低、中心账本数据维护成本高等问题。在物联网领域，利用区块链技术的点对点交易、智能验证等特点，实现物联网设备间不同类型的交易[3]。IBM 已提出将区块链技术与物联网应用相结合，形成“去中心化的自治物联网”。在知识产权领域，利用区块链的时间戳、数据难以篡改和难以伪造特性，实现数据存证、著作产权保护、作品鉴定等功能。此外，供应链、司法、信息认证等领域也逐渐应用区块链技术改善现存行业问题[4]。

区块链系统没有中心化的机构处理与维护数据，为了使各节点快速达成共识，系统中所有交易均是公开透明的，从而带来了数据隐私泄露问题。虽然区块链中用户的地址是匿名的，但一些组织或个人通过地址跟踪用户的交易数据，分析交易规律，取得用户交易地址间的关联性，并结合网络外部信息推测用户真实身份信息[5]。在金融领域及供应链中，区块链的公开透明特性使用户可以获取所有交易信息及物资供应信息，包括金额、合约内容等。而数据是金融机构盈利的关键点，同时也是供应链服务保密对象，竞争企业或个人通过分析交易数据获取利益，直接损害公司的利益。在物联网领域，设备间能实现点对点的交易，这种情况下区块链系统会泄露能源传输等敏感信息，从而对个人安全和国家安全造成威胁。因此，在使用区块链技术的同时，需要解决区块链存在的隐私泄露问题，保证用户的信息安全。

传统的数据隐私保护方案中，数据存储于中心服务器，数据管理中心可以通过提高中心服务器的抗攻击性，采用 K-匿名技术[6]、同态加密技术[7]等数据加密技术，实现数据隐私保护。在区块链系统中，系统的所有交易数据存储在分布式全节点中，节点的防御能力各不相同，恶意节点会加入区块链系统并获取交易数据。因此，传统的数据隐私保护方案并不适用于区块链。

针对区块链面临的数据隐私泄露问题，目前，已经出现了很多解决方案。本文对区块链现有的几种典型的隐私保护方法，包括安全通道支付技术、混合币技术、加密技术进行分析与总结，并将区块链数据隐私保护技术与物联网相结合，保证物联网数据安全与隐私。

2 区块链技术概述

区块链是比特币、以太坊等“加密货币”的底层技术，首次出现在“中本聪”2008 年提出的文章中[8]，随后不断发展并应用于各领域。区块链是按时间顺序将数据区块以链式结构连接，并由密码学与工作量证明算法保证的难以篡改、难以伪造的去中心化分布式账本。区块链的优良特性使比特币成为一个去中心化的货币发行系统，确保系统中各节点实现点对点对等的安全交易。

1) 比特币的交易过程

比特币的交易是由 P2P 网络技术[9]、密码学和共识机制、奖励机制共同组成的，其交易过程如图 1 所示。

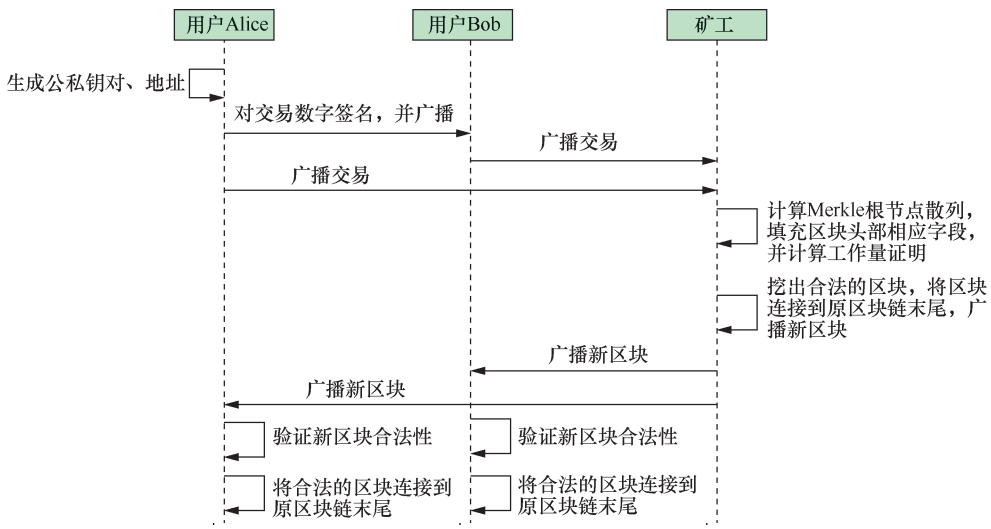

图 1 比特币的交易流程

在比特币系统中，每个节点在接入时会生成一个密钥对，即公钥和私钥。公钥和私钥是通过非对称加密技术生成的[10]。公钥作为用户的交易地址和交易中的身份认证，私钥可用于对交易进行签名[11]（ECDSA 数字签名）。图 1 是比特币的一个交易例子。当用户 Alice 向用户 Bob 发起一笔交易时，Alice 用私钥对生成的交易内容进行签名，并广播至全网节点。全网的矿工对交易信息验证成功后打包放入区块中并计算交易的 Merkle 根，同时寻找一个随机数（Nonce），使该区块的散列值小于区块设定的目标值。最快找到符合条件的 Nonce 挖矿节点拥有该区块记账权，并将新产生的区块加盖时间戳，广播至全网节点。网络中的节点对新区块进行验证，验证成功则将新区块添加至区块链末尾。由此，Alice 与 Bob 的交易成功，生成新区块的矿工获得相应奖励。

2) 比特币的数据存储结构

基于比特币系统的区块链结构如图 2 所示。

每个数据区块包含上一数据区块的散列索引。当区块中的任一数据变化时，区块的散列值也会随之发生改变，从而引起后续区块散列值的变化，使网络中的节点验证区块数据失败，因此这种链式结构能有效提高数据被篡改的难度。接下来，将对数据区块进行简要介绍。

每个数据区块由区块头和区块体构成，如图 3 所示。区块头部包括以下内容。

① 版本号：明确系统中的交易参照的规则，跟踪协议的更新。

② 前一区块散列值：散列索引，形成链式结构。

③ Mekle 根：区块中的交易按 Merkle 树计算散列值形成根散列值。

④ 随机数：满足工作量证明算法的从 0 开始的累加器（4 B）。

⑤ 时间戳：区块生成的时间（Unix 时间戳）。

⑥ 目标散列值：共识算法设定的下一区块目标难度值。

区块体主要包含验证通过的交易信息，对这些交易按 Mekle 树形式进行散列运算生成唯一的 Mekle 根。交易信息内容包括输入地址、输出地址、交易数值、手续费等。

3) 共识机制

区块链系统核心优势是去中心化，而没有中心机构的分布式系统最关键问题是如何使全网节点达成一致协议。“中本聪”设计了工作量证明（PoW）算法，来保证分布式系统数据的一致性和安全性，

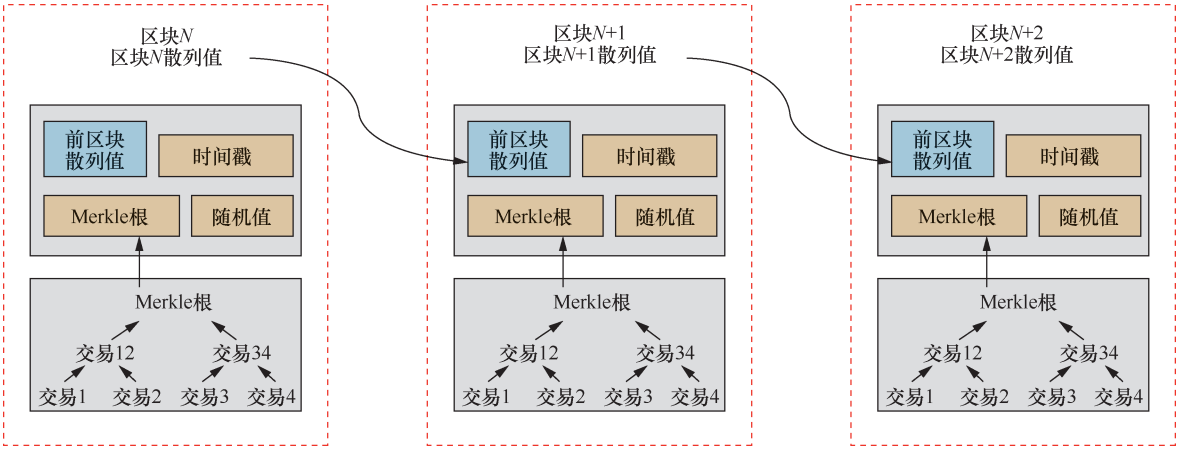

图 2　比特币中区块链结构

区块版本号	0x20000000
前一个区块散列值	00000000000000000002363fa8a69738798e715997e6a9b7a41bdfc3f0149b6e6
Merkle 根	d45e76dd3c6843ba47a5d47e1035d6a8c80859443fa1ceadd40619725b7f6589
随机数	199985413
时间戳	1526516683
下一区块目标散列值	00000000000000000002363fa8a69738798e715997e6a9b7a41bdfc3f0149b6e6

图 3　数据区块结构

随后被广泛用于以太坊等区块链平台。在比特币系统中，矿工通过算力竞争寻找一个随机数计算区块散列值[12]，使当前区块散列值小于或等于区块的目标散列值。最快解决这个数学难题的矿工将拥有当前区块的记账权，并获得一定数量比特币作为奖励。根据全网节点当前的算力，比特币系统将动态调整区块的难度值，使新区块的产生时间保持在 10 min 左右。PoW 共识机制实现比特币系统数据的同一性与难以篡改性，任意节点想改区块的交易数据需重新算出当前区块及后续区块的散列值，使该区块链长度超过主链长度。但是，这要求节点拥有超过全网 51%的算力，其算力成本远大于收益。目前，截至 2018 年 3 月，比特币系统全网算力已经超过 9 000 000 TH/S。

PoW 共识机制在保证系统的去中心化特性和数据一致性的同时造成电力资源的浪费，而且随着难度的增加，能源的消耗日渐增长。另外，10 min 的交易确认时间和 1 Mbit/s 的区块大小使系统每秒处理交易数 7 笔左右，不适用于商业应用。因此，越来越多的共识机制被提出应用于区块链系统中，包括 PBFT 共识机制[13]、PoS 共识机制[14]、Raft 共识机制[15]等。

3 区块链面临的隐私问题

区块链技术颠覆了传统中心化的交易模式，用户不需要任何可信第三方便能实现信息的传递，因此，区块链技术逐渐应用于各领域，解决传统中心化机构存在的问题。然而区块链技术在实现去中心化、去信任的同时，全网中的节点为了达成共识，需要公开全网的交易信息，因此，给用户带来严重的隐私问题。目前，在区块链系统中，主要存在用户身份隐私问题和用户交易隐私问题。

3.1 用户身份隐私威胁

在比特币系统中，用户不需要提供自己的身份信息，而是通过公钥实现双方间转账交易，攻击者通过公钥无法还原交易者身份信息。交易者可以生成多个公钥，每笔交易可使用新的公钥，从而降低同一交易者不同公钥的关联性，然而比特币的匿名性并不受技术保证。

为了保护身份隐私，用户可以为每一笔交易生成新的公私密钥对，用于找零或将自己的比特币按一定比例发送到多个新生成的账户。但是这些方法并不能保证用户身份安全。Reid 等人[16]通过构建交易网络和用户网络，分析交易网络中的输入与输出关系，得到多个输入最终汇聚到一个地址，表明多输入交易一般由同一个拥有者签名发起。根据用户的公钥，结合相关网站提供的信息，便对用户匿名产生威胁。例如，用户使用比特币在线购买商品，在线商店可以访问用户的邮件地址、送货地址、IP 地址等详细信息[17]；用户在比特币论坛等网站公开自己的公钥等，从而带来用户隐私泄露问题。

Coinbase 地址和找零地址也会暴露用户地址间的关联性。Coinbase 交易的多个输出地址属于同一个用户群，矿工通过加入矿池增加算力进行挖矿，当生成新的区块，参与挖矿的矿工均会获得相应奖励。找零地址是上一笔交易的输出地址和下一笔交易的输入地址，如果能发现找零地址，便能将两笔交易中的输入地址相关联。

通过下载比特币系统交易数据，分析地址间的关联性，不断减小交易关系图，能降低区块链地址的匿名性。Meiklejohn 等[18]采用一种聚类启发式算法，对同一用户的地址进行聚类。他们通过与一些服务提供商网站进行实际交易并结合各种论坛和网站上公开的地址，将对方的公钥有效地标记为服务提供商。从而根据标记的公钥对服务商进行分类，包含供应商、交易所、矿池等。根据服务提供商的公开账本信息，可以获取账本中地址的关联性，从而降低用户匿名性。Ron 等[19]通过 Union-Find 算法分析比特币系统交易关系，针对账本中 3 730 218 不同公钥，将每个公钥与不同地址相关联，最后获得 2 460 814 不同所有者，并推测出拥有许多不同公钥的交易所、矿池等。Koshy 等[20]通过分析比特币交易信息，创建从比特币地址到 IP 地址的映射。通过创建具有收集数据功能的 CoinSeer 比特币钱包，收集并分析 5 个月的交易数据，对不同的交易中继模式进行分类，最后分析 3 种异常中继模式，发现交易始发节点，创建比特币地址到 IP 地址的映射。这表明仅通过观察交易中继转发模式，就可以对某些比特币地址集进行去匿名化。Androulaki 等[21]通过模拟器将比特币用于大学生日常交易，从而模仿比特币的功能运作。即使采用了比特币一次性公钥的隐私保护措施，作者基于交易行为的聚类技术仍可以在很大程度上揭示 40%的比特币用户。

3.2 用户交易隐私威胁

在比特币系统中，所有的交易都是公开透明

的，用户可以获取详细的交易内容，同时区块链的链式结构和 Merkle 树结构使系统的每一笔交易均可溯源。比特币采用未花费交易输出（UTXO）交易模式，一笔交易可以有多个输入和多个输出，当前交易的输入是上一笔交易的输出，当前交易的输出是下一笔交易的输入。根据交易地址的关联性，攻击者可以对交易进行追踪，获取资金流向。而一些用户为了保护交易数据，并不希望公开交易内容。例如，在金融系统和供应链系统中，交易数据是企业盈利的核心部分，使用者不愿意公开交易数据，因此，在这些应用场景中，区块链技术并不能保护使用者的商业隐私。

在比特币交易网站，根据用户公钥可以获取与该公钥地址关联交易的详细信息。Reid 等[16]通过比特币论坛、推特等网站获取用户公开的公钥地址，追踪用户资金来源与使用情况，计算用户余额。结合盗窃案例，分析盗窃地址在盗窃前后的资金流向。Ron 等[19]对比特币系统中 364 笔大于 50 000 比特币的交易进行追踪分析，发现大额交易资金主要通过长期交易链模式、分叉合并模式、自循环模式、储蓄账户和二叉树模式分散到多个账户中，试图隐藏交易间的关联性，并且很多账户的比特币处于“休眠”状态。Ober 等[22]根据 215 399 个区块数据分析了比特币交易拓扑结构图及其动态，观察活跃实体数量与比特币汇率的关系，汇率升高会增加活跃实体数量。根据地址间的交易关系图，作者发现了比特币交易系统不同时期休眠比特币变化的数量关系，且休眠比特币一般维持在 60% 左右。

通过分析比特币系统交易规律及交易特征，攻击者能将公钥与用户身份相关联，获取资金流向与资金余额，给用户带来安全隐患。2014 年，日本最大的比特币交易所 Mt.Gox 被攻击者盗取价值 4.8 亿美元的比特币，并获取交易所用户的信息。2016 年，中国香港的比特币交易所 Bitfinex 遭到黑客入侵，价值 7 500 万比特币被盗，用户私钥被盗取。攻击者根据比特币系统交易信息，将以公钥作为假名的用户与其真实身份相关联，对用户隐私产生严重危害。

4　区块链隐私保护技术

比特币系统采用公钥散列值作为用户身份，在交易过程中用户不需要提供真实身份，因此，比特币具有化名性。用户可以通过生成多个公钥地址增加隐私性，但系统所有的交易数据都保存在公开透明的分布式账本中，通过追踪、分析地址间的交易记录，结合用户网络信息，可以推测用户身份，因此比特币不具有匿名性。为提高区块链技术的匿名性，保护用户身份隐私及交易数据隐私，多种区块链隐私保护方案被提出。将区块链隐私保护技术分为 3 类：基于混币协议的技术、基于加密协议的技术、基于安全通道协议的技术。

4.1　基于混币协议的技术

区块链中的每一笔交易均是公开的，攻击者可以查询交易双方的交易金额与交易地址，通过分析交易信息获取相应的信息，因此，区块链的公开透明特性对用户造成了严重的隐私问题。为了既保持区块链的优良特性又保证用户隐私，Bonneau 等[23]提出了一种在不改变比特币任何协议的情况下，为交易用户提供混合服务保证用户隐私的方案——Mixcoin。Mixcoin 设计的原理如图 4 所示。

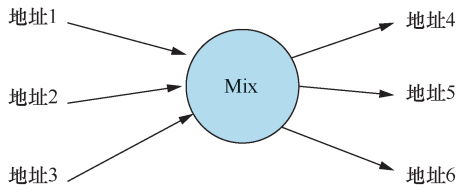

图 4　Mixcoin 原理

比特币用户将比特币发送到一个中央的混合服务器，混合服务器将交易内容混合处理后，将比特币发送至用户新地址。为提高匿名性，Mixcoin 要求多用户同时使用相同金额进行混币。通过混合服务器对资金的处理，可以隐藏交易的输入地址与输出地址之间的联系，提高了攻击者分析交易内容的难度，保证了用户交易隐私。Mixcoin 工作流程如图 5 所示。

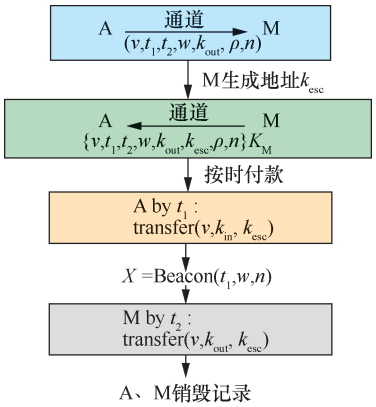

图 5　Mixcoin 工作流程

A 为需要进行混币服务的用户，M 为提供混币服务的混合器。A 首先通过一个匿名安全通道向 M 发送以下混币服务的相关参数。

v：A 要混合的数字货币金额；t_1：A 将货币发送给 M 的截止时间；t_2：M 将混合后的货币发给 A 的截止时间；w：M 等待确认 A 提交 v 的区块数；k_{out}：A 将 v 转移至新地址；ρ：A 提交的混合服务费最大值；n：用来决定支付混币服务费用的随机数。

M 接收 A 的请求参数，生成一个新的地址 k_{esc}，并用密钥 K_M 对所有参数内容进行签名保证后发送给 A。A 在截止日期 t_1 之前将金额 v 发送至地址 k_{esc}，根据密码伪随机函数 Beacon 计算服务费 X，扣除 A 相应的手续费，M 在截止日期 t_2 前将混币后的 v 发送至地址 k_{out}。如果 M 在混币过程中出现违规行为，A 可将 M 的签名数据公布到全网中，每个节点均可审计 M 是否作弊，M 则失去全网信任，不能再提供混币服务。Mixcoin 作为提供混币服务的第三方，掌握用户输入地址与输出地址之间的连接，存在泄露用户隐私问题。

Blindcoin 是由 Valenta 等[24]提出的采用盲签名技术[25]来改善 Mixcoin 缺陷的中心化混币方案。在 Blindcoin 方案中，用户对输出地址采用盲签名，使第三方能提供混币服务的同时，不会将用户的输入地址与输出地址相连接，从而保护用户交易信息。但是，Blindcoin 的混合金额仍然是固定的，并且用户必须将输出地址匿名发送到公共日志中，同时，还是无法避免第三方作弊行为。达世币[26]（Dash）是一种以保护用户隐私为目的的“数字货币”，采用链式混合及盲化技术实现混币过程。Dash 中用户用固定的几种 Dash 值进行混币交易，负责混币的主节点保证乱序输出用户所需的输出地址。为了提高交易匿名性，用户会随机选择多个混币主节点依次进行混币，降低地址间的关联性。但是 Dash 是一种中心化的混币方法，容易受到恶意主节点攻击。

CoinJoin[27]允许多笔交易输入合并构成一笔交易，当用户所要求的输出地址出现在输出地址列表时，用户才会对交易进行签名。CoinJoin 可以隐藏交易输入地址与输出地址间的关系，但是 CoinJoin 技术需要第三方混币服务平台，第三方平台掌握用户输入地址与输出地址，因此 CoinJoin 技术并不是完全匿名的。CoinShuffle[28]是一种去中心化的混币方案，解决了中心化混币服务的内部地址可链接问题。用户使用混币服务中其他用户的密钥加密输出地址，所有参与者按顺序对输出地址进行洗牌，最后将输出地址列表进行广播。CoinShuffle 能保证混币参与者无法获取交易地址间的联系，但是在混币过程中需要参与者同时在线，因此，容易遭受拒绝服务攻击。TumbleBit[29]是一种链下通道混币技术，采用 RSA 和 ECDSA 密码学技术，用户通过去信任的第三方平台 Tumbler 实现无连接的匿名交易，Tumbler 也无法获取交易信息，因此，会增加用户交易匿名性。CoinParty[30]是基于阈值的 ECDSA 签名和混合网络相结合的分布式混币技术。CoinParty 能提供单笔混币交易，并允许网络存在恶意节点的情况下，保证混币服务的有效性，增加了用户的匿名性和安全性。

混币技术方法可以在不改变比特币协议的基础上，增加用户交易匿名性和安全性，在基于区块链的“数字货币”中应用广泛。表 1 对现有混币技术的功能特性、优势、不足等方面进行了分析比较。

4.2 基于加密协议的技术

加密技术是隐私保护领域常用的解决方案。通过密钥对敏感数据加密，只有持有相应密钥的用户才能查看数据内容，从而保证用户数据的安全性。

表 1 现有混币技术特点对比

方法	结构	特点	盗窃风险	拒绝服务
MixCoin	中心化	匿名性取决于第三方混币服务与可信度提供用户	高	低
BlindCoin	中心化	匿名性取决于第三方混币服务及盲签名技术	高	低
Dash	中心化	选取几个主节点提供一连串混币服务，保证匿名性	中	低
CoinJoin	中心化	使用多重签名技术来增强匿名性	低	高
CoinShuffle	P2P	使用其他用户密钥加密用户输出地址，增加地址不可链接性	低	高
TumbleBit	P2P	使用 RSA 和 ECDSA 密码学技术，由不可信第三方实现混币	低	低
CoinParty	P2P	基于解密混合网络和阈值签名的混币服务	低	低

区块链系统中的数据是由网络中的节点共同维护的，因此，采用加密技术来保护数据隐私需保证节点可以对加密数据进行验证，达成共识。一些研究者根据比特币系统设计了匿名性和隐私性更好的“数字货币”系统，通过密码学技术，如多方安全计算、盲签名、环签名及零知识证明等，构造去中心化的匿名“数字货币”系统。下面，对几种现有典型的基于加密技术的案例进行分析。

1) 门罗币

门罗币（Monero）是基于 CryptoNote[31]、环保密交易（RingCT）[32]等密码学技术来保证用户的匿名性和隐私性。Monero 的特点是交易不可关联性和隐藏交易金额，其中，环签名（ring signature）和隐蔽地址（stealth address）解决了交易中输入地址与输出地址间的关联性问题。RingCT 保证了交易的隐私。

隐蔽地址可以实现接收方地址外部不可见性，即发送者用接收方的公钥信息和发送方随机选取的一个随机数，通过 Keccak 散列算法生成一次性公钥地址，并将一次性公钥和附加信息广播到区块链上。接收者用私钥检测区块信息获取与其相关的交易，当接收者要花费这笔交易金额时，计算出该一次性公钥对应的私钥，对交易进行签名即可。由于交易中接收者的私钥与发送者生成的一次性公钥相关，其他用户无法获取接收者的身份信息。

Monero 通过环签名方案，保护了发送者隐私。当发送者给接收者发送一笔金额时，发送者用自己的私钥对交易进行签名，交易信息包含随机选取的若干其他用户的公钥，同时提供本次交易的唯一的密钥镜像（key image）。矿工在验证交易时，需验证其他用户公钥对应的签名，并根据密钥镜像判断发送者是否双花。此外，Monero 还通过 RingCT 技术来隐藏用户的交易信息。

2) 零币

Monero 虽然能实现匿名交易及隐藏交易金额，但是仍然存在一些问题：环签名中需要加入其他用户公钥，相当于将真实交易隐藏在匿名集合中，可能存在恶意用户暴露隐私，使用户交易地址被关联，且用户在选取匿名集合时，匿名集合一般较小，攻击者可以通过分析交易信息，将交易信息与用户身份连接[33-34]。Miers 等[35]提出一种基于零知识证明[36]的零币协议——Zerocoin，解决了用户交易地址泄露问题。Zerocoin 是比特币的一种扩展协议，通过 Zerocoin 用户可以将比特币铸造成 Zerocoin 进行交易，隐藏交易输入地址与输出地址，也可将 Zerocoin 赎回成比特币。使用 Zerocoin 交易时，其他用户无法获取 Zerocoin 的交易信息，只知道该 Zerocoin 是否已被花费，从而实现交易不可链接。

用户在铸造 Zerocoin 时，首先生成一个代表该 Zerocoin 的一次性随机序列号 S，随后采用散列算法将接收者的公钥与随机数 r 生成一个承诺 C，用户将 C 广播至区块链上的铸币公告栏。为了赎回 Zerocoin，用户通过零知识证明向矿工提供一个证明 π，证明自己的序列号是真实且没有 Zerocoin 被花费的，并将币的序列号 S 发布到注销币公告栏上。矿工会验证 π，检查序列号 S 没有被使用过，从而完成兑换 Zerocoin 过程。

3) 零钞

Zerocoin 虽然能有效地保护用户匿名性和隐私性，但是 Zerocoin 只能铸造和兑换固定面值的货币，且 Zerocoin 的零知识证明的数据相对较大，需要消耗额外的区块链存储空间及计算资源。Sasson 等[37]提出了零钞（Zerocash）方案，将简洁非交互性零知识证明技术（zk-SNARK）应用于“数字货币”，实现当前“数字货币”交易最高程度的隐私性与匿名性。此外，与 Zerocoin 比较，Zerocash 对交易金额保密，支持任意面值的金额交易。Zerocash 交易发起者可以将不同面值的币铸造成多个等值的币，每个币都有自己的数额、序列号等。每一次铸币过程代表一个承诺，交易发起者将承诺添加到全网的承诺列表中。交易发起者用接收者的公钥对交易信息（交易金额、接收者地址）进行加密后广播至全网，接收者用私钥检测到交易信息后，生成新币的序列号。矿工利用非交互零知识证明验证交易时，根据交易发起者提供的证明，矿工只需要确认发起者的承诺在承诺列表中，且该承诺对应的序列号在注销币的序列中。矿工无法获取哪个承诺被使用，从而保证了用户的匿名性。由于每一个币都有唯一的一次性序列号表示，能达到有效防止双花目的。表 2 对现有几种加密货币的功能特性、优势、不足等方面进行分析。

4.3　基于安全通道协议的技术

区块链系统的交易需要经过矿工验证，并通过共识机制使全网节点达成共识，因此，系统每秒处理交易数量受到限制。为了解决区块链系统的可扩

表 2 加密货币特性对比

方法	特点	优点	缺点
Monero	基于 CryptoNote 密码学协议	通过环签名、隐蔽地址，RingCT 实现匿名	交易被链接
Zerocoin	基于零知识证明密码学技术	交易不可链接、抗盗窃和拒绝服务攻击	证明数据占内存大，验证时间长
Zerocash	简洁非交互性零知识证明技术	匿名性最强	依靠固定节点初始化内置参数，验证效率较低

展性问题，多种链下支付方案被提出[38]。双向微支付通道[39]、闪电网络[40]、Sprites[41]等链下支付技术，通过使用安全通道，用户只需要将第一次交易金额和最后一次交易金额广播到区块链上，用户之间的交易细节在链下执行，因此，保证交易信息的隐私性。但是，这几种链下交易方案在交易双方没有直接支付通道时，允许中继节点作为服务提供者完成交易。中继节点能获取交易双方的交易信息，使用户的隐私受到威胁。

针对链下安全通道交易技术的隐私保护问题，Green 等[42]提出一种匿名支付通道技术——Blot。Blot 提供 3 种链下支付方案：单向支付通道、双向支付通道、第三方支付通道。用户之间的交易可通过链下安全通道直接进行或者依靠不可信第三方。第三方支付通道运用盲签名技术及零知识证明技术，使第三方不能获取用户的交易信息，从而防止第三方从中作恶，保证用户的隐私性。Heilman 和 Baldimtsi[43]等人提出一种链下匿名支付方案使用户通过第三方实现匿名交易，但是该方案假设第三方是诚实可信的。随后 Heilman 和 Baldimtsi 等对此方案进行改进，提出一种兼容比特币系统的链下交易通道方案——TumbleBit，TumbleBit 允许交易各方通过不受信任的中介 Tumbler 实现快速匿名的链下支付。通过 RSA 和 ECDSA 密码学技术，Tumbler 能够验证用户交易的真实性，无法获取用户的交易信息，实现用户交易的不可链接性，从而保证用户隐私性。

现有的链下安全通道支付技术均通过第三方实现用户间的匿名交易，因此还存在许多不足。例如，当交易出现错误时，需要将用户的交易信息公开验证，而如何保证在不泄露用户隐私的情况下实现交易的公平性，需要研究者进一步完善。表 3 对现有的几种链下安全通道交易技术功能特性、优势、不足等方面进行分析。

5 现存区块链隐私保护技术分析

区块链技术可以在不可信环境中实现信息与价值的传递交换，是构建未来价值互联网的基石。但是区块链的公开透明特性，严重影响用户的隐私安全。随着区块链技术的发展，目前已经存在很多解决用户隐私问题的方案，然而，现有方案都存在一些不足，需要继续研究改进。

在混币协议中，现有的技术主要依靠去信任的第三方平台对多个用户的交易集进行混合后输出到相应的地址，使攻击者无法将交易的输入与输出地址进行链接。然而，随着数据分析算法的发展，攻击者可以分析混币协议的交易匿名集，从而将交易地址进行关联。另外，不可信的第三方平台会存在泄露交易信息或拒绝服务的可能。因此，需要研究采用加密技术保证混币协议的安全性和匿名性，采用奖励机制保证第三方平台正常处理交易，从而实现用户的隐私安全。

在加密协议中，现有技术主要采用环签名、零知识证明等密码学技术保护用户隐私。环签名需要随机选择一定数量的用户对交易进行签名，即将真实交易隐藏在一个匿名集中，因此需要提高匿名集

表 3 现有安全通道技术特性对比

方法	特点	优点	缺点
Bi-directional Payment	链下交易通道实现快速交易	交易内容仅交易双方可见，减少验证时间	公布用户最后的交易状态
Lightning Network	链下交易通道实现快速交易	交易内容仅交易双方可见，减少验证时间	依靠第三方平台，公布最后交易状态
Sprites	交易处理速度快	支持部分提款和存款	交易可链接
Blot	对交易内容加密，不可信第三方实现链下通道交易	提供更强的用户隐私，交易不可链接	第三方可能获取交易内容
TumbleBit	通过 RSA 和 ECDSA 密码学实现匿名的链下通道交易技术	第三方无法获取具体交易信息，保证用户隐私安全	验证时间较长

的抗攻击性。零知识证明技术需要生成初始化参数，目前 Zcash 的初始化参数由 6 个人负责生成，由于任何知道初始化参数的一方能随意生成货币，因此，Zcash 生成初始化参数的方法仍然受到怀疑。未来研究需要提高初始化参数集的可信度，可采用可信计算或多方安全计算等方法生成初始化参数集。另外，零知识证明技术生成证明的时间过长，需要消耗大量计算资源并占用较大内存，影响系统的效率使交易的吞吐量受到限制。未来需要继续研究改进基于密码学方案的计算性能和存储性能的不足，设计效率更高、性能更好的加密方案。

在安全通道协议中，用户依据链下安全通道进行交易，通过不可信第三方，没有建立直接通道的用户亦能完成交易。但是现有技术安全性与可靠性还存在许多问题。使用链下交易的用户需要将最终的交易状态公布至全网；第三方平台存在泄露用户信息的可能；攻击者通过分析用户链下支付路由获取用户交易模式及交易信息等。未来需要解决第三方平台可靠性和支付协议隐私性问题，采用加密技术保证第三方无法获取用户信息，同时设计高效的隐私保护支付路由协议。

6　区块链隐私保护技术下的物联网安全

区块链技术应用于物联网领域，能有效改善传统物联网中心化数据存储模式的不足[44]。区块链网络中的全节点记录完整的数据信息，共同维护物联网设备数据的安全，降低传统物联网应用维护中心化数据库的成本[45]。物联网设备作为区块链网络中的节点，通过公钥实现点对点间的数据交易，网络的共识机制保证全网节点与交易达成一致，同时，区块链的防篡改特性、时序性保证全网节点数据的安全性和可溯性。

区块链的公开透明特性使设备间的交易信息公开在全网中，对交易数据隐私造成严重威胁。另外，恶意用户通过分析交易信息，获取设备身份信息从而对设备进行攻击，造成安全隐患。因此，采用区块链隐私保护技术能有效解决物联网设备数据传输与存储的安全隐患[46]。通过区块链加密协议，用户无法获取网络中的交易信息，验证节点只能验证交易的有效性而无法获取具体的交易信息，从而保证交易数据隐私。通过安全通道技术，设备间的数据传输可在链下进行，减少了验证时间并增加数据隐私性，设备只需将加密后的交易记录广播至区块链网络中即可。将区块链隐私保护技术应用于物联网安全，不仅能推动物联网技术的发展，还能降低成本，保证数据的安全与隐私。未来需要研究区块链技术对物联网设备数据安全与隐私的更多作用，同时提高数据传输的验证效率及网络的吞吐量。

7　结束语

区块链技术的去中心化、安全可靠、防篡改、可溯源等特性，使其受到广泛的关注并应用于各领域。但是区块链作为一种分布式账本技术，为了全网节点快速达成共识，其交易是公开透明的，这会对用户的隐私造成严重威胁。如何保护区块链上用户隐私一直受到研究者的关注。本文首先针对区块链技术目前面临的隐私保护问题进行分析，主要存在用户身份隐私问题与用户交易隐私问题；其次，从混币协议、加密协议、安全通道协议 3 个方面详细地分析了现有隐私保护方案的保护方法；随后，分析现有的区块链隐私保护技术方案；最后提出区块链隐私保护技术下的物联网安全特点。此外，在提高区块链技术隐私性的同时，需要加大对区块链技术违法行为的监管。研究异常节点的检测方法，遏制恶意节点利用区块链技术进行非法活动。

参考文献：

[1] 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.

[2] SWAN M. Blockchain: blueprint for a new economy[M]. “O’Reilly Media, Inc.”, 2015: 212-235.

[3] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web & Grid Services, 2016: 1-19.

[4] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: beyond bitcoin [J]. Applied Innovation, 2016, 2: 6-10.

[5] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]//Interna-tional Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013: 6-24.

[6] BAYARDO R J, AGRAWAL R. Data privacy through optimal k-anonymization[C]//Proceedings. 21st International Conference on Data Engineering, 2005, ICDE 2005. 2005: 217-228.

[7] GENTRY C. A fully homomorphic encryption scheme [M]. Stanford University, 2009：112-130.

[8] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J].

Consulted, 2008.

[9] DONET J A D, PÉREZ-SOLA C, HERRERA-JOANCOMARTÍ J. The bitcoin P2P network[C]//Intern-ational Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014: 87-102.

[10] ANTONOPOULOS A M. Mastering bitcoin: unlocking digital crypto-currencies[M]. O'Reilly Media, Inc. 2014：25-36.

[11] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[12] COURTOIS N T, GRAJEK M, NAIK R. Optimizing sha256 in bitcoin mining[C]//International Conference on Cryptography and Security Systems. Springer, Berlin, Heidelberg, 2014: 131-144.

[13] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.

[14] KING S, NADAL S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake[J]. Self-published Paper, 2012(8): 19.

[15] ONGARO D, OUSTERHOUT J K. In search of an understandable consensus algorithm[C]//USENIX Annual Technical Conference. 2014: 305-319.

[16] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system[M]. Security and Privacy in Social Networks. Springer, New York, NY, 2013: 197-223.

[17] GOLDFEDER S, KALODNER H, REISMAN D, et al. When the cookie meets the blockchain: privacy risks of Web payments via cryptocurrencies[J]. 2017: 1-23.

[18] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing pay-ments among men with no names[C]// Proceedings of the 2013 Conference on Internet Measurement Conference. ACM, 2013: 127-140.

[19] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]//Intern-ational Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013: 6-24.

[20] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in bitcoin using P2P network traffic[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014: 469-485.

[21] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating user privacy in bitcoin[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013: 34-51.

[22] OBER M, KATZENBEISSER S, HAMACHER K. Structure and anonymity of the bitcoin transaction graph[J]. Future Internet, 2013, 5(2): 237-250.

[23] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014: 486-504.

[24] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for bitcoin[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015: 112-126.

[25] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Springer, Boston, MA, 1983: 199-203.

[26] DUFFIELD E, DIAZ D. Dash: a privacy centric crypto currency[J]. 2014: 1-22.

[27] Maxwell, Gregory. CoinJoin: bitcoin privacy for the real world, 2013: 1-13.

[28] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[C]//European Symposium on Research in Computer Security. Springer, Cham, 2014: 345-364.

[29] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: an untrusted bitcoin-compatibl-e anonymous payment hub[C]//Proceedings of NDSS 2017, 2017: 1-15.

[30] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: secure multi-party mixing of bitcoins[C]//Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. ACM, 2015: 75-86.

[31] Van Saberhagen N. Cryptonote v2.0[J]. 2013: 1-13.

[32] NOETHER S, MACKENZIE A, TEAM M C. Ring confidential transactions[J]. 2016: 1-12.

[33] MILLER A, MOESER M, LEE K, et al. An empirical analysis of linkability in the monero blockchain[J]. 2017: 1-15.

[34] KUMAR A, FISCHER C, TOPLE S, et al. A traceability analysis of monero's blockchain[C]//European Symposium on Research in Computer Security. Springer, Cham, 2017: 153-173.

[35] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: anonymous distributed e-cash from bitcoin[C]//2013 IEEE Symposium on Security and Privacy (SP). 2013: 397-411.

[36] RACKOFF C, SIMON D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[C]//Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1991: 433-444.

[37] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payment-s from bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP). 2014: 459-474.

[38] MCCORRY P, MÖSER M, SHAHANDASTI S F, et al. Towards bitcoin payment networks[C]//Australasian Conference on Information Security and Privacy. Springer, Cham, 2016: 57-76.

[39] DECKER C, WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]//Symposium on Self-Stabilizing Systems. Springer, Cham, 2015: 3-18.

[40] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[J]. Draft Version 0.5, 2016, 9: 14.

[41] MILLER A, BENTOV I, KUMARESAN R, et al. Sprites: payment channels that go faster than lightning[J]. 2017：1-23.

[42] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies[C]Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017: 473-489.

[43] HEILMAN E, BALDIMTSI F, GOLDBERG S. Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016: 43-60.

[44] ZHANG Y, WEN J. The IoT electric business model: using blockchain technology for the Internet of things[J]. Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994.

[45] CHAKRAVORTY A, WLODARCZYK T, RONG C. Privacy preserving data analytics for smart homes[C]//Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013: 23-27.

[46] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT security and privacy: the case study of a smart home[C]//2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerC-om Workshops). 2017: 618-623.

[作者简介]

王宗慧（1994-），女，深圳大学硕士生，主要研究方向为区块链、区块链数据隐私保护技术等。

张胜利（1978-），男，博士，深圳大学教授、博士生导师、物理层网络编码创始人，主要研究方向为无线网络、区块链关键技术、物理层网络编码等。

金石（1974-），男，博士，东南大学教授、博士生导师、国家杰出青年基金获得者，主要研究方向为 5G/B5G 移动通信理论与关键技术研究、物联网理论与关键技术研究以及机器学习与大数据处理在移动通信中的应用等。

王晖（1969-），男，博士，深圳大学教授、博士生导师，主要研究方向为物联网、无线网络等。