区块链隐私保护与监管技术研究进展

李佩丽[1,2,3], 徐海霞[1,3,4], 马添军[1,3,4]

[1]中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093
[2]广西密码学与信息安全重点实验室 桂林 中国 541004
[3]中国科学院数据与通信保护研究教育中心 北京 中国 100087
[4]中国科学院大学网络空间安全学院 北京 中国 100049

摘要 区块链是一种分布式的数据库, 是比特币等数字货币的核心技术, 受到学术界和产业界广泛关注和研究。区块链具有去中心化、去信任、高度透明等特点, 在金融、医疗、政府、军事等领域有重要的应用价值。区块链账本公开透明的特点方便了节点对交易的验证, 但同时带来了用户的隐私保护问题。用户的身份、交易金额等内容很容易被泄漏, 对其的保护是近几年区块链隐私保护的研究热点。另外,隐私保护基础上的监管问题也备受关注, 因为隐私保护本身可能会助长恶意行为, 隐藏恶意用户的身份、非法内容等。因此如何做到隐私保护与监管之间的平衡也是区块链技术走向实际应用面临的重要问题。本文总结了目前已有的区块链隐私保护与监管方法, 分析了这些方法的实现原理及存在的问题, 最后对区块链隐私保护与监管技术未来的研究方向进行了展望。

关键词 区块链; 隐私保护; 监管; 环签名; 零知识证明
中图法分类号 TP309;TP311.13 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2021.05.10

Research progress of blockchain privacy protection and supervision technology

LI Peili[1,2,3], XU Haixia[1,3,4], MA Tianjun[1,3,4]

[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]Guangxi key laboratory of Cryptography and Information Security, Guilin 541004, China
[3]Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100087, China
[4]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Blockchain is a distributed database and is the core technology of digital currency such as Bitcoin. It has received extensive attention and research from academia and industry. Blockchain has the characteristics of decentralization, trust, and high transparency. It has important application value in the financial, medical, government, military and other fields. The transparent feature of the blockchain facilitates the verification of the transaction by the node, but at the same time brings the privacy protection problem of the user. Users' identity, transaction amount and other contents are easy to be disclosed, and the protection of them has become a research hotspot of blockchain privacy protection in recent years. In addition, supervision issues based on privacy protection are also of concern, as privacy protection itself may indulge malicious behavior, hide the identity and illegal content of malicious users and so on. Therefore, how to achieve the balance between privacy protection and supervision is also an important issue when facing practical applications. This article summarizes the current blockchain privacy protection and supervision methods, analyzes the implementation principles and existing problems of these methods, and finally looks into the future research directions of blockchain privacy protection and supervision technologies.

Key words blockchain; privacy protection; supervision; ring signature; zero knowledge proof

1 引言

区块链是以比特币为代表的数字货币的核心技术[1], 受到学术界和产业界的广泛关注和研究。2016 年 12 月, 国务院关于印发《十三五国家信息化规划》中提到“将区块链作为战略前沿性技术”, 明确提出

通讯作者: 徐海霞, 博士, 副研究员, Email:xuhaixia@iie.ac.cn。
本课题得到国家重点研发计划(No. 2017YFB0802500), 广西密码重点实验室的开放课题(No. GCIS201909), 山东省重大科技创新工程（No. 2019JZZY020129）资助。
收稿日期: 2019-04-24; 修改日期: 2019-06-15; 定稿日期: 2021-03-05

加强区块链等新技术的创新、试验和应用。区块链技术是一种分布式的账本(或称数据库)技术, 解决了多中心环境下的信任问题。以往的社会的信任模式建立在存在可信中心的场景下, 例如银行、支付宝等。区块链解决了如何在没有可信第三方的情况下, 多个互相不信任的节点能够达成一致的问题。以比特币为例, 用户之间完成每笔交易都要通过验证且被记录在账本上。如果有可信中心的存在, 那么这个问题很容易解决, 直接由中心验证和记账就好。然而在没有可信中心的情况下, 大家怎么达成一致, 如何来验证交易和记账呢? 区块链技术为此提供了解决方案。

区块链的简单框架图如下图 1:

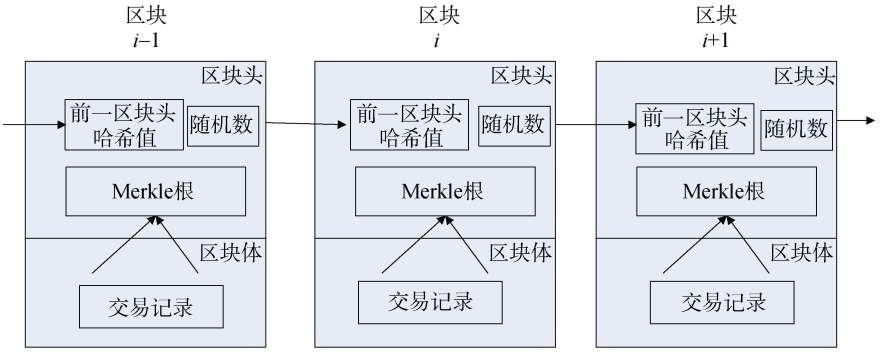


图 1 区块链框架

Figure 1 Blockchain framework

区块链中区块与区块按照时间顺序前后链接, 每个区块包含上一个区块的 hash 值、交易记录信息以及 Merkle 树根等信息。区块链并不是单一的技术, 而是现代密码学、分布式一致性协议、点对点网络通信技术等多种技术的整合[2]。

区块链具有以下特点:

(1) 去中心化: 整个网络没有中心化的机构, 节点的权利和义务均等;

(2) 集体维护: 系统中数据块由整个系统中所有节点共同维护;

(3) 高度透明: 程序开源、账本公开, 可以被所有人审查;

(4) 去信任: 没有第三方可信机构, 从技术上保证交易的进行;

(5) 匿名: 交易在匿名下进行。

区块链系统根据应用场景的不同, 可以分为: 公有链, 联盟链和私有链。

(1) 公有链对外开放, 各个节点可以自由出入网络。公有链中的数据可以被任何人查看, 任何人都可以发送交易、参与形成共识。公有链是完全去中心化的区块链, 比特币就是一个典型的例子;

(2) 联盟链有准入规则, 通过授权后方可加入和退出网络。区块链的读写权限、参与记账权限按照联盟规则指定。联盟链是一种许可链, 典型代表有区块链联盟 R3 和超级账本 Hyperledger;

(3) 私有链适用于私有组织, 各个节点的读写权限由组织内部制定, 读取权限可有选择性的对外开放。

区块链最初主要应用在金融领域, 之后随着人们对区块链的深入研究, 发现其有更广阔的应用价值, 包括医疗、保险、政务管理、军事、食品安全等领域。区块链最典型的应用比特币系统试图通过用户大量自由生成交易地址来实现用户真实身份的保密, 即匿名。比特币区块链上的交易内容包括用户的地址、转账金额等都是公开透明的, 可以让所有参与节点对交易进行验证和记录。区块链账本公开透明的特点方便了节点对交易的验证, 但同时带来了用户的隐私保护问题。近年来的研究发现, 由于区块链数据的公开透明性, 通过大量分析交易和网络数据, 可以设计去匿名方案[3]。在实际应用中, 企业或用户可能不希望自己的交易信息被公开的放在链上, 包括交易双方的身份、交易金额、交易事由等内容。隐私问题对于个人和企业都至关重要, 尤其在很多金融系统、军事领域更是如此。那么该如何保证区块链上用户身份和数据的机密性是区块链走向实际应用面临的一项重要挑战。在此基础上的监管问题也受到大家的关注, 因为隐私保护可能会助长恶意行为, 隐藏恶意用户的身份、非法内容等。因此隐私保护基础上考虑监管问题是很有必要的。

本文第 2、3 章分别对区块链隐私保护和监管技术的研究进展进行介绍; 第 4 章给出总结并引出今后可能的研究方向。

2 区块链隐私保护技术

区块链的隐私保护主要包含两个方面: 一是用

户身份的匿名性, 二是传输内容的保密性。在匿名性的具体实现方面, 又可以通过下面两个概念来描述: 1)交易不可追踪: 对于任何交易, 无法追踪其付款方是谁; 2)交易不可关联: 对于向外发送的两笔交易, 其他人无法证明其是否发给同一个收款人。关于区块链的隐私保护, 近年来涌现出不少研究成果。下面对这方面工作的研究现状进行梳理。

2.1 基于混合技术

混合技术又分为带中心的混合和去中心的混合, 目的是为了打乱输入和输出之间的对应关系, 使得其他用户不知道一笔钱来自哪个用户, 即实现交易的不可追踪性。根据有无中心节点参与, 混合方法又可以分为带中心的混合和去中心的混合:

带中心的混合方法: 1981 年, Chaum[4]首次提出了混合网络的概念并给出基本的混合协议, 协议需要可信中介器的参与。Bonneau 等人[5]在 2014 年提出了带中心的 Mixcoin 机制,方案中有多个 mix 节点(如图 2, 其中方框内的点表示 mix 节点), 只要有一个 mix 节点诚实, 那么方案的隐私性就能保证。Valenta 和 Rowan 在 mixcoin 的基础上, 采用盲签名技术对中心化混币方案进行优化, 使得中心节点在正常提供混币服务的同时, 不知道输入输出之间的对应关系[6]。

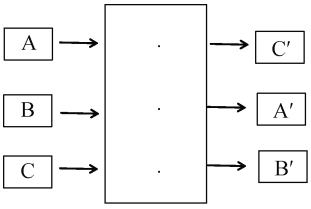


图 2 混合器
Figure 2 CoinMixer

去中心的混和方法: Maxwell 首次提出了去中心化的混合协议 Coinjoin[7]。这个协议与比特币系统比较兼容。如图 3, 多个用户的交易放在一个比特币交易内, 使得其他人不知道多个输入地址和输出消息之间的对应关系。

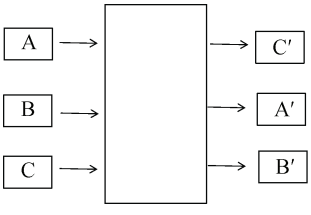


图 3 混合协议
Figure 3 Coinjoin

之后又有 CoinShuffle[8]、CoinShuffle++[9]等去中心化的混合机制被提出。CoinShuffle 结构如图 4 所示, 包含四个步骤: 公告(announcement)、混合(shuffling)、交易的产生和验证(Transaction Verification)及错误的纠察(Blame), CoinShuffle 系统的流程如下:

(1) 公告(announcement): 用户生成一对公私钥对, 并将公钥广播。

(2) 混合(shuffling): 参与混合的每个用户创建一个新的比特币地址作为混合交易的输出地址。这些用户通过混合技术, 打乱刚生成的输出地址, 得到输出地址集合, 最后一个用户广播这个集合。假设有三个用户 Alice、Bob、Charlie。具体流程为: 用户 Alice 用 Bob 和 Charlie 的公钥对其输出地址 A′加密, 得到 $Enc_{pkB}(Enc_{pkC}(A'))$发送给 Bob; Bob 用其私钥 skB 解密得到 $Enc_{pkC}(A')$, 然后将其输出地址 B′用 Charlie 的公钥加密得到 $Enc_{pkC}(B')$, 将 $Enc_{pkC}(A')$和 $Enc_{pkC}(B')$的顺序打乱发给 Charlie; Charlie 解密得到打乱后的 A′, B′,然后对 A′, B′, C'的顺序进行打乱并公开, 这样每个用户只能判断自己的输出地址是否在公开的输出地址集合里, 而不知道其他两个地址到底属于谁。在这里用户猜测成功的概率是 1/2, 在用户数量为 n 时, 用户猜测成功的概率为 $1/n–1$。从而在 n 越大时, 方案的不可追踪性越好。

(3) 交易产生和验证(Transaction Verification): 用户验证自己新产生的输出地址是否在集合中。若在, 则用户创建混合交易(输入地址, 金额和打乱的输出地址, 金额), 并对交易签名后广播。在收到所有其他用户的签名后, 用户将混合交易连同所有用户的签名发布到比特币网络。区块链中的用户验证这笔公开的交易是否包含所有参与用户的签名, 若是则继续验证输入的有效性和输入输出金额的相等, 若都验证通过则交易有效, 若缺少某一用户的签名(如图 4 所示), 则交易验证失败。

(4) 纠责阶段(Blame): 在交易产生及验证阶段, 一旦存在非法操作, 协议进入纠察阶段。用户公开各自的临时公私钥对, 检查协议执行过程, 识别行为异常的用户。存在异常行为的用户会在随后协议的运行中被剔除。

继 CoinShuffle 之后, CoinShuffle++[9]基于 DC-net 协议实现了更加高效的混合协议: P2PMixing。在 CoinShuffle++的基础上, Tim Ruffing 和 Pedro Moreno-Sanchez 设计了一个新的混币协议: Valueshuffle[10], 它既可以保证发送者匿名, 又可以保密交易金额、实现接收者匿名。Valueshuffle 利用同态承诺

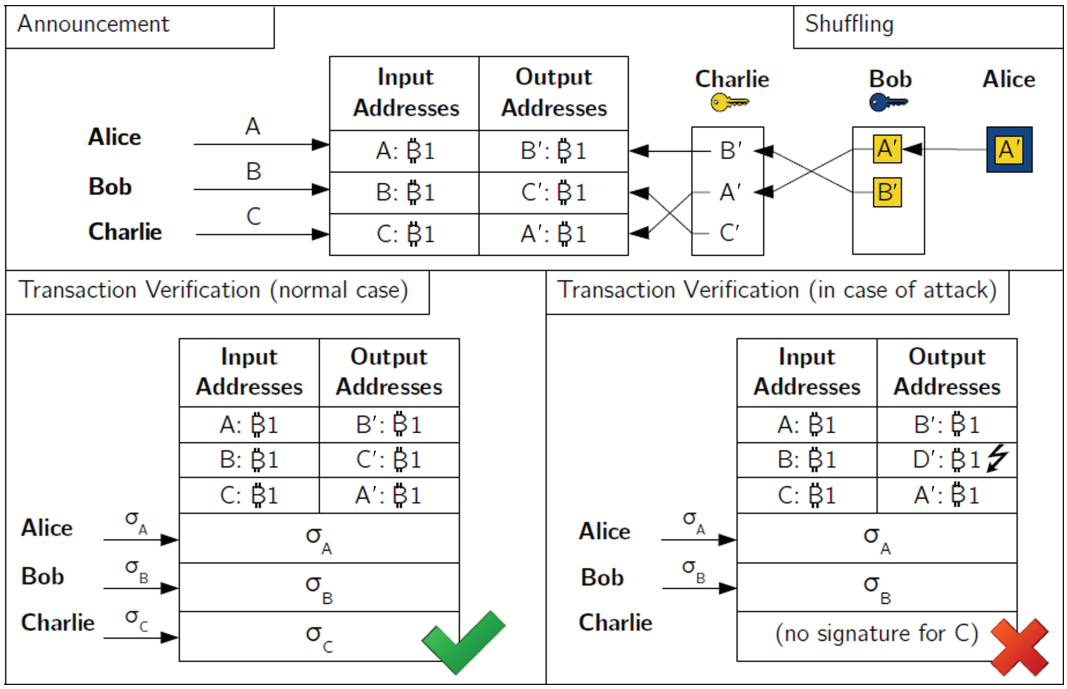


图 4　去中心化混币机制(引自文献[8])

Figure 4　Decentralized coin mixing(Citation [8])

保密交易金额, 用隐身地址的方法实现交易的不可关联。同态承诺的隐藏性可以保密交易金额, 其同态性质支持金额的密态验证[11]。隐身地址的方法具体来说就是发送方通过接收方的公开信息生成一个随机地址作为接收方的地址, 接收方可以通过自己的秘密信息恢复出相应的私钥。因此每次交易接收者的地址在变化, 其他节点不能链接哪些交易是发向同一个接收者的, 实现了交易的不可关联性。

Coinjoin 和 Coinshuffle 等去中心的混币机制由于没有中心节点, 参与混币的用户需自行协商和执行混币过程。在协商过程中, 参与混币的节点可能发现其他节点的混币信息。另外如果存在部分节点恶意操作, 会导致混币执行轮数过多, 效率低等问题[12]。

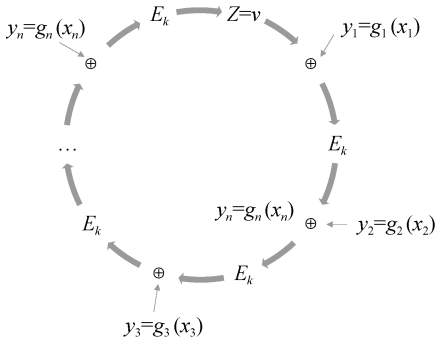


图 5　环签名

Figure 5　Ring signature

2.2　基于环签名的匿名技术

2001 年, Rivest, shamir 和 Tauman 三位密码学家首次提出了环签名。环签名是一种简化的群签名,环签名中只有环成员没有管理者,不需要环成员间的合作。其他用户只知道签名是由环中的用户所签, 但不知道是具体是哪个用户[13]。图 5 为 Rivest 等人提出的环签名算法示意图。

其构造如下:

1) 初始化阶段:

E_k 是对称加密体制, 密钥为 $k=H(m, L)$; 计算 $y_i=g_i(x_i)$容易, 在不知道陷门的情况下计算 $x_i=g_i^{-1}(y_i)$ 是困难的; 环中有 n 个用户, 其公钥分别是 $g_1, \cdots, g_n$, 私钥分别是公钥相应的陷门。

2) 签名过程: (假设环中第 s 个用户要做环签名)

- $k=H(m, L)$, $L=\{g_1(*), \cdots, g_n(*)\}$ 环中有 n 个用户
- 随机计生成 $v, x_1, \cdots, x_{s1}, x_{s+1}, \cdots, x_n$
- 计算 y_s 并可得

$$E_k(\cdots E_k(E_k(v \oplus y_1) \oplus y_2) \cdots)=v$$

- 利用陷门可解密 $x_s=g_s^{-1}(y_s)$
- 签名为$(v, x_1, \cdots, x_n)$

3) 验证过程: 计算$y_1, \cdots, y_n$并验证下式是否成立

$$E_k(\cdots (E_k(v \oplus y_1) \oplus y_2) \cdots)=v$$

若成立则签名验证通过, 否则拒绝。

环签名除了满足正确性和不可伪造性, 还满足一个重要特性就是无条件匿名性: 即攻击者无法确

定签名是由环中哪个成员所签, 即使在或者环成员私钥的情况下, 成功的概率也不超过 1/*n*。

后续有不少环签名方案被提出, 还衍生出一类叫可链接的环签名。可链接的环签名在环签名的基础上增加了可链接(linkable)的性质, 即如果一个用户用同一个私钥做了两次环签名, 那么这两个签名可以被链接到此用户, 即知道这两个签名是由同一个用户所签, 不过也不能确定具体是哪个用户。

CryptoNote 就采用可链接的环签名实现了发送者身份的隐藏[14]。一个要做交易的用户, 选择具有相同金额的公钥地址作为环中的成员, 对交易进行环签名。其他用户可以验证这笔交易, 但不知道是谁对这笔交易做的签名。如果一个用户用相同的私钥做了两次签名, 那么验证者可以判断这两个签名来自同一个用户, 但不知道具体是谁。因此可链接的环签名隐藏了发送者的身份(这里是公钥), 实现了交易的不可追踪性。另外 CryptoNote 同样采用隐身地址的方法使交易不可关联。门罗币 Monero[15]建立在 CryptoNote 基础上, 实现了交易金额的隐藏。它用到了同态承诺来保密金额, 可以实现输入输出金额一致的验证功能[16]。

基于环签名的隐私保护方案本质上是把真实的交易隐藏在一个集合中, 使得其他节点不知道实际参与者是集合中的那个节点。目前已有的不需认证机构的环签名方案中, 签名的尺寸和环的大小(集合大小)相关。也有工作研究如何进一步降低环签名的尺寸[17]。另外在实际操作中, 集合选择不当可能会带到一些问题, 攻击者可以通过分析获得交易的链接情况[18]。

2.3 基于零知识证明的方法

为了提供更好的匿名性, Miers 等人基于零知识证明设计了一种扩展的比特币系统 Zerocoin[19], 使得输入的比特币地址与输出的比特币地址之间没有直接关系。从而实现了交易的不可追踪性。不过它与比特币系统不兼容, 需要先将比特币换成零钞(Zerocoin), 然后再通过使用承诺和零知识证明打断交易发送者和接收者之间的对应关系。另外 Zerocoin 中币值金额是固定的, 无法实现金额的拆分。Ben-Sasson 等人在 2014 年提出了一种新的匿名数字货币: Zerocash[20]。Zerocash 建立在 Zerocoin 的基础上并对其进行了改进。它采用简洁的非交互零知识证明(zk-SNARKs)和同态承诺等密码工具[21-22], 被称为是一种完全匿名的货币。

Zerocash 的功能通过两类交易实现: 铸币(mint)交易和熔币(pour)交易。与比特币相同, Zerocash 也采用区块链作为去中心化的交易账本, 产生的交易会被广播并附加到区块链上。

Zerocash 的设计思想如下:

--铸币交易(Mint)

铸币交易用于产生 Zerocash。用户将指定数量的比特币转换为相同金额的 Zerocash。假设用户有面值为 v 的比特币, 用户首先随机生成三个字符串 r,s,ρ, 然后使用承诺方案(commitment scheme)来计算两个字符串 cm 和 sn, 细节如下图。

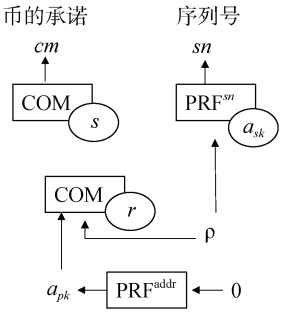


图 6 铸币

Figure 6 Mint coin

铸的币为 $c=(a_{pk},pk_{enc},v,r,s,\rho,cm)$, 图中 a_{sk} 是用户私钥, a_{pk} 为用户地址, pk_{enc} 为用户的加密公钥。铸币交易通过基于 SHA-256 散列函数的承诺方案隐藏了 Zerocash 的价值和用户的地址。

--熔币交易(Pour transaction)

熔币交易用来实现用户的保密转账, 即保密支付。假设用户 A 有一个输入, 要做一个转账交易产生两个输出(如图 7)。

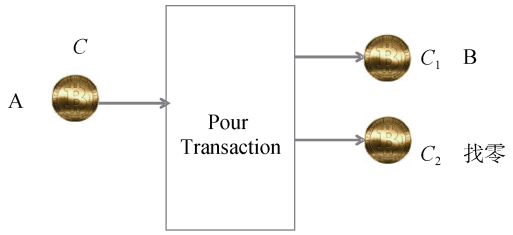


图 7 熔币交易

Figure 7 Pour coin

输入币信息 $c=(a_{pk},v,r,s,\rho,cm)$

输出 1 信息 $c_1=(b_{pk},v_1,r_1,s_1,\rho_1,cm_1)$ 其中 b_{pk} 是输出地址

输出 2 信息 $c_2=(a_{pk},v_2,r_2,s_2,\rho_2,cm_2)$ 假设 (sn,cm_1,cm_2,π) 是找零的币

那么用户 A 产生简洁的非交互零知识证明 π 来证明:

(1) 用户 A 拥有这个输入的币;

(2) 输入的币在以前的铸币交易中出现;

(3) 交易前后, 币的总价值相等。

用户 A 公布 $c_2=(a_{pk},v_2,r_2,s_2,\rho_2,cm_2)$ 到网上。

可以看出熔币交易在花费输入币时只显示币的序列号 *sn*, 不显示币的面额和地址等其他信息, 因此保护了发送者的身份和交易金额。

Zerocash 支持金额拆分且可以保密交易金额, 能够与比特币系统兼容。不过 Zerocash 需要基于一个可信的初始化阶段并依赖于一个没有被检验的密码假设(因为用到 zk-SNARKs), 因此其理论安全性还有待研究。另外 Zerocash 采用的 zk-SNARKs 算法验证比较高效, 但生成证明的过程比较慢。因此如何在实现更好匿名性的同时提升方案运行效率是一个值得继续研究的问题。

2.4 其他隐私保护方法

• 上面的工作大都针对交易信息-双方身份和金额的隐私保护, 没有考虑智能合约的隐私。Kosba 等人提出了 Hawk 方案, Hawk 是一个区块链合约开发平台, 用来解决区块链上的隐私和智能合约安全保护问题[23]。方案结合了 zk-SNARK 和安全多方计算或者可信执行环境解决了匿名安全计算问题。它可以保证合约输入的隐私, 但不保护合约代码。

• 除了前面提到的三类方法, 还有一些带中心的隐私保护方法被提出, 如 Chinaledger 提出的 CCP(中央对手方)方案和基于 Tear-off 的隐私保护方案, 这两个方案都需要引入特殊的节点(分别是中央对手方和公证人)来接收敏感信息并验证。

• 另外也有工作针对联盟链的隐私保护问题进行研究。摩根大通基于以太坊设计了 Quorum 协议, 实现了灵活的隐私策略。它默认各个节点是诚实的, 需要引入监管节点, 适用范围较窄。为了解决 Hawk 不能加密合约代码和 Quorum 通用性不强的问题, 微软提出了 Coco 框架, 它能够保证合约代码的隐私, 理论上可以保护任区块链系统的隐私, 不过其依赖于可信的硬件[24]。

综上所述, 公有链的隐私保护方法大致分为三类: 基于混合技术、基于环签名和基于简洁的非交互零知识证明(zk-SNARKs)。在特定场景下可以实现较好的隐私保护。不过仍然存在改进的空间: 基于混合技术的方法, 若用户选择集合较小、参与混合的用户恶意, 可能会泄漏用户的私密信息; 基于环签名的方法, 每次交易产生的签名尺寸和环的用户数量有关; 基于简洁的非交互零知识证明虽然实现了较好的匿名性, 但其参数的生成需要可信方的参与, 另外生成证明的效率也不高。

3 区块链监管技术研究进展

隐私保护本身可能助长恶意用户的非法行为, 在此基础上的监管问题是企业、政府、军事部门实际需要解决的重要问题, 这两年对其相关的研究开始吸引大家的关注。监管具体包括用户身份的监管, 交易内容的监管。关于区块链隐私保护基础上的监管问题研究工作较少, 根据监管内容的不同, 我们将其分为对用户身份的追踪和对用户交易内容的监管。

3.1 用户身份的追踪

在公开网络上, 大多用户希望自己的身份保持匿名, 然而匿名技术在保护诚实用户身份的同时可能助长恶意用户的恶意行为, 使得对恶意用户的追查带来困难。匿名基础上对用户身份的监管正是要解决这一问题,用户身份的监管又称用户身份的可追踪。下面我们对已有的身份追踪技术进行介绍。

1) Ateniese 等人[25]设计了一个比特币的认证系统, 使得用户可以获得可信机构颁发的证书, 从而提升其地址的可信度, 而且用户的身份可以被可信机构追踪。方案设计如下, 分为认证密钥产生阶段和验证阶段。其中 (y_T,x_T) 是注册中心 CA 的公私钥对。认证密钥 x 是用户和注册中心协同产生的, 包含用户的随机数 k, CA 的随机数 k' 以及 CA 的私钥 x_T . 在验证阶段, 验证者需要利用 CA 的公钥 y_T 算得用户的公钥 y, 若所算得的 y 和签名通过验证, 则表示交易有效, 且签名者是被 CA 认证过的。

a)认证密钥的产生:

(1) 用户随机选择 $k\leftarrow Z_q, h=g^k$,将 h 发给认证中心 CA

(2) 认证中心做如下操作:

$$k'\leftarrow Z_q,$$

$$c=h\cdot g^{k'},$$

$$e=\rho(c),$$

$$x'=k'+ex_T$$

将 c,x' 发送给用户

(3) 用户计算 $x=x'+k, A=H(c)$

x 即为用户签名用的私钥, 用户的交易记为[*T*], τ 为对交易的签名, 签名的验证过程如下。

b)交易签名的验证过程:

(1) 验证 $A=H(c)$

(2) 计算 $y:=c\cdot y_T{}^{\rho(c)}$

(3) 验证签名 $Vrf_y^{ECDSA}([T],\tau)$

这个方案实现了用户的可信认证, CA 有权追踪用户的身份。不过为了实现对其他用户的匿名性, 用户同样需要产生多个公私钥对。用户每次产生新的公私钥都需要去可信机构注册一遍。

2) El Defrawy 等人[26]基于安全多方计算设计了多个服务器协同存储账本和监管的方案。多个服务器拥有用户身份的秘密分享份额, 只有大于门限个数的服务器才可以恢复用户身份。

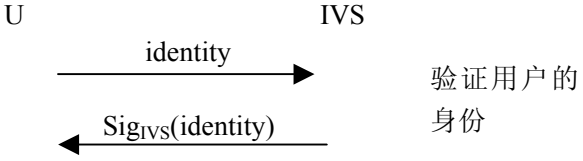
• 方案的参与方有:

账本服务器: $S_1, S_2, \cdots, S_n$

用户 : U

身份验证服务器: IVS

• 初始阶段, 用户 U 到 IVS 进行身份认证, IVS 验证用户的身份, 若通过, 则 IVS 对用户身份签名发送给用户 U,如下。



• 用户将自己公钥 PK, 以及身份 identity 的秘密分享份额, 身份的签名 Sig_{IVS}(identity) 的秘密分享份额, 分别发送给相应的账本服务器(图 8)。账本服务器协同执行验证算法, 若验证通过, 则将 PK 及用户身份的秘密分享份额添加到相应的账本中, 并将相应的账户余额 balance 设置为 0。

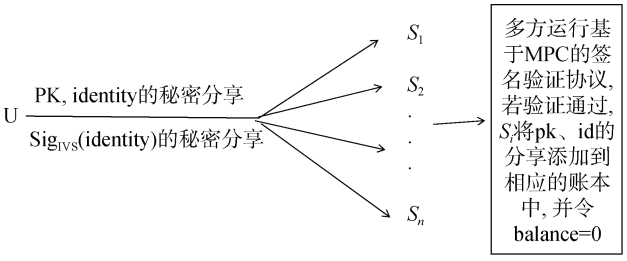


图 8 多方协同身份监管

Figure 8 Multi-party Collaborative Identity Regulation

通过初始化操作可以看出, 用户只需要去 IVS 认证一次, 之后把身份秘密分享给 n 个服务器。只有大于门限个服务器才能恢复出用户的身份, 即身份的追踪需要服务器的协同操作。

3) Zheng 等人[28]设计了可链接的群签名方案, 用于实现用户身份的可追踪, 交易内容的可审计。群签名方案满足匿名性和可追踪性。验证者可以验证群签名的确是由群中的成员所签, 但不知道是谁。群管理者能够获得签名者的身份(这里公钥即身份)。Zheng 等人设计的可链接的群签名方案包含四个主体: 用户、注册机构、审计机构和监管机构。方案将群签名管理者的权利进行分散, 把注册、审计、身份追踪操作分别交给不同的机构去做, 避免了传统群签名一个管理者的中心化和集权。

3.2 用户内容的监管

Narula 等人[27]研究了可审计的隐私保护分布式账本, 银行之间的交易信息对审计者是保密的, 但银行的资产可以被审计部门审计(获得银行现有资产、资产平均值、资产方差)。

方案的目标是: 隐藏交易数量, 交易参与者身份以及交易之间的链接; 对于审计者, 其可以获得询问的可靠回答。

银行之间每笔交易记录形式如图 9。$Bank_1$ (Bank of America)给 $Bank_2$ (Goldman Sachs)转账金额 10^6,将每个银行相应金额的增减进行承诺, 如 $Bank_1$ 金额要减少 10^6, 则对–10^6 做承诺, $Bank_2$ 的金额增加 10^6, 则对 10^6 做承诺, 其他银行无增减, 则对 0 做承诺。除了承诺值, 交易发起者需要证明这笔交易是收支平衡的, 即没有产生或丢失货币, 并且证明它的确拥有足够的钱来完成这笔交易, 这里用到了范围证明技术。这些信息写成一行作为这笔交易的记录。通过这种记录方式, 其他银行和审计者都不知道是谁在给谁转账, 因为这一条记录中的每一列都有数据, 且是不可区分的。也不知道交易金额是多少, 因为对金额做了承诺。但是可以验证其有效性。

Metadata			$Bank_1$	$Bank_2$	$Bank_3$	...	$Bank_n$
ID	Asset	Time	(Bank of America)	(Goldman Sachs)	(JPMorgan)	...	(Citigroup)
1	€	13:06:01 2/17/18	$COMM(-10^6, r_1)$ $Token_1$ $\pi_1^A, \pi_1^B, \pi_1^C$	$COMM(10^6, r_2)$ $Token_2$ $\pi_2^A, \pi_2^B, \pi_2^C$	$COMM(0, r_3)$ $Token_2$ $\pi_3^A, \pi_3^B, \pi_3^C$	... ...	$COMM(0, r_n)$ $Token_n$ $\pi_n^A, \pi_n^B, \pi_n^C$

图 9 银行保密审计(引自[27])

Figure 9 Bank confidential audit (Citation[27])

当审计者要审计某一银行的现有资产时, 银行回复其资产和一个证明(证明其回答和账本内容一致)给审计者。审计者结合银行的账本内容对反馈的信息进行验证。若通过, 则接受银行的回复。这个隐私保护与审计方法适合应用在节点数量不多的联盟链中, 另外方案只关注资产金额的审计。

Zheng 等人[28]设计了可链接的群签名, 可用来实现交易的匿名、可审计和可追踪功能。群签名拥有群管理者, 可以追踪签名者的身份。可链接的性质保证其他用户可以判断两个交易是否来自同一个发送者, 从而统计出用户发送交易的频率, 识别有异常的用户。

Li 等人[29]在 Zerocash 隐私保护方案的基础上提出了一种监管方案。其方案的设计思路是, 监管方给每一个受监管的用户颁发对称加密密钥; 受监管的用户对交易相关信息(发送者地址、接收者地址、交易金额)用对称密钥进行加密, 密文写在交易中。采用零知识证明保证加密的信息和交易信息是一致的。监管方用手中的私钥尝试一一解密每一个密文, 获得被监管者的交易内容。

总结上述区块链监管的工作, 有关身份的可追踪, 目前采取单个追踪机构[25]或多个服务器[26]协同实现。文献[25]中用户每次产生新的地址都要去注册中心认证一遍, 增加了注册中心的负担。文献[26]的方案, 用户只需去注册中心认证一次, 后续产生公私钥不必再去访问注册中心。注册中心只颁发证书, 无法追踪用户身份, 身份的追踪交由多个服务器协同完成。证书的验证需要多个服务器执行安全多方计算协同验证, 较为复杂。另外群签名的方法也可以用于用户身份追踪[28], 群管理员可以追踪签名的签署者是谁。假设用户的公钥不变, 公钥即代表用户身份。群签名比较适合用户数量数不多的联盟链中。

有关内容的监管, 文献[27]的方案可实现银行资产的查询, 文献[28]的方案可审计用户产生交易的频率, 即同一时间段内一个用户发出了多少条交易。Li 等人[29]的方案是针对 Zerocash 提出的监管策略, 其监管方式较为直接, 监管者用私钥尝试解密即可获得被监管者的交易信息。不过证明效率不高, 这个问题也是 Zerocash 本身存在的问题。

4 总结

区块链隐私保护和监管研究已经取得了一些重要研究成果。由于区块链应用场景复杂、需求多样化, 该研究方向还需要进行大量的研究工作。前面我们已经指出了目前已有工作存在的一些问题。通过对已有问题的总结, 结合区块链今后的发展趋势, 我们给出了区块链隐私保护和监管未来研究的几个热点方向。

- **联盟链的细粒度隐私保护**: 联盟链作为一种受限准入的区块链受到政府机构、军事部门和企业的广泛关注。目前对联盟链上的隐私保护问题关注较少, 前面提到的 Quorum 和 Coco 框架要么通用性不强要么依赖可信的硬件。根据联盟链的特点, 如何借鉴公有链的隐私保护方法实现联盟链的细粒度隐私保护是后续需要研究的问题。
- **智能合约隐私保护**: 除了区块链中交易的隐私, 以太坊等区块链的智能合约隐私也备受关注。智能合约的隐私保护包括合约代码本身的保密和合约输入输出的保密, 代码或输入输出的公开都可能泄漏用户的敏感信息, 因此对智能合约的隐私保护问题也是值得研究的方向。
- **高效的身份追踪机制** 目前针对区块链的监管研究工作较少。已有的监管方案还存在诸多问题, 身份追踪中用户需多次访问注册中心或需多个服务器协同追踪。需进一步研究高效实用的身份追踪技术。
- **更多场景下的内容监管技术研究**: 有关用户内容的监管, 目前工作适用场景、审计操作较单一。不同场景下, 监管的需求也不尽相同。监管还可能包含: 区块链交易金额的大额筛查技术、敏感内容保密检索、大数据分析等; 另外监管操作的授权问题也是值得研究的内容; 进一步的, 监管除了对内容进行审计, 还可以赋予内容纠错等功能。

参考文献

[1] Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). Available at http://bitcoin.org/bitcoin.pdf.

[2] ZOU J, ZHANG H N, TANG Y, et al. Guidelines for Blockchain Technology[M]. Beijing: China Machine Press.2016:97-99.
(邹均, 张海宁, 唐屹, 等.区块链技术指南[M]. 北京:机械工业出版社, 2016: 97-99.)

[3] Wang H, Song X F, Ke J M, et al. Blockchain and Privacy Preserving Mechanisms in Cryptocurrency[J]. *Netinfo Security*, 2017(7): 32-39.
(王皓, 宋祥福, 柯俊明, 等. 数字货币中的区块链及其隐私保护机制[J]. *信息网络安全*, 2017(7): 32-39.)

[4] Chaum, D. Untraceable electronic mail, return addresses,and digital pseudonyms[J]. *Communications of the ACM* 24(2): 84-88 (1981).

[5] Bonneau J, Narayanan A, Miller A, et al. Mixcoin: Anonymity for

Bitcoin with Accountable Mixes[C]. *Financial Cryptography and Data Security*, *2014*: 481–499.

[6] Valenta L, Rowan B. Blindcoin: Blinded, Accountable Mixes for Bitcoin[C]. *International Conference on Financial Cryptography and Data Security*, 2015:112-126.

[7] Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. post on bitcoin forum. 2013, https://bitcointalk.org/index.php?topic= 279249

[8] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin[C]. *European Symposium on Research in Computer Security*. 2014: 345-364.

[9] Ruffing T, Moreno-Sanchez P, Kate A. P2P Mixing and Unlinkable Bitcoin Transactions[C]. *2017 Network and Distributed System Security Symposium*, 2017.

[10] Ruffing T, Moreno-Sanchez P. ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin[C]. *Financial Cryptography and Data Security*, 2017: 133-154.

[11] Pedersen T P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[C]. *Advances in Cryptology — CRYPTO '91*, 1991: 129-140.

[12] Zhu L H, Gao F, Shen M, et al. Survey on Privacy Preserving Techniques for Blockchain Technology[J]. *Journal of Computer Research and Development*, 2017, 54(10): 2170-2186.
(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.)

[13] Chandran N, Groth J, Sahai A. Ring Signatures of Sub-linear Size Without Random Oracles[C]. *International Conference on Automata, Languages and Programming*, 2007:423-434.

[14] Bergan T, Anderson O, Devietti J, et al. CryptoNote v 2.0[J]. 2013. https://cryptonote.org/whitepaper.pdf

[15] Ruffing T, Moreno-Sanchez P. ValueShuffle: Mixing Confidential Transactions for Comprehensive Transaction Privacy in Bitcoin[C]. *International Conference on Financial Cryptography and Data Security*, 2017:133-154.

[16] Noether S. Ring Signature Condential Transactions for Monero. Cryptology eprint Archive, Report 2015/1098, 2015. http://eprint.iacr.org/.

[17] Sun S F, Man H A, Liu J K, et al. RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero[C]. *European Symposium on Research in Computer Security*, 2017:456-474.

[18] Miller A, Moeser M, Lee K, et al. An Empirical Analysis of Linkability in the Monero Blockchain[J]. CoRR abs/1704.04299 (2017).

[19] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin[C]. *2013 IEEE Symposium on Security and Privacy*, 2013: 397-411.

[20] Ben Sasson E, Chiesa A, Garman C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]. *2014 IEEE Symposium on Security and Privacy*, 2014: 459-474.

[21] Ben-Sasson E, Chiesa A, Tromer E, et al. Succinct non-interactive zero knowledge for a von Neumann architecture[C].*Usenix Conference on Security Symposium. USENIX* Association, 2014: 781-796.

[22] Pedersen T P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing[C]. *Advances in Cryptology — CRYPTO '91*, 1991:129–140.

[23] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]. *2016 IEEE Symposium on Security and Privacy*, 2016: 839-858.

[24] Zhang X, Jiang Y Z, Yan Y. A Glimpse at Blockchain: From the Perspective of Privacy[J]. *Journal of Information Security Research*, 2017, 3(11): 981-989.
(张宪, 蒋钰钊, 闫莺. 区块链隐私技术综述[J]. *信息安全研究*, 2017, 3(11): 981-989.)

[25] Giuseppe Ateniese, Antonio Faonio, Bernardo Magri, ,et al. Certified Bitcoins[C]. *ACNS, 2014:* 80-96.

[26] El Defrawy K, Lampkins J. Founding Digital Currency on Secure Computation[C]. *The 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014: 1-14.

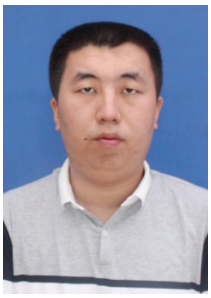
[27] Narula Neha, Willy Vasquez, Madars Virza. Privacy-Preserving Auditing for Distributed Ledgers[C]. *NSDI*, 2018: 65-80.

[28] Zheng H B, Wu Q H, Qin B, et al. Linkable Group Signature for Auditing Anonymous Communication [C]. *Australasian Conference on Information Security and Privacy*, 2018: 304-321.

[29] Li C X, XU W. Blockchain Privacy Protection and Supervision Based on Zero Knowledge Proof[J]. Communication of China Cryptography Society, 2018, 5: 21-29.
(李辰星, 徐葳. 基于零知识证明的区块链隐私保护与监管. [J] *中国密码学会通讯*, 2018, 5: 21-29.)

李佩丽 2016 年在中国科学院信息工程研究所信息安全专业获得博士学位, 现任中国科学院信息工程研究所助理研究员。研究领域为密码学、安全协议。研究兴趣包括: 区块链隐私保护与监管, 外包计算。Email:lipeili@iie.ac.cn

徐海霞 2001 年在首都师范大学数学专业获得博士学位, 现任中国科学院信息工程研究所副研究员。研究领域为密码学、安全协议。研究兴趣包括: 区块链, 数字货币, 安全多方计算。Email: xuhaixia@iie.ac.cn



马添军 2014 年在山西大学软件工程专业获得学士学位, 现在中国科学院信息工程研究所攻读博士学位。研究领域为: 密码学、区块链。研究兴趣包括: 数字货币, 智能合约。Email: matianjun@iie.ac.cn