软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(7):2260−2286 [doi: 10.13328/j.cnki.jos.006309]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链系统中身份管理技术研究综述*

姚 前[1], 张大伟[2,3]

[1](中国证券监督管理委员会 科技监管局,北京 100032)

[2](北京交通大学 计算机与信息技术学院,北京 100044)

[3](智能交通数据安全与隐私保护技术北京市重点实验室,北京 100044)

通讯作者: 张大伟, E-mail: dwzhang@bjtu.edu.cn

摘 要: 区块链技术是一种通过块链式结构、共识算法和智能合约来生成、存储、操作和验证数据的新型分布式基础架构和计算范式,其所构建的新型信任机制有助于推动互联网技术由信息互联网向价值互联网的转化.由于区块链中的账本数据采用公开交易记录、多节点共识确认的方式进行存储和验证,因此对系统中的身份管理及隐私保护提出了极大的挑战.首先分析了区块链系统交易模型的特点及其与传统中心化系统在身份认证、数据存储和交易确认方面的不同,阐述了区块链系统中身份管理技术涵盖的主要内容、关键问题及安全挑战;其次,从身份标识、身份认证和身份隐藏 3 个方面比较分析了目前主流区块链平台中身份管理和隐私保护的不同实现技术;最后,分析了现有区块链系统中身份管理的不足并对未来的研究方向进行了展望.

关键词: 区块链;密码货币;身份管理;隐私保护;匿名性;不可链接性

中图法分类号: TP311

中文引用格式: 姚前,张大伟.区块链系统中身份管理技术研究综述.软件学报,2021,32(7):2260−2286. http://www.jos.org.cn/1000-9825/6309.htm

英文引用格式: Yao Q, Zhang DW. Survey on identity management in blockchain. Ruan Jian Xue Bao/Journal of Software, 2021,32(7):2260−2286 (in Chinese). http://www.jos.org.cn/1000-9825/6309.htm

Survey on Identity Management in Blockchain

YAO Qian[1], ZHANG Da-Wei[2,3]

[1](Science and Technology Supervision Bureau, China Securities Regulatory Commission, Beijing 100032, China)

[2](School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

[3](Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing 100044, China)

Abstract: Blockchain technology is a new distributed infrastructure and computation paradigm that generates, stores, manipulates, and validates data through chain structures, consensus algorithms, and smart contracts. The new trust mechanism is built to promote the transformation of Internet technology from Internet of information to Internet of value. Since the data in the blockchain is stored and verified by means of public transaction records and multi-peer consensus confirmation, it poses a great challenge to the transaction privacy protection in the system. This study first analyzes the characteristics of the blockchain system transaction model and its differences from the traditional centralized system in identity authentication, data storage and transaction confirmation, and describes the main contents, key issues and security challenges of identity management in blockchain. Secondly, the different implementation technologies of identity management and privacy protection are analyzed in the current mainstream blockchain platform from three aspects, namely, identity identification, identity authentication, and identity hiding. Finally, the shortcoming of the existing blockchain identity management technology issummarized and the future research directionsare proposed.

* 基金项目: 国家重点研发计划(2020YFB2103802); 国家自然科学基金(U1736114)

Foundation item: National Key R&D Program of China (2020YFB2103802); National Natural Science Foundation of China (U1736114)

收稿时间: 2020-08-13; 修改时间: 2020-11-10; 采用时间: 2021-01-15; jos 在线出版时间: 2021-02-07

Key words: blockchain; cryptocurrency; identity management; privacy protection; anonymity; unlinkability

起源于比特币[1]的区块链是一种基于链式数据结构的分布式共享账本技术,被视作继大型机、个人电脑以及互联网之后计算模式的又一次颠覆式创新,其去中心化的分布式数据存储、多方维护、共识确认和不可篡改的特性为解决传统中心化系统的数据存储不安全和共享性差等问题提供了新的思路.随着人们对区块链技术的深入研究,区块链系统也从单一的去中心化公有链发展到今天开放式的公有链、具有准入机制的联盟链和私有链并存的多种技术形态,并在行业应用中得到了普及和推广.区块链技术很可能对当今互联网产生颠覆式的影响[2,3].

区块链系统在提供了灵活的分布式协同处理优势的同时,也对参与方的身份管理提出了极大的挑战.在传统的中心化交易系统中,交易由中心机构统一核验确认,且交易账本内容不公开.而在区块链交易系统中,为了实现去中心化的目标,大多采用类似于b-money[4]的设计思想,公开所有的交易记录并由网络中的特定节点采用多方共识确认的方式对交易进行背书核验.这一新型交易模式对身份管理提出了两方面的挑战:首先,如何在去(多)中心开放网络环境下安全、高效地实现用户身份的标识、认证和资产确权;其次,如何确保账本公开、多方共识情况下的身份隐私保护.因此,深入研究区块链系统中的身份管理技术具有极其重要的意义.

区块链系统中的身份管理是区块链应用中实体之间进行通信交互和资产交易的基础,它包含对实体身份从产生、存储、认证、使用、审计到注销的全生命周期的管理.身份管理一直是区块链系统中的关键组件,也是构建区块链系统安全的基础.随着区块链技术的普及和发展,区块链已从传统的去中心化密码货币发展到今天公有链、联盟链和私有链并存的多种技术形态,其系统架构、信任模型和安全需求也日益多元化.由此也对区块链系统中的身份管理技术提出了挑战.因此,系统地梳理区块链身份管理的相关工作,科学地提炼出其中的共性关键问题对未来区块链行业应用的发展至关重要.目前国内外已有多篇文献对区块链系统中的安全隐私问题进行了研究,但仍然缺乏对区块链身份管理技术的深入探讨和系统性综述研究.2017 年,祝烈煌等人[5]从身份隐私和交易隐私两方面分析了区块链中网络层、交易层和应用层的隐私问题;2018 年,Genkin 等人[6]重点对基于公有链的密码货币中的身份隐私问题进行了讨论;2019 年,付烁等人[7]对密码货币的匿名性问题进行了研究,重点讨论了中心化和去中心化密码货币中的身份隐私问题;2020 年,张奥等人[8]依据隐私保护的不同技术手段从地址混淆、信息隐藏、通道隔离这 3 方面主要对公有链中的隐私保护机制进行了研究.上述工作多以公有链密码货币为研究对象,部分涉及到了身份隐私保护问题,但并未对身份管理全生命周期过程中所涉及到的身份标识、资产确权、身份认证和隐私保护问题进行系统性的研究和梳理.此外,也未对公有链和联盟链交易过程中涉及到的身份管理共性问题,如资产权属标识和交易确权、交易身份认证和动态身份隐藏等展开更深入的讨论.本文的工作对近年来区块链身份管理技术进行了系统性的梳理.从公有链和联盟链系统中身份管理的共性问题出发,通过比较区块链与传统中心化系统在交易模型和隐私保护上的差异,阐述了区块链系统中身份管理的主要内容,分析了身份管理所面临的威胁及挑战,并由此认为,在身份标识和认证方面,区块链与中心化系统中的身份管理面临着更多的共性问题并沿用了传统中心化系统的技术体系;而在隐私保护方面,二者存在较大差异,区块链系统只有通过引入身份隐藏技术才能有效地解决公开账本下的交易身份隐私保护问题.基于这一观点,本文随后从身份标识、身份认证和身份隐藏 3 个方面对主流区块链平台中的身份管理和隐私保护技术进行了对比分析,从其所涉及的设计思路、密码算法和安全协议等方面进行了深入的探讨,并对相关技术的未来发展进行了展望.

本文第 1 节通过与传统中心化交易系统进行对比分析,总结区块链系统交易模型的特点.基于上述特点,总结区块链身份管理的主要内容,阐述区块链身份管理所面临的威胁及挑战.第 2 节分析总结区块链系统中的身份标识技术.第 3 节对比分析区块链系统中的身份认证技术.第 4 节提出交易过程中的动态身份隐藏是解决区块链身份隐私保护的关键问题,并对比分析目前主流区块链平台中实现交易身份隐藏所采取的不同技术手段:如协同混币技术、自主混币技术、全局混币技术和无标识交易技术.第 5 节归纳总结现有区块链系统的身份管理技术,并对未来的研究方向进行展望.第 6 节是结束语.

1 区块链中的身份管理问题

1.1 区块链交易模型

区块链系统中的交易在交易模型方面与传统系统有着很大的不同.首先,在传统系统中,所有交易过程的记录和确认都是由系统的中心机构集中来完成的.而在区块链系统中,客户端首先将交易发送到区块链网络中,由网络中的特定节点来对交易进行背书确认,确认后的交易才能写入区块链账本中并全网分发[1].传统交易系统与区块链交易系统的比较如图 1 所示.

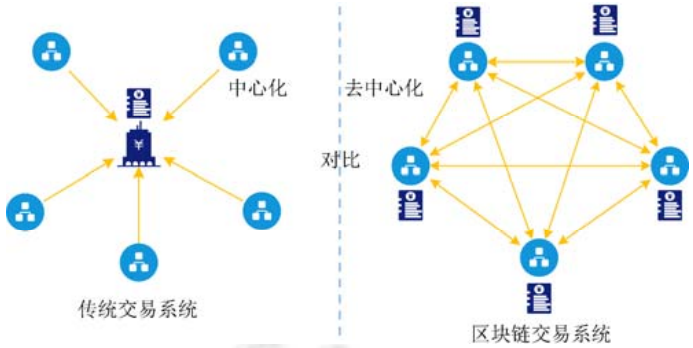


Fig.1 Comparison between traditional transaction system and blockchain transaction system

图 1 传统交易系统与区块链交易系统的比较

其次,在交易结构的表示方面,以比特币为代表的公有链(如:达世币[9]、门罗币[10]、零币[11]等)、央行数字货币原型系统 RSCoin[12]和一些联盟链(如:Corda[13]、Fabric[14]中的 Fabcoin[15]等)大多采用了未花费交易(unspent transaction output,简称 UTXO)的表示方法.每一单元的 UTXO 代表特定属主的一定数值的数字资产,对手方之间的一笔交易由若干输入和输出 UTXO 组成,输入的 UTXO 代表交易发送方支出的数字资产,输出的 UTXO 代表交易接收方收到的数字资产,可在将来作为输入的 UTXO 来使用.支付过程中产生的找零输出也会发送回交易发送方.简言之,UTXO 是一种带有属主信息和资产数量的编码型数字资产表达方式.基于 UTXO 模型的交易结构如图 2 所示.

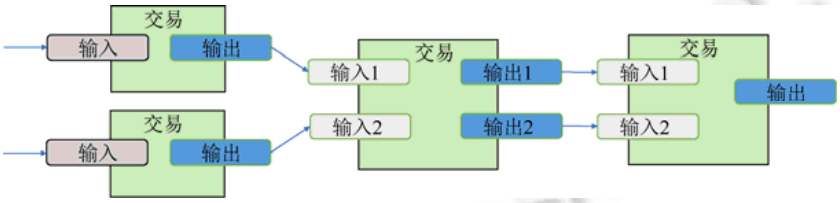


Fig.2 UTXO structures in blockchain system

图 2 区块链系统中的 UTXO 交易结构

公有链的另一个典型代表项目以太坊[16]则采用了传统的基于账户的交易模型.用户的以太坊账户中存有当前余额、交易次数、账户信息哈希值等,交易的发生反映到不同账户的余额变化上.为了便于以太坊上代币(token)的使用,以太坊社区制订了 ERC 20 标准[17]用于描述在智能合约中实现代币的标准 API,这些 API 主要提供了代币使用的一些基本功能,如转移代币、授权代币给第三方使用等.

从身份管理和隐私保护的角度来分析,传统中心化系统与区块链系统存在着显著差异.

(1) 在身份认证方面,传统交易系统采用中心化集中实名认证机制;区块链系统则大多采用用户匿名的身份认证机制,用以确保用户隐私;

(2) 在账本数据存储方面,传统交易系统采用由中心机构集中统一存储的方式,账本数据安全由存储机构确保且账本内容不公开;区块链交易系统采用全网节点共同存储账本的方式,账本数据安全由共识机制、块链式数据结构共同确保且账本内容公开、透明;

(3) 在交易内容确认方面,传统交易系统采用由中心机构统一核验、确认的中心化确认方式;而在区块链交易系统中,为了实现去(多)中心化的目标,大多采用类似于 b-money[4]的设计思想,公开所有的交易记录并由网络中的特定节点对账本进行多方共识确认.但这些交易记录结构中包含了大量的用户历史交易信息,观察者基于 UTXO 结构非常易于分析获得用户的身份隐私信息.

综上所述,区块链系统中的交易模型采用 UTXO 结构详细记录了交易流转过程,并将传统交易系统中的用户实名、账本保密的隐私保护方式变更为用户匿名、账本公开的方式,将由中心机构集中确认交易变更为全网节点多方共识确认交易.这一新型交易模型对区块链系统中的身份管理及隐私保护都提出了更大的挑战.

1.2 区块链身份管理的主要内容

区块链系统中的身份管理主要包括 3 方面的内容:身份标识、身份认证和身份隐藏.其中,身份标识是构成链上资产权属标记和支付确权的基础,而身份认证和身份隐藏方式则与交易身份的隐私保护密切相关.

1) 身份标识

身份标识是指区块链系统中用于标识交易用户身份的一种模式.在目前的区块链系统中,大多基于密码算法和认证协议来实现身份标识.此外,在交易过程中,身份标识还涉及到另外两方面的内容:首先,如何形成有效的身份标识符以用于资产(如 UTXO)的权属标记并支持基于标识符的支付确权;其次,出于隐私保护的目的,交易方大多拥有多个身份标识符,例如多对公私钥对,从而带来了相应的密钥管理问题.如何有效地在客户端管理用户的多身份标识符并优化存储空间和执行效率也是需要关注的问题.

2) 身份认证

身份认证是指在区块链系统中确认交易者身份的过程,从而确定该用户是否具有对交易数据的访问和使用权限以及对交易行为的确认和不可抵赖.区块链系统中的身份认证又可分为如下 3 种.

(1) 匿名认证

在用户身份标识的建立和认证过程中,不允许直接或间接确定交易者的真实身份.

(2) 实名认证

在用户身份标识的建立和认证过程中,应直接或间接地确定交易者的真实身份.

(3) 可控匿名认证

在用户身份标识的建立和认证过程中,除监管方以外不允许直接或间接确定交易者的真实身份.在必要时,监管方可恢复出匿名化后交易方的真实身份.

3) 身份隐藏

由于区块链系统具有账本公开、多方确认的特点,使得简单使用匿名认证技术难于保证交易方的身份隐私,因此引入了身份隐藏技术以用于实现动态交易过程中的身份隐私保护.交易身份隐私是指对于区块链系统中的某笔交易,观察者无法将交易发送方和接收方的身份与该笔交易相关联.观察者主要是指除交易参与方和监管方以外的第三方.这一定义包括两方面的内容:首先,观察者无法确认某笔交易发送方和接收方的身份.假设区块链系统中交易用户(身份)的总数为 N,理想情况下,观察者准确确认交易方身份的概率为 $1/N$;其次,系统应确保交易身份的不可链接性.即观察者无法将同一用户的不同身份链接起来;观察者也无法将一笔交易的发送方和接收方的身份链接起来.在具体交易场景中,交易身份隐私保护又可细分为交易发送方的身份隐私保护和交易接收方的身份隐私保护.因此,在交易过程中,必须采取特定的身份隐藏技术将交易方的身份隐藏在一定的匿名集合中,从而实现发送和接收方的身份隐藏,以达到隐私保护的目的.

1.3 区块链身份管理的威胁与挑战

区块链系统所采用的去(多)中心化模式下基于公开账本的交易多方共识确认模型在提供了高效的信任构

建方法的同时,也带来了更多的身份管理和隐私保护问题.其威胁主要包括:

(1) 区块链系统采用了交易账本全网公开的方式来存储全部的历史交易数据,区块链系统中的所有节点都可以看到上链数据并追溯交易流程,这给上链的身份隐私带来威胁;

(2) 区块链系统采用多方共识方式来完成交易的确认,参与共识的节点必然需要掌握更多的交易信息以实现交易确权验证,一旦共识节点出现问题,必然会给交易信息中的身份隐私带来威胁;

(3) 区块链系统中采用的UTXO模型表示方法在有效地刻画了数字资产交易流转的同时,也带来了隐私保护的问题.首先,UTXO以编码形式在公开账本中记录数字资产,这为信息追踪和阈下信道的利用提供了便利;其次,UTXO模型中清晰表达了输入输出UTXO间的关系以及权属变更过程,如:同一交易的多个输入可能属于使用不同地址(公钥)的同一所有者;交易输出的找零地址与输入地址为同一持有人等.相关研究工作表明,这些特点为身份追踪提供了极大的便利.

在传统交易系统中,用户是向中心机构公开交易身份,由中心机构完成身份管理和隐私保护.而区块链系统中并无单一中心机构,而是依靠系统整体安全机制来实现安全和隐私保护.区块链系统一旦身份管理的保护机制出现问题,所带来的后果会是向所有参与方公开交易身份和交易内容,这对于承载高价值信息的系统而言是无法接受的.因此,确保区块链系统参与方的身份隐私安全具有非常重要的意义.

但是受限于区块链系统中交易模型的设计,身份管理和隐私保护方案也面临着如下一些技术挑战.

(1) 交易身份是区块链系统中数字资产权属表达的重要方式,区块链存储的交易账本公开且交易记录易被追溯,简单的身份匿名机制无法达到隐私保护的要求.因此,如何有效地解决公开账本下动态交易过程中的身份隐私是所面临的主要挑战之一;

(2) 区块链系统采用多方共识方式来实现交易的确认和信任的构建,有时交易双方对于作为观察者的验证节点来说是存在交易身份隐私保护需求的,简单的信息隐藏方法无法满足既保护信息又可验证内容的需求.因此,如何在保护交易身份隐私的同时实现正确、有效的交易验证具有一定的挑战性;

(3) 区块链系统中采用多方确认后通过公开信道(区块链账本)进行交易信息发布,这一过程耗时较长.因此,在区块链系统中大多采用交易发送方到区块链网络节点的单向通信方式.这使得传统交易系统中的多轮双向交互的身份认证和隐私保护协议不再适用.因此,如何在区块链系统单向传输交易数据的过程中实现身份认证和隐私保护也具有一定的挑战性;

(4) 随着区块链系统在行业应用中的不断普及和发展,行业监管与隐私保护之间的矛盾也逐渐凸显.一方面,区块链系统中缺乏单一的交易中心机构;另一方面,传统的公有链中无监管式的隐私保护方法又不适合于很多现实应用场景.因此,如何在实现隐私保护的同时又可提供对于交易身份的监管也有待进一步研究.

2 区块链系统中的身份标识

在用户身份管理方面,目前的区块链系统大多基于非对称密码算法来实现用户的身份标识.但公有链和联盟链在具体实现方案上存在较大的差异.公有链中的比特币、以太坊、门罗币、零币和Libra[18]等强调用户的隐私保护,采取匿名身份认证机制,用户公钥作为身份标识符,用户自主生成和管理标识身份的密钥;以Fabric和Corda等为代表的联盟链则更关注强监管环境下客户身份识别(know your customer,简称KYC)的需求,采取实名或可控匿名的身份认证机制,使用数字证书作为身份标识符,采用证书认证中心(certificates authority,简称CA)来生成和管理数字证书.

2.1 公钥标识身份

目前区块链系统大多基于公钥密码体系的椭圆曲线密码算法来构建用户的身份标识.以比特币为例,在比特币交易中用户的身份标识符 A 称为比特币地址(address),其长度为160比特,是由用户公钥 P 通过SHA 256和RIPEMD 160的两次哈希运算(HASH160)而生成.其运算过程如下:

$$A=\text{HASH 160}(P)=\text{RIPEMD 160}(\text{SHA 256}(P)).$$

为了实现数字资产的权属标识,在比特币的UTXO中使用用户的身份标识符(地址)A 来明确标识当前

UTXO 属于用户 *A*,并通过 *A* 来控制 UTXO 的支付.比特币的支付过程是由交易脚本(script)来完成的,对于属于 *A* 的 UTXO 进行支付的交易脚本可描述为

⟨*Sig*⟩⟨*P*⟩ DUP HASH 160 ⟨*A*⟩ EQUALVERIFY CHECKSIG

为了花费 UTXO,用户必须提供公钥⟨*P*⟩和对应的私钥 *d* 所生成的交易数字签名⟨*Sig*⟩,并通过判断公钥⟨*P*⟩的 HASH 160 运算结果是否与⟨*A*⟩相等和签名验证是否通过来进行支付确权.比特币使用了基于堆栈结构的脚本语言来完成上述操作,脚本的执行过程如下.

(1) 将用户数字签名⟨*Sig*⟩压入堆栈;

(2) 将用户公钥⟨*P*⟩压入堆栈;

(3) 执行栈顶元素复制指令 DUP,将用户公钥⟨*P*⟩复制并压入堆栈;

(4) 弹出栈顶元素⟨*P*⟩并执行指令 HASH 160 计算 HASH 160(*P*),并将计算结果压入栈中;

(5) 将身份标识⟨*A*⟩压入栈中并执行指令 EQUALVERIFY,弹出栈顶两个元素并判断二者是否相等;

(6) 弹出⟨*Sig*⟩和⟨*P*⟩并执行指令 CHECKSIG,计算交易哈希值并判断签名是否正确.

由上述操作可见,比特币基于非对称密码算法的公私钥对和签名验签实现了对链上数字资产的权属标识和支付确权.

此外,为了实现交易过程中的身份隐私保护,交易地址在每次交易时可动态生成,即同一个用户通过使用多个不同的身份标识符(假名)来降低交易地址与真实身份以及不同交易之间的关联性,这带来了钱包端密钥管理的问题.目前,比特币提供了两种解决方案.第 1 种方案中用户私钥通过随机数动态地临时生成,再计算对应的公钥.随着密钥数量的增加,这会极大地增加密钥管理的开销;第 2 种方案中用户在比特币钱包中存储根私钥,使用时通过密钥派生算法来生成临时公私钥对,支持这一方法的钱包也称为 HD(hierarchical deterministic)钱包[19].在比特币 BIP 32 协议中对生成算法有详细的描述,它基于椭圆曲线的密钥叠加特性,即私钥叠加对应的公钥也会叠加,利用父密钥和索引逐级派生出子密钥,这一方法可以有效地降低钱包端的密钥管理开销.其基本结构如图 3 所示.

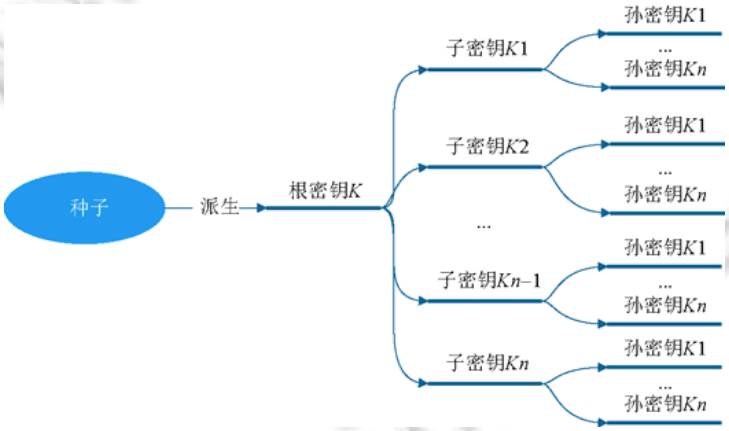


Fig.3 Key derivation in bitcoin HD wallet

图 3 比特币 HD 钱包密钥派生结构

此外,在点对点分布式存储系统 IPFS[20]中,还将公钥标识方法用于节点地址生成,采用公钥哈希作为节点的身份标识.更多的公有链将这一方法用于用户身份生成.例如,以太坊平台同样采用椭圆曲线密码算法生成用户身份标识(账户地址),并直接用于标识账户所有权,与比特币不同的是,以太坊使用 Keccak 256 哈希函数来生成用户地址.公有链中的门罗币则采用了两对公私钥对来实现身份标识,同时也采取了类似的密钥派生技术来实现钱包端的密钥管理,详细内容可参见第 4.3 节.零币在交易接收地址上使用了一对公私钥对来作为身份标识,但在货币权属标记方面则采用了基于零知识证明的方案.零知识证明是指一种证明者向验证者证明他知道

某个秘密而同时又不泄露任何秘密信息的方法,这一过程需满足正确性、完备性和零知识性.零知识证明实质上是一种涉及两方或更多方的协议,因此又可分为交互式零知识证明和非交互式零知识证明.交互式零知识证明是指证明者和验证者通过不断交换信息来完成证明.从知识复杂性的角度来看,交互式零知识证明就是证方传递的知识为 0 的交互式证明系统.非交互式零知识证明是指证明者和验证者无需多次交互也能达到零知识证明的效果.目前在区块链系统中大多使用非交互式零知识证明来实现交易身份隐私保护,零币的相关内容可参见第 4.4 节.

2.2 数字证书标识身份

以 Fabric 和 Corda 等为代表的联盟链则更关注强监管环境下客户身份识别(know your customer,简称 KYC)的需求,均提供了基于数字证书的用户身份标识,以实现实名或可控匿名认证.

例如在 Linux 基金会所主导的开源联盟链平台 Hyperledger Fabric[14]中,Fabric 的成员服务(membership services,简称 MSP)为区块链网络提供用户注册、身份管理和审计服务.Fabric 中默认的 MSP 实现使用 X.509 证书作为身份标识符,采用传统的公钥基础结构(public key infrastructure,简称 PKI)分层模型,并支持 RSA 和 ECDSA 公钥密码算法.PKI 通过引入 CA 机构为注册真实身份的用户颁发数字证书,数字证书包含用户的身份信息、用户的公钥信息、CA 数字签名和有效期等信息.数字证书作为身份标识符与用户具有一一映射关系.在区块链交易过程中,数字证书可替代公钥来作为数字资产的权属标记,用户使用对应的私钥签名来完成支付行为的确认.此外,CA 负责数字证书的全生命周期管理,包含数字证书的签发和更新,数字证书的撤销、查询或下载等.数字证书的申请、发布和使用如图 4 所示.

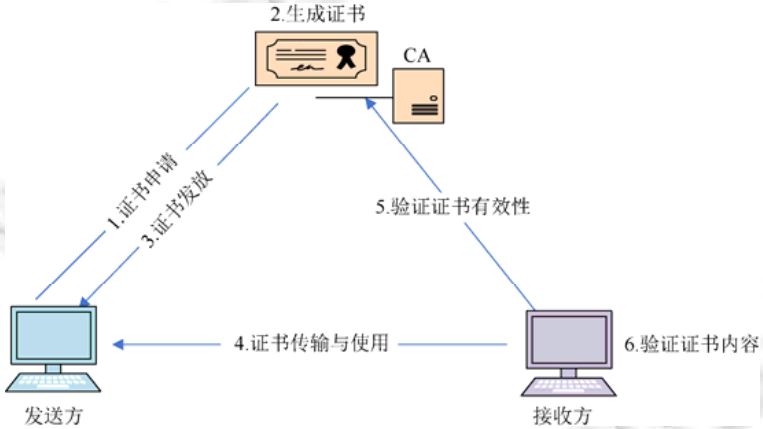


Fig.4 Management and use of certificates

图 4 数字证书的管理和使用

更多的基于数字证书的身份管理机制可参见第 3.2 节和第 3.3 节.

2.3 DID标识身份

W3C 组织将分布式数字身份标识符(decentralized identifier,简称 DID)[21]定义为一种新型的支持可验证、分布式数字身份的标识符,可用来标识人、组织、物品、抽象实体等任意主体.一般而言,数字身份通常由身份标识符及与之相关联的属性声明来表示,分布式数字身份是基于区块链去中心化特点来构建的一种扁平化、弹性化的身份管理模式,通过将身份数据所有权归还用户来解决隐私保护问题.分布式数字身份包括:分布式数字身份标识符和数字身份凭证(声明集合)两部分.W3C 的 DID 规范和可验证凭证(verifiable credential)规范[22]分别定义了代表实体的身份标识符 DID 及与之关联的属性声明.

实体在注册申请后可获得一个 DID 或多个 DID,并由自己进行管理、维护,不同 DID 所代表的身份之间没有关联性,可有效保护身份隐私.同时,每个 DID 会对应一个 DID Document.DID Document 是一个通用数据结构,

它包含与DID验证相关的密钥信息和验证方法(目前大多为公钥和数字签名),提供了一组使DID控制者能够证明其对DID控制的机制.实体在需要进行身份信息证明时,可向相关发行方申请可验证凭证,用于实现对实体特定属性的声明.可验证凭证通常由至少两组信息组成:其一表示可验证的凭证本身,包含凭证元数据(metadata)和声明(claim);其二表示数字证明,通常是数字签名.经过上述过程,分布式数字身份系统即可通过DID来标识一个实体,通过可验证凭证来向身份验证方出示实体所具有的身份属性信息,并证明自己的属性是可信的,从而完成身份认证过程.一个实体的分布式数字身份的组成如图5所示.

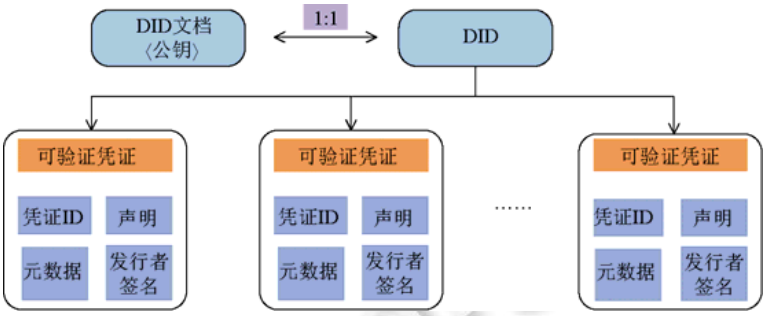


Fig.5 Composition of distributed digital identity

图5 分布式数字身份的组成

在分布式数字身份模型中,基于区块链系统将身份标识符的生成、维护与身份属性声明的生成、存储和使用相分离,有助于构建一个分布式、模块化和更具弹性的身份服务生态系统.目前国内外已有多个项目基于区块链系统实现了分布式数字身份.例如,国内微众银行的WeIdentity项目[23].此外,为了满足属性证明过程中特定的隐私保护需求,WeIdentity项目还提供了选择性信息披露的功能.发行方在构建可验证凭证签名时,将声明中的不同字段分别计算哈希值再连接其他信息进行签名.实体在进行身份证明时,希望披露的字段能够提供原文,隐藏字段仅提供哈希值.这样,验证方就仍可连接所有字段的哈希值并正确地验证签名.

综上所述,分布式数字身份提供了一种更灵活的身份标识和属性证明方法.但从目前的方案来看,DID仍然是基于非对称密码技术来实现的,用户身份与一对公私钥仍形成绑定关系并通过签名实现对DID使用的控制.因此,DID在区块链交易系统中标识资产权属时仍然可以使用与现有系统同样的方法,但也会面临相同的安全隐私威胁.

3 区块链系统中的身份认证

3.1 匿名(假名)认证

公有链中的比特币、以太坊、门罗币和零币等强调用户的身份隐私保护,为交易用户提供了匿名认证,即用户在注册过程中无需出示真实身份即可获得身份标识并将其用于身份认证.由于系统采用无准入机制的开放网络架构,系统中无类似CA的可信认证中心来管理身份,用户基于非对称密码算法自主生成和管理身份,采用第2.1节中的方法实现身份标识,即采用公钥作为身份标识符、私钥签名实现身份认证,身份管理的全周期过程中用户都是匿名的.此外,为了实现交易过程中的身份隐私保护,同一用户还可通过使用多个不同的身份标识符(假名)来降低交易地址与真实身份以及不同交易之间的关联性.

虽然匿名认证能够在一定程度上保护用户隐私,但值得注意的是,由于区块链交易系统具有账本公开、多方确认的特点,简单使用匿名(假名)认证并不能完全有效地解决交易身份隐私保护的问题.因此,必须引入相应的身份隐藏机制来解决动态交易过程中的身份隐私保护问题,详细内容可参见第4节.

3.2 实名认证

为了实现用户的准入控制并符合交易监管要求,Fabric、Corda、趣链[24]、微众银行的FISCO BCOS[25]等联

盟链更关注强监管环境下客户身份识别(know your customer,简称 KYC)的需求,在身份管理中采用基于数字证书的实名认证方案.系统中部署 PKI/CA 来管理身份,用户基于非对称密码算法通过 CA 生成和管理数字身份,用户实名认证获得数字证书身份标识的过程如下.

(1) 用户发送实名注册信息给 CA 申请数字证书;

(2) CA 核实用户实名信息,如果有误,则终止申请过程;

(3) CA 基于用户实名信息为用户生成公私钥对并签发实名数字证书,确保数字证书与用户身份的一一绑定;

(4) CA 将生成的数字证书和私钥发送给用户;

(5) 在区块链交易过程中用户使用数字证书作为身份标识符,通过私钥签名实现身份认证,身份管理的全周期过程中用户都是实名的.

基于数字证书的实名认证方案可以较好地适用于中心化系统中账本保密的应用场景.但是对于区块链中的公开账本系统,却带来了极大的隐私泄漏风险.观察者可通过对公开账本中实名身份的分析实现交易的关联和追踪,从而严重威胁到用户的交易安全.为了解决这一问题,联盟链在身份管理中也提出了相应的可控匿名认证方案.

3.3 可控匿名认证

为了解决隐私保护问题,以 Fabric 和 Corda 等为代表的联盟链在身份管理中均提供了可控匿名认证方案.例如,fabric 0.6 版本中提供了基于用户交易证书 TCerts(transaction cerficates,简称 TCerts)[26]的可控匿名认证方案.Fabric 0.6 中的成员管理服务 MSP 利用注册证书(ECert)-交易证书(TCert)两级安全证书体系实现了前台匿名后台可监管的需求.用户在 Fabric 系统中注册,获得由注册证书颁发机构(enrollment certificate authority,简称 ECA)颁发的实名证书 Ecert,在交易过程中,如果选择使用此证书进行交易签名,那么此时的交易就是实名的.当用户需匿名交易时,可以从交易证书颁发机构(transaction certificate authority,简称 TCA)获得一批由 Ecert 派生出来的匿名交易证书 TCerts.两级证书结构如图 6 所示.

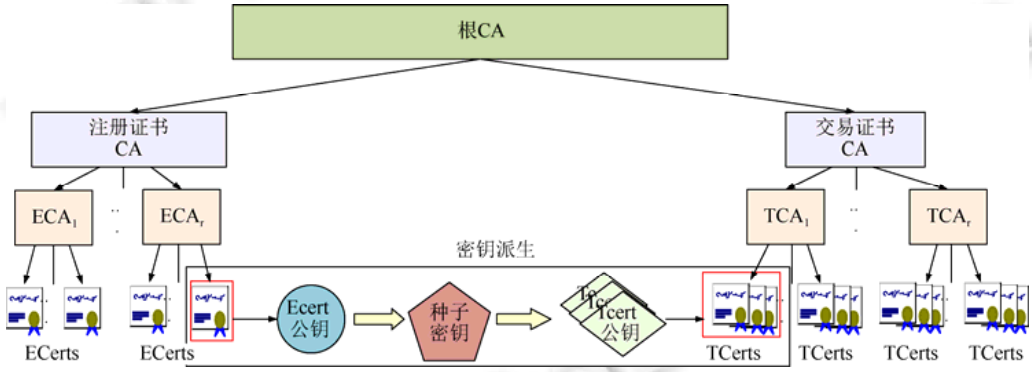


Fig.6 Tow level indentity certificates in Fabric

图 6 Fabric 中的两级身份证书

其中,根证书颁发机构(root CA),是 PKI 层次结构中最上层的 CA,它代表 PKI 体系中的信任锚.注册证书颁发机构 ECA 负责给通过注册验证的用户颁发实名注册证书 Ecerts.交易证书颁发机构 TCA 负责给提供了有效注册证书的用户颁发匿名交易证书 TCerts.匿名交易证书 TCerts 的结构见表 1.

其中,监管方拥有加密用户实名注册号 EnrollmentID 的解密密钥,在必要时可通过解密此字段获得用户实名身份.同时,为了降低客户端的密钥存储数量,*TCertIndex* 字段则用于用户密钥的派生,*TCertPub_Key* 的生成利用了椭圆曲线的密钥叠加特性,采用密钥派生的方法来完成.其工作原理类似于比特币中的 HD 钱包.用户通过扩展密钥 *ExpansionKey* 计算密钥扩展值 *ExpansionKey=HMAC*(*ExpansionKey*,*TCertIndex*),则用户私钥 *TCert*

Priv_Key=(*EnrollPrivateKey*+*ExpansionValue*) mod *n*,根据椭圆曲线的密钥叠加特性,则对应的公钥为 *TCertPub_Key*=*EnrollPub_Key*+*ExpansionValue*·*G*.

Table 1 The architecture of Tcerts

表 1 TCerts 结构

名称	描述
TCertID	Tcert 证书序列号
encEnrollmentID	EnrollmentID 的密文
encTCertIndex	TCertIndex 的密文
TCertPub_Key	TCert 的公钥
Extension	证书扩展域
Validity period	证书有效期

客户端在交易过程中使用不同的 TCerts 来完成不同的交易,因此观察者无法有效识别出用户的真实身份.但这一方案也存在一定的问题:第一,为了实现更好的身份隐私保护,这一方案要求 TCA 和用户维护大量的 TCerts 证书,从而增加了系统在密钥管理、通信和存储方面的负担;第二,如果用户重复使用 TCerts 也会带来交易的可链接性问题;第三,对于发行 TCerts 的 TCA 而言,它仍然可以链接用户的不同交易.

为了弥补 TCerts 方案的不足,目前在 Fabric 2.0 版本中引入 Idemix 方案[27]来实现用户身份的匿名性和不可链接性.Idemix 方案是基于支持多消息的盲签名和零知识证明来构建的,Fabric 2.0 版本中的 Idemix 实现方案主要是基于文献[28–30]中的工作.Idemix 提供的匿名身份认证机制具有如下特性[31].

(1) 签发者签发包含一组用户属性的凭证(credential);

(2) 用户在使用凭证进行身份认证时通过零知识证明向验证方证明其拥有凭证并可选择性地出示相应的属性.这一过程是零知识的,不会向观察者泄漏任何其他信息;

(3) 匿名性,即通过认证过程观察者无法获得用户真实身份信息;

(4) 不可链接性,即观察者无法将用户的多次认证过程链接在一起.

Idemix 方案与 X.509 数字证书认证方案的不同在于 Idemix 使用零知识证明,向验证者证明证明者拥有签名及相应属性且无需出示这些值.Idemix 与 X.509 证书方案的比较如图 7 所示.

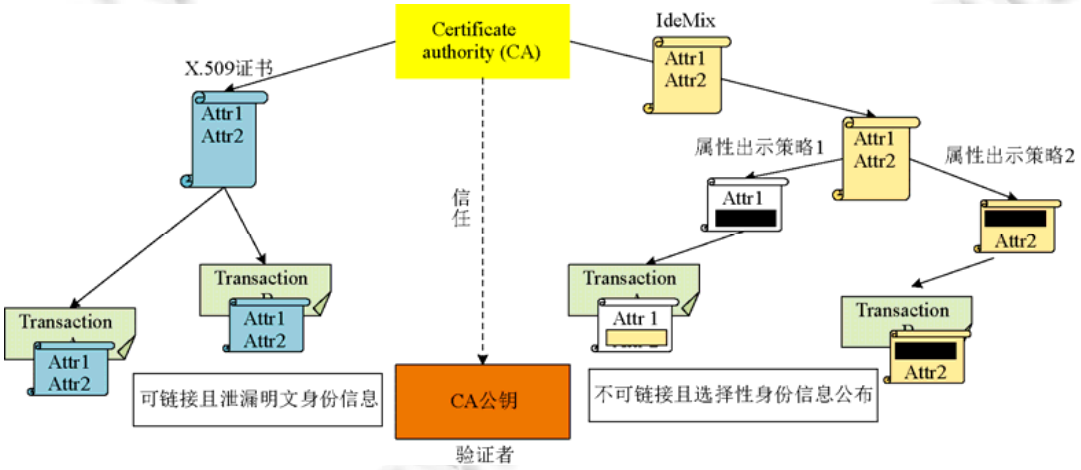


Fig.7 Comparisons between Idemix and X.509 in Fabric

图 7 Idemix 和 X.509 方案的比较

此外,Corda 中也引入了隐蔽身份(confidential identities)的概念使用临时生成的密钥对来保护隐私[32],它的设计原理类似于 Fabric 中的 TCerts 机制,这里不再赘述.

微众银行的 FISCO BCOS 区块链平台为了提高用户交易过程中的身份隐私保护,引入了群签名(group

signature)技术用于实现用户身份的可控匿名认证.在一个群签名方案中,群成员可以通过匿名的方式代表整个群体对消息进行签名,验证方可采用群公钥对签名进行公开验证以确保签名来自于合法的群成员,必要时群管理员可“打开”群签名用以恢复签名者的真实身份.

一个群签名方案包含如下过程.

(1) 创建:创建群并指定群管理员,生成群公钥和私钥;

(2) 加入:群管理员执行新增群成员操作,生成群成员私钥和证书,证书用于证明群成员身份;

(3) 签名:由群成员执行,输入消息和群成员私钥,输出消息签名;

(4) 验证:验证者通过群公钥验证签名的合法性以确保签名来自于合法的群成员,但无法确定是哪一个群成员的签名;

(5) 打开:群管理员可通过签名信息和群私钥获取签名者证书,从而恢复出签名者的真实身份.

FISCO BCOS 选择了支持群成员撤销和短签名特性的 BBS 04 方案[33],在客户端提供群签名库用以支持群成员使用私钥完成签名操作,区块链平台以预编译合约的形式集成了群签名的签名验证算法,上链的签名信息可通过预编译合约验证链上的群签名.必要时群管理员可通过签名恢复出签名者证书,从而确定签名者真实身份.FISCO BCOS 中基于群签名的可控匿名认证方案如图 8 所示.

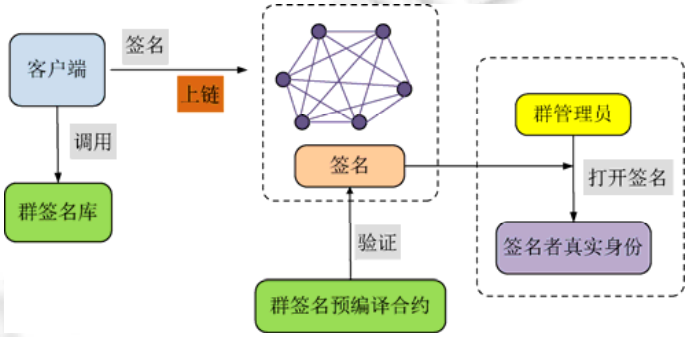


Fig.8 Group signature scheme in FISCO BCOS

图 8 FISCO BCOS 中的群签名方案

此外,FISCO BCOS 也提供了强匿名的环签名方案用于用户身份隐私保护.这些方案在联盟链中如何与数字资产交易相结合仍有待进一步加以研究.

综上所述,Hyperledger Fabric 等联盟链通过使用交易证书 TCerts 和 Idemix 来实现用户身份的可控匿名认证.对于 TCerts 方案,交易身份隐私保护的有效性取决于 TCerts 证书数量的多少,这也带来了增加计算存储开销的问题;对于 Idemix 和群环签名方案,Fabirc 和 FISCO BCOS 并未给出匿名认证与资产确权、交易流程相结合的具体实现方案,因此还有待进一步加以研究.

4 区块链系统中的身份隐藏

4.1 交易身份的隐私保护问题

值得注意的是,由于区块链交易系统具有账本公开、多方确认的特点,简单使用前述的匿名身份认证并不能有效地解决交易身份隐私保护的问题.

以使用匿名(假名)身份认证的典型代表比特币为例,虽然比特币采取了匿名身份认证的“假名”机制,但基于对公开账本数据的分析,仍可推测出参与方的交易身份隐私信息.这是由比特币 UTXO 交易模型的特点所决定的.

(1) 比特币 UTXO 交易模型中确定资产权属的身份标识为明文、确定的交易地址(假名),未采取任何身份隐藏措施;

(2) 通常在同一个交易中,所有的输入地址大多属于同一个用户;

(3) 找零地址和输入地址属于同一个用户.找零地址的特征包括:作为输出地址的情况通常只会出现 1 次;找零地址不会同时出现在输入地址和输出地址;输出地址中不能只有找零地址.通过找零地址的聚类分析,同样可以有效地识别同一用户的多个地址.

基于上述交易特征,交易分析技术通过分析公开账本中的交易记录,发现不同交易身份之间的关联关系,从而推测出匿名用户的交易规律,相关研究工作已取得了较好的分析效果[34−40].公有链的另一个典型代表以太坊[16]、央行数字货币原型系统 RSCoin[12]和 Facebook 的 Libra[16]均采取了类似的身份认证机制.相关的研究工作表明,基于上述特点,观察者可以有效地将同一用户的不同交易进行关联,在辅以其他信息的情况下,甚至可以还原出交易者的真实身份[41−43].因此,在区块链系统中单独使用匿名身份认证而不采取身份隐藏机制并不能完全有效地保护交易方的身份隐私.

为了防止通过公开账本的数据分析来获得用户身份隐私信息,相关研究工作在比特币交易模型的基础上提出了改进方案,通过引入身份隐藏技术来保护身份隐私.从身份隐藏技术保护的对象而言,可将身份隐藏划分为交易发送方的身份隐藏和交易接收方的身份隐藏.从身份隐藏所采取的不同技术手段来看,身份隐藏技术可分为两类.

(1) 混币交易技术

混币交易技术是指在交易过程中增加中间环节对多个交易进行混淆,从而增加攻击者的分析难度,保护用户身份隐私.这种方法在数字货币领域通常被称为“混币”机制,它是区块链系统中实现交易身份隐藏的基本思想.混币技术又可分为需非交易方主动参与的协同混币技术、交易方自主发起并完成的自主混币技术和系统体系架构内生的全局混币技术.上述 3 种“混币”机制分别在第 4.2 节~第 4.4 节中进行了详细的讨论.

(2) 无标识交易技术

无标识交易技术是指在链上资产的表示(如 UTXO)中不包含资产所有者的身份标识,资产权属变更过程中的交易确认是由用户采用资产表示中的秘密因子进行相应的密码运算来完成的,接收方通过密码运算的结果来判断资产权属和交易确认的正确性.无标识交易技术在第 4.5 节中给出了详细的讨论.

4.2 协同混币技术

协同混币机制的基本设计思路是:交易发送方在交易过程中引入一组并发交易用户并通过混淆器(mixer)混淆来共同完成交易,从而实现交易输入、输出地址对应关系的隐藏,使得观察者无法通过账本分析获得交易隐私信息.所谓“协同”是指混币过程中需要第三方机构或交易人的主动参与才能完成混淆过程.混币的工作机制如图 9 所示.

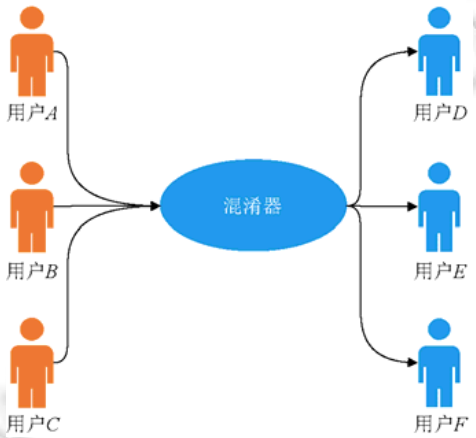


Fig.9 Mechanism of mixing coin

图 9 混币的工作机制

目前,协同混币技术可大致分为两类:中心化混币和去中心化混币.

在中心化混币方案中,第三方独立机构充当混淆器,参与混币的交易发送方首先将数字货币发送给第三方机构,第三方机构对交易进行混淆,然后将同等额度的数字货币转移给交易接收方.很多网站,如 Blockchain.info、BitCoin Fog 等均提供在线的混淆服务[44,45].但这一方案的问题在于混淆服务的提供者本身掌握用户输入输出地址的对应关系,存在隐私泄露隐患.为了提高混币机构的作恶成本,Bonneau 和 Narayanan 等人提出了 MixCoin 方案,增加了混币过程的可审计性[46].用户在与第三方机构协商混币的过程中,会获得机构对混币金额、代理地址、输出地址、混币时限等信息的签名担保(warranty).在用户完成对代理地址的支付后,一旦机构未按照约定完成对输出地址的支付,则用户可公布该机构的失信行为和担保信息,从而警示其他交易者.虽然这一方案通过信誉机制提高了混币服务机构的作恶成本,但输入、输出地址的对应关系对第三方机构仍然是可见的.针对这一问题,Valenta 和 Rowan 提出了 BlindCoin 方案,在 MixCoin 的基础上引入盲签名技术进行优化[47].盲签名技术最早是由 Chaum 在 eCash 的设计中提出来的[48],它是一种签名者对签名消息不可见、签名结果不可追踪的数字签名方案.消息发送者首先将消息进行盲化,而后让签名者对盲化的消息进行签名,最后发送者对签名信息进行脱盲操作,获得原始消息的签名.BlindCoin 方案中引入了一个公开日志(log)用于记录交互信息,用户首先将盲化后的输出地址交由混币机构签名,在完成代理地址转账确认后,将脱盲后的输出地址和签名信息公布在公开日志中,最后由混币机构按照输出地址完成支付交易.Heilman 和 Baldimtsi 等人也基于盲签名技术提出了 Blind Signed Contract 方案[49].Blind Signed Contract 方案通过引入中间机构将交易发送发的比特币转化为机构盲签名发行的匿名代币 $V=(sn,\sigma)$,交易双方通过中间机构和匿名代币为中介来完成支付.由此可见,在中心化混币方案中,中间机构充当了混淆器的角色来完成交易混淆,虽然对外部观察者而言,交易身份具有不可链接性,但中间机构却可掌握混币交易发送方和接收方的身份链接关系.

去中心化混币方案则采取了去掉第三方机构的方法来规避隐私泄露风险.在去中心化方案中,互不信任的用户无需依赖第三方,可以自由组合来构建混币交易.由 Maxwell 首次提出的 Coinjoin[50]是目前典型的去中心化混币方案.其基本思想是:想要混合他们比特币的用户产生一个单独的混合交易,其包含用户的当前地址作为输入并且洗牌的新地址作为输出.它描述了一种特殊的交易:当一个用户希望发起一笔交易时,他可以寻找另外一个想要发起交易的用户,一起构建一个联合交易.如图 10 所示,如果有用户 *A* 想转账给用户 *C*,用户 *B* 想转账给用户 *D*,则通过 Coinjoin,他们可以将两笔交易结合成一笔交易.交易包含两个输入:*A* 和 *B* 以及两个输出:*C* 和 *D*.输入和输出的顺序是完全随机的,*C* 或 *D* 可能收到 *A* 的转账或是 *B* 的转账,或是 *A* 和 *B* 两人的转账.这样就削弱了对交易输入和输出的关联分析.同时,参与 Coinjoin 交易的用户越多,交易的混淆程度就越高,参与用户还可商定一个统一的输出大小以增加隐私性.目前,Coinjoin 已在 Dark Wallet、JoinMarket、DashCoin 中得以实现.

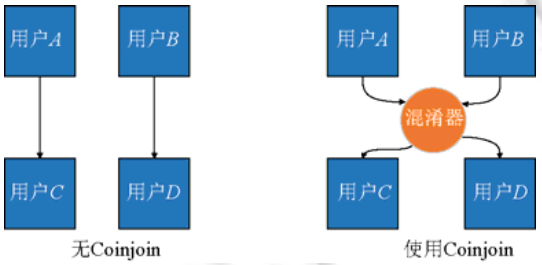


Fig.10 Mechanism of CoinJoin

图 10 CoinJoin 工作原理

虽然 Coinjoin 交易对外是不可链接的,但是对参与 Coinjoin 交易的用户来说,由于每个用户都必须对交易进行签名,所以每个用户都知道其他用户的交易信息.因此,Coinjoin 交易不满足内部不可链接性.为了解决这一问题,Ruffing 和 Moreno-sanchez 等人提出了 CoinShuffle 方案[51].CoinShuffle 不仅可以允许去中心化的 Coinjoin 交易,还可以保护交易内部各参与方的隐私.它的设计受到 Dissent[52]中匿名群组消息协议的启发,对输出地址

的隐藏采用的是 Chaum 提出的级联加密方案[53],从而使得交易混淆过程中输入、输出地址满足内部不可链接性.CoinShuffle 方案如图 11 所示.每一个混币交易者都使用后续交易者的公钥对其输出地址进行级联加密 $c_i=Enc((ek_{i+1},\ldots,ek_N),vk_i)$,其中,$ek$ 为交易者加密密钥,vk_i 为输出地址.从第 1 个交易者开始顺序进行,每个交易者解密前序地址并加密自己的地址加入洗牌向量中,最后一个交易者获得全部输出地址明文并完成交易构造.设用户数为 n,则 CoinShuffle 方案执行的公钥加密次数为$(n-1)\cdot n/2-1$;设原有地址大小为 s、加密后的地址大小为 s_e,则混淆过程所产生的身份标识信息大小为 $s_e\cdot(n-1)+s$.

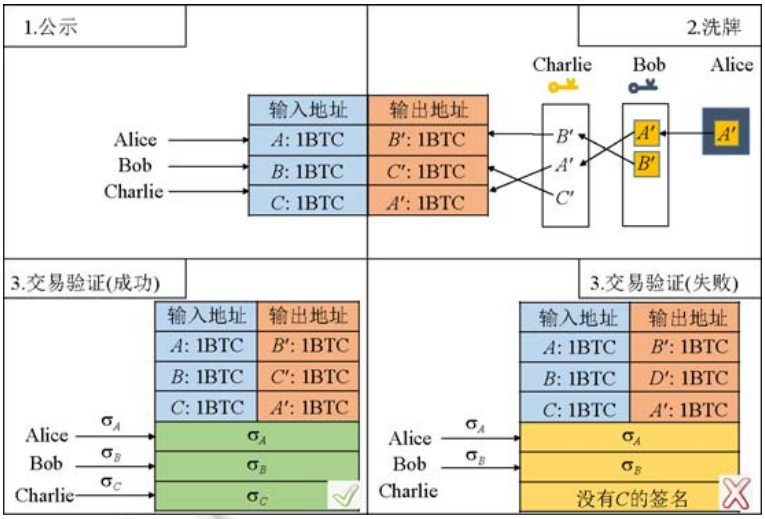


Fig.11 Mechanism of CoinShuffle

图 11 CoinShuffle 工作原理

为了进一步提高 CoinShuffle 混币过程中的通信效率,Ruffing 等人进一步提出了 CoinShuffle++改进方案[54].CoinShuffle++中混币用户的匿名群组通信采用了 DC-net(dining cryptographer net)[55]的设计思想:假设在 3 个节点 P_1、P_2 和 P_3 的群组通信过程中每一对节点(i,j)共享一个对称密钥 K_{ij}.P_1 为了匿名发布消息 m,它发送消息 $M_1=m\oplus K_{12}\oplus K_{13}$,$P_2$ 发布消息 $M_2=K_{12}\oplus K_{23}$,P_3 发布消息 $M_3=K_{13}\oplus K_{23}$.观察者可通过计算 $m=M_1\oplus M_2\oplus M_3$ 恢复出消息 m,但无法确认 m 是谁发送的.DC-net 方案较级联加密方案具有更高的效率,加密密文长度等于原文长度,同时仍可确保混币过程中输入、输出地址的内部不可链接性.设用户数为 n,则 CoinShuffle++方案执行的公钥加密次数为 $n-1$;设原有地址大小为 s、加密后的地址大小为 s_e,则混淆过程所产生的身份标识信息大小为 $s_e\cdot(n-1)\cdot n+s=s\cdot(n^2-n+1)$.

综上所述,协同混币技术在混淆过程中通过引入一组并发用户实现了交易接收方的身份隐藏,通过混淆机制隐藏了混币交易中用户输入、输出地址(交易发送、接收方)间的对应关系.假设一个混币交易集合中的用户数为 M,则对于外部观察者而言,准确确认交易接收方身份的概率为 $1/M$.因此,混币过程确保了输入、输出地址的外部不可链接性.但在中心机构或自组织用户的混币交互过程中,不同混币方案在提供内部不可链接性方面存在差异.在中心化混币方案中,直接混币和 MixCoin 中作为观察者的混淆器可查看所有的输入、输出地址的对应关系,因此对混淆器而言系统并未提供身份隐私保护;在 BlindCoin 方案中,混币过程使用盲签名技术实现了对中心混币机构的交易接收方身份隐藏;在 Blind Signed Contract 方案中,通过使用匿名代币实现了交易发送方的身份隐藏.在去中心化混币方案中,CoinJoin 在混币过程中未对交易接收方采取隐藏措施,因此不具有内部不可链接性;CoinShuffle 和 CoinShuffle++则通过匿名群组通信方案实现了交易接收方的身份隐藏,因此具有更好的内部不可链接性.

协同混币技术在提供身份隐私保护的同时,也存在着一定的问题:首先,协同混币过程必须需要其他用户的

主动参与,任何一个用户的退出都会导致混币交易失败;其次,在提供了更好隐私特性的方案中,如:MixCoin、BlindCoin、Blind Signed Contract、CoinShulffle 和 CoinShuffle++等,均在链外引入了实体(混淆器、用户等)间的多轮交互协议以提高安全性.这在一定程度上增加了系统实现的复杂性和运行开销.文献[56,57]中引入了聚合签名技术,从而实现参与混币方之间的非交互式混淆过程.所谓聚合签名(aggregate signature)是指可将多个消息的不同签名$\sigma_1,\sigma_2,\ldots,\sigma_n$聚合为一个签名$\sigma$并可进行有效验证的签名算法.非交互式聚合签名特性确保了交易用户无需主动参与混淆过程,聚合签名的单向性确保了观察者无法通过聚合签名获得原始签名,从而隐藏了真实交易的输入、输出对应关系.但交易的签名聚合过程需由第三方完成,如:矿工、Joiners 或 Merging Service 等.因此这一过程并未完全解决交易的内部不可链接性问题,仍存在一定的身份隐私泄漏风险.

4.3 自主混币技术

自主混币技术的典型代表是门罗币(Monero)[10].它是一个衍生自比特币的开源加密货币,其用户在混币过程中无需第三方中心机构和其他用户的参与,可实现自主混币,能够有效杜绝原有混币方案面临的问题.门罗币的设计基于 CryptoNote 协议[58],并且提供了更强的隐私保护特性.在身份隐私保护方面,首先门罗币沿用了比特币中基于椭圆曲线公钥密码体制的匿名身份认证技术,门罗币中每个用户随机生成两个椭圆曲线公钥(A,B)作为用户的公开身份标识,相对应的私钥(a,b)由每个用户私自持有,并在交易过程中用于生成签名信息,完成用户的身份认证和支付确认.但它不同于比特币所使用的 NIST 曲线和 ECDSA 签名算法[59],门罗币选用了设计更为公开和高效的 ED 25519 数字签名模式[60,61];其次,门罗币实现了交易过程中的身份隐藏机制,它使用环签名实现了交易发送方的身份隐藏,使用隐蔽地址(stealth address)实现了交易接收方的身份隐藏[62].一次性地址和环签名组合方案构成了门罗币的自主混币技术.

门罗币沿用了比特币中的 UTXO 交易模型并设计了基于隐蔽地址的交易接收方身份隐藏机制.在每次交易过程中,通过使用发送方生成的随机数和接收方的身份标识(A,B)来运行一个半 Diffie-Hellman 密钥交换协议派生出一个一次性接收地址,从而将真正的交易接收方身份隐藏在整个可能的用户空间中,而只有持有相应私钥(a,b)的人才能够判断出这是一笔发送给(A,B)的交易.此时对于系统总用户数为 N 的情况,观察者可成功判断出接收方身份的概率为 $1/N$.

设椭圆曲线中的基点为 G,G 的阶数为 l,则门罗币中的隐蔽地址计算流程如图 12 所示.

(1) Alice 想要付款给 Bob,Alice 先需获取 Bob 的公钥信息(A,B);

(2) Alice 产生一个随机数 $r\in[1,l-1]$,然后计算一次性公钥 $P=H_S(rA)G+B$;

(3) Alice 计算 $R=rG$,然后生成一笔交易将 P 作为目的地址,并将 R 也放入交易中;

(4) Alice 将交易广播到区块链上;

(5) Bob 检查区块链上每一笔交易,并用他自己的私钥(a,b)计算出相应的 $P'=H_S(aR)G+B$,因为 $aR=arG=rA$,如果 $P=P'$,那么说明这笔交易就是发送给自己的;

(6) Bob 找到自己的交易后就可以算出对应的一次性私钥 $x'=H_S(aR)+b$,且 $P'=x'G$,他可以使用私钥 x' 签名交易来进行支付.

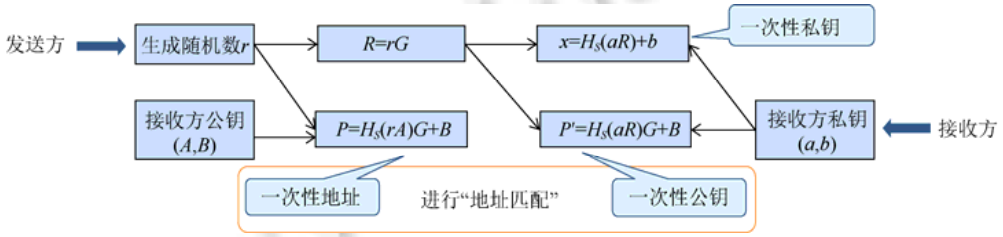


Fig.12 Generation algorithm of stealthy address

图 12 隐蔽地址的生成算法

为了满足门罗币用户使用和管理多个地址(身份标识)的需求,类似于比特币中的 HD 钱包方案,门罗币又提出了用户子地址(sub-address)的概念[63],用户可通过自己的主钱包地址派生出任意数量的不可链接的子地址.在进行交易接收地址搜索时,使用主私钥进行一次计算既可以判断出是否为子地址对应的输出地址,从而避免了使用多个私钥进行多次计算匹配的复杂操作开销.用户通过自己的主钱包地址(A,B)和索引 i 派生出相应的子地址并存储在列表中,生成方法如图 13 所示.

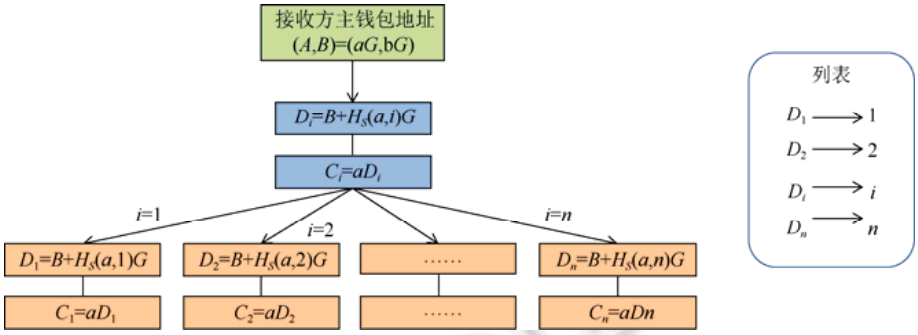


Fig.13 Generation algorithm of sub-address

图 13 子地址的生成方法

交易过程中生成的一次性子地址的判断方法如图 14 所示.接收方在判断子地址时只需通过主私钥 a、一次性子地址 P 和交换的随机变量 R 进行计算获得 D'_i 并和列表中的 D_i 比较即可.匹配成功后,用户可通过主私钥(a,b)和索引 i 生成相应的一次性私钥.

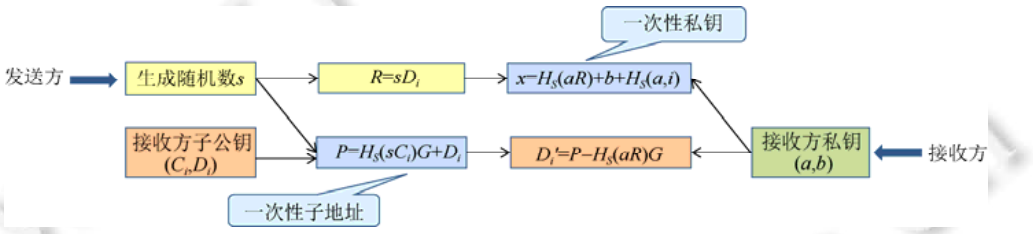


Fig.14 Decision of stealthy sub-address

图 14 一次性子地址的判断方法

门罗币中交易发送方的身份隐藏是通过环签名技术来实现的.环签名是由 Rivest 等人在如何匿名泄漏秘密背景下提出来的新型签名技术[64].环签名不同于群签名[65],它在构造匿名集合的过程中无需配置过程和管理者,因此为自主混淆提供了便利.在环签名中,签名者将自己的公钥和另外一些公钥(但不知道私钥)进行混淆构成匿名集合,然后再对消息进行签名.这样对于观察者而言,无法区分签名来自匿名集合中的哪一个公钥(真正的签名者).环签名的定义如下.

给定一个环 $U=\{U_1,U_2,U_3,\ldots,U_n\}$,环中每个成员的公私钥对为$(pk_i,sk_i)$,$i=1,2,\ldots,n$.不失一般性,假设 $U_k(1\leqslant k\leqslant n)$是签名人,则环签名、验签算法可如下定义.

环签名生成算法.由签名人运行.其输入是待签名的消息 m、环中所有成员的公钥 pk_i、真正签名人的私钥 sk_k;其输出就是 U_k 对消息 m 的环签名σ.

环签名验证算法.由签名验证者运行.其输入是待验证的消息签名对(m,σ)、环中所有成员的公钥,当接受该签名时输出为 1,否则输出为 0.

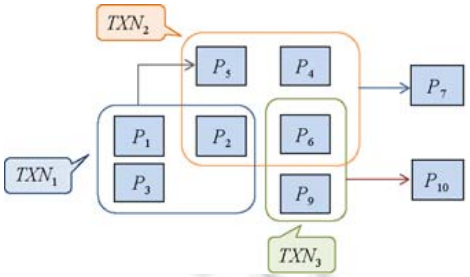
门罗币中所使用的是一类具有可链接性的环签名,称为可链接环签名.可链接性是指如果环 $U=\{U_1,U_2,U_3,\ldots,U_n\}$中的某个签名人产生了两个消息签名对$(m,\sigma_1)$、$(m,\sigma_2)$,则存在有效算法使得签名验证者可以确定这两

个消息是由环中同一个签名人产生的.其中,判断链接性的算法如下定义.

签名链接算法.其输入是环 $U=\{U_1,U_2,U_3,\ldots,U_n\}$的两个消息签名对$(m,\sigma_1)$、$(m,\sigma_2)$,当签名$\sigma_1$、$\sigma_2$是由同一个环成员产生时,算法输出为 1,否则为 0.

门罗币用户在进行交易时首先执行自主混币过程,即搜索链上具有相同面额的 UTXO,选择它们的公钥和自身公钥一起来构成环(匿名集合);其次,用户通过自身私钥和环成员的公钥对支付消息生成环签名;最后,验证节点验证环签名的有效性和链接性(防双花).门罗币自主混币过程的实例如图 15 所示:以其中的交易 TXN_2 为例,交易发送方 P_4 与具有同等货币面额的支付者 P_2、P_5、P_6 混淆在一起构成一个环进行交易.对于观察者来说,通过支付信息和签名无法辨别出交易发送方的真实身份.

通过对上述分析可知,门罗币采用基于可链接环签名技术的混淆方案实现了如下 3 个功能:(1) 利用环签名的匿名性将交易发送方的身份隐藏在环成员构成的匿名集合中;(2) 利用环签名的不可伪造性实现了用户对交易行为的确认和不可否认;(3) 利用可链接环签名的可链接性防止货币(UTXO)双花(double spending).



交易	可能的输入	输出地址
TXN_1	P_1,P_2,P_3	P_5
TXN_2	P_2,P_4,P_5,P_6	P_7
TXN_3	P_6,P_9	P_{10}

Fig.15 Mixing coin in Monero

图 15 门罗币自主混币过程

门罗币早期版本使用的是 CryptoNote 协议中定义的一次性环签名算法[58],该算法是对 Fujisaki 和 Suzuki 工作的改进[66].

(1) 密钥生成

签名者首先随机选择一个私钥 $x\in[1,l-1]$,然后计算对应的公钥 $P=xG$ 和密钥镜像 $I=xH_p(P)$.其中,密钥镜像用于可链接性的判断.

(2) 签名验签

签名者随机选择一个包含 $n-1$ 个元素的公钥集合,然后与自己的公钥进行混淆产生混合后的集合 $S=(P_1,P_2,\ldots,P_n)$,使用输入消息 m、集合 S 和私钥 x 基于文献[67]中的零知识证明技术来生成签名信息$\sigma=(I,c_1,\ldots,c_n,r_1,\ldots,r_n)$.这一协议过程是证明签名者知道私钥$x$,该私钥对应于集合$S$中的某个公钥$P=xG$且$H_p(P)=I\cdot x^{-1}$.验证者接收到签名后使用输入消息 m 和公钥集合 S 对签名进行验证.

(3) 链接算法

若验签通过,则验证者还需进一步检查 I 是否曾被用于过去的签名.如果存在重复使用,则说明签名来自同一个私钥x,意味着存在货币双花问题.

门罗币在发展过程中也在不断进行环签名技术的优化.2015 年,Back 等人提出了对 CryptoNote 一次性环签名结果存储空间的优化方案[68].该方案基于 Liu 等人提出的可链接自组织匿名群签名方案 LSAG(linkable spontaneous anonymous group signatures,简称 LSAG)[69],改进后的签名数据为$\sigma=(I,c_1,r_1,\ldots,r_n)$,在存储空间上约缩减为原来的一半.但采用 LSAG 的 CryptoNote 方案也存在不足.首先,明文的交易金额为观察者提供了分析的便利,基于特定金额可实现身份追踪;其次,由于交易发送方在自主混币过程中需在公开账本中寻找相同金额的 UTXO 并使用其属主身份构成环(匿名集合),这在一定程度上带来了交易过程中匿名集合过小的问题,从而造成身份隐私泄漏.此外,LSAG 方案只能支持单输入交易的身份混淆,这限制了其应用范围.

为了解决 LSAG 方案的上述问题,后续的门罗币 Ring CT(ring confidential transactions)版本又提出了多层

可链接自组织匿名群签名方案 MLSAG(multilayer linkable spontaneous anonymous group signature,简称 MLSAG)[62].Ring CT 是将环签名、同态承诺与范围证明相结合来构建的基于自主混淆的身份隐私保护方案.Ring CT 使用了基于 Pedersen 承诺的保密交易技术来实现交易金额的隐藏,在交易平衡性验证上使用了类似于 MimbleWimble 的盲化因子差值的签名验证(关于保密交易技术的详细介绍可参见第 4.5 节中的分析),不同点在于门罗币在通过同态承诺隐藏金额的同时还需通过混淆过程实现交易身份的隐藏.Ring CT 方案在如下几个方面进行了改进:首先,Ring CT 方案通过交易内容的隐藏避免了 CryptoNote 混淆方案中明文金额易追踪和相同金额用户匿名集合过小的问题.其次,为了在确保交易身份和输入承诺一一绑定的情况下支持多输入交易成组混淆和密态交易平衡性验证,MLSAG 方案将 UTXO 中 Pedersen 承诺的交易平衡性证明加入到环签名中,并一次性地对用户密钥组进行运算生成多层环签名.在 MLSAG 方案中,假设有 n 个环成员,每个环成员都有 m 对密钥,则这些成员公钥组成的密钥向量为 $\left\{P_i^j\right\}_{i=1...n}^{j=1..m}$,签名用户 π 的镜像向量为 $\left\{P_\pi^j\right\}^{j=1...m}$,其中,$i$ 为环成员的索引,表示环集合中第 i 个成员,j 为成员密钥的索引,表示某成员的第 j 个密钥.对于一个用户的一组交易输入而言,构成如下的交易组向量 $\left\{\left(P_\pi^1,C_\pi^1\right),...,\left(P_\pi^m,C_\pi^m\right),\left(\sum_{j=1}^m P_\pi^j+\sum_{j=1}^m C_\pi^j-\sum_i C_{i,out}\right)\right\}$,其中的公钥即可构成了该成员的公钥向量,MLSAG 可使用匿名集合成员的公钥向量构造多层环签名以实现交易的成组混淆.假设运算密钥为 $n\cdot m$ 个,则 MLSAG 生成的多层环签名为 $\sigma=\left(I_1,...,I_m,c_1,r_1^1,...,r_1^m,...,r_n^1,...,r_n^m\right)$.不同于 LSAG 使用匿名集合用户的 n 个密钥签名,MLSAG 是使用用户的 n 个密钥向量进行签名.验证者(矿工)在未知具体交易输入 UTXO 的情况下可通过验证该签名确保交易平衡性并通过镜像向量 $\left\{I_\pi^j\right\}^{j=1...m}$ 的重复性检测实现防双花.这既支持了多输入交易成组混淆,又有效提高了签名效率.2019 年,Brandon 等人又提出了紧凑可链接自组织匿名群签名方案(compact linkable spontaneous anonymous group signature,简称 CLSAG),CLSAG 方案在运算密钥数为 $n\cdot m$ 的情况下,生成的多层环签名为 $\sigma=(I_1,\ldots,I_m,,c_1,r_1,\ldots,r_n)$,提供了更高的运算效率以及更短的签名长度[70].

综上所述,门罗币在使用匿名身份认证的同时,在交易过程中又提供了基于自主混币的交易身份隐藏技术.它通过隐蔽地址技术实现交易接收方的身份隐藏,在设定系统总用户数为 N 的情况下,观察者有效识别接收方身份的概率为 $1/N$,具有很好的隐私保护特性;通过可链接环签名完成了交易发送方的自主混币过程,从而实现了发送方的身份隐藏.理想情况下,环成员个数为 M 时观察者可有效识别发送方身份的概率为 $1/M$.

门罗币通过一次性地址和环签名所构建的自主混币与协同混币技术存在着类似的混淆过程,但二者又存在不同:(1) 门罗币的混淆过程无需发起方与参与方间的交互;(2) 参与方无需真正发起交易.这些特点使得门罗币基于非交互模式的自主混淆过程实现了发送方的身份隐私保护.

但门罗币的自主混币方案也存在一定的风险:首先,在接收方身份隐藏机制方面,如果交易发送方在与同一用户交互过程中使用相同的随机数,则两笔不同交易的接收地址相同,会带来两笔交易产生关联的问题.因此,接收方交易关联的隐私问题会一定程度地依赖于发送方的行为可信.其次,在发送方身份隐藏机制方面,发送方身份隐私的保护程度依赖于混淆过程中环成员的多少以及参与混淆的 UTXO 在其他交易中的使用情况.相关研究工作表明,在用户自主混淆过程中选择较少的环成员(如 2 个)会带来一定的隐私泄露风险[71,72];而参与混淆的 UTXO 在其他交易中的信息泄露又进一步增加了分析成功的概率[73,74].由此也说明,在区块链交易模型中账本公开的特性使得交易方的身份隐私强度并不简单等同于所采用的密码算法所提供的匿名性.以门罗币交易发送方的身份隐藏为例:在文献[73,74]中分析的特定情况下,当环成员个数为 M 时,观察者可有效识别发送方身份的概率是大于 $1/M$ 的.

4.4 全局混币技术

全局混币技术的典型代表是零币(Zcash)[75].它是由麻省理工学院和霍普金斯大学的研究者发起的一种强隐私保护的开源加密货币.它仍然沿用了比特币中的 UTXO 交易结构,但对于完全基于零币的隐蔽(shielded)交易而言,交易结构中隐去了交易地址,通过引入承诺 Merkle 树、零知识证明和加密技术提供了更强的隐私保护特性.零币的设计思想来源于 1999 年 Sander 等人设计的一种可审计匿名电子货币系统[76],它将传统电子货币的

防伪验证由中心机构的签名验签问题转变为一个已发行货币列表的成员证明问题,这也是实现零币中全局混币技术的基础.2013 年,Miers 等人设计了基于区块链的匿名分布式电子现金系统 Zerocoin[77],它通过使用区块链来确保货币列表的完整性.2014 年,Ben-Sasson 等人设计了 Zerocoin 的升级版本 Zerocash[78],由此奠定了 Zcash 交易协议的理论基础.基于 Zerocash 设计的密码货币 Zcash,目前已经过 Sprout 和 Sapling 两个主要版本的开发[79].在身份隐私保护方面,首先,零币沿用了比特币中基于椭圆曲线公钥密码体制的匿名身份认证技术,但其用户地址形式和作用不同于比特币;其次,零币实现了交易过程中的身份隐藏机制,通过全局混币和基于零知识证明的货币权属确认实现了交易发送方的身份隐藏,通过交易内容的链上加密传输实现了交易接收方的身份隐藏.

在此,我们以 Zcash 中实现方式最接近于原 Zerocash 论文的 Sprout 版本为例介绍零币中的身份隐私保护.零币中仍然沿用了比特币中的匿名身份认证机制,但密钥形式和作用与比特币有很大的不同.在 Sprout 中,用户密钥和地址之间的关系如图 16 所示:零币中的每个用户均具有两个密钥对(a_{pk},a_{sk})和(pk_{enc},sk_{enc}),由用户自主匿名生成.其中,a_{pk} 和 pk_{enc} 统称为支付地址,作为用户交易过程中的身份标识符.a_{pk} 称为支付密钥,在发起交易时用于计算新生成硬币的承诺,pk_{enc} 称为传输密钥,用于加密消息,指定交易的接收者.a_{pk} 和 sk_{enc} 统称为收入查看密钥,sk_{enc} 又称为接收密钥,这两个密钥在接收某笔交易时使用.a_{sk} 称为花费密钥,a_{pk} 和 sk_{enc} 密钥均是由 a_{sk} 通过伪随机函数(pseudo random function,简称 PRF)派生而来.(pk_{enc},sk_{enc})则是 ED 25519 算法中的一对公私钥.在 Sprout 系统中可以简单地理解为用户只有拥有了 a_{sk},才能有花费某个匿名资产的权利.零币中的密钥体系是系统实现交易隐私保护的基础.

为了实现交易的隐私保护,零币系统并未将货币明文直接存储在公开账本中,而是将系统已生成货币的承诺值列表和已花费货币的序列号列表公开,交易过程中的货币合法性验证即成为一个承诺列表的成员证明问题,防双花问题则通过已花费货币的序列号比对来完成.零币中的每个货币 *np* 可以表示为由以下内容构成:

$$np:=\{a_{pk},v,\gamma,rcm\},$$

其中,a_{pk} 是货币持有者公钥,v是货币金额,γ是一个秘密值,用于计算硬币承诺和硬币的序列号,*rcm* 是门限值.货币承诺的计算方式如下:

$$cm:=\text{SHA 256}(10110000|a_{pk}|v|\gamma|rcm).$$

零币系统通过两类交易实现新币承诺的生成:*mint* 和 *pour* 交易.其中,*mint* 用于由基础币(Basecoin)生成零币;*pour* 用于实现用户间的交易支付.每个新生成的货币承诺 *cm* 会被加入一棵承诺 Merkle 树中,如图 17 所示.

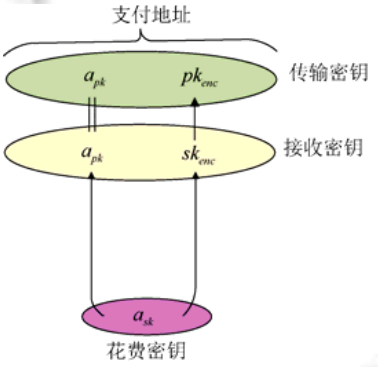


Fig.16 User addresses and keys in ZCash
图 16 零币中的用户密钥和地址

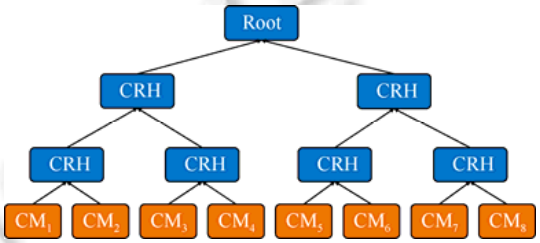


Fig.17 Commitment Merkle tree in ZCash
图 17 零币中的承诺 Merkle 树

整棵 Merkle 树构成了系统中已经出现过的所有匿名货币列表(包括已经花费和未花费的),其中每个币的承诺值 *cm* 充当这棵树的叶子节点,每个承诺 Merkle 树均具有一个根散列值 *rt*.由此,对于交易过程中所使用的货币合法性验证即转化为一个证明承诺值 *cm* 是否属于承诺 Merkle 树的成员证明问题.此外,为了防止货币双花,零币系统还维护了一个已花费货币序列号 *Nullifier Set*,矿工如果检测到支付出现在列表 *Nullifier Set* 中的货

币,则终止交易.其中,序列号 *Nullifier* 的生成方式如下:

$$Nullifier:=\text{SHA 256compress}(1110|a_{sk}|\gamma).$$

零币用户在使用 *pour* 交易进行支付时,假设持有密钥对 $\left(a_{pk}^{old},a_{sk}^{old}\right)$ 的交易发送方使用拥有的零币 $c^{old}:=\left(a_{pk}^{old},v^{old},\gamma^{old},rcm^{old}\right)$ 分别向地址为 $\left(a_{pk}^{new1},pk_{enc}^{new1}\right)$ 和 $\left(a_{pk}^{new2},pk_{enc}^{new2}\right)$ 的交易接收方支付货币 $c_1^{new}:=\left(a_{pk}^{new1},v^{new1},\gamma^{new1},c_1^{new}:=rcm^{new1}\right)$ 和 $c_2^{new}:=\left(a_{pk}^{new2},v^{new2},\gamma^{new2},rcm^{new2}\right)$,则交易发送方在构建 *pour* 交易时使用接收方支付密钥 a_{pk}^{new*} 和新生成的秘密值 γ^{new*} 构建新币的承诺 cm_1^{new} 和 cm_2^{new},公开已支付货币的序列号 $Nullifier^{old}$ 并确保 $v^{old}=v^{new1}+v^{new2}$.交易发送方将构建后的 *pour* 交易向全网广播.为了实现对上述非明文交易内容的验证,零币采用了零知识证明技术 zk-SNARK[80−87]生成交易对应的证明信息 π_{POUR}:发送方持有的货币 c^{old} 所对应的承诺 cm^{old} 为根散列值为 *rt* 的 Merkle 树中的叶子节点;发送方持有花费密钥 a_{sk}^{old};能够正确地构建出所有的货币 c^{old}、c_1^{new}、c_2^{new} 及其承诺 cm^{old}、cm_1^{new}、cm_2^{new};给出了 c^{old} 所对应的真实的 $Nullifier^{old}$.其中,Zk-SNARKs 零知识证明的过程主要有以下 3 个步骤.

(1) $KeyGen(1^{\lambda},C)\rightarrow(pk,vk)$.输入一个安全参数 λ 和 *F* 域-算数电路 *C*,生成零知识证明中的证明密钥 *pk* 和验证密钥 *vk*;

(2) $Prove(pk,x,a)\rightarrow\pi$.输入一个证明密钥 *pk* 和信息 *x*(证明者和验证者均能够获得)以及证明者自己所拥有的某些秘密信息 *a*(只有证明者知道),输出一个非交互式证明 π,来表示证明者确实拥有某些知识;

(3) $Verify(vk,x,\pi)\rightarrow b$.输入一个验证密钥 *vk*、一个 *x*、一个证明 π,如果验证者验证通过,即他相信证明者确实拥有某种知识,则验证输出为 b=1.

由此可见,零币的支付过程将发送方的支付货币混淆在 Merkle 树的全部成员(已生成货币)中,交易结构中并不包含交易发送方的身份信息,只需发送者证明他拥有输入货币承诺对应的花费密钥 a_{sk} 即可,由此声明自己对该货币的权属并实现支付行为的确认.当矿工验证交易时,会对该证据 π_{POUR} 进行验证,如若通过验证,则交易有效.整个验证过程是零知识的,矿工只能判断出发起者是不是货币的拥有者,而不会得到有关 a_{Pk}、a_{sk}、cm^{old} 的任何信息.在 Zcash 中,除了发送者自身外,矿工及第三方(包括交易的接收者)都无法得知发送者的身份.这一方案既实现了交易发送方的身份隐藏,又实现了支付货币的全局混币,极大地提高了交易隐私保护的力度.

在零币的交易结构中同样不存在接收方的任何地址信息,而是通过对交易内容的加密来指定交易接收方.Zerocash 方案中使用 key-private encryption scheme[88]的公钥加密模式[88],通过使用接收者的公钥对交易中的敏感信息(v,γ,rcm)进行加密,然后将密文包含在隐蔽交易中并广播到区块链.接收方需要监听区块链上的交易,尝试用自己的私钥解密隐蔽交易中包含的加密信息,如果解密成功,则代表该隐蔽交易的接收方是自己,存储解密后的敏感信息并在未来支付时使用.零币中的 Sprout 版本则通过 Curve 25519 密钥协商协议[89]在发送方与接收方之间产生一个共同的会话密钥,而后通过一次性认证对称加密方案(authenticated one-time symmetric encryption)对敏感交易信息进行加密.接收者监听链上的交易,尝试利用自己的私钥 sk_{enc} 计算会话密钥并解密隐蔽交易中包含的加密信息,如果解密成功,则代表自己是该交易的接收方,并接受这笔交易.

此外,基于企业以太坊 Quorum 平台 ZCash 开发团队开发了 ZSL[90]强隐私保护的密码货币交易模型.在 ZSL 交易模型中,仍使用零币中的全局混币方案,通过货币承诺列表和 *Zk*-SNARKs 来实现货币的支付与正确性验证,由此构成的隐蔽交易由 Quorum 主链平台上的 *z*-contract 合约来实现,交易流程隐藏了交易方身份和交易金额.基于 Quorum 构建隐私交易系统时,可通过 *z*-contract 来发行代币资产,以保护交易隐私.交易双方的代币资产在进行交易时,通过私有合约(private contract)来定义特定交易流程,私有合约由 Quorum 中的 Constellation 系统来完成,用以确保交易内容的保密性.不同于零币方案交易信息加密传输,ZSL 中的货币 *np* 是由私有合约直接传送给接收方的,私有合约的保密性确保了交易隐私.ZSL 方案如图 18 所示.

综上所述,零币在使用匿名身份认证的同时在交易过程中又提供了基于全局混币的交易身份隐藏技术.它通过零知识证明和(自主)全局混币技术实现了交易发送方的身份隐藏;通过交易内容的加密接收实现了交易接收方的身份隐藏.在设定系统总用户数为 *N* 的情况下,观察者有效识别发送方和接收方身份的概率为 1/*N*,具有

很好的隐私保护特性.但零币的隐私保护方案也存在一定的问题:首先,由于系统大量引入了零知识证明算法,因此增加了交易操作的时间复杂度和空间复杂度.设 n 为算数电路门数,l 为证明实例大小,则 *zk*-SNARK 证明算法的时间复杂度为 $O(n\log n)$,验证算法的时间复杂度为 $O(l)$;其次,*zk*-SNARK 在系统初始化时需要安全地生成公共参数(public parameters),如果初始化各方私自留存秘密信息,则可以共谋伪造 *zk*-SNARK 证明证据从而伪造新币,这给零币的安全隐私带来较大的威胁.文献[91]在公共参数生成过程中引入多方安全计算以提高生成过程的安全性.目前系统初始化参数的可信生成问题仍有待进一步加以研究[92];此外,零币系统中也存在着透明交易以及基础币和零币之间的转换交易,2019 年,Alex 等人在文献[93,94]工作的基础上进一步分析了通过交易数据特征值及利用密码算法特点构建阈下信道从而发现交易关联性的身份隐私泄露风险[95].这进一步说明了编码型数字资产在账本公开条件下实现隐私保护所面临的巨大挑战.

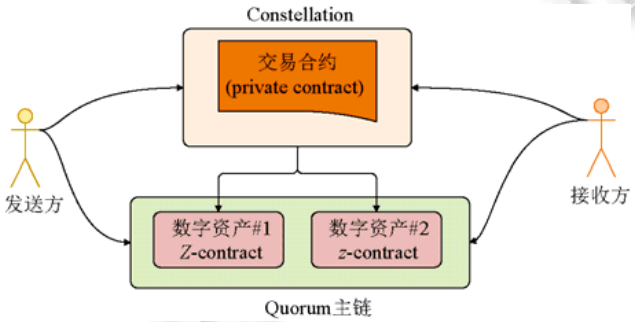


Fig.18 ZSL transaction model

图 18 ZSL 交易模型

4.5 无标识交易技术

无标识交易技术的典型代表为 MimbleWimble 协议[96].2016 年 7 月,化名作者 Jedusor 首次提出了 MimbleWimble 协议.2016 年 10 月,Poelstra 在最初版本上进一步进行了研究和完善[97].Wimble 沿用了比特币的 UTXO 交易结构,但采用了保密交易(confidential transaction,简称 CT)技术[98,99],并去除了交易地址,从而提供了更好的交易隐私保护特性.Fuchsbauer 等人于 2019 年对 MimbleWimble 协议进行了可证明安全的分析[100].目前,实现 MimbleWimble 协议的项目主要包括 Grin[101]和 Beam[102].

为了实现交易内容的隐私保护,MimbleWimble 使用了保密交易(confidential transaction)技术对交易金额进行隐藏.保密交易技术最初是由比特币开发人员 Back 和 Maxwell 提出来的[98,99],通过在比特币网络中使用 Pedersen 承诺(Pedersen commitment)[103]实现对 UTXO 中交易金额的隐藏和隐藏交易的验证.承诺是密码学中重要的安全原语.承诺方在对一个选定的值进行承诺后将承诺值发送给接收方,并能够在之后揭示所承诺的值.Pedersen 承诺在 1991 年由 Pedersen 提出后得到了广泛应用,CT 中使用的是基于椭圆曲线构建的 Pedersen 承诺方案.设 G 为椭圆曲线点群中的生成元,H 为椭圆曲线中的一个点,则对金额 v 的 Pedersen 承诺为

$$C(r,v)=rG+vH,$$

其中,r 为随机生成的盲化因子且不公开.Pedersen 承诺所具有的隐藏性(hiding)和绑定性(binding)使得观察者无法通过公开账本中记录的承诺值 $C(r,v)$还原出交易金额,从而实现了交易内容的隐私保护.此外,Pedersen 承诺具有加法同态特性,即:

$$C(r_1,v_1)+C(r_2,v_2)=C(r_1+r_2,v_1+v_2).$$

这为矿工(验证者)使用金额承诺进行隐藏交易验证提供了便利.假设一个交易的输入为 v_1、v_2,输出为 v_3.为了确保交易平衡,即 $v_1+v_2=v_3$,构建的交易承诺应满足:

$$C(r_1,v_1)+C(r_2,v_2)=C(r_1+r_2,v_1+v_2)=C(r_1+r_2,v_3).$$

因此,矿工只需通过公开承诺的加法运算即可完成交易平衡性的验证.

为了实现交易过程中的身份隐藏,MimbleWimble 采用了改进的 CT 方案.首先,MimbleWimble 系统中取消

了用户交易地址,公开账本中记录的每一条 UTXO 中不再存有标识用户身份的公钥信息,这使得所有基于交易地址的关联分析技术失效,尤其是增加了交易可链接性的分析难度;其次,为了解决无用户地址情况下的 UTXO 确权问题,MimbleWimble 在交易输出承诺的构建过程中指定接收方随机秘密选择交易输出的盲化因子 r,并由此实现对该 UTXO 的权属控制.由于这一过程带来了输入输出承诺盲化因子的差值 excess[101],因此也将矿工对交易平衡的等式验证过程转化为验证交易双方共同构建以 excess 为私钥的正确签名过程.此外,在隐去交易身份标识的同时,基于签名方案的平衡性验证也使得在 MimbleWimble 中实现交易聚合的 CoinJoin 方案成为可能.如果在以 excess 为私钥构建签名的过程中使用可聚合签名技术,如文献[104−106]中的聚合签名方案,则矿工在出块过程中可将同一区块内的交易与 excess 签名进行聚合构成多输入输出交易,从而更好地实现了交易双方的身份隐私保护.

综上所述,MimbleWimble 通过无标识交易的方式来实现交易发送方和接收方的身份隐藏,具有较好的隐私保护特性.但这一方案也存在着一定的问题:首先,由于 MimbleWimble 隐藏了身份标识,因此交易构建过程需要双方通过链外方式进行参数交互,这一方面增加了交易过程的复杂度,另一方面也带来了链外通信的隐私泄露风险;其次,MimbleWimble 并未采取混币技术进行交易身份隐藏,因此 UTXO 间的对应关系仍可为观察者提供关联分析的便利.即使是采用 CoinJoin 聚合方法,矿工在交易聚合过程中仍可看到原始交易输入输出的对应关系,这一过程并未完全解决交易的内部不可链接性问题,仍存在一定的隐私泄漏风险;此外,文献[95]通过在 Pedersen 承诺所提供的阈下信道中嵌入特征值来实现货币追踪的方法,这同样会对 MimbleWimble 中的交易链接和身份隐私构成威胁.

5 总结及未来展望

区块链系统中的身份管理技术是当前的研究热点,也是制约区块链系统整体安全和应用推广的关键要素.但是由于在应用需求、信任模型和法规遵从等方面存在较大的差异,因此目前主流区块链身份管理系统所采取的研究方法和技术路线上也各有不同.

首先,在身份标识方面,目前的区块链系统大多采用基于非对称密码体制的公私钥对来进行用户的身份标识.目前的公有链密码货币项目大多选择 ECDSA 和 ED 25519 算法,出于对算法的安全性、签名验签性能、密钥交换效率等方面的考虑,不同的项目,有不同的选择.此外,如零币中并不使用身份标识的私钥签名来完成货币支付行为的确认,因此在其身份标识中引入了另一对用于零知识证明的算法因子,以实现对货币的权属控制.对于无标识交易技术 MimbleWimble,虽然可以通过取消身份标识来增加隐私保护,但也带来了链外通信的额外开销.对于目前的联盟链,如 Hyperledger Fabric、Corda 等,多以选择 ECDSA、RSA 等传统的公私钥密码体制为主,并通过 CA 颁发数字证书来实现用户身份的实名或可控匿名认证.

其次,在身份认证方面,为了解决身份隐私保护的问题,公有链和联盟链都提供了匿名身份认证的机制.与公有链中用户自主生成标识身份的公私钥不同,为了实现监管友好的目的,联盟链更多地采用由中心机构 CA 来生成用户实名或匿名认证的身份标识,从而实现实名认证和可控匿名的设计需求.但应注意的是,由于区块链交易系统具有账本公开、多方确认的特点,简单使用匿名身份认证并不能有效地解决交易身份隐私保护的问题.

此外,为了有效解决交易身份的隐私保护问题,必须在交易过程中采取相应的交易身份隐藏技术.目前的隐藏方法多以“混淆”思想为主,如何构建更为高效、安全的混币过程得到了密码货币项目的广泛关注.在联盟链中,这一问题关注得较少,仍有待进一步加以研究.对于区块链系统的行业应用而言,自主混币和全局混币技术明显具有更广泛的应用场景.

综上所述,我们将目前主流区块链系统中的身份管理技术加以总结,详见表 2.

随着区块链技术在多领域的广泛推广和深入应用,基于区块链构建的交易系统也对隐私保护技术提出了更多的需求,未来亟需在以下几个方面展开作更进一步的研究.

首先,在身份管理的功能需求层面,随着区块链技术在金融、社会治理等领域的广泛应用,传统公链中无监

管的身份隐私保护方案无法满足交易可监管的需求.因此必须提供内置于交易模型和交易流程中的可监管技术,在必要时可正确地恢复出交易身份和内容,以防止非法交易行为.如何设计更高效、安全的可监管隐私保护方案有待进一步研究.此外,随着近年来分布式身份管理和分布式数字身份(decentralized ID)概念的提出,如何将分布式数字身份管理与区块链系统相融合,实现 DID 在区块链系统中的应用也是未来的关注点.

Table 2 Summay of the identity management in blockchain

表 2 区块链系统身份管理技术总结

	身份标识	身份认证	身份隐藏		实现复杂度
			发送方身份隐藏	接收方身份隐藏	
比特币[1]	公钥	匿名	无	无	低
协同混币[46,50,51]	公钥	匿名	混淆	混淆	中
自主混币[10]	公钥	匿名	可链接环签名	一次性地址	高
全局混币[75]	公钥+零知识证明	匿名	零知识证明	一次性认证加密	高
无标识支付[96]	无标识	匿名	无地址	无地址	低
Hyperledger Fabric[14]	数字证书	实名	无	无	低
	Idemix	可控匿名	无	无	中
Corda[13]	数字证书	实名	无	无	低
	隐蔽身份	可控匿名	无	无	低
FISCO BCOS[25]	数字证书	实名	无	无	低
	群签名	可控匿名	无	无	中
趣链[24]	数字证书	实名	无	无	低

其次,身份管理的算法设计一直是研究的热点.一方面,随着新应用场景的不断出现,区块链系统已经从简单的密码货币应用走向分布式基础信任架构,设计适合于新需求的身份认证和隐私保护算法是推进区块链系统深入发展的必然要求,如基于身份的密码体制、零知识证明、多方安全计算、同态加密等密码学机制在交易身份和内容隐藏的研究方面都得到了广泛关注;另一方面,原有的算法方案在安全性和性能方面的不足,也会推动相关问题的进一步研究.门罗币、零币、Fabric 等隐私保护方案的快速迭代充分表明了这一方向的研究工作非常活跃.

最后,在身份管理方案的实现层面,提高算法实现的性能和安全性也有待深入研究.身份认证和隐私保护方案大多基于复杂的密码学运算,较低的性能一直是制约其大范围推广的瓶颈环节,因此,高效的算法实现方案备受关注;此外,通过引入,如 TEE、SGX 和 USB Key 等系统安全技术,为隐私保护方案提供安全存储和安全计算环境,从而提高性能和安全性也具有非常好的研究和应用前景.

6 结束语

本文基于区块链交易模型的特点,分析了区块链系统中身份管理技术涵盖的主要内容、关键问题及安全挑战,从身份标识、身份认证和身份隐藏 3 个方面比较分析了目前主流区块链平台中身份管理和隐私保护的不同实现技术,并展望了相关领域的未来研究方向.随着区块链技术的不断普及和推广,其应用场景和应用模式也会日益丰富,作为区块链系统基础组件的身份管理必然会受到更多的关注,希望本文能够为未来的研究工作提供有益的借鉴.

References:

[1] Nakamoto S. Bitcoin: A peer to peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[2] Zhou P, Du Y, Li B. White Paper of Blockchain Technology and Development in China. Beijing: Ministry of Industry and Information Technology, 2016. 5–25 (in Chinese).

[3] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. ACTA AUTOMATICA SINICA, 2016,42(4):481–494 (in Chinese with English abstract).

[4] Dai W. B-money. 2018. http://www.weidai.com/bmoney.txt

[5] Zhu LH, Gao F, Shen M, *et al*. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017,54(10):2170–2186 (in Chinese with English abstract).

[6] Genkin D, Papadopoulos D, Papamanthou C. Privacy in decentralized cryptocurrencies. Communications of the ACM, 2018,61(6): 78–88.

[7] Fu S, Xu HX, *et al*. A survey on anonymity of digital currency. Chinese Journal of Computers, 2019,42(5):1045–1062 (in Chinese with English abstract).

[8] Zhang A, Bai XY. Survey of research and practices on blockchain privacy protection. Ruan Jian Xue Bao/Journal of Software, 2020,31(5):1406−1434 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[9] Dash. https://www.dash.org/

[10] Monero. https://www.getmonero.org/

[11] Sasson EB, Chiesa A, Garman C, *et al*. Zerocash: Decentralized anonymous payments from bitcoin. In: Proc. of the IEEE Symp. on Security and Privacy 2014. IEEE, 2014. 459–474.

[12] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. In: Proc. of the Network and Distributed System Security Symp. Internet Society, 2016. 1–14.

[13] Corda. https://www.corda.net/

[14] Hyperledger Foundation. Hyperledger Fabric. https://github.com/hyperledger/fabric

[15] Androulaki E, Barger A, Bortnikov V, *et al*. Hyperledger Fabric: A distributed operating system for permissioned blockchains. In: Proc. of the 13th European Systems Conf. New York: ACM, 2018. 30–45.

[16] Ethereum. https://www.ethereum.org/zh/

[17] Ethereum. ERC20. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md

[18] Facebook. Libra White Paper. https://libra.org/en-US/white-paper/

[19] Bitcoin. Hierarchical Deterministic Wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[20] IPFS. https://github.com/ipfs/

[21] W3C. DID. https://www.w3.org/TR/did-core/

[22] W3C. Verifiable Credential. https://www.w3.org/TR/vc-data-model/

[23] 微众银行. WeIdentity. https://github.com/WeBankFinTech/WeIdentity

[24] 趣链科技.趣链. https://github.com/hyperchain

[25] 微众银行. FISCO BCOS. https://github.com/bcosorg

[26] Cachin C. Architecture of the hyperledger blockchain Fabric. In: Proc. of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Zurich: IBM Research, 2016. 1–4.

[27] Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. New York: ACM, 2002. 21–30.

[28] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps. In: Proc. of the CRYPTO 2004. Berlin: Springer-Verlag, 2004. 56–72.

[29] Au MH, Susilo W, Mu Y. Constant-size dynamic *k*-TAA. In: Proc. of the Int'l Conf. on Security and Cryptography for Networks. Berlin: Springer-Verlag, 2006. 111–125.

[30] Camenisch J, Drijvers M, Lehmann A. Anonymous attestation using the strong Diffie Hellman assumption revisited. In: Proc. of the Int'l Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag, 2016. 87–101.

[31] Camenisch J, Dubovitskaya M, Enderlein RR, *et al*. Concepts and languages for privacy-preserving attribute-based authentication. Journal of Information Security and Applications, 2014,19(1):25–44.

[32] Corda. Corda API references. https://docs.corda.net/api-identity.html

[33] Boneh D, Boyen X, Shacham H. Short group signatures. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 2004. 41–55.

[34] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system. In: Proc. of the Security and Privacy in Social Networks. Berlin: Springer-Verlag, 2013. 197–223.

[35] Liao K, Zhao Z, Doupé A, *et al*. Behind closed doors: Measurement and analysis of CryptoLocker ransoms in bitcoin. In: Proc. of the APWG Symp. on Electronic Crime Research. IEEE, 2016. 1–13.

[36] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security 2013. Berlin: Springer-Verlag, 2013. 6–24.

[37] Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in bitcoin P2P network. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM, 2014. 15–29.

[38] Gao F, Mao HL, Wu Z, *et al*. Lightweight transaction tracing technology for bitcoin. Chinese Journal of Computers, 2018,41(5): 989–1004 (in Chinese with English abstract).

[39] Meiklejohn S, Pomarole M, Jordan G, *et al*. A fistful of bitcoins: Characterizing payments among men with no names. In: Proc. of the ACM Conf. on Internet Measurement Conf. New York: ACM, 2013. 127–140.

[40] Zhao C, Guan Y. A graph-based investigation of bitcoin transactions. In: Proc. of the IFIP Int'l Conf. on Digital Forensics. Berlin: Springer-Verlag, 2015. 79–95.

[41] Zheng B, Zhu L, Shen M, *et al*. Malicious bitcoin transaction tracing using incidence relation clustering. In: Proc. of the Int'l Conf. on Mobile Networks and Management. Berlin: Springer-Verlag, 2017. 313–323.

[42] Chen T, Zhun YX. Understanding Ethereum via graph analysis. In: Proc. of the IEEE Conf. on Computer Communications. IEEE, 2018. 1484–1492.

[43] Spagnuolo M, Maggi F, Zanero S. Bitiodine: Extracting intelligence from the bitcoin network. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2014. 457–468.

[44] Blockchain. https://Blockchain.info/wallet

[45] Bitcoin Fog. Accessing bitcoin fog. http://bitcoinfog.info/

[46] Bonneau J, Narayanan A, Miller A, *et al*. Mixcoin: Anonymity for bitcoin with accountable mixes. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2014. 486–504.

[47] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for bitcoin. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2015. 112–126.

[48] Chaum D. Blind signatures for untraceable payments. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 1983. 199–203.

[49] Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2016. 43–60.

[50] Maxwell G. CoinJoin: Bitcoin privacy for the real world. https://bitcointalk.org/index.php?topic=279249.0

[51] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for bitcoin. In: Proc. of the European Symp on Research in Computer Security. Berlin: Springer-Verlag, 2014. 345–364.

[52] Corrigan-Gibbs H, Ford B. Dissent: Accountable anonymous group messaging. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM, 2010. 340–350.

[53] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981,24(2):84–90.

[54] Ruffing T, Moreno-Sanchez P, Kate A. P2P Mixing and unlinkable Bitcoin transactions. In: Proc. of the Network and Distributed System Security Symp. Internet Society, 2017. 43–58.

[55] Chaum D. The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1988, 1(1):65–75.

[56] Saxena A, Misra J, Dhar A. Increasing anonymity in bitcoin. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2014. 122–139.

[57] Wang ZY, Liu JW. Full anonymous blockchain based on aggregate signature and confidential transaction. Journal of Computer Research and Development, 2018,55(10):2185–2198 (in Chinese with English abstract).

[58] Saberhagen NV. CryptoNote v2.0. https://cryptonote.org/whitepaper.pdf

[59] NIST, FIPS 186-4, Digital signature standard. https://csrc.nist.gov/publications/detail/fips/186/4/final

[60] Bernstein DJ, Duif NN, Lange T, *et al*. High-speed high-security signatures. Journal of Cryptographic Engineering, 2012,2(2): 77–89.

[61] Bernstein DJ, Lange T. Faster addition and doubling on elliptic curves. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2007. 29–50.

[62] Noether S, Mackenzie A. Ring confidential transactions. Ledger, 2016,1:1–18.

[63] Noether S, Goodell B. An efficient implementation of Monero subaddress. https://lab.getmonero.org/pubs/MRL-0006.pdf

[64] Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2001. 552–565.

[65] Chaum D, Heyst E. Group signatures. In: Proc. of the Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer-Verlag, 1991. 257–265.

[66] Fujisaki E, Suzuki K. Traceable ring signature. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin: Springer-Verlag, 2007. 181–200.

[67] Cramer R, Damgård I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 1994. 174–187.

[68] Back A. Ring signature efficiency. https://bitcointalk.org/index.php?topic=972541.msg10619684#msg10619684

[69] Liu JK, Wei VK, Wong DS. Linkable spontaneous anonymous group signature for ad hoc groups. In: Proc. of the Australasian Conf. on Information Security and Privacy. Berlin: Springer-Verlag, 2004. 325–335.

[70] Goodell B, Noether S. Compact linkable ring signatures and applications. https://lab.getmonero.org/pubs/MRL-0011.pdf

[71] Moser M, Soska K, Heilman E, *et al*. An empirical analysis of traceability in the Monero blockchain. Privacy Enhancing Technologies, 2018,(3):143–163.

[72] Kumar A, Fischer C, Tople S, *et al*. A traceability analysis of Monero's blockchain. In: Proc. of the Symp. on Research in Computer Security. Berlin: Springer-Verlag, 2017. 153–173.

[73] Yu J, Au MH, Esteves-Verissimo P. Re-thinking untraceability in the CryptoNote-style blockchain In: Proc. of the 32nd IEEE Computer Security Foundations Symp. IEEE, 2019. 94–9413.

[74] Yuen TH, Sun SF, Liu JK, *et al*. Ring CT 3.0 for blockchain confidential transaction: Shorter size and stronger security. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin: Springer-Verlag, 2020. 464–483.

[75] Zcash Foundation and Electric Coin Company. Zcash. https://z.cash/zh/get-started/

[76] Sander T, Ta-Shma A. Auditable, anonymous electronic cash. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 1999. 555–572.

[77] Miers I, Garman C, Green M, *et al*. Zerocoin: Anonymous distributed e-cash from bitcoin. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2013. 397–411.

[78] Sasson EB, Chiesa A, Garman C, *et al*. Zerocash: Decentralized anonymous payments from bitcoin. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2014. 459–474.

[79] Zcash Foundation and Electric Coin Company. Zcash Documentation. https://zcash.readthedocs.io/en/latest/

[80] Groth J. Short pairing-based non-interactive zero-knowledge arguments. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2010. 321–340.

[81] Lipmaa H. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In: Proc. of the Theory of Cryptography Conf. Berlin: Springer-Verlag, 2012. 169–189.

[82] Bitansky N, Chiesa A, Ishai Y, *et al*. Succinct non-interactive arguments via linear interactive proofs. In: Proc. of the Theory of Cryptography Conf. Berlin: Springer-Verlag, 2013. 315–333.

[83] Gennaro R, Gentry C, Parno B, *et al*. Quadratic span programs and succinct NIZKs without PCPs. In: Proc. of the Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2013. 626–645.

[84] Parno B, Howell J, Gentry C, *et al*. Pinocchio: Nearly practical verifiable computation. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2013. 238–252.

[85] Ben-Sasson E, Chiesa A, Genkin D, *et al*. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 2013. 90–108.

[86] Lipmaa H. Succinct non-interactive zero knowledge arguments from span programs and linear error-correcting codes. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2013. 41–60.

[87] Ben-Sasson E, Chiesa A, Tromer E, *et al*. Succinct non-interactive arguments for a von neumann architecture. In: Proc. of the 23rd USENIX Conf. on Security. New York: ACM, 2014. 781–796.

[88] Bellare M, Boldyreva A, Desai A, *et al*. Key-privacy in public-key encryption. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2001. 566–582.

[89] Bernstein DJ. Curve 25519: New Diffie-Hellman speed records. In: Proc. of the Int'l Workshop on Public Key Cryptography. Berlin: Springer-Verlag, 2006. 207–228.

[90] Zero Coin Co. ZSL. https://github.com/ConsenSys/zsl-q/

[91] Ben-Sasson E, Chiesa A, Green M, *et al*. Secure sampling of public parameters for succinct zero knowledge proofs. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2015. 287–304.

[92] Wilcox Z. How to generate SNARK parameters securely. https://electriccoin.co/blog/snark-parameters/

[93] Kappos G, Yousaf H, Maller M, *et al*. An empirical analysis of anonymity in Zcash. In: Proc. of the 27th USENIX Security Symp. USENIX, 2018. 463–477.

[94] Quesnelle J. On the linkability of Zcash transactions. https://arxiv.org/abs/1712.01210

[95] Biryukov A, Feher D, Vitto G. Privacy aspects and subliminal channels in Zcash. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM, 2019. 1813–1830.

[96] Jedusor TE. MIMBLEWIMBLE. https://github.com/mimblewimble/docs/wiki/MimbleWimble-Origin

[97] Poelstra A. Mimblewimble. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf

[98] Maxwell G. Confidential transactions. https://people.xiph.org/~greg/confidential_values.txt

[99] Back A. Bitcoins with homomorphic value. https://bitcointalk.org/index.php?topic=305791.0

[100] Fuchsbauer G, Orrù M, Seurin Y. Aggregate cash systems: A cryptographic investigation of Mimblewimble. In: Proc. of the EUROCRYPT. Berlin: Springer-Verlag, 2019. 657–689.

[101] Grin. https://github.com/mimblewimble/grin

[102] Beam. https://github.com/BeamMW/beam

[103] Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. In: Proc. of the CRYPTO. Berlin: Springer-Verlag, 1991. 129–140.

[104] Bellare M, Namprempre C, Neven G. Unrestricted aggregate signatures. In: Proc. of the Int'l Colloquium on Automata, Languages, and Programming. Berlin: Springer-Verlag, 2007. 411–422.

[105] Boneh D, Gentry C, Lynn B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps. In: Proc. of the EUROCRYPT. Berlin: Springer-Verlag, 2003. 416–432.

[106] Boneh D, Drijvers M, Neven G. Compact multi-signatures for smaller blockchains. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin: Springer-Verlag, 2018. 435–464.

附中文参考文献:

[2] 周平,杜宇,李斌.中国区块链技术和应用发展白皮书.北京:工业和信息化部,2016.5–25.

[3] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481–494.

[5] 祝烈煌,高峰,沈蒙,李艳东,郑宝昆,毛洪亮,吴震.区块链隐私保护研究综述.计算机研究与发展,2017,54(10):2170–2186.

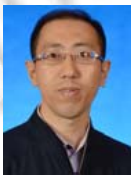
[7] 付烁,徐海霞,李佩丽,等.数字货币的匿名性研究.计算机学报,2019,42(5):1045–1062.

[8] 张奥,白晓颖.区块链隐私保护研究与实践综述.软件学报,2020,31(5):1406−1434. http://www.jos.org.cn/1000-9825/5967.htm [doi: 10.13328/j.cnki.jos.005967]

[38] 高峰,毛洪亮,吴震,沈蒙,祝烈煌,李艳东.轻量级比特币交易溯源机制.计算机学报,2018,41(5):989–1004.

[57] 王子钰,刘建伟,张宗洋,喻辉.基于聚合签名与加密交易的全匿名区块链.计算机研究与发展,2018,55(10):2185–2198.

姚前(1970－),男,博士,教授级高工,博士生导师,主要研究领域为金融科技与监管,区块链,数字资产与数字货币,资产证券化.



张大伟(1974－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为信息安全,区块链.