Journal of Computer Applications ISSN 1001-9081
计算机应用 CODEN JYIIDU http://www.joca.cn

doi:10.11772/j.issn.1001-9081.2022101555

区块链交易隐私保护技术综述

谢晴晴[1,2*]，杨念民[1,2]，冯霞[3]

(1.江苏大学 计算机科学与通信工程学院，江苏 镇江 212013；
2.江苏省工业网络安全技术重点实验室(江苏大学)，江苏 镇江 212013；
3.江苏大学 汽车与交通工程学院，江苏 镇江 212013)

(*通信作者电子邮箱 xieqq@ujs.edu.cn)

摘 要: 区块链账本数据是公开透明的，攻击者通过分析账本数据以获取敏感信息，对用户的交易隐私产生威胁。鉴于区块链交易隐私保护的重要性，首先分析产生隐私泄露的原因，并将交易隐私分为交易者身份隐私和交易数据隐私两类；然后，从这两种不同类型的隐私出发，阐述现有的面向区块链交易的隐私保护技术；接着，鉴于隐私保护和监管之间矛盾性，介绍兼具监管的交易身份隐私保护方案；最后，对区块链交易隐私保护技术未来的研究方向进行了总结和展望。

关键词: 区块链；交易隐私保护；身份隐私；交易数据隐私；交易监管

中图分类号: TP309 **文献标志码: A**

Survey on privacy-preserving technology for blockchain transaction

XIE Qingqing[1,2*], YANG Nianmin[1,2], FENG Xia[3]

(1. College of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang Jiangsu 212013, China;
2. Jiangsu Key Laboratory for Industrial Network Security Technology (Jiangsu University), Zhenjiang Jiangsu 212013, China;
3. College of Automotive and Traffic Engineering, Jiangsu University, Zhenjiang Jiangsu 212013, China)

Abstract: Blockchain ledger is open and transparent. Some attackers can obtain some confidential information through analyzing the ledger data. It causes a great threat to users' privacy preservation. In view of the importance of transaction privacy preservation, the causes of the transaction privacy leakage were analyzed at first , and the transaction privacy was divided into into two types: the transaction participator's identity privacy and transaction data privacy. Then, in terms of these two types of transaction privacy, some existing privacy-preserving technologies were presented. Next, in view of the contradiction between the transaction identity privacy preservation and supervision, some exiting blockchain supervision schemes were introduced. Finally, the future research directions of the privacy-preserving technologies on the blockchain transaction were summarized and prospected.

Keywords: blockchain; transaction privacy preservation; identity privacy; transaction data privacy; transaction supervision

0 引言

区块链最初依托于中本聪发明的比特币[1]被提出。区块链集成了加密算法、点对点传输、智能合约和共识机制等技术，具有公开透明性、不可篡改性、去中心化、交易假名化等优点[2]，广泛应用于数字货币[3-4]、供应链[5-6]、电子投票[7-8]、车联网[9-10]、医疗业[11-12]等多领域。以金融供应链为例，传统金融体系存在着信息不对称、信息孤岛、结算不能自动完成等诸多缺点[13]。金融供应链可以采用区块链技术将银行、核心企业、二三级供应商和其他金融机构上链，支持资金流、信息流、信任流同时传递，并通过嵌入智能合约实现协议的自动执行，提高了信息共享效率，降低了信任和资金传递成本。

区块链账本数据的公开透明性一方面极大地方便了各节点对数据进行维护验证，另一方面又会给用户隐私保护带来威胁。攻击者对全局账本进行分析，获取用户的身份隐私信息和数据隐私信息。尽管区块链地址是匿名的，但是攻击者可以采取聚类技术或交易图分析技术，建立地址与地址，地址与交易的联系，进而获取地址的交易规律、交易特征、交易轨迹等[14]。通过这些交易细节，攻击者可以将现实中的用户交易行为和对账本数据分析所勾勒出的用户行为进行匹配，从而获取用户真实身份，造成用户身份隐私的泄露。除此之外，攻击者可通过数据分析、数据挖掘、深度学习等方法从海量数据中提取出有价值的信息；经过处理(如属性匹

收稿日期: 2022-10-18; 修回日期: 2023-01-09; 录用日期: 2023-01-10。
基金项目: 国家自然科学青年基金项目（NO.62002139）；国家自然科学基金面上项目（NO.62272203）；中国博士后科学基金资助项目（NO.2019M651738）；江苏省自然科学青年基金项目（NO.BK20200886）。
作者简介: 谢晴晴(1990—)，女(汉)，安徽宿州人，讲师，博士，CCF 会员，主要研究方向：区块链监管、应用密码学；杨念民(1998—)，男(汉)，江西赣州人，硕士研究生，主要研究方向：区块链监管、数子货币；冯霞(1983—)，女(汉)，江苏镇江人，副教授，博士，主要研究方向：物联网认证协议、区块链和应用密码学。

配、信息关联)的数据存在泄露敏感信息的可能[15]。例如：在网购链中，攻击者通过分析交易金额来推断用户的购买力、收入水平、消费习惯等，甚至推测出用户的真实身份；在医疗链中，攻击者能够获取用户的病历信息或者家庭住址信息等，这将对用户的日常工作生活造成不便，甚至对自身安全造成威胁。因此，区块链交易隐私泄露问题亟待解决。保证区块链上用户的身份隐私和数据隐私是区块链能够真正落地所面临的一项重要挑战。但是身份隐私并不是无条件的，因为非法用户会利用匿名身份逃避监管。因此兼顾监管的身份隐私也受到关注。

区块链交易隐私保护是目前的研究热点，，2017 年，祝烈煌等[16]从混币技术、加密技术和限制发布技术三方面探讨了目前的交易层的隐私保护技术；2018 年，王宗慧等[17]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了总结。2019 年，李旭东等[18]从两个方面对比特币隐私保护技术做了总结：一方面是不需要修改现有比特币协议的技术，如混币技术、离链支付协议；另一方面是需要修改现有比特币协议的技术，如密码学方案。2020 年，张奥等[19]主要通过技术实现原理，将保护技术划分为地址混淆、信息隐藏和通道隔离。上述相关工作对区块链隐私做了分类定义，如分为身份隐私和交易内容隐私等[17]。然而在探讨具体的隐私保护技术时，上述工作将交易身份和交易内容的隐私保护放在一起讨论，没有集中分析面向交易内容和交易身份的隐私保护在设计思路和实现手段上的差异。考虑到实际应用对需要保护隐私的对象不同，本文有必要将交易身份隐私和交易内容隐私分开讨论。另外交易身份隐私之上的身份监管问题在行业应用中日益凸显，为此本文也对兼顾监管的交易身份隐私保护技术进行了讨论。

依据保护对象的不同，本文将交易隐私保护技术分为交易身份隐私保护技术和交易数据隐私保护技术。其中交易身份指交易地址所关联的真实用户身份，交易数据是指双方交易的内容，如交易金额。在“区块链+供应链”的应用中[20]，交易身份指发送者地址、接收者地址所关联的真实身份；交易数据是指产品描述、价格、交易数量等数据。

如图 1 所示，本文从保护对象的分类，隐私攻击的手段，身份隐私保护措施，数据隐私保护措施以及身份隐私保护上的监管等五个方面来组成区块链交易隐私保护技术的框架。

图1 区块链交易隐私保护技术框架

Fig. 1 Technical framework for blockchain transaction privacy-preserving

1 区块链交易隐私问题分析

区块链中的交易信息包含账户地址信息和交易数据信息，其中账户地址信息与用户身份相关，地址信息的关联性会导致用户身份隐私的泄露。而交易数据在不同场景下具体表现不同，例如在数字货币领域，交易数据主要是指交易金额，在医疗链领域交易数据主要是指医疗数据。这两类信息保护的措施不同，就身份隐私保护而言，主要采用混淆技术(借助混合服务器或者密码学技术)隐藏账户地址的关联性；就数据隐私保护而言，对于交易金额这类需要可验证的数据主要采同态加密技术，一是可以提供机密性，二是节点可以利用同态加密算法的同态性验证隐藏交易金额的平衡性；对于其他的交易数据可以采用属性基加密、可搜索加密等。为此，本章将交易隐私分为交易身份隐私和交易数据隐私两类，并介绍了相应的隐私泄露问题。

1.1 交易身份隐私泄露

交易身份隐私是指用户的真实身份与交易账户地址（即交易假名）的关联关系。区块链地址的生成无需实名认证，而且同一拥有者可以产生各种不同的交易账户地址，不同的交易账户地址之间无直接关联关系。因此区块链在一定程度上为用户匿名交易提供了技术支持。但由于所有的交易路径都是公开的，攻击者可以通过地址跟踪用户的交易数据，分析交易规律，从而取得用户交易地址间的关联性，并结合网络外部信息进一步推测用户真实身份信息[21]。Reid 等[22]根据比特币交易结构特征提出了交易图和用户图的理论，对用户身份去匿名化。Meiklejohn 等[23]在 Reid 等[22]工作的基础上，

结合区块链交易的隐藏知识即“交易的找零地址和输入地址都同属于一个用户地址”，提出了一种启发式聚类方法对用户身份进行去匿名化。Androulaki 等[24]使用模拟器来模拟显示大学环境中比特币的使用，发现即使通过手动创建新地址来增强隐私，但是依靠交易聚合技术仍然可以在很大程度上揭露 40%比特币用户的真实身份。Shen 等[25]在底层网络中使用传播模式分析的方法对大规模的比特币交易进行去匿名化。Teng 等[26]通过量化的启发式去匿名方法提出一种 IP 匹配方法。该方法可以将 IP 的活动信息与区块链中的交易记录进行匹配，以准确确定交易者及其相应的区块链地址。

1.2 交易数据隐私泄露

交易数据隐私是指存储在区块链的交易内容隐私，例如交易金额、交易数量等。区块链公开透明的特性虽然可以减少重复对账行为和信用风险，但是同时也会导致交易数据隐私泄露[27]。以供应链为例，区块链技术的使用可以打造出一个可信透明的数据网络，提升企业决策有效性，促进供应链上下游企业数据之间的流通。但同时供应链中包含着丰富的敏感数据，如信息流、资金流、物流、商流等。一般情况下这些数据只能在具有合作伙伴关系的企业之间流动，如果将这些数据直接上链存储，竞争对手可以通过这些公开数据推断出商业合作关系、市场供求关系和资金流转情况等，对企业的核心竞争力造成威胁，不利于社会经济稳定。因此，解决交易数据隐私泄露问题对区块链的实际落地具有重要意义。

交易身份隐私保护方案主要有以下两类：混币机制[28-37]和基于密码学技术的身份隐私保护机制[38-41]；其中混币机制分为中心化混币机制[28-31]和去中心化混币机制[32-37]。基于密码学技术的身份隐私保护机制主要用到的密码学技术有零知识证明[38-39]、环签名[40-41]。交易数据隐私保护方案主要依赖于密码学技术，如：同态加密算法[42-44]、可搜索加密算法[45]、属性基加密算法[46-47]。

2 身份隐私保护方案

2.1 混币机制

混币机制通过割裂交易输入和输出的关系来达到保护用户身份隐私的效果。根据有无中心化服务器的参与，混币机制可以分为中心化混币机制和去中心化混币机制两类。

2.1.1 中心化混币机制

中心化混币机制由第三方混币服务器完成混币过程。首先混币需求者将混币资金发送给第三方混币服务器，第三方混币服务器将收集的资金进行分配，最后将混币金额发送至用户指定输出地址上。中心化混币服务的过程一般包含 4 个阶段[48]：

1）协商阶段：混合用户和第三方混币服务器关于混币输入地址、混币输出地址、第三方混币服务器的托管地址和混合手续费等交易细节内容达成一致。

2）输入阶段：混合用户将商定的混币金额从输入地址发送到第三方混币服务器的托管地址上。

3）输出阶段：第三方混币服务器从混合池里随机选择等额的混合资金转移至混合用户指定的输出地址上。

4）混币记录删除阶段：混币协议正常结束后，混币用户和第三方混币服务器销毁本次混币记录，防止泄露混币信息。

目前第三方混币服务提供商有 BitLaundry[28]、BitFog[29]等。但是中心化混币机制主要存在着以下问题:1）安全性依赖于混币服务器，混币服务器可能盗窃资金和私自保留混币信息，泄露混币过程；2）相近时间内参与混币的用户的混合金额需相同；3）需要支付手续费。针对早期中心化混币方式存在盗窃风险的问题， Bonneau 等[30]于 2014 年提出了可问责的混币方案—Mixcoin。相较于早期的混币方式，Mixcoin 做了以下两点改进：一是 Mixcoin 添加了问责机制来惩罚混币服务器的盗窃行为。若混合用户在规定的时间内没收到混币服务器的转账交易，可以公布签名承诺追责混币服务器的盗窃行为；二是在手续费用问题上，Mixcoin 采取的是随机手续费策略，避免因手续费固定而降低用户匿名性。Mixcoin 实现混合的不可区分性，被动攻击者无法确定用户和匿名集中的哪一个用户在交互；针对可以破坏混合不可区分性的主动攻击者，Mixcoin 利用匿名通信网络将多个混合交易链接在一起形成比特币混合网络，从而增加攻击者的难度。然而混币服务器仍然可以学习混合用户输入地址到输出地址的映射，进而泄露混币过程。为此，Valenta 等[31]于 2015 年提出了改进的中心化混币方案—盲币(BlindCoin) 。该方案使用盲签名技术来屏蔽混币服务器学习混合用户的输入地址到输出地址的映射。然而 Blindcoin 方案中的用户必须将他们的签名发布到公共日志上。这允许攻击者将输出地址链接到混币服务器的签名密钥上，打破了混合的不可区分性。此外，Blindcoin 没有解决混币服务器可以私自截留资金的问题。

2.1.2 去中心化混币机制

中心化的混币模式在一定程度上保护了交易者身份隐私。但是由于第三方混币服务器的参与，不但用户的资产会被混币服务器盗窃，而且用户的交易信息也会被服务器泄露，另外混合用户需要缴纳额外的手续费。去中心化混币机制由多个参与者协作运行混币协议，抛弃了第三方中心化的混币服务器，解决了第三方混合服务器的加入所带来的信任问题。去中心化混币机制的交易流程主要分为 4 个阶段[48]：

1）协商阶段：参与混币的用户关于混币金额、输入地址和输出地址等达成一致。

2）混淆阶段：参与混币用户根据混币协议对所有输出地址进行混淆。混淆阶段的目的是打乱用户输入和输出地址间的关联性。

3）广播阶段：根据混淆阶段得到的输出地址构造混合交易，确认交易无误后广播交易信息，将资产转移至各混币用户指定的输出地址。

4）混币记录删除阶段：若混合过程无异常，则所有参与此次混合的用户销毁本次交易记录，混合交易结束；若混合过程出现错误，则需要参与混币的用户们找出并排除行为不端的用户。

2013 年，Gregory[32]提出了第一个不需要第三方服务器参与的去中心化混币方案—联合混币(Coinjoin)。有混合意愿的用户共同组成一个混合群，该群共同生成一个混合交易，包含了所有混合用户的输入地址和随机排序后的输出地址。由于混币的金额是相同的，攻击者无法分辨出交易输入和输出地址的关系。然而交易输入和输出地址的链接关系对于参与混币交易的节点是可见的，无法保证交易内部的不可链接性。在 Coinjoin 的基础上，Duffield[33]于 2014 年提出了达世(Dash)币。该项目中的混币交易是由网络中的主节点来构造，从而保证了内部隐私性。多个主节点为用户的交易进行链式混币，即上一个主节点的交易输出作为下一个主节点的交易输入进一步混淆，最多可以进行 16 轮混合。当混合轮数越多时，Dash 币匿名性越强，但是与之相应的混合费用和时间开销也会增大。另外为了增强混合的匿名性，所有的交易输入和输出都是相同的标准面额，如 0.001、0.01、0.1、1 和 10。同年， Ruffing 等[34]沿用 Coinjoin 技术提出了一种基于解密混合网的混币方案(Coinshuffle)。Coinshuffle 方案采用解密混合网络技术[49]打乱输出地址集合，解决了内部节点知道其他节点输出地址的问题。然而，CoinShuffle 方案混淆阶段的计算开销和通信开销会随着混合用户的增加而急剧增大，不适合大规模用户混合。Ziegeldort 等[35]于 2015 年提出了一种基于解密混合网络技术和 门限椭圆曲线数字签名算法[50]的安全多方混币方案(Coinparty)。Coinparty 通过使用安全多方计算协议来模拟受信任的第三方以实现用户之间的匿名混币。类似于 CoinShuffle 方案，Coinparty 在混淆阶段同样采用了解密混合网络技术来保障内部隐私性。另外，相比较于 CoinShuffle 方案 Coinparty 做了如下两点改进:一是采用秘密分享验证混淆的正确性;二是要求最后一位参与者以字典序对输出集进行排序,再增加公共随机置换得到最终混淆结果,避免最后一位用户操纵排序结果。

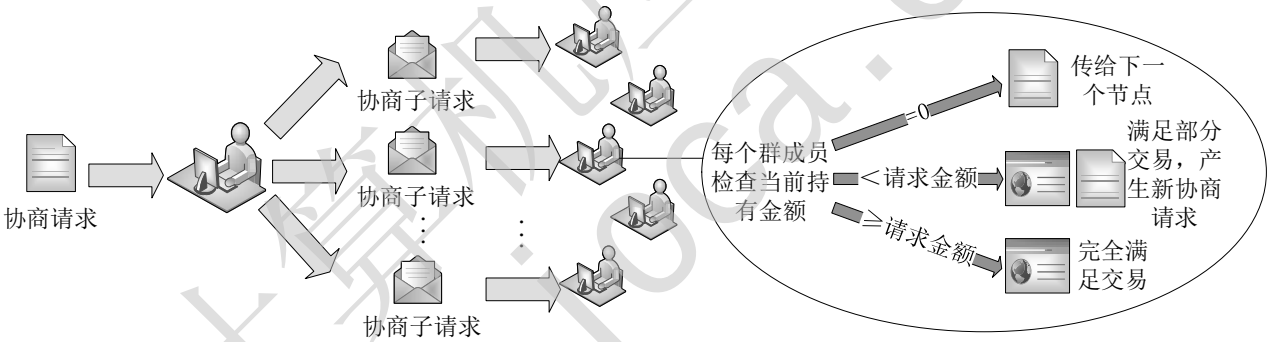

图2 去中心化混币方案过程

Fig. 2 Process of decentralized coin mixing scheme

2021 年，Xiao 等[36]提出了一种基于去中心化分布式签名的混币方案。该方案采用协商方式进行混合交易，从而避免群成员获悉其他成员的初始交易。另外，为了避免对第三方的依赖以及额外的混合费，该方案采用多方签名协议来签署交易。图 2 为去中心化混币方案的过程[36]，有混合意愿的用户组成一个混合群。群成员将协商请求分解成 k 个相互独立的协商子请求,并将协商子请求随机分发给不同的群成员。其他群成员接收到协商子请求后做如下处理：若当前持有金额为 0，将子协商请求分发给其他节点；若其持有金额小于协商子请求的协商金额，将当前持有金额全部转给协商子请求中的输出地址，并向其他节点发送新的协商请求以满足剩余协商金额的需求；若当前持有金额大于或等于协商子请求的协商金额，向协商子请求中的输出地址发送一笔交易，交易金额为协商金额。然后，群成员将所有协商交易汇总成最终混合交易，验证自身输出地址是否收到相应金额。若无差错，群成员使用基于 Elgamal 的去中心化签名协议来签署最终交易。然而，协商过程存在较大的通信开销。此外，群内成员需要相互保持匿名性，否则恶意成员根据协商请求消息能够以高概率分析出交易输入和输出的链接关系。2022 年，Lu 等[37]提出了一种面向大规模比特币交易的高效混币方案(CoinLayering)。为了防止混合节点分辨出输入和输出地址关系，CoinLayering 使用中国剩余定理和 Schnoor 签名构造的群签名作为资产转移凭证，以此来消除用户输入和输出地址的关系。然而，该方案并不能防止合谋攻击，混合节点合谋将会暴露用户的输入和输出地址关系。

本节从混币的角度介绍相关的身份隐私保护方案。在早期，交易用户为了保持身份的匿名性，可以向混合服务器请求提供混币服务，但是这种中心化的混币方式存在混合服务器盗窃资产的行为，尽管有一些改进的方案如 Mixcoin，Blindcoin 通过添加签名承诺的方式对混合服务的行为加以约束，但是如果混合服务器不顾自己的声誉，依然可以盗窃交易用户的资产。为此相关学者提出了去中心化的混币方案，

摒弃了中心化混合服务器，由参与混合的用户自行协商混币方式。但是去中心化的解决方式又容易产生混合节点内部泄露混币信息的风险和混合节点拒不签名的行为。针对混合节点内部泄露混币信息的风险，可以采用解密混合网技术如 Coinshuffle，Coinparty 方案。针对混合内部节点盗窃资产或者拒不签名的行为,可以采用阈值签名的方式控制输入资产，增加恶意混合节点拒不履行协议的成本如 Coinpary，CoinLayering 方案。除此之外，还可以使用去中心化式的签名方式以相互协商的方式完成去中心化式的混币如文献[36]。表 1 对以上方案的结构、不可链接性、盗窃风险、抗 DOS 攻击和抗 Sybil 攻击这五个方面的特点进行总结和对比。其中 DOS 攻击和 Sybil 攻击是两种比较常见的攻击方式，所以表 1 中还比较了混币机制对这两种攻击的抵抗性。

表1 混币机制总结

Tab. 1 Summary of confusion mechanism

方案	结构	不可链接性	盗窃风险	抗 DOS	抗 Sybil
可问责的混币方案[30]	中心化	部分	中	高	高
盲币[31]	中心化	√	中	高	高
联合混币[32]	去中心化	部分	低	低	低
达世币[33]	去中心化	部分	中	高	高
基于解密混合网的混币方案[34]	去中心化	√	低	低	低
安全多方混币方案[35]	去中心化	√	低	高	高
基于去中心化分布式签名的混币方案[36]	去中心化	√	低	高	高
面向大规模比特币交易的高效混币方案[37]	去中心化	√	低	高	高

2.2 基于密码学技术的身份隐私保护机制

2.2.1 混币方案

通过将交易地址打乱的方式来隐藏交易之间的关联性，从而保护交易者身份隐私。但是交易地址仍然公开可见，恶意节点通过分析混合交易特征可以将交易地址关联到用户的真实身份上。而且混币方案易遭受资金盗窃、拒绝服务和信息泄露等攻击。为此研究者们利用零知识证明和环签名等密码学手段，对交易地址进行隐藏，以此增加攻击者通过分析账本数据来获取交易者真实身份的难度。基于零知识证明的加密货币方案

零知识证明(Zero-Knowledge Proof, ZKP) [51]能够让证明者在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。零币(Zerocoin)[38]和零钞(Zerocash)[39]采用零知识证明技术来保护交易者身份隐私。这类加密货币通常包含如下两个部分：

铸币：封装交易来源、去向和金额，将比特币转换为相应的加密货币，并将对应的承诺加入到承诺列表中。

熔币：交易发起者采用零知识证明技术来证 明对交易输入的所有权，从而花费所持有的加密货币。

Zerocoin 是 2013 年 Miers 等 [38] 采用 RSA(Rivest-Shamir-Adleman)累加器[52]和非交互式零知识证明技术[53]提出的加密货币方案。ZeroCoin 系统通过铸币交易将比特币转换为 zerocoin，并将 zerocoin 对应的唯一承诺加入到混淆集 RSA 累加器中。用户在花费时仅需出示零知识证明来表明累加器中有一枚未花费的硬币即可。矿工验证零知识证明的正确性并检验硬币是否在其他交易中出现过（避免双重支付）。若这两个条件都满足，则交易成功。由于借助了零知识证明技术，整个过程在花费交易时不必出示一枚具体的硬币信息,从而隐藏了铸币交易和花费交易的链接关系，使得攻击者难以通过交易图分析技术来窥探交易者身份隐私。然而 ZeroCoin 使用固定面值的硬币，不支持精确值支付。另外，在花费阶段用户采用双离散对数证明机制来证明其对特定 Zerocoin 的所有权，存在存储代价高、验证时间长和交易效率低的缺点。

针对 Zerocoin 的缺陷 ，Eli Ben Sasson 等[39]于 2014 年基于简洁的非交互式零知识证明技术(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, ZK-SNARKs)[54]又提出了一种改进方案 Zerocash。同 Zerocoin 一样，Zerocash 分为铸币交易和花费交易两个部分。在铸币过程中，交易发起者将指定数量的基础币兑换成相同金额的 Zerocash，每个币有独特的序列号。铸币过程实质上是承诺生成过程。该承诺封装了交易来源、去向和金额。为了达到混淆的目的，生成的承诺将被添加到承诺列表中。在熔币交易中，交易发起者将旧币拆分或合并成新币，并采用零知识证明技术来证明以下内容：1）交易发起者在承诺列表中拥有未花费的硬币；2）交易前后，硬币的总价值相等。为了使接收方使用新币，发起者用接受方的公钥对新币参数加密。接受方用私钥扫描到交易内容后，解密密文，生成新币的序列号。矿工根据交易发起者给出的证明，确认承诺在承诺列表中且序列号未在花费列表中。由于每一枚币都有唯一的一次性序列号表示，序列号的唯一性保证了匿名资产不能被双重花费。

ZeroCash 在熔币交易中采用零知识证明技术来证明用户对交易输入的所有权，而非采用签名的方式来解锁未花费交易输出，从而割裂了铸币交易与熔币交易以及熔币交易与

熔币交易之间的关联性，使得攻击者无法通过交易图技术将不同交易关联起来。此外，在熔币交易过程中，接收者的交易信息被加密，保护了接收者身份隐私。相较于 Zerocoin 系统，Zerocash 做了如下改进：1）使用 zk-SNARKs 技术减少 Zerocoin 中证明所花费的存储空间和验证时间；2）支持可变金额的匿名交易和交易后找零；3）支持使用 zerocash 直接向用户支付。但是 Zerocash 存在的缺点是：需要可信的第三方设置系统的初始参数和公共参数，这会影响系统安全性；熔币交易需要耗时 2min 左右，导致交易效率低下。

2.2.2 基于环签名算法的加密货币方案

环签名算法最初是由 Rivest 等[55]提出，系统中只有地位相等的环成员而没有管理者。在签名过程中，签名者的公私钥和群里其它成员的公钥混合在一起对消息进行签名。在签名验证过程中，验证者使用环参数和群成员的公钥列表来验证签名的有效性。验证者只能验证出群中有环成员对消息进行了签名，而无法确定具体的签名者，从而保护了签名者身份隐私。

2014 年，Saberhagen[40] 提出了一种基于环签名和一次性公钥的电子货币系统 (CryptoNote) 。为了实现交易接受者身份的不可链接性，CryptoNote 采用一次性公私钥技术为接收者生成接收地址，使得攻击者难以推测出任何两个交易输出属于同一个接收者。为了实现交易发起者身份的不可追踪性，CryptoNote 在可追溯环签名机制的基础上提出了一次性环签名机制。该机制将真实的交易发起者隐藏于其他交易输出地址中，来实现对交易发起者身份的隐藏。CryptoNote 过程如下:

1)构造交易输出地址:交易的发起者获取接收者的公钥，并生成一次性公钥兼目的地址。

2）签署交易：交易的发起者生成一次性环签名，以隐藏身份。交易发起者将引用多个相同金额的外部交易输出地址，随同发起者的一次性输出地址 P_i、P_i 对应的私钥 x_i、以及密钥镜像 $I = x_i \cdot H_p(P_i)$ 对交易进行签名 $\delta = Sig(pkList \cup P_i, x_i, I)$。

3）签名验证及双花检测：矿工对接收到的交易进行签名验证以及双花检测。矿工根据签名验证算法 来验证签名的有效性即。签名验证通过后，矿工检查密钥镜像是否在之前的签名中被使用过。如果已经使用过，则表明两笔交易被同一密钥签署，即存在双花现象。

4）接收交易：接收者通过用私钥检测上传到区块链的每笔交易，来确定目标交易，然后计算一次性私钥来解密目标交易输出。

CryptoNote 通过结合不可链接的一次性公钥和不可追踪的一次性环签名实现了交易与交易之间的不可关联性，对交易发起者和接收者身份起到了很好的保护作用。但是随着环成员增多，交易签名的大小也会跟着线性增长，给区块链的存储增加了负担；此外环签名匿名性强度取决于环成员的数量。Liu 等[41]于 2018 年采用带有环签名的输出地址来阻止混币服务器学习输入和输出的映射关系，提出了一个不可链接的交易混合方案。

本节介绍了基于密码学技术的身份隐私保护技术。目前对身份隐私保护技术所采取的隐私保护技术主要有零知识证明、环签名等。这些密码学技术与混淆技术的原理类似，将真正的交易用户隐藏于其他与交易无关的用户中。与混币技术相比，基于密码学的身份隐私保护技术匿名性更强，但是存在较大的计算开销和验证开销。表 2 对上述基于密码学技术的身份隐私保护机制的优缺点进行了总结。

表2 基于密码学技术的身份隐私保护机制

Tab. 2 Summary of identity privacy-preserving mechanism based on cryptography

技术名称	优点	缺点
零币[38]	具有强匿名性	不支持精确值支付，计算和存储开销大，验证时间长
零钞[39]	支持精确值支付，匿名性强	依赖可信第三方，交易效率低下，计算和存储开销大
基于环签名和一次性公钥的电子货币系统[40]	具有不可链接性和不可追踪性	匿名性强度取决于环成员数量
基于环签名的交易混合方案[41]	具有不可链接	交易金额需保持一致

3 交易数据隐私保护方案

目前针对交易数据的隐私保护方案一般采用同态加密、可搜索加密和属性基加密这三类技术:

同态加密技术提供了一种对加密数据进行处理的工具[56-57]。许多学者采用同态加密技术对区块链系统中的交易金额进行保密处理，以此来保护交易隐私。Back[58]于 2013 年提出了“具有同态价值的比特币”。Maxwell [42]于 2015 年在 AdmBack 工作的基础上进行了完善和改进，提出了机密交易方案。该方案所采用的佩德森承诺机制具有加法同态特性[59]，借此矿工可以在不知晓交易金额的情况下，来验证区块链交易的收支平衡。承诺中不但加入盲化因子，来防止恶意用户暴力破解金额承诺值，而且还添加一个范围证明以保证承诺的金额在 0 和特定值之间。Maxwell G 所提出的机密交易方案流程包括三步：1）金额盲化：交易者采用佩德森承诺对交易输入金额和输出金额进行盲化。2）金额范围证明：交易者基于 Borromean Ring Signatures[60]技术对每个输入和输出金额承诺值添加范围证明。3）验证：矿工验证输入金额承诺值总和与输出金额承诺值总和是否平衡，根据范围证明判断被盲化的金额值是否为正值。但是，该方案对交易金额进行盲化后，交易接收者无法恢复出原数据，需要额外的通信通道接收交易金额，而且机密交易所占空间是普通交易的 60

倍，给区块链存储带来了负担。Wang 等[43]于 2017 年提出使用 Paillier[61]提出的同态加密算法对交易金额进行保密处理，见图 3 所示，其过程为：1）交易金额加密：交易发起者分别使用交易接收者的公钥 pk_i 和系统公钥 pk_d 对交易金额 V_i 进行加密得到密文 $C_i = Enc_{pk_i}(V_i)$ 和 $C_i' = Enc_{pk_d}(V_i)$，其中 C_i' 被发送至验证层的 dump 账户。2）交易金额承诺和验证：发送者生成两类承诺证明，一类用于证明交易输入之和等于交易输出之和[62]；另一类用于证明被盲化的输出金额为 V_i 正值[63]。通过验证 Dump 账户中的金额密文 C_i' 符合上述两类承诺证明后，每个交易金额密文 C_i 被发送给相应的接收者 i。3）交易金额解密：每个接收者 i 对接收的密文 C_i 进行解密得到交易金额 $V_i = Dec_{sk_i}(C_i)$，将接收到的交易金额 V_i 作为下一个交易输入。但是该方案中交易金额的合法性验证计算开销较大，而且交易金额密文占用存储空间较大，增加了区块链存储成本。2020 年 Chen 等[44]引入了一种新的同态加密公钥方案 twisted Elgamal，并利用 twisted Elgamal 实现了账户余额的隐藏和交易金额的隐藏。其过程为：1）交易的参与者在发起交易前使用自己的公钥加密账户余额。2）当发起交易时，交易的发起者分别使用自身公钥和接收方的公钥加密交易金额得到交易密文 (C_s, C_r)，并采用零知识证明技术证明交易的正确性即①交易发起者的账户余额大于交易余额;② C_s 和 C_r 对同一交易金额的承诺。3）当验证者对该笔机密交易的正确性验证成功后，交易的发起者和交易的接收者可以根据 twisted Elgamal 的加法同态性使用交易密文 (C_s, C_r) 更新账户余额。与 Paillier 同态加密算法相比，twisted ElGamal 的加解密效率更高，密文和密钥所占的存储空间更小。

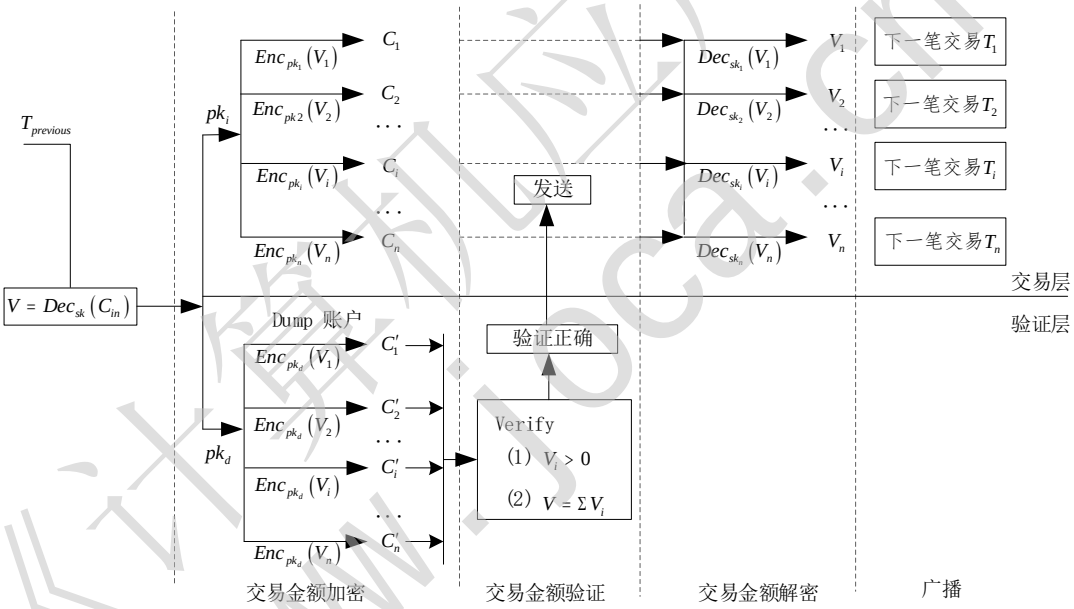

图3 基于 paillier 加密算法的交易金额保密方案示意图

Fig. 3 View of transaction amount privacy-preserving scheme based on the paillier encryption algorithm

可搜索加密技术是搜索技术和加密技术的结合，支持对加密数据进行关键字搜索[64-65]。Liu 等[45]将区块链技术与可搜索加密技术相结合，实现对医疗数据隐私的保护。首先，数据拥有者对数据进行加密，并上传到星际文件系统(Inter Planetary File System, IPFS)中。若上传成功，IPFS 会返回数据存储地址。数据拥有者通过访问策略加密数据存储地址、关键字索引以及数据密钥，并将加密结果上传到区块链网络中。然后，数据查询者利用自己的私钥以及查询的关键字计算搜索陷门，并调用搜索智能合约。若数据查询者的属性满足访问策略，合约将返回数据的存储地址以及数据密钥。最后，数据查询者便可以根据存储地址从 IPFS 中下载数据。该方案基于许可链和分布式 IPFS 构建链上和链下的存储模型，采用可搜索加密算法实现了数据的可信存储、安全存储、可验证。但是搜索算法的计算开销会随着属性数量的增加而线性增长，而且仅支持单一关键词的搜索。

密文策略属性基加密技术是一种可支持访问控制的数据加密方式[66-67]，与区块链相结合可以实现数据的隐私保护和访问控制。Guan 等[46]于 2020 年结合区块链和属性基加密技术提出了一套智能电网交易数据隐私保护方案。该方案在密文策略属性基加密（Ciphertext Policy Attribute-Based Encryption, CP-ABE）算法[68]的基础上提出了一种可更新的双层密文结构的属性基加密算法，实现对交易数据的细粒度访问控制。首先，用户在客户端发出账户注册交易申请。系统采用类似比特币账户生成算法为节点生成地址和私钥。然后，交易发起者制定一个访问策略并生成一个线性密钥共享(Linear Secret-Sharing Scheme, LSSS)的访问结构[69]，对第一

层明文和第二层明文加密。第一层明文包含详细的交易合同信息。第二层明文包括基本的交易信息。只有满足访问策略的交易用户才能查看第二层明文。在获取第二层明文的基础上，产生交易意愿的节点可以通过应用获得第一层明文。交易双方就交易内容达成一致后，加密的交易合同将被传播到网络中，由记账节点负责将交易信息打包成区块，并加入到区块链中。双方发生争议时，可以向仲裁节点申请仲裁。仲裁结果生成后，原始的密文会被更新，形成新的交易记录，以保证仲裁节点不会解密新的交易内容。但是随着属性的增多，其计算开销也会线性增长。Li 等[47]于 2020 年结合区块链技术和密文策略属性基加密(Ciphertext Policy Attribute-Based Encryption, CP-ABE)，提出了一种基于区块链的车用自组织网络(Vehicular Ad-hoc Network, VANET)数据细粒度访问控制方案。该方案使用区块链替代第三方混合服务器进行用户身份管理和数据存储，并根据用户属性建立不同的 VANET 数据访问权限。但是，存储在区块链中的消息易导致数据冗余，给区块链存储带来负担。

本节从同态加密技术、可搜索加密技术、属性基加密技术对当前的交易数据隐私方案做了总结。同态加密技术可以对隐私数据进行合法性验证如交易输入和输出金额平衡性验证，也适用于需要执行隐私计算的数据。目前用到的同态加密算法主要有佩德森承诺算法、Paillier 加密算法和 ElGamal 加密算法等。佩德森承诺是一种单向承诺，无法由承诺结果得到被承诺值，还需要额外的开销传输明文值。Paillier 加密算法中的承诺值可以被解密成明文，并且相比于采用佩德森诺算法的机密交易所占存储空间更小。Twisted Elgamal 是一种加法同态加密算法，加解密效率优于另外两种。属性基加密算法适用于对数据进行细粒度访问控制，但是目前属性基加密算法存在着计算开销随属性增长而线性增长、访问策略暴露等问题。可搜索加密技术实现了隐私数据的关键字搜索，但是存在着搜索效率问题。表 3 对上述交易数据隐私保护方案的优缺点进行了总结。

表3 交易数据隐私保护方案总结

Tab. 3 Summary of privacy-preserving schemes for transaction data

方案	优点	缺点
机密交易[42]	支持密文验证	占据较大存储空间，交易接收者无法解密输出密文
基于 Paillier 加密算法的隐私交易[43]	支持密文验证，交易双方都可解密各自密文	计算开销大，占据较大的存储空间
基于 Twisited Elgamal 加密算法的隐私交易[44]	支持密文验证，加解密效率高	需要一定的验证开销
基于区块链和属性基可搜索加密的医疗数据保护方案[45]	支持密文检索和数据的安全存储，避免单点故障	计算开销随属性增多而线性增长，仅支持单一关键字搜索
基于区块链和属性基加密的隐私保护能源交易[46]	实现对交易数据的细粒度访问控制	计算开销随属性增多而线性增长
基于区块链的车用自组织网络数据细粒度访问控制方案[47]	提供分布式的、细粒度的数据共享服务	易导致数据冗余，增加区块链存储负担

。

4 兼顾监管的交易身份隐私保护方案

隐私保护一方面增强用户的隐私性，另一方面也给违法犯罪分子从事犯罪活动提供了可乘之机。在区块链交易隐私保护基础上实现交易监管引起了学者们的高度关注[70]。

2019 年 Li 等[71]改进门罗币[72]并提出可追踪的门罗币(Traceable Monero)系统。该系统在原有系统基础上增加了问责机制，一方面可以追踪资金的流动轨迹，另一方面可以从一次性匿名地址中推出用户的长期地址。为了追踪交易双方真实的交易地址，可追踪门罗币系统要求交易发起者基于 ElGamal 加密算法使用监管者的公钥来加密关键隐私信息。在构造交易输入时，交易发起者使用环签名技术来隐藏交易发起者身份，并将真实的交易输入账户在交易输入群中的索引进行加密。在构造交易输出时，交易发起者对用户的长期地址加密并做为标签，以此来构造一次性匿名地址。在发现可疑交易时，监管者可以解密标签和密文获取关键信息，从而追踪用户交易过程。Lin 等[73]于 2020 年提出了一种基于区块链的去中心化条件匿名支付(Decentralized Conditional Anonymous Payment, DCAP)系统。该系统使用自更新的假名算法[74]在隐私和监管之间取得平衡，不仅支持用户进行匿名交易，而且还引入监管部门来监控交易记录。用户借助自更新的假名算法基于长期公钥派生出许多不可链接的匿名公钥，并在匿名公钥中嵌入监管者公钥。在交易时，交易双方采用匿名公钥作为交易双方账户。为了证明拥有对交易输入的所有权，交易发起者借助知识签名技术[75]证明拥有匿名公钥所对应的私钥。在追踪可疑交易时，监管者可以借助其私

钥通过匿名公钥反推出长期公钥，并根据公钥信息查询用户证书以获取其真实身份。然而该方案采用的是未花费的交易输出(Unspent Transaction Output, UTXO)记账模型，尽管使用了匿名公钥做为匿名账号，但没有消除交易与交易之间的关联性，对用户身份隐私仍存在威胁。此外，监管者拥有绝对的追踪权限，安全性过于依赖监管者。同年，Androulaki 等[76]提出了一套隐私保护下可审计的代币系统，该具有隐私保护可审计的货币系统结构[76]如图 4 所示。为了实现隐私保护和可审计性，交易发起者基于 ElGamail 加密算法采用审计者的公钥来加密转移交易信息并采用零知识证明技术来证明交易信息被正确加密。在发行交易时，货币发行者发布基于承诺的代币。在转移交易时，交易发起者不直接引用历史有效交易的代币，而是通过向认证者提交认证请求的方式来证明代币的合法性，其中认证请求包含一个代币（即承诺）。认证者收到此类请求后会检查代币是否包含在分类帐本的有效交易中。如果存在，认证者使用分布式阈值盲签名技术[77-78]对代币进行盲签名。交易发起者在收到签名后，通过零知识证明技术向矿工证明代币存在分类账本中且自身已注册，从而不暴露代币的隐私信息。

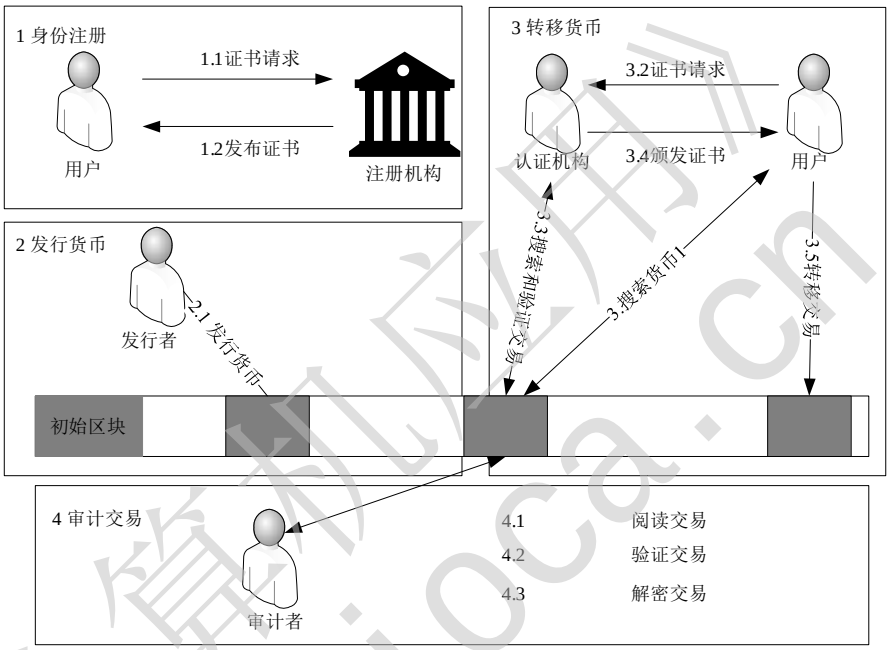

图4 具有隐私保护可审计的货币系统示意图

Fig. 4 View of privacy-preserving auditable currency system

Shao 等[79]于 2020 年提出了一种基于标签公钥加密算法的隐私保护框架。该框架基于许可链，一方面为合法交易提供了不可链接性和匿名性，另一方面也为可疑交易提供了问责机制。交易发起者在发起交易前，需向属性权威机构申请认证。属性权威机构认证成功后，使用基于属性的签名算法[80]为交易发起者生成证书。在发起交易时，交易发起者采用基于标签的公钥加密算法[81]来加密真实身份，并生成零知识证明来证明其证书满足访问策略以及真实身份被正确加密。在交易追踪时，追踪节点集齐 t 个解密分享后，就可以恢复出真实的用户身份。该方案采用基于标签的公钥加密算法，将追踪不法用户的权力分配给多个独立的跟踪成员，而不是依赖于单点管理，避免了权力的滥用，而且显著改善了许可网络中的用户隐私保护和自主权，但是未能保护交易接收者身份隐私。

Barki 等[82]于 2020 年提出了一种可追溯、可转让和可分割的数字货币系统，兼顾了合法用户的隐私保护和非法用户的身份追溯。该系统实现了中心化资产和去中心化资产的互相转换。用户可以将存在银行的资产取出换做数字货币，以去中心化的方式进行匿名交易。在该数字货币系统中，银行在仅知交易金额和不知对应的用户接收地址的情况下，就可以采用部分盲签名技术[83]对交易金额和用户接收地址产生签名，从而保证了交易的匿名性。用户收到数字货币后，可以类似于比特币那样进行交易。为了实现交易的可审计性，该系统采用 ElGamal 加密算法来加密用户的身份公钥，并利用零知识证明的方式来证明身份公钥被正确加密。然而，交易与交易之间存在链接性，关联的交易特征容易成为攻击者挖掘用户身份的推手。

Yuen[84]于 2020 年提出了一种实现隐私交易、可认证且可审计的联盟链（Private, Authenticated & Auditable Consortium Blockchain，PAChain）。PAChain 有交易发起者隐私、交易金额隐私和交易接收者隐私三个独立的保护模块。在交易发起者隐私保护模块中，发起者不直接引用未花费的交易输出，而是采取匿名证书的形式来证明拥有未花费的输出。具体过程为：发送者采用离散对数知识签名技术向背书节点证明其拥有某未花费的交易输出所对应的私钥。背书节点验证通过后采用 BBS 群签名算法[85]为该未花费交易输出

颁发证书。在之后的交易中，发起者采取零知识证明的方式证明其拥有背书节点所颁发的交易输出证书。在交易金额隐私保护模块中，发送者基于 Elgamal 加密算法使用审计者的公钥对交易输入金额和输出金额进行加密，并利用基于 Boneh-Boyen signature 的范围证明算法[86]为承诺值中的金额提供区间证明。在交易接收者隐私保护模块中，发起者根据接收者的长期公钥生成一次性公钥作为输出地址，并采取零知识证明的方式证明接收者长期公钥通过认证机构(Certification Authority, CA)认证。为了实现可审计，三个模块中的关键信息如发起者身份信息、交易金额、接收者身份信息被审计者的公钥所加密。交易用户可以调用三个模块构造一个完整、隐私保护、可认证且可审计的交易，并且可以与 Fabric 相融合。然而，该方案过多的使用零知识证明技术导致交易所占存储空间增大，验证开销增大，交易效率低下。

Lin 等[87]于 2021 年在 Ethereum 架构基础上提出了一种面向加密货币的隐私保护的许可链架构（Privacy-preserving Permissioned blockChain， PPChain）。PPChain 兼顾了用户身份的匿名保护和可监管性，以及数据的公开透明性和机密性。交易发起者生成一笔类似于以太坊的交易后，采用广播加密算法[88]对交易进行加密，并使用群签名算法[89]对加密后的交易进行签名。验证节点使用群公钥验证签名，若签名正确，首先使用广播加密中对应的私钥解密密文，然后验证交易金额是否超出世界状态里的账户余额。若验证正确，交易将被发送到记录节点，由记录节点提交到区块链。该方案采用群签名算法对交易进行签名，既保证用户身份的合法性，也支持对不法用户身份进行追踪。该方案所采用的广播加密算法实现了交易数据的隐私保护和接收者的匿名保护。但是验证节点可以解密数据，窥探数据隐私，该架构对验证节点可信度要求较高。

本节对身份隐私保护基础上的监管方案做了探讨。这些方案在实现监管上主要采用加密技术如 Elgamal 加密技术对用户的身份标识公钥进行加密，在配合零知识证明技术保证加密的正确性，此外还可以利用群签名的打开特性或者可反推的匿名算法揭露匿名身份。表 4 对上述兼顾监管的交易身份隐私保护方案的优缺点进行了总结和对比。

表4 兼顾监管的交易身份隐私保护方案总结

Tab. 4 Summary of transaction identity privacy-preserving scheme considering supervision

方案	优点	缺点
可追踪的门罗币[71]	隐私保护能力强，可追踪交易双方身份	计算开销大
基于区块链去中心化条件匿名支付系统[73]	可监管、假名管理方便	未消除交易前后之间的关联性
隐私保护下可审计的代币系统[76]	可审计、隐私保护能力强	计算开销和通信开销大
基于标签公钥加密算法的隐私保护框架[79]	多方监管	未能保护交易接收者身份
可追溯、可转让和可分割的数字货币系统[82]	实现了数字货币和现实货币互换	通信开销大
可认证且可审计的联盟链[84]	可审计、隐私保护能力强	计算和存储开销大、验证时间长、交易效率低下
面向加密货币的隐私保护的许可链架构[87]	数据的公开透明和机密性	对验证节点可信度要求高

5 未来研究工作

针对交易身份隐私保护和数据隐私保护以及相应的监管需求，目前已经有相应的解决方案。但是也存在一些不足如安全性问题，计算开销问题等。鉴于此，未来可以从以下三个方向来开展研究：

1）兼顾强安全性和高可用性的交易隐私保护技术研究：以数字货币为代表的应用场景对安全性和高可用性要求高。一项成熟的数字货币其资产安全性应得到保证，交易能及时处理。隐私保护技术的引入是为了保护数字货币系统的隐私性，但是不能为了隐私保护而降低其实际需求。在隐私保护的实际过程中，一些隐私保护方案借助零知识证明和环签名等密码学技术来应对隐私威胁，但这些方案也引入一定的安全风险。例如 Zerocash 方案中所采用的简洁的非交互式零知识证明技术(Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, ZK-SNARK)技术依赖于第三方来生成秘密参数，因此第三方的可信性直接决定了整个系统的安全性。为此，未来可以考虑采用安全多方计算形式来生成秘密参数[90]，以取代第三方。另外，现有隐私保护方案在性能上也存在一定不足，如采用零知识证明技术需要大量的计算开销和验证开销，这使其难以应用到一些对交易处理速度要求高的场景中[91]。为此，根据实际的应用场景，考虑对数据敏感性进行细粒度分类[92]，对于敏感度较低的数据，系统性能将做为首要参考因素；而对于高敏感数据，强隐私保护性仍然是首要考虑因素。从而实现性能和隐私保护两者的折中。

2）多方监管技术研究：多方监管技术对以金融链为代表的应用场景很有必要。以金融场景为例，我国的金融体系是采用多方监管的方式对金融机构加以约束。多方监管体制可以有效降低金融市场的成本，维持正常的金融秩序。 区块链技术应用到金融体系中也应保留多方监管的特点。然而，目前的交易监管方案大多仅支持单方监管，单方监管存在监

管权力滥用、隐私泄漏、单点故障等问题。要将区块链技术落地，应考虑多方监管。为此，可以考虑基于访问控制策略、秘密分享[93]或安全多方计算[94]等机制向多个可信机构赋予监管权力。

3）跨链操作中的隐私保护研究：随着区快链技术的不断发展和创新，越来越多的数字货币涌现，应用到其他领域的区块链系统更是不胜枚举。区块链技术在其他场景得到不断深入应用，场景之间融合的需求也越来越大。如供应链之间的融合。然而，如今的区块链系统大多是异构，链与链之间无法进行直接的数据流通[95]。在此背景下，打破区块链间的数据孤岛，实现不同区块链之间的资产信息互通、原子性交易、服务互补等功能是必然的发展趋势。跨链技术在此发挥了巨大的作用。然而，在跨链过程中易发生信息泄露、资产盗窃等。解决其中的隐私和安全问题，才有可能借助跨链技术将不同的区块链连接成链联网，实现应用场景的需求如资产转移、信息共享等。当同一事务需要跨越多个区块链系统执行时，在保证数据高效性和一致性的前提下，降低隐私泄露的风险显得尤为重要。所以，跨链操作中的隐私保护是未来的重要研究方向。为此，可以考虑将隐私智能合约[96]、可信硬件执行环境[97]、身份认证[98]等手段结合起来解决跨链过程中存在的隐私泄露问题。

6 结语

区块链技术有着广阔的应用场景，在应用过程中所产生的交易隐私问题成为了专家的重点研究方向。我们将区块链交易隐私分为身份隐私和数据隐私两类，并给了相关的定义，以及对隐私泄露的原因进行了分析。针对身份隐私保护，我们从混币机制和基于密码学技术的身份隐私保护机制着手出发总结了相应的解决方案。针对数据隐私保护方案，我们介绍了同态加密技术、可搜索加密技术、属性基加密技术等相关解决方案。其次，面对身份隐私保护技术可能会被不法分子利用的问题，我们还介绍了在身份隐私保护基础上的监管方案。最后，针对区块链交易隐私保护方案存在的一些问题，我们对未来研究方向进行了展望。

参考文献

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system. [EB/OL].(2008-11-01) [2021-07-21]. http://bitcoin.org/bitcoin.pdf.

[2] 傅丽玉,陆歌皓,吴义明,等.区块链技术的研究及其发展综述[J].计算机科学,2022,49(S1):447-461,666.(FU L Y, LU G H, WU Y M, et al. Review on the research and development of blockchain technology [J]. Computer Science,2022,49(S1):447-461,666.)

[3] HAN X, YUAN Y, WANG F Y. A Blockchain-based Framework for Central Bank Digital Currency[C]//Proceedings of the 2019 International Conference on Service Operations and Logistics, and Informatics. Piscataway: IEEE, 2019:263-268

[4] 李娟娟,袁勇,王飞跃.基于区块链的数字货币发展现状与展望[J].自动化学报,2021,47(4):715-729. (LI J J, YUAN Y, WANG F Y. Based on digital currency development present situation and prospect of block chain [J]. Journal of automation, 2021, 47 (4) : 715-729).

[5] MANE A E, CHIHAB Y, TATANE K, et al. Agriculture Supply Chain Management Based on Blockchain Architecture and Smart Contracts[J]. Applied Computational Intelligence and Soft Computing, 2022, 2022(8011525): 23.

[6] 许蕴韬,朱俊武,孙彬文,等.选举供应链：基于区块链的供应链自治框架[J].计算机应用,2022,42(06):1770-1775.(XU Y T, ZHU J W, SUN B W, et al. Electoral Supply chain: a framework of Supply chain autonomy based on blockchain [J]. Journal of Computer Applications, 2022, 42(06): 1770-1775)

[7] 吴芷菡,崔喆,刘霆,等.基于区块链的安全电子选举方案[J].计算机应用,2020,40(07):1989-1995.(WU Z H, CUI Z, LIU T, et al. Secure electronic election scheme based on blockchain [J]. Journal of Computer Applications, 2020, 40(07): 1989-1995)

[8] 张伯钧,李洁,胡凯,等.基于区块链的分布式加密投票系统[J].计算机科学, 2022, 49(S2):679-684.(ZHANG B J, LI J, HU K, et al. Distributed cryptographic voting system based on blockchain [J]. Computer Science, 2022, 49(S2): 679-684).

[9] 熊啸,李雷孝,高静,等.区块链在车联网数据共享领域的研究进展[J].计算机科学与探索,2022,16(05):1008-1024.(XIONG X, LI L X, GAO J, et al. Research progress of blockchain in data sharing of Internet of Vehicles [J]. Computer Science and Exploration, 2022, 16(05): 1008-1024.)

[10] 陈葳葳,曹利,邵长虹.基于区块链技术的车联网高效匿名认证方案[J].计算机应用,2020,40(10):2992-2999.(CHEN W W, CAO L, SHAO C H. Efficient Anonymous Authentication scheme for Internet of Vehicles based on blockchain technology [J]. Journal of Computer Applications, 2020, 40(10): 2992-2999.)

[11] VARDHINI B; SHREYAS N D, SAHANA R, et al. A Blockchain based Electronic Medical Health Records Framework using Smart Contracts [C]// Proceedings of the 2021 International Conference on Computer Communication and Informatics. Coimbatore: IEEE, 2021:1-4

[12] 林超,何德彪,黄欣沂.基于区块链的电子医疗记录安全共享[J].计算机应用,2022,42(11):3465-3472.(LIN C, HE DEBIAO, HUANG X Y. Electronic medical record based on the block chain security share [J/OL]. Computer application, 2022, 42(11): 3465-3472.)

[13] JIANG C and RU C. Application of Blockchain Technology in Supply Chain Finance[C]// Proceedings of the 2020 International Conference on Mechanical, Control and Computer Engineering, Piscataway: IEEE, 2020:1342-1345.

[14] RON D, SHAMIR A. Quantitative Analysis of the Full Bitcoin Transaction Graph[C]// Proceedings of the 2013 International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2013: 6-24.

[15] 刘炜,彭宇飞,田钊,等.基于区块链的医疗信息隐私保护研究综述[J].郑州大学学报(理学版),2021,53(02):1-18.(LIU W, PENG Y F, TIAN Z, et al. Health information privacy protection based on block chain research review [J]. Journal of zhengzhou university (science edition), 2021 53(02): 1-18).

[16] 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.(ZHU L H, GAO F, SHEN M, et al. Journal of Computer Research and Development,2017,54(10):2170-2186.)

[17] 王宗慧,张胜利,金石,等.区块链数据隐私保护研究[J].物联网学报,2018,2(03):71-81.(WANG Z H, ZHANG S L, JIN S，et al. Research on data privacy protection in blockchain [J]. Journal of Internet of Things,2018,2(03):71-81).

[18] 李旭东,牛玉坤,魏凌波，等.比特币隐私保护综述[J].密码学报,2019,6(02):133-149.(LI X D, NIU Y K, WEI L B, et al. COINS

privacy protection review [J]. Journal of password, 2019, 6 (02) : 133-149.).

[19] 张奥,白晓颖.区块链隐私保护研究与实践综述[J].软件学报,2020,31(05):1406-1434.(ZHANG A, BAI X Y. Block chain summarized research and practice of privacy protection [J]. Journal of software, 2020, 31 (5): 1406-1434).

[20] SAHAI S , SINGH N , DAYAMA P . Enabling Privacy and Traceability in Supply Chains using Blockchain and Zero Knowledge Proofs[C]// Proceedings of the 2020 International Conference on Blockchain. Piscataway: IEEE, 2020: 134-143.

[21] MAESA D, MARINO A , RICCI L. Uncovering the Bitcoin Blockchain: An Analysis of the Full Users Graph[C]// Proceedings of the 2016 International Conference on Data Science and Advanced Analytics. Piscataway: IEEE, 2016: 537-546

[22] REID F, HARRIGAN M. An Analysis of Anonymity in the Bitcoin System[C]//Proceedings of the 2011 International Conference on Social Computing Privacy, Security, Risk and Trust. Piscataway: IEEE, 2011: 1318-1326.

[23] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names [C]//Proceedings of the 2013 conference on Internet measurement conference. New York: ACM 2013: 127-140.

[24] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating User Privacy in Bitcoin[C]// Proceedings of the 2013 International Conference on Financial Cryptography and Data Security. Cham: Springer, 2013: 34–51.

[25] SHEN M, DUAN J, SHANG N, et al. Transaction Deanonymization in Large-Scale Bitcoin Systems via Propagation Pattern Analysis[C]//Proceedings of the 2020 International Conference on Security and Privacy in Digital Economy. Cham: Springer, 2020: 661–675.

[26] TENG L, JIA S X, LUO Y F, et al. Analyzing and De-Anonymizing Bitcoin Networks: An IP Matching Method with Clustering and Heuristics[J]. China Communications. 2022, 19(6): 263-278.

[27] 许重建,李险峰. 区块链交易数据隐私保护方法[J]. 计算机科学, 2020, 47(3): 281-286.(XU C J, LI X F. Data Privacy Protection Method of Block Chain Transaction[J]. Computer Science, 2020, 47(3): 281-286.

[28] Bitlaundry. Accessing bitlaundry. [EB/OL].(2011-5-19)[2021-7-21] http://bitlaundry.com/.

[29] Bitcoin Fog. Accessing bitcoin fog.[EB/OL].(2011-10-1) [2021-07-21]. http://bitcoinfog.info/

[30] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for Bitcoin with Accountable Mixes[C]// Proceedings of the 2014 International Conference on Financial Cryptography and Data Security. Cham: Springer, 2014: 486–504.

[31] VALENTA L , ROWAN B. Blindcoin: Blinded, Accountable Mixes for Bitcoin[C]// Proceedings of the 2015 International Conference on Financial Cryptography and Data Security. Cham: Springer, 2015: 112–126.

[32] GREGORY M. Coinjoin: Bitcoin privacy for the real world. [EB/OL] (2013-8-22) [2021-07-21]. http://bitcointalk.Org/index.php?topic=279249.0

[33] DUFFIELD E. Dash: A Payments-Focused Cryptocurrency.[EB/OL] (2018-8-23) [2021-7-21]. https://github.com/dashpay/dash/wiki/Whitepaper

[34] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin[C]// Proceedings of 2014 European Symposium on Research in Computer Security. Cham: Springer, 2014: 345–364.

[35] 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. Association for Computing Machinery, New York: ACM, 2015: 75–86.

[36] XIAO R Y, REN W, ZHU T, et al. A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain[J]. in IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 1793-1803.

[37] LU N, CHANG Y, SHI W，et al. CoinLayering: An Efficient Coin Mixing Scheme for Large Scale Bitcoin Transactions[J]. in IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 1974-1987.

[38] MIERS I, GARMAN C, GREEN MAND A, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin[C]//2013 IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2013: 397-411.

[39] SASSON E B, CHIESA A, GARMAN C. et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]//Proceedings of the 2014 International Conference on Security and Privacy. Piscataway: IEEE, 2014: 459-474.

[40] SABERHAGEN N V. CryptoNote v 2.0[EB/OL]. (2013) [2021-7-21].https://cryptonote.org/whitepaper.pdf.

[41] LIU Y, LIU X, TANG C, et al. Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin[J]. IEEE Access, 2018, 6: 23261-23270.

[42] MAXWELL G. Confidential transactions [EB/OL]. (2017-04-28) [2021-7-21]. https://elementsproject.org/features/confidential-transactions.

[43] WANG Q, BO Q, HU J K, et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems, 2020, 107: 793-804.

[44] CHEN, Y., MA, X., TANG, C, et al. PGC: Decentralized Confidential Payment System with Auditability[J]. European Symposium on Research in Computer Security, 2020, 12308: 591–610.

[45] LIU J W, WU M L, SUN R, et al. BMDS: A Blockchain-based Medical Data Sharing Scheme with Attribute-Based Searchable Encryption[C]//Proceedings of the 2021 International Conference on Communications. Piscataway: IEEE, 2021: 1-6.

[46] GUAN Z T, LU X, YANG W T, et al. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid[J]. Journal of Parallel and Distributed Computing, 2021, 147: 34-45.

[47] LI H, PEI L S, LIAO D, et al. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain[J]. IEEE Access, 2020, 8: 85190-85203.

[48] 王晨旭,程加成,桑新欣,等.区块链数据隐私保护：研究现状与展望[J].计算机研究与发展,2021,58(10):2099-2119.(WANG C X, CHE NG J C, SANG X X, et al. Data privacy protection in blockchai n: research status and prospect [J]. Journal of Computer Research and Development,2021,58(10):2099-2119.)

[49] CORRIGAN-GIBBS H, FORD B. Dissent: accountable anonymous group messaging[C]//Proceedings of the 17th ACM conference on Computer and communications security. New York: ACM, 2010: 340–350.

[50] IBRAHIM M H, ALI I A, IBRAHIM I I, et al. A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme.[C]// Proceedings of the 46th Midwest Symposium on Circuits and Systems. Piscataway: IEEE, 2003: 276-280.

[51] BLUM M, FELDMAN P, AND MICALI S. Non-interactive zero-knowledge and its applications[C]// Proceedings of the 20th annual ACM symposium on Theory of computing Association for Computing Machinery, Piscataway: IEEE. 1988: 103–112.

[52] CAMENISCH J , LYSYANSKAYA A . Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials[C]// Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology Cham: Springer, 2002: 61–76.

[53] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of cryptology, 1991, 4(3): 161-174.

[54] BEN-SASSON E, CHIESA A, GENKIN D, et al. (2013) SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge[C]// Proceedings of the 33nd Annual International Cryptology Conference on Advances in Cryptology . Cham: Springer, 2013: 90–108.

[55] RIVEST R L, SHAMIR A, TAUMAN Y. How to Leak a Secret: Theory and Applications of Ring Signatures [J]. Theoretical Computer Science, 2006, 3895: 164–186.

[56] RIVEST R L, ADLEMAN L M, DERTOUZOS M L . On Data Banks and Privacy Homomorphisms [J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

[57] 杨亚涛,赵阳,张卷美,等.同态密码理论与应用进展[J].电子与信息学报,2021,43(02):475-487. (YANG Y T, ZHAO Y, ZHANG Z M, et al. Advances in homomorphic cryptography theory and Applications [J]. Journal of Electronics and Information Technology, 201, 43(02): 475-487).

[58] BACK A. Bitcoins with homomorphic value (validatable but encrypted)[EB/OL]. (2013-10-1) [2021-07-21]. https://bitcointalk.org/index.php?topic=305791.0.

[59] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]// Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology. Berlin: springer, 1991: 129-140.

[60] MAXWELL G, POELSTRA A. Borromean Ring Signatures[EB/OL]. (2015-06) [2021-07-21]. https://raw.githubusercontent.com/Blockstream/borromean_paper/master/borromean_draft_0.01_34241bb.pdf

[61] PAILLIER P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[C]// Proceedings of the 1999 International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer, 1999: 223–238.

[62] FUJISAKI E, OKAMOTO T. Statistical Zero-Knowledge Protocols to Prove Modular Polynomial Relations [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1997, E82-A(1): 81-92.

[63] 伍前红,张键红,王育民.简单证明一个承诺值在特定区间内[J].电子学报,2004(07):1071-1073.(WU Q H, ZHANG J H, WANG Y M. Simple Proof of a Promise Value in a Specific Interval [J]. Acta Electronica Sinica, 2004(07): 1071-1073).

[64] SONG X D D, WAGNER D , PERRIG A. Practical techniques for searches on encrypted data[C]// Proceedings of the 2000 International Conference on Security and Privacy. Piscataway: IEEE, 2000:44-55.

[65] 李经纬,贾春福,刘哲理,等.可搜索加密技术研究综述[J].软件学报,2015,26(01): 109-128. (LI J WEI, JIA C F, LIU S W, et al. Searchable encryption technology research review [J]. Journal of software, 2015, 26 (01): 109-128.)

[66] 王生玉,汪金苗,董清风,朱瑞瑾.基于属性加密技术研究综述[J].信息网络安全,2019(09):76-80.(WANG S Y, WANG J M, DONG Q F, et al. Overview of Research on Attribute-Based Encryption Technology [J]. Information Network Security, 2019(09): 76-80.)

[67] 赵志远,王建华,朱智强,等,.云存储环境下属性基加密综述[J].计算机应用研究,2018,35(04):961-968,973. (ZHAO Z Y, WANG J H, ZHU Z Q, et al. Application Research of Computers, 2018, 35(04): 961-968,973).

[68] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//Proceedings of the 2011 International Workshop on Public Key Cryptography. Cham: Springer, 2011: 53-70.

[69] BEIMEL A: Secure Schemes for Secret Sharing and Key Distribution[D]. Haifa: Israel Institute of Technology, 1996: 59-90.

[70] 王俊生,李丽丽, 颜拥,等. 区块链技术应用的安全与监管问题[J]. 计算机科学, 2018, 45(6A): 352-355.(WANG J S, LI L L, YAN Y, et al. Security Incidents and Solutions of Blockchain Technology Application[J]. Computer Science, 2018, 45(6A): 352-355).

[71] LI Y N, YANG G M, SUSILO W, et al, Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability[J]. in IEEE Transactions on Dependable and Secure Computing, 2019, 18(2): 679-691.

[72] SUN S F., AU M H, LIU J K, et al. RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero[C]//Proceedings of the 2017 European Symposium on Research in Computer Security. Cham: Springer, 2017: 456–474.

[73] LIN C, HE D B, HUANG X Y, et al. DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain[J]. in IEEE Transactions on Information Forensics and Security, 2020, 15: 2440-2452.

[74] EUN H, LEE H AND OH H. Conditional privacy preserving security protocol for NFC applications[J]. in IEEE Transactions on Consumer Electronics, 2013, 59(1): 153-160.

[75] CHASE M, LYSYANSKAYA A. On signatures of knowledge[C]// Proceedings of the 26th Annual International Cryptology Conference on Advances in Cryptology . Cham: Springer, 2006: 78-96.

[76] ANDROULAKI, E, CAMENISCH J, CARO A D, et al. Privacy-preserving auditable token payments in a permissioned blockchain system[C]//Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery. New York: ACM, 2020: 255–267..

[77] POINTCHEVAL D, SANDERS O. Short Randomizable Signatures[C]// Proceedings of the 2016. Conference on Cryptographers' Track at the RSA Cham: Springer, 2016: 111–126.

[78] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems[J]. Journal of Cryptology, 2007, 20: 51–83.

[79] SHAO W, JIA C F, XU Y K, et al. AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain[J]. Computers & Security, 2020, 99:102069.

[80] EL KAAFARANI A, GHADAFI E, KHADER D. Decentralized Traceable Attribute-Based Signatures[C]//Proceedings of the 2014 Conference on Cryptographers' Track at the RSA.. Cham: Springer, 2014: 327–348.

[81] GHADAFI E. Efficient Distributed Tag-Based Encryption and Its Application to Group Signatures with Efficient Distributed Traceability[C]//Proceedings of the 2014 International Conference on Cryptology and Information Security in Latin America. Cham: Springer, 2014: 327-347.

[82] BARKI A, GOUGET A. Achieving privacy and accountability in traceable digital currency[J]. Cryptology ePrint Archive, 2020.

[83] BALDIMTSI F AND LYSYANSKAYA A. 2013. Anonymous credentials light[C]// Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. New York: ACM , 2013:1087–1098.

[84] YUEN T H. PAChain: private, authenticated & auditable consortium blockchain and its implementation[J]. Future Generation Computer Systems, 2020, 112: 913-929.

[85] AU M H, SUSILO W, MU Y. Constant-size dynamic k-TAA[C]//Proceedings of the 2006 International conference on security and cryptography for networks. Cham: Springer, 2006: 111-125.

[86] CAMENISCH J, CHAABOUNI R. Efficient protocols for set membership and range proofs[C]//Proceedings of the 2008 International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2008: 234-252.

[87] LIN C, HE D, HUANG X, et al. PPChain: A privacy-preserving permissioned blockchain architecture for cryptocurrency and other regulated applications[J]. IEEE Systems Journal, 2021, 15(3): 4367-4378.
[88] ISLAM S K H, KHAN M K, AL-KHOURI A M. Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing[J]. Security and communication networks, 2015, 8(13): 2214-2231.
[89] HO T H, YEN L H, TSENG C C. Simple-yet-efficient construction and revocation of group signatures[J]. International Journal of Foundations of Computer Science, 2015, 26(5): 611-624.
[90] RIVINIUS M, REISERT P, RAUSCH D, et al. Publicly Accountable Robust Multi-Party Computation.[C]//Proceedings of the 2022 Symposium on Security and Privacy. Piscataway: IEEE, 2022: 2430-2449.
[91] 曹雪莲,张建辉,刘波.区块链安全、隐私与性能问题研究综述[J].计算机集成制造系统,2021,27(07) 2078-2094:.(CAO X L, ZHANG J H, LIU B. Block chain security, privacy, and performance issues research review [J]. Journal of computer integrated manufacturing system, 2021, 27(7): 2078-2094.)
[92] SAHA S., MALLICK S. & NEOGY S. Privacy-Preserving Healthcare Data Modeling Based on Sensitivity and Utility[J]. SN Computer Science, 2022, 3(482)：1–13.
[93] MASHAHDI S, BAGHERPOUR B. & ZAGHIAN A. A non-interactive (*t*,*n*)-publicly verifiable multi-secret sharing scheme[J]. Designs, Codes and Cryptography, 2022, 90: 1761–1782.
[94] VEUGEN T. Secure Multi-party Computation and Its Applications[C]// Proceedings of the 2022 International Conference on Innovations for Community Services. Cham: Springer, 2022: 3–5.
[95] 孙浩，毛瀚宇，张岩峰,等.区块链跨链技术发展及应用[J]. 计算机科学, 2022, 49(5): 287-295.(SUN H, MAO H Y, ZHANG Y F, et al. Development and Application of Blockchain Cross-chain Technology[J]. Computer Science, 2022, 49(5): 287-295.
[96] PEREZ A J, ZEADALLY S. Secure and privacy-preserving crowdsensing using smart contracts[J]. Computer Science Review, 2022, 43: 100450..
[97] HOANG T T, DURAN C, SERRANO R, et al. Trusted Execution Environment Hardware by Isolated Heterogeneous Architecture for Key Scheduling[J]. IEEE Access, 2022, 10: 46014-46027.
[98] SHENG G, QIAN Q S, RUI Z . A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain[J]. Security and Communication Networks, 2021, 2021: 10.

This work is partially supported by National Natural Science Foundation of China(NO.62002139), National Natural Science Foundation of General Program of China(NO.62272203), Natural Science Fundation of Jiangsu Province(NO.BK20200886), China Postdoctoral Science Foundation(NO.2019M651738).

XIE Qingqing, born in 1990, Ph. D, lecture. Her research interests include blockchain supervison, applied cryptography.
YANG Nianmin, born in 1998, M. S. candidate. His research interests include blockchain supervison, digital currency.
FENG Xia, born in 1983, Ph.D., associate professor , Her research interests include internet of things, authentication protocols, blockchain, and applied cryptography.