区块链密码学隐私保护技术综述

刘峰[1,2]，杨杰[2]，齐佳音[2]
（1. 华东师范大学计算机科学与技术学院，上海 200062；
2. 上海对外经贸大学人工智能与变革管理研究院，上海 200336）

摘　要：近年来，数据隐私问题日益明显，如何在区块链中实现有效的隐私保护是研究热点。针对区块链在隐私保护上的研究现状与发展态势，阐述了区块链在交易地址、预言机以及智能合约上的隐私保护方法，归纳出区块链在基本要素防护上的隐私策略。基于国内外高水平文献梳理分析了特殊密码学原语、后量子密码学两类区块链密码学防护方法及使用场景，综述其研究思路，并给出属性基加密、特殊数据签名、同态加密、安全多方计算、零知识证明、格密码等适用于区块链隐私保护的密码学技术的优缺点，得出区块链应用的隐私防护离不开密码学技术支持的结论。针对区块链隐私保护技术，从基本要素防护和密码学防护两个方面进行了分析，总结出仅从区块链的应用层、合约层出发难以有效解决隐私问题，还需要利用各类密码学技术根据需求和应用场景的不同进行优势互补。根据区块链隐私加密技术发展现状，从区块链基本要素防护和基于密码学的防护展开叙述。从内生性基本要素安全和外生性密码学隐私安全两个角度出发，先研究基本要素隐私防护，再深入分析区块链隐私密码学防护技术。在对应防护措施中以技术联合实际应用发展，考虑技术时效性的同时，衡量其隐私处理方面的优劣势以及潜在价值。展望了未来区块链隐私保护技术的发展方向，说明了需要重点解决的问题。

关键词：区块链；隐私保护；密码学原语；现代密码学；后量子密码学
中图分类号：TP311
文献标志码：A
DOI: 10.11959/j.issn.2096−109x.2022054

Survey on blockchain privacy protection techniques in cryptography

LIU Feng[1,2], YANG Jie[2], QI Jiayin[2]
1. School of Computer Science and Technology, East China Normal University, Shanghai 200062, China
2. Institute of Artificial Intelligence and Change Management, Shanghai University of International Business and Economics, Shanghai 200336, China

Abstract: In recent years, the issue of data privacy has attracted increased attention, and how to achieve effective privacy protection in blockchain is a new research hotspot. In view of the current research status and development trend of blockchain in privacy protection, the privacy protection methods of blockchain in transaction address,

收稿日期：2021−03−16；**修回日期：**2021−06−10
通信作者：齐佳音，qijiayin@139.com
基金项目：国家自然科学基金（72042004）
Foundation Item: The National Natural Science Foundation of China (72042004)

引用格式：刘峰, 杨杰, 齐佳音, 等. 区块链密码学隐私保护技术综述[J]. 网络与信息安全学报, 2022, 8(3): 29-44.
Citation Format: LIU F, YANG J, QI J Y, et al. Survey on blockchain privacy protection techniques in cryptography[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 29-44.

prophecy machine and smart contract were explained, and the privacy strategies of blockchain in the protection of basic elements were summarized. Based on high-level literature at home and abroad, two types of blockchain cryptographic protection methods and usage scenarios were analyzed, including special cryptographic primitives and post-quantum cryptography. The advantages and disadvantages of seven cryptographic techniques applicable to current blockchain privacy protection were also reviewed, including attribute-based encryption, special data signature, homomorphic encryption, secure multi-party computation, zero-knowledge proofs, and lattice ciphers. It was concluded that the privacy protection of blockchain applications cannot be achieved without cryptographic technology. Meanwhile, the blockchain privacy protection technologies were analyzed in terms of both basic element protection and cryptographic protection. It was concluded that it was difficult to effectively solve the privacy problem only from the application and contract layers of the blockchain, and various cryptographic technologies should be used to complement each other according to different needs and application scenarios. In addition, according to the current development status of blockchain privacy cryptography, the narrative was developed from blockchain basic element protection and cryptography-based protection. From the perspectives of both endogenous basic element security and exogenous cryptographic privacy security, basic element privacy protection should be studied first, followed by an in-depth analysis of cryptographic protection techniques for blockchain privacy. The strengths and weaknesses and the potential value of the privacy handling aspects of the corresponding safeguards should be measured in terms of the development of technology in conjunction with practical applications, while considering the timeliness of the technology. Finally, an outlook on the future direction of blockchain privacy protection technologies was provided, indicating the issues that need to be addressed in focus.

Keywords: blockchain, privacy protection, cryptographic primitives, modern cryptography, post-quantum cryptography

0 引言

随着信息化时代分布式网络架构的快速兴起，区块链这一分布式账本技术凭借着可追溯、公开透明等特性备受瞩目。基于区块链技术的点对点可信交易机制受到越来越多用户的青睐，然而随着个人隐私数据保护意识的觉醒，大众及组织机构对现有区块链数据的弱隐私性愈感不安。以比特币为例，虽凭借交易费用低、易于流通等特点立足于当前的金融社会体系，但随着用户数量的持续性增长，其信息隐私问题逐渐凸显。绝大多数用户并不希望敏感信息在区块链中被公示，因为不受限制的信息暴露易带来安全隐患，造成潜在隐私危险。Lischke 等[1]尝试对比特币进行信息地址的匿名，提出用 Tor 网络对比特币的真实交易地址进行防追踪处理，但隐私性、安全性能仍不完善。Neudecker 等[2]通过对比聚类的区块链信息与泛洪比特币网络过程中提取的 IP 地址，得出了小部分聚类的区块链信息地址与 IP 地址有明显的关联，可以借此 IP 地址找出用户敏感信息。Goldfeder 等[3]表明，比特币交易中交易接收方可以轻松将比特币的支付流通信息与用户 Cookies 相关联，从而去除比特币交易的匿名性，迫使其暴露出用户的真实身份。

此外，区块链网络中一些影响较大的恶意攻击事件的频频爆出，增加了用户对身份信息与财产信息遭受泄露的担忧度。2019 年 1 月，Ethereum Classic（ETC）遭受了 51%攻击，使某些交易所损失了大量资金。这种攻击在完全被执行前无法被检测，在攻击发生后造成不少 ETC 持有者的恐慌[4]。2020 年，比特币硬件钱包制造商 Ledger 的 27 万用户数据信息被盗，数万人姓名、地址信息等敏感数据被泄露至互联网，对个人身份信息造成了极大危害。若无法有效提升区块链的隐私安全保护能力而让此类安全事件频发，那么以区块链驱动数字文明的进展将会受到明显制约。很多原本可以用于科学研究和商业应用的数据将无法上链被公开披露或者被迫中断，进而产生数据孤岛效应，导致优良商业模式与科学研究无法持续推进。因此，区块链的隐私数据保护成为分布式网络生态安全的核心问题之一，隐私加密技术的理论研究与实际应用扩展刻不容缓。

由于针对当前区块链隐私方面存在的匿名性

差、安全性能低等问题的研究较为零散，同时用户对隐私数据防护的迫切需求日益明显，梳理分析区块链隐私防护方法将有助于区块链隐私研究的进一步发展。本文根据区块链隐私加密技术发展现状，从区块链基本要素防护和基于密码学的防护展开叙述。如图 1 所示，主要从内生性基本要素安全和外生性密码学隐私安全两个角度出发，首先研究基本要素隐私防护，再深入分析区块链隐私的密码学防护。本文在对应防护措施中以技术联合实际应用发展，考虑技术时效性的同时，衡量其隐私处理方面的优劣势以及潜在价值。

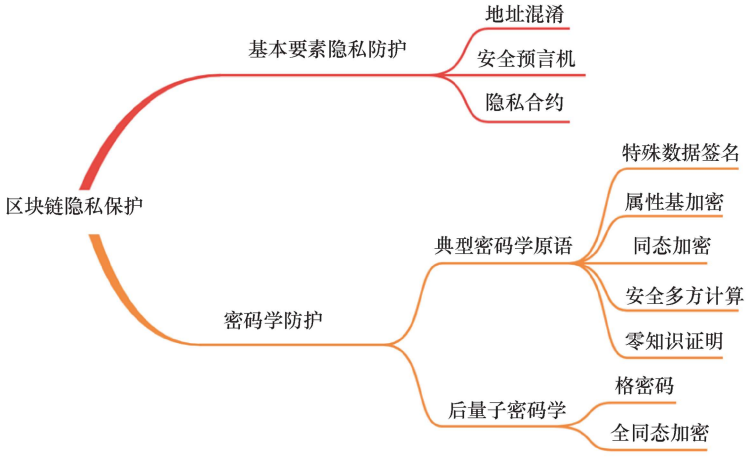

图 1　区块链隐私保护技术脉络示意
Figure 1　The pulse of blockchain privacy encryption technology

1　区块链基本要素防护

区块链基本要素的隐私安全，通常会从交易地址、链上与链下数据交互的接口以及智能合约 3 个方面进行考虑。从隐私视角率先切入与区块链应用设计安全密切相关的基本内容，有助于理解区块链隐私加密技术方式。

1.1　地址混淆

地址混淆技术在交易地址隐私保护中应用最为广泛，它是指将进行交易的地址加密重组，使混淆处理过后的地址无法被判别直接源头，从而实现交易隐私的目的。地址混淆在区块链中主要分为两类：一类是一次性交易地址，另一类是混币技术。

（1）一次性交易地址

在区块链中持续使用同一个交易地址会使交易和用户身份容易被追踪，最直接的解决方法是在进行不同交易时使用不同的交易地址，给追踪和分析增加难度。

一般而言，区块链允许用户便捷地生成不同的交易地址。单笔交易中，付款方可以生成并公开一个交易地址，利用该地址与收款方发生交易行为，从而降低被追踪的风险[5]。然而，通过交易图形分析[6]技术仍可以有效判别交易者身份。另外，一次性交易地址每次都需产生新地址进行交易，在交易场景中不断切换新地址反而会影响用户体验、降低交易效率。为了消除这种弊端，隐身地址应运而生。

隐身地址流程如图 2 所示，为了不暴露自己的交易地址，收款方把正常交易中使用的公钥进行隐藏，然后发送隐身地址公钥给付款方。付款方则利用该隐身地址和一个随机数进行非对称加密，生成一个临时存放交易资金的一次性收款地址。然后，收款方可借助隐身地址私钥对该一次性收款地址进行解密，获取可以转出该笔资金的付款私钥。

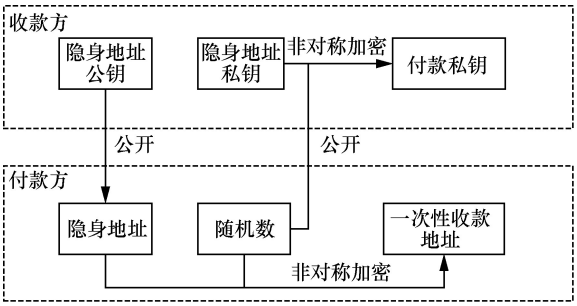

图 2　隐身地址流程
Figure 2　Flow for stealth address

在进行交易的过程中，虽然一次性收款地址是由付款方生成的，但依据非对称加密算法，对交易资金拥有使用权的，只有可以解密转出资金私钥的收款方。相对于“一次一密”的交易方式，隐身地址并不要求付款方每笔交易都生成新的一次性收款地址，这在一定程度上提高了效率的同时保护了收款方的隐私。一般地，隐身地址与环签名等密码学技术相结合，以提供更好的隐私性。

（2）混币技术

混币技术是指将多个不相关输入进行混合后再输出，使外界无法分辨出数字货币的流向[7]。一般地，混币主要利用混淆器实现地址隐私保护，在混淆服务通证池中将若干用户的交易通证进行混淆处理后，输出给匿名交易地址，从而减少敌手窃取资金的可能性。然而，借助混淆器进行地址隐藏来间接保护交易隐私的方式效果甚微，存在不少弊端。早期中心化混币服务的部署方式，典型如 Mixcoin 协议[8]，虽然具备可审计性，但混淆服务器仍掌握着交易地址的关联信息，对用户隐私威胁较大。研究表明即使经过多轮混淆处理，如果交易支付的 Cookie 不及时清除，仍然可以通过技术手段辨别出用户的钱包再窃取其敏感信息[3]。TumbleBit 是 2017 年提出的一种能够兼容比特币的新型中心化混币协议，相对于 Mixcoin，TumbleBit 以简洁的密码学原语在保证混币隐私时减少了与敏感数据进行交互的次数，扩展了交易量[9-10]。该混币方案主要分为资金托管、链下支付、链上提现 3 个阶段，交易安全方面的防护主要在链下支付阶段，使用了 RSA-Puzzle-Solver 协议进行签名加密与密钥隐藏。虽在此过程中增加了资金安全、提速了交易[11]，却依旧无法解决单点攻击产生的隐私风险。

近些年，为进一步改进中心化混币协议，BlindCoin[12]利用盲签名对隐私泄露进行防范，同时降低了交易的时间开销。此外，为解决中心化混币技术的信任问题，涌现出 CoinParty[13]、Xim[14]等分布式混币技术。然而，这些技术并不完美，在计算开销、通信复杂度以及交易隐私性等问题上仍留有缺口，对比如表 1 所示。此外，一些反匿名攻击将用户身份的解密转变为对其行为的聚类分析[15-16]，不仅包括网络流量的 IP 地址聚类[1-2]，还包括交易数据的地址聚类[17]、交易行为的启发式模型学习[18]，这对混币技术的隐私安全造成了巨大的威胁。在实际应用的部署方面，混币技术应经过精细的审查与功能测试，融合密码学算法增强安全性，尽可能规避此类恶意隐私攻击。

1.2 预言机隐私处理

关于链上链下数据交互接口的隐私保护，首要考虑区块链预言机的隐私处理。预言机是智能合约连接链下数据和系统的数字化代理，能够将区块链与外部世界进行链接。在基础要素防护方面，隐私预言机的设计是区块链隐私保护的战略枢纽。

尽管在应用方面，区块链预言机项目的实施已经屡见不鲜，然而像 Chainlink、Oraclize 等预言机网络仍然只能基于各自机制为区块链提供一些基本公开信息，如价格、交易量等，在信息隐私

表 1 混币技术对比

Table 1 The comparison of token confusion technologies

类别	混币机制	性能开销	主要隐私安全问题及风险
中心化混币	Mixcoin	交易时延高	混币服务商掌握用户隐私
	BlindCoin	计算开销与存储开销大	混币服务商掌握用户隐私
	TumbleBit	交易时延与交易费用高	易遭受中继节点窃取个人隐私
去中心化混币	CoinJoin	交易时延随参与用户增加而增加	混币服务商掌握用户隐私
	CoinShuffle	交易时延随参与用户增加而增加	易遭受分布式拒绝服务攻击
	CoinParty	交易时延随参与用户增加而增加	未经认证的恶意用户易盗取他人资产
	Xim	混币时间长且混币轮换次数多	混币期间易遭受攻击和盗窃

脱敏处理上很难满足真实商业需求。在学术研究方面，康奈尔大学提出了隐私预言机协议 DECO[19]，该协议扩展了 HTTP/TLS 协议的数据安全功能，保障了各类隐私和付费数据源传输数据时的隐私性和不易篡改性。DECO 协议工作流程如图 3 所示。

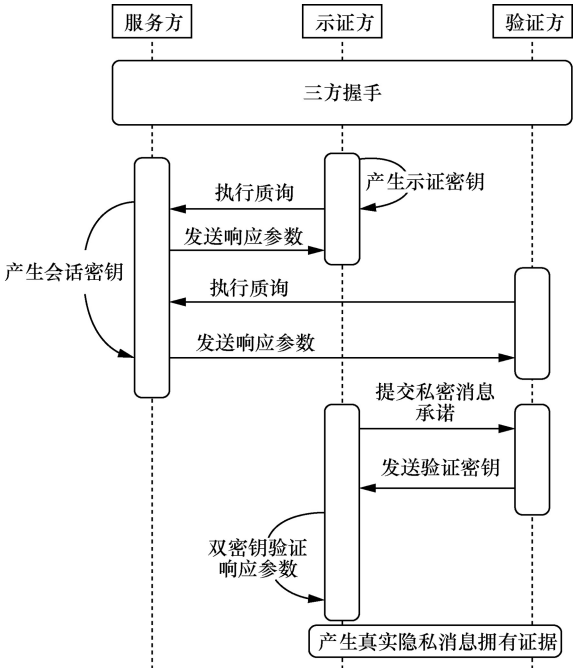

图 3　DECO 协议工作流程

Figure 3　The workflow of DECO protocol

从图 3 的工作流程可以看出，DECO 在使用 HTTP/TLS 协议的服务器中实现了传输层安全（TLS，transport layer security）的短时间握手和零知识性，使数据在建立握手连接过程中不会被轻易泄露。DECO 协议通过提交私密消息承诺给验证方，使即使是最终使用数据的计算机也无法查看数据内容，借助预言机在无须公示私密信息的情况下可进行脱链验证。除此之外，随着 Polkadot[20]跨链技术兴起，隐私预言机网络 ZK Oracle 结合 SERO[21]隐私技术，创建出可扩展的区块链 Layer2 层进行隐私数据处理，以保障数据在链上链下的通信隐私安全。

客观来看，预言机在隐私方面研究正不断向前推进，并且更多地倾向于去中心化预言机可扩展运算中的隐私。此种态势下，可信执行环境（TEE，trusted execution environment）可以发挥一定作用，如借助机器学习相关软件在 TEE 内进行大量复杂运算保障区块链预言机隐私安全。再者，需要考虑数据交互、通信过程中的安全，如利用 DECO 协议获取区块链相关应用的 Web 数据，在传输过程中保障隐私。此外，预言机交互合约上的隐私应进行一些安全治理。

1.3　智能合约安全治理

智能合约是区块链 2.0 时代基本要素的重要组成部分，是解决区块链信任问题的突破性技术之一。合约具备图灵完备的编程语言，能够扩充区块链的使用场景和功能。随着区块链应用的不断开发，各式各样的智能合约在不断增多，对合约隐私安全的治理显得尤为重要。

在诸多合约隐私研究中，有支持预言机特殊形式的隐私智能合约 Mixcles[22]，通过结合通证混淆技术为以太坊提供隐私保障。也有针对以太坊智能合约设计的隐私协议 Zether，作为 ElGamal 公钥账户之间传输的载体，支持匿名的智能合约交互[23]。此外，共识计算成本高，可被委托链外的隐私计算能力受人青睐。例如，Ekiden 隐私计算平台将计算与共识进行分离，利用 Intel SGX 处理器[24]在链下委托计算合约隐私数据，再向区块链提供数据形式的确切证明。类似地，还有 Enigma[25]隐私模型，为支持去中心化应用开发，利用特殊合约处理隐私数据，使公开数据处理在链上执行，隐私数据处理在链下执行。为了提升区块链性能吞吐量并实现细粒度的隐私保护，双链形式下包含合约级别的联盟链隐私架构[26]是现阶段可行的隐私保护方式之一。总体来说，虽然合约隐私技术在不断突破，并且隐私研究与应用越来越受到关注，但合约上隐私安全问题的要因还需要注意以下几点。

1) 缺少审查。合约逻辑的审计是必不可少的，规范化合约能够助推合约的法理性研究，如考虑匿名性检测[27]、隐私威胁预警[28]、脆弱性检测[29-30]、漏洞挖掘[31-32]等。

2) 缺乏形式化证明[33-34]。大多数智能合约在编写之初并没有考虑过形式化验证，当部署在某一区块地址后，因为不能修改，如果存在 BUG，会很容易被黑客利用进行恶意攻击，造成不可弥补的经济损失[35]。

3) 智能合约编程语言内生性安全问题。早些年合约常用语言 Solidity 因为空指针等逻辑设计缺

陷饱受诟病。另外，相关的开发者社区并不健全，需要多方努力对合约编程语言进行分析测试。

关注基于智能合约的隐私计算技术将有助于建立社会化数据闭环，真正打消数据价值链不同环节对数据归属、数据安全和隐私保护的顾虑，但仍然有不小的鸿沟需要结合数理逻辑较强的技术进行跨越。

整合区块链基本要素隐私方法，不难看出实现真正意义的区块链隐私保护仍然需要防范很多风险。读写限制、一次性交易地址等解决方法虽然相对简单且具备低风险，但都有各自非常明显的局限性。若只从区块链基本要素应用上考虑隐私防护，始终不能有效解决区块链隐私安全问题。面对这种局面，越来越多的研究者以及产业界人士开始关切可以精确评估数据隐私性的密码学知识。这类科学技术能够与区块链接洽得当，为防范隐私泄露这一技术难题带来新的契机。

2 基于典型密码学原语的隐私保护技术

有别于操作系统原语，密码学原语如签名、密钥交换等，主要侧重在解决问题的动机上。区块链本质上是一个基于密码学的技术，使用的密码学原语比较广泛，包括椭圆曲线签名 ECDSA、安全哈希等。本节归类面向区块链的具备隐私效应的典型密码学原语，分析它们各自的特点以及使用场景，并给出客观评价。

2.1 特殊数字签名隐私性简述与分析

一般而言，区块链上交易信息是通过签名标定交易发起方的身份，然后由区块链通过特定规则验证签名以确保交易信息的正确性，这一切得益于签名的不易篡改和校验性。区块链主流平台，RSA、ECDSA 等交易签名方式已被普遍使用，但这些签名隐私保护效果不是十分理想，存在参与方身份信息隐匿性弱、多方签名消息保密性差等弊端。在一些区块链新兴应用场景中，能够实现身份匿名、交易内容隐藏等特殊隐私保护的聚合式数字签名技术极具价值。

（1）群签名

在需要监管方参与的多方协作场景中，群签名技术适得其所。群签名首先由群管理者建立群资源，然后向外界隐蔽群成员身份的隐私信息，让群成员在群组内进行签名。签名完成后只有群公钥被公开，交由区块链上验证节点或者逻辑合约进行验证。整个过程中，群管理者可以利用群私钥对群成员生成的群签名进行追踪以实现监管目的。

因为签名过程中只有群管理者掌握单个群成员隐私信息，所以在使用过程中需要对群管理者的私钥集合进行加密保护，否则即使实现了有效监管，如果隐私数据得不到保护，也无法在群成员之间建议信任关系。该签名方案在区块链上隐私局限性在于对群管理者是否构建了较强信任关系。

（2）环签名

环签名是一种特殊的群签名[36-37]，无群管理者且不需要可信中心。基于区块链技术的环签名逻辑示意如图 4 所示。

从图 4 中可以看出，环签名会为一组交易成员提供各自的对外公钥，使区块链公开数据只能追踪到交易成员所在组，无法解析出个人信息。

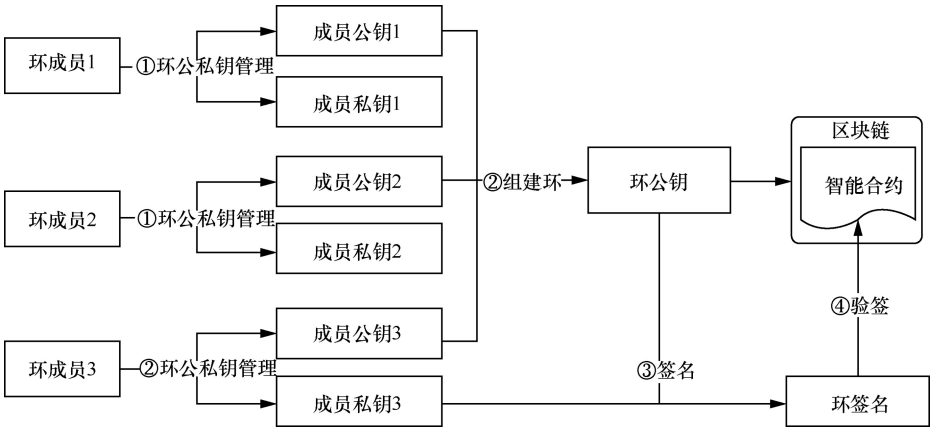

图 4 基于区块链技术的环签名逻辑示意

Figure 4 Blockchain technology based ring signature logic schematic

这种无条件的匿名性与不可伪造性，为区块链签名时的数据隐私提供了极大便利。对于无条件匿名，敌手即使窃取了成员私钥，能确定成员真实身份的概率不会超过 $1/N$（N 为环组成员数）；对于不可伪造性，外部攻击在对成员私钥不知情时，即使能窃取交易消息的签名，伪造签名的概率也可忽略不计。区块链上第一个应用环签名技术进行隐私匿名的是 CryptoNote 协议[5]，典型如门罗币（Monero），使用环签名机制实现交易发送方和交易信息的匿名性。

然而，环签名机制在交易使用的关联性上仍留有隐私问题。在 2017 年 2 月门罗币代码被修改前，Möser 等[18]曾通过分析门罗币用户的使用习惯，对环匿名交易进行可追踪分析，找出了部分用户的真实地址。此外，在环签名隐私技术演变过程中，为防止区块链伪造币产生的同时避免交易金额留存非法，有学者提出 Borromean[38]环签名方案，对交易的输出金额进行范围证明以便加强交易隐私性，但其证明大小与范围区间的上限呈线性关系，影响了区块链的整体效率。总而言之，环签名、群签名为主的技术适用于无监管或弱监管的匿名自治组织身份保密上，在大规模应用时应关注其合法性。

（3）盲签名

盲签名[39]是数字签名的变种，主要借助盲因子对签名数据进行盲化签名，验证时则需利用盲化因子进行解盲实现隐私交易。其实现消息隐私的泛化公式如下：

$$\mathrm{sign}_m = \mathrm{Blind}(m, b_r) \tag{1}$$

给定消息 m，有随机生成的盲化因子 b_r，经盲函数 Blind 后生成加密签名消息 sign_m 对此签名消息利用私钥 $\mathrm{pr_{key}}$ 进行签名，如式(2)所示。

$$\mathrm{sign}_b = \mathrm{sign}(\mathrm{sign}_m, \mathrm{pr_{key}}) \tag{2}$$

解盲时，需再次借助盲化因子 b_r 在解盲函数 UnBlind 进行反解，如式(3)所示。

$$\mathrm{sign}' = \mathrm{UnBlind}(\mathrm{sign}_b, b_r) \tag{3}$$

对于发送至区块链的签名消息 sign_b，敌手难以通过盲化的签名消息反推出明文。只有合法验签者对原签名进行解盲后，才能使用公钥验证消息，判断签名合法性。盲签名凭借盲化性与不可追踪性在区块链上有很多应用，如通过盲签名解决微型支付通道中隐私问题[40]，构建盲签合约解决链上与链下交易通信的不信任问题与安全问题[41]。然而，频繁的盲化会造成签名请求滥用[42]，往往需要引入可信的第三方进行验证以构建公正的盲签名方案。

（4）聚合签名

随着区块链多方签名交易需求越来越多，低效单一签名的方式已经不能满足多数用户参与的应用场景，且签名过程中如何有效处理隐私也是亟须考虑的问题。在此现状下，能够对多方签名消息进行合并签署的聚合签名逐步占据优势，典型如 Schnorr 签名与 BLS 签名聚合方案。

Schnorr[43]签名是一种能够聚合签名并对单一签名进行验签的签名技术，构造如下：

$$S_i = r + kH(m \mid R \mid P), i \in \{1, 2, \cdots, n\} \tag{4}$$

其中，r 为盲因子，k 为加密私钥，R 为公钥，m 为需要签名的消息。首先对 n 个签名进行合并签署，生成聚合签名 S 后将签名对 (S, R) 发送至验签者，如式(5)所示。

$$S = S_1 + S_2 + \cdots + S_n \tag{5}$$

通过核验签名对 (S, R) 是否合法即可证明签名消息是否正确。

$$SG = R + PH \tag{6}$$

其中，G 为椭圆曲线上一点。从式(6)可以看出，验证者只需利用聚合公钥及合并的签名消息即可判断签名的有效性。聚合签名的参与方无须提供与自己直接相关的公钥给验证者，这就使在减少用户隐私泄露的同时提高了签名的效率。常见的如基于 Schnorr 签名的 MuSig 协议，在隐私上保证参与方私钥隐藏，将多方的签名、公钥分别聚合后发送至单一参与方进行合并签名，并消除了流氓密钥攻击的威胁。然而，签名过程中需要各参与方进行多轮信息交互，且聚合签名时间并不可控[44]。2020 年，Nick 等[45]对 MuSig 再次进行改进，使其减少了一次签名轮数且无须参与方间进行零知识证明（ZKP，zero-knowledge proof）即可确保隐私安全性。在多方参与的场景中，Schnorr 聚合签名的同态特性可以很好地调动参与方互相协作的积极性，以实现互利共赢。

BLS 签名[46]则是另一种在区块链隐私上可实现签名聚合和密钥聚合的算法，无须额外通信即

可对不同签名消息进行合并签署，同时能避免使用随机数生成器，降低额外开销。BLS 签名通过 n 个签名进行聚合生成签名 S，验签时需利用各自公钥 $P_i, i \in \{1,2,\cdots,n\}$ 与签名消息进行对比，参照公式如下：

$$E(G,S)=E\left(P_1,H(m_1)\right)\cdots E\left(P_n,H(m_n)\right) \quad (7)$$

虽然 BLS 签名不需要随机数即可完成签名认证，但其过分依赖双线性映射，导致计算使用的配对函数并不高效，在验签时间效率上反而不如 Schnorr。此外，复杂配对函数要求选择线性配对友好的椭圆曲线，以防 MOV 攻击[47]。有关 BLS 签名的研究在持续推进，Boneh 等[48]在 2018 年对此签名方式进行二次更新，在保留原有隐私性上减少了占用比特币区块链的空间。未来仍可以在 BLS 签名使用的配对函数、映射方式上寻找改进方向，以便 BLS 签名能够进一步适用于多方协作的区块链产业链中。

为了辨析具备隐私性的特殊数据签名的优劣势，更为直观的比较如表 2 所示。

表 2 特殊数字签名隐私性能

Table 2 Special digital signature privacy features

对比内容	参与方隐私性	签名消息隐私性	地址隐私性
环签名	基于环密钥分发中心	基于环状签名结构	隐私性强
盲签名	盲化消息者隐私性强	基于盲化函数与因子	盲化消息者隐私性强
Schnorr 签名	签名时隐私性差	基于离散对数难解	签名后隐私性强
BLS 签名	签名时隐私性差	基于离散对数难解	签名后隐私性强

此类特殊数字签名在区块链隐私保护上的侧重点各不相同，使用时需要综合考虑场景进行隐私应用。除此之外，门限签名如门限 ECDSA[49-50]、Shamir 门限签名[51]等新型多方参与的签名方案，在改善交易性能的同时，通过签名聚合、密钥聚合等方式拔高了交易隐私性。然而单一签名技术的改造对区块链隐私处理十分有限，融合其他密码学技术进行交叉应用，扬长避短是大势所趋。例如，借助 Schnorr 同态特性，与 Pedersen 承诺融合设计可以合并签署不同消息的高效安全多方计算协议[48]；考虑去中心化托管保障用户隐私信息和资产安全，基于安全多方计算的门限签名技术进行密钥的分布式管理（DKMS，distributed key manage system）[52]；提出复合签名技术[53]削弱数据的关联性，基于 Diffie-Hellman 假设保证计算困难性、提高隐私性等。

2.2 基于属性基加密的区块链访问控制

属性基加密[54]（ABE，attribute-based encryption）源自对身份信息属性的识别，其安全性在于使不满足既定策略的攻击者所拥有的密钥无法解密密文。密文可在不安全的信道上进行传输，也可上传至开放的网络存储设备中。

属性基加密主要分为两种：一种是密钥策略的属性基加密[55]（KPABE，key-policy attribute encryption），另一种是密文策略的属性基加密[56]（CPABE，ciphertext-policy attribute-based encryption）。其中，CPABE 方案能够有效处理区块链隐私，此方案中数据拥有者可以设定访问策略，只有满足访问策略的用户可以解密共享一份数据内容。Rahulamathavan 等[57]利用属性加密对区块链数据进行隐私预留，以实现物联网中端到端的隐私关联。汪金苗等[58]在单授权 CPABE 方案下进行扩展，给出了多授权属性分发管理、访问可控的隐私保护方案。闫玺玺等[59]在以太坊上设计了可控制关键词语义安全的属性基加密方案，防止隐私数据泄露实现密文检索。

因为基于 CPABE 的访问控制隐含授权集合的访问树结构，所以在区块链隐私保护上能够进行小群体范围内的信息隐私保护。任何一种加密技术都会有其劣势，基于属性基加密的访问控制也不例外，如加密过程中大量的双线性映射，使属性基加密在数据计算上非常耗时；密文长度会随着属性数量增加而增加，从而占用过多区块存储空间。因此，优化时间和空间上的研究将会进一步改善区块链访问控制的性能。此外，如果使用智能合约实现访问控制[60]，直接将访问策略暴露给全网并不是一个很好的选择，需要对智能合约设计额外隐私方案。跨组织跨链的访问控制正

备受瞩目，如何在多链并存的条件下解决基于此类新型密码学技术的访问控制策略冲突、适应合约自动化控制有十分重要的探讨价值。然而，区块链对于密码学而言，绝不仅仅是在于使用了签名协议，或者基于工作量证明（PoW，proof of work）等验证的共识算法使用了哈希函数。在区块链的分布式网络中，进一步稳固数字世界中共识和交易的基础设施的正是焕发活力不断改良的密码学技术，如同态加密、安全多方计算以及零知识证明。

2.3　同态加密

同态加密属于基于非噪声方法的安全计算，可以使数据在密文状态下进行计算，解密后可获得与明文进行同样运算后的结果。对于区块链应用同态加密的理论很多，如 Pedersen 承诺[61]、ElGamal 承诺等密码学承诺，这些承诺或具备加法同态特性或具备乘法同态特性，可以将数据进行私密保存并通过公布数据的哈希值来承诺它的真实性，如利用 ElGamal 乘法同态特性进行隐私计算，实现安全可信的交换承诺[62]等。在区块链中，不管是公有链、私有链还是联盟链，直接对明文信息进行处理并发布至智能合约将会很大程度地泄露敏感数据。应用同态加密既能保证链上数据隐私，也能实现节点与节点之间数据的可计算性。区块链同态加密理论模型如图 5 所示，参与方首先需要进行算法协商，协定公共参数；然后由加密方对交易信息进行同态加密，并将完成签名的数据传送上链。等到数据经智能合约验签后，使用方将在链下解密数据，获取明文信息；最后由合约对验签数据进行销毁。

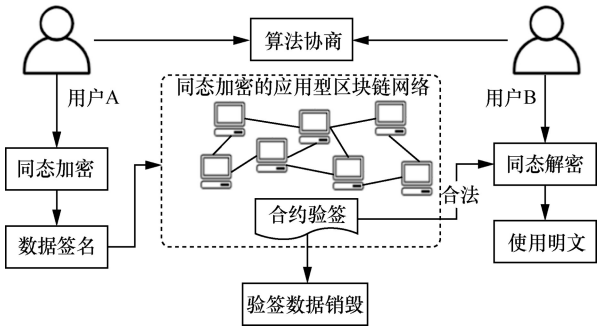

图 5　区块链同态加密理论模型

Figure 5 Blockchain homomorphic cryptography theoretical model

同态加密是密码学重要的研究领域之一，不少区块链应用使用到同态加密，典型如 Hawk[63]，基于同态映射实现加密数据运算和智能合约的私密信息处理。此外，使用同态加密可以对交易资金进行加密，实现私密交易[64]。然而，在区块链隐私保护方面，交易隐私或者数据运算隐私并不代表全部，同态加密仅能解决密文计算的问题隐私。由于私钥并不上链公开，依靠同态加密技术难以在智能合约上非公开地验证明文计算的结果，通常情况下同态加密会和其他技术一起使用，如安全多方计算、零知识证明等。

2.4　安全多方计算

信息安全，包括数据安全、通信安全以及计算安全。计算安全在多方协作交易中尤为重要，在密码学知识领域被称为安全多方计算（SMPC，secure multi-party computation）。SMPC 可以解决协同计算隐私保护问题，具有输入隐私性、计算正确性以及去中心化特征，能使数据既保持隐私又能被使用，从而释放隐私数据分享、隐私数据分析以及隐私数据挖掘的巨大价值。个人信息在共享和计算中容易出现安全问题和隐私问题，安全多方计算可以结合区块链特征使用户数据隐私得以保护[65]，使不可信多方之间进行敏感数据联合计算、敏感数据求交集、敏感数据联合建模等。例如，隐私计算平台 Enigma[25]，通过 SMPC 以分布式形式计算数据，同时改进分布式哈希表进行数据存储，并分散到多个区块链节点上进行责任分摊。

考虑到区块链空间有限，对于大量数据的隐私计算，往往会使用 SMPC 把敏感信息放到链下进行计算，再采用有状态变化的复用微型支付通道构建信息传输、交易支付[66]等，通过安全哈希来验证交易的有效性与可信性。虽然对于计算本身，在区块链链外的数据计算隐蔽性较强，但某种程度上会使区块链可信性降低。如果过于依赖链外多方计算，则需要额外的可信第三方参与验证和确认交易，从而增加交易开销和单点故障风险。可信执行环境[67]一定程度上可增强安全多方计算在区块链隐私保护上的安全效益，但高要求的硬件环境对于目前应用而言，仍然存在差距，

大规模应用仍有待时日。

在区块链通用计算领域，SMPC 的“低效”是需要克服的问题。一般地，多方计算中需要多轮交互，尤其在某些协作计算的场景下要求参与方保持在线，交易的效率偏低。此外，区块链中应用 SMPC，协作计算方的身份往往无法确定，身份识别不可避免地需要揭露参与方的部分隐私，单靠安全多方计算可能无法处理这方面的隐私问题。在大规模商业部署中，SMPC 仍存在不小阻力。首先是意愿，很多大企业和机构并不愿意尝试隐私计算，数据输出一旦操作不当将会带来灾难级的隐私风险。其次是协作难度，多方数据清理、数据格式统一、接口统一且完整部署好隐私计算的系统，需要大量可信协作方资源参与合作，实现难度较高。

总体来说，在这一密码学技术领域上，要想链上数据相对可信，可先使数据上链，然后利用多方隐私计算榨取数据价值，保护数据隐私。然而，现有信息系统是否允许，或者说是否有足够用于多方协作的数据值得考虑和探究。

2.5 零知识证明

零知识证明是一种不泄露敏感数据信息即能向他人证明信息归属权的密码学技术，善于平衡隐私和透明的需求[68]。ZKP 作用于区块链上不仅可以解决数据上链隐私泄露，也可以在性能提优、数据量大无法上链方面做出改善。本节从目前主流的区块链零知识证明技术入手，剖析近期零知识证明技术的发展现状。

零知识证明在区块链上最具规模的算法当属 zk-SNARK，是一种无须交互的零知识算法。在应用 zk-SNARK 的交易输出中，通过验证交易内容值正确性承诺的合法性确保数据内容不会被泄露。例如，在 Zerocash[69]的 UTXO 模型中，付款来源存在于指定默克尔树（Merkle Tree），借助 zk-SNARK 算法则不需要将其暴露出来即可验证来源的正确性，实现隐私交易。然而，zk-SNARK 算法在进行零知识证明处理前需要对一些公共参考数据集（CRS，common reference string）进行可信设置，CRS 一旦遭受破坏就会降低零知识证明具备的隐私效益。因此，现今研究发展中，逐渐着眼于去可信设置的零知识证明算法，如 zk-STARK[70]。zk-STARK 在既需要互信又存在很多动机的应用场景中，使用同态隐藏、杂凑函数进行抗量子防御。此外，在数据隐私处理方面，STARK 组件允许在不损害计算完整性的情况下屏蔽私有输入且允许区块链进行大规模扩展，对于验证方的算法复杂度方面可以控制到多项式时间级别。类似无须可信设置的还有 BulletProof[71] 协议，该协议借助 Pedersen 承诺代替输入输出金额，然后在可公开验证交易余额情况下，隐藏特定的提交金额。2018 年，在遭受一系列隐私问题后，BulletProof 算法被引入，在保证区块链隐私基础上优化交易，提高效率。BulletProof 算法产生的证明大小与范围区间上限呈对数关系，可将多个证明进行合并，使原本占用区块链的数据空间以及交易费用缩减至 70%~80%。常见零知识证明算法对比如表 3 所示。

SNARK 算法虽然具有高效的验证速度和高强的密码学假设，但需要初始化可信设置，并且生成的交易要花费大量存储空间。相比之下，BulletProof 更适合在中低复杂度的交易中使用，但对于高复杂度的交易中验证过程相对耗时。

表 3 常见零知识证明算法对比

Table 3 Comparison of common zero-knowledge proof algorithms

算法	算数复杂度：证明方	算数复杂度：验证方	通信复杂度（证明大小）	单笔交易大小评估	1 万笔交易大小评估	以太坊 gas 费用	可信设置	后量子安全	密码学假设性强度
SNARK	$O(n\log(N))$	$O(1)$	$O(1)$	Tx:200 byte, Key:50 MB	Tx:200 byte, Key:500	600 kB（Groth16）	是	否	强
STARK	$O(n\,\text{poly-log}(N))$	$O(\text{poly-log}(N))$	$O(\text{poly-log}(N))$	45 kB	135 kB	2.5 MB（预估）	否	是	抗强哈希碰撞
BulletProof	$O(n\log(N))$	$O(N)$	$O(\log(N))$	1.5 kb	2.5 kB	N/A	否	否	离散对数安全

STARK 在证明方算数复杂度上优于 SNARK，在验证方算数复杂度上优于 BulletProof，同时是一种后量子安全的算法，但以太坊 gas 开销偏大。除了上述提及的零知识证明算法，一些新型零知识证明技术也在不断涌现。Sonic[72]和 PLONK[73]是基于 zk-SNARK 算法的零知识证明扩展版本，虽仍需要进行可信设置，但设置的数据信息广且可重用，因而可拓展性高。最近发布的密码学工具 DARK Proof[74]，对 Sonic 和 PLONK 的性能进一步调优，移除了其可信设置（该改进算法被称为 Supersonic）。因此，在计算复杂度高的交易或需提供证明的场景中，Supersonic 的验证非常高效。此外，该证明产生的数据体积远小于 SNARK、STARK 这类证明。

虽然零知识证明在区块链隐私保护上效果显著，用户可以借助其离线计算数据达到在区块链上的交易信息隐藏[75]，但在实现上仍存在一些问题亟须解决。首先是电路设计，因为区块链公开透明，在零知识电路设计上需要大量密码封装实现，不可避免地依赖了很多约束和参数调优。其次是侧信道攻击，因为生成零知识证明的时间取决于隐私交易的数据，所以尽管交易机制具备零知识特性，但值得注意的是，能够测量证明生成时间的攻击者可能会破坏交易的隐私性。

3　基于后量子密码学的隐私保护技术

区块链隐私加密技术发展需考虑未来挑战及如何实现加密技术的升级与替换。量子计算是当前区块链面临的最具挑战性的前沿技术，虽然实用型量子计算机的发展还处于起步阶段，但已经可以断定目前区块链很多加密技术可以轻易地被量子计算攻破。例如，利用 Shor 算法[76]可以快速解决大整数分解及离散对数解困难的问题。研究人员已经确定，使用 1 000 量子位的量子计算机就可以攻破 160 位的椭圆曲线，而 1 024 位的 RSA 大约需要 2 000 量子位。尽管已知的量子计算机求解能力有限，但随着技术的迅猛发展，不排除将来有更高效的量子破解算法面世。由我国研制出的 76 光子“九章”量子计算原型机，已被证实可以在运算速度和运算能力上远超当前超级计算机。换言之，量子计算机攻破当前的区块链隐私加密技术可能只是时间问题。因此，寻找能够应用至区块链的抗量子计算密码学理论已成为下一代隐私加密技术研究的热点话题，而抗量子计算的区块链隐私计算的研究重点在于格密码与全同态加密。

3.1　格密码尝试

格密码主要是基于格困难问题产生的一类噪声加密密码。格是一组线性无关的非零向量的整系数线性组合，普遍认为一个高维的格中，随机选取格基找短格基或得到线性无关的短格向量是困难的，且具备最坏情况困难性[77]。对于量子时代区块链隐私数据保护，格密码可结合同态加密，建立具备加同态的后量子安全承诺方案保护数据隐私[78]；也有学者利用盆景树模型改进晶格签名[79]，以保证公私钥的随机性和安全性，使反量子加密技术适用于区块链用户地址的生成，从而保护隐私。

基于格密码的算法可以加快区块链用户交易速度，在实现密钥生成、签名上计算复杂度相对较低，可以在后量子时代高效安全地执行区块链隐私数据计算。

3.2　全同态加密初探

一个算法或协议同时具备加法同态和乘法同态的特性即可视为全同态加密（FHE，fully homomorphic encryption）。区块链隐私保护上寻求全同态加密，主流方法是构造容错学习（LWE，learning with errors）或环容错学习（RLWE，ring learning with errors）的困难问题来实现全同态场景的近似替代。现今仍以理论研究为主，如快速隐私集合求交[80]、多身份隐私加密[81]等，全同态加密在区块链中的隐私应用方案，距离高效的工程应用还有着难以跨越的鸿沟[81-83]，主要有以下几点问题需要解决。

1) 缺乏国际统一标准。当前学术和工程应用方面均处于探索阶段，使开发者难以参照规范进行系统性开发。

2) 存在计算和存储开销大等无法规避的性能问题。2009 年，Gentry 开创基于理想格的全同态方案[78]，从理论上可实现任何同态加密，但目前硬件水平无法支撑。

3) 开源技术社区运营少。开发项目软件质量

差。目前工程化和商业化均处于早期，全同态加密的开发人员少，知识储备十分不足，从而开发的项目使用少，维护投入比较低。

全同态加密区块链隐私计算应用有着广阔前景，如果未来能够出现某种高效的异构加速技术或者硬件产品极大地降低乃至消除性能瓶颈，那么全同态加密可替代可信执行环境中以 SGX 为主的隐私计算，也可以替代安全多方计算中半同态加密的位置，从而实现“隐私计算直通车”的目的。

3.3 挑战与风险

除格密码和全同态加密外，后量子密码学在区块链隐私加密方案上仍有可扩展的空间。然而，目前抗量子的区块链隐私加密技术面临着以下几个挑战，及时解决这些技术瓶颈，方可在未来游刃有余地应对量子计算机带来的风险。

签名方案的改变是迫切需要解决的问题之一。因为旧公钥和私钥产生的脆弱签名无法在量子计算面前确保交易的安全，所以需要将其更新为新的抗量子计算的签名方案。如果对旧签名进行更换，那么需要区块链网络中的大部分节点进行分叉达成新的共识，意味着需要对大规模节点进行升级，从而使基于旧的签名方案产生的区块被拒绝。由于拥有节点控制权限的人的更新选择是自由的，共识势必是一个缓慢的过程。并且，将区块链升级成具备抗量子的签名方案绝不仅仅是简单复制粘贴以及更改一些代码块，重排编码的工作量也非常巨大。

区块链用户地址的治理也是迫切需要解决的问题之一。区块链用户地址的转移直接影响了用户的资金利益链。即使区块链进行量子化的升级，也只是对共识完成后生成的新地址的密钥产生影响，而共识前的地址并不会被变更和销毁。理论而言，只有用户自己选择将资金转移到具备量子抗性的地址，才能保障个人财产安全与隐私。值得注意的是，如果转移过程中共识前的地址发生了丢失，那么没有人能够触碰到共识前地址上的资金，这些资金也永远无法被转移，也就永远容易被敌手利用新型破解技术进行窃取。

加密效能的提升也是迫切需要解决的问题之一。目前的后量子签名技术，包括现阶段提交到美国国家标准技术研究所（NIST）的签名方案，如 CRYSTALS[84]、FALCON[85]、Rainbow[86]等，都会增加区块的大小，意味着需要更多的计算资源，进而降低每笔交易的速度。抗量子签名方案会对区块链性能产生很大影响，同时对现有的大部分区块链项目进行安全降级。解决抗量子区块链的问题是当前正在进行的研究，并且有待更深入的研究。

4 结束语

区块链技术在数据可信性与完整性方面已取得较多成果，但在其他方面，尤其是匿名、隐私等技术方面还不够成熟。本文针对区块链隐私保护技术，从基本要素防护和密码学防护两个方面进行了分析，总结出仅从区块链的应用层、合约层出发难以有效解决隐私问题，需要利用各类密码学技术根据需求和应用场景的不同进行优势互补。为了进一步突显文章所涉及的区块链密码学隐私保护技术以及关联性，对区块链密码学隐私保护技术进行对比，如表 4 所示。

表 4 区块链密码学隐私保护技术对比

Table 4 Comparison of Blockchain privacy protection techniques in cryptography

名称	主要技术特点	主要适用场景
聚合签名	签名分片	多方参与
属性基加密	访问控制	身份验证
同态加密	密文计算	敏感数据处理
安全多方计算	多方计算	多方协作
零知识证明	零知识性	保密交易
格密码	抗量子计算	隐私技术融合
全同态加密	抗量子计算	隐私技术融合

结合前文所归纳的各类区块链隐私保护技术以及表 4 内容，下一步工作应从以下方面来推进。

1) 在基础要素防护方面，区块链隐私保护技术在原有技术架构的基础上应融入现代乃至未来可期的隐私密码学技术。前沿密码学协议和区块链技术之间的相辅相成将会推动数字世界发展，衍生出安全数据分享、隐私保护，或者更多应用。Ben-Sasson 等[87]最近提出的交互式预言机证明（IOP，interactive oracle proof），融入零知识通过逻辑合理的形式化定义构建了验证时间短、计算

复杂度为多项式时间的隐私方案。简言之，与时俱进才能更加长久地对区块链隐私保护产生深远影响。例如，天然适配于分布式网络的安全多方计算，可以联合机器学习等应用在区块链上构建安全数据流转平台；拥有特别性质的零知识证明技术也为多方参与的可验证的匿名交易[88]提供了隐私保障。

2) 在密码学防护方面，区块链隐私保护技术在底层技术上应继续推进基础协议与可证明的安全技术创新。不管是应用在区块链上的现代密码学工具还是实用性协议，都需要提供安全性证明。例如，Ouroboros 首次提出具备实用性的 PoS 协议，通过可证明安全提出了隐私合约机制而被广泛推崇与研究[89]。如果没有可证明安全，分布式网络中的节点单位用户仍然会留有不信任感，可证明安全是基于数学的、客观的，也是真正意义上有价值的隐私保护证明方式。

3) 除了上述的研究建议，区块链隐私保护技术也可融合非密码隐私技术、跨领域乃至多领域技术进行拓展。虽已有 Tor 网络、混币技术以及各类复杂度更高的非对称加密算法被提出，但方法仍然非常局限，未来有很大改进空间。在数字经济框架下，区块链可以与匿名[90]、泛化[91]、差分隐私[92]等技术进行优势互补，增强数据输入输出隐私能力。未来区块链隐私加密技术可以与物联网技术[93-94]进行深度融合，链下数据无损安全地移到链上，离不开物联网智能设备的支持，同时，区块链对物联网智能设备的一些监控监管有巨大的应用前景。另外，一旦联邦学习、可信执行环境等隐私 AI 技术[95]融合了区块链，将具有强大纠错能力和复利生成能力。在面对环境变化时，数据资产的安全流动，让个人隐私信息、商业秘密在防止泄露条件下进行交易，同时实现公共利益最大化。在数据、应用隐私保护合理的情况下最终形成可信[96]、共赢的新型价值联盟，实现社会化生产的提效降本，并促进和深化社会创新。

本文着眼于区块链上隐私保护技术，梳理了区块链基本要素隐私防护、隐私密码学等为核心的技术及思想，展望了未来区块链隐私保护技术的发展趋势，以积极推动区块链隐私加密技术的研究与发展。

参考文献：

[1] LISCHKE M, FABIAN B. Analyzing the bitcoin network: the first four years[J]. Future Internet, 2016, 8(4): 7-47.

[2] NEUDECKER T, HARTENSTEIN H. Could network information facilitate address clustering in bitcoin[C]//International Conference on Financial Cryptography and Data Security. 2017: 155-169.

[3] GOLDFEDER S, KALODNEEER H, REISMAN D, et al. When the cookie meets the blockchain: privacy risks of web payments via cryptocurrencies[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(4): 179-199.

[4] SAYEED S, MARCO-GISBERT H. Assessing blockchain consensus and security mechanisms against the 51% attack[J]. Applied Sciences, 2019, 9(9): 1788-1805.

[5] Nicolas van Saberhagen. CryptoNote v 2. 0[EB].

[6] CHAN W, OLMSTED A. Ethereum transaction graph analysis[C]//Proceedings of 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 2017: 498-500.

[7] RUFFING T, MORENO-SANCHEZ P A. Mixing confidential transactions: comprehensive transaction privacy for bitcoin[J]. IACR Cryptol EPrint Arch, 2017, 2017: 238-260.

[8] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes[C]//Financial Cryptography and Data Security. 2014: 486-504.

[9] RANSHOUS S, JOSLYN C A, KREYLING S, et al. Exchange pattern mining in the bitcoin transaction directed hypergraph[C]//Financial Cryptography and Data Security, 2017: 248-263.

[10] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: an untrusted bitcoin-compatible anonymous payment hub[C]//Proceedings 2017 Network and Distributed System Security Symposium. 2017.

[11] FERRETTI C, LEPORATI A, MARIOT L, et al. Transferable anonymous payments via tumblebit in permissioned blockchains[C]//DLT@ ITASEC. 2019: 56-67.

[12] VALENTA L, ROWAN B. BlindCoin: blinded, accountable mixes for bitcoin[M]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 112-126.

[13] 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. 2015: 75-86.

[14] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for bitcoin[C]//Proceedings of the 13th Workshop on Privacy in the Electronic Society. 2014: 149-158.

[15] LEE S, YOON C, KANG H, et al. Cybercriminal Minds: an investigative study of cryptocurrency abuses in the Dark Web[C]//Proceedings 2019 Network and Distributed System Security Symposium. 2019: 1-15.

[16] CHEN W L, WU J, ZHENG Z B, et al. Market manipulation of bitcoin: evidence from mining the Mt. gox transaction network[C]//Proceedings of IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. 2019: 964-972.

[17] ERMILOV D, PANOV M, YANOVICH Y. Automatic bitcoin address clustering[C]//Proceedings of 2017 16th IEEE International

Conference on Machine Learning and Applications. 2017: 461-466.
[18] MÖSER M, SOSKA K, HEILMAN E, et al. An empirical analysis of traceability in the monero blockchain[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(3): 143-163.
[19] ZHANG F, MARAM D, MALVAI H, et al. DECO: liberating web data using decentralized oracles for TLS[C]//Proceedings of CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 1919-1938.
[20] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework. White Paper[EB].
[21] JIANG Y M, WANG C X, WANG Y W, et al. A privacy-preserving E-commerce system based on the blockchain technology[C]//Proceedings of 2019 IEEE International Workshop on Blockchain Oriented Software Engineering. 2019: 50-55.
[22] BREIDENBACH L. Mixicles: simple private decentralized finance ari juels[EB].
[23] BÜNZ B, AGRAWAL S, ZAMANI M, et al. Zether: towards privacy in a smart contract world[C]//Financial Cryptography and Data Security. 2020: 423-443.
[24] ZHANG F, HE W, CHENG R, et al. The ekiden platform for confidentiality-preserving, trustworthy, and performant smart contracts[C]//Proceedings of IEEE Security & Privacy. 2019: 185-200.
[25] ZYSKIND G, NATHAN O, PENTLAND A. Enigma: decentralized computation platform with guaranteed privacy[EB].
[26] 蔡亮, 端豪, 鄢萌, 等. 基于双层协同的联盟区块链隐私数据保护方法[J]. 软件学报, 2020, 31(8): 2557-2573.
CAI L, DUAN H, YAN M, et al. Private data protection scheme for consortium blockchain based on two-layer cooperation[J]. Journal of Software, 2020, 31(8): 2557-2573.
[27] PODGORELEC B, TURKANOVIĆ M, KARAKATIČ S. A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection[J]. Sensors (Basel, Switzerland), 2019, 20(1): 147.
[28] 黄克振, 连一峰, 冯登国, 等. 基于区块链的网络安全威胁情报共享模型[J]. 计算机研究与发展, 2020, 57(4): 836-846.
HUANG K Z, LIAN Y F, FENG D G, et al. Cyber security threat intelligence sharing model based on blockchain[J]. Journal of Computer Research and Development, 2020, 57(4): 836-846.
[29] ASHIZAWA N, YANAI N, CRUZ J P, et al. Eth2Vec: learning contract-wide code representations for vulnerability detection on ethereum smart contracts[C]//Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure. 2021: 47-59.
[30] HE N, ZHANG R, WANG H, et al. {EOSAFE}: security analysis of {EOSIO} smart contracts[C]//30th {USENIX} Security Symposium. 2021: 1271-1288.
[31] KRUPP J, ROSSOW C. teether: gnawing at ethereum to automatically exploit smart contracts[C]//27th {USENIX} Security Symposium. 2018: 1317-1333.
[32] KALRA S, GOEL S, DHAWAN M, et al. ZEUS: analyzing safety of smart contracts[C]//Proceedings 2018 Network and Distributed System Security Symposium. 2018: 2017: 16-17.
[33] BHARGAVAN K, DELIGNAT-LAVAUD A, FOURNET C, et al. Formal verification of smart contracts: short paper[C]// Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. 2016: 91-96.
[34] ABDELLATIF T, BROUSMICHE K L. Formal verification of smart contracts based on users and blockchain behaviors models[C]//Proceedings of 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2018: 1-5.
[35] MEHAR M I, SHIER C L, GIAMBATTISTA A, et al. Understanding a revolutionary and flawed grand experiment in blockchain[J]. Journal of Cases on Information Technology, 2019, 21(1): 19-32
[36] CHAUM D, VAN-HEYST E. Group signatures[C]//Workshop on the Theory and Application of of Cryptographic Techniques. 1991: 257-265.
[37] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2001: 552-565.
[38] MAXWELL G, POELSTRA A. Borromean ring signatures[EB].
[39] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. 1983: 199-203.
[40] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 473-489.
[41] HEILMAN E, BALDIMTSI F, GOLDBERG S. Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions[C]//Financial Cryptography and Data Security. 2016: 43-60.
[42] 江泽涛, 徐娟娟. 云环境下基于代理盲签名的高效异构跨域认证方案[J]. 计算机科学, 2020, 47(11): 60-67.
JIANG Z T, XU J J. Efficient heterogeneous cross-domain authentication scheme based on proxy blind signature in cloud environment[J]. Computer Science, 2020, 47(11): 60-67.
[43] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.
[44] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple schnorr multi-signatures with applications to bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.
[45] NICK J, RUFFING T, SEURIN Y, et al. MuSig-DN: schnorr multi-signatures with verifiably deterministic nonces[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020: 1717-1731.
[46] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. 2001: 514-532.
[47] SCHOLL T. Isolated elliptic curves and the MOV attack[J]. Journal of Mathematical Cryptology, 2017, 11(3): 131-146.
[48] BONEH D, DRIJVERS M, NEVEN G. Compact multi-signatures for smaller blockchains[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2018: 435-464.
[49] DOERNER J, KONDI Y, LEE E, et al. Secure two-party threshold ECDSA from ECDSA assumptions[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. 2018 : 980-997
[50] CASTAGNOS G, CATALANO D, LAGUILLAUMIE F, et al.

Two-party ECDSA from hash proof systems and efficient instantiations[C]//Advances in Cryptology-CRYPTO 2019. 2019: 191-221.

[51] AHMAT D, CHOROMA M, BISSYANDÉ T F. Multipath key exchange scheme based on the diffie-Hellman protocol and the Shamir threshold[J]. Int J Netw Secur, 2019, 21: 418-427.

[52] SOLTANI R, NGUYEN U T, AN A J. Practical key recovery model for self-sovereign identity based digital wallets[C]//Proceedings of 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress. 2019: 320-325.

[53] SAXENA A, MISRA J, DHAR A. Increasing anonymity in bitcoin[C]//International Conference on Financial Cryptography and Data Security. 2014: 122-139.

[54] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT 2005. 2005: 457-473.

[55] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conf on Computer and Communications Security. 2006. 89-98.

[56] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//2007 IEEE Symposium on Security and Privacy (SP '07). 2007: 321-334.

[57] RAHULAMATHAVAN Y, PHAN R C W, RAJARAJAN M, et al. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption[C]//Proceedings of 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems. 2017: 1-6.

[58] 汪金苗, 谢永恒, 王国威, 等. 基于属性基加密的区块链隐私保护与访问控制方法[J]. 信息网络安全, 2020, 20(9): 47-51.
WANG J M, XIE Y H, WANG G W, et al. A method of privacy preserving and access control in blockchain based on attribute-based encryption[J]. Netinfo Security, 2020, 20(9): 47-51.

[59] 闫玺玺, 原笑含, 汤永利, 等. 基于区块链且支持验证的属性基搜索加密方案[J]. 通信学报, 2020, 41(2): 187-198.
YAN X X, YUAN X H, TANG Y L, et al. Verifiable attribute-based searchable encryption scheme based on blockchain[J]. Journal on Communications, 2020, 41(2): 187-198.

[60] 杜瑞忠, 刘妍, 田俊峰. 物联网中基于智能合约的访问控制方法[J]. 计算机研究与发展, 2019, 56(10): 2287-2298.
DU R Z, LIU Y, TIAN J F. An access control method using smart contract for Internet of Things[J]. Journal of Computer Research and Development, 2019, 56(10): 2287-2298.

[61] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Annual international cryptology conference. 1991: 129-140.

[62] RUFFING T, MALAVOLTA G. Switch commitments: a safety switch for confidential transactions[C]//International Conference on Financial Cryptography and Data Security. 2017: 170-181.

[63] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//Proceedings of 2016 IEEE Symposium on Security and Privacy. 2016 : 839-858.

[64] POELSTRA A, BACK A, FRIEDENBACH M, et al. Confidential assets[C]//International Conference on Financial Cryptography and Data Security. 2018: 43-63.

[65] 王童, 马文平, 罗维. 基于区块链的信息共享及安全多方计算模型[J]. 计算机科学, 2019, 46(9): 162-168.
WANG T, MA W P, LUO W. Information sharing and secure multi-party computing model based on blockchain[J]. Computer Science, 2019, 46(9): 162-168.

[66] BENTOV I, KUMARESAN R, MILLER A. Instantaneous decentralized poker[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2017: 410-440.

[67] CHOUDHURI A R, GREEN M, JAIN A, et al. Fairness in an unfair world: fair multiparty computation from public bulletin boards[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 719-728.

[68] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//Proceedings of 26th Annual Symposium on Foundations of Computer Science (sfcs 1985). 1985: 383-395.

[69] BEN SASSON E, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]//Proceedings of 2014 IEEE Symposium on Security and Privacy. 2014: 459-474.

[70] BEN-SASSON E, BENTOV I, HORESH Y, et al. Scalable, transparent, and post-quantum secure computational integrity[J]. IACR Cryptol ePrint Arch. 2018, 2018: 46-129.

[71] BÜNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: short proofs for confidential transactions and more[C]//2018 IEEE Symposium on Security and Privacy (SP). 2018: 315-334.

[72] MALLER M, BOWE S, KOHLWEISS M, et al. Sonic: zero-knowledge SNARKs from linear-size universal and updatable structured reference strings[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 2111-2128.

[73] GABIZON A, WILLIAMSON Z J, CIOBOTARU O . PLONK: permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge[J]. IACR Cryptol ePrint Arch, 2019, 2019: 953.

[74] BÜNZ B, FISCH B, SZEPIENIEC A. Transparent snarks from dark compilers[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2020: 677-706.

[75] BOWE S, CHIESA A, GREEN M, et al. Zexe: enabling decentralized private computation[C]//2020 IEEE Symposium on Security and Privacy (SP). 2020: 947-964.

[76] FERNÁNDEZ-CARAMÈS T M, FRAGA-LAMAS P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks[J]. IEEE Access, 2020,8: 21091-21116.

[77] ESGIN M F, STEINFELD R, SAKZAD A, et al. Short lattice-based one-out-of-many proofs and applications to ring signatures[C]//International Conference on Applied Cryptography and Network Security. 2019: 67-88.

[78] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. 2009: 169-178.

[79] YIN W, WEN Q, LI W, et al. A anti-quantum transaction authentication approach in blockchain[J]. IEEE Access, 2018, 6: 5393-5401.

[80] CHEN H, LAINE K, RINDAL P. Fast private set intersection from homomorphic encryption[C]//Proceedings of the 2017 ACM SIG-

SAC Conference on Computer and Communications Security. 2017: 1243-1255.

[81] 汤永利, 胡明星, 叶青, 等. 改进的格上基于多身份全同态加密方案[J]. 北京邮电大学学报, 2018, 41(1): 125-133.
TANG Y L, HU M X, YE Q, et al. Improved multi-identity based fully homomorphic encryption scheme over lattices[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(1): 125-133.

[82] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[C]//Annual Cryptology Conference. 2013: 75-92.

[83] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (leveled) fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory, 2014, 6(3): 1-36.

[84] DUCAS L, KILTZ E, LEPOINT T, et al. CRYSTALS-dilithium: a lattice-based digital signature scheme[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018: 238-268.

[85] FOUQUE P A, HOFFSTEIN J, KIRCHNER P, et al. Falcon: Fast-Fourier lattice-based compact signatures over NTRU[J]. Submission to the NIST's Post-Quantum Cryptography Standardization Process, 2018, 36.

[86] DING J, SCHMIDT D. Rainbow, a new multivariable polynomial signature scheme[C]//International Conference on Applied Cryptography and Network Security. 2005: 164-175.

[87] BEN-SASSON E, BENTOV I, HORESH Y, et al. Scalable zero knowledge with no trusted setup[C]//Advances in Cryptology – CRYPTO 2019, 2019: 701-732.

[88] CHOUDHURI A R, GOYAL V, JAIN A. Founding secure computation on blockchains[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2019: 351-380.

[89] KERBER T, KIAYIAS A, KOHLWEISS M, et al. Ouroboros crypsinous: Privacy-preserving proof-of-stake[C]//2019 IEEE Symposium on Security and Privacy (SP). 2019: 157-174.

[90] 刘海, 李兴华, 雒彬, 等. 基于区块链的分布式 K 匿名位置隐私保护方案[J]. 计算机学报, 2019, 42(5): 942-960.
LIU H, LI X H, LUO B, et al. Distributed K-anonymity location privacy protection scheme based on blockchain[J]. Chinese Journal of Computers, 2019, 42(5): 942-960

[91] LI H, PEI L S, LIAO D, et al. Blockchain meets VANET: an architecture for identity and location privacy protection in VANET[J]. Peer-to-Peer Networking and Applications, 2019, 12(5): 1178-1193.

[92] 董祥千, 郭兵, 沈艳, 等. 一种高效安全的去中心化数据共享模型[J]. 计算机学报, 2018, 41(5): 1021-1036.
DONG X Q, GUO B, SHEN Y, et al. An efficient and secure decentralizing data sharing model[J]. Chinese Journal of Computers, 2018, 41(5): 1021-1036.

[93] YAJI S, BANGERA K, NEELIMA B. Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications[C]//Proceedings of 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW). 2018: 81-85.

[94] MENDKI P. Blockchain enabled IoT edge computing: addressing privacy, security and other challenges[C]//Proceedings of the 2020 The 2nd International Conference on Blockchain Technology. 2020: 63-67.

[95] PASSERAT-PALMBACH J, FARNAN T, MCCOY M, et al. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data[C]//Proceedings of 2020 IEEE International Conference on Blockchain (Blockchain). 2020: 550-555

[96] 周家顺, 王娜, 杜学绘. 基于区块链的数据完整性多方高效审计机制[J]. 网络与信息安全学报, 2021, 7(6): 113-125.
ZHOU J S, WANG N, DU X H. Multi-party efficient audit mechanism for data integrity based on blockchain[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 113-125.

[作者简介]

刘峰（1988– ），男，湖北荆州人，华东师范大学博士生，主要研究方向为区块链技术、可计算情感。

杨杰（1998– ），男，江苏泰州人，上海对外经贸大学科研助理，主要研究方向是研究方向为密码学、区块链、信息隐私和安全多方计算。

齐佳音（1972– ），女，陕西洛南人，上海对外经贸大学教授、博士生导师，主要研究方向为先进技术和管理创新。