区块链的网络安全: 威胁与对策

房卫东[1,2], 张武雄[1,2*], 潘 涛[3], 陈 伟[4], 杨 旸[1,2]

[1]中国科学院 上海微系统与信息技术研究所 无线传感器网络与通信重点实验室, 上海 中国 201899
[2]上海无线通信研究中心, 上海 中国 201210
[3]神华信息技术有限公司, 北京 中国 100011
[4]中国矿业大学 计算机科学与技术学院, 徐州 中国 221116

摘要 区块链以其特有的安全性, 已在许多领域中得到应用。然而, 对其网络安全的进一步研究往往被忽略, 较为突出的表现之一就是关于这方面的研究成果很少被关注并发表。本文针对区块链数据的完整性、匿名性与隐私保护的安全需求, 系统分析了区块链的安全攻击, 综述了安全保护技术研究进展, 尤其对区块链密码学安全防护技术进行了对比分析。本文对当前区块链安全防护技术的综述工作, 将有效地帮助区块链的架构优化与安全算法改进。

关键词 区块链; 网络安全; 安全攻击; 完整性
中图法分类号 TN915.08 DOI 号 10.19363/j.cnki.cn10-1380/tn.2018.03.05

Cyber Security in Blockchain: Threats and Countermeasures

FANG Weidong[1,2], ZHANG Wuxiong[1,2*], PAN Tao[3], CHEN Wei[4], YANG Yang[1,2]

[1] Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China
[2] Shanghai Research Center for Wireless Communication, Shanghai 201210, China
[3] Shenhua Information Technology Co., LTD, Beijing 100011, China
[4] School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China

Abstract Since the blockchain has unique security, it has been applied in many areas. However, further research on cyber security is often ignored in blockchain. One of the more prominent phenomena is that, the research results on cyber security are seldom concerned and published. In this paper, based on the following security requirements of blockchain: the integrity, the anonymity and the privacy preservation, we systematically analyze the security attacks in blockchain, and summarize the state-of-the-art research progress of security protection technology, especially the cryptography security protection technology for blockchain. The contributions of this paper will facilitate to optimize the system architecture, and improve the security algorithm for blockchain effectively.

Key words blockchain; cyber security; security attack; integrity

1 引言

2008 年, 中本聪首次提出区块链(Blockchain)的概念[1], 并在 2009 年创立了比特币社会网络, 开发出第一个区块, 称为“创世区块”[2]。区块链, 即(交易/数据)块(Block)的链(Chain), 也称为价值互联网[3], 本质上是一个对等网络的分布式账本数据库(交易), 是一串使用密码学相关联而产生的数据块, 每笔交易均经过系统大多数参与者的一致认可, 在参与方之间发生和共享。区块链技术首先被应用于比特币当中, 比特币区块链也是目前规模最大、应用范围最广的区块链。

一个完整的区块链系统包含了很多技术, 其中有存储数据的数据区块及其之上的加密、数字签名、时间戳等技术, 有作为支撑的 P2P(Peer to Peer, P2P)网络和维护系统的共识算法, 有采矿和工作量证明

通讯作者: 张武雄, 博士 研究生, 副研究员, Email: wuxiong.zhang@mail.sim.ac.cn
本课题得到国家自然科学基金(No.61471346, No.61461136003); 上海市自然科学基金(No.17ZR1429100); 国家重点研发计划专项(No.2016YFC0801805); 上海市科技创新行动计划(No.17511105903, No.17DZ1200302)资助。
收稿日期: 2017-10-16; 修改日期: 2018-02-04; 定稿日期: 2018-02-05

机制, 有匿名交易机制和比特币钱包, 还有链龄、UTXO(Unspent Transaction Output)、Merkle 树、双重花费等相关技术概念。正是这些技术, 使得区块链在分布式的网络上形成了运转不息的引擎, 为区块链上的交易、验证、链接等功能提供了源源不断的动力。也许比特币在未来显得不是那么重要, 但是区块链技术在金融界和非金融界中的作用不容忽视。Patel 等学者[4]提出了区块链技术如何运作的整体观点、指出其改变企业现在以及未来发展方式的作用。

对于区块链, 以参与方式进行分类, 可以分为: 公有链(Public Blockchain)、联盟链(Consortium)和私有链(Private Blockchain); 以链和链的关系进行分类, 可以分为: 主链和侧链。此外, 不同区块链还可形成网络, 网络中链与链的互联互通, 产生互联链(Interchain)。区块链分类关系如图 1 所示。

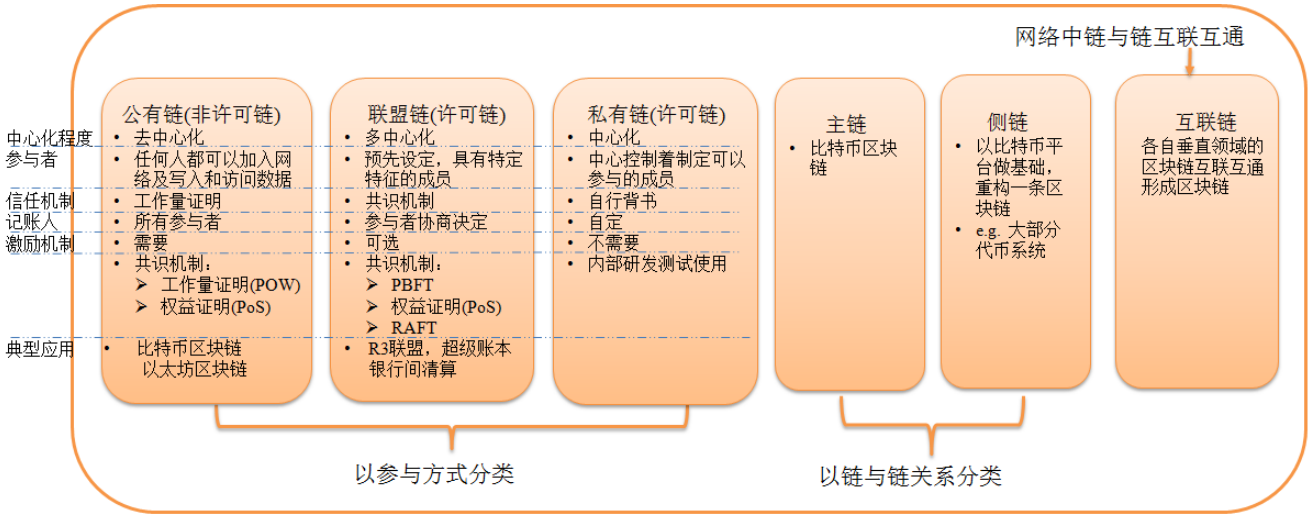


图 1 区块链的分类

Figure 1 Blockchain Classification

目前, 区块链以其特有的安全性, 已在许多领域中得到应用。然而, 进一步对其网络安全的研究似乎不太受到关注, 与为数众多的区块链应用成果相比, 其网络安全的研究成果发表不多。因此, 本文针对区块链数据的完整性、不可否认性、匿名性与隐私保护的安全需求, 广泛地检索并调研各类文献, 系统分析区块链的安全威胁与防御技术。

本文后续组织结构如下, 第二节研究区块链的安全攻击与威胁, 第三节综述区块链安全保护技术, 尤其对区块链密码学安全防护技术进行了对比分析, 最后总结了全文的工作。

2 区块链安全威胁

本节中, 我们将针对区块链存在的安全问题以及攻击威胁开展分析, 主要围绕以下几个方面: 区块链数据的完整性、不可否认性、匿名性与隐私保护以及其它安全问题。

2.1 区块链数据完整性威胁

本小节调研了区块链, 尤其是比特币面临的主要安全攻击, 综述了相关的文献研究情况, 并分析安全攻击对数据完整性的影响。其中, 本文对于完整性(Integrity)的定义参照了 ISO 25010[5]。

2.1.1 双重花费攻击

双重花费攻击(Double Spending Attack)是针对比特币系统的一种特有攻击。该攻击分为两种类型: 1)攻击者使用一笔金额, 同时和多个对象进行交易。若这些交易对象在这笔交易未被记录进合法区块链的情况下, 完成了交易, 则攻击者达到了双重消费[6]甚至多重消费的目的。尽管在攻击者发起的多笔交易中, 最终只会有一笔交易认定为合法并记录入区块链中, 但交易对象完成了交易(如已经把攻击者购买的货物发给攻击者), 攻击者已经从这次攻击中受益。2)攻击者利用自身的算力发起双重花费攻击: 攻击者利用同一笔金额, 同时和两个交易对象进行交易 A 和 B。其中一笔交易 A 被确认记录进区块链, 使得交易 A 完成。由于攻击者拥有强大的算力, 他将交易 B 记录在私人区块链里, 并挖出一条比合法连更长的链, 促使交易 B 也得到了确认, 并完成交易 B。

在双重花费攻击中, 第二种类型攻击的危害性更大。这是由于, 对于第一种类型攻击, 交易者只需要在交易得到确认 6 次以上, 再完成交易就可以避免; 对于第二种攻击, 由于攻击者将“非法”交易加

入私人区块链, 并且最终这条链被认定为合法, 相当于更改了区块链中的这笔交易(将交易 A 更改为交易 B), 这种对区块链数据进行篡改的行为严重影响了区块链的完整性。

2.1.2 自私采矿攻击

自私采矿攻击(Selfish Mining Attack)[7, 8]是针对区块链的一种典型攻击。由于挖取像比特币这样的加密货币, 对于一个矿工(Miner)来说, 需要高计算能力来解决密码难题(即工作量证明), 因此采矿变得十分困难。鉴于此, 一组矿工(Mining pool, 采矿池)通常会相互组合起来, 并在成功解决密码难题之后, 分享收到的奖励。这样有助于个体矿工在单独采矿时, 产生较连续恒定的收入, 而不是很少的收益。Eyal 和 Sirer 认为[7]如果存在一群自私的矿工, 采用自私的采矿战略, 并获得成功, 就可能会使诚实矿工的工作无效。这种自私采矿攻击表现为: 一个恶意的采矿池决定不发布它发现的块, 进而创建一个分叉, 因此, 网络中就存在由诚实矿工维护的公共链和恶意采矿池的私人分叉, 恶意采矿池在此私人分叉下继续进行挖掘, 当私人分叉比公共链长的时候, 恶意采矿池就发布该私人分叉, 由于该分叉是当前网络中最长的链, 因此会被诚实的矿工认定为合法链, 所以, 原公共链及其包含的诚实数据将被丢弃。研究结果表明, 一般情况下恶意采矿池采用自私采矿策略将获得更多的收益。

2.1.3 日蚀攻击

作为比特币系统信息交互的重要支撑, P2P 网络采用节点间广播来发布比特币信息, 日蚀攻击(Eclipse Attack)[9], 或称掩蔽攻击, 正是利用这种广播特性进行攻击。在比特币系统中, 攻击节点随机选择 8 个其他对等节点, 并保持长时间的传输连接, 用于传输和存储有关其他对等体的信息。由于具有公共 IP 的节点最多可以接收来自其他 IP 节点 117 个未经请求的入站连接(Incoming Connection), 攻击者“策略性”地控制受害节点所有信息的接收与发送, 使得受害节点的入站连接数量达到上限, 从而阻止其他合法节点的连接请求。其攻击行为表现为, 攻击者不断向上述 8 个对等节点发出请求, 并且发送大量无用的信息, 直到这些对等节点重新启动; 而这些对等节点即使重新启动后, 也将首先收到攻击者连接请求与无用信息, 进而被比特币系统“隔离”出来, 导致受害节点的采矿工作无效, 从而达到攻击目的。

一般意义上, 该攻击是指攻击者入侵并恶意修改节点的路由表, 将足够多的恶意节点添加到该节点的邻节点集合中, 从而将该节点恶意“隔离”于正常网络之外, 因此, 日蚀攻击也称为“路由表毒化”。当某个节点遭受日蚀攻击时, 其大部分对外数据交互都会被恶意节点所劫持, 由此恶意节点得以进一步实施后续的攻击, 诸如: 路由欺骗、存储污染、拒绝服务(Denial of Service attack, DoS)以及 ID 劫持等。

2.1.4 扣块攻击

扣块攻击(Block Withholding Attack)[10]是区块链的典型攻击之一。在扣块攻击中, 某些已加入联合采矿池的恶意成员不布任何挖到的区块, 从而降低了采矿池的收益, 浪费了其他成员提供的算力。这种攻击也被称为“破坏(Sabotage)”攻击, 通常恶意矿工不会有任何收益, 但 Courtois 和 Bahack 通过实际的实例分析, 发现恶意矿工也可以从这种攻击中获利[11]。扣块攻击的主要危害是浪费矿池算力资源, 减少矿池收入。

从上面的分析可以看出, 扣块攻击会使矿工和采矿池都受不同程度的损失, 相对于矿工很低的成本, 采矿池的损失则比较大。从利益方面考虑, 发起扣块攻击多为互相竞争的采矿池, 一般矿工则较少。尽管扣块攻击理论上成立, 但是实际上实施该攻击却很难。这是因为, 扣块攻击的代价非常大, 这一点与比特币的 51%攻击相似, 即发起该攻击必要的基础是需要掌握巨大的算力, 所以基本上扣块攻击在现实中极少发生。

2.1.5 贿赂攻击

典型的贿赂攻击(Bribe Attack)的流程如下[12]: 首先, 攻击者购买某个商品或服务, 商户开始等待网络确认这笔交易; 若此时, 攻击者开始在网络中首次宣称, 对目前相对最长的不包含这次交易的主链进行奖励; 当主链足够长时, 攻击者开始放出更大的奖励, 奖励那些在包含此次交易的链条中挖矿的矿工; 当六次确认达成后, 放弃奖励; 最后, 当货物到手时, 放弃攻击者选中的链条。

因此, 只要此次贿赂攻击的成本小于货物或者服务费用, 此次攻击就是成功的。值得注意的是, 该攻击对 PoW(Proof of Work)机制基本无效, 因为在 PoW 机制中, 贿赂攻击就需要贿赂大多数矿工, 因此成本极高, 难以实现。

2.1.6 其他潜在的攻击威胁

除了上述几种较为典型的安全攻击外, 区块链还面临着其他若干种安全攻击的威胁, 如丢块攻击(Block Discarding Attack)、历史修复攻击(History-Revision Attack)等。

Bahack[13]指出, 与普通节点相比, 具有良好网

络连接的攻击者更容易发起块丢弃攻击(Block Discarding Attack)。攻击者将多个具有良好网络连接的节点置于网络中, 使其具有网络连接优势, 进而不但可以方便地获知新被挖掘的区块, 也可以比其他节点更加快速传播某个区块。在此攻击中, 当攻击者挖出新区块时, 先不公布, 一旦得知任何合法节点公布区块时, 攻击者便立即发布自己的采矿块, 并且利用布置好的节点快速地播报到整个网络, 使得该合法节点开采的区块被丢弃。块丢弃攻击带来的威胁十分巨大, 攻击者不仅浪费了合法节点的算力资源, 而且可以选择地记录某些交易(每个区块大小有限, 因此每个区块记录的交易数目有限), 从而使得另一些重要合法交易的确认被延误。

Feld 等学者[14]研究表明, 比特币系统中, 若对等节点所连接的大部分对等节点都位于同一个自治系统, 则意味着 P2P 网络连接不良。在这种情况下, 添加新的区块到区块链中可能存在困难。若有攻击者发起类似这样的攻击, 则将使得分布式共识的实现变得十分困难, 区块链数据的合法性与完整性将无法得到保障, 这将给区块链的正常运行带来严重的灾难。

Dev 等学者[15]通过研究发现, 攻击者即使没有很强大的计算能力, 但是如果控制了大量节点, 就可以在小型区块链系统中使得总体计算能力相对比较强大。在这种情况中, 攻击者会故意制造分叉, 进行攻击, 严重威胁到系统的完整性。

Barber 等学者[16]指出了另一种攻击, 称为历史修复攻击。它们指出, 在攻击者拥有诚实节点的计算能力的倍数(例如, 攻击者算力为所有诚实节点算力总和的两倍)的情况下, 能够产生一个可以超越当前区块链长度的新链, 新链会被其他矿工接受, 从而改变了区块的“历史”。

Gervais 等学者[17]的研究结果表明, 攻击者通过将区块或交易延迟传递到比特币 P2P 网络中的其他节点, 也可以达到攻击目的。这个攻击带来的威胁如下: 1)如果攻击者能够阻止诚实矿工开采的区块被传递给网络中的某部分, 相比自私采矿攻击, 这种攻击将会给攻击者带来更多收益; 2)如果攻击者控制了多个节点, 可以阻止信息在网络中的传播, 从而导致某些服务被拒绝, 也就是 DoS 攻击。

Nayak 等学者[18]描述了一个自私采矿的扩展, 即固执采矿(Stubborn mining)。它们的结果表明, 在某些情况下, 对攻击者来说, 相对于自私采矿, 固执采矿会给它们带来更多好处。

作为另一种典型的公有区块链, 以太坊(Ethereum)也同样面临着多种安全攻击的威胁。除了上文所提到的双重花费攻击、DoS 攻击外, 针对以太坊的攻击还有 DAO attack, 51%攻击等。其中, DAO attack 的命名来源于 2016 年 6 月 18 日, 针对最大众筹项目 The DAO 的安全攻击[19]。攻击者通过 The DAO 编写的智能合约中 splitDAO 函数漏洞, 反复使用自己的 DAO 资产来不断从 The DAO 项目的资产池中分离 DAO 资产给预先设定的独立的团组 child DAO, 最终, 导致 300 多万以太币资产从 The DAO 资产池中被分离出来。51%攻击, 是指攻击者具备全网的 51%算力, 并持有大量虚拟币, 所发动的攻击(该攻击同样威胁比特币系统)。攻击过程简述如下: 把虚拟币转到交易所或某个机构或个人, 卖出所有上述币, 并将收到钱、提现到银行账号; 用 51%算力从还没向交易所转币的区块开始重新生成区块, 由于攻击者持续拥有 51%算力, 因此所生成的攻击块链一定能追上原块链; 当攻击块链的长度超过原块链 2 个区块, 所有的客户端将丢弃原块链, 接受攻击块链。至此, 51%攻击成功。据报道, 2016 年 8 月 26 日以太坊平台 Krypton 遭受 51%攻击, 损失 21465 个 KR 代币, 价值 3000 美元。同期, 以太坊代币 Shift 也遭受到同样的攻击[19]。调用深度攻击(Call Depth Attack)[20], 由于以太坊中调用栈深度是有限的, 若攻击者发起一系列的递归调用, 使得栈深度到达 1023, 进而任何调用失败, 即使该调用是完全可信且正确的。

此外, 庞氏骗局也是针对以太坊的安全威胁, Rubixi 就是一个此类的合约。这是一个欺诈性的高收益投资计划[21,22], 参与者从新投资者的投资中获得收益。 此外, 合约的持有者可以收取一些费用, 在投资时支付给合同。攻击者利用了“不可改变的漏洞(Immutable bugs)”漏洞, 从合约中偷取一定数量的 Ether。

从上面的分析可以看出, 改进和增强区块链完整性仍然是任重道远的挑战性任务。针对这些挑战, 产业界和学术界已经开展了大量尝试性的研究工作, 从算法、协议、系统和实现等方面提高了区块链的完整性, 为区块链系统的长期稳定运行奠定了基础。

2.2 区块链的匿名性与隐私保护威胁

尽管区块链可以实现隐私保护, 但是实际上它是伪匿名的, 也就是说, 仍然存在可能将不同的交易和地址联系起来, 从而找到其中的对应关系。当用户发出多个地址作为输入的交易时, 攻击者就可能会揭露这些地址和用户的对应关系。

Spagnuolo 等学者[23]、Herrera 等学者[24]和 Moser 等学者[25]均指出, 依据同一交易的多重输入地址均

属于发起该多重输入交易的用户, 从而找到了地址和用户的对应关系。在比特币系统里, 用户有时候将比特币发送到属于自己的特定地址, 这个行为称为更改地址。这些研究学者依然能够将这个用户的特定地址链接到其本人的其他地址。

除此之外, 还有一些针对安全攻击的研究也揭露了区块链的隐私安全威胁。Feld 等学者[26]和 koshy 等学者[27]从分析网络流量为出发点, 提出了一种能够将比特币地址与 IP 地址相关联的方法。而 Moser 等学者[25]和 Bahack[12]则使用集中的服务器来跟踪同一个用户的多个地址或者用户的真实身份, 该用户的地址就存在匿名性风险。

进一步, 我们根据文献中提到的去匿名技术(De-Anonymization Techniques)对进行了分类, 归纳总结以下四种类型: 多个输入(Multiple inputs), 更改地址(Change address), 与IP关联(Associations with IP)以及集中式服务的使用(Usage of centralized services)。如表 1 所示。

表 1 去匿名技术分类总结

Table 1 Classification of De-Anonymization Techniques

去匿名方法(技术)	文献
Multiple inputs	[23], [24], [25]
Change address	[23], [24], [25]
Associations with IP	[26], [27]
Usage of centralized services	[12], [25]

由表 1 可以看出, 区块链的伪匿名已经被研究者所发现, 并且有很多学者在关注研究如何从区块链的伪匿名性当中找到去匿名的方法, 也就是说得到真实的对应关系。由此可见, 区块链的匿名性以及隐私安全正面临着严重的威胁。

2.3 其他安全威胁

我们知道, 缺乏信任是跨组织业务流程整合的障碍。Weber 等学者[28]坚持认为, 区块链可能是一种用于在不信任网络中, 对数据共享进行安全保障的新兴技术。他们开发了一种将块链整合到流程编排中的技术, 该技术的核心是基于信任, 不需要中央权力机构。

同时, 也有一些研究人员试图解决区块链存在的某些缺陷, 特别是可扩展性问题。McConaghy 等学者[29]描述了 BigchainDB, 它将分布式数据库(Distributed Database, DD)与区块链特征相结合。因此, 它不仅具有分布式数据库的特点: 吞吐量和容量的线性缩放, 有效的查询和许可, 也具有区块链特征: 分布式, 不可篡改性。Dennis 等学者[30]提出了一个解决可扩展性的方案, 期望能对所有基于区块链的系统可扩展性有所改善。在这个方案中, 为了解决当前区块数量需求指数增长的问题, 它们提出了时间“滚动”区块(Rolling blockchain)的概念, 即区块的大小随着时间的推移而逐渐变大, 而非现在一直采用固定大小的区块。在此区块链中, 只有存储了预设时间段的数据才会包含在区块链中; 任何比这段时间更早的数据将被自动删除。滚动区块链通过在区块链网络上部署完全分散且不受信任的检查点, 创建一个自我删除和自我管理的区块链。与以往区块链可伸缩性问题的解决方案不同, 在滚动区块链中, 矿工不需要下载所有的共识, 并手动删除“花费块”(Spent block)。在这里, 花销块是没有交易的块, 可以在新块中用作输入。目前, 从本地存储的块链中除去这些花费的唯一方法是手动搜索区块链, 并将其从本地区块链中删除。该方案的优点是, 不再需要任何节点来存储来自第一个“创世”区块的区块链历史, 且删除数据不会对区块链数据的安全性造成影响。

此外, Croman 等学者[31]研究了区块链在支持较高吞吐量和较低延迟方面的瓶颈。它们依据研究结果指出, 区块大小和间隔应当视为实现下一代区块链的首要考虑点。此外, 它们从底层到顶层, 网络, 共识, 存储, 视图和侧面平面等级的依赖关系这五个层面讨论了区块链的可扩展性。

目前, 区块链的增长仍然存在某些技术瓶颈与障碍。Donet 等学者[32]研究指出, 弱连接和不正确的协议将会增加 IP 网络中的传播延迟, 并致使某些系统中的区块链分叉。尽管区块链是一个完全分散的系统, 但在实际中很难建立均匀的节点间连接。例如, 利用比特币中的邻居发现, 推荐志愿者的某些 IP 地址作为用户的连接选项。这些志愿者通常被称为 DNS 种子节点, 它们作为基础设施来帮助正常用户彼此通信, 但是它们的存在, 增加了超节点存在的可能性, 并带来了附加的不安全因素, 如欺诈和单点故障。此外, TCP / IP 协议不提供本地化的多播支持, 这必然导致数据传输开销的增加。

从以上的分析可知, 攻击者对区块链的攻击主要分为如下两个方面: 1)攻击者利用自身强大的算力进行的攻击。这些强大的算力为发起攻击提供了有利的支持, 如双重花费攻击、自私采矿攻击等等, 这些攻击不仅给区块链数据的完整性造成了安全威胁, 甚至对区块链系统的整体安全、正常运行都构成了严重的威胁; 2)攻击者利用协议的漏洞进行攻击。例

如, 新被挖到的块在网络中需要被广播到全网以达成共识, 攻击者可以利用广播新块与接收新块的传输过程进行攻击。

3 区块链安全保护技术

目前, 数字经济是依赖某一受信任的权威机构, 也就是说, 我们所有的在线交易都依赖并信任这一权威机构所提供的事实真相。例如, 电子邮件服务提供商告知我们电子邮件是否已经交付; 认证机构告知我们某个数字证书是否值得信赖; 社交网络(如Facebook、微博等)告知我们生活事件的帖子只与我们的朋友分享; 再或者网上银行告知资金已经可靠地支付给了对方。

事实上, 仅依靠第三方的可信实体为数字资产安全与隐私保护提供安全保障是远远不够的, 不但黑客入侵, 操纵或可信实体妥协将会造成个人数据与隐私泄露, 以及财产和名誉的损失, 而且更有甚者, 若某些较高机密的信息泄露将导致社会混乱。区块链技术可以较好地解决这一问题, 它通过分布式共识与匿名性, 不但可以将任何涉及数字资产的在线交易进行验证。而且可以较好地保护交易各方的隐私[33]。

当前, 针对区块链安全性的研究, 各国学者主要关注于完整性, 隐私保护和可扩展性等方面。2016 年 4 月, Hurlburt 在“区块链可能生存于比特币之外吗? ”一文中指出, 区块链在成为传统交易数据库的常见替代品之前, 需要遵守道德规范和操作指导性, 需要具有严格的标准, 要准备阐述行为准则等, 这引发了对区块链安全保护的广泛讨论。Zyskind 等学者[34]指出, 区块链的安全性可以通过内嵌式设计实现: 首先, 它通过共识来管理大多数网络节点, 使任何节点都难以改变其状态, 从而保持不变性。其次, 它使用加密和数字签名来保护数据并验证交易的真实性, 同时, 通过检查特定用户是否是区块链上特定资产的合法所有者, 以验证区块链的真实性。下面就结合相关文献研究, 综述区块链的现有安全防护。

3.1 区块链完整性保护机制

对于第二节所述的攻击, 一些文献已经给出了相应的防御对策。例如, 对于自私的采矿攻击, Eya[7]以及 Heilman[35]提出了防御措施: 为了减少恶意采矿池中诚实节点的数量的比例, 矿工可以决定延伸哪个区块。由此, 可以得出这样的结论: 区块链系统中若恶意矿工拥有较大比例的计算能力, 那么将对区块链完整性构成较大的安全风险, 这是由于这些恶意矿工可能会生成虚假的区块链分叉, 进而导致分布式共识难以实现, 甚至造成某些历史信息的丢失。此外, 这些恶意矿工还可能会使用无效的数据或交易来污染区块链。值得庆幸的是, 对于比特币系统这样的大型的、稳定的区块链而言, 由于工作量证明的复杂性以及大量诚实矿工的存在, 恶意矿工想要获得高比例的计算能力是很困难的, 因此可以一定程度上避免这种安全风险。除此之外, 通常比特币系统通过诱人的奖励机制鼓励矿工们的诚实工作, 然而, 初始化某个全新的区块链, 要保证不存在大量的恶意节点是很困难的, 即使结合社会经济因素, 这也不是完全可行的。鉴于此, 我们不建议从零开始设计一个全新的区块链, 而尽量在已有的比特币系统或某个安全稳定的区块链上, 利用分层架构来开发构建物联网的分布式应用程序, 该程序的附加功能可以在区块链顶上层定义。此外, 由于区块链隐藏在应用层, 所以不需要综合性能较低的 IoT(Internet of Things)设备来计算 PoW。通过这种方式, 借助于比特币系统或者相应稳定区块链的安全性, 以及绝大部分节点诚实性, 可以一定程度上确保新构建的区块链应用的数据完整性以及隐私性。

此外, 区块链通常采用“最长链原则”(Longest Chain Rule)应对某些分叉攻击, 即若出现多条区块链分支, 所有节点将最长链视为主链添加新块。但是, “最长链原则”也带来了一些问题, 这些问题包括, 位于其他分支上的区块成为无效区块; 区块中包含的交易将被延迟确认; 有可能面临双重花费的风险。此外, 为了确定一个新区块是否在主链上, 通常要求该区块后面连接足够多的区块才能确认有效, 但“最长链原则”并未解决该问题, 而且在使用“最长链原则”过程中, 用户确认交易完成的时间通常是不可接受的, 这也是区块链需要重点解决的问题。

3.2 区块链匿名性和隐私保护技术

比特币系统的区块链技术本质上并不完全是匿名的。这些交易永久记录在公开分类账本中, 每个用户不但可以看到余额, 而且可以获取与任何比特币地址相关的交易信息。因此, 用户在交易或任何特殊情况下显示出来的特定信息(如, 比特币地址等), 都可能使用户的真实身份和个人隐私暴露。为了保护高级别的用户隐私和维护更好的匿名性, 比特币系统鼓励用户持有多个比特币地址来经行交易, 并支持用户可以任意地生成新的交易地址。

从表 1 可以看出, 由于区块链是公开的, 攻击者可以通过分析网络流量或区块链本身来对用户进行去匿名化。尽管有研究表明, 假名机制可以一定程度保障匿名性, 但其中映射关系的时效性决定了其不

足以保证完全匿名。有研究[15, 36-39]相应地提出了去匿名对策。在[37-39]文献中, 学者们分析并给出了混合机制, 其主要技术思路是, 用户从一个地址发送一些比特币, 并用难以发现同一用户的输入和输出地址之间的对应关系的方式将这些比特币放进另一个地址。Barber 等学者[16]描述的公平交换协议也是基于上述混合机制, 并允许双方安全地交换比特币。Axon[36]提出了一种密钥更新方法, 能够让用户更新公钥, 并使这个公钥与系统中的 ID 不存在关联。此外, Thomas 和 Alex 的系统中详细地描述了基于区块链的访问控制管理, 以权限控制的方式来保护匿名性。Chain Anchor 系统可以为那些试图获取许可的区块链执行事务的实体, 提供匿名性支持, 同时可验证其身份。Hardjono 和 Smith 提出使用增强隐私 ID(Enhanced Privacy ID, EPID)的零知识量证明方案, 来提升区块链用户的匿名性。

目前, 针对区块链隐私保护的方法, 总结起来主要有两类: 一个是通过诸如“保密传输”之类的技术向现有的区块链添加匿名保护机制。另一种可能的方法是创建与比特币系统不兼容的新的区块链, 例如 Zerocash, 通过在其区块中使用新的原语来提供匿名性, 特别是零知识的“简洁的非交互知识”(SNARKS)[40]来提供更为增强的匿名性。尽管许多机构宣称通过某种混合方案来增加隐私权, 但不同用户的比特币交易需要依靠第三方来混合在一起, 这并不总是安全的或有益的[41]。一些更加深思熟虑的通用技术, 例如 Coin join(联合多个付款)和保密交易已经被创建了, 以获得更好的匿名保证, 匿名创建的软件, 如 Mimblewimble 声称实现非常强大的匿名属性, 但是破坏了与比特币的兼容性。

实际上, 一些更加具有前瞻性的技术已经陆续被研究(如, Coin join 方案等), 以期获得更好的匿名保证。目前, 尽管某些提供匿名功能的软件(如, Mimble wimble)声称能够帮助区块链用户实现非常强大的匿名属性, 但是该软件无法与比特币系统兼容。此外, 针对数据隐私, 功能性加密(Functional cryptography)技术被广泛地研究, 以属性基加密(Attribute-based Encryption, ABE)为代表的新一代加密技术为保障区块链隐私提供了另一种选择。具体来说, 属性基加密是一种通过将属性表示的(通常采用布尔函数)安全策略用于加密数据, 每个用户按照身份(可分解为一组属性)分配密钥, 只有用户身份满足加密数据中的策略时, 解密才能得以实现。这种基于策略和属性表示的加密方法非常有利于区块链中数据按照等级分类或定制方式进行隐私保护。

至今, 我们尚未调研到某个兼容比特币系统, 且被广泛接受和采纳的匿名解决方案。针对比特币区块链上匿名技术的第一次大规模研究是从[42]开始的, 我们希望未来的工作将继续研究区块链记录的匿名性, 研究分析新的匿名机制, 实现真正的匿名, 从而保护区块链的用户隐私安全。

3.3 区块链密码学技术安全保护技术

3.3.1 Hash 函数

分布式货币设计的主要问题是如何管理网络节点之间的共识, 区块链也面临同样问题(如, 若用户恶意更改并广播区块内容等)。这些问题引出了比特币的工作量证明制度, 简单的说, 任何想要将添加区块到链中的用户首先必须做大量的工作, 产生一个工作量证明。尽管生产某个工作量证明需要大量的计算能力, 但验证该工作量证明却十分容易, 网络中的任意节点都可以轻松地验证新产生的区块是否合法, 某种意义上, 这也防止恶意用户操纵区块链, 从而保证区块链的完整性。

在比特币区块链中, 加密哈希函数使用的是 SHA-256, 哈希字节为 32 字节。由哈希函数的特性可知, 输入数据的微小改变将会大大地改变其哈希值, 通常情况下, 没有节点可以创建两个不同的数据块, 使得它们具有相同的哈希值。因此, 对于一组哈希值, 可以确认它只匹配某特定的输入数据。

比特币系统采用 Hashcash 成本函数。 Hashcash 是第一个支持安全有效验证的成本函数或工作证明函数。其优点在于它是非交互式的, 不需要由中央服务器产生和管理密钥, 因此 Hashcash 是完全分布的且可无限可扩展的(Hashcash 使用对称密钥加密, 即单向 Hashcash 函数, 通常是 SHA1 或 SHA-256)。Hashcash 难度因子通过要求散列输出具有多个前导零来实现, 例如, 让十六进制的目标值为 00000fff。所以为了解决工作难题的证明, 我们需要找到一个随机数, 当附加到消息时产生小于 00000100 的哈希值, 即以 6 个零开始。在比特币区块链中, 确保区块完整性与区块的链接, 以及 Hashcash 成本函数, 都使用 SHA256 作为底层加密哈希函数。

哈希函数主要用来完成认证消息、数据完整性以及数字签名的验证, 能够保障区块链数据的不可篡改性与完整性, 保护了信息的安全。但是, 理论上任何密码学都不存在绝对的安全, 因此, 一些新的、更具安全性的算法也陆续被研究并被提出来。对此, 我们将首先给出哈希函数的描述, 再综述其最新的研究进展。

1) 哈希函数定义和性质

在密码学中, 哈希函数又称为单向散列函数, 它可以将任意长度的消息散列为固定长度的哈希值。哈希值也被称为消息摘要、数字指纹、密码校验和、信息完整性的校验码、操作检验码等等[43]。哈希值对输入消息非常敏感, 如, 对字符串“Shanghai Wireless Communication”用 MD5 生成的“指纹”为: “f224814068cfc79cc5ae5ef07c10f35c”。如果对该字符串中的字符稍加改动, 则会获得截然不同的“指纹“结果, 如, 在“Shanghai”中增加了一个空格, 变为“Shang hai”, 即对字符串“Shang hai Wireless Communication”利用 MD5 生成的哈希数字“指纹”为: “3cd624853b1aca4afe9c1a62451af139”。

通常, 一个安全的哈希算法需要满足如下三个性质:

a) 抗原像攻击(单向性): 对于任意给定的哈希值, 根据哈希值推导出原消息是计算不可行的。

b) 抗第二原像攻击: 对于任意给定的消息, 要找到另外一个消息, 使得计算得到的哈希值相同是计算不可行的。

c) 抗碰撞攻击: 要找到两个相同的消息, 使得它们计算得到的哈希值相同是计算不可行的。

在这里, “计算不可行”也可视为“计算困难”, 是从计算复杂性角度给出的概念, 可以理解: 所需要计算资源在时间和空间等维度上, 超越了现有可获得的资源。

进一步, 一个性能优异的哈希算法将能实现:

- 正向快速: 给定消息和哈希算法, 在有限时间和有限资源内能计算出哈希值。
- 逆向困难: 给定(若干)哈希值, 在有限时间内, 很难(基本不可能)逆推出原始消息。
- 输入敏感: 原始输入信息的微小改变, 产生的哈希值看起来都应存在很大不同。
- 冲突避免: 很难找到两段内容不同的消息, 使得它们的哈希值一致(发生冲突)。

冲突避免又被称为“抗碰撞性”。如果给定一个消息前提下, 无法找到碰撞的另一个消息, 称为“弱抗碰撞性”; 如果无法找到任意两个消息, 发生碰撞, 则称算法具有“强抗碰撞性”。除此之外, 许多应用场景下, 要求对于任意长的输入内容, 输出定长的哈希结果。

2) 哈希函数分类

从安全证明的角度, 哈希函数可分为可证安全哈希函数和非可证安全哈希函数。可证安全哈希函数, 是基于复杂性理论的设计思路来构造的哈希函数, 此类哈希函数都能进行安全性的证明, 但是效率不高。非可证安全哈希函数, 即不能给出安全性证明的哈希函数, 实际中使用的哈希函数(又称为专门的哈希函数), 就属于此类。专门的哈希函数效率很高, 适合在十几种应用, 但是缺乏安全性证明, 时刻存在着被攻击成功的危险。

本文后续所讨论的哈希函数正是这一类专门哈希函数。现有的专门哈希函数都没有具体的安全证明, 只有一个安全性猜想(即假定是安全的), 这类函数的最大优点是效率非常高, 从某些实时应用的角度讲, 这类哈希函数还是具有一定吸引力的。

3) 哈希函数的研究进展

在实际中大量应用的哈希函数, 主要分为三个子系列: MD 系列、RIPEMD 系列和 SHA 系列。

a) MD 系列

1989 年, Rivest 首先提出 MD2 算法, 随后他又对其进行了改进, 1990 年提出了 MD4 算法, 1992 年提出了 MD5 算法。其中, MD4 设计原则采用 Merkel-Dagard 迭代结构思想, 而 MD5 是 MD4 的强化版。1992 年, Zheng 提出了 HAVAL 算法, 相比 MD4、MD5, 该算法使用了 5 个具有优良特性的布尔函数, 具有可变输出长度, 以及可变轮数。

b) RIPEMD 系列

RIPEMD 系列包括 RIPMD, RIPEMD-128, RIPEMD-160 等多种具体算法。其中, RIPEMD (RACE Integrity Primitives Evaluation Message Digest) 是欧洲计划 RIPE(RACE Integrity Primitives Evaluation)选定的标准, 后续 RIPEMD-128、RIPEMD-160 对其进行了安全性改进。

c) SHA 系列

与 MD4 算法相比, SHA 系列的设计更注重安全性, 它增加了消息预处理, 使用消息扩展替换了 MD 系列里的消息置换。该系列主要包括以下三类算法:

SHA-1: 它于 1995 年面世, 其输出为长度 160 位哈希值, 抗穷举性更好。其设计原理与 MD4 相同, 其安全性高于 MD5 算法, 但运行效率相对较低, 且已被证明不具备“强抗碰撞性”。

SHA-2: 为提高安全性, 美国国家标准与技术研究所(NIST)设计了 SHA-224、SHA-256、SHA-384 和 SHA-512 算法(统称 SHA-2), 其设计原理与 SHA-1 算法类似。

SHA-3: NIST 于 2007 年 11 月面向全世界公开征集安全高效的哈希算法[44], 在长达五年的公开竞赛之后, 2012 年 10 月 2 日, NIST 宣布由 Guido Bertoni,

Joan Daemen, Michal Peeters, Gilles Van Assche 提出的 Keccak 为胜出算法[45], 即 SHA-3。

对于如 MD5、SHA0、SHA-1、RIPEMD 等这几种当前被广泛使用的哈希函数, 密码分析者都已经能在较短的时间内有效地找到碰撞[46-49]。目前还没有针对 SHA-2 完全的攻击碰撞, 但是存在局部的攻击碰撞[50]。SHA-3 Keccak 比其他散列函数更安全, 因为 Keccak 使用随机排列结果的海绵结构, 拥有良好的加密性能以及抗解密能力[51]。目前, 一般认为 MD5 和 SHA-1 已经无法为区块链提供足够的安全保障, 推荐至少使用 SHA-256 算法。

3.3.2 非对称加密

非对称加密机制在区块链中有着十分重要的应用。在比特币系统中, 每个比特币与其当前所有者的公共 ECDSA(Elliptic Curve Digital Signature Algorithm)密钥相关联。当用户向某个对象发送一些比特币时, 该用户将创建一个消息(事务), 将对象的公钥附加到这些比特币上, 并使用该用户的私钥进行签名。当这笔交易广播到比特币系统时, 全网便知道这些比特币的新拥有者是该公钥的所有者。交易的完整历史由系统中每个节点保留, 任何用户在任何时候都可以验证谁是某特定比特币的当前持有者。

为了保持区块链信息的完整性, 链中的每个区块确认了前一个区块的完整性, 一直回溯并确认到创始区块。记录插入或是篡改区块信息的代价是巨大的, 因为每个块的生成都需要花费巨大的计算资源, 且具有前后的相关性。这样一来, 任何用户都不能通过分支链来覆盖以前的记录,这确保了区块的完整性。

非对称加密机制可以很好地解决对称加密所需要的提前分发密钥问题。加密体系中, 加密密钥和解密密钥分别称为公钥和私钥, 公钥是公开的, 任何用户均可获取的, 私钥一般是用户自己持有, 不能被他人获取。非对称加密机制的优点是公钥与私钥分开, 即使在不安全通道仍可使用; 其缺点是加/解密速度较慢, 通常, 与对称加/解密算法相比, 非对称加/解密算法要慢两到三个数量级, 而且其加密强度相比对称加密要差。

非对称加密算法的安全性往往需要基于数学问题求解来保障, 例如, 基于大数质因子分解、离散对数、椭圆曲线等的几种思路, 多用于签名场景或密钥协商, 不适于大量数据的加解密。目前, 非对称加密的代表算法包括: RSA、ElGamal、椭圆曲线(Elliptic Curve Cryptosystems, ECC)系列算法, 具体描述如下:

1) RSA

经典的公钥算法, 1978 年由 Ron Rivest、Adi Shamir 和 Leonard Adleman 三位学者共同提出。该算法的设计利用了对大数进行质因子分解困难的特性, 但目前尚未有数学证明两者难度等价, 未来或许存在某种未知算法, 在不进行大数分解的前提下解密。

2) Diffie-Hellman 密钥交换

利用了基于离散对数无法快速求解的特性, 可以在不安全的通道上, 双方协商一个公共密钥。

3) ElGamal

由 Taher ElGamal 设计, 该算法利用了模运算下求离散对数困难的特性。被广泛应用在 PGP 等安全工具中。

4) 椭圆曲线算法

ECC 算法在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出, 它基于对椭圆曲线上特定点进行特殊乘法逆运算难以计算的特性。该系列算法一般被认为具备较高的安全性, 但加解密计算过程往往比较费时。

当前, 普遍认为 RSA 算法等已无法提供足够的安全性, 一般推荐采用 ECC 系列算法。在比特币区块链中, 就采用 ECC 系列算法生成加密的比特币地址等信息, 同时, 建立了公钥加密体制。

3.3.3 加密技术在区块链中应用

加密技术在区块链中的典型应用之一就是“数字签名”。数字签名是一种用于证明数字消息或文档真实性的数学方案, 为通过非安全通道发送的消息提供了一层验证和安全性保障。数字签名的正确实现使得接收者有理由相信该消息是由被请求的发送方发送的。目前, 应用于区块链中信息不可否认性的数字签名技术主要包括以下几种。

1) 聚合签名

Boneh 等学者提出基于 co-GDH 和双线性映射的聚合签名(Aggregate Signature)机制[52], 该机制支持聚合行为, 其中, 聚合是将给定来自 n 个不同用户的 n 个不同的消息上的 n 个签名, 汇总成一个简短的签名。这个单一签名(n 个原始消息)将使验证者确信这 n 个用户确实签署了 n 个消息(如, 用户 i 从 i=1 到 n 对消息 M_i 进行签名)。通常, 在区块链中, 聚合签名具有以下性质: 给定签名 σ 的验证者以及所涉及的各方的身份以及它们各自的消息来确保每个用户都签署了它们各自的消息。

2) 群签名

群签名(Group Signature)机制由 Chaum 等学者首

次提出[53], 随着后续的优化与完善, 其安全性和效率都有了不同程度的提高, 如 Boneh 等学者提出的基于双线性映射的短群签名机制[54]。群签名机制允许群组中的成员匿名地代表群签名消息, 其构成的安全要素必须遵循以下几个要点:

- 可靠性和完备性: 群成员的有效签名始终验证正确, 无效签名总是无法验证。
- 不可伪造性: 只有该组的成员才能创建有效的群签名。
- 匿名性: 给定一个消息及其签名, 若没有群管理者的密钥, 就无法确定私人签名者的身份。
- 可追溯性: 给定任何有效的签名, 群管理者能够跟踪是哪个用户签发了该签名。
- 无关联性: 给定两个消息和它们的签名, 第三方无法确定签名是否来自同一个签名者。
- 无框架: 即使所有其他小组成员(和管理人员)勾结, 也不能为非参与小组成员签字。
- 不可伪造的追踪验证: 撤销管理员不能错误地指责签名者创建他没有创建的签名。
- 抗联合攻击性: 组成员的勾结子集不能生成组管理员不能链接到共谋组成员之一的有效签名。

由于区块链应用场景的差异, 群签名机制的执行效率就变得非常重要。如上文所提出的短群签名机制中, 其签名大约是标准 RSA 签名的大小(大约 200 字节), 因此具有较好的适用性。通常, 群签名机制的执行效率可以通过群签名的长度、公钥的尺寸、签名生成及验证的时间等指标来评估。

3) 环签名

Rives 等学者提出基于 RSA 算法的环签名(Ring Signature)机制[55], 该机制主要思想是, 在一个集合 U 上使用所有用户的公钥和任意一个集合 U 上用户的单个私钥所构成的签名机制。典型的环签名机制的技术特性是: 验证者可以确信这个签名确实由集合 U 上的一个私钥产生, 但是却无法追踪到具体是哪一个私钥所产生的, 这个特性被称为签名者歧义[56]。与群签名不同, 环签名没有群管理者, 没有设置程序, 没有撤销程序, 也没有协调。任何用户都可以选择包括其自身在内的任何可能的签名者, 并使用自己的私钥和其他用户的公钥而不需要对方的批准和协助, 上述特点也符合区块链技术的去中心化要求。此外, 环签名可应用于区块链匿名支付的场景中, 具有交易的不可追踪性, 签名人处于完全匿名的状态, 对信息需要长期保护的一些特殊环境中有显著的使用价值, 需要说明的是, 任何环签名的大小必须与环的大小成线性正相关, 这是由于它必须列出所有环成员, 这对于那些计划使用预定义群的签名机制的区块链是不利的。

4) 盲签名

Chaum 等在学者基于密码学中大数因子分解、离散对数以及椭圆曲线等问题, 提出了盲签名(Blind Signature)机制[57]。它可以通过常规的数字签名机制与原始非盲的消息进行公开验证。其特点是消息在被签名之前便被伪装起来, 通常应用于发送者隐私具有高度重要性的情况下, 如用于与隐私有关的协议中签名者和消息作者是不同的人。而在区块链应用中, 盲签名多用于的加密选举系统和数字现金计划等。

尽管盲签名可以将消息 m 隐藏伪装, 但是对于 RSA 盲签名来说, 通过欺诈方式来解密另一条通过盲签名的消息, 使得它可能遭受 RSA 盲化攻击威胁[58]。这是因为, 盲签名过程相当于用签名者的密钥进行解密, 攻击者 A 可提供一个通过签名者的公钥来为它们提供一个盲消息 m 的加密版本, 造成欺诈。

5) 代理签名

代理签名(Proxy Signature)机制[59]允许一个被指定的签名者(通常称为: 代理签名者), 来代表一个原始签名者。本质上, 代理签名是基于密码学中离散对数问题的签名机制。与普通数字签名机制的连续执行相比, 代理签名具有直接的形式, 验证者在验证阶段不需要原始签名者以外的用户的公钥; 性能方面, 则需要较少量的计算工作。未来在面向物联网的区块链中, 具有一定的应用前景。针对上述签名机制, 其安全性、以及性能对比见表 2。

目前, 面向区块链的安全需求, 基于传统的数字签名机制, 一些适用于区块链技术特性的数字签名技术成为研究热点, 近期提出的较有代表性的数字签名算法表述如下:

Zhu 等学者提出了可以保障所有者的信息不可伪造和交易人信息不可否认的交互式数字签名协议 IIS(Interactive Incontestable Signature)[60]。与传统交易签名比较, 该签名技术有如下不同:

- 无论所有者还是交易者均能够自己产生公钥或私钥。
- 生成签名的过程是一个交易者和所有者两个部分间的交互证明过程。
- 签名的认证同时要求双方提供公钥, 这意味着此签名获得了双方的认可。
- 每个区块中的证明是唯一的, 并且在该区块中的所有事务中共享, 这在所有事务和该区块之间建立了强大的成员关系。

表 2 区块链中数字签名机制对比分析

Table 2 Comparison and Analysis of Digital Signature SCHEME in Blockchain

签名机制	原理	安全性	性能
聚合签名	基于 co-GDH 和双线性映射	在约束条件下, 即仅在不同消息上的签名进行聚合行为才有效, 聚合签名具有抵御攻击者伪造签名的能力	聚合签名的认证时间和签名数成线性关系, 在特殊情况下, 当所有 n 个签名由同一个公钥 k 发布时, 聚合验证速度更快
群签名	基于不可否认签名	可靠性和完备性; 不可伪造性; 匿名性; 可追溯性; 无关联性; 无框架; 不可伪造的追踪验证; 抗联合攻击性	公钥长度、签名长度与群成员数成线性关系, 但是新增成员需要重启整个系统, 故性能相对较低
环签名	群签名的变形, 拥有基于 RSA 和基于拉宾版本的两种环签名	攻击者即使拥有所有成员的私钥也无法找到谁是具体签名者, 因为确定真正签名者的概率为 $1/n$(n 为整个环成员数), A 无法从各种不可忽略的概率中产生消息 m 的环签名	签名过程需要一个模幂运算, 对于每个非签名者加上一个或两个模乘运算, 而验证过程需要每个环成员一个或两个模乘运算。由于其生成或验证环签名的开销, 与常规签名加上为每个非签名者加上一或两次额外的乘法开销是相同的, 故即使当环包含数百个成员时, 该机制依然高效可行
盲签名	基于 RSA 或 DSA 算法	若签名者不是消息的发送方, 则盲签名可以通过盲化将消息 m 隐藏起来, 签名者无法得知消息的内容, 从而保护消息的隐私	取决于密钥长度、签名长度和签名和验证时间, 尽管其基于的算法理论存在差异, 但总体上与 RSA 签名或 DSA 签名机制的开销量类似
代理签名	基于离散对数问题	由于离散对数问题存在的固有问题, 使得代理人可以伪造原始签名进行安全攻击, 以及发生替换公钥等安全问题	由于离散对数的运算问题, 所以该机制在计算复杂度和通信开销等方面, 均劣于基于椭圆曲线问题的签名机制

该签名机制提供了对所有参与者的不可伪造性与不可抵赖性, 并解决了保证不可否认性的即时确认问题。

田海博等学者提出了基于传统的可验证加密签名和盲签名思想所构建的盲的可验证加密签名(Blinded Verifiable Encrypted Signature, BVES)机制[61]。由于在交易的过程中区块链的每一个节点都可以读取交易数据, 来验证所交易的数据是否是正确的, 但是交易数据中涉及了隐私的内容, 于是, 既要公开验证, 又要保护隐私。他们基于所提出的签名机制, 构造了公平且保密的合同签署协议, 既能够让合约的签署人通过区块链完成公平的合同签署, 又能保护与合同相关的隐私内容。

Sato 等学者分析了当底层加密算法(哈希功能和数字签名)发生妥协时, 对区块链的信息安全的影响[62], 他们指出当 SHA256 发生妥协时, 会造成电子货币被盗、双重支付和完成协议的失败; 当 RIPEMD160 发生妥协时, 会造成支付的否认; 当 ECDSA 发生妥协时, 会造成货币被盗和发送虚假警报声称未收到支付; 哈希函数和数字签名机制产生妥协现象并相结合时, 会导致交易被否认、货币被盗、双重支付和改变现有的交易。

为了解决以上区块链中的安全问题, Aitzhan 等学者提出了利用类似 ETSI 标准, 并且不需要可信第三方(TTP Trusted Third Party)机制的长期签名机制[63]。鉴于现存的长期签名机制是为了 PKI(Public Key Infrastructure)模型所设计的, 并假定存在可信第三方颁发的时间戳令牌。而在长期签名机制中, 时间信息对于管理公钥证书的有效性和撤销具有重要意义。然而, 在比特币或其他公有链的应用场景下, 数字签名验证中不需要准确的时间信息; 同时, 他们指出比特币或其他公有链与 PKI 之间的信任模型和系统模型均不同, 因此, 现存的长期签名机制无法直接应用到区块链中。尽管当签名机制发生妥协时, 无法避免钥匙对和硬分叉(Hard fork)的出现, 但是通过他们提出的协议, 可以利用附加区块链, 在一定的时间内(几年内)进行过渡调节。

Yuan 等学者提出了一种在区块链大数据交易环境下基于聚合签名算法的新签名机制[64]。该机制充分考虑了椭圆曲线离散对数问题和双线性映射的重要作用, 分析了包括 Dash 中的 CoinJoin, Monero 环签名以及 Zcash 中的零知识证明, 研究了有利于密钥保护和提高区块链性能的加密技术(如椭圆曲线加密技术(ECC)[65], 双线性映射和聚合签名), 在此基础上, 提出了一个面向区块链交易的新型签名机制。该机制特别适用于金额将被隐藏包含多个输入和输出的交易中, 由于交易中恒定的签名大小, 可以有效地提高签名的性能。该机制在安全性方面等价于传统的双线性聚合签名, 安全分析也与[20]中关于聚合签名的分析相同, 可以间接证明此机制具有不可伪造性。

此外, Sheshasaayee 等学者研究并提出怎样保障交易中的通信安全, 以便在不同的情况下辨认捏造和篡改行为[66]。最新的数字签名分析详见表 3。

在密码算法方面, 大量新型密码技术能被用于区块链平台和应用系统的构造, 为区块链在未来应

表 3 区块链中数字签名机制最新研究对比

Table 3 State of the Art of Digital Signature Scheme in Blockchain

签名机制	原理	安全性	性能
不可否认的交互式数字签名(IIS)	基于双线性映射群系统的椭圆曲线对	可以保障所有者的不可伪造性和交易者的不可否认性	利用线性群的指数次数和元素长度计算复杂度和通信/存储成本两方面说明方案性能
盲的可验证加密签名(BVES)	基于盲签名和可验证签名	通过设置安全定义的三个方面, 分别验证满足假设, 其具有抵御欺诈的能力, 以此证明方案的安全性	分别从区块产生时间和通过公平合同签署协议的通信花费来评估签名和协议的性能
类似 ETSI 下长期签名的新签名方案	基于 ETSI 长期签名方案	当签名方案发生妥协现象时, 此方案可以避免密钥对的改变和 hard-fork	开销方面, 在改变哈希算法时, 区块大小的开销取决于新散列函数的输出长度和块中交易数(交易的哈希值之间的相互引用数量)
在区块链交易环境下基于聚合签名所提出的新签名方案	基于椭圆曲线离散对数问题和双线性映射	根据安全分析, 攻击者的潜在伪造能力无法实现, 安全性能和聚合签名基本相同	通过聚合签名时间、聚合验证时间和签名空间大小来进行评估

用中的安全奠定了坚实的理论基础。例如, 随着 SHA-1 哈希碰撞已被发现, 建议以此构建的区块链系统尽快更换为第二代及以上哈希函数来保证区块链的完整性和一致性。以目前“天河二号”的算力来说, 发现一个 SHA256 哈希碰撞可能需要上百年, 随着 SHA-3 的广泛应用, 其状态空间比 SHA-2 增加了 2~4 倍, 极大地增加了攻击难度。未来, 随着量子计算时代的到来, 后量子密码(Post-quantum Cryptography)设计已经提上了日程。近年来一些抗量子计算攻击的哈希函数方案也已经被提出, 可保障未来量子计算时代区块链系统的安全。

随着区块链应用越来越广泛, 原有基于加密技术的单一数字签名机制已无法满足区块链信息不可否认性的安全需求, 从近几年相关领域的研究分析可以看出, 两种以及以上签名机制的融合是未来一段时间内的技术发展趋势。

目前, 区块链的应用多面向单一领域, 未来的区块链系统的互联互通将成为必然的趋势, 随之而来的是, 密码技术将面临着更多的挑战, 尤其是对于跨平台的密钥管理, 如密钥的生成、密钥的分发等方面。

3.4 P2P 网络

P2P 是一种分布式通信模式, 其中每个节点具有相同的能力, 并且任一方可以发起通信会话。由于区块链本质上是分布式的分类账本, 因此 P2P 网络模式是比特币系统运作的基础。它为区块链提供了如下的技术优势:

1) 防止单点攻击

尽管当网络中某个节点丢失而导致数据丢失, 但其它节点仍然保留该数据副本, 因此并不会造成整个网络中该数据丢失;

2) 较强的容错性

即使某些节点出现故障, 也不会对整个网络造成损害, 因为有多个信息来源可用;

3) 较好的兼容性与可扩展性

可以轻松适应越来越多的节点, 并适应网络配置的频繁变化。

比特币区块链中, 节点负责运行维护整个比特币系统。节点通过一种发送事务的机制, 更新区块链, 并有效地将信息传递到网络上的每个节点。该发送事务机制中, 实现信息的全网发布就是采用了“绯闻协议”[67], 即任意节点都将数据发送给它所知道的每个节点, 并从这些节点接收数据, 然后所有的节点依据它们收到的数据更新相应的内容, 这样, 实现了信息在整个网络中有效传播。

3.5 共识机制

区块链的本质属性就是去中心化, 而去中心化的核心就是共识机制。通常, 共识机制就是区块链事务达到分布式共识的算法, 它用来使得区块链达到一致的状态, 它实现了驻留在网络的每个节点上的许多副本。共识机制应该将一个状态与其余状态分开, 以便该状态可被整个网络所接受。尽管密码学技术占据了区块链的半壁江山, 但是共识机制是保障区块链系统不断运行并不断发展的关键。本文将 10 种典型的共识机制描述如下:

1) 工作量证明(PoW)

在比特币区块链中, PoW 就是一份证明, 用来确认用户做过一定量的工作。其基本工作流程为:

- 节点监听全网数据记录, 通过基本合法性验证的数据记录将进行暂存。
- 节点消耗自身算力, 尝试不同的随机数, 进行指定哈希计算, 并不断重复该过程直至找到合理

的随机数。

- 找到合理的随机数后, 生成区块信息, 首先输入区块头信息, 然后是区块记录信息。
- 接着对外广播出新产生的区块, 其他节点验证通过后, 连接至区块链中, 主链高度加一, 然后所有节点切换至新区块后面继续进行工作量证明的区块产生。

实际上, PoW 是一种应对拒绝服务攻击和其他服务滥用的经济对策, 工作的整个过程通常极为低效, 需要大量计算资源, 而通过对工作的结果进行认证来证明完成了相应的工作量却是十分高效的。

目前, 使用 PoW 的项目有: 比特币、莱特币等货币型区块链, 以太坊的前三个阶段(Frontier 前沿、Homestead 家园、Metropolis 大都会)。而以太坊的第四个阶段 Serenity 宁静将采用权益证明机制(PoS)。

2) 股权证明(Proof of Stake, PoS)

股权证明(PoS)理念是节点记账权的获得难度与节点持有的权益成反比, 与 PoW 相比, 一定程度上减少数学运算带来的资源消耗, 性能获得相应的提升, 但依然是基于哈希运算, 竞争获取记账权的方式, 可监管性弱。

其本质是指根据虚拟货币的持有比率, 在散列计算中分配优先级的方法。它是 PoW 的一种升级, 根据每个节点所占代币的比例和时间, 等比例地降低挖矿难度, 从而加快找到随机数的速度。例如, 矿工持有比特币数量的1%以占据“股权证明”的1%[68]。这个工作量证明也存在非法控制区块链的几种攻击方式, 需要进一步研究相应的对策。

目前, 使用PoS的项目有: Bitshares和qutm等合约型区块链。

3) 股份授权证明(Delegated Proof of Stake, PoS)

基于PoS, BitShares(比特股)社区提出了DPoS机制[69]。它与 PoS 区别在于, 节点选举若干代理人, 由代理人验证和记账, 其合规监管、性能、资源消耗和容错性与 PoS 相似。类似于董事会投票, 持币者投出一定数量的节点, 进行代理验证和记账。工作原理由如下两个步骤组成:

- 成为代表: 必须在网络上注册公钥, 然后分配一个 32 位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。
- 授权选票: 每个钱包有一个参数设置窗口, 在该窗口里用户可以选择一个或更多的代表, 并将其分级。一经设定, 用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。

4) 投注共识(Casper)

投注共识(Casper)是一种以太坊下一代的共识机制, 与前三代的共识机制(PoW)不同, 投注共识属于PoS。它是按块达成, 而不是像 PoS 那样按链达成[70]。其工作过程包括: “出块”和“投注”两个活动。具体如下:

- 出块: 是一个独立于其他所有时间而发生的过程, 验证人收集交易, 当轮到它们的“出块”时间时, 它们就制造一个区块, 并签名, 然后发送到网络上。
- 投注: 目前 Casper 默认的验证人策略被设计为模仿传统的拜占庭容错共识: 观察其他的验证人如何投注, 取 33%处的值, 向 0 或 1 进一步移动。

为了防止验证人在不同的世界中提供不同的投注, 该机制还有一个简单严格的条款: 如果有客户两次投注序号一样, 或者说提交了一个无法让 Casper 合约处理的投注, 那么他将失去所有保证金。

5) 重要性证明(Proof of Importance, PoI)

新经币(NEM, New Economy Movement)将信誉作为重要性元素, 引入到分布式共识算法中。即只需要向整个经济体证明自己的重要性(信誉)来获取区块奖励。这样它也无须特殊的挖矿硬件, 能运行在一个树莓派设备上, 故省电环保, 有助于解决令人头疼的地球高碳排放带来的温室变暖问题。

本质上, PoI 是指通过交易图分析对节点进行聚类的方法。它使用各个节点的交易量和余额作为指标, 计算每个节点的重要性, 并将哈希计算中的优先级分配给更重要的节点, 集群可以检测某些可能进行非法交易的节点[71]。

6) 瑞波共识(Ripple Consensus)

该机制是一种数据正确性优先的网络交易同步机制, 它是基于特殊节点列表达成的共识。在这种共识机制下, 必须首先确定若干个初始特殊节点, 如果要新接入一个节点, 必须获得 51%的初始节点的确认, 并且只能由被确认的节点产生区块[72]。因此, 与前面几类共识机制相比, 该共识机制具有一定的“中心化”特征。其工作过程如下:

- 验证节点接收、并存储待验证交易。
- 活跃信任节点发送提议。
- 本验证节点检查收到的提议是否来自信任节点列表中的合法信任节点。
- 验证节点, 并根据提议确定认可交易列表。
- 达成账本共识。
- 共识过程结束后, 形成最新的账本。

7) 实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)

PBFT 是解决拜占庭故障导致失败而提出的拜占庭算法。由于该算法计算量大, 一度被认为难以将其应用于实际应用中。文献[73]提出了一种可以避免拜占庭故障, 在判断共识形成时, 增加一个较小滞后的实用算法, 叫做“41”。当前正在努力将该算法应用于区块链, 然而该算法必须知道节点总数, 并且需要设置非法节点的最大数量, 这样的技术要求使得其应用于公共区块链中。

PBFT 机制及其改进算法为目前使用最多的联盟链共识算法, 其改进算法侧重于以下方面: 修改底层网络拓扑的要求, 使用 P2P 网络; 可以动态地调整节点数量; 减少协议使用的消息数量。

8) 授权拜占庭容错(Delegated BFT, DBFT)

DBFT 是一种改进的拜占庭容错算法, 主要改进包括:

- 将 C/S 架构的主从模式改进为适合 P2P 网络的对等节点模式。
- 将静态的共识参与节点改进为可动态进入、退出的共识参与节点。
- 为共识参与节点的产生设计了一套基于持有权益比例的投票机制, 通过投票决定共识参与节点(记账节点)。
- 在区块链中引入数字证书, 解决了投票中对记账节点真实身份的认证问题。

DBFT 机制的核心, 就是最大限度地确保系统的最终性, 使区块链能够适用于真正的金融应用场景。

9) Paxos 算法

该算法是一种基于选举领导者的共识机制[74]。领导者节点拥有绝对权限, 并允许强监督节点参与。算法中将节点分为三种类型: proposer: 提出一个提案, 等待大家批准为结案; acceptor: 由客户端担任, 负责对提案进行投票; learner: 由服务端担任, 通常被告知结案结果, 不参与投票过程。其基本过程包括, proposer 提出提案, 先争取大多数 acceptor 的支持, 超过一半支持时, 则发送结案结果给所有人进行确认。

10) Pool 验证池

基于传统的分布式一致性技术加上数据验证机制, Pool(联营)验证池是目前行业内大范围使用的共识机制。其中, 表 4 综合分析上了以上 10 种典型共识机制的特性。

除了以上所述的几类常见共识机制外, 针对不同的区块链应用, 还存在着许多的依据特定业务逻辑自定义的共识机制, 如小蚁的“中性记账”、类似 Ripple 共识的 Stellar 共识机制、Factom 等众多以“侧链”形式存在的共识机制等。

表 4 典型的区块链共识机制

Table 4 Typical Consensus Schemes in Blockchain

名称	技术优势	技术不足
PoW	• 算法简单, 易于实现。 • 节点间无需交换额外的信息即可达成共识。 • 破坏系统需要投入极大的成本。	• 算力的消耗与浪费。 • 区块确认时间难以缩短。 • 新的区块链须找到一种不同的散列算法, 否则会面临比特币的算力攻击。 • 容易产生分叉, 需要等待多个确认。
PoS	• 对节点性能要求低。 • 达成共识时间短(可实现毫秒级)。	• 同 PoW 一样仍需要挖矿。 • PoS 会使得“富者更富”。 • 没有最终一致性。
DPoS	• 不需要挖矿产生区块。 • 大幅缩小参与验证和记账节点的数量, 属于弱中心化, 效率提高。 • 可达到秒级共识验证。	• 整个共识机制依赖于代币, 而很多商业应用不需要代币。 • 牺牲了去中心化的概念, 不适合公有链。
投注共识	• 引入惩罚机制。 • 有效抵御“51%”攻击。 • 理论上, 该共识模型中的出块时间甚至可比网络传播时间还要块。	• 由于该共识过程是在某个高度上对区块状态的决策是独立于其他所有高度的, 这将会导致一定程度的低效。
PoI	• 提供了一种分布更为均匀的挖矿方法。 • 解决比特币生态资源浪费与挖矿设备竞争。 • 看重交易量、活跃度, 以及和谁做交易。	• 仅适用于 NEM 用户。 • 对于 NEM 用户的重要性: 取决于他拥有多少数量的货币和他的钱包交互数量。

续表

名称	技术优势	技术不足
瑞波共识	• 保证任何时候都不会产生硬分叉。 • 交易能被实时的验证。	• 新加入节点要取得与其他节点的共识所需时间较长。
PBFT	• 系统运转可以脱离币的存在, 安全性与稳定性由业务相关方保证。 • 共识的时延大约在2~5秒钟, 基本达到商用实时处理的要求。 • 共识效率高, 可满足高频交易量的需求。	• 当系统仅剩33%节点运行时, 系统会停止运行。 • 当有 1/3 或以上记账人联合作恶, 且其他所有的记账人被恰好分割为两个网络孤岛时, 恶意记账人可以使系统出现分叉, 但是会留下密码学证据。
DBFT	• 专业化的记账人。 • 可容忍任何类型错误。 • 记账由多人协同完成。 • 每一个区块都有最终性, 不会分叉。 • 算法的可靠性有严格的数字证明。	• PBFT 机制的缺陷依然存在。
Paxos 算法	• 性能高, 资源消耗低。 • 所有节点一般有线下准入机制。	• 不允许有作恶节点。 • 不具备容错性。
Pool 验证池	• 不需要代币也可工作。 • 在成熟分布式一致性算法(Paxos、Raft)基础上, 实现秒级共识。	• 去中心化程度不如比特币, 适合多方参与的多中心商业模式。

3.6 其他安全保护技术

区块链是一个可加密验证的数据列表。区块链之所以广受关注的原因之一是, 数据库没有任何密码保密的完整性保护, 确保完整性对于在对抗环境中运行的任何数据库都是必需的保证。因此, 在任何环境下, 保障区块链的安全都是首要的任务, 本小节将从其他角度来分析区块链安全的研究现状。

众所周知, 故障(bug)会严重损害区块链系统的可靠性。例如, 攻击者利用了 DAO 项目(该项目是在以太坊区块链[75]上启动的)中的一个故障, 结果在2016年6月18日之前成功控制了约6000万美元, 直到后来采用硬分叉的方式丢弃了涉及攻击的交易。因此, 了解区块链故障特性, 进而设计出有效的工具来防止、检测和减轻故障, 是保证区块链正常运行的重要维护方式。鉴于此, Wan 等学者[76]对 8 个代表性的开源区块链系统中的故障特性进行了研究, 并给出了一些关于区块链故障的特点以及分布情况。他们手动检查了 1108 个故障报告, 了解了所报告故障的性质, 然后, 利用卡片排序来标记故障报告, 并在区块链系统中总结出了 10 个故障类别。此外, 他们还进一步调查了项目和编程语言的故障类别的频率分布, 并研究了故障类别和故障修复时间之间的关系。结果表示, 对于区块链的故障分析主要包括: (1)语义错误是主要的运行时故障类别; (2)不同项目和编程语言的故障类型的频率分布有相似趋势; (3)安全漏洞需要最长的中间时间来修复; (4) 35.71%的性能故障需要超过一年的时间才能修复; 性能故障需要最长的平均时间来修复。Wan 等学者的研究具有十分重要的意义, 因为了解故障特征可以帮助设计有效的工具来防止、检测和减轻故障。这样才能进一步地有针对性的设计手段来确保区块链的安全性。

区块链分布技术已经成为解决分布式系统中性能和安全问题的有效解决方案。区块链的基本共识机制允许构建防篡改环境, 其中任何数字资产的交易都由一组真实的参与者或矿工进行验证。区块链系统使用强大的加密方法, 将交易块链接在一起, 以使记录可回溯且不可改变。然而, 这个过程是仍存在某些问题, 即达成共识需要矿工的计算能力来换取丰厚的回报, 因而贪婪的矿工总是试图利用这个系统来增加它们的采矿能力。由于贪婪获利的存在, 在区块链中仍然存在一些漏洞。例如, Deepak 等学者[77]考虑了不同的奖励机制, 并在区块链云中模拟扣块攻击, 仿真结果发现, 若扣块攻击为区块云中的恶意矿工提供了充足的资源, 破坏了诚实的矿工采矿工作, 就能够使得攻击成功入侵。鉴于此, 它们讨论分析了区块链在云中如何提供有保证的数据来源的能力, 指出了区块链云中的漏洞, 并给出了相应的安全建议。

区块链平台(如, 以太坊等), 承诺在去中心化的计算平台上促成尚未建立信任的各方之间的交易。对此, 识别区块链编程的独特挑战激发了开发人员为区块链创建特定的变成语言, 如 Solidity。然而, 最近发现, Solidity 程序中的错误被利用来窃取交易资

金。因此, Coblenz[78]提出一种新的编程语言 Obsidian, 使程序员更容易编写正确的程序, 从而在根本上提供了一种确保区块链安全的可选择办法。过用户研究显示, Obsidian 能够避免一些常见的错误, 是区块链平台语言设计的一种未来的发展方向。

此外, 虽然区块链为参与者提供了一种在没有集中权限的情况下、在不可信网络中维护可靠的数据库的新方法, 然而, 在 IP 网络中的实际部署的区块链系统仍然存在许多严重问题, 例如, 缺乏对组播和状态等级的支持。为解决此类问题, Jin 等学者[79]在数据网络中设计了一个名为 BlockNDN 的比特币式区块链系统, 并在集群上实现与部署。这个设计不但有效地解决了 IP 网络中的上述问题, 而且提供完全分布式的系统, 简化了系统架构, 改善了弱连接现象, 降低了广播开销。

4 结论

区块链作为一种新兴的框架协议, 其与生俱来的数据安全性和有效的隐私保护, 使得区块链的行业应用越来越广泛。但值得注意的是, 随着其应用范围的扩展, 针对区块链不断涌现的各种新型安全威胁也越来越多, 如何加强对区块链的安全保护更是亟待进一步的研究。

但令人忧虑的是, 区块链自身的技术特性造成了对其安全性过度的信任与依赖。从目前调研的大量文献来看, 对于区块链的研究绝大多数都是围绕区块链的应用展开; 少部分文献关注区块链的安全攻击, 指出了区块链存在的一些安全威胁; 极少部分文献对区块链存在的一些安全问题给出了相应的解决方案。因此, 结合当前的研究现状, 笔者建议: 区块链作为一种尚未完全成熟的技术, 一方面, 在其应用的时候一定要结合具体的领域, 解决适用性的问题; 另一方面, 要正视区块链的网络安全和隐私保护仍然存在威胁, 现有的伪匿名技术无法达到对用户信息完全匿名保护, 建议后续可适当关注块链记录的匿名性研究等。希望本文的工作可以警醒同行, 区块链网络安全的未来之路依然很漫长, 同时, 可以有效地帮助区块链架构的安全优化与安全算法改进。

参考文献

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[2] “Bitcoin Blockchain Statistics,” [Online]. Available: https://blockchain.info/.

[3] 赵刚, 区块链：价值互联网的基石, 电子工业出版社, 2016.

[4] D. Patel, J. Bothra, V. Patel, “Blockchain exhumed,” in Proc. *ISEA Asia Security and Privacy (ISEASP)*, pp. 1-12, 2017.

[5] ISO/IEC. “ISO/IEC 25010 System and software quality models.” Tech. Rep, 2010.

[6] M. Rosenfeld, “Analysis of hashrate-based double spending,” arXivpreprint arXiv: 1402.2009, 2014.

[7] I. Eyal, E. G. Sirer. “Majority is not enough: Bitcoin mining is vulnerable.” *in Proc. Int’l Conf. Financial Cryptography and Data Security*. pp. 436-454, 2014.

[8] A. Sapirshtein, Y. Sompolinsky, A. Zohar, “Optimal selfish mining strategies in bitcoin,” in Proc. *Int’l Conf. Financial Cryptography & Data Security*, pp. 515-532, 2016.

[9] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, “Eclipse attacks on bitcoins peer-to-peer network,” *in Proc. the 24th USENIX Security Symposium (USENIX Security 15)*, pp. 129-144, 2015.

[10] M. Rosenfeld, “Analysis of bitcoin pooled mining reward systems,” Technical report, CoRR, 2011.

[11] N. T. Courtois, L. Bahack., “On subversive miner strategies and block withholding attack in bitcoin digital currency,” arXiv preprint arXiv:1402.1718, 2014.

[12] A Chepurnoy. “Interactive Proof-of-stake,” arXiv:1601.00275v2 [cs. CR], Jan 11,2016. [Online]. Available: https://arxiv.org/pdf/1601.00275.pdf

[13] L. Bahack, “Theoretical bitcoin attacks with less than half of the computational power （draft）,” Technical Report abs/1312.7013, CoRR, 2013.

[14] S. Feld, M. Sch¨onfeld, and M. Werner, “Analyzing the Deployment of Bitcoin’s P2P Network under an AS-level Perspective,” ANT/SEIT, ser. *Procedia Computer Science, vol.* 32, pp. 1121-1126, 2014.

[15] J. A. Dev, “Bitcoin mining acceleration and performance quantification,” in Proc. *IEEE 27th Canadian Conf. on Electrical and Computer Engineering (CCECE)*, pp. 1-6, 2014.

[16] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to Better - How to Make Bitcoin a Better Currency,” *in Proc. Financial Cryptography vol.* 7397 of LNCS, pp. 399–414, 2012.

[17] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the Delivery of Blocks and Transactions in Bitcoin,” *in Proc. ACM Conf. Computer and Communications Security*, pp. 692-705, 2015.

[18] K. Nayak, S. Kumar, A. Miller, and E. Shi, “Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack,” *IACR Cryptology ePrint Archive*, vol. 2015, p. 796, 2015.

[19] “Krypton Recovers from a New Type of 51% Network Attack.” [Online] https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack.

[20] “Smart Contract Best Practices,” [Online] https://consensys.github.io/smart-contract-best-practices/known_attacks/.

[21] “Etherscan: Rubixi code,” [Online] https://etherscan.io/address/0xe82719202e5965Cf5D9B6673B7503a3b92DE20be.

[22] “Bitcointalk: Hi! My name is Rubixi.” [Online] https://bitcointalk.org/index.php?topic=1400536.60.

[23] M. Spagnuolo, F. Maggi, and S. Zanero, “BitIodine: Extracting Intelligence from the Bitcoin Network,” in Proc. Financial Cryptography, vol.

8437 of LNCS, pp. 457–468, 2014.

[24] J. H. Joancomart´ı, "Research and Challenges on Bitcoin Anonymity," *in Proc. the 9th Int'l Workshop on Data Privacy Management*, pp. 3-16, 2014.

[25] M. Moser, R. Bohme, and D. Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem," [Online]. Available: https://maltemoeser.de/paper/money-laundering.pdf.

[26] S. Feld, M. Schönfeld, and M. Werner, "Analyzing the Deployment of Bitcoin's P2P Network under an AS-level Perspective," in ANT/SEIT, ser. *Procedia Computer Science*, vol. 32, pp. 1121-1126, 2014.

[27] P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in," *Financial Cryptography Bitcoin Using P2P Network Traffic*, vol. 8437, pp. 469–485, 2014.

[28] I. Weber, X. Xu, R. R. Riveret, G. Governatori, A. Ponomarev, J. Mendling, "Untrusted business process monitoring and execution using blockchain," *in Proc. Int'l Conf. Business Process Management*, pp. 329-347, 2016.

[29] T. McConaghy et al., "A scalable blockchain database," Bigchaindb-Whitepaper, 2016.

[30] R. Dennis, G. Owenson, B. Aziz, "A Temporal Blockchain: A Formal Analysis," *in Proc. Int'l Conf. Collaboration Technologies and Systems*, pp. 430-437, 2017.

[31] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer,, "On scaling decentralized blockchains," *in Proc. Int'l Conf. Financial Cryptography and Data Security*, pp. 106-125, 2016.

[32] J. A. D. Donet, C. P. Solà, and J. H. Joancomarti, "The Bitcoin P2P Network," *in Proc. Workshop on Bitcoin Research*, pp. 87-102, 2014.

[33] M. Crosby, N. Pan, P. Pattanayak, S. Verma, V. Kalyanaraman, "BlockChain Technology Beyond Bitcoin," *Sutardja Center for Entrepreneurship & Technology Technical Report*, Berkeley, 2015.

[34] G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *in Proc. Security and Privacy Workshops (SPW)*, pp. 180-184, 2015.

[35] E. Heilman, "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner," *IACR Cryptology ePrint Archive*, vol. 2014, p. 7, 2014.

[36] L. Axon, "Privacy-awareness in Blockchain-based PKI," 2015. [Online]. Available: http://goo.gl/3Nv2oK.

[37] L.Rowan, B. Valenta, "Blindcoin: Blinded, Accountable Mixes for Bitcoin," *in Proc. Int'l Conf. Financial Cryptography Workshops*, pp. 112-126, 2015.

[38] G. D. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-Resistant Mixing for Bitcoin," *in Proc. Workshop on Privacy in the Electronic Society*, pp. 149-158, 2014.

[39] S. Orlandi, C. Meiklejohn, "Privacy-Enhancing Overlays in Bitcoin," in Proc. *Int'l Conf. Financial Cryptography Workshops*, pp. 127-141, 2015.

[40] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza., "Zerocash: Decentralized anonymous payments from bitcoin," *in Proc. IEEE Symposium on Security & Privacy*, pp. 459-474, 2014.

[41] S. Meiklejohn, M. Pomarole, G. Jordan, K. evchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names.," *in Proc. Int'l Conf. Internet Measurement*, pp. 127-140, 2013.

[42] M. Möser, R. Böhme, "Anonymous alone? Measuring Bitcoin's second-generation anonymization techniques," *in Proc. EuroS&P Workshops*. pp. 32–41, 2017.

[43] 李志敏, 哈希函数设计与分析, 北京邮电大学, 2009.

[44] Kayser, F. Richard, "Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family," *Federal Register*, vol. 72, p. 62, 2007.

[45] "CSRC," [Online]. Available: http://csrc.nist.gov/groups/ST/hash/sha-3/winner_sha-3.html.

[46] X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD," *in Proc. the 24th Annual Int'l Conf. Theory and Applications of Cryptographic Techniques*, pp. 1-13., 2005.

[47] X. Wang, H. Yu, "How to break MD5 and other hash functions," in Proc. *the 24th Annual Int'l Conf. Theory and Applications of Cryptographic Techniques*, pp. 19-35, 2005.

[48] X. Wang, Y. L. Yin, H. Yu, "Finding collisions in the full SHA-1," in Proc. *the 24th Annual Int'l Conf. Theory and Applications of Cryptographic Techniques*, pp. 17-36, 2005.

[49] X. Wang, H. Yu, Y. Yin, "Efficient collision search attacks on SHA-0," *in Proc. of the 25th Annual Int'l Conf. Cryptology*, pp. 1-6, 2005.

[50] P Hawkes, M Paddon, GG Rose, "On Corrective Patterns for the SHA2 Family," *IACR Cryptology ePrint Archive*, 2004.

[51] "CSRC," [Online]. Available: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

[52] Dan B, Gentry C, Lynn B, H Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. in Proc. *Int'l Conf. on the Theory and Applications of Cryptographic Techniques*. pp. 416-432, 2003.

[53] Chaum D, Heyst E V. Group Signatures. in Proc. Advances in Cryptology — EUROCRYPT '91. pp. 257-265, 1993.

[54] Boneh D, Boyen X and Shacham H. Short group signatures. in Proc. Crypto, pp. 41-55, 2004.

[55] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret. in Proc. *Advances in Cryptology — ASIACRYPT*, pp. 552-565, 2001.

[56] Fujisaki E, Suzuki K. Traceable ring signature. in Proc. *Int'l Conf. on Practice and Theory in Public-Key Cryptography*. pp. 181-200, 2007.

[57] Chaum D. Blind Signature System. in Proc. Advances in Cryptology, *Proceedings of CRYPTO*, pp. 153, 1984.

[58] Shentu Q C, Yu J P. A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm[J]. *Computer Science*, 2015.

[59] Mambo M, Usuda K, Okamoto E. Proxy signatures for dele-gating signing operation. *in Proc. ACM Conference on Computer and Communications Security*. pp. 48-57, 1996.

[60] Zhu Y, Guo R, Gan G, Tsai WT. Interactive Incontestable Signature for Transactions Confirmation in Bitcoin Blockchain. *in Proc. Computer Software and Applications Conference*. pp. 443-448, 2016.

[61] 田海博, 何杰杰, 付利青. 基于公开区块链的隐私保护公平合同签署协议. *密码学报*, 2017, 4(2):187-198.

[62] Sato M, Matsuo S. Long-Term Public Blockchain: Resilience agai

nst Compromise of Underlying Cryptography. in Proc. IEEE European Symposium on Security and Privacy Workshops. pp. 1-8, 2017.

[63] Aitzhan N Z, Svetinovic D. Security and Privacy in Decen-tralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams. *IEEE Transactions on Dependable & Secure Computing*, 2016, PP(99):1-1.

[64] Yuan C, Xu M X, Si X M. Research on a New Signature Scheme on Blockchain. Security and Communication Networks, Volume 2017 (2017), Article ID 4746586, 10 pages, https://doi.org/10.1155/2017/4746586.

[65] Bos J W, Halderman J A, Heninger N, Moore J, Naehrig M, Wustrow E. Elliptic Curve Cryptography in Practice. *IN Proc. Financial Cryptography and Data Security*. pp. 157-175, 2014.

[66] Sheshasaayee A, Anandapriya B. Digital signatures security using cryptography for industrial applications. *in Proc. International Conference on Innovative Mechanisms for Industry Applications*. pp. 379-382, 2017.

[67] J. Leitao, J. Pereira, L. Rodrigues, "HyParView: A Membership Protocol for Reliable Gossip-Based Broadcast," *in Proc. IEEE/IFIP Int'l Conf. Dependable Systems and Networks*, pp. 419-429, 2007.

[68] "Proof of Stake," BitcoinWiki, [Online]. Available: https://en.bitcoin.it/wiki/Proof of Stake.

[69] Delegated Proof of Stake (DPOS) White Paper. [Online]. Available: http://www.bitsharestalk.org/index.php?topic=4009.0

[70] Ethereum.org 2.0 Mauve Paper: [Online]. Available: https://docs.google.com/document/d/1maFT3cpHvwn29gLvtY4WcQiI6kRbN_nbCf3JlgR3m_8

[71] "Survey on Blockchain Technologies and Related Services," Wikipedia, [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf.

[72] A. D. Luzio, A. Mei, J. Stefa. Consensus Robustness and Transaction De-Anonymization in the Ripple Currency Exchange System. *In Proc. IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp: 140-150, 2017.

[73] "Survey on Blockchain Technologies and Related Services," Wikipedia, [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf.

[74] A. Ailijiang, A. Charapko, M. Demirbas. Consensus in the Cloud: Paxos Systems Demystified. *In Proc. 25th International Conference on Computer Communication and Networks (ICCCN)*, pp: 1-10, 2016.

[75] "Ethereum blockchain," [Online]. Available: http://www.coindesk.com/understanding-dao-hack-journalists/.

[76] Z. Wan, D. Lo, X. Xia, and L. Cai, "Bug Characteristics in Blockchain Systems: A Large-Scale Empirical Study," *in Proc. IEEE/ACM 14th Int'l Conf. on Mining Software Repositories (MSR)*, pp. 413-424, 2017.

[77] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, L. Njilla, "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack," *in Proc. IEEE/ACM Int'l Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 458 – 467, 2017.

[78] M. Coblenz, "Obsidian: A Safer Blockchain Programming Language," *in Proc. IEEE/ACM 39th IEEE Int'l Conf. Software Engineering Companion (ICSE-C)*, pp. 97-99, 2017.

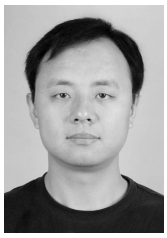
[79] T. Jin, X. Zhang, Y. Liu, K. Lei, "BlockNDN: A Bitcoin Blockchain Decentralized System over Named Data Networking," *in Proc. the Ninth Int'l Conf. Ubiquitous and Future Networks (ICUFN)*, pp. 75 - 80, 2017.

房卫东 山东济南人, 博士, 中国科学院上海微系统与信息技术研究所高级工程师, 主要研究方向为物联网/无线传感网可信传输技术、信任管理、隐私保护。E-mail: Weidong.fang@mail.sim.ac.cn

潘涛 江苏连云港人, 博士, 神华信息技术有限公司教授级高级工程师, 主要研究方向为矿山自动化、信息化、智能化。

杨旸 江苏南京人, 博士, 中国科学院上海微系统与信息技术研究所研究员、博导, 主要研究方向为无线传感器网络(物联网)、新一代移动通信系统(5G)、雾计算与网络技术, 开放无线测试验证平台。

张武雄 湖北孝感人, 博士, 中国科学院上海微系统与信息技术研究所副研究员, 主要研究方向为车联网体系架构及组网技术、异构多网协作。



陈伟 江苏徐州人, 博士, 中国矿业大学计算机科学与技术学院教授, 主要研究方向为智能信息处理、无线通信、大数据与云计算。