密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(5): 484–500

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

区块链技术专刊

区块链理论研究进展*

单进勇[1,2], 高 胜[1,2]

1. 数据通信科学技术研究所, 北京 100191
2. 兴唐通信科技有限公司, 北京 100191

通信作者: 高胜, E-mail: gs14011@163.com

摘 要: 区块链技术是一门新兴的技术, 受到各行各业的广泛关注. 各个国家正在积极研究区块链技术可能给金融乃至生活的方方面面带来的变革. 本文先从比特币区块链的视角出发, 通过了解它的运行机制、基本特征、关键技术、技术挑战等, 给读者建立一个对区块链的直观感受. 然后给出区块链的形式化定义, 并总结目前区块链在相关密码技术、安全性分析、共识机制、隐私保护、可扩展性等方面的最新研究进展. 密码技术是保障区块链安全的关键技术之一, 也是实现区块链具体应用的基本手段. 本文同时指出了多种密码技术如特殊数字签名、零知识证明、同态密码、安全多方计算等在区块链系统中的 (潜在) 应用价值. 尽管区块链技术的研究和应用发展迅速并取得很大进展, 但区块链所面临的诸如吞吐量低、延迟高、耗能高等一系列技术瓶颈, 严重影响大规模应用的真正落地, 区块链技术的研究和应用还有很长的路要走, 需要各方共同努力.

关键词: 比特币; 密码货币; 区块链; 共识协议; 可扩展性

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000258

中文引用格式: 单进勇, 高胜. 区块链理论研究进展[J]. 密码学报, 2018, 5(5): 484–500.

英文引用格式: SHAN J Y, GAO S. Research progress on theory of blockchains[J]. Journal of Cryptologic Research, 2018, 5(5): 484–500.

Research Progress on Theory of Blockchains

SHAN Jin-Yong[1,2], GAO Sheng[1,2]

1. Data Communication Science and Technology Research Institute, Beijing 100191, China
2. Xingtang Telecommunications Technology Co. Ltd., Beijing 100191, China

Corresponding author: GAO Sheng, E-mail: gs14011@163.com

Abstract: Blockchain is an emerging technology that has received an exceptional amount of attention from all walks of life. Many countries are actively studying how blockchain technology could change finance and even aspects of our lives. In this paper, by introducing the operating mechanism, basic features, key technologies, and technical challenges of the Bitcoin blockchain, we firstly build an intuitive feeling of blockchains for readers. Then we propose a formal definition of blockchains, and summarize the current research progress of blockchains in cryptography, security analysis, consensus,

* 基金项目: 国家重点研发计划 (2017YFB0802500)
Foundation: National Key Research and Development Program of China (2017YFB0802500)
收稿日期: 2018-07-28 定稿日期: 2018-09-27

privacy, and scalability. Cryptography is one of the key technologies ensuring security in blockchains, and is also the basic means to realize the specific applications of blockchains. In this paper, we also point out the potential application value of the various cryptographic techniques in blockchains, such as special digital signatures, zero-knowledge proofs, homomorphic ciphers, and secure multi-party computations. Although the research and application of blockchain technology has developed rapidly and made great progress, blockchain technology faces a series of technical challenges such as low throughput, high latency, and high energy consumption, which seriously affects its large-scale applications. Therefore, the research and application of blockchains still has a long way to go, and people need to work together.

Key words: Bitcoin; cryptocurrency; blockchain; consensus; scalability

1 引言

自 2009 年比特币系统 [1] 运行以来, 涌现出大量竞争性数字货币, 亦可称之为民间数字货币 (以区别于法定数字货币的概念). 这些竞争币 (如 Litecoin [2]、Zcash [3]、Monero [4] 等) 大都采用类似于比特币的基础架构, 并根据自身需求进行了适当优化. 据不完全统计, 截止 2018 年 7 月 25 日, 民间数字货币已达 1600 多种, 总市值约 3000 亿美元[1]. 同时, 民间数字货币的出现推动了各国央行对法定数字货币的研究, 如英国的 RSCoin [5], 加拿大的 Jasper 项目 [6], 新加坡的 Ubin 项目 [7] 等. 我国央行也早在 2014 年就成立了法定数字货币研究小组, 论证法定数字货币发行的可行性, 发表了多篇相关学术论文 [8–12], 并推出了电子票据交易平台原型系统. 区块链技术是比特币等民间数字货币的底层核心技术, 融合了 P2P 网络、共识机制、密码等关键技术, 具有去中心化、不可篡改、匿名性、可追溯性、开放透明等特点, 有着非常广阔的应用前景, 受到政府部门、金融机构、科技公司、学术界的广泛关注. 甚至有人认为, 区块链技术是继大型计算机、个人计算机、互联网、移动互联网之后的第五次计算变革, 是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第四个里程碑 [13].

虽然各个国家对待数字货币的态度不尽相同, 同一国家对待数字货币的前后态度也不尽相同, 但是各个国家对待数字货币的底层区块链技术的态度却是高度一致的, 先后出台了一系列鼓励区块链技术发展和应用的政策. 美国、欧盟、日本等发达国家正在积极推动区块链技术理论研究、标准制定、应用落地等相关工作. 国际上同时成立了不少区块链联盟, 如 R3 联盟、HyperLedger 等, 旨在推动区块链技术的理论和应用研究. 在我国, 区块链技术已经上升到国家科技战略层面. 2016 年 12 月,《国务院关于印发 “十三五” 国家信息化规划的通知》中首次提及区块链, 明确提出加强区块链等新技术的创新、试验和应用. 目前区块链的应用已延伸到社会管理、物联网、医疗健康、智能制造等多个领域.

密码技术是区块链的关键技术之一, 不仅关系区块链安全和效率, 也是实现区块链具体应用的基本手段. 区块链技术的发展, 将一些密码技术从幕后推到台前, 进一步促进了密码理论和应用的研究. 越来越多的密码学者开始关注并研究区块链相关密码技术. 一方面, 密码学者从区块链安全性分析、共识机制、隐私保护等具体应用需求开展特殊数字签名、零知识证明、同态密码、安全多方计算等密码算法和协议的研究工作; 另一方面, 密码学者又利用区块链去中心化、公开透明、不可篡改等特性构造安全多方计算协议、可公开验证的随机数种子等.

尽管区块链技术具有广泛的应用前景, 甚至被认为是一种颠覆性技术, 但是区块链也面临一些技术瓶颈, 如吞吐量低、延迟高等. 这些问题都严重影响了大规模区块链应用的真正落地. 区块链技术的理论研究和应用实践还有很长的路要走.

本文对区块链技术展开调研, 总结区块链技术的热点研究方向, 突出密码在区块链技术中的重要地位. 全文结构如下, 第2节介绍区块链相关术语. 第3节介绍比特币区块链的基本特征、关键技术以及面临的技术挑战. 第4节给出区块链的形式化定义. 第5节主要介绍区块链技术的研究和应用进展. 第6节给出总结和建议.

[1]数据来源: https://coinmarketcap.com.

2 相关术语

为了方便叙述, 本节列出一些常见的区块链相关术语. 需要说明的是, 作为一种新技术, 区块链的很多术语在不同的参考资料中略有不同, 理解上也可能略有不同. 这里我们尽可能给出明确定义, 并确保本文其他地方相同术语含义的一致性.

区块链 (Blockchain)

狭义地, 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 并以密码学方式保证的不可篡改和不可伪造的分布式账本. 广义地, 区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式 [14].

区块链分类

根据应用场景和参与者的不同, 将区块链分成三类: 公有链、联盟链和私有链.

公有链 (Public blockchain): 任何节点都可以自由加入和退出区块链系统, 都可以发送和确认交易, 都可以参与共识过程, 没有中心化的机构. 常见系统有比特币、以太坊等.

私有链 (Private blockchain): 只有单一组织拥有写入权限, 可以制定和修改区块链规则, 信息一般不公开. 私有链可用于协调企业内部各部门之间的工作.

联盟链 (Consortium blockchain): 介于公有链和私有链之间, 若干组织构成利益相关的联盟, 约定区块链规则. 节点的加入与退出需要联盟授权, 只允许有限的、经过授权的节点参与共识过程. 常见系统有 Corda、Fabric 等.

共识机制 (Consensus)

共识机制是参与者对某个提案达成一致意见的过程. 常用的共识机制主要有工作量证明 (proof of work, PoW)、权益证明 (proof of stake, PoS)、实用拜占庭容错 (practical Byzantine fault tolerance, PBFT) 等.

分叉 (Fork)

区块链系统升级时可能发生分叉. 对于一次升级, 升级过的节点称为新节点, 未升级的节点称为旧节点. 根据新旧节点相互兼容性上的区别, 可分为软分叉 (soft fork) 和硬分叉 (hard fork).

软分叉: 旧节点可能无法理解新节点产生的部分数据但是仍然会接受, 新节点也接受旧节点产生的交易和区块.

硬分叉: 旧节点不接受新节点产生的交易和区块, 新节点接受旧节点产生的交易和区块, 会因为新旧节点认可的区块不同分成两条链.

可扩展性 (Scalability)

可扩展性是指随着节点的增多, 交易量的增加, 区块链系统处理交易和达成共识的能力. 主要涉及吞吐量 (单位时间内处理的交易量) 和延迟性 (交易从提出到记入区块链需要的时间) 两个方面.

交易图 (Transaction graph)

交易图是指将地址作为顶点, 交易 (一个地址发送给另一个地址) 作为有向边, 构成的有向图. 可以通过交易图分析出交易之间的关联性, 甚至恢复出交易者的真实身份.

智能合约 (Smart contract)

智能合约是一种允许在没有第三方参与的情况下, 以代码方式形成、验证或执行合同的计算机协议. 最早可追溯到 1994 年 Nick Szabo 给出的定义: 一套以数字形式定义的承诺, 包括合约参与方可以在上面执行这些承诺的协议.

3 比特币区块链

区块链技术是中本聪设计比特币系统首次提出和使用的, 同时比特币也是区块链第一个成熟的应用, 因此为了本文更好地介绍区块链, 本节先介绍比特币区块链 [1,15], 让读者对区块链先有一个直观的了解.

比特币系统主要活跃两大类角色, 用户和矿工: 用户使用比特币进行交易, 矿工竞争挖矿, 争夺记账权, 产生区块链. 比特币区块链的具体结构见图1. 具体地, 每个区块是由区块头和区块体两部分组成, 其中区块头主要包含前一个区块的区块头哈希值、随机数 (IV) 等, 区块体则是一些具体交易的集合. 挖矿就是寻找随机数 IV 使得其区块头哈希值小于某个预先给定的值 (目标哈希值). 当目标哈希值很小时, 挖矿是一件非常困难的事, 需要搜索大量的随机数 IV, 目前比特币网络每产生一个区块大约需要进行超过 2^{70} 次的哈希运算. 竞争记账是指先找到合法区块的矿工, 通过 P2P 网络广播给其他矿工, 并得到其他矿工的认可, 该矿工就拥有这个区块的记账权, 也会得到由此产生的收益 (比特币). 比特币系统通过调整目标哈希值, 控制全网大约每 10 分钟产生一个区块.

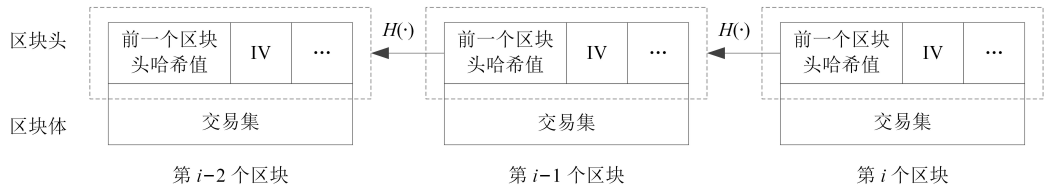

图 1 比特币区块链示意图
Figure 1 Structure of Bitcoin blockchain

图1表示当前网络有 i 个区块, 所有的矿工都在寻找第 $i+1$ 个合法区块 (每个矿工工作的区块是不同的). 如果某个矿工率先找到第 $i+1$ 个合法区块, 将其广播出去, 并得到全网节点的认可, 那么就意味着该矿工获得第 $i+1$ 个区块的记账权, 而其他矿工的工作无效, 紧接着所有矿工转到争夺第 $i+2$ 个区块记账权的竞赛当中. 如此这样, 每一个区块都包含上一个区块头的哈希值[2], 所有的区块构成一条区块链 (又称全网总账本).

3.1 基本特征

通过以上介绍, 梳理总结比特币区块链的基本特征如下:

去中心化: 任何节点的地位都是均等的, 任何节点都可以自由退出或加入比特币系统, 所有节点参与数据的验证、存储、传输和更新, 不存在中心化的节点或管理机构.

不可篡改: 一旦数据被记录到区块链中, 并经过多次确认之后, 所存储的数据就会永久存储起来, 除非能够同时控制全网总算力的 51% 以上. 此外, 比特币采用分布式存储技术, 每个节点都独立保存完整的区块链, 任何节点修改自己的区块链数据都是无效的, 因此区块链存储的数据稳定性和可靠性极高.

匿名性: 比特币系统通过比特币地址 (假名) 进行交易. 比特币地址无法和用户真实身份对应起来, 比特币地址对应的私钥是比特币所有权的唯一凭证. 因此比特币使用假名实现一定的匿名性.

可追溯性: 区块链记录了所有历史数据, 每一笔比特币都可以追溯其来源.

开放透明: 系统和区块链数据对所有节点开放, 任何人都可以通过公开的接口查询区块链数据和开发相关应用.

3.2 关键技术

比特币系统并不复杂, 但是涉及到了 P2P 网络、共识机制、密码等多个关键技术, 比特币区块链的基本特征都是由这些技术保证的.

P2P 网络

比特币采用 P2P 网络架构. 整个系统没有中心化的硬件或者管理机构, 任意节点之间的权利和义务都是均等的, 每个节点通过多播实现节点识别和数据传播等功能. 当发生交易或找到合法区块时, 可以通过 P2P 网络发送给每一个节点. 全网总账本是由全节点集体维护的, 每个全节点都能获得一份完整数据库的拷贝, 单个节点篡改账本是不可能的, 从而保证了比特币系统的安全性.

[2]区块链的这种连接方式, 和链表通过指针链接很类似, 所以通过哈希值将区块和前一个区块链接起来称为哈希指针.

共识机制

比特币系统是通过矿工竞争记账, 来维护全网总账本, 从而获得一定数量的比特币奖励. 为此, 矿工争相解决一种基于哈希函数的困难问题, 即寻找随机数 IV, 使得区块头的哈希值小于某个目标哈希值. 这个问题难于计算却易于验证, 并且当矿工提供这样的随机数 IV, 任何人都确信该矿工为了得到 IV 已经付出足够多的计算工作. 这个过程就称为基于 PoW 的共识机制. 之所以选择哈希函数设计困难问题, 还因为容易调整挖矿难度.

密码技术

比特币系统的安全性不是基于可信第三方和任何物理实体, 而是密码学原理. 事实上, 比特币使用的密码学技术都是相当成熟的, 具体算法采用的也是国际通用的标准算法, 如哈希函数 SHA256 是 SHA-2 算法簇中的一类 [16], 数字签名 ECDSA [17] 使用的椭圆曲线是 secp256k1 [18].

哈希函数在比特币区块链中主要用于区块的产生和共识过程. 这里主要介绍区块的产生. 图2是比特币区块的结构示意图. 哈希函数用于计算区块头的哈希值, 还用于生成 Merkle 树. 所谓 Merkle 树, 就是通过二叉树的形式将交易集合打包成一个哈希值 (Merkle 根), 其作用是快速归纳和校验区块数据的存在性和完整性.

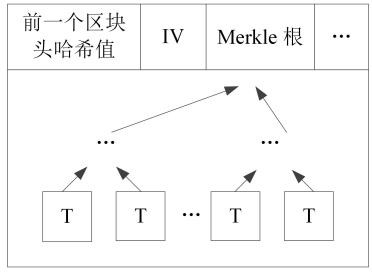

图 2 比特币区块结构示意图

Figure 2 Structure of Bitcoin blocks

数字签名在比特币系统中主要用于比特币的接收和花费. 图3描述的是比特币公私钥和地址之间的对应关系. 一般地, 我们可以将地址和公钥等同起来看, 因为地址和公钥都是公开的. 公钥 (或地址) 用来接收比特币, 私钥用来花费比特币. 由于比特币系统没有可信第三方, 也没有用户管理系统, 一方面公钥和用户真实身份无法对应起来, 从而实现一定的匿名性保护用户的隐私; 另一方面, 私钥是证明比特币所有权的唯一凭证, 私钥的产生、存储、使用需要格外谨慎.

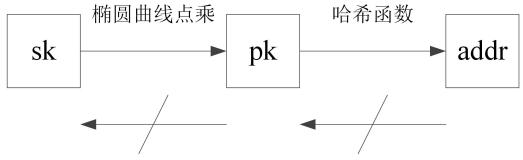

图 3 比特币私钥、公钥、地址关系图

Figure 3 Relationship of Bitcoin's private key, public key, and address

3.3 技术挑战

比特币区块链尽管有很多优点, 但是也面临一些技术挑战, 如可扩展性问题等. 不仅如此, 一些被认为是比特币区块链的优点, 针对具体应用场景也存在争议.

可扩展性问题严重影响比特币更广泛的使用, 主要存在以下问题: 第一, 吞吐量低. 理论上, 比特币系统每秒只能处理 14 笔交易[3], 这和银行等中心化系统每秒动辄需要处理上万笔交易相比, 相差甚远. 第二, 延迟高. 比特币系统中每笔交易至少需要 10 分钟才能被确认. 出于安全考虑, 大额交易甚至需要 1 个小

[3]按照每十分钟出一个区块, 区块的大小为 2 MB, 交易的大小为 250 B 计算.

时以上才能最终确认. 第三, 高耗能. 比特币在挖矿竞争中吸收了大量的算力资源, 需要消耗大量的能源. 最后, 存储空间大. 每个节点都需要独立备份完整的区块链数据, 占用较大的存储空间. 目前整个区块链数据已经超过 200 GB, 而且还在进一步增加.

去中心化是区块链的显著特征, 被很多理论学家、无政府主义者所推崇, 但是去中心化也带来一些问题, 产生分歧时将很难达成一致意见, 比如 2017 年 8 月 1 日比特币和比特币现金因为扩容问题造成硬分叉. 实际上, 去中心化并不能实现 “真正的民主”, 群体之间也不会按照 “ 少数服从多数” 的原则协商一致, 而是由于理念不可调和或自身利益造成社区分裂[4]. 这对整个比特币社区的打击很大. 目前很多人纯粹为了发币而分叉 (即 IFO, initial fork offering, 首次分叉发行), 并非理念上不可调和. 表1[5]列举了多种从比特币分叉而来的数字货币, 可以看出这种分叉越来越频繁. 此外, 由于比特币的算力越来越集中于一些大型的矿池手中, 也很难达到真正意义上的去中心化.

表 1 比特币分叉

Table 1 Forks of Bitcoin

时间	分叉高度	名称	缩写
2017.10.24	491 407	Bitcoin Gold	BTG
2017.12.12	498 888	BitcoinX	BCX
2017.12.19	499 999	Lightning Bitcoin	LBTC
2017.12.28	501 407	Bitcoin Cash Plus	BCP
2018.1.20	505 083	Bitcoin Interest	BCI
2018.1.24	505 888	Bitcoin Atom	BCA
2018.2.28	511 346	Bitcoin Private	BTCP
2018.4.1	516 095	Classic Bitcoin	CBTC

不可篡改在提高账本可信性的同时, 也带来一些问题. 现在比特币区块链已经出现非法信息 [19,20], 并且无法删除. 除了非法信息, 一旦个人信息被永久地存储在区块链中也与被遗忘权 (right to be forgotten) 相抵触 [21]. 在现实的复杂的金融体系里, 数据修改、交易撤销也是必要需求, 比如账户被盗需要追回资金, 数据传输过程中发生故障, 造成交易错误操作, 也需要对交易进行撤销 (银行对已经成功记账的交易进行撤销的过程, 称为冲正). 因此, 在现实场景中, 有时候需要对交易信息进行适当地修改, 当然这种修改需要在极其严苛的条件下进行.

匿名性满足了人们对隐私保护的部分需求, 但是比特币也广泛使用于暗网和黑市交易. 如 “丝绸之路” 就是一个专门提供各种非法物品和服务的网络黑市, 2013 年美国多个执法部门配合关闭 “丝绸之路” 网站并查封资产, 其中包括 26 000 个比特币. 2017 年 5 月 12 日, WannaCry 病毒感染大量计算机, 向计算机植入敲诈者病毒, 导致电脑大量被加密, 受害者电脑被黑客锁定后, 病毒会提示支付价值相当于 300 美元的比特币才可解锁. 这些事件表明匿名性让犯罪分子有了可乘之机. 因此, 在满足用户隐私保护需求的同时, 也需要得到监管. 从另一方面讲, 比特币的匿名性在理论上并不完美. 由于比特币所有交易都是以明文的形式存储在区块链中, 一旦地址和用户真实身份对应起来, 那么该用户在该地址下的所有交易信息都可以追踪到.

总之, 比特币区块链仍有许多不足. 在实际应用中, 区块链技术要进行相应的改进才能适应具体的应用场景.

4 区块链形式化定义

为了深入理解区块链的本质及安全特性, Garay 等人首次给出比特币骨架协议的形式化定义 [22]. 这对基于其他共识机制的区块链的安全性分析也起到参考借鉴作用. 本节介绍的区块链形式化定义主要来自参考文献 [22, 23].

[4]这里并没有使用 “分叉” 一词, 因为我们认为去中心化造成的社区分裂比分叉来得严重得多.

[5]数据来源: https://coinmarketcap.com.

4.1 基本符号和概念

区块

区块是具有如下形式的三元组: $B =< s, x, \mathrm{ctr} >$, 其中 $s \in \{0,1\}^{\kappa}$, $\mathrm{ctr} \in N$ 满足 $\mathrm{validblock}_q^D(B)$. $\mathrm{validblock}_q^D(B)$ 表示判断区块 B 的合法性: $(H(\mathrm{ctr}, G(s,x)) < D) \wedge (0 \leqslant \mathrm{ctr} < q)$, 其中 $G(\cdot)$ 和 $H(\cdot)$ 是哈希函数. 参数 $D \in N$ 是区块的目标哈希值, $q \in N$ 决定了寄存器 ctr 的大小. 在比特币系统中, s 表示上一个区块头的哈希值, x 表示时间戳 (T)、Merkle 根等当前块的一些基本信息, 目标哈希值 D 每 2016 个区块调整一次.

区块链

区块链 $\mathcal{C}$ 是区块序列 $\mathcal{C} = (B_1, B_2, \cdots, B_n)$, 其中 B_1 是事先给定的创世区块, $B_i =< s_i, x_i, \mathrm{ctr}_i >$, $s_i = H(\mathrm{ctr}_{i-1}, G(s_{i-1}, x_{i-1}))$, $2 \leqslant i \leqslant n$. 定义 i 为区块 B_i 在区块链 $\mathcal{C}$ 中的高度, 最高的区块 B_n 称为区块链的头, 记为 $\mathrm{head}(\mathcal{C}) = B_n$. 区块链的高度为 n, 记为 $\mathrm{height}(\mathcal{C}) = n$. 用空字符 ε 表示空链, 定义 $\mathrm{head}(\varepsilon) = \varepsilon$, $\mathrm{height}(\varepsilon) = 0$.

通过添加合法区块 $B' =< s', x', \mathrm{ctr}' >$, 可以将一个高度为 n 的区块链 $\mathcal{C}$, 扩展成高度为 $n+1$ 的区块链 $\mathcal{C}'$ 满足 $s' = H(\mathrm{ctr}_n, G(s_n, x_n))$, 记为 $\mathcal{C}' = (\mathcal{C}, B')$. 此时, $\mathrm{head}(\mathcal{C}') = B'$. 任何满足 $\mathrm{validblock}_q^D(\cdot)$ 的区块 B 都可以扩展空链 ε. 如果区块链 $\mathcal{C}_2$ 由区块链 $\mathcal{C}_1$ 扩展而来, 那么 $\mathcal{C}_2$ 包含了 $\mathcal{C}_1$ 的所有区块, 即 $\mathcal{C}_1$ 是 $\mathcal{C}_2$ 的前缀, 记为 $\mathcal{C}_1 \preceq \mathcal{C}_2$. $\mathcal{C}^{\lceil k}$ 表示 "裁剪掉" 区块链 $\mathcal{C}$ 最高的 k 个区块, 如果 $k \geqslant \mathrm{height}(\mathcal{C})$, 那么 $\mathcal{C}^{\lceil k} = \varepsilon$.

$\mathrm{VIEW}_{\Pi,\mathcal{A},\mathcal{Z}}^{H(\cdot)}(\kappa, q, z)$ 表示在环境 $\mathcal{Z}$ 和敌手 $\mathcal{A}$ 下运行协议 Π 所有节点的视图, 可以看成一个系统中每个节点保存的本地区块链的集合.

为了能够集中的描述比特币骨架协议, 我们不去指定插入链中数据的类型, 不去强调检查区块结构的哪些合法性 (除了验证和哈希函数 $G(\cdot)$ 和 $H(\cdot)$ 相关的之外), 也不去解释链的方式, 而是将这些检查和操作定义成三个外部函数: 内容验证函数 $V(\cdot)$、输入贡献函数 $I(\cdot)$ 和链读取函数 $R(\cdot)$.

4.2 比特币骨架协议

在介绍比特币骨架协议之前, 先简单介绍三个子算法: 链验证、链比较和工作量证明, 算法的详细描述可以参考文献 [22].

链验证$\mathrm{validate}(\mathcal{C})$ 该算法验证区块链 $\mathcal{C} = (B_1, B_2, \cdots, B_n)$ 的结构属性: (1) 使用函数 $V(\cdot)$ 验证区块链 $\mathcal{C}$ 的数据类型和格式; (2) 验证每个区块的合法性 $\mathrm{validblock}_q^D(B_i)$, $1 \leqslant i \leqslant n$ 和链接关系 $s_i = H(\mathrm{ctr}_{i-1}, G(s_{i-1}, x_{i-1}))$, $2 \leqslant i \leqslant n$.

链比较$\mathrm{maxvalid}(\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\tau)$ 该算法寻找 "尽可能好的" 链. 首先使用链验证算法 $\mathrm{validate}(\cdot)$ 保证每个区块链都是合法的, 然后使用函数 $\max(\mathcal{C}_1, \mathcal{C}_2)$ 来找到两个区块链中的最好链, 进而找到多条区块链的最好链. 具体地, 如果 $\mathrm{height}(\mathcal{C}_1) \geqslant \mathrm{height}(\mathcal{C}_2)$, 那么 $\max(\mathcal{C}_1, \mathcal{C}_2) = \mathcal{C}_1$, 否则 $\max(\mathcal{C}_1, \mathcal{C}_2) = \mathcal{C}_2$. 一般认为, 区块链越高, 意味着付出的工作量越多.

工作量证明$\mathrm{pow}(x, \mathcal{C})$ 该算法用来扩展区块链. 假设 $\mathrm{head}(\mathcal{C}) = B_n =< s_n, x_n, \mathrm{ctr}_n >$, B_n 的哈希值为 $s_{n+1} = H(\mathrm{ctr}_n, G(s_n, x_n))$, 寻找 ctr 使得 $H(\mathrm{ctr}, G(s_{n+1}, x)) < D$, 这是需要付出大量工作的地方. 一旦找到合法的 ctr_{n+1}, 就可以获得区块 $B_{n+1} =< s_{n+1}, x_{n+1}, \mathrm{ctr}_{n+1} >$, 其中 $x_{n+1} = x$.

有了上面三个子算法, 我们给出比特币骨架协议.

骨架协议

每个矿工保存本地区块链 $\mathcal{C}$, 尝试通过 pow 算法来扩展 $\mathcal{C}$. 在更新区块链之前, 矿工通过他的通信带 Receive() 检查是否收到更好的链. 矿工打算插入区块链的数据 x 是由函数 $I(\cdot)$ 来决定的. $I(\cdot)$ 的输入包括状态 st, 当前区块链 $\mathcal{C}$, 输入带 Input() 上的数据内容, 通信带 Receive() 和当前区块链的高度 height. 输入带 Input() 只包含 Read() 和 Insert(value) 两个操作. 当 x 确定之后, 矿工就通过 pow 算法将 x 插入到区块链中. 如果矿工扩展了区块链 $\mathcal{C}$, 那么矿工就将新的区块链 $\mathcal{C}_{\mathrm{new}} = (\mathcal{C}, B)$ 广播给其

他参与者. 最后使用函数 $R(\cdot)$, 将结果写到输出带 OUTPUT() 上. 下面是骨架协议的伪代码描述.

算法 1 比特币骨架协议

```
1  C ← ε, st ← ε, height ← 0;
2  while TRUE do
3  |  C̃ ← maxvalid(C, RECEIVE()中的任何链C′);
4  |  < st, x >← I(st, C̃, height, INPUT(), RECEIVE()) ;        // 确定打算插入的内容 x
5  |  C_new ← pow(x, C̃);
6  |  if C ≠ C_new then
7  |  |  C ← C_new;
8  |  |  BROADCAST(C);
9  |  end
10 |  height ← height + 1;
11 |  if INPUT() 包含 READ 标识 then
12 |  |  将 R(C) 写到 OUTPUT();
13 |  end
14 end
```

4.3 安全性质

Garay 等人给骨架协议定义了两个基本性质: 共同前缀 (common prefix property) 和链质量 (chain quality property) [22]. Kiayias 等人在此基础提出一个新的性质: 链成长 (chain growth property) [23].

共同前缀 [22]: 对于参数 $k \in N$, 视图 $\text{VIEW}^{H(\cdot)}_{\Pi,\mathcal{A},\mathcal{Z}}(\kappa,q,z)$ 中两个诚实节点各自拥有的本地区块链 $\mathcal{C}_1,\mathcal{C}_2$ 满足 $\mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$ 和 $\mathcal{C}_2^{\lceil k} \preceq \mathcal{C}_1$. 这个性质说的是, 诚实节点之间除了最近的 k 个区块可能不一致外, 之前的区块都是一致的, 即不可篡改. 在比特币系统中, k 一般认为大于等于 6.

链质量 [22]: 对于参数 $l \in N$ 和 $\mu \in (0,1) \subset R$, 视图 $\text{VIEW}^{H(\cdot)}_{\Pi,\mathcal{A},\mathcal{Z}}(\kappa,q,z)$ 中每个诚实节点满足其本地区块链 $\mathcal{C}$ 的任意连续 l 个区块中敌手产生区块的比例不会超过 μ. 这个性质说的是, 诚实节点贡献了足够长、足够多的区块, 从而保证了区块链的 "质量".

链成长 [23]: 对于参数 $\tau \in R$ 和 $r \in N$, 节点 i 在高度为 t 的区块链记为 $\mathcal{C}_i^t$, 视图 $\text{VIEW}^{H(\cdot)}_{\Pi,\mathcal{A},\mathcal{Z}}(\kappa,q,z)$ 中诚实节点在高度为 t 和 $t+r$ 时满足 $\min\limits_{i,j}(|\mathcal{C}_i^{r+t}| - |\mathcal{C}_j^t|) \geqslant \tau \cdot r$, 其中 τ 称为速率系数. 这个性质保证了链成长的最小速率, 防止敌手通过降低全网处理交易的速度来对区块链进行攻击.

5 区块链研究和应用进展

区块链技术的发展日新月异. 本节主要从区块链的相关密码技术、安全性分析、共识机制、隐私保护、可扩展性等方面总结区块链技术的最新理论和应用研究进展.

5.1 区块链相关密码技术

密码技术是保障区块链安全的基础与核心, 具有不可替代的重要作用. 区块链中除了使用哈希函数、数字签名等基本密码技术之外, 在涉及隐私保护、安全监管、权限管理、跨链交易等具体应用需求时, 可能还会用到更多密码算法和协议. 目前, 已经有多种密码算法和协议应用到区块链, 如环签名、零知识证明、同态密码、安全多方计算等, 它们广泛用于匿名交易、交易额加密验证、数据共享、身份管理等方面.

首先, 区块链现有或潜在应用的密码技术总结如下.

特殊数字签名

为实现不可追踪的电子支付系统, Chaum 提出盲签名的概念 [24]. 盲签名具有签名者对所签消息不可见以及签名者不可追踪签名的特性. 环签名是另一种实现匿名性的签名, 用于一个成员代表一个群体进行签名的应用场景, 签名者利用自己的公私钥对和其他成员的公钥, 将签名首尾闭合形成环状结构, 使各成员之间身份平等, 从而实现签名者的无条件匿名性. 群签名也可以实现群成员的匿名签名, 但是又能使得群管理员按需跟踪群签名, 具有可控匿名的特性. 这些特殊数字签名不仅可以用来实现匿名交易、范围证

明, 也可以实现监管需求, 如群签名可以同时实现匿名保护和合法监管. 此外, 门限签名、多重签名、代理签名等特殊数字签名也可用于保障区块链交易的安全与便捷.

零知识证明

零知识证明是指证明者能够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, 分为交互和非交互两类. zk-SNARK 是一种简洁的非交互零知识证明, 证据较短容易验证, 将需要证明的问题转换成可满足性电路, 经过 R1CS 和 QAP 两个步骤, 再进行非交互零知识证明 [25]. 零知识证明可用于解决区块链隐私保护, 交易合法性验证等问题.

同态密码

同态密码使对密文进行特定运算与对明文进行相应操作再加密的效果相同. 按照对明文的运算处理能力可分为部分同态和全同态. 其中部分同态是指只支持加法运算或者乘法运算或者两者都支持但是操作次数受限的情况. 全同态是指可以支持任意函数. 尽管全同态密码的效率还不是很高, 存在计算量和密钥量过大等问题, 但是部分同态技术已经在现实中使用. 同态密码可在区块链中用于实现数据隐私保护、安全数据共享等需求.

安全多方计算

安全多方计算是指多个参与者通过各自持有的秘密输入共同完成对某函数的计算, 要求每个参与者除计算结果外均不能得到其他参与者的任何秘密输入信息. 安全多方计算主要针对无可信第三方的情况下, 如何安全地计算给定函数的问题, 在区块链中可用于秘密共享、数据隐私保护、共识算法设计等方面.

公钥密码基础设施 (PKI)

PKI 是一种用非对称密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施. 在 PKI 中, 由证书认证中心签发数字证书, 绑定用户的身份信息和公钥. 可用于在区块链中建立基于真实身份的可信身份管理系统. 同时还可研究探索基于身份、属性的密码在区块链身份管理中的应用.

目前这些密码算法和协议在低频、小规模的应用场景中也许还能胜任, 但是距离高频、大规模的应用场景还有较大差距, 效率有待进一步提高. 面对一些新的应用场景和需求, 可能还需要设计新的密码算法和协议 (如轻量级算法和协议).

其次, 由于公开透明、不可篡改等特性, 区块链又被密码学者用于构造密码算法和协议. 例如, 利用区块链构造时控承诺 (timed commitment), 承诺者要么在一定时间内揭示自己的秘密值, 要么支付罚金, 通过这种保证金机制实现公平安全多方协议 [26–28]. 由于内在的不可预测性, 区块链还可以作为公开可验证的随机数种子 [29,30].

最后, 量子计算对现代密码体制的影响巨大. Shor 量子算法可以在多项式时间内分解大整数和求解离散对数问题 [31], 造成基于这些困难问题的公钥密码体制不再安全. Grover 搜索算法实现了对传统搜索算法的二次加速 [32], 为了保持原有安全目标, 需要增加哈希函数的输出长度和对称密码的密钥长度. 因此, 针对目前区块链普遍使用传统密码算法的现状, 需要做好向后量子区块链迁移的准备工作. 近几年已经有一些后量子区块链的研究 [33–36]. 如 Zhang 等人在 CryptoNote 的基础上, 通过理想格上可链接环签名, 设计了匿名的后量子密码货币 [34]. Torres 等人构造了基于格的一次可链接环签名, 并扩展到格上的环秘密交易 (lattice ring confidential transactions) [35].

5.2 安全性分析

从比特币诞生开始, 对比特币系统和区块链的安全性分析就没有停止过. 比特币白皮书就指出只要诚实节点控制的算力超过全网算力的 51%, 比特币系统就是安全的 [1]. 早期针对区块链的安全性分析主要是提出具体的攻击方法, 如双花攻击 [37]、日蚀攻击 [38]、自私挖矿攻击 [39,40]、路由攻击 [41] 等. 此外还有针对矿池的攻击, 如区块截留攻击 (block withholding attack) [42]. 但是对于区块链基本的安全性质是什么、有哪些, 这些具体的攻击并没有给出.

对区块链进行安全性分析是一个非常困难的任务. 直到 2015 年, Garay 等人才在参与者不变、同步网络的情形下, 第一次提取出比特币区块链的基本性质: 共同前缀和链质量, 并给出了可证明安全模型 [22]. 在该模型下, 全网算力、挖矿难度都是不变的. 具体地, γ 和 β 分别表示诚实节点和恶意节点在一个出块周期内找到困难问题解的期望, 反映的是各自的哈希算力; f 是 γ、β 之和, 反映的是全网的哈希算力.

(1) 共同前缀: 假设 $f<1$, $\gamma\geqslant(1+\delta)\lambda\beta$, 其中 $\delta\in(0,1)$, $\lambda\geqslant 1$ 且 $\lambda^2-f\lambda-1\geqslant 0$. 令 S 表示给定高度, 诚实节点拥有的区块链集合. 那么在参数 k 下, S 不满足共同前缀的概率最多为 $e^{-\Omega(\delta^3 k)}$.

(2) 链质量: 假设 $f<1$, $\gamma\geqslant(1+\delta)\lambda\beta$, 其中 $\delta\in(0,1)$. $\mathcal{C}$ 是诚实节点的区块链, 那么对于 $\mathcal{C}$ 中任意连续 l 个区块, 敌手贡献超过 $(1-\frac{\delta}{3})\frac{1}{\lambda}l$ 个区块的概率小于 $e^{-\Omega(\delta^2 l)}$.

随后, Kiayias 等人提出链成长性质 [23], 分析了比特币骨架协议和 GHOST 协议 [43].

(3) 链成长: 假设出块系数为 $(1-\delta)\gamma$, 其中 $\delta\in(0,1)$. 那么不满足链成长性质的概率最高为 $e^{-\Omega(\delta^2 r)}$.

在此基础上, Pass 等人对区块链在异步网络的情形下进行了分析 [44], Garay 等人则是针对参与节点不固定, 即挖矿难度是动态调整的的情形进行分析 [45].

除了对 PoW 区块链进行安全性分析, 对 PoS 区块链的安全性分析也越来越多. Bentov 等人对 PoS 进行了一些具体的攻击分析 [46,47], 但是同样缺乏正式明确的安全模型和证明. Kiayias 等人给出了第一个关于 PoS 的安全性分析, 该模型基于参考文献 [22], 关注鲁棒公开交易账本的两个性质: 持久性 (persistence) 和活跃性 (liveness), 这两个性质可以由区块链的三个安全特性获得 [48]. David 等人给出了基于 PoS 的区块链共识机制, 可以在半同步网络下抵抗完全自适应 (fully-adaptive) 攻击 [49].

5.3 共识机制

共识机制并不是一个新问题, 在分布式系统中早有研究. 之所以需要共识机制, 是因为分布式系统中多个节点掌握的数据副本可能不一致. 按照节点发生的故障类型, 共识算法可分为两类情况. 一类是停机故障, 节点可以在任何时间出现故障, 但是它们会停止工作, 不会发送或接收消息, 常用算法包括 Paxos [50]、RAFT [51]、ZAB [52] 等. 另一类是拜占庭故障, 故障节点可以随意发送任何 (恶意) 消息, 或被敌手控制, 解决这类故障也有一些算法如 PBFT [53]、HQ [54]、Zyzzyva [55] 等.

早期共识机制大都是针对封闭群体设计的, 而比特币的一个创新工作是可以在一个开放的、去中心化的、互不信任的节点之间达成共识. 比特币采用了基于 PoW 的共识机制, 早在 1992 年 Dwork 等人就已经提出 PoW 的概念 [56], 最初是为了阻止垃圾邮件和 DoS 攻击. 尽管 PoW 有很多应用, 但是它的缺点也很明显, 如消耗能源、算力过于集中等. 因此, 共识机制是区块链技术研究的重要方向. 关于共识机制的介绍还可以参考文献 [57].

5.3.1 设计新的困难问题

要想成为 PoW 的困难问题, 需要具备以下几个条件: (1) 难于计算却易于验证, (2) 提供困难问题的解时任何人都确信付出足够多的工作, (3) 容易调整难度. 很显然, 比特币区块链中使用的基于 SHA256 的困难问题满足上面的条件, 但是由于 SHA256 算法简单, 很容易使用 ASIC 实现, 造成算力过于集中. 为了解决这一问题, 人们尝试使用更难的算法来替换 SHA256. 比如在 Litecoin 中 PoW 使用的哈希函数是 scrypt 算法 [58], 该算法的特点是在运算过程中需要大量的内存支持, 矿工大部分仍然依靠显卡挖矿. 但是 scrypt 算法存在计算太慢、验证也需要内存等缺点, 如 scrypt 算法需要 128 KB 的内存来验证. 2016 年, Biryukov 等人提出了内存不对称的概念, 即产生证明需要大量的内存, 但是验证几乎不需要内存, 并利用广义生日问题构造困难问题 Equihash [59], 该困难问题已经在 Zcash 系统中使用 [3].

5.3.2 设计新的共识机制

虽然通过设计新的困难问题, 可以部分解决 PoW 所带来的一些问题, 但是并不能解决高耗能、吞吐量低、交易延迟高等问题. 人们也在设计新的共识机制 PoX (proof of X), 以解决或部分解决 PoW 的缺陷.

PoS (proof of stake)

PoS 的概念最早是在比特币论坛上讨论的, 用来替换 PoW. PoS 是根据参与者在系统中占有的股份 (记录在区块链中) 决定记账权. PPcoin 是第一个采用 PoS 的数字货币 [60], 但是采用 PoW+PoS 的模式. Nxt 只采用 PoS 模式 [61]. 以太坊也打算用 PoS 代替 PoW, 作为过渡, 目前每 100 个区块使用一次 PoS. 最近, 有人提出可证明安全的 PoS 共识机制, 如 Ouroboros [48]、Snow White [62]、Ouroboros Praos [49]. 关于 PoS 还有几个变种, 如 Proof of Deposit [63]、Proof of Burn [64]、Proof of Coin Age [60].

PoC (proof of capacity)

PoC 指的是参与节点根据能够分配的磁盘空间来决定记账权. 比如, PermaCoin 要求矿工存储大型文件的一部分, 才可以挖矿 [65]. 2015 年, Dziembowski 等人提出了 PoSpace (proof of space) 的共识协

议, 这是 PoC 的一种变形. 这种共识协议基于 hard-to-pebble 图, 需要证明者存储大量的文件, 而验证者只保留简单的信息 [66]. 但是 PoSpace 的证明量需要数兆存储空间, 并且这个过程是交互的. Abusalah 等人构造了简单的 PoSpace, 并且能够抵抗 Hellman 时间 -存储折中攻击 [67].

PoET (proof of elapsed time)

PoET 是由 Intel 构建在可信执行环境的一种彩票协议, 核心是使用 Intel SGX 技术的 CPU 硬件, 在受控安全环境下随机产生一些延时, 同时 CPU 从硬件级别证明延时的可信性, 谁的延时最低谁就获得记账权 [68]. Zhang 等人采用另一个途径 REM (resource-efficient mining), 使用可信硬件做有用的 PoW 计算 [69].

除了上面介绍的共识机制之外, 还有很多 PoX 共识机制, 如 PoSW (proof of sequential work) [70,71]、PoST (proof of space time) [72]、PoA (proof of activity) [46] 等.

5.3.3 混合共识机制

混合共识机制, 一般是将参与节点分成一个或多个 committe (也称 sharding), 每个 committe 并行处理交易. 例如以太坊基于校验器管理合约 (validator manager contract, VMC) 的分片方案以及 Zillipa 等. 为了达到强一致性和高吞吐量, 有人建议将 BFT 类的传统共识机制用于区块链 [73]. 图灵奖获得者 Micali 在 2016 年提出的 Algorand 协议使用 Byzantine agreement, 每个区块的产生都需要很多步, 并且每一步都需要产生一个不同的 committe, 这样可以抵抗自适应攻击 [74]. Elastico 共识协议将参与节点分成多个 committe, 每个 committe 使用 PBFT 共识机制处理不同的交易集合 [75]. 每个 committe 包含的节点数是固定的, 都是通过上一个 committe 计算困难问题产生. RSCoin 由央行掌握货币供应, 但是交易的处理却是由经过授权的 mintette 来处理并记录到各自的区块链中, 央行公布最终的区块链 [5]. 除了上述混合共识机制方案, 相关工作还有很多 [76–78].

5.4 隐私保护

比特币是通过假名的方式实现匿名性. 尽管在某种程度也起到保护用户隐私的作用, 但是比特币所有交易都是通过明文的方式公开记录在分布式账本上, 任何人都可以知道每个地址交易的详细情况. 一旦和现实身份联系起来, 就会泄露用户的隐私. 尽管用户可以使用多个假名来提高匿名性, 但是研究表明通过区块链的一些信息, 如交易图、交易金额、交易时间等, 仍然可以恢复用户的隐私 [79–81]. 因此, 人们开始追求更强的匿名性 [4,82–84]. 确切地说, 强匿名性指的是既隐藏交易图, 也隐藏交易金额. 为了实现强匿名性, 有的方案将隐藏交易图和隐藏交易金额分开实现 [4,84], 有的方案将这两部分合在一起实现 [83].

隐藏交易金额

假设 Alice 和 Bob 的账户余额分别为 x_A 和 x_B, 公开的是对应密文 $E(x_A)$ 和 $E(x_B)$, 其中 $E(\cdot)$ 是某个加密算法. Alice 向 Bob 转移金额 y, 公开的也是对应密文 $E(y)$. 那么转账之后, Alice 的账户余额的密文 E_A 要和 $x_A - y$ 对应, 而 Bob 的账户余额的密文 E_B 要和 $x_B + y$ 对应, 且在密文状态下证明 $x_A \geqslant y$.

要 E_A 和 $x_A - y$ 对应, 可以通过加法同态来实现, 即 $E_A = E(x_A) - E(y) = E(x_A - y)$; 对 Bob 的账户余额采用同样的方法. 在密文状态下证明 $x_A \geqslant y$ 则要复杂得多, 可以转换成问题: 已知 $E(x_A - y)$ 证明余额 $x_A - y$ 非负, 即余额非负判断. 余额非负判断的主要依据是, 如果余额为负数, 那么余额取模之后是一个非常大的数, 这是因为余额的绝对值相对于模数而言很小. 所以只需要证明余额 x 在某个范围, 如 $x \in [0, 2^\tau)$. 通常的做法是将余额 x 写成 u 进制数, 即 $x = \sum_{0 \leqslant j \leqslant t} x_j u^j + \sum_{j>t} x_j u^j$, 其中 $x_j \in \{0, 1, \cdots, u-1\}$, t 满足 $\sum_{0 \leqslant j \leqslant t} (u-1)u^j < 2^\tau \leqslant u^{t+1}$. 如果 $E(x) = E(\sum_{0 \leqslant j \leqslant t} x_j u^j) = \sum_{0 \leqslant j \leqslant t} E(x_j u^j)$ 说明 $x \in [0, 2^\tau)$, 余额非负; 如果 $E(x) \neq \sum_{0 \leqslant j \leqslant t} E(x_j u^j)$ 说明 $x > 2^\tau$(x 非常接近模数), 余额为负. 需要进一步证明的是, $x_j \in \{0, 1, \cdots, u-1\}$, 这一步可以使用环签名、广义 Schnorr 证明、双线性对等方法证明.

Maxwell 提出的 CT (confidential transaction) 方案就是采用上述方法, 其中余额按二进制展开, 加密算法使用的是具有加法同态属性的 Pedersen 承诺, 通过广义 Schnorr 证明 $x_j \in \{0, 1\}$ [82]. Monero [4] 和 Solidus [84] 在隐藏交易金额时都采用该方法. Camenisch 等人的方案 [85] 中余额按 u 进制展开 (如 $u = 2^8$), 采用的也是 Pedersen 承诺, 将成员集合 $\{0, 1, \cdots, u-1\}$ 做 Boneh-Boyen 签名 (预计算), 并利

用双线性对证明 $x_j \in \{0, 1, \cdots, u-1\}$. 整个方案是交互式的, 可以通过 Fiat-Shamir 假设变为非交互式的. 最近的工作还有 Ma 等人 [86] 和 Bunz 等人 [87] 的方案.

除了上述方法之外, 早期的方案还有采用 Fujisaki-Okamoto 承诺 [88] 进行范围证明 [89,90].

隐藏交易图

为了隐藏交易双方的身份, CryptoNote 采用的是可链接环签名技术, 将交易发送者的身份 (签名公钥) 隐藏在一个公钥集合中; 通过产生临时公钥的方法隐藏交易接收者的身份 [91]. 另一个方案 Solidus 则是通过可公开验证的健忘 RAM 机 (publicly-verifiable oblivious RAM machine, PVORM) 实现交易双方的身份隐藏 [84].

Zerocash [83] 是在 Zerocoin [92] 基础上改进得到的协议. 该协议基于 zk-SNARKs [25,93], 能够同时很好地隐藏交易者双方的身份和交易金额. Kosba 等人在 Zerocash 的基础上类似地构造了他们的隐私保护方案 Hawk, 用来实现智能合约的隐私保护 [94].

除此之外, 还有很多工作致力于实现无中心数字货币的匿名, 如 TumbleBit [95]、CoinParty [96] 和 CoinShuffle [97], 都基于 CoinJoin [98] 工作的基础上. 这些方案通过各种形式的混合, 来掩盖交易者的身份, 但是这些方案可以通过统计分析破坏匿名性.

概括起来看, 目前很多方案都已经实现了很强的匿名性. 在今后的研究中, 一方面, 是否可以进一步强化匿名性, 因为交易还有可能通过交易时间来泄露信息. Solidus 建议在有规律的时间间隔下, 通过添加一些值为 0 的假交易和真交易一起分批发送, 来消除交易时间带来的泄露风险 [84]. 另一方面, 强匿名性可能用于非法目的, 必然会遭到监管机构的强烈反对, 如何做到监管和隐私保护之间的平衡是值得思考的. 群签名既能实现群成员的匿名签名, 又能使得监管机构按需跟踪签名者, 具有可控匿名的特性, 可能在区块链应用中实现隐私和监管之间的平衡.

5.5 可扩展性

可扩展性问题严重影响区块链更广泛的使用. 关于如何改进区块链的可扩展性, 区块链社区发生很多争论. 解决可扩展性问题, 一般从链上 (on-chain) 和链下 (off-chain) 两个方面考虑.

链上处理是指修改区块链本身的协议提升可扩展性. 比如通过修改区块链参数, 如区块大小、出块时间等, 但是这种方法提升有限, 而且容易导致分叉. Bitcoin-NG 是另一种尝试 [99], 将时间分成 epoch, 记账者在一个 epoch 内可以产生多个区块, 直到下一个记账者产生. 为此, Bitcoin-NG 有两种区块, 一种叫 keyblock 包含困难问题的解, 以及选出来的记账者公钥; 一种叫 microblock 是由记账者通过签名产生. Byzcoin 是 Bitcoin-NG 的扩展, 每个 keyblock 不是选出一个记账者, 而是记账者的集合, 记账者集合使用 PBFT 协议产生 microblock [78].

链下处理主要针对小额高频交易提升可扩展性. 如闪电网络技术 [100], 交易双方通过多重签名将双方的初始金额锁定到区块链中, 从而建立一个支付通道, 中间交易造成双方金额的变化不记录到区块链中, 而是将最终双方金额状态记录到区块链中. 同时, 如果双方没有建立支付通道, 也可以通过已经存在的第三方支付通道 (一方或多方) 进行链下交易. 还有的社区采用侧链技术 [101]、雷电网络技术 [102] 等链下技术解决区块链的可扩展问题.

总的来说, 无论采用何种技术, 解决方法都是寻找可扩展性和去中心化之间平衡, 想要提高可扩展性就要适当中心化. 目前一些基于有中心的区块链方案, 可扩展性可以做到很好. 如 RScoin 通过适度中心化, 在 30 个节点 mintette 的情况下每秒可以处理 2000 笔交易, 而且随着节点 mintette 的增加, 每个 mintette 的平均通信量还会降低 [5]. 一些论坛表明 Corda 和 Fabric 平台也可以达到每秒千笔以上的处理速度.

5.6 交易撤销

当区块链项目出现 Bug 或受到攻击时, 为了减少大家的损失, 不得不通过硬分叉的形式来修复 Bug 或弥补损失. 但是这种方式会给无关交易造成影响, 且越晚分叉影响越大. 目前已经有一些其他方案可以实现区块链数据的撤销或修改 [21,103,104]. Reversecoin 是第一种支持交易撤销的竞争币 [103]. Reversecoin 的地址由在线密钥和离线密钥两部分组成, 其中在线密钥用于一般交易, 离线密钥用于撤销交易. 为了防止用户滥用该功能, 需要在交易上加一个时间窗口, 超过时间窗口交易无法撤销. 使用在线密钥进行交易会造成交易确认延迟. 如果想要交易即时确认, 也可以用离线密钥进行签名. Ateniese 等人

使用变色龙杂凑函数 (Chameleon Hash, CH) 来修改区块链内容 [21]. CH 可以通过陷门高效地找出碰撞. 该陷门可以由中心化的权威机构掌握, 也可以通过安全多方计算得到. Puddu 等人通过在交易上添加修改条件, 如谁可以修改这笔交易、什么时间窗口可以修改这笔交易等, 设计了 μ 链: 不通过硬分叉对区块链进行修改 [104]. 这个方案不改变区块链的内容, 只是同一笔交易在区块链中有多个状态, 全网只认可最新的状态. 此外, 可扩展签名方案 [105] 也可能用于实现交易撤销.

6 小结

作为一门新兴技术, 区块链技术的发展日新月异. 本文通过介绍比特币区块链, 总结了区块链技术主要研究方向和相关密码技术, 以及近年来具有代表性的科研和应用成果. 通过调研分析, 区块链技术仍然面临一些技术挑战, 基于此提出以下几点建议:

(1) 建立合理信任假设. 节点之间的信任关系在很大程度上影响系统的实现和效率. 可以通过身份管理、权限管理、适当的中心化等方法, 建立合理的信任假设, 降低信任成本, 大幅提升区块链性能.

(2) 不同需求区别对待. 同一个技术不可能高效地解决所有问题, 要不断细分需求区别对待. 如小额和大额交易可以采用不同的安全和实现策略, 以达到小额交易快速便捷、大额交易安全可靠等目标.

(3) 注重指标间的权衡. 匿名和监管、安全和性能等指标是矛盾的, 注重指标间的权衡, 而不是过度追求某一方面, 可能更具现实意义.

References

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. http://bitcoin.org/bitcoin.pdf. 2008.

[2] Litecoin[EB/OL]. https://litecoin.com/.

[3] Zcash[EB/OL]. https://z.cash/.

[4] Monero[EB/OL]. https://getmonero.org/.

[5] DANEZIS G, MEIKLEJOHN S. Centrally banked cryptocurrencies[C]. In: Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS). San Diego, CA, USA. 2016. [DOI: 10.14722/ndss.2016.23187]

[6] Project Jasper: A Canadian experiment with distributed ledger technology for domestic interbank payment settlement[EB/OL]. https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf. 2017.

[7] Project Ubin: SGD on distributed ledger[EB/OL]. http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx. 2017.

[8] YAO Q. Prototype of Chinese digital fiat currency[J]. China Finance, 2016, 2016(17): 13–15.
姚前. 中国法定数字货币原型构想 [J]. 中国金融, 2016, 2016(17): 13–15.

[9] WANG Y H. Digital currency technology implementation framework[J]. China Finance, 2016, 2016(17): 15–16.
王永红. 数字货币技术实现框架 [J]. 中国金融, 2016, 2016(17): 15–16.

[10] XU Z, YAO Q. Preliminary scheme for digital ticket trading platform[J]. China Finance, 2016, 2016(17): 31–33.
徐忠, 姚前. 数字票据交易平台初步方案 [J]. 中国金融, 2016, 2016(17): 31–33.

[11] XU Z, TANG Y W, LIN X. Discussion on theory of central bank digital currency[J]. China Finance, 2016, 2016(17): 33–34.
徐忠, 汤莹玮, 林雪. 央行数字货币理论探讨 [J]. 中国金融, 2016, 2016(17): 33–34.

[12] YAO Q. Digital currency and bank account[J]. Tsinghua Financial Review, 2017, 7: 63–67. [DOI: 10.19409/j.cnki.thf-review.2017.07.016]
姚前. 数字货币与银行账户 [J]. 清华金融评论, 2017, 7: 63–67. [DOI: 10.19409/j.cnki.thf-review.2017.07.016]

[13] SWAN M. Blockchain: Blueprint for a New Economy[M]. USA: O'Reilly Media, Inc., 2015.

[14] MIIT. China's Blockchain Technology and Application Development Whitepaper[M]. 2016.
工信部. 中国区块链技术和应用发展白皮书 [M]. 2016.

[15] ANTONOPOULOS A. Mastering Bitcoin: Programming the Open Blockchain[M]. 2nd edition. USA: O'Reilly Media, Inc., 2017.

[16] National Institute of Standards and Technology (NIST). FIPS PUB 180-4, Secure Hash Standard (SHS)[S]. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. 2005. [DOI: 10.6028/NIST.FIPS.180-4]

[17] National Institute of Standards and Technology (NIST). FIPS PUB 186-4, Digital Signature Standard (DSS)[S]. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf. 2013. [DOI: 10.6028/NIST.FIPS.186-4]
[18] Standards for Efficient Cryptography Group. SEC 2: Recommended elliptic curve domain parameters[S]. http://www.secg.org/sec2-v2.pdf. 2010.
[19] MATHEW J. Bitcoin: Blockchain could become 'safe haven' for hosting child sexual abuse images[EB/OL]. http://www.dailydot.com/business/bitcoinchild-porn-transaction-code/. 2015.
[20] SHIRRIFF K. Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson mandela, wikileaks, photos, and python software[EB/OL]. http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html. 2014.
[21] ATENIESE G, MAGRI B, VENTURI D, et al. Redactable blockchain, or rewriting history in Bitcoin and friends[C]. In: Proceedings of 2017 IEEE European Symposium on Security and Privacy (EuroS&PW 2017). IEEE, 2017: 111–126. [DOI: 10.1109/EuroSP.2017.37]
[22] GARAY J, KIAYIAS A, LEONARDOS N. The Bitcoin backbone protocol: Analysis and applications[C]. In: Advances in Cryptology—EUROCRYPT 2015, Part II. Springer Berlin Heidelberg, 2015: 281–310. [DOI: 10.1007/978-3-662-46803-6_10]
[23] KIAYIAS A, PANAGIOTAKOS G. Speed-security tradeoffs in blockchain protocols[J]. IACR Cryptology ePrint Archive, 2015: 2015/1019. https://eprint.iacr.org/2015/1019.
[24] CHAUM D. Blind signatures for untraceable payments[C]. In: Advances in Cryptology: Proceedings of CRYPTO 82. Springer Berlin Heidelberg, 1983: 199–203. [DOI: 10.1007/978-1-4757-0602-4_18]
[25] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: Nearly practical verifiable computation[C]. In: Proceedings of 2013 IEEE Symposium on Security and Privacy (SP). IEEE, 2013: 238–252. [DOI: 10.1109/SP.2013.47]
[26] BENTOV I, KUMARESAN R. How to use Bitcoin to design fair protocols[C]. In: Advances in Cryptology—CRYPTO 2014, Part II. Springer Berlin Heidelberg, 2014: 421–439. [DOI: 10.1007/978-3-662-44381-1_24]
[27] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. Secure multiparty computations on Bitcoin[C]. In: Proceedings of 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 443–458. [DOI: 10.1109/SP.2014.35]
[28] KUMARESAN R, MORAN T, BENTOV I. et al. How to use Bitcoin to play decentralized poker[C]. In: Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2015: 195–206. [DOI: 10.1145/2810103.2813712]
[29] BONNEAU J, CLARK J, GOLDFEDER S. On Bitcoin as a public randomness source[J]. IACR Cryptology ePrint Archive, 2015: 2015/1015. https://eprint.iacr.org/2015/1015.
[30] PIERROT C, WESOLOWSKI B. Malleability of the blockchain's entropy[J]. Cryptography and Communications, 2018, 10(1): 211–233. [DOI: 10.1007/s12095-017-0264-3]
[31] SHOR P. Algorithms for quantum computation: Discrete logarithms and factoring[C]. In: Proceedings of 35th Annual Symposium on Foundations of Computer Science (FOCS). IEEE, 1994: 124–134. [DOI: 10.1109/SFCS.1994.365700]
[32] GROVER L. A fast quantum mechanical algorithm for database search[C]. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC). ACM, 1996: 212–219. [DOI: 10.1145/237814.237866]
[33] TAN A. Post-quantum blockchain[EB/OL]. http://andrewt.me/assets/documents/phy372-final-report.pdf. 2018.
[34] ZHANG H, ZHANG F G, TIAN H B, et al. Anonymous post-quantum cryptocash[C]. In: Financial Cryptography and Data Security—FC 2018. Springer Cham, 2018. (to appear)
[35] TORRES W, STEINFELD R, SAKZAD A, et al. Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (Lattice RingCT v1.0)[C]. In: Information Security and Privacy—ACISP 2018. Springer Cham, 2018: 558–576. [DOI: 10.1007/978-3-319-93638-3_32]
[36] KIKTENKO E, POZHAR N, ANUFRIEV M, et al. Quantum-secured blockchain[J]. Quantum Science and Technology, 2018, 3(3): 035004. [DOI: 10.1088/2058-9565/aabc6b]
[37] ROSENFELD M. Analysis of hashrate-based double spending[J]. arXiv: 1402.2009v1, 2014.
[38] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's per-to-peer network[C]. In: Proceedings of the 24th USENIX Security Symposium. USENIX, 2015: 129–144.
[39] EYAL I, SIRER E. Majority is not enough: Bitcoin mining is vulnerable[J]. Communications of the ACM, 2018, 61(7): 95–102. [DOI: 10.1145/3212998]
[40] BAHACK L. Theoretical Bitcoin attacks with less than half of the computational power[J]. arXiv:1312.7013v1, 2013.
[41] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking Bitcoin: Routing attacks on cryptocurrencies[C]. In: Proceedings of 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 2017: 375–392. [DOI:

10.1109/SP.2017.29]

[42] EYAL I. The miner's dilemma[C]. In: Proceedings of 2015 IEEE Symposium on Security and Privacy (SP). IEEE, 2015: 89–103. [DOI: 10.1109/SP.2015.13]

[43] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in Bitcoin[C]. In: Financial Cryptography and Data Security—FC 2015. Springer Berlin Heidelberg, 2015: 507–527. [DOI: 10.1007/978-3-662-47854-7_32]

[44] PASS R, SEEMAN L, SHELAT A. Analysis of the blockchain protocol in asynchronous networks[C]. In: Advances in Cryptology—EUROCRYPT 2017, Part II. Springer Cham, 2017: 643–673. [DOI: 10.1007/978-3-319-56614-6_22]

[45] GARAY J, KIAYIAS A, LEONARDOS N. The Bitcoin backbone protocol with chains of variable difficulty[C]. In: Advances in Cryptology—CRYPTO 2017, Part I. Springer Cham, 2017: 291–323. [DOI: 10.1007/978-3-319-63688-7_10]

[46] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: Extending Bitcoin's proof of work via proof of stake [extended abstract][J]. SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34–37. [DOI: 10.1145/2695533.2695545]

[47] BENTOV I, GABIZON A, MIZRAHI A. Cryptocurrencies without proof of work[C]. In: Financial Cryptography and Data Security—FC 2016. Springer Berlin Heidelberg, 2016: 142–157. [DOI: 10.1007/978-3-662-53357-4_10]

[48] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]. In: Advances in Cryptology—CRYPTO 2017, Part I. Springer Cham, 2017: 357–388. [DOI: 10.1007/978-3-319-63688-7_12]

[49] DAVID B, GAZI P, KIAYIAS A, et al. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain[C]. In: Advances in Cryptology—EUROCRYPT 2018, Part II. Springer Cham, 2018: 66–98. [DOI: 10.1007/978-3-319-78375-8_3]

[50] LAMPORT L. The part-time parliament[J]. ACM Transactions on Computer Systems (TOCS), 1998, 16(2): 133–169. [DOI: 10.1145/279227.279229]

[51] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]. In: Proceedings of 2014 USENIX Annual Technical Conference (ATC). USENIX, 2014: 305–319.

[52] JUNQUEIRA F, REED B, SERAFINI M. Zab: High-performance broadcast for primary-backup systems[C]. In: Proceedings of 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN). IEEE, 2011: 245–256. [DOI: 10.1109/DSN.2011.5958223]

[53] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI). USENIX, 1999: 173–186.

[54] COWLING J, MYERS D, LISKOV B, et al. HQ replication: A hybrid quorum protocol for Byzantine fault tolerance[C]. In: Proceedings of the 7th Symposium on Operating Systems Design and Implementation (OSDI). USENIX, 2006: 177–190.

[55] KOTLA R, ALVISI L, DAHLIN M, et al. Zyzzyva: Speculative Byzantine fault tolerance[C]. In: Proceedings of 21st ACM SIGOPS Symposium on Operating Systems Principles (SOSP). ACM, 2007: 45–58. [DOI: 10.1145/1294261.1294267]

[56] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]. In: Advances in Cryptology—CRYPTO'92. Springer Berlin Heidelberg, 1993: 139–147. [DOI: 10.1007/3-540-48071-4_10]

[57] BANO S, SONNINO A, AL-BASSAM M, et al. SoK: Consensus in the age of blockchain[J]. arXiv:1711.03936v2, 2017.

[58] PERCIVAL C. Stronger key derivation via sequential memory-hard functions[EB/OL]. http://www.bsdcan.org/2009/schedule/attachments/87_scrypt.pdf. 2009.

[59] BIRYUKOV A, KHOVRATOVICH D. Equihash: Asymmetric proof-of-work based on the generalized birthday problem[C]. In: Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS). San Diego, CA, USA, 2016. [DOI: 10.14722/ndss.2016.23108]

[60] KING S, NADAL S. PPcoin: Peer-to-peer crypto-currency with proof-of-stake[EB/OL]. https://peercoin.net/assets/paper/peercoin-paper.pdf. 2012.

[61] The NXT Community. Nxt Whitepaper[EB/OL]. https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf. 2014.

[62] DAIAN P, PASS R, SHI E. Snow white: Provably secure proofs of stake[J]. IACR Cryptology ePrint Archive, 2016: 2016/919. https://eprint.iacr.org/2016/919.

[63] KWON J. Tendermint: Consensus without mining[EB/OL]. https://tendermint.com/static/docs/tendermint.pdf. 2014.

[64] Proof of burn[EB/OL]. https://en.bitcoin.it/wiki/Proof_of_burn.
[65] MILLER A, JUELS A, SHI E, et al. Permacoin: Repurposing Bitcoin work for data preservation[C]. In: Proceedings of 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 475–490. [DOI: 10.1109/SP.2014.37]
[66] DZIEMBOWSKI S, FAUST S, KOLMOGOROV V, et al. Proofs of space[C]. In: Advances in Cryptology—CRYPTO 2015, Part II. Springer Berlin Heidelberg, 2015: 585–605. [DOI: 10.1007/978-3-662-48000-7_29]
[67] ABUSALAH H, ALWEN J, COHEN B, et al. Beyond Hellman's time-memory trade-offs with applications to proofs of space[C]. In: Advances in Cryptology—ASIACRYPT 2017, Part II. Springer Cham, 2017: 357–379. [DOI: 10.1007/978-3-319-70697-9_15]
[68] INTEL. Sawtooth lake–introduction[EB/OL]. https://intelledger.github.io/introduction.html. 2016.
[69] ZHANG F, EYAL I, ESCRIVA R, et al. REM: Resource-efficient mining for blockchains[C]. In: Proceedings of the 26th USENIX Security Symposium. USENIX, 2017: 1427–1444.
[70] MAHMOODY M, MORAN T, VADHAN S. Publicly verifiable proofs of sequential work[C]. In: Proceedings of the 4th Conference on Innovations in Theoretical Computer Science (ITCS). ACM, 2013: 373–388. [DOI: 10.1145/2422436.2422479]
[71] COHEN B, PIETRZAK K. Simple proofs of sequential work[C]. In: Advances in Cryptology—EUROCRYPT 2018, Part II. Springer Cham, 2018: 451–467. [DOI: 10.1007/978-3-319-78375-8_15]
[72] MORAN T, ORLOV I. Proofs of space-time and rational proofs of storage[J]. IACR Cryptology ePrint Archive, 2016: 2016/035. https://eprint.iacr.org/2016/035.
[73] VUKOLIC M. Eventually returning to strong consistency[J]. IEEE Data Engineering Bulletin, 2016, 39(1): 39–44.
[74] MICALI S. ALGORAND: The efficient and democratic ledger[J]. arXiv:1607.01341v6, 2017.
[75] LUU L, NARAYANAN V, ZHENG C D, et al. A decure sharding protocol for open blockchains[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2016: 17–30. [DOI: 10.1145/2976749.2978389]
[76] PASS R, SHI E. Hybrid consensus: Efficient consensus in the permissionless model[C]. In: Proceedings of the 31st International Symposium on Distributed Computing (DISC). Dagstuhl, Germany, 2017: 39. [DOI: 10.4230/LIPIcs.DISC.2017.39]
[77] DOUNG T, FAN L, ZHOU H. 2-hop blockchain: Combing proof-of-work and proof-of-stake securely[J]. IACR Cryptology ePrint Archive, 2016: 2016/716. https://eprint.iacr.org/2016/716.
[78] KOGIAS E, JOVANOVIC P, GAILLY N, et al. Enhancing Bitcoin security and performance with strong consistency via collective signing[C]. In: Proceedings of the 25th USENIX Security Symposium. USENIX, 2016: 279–296.
[79] REID F, MARTIN H. An analysis of anonymity in the Bitcoin system[C]. In: Security and Privacy in Social Networks. Springer Berlin Heidelberg, 2012: 197–223. [DOI: 10.1007/978-1-4614-4139-7_10]
[80] BARBER S, BOYEN X, SHI E, et al. Bitter to better—How to make Bitcoin a better currency[C]. In: Financial Cryptography and Data Security—FC 2012. Springer Berlin Heidelberg, 2012: 399–414. [DOI: 10.1007/978-3-642-32946-3_29]
[81] RON D, SHAMIR A. Quantitative analysis of the full Bitcoin transaction graph[C]. In: Financial Cryptography and Data Security—FC 2013. Springer Berlin Heidelberg, 2013: 6–24. [DOI: 10.1007/978-3-642-39884-1_2]
[82] MAXWELL G. Confidential transactions[EB/OL]. https://people.xiph.org/ greg/confidential_values.txt.
[83] BEN-SASSON E, CHIESA A, GARMAN C, et al. Zerocash: Decentralized anonymous payments from Bitcoin[C]. In: Proceedings of 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 459–474. [DOI: 10.1109/SP.2014.36]
[84] CECCHETTI E, ZHANG F, JI Y, et al. Solidus: Confidential distributed ledger transactions via PVORM[C]. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, 2017: 701–717. [DOI: 10.1145/3133956.3134010]
[85] CAMENISCH J, CHAABOUNI R, SHELAT A. Efficient protocols for set membership and range proofs[C]. In: Advances in Cryptology—ASIACRYPT 2008. Springer Berlin Heidelberg, 2008: 234–252. [DOI: 10.1007/978-3-540-89255-7_15]
[86] MA S L, DENG Y, HE D B, et al. An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain[J]. IACR Cryptology ePrint Archive, 2017: 2017/1239. https://eprint.iacr.org/2017/1239.
[87] BUNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: Efficient range proofs for confidential transactions[J]. IACR Cryptology ePrint Archive, 2017: 2017/1066. https://eprint.iacr.org/2017/1066.
[88] FUJISAKI E, OKAMOTO T. Statistical zero knowledge protocols to prove modular polynomial relations[C]. In: Advances in Cryptology—CRYPTO'97. Springer Berlin Heidelberg, 1997: 16–30. [DOI: 10.1007/BFb0052225]
[89] BOUDOT F. Efficient proofs that a committed number lies in an interval[C]. In: Advances in Cryptology—

EUROCRYPT 2000. Springer Berlin Heidelberg, 2000: 431–444. [DOI: 10.1007/3-540-45539-6_31]
[90] CHAN A, FRANKEL Y, TSIOUNIS Y. Easy come–easy go divisible cash. Updated version with corrections [EB/OL]. http://www.ccs.neu.edu/home/yiannis/. 1998.
[91] SABERHAGEN N. Cryptonote v 2.0[EB/OL]. https://cryptonote.org/whitepaper.pdf. 2013.
[92] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: Anonymous distributed e-cash from Bitcoin[C]. In: Proceedings of 2013 IEEE Symposium on Security and Privacy (SP). IEEE, 2013: 397–411. [DOI: 10.1109/SP.2013.34]
[93] BEN-SASSON E, CHIESA A, GARMAN C, et al. Snarks for C: Verifying program executions succinctly and in zero knowledge[C]. In: Advances in Cryptology—CRYPTO 2013, Part II. Springer Berlin Heidelberg, 2013: 90–108. [DOI: 10.1007/978-3-642-40084-1_6]
[94] KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]. In: Proceedings of 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016: 839–858. [DOI: 10.1109/SP.2016.55]
[95] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub[C]. In: Proceedings of the 24rd Annual Network and Distributed System Security Symposium (NDSS). San Diego, CA, USA, 2017. [DOI: 10.14722/ndss.2017.23086]
[96] ZIEGELDORF J, GROSSMANN F, HENZE M, et al. Coinparty: Secure multi-party mixing of Bitcoins[C]. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY). ACM, 2015: 75–86. [DOI: 10.1145/2699026.2699100]
[97] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: Practial decentralized coin mixing for Bitcoin[C]. In: Computer Security—ESORICS 2014. Springer Berlin Heidelberg, 2014: 345–364. [DOI: 10.1007/978-3-319-11212-1_20]
[98] MAXWELL G. CoinJoin: Bitcoin privacy for the real world[EB/OL]. http://bitcointalk.org. 2013.
[99] EYAL I, GENCER A, SIRER E, et al. Bitcoin-NG: A scalable blockchain protocol[C]. In: Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI). USENIX, 2016: 45–59.
[100] POON J, DRYJA T. The Bitcoin lightning network: Scalable off-chain instant payments (v0.5.9.2)[EB/OL]. https://lightning.network/lightning-network-paper.pdf. 2016.
[101] BACK A, CORALLO M, DASH L JR. Enabling blockchain innovations with pegged sidechains[EB/OL]. https://www.blockstream.ca/sidechains.pdf. 2014.
[102] Raiden network[EB/OL]. https://raiden.network/.
[103] Reversecoin[EB/OL]. http://www.reversecoin.org/.
[104] PUDDU I, DMITRIENKO A, CAPKUN S. μchain: How to forget without hard forks[J]. IACR Cryptology ePrint Archive, 2017: 2017/106. https://eprint.iacr.org/2017/106.
[105] CHASE M, KOHLWEISS M, LYSYANSKAYA A, et al. Malleable signatures: New definitions and delegatable anonymous credentials[C]. In: Proceedings of 2014 IEEE 27th Computer Security Foundations Symposium (CSF). IEEE, 2014: 199–213. [DOI: 10.1109/CSF.2014.22]

作者信息

单进勇 (1987–), 江苏大丰人, 博士. 主要研究领域为数字货币与区块链、密码理论与应用等.
shan20051@126.com

高胜 (1982–), 山西朔州人, 博士, 高级工程师. 主要研究领域为数字货币与区块链、密码理论与应用等.
gs14011@163.com