密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2017,4(2):176–186

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

比特币与法定数字货币*

秦 波[1], 陈李昌豪[1], 伍前红[2], 张一锋[3], 钟 林[2], 郑海彬[2]

1. 中国人民大学 信息学院, 北京 100872
2. 北京航空航天大学 电子信息工程学院, 北京 100191
3. 中钞信用卡产业发展有限公司 北京智能卡技术研究院, 北京 100088
通讯作者: 伍前红, E-mail: qianhong.wu@buaa.edu.cn

摘 要: 比特币是一种开放的密码货币, 它的诞生与流通标志着以信息产生与流动为特征的互联网络加速迈入以价值产生与转移为特征的价值互联网新时代. 本文首先综述比特币的发展、体系架构, 分析比特币在无信任环境下利用现代密码学方法在去中介、去中心化、公开可验证和点对点支付等方面的技术优势, 以及比特币对法定货币的冲击. 在分析比特币研究与应用基础上, 指出比特币系统资源浪费严重、可扩展性差、吞吐率低、交易延迟过长、缺少系统级安全论证、隐私保护不足、难以审计监管从而带来金融犯罪等诸多方面的问题. 最后, 面向法定数字货币设计需求, 论文探讨吸收类比特币数字货币的技术优势, 发展和创新现代密码理论与技术, 解决法定数字货币设计面临的技术挑战, 调和便利性需求和安全性需求之间的功能性冲突, 解决隐私保护、金融情报机密性需求, 与安全审计、监管、追踪、打击违法犯罪活动需求之间的技术性冲突, 从而保障货币政策的有效运行和传导, 确保法定机构对货币主权的控制.

关键词: 密码货币; 比特币; 区块链; 法定数字货币
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000172

中文引用格式: 秦波, 陈李昌豪, 伍前红, 张一锋, 钟林, 郑海彬. 比特币与法定数字货币[J]. 密码学报, 2017, 4(2): 176–186.
英文引用格式: QIN B, CHEN L C H, WU Q H, ZHANG Y F, ZHONG L, ZHENG H B. Bitcoin and digital fiat currency[J]. Journal of Cryptologic Research, 2017, 4(2): 176–186.

Bitcoin and Digital Fiat Currency

QIN Bo[1], CHEN Li-Chang-Hao[1], WU Qian-Hong[2], ZHANG Yi-Feng[3], ZHONG Lin[2], ZHENG Hai-Bin[2]

1. School of Information, Renmin University of China, Beijing 100872, China
2. School of Electronic and Information Engineering, Beihang University, Beijing 100191, China
3. Beijng Smart Card Technology Research Institute, Zhongchao Creditcard Industry Development Co., LTD. Beijing 100088, China
Corresponding author: WU Qian-Hong, E-mail: qianhong.wu@buaa.edu.cn

Abstract: The emergence and circulation of Bitcoin, an open cryptocurrency, indicates that the Internet characterized by information generation and mobility is entering a new era of Internet of values, featured with value generation and transfer. This paper first surveys the development and architecture of Bitcoin, discusses the technical advantages in point-to-point payment achieving public verifiability and safe transaction based on

* 基金项目: 国家自然科学基金项目(61672083, 61370190, 61472429); 国家自然科学基金重点项目(61532021)
收稿日期: 2017-03-23 定稿日期: 2017-04-02

modern cryptographic technologies in the absence of trust, mediation and centralized authority, and explores the impact of Bitcoin on fiat currencies. By analyzing the research and application of Bitcoin, this paper identifies its deficiencies of resource waste, poor scalability, low throughput, long transaction latency, unresolved security, privacy leakage risk, tool for extortion and money laundering free from governmental audit and supervision and so on. Finally, oriented by digital fiat currency, by incorporating the advantages of Bitcoin like cryptocurrencies and innovating the modern cryptography theory and technology, this paper discusses the technical challenges in developing digital fiat currency, consisting of reconciling the convenience demand and the safety requirement, balancing between the privacy protection, financial intelligence confidentiality needs, and audit, supervision, forensics of monetary crimes, so as to ensure the effective operation and transmission of the monetary policies, and the statutory control of monetary sovereignty.
Key words: cryptocurrency; Bitcoin; blockchain; digital fiat currency

1 引言

2008 年 10 月 31 日, 一个化名中本聪的人在一个隐秘密码学论坛上公开了一篇题目为《比特币: 一种点对点电子现金系统》的报告[1], 悄然掀开了互联网新的一页. 次年 1 月, 中本聪发布了比特币系统软件的开源代码, 并发行了第一批 50 枚比特币, 一种全新的虚拟货币诞生了. 随后, 逐渐有新技术爱好者加入比特币这种虚拟货币系统的开发与维护、持有或交易比特币, 形成了比特币社区. 2010 年 5 月 22 日, 程序员 Hanyecz 花费 10000 比特币向比特币论坛用户购买了两个披萨, 比特币首次实现了由名义货币向实物货币的转变. 根据比特币观察网, 截止 2017 年 3 月 29 日, 已发行 1600 多万比特币, 总值超过 170 亿美元. 从此, 以信息产生与流动为特征的互联网络加速迈入以价值产生与转移为特征的价值互联网新时代.

比特币是一种开放的密码货币系统. 任何人可以随时加入或离开比特币系统, 成为其中一个点对点网络的节点, 获得货币发行和交易的权利. 比特币交易必须得到全网节点的共识, 交易单被收集整理成区块并记录到全网唯一的一条数据链上, 该链被称为区块链. 形成的全网唯一的区块链也称为比特币账本, 所有节点都可以读取和验证该账本上的所有交易, 保存并实时更新该账本的拷贝. 最先将一些新交易单验证并记录到链上, 证明自己完成了要求的工作量, 并得到全网其他节点认可的节点将获得一定数量比特币的奖励, 产生一个特殊的交易, 这个过程称为挖矿, 这样的节点也被称为矿工. 用户加入节点也可以只持有或交易比特币, 而不参与挖矿以发行比特币. 区块链浓缩了诸多密码技术, 决定着数字货币发行、价值产生(物化)、交易流通的特征, 并提供数字货币防伪、防双花、交易方身份隐私等安全与隐私保护功能, 因此, 区块链构成了密码货币和价值互联网的基因.

比特币相较于传统法定货币或其他传统电子货币具有显著优势. 首先, 结合点对点网络技术与现代密码技术, 比特币系统具有很强的系统健壮性和抗攻击能力. 虽然兑换法定货币的比特币兑换平台时不时爆出被黑客攻破的报道, 然而, 迄今对开源并公开运行的比特币系统本身没有发现任何成功的攻击, 也没有发现严重的漏洞. 第二, 比特币使用便捷, 发行和交易完全采用电子方式, 交易安全由密码算法保证, 社会信用成本极低. 与此相对, 传统货币发行中制版、印刷、押运需要高昂成本. 比特币采用去中心化结构, 所有交易不需要中介, 支持用户到用户的直接交易, 可以在全球/网范围内用假名实时转账; 与此相对比, 传统货币转账需要中介/银行的参与, 涉及复杂的清结算手续和高昂的交易成本, 尤其是跨国转账极为复杂且存在隔夜汇差风险. 第三, 比特币安全性高, 保护用户隐私. 比特币采用已被理论和实践证明安全的现代密码技术, 能有效防止对比特币的伪造和重复花费, 并保护用户交易的身份隐私. 而在传统货币中, 假币难以识别, 几乎所有传统货币下都有大量用户蒙受过假币造成的损失, 打击假币耗费了大量的人力、物力和财力. 第四, 比特币使一种可编程的数字代码成为可自动交易的货币, 按时序以不可抵赖的方式记录, 交易可公开验证和审计, 使得实现密码学家设计的智能合约成为可能, 高效解决维系社会运行的传统

合约系统中合约签署与执行中的高昂成本, 并在很大程度上消除信用违约风险以及由此造成的社会经济问题.

比特币为传统金融系统同时带来严峻挑战和新的机遇. 比特币由于其安全便捷等优势, 吸引了日益众多的参与者. 目前每天全网比特币交易量近 30 万笔, 交易金额按美元计接近 20 亿美元. 越来越多的个人与商户接受比特币的支付. 以日本为例, 据统计, 2016 年已有 4200 家商户接收比特币付款, 比 2015 年的 4 倍还多, 预计这样的商户在 2017 年将达到 2 万户. 任由难以监管的类比特币等私人发行的数字货币野蛮生长,必将造成货币入侵和金融污染, 严重侵蚀法定货币的地位, 干扰宏观经济调控政策与金融政策的运行与传导, 并为洗钱、敲诈、勒索等违法犯罪活动提供地下资金通道. 为了充分利用数字货币的优势, 减少或杜绝私人发行数字货币造成的风险, 部分国家的中央银行、商业银行积极探索研究与实现法定数字货币, 逐步形成了竞争性研究的趋势. 英国于 2016 年率先提出可由央行调控的 RSCoin 数字货币框架[2]. 2016 年 1 月 20 日, 中国人民银行召开研讨会, 宣布已经启动央行发行的法定数字货币的研究. 考虑到各种因素, 2 月 13 日央行行长周小川在接受采访中指出, 面向大众的法定数字货币推出还没有既定的时间表. 2017 年 1 月 25 日, 媒体报道我国央行正推动基于区块链的数字票据交易平台的验证与测试, 引发业内广泛关注. 2 月 27 日, 央行科技司司长李伟在接受媒体采访时强调, 数字票据交易符合区块链适用的场景, 即非实时、轻量级信息、交易量小、信息敏感度较低; 然而, 支撑一个国家法定数字货币系统运转的技术则需要适用于实时、高频、大额交易. 因此, 迫切需要对相关技术进行深入、系统的研究.

伴随比特币的流行与成功, 全球各主要国家和工业界高度重视类比特币系统的研究和应用. 2013 年 8 月, 德国宣布承认比特币的合法地位, 纳入国家监管体系并表示比特币可当作私人货币和货币单位. 2015 年 1 月, 纽交所入股的 Coinbase 成立比特币交易所, 美国以纽约州为代表的比特币监管立法进程初步完成, 并发布了最终版本的监管框架 Bit License. 2015 年 3 月, 英国财政部发布相关报告, 建议反洗钱法规将适用于英国的比特币交易所, 英国财政部将商议监管的模式, 英国政府将与英国标准协会(BIS)以及行业共同制定一个“最佳”的监管框架. 2016 年 5 月, 日本批准比特币监管法案, 并将其定义为财产. 基于对类比特币底层区块链技术全球发展趋势的研判, 以及我国区块链技术和应用发展的现状和趋势, 2016 年 10 月 18 日我国工信部发布了《中国区块链技术和应用发展白皮书》, 围绕扶持政策、技术攻关和平台建设、应用示范等方面提出了相关建议.

以比特币为代表的融合密码学、互联网的新技术正在重塑我们的物理社会. 现代密码学使得人们在无信任的环境下能够防范欺诈, 并防止信息被非授权获取. 移动互联网将人们随时随地联系在一起, 打破了传统时空对人们的社会行为的限制. 移动互联网与现代密码学的结合有望帮助人们突破时空和信任的藩篱, 从而重塑后信息时代的物理社会, 比特币的诞生与流行即是一个显著的例子. 然而, 比特币作为一种私人发行的货币, 未有任何法定机构为其信用背书; 而且, 货币发行被视为国家主权行为之一, 因此需要借鉴比特币的先进技术, 结合国家对数字货币的需求, 研究法定数字货币的设计与实现, 调和便利性需求和安全性需求之间的功能性冲突, 解决隐私保护、金融情报机密性需求, 与安全审计、监管, 追踪、打击违法犯罪行为需求之间的技术性冲突, 保障货币政策的有效运行和传导, 确保法定机构对货币主权的控制.

研究和部署法定数字货币系统具有多方面的意义. 首先, 研究法定数字货币系统安全具有重要的科学意义. 密码学是保障数字货币系统安全的关键性技术方法. 与私人数字货币不同, 面向国家需求的法定数字货币系统需要保守国家金融秘密, 保护交易者隐私, 同时必须保证安全审计、安全监管和打击犯罪等需求, 这对密码技术提出了更高的要求. 研究适用于法定数字货币的密码学技术, 必将创新和发展现有密码学理论和技术. 第二, 研究和部署法定数字货币系统具有重要的经济意义. 我们所处的信息化时代一个突出特征是经济活动数字化, 其中货币的安全数字化, 可以消除传统货币设计、印制的成本和押运、存储和流通过程中被盗抢的风险, 极大地减少跨地域、跨机构的资金流通成本, 减少货币流通障碍; 而且, 货币

数字化有利于实现对货币总量、流向和流速等的精准调控, 保障国家宏观经济政策和货币政策的有效运行和传导, 促进经济发展. 第三, 研究和部署法定数字货币系统具有重要的社会意义. 数字货币不只是简单地将货币进行数字方式记账或符号化, 而且可以使数字化后的货币支持代码执行, 这是数字货币与传统电子货币或虚拟货币, 包括信用卡、银行储蓄卡、支付宝、微信支付和游戏币等的本质区别之一. 可自动执行、能编程的数字货币呈现智能化的特征, 通过自动且可信执行的智能合约可以在技术上提供降低合约背离和信用违约风险的新手段, 有利于建设和谐的信用社会.

2 比特币研究现状与发展动态

尽管比特币取得了巨大成功, 但是随着研究的深入, 人们发现它还有诸多方面的缺陷, 尤其是改造比特币成为一个国家的法定数字货币系统还需解决多方面的理论与技术难题.

2.1 比特币的系统设计缺陷

比特币系统一个广受诟病的缺陷是其需要消耗大量能源以产生比特币并保障比特币安全流通, 使得比特币经济体已成为高耗能的资本密集型行业. 为了防止双重花费, 比特币挖矿和记账采用对密码学杂凑函数部分求逆的工作量证明(POW, Proof Of Work)机制, 需要极为高昂的计算, 严重浪费资源. Gervais 等[3]提出了一个量化框架, 分析 POW 区块链在不同共识和网络参数中的安全性和性能, 以及安全性和效率之间的转换. King 等[4]指出 POW 机制主要在初始挖矿阶段起作用, 在比特币长期运行中并非至关重要, 提出采用权益证明机制(POS, Proof Of Stake)代替 POW 机制, 依据币龄在有限空间寻找随机值, 通过中央广播的校验机制, 保护区块链历史和交易处理, 可提供更好的安全性. Duong 等[5]结合 POW 机制和 POS 机制, 利用诚实矿工资源优势以及诚实用户的币龄/权益(cions/stake), 提出可证安全的 2 级区块链. Dziembowski 等[6]和 Park 等[7]提出向系统贡献存储空间的空间证明协议, 用于替代比特币协议中 POW 机制. 在基于空间证明的空间挖矿(SpaceMint)中, 矿工仅需关注磁盘空间而非算力, 解决比特币挖矿动力降低以及维持货币运行需要浪费大量能源等问题. Bentov 等[8]结合 POW 和 POS 机制, 在比特币协议基础上提出了一种活动证明(POA, Proof Of Activity)机制, 在网络通信和存储空间方面所需开销较低, 并具有较高的安全性. 目前已有的 POW 机制、POS 机制及其改进机制仍然会导致矿池垄断、交易确认缓慢、财富集中、资源浪费等一个或多个方面的问题, 因此需要研究更加高效、公平、低资源消耗的交易确认机制.

对法定数字货币而言, 比特币系统的一个严重问题是它的系统吞吐率极低, 难以支持法偿货币的日常交易. 当前的比特币系统仅能支持每秒 7 笔交易[9], 远远不能满足大规模应用需求. 为了解决该问题, 研究人员不断引入新技术, 比如扩容和闪电网络等方案. 其中, 扩容包括隔离见证和硬分叉区块扩容[10−12]. 闪电网络是一种侧链技术, 能够大幅减轻主链的交易负担, 拓展更多的支付模式[13]. 与此同时, Sompolinsky 等[14]在高交易吞吐量的情况下, 提出了使用比特币节点构造和重组区块链的变形 GHOST 准则来解决效率问题. Kiayias 等[15]研究了可证明安全与交易速度之间的关系, 把交易速度视为区块生成率的函数, 提出用区块可生长性证明交易账簿的鲁棒性和安全性. Eyal 等[16]引入新的利益度量方法, 用于分析类比特币区块链协议的安全性和效率之间的关系. Micali 提出一种高效的公开账本协议[17], 是权益证明机制的一种变型, 可以解决比特币交易延迟、能源浪费和分叉问题, 该协议需要假定攻击者数量或攻击者控制的资产数量低于总数量的 1/3. Luu 等[18]提出一种分片记账机制, 通过将全网划分成多个片区, 各个片区由各自的委员会进行记账, 从而提高系统的吞吐率, 代价同样是需要假设攻击者算力至多占全网算力的 1/3. Zhu 等提出利用交互式不可否认签名方案加速比特币交易速度[19]. Miller 等[20]提出一种蜜獾拜占庭协议, 采用一种原子广播技术, 可以大大缩短达成拜占庭共识需要的时间, 从而提高系统的吞吐率. 一方面, 该方案松弛了同步的要求, 可以是完全异步网络; 另一方面, 该方案假定所有节点之间认证链接, 所有消息不会被丢弃, 诚实节点之间的消息最终是可达的. 这些假设和开放的数字货币网络现状不完全一致. 在各种改进的类比

特币系统中, 已有系统宣称可以支持每秒上万次交易, 然而与此对比, 全球 VISA 支付网络可处理的每秒交易频次为 4 万次, 支付宝在 2016 年双十一活动中每秒需要处理的交易峰值已达到了 12 万次. 法定数字货币意味着一国任何时间所有交易都将由系统完成, 现有类比特币系统还远远没有如此超大规模的处理能力, 因此亟需研究可支持高吞吐率、低交易延迟的法定数字货币系统.

2.2 比特币的安全与隐私问题

比特币的另一个问题是系统是否安全仍然不得而知. 在可预见的将来, 尽管计算技术的发展不会对比特币所使用的密码学组件构成威胁, 然而在系统级别, 它是否安全, 能否持续运行下去, 迄今没有已证明的公开结论, 这可能出乎很多人士的预料. 例如, 设计者的初衷是实现一种去中心化, 不受任何个人或组织控制、公平的货币系统. 为此目的, 比特币一开始就允许任何人随意加入或离开节点, 自愿决定是否参与发行比特币. 然而, 由于竞争机制的引入, 目前个人甚至小的组织通过挖矿获得比特币已经风险大过收益. 比特币的发行甚至其未来走向, 越来越受到极少数具有超级算力的矿主和矿池控制, 偏离了设计者的初衷.

目前对比特币系统组件之间的关系已有一些零星的理论成果. Kiayias 等[15]研究了可证明安全性与交易速度之间的关系, 把交易速度视为区块生成率的函数, 提出用区块可生长性证明交易账簿的鲁棒性和安全性. Eyal 等[16]提出了容忍拜占庭错误的下一代比特币(Bitcoin-NG)系统, 引入新的利益度量方法, 用于量化类比特币区块链协议的安全性和效率. Velner 等[21]提出一种新的攻击, 在运行智能合约的情况下, 比特币矿池很容易被恶意参与的矿工攻破. Forte 等[22]指出, 在基于区块链的系统中大规模的挖矿是不可持续的, 并针对比特币系统安全、激励、竞争与协作问题, 提出了一种新的算法框架以实现在不同背景下基于区块链的系统的可持续性. 对于基于 POW 机制的类比特币系统, Vasin 提出一种方法[23], 旨在防范币龄被恶意节点滥用以获得更大网络权重, 实现双重花费等问题. Garay 等[24]对类比特币协议进行了抽象处理, 提出了比特币骨架协议, 在同步或部分同步网络环境下假定攻击者占少数, 对比特币的系统级安全进行了分析. 在该分析框架中, 算力在各参与者中均匀随机分布, 这和比特币的现实并不一致. 这些方案从不同角度分析或改进比特币系统的安全性和可持续性. 然而, 无论是原始比特币系统还是其改进系统, 都没有给出符合其运行现状的系统级安全论证, 也未给出系统是否安全或可持续的判别准则.

比特币系统的另一个缺陷是其仅能提供较弱的隐私保护. 由于比特币系统公开交易金额, 因此必须保护交易者的身份隐私. 比特币采用一次性公钥, 用公钥作为用户假名和账号, 从而提供对交易者身份的隐私保护. 最初, 设计者和大众认为, 由于用户每次交易可以采用不同的假名, 因而比特币具有很好的隐私保护能力, 这也是比特币一开始就受到青睐的重要原因之一. 然而, 最近的分析和研究表明[25–30], 随着比特币从虚拟货币向实物货币转化, 当用户需要利用比特币购物时, 其付款所用假名或账号立即将用户的个人信息泄露了. 同样, 当用户公开自己的比特币假名以接受付款或捐款时, 其在比特币系统中的真实物理身份也暴露了. 更为严重的是, 由于全网交易账本可以公开获取, 比特币找零地址进一步泄露了该用户历史上的比特币账号, 从而大大削弱了比特币系统的用户隐私保护能力. 近期的分析[31]还表明, 即使采用匿名路由, 比特币系统也不能提供真正的匿名保护, 甚至变得更加糟糕.

比特币用户隐私泄露主要有两个方面的原因. 一是公开的交易额、交易元数据和全网账本使得攻击者可以提取有关用户身份特征的大量信息. 二是交易中付款账号与收款账号明确关联的特征使得攻击者可以追踪整个历史交易路径, 结合比特币作为实物货币时的真实身份泄露, 系统的隐私保护能力被严重削弱. 针对这两个方面, 人们相继提出了各种改进比特币匿名性的方法. Bonneau 等提出 Mixcoin 协议[32], 试图打乱支付账号和收款账号之间的关系, 从而提高比特币及类似系统的匿名性. Wijaya 等亦通过解除交易双方关联性, 提出了一种增强比特币匿名性的改进方案[33]. Maxwell 提出 Coinjoin 混币技术, 混淆比特币交易数据中用户敏感信息的关联性[34], 但仍可以通过找零地址金额不对称分析出地址/账号之间的关联性.

Saberhagen 提出利用环签名和隐蔽地址技术建立匿名性更高的电子现金方案 CryptoNote[35]. 在该方案中, 用户的地址(账号)长度约为普通比特币地址长度的两倍, 增加了数据存储的开销, 而且环签名的验证复杂性随着提供的匿名程度呈线性增长, 并需要全网节点的验证与确认, 使类比特币系统中的资源耗损问题更加严重. 霍普金斯大学的 Miers 等[36]基于零知识证明技术提出了一种扩展比特币方案 Zerocoin, 并建立分散式"清洗"机制, 该方案系统效率和性能较低. Groth 和 Kohlweiss 给出了一个对数复杂性的多选一零知识证明协议[37], 可以用于强化比特币协议中交易发起方身份隐私. 根据 E-cash 的思路, Heilman 等[38]提出基于盲签名的比特币匿名协议, 增强比特币的匿名性和公平性, 从而增强用户隐私保护. Ben-Sasson 等在 Zerocoin 协议的基础上进一步提出了 Zerocash[39], 利用 zk-SNARKs 非交互式零知识证明算法[40]实现匿名性更强的电子现金系统, 并保护交易额的隐私. 到目前为止, Zerocash 是提供最强用户隐私保护的系统之一, 然而它需要人们相信系统开发人员诚实地销毁了系统启动用到的秘密参数, 但这是不可证实的. Zerocash 将匿名性增强建立在对特定人群的信任假设之上, 背离了类比特币的去信任化初衷. 因此, 交易方的隐私保护, 尤其是交易额隐私, 交易元数据的保护还需更加深入的研究.

2.3 比特币的审计与监管问题

比特币的设计旨在绕开任何现行组织或机构的监管, 这与法定货币的监管需求严重不符. 由于监管机制的缺失, 没有任何机构或组织为比特币做信用背书, 容易出现频繁的剧烈币值波动, 并滋生利用比特币偷税漏税、勒索洗钱等违法犯罪; 而且, 比特币的日益流行不断侵蚀各国的货币主权, 甚至使各国利用货币发行与流通实施的宏观经济调控政策失效. 正因为此, 多数国家对比特币在本国的流通都持谨慎的态度, 接受比特币的国家同时提出要加强对比特币的监管. 尽管比特币未能实现真正的匿名, 但这是对攻击者而言的. 犯罪分子利用比特币系统中用户的身份信息泄露发起敲诈勒索等攻击, 并不需要唯一确定比特币账号所有人的身份, 只需将目标攻击对象缩小到一定范围即可. 与此不同, 对于政府监管或司法调查来说, 则需要唯一确定某账号所有人, 并能关联该用户其他所有账号, 比特币匿名机制保证了对正确使用比特币系统的账号难以建立这样的关联关系, 因此对比特币的监管难度极大.

一些最近的研究工作探讨了加强对比特币监管的方法. 针对比特币兑换平台在资不抵债的情况下运行给用户带来的风险, Dagher 在比特币系统中提出了一种保护隐私的准备金证明方法[41]. 但是该方法并不能保证用户的未来资产安全, 因为兑换平台在完成资产证明后其资产仍然可能因为各种原因消失, 从而失去对平台用户比特币资产的担保能力. Ogunbadewa 提出政府需要和投资专家建立"高科技犯罪"的执法机构计划[42], 通过对比特币地址进行追踪, 实现在比特币经济体内的在线监控. Kaplanov[43]提出一种利用第三方兑换平台跟踪和定位非法使用比特币的方案. Marian[44]鼓励用户标识个人识别号码, 放弃比特币系统提供的匿名性保护, 以提高对匿名犯罪可疑用户的检测概率, 从而查处和制裁利用比特币系统进行违法犯罪活动的交易人. 最近, 有学者提出"多中心化"的类比特币替代方案[45], 通过对各个中心赋予特殊权限, 实现对数字货币系统的监管. 显然, 这些加强比特币监管的方案的可行性需要实践的检验.

由于比特币从设计原理上就非常注重匿名性、不可逆性等特点, 从政策法规与技术补充层面进行监管似乎难以从根本上防范比特币带来的洗钱、地下钱庄以及作为违法犯罪潜在资金通道的风险. 从各国公开的监管措施实施现状来看, 由于各国不能改变比特币本身的形态, 几乎都是通过严格控制比特币与该国法定货币兑换的入口和出口来实施监管. 然而, 一旦获得比特币, 由于其匿名性, 其交易就会完全脱离监管, 通过比特币兑换平台入口和出口进行监管所能获得的监管力度与效果非常有限. 因此, 解决隐私保护与安全监管的冲突是设计法定数字货币需要突破的关键技术.

2.4 比特币的变型与扩展

比特币的成功吸引人们研究了多种变型和扩展. 比特币以账簿的方式公开记录用户交易, 该过程具有交易公开性、身份隐私性、交易不可逆等特点. 随着类似于比特币的系统越来越多, 它们彼此隔离, 因

此一些研究致力于使不同类比特币系统互联互通. Back 等[46]提出一种把攻击完全限制在侧链内部的楔入式侧链, 用户可以根据已有资产访问新的系统, 完成比特币和其他分账资产在多个区块之间的转移. Muadh 提出以两种方式楔入主链的侧链技术[47], 比特币可以在主链和侧链之间来回转移, 侧链中的比特币可以用主链进行操作, 但侧链出现的安全问题不会影响到主链. Todd 提出树状区块链[48], 将交易数据随机分布到整个树的最底层, 独立矿工可任意挑选底链, 在叶子节点进行安全挖矿. Lewenberg 等[49]提出了一种由区块包含有向非循环图(DAG, Directed Acylic Graph)组成的区块链系统结构, 用以提高区块容量. 它允许区块参考多个处理器的生成结果, 支持更宽松的、融合似乎矛盾的区块交易接受准则, 可容忍大区块更长的传播时间. Poon 提出一种新的去中心化的交易系统[13], 利用地址可扩展的签名摘要进行签名, 通过合同验证交易路线的方式, 在不可信参与方之间实现价值转让, 并防范不合作参与方和恶意参与方. 另一些研究工作致力于扩展比特币系统的功能和应用. 笔者与合作者于 2015 年提出基于部分盲门限签名的比特币协同交易模型和协议[50], 随后, 笔者与合作者提出了一种基于属性的比特币账号联合监管方法[51]. Wood 扩展比特币系统的单一交易运行模式, 提出以太坊智能合约[52], 通过信息传递框架进行沟通, 可根据不同状态和运算指令完成去中心化的任意计算服务.除了对比特币进行功能扩展外, 一些研究工作基于比特币及其底层区块链技术提出了新颖的应用. Zerocoin 方案描述了在不可信 P2P 网络环境下的诸多应用, 包括自组织方式的资源管理、匿名认证、可审计账户等[35,38,53]. Kumaresan 等[54]设计了具有奖罚功能的多方计算协议, 以及无可信中心的安全智能合约. Bentov 等[55]研究安全多方计算的公平性模型, 基于比特币网络, 提出了公平多方计算和公平彩票协议. 为了惩罚不诚信的协议方, Ruffing 等[56]利用可审计密码模型以及区块链技术, 设计了无可信中心的智能合约. 笔者与 Huang 等[57]提出了基于比特币的公平付费协议. Zhang 等提出了基于区块链的物联网安全模型[58].

一些扩展变型的密码货币也得到了市场的认可。目前市场占有率排名前五的密码货币分别是比特币, 以太坊(Ethereum), 达世币(Dash), 门罗币(Menero), 瑞波币(Ripple). 以太坊由 ETHDEV 团队开发, 是去中心化智能合约平台, 应用程序在该平台上运行, 没有停止时间, 不受审查机构、欺骗、第三方干扰等影响, 市场占有率 39.7 亿美元. 以太坊可以视为一台“全球计算机”, 任何人都可以上传和执行应用程序, 并且程序的有效执行能得到保证, 这种保证依赖于以太坊系统中去中心化的、由全球成千上万的计算机组成的、鲁棒性极强的共识网络, 它以比特币中类似的区块链技术作为基础, 并以类似的密码学方法和经济激励手段作为安全性的保障, 其隐私保护与比特币类似. 达世币是一种增强保护隐私的密码货币, 市场占有率约 7.4 亿美元; 它以比特币为基础, 添加如双层奖励制网络(也称主节点网络)等多项新功能, 其中还包含为提高可互换性的匿名支付、在不依赖中心权威下实现即时交易. 是 CoinJoin 的改进和扩展版, 采用了去中心化、面值相同和混币等增强隐私的技术. 在交易合并过程中, 主节点在用户资金流过时可能进行“窥探”. 由于用户可随机选择主节点, 所以恶意主节点“窥探”的影响性不大.门罗币使用 PoW 机制, 扩展了 CryptoNote 协议, 保护交易额隐私, 市场占有率 3.1 亿美元. 其隐私保护原理与比特币系统不同, 利用了比特币闪电侧链中的保密交易以及环签名技术, 把可链接的自组织匿名群签名扩展为多层可链接的自组织匿名群签名, 使用环签名和一次秘钥隐藏交易支付方和接收方, 使用秘密承诺隐藏交易额支持多输入多输出以实现隐私增强交易, 采用零知识证明防止双花. 环签名技术会导致块区的膨胀, 如果交易量较大, 区块膨胀问题会非常严重, 交易验证时间与隐私保护力度正相关. 安全性与比特币类似, 隐私保护强度明显高于比特币. 瑞波币是一种开放的、分布式的支付网络, 允许用户在金融网络如信用卡、银行支付、以及其他货币转换需收费的机构之间进行免费使用, 交易延迟低, 市场占有率约 2.5 亿美元. 瑞波币自有共识机制, 采用 OpenCoin 算法, 与其他数字货币不同, 运行在瑞波网络中的瑞波币是不同数字货币之间的桥梁, 通过这个支付网络可以转账任意一种货币, 简便快捷, 交易可在几秒以内完成. 其共识协议通过引入特殊节点列表(UNLs)把 51%攻击排除在外, 系统对每个交易收费且用户最低需拥有 20 个币, 以此防范拒绝服务攻击, 隐私保护与比特币类似.

比特币作为一种私人货币，以及支撑比特币系统安全的区块链技术和由比特币发展起来的、支持智能合约的以太坊系统，展示了新技术重塑社会和经济活动的强大能力，打开了极为广阔的应用和创新空间. 这些新技术、新思想可以被法定数字货币系统吸收和发展，使得研究和部署法定数字货币极具现实意义.

3 法定数字货币的技术挑战

为了利用比特币等新兴数字货币的技术优势，并应对众多私人数字货币带来的挑战，全球主要国家在加强比特币等私人数字货币交易监管的同时，也在积极研究和部署法定数字货币. Danezis 等[2]提出的类比特币系统 RSCoin，是目前唯一公开的由一国政府推出的法定数字货币框架，它允许该国央行对货币发行量进行调控，借助该中央银行的信用背书，极大提高了交易处理的速度. 然而，与比特币相比，它对货币流通几乎没有增加额外的监管机制，尤其是缺少对数字货币交易过程的隐私增强和审计监管机制. 当然，目前公开的 RSCoin 只是英国法定数字货币的框架，其具体实现与部署相信在今后还会有所改进.

与比特币等私人数字货币类似，法定数字货币的设计同样面临系统可扩性与效率、安全与隐私保护、以及审计与监管等方面的挑战. 然而，由于法定数字货币具有强制性，并由国家信用背书，其交易涉及国家经济与金融情报，因此这三方面的挑战更加严峻.

在系统可扩性与效率方面，需要考虑以下因素. 第一，考虑到法人用户与个人用户等因素，在我国这样的人口大国，法定数字货币系统支持的用户规模应在 20 亿以上，这远远超过目前比特币等私人数字货币系统数百万的用户规模. 第二，法定数字货币系统应有利于激发多方参与的积极性，便于系统扩展与提升效率. 第三，法定数字货币的部署是一个渐进的过程，因此系统要能适应用户规模的自然增长，具备良好的扩展能力. 第四，为了更好地服务大众，法定数字货币应允许用户随时随地访问，并支持智能合约. 第五，在特殊情况下，法定数字货币易成为大规模攻击目标，因此法定数字货币所依赖的网络系统应具有良好的鲁棒性和生存能力. 第六，法定数字货币需支持用户到用户的直接支付，减少中间交易环节. 第七，法定数字货币需要支持对不同币种的数字货币兑换和外汇交易. 第八，法定数字货币系统的运行应是低资源消耗，低交易延迟，高吞吐率的，支持数百万频次的峰值交易.

在安全与隐私保护方面，需要考虑以下因素. 第一，法定数字货币必须做到铸币能防伪造，交易防篡改、防抵赖和防双重花费. 第二，现有的比特币等私人数字货币系统对交易额、尤其是交易元数据很少保护，然而，由于一国的货币流通情况涉及该国的经济与金融机密，法定数字货币交易中需要保护交易额度、交易元数据的隐私. 第三，法定数字货币需要保护货币持有者、货币交易方的身份隐私，不能因为利用数字货币账号购物、捐赠等泄露用户的身份隐私. 第四，所有交易应具有可公开验证性，在机制上预防舞弊行为. 第五，对小额交易以及经过授权的特殊交易，法定数字货币系统应提供类似于现金交易的匿名保护能力. 第六，在用户账户被盗、口令遗忘等情况下，系统应能支持用户对所属账户进行确权和挂失，并尽可能支持找回被盗款等功能. 第七，法定数字货币系统必须防范因为安全失败或金融事件引发的风险传播，必须能将各种风险限制在足够小的范围内，防止风险大面积超高速扩散. 第八，在部分网点被攻破和用户账户泄露的情况下，上述安全与隐私保护能力仍然可以得到充分保障，显然这是一项巨大的挑战.

在审计与监管调控方面，需要考虑以下因素. 第一，系统应能支持国家对货币发行总量、发行速度、货币流向、货币流量、货币流速的监管与调控. 第二，系统应能支持国家宏观经济政策、金融与货币政策的运行与传导，确保相关授权机构及时获得政策执行效果的反馈. 第三，系统应能支持获得授权的机构对交易额、交易频次、关联交易等的审计，及时发现异常交易或利用数字货币实施违法犯罪活动的嫌疑. 第四，在审计发现异常，或外部违法犯罪调查需要等情况下，经授权的机构应能依法追踪涉嫌的数字货币账号、其关联账号以及账号所有人的物理身份，系统应提供对涉案账户的依法强制措施，支持对犯罪赃款的

冻结与追回. 第五, 系统应能依法提供真实的、完整的、时序的、不可伪造的、不可篡改的、不可否认的交易链, 供犯罪调查、司法取证等用途. 第六, 在实施审计、犯罪调查等情形, 诚实的合法用户的隐私不应受到侵犯.

4 小结

比特币促进了价值互联网的诞生与发展, 由比特币发展起来的以太坊系统支持功能强大的智能合约, 正在孕育信用互联网和智能契约社会的新时代, 显示出新技术革命性地重塑虚拟空间与物理社会经济与生活的能力, 这些新技术、新思想可以被法定数字货币系统吸收和发展. 但是, 类似比特币的私人数字货币系统在可扩性、系统吞吐率、安全性、匿名性、可调控性、审计监管等方面还有诸多不足, 尚需系统深入的研究. 类比特币系统安全与隐私保护涉及大量现代密码技术, 包括杂凑函数、公钥加密、数字签名、群签名、环签名、盲签名、零知识证明、同态加密、安全多方计算等. 我国密码学者在这些领域及相关领域做出了众多突出工作, 限于篇幅, 本文未一一赘述. 总之, 在产学研用方面, 我国广大科技工作者和从业人员拥有深厚的密码学及相关领域理论、技术、工程和应用积累, 为研究和部署法定数字货币奠定了坚实的基础, 通过对法定数字货币系统模型、原理与技术、安全与隐私保护、审计与监管等方面开展应用基础研究和实验验证, 有利于促进数字货币在我国的健康发展, 提升数字金融科技实力, 改善国际金融体系.

References

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. 2008.

[2] DANEZIS G, MEIKLEJOHN S. Centrally banked cryptocurrencies[J]. arXiv preprint arXiv:1505.06895, 2015.

[3] GERVAIS A, KARAME G O, WÜST K, et al. On the security and performance of proof of work blockchains[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 3–16.

[4] KING S, NADAL S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19.

[5] DUONG T, FAN L, ZHOU H S. 2-hop Blockchain: combining proof-of-work and proof-of-stake securely[J]. 2016.

[6] DZIEMBOWSKI S, FAUST S, KOLMOGOROV V, et al. Proofs of space[C]. In: Annual Cryptology Conference. Springer Berlin Heidelberg, 2015: 585–605.

[7] PARK S, PIETRZAK K, KWON A, et al. Spacemint: a cryptocurrency based on proofs of space[R]. Technical report, Cryptology ePrint Archive, Report 2015/528, 2015.

[8] MIZRAHI I B C L A, ROSENFELD M. Proof of activity: extending bitcoin's proof of work via proof of stake[J].

[9] WIKI B. Scalability[OL]. https://en.bitcoin.it/wiki/Scalability, 2015.

[10] MCCONAGHY T, MARQUES R, MÜLLER A, et al. BigchainDB: a scalable blockchain database[J]. 2016.

[11] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2016: 106–125.

[12] VUKOLIĆ M. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication[C]. In: International Workshop on Open Problems in Network Security. Springer International Publishing, 2015: 112–125.

[13] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[J]. 2015.

[14] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 507–527.

[15] KIAYIAS A, PANAGIOTAKOS G. Speed-security tradeoffs in blockchain protocols[J]. IACR Cryptology ePrint Archive, 2015, 2015: 1019.

[16] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-ng: a scalable blockchain protocol[C]. In: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). USENIX Association, 2016: 45–59.

[17] MICALI S. Algorand: the efficient and democratic ledger[J]. arXiv preprint arXiv:1607.01341, 2016.

[18] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 17–30.

[19] ZHU Y, GUO R, GAN G, et al. Interactive incontestable signature for transactions confirmation in bitcoin blockchain[C]. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2016: 443–448.

[20] MILLER A, XIA Y, CROMAN K, et al. The honey badger of BFT protocols[C]. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 31–42.

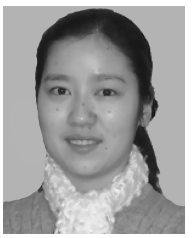
[21] VELNER Y, TEUTSCH J, LUU L. Smart contracts make bitcoin mining pools vulnerable[J].

[22] FORTE P, ROMANO D, SCHMID G. Beyond bitcoin—part II: blockchain-based systems without mining[J]. 2016.

[23] VASIN P. Blackcoin’s proof-of-stake protocol v2[J]. 2014.
[24] GARAY J, KIAYIAS A, LEONARDOS N. The bitcoin backbone protocol: Analysis and applications[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2015: 281–310.
[25] CHRISTIN N. Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace[C]. In: Proceedings of the 22nd International Conference on World Wide Web. ACM, 2013: 213–224.
[26] MOORE T, CHRISTIN N. Beware the middleman: empirical analysis of Bitcoin-exchange risk[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013: 25–33.
[27] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013: 6–24.
[28] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system[C]. In: Security and Privacy in Social Networks. Springer New York, 2013: 197–223.
[29] BIRYUKOV A, KHOVRATOVICH D, PUSTOGAROV I. Deanonymisation of clients in Bitcoin P2P network[C]. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014: 15–29.
[30] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in bitcoin using p2p network traffic[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014: 469–485.
[31] BIRYUKOV A, PUSTOGAROV I. Bitcoin over Tor isn't a good idea[C]. In: 2015 IEEE Symposium on Security and Privacy (SP). IEEE, 2015: 122–134.
[32] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014: 486–504.
[33] WIJAYA D A, LIU J K, STEINFELD R, et al. Anonymizing bitcoin transaction[C]. In: International Conference on Information Security Practice and Experience. Springer International Publishing, 2016: 271–283.
[34] MAXWELL G. Coin join: bitcoin privacy for the real world[OL]. https://bitcointalk.org/ index.php, 2013.
[35] VAN SABERHAGEN N. CryptoNote v 2.0, 2013[J]. 2014.
[36] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: anonymous distributed e-cash from bitcoin[C]. In: 2013 IEEE Symposium on Security and Privacy (SP). IEEE, 2013: 397–411.
[37] GROTH J, KOHLWEISS M. One-out-of-many proofs: or how to leak a secret and spend a coin[C]. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2015: 253–280.
[38] HEILMAN E, BALDIMTSI F, GOLDBERG S. Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2016: 43–60.
[39] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]. In: 2014 IEEE Symposium on Security and Privacy (SP). IEEE, 2014: 459–474.
[40] BEN-SASSON E, CHIESA A, TROMER E, et al. Succinct non-interactive zero knowledge for a von Neumann architecture[C]. In: USENIX Security. 2014, 2014.
[41] DAGHER G G, BÜNZ B, BONNEAU J, et al. Provisions: privacy-preserving proofs of solvency for bitcoin exchanges[C]. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 720–731.
[42] OGUNBADEWA A. The virtues and risks inherent in the bitcoin virtual currency[J]. 2014.
[43] KAPLANOV N. Nerdy money: bitcoin, the private digital currency, and the case against its regulation[J]. Loy. Consumer L. Rev., 2012, 25: 111.
[44] MARIAN O Y. A conceptual framework for the regulation of cryptocurrencies[J]. 2014.
[45] Caixin: How far is the digital yuan[OL]. http://economy.caixin.com/2016- 02-13/100908683.html, 2016.
财新网: [专访周小川之五]数字人民币还有多远[OL]. http://economy.caixin.com/2016- 02-13/100908683.html, 2016.
[46] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[OL]. URL: http://www. Open sciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014.
[47] MUADH Z. Introduction To Sidechains and Blockchain 2.0[OL]. http://www.deepdotweb.Com/2014/06/26/sidechains-blockchain-2-0/.2014.
[48] TODD P. [Bitcoin-development]tree-chains preliminary summary[OL]. https://lists.linux foundation.org/pipermail/bitcoin-dev/2014-March/004797.html, 2014.
[49] LEWENBERG Y, SOMPOLINSKY Y, ZOHAR A. Inclusive block chain protocols[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015: 528–547.
[50] WU Q, ZHOU X, QIN B, et al. Secure joint Bitcoin trading with partially blind fuzzy signatures[J]. Soft Computing, 2015: 1–12.
[51] ZHOU X, WU Q, QIN B, et al. Distributed Bitcoin Account Management[C]. In: Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016: 105–112.
[52] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151.

[53] GARMAN C, GREEN M, MIERS I, et al. Rational zero: economic security for zerocoin with everlasting anonymity[C]. In: International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014: 140–155.
[54] KUMARESAN R, MORAN T, BENTOV I. How to use bitcoin to play decentralized poker[C]. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 195–206.
[55] BENTOV I, KUMARESAN R. How to use bitcoin to design fair protocols[C]. In: International Cryptology Conference. Springer Berlin Heidelberg, 2014: 421–439.
[56] RUFFING T, KATE A, SCHRÖDER D. Liar, liar, coins on fire![J]. Penalizing Equivocation.
[57] HUANG H, CHEN X, WU Q, et al. Bitcoin-based fair payments for outsourcing computations of fog devices[J]. Future Generation Computer Systems, 2016.
[58] ZHANG Y, WEN J. The IoT electric business model: Using blockchain technology for the internet of things[J]. Peer-to-Peer Networking and Applications, 2016: 1–12.

作者信息

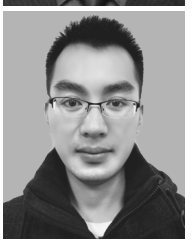


秦波(1977–), 湖北人, 博士, 讲师. 主要研究领域为密码学、云计算安全、密码货币、区块链、数据画像、信息网络安全.
E-mail: bo.qin@ruc.edu.cn

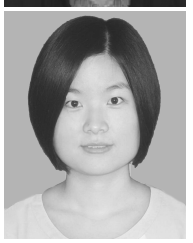
陈李昌浩(1995–), 新疆人, 硕士研究生. 主要研究领域为公钥密码学、密码货币、社会工程学.
E-mail: clch@ruc.edu.cn

伍前红(1973–), 四川人, 博士, 教授. 主要研究领域为密码学、数据安全、密码货币、区块链、云计算安全、智能安全.
E-mail: qianhong.wu@buaa.edu.cn

张一锋(1976–), 浙江人, 高级工程师. 主要研究领域为移动支付、数字货币、区块链.
E-mail: zhangyifeng@zccp.com



钟林(1987–), 四川人, 博士研究生. 主要研究领域为公钥密码学、网络与信息安全.
E-mail: zhonglin@buaa.edu.cn



郑海彬(1989–), 山东人, 博士研究生. 主要研究领域为公钥密码学、信息与网络安全.
E-mail: zhenghaibin29@buaa.edu.cn