面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题

曾 帅 [1, 2, 3] 袁 勇 [1, 2, 3] 倪晓春 [1, 2, 3] 王飞跃 [1, 2, 3, 4, 5]

摘 要 比特币是一种利用区块链技术的点对点记账系统. 随着比特币的发展, 现有的比特币系统架构已经不能满足日益增长的交易需求, 亟需扩容以寻求长期发展. 比特币是以人为核心的复杂社会经济系统, 比特币扩容是涉及多方利益的复杂问题, 引起了业界与学术界的广泛关注. 本文提出了一个比特币系统扩容问题的研究框架, 包括关键技术, 制约因素与衍生问题三部分, 以深入探讨和研究比特币扩容问题. 在该研究框架下, 首先介绍链上和链下两类扩容关键技术及发展现状; 其次从网络负载和节点瓶颈两方面, 总结制约比特币扩容方案的宏观与微观因素; 最后, 探讨两类衍生问题: 从系统安全性的角度, 探讨比特币扩容可能引发的安全问题及解决策略; 从币值、交易费与矿工收益等方面, 阐述比特币扩容涉及的经济问题.

关键词 区块链, 比特币, 扩容, 隔离见证, 闪电网络

引用格式 曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题. 自动化学报, 2019, **45**(6): 1015−1030

DOI 10.16383/j.aas.c180100

Scaling Blockchain Towards Bitcoin: Key Technologies, Constraints and Related Issues

ZENG Shuai[1, 2, 3] YUAN Yong[1, 2, 3] NI Xiao-Chun[1, 2, 3] WANG Fei-Yue[1, 2, 3, 4, 5]

Abstract Bitcoin is a peer-to-peer ledger system based on the blockchain technology. With the development of Bitcoin, the existing Bitcoin system architecture can no longer meet the demand of the increasingly large volume of transactions, so that Bitcoin scalability becomes one of the most important problems to solve in Bitcoin-related systems today. The Bitcoin system is a complex human-centered socio-economic system, and the Bitcoin scalability problem is a complex problem involving multi-party interests, which has attracted increasing attention of both industries and academia. This paper presents a research framework for the Bitcoin scalability problem, including the key technologies, constraints and related issues, in order to help explore and study the Bitcoin scalability problem. Under the framework, we first introduce two kinds of key technologies and their current developments. Secondly, we summarize factors that restrict the Bitcoin scalability from the aspects of network load and node performance. Finally, we explore the related security issues and economic issues involved in the Bitcoin scalability.

Key words Blockchain, Bitcoin, scalability, segregated witness, lightning network

Citation Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards Bitcoin: key technologies, constraints and related issues. *Acta Automatica Sinica*, 2019, **45**(6): 1015−1030

比特币是一种利用区块链技术的点对点记账系统. 它采取去中心化的方式, 由节点 (一般称为矿工) 通过工作量证明争夺记账权. 获得记账权的矿工可以从记录交易的缓冲区中取出交易, 生成区块并在比特币网络中进行广播. 目前, 比特币区块的生成间隔大约是 10 分钟, 区块大小被限制在 1 MB. 这两个因素制约了一个交易从提交到被记录下来所耗费的时间, 从而限制了比特币网络的链上交易量[1−2].

在中本聪创建比特币之初, 并未对区块大小进行硬性规定. 然而, 由于彼时比特币尚在发展初期, 参与挖矿的节点大部分是个人电脑, 其网络带宽与处理能力都十分有限, 而且当时比特币价格低廉, 攻

收稿日期 2018-02-13 录用日期 2018-04-16
Manuscript received February 13, 2018; accepted April 16, 2018
国家自然科学基金 (71472174, 71102117, 61533019, 71232006, 61233001, 71402178, 71702182) 资助
Supported by National Natural Science Foundation of China (71472174, 71102117, 61533019, 71232006, 61233001, 71402178, 71702182)
本文责任编委 刘向杰
Recommended by Associate Editor LIU Xiang-Jie
1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 2. 青岛智能产业技术研究院 青岛 266109 3. 北京市工程技术研究中心 北京 100190 4. 国防科学技术大学军事计算实验与平行系统技术中心 长沙 410073 5. 中国科学院大学中国经济与社会安全研究中心 北京 101408
1. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. Qingdao Academy of Intelligent Industries, Qingdao 266109 3. Beijing Engineering Research Center of Intelligent Systems and Technology, Beijing 100190 4. Research Center of Military Computational Experiments and Parallel System, National University of Defense Technology, Changsha 410073 5. Center of China Economic and Social Security, The University of Chinese Academy of Sciences, Beijing 101408

击者仅需付出极小代价, 便可创建包含大量交易的大区块 (Huge blocks) 造成粉尘攻击.

因此, 中本聪将区块容量上限设置为 1 MB[3−4]. 同时, 他指出这个限制是暂时的, 在比特币区块容量接近上限时, 可以将上限数值提高 (中本聪举例的修改方案为: 在区块高度达到 115 000 时, 提高区块容量上限.).

随着比特币平均区块大小稳步上升, 至 2017 年接近上限 (如图 1 所示), 比特币扩容的呼声越来越高. 一个公认的事实是, 1 MB 的区块上限已经不能满足用户的交易需求, 需要扩容比特币网络, 以提高交易速度和使用率[5]. 目前比特币网络的最大吞吐量仅为 3.3 ∼ 7 个交易/秒[6] (下限基于平均交易大小 500 bytes 而得, 上限基于最小交易大小 250 bytes 而得.). 此外, 区块上限还造成了交易手续费的增加. 图 2 为近一年中单笔交易中手续费的平均比例, 大约在 0.5 % 到 1.5 % 之间浮动. 考虑到比特币价格高昂, 实际上用户为单笔交易所付的手续费相当可观. 图 3 为近 1 年中平均每笔交易支付的手续费, 可以明显看到已从 2017 年初的不足 10 美元 (United States Dollar, USD) 逐渐提高到 100 美元.

然而, 对于是否遵照中本聪的原有设计解除区块大小限制, 维护比特币主流软件的比特币核心 (Bitcoin core) 开发团队内部乃至整个比特币生态圈都产生了分歧. 支持者认为这是一种简单有效的手段, 可以缓解当前的交易压力; 反对者认为它会造成比特币社区的分裂, 不利于比特币健康发展.

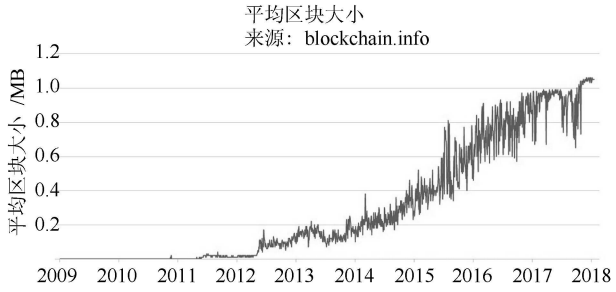

图 1 平均区块大小 (日期: 2018-01-18)

Fig. 1 The average block size (Date: 2018-01-18)

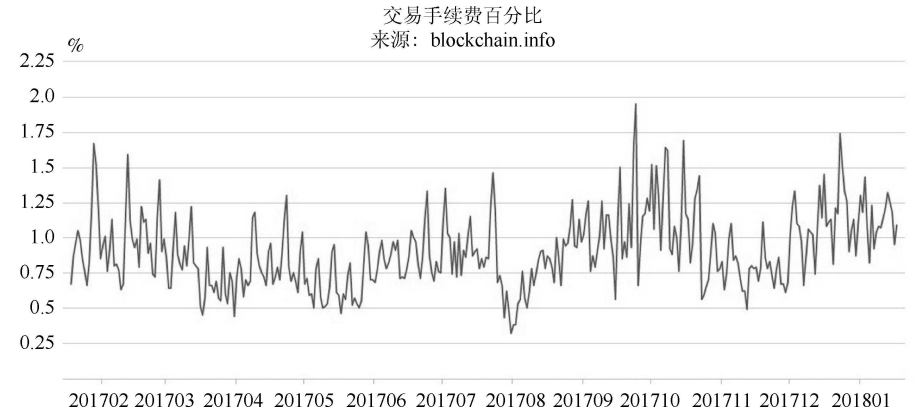

图 2 交易手续费百分比 (日期: 2017-01-19 至 2018-01-18)

Fig. 2 Cost of transaction volume (Date: 2017-01-19 ∼ 2018-01-18)

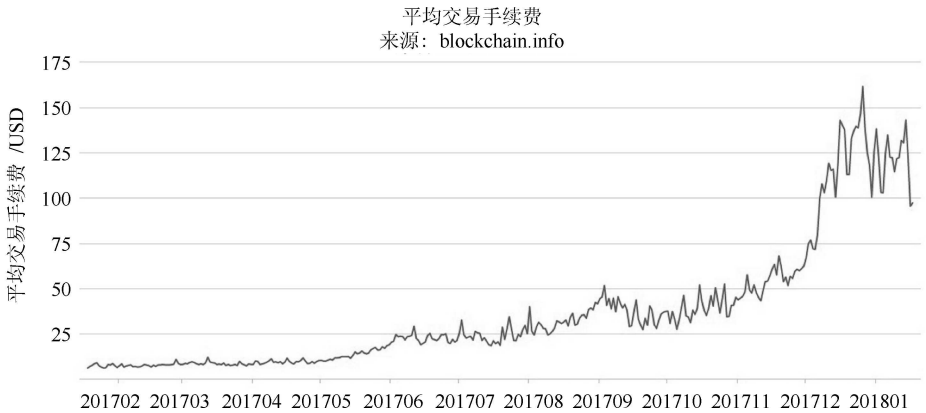

图 3 平均交易手续费 (日期: 2017-01-19 至 2018-01-18)

Fig. 3 Cost per transaction (Date: 2017-01-19 ∼ 2018-01-18)

比特币系统是以密码学方法为底层技术支撑而构建的一个以人为核心的复杂社会经济系统, 人的主观意识对比特币系统的发展具有极大影响[7−8]. 比特币系统扩容是一个涉及多方利益的复杂问题, 无论是开发者、投资者、交易平台, 还是矿工, 都有各自不同的利益和主观的决策. 这些为数众多的决策者, 所获得的信息具有不对称性, 对事物的认知度也有偏差, 使得整个问题变得十分复杂[2, 9−11].

比特币扩容问题是当前比特币社区最热门的话题, 也是将比特币性能提升到主流支付工具的水准需要解决的首要关键问题, 具有很高的研究价值. 目前业界已经召开了五次比特币扩展性研讨会 (Scaling Bitcoin) (也称为比特币圆桌会议或比特币扩容大会, 先后于 2015 年 9 月 12 日 ∼13 日在加拿大蒙特利尔, 2015 年 12 月 6 日 ∼7 日在中国香港, 2016 年 10 月 8 日 ∼9 日在意大利米兰, 2017 年 11 月 4 日 ∼5 日在美国斯坦福, 2018 年 10 月 6 日 ∼7 日在日本东京召开.), 相关人士围绕如何扩容提出了数个有价值的方案, 并引起了广泛的关注和讨论. 与此同时, 学术界也密切关注区块扩容问题, 从共识协议、网络负载、系统安全等角度提出了改进的方案.

已有工作一般是对比特币扩容方案可行性与扩容效果的分析[6, 12]. 为了更全面地探讨与研究比特币扩容问题, 通过对现有文献资料的分析提炼, 我们提出了一个面向比特币的区块链系统扩容问题的研究框架, 如图 4 所示. 具体而言, 研究框架分为关键技术、制约因素和衍生问题三个部分. 其中, 关键技术是指致力于解决比特币扩容问题的重要方案, 分为链上与链下两类, 两者的区别在于是否直接修改比特币系统协议; 制约因素是指限制比特币扩容关键技术实施与推广的指标与条件, 从宏观层面上来说为网络负载, 从微观层面来说为节点瓶颈; 衍生问题是由比特币系统扩容演变而产生的相关问题, 主要涉及安全问题与经济问题两方面. 在接下来的章节, 我们将在该研究框架下, 对各部分内容分别展开叙述.

1　关键技术

关键技术包括链上扩容方案与链下扩容方案, 前者通过直接提高区块容量或生成频率, 使比特币系统可以容纳更多交易, 而后者则是在保持比特币系统现有架构的同时, 通过增设子网、子链等手段, 使比特币交易可以转移到其他网络中完成.

1.1　链上扩容 (On-chain Scaling)

链上扩容主张对比特币区块进行扩展, 使得比特币网络本身可以负荷更大的交易量, 这类方案的实施需要对比特币进行硬分叉 (Hard fork) (硬分叉是指在新的共识规则公布后, 未升级的节点会将新区块识别为无效而导致的永久分歧.), 主要分为区块扩容和频率扩容.

1.1.1　区块扩容

区块扩容方案是指通过提高区块大小上限, 从而增加单次可以被 “写入” 区块链的交易数量. 与区块扩容相关的比特币改进提议 (Bitcoin improvement proposals, BIPs) 共 9 个, 如表 1 (https://github.com/bitcoin/bips) 所示, 可以分为三类: 1) 以算力为中心: 包括 100、101、105、109, 其共同特点是由矿工投票决定区块容量的调整方案; 2) 以交易量为中心: 包括 104、106、107 (第二阶段), 其共同特点是基于前一阶段的区块大小调整区块容量; 3) 随时间递增: 包括 102、103、107 (第一

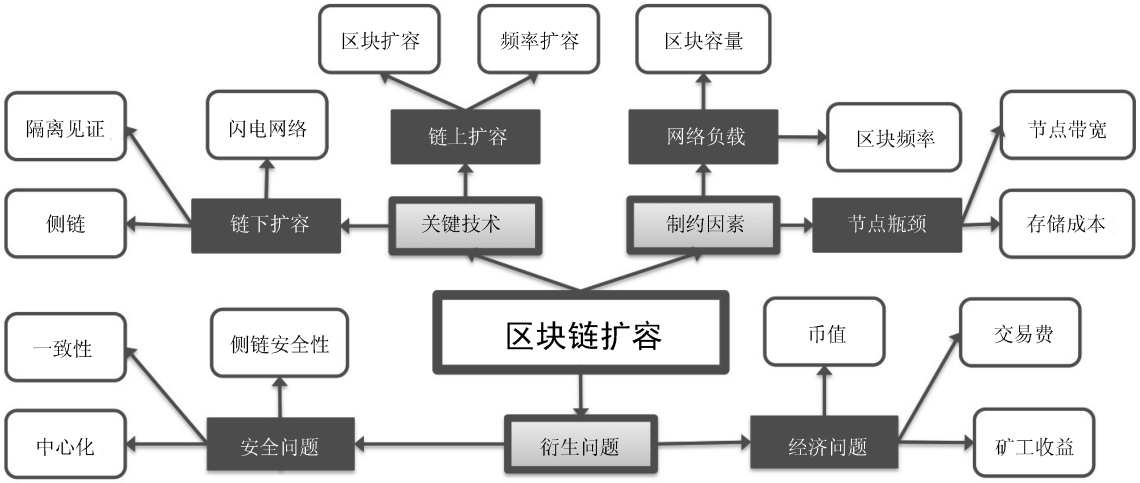

图 4　面向比特币的区块链扩容研究框架

Fig. 4　The research framework of the blockchain scalability problem towards Bitcoin

表 1 区块扩容方案比较

Table 1 Comparison among BIPs related to increasing block size

编号	主要内容	提出者	提出时间	状态
100	区块大小可为 1 MB 至 32 MB 之间的浮动值, 由矿工投票决定实际区块大小	Jeff Garzik, Tom Harding, Dagur Valberg Johannsson	2015-06-11	Removed
101	在全网 75 % 算力支持下在 2016-01-11 将区块大小限制提高到 8 MB, 并在 2036-01-06 前每两年对上限值进行翻倍, 直到达到 8 GB.	Gavin Andresen	2015-06-22	Withdrawn
102	在 2015-11-11 将区块大小限制提高到 2 MB.	Jeff Garzik	2015-06-23	Draft
103	在 2063 年前每年将区块大小限制提高 17.7 %.	Pieter Wuille	2015-07-21	Draft
104	按照最近 2016 个区块的大小调整上限.	t.khan	2017-01-13	Draft
105	按照最近 2016 个区块的矿工投票调整上限.	BtcDrak	2015-08-21	Draft
106	1) 按照最近难度区间的区块大小调整上限; 2) 按照最近 2 个难度区间的区块大小以及交易手续费调整上限.	Upal Chakraborty	2015-08-24	Draft
107	分两阶段扩容进行扩容. (阶段一) 2016 ∼ 2017: 2 MB; 2018 ∼ 2019: 4 MB; 2020: 6 MB; (阶段二) 从 2020 年以后, 每 4 周按照区块大小决定是否将上限提高 10 %.	Washington Y. Sanchez	2015-09-11	Draft
109	在全网 75 % 算力支持下将区块大小限制提高到 2 MB.	Gavin Andresen	2016-01-28	Rejected

阶段), 其共同特点是预估比特币交易需求量, 按年度调整区块容量.

1.1.2 频率扩容

频率扩容方案是指提高区块生成频率, 缩短区块生成间隔, 从而增加单位时间内被 “写入” 区块链的区块数量.

1) 降低难度

比特币通过调整难度, 控制区块生成间隔在 10 分钟左右. 每生成 2016 个区块, 难度就会依据生成这些区块的耗时而调整. 如果耗时超过两周 (14 天) 的时间, 难度会降低. 反之, 则难度升高. 通过降低难度, 可以很容易地缩短区块生成间隔, 这类方案也得到了一些来自社区的支持[13−14].

2) Bitcoin-NG

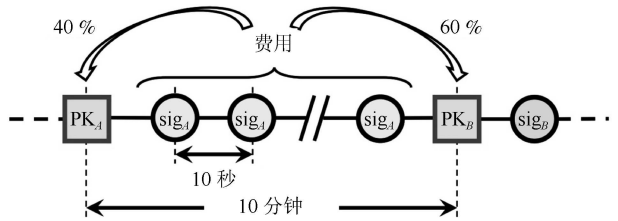

图 5 Bitcoin-NG 链结构示例

Fig. 5 An illustrative example of chain structure in Bitcoin-NG

康奈尔大学的 Eyal 等提出一种新的比特币协议 Bitcoin-NG[15]. 该协议将时间切分为不同的时间段. 在每一个时间段上, 由一个领导者负责生成区块, 打包交易. 该协议引入了两种不同的区块: 用于选举领导的关键区块 (Key blocks) 和包含交易数据的微区块 (Micro blocks). 每一个区块的头部都包含了前一个区块的加密哈希值.

关键区块的生成方式与原始的比特币协议一样. 具体而言, 都是基于工作量证明, 由节点寻找一个特殊的随机数. 一旦一个节点率先找到随机数, 它将生成关键区块并向其他节点广播, 成为本轮的领导者. 与比特币协议不同的是, 关键区块中还包含了一对公私钥中的公钥, 用于微区块的签名.

在生成关键区块之后, 领导者被允许以小于预设阈值的速率 (如 10 秒) 生成微区块. 微区块的大小是有界的, 小于一个预设值, 如 1 MB. 图 5 为 Bitcoin-NG 链结构示例, 微区块 (图中表示为圆形) 被关键区块 (图中表示为方形) 中公钥相应的私钥签名. 为了避免自私挖矿, 交易费用的 40 % 分配给本轮的领导者, 60 % 分配给下一轮的领导者.

Bitcoin-NG 可以在不改变区块容量的基础上, 通过选举领导者生成更多的区块, 解决比特币的扩容问题. 关键区块的生成间隔依然为 10 分钟, 因而无需降低难度. 此外, 由于存储交易的微区块的生成不需要节点寻找工作量证明, 因此不会额外增加矿工的工作量.

1.2 链下扩容 (Off-chain Scaling)

链下扩容方案主要包括隔离见证、闪电网络与侧链等软分叉方案 (软分叉是指新的共识规则公布后, 未升级的旧节点会将新区块识别为有效. 软分叉

是向后兼容的.). 其中, 隔离见证是针对交易延展性的问题而提出的, 其扩容效果十分有限, 但它是保障闪电网络与侧链安全性的基础.

1.2.1　隔离见证

隔离见证于 2015 年 12 月中国香港比特币扩容会议中被 Bitcoin core 开发团队的 Pieter Wuillle 提出.

隔离见证涉及五项 BIPs: 141, 142, 143, 144 和 145.

1) BIP141 描述了 "见证" 的结构;

2) BIP142 描述了隔离见证的地址格式;

3) BIP143 描述了隔离见证交易签名的验证方式;

4) BIP144 定义了新的消息和序列化格式, 用于节点之间传播交易和区块;

5) BIP145 描述了 getblocktemplate 协议以 JSON-RPC 调用的变化, 以支持隔离见证.

每一个比特币交易包括两部分: 一部分是基础交易数据, 包括交易的输入地址、输出地址; 第二部分为其他的事务数据, 包含了签名脚本等验证交易有效性的数据. 对交易数据进行双 SHA256 计算, 即可获得交易的唯一标识 txid (Transaction ID). 签名脚本 (Signature script) 包含一个 secp256k1 的椭圆曲线加密签名, 可以对基础数据签名, 但是不能对签名脚本自身签名, 这使得攻击者可以对交易进行非功能性的修改, 这一性质被称为交易延展性 (Transaction malleability). 此时交易依然有效, 但 txid 会发生改变.

攻击者利用交易延展性在交易未被写入区块前更改其 txid, 将有一定概率 "顶替" 原交易被打包. 当交易所或用户基于 txid 查询交易时, 会无法确认交易完成, 发送大量交易请求, 造成一定程度的 DOS 攻击. 2014 年 2 月, Mt.Gox 交易所声称由于 "交易延展性问题" 导致重复提现, 造成部分比特币的丢失. 受到 Mt.Gox 事件的影响, Bitstamp 等交易所发布公告称将会开始检查自己的内部系统以防止相同的错误出现, 并暂时停止了比特币提现.

Bitcoin Core 提议进行隔离见证, 即将签名脚本等验证交易有效性的数据转移到一个叫 "见证 (Witness)" 的新结构中. txid 的定义不变, 即以下交易数据的双 SHA256 值:

$$[nVersion][txins][txouts][nLockTime] \tag{1}$$

新的 wtxid 被定义为包括以下交易数据和见证数据的双 SHA256 值:

$$\begin{aligned}&[nVersion][marker][flag][txins]\\&[txouts][witness][nLockTime]\end{aligned} \tag{2}$$

Coinbase 交易的 wtxid 为 0x0000$\cdots$0000. 区块中的所有 wtxid 被存储在一棵梅克尔树的叶子结点上, 这棵树的根节点哈希记录在 coinbase 交易的 scriptPubKey 中.

隔离见证的本质不是针对扩容, 而是对不合理的原比特币交易结构的优化, 但它间接达到了扩容的目的. 在隔离见证成功实施后, 比特币打破了 1 MB 的区块限制, 截至目前峰值达到 1.3 MB.

1.2.2　闪电网络

2015 年, Poon 和 Dryja 两位开发者发布了闪电网络白皮书[16], 首次提出了闪电网络的概念, 其基本思想是建立交易方的微支付渠道 (Micropayment channels) 网络, 将小额交易从比特币主网中带离, 从而促进比特币的交易吞吐量达到每秒百万笔.

1) 双向支付通道

闪电网络的基础是交易双方之间的双向支付通道 (Bidirectional payment channels), 下面我们将从创建通道、交易方式、关闭通道和违规惩罚等四方面对通道进行介绍.

a) 创建通道

首先构建一个未签名的基金交易 (Unsigned funding transaction). 该交易的输出为 2-2 多重签名脚本, 意即动用这笔资金需要双方签名 (多重签名是一种允许多个公钥共同签署一笔比特币交易的技术.). 交易双方交换 "赞助" 该笔基金交易的输入地址与随后用于签名的公钥.

闪电网络使用 Sighash noinput (Sighash noinput 交易只对输出进行签名, 由于该交易的输入未被签名保护, 因而可以很容易被修改, 除非输入被其他形式的签名保护.) 格式的交易花费基金交易中的资金, 确保该交易可以在双方对基金交易签名之前进行, 这些交易被称为承诺交易 (Commitment transactions).

如图 6 所示, 假设 Alice 和 Bob 同意建立支付通道, 双方各拿出 0.5 BTC (Bitcoin) 用于创建基金交易. 然后 Alice 创建一笔初始的承诺交易 C1b, 该交易的输出为 Alice: 0.5 BTC, Bob: 0.5 BTC, Alice 对 C1b 签名后将该笔交易发送给 Bob; Bob 以同样的方式创建并签署 C1a, 并发送给 Alice. 双方交换完毕后, 就可以对基金交易进行签名, 并在比特币系统中广播.

b) 交易方式

为了进行交易, 双方可以通过生成新的承诺交易, 并将旧的承诺交易作废, 以达到资金重新分配的目的. 值得注意的是, 每组承诺交易使用独立的公钥, 公钥不会重复使用.

假设 Alice 需要向 Bob 支付 0.1 BTC, Alice 可以在 C1b 基础上创建一笔新的承诺交易 C2b, 该交易的输出为 Alice: 0.4 BTC, Bob: 0.6 BTC, Alice 对 C2b 签名后将该笔交易发送给 Bob; Bob 以同

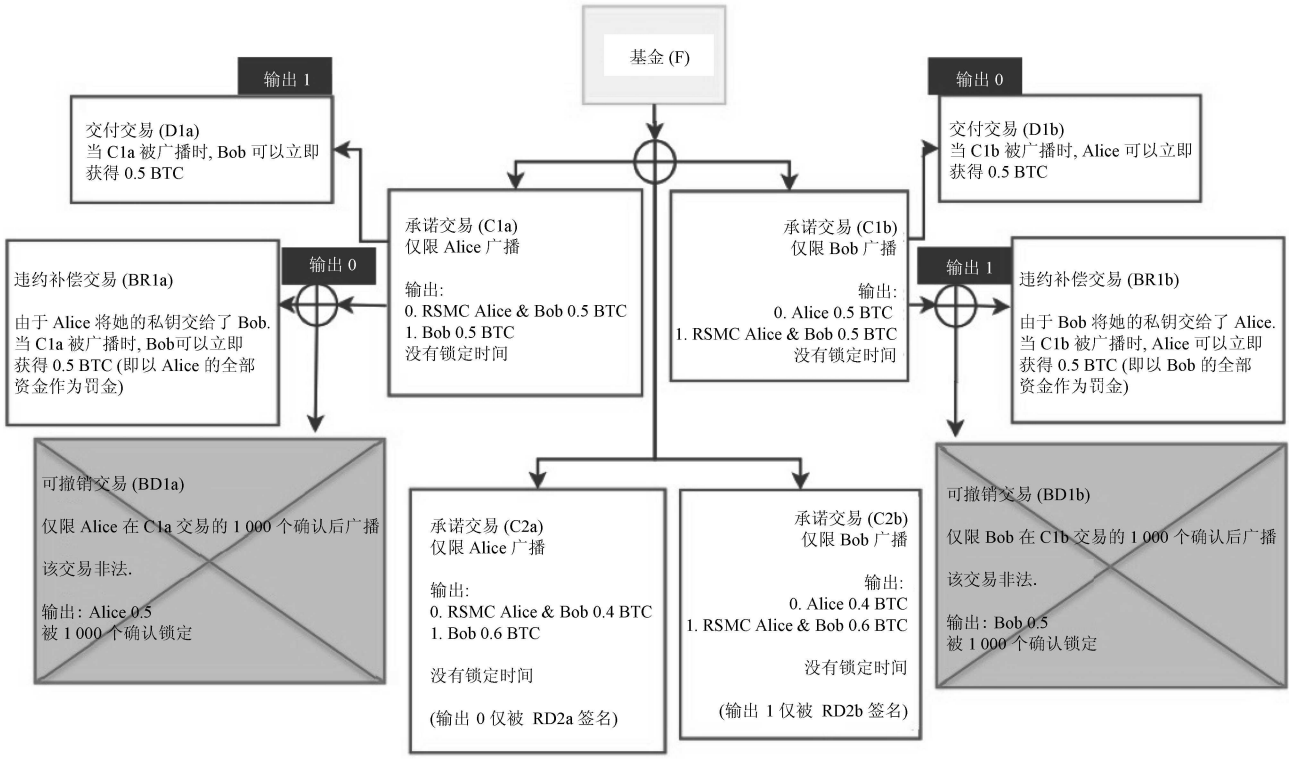

图 6 闪电网络微支付通道

Fig. 6 Micropayment channels based on Lightning Network

样的方式创建并签署 C2a, 并发送给 Alice. 为了让 C1a 和 C1b 失效, 双方可以交换用于 C1a 和 C1b 签名的私钥, 或者创建并交换违约补偿交易 (Breach remedy transaction) BR1a/BR1b.

c) 关闭通道

任意一方广播承诺交易, 即可关闭支付通道. 闪电网络设计了一个序列到期可撤销合约 (Revocable sequence maturity contract, RSMC), 该智能合约中规定: 率先广播承诺交易的一方, 需要等待一段时间才能拿到资金, 而另一方则可以立即获得资金. 具体的等待时长由双方事先商议. 如图 6 所示, 等待时长被设定为 1 000 个区块确认时间. 那么, 在 Bob 向比特币网络广播了最新的承诺交易 C2b 之后, Alice 可以立即获得 0.4 BTC, 而 Bob 需要等待主链再生成 1 000 个区块之后, 广播一个可撤销交付交易 (Revocable delivery transaction), 获得 0.6 BTC.

如果双方都同意关闭通道, 可以创建一个结算交易 (Exercise settlement transaction), 经双方签名并广播后, 双方都可以立即获得结算资金.

d) 违规惩罚

如果有一方广播的承诺交易不是最新版本, 那么将受到惩罚, 失去所拥有的资金, 通道中的全部资金都将属于另一方. 例如, Bob 在广播了旧的承诺交易 C1b 之后, Alice 可以在 1 000 个区块确认时间内提供 C1b 失效的证据, 最终 Alice 将获得 1 BTC, 而 Bob 将一无所有.

2) 哈希时锁合约 (Hashed timelock contract, HTLC)

HTLC 的目的是通过哈希运算允许跨多个节点的全局状态. 具体而言, 它可以锁定一项交易, 并以一个约定的时间 (某个未来的区块高度) 和承诺披露的知识作为解锁条件. 通过这种方式, 实现了网络中有条件的资金支付, 不需要通道双方及网络中其他人之间建立信任.

例如, 通过 HTLC, Alice 和 Bob 可以达成如下约定: 锁定 Alice 的 0.1 BTC, 如果在区块高度达到 T 之前, Bob 能够向 Alice 披露一项知识 R, R 经过某个已知的哈希计算 $hash(R)$ 等于某个值 h, 那么 Bob 就能获得这 0.1 BTC; 如果当区块高度高于 T 时, Bob 未能及时向 Alice 披露合适的 R, 那么这 0.1 BTC 将自动解锁并归还给 Alice.

3) 多节点支付通道

基于 RSMC, 闪电网络实现了节点之间的直接支付通道, 而基于 HTLC, 闪电网络实现了节点之间的间接支付通道.

如图 7 所示, 假设 Alice 需要向 Dave 转账 (金额为 0.1 BTC), 她可以通过两个节点 Bob、Carol 建立一条支付通道, 沿着该通道的节点两两之间建

立 HTLC 交易, 且各交易的时锁递减. 在该示例中, Alice 根据路由的长度, 将她和 Bob 的 HTLC 交易的 T 设置为 3 天 (实际为三天后的区块高度预估值). 在 Bob 和 Carol、Carol 和 Dave 之间, 也创建 HTLC 交易, 并分别设置 T 为 2 天、1 天.

图 7　基于闪电网络的多节点支付通道

Fig. 7　Payment over the Lightning Network using HTLCs

如果 Dave 在 1 天内向 Carol 披露 R, 就可以获得 0.1 BTC. 同样地, 如果 Carol、Bob 按时传递 R, 就可以分别从 Bob、Alice 处获得 0.1 BTC (以及手续费). 通过这种方式, Alice 完成了 Dave 的转账.

1.2.3　楔入式侧链技术 (Pegged Sidechains)

侧链被定义为可以验证来自其他区块链数据的区块链[17]. 侧链技术允许用户在比特币系统之外的其他区块链上使用他们的资产. 比特币系统被称为 “父链”, 而其他区块链被称为 “侧链”. 侧链虽然依赖于父链, 然而其事务处理与父链完全独立.

侧链的工作基础是简单支付验证 (Simplified payment verification, SPV) 证明, 它是一种动态成员多方签名 (Dynamic membership multi-party signature, DMMS), 发生在基于工作量证明 (Proof of work, POW) 的区块链中 (如比特币系统). 一个 SPV 证明包含 a) 一个展示工作量证明的区块头 (Block headers) 列表, 和 b) 一个表明列表中的某一区块中存在某项输出的密码学证明. 基于 SPV 证明, 无需运行全节点即可验证支付信息.

根据资金从父链流入侧链时, 侧链是否需要父链的 SPV 证明, 侧链可分为对称与不对称两种类型. 图 8 是一个对称楔入式侧链示例. 为了将父链上的资金转移到侧链, 首先需要将这笔资金转到父链上的一个特殊输出, 该输出只能由侧链上的 SPV 证明来解锁. 然后用户等待一个确认期后, 在子链上创建一个引用该输出的交易, 并提供该输出已被父链上足够工作量证明覆盖的 SPV 证明. 接着用户需要等待一个竞赛期, 在此期间如果收到新的 SPV 证明, 且比之前的 SPV 证明有更多工作量证明, 那么将替代原来的 SPV 证明. 这是为了防止双花攻击. 竞赛期结束后, 用户就可以在侧链上自由使用这笔资金了. 资金在侧链上依然保持自己 “父链币” 的身份, 只能转回到相应的父链, 并且侧链不允许来自不同父链的币之间进行交易或兑换. 当用户想把币从侧链上转回父链时, 需要经历相同的过程: 在子链上将这笔资金发送到一个特殊输出, 产生一个 SPV 证明给父链, 用于解锁父链上的等额资金.

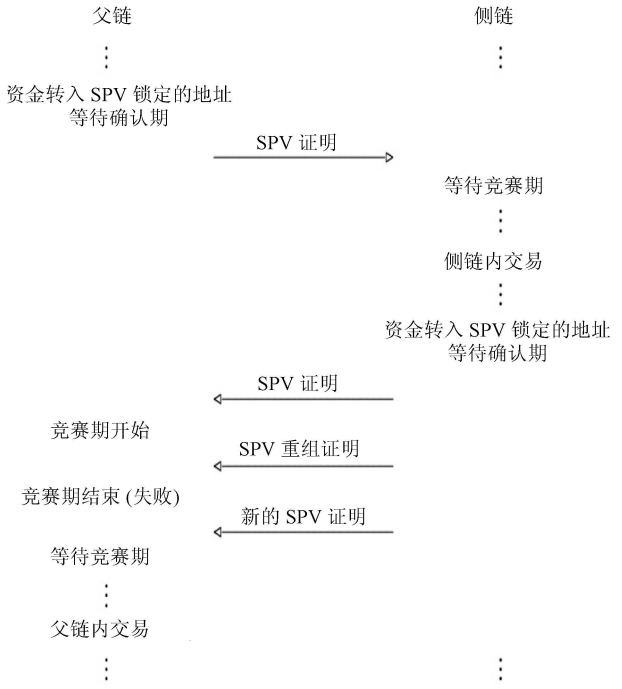

图 8　对称楔入式侧链示例

Fig. 8　An example of two-way peg protocal

1.3　发展现状

图 9 所示为 2015 年以来比特币扩容相关的重大事件构成的进展时间轴, 相关的重要提案见表 2 (https://github.com/bitcoin/bips.).

1.3.1　链上扩容进展

目前, 比特币还没有完成链上扩容. 经过香港共识、纽约共识两次努力的失败, 于 2017 年 8 月 1 日, 在 ViaBTC 等大矿池的推动下, 比特币通过硬分叉产生了一条新的区块链, 被称为 “比特币现金 (Bitcoin cash)”. 比特币现金起初支持 8 MB 的大区块, 而后进一步将限制提高到 32 MB, 并于 2018 年 11 月 10 创建出历史上第一个接近 32 MB 的大区块.

1.3.2　链下扩容进展

1) 隔离见证

Bitcoin Core 开发团队主导开发并推动了隔离见证的发展. 2016 年 10 月, Core 发布第一个支持隔离见证 (Segregated witness, SegWit) 的版本 0.13.1. 该版本遵循 BIP9 提案制定 SegWit 的激活条件, 即至少 95 % 的矿工表示支持才能在比特币网络上激活 SegWit. 最终由于没有在时限前 (2016 年 11 月 15 日) 得到足够算力支持而宣告 SegWit 激活失败.

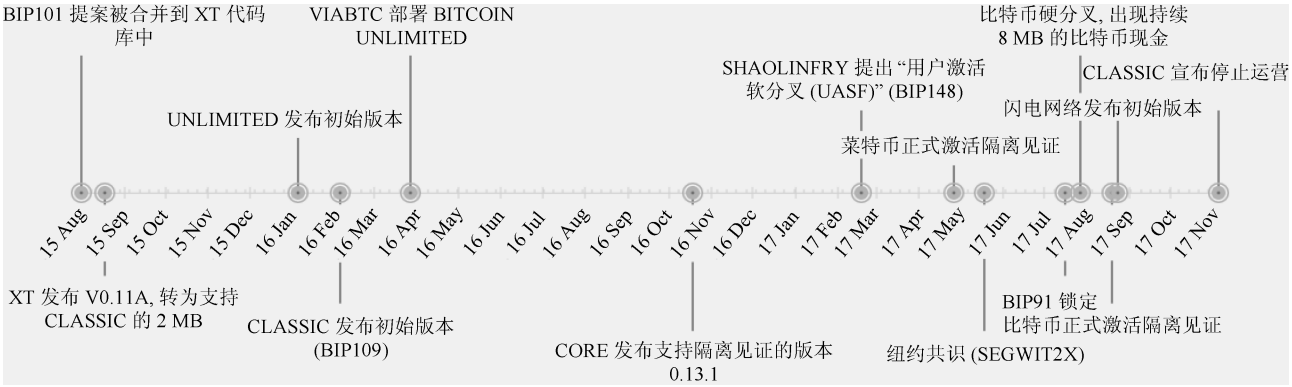

图 9 比特币扩容进展时间轴

Fig. 9 Timeline of Bitcoin scalability progress

表 2 比特币线上扩容重要提案

Table 2 BIPs related to on-chain scaling

编号	主要内容	提出者	提出时间	状态
9	对区块中的版本字段的语义进行更改, 让多个软分叉方案可以并行执行. 它将版本字段表示为位向量, 每个位可以用于跟踪独立的改变. 矿工通过更新某个位的值表示对某项软分叉准备就绪. 在软分叉开始 ([$STARTED$]) 后, 当一个难度区间内 (即 2 016 个区块) 中 95 % 的区块都表示支持该项软分叉, 则它进入锁定阶段 ([$LOCKED\_IN$]), 否则失败 ([$FAILED$]); 被锁定的软分叉需要再等 2016 个区块, 才能正式激活.	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	2015-10-04	Final
91	该提案削弱了原 SegWit 激活条件 (即 BIP9): 1) 确认窗口从 2016 个区块下降到 336 个区块; 2) 激活阈值从 95 % 削减到 80 %; 3) 接受 bit1 和 bit4 两种信号发送方式, 在激活后拒绝没有发送 bit1 的区块.	James Hilliard	2017-05-22	Final
148	采取 UASF 方案激活 SegWit, 支持 UASF 的节点会在 2017-08-01 开始强制执行新规则, 不符合新规则的区块将被这些节点拒绝.	Shaolin Fry	2017-03-12	Final

匿名用户 “Shaolin Fry” 提出采取用户激活软分叉 (User-activated soft fork, UASF) 方案激活 SigWit (BIP 148, 内容详见表 2), 以迫使矿工接受 SegWit. 该提案备受争议, 如果 BIP148 没有得到大多数矿工的支持, 就会导致比特币的分裂. 然而 Core 接受了该方案, 并将生效日期设定为 2017 年 8 月 1 日.

基于纽约共识, Jeff Garzik 开发了新客户端 “BTC1”, 将隔离见证的阈值设定为 80 %, 并以 bit 4 作为信号发送方式.

由于 Bitcoin Core 版本中隔离见证的激活阈值为 95 %, 并以 bit 1 作为信号发送方式, 与 BTC1 有冲突. 为此, James Hilliard 提出了 BIP91 (内容详见表 2) 融合两种方案. 最终, BIP91 被成功锁定并激活了 SegWit, 比特币避免了 BIP148 带来的硬分叉.

2) 闪电网络

在隔离见证成功实施之后, Elements Project (Blockstream)、Lightning Labs、ACINQ 等三个闪电网络开发团队在 2017 年 12 月 6 日宣布完成了闪电网络的初始版本 1.0 RC. 该版本成功实现了支付渠道驱动的网络中不同协议实现之间的交易. 目前, 这些开发团队正在寻求开发社区的同行评审与反馈, 以获得最终的 1.0 正式版本, 并计划在比特币主网上实施测试版本.

2 制约因素

本节主要讨论制约比特币扩容的主要因素, 分为网络负载与节点性能两方面. 前者主要关注比特币网络整体性能, 后者侧重于单个节点的性能.

2.1 网络负载

比特币系统基于 P2P 网络而搭建, 采用非集中式的拓扑结构, 其优点是维护简单, 面对网络的动态变化具有较好的容错能力, 缺点是随着节点的不断

增多, 网络规模不断扩大, 区块传播性能有所下降, 因而有必要研究当前网络状况是否可以承载比特币的进一步扩容.

2.1.1　区块容量

Decker 和 Wattenhofer[18] 对 2012 年比特币网络的区块传播状况进行了度量, 他们的分析结果表明, 对于较大的区块 (超过 20 KB), 其传播时间随着大小呈线性增长趋势.

来自 7 家知名大学与研究机构的 12 位研究人员进一步分析了 2014 年和 2015 年比特币网络的区块传播状况. 他们采用了 "X % 有效吞吐量" (X % effective throughput) 的度量标准, 它被定义为接收到区块的节点百分比, 用于表示区块传播时延. 他们通过分析发现, 按照平均 10 分钟的区块生成区间, 如果在一个区间内要达到 50 % 有效吞吐量, 即至少 50 % 的节点能接收到区块, 则区块大小最多不能超过 38 MB; 如果要达到 90 % 有效吞吐量, 则区块大小最多不能超过 4 MB[6].

2.1.2　区块频率

区块的生成频率同样会影响 X % 有效吞吐量. 以 80 KB 的区块为例, 如果要达到 90 % 有效吞吐量, 则区块生成间隔不得低于 12 秒[6].

从网络负载来看, 无论是扩大区块容量, 还是提高区块生成频率, 都不能无限制地进行链上扩容, 否则矿工挖掘出孤立块的概率增加, 导致资源浪费和系统的不安全性.

2.2　节点瓶颈

节点是处理比特币系统交易的独立工作单元, 它们的工作效率直接影响比特币系统的运营效率.

2.2.1　节点性能

每一条交易都需要被节点验证、传播, 才能被写入比特币账本中. 因此理论上, 节点带宽也会影响比特币系统的性能. 但根据分析, 现有的节点平均带宽完全高于实际需要的网络传播效率, 提高网络传播效率应该从其他方面入手, 如优化网络结构、优化交易处理流程等[6].

2.2.2　存储成本

比特币的本质是分布式账本, 为了支撑比特币系统的日常运营, 需要运行足够数量的全节点, 它们存储了全部的账本信息. 据 2017 年 12 月 17 日的数据, 比特币系统中的全节点个数大约为 11 500 余个 (https://bitnodes.earn.com/), 而数据总量约 147 GB (https://blockchain.info/charts/blocks-size).

通过比较几种比特币数据的常用存储方案, 包括本地存储方案与云存储方案, 研究者认为是 CPU+SSD 的组合是最经济的方案[19]. 以该方案为例, 一台高性能终端 (例如 Intel Core i7, 3.4 GHz, 8 个虚拟内核) 大约价值 300 美元, 容量 200 GB 的 SSD 大约 100 美元 (原文为 2014 数据, 本文根据 Amazon 美国网站查询结果更新数据). 假设使用年限为三年, 则设备成本约 4.23×10^{-6} 美元/秒. 此外, 按 40 W 的耗电量和 15 美分/kWh, 还可计算出耗电成本约 1.67×10^{-6} 美元/秒. 综上可以计算得出, 每天全节点的运行成本总和约为 5 862.24 美元.

从节点瓶颈来看, 链上扩容意味着节点需要下载、存储和验证更多的区块, 而那些不参与挖矿的全节点不能从维护比特币系统中获得任何直接收益. 随着成本的上升, 或许会造成全节点数量的下降, 这对比特币系统的长期发展是不利的, 详见第 3.2 节.

3　衍生问题: 安全问题

比特币与区块链的安全性研究, 包括安全体系架构、数据可靠性、用户隐私保护、常见攻击手段等, 是较热门的一类研究问题[20−22]. 比特币扩容方案的应用, 可能会引入更多的安全隐患. 本节将针对这点展开讨论.

3.1　高通量引发的安全问题

2014 年, 康奈尔大学的 Eyal 和 Sirer 的研究指出[23], 攻击者只需 33 % 的算力就可通过自私挖矿 (Selfish mining) (自私挖矿是指矿工在挖到新矿时不向比特币网络广播, 而是隐瞒它, 并在新矿分支上继续挖矿.) 导致比特币系统不安全, 而不是人们以为的 51 %.

对网络区块传播状况的分析表明, 在高交易吞吐量时, 系统的安全性将降为 0[24], 例如遭受双花攻击 (Double-spending attacks), 即攻击者将已花费交易伪造为未花费交易. 随着区块容量或生成速率的提高, 将会引起系统交易吞吐量的上升, 并提高产生分叉的概率, 并降低系统安全性, 如图 10 所示[25].

3.1.1　GHOST 协议

比特币采用工作量证明机制, 由矿工相互竞争求解复杂的数学难题, 率先解出答案的矿工获得本轮的区块生成权. 然而, 如果两个 (或多个) 矿工同时解开难题, 比特币就会产生分叉. 出现分叉后, 矿工需要按照一定规则选择主链, 并在主链上继续工作. 目前, 比特币采用的协议是寻找累计工作量证明最大的链. 由于难度在一个阶段内保持不变, 因此该协议也称为最长链规则 (Longest chain rule), 即将长度最长的链作为主链.

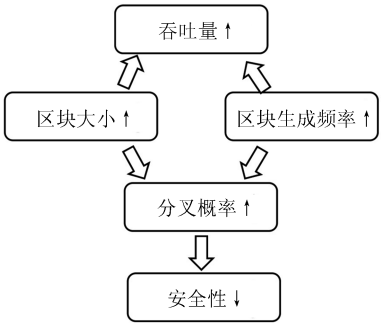

图 10 提高区块容量或生成速率引起的系统变化

Fig. 10 System changes caused by increasing the block size or block rate

如前所述, 在高交易吞吐量下, 由于区块传播延时, 比特币分叉的概率会大为提高. 图 11 描述了一个由诚实网络创建高分叉区块树的场景. 以 A、B、C、D、E 为矿工的编号, 其中 A 为攻击者, 其余为诚实节点. 攻击者私下创建了一个明显长于诚实网络最长链 (以 5B 结尾的链条) 的 6 个块的链 (表示为 1A, 2A, ⋯, 6A), 在最长链规则下, 将替代诚实网络成为主链. 对于接受零确认交易 (Zero-confirmation transactions) (无需等待 6 个区块确认时间, 只要交易的输入是 UTXO (未花费交易, Unspent transaction outputs), 就可以确认交易完成) 的节点, 攻击者可以利用这一漏洞造成双花攻击.

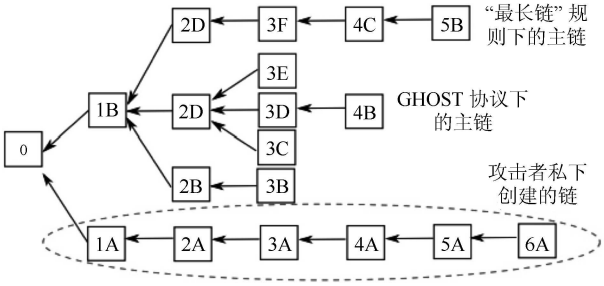

图 11 GHOST 协议示例

Fig. 11 An example of the GHOST protocol

为了解决这一问题, Sompolinsky 与 Zohar 提出了 GHOST (Greedy heaviest-observed subtree)[25]. 在该协议下, 当分叉出现时, 节点应选择累计子节点工作量最大的链条. 以图 11 为例. 当攻击者与诚实节点各自生成的区块产生分叉时, 节点会选择诚实节点的区块 (1B), 因为区块 1B 的子节点远多于区块 1A 的子节点.

值得一提的是, 作为第二大区块链应用, 以太坊 (Ethereum) 的区块生成间隔不到 1 分钟, 然而它巧妙地采用了 GHOST 的一个变种, 对孤立块 (称为叔块, Uncle block) 加以利用, 提高了系统的安全性和矿工的积极性 (https://www.ethereum.org/).

3.1.2 SPECTRE 协议

Sompolinsky 等提出了 SPECTRE 协议[24], 证明了在高交易吞吐量下, 该协议仍保持 50 % 的安全阈值, 即只要攻击者的算力不超过全网 50 %, 系统仍然可以维持安全性.

首先, 他们将比特币区块表示为一个有向无环图 (DAG), 图中节点不仅包括主链上的区块, 也包括那些不在主链上、被废弃的区块. 具体而言, 他们修改了区块头部结构. 在原始的比特币协议中, 每个区块的头部包含了对上一个区块的引用. 而在这个新方案中, 区块头部包含了所有未被其他区块引用、并且合法的区块引用.

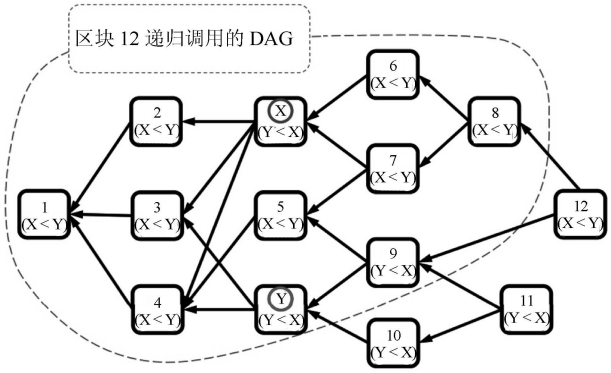

图 12 SPECTRE 协议示例

Fig. 12 An example of the SPECTRE protocol

基于 DAG, 区块之间构成了因果顺序. 对区块 x 而言, 以 $Past(x)$ 表示在 x 之前出现、可由 x 到达的区块集合, $Future(x)$ 表示在 x 之后出现、可到达 x 的区块集合. 当比特币出现分叉, 需要判断主链时, SPECTRE 采用了一种基于区块投票的方法. 设 x 和 y 为分叉的两个区块, 以 $x < y$ 表示 x 获胜, $y < x$ 表示 y 获胜. 以区块 B 为例, 比特币网络中的所有区块将按照以下规则进行投票.

1) 如果 $x, y \in Past(B)$, 则依据 $Past(B)$ 多数派结果进行投票;

2) 如果 $x \in Past(B)$ 且 $y \notin Past(B)$, 则投 $x < y$;

3) 如果 $y \in Past(B)$ 且 $x \notin Past(B)$, 则投 $y < x$;

4) 如果 $x, y \notin Past(B)$, 则依据 $Future(B)$ 多数派结果进行投票.

图 12 描述了一个比特币区块构成的 DAG. 区块 x 和 6 ∼ 8 投票 $x < y$, 而区块 y 和 9 ∼ 11 投票 $y < x$. 区块 12 依据 $Past(12)$ (除 10 ∼ 12 以外的其他区块) 的选择, 投票 $x < y$. 区块 1 ∼ 5 依据 $Future(.)$ 的选择, 投票 $x < y$. 最终 x 将获胜而成为主链的一员.

3.2　中心化

比特币的设计理念是去中心化的分布式账本, 然而现在它正在逐渐陷入中心化的困境. 大区块带来的区块和带宽成本增长, 使得拥有更强大处理能力的少数节点 (如矿池、交易所等) 优势进一步上升, 加剧中心化的到来.

3.2.1　算力中心化

通过对 2010～2014 年比特币区块的分析, 研究者发现了算力中心化呈现逐年加剧的趋势[26].

图 13 是 2018 年 1 月 18 日比特币网络哈希率的分布状况. 排名前五的大矿池所占据的算力总和已经超过了 70%, 由此可见目前大部分算力已被掌握在少数几个大矿池手中.

究其原因, 由于比特币采用的共识机制为 POW, 在一轮竞争中, 矿工需要成为最早找到某个随机数的赢家, 才能获得收益, 而拥有强大计算能力的矿池更有可能成为赢家. 为了获得稳定的收益, 矿工不得不选择成为矿池的一份子. 有学者认为应该鼓励矿池内部组织的去中心化, 例如 P2Pool (http://p2pool.org/), 以缓解算力中心化的问题[27].

3.2.2　节点中心化

此外, 如第 2 节所提到的, 考虑到大区块造成的成本和效率问题, 更多用户将选择安装轻量级 SPV 节点 (如手机终端), 或使用交易平台或网络钱包. 前者需要通过全节点同步数据, 后者则完全依赖于少数几个交易平台和网络钱包运营商. 举例而言, 截至 2014 年 3 月, 三家比特币交易所 Bitstamp, Bitfinex 和 btc-e 处理超过 80% 的美元比特币交易. 为了缓解节点中心化, 可行的方法之一是鼓励更多的比特币交易所加入竞争[27].

3.2.3　客户端中心化

目前 Bitcoin Core 版本的客户端占据绝对优势, Bitcoin Core 开发人员拥有极大的权限, 可以更新客户端规则. 虽然比特币扩容争议导致多个开发小组的出现, 然而并没有动摇 Bitcoin Core 的地位. 图 14 为 2018 年 1 月 18 日比特币网络客户端分布情况, 其中 Bitcoin Core 的市场占有率高达 87.22%, 远超过其他版本.

3.3　侧链安全性

通过侧链方案, 比特币交易被分散到多个侧链上, 缓解了交易压力. 然而, 与比特币系统相比, 侧链极有可能无法拥有庞大的算力, 以保证交易和区块的安全性. 攻击者可以用相对小的代价, 对侧链展开 51% 攻击. 由于侧链方案只依赖 SPV 证明来验证交易, 即它只检查所涉及的币是否来自已知的最长链, 而并不追溯至创世区块. 因此攻击者一旦成功攻破侧链, 他们可以创建一条更长的侧链主链, 进行双花攻击甚至凭空生出新的侧链币.

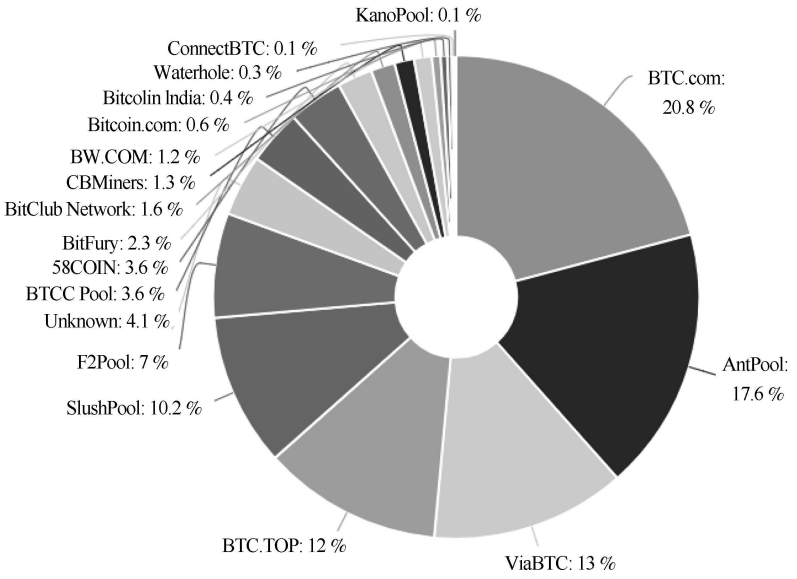

图 13　哈希率分布 (日期: 2018-01-18)

Fig. 13　Hashrate distribution (Date: 2018-01-18)

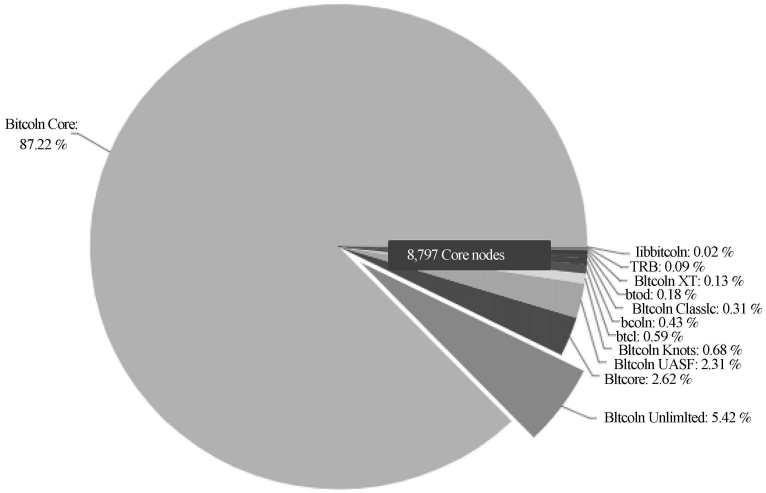

图 14 客户端分布情况 (日期: 2018-01-18)[28]

Fig. 14 Software distribution (Date: 2018-01-18)[28]

解决这个问题的一个办法是合并挖矿[17], 以确保所有侧链同时以相同哈希率开采. 合并挖矿的情形下, 所有侧链使用相同的哈希算法, 这样可以在同一时刻为多个侧链生成工作量证明. 然而, 合并挖矿要求矿工运行所有侧链的完整节点, 这就会造成中心化挖矿的趋势. 此外, 如果任意侧链受到 51 % 攻击, 风险依旧存在.

此外, Peter Todd 提出了树链 (Tree chains), 其基本思想是将多条区块链构成树状结构, 通过在父链 (如比特币) 区块中存储子链区块的哈希值, 为子链区块提供有效性证明, 即在保证父链和子链事务处理独立性的同时, 将父链安全性共享给了子链.

4 衍生问题: 经济问题

比特币 (或者说区块链) 生态圈涵盖了矿工、交易所、开发者 (钱包)、商家、用户、研究人员等诸多人群. 比特币扩容涉及到了多方利益. 区块容量决定了比特币网络处理交易量的效率, 有限的区块大小导致交易费的居高不下, 另一方面, 比特币的安全性由庞大的算力而支撑, 为此矿工付出了硬件和运维的成本, 考虑到系统的区块奖励持续下降, 长期来看需要交易费来激励矿工持续投入工作. 无论是链上扩容派还是链下扩容派, 双方都致力于提高比特币交易吞吐量, 分歧在于采取何种扩容方法给比特币生态圈带来的经济影响, 本文将从币值、交易费与矿工收益等方面进行阐述.

4.1 币值

图 15 为 2017 年 1 月 19 日至 2018 年 1 月 18 日比特币的价格变化情况. 可以看出, 比特币的价格极不稳定, 屡次陷入剧烈震荡的境地.

比特币价格波动是多种复杂因素共同作用的结果[29−33], 综合已有研究结果, 我们认为比特币扩容可以从以下方面影响比特币价格.

4.1.1 比特币供需关系的市场力量

比特币需求主要受到其作为商品和服务交换媒介的价值的驱使, 也就是它在未来交换中的价值. 而比特币供给是由流通的比特币库存给出的[31]. 由于比特币限量 2 100 万个, 它被认为和稀缺贵金属黄金类似, 都可以作为价值储存手段. 解决扩容问题, 也就是要解决如何将比特币的性能提升到主流支付工具的水准[6]. 显然扩容可以使比特币网络支撑更多支付需求, 导致用户数量的提高. 越来越多的用户和有限的供应量所带来的需求不断增加, 这自然会导致价格上涨[32]. 当用户的数量逐渐趋于稳定, 比特币价格将随之稳定在一个均衡价格上.

4.1.2 比特币系统安全性

比特币的价格可能受整个比特币系统的风险和不确定性的影响. 比特币与黄金不同, 没有从消费或其在生产过程中的使用中获得的潜在价值. 目前它正处于通过在市场参与者之间建立信任和信誉来建立其市场份额的阶段. 比特币的可信度主要与比特币系统提供给持有者的安全性以及在交换中使用的安全性有关. 鉴于比特币交易完全通过互联网进行, 网络安全是其主要挑战. 网络攻击可能会破坏整个比特币系统, 并最终导致其崩溃. 事实上, 比特币很容易受到网络攻击[31]. 比特币系统安全性的好消息, 比如升级到更安全的比特币网络软件, 可以增加对投资者的吸引力. 而关于比特币系统安全性的负面消息, 比如比特币扩容引起的安全问题 (详见第 3 节), 可能会一定程度上降低对投资者的吸引力.

4.1.3 用户交易成本

比特币吸引力是由潜在投资者和用户的交易成

本决定的. 交易成本包括:

1) 信息成本: 鉴于投资需求取决于寻找市场上可用投资机会信息的相关成本, 那些在新闻媒体中受到特别关注的投资机会可能会被潜在投资者所偏好[31]. 除此以外, 比特币价格和 Google trends 和 Wikipedia 上的搜索查询也存在显著的正相关性和动态的双向关系[33]. 因此, 比特币扩容引发的学术界和业界的报道和关注, 可能影响潜在的投资者和用户的决定.

2) 交易费成本: 交易费与比特币区块大小有密切联系, 详见第 4.2 节. 交易费的上升不利于比特币作为交易媒介, 进而会降低投资者和用户的兴趣.

4.2　交易费与矿工收益

比特币系统的安全性依赖于矿工的挖矿行为, 而矿工挖矿是为了获得挖矿所得的系统奖励和 "打包" 交易所得的手续费, 这是经济外部性的一个完美案例[34]. 为了真正写入一个区块, 需要得到超过半数的节点认可. 更大的区块可以支持更高的交易速率, 但会加大验证方的工作量. 较小的区块所占用网络带宽、存储空间更小, 包含交易规模更少, 更容易被验证; 反之, 较大的区块或许因为难以验证, 导致被其他区块代替.

在比特币发展初期, 系统奖励在收益中所占比例较高, 且交易费较低甚至为零. 较小的区块对于矿工的短期收益来说更有利. 然而, 已有研究表明指出零或无限小的交易费用不可能持续, 其原因是随着比特币高度的增加, 系统奖励周期性减半[32]. 此时, 同时维持零交易费与矿工收益的一个可能是, 随着时间的推移, 比特币的价格越来越高. 换句话说, 为了在价格上与矿工的激励保持一致, 2030 年后每年生产的数以万计的比特币应该与现在每年生产的数百万比特币具有相同的价格. 这种预期过于乐观而发生的概率极低. 更可能的预计是, 随着时间的推移, 有限的供给和比特币价格的最终限制共同作用, 导致采矿的边际生产成本急剧增加.

由于矿工没有动力打包一个没有手续费的交易, 为了减少等待时间, 用户需要缴纳交易费. 通过交易手续费, 比特币可以建立矿工打包最新交易的激励机制[35]. 从长远来看, 应该制定交易费用政策, 以便有足够多的矿工有激励来运行足够高的算力来保障比特币网络免于 51 % 攻击. 但同时作为一种交易媒介, 交易费不应高到阻止用户交易[32].

研究者对静态场景下的比特币交易费问题进行探索[34], 其结论是强制性的交易费用、限制区块容量以及在去中心化市场中确定区块空间价格, 三者是等价的. 如果区块容量没有限制, 当矿工挖矿时, 待打包的交易已经存在, 这时矿工是 Stackelberg 博弈追随者, 不考虑交易费、打包所有交易是这个博弈中唯一的子博弈完美纳什均衡. 因此作者认为区块容量必须有限制, 并且不能由矿工确定限制, 防止矿工没有收入导致矿工流失和比特币网络的死亡.

Gavin Andresen 持相反观点, 他基于 Evenly rotating economy (ERE) 经济理论提出, 在一个竞争性的市场中, 供给、需求和价格将会找到一个平衡点, 价格等于供应商的边际成本加上一些净收入 (因为供应商总是可以选择用他们的时间或金钱做一些更有利可图的事情). 因此, 如果没有人为限制 (例如区块大小上限), 交易费用将会下降到矿商支付的边际成本, 但不为零 (为了使 ERE 理论成立, 供给和需求必须保持不变, 然而在实际市场中难以达到, 详见 https://99Bitcoins.com/Bitcoin-block-size-economics-revised/).

图 15　比特币价格波动

Fig. 15　Bitcoin price fluctuations

挖矿所用的硬件设备经历了从 CPU 到 GPU, 再到 ASIC (Application specific integrated circuit, 专用集成电路) 三个阶段的发展历程, 提高了比特币网络的哈希率, 降低了每哈希率的单位功耗, 提高了矿工的门槛和成本. 研究者提出了比特币挖矿过程和比特币交易的人工市场模型[36]. 在挖矿博弈中, 矿工可以自由选择是否参与挖矿, 其纳什均衡是矿工的期望收益为零. 此外, 矿工数量还需满足一定大小, 以维持新区块的到达率. 假设没有交易费用, 而比特币价格保持稳定, 那么随着区块奖励下降 (但仍然在一定水平之上), 矿工数量也会随之下降, 导致比特币难度降低; 假设区块奖励稳定, 而比特币价格或者交易费上升, 那么矿工数量会增加, 导致比特币难度提高. 这两种情况都能保持不变的新区块生成速率. 在交易费支付博弈中, 根据新交易流入内存池的速率与矿工从内存池取出交易的速率, 该博弈的均衡有三种: a) 所有用户都不支付手续费; b) 部分用户支付手续费; c) 所有用户都支付手续费.

综合来看, 相关研究尚未能解决两个根本问题: 1) 建立合理的交易费机制, 保障矿工交易费以免算力流失, 同时避免交易成本过高引起用户的流失; 2) 区块容量限制与交易费的关系.

5 总结与展望

中本聪在比特币白皮书中提到, 互联网交易需要基于可信第三方, 增加了交易的成本, 限制了实际可行的最小交易规模, 也限制了日常的小额支付交易, 比特币的设计初衷是一种点对点的电子货币系统, 它基于密码学原理而不基于中心化的信用, 使得任何达成一致的双方, 能够不需要第三方中介的参与而直接交易, 从而降低交易成本. 然而, 考虑到比特币价格的急剧震荡以及交易手续费比例的居高不下, 基于比特币进行小额交易的代价已经远远高于传统交易方式. 比特币扩容已成大势所趋, 引起了业界与学术界的密切关注. 本文从关键技术、制约因素和衍生问题三方面, 对比特币扩容问题进行分析与总结.

扩容问题不是比特币系统独有的问题, 而是整个区块链生态圈都亟待解决的问题. 目前, 包括闪电网络、侧链在内的并行扩容方案已成为当前热点, 这类方案的特点是在原有的主链之上, 增设多条并行的交易结算和清算通道, 从而达到提高交易吞吐量的目的. 虽然扩容方案百花齐放、蓬勃发展, 比特币乃至大部分区块链系统的扩容进展却相对滞后. 究其原因, 主要归因于现有方案欠缺对于区块链系统在自身不同配置条件下和各类应用场景下的计算实验与预测解析能力, 因此只能依靠真实系统的 "链上" 增量式试错实验、或者利用沙盒等 "摸着石头过河" 的经验性预测方法, 来预估区块链扩容效果[9]. 而区块链的分布式运行性质, 使得一旦方案实施中出现偏差或错误, 难以进行系统回滚与纠错. 平行区块链作为平行智能与区块链技术的深度结合, 是有效解决区块链建模、实验与决策相关问题的理论方法. 因此, 我们的下一步工作是在平行智能和平行区块链理论的指导下, 采用 ACP 方法 (Artificial systems + Computational experiments + Parallel execution, 人工系统 + 计算实验 + 平行执行)[37−38], 提出平行扩容方案, 为相关人士提供有意义的建议.

References

1 Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

2 Yuan Yong, Zhou Tao, Zhou Ao-Ying, Duan Yong-Chao, Wang Fei-Yue. Blockchain technology: From data intelligence to knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1485−1490
(袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, **43**(9): 1485−1490)

3 Shen Xin, Pei Qing-Qi, Liu Xue-Feng. Survey of block chain. *Chinese Journal of Network and Information Security*, 2016, **2**(11): 11−20
(沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述. 网络与信息安全学报, 2016, **2**(11): 11−20)

4 Li Mu-Nan. Analyzing intellectual structure of related topics to blockchain and Bitcoin: From co-citation clustering and bibliographic coupling perspectives. *Acta Automatica Sinica*, 2017, **43**(9): 1509−1519
(李牧南. 区块链和比特币相关主题的知识结构分析: 共被引和耦合聚类分析视角. 自动化学报, 2017, **43**(9): 1509−1519)

5 Jia Da-Yu, Xin Jun-Chang, Wang Zhi-Qiong, Guo Wei, Wang Guo-Ren. A storage capacity scalable model for blockchain. *Journal of Frontiers of Computer Science & Technology*, 2018, **12**(4): 515−535
(贾大宇, 信俊昌, 王之琼, 郭薇, 王国仁. 区块链的存储容量可扩展模型. 计算机科学与探索, 2018, **12**(4): 515−535)

6 Croman K, Decker C, Eyal I, Gencer A E, Juels A, Kosba A, et al. On scaling decentralized blockchains. In: Proceedings of the 20th International Conference on Financial Cryptography and Data Security. Barbados, West Indies: Springer, 2016. 106−125

7 Wang Fei-Yue. Parallel system methods for management and control of complex systems. *Control and Decision*, 2004, **19**(5): 485−489
(王飞跃. 平行系统方法与复杂系统的管理和控制. 控制与决策, 2004, **19**(5): 485−489)

8 Wang Fei-Yue. On the modeling, analysis, control and management of complex systems. *Complex system and complexity science*, 2006, **3**(2): 26−34
(王飞跃. 关于复杂系统的建模、分析、控制和管理. 复杂系统与复杂性科学, 2006, **3**(2): 26−34)

9 Yuan Yong, Wang Fei-Yue. Parallel blockchain: Concept, methods and issues. *Acta Automatica Sinica*, 2017, **43**(10): 1703−1712
(袁勇, 王飞跃. 平行区块链: 概念, 方法与内涵解析. 自动化学报, 2017, **43**(10): 1703−1712)

10 Yuan Yong, Wang Fei-Yue. Towards blockchain-based intelligent transportation systems. In: Proceedings of the 19th International Conference on Intelligent Transportation Systems (ITSC). Rio de Janeiro, Brazil: IEEE, 2016. 2663−2668

11 Lou Yao-Xiong, Wu Jun. Analysis of Legal Issues of Bitcoin. *Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition)*, 2013, **15**(4): 25−31
(娄耀雄, 武君. 比特币法律问题分析. 北京邮电大学学报 (社会科学版), 2013, **15**(4): 25−31)

12 Yu Hui, Zhang Zong-Yang, Liu Jian-Wei. Research on Scaling Technology of Bitcoin Blockchain. *Journal of Computer Research and Development*, 2017, **54**(10): 2390−2403
(喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究. 计算机研究与发展, 2017, **54**(10): 2390−2403)

13 Increasing the block size [online], available: https: //www. reddit.com/r/Bitcoin/comments/2vefmp/please_eli5_besides_increasing_the_block_size_why/, February 10, 2015.

14 Why we cannot decrease [online], available: https: //www. reddit.com/r/Bitcoin/comments/35hpkt/please_remind_me_once_again_why_we_cant_decrease/, May 10, 2015.

15 Eyal I, Gencer A E, Sirer E G, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In: Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI). Santa Clara, USA: USENIX, 2016. 45−59

16 Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments [online], available: http: //lightning.network/lightning-network-paper.pdf, January 1, 2015.

17 Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, et al. Enabling blockchain innovations with pegged sidechains [online], available: http: //www.opensciencereview.com/papers/123/enabling blockchain-innovations-with-pegged-sidechains, October 22, 2014.

18 Decker C, Wattenhofer R. Information propagation in the Bitcoin network. In: Proceedings of the 2013 IEEE Peer-to-Peer Computing (P2P). Trento, Italy: IEEE, 2013. 1−10

19 Miller A, Juels A, Shi E, Parno B, Katz J. Permacoin: Repurposing bitcoin work for data preservation. In: Proceedings of the 35th IEEE Symposium on Security and Privacy (SP). San Jose, USA: IEEE, 2014. 475−490

20 Zhang Bin. Security risk study of blockchain. *Telecom Engineering Technics and Standardization*, 2017, **30**(11): 1−5
(张滨. 区块链安全风险研究. 电信工程技术与标准化, 2017, **30**(11): 1−5)

21 Zhu Yan, Gan Guo-Hua, Deng Di, Ji Fei-Fei, Chen Ai-Ping. Security Architecture and Key Technologies of Blockchain. *Journal of Information Securyity Research*, 2016, **2**(12): 1090−1097
(朱岩, 甘国华, 邓迪, 姬菲菲, 陈爱平. 区块链关键技术中的安全性研究. 信息安全研究, 2016, **2**(12): 1090−1097)

22 Xie Hui, Wang Jian. Study on block chain technology and its applications. *Netinfo Security*, 2016, 9: 192−195
(谢辉, 王健. 区块链技术及其应用研究. 信息网络安全, 2016, 9: 192−195)

23 Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Barbados, West Indies: Springer, 2014. 436−454

24 Sompolinsky Y, Lewenberg Y, Zohar A. SPECTRE: A fast and scalable cryptocurrency protocol [online], available: https: //eprint.iacr.org/2016/1159.pdf, January 1, 2016

25 Sompolinsky Y, Zohar A. Secure high-rate transaction processing in Bitcoin. In: Proceedings of the 19th International Conference on Financial Cryptography and Data Security. Puerto Rico, USA: Springer, 2015. 507−527

26 Beikverdi A, Song J. Trend of centralization in Bitcoin′s distributed network. In: Proceedings of the 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). Takamatsu, Japan: IEEE, 2015. 1−6

27 Gervais A, Karame G, Capkun S, Capkun V. Is Bitcoin a decentralized currency? In: Proceedings of the 35th IEEE Symposium on Security and Privacy (SP). San Jose, USA: IEEE, 2014. 54−60

28 Bitcoin Nodes Summary [online], available: https: // coin.dance/nodes, January 18, 2018

29 Deng Wei. Price bubbles in Bitcoin: Evidence, causes and implications. *Journal of Shanghai University of Finance and Economics*, 2017, **19**(2): 50−62
(邓伟. 比特币价格泡沫: 证据、原因与启示. 上海财经大学学报, 2017, **19**(2): 50−62)

30 Han Yu-Guang, Sun Wei, Zhu Li. The rise of Bitcoin: Diffusion rate and diffusion power. *East China Economic Management*, 2015, 3: 171−177
(韩裕光, 孙伟, 朱力. 比特币的崛起: 扩散速度与扩散动力. 华东经济管理, 2015, 3: 171−177)

31 Ciaian P, Rajcaniova M, Kancs D A. The economics of Bitcoin price formation. *Applied Economics*, 2016, **48**(19): 1799−1815

32 Kaskaloglu, Kerem. Near zero Bitcoin transaction fees cannot last forever. In: Proceedings of the 2014 International Conference on Digital Security and Forensics (DigitalSec2014). Ostrava, Czech Republic: SDIWC, 2014. 91−99

33 Kristoufek L. Bitcoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific reports*, 2013, 3: 3415

34 Houy N. The economics of Bitcoin transaction fees [online], available: https: //ssrn.com/abstract=2400519, February 24, 2014

35 Dwyer G P. The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 2015, 17: 81−91

36 Cocco L, Marchesi M. Modeling and simulation of the economics of mining in the Bitcoin market. *PloS one*, 2016, **11**(10): e0164603

37 Wen D, Yuan Y, Li X. Artificial societies, computational experiments, and parallel systems: An investigation on a computational theory for complex socio-economic systems. *IEEE Transactions on Services Computing*, 2013, **6**(2): 177−185

38 Wang Fei-Yue, Zeng Danial Dajun, Yuan Yong. An ACP-based approach for complexity analysis of E-commerce system. *Complex Systems and Complexity Science*, 2008, **5**(3): 1−8
(王飞跃, 曾大军, 袁勇. 基于 ACP 方法的电子商务系统复杂性研究. 复杂系统与复杂性科学, 2008, **5**(3): 1−8)

曾 帅 中国科学院自动化研究所复杂系统管理与控制国家重点实验室助理研究员. 2011 年于北京邮电大学获得信号与信息处理专业博士学位. 主要研究方向为社会计算, 策略优化与区块链.
E-mail: shuai.zeng@ia.ac.cn
(**ZENG Shuai** Assistant professor at The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. She received her Ph. D. degree in signal and information processing from Beijing University of Post & Telecommunication in 2011. Her research interest covers social computing, strategy optimaization and blockchain.)

袁 勇 中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员. 2008 年于山东科技大学获得计算机软件与理论专业博士学位. 主要研究方向为社会计算, 计算广告与区块链. 本文通信作者. E-mail: yong.yuan@ia.ac.cn
(**YUAN Yong** Associate professor at The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his Ph. D. degree in computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers social computing, computational advertising and blockchain. Corresponding author of this paper.)

倪晓春 中国科学院自动化研究所复杂系统管理与控制国家重点实验室工程师. 2008 年于大连海事大学获得管理科学与工程专业硕士学位. 主要研究方向为社会计算与区块链.
E-mail: xiaochun.ni@ia.ac.cn
(**NI Xiao-chun** Engineer at The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his master degree in management science and engineering from Dalian Maritime University in 2008. His research interest covers social computing and knowledge automation.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任, 国防科技大学军事计算实验与平行系统技术研究中心主任, 中国科学院大学中国经济与社会安全研究中心主任, 青岛智能产业技术研究院院长. 主要研究方向为平行系统的方法与应用, 社会计算, 平行智能以及知识自动化.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** State specially appointed expert and director of the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Professor of the Research Center for Computational Experiments and Parallel Systems Technology, National University of Defense Technology. Director of China Economic and Social Security Research Center in University of Chinese Academy of Sciences. Dean of Qingdao Academy of Intelligent Industries. His research interest covers methods and applications for parallel systems, social computing, parallel intelligence, and knowledge automation.)