计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170416
54(10):2390-2403,2017

比特币区块链扩容技术研究

喻 辉[1] 张宗洋[1,2] 刘建伟[1]

[1](北京航空航天大学电子信息工程学院 北京 100191)

[2](信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)

(yhsteven@outlook.com)

Research on Scaling Technology of Bitcoin Blockchain

Yu Hui[1], Zhang Zongyang[1,2], and Liu Jianwei[1]

[1](*School of Electronic and Information Engineering, Beihang University, Beijing* 100191)

[2](*State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing* 100093)

Abstract Bitcoin is a crypto currency introduced by Satoshi Nakamoto in 2008. It has the features of decentralization, cross-border and fixed total amount and has become one of the most widely used crypto currencies. Due to some initial limitations set by the inventor and the following developers, the transaction throughput of the Bitcoin network is much limited. Recently, the transaction throughput has been close to the maximum limit, and the corresponding transaction confirmation time has been greatly increased. Not only this affects user experiences of Bitcoin and limits its usage, but also this puts forward higher requirements for Bitcoin protocol design. Focusing on the challenges of transaction processing performance, this paper aims to promote blockchain capacity and takes a deep research on Bitcoin protocol. Firstly, we do a research on the current network status of Bitcoin, and analyze the transaction delay according to Bitcoin transaction data. Secondly, we analyze the feasibility and effectiveness of on-chain scaling proposals. Thirdly, we analyze mechanics and effects of off-chain scaling proposals. Finally, we analyze the advantages and disadvantages of on-chain/off-chain scaling proposals, and propose a scaling roadmap which meets the community requirements. The recent progress on the Bitcoin scaling shows the correctness of our proposals.

Key words Bitcoin; blockchain; scaling; segregated witness; lightning network

摘 要 比特币是中本聪(Nakamoto)于2008年提出的数字货币,它具有去中心化、跨国界和发行总量固定等特性,现在已经成为使用最广泛的数字货币之一.然而,比特币设计初期的一些人为限制,导致现有网络处理交易的速率十分有限,最近交易处理能力已经接近上限,交易确认时间显著增加.这不仅严重影响比特币的使用体验,进而限制使用范围,而且对比特币的设计提出更高的要求.针对比特币所面临的交易处理性能挑战,以提升区块链容量为目标对比特币展开深入研究.首先,分析比特币当前网络状态,根据比特币交易数据,统计交易延迟情况;其次,针对链上扩容方案,分析可行性,研究扩容效果;

收稿日期:2017-06-09;**修回日期**:2017-08-02

基金项目:中国科学院信息工程研究所信息安全国家重点实验室开放课题(2017-MS-02)

This work was supported by the Fund of the State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences) (2017-MS-02).

通信作者:张宗洋(zongyangzhang@buaa.edu.cn)

再次,针对链下扩容方案,分析作用原理,研究扩容效果;最后,分析链上/链下扩容方案优缺点,提出适应社区的可行的比特币扩容路线方案.最新比特币扩容的进展进一步证明了我们结论的正确性.

关键词　比特币;区块链;扩容;见证隔离;闪电网络

中图法分类号　TN918; TP309

比特币是一种去中心化的数字货币,最早由中本聪(Nakamoto)于2008年10月提出[1],其目的是避免传统金融体系中存在中心机构可能带来的风险.和传统电子货币相比,比特币具有系统健壮性强、使用便捷和安全性高等优势.自从被推出以来,比特币正受到越来越多的关注[2].随着比特币的广泛使用,比特币设计之初的一些缺陷逐渐显露出来,其中非常严重的缺陷就是区块链容量不足.

从2012年开始,平均区块大小不断增加.在2016年年中左右,区块容量已经接近1 MB上限[3].这意味着一些交易将不能及时地被收集到区块中,交易双方需要等待更长的时间确认交易.如果交易频次继续增加而区块容量保持不变,那么一些交易可能永远也不能入块.因此,这一问题将会严重影响比特币的使用体验.

文献[4]针对研究交易延迟问题,分析2016年5月交易入块情况,结果表明:43%的交易在发布超过1 h后仍未进入区块链.文献[5]列举出比特币等密码货币的研究远景和面临的各种挑战,其中之一就是可扩展性问题.由于改变比特币规则需要引入分叉,同时造成各方面的影响,因此比特币扩容是一个非常复杂的问题.

文献[6]指出,将交易杂凑值代替交易数据可以提升网络处理交易的能力.同时,该文献主张以修改区块链本身结构的方式达到扩容的目的.文献[7]研究区块在网络中的传播情况,指出过大区块需要更长的时间传播至整个网络,传播延迟将不再远小于区块间隔,这会影响网络的共识机制,造成高孤块率等问题.同时作者指出当前网络未被充分利用,可以改进比特币协议以提高网络利用效率.文献[8]引入定量框架分析基于工作量证明的区块链安全和性能,并分析了区块参数改变对于比特币系统安全性的影响.作者得出结论:在区块大小是1 MB的前提下,将区块间隔降低至1 min不会显著影响比特币区块链的安全性.

为解决比特币区块链容量不足带来的问题,比特币社区已经提出多个解决方案,下面依次介绍代表性方案.

2015年6月,Andresen在比特币改进建议(bitcoin improvement protocol)BIP101中提出区块容量限制在未来一段时间内以可预测方式增大[9];同月,Garzik在BIP102中提出区块容量上限一次性从1 MB增长到2 MB[10];同期,相关人员提出很多类似的直接提高区块链上限的改进建议[11-12].由于交易数目与区块大小成正比,因此通过增大单个区块的大小,可以使得更多的交易被容纳.

2015年12月,Lombrozo,Lau和Wuille在BIP141中提出的见证隔离(segregated witness)技术也对区块链扩容有帮助[13].当前的比特币交易中,交易数据与签名数据保存于同一数据结构中.见证隔离则将签名数据从交易中分离出来,组成新的结构另行保存.由于旧节点不能解析这些新的数据,因此他们认为区块大小要小于新节点,这意味着区块实际大小可以超过1 MB.

2015年,Poon和Dryja提出闪电网络方案,将频繁的小额支付利用事先建立的通道离链完成[14].这种方案可以避免大量小额交易占用区块链容量;文献[15]提出了建立双向微支付通道的协议,允许用户建立离线通道,实现无延迟的实时支付,同时保证了端到端的安全性;文献[16]对上述方案作了改进,提出了新的支付通道Sprites.利用状态通道,Sprites将闪电网络在最坏情况下的抵押开销复杂度大为降低,由$O(\ell\Delta)$变为$O(\ell+\Delta)$,其中ℓ,Δ分别代表通道个数和链上交易确认时间;文献[17]引入Teechan,它是一种全双工的支付通道框架,可直接部署在现有区块链上,比闪电网络具有更高的交易容量和更低的交易延迟.但是,它需要利用具备可信执行环境的安全硬件,例如Intel SGX,因此会额外增加开销;Teechan的升级版Teechain实现了沿路径支付,允许未直接建立连接的用户交换资金[18].

可见,针对区块链容量不足的情况,社区和学术界都已经提出多个扩容方案.但是依然存在区块链统计数据不直观、链上扩容方案缺乏可行性分析、见证隔离对区块容量的贡献不明确和社区意见不统一等问题.

本文主要贡献有3个方面：

1）针对区块容量达到上限的问题，分析当前比特币网络中交易确认状态. 通过抓取2017年1～3月的比特币交易数据，统计分析交易确认理论时间和实际时间的差别. 已经进入区块的交易中，有16%等待时间超过1 h，甚至有1%等待时间超过1 d. 另外，待确认交易(unconfirmed transaction)池不断扩大，一度超过110 MB.

2）针对链上扩容方案争论，分析方案的优点和缺点. 链上扩容提倡增大区块容量上限，此方案对改善交易延迟效果显著，将区块容量上限设定为2 MB，即可解决当下交易延迟问题. 但考虑到当前网络情况，为避免过高的孤块产生率，最大区块不应超过4MB. 链上扩容优势在于见效快，但是无限扩容易造成中心化.

3）针对链下扩容方案的不确定性，分析链下扩容效果. 链下扩容方案也附带有链上扩容效果，基于当前交易比例的统计显示，见证隔离最多可以将区块容量提升83%. 基于见证隔离的闪电网络技术，完全部署可以极大提高交易处理能力，缩短确认时间. 链下扩容可以达到近乎无限的交易处理能力，但网络建立需要时间.

1 背景知识

本节简要介绍比特币的相关背景知识，包括比特币的交易、区块链形式和工作量证明机制等，详细的介绍可以参考文献[19-20].

1）比特币交易. 比特币是一种基于交易的数字货币，一切行为均通过交易完成. 每一项交易均有至少一个输入和至少一个输出. 每一个交易指向另一个交易的输出，用于表明资金的来源，仅当交易被正确签名之后，验证方可通过. 交易可以包含多个输入和多个输出，从而起到拆分与合并资金的功能.

2）比特币脚本. 交易输出中存在scriptPubKey脚本，在标准P2PKH交易中，scriptPubKey包含收款人的公钥杂凑值. 交易输入中存在scriptSig脚本，包含公钥和签名等信息. 验证交易时，依次运行scriptSig脚本与前一交易中的scriptPubKey脚本，如果成功运行并在栈顶设置true，即相当于成功验证交易发起人的公钥与签名，那么证明交易发起人具备对应输出的使用权限，验证通过[21]. 在BIP16中，P2SH类型的交易被引入. 该类型允许输出中不指明收款人公钥杂凑，并用一段脚本的杂凑替代. 这种交易将复杂性从输出脚本转移到了输入脚本，使得付款更加方便，利于多重签名等交易普及[22].

3）比特币账本. 基于交易的数字货币存在的最大问题是双花(double-spending)，即支付者生成2笔交易，共用同一项输出. 解决办法之一是维护一个任何人都可以访问的账本，记录所有历史交易，使收款方可以查看一项输出是否已被使用过. 比特币使用梅克尔树与区块链构建全局账本. 当交易双方需要交易快速完成时，收款方会选择在交易未进入区块链时即接受，这会带来额外的双花风险[23]. 只要攻击者算力资源不超过全网算力的50%，此风险随时间增长呈指数级下降[1].

4）梅克尔树. 梅克尔树是一种二叉树，其叶子节点用于存放数据，其他节点为2个子节点串联的杂凑值. 比特币将交易杂凑值存放于梅克尔树叶子节点中，任何一笔交易的变动都将影响到梅克尔树根的值. 因此，只要保留梅克尔树根的值，即可验证每一笔交易是否被篡改[19].

5）区块链. 每个区块中包含一个梅克尔树根，作为当前区块所有交易的指代. 除此之外，区块中还包含上一个区块头的杂凑值，作为此前区块的指代. 区块依次相连形成区块链，使用这种链状结构，只要保存最后一个区块头的杂凑值，就能保证整条区块链上所有交易不被篡改[19]. 比特币区块头包含如下字段：version字段，表示当前区块版本号，被解释为比特向量，用于表明支持的特性；previous block header Hash字段，表示前一区块头的杂凑值，是所有历史数据的指代；merkle root Hash字段，表示梅克尔树根，是区块中所有交易的指代；time字段，表示区块产生的时间，是Unix时间戳；nBits字段与nonce字段是工作量证明相关的字段[24].

6）工作量证明. 作为一种去中心化的数字货币，比特币区块链的维护工作无法由中心化机构完成. 实际中区块链由运行于互联网上的节点进行维护. 在新区块生成问题上，所有节点需要达成共识. 比特币采用的解决方案是工作量证明机制. 所有节点利用算力解决一个难题，得到正确结果的节点有资格发布新的区块. 因此，难题应该是难于求解和易于验证的. 比特币采用的难题为：改变区块头中的nonce字段(如果nonce字段遍历完毕，那么矿工也可以改变coinbase交易中的coinbase script字段，从而改变梅克尔根的值)，计算区块头杂凑值，仅当杂凑值低于某个目标值时，区块合法，目标值越低，难度越高. 这样，计算出合法区块的节点即可证明自

己已经花费足够多的算力.目标值保存在区块头的nBits字段中,每经过2016个区块(约2周),根据平均区块间隔重新确定目标值,调整难题难度,以保证平均区块间隔的稳定.

2　比特币网络状态

本节对比特币网络的当前状态进行分析.当前,比特币区块大小已经接近上限.通过统计最新数据,计算交易延迟时间与待确认交易内存池的大小,借此反映区块链容量不足对比特币使用体验的影响,揭示出区块链扩容的紧迫性,同时为后续分析提供数据支撑.

2.1　交易延迟时间

比特币的交易由交易发起者生成,并广播至比特币网络,等待矿工确认.矿工将这些未确认的交易打包放入新的区块中.大约每10 min一个新的合法区块产生并连接至现有区块链末端.交易从被发起到最终进入区块链的时间为交易延迟时间.因此,正常情况下,如果忽略交易传播至整个网络所用的时间,平均交易延迟时间应在5 min左右.我们通过分析2017年初的区块链数据,研究当前交易的延迟状况.

文献[4]通过运行比特币节点,统计每笔交易的产生时间与入块时间,统计交易的入块情况.与此方法不同,本文通过分析已存在于区块中的数据进而统计交易延迟情况.每一项交易在产生时,都会包含time字段(此信息不存在于区块链,由网站提供),用于表明交易产生时间.同时,每一个区块的头部都包含有time字段,记录区块的产生时间.因此可以通过区块中time字段与交易中time字段的比较,估算出交易的延迟时间.具体步骤如下:

1)获取时间戳位于2017-01-01 0:0:0—2017-03-16 0:0:0之间的区块,区块高度在446 033～457 418之间.采用https://blockchain.info/网站提供的API,获取JSON格式的区块数据.

2)对于每一个区块,将区块时间戳记为T_B,将当前区块中每笔交易的时间戳与T_B相减,差值即为该交易的延迟时间,将其记录.

3)以分钟为单位进行统计,并做出交易占比-延迟时间统计图.

图1为交易延迟时间的统计图.曲线代表交易延迟时间小于某值的交易占比,横轴采用对数坐标.3条虚线分别代表延迟10 min,60 min和1 d.实线与虚线3个交点分别为(10,48.34%)、(60,83.71%)、(1440,98.96%).因此可以得出结论,大约有16%的交易延迟时间超过1 h,甚至有1%的交易在1 d之后才能进入区块链,这个时间严重超出正常情况下的延迟时间.另外,将步骤2中计算的延迟时间求算术平均数,得到本次测得的交易延迟时间平均值为76.53 min,和5 min的理论值相比也过长.根据交易额进行加权平均,得到的交易延迟时间平均值为68.12 min,小于算术平均值,这说明交易额大的交易更容易入块.根据交易大小进行加权平均,得到的交易延迟时间平均值为116.59 min,这证明矿工更倾向于收录体积较小的交易.

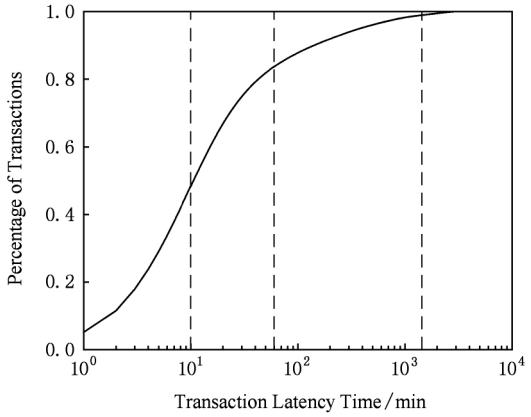


Fig. 1　Transaction latency time from 2017-01-01—2017-03-15

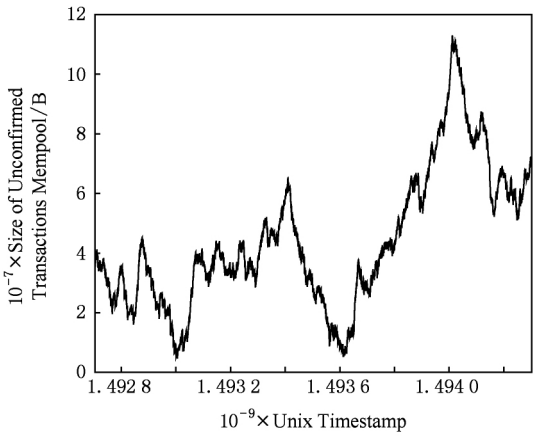
图1　2017-01-01—2017-03-15交易延迟时间统计

在正常情况下,矿工会尽可能在新区块中打包所有未确认交易.因为,每笔交易都包含交易费,打包更多的交易几乎不会影响成本却这可以使矿工获得更多的收益.因此,在正常情况下,交易的滞留不会发生.但是,当矿工受限于区块容量时,会尽可能将包含交易费较多的交易收入区块,将其他交易推迟处理,以获得最大收益.在这种环境下,小额交易的延迟时间增加.因此,当前区块容量已经成为交易延迟时间的主要影响因素.

2.2　待确认交易数量

如1.1节中所述,当一项交易被广播至全网并等待进入区块链时,它是一项待确认交易.通常,待确认交易的总大小不会超过1 MB,这样可以保证新区块能够将它们全部包含.我们从https://btc.com/获取实时数据,每分钟记录待确认交易内存池的总大小,并利用北京时间2017-04-21 0:0:0—2017-05-09 12:0:0的数据绘出图2.

图 2 展示待确认交易内存池的总大小随时间的变化状况. 在正常情况下,曲线应以约 10 min 一次的频率归零,峰值也不应超过 1 MB. 而实际的曲线在 19 d 的统计中从未归零,最小值为 4.7 MB,最大值高达 113.0 MB,远超正常值. 从图 2 可以明显看到,由于比特币区块链容量不足,导致大量的交易滞留,排队等待确认. 这可以印证 2.1 节的结论.



PS: The timestamp of x-axis is from 2017-04-21 0:0:0 to 2017-05-09 12:0:0(19.5 d)

Fig. 2 Size of unconfirmed transactions mempool

图 2 待确认交易内存池大小

3 链上扩容方案

本节研究比特币扩容方案之一:链上扩容(on-chain scaling). 这种方案提议直接修改比特币区块容量上限,使其可以容纳更多的交易. 针对链上扩容方案,本节分析单区块大小受限于网络承载力的上限,对比现有链上扩容方案,说明可行性. 其次,分析链上扩容方案对当前交易延迟问题的改善效果. 最后,对于链上扩容方案普遍使用的硬分叉风险进行分析.

3.1 现有链上扩容方案

最容易的方案就是在设计上改变单个区块 1 MB 大小的限制,以达到扩容的目的. 现在有多个提案建议通过硬分叉直接提高单个区块大小:

在 BIP101 中,建议区块容量上限在 2016-01-11 0:0:0 直接提高到 8 000 000 B. 此后,每过 63 072 000 s (2 年)上限翻倍,直至 2036-01-06 0:0:0 达到 8 192 000 000 B(即 8 GB)[9].

在 BIP102 中,建议区块容量直接从 1 MB 提升至 2 MB,在不改变任何其他规则的前提下解决当下困境[10].

Bitcoin Unlimited 方案提出,区块容量上限不再是固定值,而是可由矿工投票改变. 矿工可以通过投票以当前区块容量上限为基准,在一定浮动范围内决定新区块容量上限[25].

3.2 网络承载力分析

在 3.1 节所列举的链上扩容方案存在一个关键的隐患:不能确定在未来某段时间内,网络带宽和存储容量是否足以支撑更大的区块.

由于比特币网络的去中心化,测试整个网络的承载能力并不容易. 文献[7,26]提供了一种分析方案. 根据比特币协议,当节点 A 收到一个新的区块时,首先验证区块的正确性. 如果验证通过,节点 A 会广播 inv 消息,通知其他节点新区块的存在. 如果某节点 B 在此之前未收到同样的 inv 消息,则会向节点 A 发送 getdata 消息,向节点 A 索取 block[27]. 因此,可以认为节点 A 发送 inv 消息的时间,是其收到新区块的时间. 测量者可以伪装成正常节点接入比特币网络,连接大量其他节点,监测 inv 消息的发送情况,从而判断区块在网络中的传播情况. 以一个新区块发布时,上一个区块应已传播至 90% 的节点为标准,可以计算出网络中可以传输的最大区块容量.

由表 1 可见,在 2015 年,网络可承载的区块大小上限为 4 MB 左右. 从 2012—2015 年的 3 年时间,网络状态提升 100%. 但是传播延迟主要来自于 2 个方面:1)inv 与 getdata 消息的网络延迟 T_d,这部分与区块大小无关;2)block 数据的传输延迟 T_t,这部分和区块大小成正比. 当区块较大时,$T_t \gg T_d$,传播延迟主要来自于 T_t,由此计算的区块大小上限更为准确. 当区块较小时,T_t 与 T_d 均对传播延迟有贡献,此时计算的区块大小上限偏小. 因此,从 2012—2015 年,比特币网络状态提升小于表 1 所表现的 100%.

Table 1 Block Size Limit Constrained by Network

表 1 受限于网络的区块大小上限

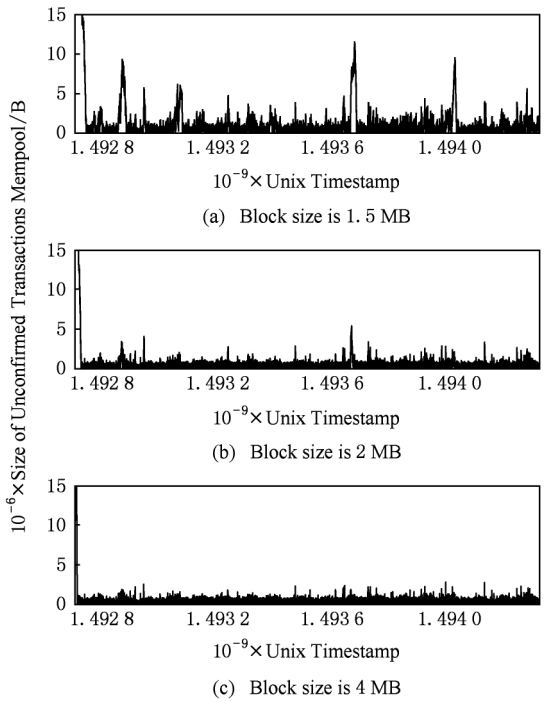
Year	90% Effective Throughput /Kbps	Block Interval /min	Maximum Block Size /KB	Data Source
2012	26.8	10	2 010	Ref[7,26]
2015	54.7	10	4 102	Ref[7]

根据上述测量,BIP101 提出的方案"立即提升区块大小上限至 8 MB,之后每 2 年提升 100%"是不合理的. 首先,提升区块大小上限至 8 MB 会超出网络承载能力,这意味着新区块产生时,依然有 10%

以上的节点没有收到上一个区块,增加孤块产生的风险.另一方面,每 2 年提升 100%的方案也超过网络发展速度,使得未来孤块产生风险进一步提高,影响网络稳定性.根据文献[28]的研究,区块的传播延迟与区块大小是线性相关的.更大的传播延迟意味着部分节点的算力并未用于主链计算,这部分算力无法用于增强比特币安全性.同时,孤块造成的分叉会导致算力进一步分散,增加链的维护难度,同时也降低了算力攻击的难度[28].

3.3　改变区块容量效果分析

为验证增大区块容量对于当前交易延迟的改善作用,利用 1.2 节中的数据,模拟当区块容量增加到 1.5 MB,2 MB 和 4 MB 时,待确认交易内存池中交易大小的状况.假设:1) 在 2017 年 4 月 21 日,区块容量立即增大;2) 矿工是完全理性的,会尽可能提高自己的收益;3) 每 10 min 产生一个新的区块.模拟结果如图 3 所示.对比图 2 与图 3 可以看出,提升区块容量可显著减少待确认交易内存池大小.假设交易在时间轴上均匀分布而且每 10 min 产生一个新区块,待确认交易值平均值小于 0.5×区块容量时,可以保证所有交易延迟不超过 10 min.以此为标准,区块容量提升至 1.5 MB 并不能完全解决当下问题.区块容量提升至 2 MB 可以解决当下交易延迟问题.



PS: The timestamp of x-axis is from 2017-04-21 0:0:0 to 2017-05-09 12:0:0 (19.5 d)

Fig. 3　Size of unconfirmed transactions mempool when the block size is increased

图 3　区块容量不同的待确认交易内存池大小

当交易内存池不为空时开始计时,直到交易内存池再次清空计时结束.将计时的最大值记为交易内存池的最大清空时间.在交易内存池第 1 次清空后开始统计交易内存池的最大清空时间、峰值和平均值,结果统计如表 2 所示:

Table 2　Indexes of Unconfirmed Transactions Mempool Upon Block Size Increase

表 2　区块容量提高后待确认交易内存池指标

Block Size/MB	Maximum Cleance Time /min	Peak Size of Unconfirmed Transactions Mempool/B	Average Size of Unconfirmed Transactions Mempool/B
1(now)	∞	112 979 535	44 181 699
1.5	479	11 535 845	953 141
2	157	5 367 455	397 162
4	16	2 816 053	327 717

3.4　实现方法分析

增大单个区块容量的方式优点在于逻辑简单、易于实现、几乎不会增加复杂度;但是缺点在于在这种情况下,新节点产生的区块在旧节点看来是无效的,这意味着将不可避免地引入硬分叉.旧节点不会接受新节点产生的区块,他们认为包括这些新区块的区块链是无效的,因此会选择继续延长不包含新区块的链.从硬分叉部署的一刻起,只要旧节点存在,区块链将出现 2 条并行的分支,分别独立运行.

支撑以太坊(Ethereum)平台的数字货币以太币经历过硬分叉.自 2016 年 7 月实施硬分叉开始,以太币分裂为 ETH 与 ETC(Ethereum Classic)两种数字货币,其中 ETC 坚持以旧规则延续区块链,而 ETH 以新规则运行[29].至今,2 种数字货币都在稳定运行之中.以太坊的分裂事件证实未达到足够共识的情况下实施区块链硬分叉存在分裂风险.

4　链下扩容方案

除第 2 节提到的链上扩容方案之外,还有另外一套扩容方案:链下扩容(off-chain Scaling).见证隔离方案解决交易延展性问题,是链下扩容的基础.与此同时,见证隔离技术还能带来一定的链上扩容的效果.链下扩容方案的关键在于允许交易离链(off-chain)完成,这通常需要在比特币网络之上建

立第2层网络,闪电网络就是其中的一种.闪电网络通过序列到期可撤销合约(revocable sequence maturity contract, RSMC)和杂凑时间锁定合约(hashed timelocked contract, HTLC)形成离链的微支付模式.这2种合约均需要在见证隔离的基础上构建.

在4.1节首先分析见证隔离的技术细节,统计分析当前网络中各种交易的比例,并基于此对见证隔离附带的链上扩容效果进行计算.然后,在4.2节分析闪电网络实现方式与预期效果.

4.1 见证隔离

4.1.1 技术介绍

见证隔离技术在BIP141～BIP144中被提出并详细描述[13,30-32].

在当前的比特币交易中存在一个问题,交易数据与签名数据存在于同一数据结构中.签名延展性指,可以在不知道私钥的情况下改变签名值,使其依然能够验证通过(这个过程中被签名内容不会改变,即不能通过这种方式篡改交易输出)[33].签名虽然保证交易数据不会被篡改,但是交易ID是整个交易的双杂凑,既包含交易数据,又包含签名数据,签名的延展性导致交易ID不是唯一确定的.而每项交易都会指向其前一项交易的输出,因此基于未确认交易的所有交易都是不安全的[34].文献[35]通过实验证实,主流钱包软件无法正确处理交易延展性带来的问题.

为解决这个问题,BIP62对比特币签名验证增加了额外的限制,避免了第三方利用交易延展性进行攻击的可能,但依然不能阻止交易发起者利用交易延展性的漏洞[36].见证隔离可以彻底解决交易延展性问题.见证隔离将签名数据从交易中撤出,将签名放入被称为见证的数据结构中.一个交易将具有2个ID.其中交易ID依然和原来是相同的,是以下内容序列化(将数据依次转换为字节序列并连续存储)的双杂凑:

[nVersion][txins][txouts][nLockTime]

另外定义见证ID,其为以下新结构序列化后的双杂凑:

[nVersion][marker][flag][txins][txouts][witness][nLockTime]

和旧版本不同的是,签名数据已经从txins中取出并放在见证中,因此交易ID不会具有延展性且唯一.

由于区块头部和新加入的见证结构无关,这意味着见证不会被区块链保护,需要将见证加入当前结构以达到保护见证的目的.为保证通过软分叉完成,考虑到每一个区块的第1项交易必须是一项coinbase交易,用于将挖矿奖励发送给矿工指定的地址,可以将见证数据通过梅克尔树整理,并将梅克尔树根部放入coinbase交易中.当见证数据被改动,coinbase交易ID会改变,从而导致交易梅克尔树根部的改变,最终影响到区块杂凑值,因此区块链可以保证见证数据不被篡改[13].

BIP141～BIP144通过软分叉实现见证隔离,如果它被部署,意味着交易ID是可以唯一确定的,这为后面闪电网络的展开提供条件.

4.1.2 区块容量提升分析

见证隔离可以提高区块的实际大小.因为签名从交易中提出,放入见证数据之中,而旧的节点看不到这部分数据,这意味着他们能看到的部分相对较少,那么保证旧节点看到的区块小于1 MB的同时,区块可以包含更多的交易,新节点识别的实际大小也大于1 MB.

实际部署中,见证隔离本身对于区块链的扩容效果不易确定,因为对于不同类型的交易,提升效果是不同的.因此需要先计算出见证隔离对各种常见交易的空间节约效果,再结合当前网络中各种交易的比例计算出最终结果.

当前最常用的比特币交易为P2PKH与P2SH两种.P2PKH是直接向某公钥的杂凑支付,意味着直接支付给某人,收款人可以用自己的私钥取得交易中币所有权;P2SH是向某个脚本的杂凑值支付,收款时需要运行对应的脚本,通常用于完成多人签名支付,允许指定m个公钥,使用其中n个公钥对应的私钥($n\leqslant m$),即可取得交易中的币.

对应上述2种交易,在见证隔离中,提出2种新的交易类型,即P2WPKH和P2WSH,除交易结构的变化外,输入字段中的scriptSig和输出字段中的scriptPubKey也发生相应变化[13].将scriptSig长度记为s,将txins字段中单个输入的长度记为in,将txouts字段中单个输出的长度记为out,将witnesses字段中单个见证数据长度记为$witness$,交易结构中其他字段总长度记为$meta$.交易各部分占用空间如表3和表4所示.

表3和表4默认输入与输出计数不会超过252,这与通常情况是相符的,包含大量输入/输出的交易是十分稀少的.根据表3和表4,以及常用交易的scriptSig长度,可以得到图4.

Table 3　Space Comparison Between P2PKH and P2WPKH
表 3　P2PKH 与 P2WPKH 占用空间比较

Field	Size of P2PKH Transactions /B	Size of P2WPKH Transactions /B
*in*①	41+*s*	41
out	34	31
meta	10	12
witness	0	*s*

① If $s>252$ B, *in* should be added 2 B.

Table 4　Space Comparison Between P2SH and P2WSH
表 4　P2SH 与 P2WSH 占用空间比较

Field	Size of P2SH Transactions /B	Size of P2WSH Transactions /B
*in*①	41+*s*	41
out	32	43
meta	10	12
witness	0	*s*

① If $s>252$ B, *in* should be added 2 B.

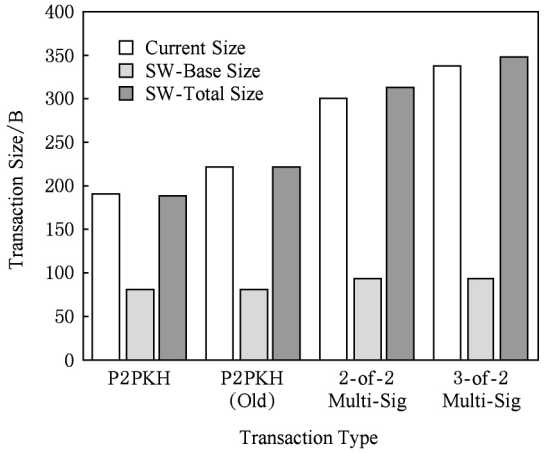


Fig. 4　Space comparison of typical transactions
图 4　典型交易数据占用空间对比

图 4 中基础数据(SW-Base)指除 *witness* 字段之外的数据.这里暂时假设每笔交易都是单输入单输出.存在 2 种 P2PKH 是因为早期的〈PublicKey〉直接使用公钥,而近期普遍使用经过压缩的公钥.因此现在存在 2 种不同长度的 P2PKH 交易.由图 4 可见,见证隔离相对现有设计在基础数据上可以节约 50%左右的空间.同时能看到,交易中签名数据所占比例越大,空间节约效果越明显.用同样的方法,可以计算出其他类型交易相对现有设计的空间节约效果.

为计算见证隔离对于整个网络交易容量的提升效果,需要分析不同类型的交易所占比例.我们用 1.1 节的方法,获取 2017-01-01 0:0:0—2017-03-16 0:0:0 的所有区块.通过交易中包含的地址信息和脚本长度,可以用于判断其类型.图 5 和图 6 显示统计结果.

图 5(a)是对 P2PKH 输出脚本的统计.其中只有一个明显的峰值,在脚本长度 25 B 处,这是标准的 P2PKH 输出脚本.图 5(b)是对 P2SH 输出脚本的统计,由于输出脚本已被规定,因此所有该类型的输出脚本长度都是 23 B.图 5(c)是对于其他类型交易输出脚本的统计,这里包含任何人都可花费的输出、OP_RETURN 销毁证明等[37].

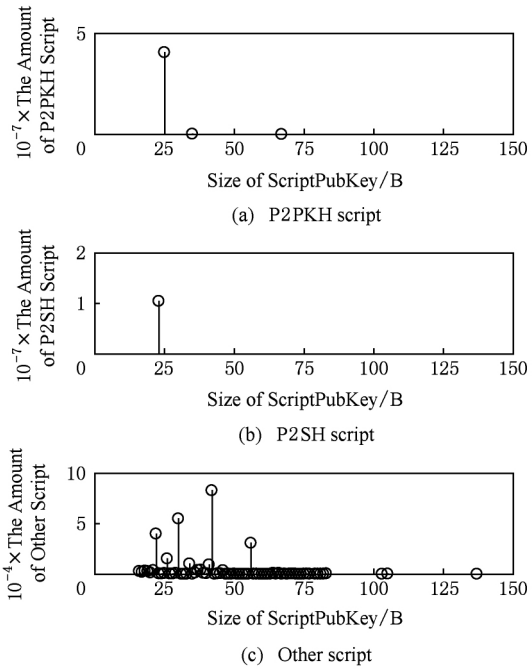


Fig. 5　Length statistics of different types of output scripts
图 5　不同类型输出脚本长度统计

图 6(a)统计 P2PKH 输入脚本.可以看出最高峰值出现在 106～107 B 附近,这是当前最常用的 P2PKH 输入脚本;另外一个峰值在 138～139 B 附近,这是使用早期未压缩的公钥格式产生的交易.图 6(b)统计 P2SH 输入脚本,2 个明显峰值分别在 218 B 和 253 B 附近;它们分别对应 2-of-2 多重签名交易和 2-of-3 多重签名交易.图 6(c)统计其他类型的输入脚本,从纵坐标可以看出,这些交易相对于前面 2 种交易低 4～5 个数量级,因此可以忽略不计.

BIP141 中定义块重(block weight)为 3×基础数据大小+总大小.其中基础数据为区块中不包括见证数据的部分,这是旧节点所能看到的内容;总大小为包含所有字段的数据大小,是新节点看到的区

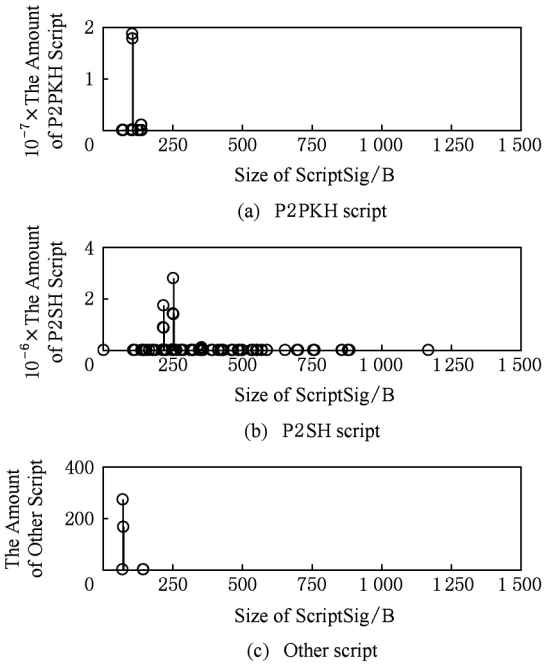


Fig. 6 Length statistics of different types of input scripts

图 6 不同类型输入脚本长度统计

块大小. 新规则规定:块重不大于 4 000 000 B[13]. 在此规则下,可以保证基础数据不大于 1 000 000 B. 根据新规则,假设所有 P2PKH 交易都被 P2WPKH 替代,所有 P2SH 交易都被 P2WSH 替代,将原有统计数据中的交易大小替换为新交易的基础大小与总交易大小,结合各类型交易比例得出结论:新区块中的平均基础数据大小是 361.7 KB,平均总大小是 921.6 KB,平均块重为 2 006.7 KB. 考虑到当前平均区块大小未达理论上限,如果当前区块容量达到理论上限 1 MB,计算出新区块块重为 2 185.4 KB. 新规则允许的最大块重为 4 000 KB,因此新规则允许多容纳 83.0%的交易. 考虑到比特币钱包软件开发商对于见证隔离支持度很高(参看本文 5.1 节),见证隔离部署后,新交易使用比例会持续上升,最终完全替代旧交易.

4.1.3 实现方法分析

见证隔离技术通过软分叉实现,这要求新节点产生的区块对旧节点而言依然是有效的,即交易有效的条件比更新前更加严格. 在大部分节点部署更新之后(见证隔离要求 95%节点支持),更新会激活. 这种情况下区块链不会出现分裂,大部分节点会沿着正确的链工作,即使是少部分未更新的节点也会跟随在最长链上工作(和硬分叉不同,软分叉后主链对旧节点来说是有效的).

软分叉通常通过 BIP9 提供的方式投票部署. 区块头部的 version 字段被解释为比特向量,每一位都可用于一种新特性的标志位[38]. 见证隔离占用第 1 位. 如果矿工将产出区块的 version 第 1 位设定为 1,代表其投票支持见证隔离的激活,否则代表反对. 如果一段时间内支持见证隔离的区块超过 95%,就意味着网络中 95%的算力投票支持见证隔离,新特性随之激活. 主链投票从 2016-11-15 0:0:0—2017-11-15 0:0:0[13]. 如果截止时间前未获得足够支持,投票结束,version 字段投票位收回. 见证隔离的投票与激活过程是开发者提议,矿工算力投票表决.

4.2 闪电网络

闪电网络主要由 RSMC 和 HTLC 两种合约构成. 其中,RSMC 允许 2 用户构建双向离链微支付通道,在限额内实现无限次快速离链转账;HTLC 允许未直接建立通道的 2 用户通过其他中继用户实现转账,同时保证资金不会因中继用户错误或恶意行为而丢失. 这 2 种合约均需要在见证隔离的基础上构建.

4.2.1 序列到期可撤销合约

进行交易的双方可以通过向脚本的杂凑地址进行支付的方式[22],将资金注入资金池,并将资金池输出按照注资比例发往各自的地址. 双方只将前一项交易广播至网路,后一项交易签名后相互交换. 当双方需要进行支付时,只需改变资金池的分配方案,并将旧方案作废处理. 只有当决定终止交易时,才会将分配方案最终公布到区块链上. 这样,无论交易双方之间进行过多少次离链交易,都不会对区块链造成更大的负担.

4.2.2 杂凑时间锁定合约

更进一步地,除双方的微支付通道之外,杂凑时间锁定合约使得未建立通道的 2 人,可以通过多个非可信第三方完成支付. 这里额外引入条件支付. 如果 A 和 C 都与 B 建立支付通道,A 可通过这种方法向 C 支付 0.5 BTC:收款方 C 生成一个秘密值 R,并将杂凑值 $H(R)$ 交给 A,A 与 B 建立条件支付,如果 B 能在一段时间内(假设区块高度 100)出示 R,则 A 向 B 支付 0.51 BTC. 同样,B 与 C 建立条件交易,如果 C 能在一定时间内(假设区块高度 80)出示 R,则 B 向 C 支付 0.5 BTC. 由于 R 由 C 生成,因此条件支付显然可以达成. 通过这种方法,也可以像路由寻址的方式一样经过多跳完成支付. 因此,在此过程中,不必信任 B,即可达成交易. 对于 B 而言,输入和输出的差值 0.01 BTC 就是此过程获得的交易费.

如果大量的双向支付通道建立起来,那么陌生的双方通过第三方交易也将变得十分简单.届时,甚至不需要资金重新回到区块链上,所有交易都可以在闪电网络中离链完成.离链交易速度很快,无需等待确认,只要双方完成互换交易即时达成.由此可见,闪电网络的方案可以大幅降低链上的小额支付交易,避免大量的带宽和存储空间占用.但是缺点在于钱包实现相对复杂.传统钱包只需要关注区块链上的交易或向网络发布交易,钱包开发者遵循比特币的规则即可.而闪电网络钱包还需要关注一个离链的网络,钱包需要具有类似于当前路由协议的功能,以找到从发送方到接收方之间的最佳路径.为能够相互兼容,钱包开发者必须建立统一的规则.因此,闪电网络的钱包普及需要时间.只有当大量支付通道建立起之后,闪电网络的效果才能最终展现出来.

2017 年 4 月,德国酒吧 Room77 尝试在比特币测试网络中建立闪电网络,结果表明:转账可在数毫秒之内完成[39].2017 年 5 月,莱特币激活见证隔离后,Blockstream 的 Christian Decker 在莱特币中测试了闪电网络,通道建立之后,从苏黎世向旧金山的转账在 1 s 内完成[40].由此可见,闪电网络在扩容同时,亦可大幅减少交易确认时间.

4.2.3　实现方法分析

为保证公平交易,闪电网络需要先对子交易签名,再对父交易签名.由于交易延展性,当前比特币规则无法支持这种签名顺序.为解决这个问题,闪电网络白皮书中提出一种解决方案.通过软分叉引入 SIGHASH_NOINPUT 操作.与当前的签名方式不同,SIGHASH_NOINPUT 不对输入中的交易 ID 签名.这样,父交易的交易 ID 变化不会破坏子交易中签名的有效性.见证隔离提供另一种解决思路,通过将签名数据转移出输入字段,彻底解决交易延展性的问题.与闪电网络白皮书中提到的方案相比,见证隔离更彻底将上述问题解决,且更具有通用性.因为每一次引入软分叉都意味着系统的复杂度提升,社区更期望能够通过一次软分叉解决尽可能多的问题,所以见证隔离的软分叉相对闪电网络中提到的 SIGHASH_NOINPUT 更容易被社区接受.

见证隔离+闪电网络是比特币核心开发者(Bitcoin Core)大力支持的升级路线图.见证隔离可以在短期内提升区块链容量,解决当前交易延迟的问题.随着闪电网络的成熟,大量交易可以在区块链之外完成,缓解区块链压力.

5　扩容技术分析

本节分析比特币社区对扩容方案的态度.在扩容问题上,社区明显分为 2 派,大矿池为主的一派更倾向于链上扩容,甚至希望彻底取消区块容量上限,交易所和核心开发者为主的一派则更支持链下扩容方案,2 派均为推动扩容方案的实现做出不懈努力.

5.1　社区分歧

对于比特币未来的发展方向,社区有 2 种不同的看法.以 Bitcoin Core 为主的一派认为比特币应该作为结算系统,采用见证隔离+闪电网络的方式,以现有比特币网络为基础,建立第 2 层网络(如闪电网络),大部分交易都在第 2 层网络中完成,底层的比特币网络只为上层网络提供安全保障[41].但是也有人持反对态度,原因是作为结算系统的比特币与中本聪的比特币白皮书的设想走向了完全不同的方向.他们着力于保持比特币现有的特性,使其继续以现金系统的方式运行下去.为达到这个目的,唯一的解决方案就是扩大区块容量上限(或减少区块产生间隔).由于和 Bitcoin Core 理念不同,部分开发者选择放弃 Bitcoin Core 的客户端,独立开发出 Bitcoin Unlimited(BU)客户端.因此,和通过 BIP9 部署的闪电网络不同,支持 BU 方案是通过使用不同客户端的方式达成的.

上述 2 种方案均有一定支持度.结算系统的代表是见证隔离+闪电网络方案,现金系统的代表是 Bitcoin Unlimited 方案.2017 年 4 月,BU 方案支持度略高于见证隔离,二者支持度均在 30%以上[42].

从见证隔离的历史支持度来看,在 BIP141 规定的投票时间开始时,支持见证隔离的区块迅速增多,但是,此后一直保持在 30%左右[43].按照此趋势,见证隔离很难在规定时间内(2017 年 11 月 15 日)通过."用户激活软分叉(UASF)"方案提出,若大多数实体(包括用户、交易所、钱包软件开发者等)同意,节点客户端将强制开启更新.BIP148 中加入规定:从 2017 年 8 月 1 日起,未宣布同意支持新版本的区块将会被其他节点拒绝[44].此方案相当于开发者绕过矿工激活见证隔离.为应对 UASF,比特大陆(bitmain.com)提出"用户激活硬分叉(UAHF)"方案.此方案不包含见证隔离,同时将区块容量上限提升至 8 MB.UAHF 在 UASF 激活 12 h 20 min 后启动[45].上述 2 种方案均不考虑算力支持度,因此极易造成比特币分叉.

相比于矿工对见证隔离支持的犹豫不决,矿工之外的群体中,见证隔离的支持度远高于 BU,在对公司的统计中,见证隔离的支持度(包括确认支持和准备就绪的公司)超过 70%,而 BU 方案仅 20%左右[46]. 这些公司中除矿池之外,还包括比特币交易所、钱包软件开发商等. 由此可见,矿工与交易所对于比特币的发展方向问题存在分歧.

5.2 链上方案扩容风险分析

5.2.1 中心化风险

比特币社区一直对于比特币网络的中心化趋势十分警惕. 中本聪在比特币白皮书中就提到,"如果决定大多数的方式是基于 IP 地址的,一 IP 地址一票,那么如果有人拥有分配大量 IP 地址的权力,则该机制就被破坏. 而工作量证明机制的本质则是一 CPU 一票[1]."在最初的设计中,比特币节点可以运行在个人计算机上. 由于运行门槛极低,所有人都可以作为矿工运行节点. 这一点保证主链的投票权分散在用户手中.

社区担心,支持 BU 的团体取消区块容量上限的方案会增大中心化风险. 较大的区块需要更好的网络条件进行传输、更大的硬盘空间用于存储,这会提高全节点的运行门槛. 如果比特币平均交易大小保持不变,即 490 B,全网交易速率达到 visa 的当前平均水平 2 000 交易/秒[7],则平均区块大小将超过 500 MB,远远超过 3.3 节中网络的承载力. 另外,网络每月产生的数据量高达 85 GB,每年产生数据量超过 1 TB,造成很大的存储负担. 不断增高的带宽和存储成本对小矿工而言是致命的,但是对于大型公司而言是可以接受的. 在此情况下,大量的小矿工将被迫退出,比特币的去中心化特性将被削弱.

因此,对于大小不受限制的区块,社区持怀疑态度. 比特币难以作为去中心化现金系统持续运行.

5.2.2 攻击风险

实施链上扩容的方案之后,会导致区块传播延迟的增长,从而降低部分攻击的难度. 下面分析常见攻击方式与链上扩容的关系.

1) 双花攻击(double spending). 链上扩容后,零确认双花攻击难度不会改变,N 确认双花攻击难度会下降.

零确认双花与区块传播关系不大. 在需要快速交易且交易金额不大的情况下,收款方会在收到网络上广播的交易后即认为收款成功,此时交易还未进入区块链. 恶意付款者可以在付款后,网络上广播另一项同输入的交易,输出指向自己控制的地址,两交易互斥,但均有机会进入区块链. 若最终后者入块,则恶意付款者获利[23]. 此攻击方式与交易在比特币网络中传播延迟相关,链上扩容对此影响不大.

N 确认双花是指攻击者在 N 个区块确认之后,通过改变主链走向,达到撤回某项交易的目的. 当攻击者拥有算力超过全网 50%时,即可使用此攻击方式. 3.2 节指出:更大的区块会导致区块传播延迟增加,自然分叉有可能出现,从而造成有效算力的减少. 这使比特币网络的安全性降低,攻击者可以利用更少的算力制造超过主链长度的分支,从而改变主链走向[28].

2) 自私挖矿(selfish mining). 链上扩容会使得比特币更容易受到自私挖矿影响.

文献[47]提出,当算力达到一定水平之后,矿工可以通过暂时隐瞒挖到区块的方式获利. 获利情况由矿工算力占比 α 和追随者占比 γ(即诚实结点和攻击者分别生成的 2 个合法区块同时广播时,诚实节点支持攻击者的比例)决定. 在不考虑延迟,且 $\gamma=50\%$ 的情况下,α 达到 25%的矿工即可通过自私挖矿获利. 当区块传播延迟不可忽略时,虽然自私矿工 γ 可能降低,但是由于 3.2 节提到的全网算力损失,自私矿工 α 有所上升. 由于自然分叉的存在,自私挖矿的获利阈值可能比 25%更低[48].

3) 日蚀攻击(eclipse attack)等传播阻断. 这类攻击的难度不会因链上扩容的实施而下降.

通过分割比特币网络,使得部分节点数据的更新晚于其他节点,这种作法可以协助实施某些攻击(如零确认双花). 在网络层面阻断数据传播[49],或利用比特币协议中对比特币区块和交易广播过程中的声誉管理系统、基于广告的请求管理系统和超时规定等措施的缺陷[50],均可达到此目的. 如果仅仅实行链上扩容,而不改动比特币协议的其他部分,那么这类攻击的难度不会下降.

5.3 链下方案短期效果分析

虽然见证隔离理论上可以等效提高区块容量上限,但是达到理论的效果需要一段过渡时间. 根据 3.1 节的计算,基于当前的交易比例,见证隔离技术可以使区块多容纳 83%的交易数量,即相当于通过软分叉将区块容量最多提升至 1.83 MB. 利用 2.3 节使用的方法,计算出待确认交易内存池平均大小为 479 665 B,可以解决当下的区块链容量不足的难题. 但是,花费旧版本的交易时,输入中依然需要使用包含签名的旧格式 scriptSig,无法节约空间. 见证隔离部署之后的时间点上,用户持有的货币依然保存在

旧版本的交易中,因此扩容的效果不会在短时间内立即显现.

6 结　　论

本文对比特币网络当前状态进行详细分析,结果显示:2017 年初,有 16%的交易需要 1 h 以上的时间进行确认,等待确认的交易内存池大小一度超过 110 MB. 对链上扩容的分析指出,不改变区块间隔前提下,单个区块大小不应超过 4 MB,否则会超出当前网络负载能力,导致孤块率上升等问题. 另外,单个区块大小增大至 2 MB 可以缓解当前交易延迟的问题.

对于链下扩容方案的分析发现,见证隔离技术具有增大区块容量的效果. 基于当前交易数据计算得出的结论是,见证隔离可以将区块容量增大 83%. 更重要的是,见证隔离技术可以解决当前的交易延展性问题,从而为闪电网络等基于比特币的第 2 层网络搭建铺平道路. 一旦闪电网络搭建完成,可以极大减轻区块链负担,增大比特币系统对交易的处理能力,减少交易确认等待时间.

比特币扩容问题的关键在于社区对当前扩容方案的认同度. 比特币扩容技术无法部署的主要原因在于社区意见的不统一. 链上扩容方案见效快,但是增大中心化风险,适合作为短期方案使用. 链上扩容方案虽然能极大提升容量,但是见效慢,适合作为长期扩容方案. 重要的是 2 种方案从技术上分析并不是互斥的.

一种合理的路线图是将区块容量上限提高至 2 MB(引入见证隔离后的区块实际大小保持在 4 MB 以下,符合 3.3 节分析),缓解当下交易大量延迟问题. 同时引入见证隔离,开始部署闪电网络,逐渐将小额交易移到链外,减少区块链的容量负担,达成长期平稳运行目标.

比特币区块链扩容技术已经准备就绪,一旦社区达成一致,相应技术即可部署应用. 我们很高兴地看到,社区正在持续努力实现这个目标. 最新的进展是 2017 年 5 月 23 日分布于 21 个国家的 56 家公司就比特币扩容问题达成共识,其中包括蚁池等大型矿池以及 Coinbase 等比特币交易所,这个群体占有全网 83.28%的比特币算力. 达成的共识包括:以 80%阈值激活见证隔离,以 bit4 为信号;在 6 个月内激活 2 MB 区块硬分叉[51]. 此共识通过 SegWit2x 扩容方案实施(硬分叉激活时间变为见证隔离激活后 3 个月). BIP91 规定,若 336 个区块中 80%以上包含 bit4 信号则可激活,确认期后,矿工将拒绝所有未包含 bit1 信号的区块[52],以此实现了 SegWit2x 与 BIP141 的兼容. 根据 Coin Dance 的统计,SegWit2x 算力支持度在 2017 年 7 月已超过 80%[53]. BIP91 已于 7 月 23 日正式生效,矿池拒绝不支持见证隔离的区块,如果见证隔离支持度达到 95%而且持续 2016 个区块,则见证隔离被锁定,再经过 2016 个区块,见证隔离将在 8 月完成激活[54]. 根据本文的计算,如果各方能够执行协议,那么现阶段比特币扩容问题将被很好地解决.

后记:本文审稿完成后,比特币扩容又发生新的进展. SegWit2x 的成功激活避免了 2017 年 8 月 1 日激活 UASF 可能产生的分叉[54],但是作为应对 UASF 可能分叉的 UAHF,却由于 Bitcoin Cash 在 2017-08-01 20:20 开始生成新的区块,进而产生新的竞争币 Bitcoin Cash (BCC)[55].

参　考　文　献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [OL]. (2008-10-31) [2016-11-02]. https://bitcoin.org/bitcoin.pdf

[2] Qin Bo, Chenli C, Wu Qianhong, et al. Bitcoin and digital fiat currency [J]. Journal of Cryptologic Research, 2017, 4(2): 176-186 (in Chinese)
(秦波, 陈李昌豪, 伍前红, 等. 比特币与法定数字货币[J]. 密码学报, 2017, 4(2): 176-186)

[3] Blockchain Luxembourg S A. Average Block Size [OL]. [2017-01-05]. https://blockchain.info/en/charts/avg-block-size

[4] Pappalardo G, Di Matteo T, Caldarelli G, et al. Blockchain inefficiency in the Bitcoin peers network [DB/OL]. [2017-06-01]. https://arxiv.org/pdf/1704.01414.pdf

[5] Bonneau J, Miller A, Clark J, et al. Sok: Research perspectives and challenges for Bitcoin and cryptocurrencies [C] //Proc of the 36th IEEE Symp on Security and Privacy (SP 2015). Piscataway, NJ: IEEE, 2015: 104-121

[6] Sompolinsky Y, Zohar A. Accelerating Bitcoin's transaction processing, fast money grows on trees, not chains [DB/OL]. [2017-03-05]. https://eprint.iacr.org/2013/881.pdf

[7] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains [G] //LNCS 9604: Proc of the 20th Int Conf on Financial Cryptography and Data Security (FC 2016). Berlin: Springer, 2016: 106-125

[8] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains [C] //Proc of the 2016 ACM SIGSAC Conf on Computer and Communications Security (CCS 2016). New York: ACM, 2016: 3-16

[9] Andresen G. BIP101: Increase maximum block size [OL]. [2017-06-01]. https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

[10] Garzik J. BIP102: Block size increase to 2 MB [OL]. [2017-06-01]. https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki

[11] Wuille P. BIP103: Block size following technological growth [OL]. [2017-06-01]. https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki

[12] Andresen G. BIP109: Two million byte size limit with sigop and sighash limits [OL]. [2017-06-01]. https://github.com/bitcoin/bips/blob/master/bip-0109.mediawiki

[13] Lombrozo E, Lau J, Wuille P. BIP141: Segregated Witness (Consensus layer) [OL]. [2016-11-15]. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[14] Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments [OL]. [2016-12-17]. https://lightning.network/lightning-network-paper.pdf

[15] Decker C, Wattenhofer R. A fast and scalable payment network with Bitcoin duplex micropayment channels [G] //LNCS 9212: Symp on Self-Stabilizing Systems (SSS 2015). Berlin: Springer, 2015: 3-18

[16] Miller A, Bentov I, Kumaresan R, et al. Sprites: Payment channels that go faster than lightning [DB/OL]. [2017-05-06]. https://arxiv.org/pdf/1702.05812

[17] Lind J, Eyal I, Pietzuch P, et al. Teechan: Payment channels using trusted execution environments [DB/OL]. [2017-05-20]. https://arxiv.org/pdf/1612.07766

[18] Higgins S. IC3 Debuts Upgraded Off-Chain Transaction Protocol "Teechain" [OL]. [2017-05-07]. http://www.coindesk.com/ic3-debuts-upgraded-off-chain-transaction-protocol-teechain/

[19] Narayanan A, Bonneau J, Felten E. Bitcoin and Cryptocurrency Technologies [M]. Princeton: Princeton University Press, 2016

[20] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies [J]. IEEE Communications Surveys & Tutorials, 2015, 18(3): 2084-2123

[21] Theymos. Bitcoin wiki: Script [OL]. [2017-05-05]. https://en.bitcoin.it/wiki/Script

[22] Andresen G. BIP16: Pay to Script Hash [OL]. [2016-11-14]. https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki

[23] Karame G O, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin [C] //Proc of the 19th ACM Conf on Computer and Communications Security. New York: ACM, 2012: 906-917

[24] Sanders G, Harding D A. Bitcoin Developer Reference [OL]. [2017-05-05]. https://bitcoin.org/en/developer-reference#block-chain

[25] Bitcoin Unlimited Organization. Bitcoin Unlimited: Articles of Federation [OL]. [2017-04-20]. https://www.bitcoinunlimited.info/resources/BUarticles.pdf

[26] Decker C, Wattenhofer R. Information propagation in the Bitcoin network [C] //Proc of the 13th IEEE Int Conf on Peer-to-Peer Computing (P2P). Piscataway, NJ: IEEE, 2013: 1-10

[27] Karpelès M. Bitcoin Protocol Documentation [OL]. [2017-05-15]. https://en.bitcoin.it/wiki/Protocol_documentation

[28] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in Bitcoin [G] //LNCS 8975: Proc of the 19th Int Conf on Financial Cryptography and Data Security. Berlin: Springer, 2015: 507-527

[29] Wirdum V A. Ethereum Classic Community Navigates a Distinct Path to the Future [OL]. [2017-02-15]. https://bitcoinmagazine.com/articles/ethereum-classic-community-navi gates-a-distinct-path-to-the-future-1471620464/

[30] Lau J. BIP142: Address format for segregated witness [OL]. [2016-11-15]. https://github.com/bitcoin/bips/blob/master/bip-0142.mediawiki

[31] Lau J, Wuille P. BIP143: Transaction signature verification for version 0 witness program [OL]. [2016-11-15]. https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki

[32] Lombrozo E, Wuille P. BIP144: Segregated witness (peer services) [OL]. [2016-11-16]. https://github.com/bitcoin/bips/blob/master/bip-0144.mediawiki

[33] Andrychowicz M, Dziembowski S, Malinowski D, et al. How to deal with malleability of Bitcoin transactions [DB/OL]. [2016-12-03]. https://arxiv.org/pdf/1312.3230

[34] Decker C, Wattenhofer R. Bitcoin transaction malleability and MtGox [G] //LNCS 8713: Proc of European Symp on Research in Computer Security (ESOCRIS 2014). Berlin: Springer, 2014: 313-326

[35] Andrychowicz M, Dziembowski S, Malinowski D, et al. On the malleability of Bitcoin transactions [G] //LNCS 8976: Proc of the 19th Int Conf on Financial Cryptography and Data Security (FC 2015). Berlin: Springer, 2015: 1-18

[36] Wuille P. BIP62: Dealing with malleability [OL]. [2017-02-05]. https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki

[37] Sanders G, Harding D A. Bitcoin Developer Guide [OL]. [2017-05-18]. https://bitcoin.org/en/developer-guide#term-null-data

[38] Wuille P, Todd P, Maxwell G, et al. Version bits with timeout and delay [OL]. [2016-11-16]. https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki

[39] Helms K. Lightning Network Used to Sell Beer at Room77 [OL]. [2017-04-10]. https://news.bitcoin.com/lightning-network-beer-room77/

[40] Russell R. Major Milestone: The First Lightning Payment on Litecoin pays from Zurich to San Francisco [OL]. [2017-05-23]. https://blockstream.com/2017/05/11/lightning-on-litecoin.html

[41] Tremback J, Hess Z. Universal payment channels [OL]. [2016-12-20]. http://jtremback.github.io/universal-payment-channels/universal-payment-channels.pdf

[42] Coin Dance. Bitcoin Block Details [OL]. [2017-04-07]. https://coin.dance/blocks

[43] Blockchain Luxembourg S A. Percentage of blocks signalling SegWit support [OL]. [2017-04-04]. https://blockchain.info/charts/bip-9-segwit

[44] Fry S. Mandatory activation of segwit deployment [OL]. [2017-04-05]. https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki

[45] Bitmain Technologies. UAHF: A contingency plan against UASF (BIP148) [OL]. [2017-07-28]. https://blog.bitmain.com/en/uahf-contingency-plan-uasf-bip148/

[46] Coin Dance. Global Bitcoin Political Support & Public Opinion [OL]. [2017-04-07]. https://coin.dance/poli

[47] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable [J]. Computer Science, 2013, 8437: 436-454

[48] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin [G] //LNCS 9603: Proc of the 20th Int Conf on Financial Cryptography and Data Security. Berlin, Springer, 2016: 515-532

[49] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on Bitcoin's peer-to-peer network [C] //Proc of the 24th USENIX Conf on Security Symp. Berkeley, CA: USENIX Association, 2015: 129-144

[50] Gervais A, Ritzdorf H, Karame G O, et al. Tampering with the delivery of blocks and transactions in Bitcoin [C] //Proc of 2015 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2015: 692-705

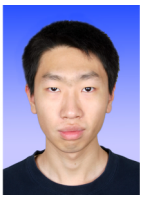
[51] Digital Currency Group. Bitcoin Scaling Agreement at Consensus 2017 [OL]. [2017-05-24]. https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77

[52] Hilliard J. BIP91: Reduced threshold Segwit MASF [OL]. [2017-07-21]. https://github.com/bitcoin/bips/blob/master/bip-0091.mediawiki

[53] Blockchain Luxembourg S A. Percentage of blocks signalling support for the New York agreement [OL]. [2017-07-22]. https://blockchain.info/charts/nya-support

[54] Rizzo P. What's Left Before SegWit Goes Live? Bitcoin's Path to More Capacity [OL]. [2017-07-25]. https://www.coindesk.com/whats-left-before-segwit-goes-live-bitcoins-path-more-capacity/

[55] Séchet A. Bitcoin Cash [OL]. [2017-08-02]. https://www.bitcoincash.org/



Yu Hui, born in 1994. Bachelor. Student member of CCF. His main research interests include cryptography, blockchain, and smart contract.

Zhang Zongyang, born in 1984. PhD, assistant professor, master supervisor. His main research interests include cryptography and blockchain.

Liu Jianwei, born in 1964. PhD, professor, PhD supervisor. His main research interests include network security and cyberspace security (liujianwei@buaa.edu.cn).