计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180440
55(10):2099-2110,2018

区块链可扩展性研究:问题与方法

潘 晨 刘志强 刘 振 龙 宇
(上海交通大学计算机科学与工程系 上海 200240)
(zpc48@sjtu.edu.cn)

Research on Scalability of Blockchain Technology: Problems and Methods

Pan Chen, Liu Zhiqiang, Liu Zhen, and Long Yu
(*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)

Abstract As one of the key technologies of distributed ledgers, blockchain solves the trust problem in open network without relying on any trusted third party. Its decentralized feature makes it potential for a wide range of application scenarios. However, it still faces scalability problems. The bottleneck of blockchain scalability is mainly in two aspects: low efficiency and difficulty in functional extension. For instance, Bitcoin can only deal with 7 transactions per second averagely. Obviously, it cannot meet the requirement of current digital payment scenarios, nor can it be carried in other applications such as distributed storage and credit investigation service. On the other hand, the data or assets within different blockchains are difficult to interact with each other. This restricts the functional extension of blockchain system. In reality, there are a variety of blockchain systems which are specially devised for various functionalities or applications. Therefore, it is crucial to establish interaction channels among different blockchains to make them form the Internet of value. So far the research of blockchain scalability has attracted much attention from both academia and industry due to its importance. This paper introduces and analyzes the blockchain scalability related technologies from the aspects of improving efficiency and extending functionality of blockchain system, respectively. Firstly, we introduce three major schemes for performance enhancement of blockchain, including off-chain payment network, Bitcoin-NG and sharding mechanism; and four typical cross-chain approaches for blockchain functionality extension. Then we analyze the merits and demerits of each technology, based on which we give the challenges and suggestions for further research in blockchain scalability.

Key words blockchain; scalability; off-chain payment channel; Bitcoin-NG; sharding; cross-chain

摘 要 区块链技术作为分布式账本的关键技术之一,其在不依赖于任何第三方可信机构的前提下,解决开放网络中的信任问题,去中心化的特点使其有着广泛的应用前景,但面临着可扩展性不足的瓶颈.目前,区块链可扩展性的瓶颈主要体现在2个方面:性能效率低下、功能难以扩展.以比特币为例,从性能上讲,当前仅支持7笔/秒的交易吞吐量,显然无法满足现今数字支付的场景,也无法承载在数字支付领域外的其他应用.从功能上讲,当前不同区块链系统之间的资产或数据难以交互.在现实情况中,不同的区块链系统承载着不同的业务和需求.为此,需要实现链与链之间的交互,才能打通不同区块链之间的信息或价值通道,避免每一区块链成为信息或价值孤岛,并在此基础上实现价值互联网.区块链

收稿日期:2018-06-11;**修回日期**:2018-08-06
基金项目:国家自然科学基金项目(61672347,61672339,61572318)
This work was supported by the National Natural Science Foundation of China (61672347, 61672339, 61572318).
通信作者:刘志强(ilu_zq@sjtu.edu.cn)

可扩展性的研究已经引起了学术界及产业界越来越多的关注,将从区块链性能提升及功能扩展2个角度出发,分别介绍区块链可扩展性领域的相关技术和研究进展,其中包括3类当前主流的、提升区块链交易吞吐量的方案:链下支付网络、Bitcoin-NG和分片机制;以及4类代表性的、实现区块链功能扩展的跨链互通技术.分析对比不同方案的特性、适合场景及可能存在的不足之处,并在此基础上给出进一步研究方向.

关键词 区块链;可扩展性;链下支付通道;Bitcoin-NG;分片机制;跨链技术

中图法分类号 TP393

区块链技术起源于中本聪[1]提出的比特币系统,其真正在开放式的P2P网络中实现了不依赖于可信第三方的数字支付系统.这种去中心化的特性大大有别于现有的商业支付系统,改变了现有系统中的安全信任模型.在比特币的信任模型中,用户之间的信任源于对整个系统的信任,而不是任何第三方中介,只要整个系统的安全假设被满足,这种信任关系就可以持续.去中心化的特性使得区块链技术受到了越来越多的关注,有着广阔的应用前景.

然而当前的区块链系统存在严重的可扩展性瓶颈:

1) 交易吞吐量不足.以比特币系统为例,当前系统最高只能支持7笔/秒的交易确认(以区块大小为1 MB为例)[2],这使得其难以承担大量交易的及时确认,无法满足现实的应用需求.同时由于其共识过程中可能存在分叉,一笔交易至少需要6个区块的确认(这是推荐的确认数),即至少需要等待1 h才能确认单笔交易,这些都限制了其大规模的应用[3];

2) 链与链之间的资产(数据)难以交互.不同的应用场景有着不同的用户和需求,因此在现实情况中,很难要求一个区块链系统来承载整个现实生活中的所有应用.为此需要实现链与链之间的交互,才能使得区块链之间不会彼此成为孤岛,从而实现真正的价值互联.

本文阐述当前区块链可扩展性问题的现状,从区块链提升性能和功能扩展2个方面,综述当前主流的解决区块链可扩展性的技术:链下支付网络、Bitcoin-NG、分片机制和跨链技术,分析比较它们的优缺点,并指出现有方案所面临的主要问题和未来研究方向.

1 概 述

区块链技术提供了在开放网络中新的信任模型,使得任何用户可以在不需要第三方信任机构的情况下建立信任关系,这样的信任关系源于用户对整个系统的信任,而无需信任单个节点.

这样的去中心化特性带来的代价之一就是区块链的性能,主要的指标就是系统的交易吞吐量.当前比特币系统只能支持最高7笔/秒的交易吞吐量,而主流的支付平台如Visa,能够实现平均2000笔/秒,以及峰值56 000笔/秒的交易处理速度[4],显然两者之间存在着巨大的差异.

这主要是由于比特币系统的共识机制所带来的代价.在传统的数字支付平台中,往往存在着中心化的第三方机构来完成交易的确认,系统中的其他节点无条件信任第三方机构的执行结果.而在以比特币为代表的数字货币系统中,需要全网的节点来对系统中的每一笔交易进行共识,每个节点都拥有各自的账本并且通过共识机制来完成对账本的修改并保证一致性.在当前区块链的共识机制中,无论是工作量证明机制(proof of work, PoW)还是权益证明机制(proof of stake, PoS)本质上都是全网节点参与并竞争账本的记账权,并且保证了系统中的任何节点能够独占记账权并进行双花攻击的代价极高或者攻击成功的可能性极低.每轮拥有记账权的用户以区块的形式确认交易,这样的共识机制和区块大小的限制使得每轮共识的交易确认数有限,造成了区块链系统交易吞吐量的瓶颈.

显然增大区块容量是一个能够提升区块链交易吞吐量的简单办法[5-6].更大的区块能够使得一轮的共识过程中确认更多的交易.然而仅仅提高区块大小并不能完全解决问题.首先是更大的区块可能会导致网络的拥塞,影响系统的性能,其次以比特币为例,即使将当前的区块大小提升到8 MB,系统的交易吞吐量依然小于100笔/秒,依旧无法满足现实的业务需求.

当前针对区块链性能提升的主流方案主要包含3类:

1) 利用支付通道技术,通过链下交易的方式来提升交易的吞吐量,同时保证交易的安全性;

2) Bitcoin-NG[7]等方案,将原先比特币中的共识过程拆分成记账人选取和交易排序2个阶段,通过记账人选取阶段保证区块链安全性,在交易排序阶段由记账人进行大量交易数据的处理.其在保证了分布式一致性的基础上,提升了一轮共识过程中的交易确认数,从而在区块链上增加交易吞吐量;

3) 分片机制,通过将全网节点划分成不同的集合(shard),每个集合并行地进行共识,确认交易,从而使得系统的交易吞吐量随着全网中参与共识节点的增加而近似线性地增加.

区块链的可扩展性问题除了表现在性能上,即系统的交易吞吐量外,在功能上也同样存在瓶颈.区块链技术诞生之初,主要是为了实现去中心化的数字支付系统,然而随着人们对区块链的理解和技术的发展,出现了各种区块链项目,他们有着不同的特性,能够满足不同的业务需求.在数字支付领域,有ETH[8]基于账户模型实现了图灵完备的智能合约,Zcash[9]利用零知识证明技术实现了交易过程中的隐私保护等.利用区块链去中心化的特性,也可以实现除数字支付以外的应用[10],如分布式文件存储、征信、供应链及金融应用等.然而在区块链设计之初很少考虑到不同的链之间交互的需求,这使得不同的链之间完全割裂,不同的资产无法相互转换,不同的应用无法相互协同,从而无法实现真正的价值互联.为此,需构建跨链技术来解决链与链之间的交互问题.

当前代表性跨链技术主要包含4类:

1) 公证人技术;

2) 侧链/中继技术;

3) 基于Hash锁定技术;

4) 分布式密钥控制技术.

其中公证人技术引入了可信第三方,作为跨链过程中的资产保管人,侧链/中继技术利用SPV(simplified payment verification)证明、中继链等技术,实现了不同区块链之间的可信互通,基于Hash锁定利用了Hash原像脚本,实现了公平的跨链资产交换,分布式密钥控制技术利用分布式密钥生成算法,使得跨链过程中的资产保管人角色由全网节点承担,而不是少数第三方.

2　性能扩展的主流技术

在本节中,我们主要介绍3类提升区块链性能的主流技术,包括链下支付网络技术,涉及经典闪电网络及其相关改进方案的构造;提升链上交易容量的Bitcoin-NG方案;提升链上交易容量的分片机制.

2.1　链下支付网络

链下支付网络通过将大量交易离线处理,同时将区块链作为仲裁平台,处理通道支付过程中的异常情况,如双方对通道的状态有分歧等,其间接地提升了系统的交易吞吐量.

双向通道支付过程可分为3个阶段:1)初始阶段,用于双方建立通道;2)支付阶段,通道双方完成支付,即通道状态的更新;3)关闭通道阶段,双方关闭通道,赎回通道中自己的资金,在关闭通道过程中,一旦某一方作恶,即利用之前的通道状态来谋利,将会触发提交阶段.在提交阶段中,双方提交证据(交易)使得外界(区块链)确定通道内的真实状态.

2.1.1　闪电网络

闪电网络[11]是最早的通过链下支付通道形成支付网络、提升区块链交易吞吐量的方案.闪电网络主要包含2个协议RSMC(recoverable sequence maturity contract)和HTLC(hashed timelock contract)[12].其相关其他方案主要是在2个协议上进行修改.RSMC主要实现了双人双向的支付通道,使得通道双方可以在交易不上链的情况下即时确认交易.HTLC则实现了系统内任意2个节点的转账可以通过一条支付通道来实现.通过这样的方式,只要在系统中存在一条Alice到Bob之间的通路,Alice就可以借用他人的通道来实现支付操作,无需直接与Bob建立通道.跨通道支付协议是基于条件支付的想法,即接收者必须满足一定的条件才能接受到钱款.在该协议中,条件支付的构造基于Hash原象,从而来同步支付路径上所有用户的支付情况[13].类似的条件支付在其他方案中也广泛存在[14-15].

Spilman[16]首次提出了基于比特币系统的通道支付协议.该协议包含2个阶段,初始阶段和支付阶段.初始阶段Alice首先向一个智能合约的脚本地址中进行充值,这个智能合约就是Alice和Bob的多签名脚本,只有在2人共同对交易签名时,才能从该脚本地址将钱转出.这样的支付通道建立后,双方就可以在交易不上链的情况下即时确认交易.具体的过程:以Alice向Bob支付为例,Bob将包含此次支付后通道中金额的分配情况的交易发送给Alice,Alice确认金额后签名并将其发送给Bob,Bob收到该交易后即确认这个支付操作的完成.当Bob想要

关闭支付通道时,只需在最新的由 Alice 签名的交易中附上自己的签名后在系统中广播,矿工确认这笔交易并上链后,该支付通道即为关闭.通道支付协议实现了交易的即时确认.这个通道支付协议的特点是在通道的支付过程中属于 Bob 的金额始终是增长的,这保证了 Bob 只会向区块链公布通道内的最新状态,不然 Bob 就会受到损失.但是这样的特点使得通道支付协议存在局限性,即该通道支付协议只支持单向的支付,只满足单一的用户向商家支付的场景.

然而当支付通道协议要支持双向支付时,需要一种机制来保证通道双方始终公布通道内的最新状态,闪电网络中的 RSMC 实现了这个机制.

主要原理.通过时间锁(timelock)[17]的机制来延迟通道一方取回通道资产的时间,同时引入惩罚交易的概念来保证通道双方的资产状态是基于最新的交易情况,一旦某一方试图使用之前的通道状态来谋利,另一方可以在这段延迟时间内(timelock)发现,并没收其通道内资产作为惩罚.

如图 1 所示,每一轮通道状态更新需要通道双方更新 Commitment 交易以及上一轮 Commitment 交易所对应的惩罚交易.

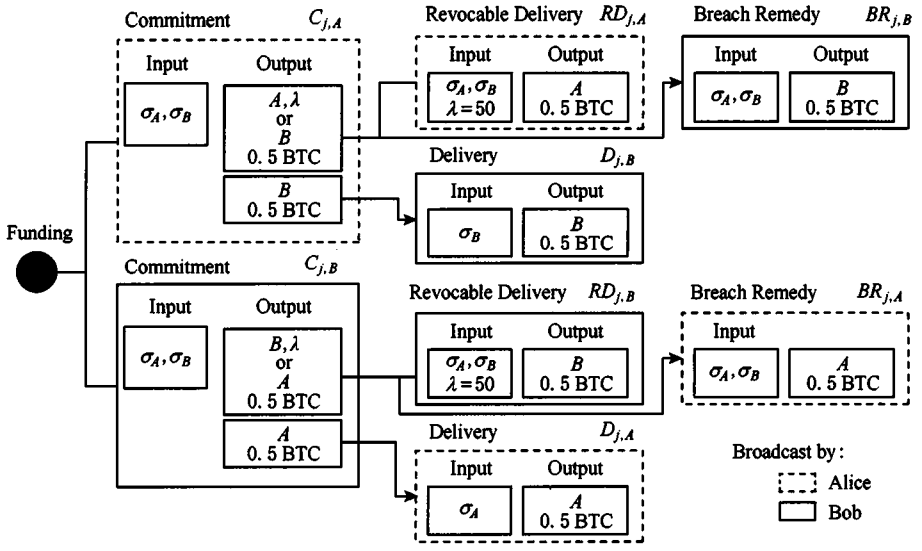

Fig. 1 The transaction structure of lightning payment channel

图 1 闪电网络双向支付通道结构

1) 初始阶段.通道双方 A,B 生成未签名的 funding 交易,将各自的押金存入通道中,funding 交易引用 A 与 B 的输出.A,B 生成初始的 commitment 交易 $C_{1,A},C_{1,B}$,确定通道内的初始状态,并且交换对双方 commitment 交易的签名 σ_A,σ_B.之后 A,B 双方交互对 funding 交易的签名,并将交易广播到区块链中.

2) 支付阶段.支付过程相当于通道状态的更新,即产生新的 commitment 交易 $C_{j,A},C_{j,B}$.此时通道内上一轮状态交易 $C_{j-1,A},C_{j-1,B}$ 和新产生的状态交易 $C_{j,A},C_{j,B}$ 同时处于有效状态,因此需要额外交互惩罚交易来作废上一轮的状态交易 $C_{j-1,A}$,$C_{j-1,B}$.以 A 为例,A 拥有状态更新交易 $C_{j,A}$,包含 2 笔输出:输出 1 是 A 在通道内的资金,输出 2 是 B 在通道内的资金.正常情况下输出 1 的花费交易 $RD_{j,A}$ 设置了时间锁 λ,即需要等待 $C_{j,A}$ 经过 λ 区块确认后,该交易才能上链.在惩罚交易的机制中,为了防止 A 公布上一轮的状态交易 $C_{j-1,A}$,A 需要向 B 交互 $BR_{j-1,B}$,并签名 σ_A,该交易没有时间锁,可以在 $C_{j-1,A}$ 上链后立即上链确认.一旦 A 公布 $C_{j-1,A}$ 进行作恶,B 立刻公布 $BR_{j-1,B}$,将 $C_{j-1,A}$ 的输出 1 作为罚金输入到自己的地址中.

3) 结束阶段.关闭通道需要通道双方公布最新的通道状态信息 $C_{j,A}$ 或者 $C_{j,B}$.

HTLC 用于跨通道支付,实现了多个支付通道间资产的公平交换.其利用的是条件支付,即支付成功的条件为收款者给出秘密(Hash 的原像).在不同的通道间可以利用这个秘密完成跨通道的支付,保证了支付的原子性,即不同通道同时支付成功或者同时失败.

如图 2 所示,假设 Alice 需要向 Dave 完成支付,Alice 并没有直接和 Dave 建立的通道,但是 Alice 找到一条支付通路,即 Alice, Bob, Caroline, Dave,使得 Alice 可以通过向 Bob 支付,Bob 向 Caroline

支付,Caroline 向 Dave 支付的方式完成支付. 协议可以分为 2 个阶段:第 1 阶段 Dave 随机生成原像 R,并且将 Hash 值 $H(R)$ 发送给 Alice,Alice 与 Bob 依此建立条件支付合约,通路上的其他节点以此类推. 第 2 阶段,当通路上所有通道都建立条件支付合约后,Dave 通过出示 Hash 原像 R,完成与 Caroline 的支付,Caroline 获得原像 R 后,能够完成与 Bob 的支付,以此类推,最终 Alice 与 Bob 完成支付后整个流程结束.

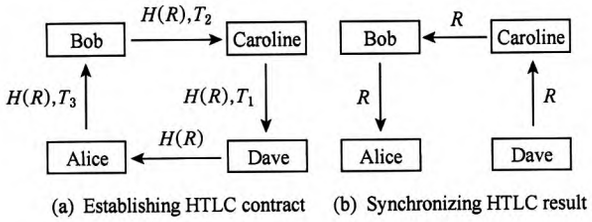

Fig. 2　The process of cross channel payment

图 2　跨通道支付流程

2.1.2　相关改进方案

针对闪电网络的改进主要包含效率、支付成本、通信开销、可持久化、寻路算法等.

1) Duplex payment channel

Duplex[18] 支付通道协议利用了比特币系统中的时间锁机制设计了 Invalidation Tree 的结构,来保证通道的可持久性. 同时利用 2 条单向通道,来实现 A,B 之间的双向支付.

如图 3 所示,A 与 B 之间有 2 条单向支付通道,用于完成 A,B 间的相互支付. 不同于闪电网络需要设计惩罚机制来保证结束通道时,双方公开最新的通道状态,Duplex 利用了单向通道支付方向单一的特点,保证了分别作为 2 条通道的收款者 A,B 只会公开各自收款通道的最新状态. 由于 2 条通道的金额互不联通,在高频交易的场景下,2 条通道中付款者的押金将会很快被耗尽. 因此,利用 Invalidation 树和时间锁机制设计了 reset 阶段,使得 2 条通道内的资金可以相互转移.

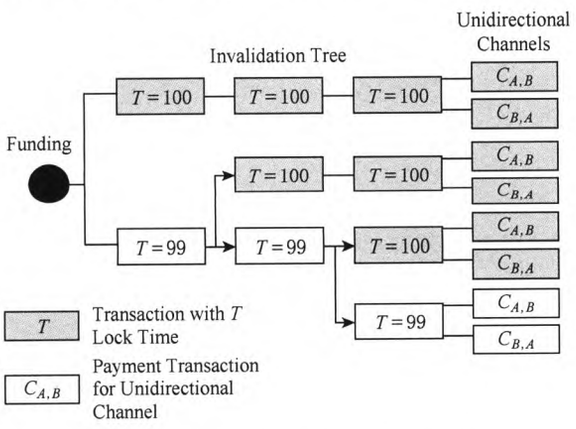

Fig. 3　The structure of invalidation tree

图 3　Duplex 通道支付协议结构

在 reset 阶段中,通道双方基于 2 条通道内共同的资金分配情况,调整 2 条单向通道的状态,如 A 在通道中 C_{AB} 作为付款者,在 C_{BA} 中作为收款者,通过 reset 阶段,A 可以将自己在 C_{BA} 中收到的资金转入 C_{AB} 中用作之后的支付. 为了作废原先的状态,新的交易设置较小的时间锁,使得新的状态更新交易进入区块链. 每进行一轮 reset 将会使新的记录通道状态的交易上的时间锁递减.

支付阶段和提交阶段与传统的单向通道支付协议类似,区别在于 Duplex 在结束通道时需要同时公开 2 条通道内的状态.

2) Raiden network

在闪电网络方案中存在着效率及可用性不足的缺陷. 在其双向支付通道协议中,受制于比特币系统脚本的限制,为了防止通道某一方作恶,另一方需要存储对方在之前的每一轮交互的惩罚交易,而伴随着高频交易持续的发生,存储这些交易的代价将会越来越大,给用户带来极大的负担. 而在跨支付通道协议中,在当前比特币系统中也仅支持基于 Hash 原象的构造,无法支持其他更灵活的条件.

这些问题在以太坊的方案中得到了解决. 由于以太坊实现了图灵完备的脚本系统,可以实现更为灵活的智能合约. 因此基于以太坊模型设计的 Raiden[19] 网络尽管借鉴了上述闪电网络的构造,却并不存在上述问题. 在 Raiden 网络中,通道支付的惩罚交易是基于用户双方对交易轮数 i 的签名,只要一方出示了双方对更高交易轮数 i 的交易的签名,即可判定另一方作恶[20].

3) Sprites

Miller 等人[21] 提出了 Sprites 的方案,是针对闪电网络方案效率方面的改进,目的是解决当跨通道支付不成功时,用户所消耗的时间成本过大的问题. 显然,通道支付协议可以看作一种储蓄卡机制,用户可以通过通道内储蓄的金额,来为他人提供跨通道支付,跨通道支付的手续费即用户提供跨通道支付的激励,类似储蓄卡的利息. 然而用户在跨通道支付的过程中,用于支付的资金是处于冻结状态,直到跨通道支付成功或者失败. 在该过程中用户无法使用被冻结的资金,因此用户在跨通道支付时所付出的成本可以用支付过程中被冻结的资金和所冻结的时间的乘积来衡量.

在原先的跨通道支付协议中,为了保证安全性,在通路上的所有用户获知 Hash 原象,从而完成支付的行为是串行的,因此在最坏情况下,支付路径上最后的用户需要等待支付路径的跳数(L)乘以每一跳交互的最长时延(t)的时间才能确认交易是否成功完成,而在这期间内他的资金处于冻结状态,而在 Sprites 的方案中,利用以太坊平台所提供的智能合约,设计了全局的 Hash 原像管理合约(preimage manage contract),从而使得用户可以通过调用该合约的状态,近似并行地获知交易是否成功完成,大大减少了在最坏情况下用户的等待时间,从而减少了时间成本.

Sprites 的支付过程与 Raiden 网络类似,区别在于跨通道支付时条件支付协议. HTLC 的条件是基于 Hash 原像的公布,在 Sprites 中条件支付的条件为 Hash 原像管理合约的输出. 一旦支付通路上的某个节点向 Hash 原像管理合约提交 Hash 原像,通路上的其他节点就可以同时得知 Hash 原像的公布结果,并且确认跨通道支付的完成.

4) 可持久化机制

对上述支付网络的分析可知,支付网络对系统的交易吞吐量的提升是巨大的,方案理论上对系统的交易吞吐量没有限制. 然而在实际应用中,由于链下支付网络将区块链看作解决通道双方争议,防止攻击者作恶的仲裁平台[22],因此所有结束通道的交易必须上链进行共识. 因而频繁的开关通道势必会影响区块链的交易吞吐量,限制链下支付网络的优势.

Revive[23]实现了通道支付网络中的可持久化机制. 主要原理为:利用跨通道支付协议,使得在支付网络中存在支付环路的节点间可以通过跨通道支付,模拟正常的支付,将押金充裕的通道内的资金流向押金将要耗尽的通道.

5) 寻路算法

在实际应用中一个完整的链下支付网络方案除了需要解决双向通道支付和跨通道支付外,还需要设计高效的寻路算法. 在链下支付网络方案中,节点间建立通道需要较高成本(交易费、押金和交易确认时间),因此一个节点能够维持的通道数是有限的,而频繁的建立和关闭通道会影响到通道支付协议的效率和可用性. 从支付开销的角度讲,在实际应用中,链下支付网络应尽量借助他人已有的通道来实现支付功能,而不是直接建立与收款者建立通道. 因此存在着在支付网络中寻找支付通路的需求. 现有相关的研究成果较少,主要包含 2 类:基于最大流算法和基于 Landmark 算法. 基于最大流算法要求节点保存着全网的通道图,并利用经典最大流算法,如 Push-Relabel[24]等算法寻找到目标点的可行支付路径;基于 landmark 算法主要包括 Flare, Landmark Routing[25-27]等方案,将支付网络中建立的通道较多的若干节点作为信标点,使得用户只需存储相邻通道及到信标点的路径信息,支付时双方交换存储的路径信息并取交集,即可得到双方之间的支付路径.

2.2 Bitcoin-NG

比特币的共识机制 PoW 保证了开放网络中区块链状态的一致性(弱一致性),但其并未考虑效率,因此 Eyal 等人提出了 Bitcoin-NG 的方案,旨在提升一轮共识中的交易确认数,从而提升系统的交易吞吐量. Bitcoin-NG 将比特币的共识过程拆分成 2 个阶段:记账人选取和交易排序. 在记账人选取阶段仍然采用原先的工作量证明算法,由全网节点竞争该轮的记账权,在交易排序阶段由该轮的记账人确认交易并打包区块、全网广播. 记账人选取阶段产生 key-block 的过程和原先比特币中产生区块的过程一致,因此 Bitcoin-NG 基于 key-block 的最长链原则保证了其安全性(容错)和比特币一致. 同时,当节点通过工作量证明成为记账人后,其可以在下一位记账人产生之前,确认打包交易并生成 micro-block. 其实质是利用了两轮记账人选取阶段的空隙,由记账人产生包含交易数据的 micro-block,在不影响其容错性的前提下,提升了一轮共识过程中的交易确认数.

然而,在 Bitcoin-NG 中也引入了记账人大量广播 micro-block 造成系统网络阻塞的风险. 因此 Wan 等人[28]提出了 Goshawk 方案,设计了双层链+两级挖矿机制,即 key-block 和 micro-block 是由全网节点通过 2 个难度不同的工作量证明机制来产生,从而有效避免了 micro-block swamping 攻击;此外, Goshawk 引入了投票机制来抵抗自私挖矿和 51%算力攻击,并支持系统协议的动态升级. 该方案在保持了 Bitcoin-NG 原有的效率提升基础上,进一步加强了系统的安全性和可用性.

2.3 分片机制

除 2.1 节和 2.2 节 2 类方案外,在借鉴传统分布式数据库领域的分片技术的基础上,通过在开放的区块链网络中设计可靠的分片机制也可以提高系统的交易吞吐量[29-31].

分片机制通过将全网节点划分成不同的集合(shard),使每个集合独立并行地运行共识协议,

完成交易确认,从而使得系统的交易吞吐量随着全网节点的增加而近似线性地增加.

传统的区块链共识机制的容错上限为51%,如比特币的工作量证明敌手在不掌握51%算力的情况下难以发动双花攻击.不同于传统区块链共识机制,在原有系统容错性保持不变的情况下,分片机制需要面临的挑战是1%攻击,即保证攻击者在分片过程中无法在任何一个分片中实现51%攻击,以及如何保证攻击者无法在分片处理交易的过程中,实现双花攻击.

2.3.1　随机算法

有效抵御1%攻击的措施是在分片的过程中,参与共识的节点需要随机地被分配到不同的分片,这样当分片大小(size)足够大时,分片内出现51%攻击的概率可以忽略不计.当前在区块链分片机制中被使用的随机算法主要基于2类:工作量证明(PoW)和权益证明(PoS).两者实质都是随机过程.

在Elastico和Zilliqa的方案中都采用了工作量证明作为分片的随机算法.上述方案在片内进行共识时采用了PBFT算法.PBFT算法的安全假设基于在参与共识的节点数中恶意节点不超过1/3,因此为了抵御女巫攻击[32](sybil attack),节点需要在一轮共识开始的阶段,进行简单的工作量证明以获得参与PBFT[33]共识的身份.将节点划分成不同集合的标准基于节点工作量证明的结果.通过建立概率模型可以得到当分片大小达到600时,即使攻击者拥有1/3的算力,其能够控制一个分片(即在任何分片中拥有超过1/3节点)的可能性可以忽略不计(2^{-20}).

其具体过程可抽象为:

1) 节点进行工作量证明获得身份,并划分成不同的集合.

2) 在各个分片内部通过PBFT算法,进行分片内的交易共识

3) 将各个分片共识后的交易集及共识过程中的签名广播给某一个分片,由该分片校验签名,进行分片内共识后,打包成区块并全网广播.

2.3.2　交易处理

根据区块链的模型可以将系统的交易处理分为2类:基于UTXO模型和基于账户模型.

Elastico的方案基于UTXO模型,因此在交易处理时,通过交易的输入作为基准映射到不同的分片处理.在UTXO模型中,攻击者想要实现双花必须产生2笔引用同一输出的交易.因此Elastico可有效抵御在交易处理过程中的双花攻击.

Zilliqa的方案基于账户模型,因此在交易处理时,通过发送者的身份作为基准映射到不同的分片中.一轮共识过程中,不同发送者的交易可能映射到不同的分片(不同验证者),但同一发送者的交易都会由同一分片处理,因此分片内的诚实节点对特定发送者的状态是确定的.因此其能够在基于账户的模型下抵御双花攻击.

3　性能扩展技术分析与展望

在本节中,我们将首先分析比较各种链下支付协议,再分析对比Bitcoin-NG、链下支付协议及分片机制的优缺点和适用场景,并基于此给出下一步研究方向.

3.1　现有方案分析对比

如表1所示,不同的支付通道协议在不同的阶段交互所需要的签名数不同.在建立通道阶段,所有的通道支付协议都需要对funding交易进行签名,闪电网络需要通道额外交互初始的commitment交易来确定初始状态,Duplex方案中则需要额外建立深度为d的初始Invalidation树来确定初始状态.Raiden和Sprites中初始状态由funding交易生成,智能合约通过funding交易确认通道初始状态,不需要额外的update交易.在支付阶段,由于Duplex使用了2条单向通道实现双向通道的功能,因此,一轮支付只需要更新一条单向通道的状态,单向通道的状态更新在交互时只需要付款者一方的签名.而其他方案基本采取了与闪电网络相同的通道更新方式,因而每轮更新需要通道双方各自对通道内的最新状态进行签名.在结束通道阶段,Duplex需要提交2个单向通道的状态,而闪电网络由于设计了惩罚交易来作废通道之前的状态,因此需要在提交阶段公开3笔交易,而Raiden和Sprites等方案采用了其他更新状态的机制,因此只需要在提交阶段公开记录最新状态的交易,而不需要额外的惩罚交易.Duplex在协议运行中还包括reset阶段来调节2条单向通道间的资金分配,而其他协议均设计了双向支付通道,并不包含该阶段.

如表2所示,不同的支付通道协议在性能,隐私性,存储开销,支付开销上存在着差异和折中.所有通道支付协议都实现了双向支付的功能,Duplex采用2条单向支付通道,而其他协议都只有一条双向支付通道.在通道双方的本地存储开销上,Duplex采用了Invalidation树的结构来作废通道之前的状态,

其存储开销取决于树的深度 d. 闪电网络需要双方存储作废之前状态的所有惩罚交易,因此其存储开销取决于交易的轮数 N. 在其他方案中双方都只需存储最新一轮的状态更新交易. 当结束通道时,基于通道内最新状态的交易会进行上链共识,闪电网络引入了惩罚交易,一轮完整的状态更新需要 3 笔交易. 而 Duplex 需要公开 2 个单向通道内的最新状态,因此需要上链 2 笔交易,其他支付通道协议只需要共识一笔交易. 在支付开销上,Sprites 使用了基于智能合约执行结果的条件支付协议,因此在跨通道支付过程中资金所需要被冻结的时间最短,为通路跳数 L 加上通道内双方交互的最长时延 t. 其他协议均需要两者相乘.

Table 1 Comparison on the Number of Signatures Required for Each Stage

表 1 支付通道协议在不同阶段交互所需要的签名数对比

Project	Set Up	Payment	Reset	Settle (Dispute)
Lightning	2×2	1×2	no	3
Duplex	$(d+2)\times 2$	1	yes	1×2
Raiden	2	1×2	no	1×2
Sprites	2	1×2	no	1×2

Table 2 Characters of Different Payment Channels

表 2 不同支付通道协议的特性对比

Project	Bidirectional	Storage (Local)	Storage (Chain)	Cost
Lightning	yes	$O(N)$	2 or 3	$L\times t$
Duplex	yes	$1+d$	2	$L\times t$
Raiden	yes	$O(1)$	1	$L\times t$
Sprites	yes	$O(1)$	1	$L+t$

在 3 类主流的提升区块链性能的方案中,链下支付网络并未真正提升区块链本身的交易容量,其大量交易在离线情况下完成,而将区块链作为仲裁平台,只有在关闭通道分配通道资金或者通道双方对通道状态存在不一致的情况下,才将交易公开上链. 因此,尽管链下支付网络对交易吞吐量的提升是巨大的,完全可以满足现有需求,但是其只能支持数字支付领域,在区块链的其他应用场景中,链下支付网络技术无法提升区块链的性能. 同时,链下支付网络在建立通道和关闭通道阶段均有交易上链的过程,因此在实际应用中其性能提升有赖于区块链本身的交易容量. 而 Bitcoin-NG 和分片机制旨在提升区块链本身的性能,提高了一轮共识过程中的交易处理数. 然而受制于分布式网络结构复杂,节点的存储空间和处理性能有限等限制,两者对系统交易吞吐量的提升无法和链下支付网络相比. 实验表明,在 Bitcoin-NG 等方案中,系统交易吞吐量的量级在 10^2,分片机制对系统交易吞吐量的提升与全网参与共识的节点呈近似线性关系,而链下支付网络对系统的交易吞吐量在理论上没有作限制. 但是后 2 个方案是直接提升区块链本身的性能,因此其能够在区块链的其他应用场景,如分布式文件存储、征信、供应链及金融领域等起到提升系统性能的效果.

3.2 下一步研究方向

基于上述对提升区块链性能的 3 类主流方案的分析,未来进一步的研究方向包括 4 个方面:

1) 在链下支付网络方案中,当前在支付开销、交互开销上最优的方案是 Sprites,然而其引入的原像管理合约只能应用于以太坊等平台中,无法在现有比特币中实现. 而实际中基于比特币的区块链平台众多,因此需要研究基于比特币平台的链下支付网络效率改进方案.

2) 在实际应用中,链下支付网络的高效寻路算法也值得进一步研究,当前的 2 类方案中,基于最大流方案存储开销和运行成本过大,基于 Landmark 的方案中虽然不需要节点存储整个网络图,但其寻路的成功率取决于选取信标点集的方式和大小,并且无法保证寻找到的路径是否为最优路径.

3) 在分片机制中系统交易吞吐量的提升取决于参与全网参与共识的节点数,然而当前在其激励机制方面研究不足,同时对其安全性的相关分析也较少,并且已有的方案在分片过程中,如 Elastico 和 Zilliqa,由于网络延迟等因素可能存在被恶意者攻击的可能.

4) 在 Bitcoin-NG 等方案中,可考虑结合 DAG (directed acyclic graph) 结构进一步提升交易吞吐量.

4 代表性跨链技术

跨链技术旨在解决链与链之间的交互问题[34]. 当前跨链交互的过程可分为 2 个阶段:资产在链 A 上的锁定阶段和相应资产在链 B 上的解锁阶段. 其面临的主要挑战是链 A 上的资产如何保证被锁定,如何确定解锁链 B 上的资产以及保证资产的锁定

与解锁在链 A,B 之间保证原子性,即 2 条链之间相应的资产要么同时锁定/解锁成功,要么同时锁定/解锁失败.针对上述 2 个挑战,不同的跨链技术被提出,主要包含 4 类:

1) 多中心化公证人;

2) 侧链/中继技术;

3) 基于 Hash 锁定;

4) 分布式密钥控制.

4.1　公证人机制

公证人机制利用公证人来保证资产在不同链上的锁定与解锁.主要利用了区块链脚本中的多签名脚本,可以实现链与链之间双向的交换.具体流程为:用户在链 A 上向多个公证人的多签名脚本地址上转入链 A 的资产进行锁定,公证人在确认(共识)后在链 B 向用户的地址释放相应的资产.

4.2　侧链/中继

侧链技术[35-36]或者中继技术[37-38]提供的是一种更去中心化的解决方案.不同于公证人机制,侧链技术或者中继技术旨在通过去中心化的方式使得不同链之间的状态可以互相交互.

以较早的 BTC-Relay 为例,BTC-Relay 通过 ETH 上的智能合约存储比特币中的区块头,使得 ETH 链上可以获知比特币系统中发生的事件,实现了 ETH 作为比特币侧链的功能.利用比特币区块头数据相当于在 ETH 里创建了一条简易的比特币区块链.但是由于 ETH 智能合约中比特币的区块头信息是由中心化的节点(Relayer)提供的.因此其去中心化程度不足.使用 BTC-Relay 可以实现比特币和 ETH 之间的兑换,具体流程如下:

1) Alice 和 Bob 使用智能合约来进行交易,Alice 使用 BTC 币兑换 Bob 的 ETH 币,Bob 把他的 ETH 币发送到智能合约中;

2) Alice 向 Bob 的地址发送 BTC 币;

3) Alice 通过比特币的交易信息,生成 SPV 证明,并将证明输入到 ETH 系统上的合约中;

4) 合约在被触发后确认 SPV 证明,然后释放之前 Bob 的 ETH 币到 Alice 的地址中.

Cosmos 使用中继技术来实现不同区块链之间数据的交互.如图 4 所示,在 Cosmos 中不同的区块链相当于不同的区域(Zone),Hub 连接所有的区块链,实现链于链之间的中继功能,每条链上状态的更新都需要告知 Hub,因此 Hub 中的状态相当于所有链的叠加,保证了所有链中的代币总量不变.Cosmos 中链 A 与链 B 之间状态的确认可以通过 Hub 来实现.

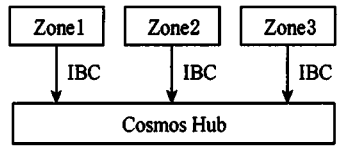

Fig. 4　Structure on cosmos relay network

图 4　Cosmos 中继技术结构

4.3　Hash 锁定

Hash 锁定的原理与闪电网络中 HTLC 相同,将 Hash 的原象作为秘密,利用条件支付,可以在无可信第三方参与的情况下保证不同交易的原子性,实现公平的跨链交换.

如图 5 所示,跨链原子交换的流程为:

1) A 产生随机数 r,并计算 r 的 Hash 值 h,将 h 发送给 B.

2) A 与 B 利用 HTLC 相继将用于交换的资产锁定.要求 A 的锁定时间需要比 B 长,即 $T_1 < T_2$.从 A 的角度看,在时间 T_1 内,B 可以通过公布原像 r 获得 A 锁定的资产,否则 A 赎回自己的资产.从 B 的角度看,在时间 T_2 内,A 可以通过公布原像 r 获得 B 锁定的资产,否则 B 赎回自己的资产.

3) A 通过公布原像 r 获得 B 锁定的资产.同时 B 得到了秘密 r,并且通过公布 r 在另一条链上得到 A 锁定的资产.

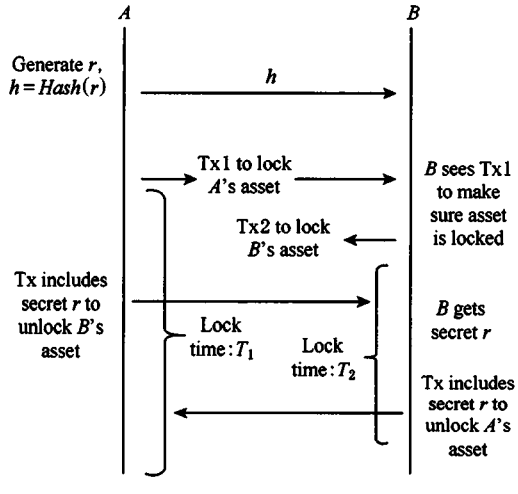

Fig. 5　Process of cross-chain atomic swap

图 5　跨链原子交易流程

4.4　分布式密钥控制

通过分布式密钥控制机制来实现去中心化的跨链交换的方案是由 Fusion[39]提出的,其利用密码学

中的分布式密钥生成算法[40]和门限签名技术[41]保证了跨链过程中资产锁定和解锁由系统参与共识的所有节点决定并且在此过程系统中的任何节点或者少数节点联合都无法拥有资产的使用权. 整个过程可分为2个阶段:锁定资产阶段和解锁资产阶段. 以比特币和Fusion交互为例:

锁定阶段:

1) A 向Fusion发起锁定资产请求,通过调用智能合约,利用分布式密钥生成算法. 该过程中,智能合约将密钥碎片随机分发给Fusion中不同的节点.

2) 智能合约返回私钥对应的公钥地址. A 收到地址后,将资产锁定在该公钥地址中.

3) 智能合约确认 A 的资产确实锁定后更新 A 在Fusion中的资产信息.

解锁阶段:

1) A 向Fusion发起解锁资产请求.

2) 智能合约确认 A 在Fusion中的资产信息后,锁定 A 在Fusion中的相应资产并广播解锁交易签名请求.

3) 拥有私钥碎片的节点检查解锁交易后签名.

4) 节点将签名后的交易在比特币平台广播,将锁定的资产输出到 A 的地址.

5) 智能合约确认 A 的资产确实解锁后更新 A 在Fusion中的资产信息.

5 跨链技术分析对比与挑战

在本节中,我们将分析比较各种典型跨链技术的优缺点和适用场景,并在此基础上给出相关研究挑战.

5.1 现有技术分析对比

如表3所示,不同的跨链技术在适用的场景、信任模型、支持的功能以及实现难易程度上存在差异和折中. 在应用场景中,中继技术中的BTC-Relay只支持单向的跨链交换,如通过BTC-Relay实现了ETH作为BTC的侧链功能,然而BTC不是ETH的侧链,而采用中继链技术的其他中继方案和另3种技术都实现了不同链之间的双向交换. 从信任模型上,公证人机制通过多中心化的方式,安全假设要求多数公证人的诚实,而其他方案的安全假设则和主链一致,即51%假设. 在具体应用上,Hash锁定只支持代币的兑换,链之间的数据仍是不相通的,而其他方案既支持代币的兑换,又能实现数据的交互,可以满足更多的应用场景,如跨链资产抵押,跨链信息交互等. 从实现角度说,公证人机制和Hash锁定都是较成熟且简便的方案,但是带来的缺点是引入中心化机构,改变了原本的信任模型行或者支持功能单一,只能满足代币兑换场景,而其他方案设计较为复杂,但是能满足更多业务场景.

Table 3 Characters of Cross-Chain Technology

表3 不同跨链技术的特性对比

Technology	Scene	Trust Model	Application	Degree of Difficulty	Implementation
Witness	bidirectional	Majority witness	all	easy	Ripple[42]/multi-sig
Relay	unidirectional/bidirectional	51%	all	hard	BTC-Relay/Cosmos
Hash lock	bidirectional	51%	Cross chain exchange	easy	Atomic swap
Distributed key	bidirectional	51%	all	hard	Fusion

5.2 相关研究挑战

在跨链技术方面,当前的研究挑战主要包括2个方面:

1) 当前支持双向跨链信息交互的跨链技术如中继和分布式密钥,都需要不同链之间彼此获知链的更新状态,其大多采用了成熟的SPV证明技术,使用区块头在不同链中构建了微型的目标链,然而当需要交互的链数目较多时,其带来的开销必然对区块链的性能带来影响.

2) 在当前的跨链技术中,除了支持应用有限的基于Hash锁定方案,其余方案出于安全和效率的考虑,直接或间接的引入了第三方,如SPV证明中区块头的提供者,因此可能存在着第三方作恶的风险.

6 总 结

区块链技术拥有去中心化、不可篡改、可编程等特点,这使得其在数字支付、分布式存储、征信、供应链、金融等领域中拥有广泛的应用前景. 然而其所

面临的可扩展性瓶颈,包括性能效率低下、功能难以扩展,都限制了区块链技术的应用.

本文对近些年来解决区块链可扩展性问题的方案和技术进行了综述,讨论了提升区块链性能的3类主流方案和扩展区块链功能的4类代表性跨链技术,详细分析比较了各种方案和技术的优缺点及适用场景,并讨论了需进一步研究的问题和方向.

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008-10-31) [2017-02-11]. https://bitcoin.org/bitcoin.pdf

[2] 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. New York: ACM, 2016: 3-16

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

[4] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains [C] //Proc of the Int Conf on Financial Cryptography and Data Security. Berlin: Springer, 2016: 106-125

[5] Andresen G. BIP 101: Increase maximum block size [EB/OL]. [2016-04-19] https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

[6] Yu Hui, Zhang Zongyang, Liu Jianwei. Research on scaling technology of bitcoin blockchain [J]. Journal of Computer Research and Development, 2017, 54(10): 2390-2403 (in Chinese)
(喻辉,张宗洋,刘建伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390-2403)

[7] Eyal I, Gencer A E, Renesse R V. Bitcoin-NG: A scalable blockchain protocol [C] //Proc of USENIX Conf on Networked Systems Design and Implementation. Berkeley CA: USENIX Association, 2016: 45-59

[8] Wood G. Ethereum: A secure decentralised generalised transaction ledger [EB/OL]. (2017-08-07) [2018-03-04]. https://pdfs.semanticscholar.org/f65e/e3a9f171da68b57039-a5d5f2f1ad70798488.pdf

[9] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin [C] //Proc of 2014 IEEE Symp on Security and Privacy (SP). Piscataway, NJ: IEEE, 2014: 459-474

[10] SWAN M. Block chain thinking: The brain as a decentralized autonomous corporation [J]. IEEE Technology and Society Magazine, 2015, 34(4): 41-52

[11] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments [EB/OL]. (2015-11-20) [2017-04-11]. https://lightning.network/lightning-network-paper.pdf

[12] Bitcoin Wiki. Hashed timelock contracts [EB/OL]. [2017-05-22]. https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts

[13] Bentov I, Kumaresan R. How to use bitcoin to design fair protocols [C] //Proc of the Int Cryptology Conf. Berlin: Springer, 2014: 421-439

[14] Mccorry P, Heilman E, Miller A, et al. Atomically trading with roger: Gambling on the success of a hardfork [M] // Data Privacy Management, Cryptocurrencies and Blockchain Technology. Berlin: Springer, 2017: 334-353

[15] Nolan T. Alt chains and atomic transfers [EB/OL]. [2017-11-03]. https://en.bitcoin.it/wiki/Atomic_cross-chain_trading

[16] Spilman J. Anti dos for tx replacement [EB/OL]. [2018-01-08]. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002417.html

[17] Mark F. BIP 0068: Consensus-enforced transaction replacement signaled via sequence numbers (relative locktime) [EB/OL]. [2016-09-22]. https://github.com/bitcoin/bips/blob/master/bip-0068.mediawiki

[18] Decker C, Wattenhofer R. A fast and scalable payment network with bitcoin duplex micropayment channels [C] // Proc of the Int Symp on Stabilization, Safety, and Security of Distributed Systems. New York: Springer, 2015: 3-18

[19] Raiden Foundation. Raiden network whitepaper [EB/OL]. [2018-05-11]. http://raiden.network/

[20] Peterson D. Sparky: A lightning network in two pages of solidity [EB/OL]. [2018-01-22]. https://www.blunderingcode.com/a-lightning-network-in-two-pages-of-solidity/

[21] Miller A, Bentov I, Kumaresan R, et al. Sprites: Payment channels that go faster than lightning [EB/OL]. (2017-11-30) [2018-01-07]. https://arxiv.org/pdf/1702.05812.pdf

[22] Mccorry P, Möser M, Shahandasti S F, et al. Towards bitcoin payment networks [C] //Proc of the 8th Int Conf on Information Security and Privacy. Berlin: Springer, 2016: 57-76

[23] Khalil R, Gervais A. Revive: Rebalancing off-blockchain payment networks [C] //Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2017: 439-453

[24] Rohrer E, Laß J F, Tschorsch F. Towards a concurrent and distributed route selection for payment channel networks [C] //Proc of Int Workshop on Data Privacy Management, Cryptocurrencies and Blockchain Technology. Berlin: Springer, 2017: 411-419

[25] Tsuchiya P F. The landmark hierarchy: A new hierarchy for routing in very large networks [J]. ACM Sigcomm Computer Communication Review, 1988, 18(4): 35-42

[26] Prihodko P, Zhigulin S, Sahno M, et al. Flare: An approach to routing in lightning network [EB/OL]. (2016-07-07) [2017-08-15]. https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf

[27] Roos S, Moreno-Sanchez P, Kate A, et al. Settling payments fast and private: Efficient decentralized routing for path-based transactions [J]. arXiv preprint, arXiv: 1709.05748, 2017

[28] Wan Cencen, Zhang Yuncong, Pan Chen, et al. Goshawk: A novel efficient, robust and flexible blockchain protocol [EB/OL]. [2018-05-31]. https://eprint.iacr.org/2018/407.pdf

[29] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains [C] //Proc of the ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 17-30

[30] Zilliqa Foundation. Zilliqa Whitepaper [EB/OL]. [2018-05-05]. https://docs.zilliqa.com/whitepaper.pdf

[31] ETH. ETH sharding research [EB/OL]. [2018-04-11]. https://ethresear.ch/t/fork-free-sharding/1058/

[32] Douceur J R. The sybil attack [C] //Proc of the Int Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251-260

[33] Castro M, Liskov B. Practical Byzantine fault tolerance [C] //Proc of the Symp on Operating Systems Design & Implementation. New York: ACM, 1999: 173-186

[34] Buterin V. Chain interoperability [EB/OL]. [2018-03-05]. https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf

[35] Back A, Corallo M, Dashjr L, et al. Enabling blockchain innovations with pegged sidechains [EB/OL]. (2014-10-22) [2017-10-22]. https://www.blockstream.com/sidechains.pdf

[36] Rootstock. Sidechains, Drivechains and RSK 2-way peg designs [EB/OL]. (2016-04-06) [2017-11-06]. https://www.rsk.co/blog/sidechains-drivechains-and-rsk-2-way-peg-design

[37] BTC-relay. BTC-relay [EB/OL]. [2018-02-21]. http://btcrelay.org

[38] Cosmos. Cosmos Whitepaper [EB/OL]. [2018-03-15]. https://cosmos.network/resources/whitepaper

[39] Fusion. Fusion: An inclusive cryptofinance platform based on blockchains [EB/OL]. [2018-05-22]. https://docs.wixstatic.com/ugd/76b9ac_6919c49798d84a65bfb2e421cefbfbd3.pdf

[40] Gennaro R, Jarecki S, Krawczyk H, et al. Secure distributed key generation for discrete-log based cryptosystems [G] // Advances in Cryptology—EUROCRYPT'99. Berlin: Springer, 1999: 51-83

[41] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613

[42] Armknecht F, Karame G O, Mandal A, et al. Ripple: Overview and outlook [G] //Trust and Trustworthy Computing. Berlin: Springer, 2015: 163-180

Pan Chen, born in 1992. Master candidate of Shanghai Jiao Tong University. His main research interest is blockchain technology.

Liu Zhiqiang, born in 1977. PhD. Associate professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. Member of CCF. His main research interests include blockchain technology and symmetric-key cryptography.

Liu Zhen, born in 1976. PhD. Associate professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. His main research interests include blockchain technology and public-key cryptography.

Long Yu, born in 1980. PhD. Associate professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University. Her main research interests include blockchain technology and public-key cryptography.