【电子与信息科学 / Electronics and Information Science】

高性能许可公链

张胜利，王滔滔，杨 晴，王 晖

深圳大学电子与信息工程学院，人工智能与数字经济广东省实验室，广东深圳 518060

摘 要：现有区块链主要分为公链和联盟链，公链是区块链思想的本源，然而公链体系存在匿名账户难以与现实世界对应，以及系统执行效率低两大缺陷，同时，联盟链较差的隐私性和信息安全性又备受诟病，鉴于此，提出许可公链的概念和实现方案. 许可公链通过链上分布式密码学注册方案，实现公共许可机制；通过可订阅二层合约、区块快速转发和结构化广播 3 个技术提高大规模区块链的交易速度. 因此，许可公链融合联盟链的许可机制与公链技术，是面向公众用户的、可监管的创新公链方案. 所提出许可公链系统不仅建立了个人和账户的安全隐私对应关系，而且新架构灵活高效，可支持复杂的实际应用，尤其适用于金融业务与智能金融监管.

关键词：计算机网络；区块链；公链；联盟链；许可公链；扩展性；对等网络；智能合约

中图分类号：TN919.2；TP393.4 **文献标志码**：A **doi**：10.3724/SP.J.1249.2020.03227

Permissioned public blockchain with high performance

ZHANG Shengli, WANG Taotao, YANG Qing, and WANG Hui

College of Electronic and Information Engineering, Shenzhen University, Guangdong Province Lab of Artificial Intelligence and Digital Economy, Shenzhen 518060, Guangdong Province, P. R. China

Abstract: The existing blockchain can be mainly divided into public blockchain and consortium blockchain. The idea of blockchain originates from public blockchain. However, there are two defects in the existing public blockchain system: anonymous account is difficult to correspond with the real world, and system execution efficiency is low. At the same time, the consortium blockchain suffers from poor privacy and information security. In view of these problems, especially the problems of public blockchain, we design and develop a high performance permissioned public blockchain (PPC). We propose an on-chain cryptography registration scheme, which establishes a private mapping between the real-world entity and blockchain address. We also propose three novel techniques, i. e., the subscibable layer-2 contract, fast block propagation, and optimized structured broadcast protocol, to significantly improve the transaction speed. Therefore, the license mechanism of consortium blockchain and public chain technologies are combined and can be used by public users. As a result, the proposed permissioned public blockchain not only establishes the security privacy correspondence between individuals and accounts, but also has a flexible and efficient new architecture, which can support various applications to all customers, especially for the financial services and the supervision therein.

Key words: computer networks; blockchain; public blockchain; consortium blockchain; permissioned public blockchain; scalability; peer-to-peer (P2P) network; smart contract

Received: 2020-01-22; **Accepted**: 2020-03-06
Foundation: National Key R & D Program of China (2018YFB2100705); National Natural Science Foundation of China (61771315)
Corresponding author: Professor WANG Hui. E-mail: wanghsz@szu.edu.cn
Citation: ZHANG Shengli, WANG Taotao, YANG Qing, et al. Permissioned public blockchain with high performance [J]. Journal of Shenzhen University Science and Engineering, 2020, 37(3): 227-233. (in Chinese)

区块链最初是作为在对等(peer-to-peer，P2P)用户间进行安全、有效和透明的数字资产交易的支撑技术而诞生的[1]，由于能够在未经许可的去中心化网络上实现分布式拜占庭协容错[2-3]，已被认为是在金融科技、物联网和供应链等领域[4-6]具有颠覆能力的技术. 当前区块链技术为适应不同应用场景，正在向两种类型演化，即公链(public blockchain)技术和联盟链技术. 区块链可以定义为在大规模不可靠计算机网络中实现数据记录的可信性、合法性、一致性和实时性的软件系统. 公链技术是区块链去中心化理念最核心的体现. 比特币和以太坊等公链分别给区块链世界带来了“数字加密货币”和“智能合约”等崭新概念. 公链的技术标签是公共开放，这也是去中心化的自然属性. 因此，公链承担的角色是网络基础设施，其用户多且易形成网络经济效应. 公链使社会合作具有自我管理进化的可能. 然而，现有的公链体系存在两大缺陷：① 转账主体都是账户地址，匿名账户难以与现实世界对应. 联盟链对用户采用准入机制，用户在联盟链上转账都必须到认证节点进行认证. 与联盟链不同，在公共开放的公链上，为保护用户隐私，用户都广泛采用无需许可的匿名系统. 这种匿名账户与现实世界隔离，造成公链难以被有效监管，进而令许多物理世界中针对人的应用在区块链上难以实现. 例如，比特币日渐成为洗钱和走私等违法犯罪活动的工具[7]；以太坊上发生大量基于 ERC20 Token 标准的非法集资乱像[8]. ② 受限于网络协议等技术因素，公链交易处理速度都非常低，限制了它大规模应用的扩展性[9-10]. 为此，本研究提出并设计了高性能许可公链(permissioned public blockchain，PPC).

现实网络应用的主体应当是社会中的自然人或者物联网中的设备等物理实体. 所以，公链的大范围应用落地必须要建立地址与社会自然人和物联网设备等实体之间的关系镜像，且该镜像关系能够在不破坏链上隐私的情况下用来实现有效监管. 为提高公链的交易处理速度，当前研究工作主要集中在设计新的共识协议上[11-23]. 但是，这些新的共识协议大部分都是以牺牲安全或去中心化的代价换取性能的提高. 当前公链的网络协议并没有发挥全部的数据处理潜力，更未针对区块链的需求进行优化. 公链性能瓶颈主要是网络协议[10,24]，提高公链的数据处理速度，应该从改进其网络协议着手.

PPC 旨在研发一条具有实体映射功能的基础设施公链，通过分布式认证和网络协议优化实现一个面向实体用户的高性能公链. 在充分保护实体隐私的条件下，许可公链上信息全部公开透明，链上地址都对应了社会自然人或物联网设备. 通过实体映射协议和零知识证明等密码学方案，实现实体身份(identification，ID)信息和实体认证的分离，使许可公链在达到与匿名公链同等隐私安全水平的前提条件下，实现链上地址和自然人或设备身份镜像映射，如图 1. 充分利用实体映射信息，一方面可显著优化现有区块链算法，包括网络分片算法、共识算法和虚拟机等；另一方面可提供一些现有匿名区块链不具备的功能，如按人投票和地址惩罚等. 本研究通过改进现有公链的消息网络协议，以期在不改变共识层协议的条件下，仍能极大提高许可公链数据处理性能，使许可公链本身真正能够承载大规模的商业应用，发挥其潜在的巨大商业价值.

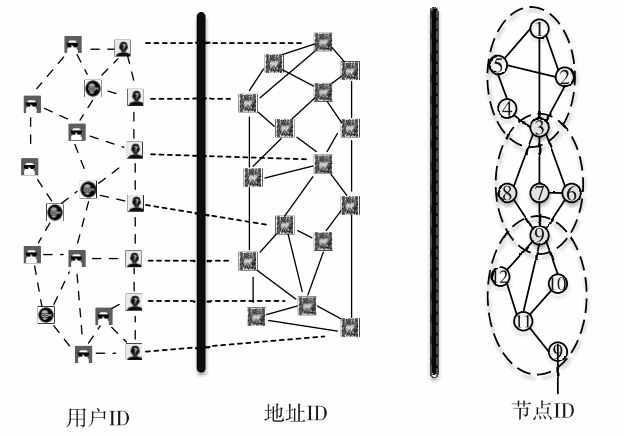


图 1 许可公链多层 ID 模型

Fig. 1 Multiple ID model of permissioned public blockchain

1 隐私许可接入公链

现有的区块链公链大多使用本地随机生成的密钥对，无注册机制，更未与实体信息关联，这样不利于监管，易造成负面影响；还有一些具有身份认证功能的区块链应用都是中心化的，实体用户的隐私信息都存储在中心化的服务器上，信息安全得不到保证.

为实现链下实体与链上某个主地址的一一对应，但具体对应关系不可见，用户用于认证的隐私信息都需保存在本地；同时每个主地址可自主生成多个隐私地址，隐私地址和主地址之间的对应关系

也不可见. 这样既可保证隐私安全，也便于监管链上账户. 该功能主要通过零知识证明的密码学算法与生物认证信息实现. 为达到上述技术要求，本研究利用链上零知识证明技术与一次性密钥算法的加密方案，设计了一套如图 2 的注册流程，并通过用户（钱包）与区块链的多次合约交易来实现实体验证过程. 采用零知识证明技术，在用户不提供个人数据前提下进行分布式注册，保证个人数据的安全性，并使用可链接环签名技术来确保 3 种 ID 之间的内在关联性.

用户在使用区块链系统时，已经注册的地址(包括主地址和隐私地址)可以正常发送交易，没有注册的地址会被其他节点拒绝服务.

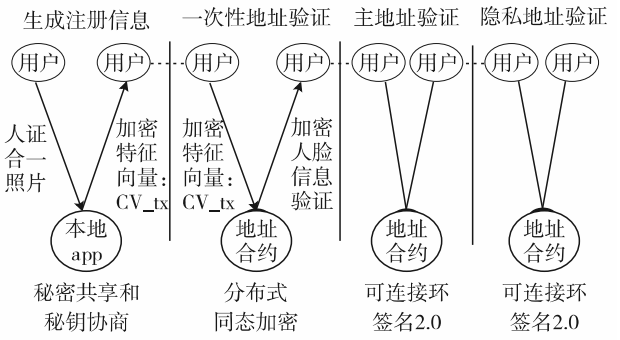


图 2　许可公链的注册流程

Fig. 2　Register process of permissioned public blockchain

2　高性能 3 层系统架构

当前公链的一个弱点是交易处理速度很低. DECKER 等[10]研究了区块大小和区块确认率对交易吞吐量的影响，实证结果表明，仅通过调整这些参数，很难在不损害系统安全性和完整性的情况下提高交易吞吐量. 为根本性解决公链系统性能瓶颈，本研究提出并设计实现了一套优化的公链架构，主要包括 L_0 网络分发层(底层 P2P)、L_1 交易同步与确认层和 L_2 可订阅应用层(合约层)的技术创新，如图 3. 其中，网络分发层主要实现节点组网以及数据在不同网络节点之间快速的转发广播，提供一种不可靠最大努力服务，是区块链系统性能的基础；交易同步和交易确认是在网络分发基础上，实现不同节点之间交易数据一致性(包含共识算法与数据调和算法等)，是区块链系统的核心；可订阅应用层基于智能合约实现，节点可以根据自身应用订阅对应合约，达到应用分组以及应用与底层系统的隔离，是实现区块链高性能应用的主要手段.

图 3　高效公链 3 层系统架构

Fig. 3　Three layer architecture of permissioned public blockchain

2.1　可订阅 L_2 智能合约技术

以以太坊为代表的大多数公链项目的智能合约与普通交易是合二为一的，账户是作为世界状态存储的，所以，即便用户仅有转账需求，仍需执行所有合约交易，存储所有合约状态. 这种做法造成以下问题：① 交易无法并行执行，导致系统性能过低，主要表现在每秒处理事务数(transactions per second，TPS)过低，无法满足业务需求；② 用户主要执行自己不关心的不重要的合约代码，造成算力浪费.

针对以上问题，本研究提出可订阅 L_2 智能合约技术，将智能合约与交易分成相对独立的两层进行处理. 具体包括以下 3 点：

1) 用户分组：普通转账交易(包括合约账户参与的转账交易)由底层链进行共识与打包出块，这些交易形成的区块链由所有用户共同维护；合约交易则分别由具体参与合约的用户维护，每个合约可根据需要选择自己的合约内部共识，进行合约交易的打包和出块，形成合约区块链. 每个合约的交易都独立计算与打包，合约交易与普通转账交易并行执行. 每个合约都会维护一个合约交易区块链.

2) 分层存储与计算：合约账户有全局状态和局部状态之分. 全局状态记账户余额和索引等，与普通账户一致，这部分数据记录在底层链上；局部状态是合约内定义的变量等信息，由每个参与具体合约的参与者共同记录与维护.

3) 合约链与底层链的交互：合约业务与底层业务涉及到的交互分为两类：一类是合约业务需底层账户余额做支撑；另一类是合约链状态更新后需在底层链上做数据存证.

合约创建者创建合约后，会把合约地址和创建

者节点记录在合约注册表中，合约注册表模块目前采用全局合约的形式完成. 其他用户若需订阅则可查询合约注册表，从该节点同步合约的链数据. 参与合约的用户发起的调用交易户被所有合约参与者维护，根据合约的共识规则进行交易打包出块. 合约出块后，需由合约链发起一笔合约存证交易把当前合约链的状态根哈希记录在底层链上进行存证. 所有不需要状态存证，仅提供计算功能的合约被称为子合约，所有的子合约形成子合约库可供所有主合约进行调用. 自适应 L_2 智能合约的整体流程图如图 4. 可订阅 L_2 智能合约隔离了不同合约用户对网络的影响，可将交易速度提升 10 倍以上.

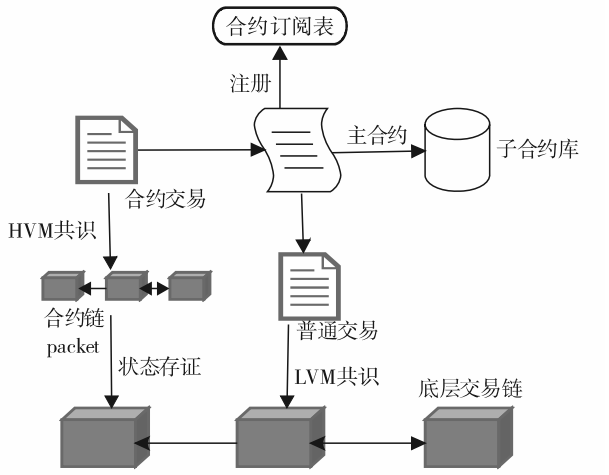


图 4 可订阅智能合约

Fig. 4 Subscribe smart contract

2.2 L_1 层交易与区块快速转发技术

许可公链通过对公链数据通信协议进行重新设计，提出创新的交易和区块快速转发技术，实现交易处理速度的提升. 许可公链采用的交易和区块快速转发技术，包含区块预打包和交易池滑动窗口同步机制 2 个技术组件.

2.2.1 区块预打包技术

在传统公链中，当区块产生后，需在全网进行区块广播，其他节点在进行区块同步时，需要请求整个新区块的信息，且在本地还需通过执行区块中的每笔交易进行验证. 新区块传输以及对其中交易进行验证的时间开销大大降低了区块同步的效率，导致节点间出现了状态不同步的现象(即区块链分叉)，限制了公链的交易处理速度.

在许可公链中，节点在本地提前计算预打包区块，完全按照打包规则在本地提前构建一个预区块，并保存每一笔交易(transaction，Tx)执行后的状态改变. 因此，在区块同步时不需传输整个区块，只要传输区块中每笔交易的哈希和区块头就可完成区块同步；且因已在预打包阶段进行验证，在交易验证时不需执行每一笔交易，大幅减少了交易验证的时间开销，提高了许可公链处理交易的速度. 如图 5，提前计算对交易进行预排序和按关系重新分组后预打包成一个区块进行提前验证. 预打包可以将每个区块中的交易数目提升 10 倍.

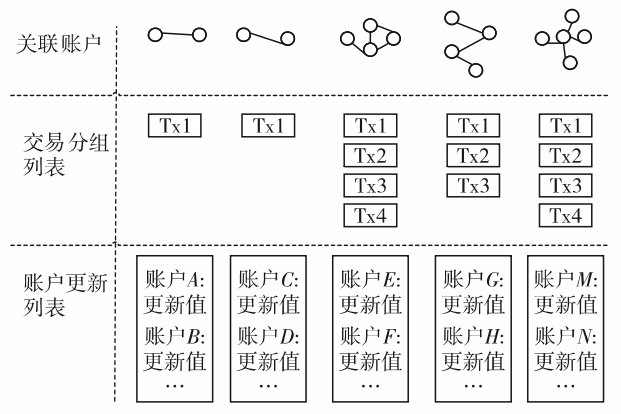


图 5 交易预分组打包和提前计算技术

Fig. 5 Transactions grouping and blocking for pre-computing

2.2.2 交易池滑动窗口同步机制

每个区块链节点都会在本地维护一个存有未被打包进入区块的交易池. 交易池通常不同步，预打包区块和新收到的区块不同，网络就会消耗额外时间和带宽去获取在节点间丢失的交易. 实际测量结果发现，以太坊节点间交易池相似度约为 75.7%.

为进一步提高节点间的交易池相似度，提高区块链交易处理的性能，在许可公链中引入交易池滑动窗口同步机制来快速同步交易池. 快速同步交易池首先使用可逆布隆查找表和布隆过滤器技术来对节点的本地交易池进行数据压缩. 压缩后的交易池在节点间进行交换同步. 在此基础上使用类似传输控制协议/网际协议(transmission control protocol/internet protocol，TCP/IP)的滑动窗口机制触发交易池的同步流程(图 6)，发送尽可能少的信息获取节点间交易池的差异，如此，既能提高节点间的交易池相似度，也能最大限度减少公链网络的负担. 假设固定的时间间隔为 t，该参数可根据网络交易的生成速度和区块大小确定. 交易池利用滑动窗口机制进行快速转发的步骤为：① 当节点间互相连接后，调节窗口时间为 t，即经过时间 t 后触发第 1 次基于可逆布隆查找表(invertible Bloom lookup table，

IBLT) 和布隆过滤器的快速转发；② 若交易池间存在差异，调节窗口不变，交换信息后重新计时，再经过时间 t 后触发第 2 次快速转发；③ 第 2 次交换信息时若发现两者间无差异，则将调节窗口设为 $2t$，重新计时并经过 $2t$ 后触发第 3 次快速转发；④ 若第 3 次交换信息还是不存在差异，则将调节窗口设为 $4t$，并依次类推；⑤若在③和④中任意一次发现差异，则将调节窗口重新设为 t，并重新计时.

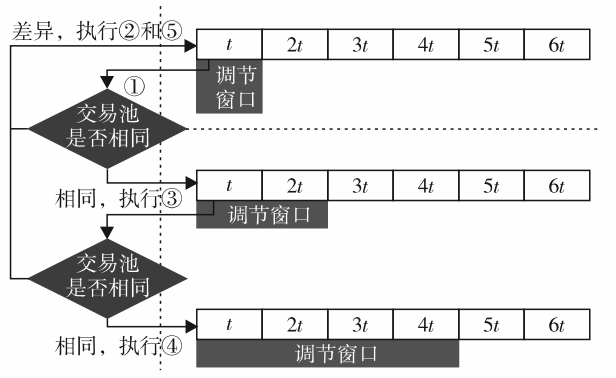


图 6　滑动窗口交易池同步机制

Fig. 6　Transaction pool synchronization mechanism with sliding windows

2.3　L_0 层 P2P 网络优化技术

区块链底层的数据通信网络是支撑区块链的基础设施，一般采用对等网络技术实现. 在区块链的通信网络中，交易数据和区块数据的传输效率对区块链系统的整体性能有决定性影响. 例如，交易数据的传播速度关系到交易被执行和打包进区块的延迟；区块数据的传播速度则关系到交易确认时间以及区块链分叉的概率. 在实际的区块链系统中，每个节点的数据传输总带宽和能够维持的最大连接数都是有限的，因此，如何利用有限的网络资源最大化区块链系统的吞吐量，是目前区块链网络优化的重大挑战之一.

2.3.1　DHT 结构化网络广播协议

针对工作量证明(proof of work，POW) 共识算法，基于 Gossip 协议广播的覆盖网络拓扑都是无结构的，网络中的节点随机选择邻居节点传输消息，直至所有节点都收到消息. Gossip 协议设计简单，但是无法避免消息延迟和冗余问题，这是导致当前公链交易、区块传播速度低下的一个主要原因.

许可公链采用新的基于分布式哈希表(distributed hash table，DHT) 结构的网络广播协议. 如图 7，无结构的 Gossip 网络广播虽然可确保较高容错率，但这是以信息传输冗余为代价，增加了网络负担；结构化的网络广播减少了重复消息的发送次数，因此提高了网络传输性能.

本研究采用 Kademlia DHT 协议[25] 实现结构化的 P2P 覆盖网络拓扑. 方案设计最主要的是修改了每次广播的目的节点的选取方式. 在当前公链的 Gossip 广播协议中，目的节点都是随机挑选的；新方案则是将目的节点设定为 Kademlia DHT 协议中的 k 桶来选取. k 桶是与本地节点存在异或距离关系的节点集合[23]，每次广播只需与 k 桶中的任一节点传输消息即可. 不同于以太坊公链 Gossip 广播协议随机选取节点，许可公链 DHT 结构广播协议利用 Kademlia DHT 覆盖网络的树状拓扑结构来优化消息的广播路径. 通过制定选取规则，可确保 k 桶里的节点都是未接收到消息的，这解决了 Gossip 协议消息冗余的问题，节点之间无需交互，也能知道接下来需传输消息的是哪些节点.

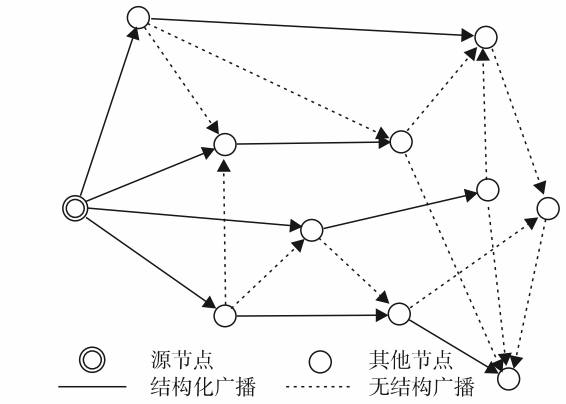


图 7　无结构广播和结构化广播

Fig. 7　Structureless and structured broadcasting

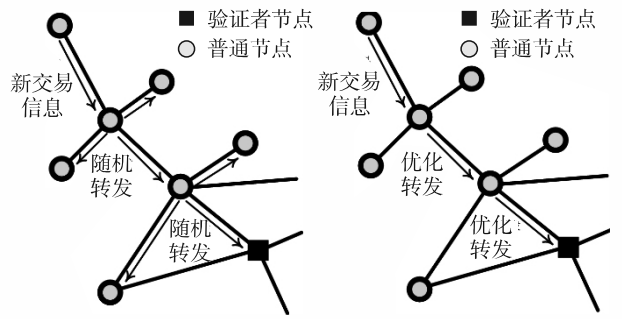
2.3.2　软件可定制网络广播协议

还有一些公链采用实用拜占庭容错(practical Byzantine fault tolerance，PBFT)、权威证明(proof-of-authority，PoA)、权益证明(proof of stake，PoS) 和代理权益证明(delegated proof of stake，DPoS) 等[9] 共识算法. Gossip 这种随机转发的消息传播机制虽然有很好的稳定性和泛用性，但其随机性导致消息在全网传播的延迟不确定性，严重降低了区块链系统性能.

本研究提出适用于采用 PBFT 共识协议和 BFT 类共识协议的区块链系统的自适应软件定义消息传输算法及其系统，如图 8. 由图 8 可见，在 PBFT 共识协议中，区块链节点有验证者节点和普通节点两种类型. 其中，验证者节点负责收集网络中的交易、执行交易(包括转账和智能合约的执行) 和打包

交易并出块；普通节点只能发起交易，不负责交易的执行和打包. 在这样的网络拓扑中，本研究通过改进 Gossip 算法来实现最优通信效率：① 在采用 PBFT 共识的网络中，优先尽快传输所有交易消息到验证者节点，使交易能被尽快执行并打包到最新区块中，而 Gossip 协议的交易转发具有很大的随机性，无法做到这一点；② 在采用 PBFT 共识的网络中，优先将新打包的区块传输给所有的普通节点，从而缩短交易确认时间，且在区块广播的过程中主动避免向已有该区块的节点重复发送区块，以防浪费带宽网络和节点的消息处理能力.

网络优化技术可减少广播消息的数量一半以上，降低传播时延一半左右.



（a）Gossip的随机转发算法　　（b）软件定义的转发算法

图 8　采用 PBFT 共识协议的区块链网络拓扑结构中新交易信息的传输机制

Fig. 8　New block broadcasting in a PBFT based blockchain system

3　许可公链应用场景

本研究提出的许可公链既综合了现有的公链和联盟链的优点，又克服了它们各自的缺点，不仅可支持已有的各种区块链应用，还可用于以往两类系统都不支持的应用，具体表现为：

1）现有的基于公链的公众平台都是匿名非许可的，容易造成大量水军、谣言、甚至是网络攻击拒绝服务攻击等，基于手续费的手段又会增加系统的使用成本，在许可公链中，每个用户都只有一个主地址，可轻易实现对地址行为的分析与对应处理. 因此，将许可公链用于分布式论坛和共享经济平台等，可促进相关行业的发展.

2）在区块链金融系统中，需对用户进行了解客户（know-your-customer，KYC）认证，同时还要保护用户隐私，且不同的金融应用认证条件不同. 金融机构可利用安全认证（certification authority，CA）系统对用户进行 KYC 认证，然后用户基于 CA 认证信息和个人身份信息注册许可公链主地址，实现链上分布式金融应用.

3）基于许可公链的 L_2 智能合约技术可自动实现灵活的应用分组，保证应用的安全与效率，从而支持各种大规模不同需求的应用. 比如，有些高吞吐量需求的应用和高安全需求的应用在一条公链上并行部署，可互相促进，同时避免互相干扰.

结　语

本研究针对当前公链与联盟链的限制，提出许可公链的系统概念与实现方案. 重新设计了区块链的 L_0、L_1 和 L_2 层实现方案，解决了现有区块链交易速度慢的瓶颈. PPC 的开发结果表明，许可公链的架构方案可行，该架构可以将目前的区块链系统 TPS 提高 400 倍以上. 许可公链的研发将极大促进区块链应用的发展.

基金项目：国家重点研发计划资助项目（2018YFB2100705）；国家自然科学基金资助项目（61771315）
作者简介：张胜利（1978—），深圳大学教授、博士生导师. 研究方向：区块链及无线网络等. E-mail：zsl@szu.edu.cn
引　　文：张胜利，王滔滔，杨　晴，等. 高性能许可公链[J]. 深圳大学学报理工版，2020，37(3)：227-233.

参考文献 / References:

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [DB/OL]. (2008-10-31) [2019-10-02]. http://bitcoin.org, 2008.

[2] GARAY J A, KIAYIAS A, LEONARDOS N. The bitcoin backbone protocol: analysis and applications [C]// Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia: Springer, 2015: 281-310.

[3] PASS R, SEEMAN L, SHELAT A. Analysis of the blockchain protocol in asynchronous networks [C]// Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Paris: Springer, 2017: 643-673.

[4] FERRAG M A, DERDOUR M, MUKHERJEE M, et al. Blockchain technologies for the internet of things: research issues and challenges [J]. IEEE Internet of Things Journal, 2018, 6(2): 2188-2204.

[5] FANNING K, CENTERS D P. Blockchain and its coming impact on financial services [J]. Journal of Corporate

Accounting & Finance，2016，27(5)：53-57.

[6] DAI Hongning，ZHENG Zibin，ZHANG Yan. Blockchain for internet of things：a survey [J]. IEEE Internet of Things Journal，2019，6(5)：8076-8094.

[7] KETHINENI S，CAO Ying，DODGE C. Use of bitcoin in dark net markets：examining facilitative factors on bitcoin-related crimes [J]. American Journal of Criminal Justice，2018，43(2)：141-157.

[8] FENU G，MARCHESI L，MARCHESI M，et al. The ICO phenomenon and its relationships with Ethereum smart contract environment [C]// Proceedings of 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). Campobasso，Italy：IEEE，2018：26-32.

[9] WANG Wenbo，THAI H D，XIONG Zehui，et al. A survey on consensus mechanisms and mining strategy management in blockchain networks [J]. IEEE Access，2019，7：22328-22370.

[10] DECKER C，WATTENHOFER R. Information propagation in the bitcoin network [C]// Proceedings in the 13th International Conference on Peer-to-Peer Computing. Trento，Italy：IEEE，2013：1-10.

[11] SOMPOLINSKY Y，ZOHAR A. Accelerating bitcoin's transaction processing. Fast money grows on trees，not chains [DB/OL]. (2013-12-31) [2017-10-22]. https://eprint.iacr.org/2013/881.pdf.

[12] SOMPOLINSKY Y，ZOHAR A. Secure high-rate transaction processing in bitcoin [C]// Proceedings of International Conference on Financial Cryptography and Data Security. San Juan，Puerto Rico：Springer，2015：507-527.

[13] RIZUN P R. Subchains：a technique to scale bitcoin and improve the user experience [J]. Ledger，2016，1：38-52.

[14] BAGARIA V，KANNAN S，TSE D，et al. Deconstructing the blockchain to approach physical limits [EB/OL]. (2018-10-18) [2019-10-02]. https://arxiv.org/abs/1810.08092v1.

[15] SOMPOLINSKY Y，LEWENBERG Y，ZOHAR A. Inclusive block chain protocols [C]// Proceedings of the 19th International Conference on Financial Cryptography and Data Security. San Juan，Puerto Rico：Springer，2015：528-547.

[16] SOMPOLINSKY Y，LEWENBERG Y，ZOHAR A. SPECTRE：a fast and scalable cryptocurrency protocol [DB/OL]. (2016-12-18) [2018-01-15]. https://eprint.iacr.org/2016/1159.

[17] YONATAN S，WYBORSKI S，ZOHAR A. PHANTOM and GHOSTDAG：a scalable generalization of Nakamoto consensus [J]. IACR Cryptology ePrint Archive，2018，2018：104.

[18] LI Chenxing，LI Peilun，ZHOU Dong，et al. Scaling Nakamoto consensus to thousands of transactions per second [DB/OL]. (2018-05-10) [2018-08-31]. https://arxiv.org/pdf/1805.03870.pdf.

[19] EYAL I，GENCER A E，SIRER E G，et al. Bitcoin-NG：a scalable blockchain protocol [C]// Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation. Berkeley，USA：USENIX Association，2016：45-59.

[20] PASS R，SHI E. Fruitchains：a fair blockchain [C]// Proceedings of the ACM Symposium on Principles of Distributed Computing. Washington D C：ACM，2017：315-324.

[21] RAFAEL P，ELAINE S. Hybrid consensus：efficient consensus in the permissionless model [C]// The 31st International Symposium on Distributed Computing. Dagstuhl，Germany：Schloss Dagstuhl：Leibniz-Zentrum Fuer Informatik，2017，91：39.

[22] PASS R，SHI E. Thunderella：blockchains with optimistic instant confirmation [C]// Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin：Springer，2018：3-33.

[23] LUU L，NARAYANAN V，ZHENG Chaodong，et al. A secure sharding protocol for open blockchains [C]// Proceedings of ACM SIGSAC Conference on Computer and Communications Security. Vienna：ACM，2016：17-30.

[24] HUANG Dongyan，MA Xiaoli，ZHANG Shengli. Performance analysis of the raft consensus algorithm for private blockchains [J]. IEEE Transactions on Systems，Man and Cybernetics：Systems，2019，50(1)：172-181.

[25] MAYMOUNKOV P，MAZIÈRES. Kademlia：a peer-to-peer information system based on the XOR metric [C]// Proceedings of the 1st International Workshop on Peer-to-Peer Systems. Cambridge，USA：Springer，2002：53-65.

【中文责编：张　英；英文责编：木　柯】