doi:10.11887/j.cn.202403024 http://journal.nudt.edu.cn

区块链技术下的智能安全可靠支付系统设计

张艳硕*,刘 宁,刘天野,陈 颖,张黎仙
(北京电子科技学院 密码科学与技术系,北京 100070)

摘 要:为了增强支付系统的安全性和可靠性,设计了一种区块链技术下的智能支付系统。这个系统利用区块链的去中心化和分布式账本特性,提供了一种更加安全和透明的支付解决方案。系统将区块链技术、国密算法与支付系统相结合,给传统互联网支付系统提供一个更安全的保障。利用区块链技术的点对点特点,解决支付效率和数据安全等方面的问题。借助互联网大数据技术,对用户进行信用评级,提供信贷服务。结合跨链技术可以对不同区块链的数据进行共享,更好地解决资金流动性。相比比特币和以太坊等电子货币系统,该系统在安全性、交易吞吐率和交易时延等方面做到了权衡发展,使得各方面的性能有了一定程度的均衡提升,更能满足当前环境下的应用需要。

关键词:区块链;共识机制;支付系统;安全;智能
中图分类号:TN911.7 **文献标志码**:A **开放科学(资源服务)标识码(OSID)**:
文章编号:1001-2486(2024)03-237-10

Design of intelligent security and reliable payment system based on blockchain technology

*ZHANG Yanshuo**, *LIU Ning*, *LIU Tianye*, *CHEN Ying*, *ZHANG Lixian*
(Department of Cryptography and Technology, Beijing Electronic Science & Technology Institute, Beijing 100070, China)

Abstract: In order to enhance the security and reliability of the payment system, an intelligent payment system under blockchain technology was designed. This system leverages the decentralized and distributed ledger nature of blockchain to provide a more secure and transparent payment solution. The system combined blockchain technology, state secret algorithm and payment system to provide a more secure guarantee for the traditional internet payment system. The point-to-point characteristics of blockchain technology was used to solve the problems of payment efficiency, data security, etc. With the help of big data technology of internet, credit rating was provided to users and credit services are provided. Using trans-chain technology, the data of different blockchains can be shared to figure out a better solution to the liquidity of funds. Compared with Bitcoin, Ethereum and other electronic money systems, the system has achieved a balanced development in terms of security, transaction throughput and transaction delay, which has improved the performance of all aspects to a certain extent, and can better meet the application needs in the current environment.

Keywords: blockchain; consensus mechanism; payment system; security; intelligence

作为具有颠覆性潜力的互联网技术,区块链在近年来得到了快速发展。以比特币为首的数字加密货币已经获得了广泛的市场认可,吸引了工程应用领域关注并在其领域进行了布局[1]。Nakamoto[2]发表区块链技术的奠基性论文,同时率先提出比特币。2013年Buterin[3]发布以太坊白皮书,并上线以太坊区块链应用平台,将智能合约应用到区块链服务平台中。2015年由Linux基金会主导发起了Hyperledger区块链项目。以IBM为主要贡献者开发的Hyperledger Fabric[4]成为其中最重要的子项目。2016年Eyal等[5]提出Bitcoin-NG共识机制,旨在提升比特币处理交易的能力。2017年Kiayias等[6]提出Ouroboros共识机制,利用形式化的方法建立了权益证明(proof of stake,PoS)共识机制的模型,并证明了Ouroboros能够满足安全性。2018年Kokoris-Kogias等[7]提出Omniledger共识机制,解决了分片共识中存在的问题。2019年Wang等[8]提出Monoxide共识机制,通过构建异步共识组来拓展区块链应用。

但针对比特币和以太坊等电子货币系统存在的交易吞吐率低,交易确认时间长等问题一直受

收稿日期:2022-01-20
基金项目:国家重点研发计划基金资助项目(2017YFB0801803);国家自然科学基金资助项目(62002003)
*第一作者:张艳硕(1979—),男,陕西宝鸡人,副教授,博士,硕士生导师,E-mail:zhang_yanshuo@163.com

到行业内部的诟病[9]，同时其无法支持信用借贷的问题也限制着当前应用环境，无法较好地满足当下用户的多样化需求。

针对以上问题，本文提出了基于区块链技术的智能安全可靠支付系统，使用区块链技术完成即时支付、延时支付、分期支付和信用借贷等功能，利用国密算法增强安全性；设计了混合共识机制提高系统安全性和交易吞吐率，优化权限管理保证数据的私密性；提供了信用借贷功能促进资金的流动性，同时满足用户个性化需求。相比比特币和以太坊等电子货币系统，本系统在安全性、交易吞吐率和交易时延等方面做到了权衡发展，使得各方面的性能有了一定程度的均衡提升，更能满足当前环境下的应用需要。

1 支付系统

互联网支付系统利用移动技术、云计算、搜索引擎等互联网资源，实现了一种便捷的移动支付解决方案，它代表了互联网技术与传统金融交易结合的新兴趋势。这种系统使得用户能够通过互联网轻松完成债务偿还和资金转账。

然而，当前的互联网支付系统及安全性仍有所欠缺，黑客攻击、服务器宕机以及硬盘等时有发生，这都将阻碍互联网支付系统的发展[10]。参与互联网支付的移动终端需要考虑设备硬件、操作系统和应用程序等安全问题，风险防控工作十分复杂且艰难。

2 区块链技术

2.1 区块链简介

狭义上区块链被定义为一种链式数据结构，通过时间顺序连接的区块组成，并利用哈希函数确保数据的不可篡改性和真实性，形成一种分布式账本技术。而从广义角度来看，区块链是一种创新的分布式基础设施和计算模式[11]。区块链通过块链结构来存储数据，借助共识机制确保节点间数据的一致性，借助密码技术让数据能够在不可信的信道中安全传输，利用智能合约编程和操作数据。

2.2 技术优势

区块链之所以能够在众多领域大放异彩，正是得益于它的去中心化、信息透明、合约智能化以及可追溯性等诸多优势[12]。利用其技术特点可构建一个安全可靠的区块链应用系统。

去中心化。中心数据库在传统的网络系统中得到了广泛的应用，然而区块链技术创新地将数据以去中心化的方式进行存储、管理[13]，并通过共识机制来保障账本信息的一致性。

信息透明。基于区块链技术的系统中的去中心化数据库对所有用户进行开放。用户可向节点发送查询请求来获取相关数据。

合约智能化。智能合约是运行在区块链节点上的程序代码，当智能合约预设的条件被触发时，合约条款将自动执行[14]。本文系统可以通过运行相关节点上的程序代码，实现合约智能化。

可追溯性。区块链中每一个区块都承载了上一个区块的 Hash 值，把 Hash 值当作索引将所有区块按顺序连接。这种方式使得数据具备防篡改能力以及可追溯能力[15]。

3 智能安全可靠支付系统

3.1 方案设计

智能安全可靠支付系统分为数据层、网络层、共识层、激励层、合约层和应用层，其层级架构如图 1 所示。

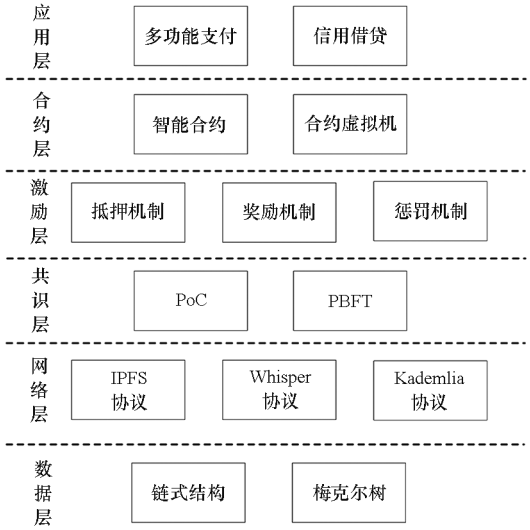

图 1 智能安全可靠支付系统层级架构

Fig. 1 Hierarchical architecture of intelligent secure and reliable payment system

在数据层主要使用了 Merkle Tree 来进行大规模交易数据校验，同时使用链式结构对区块数据进行存储。在网络层采用了 Kademlia 协议[16]进行 P2P(peer to peer)网络的构建，使用 Whisper 协议[3]进行消息的传递与分发。考虑到互联网的发展趋势，本文设计的支付系统在网络层同时使用了星际文件系统(inter planetary file system，IPFS)协议[17]作为拓展协议，时机成熟时可进行协议切换。在共识层采用了贡献量证明(proof of contribution，PoC)机制 + 实用拜占庭容错(practical

Byzantine fault tolerance, PBFT) 机制的混合共识机制来进行区块共识,在满足高安全性的同时保障了交易的低时延和高吞吐率。在激励层上结合了抵押机制、奖励机制和惩罚机制,确保区块链网络的节点能够按照规定的方式正常运行。在合约层建立了智能合约虚拟机和图灵完备的智能合约脚本,增强系统的可拓展性。在应用层实现了多功能支付模块以及信用借贷模块,以满足用户的个性化需求。

3.1.1　智能合约子系统

智能合约概念于 1994 年由 Szabo[18] 提出。智能合约是一种计算机协议,采用信息化方式传达、验证和执行合同条款,使得在无须第三方介入的情况下,能够实施可信交易。

在本文设计的支付系统中,智能合约作为一个重要的子系统,管理和控制区块链中交易的执行情况。可根据用户指定的交易规则和逻辑生成合约代码,在约定条件触发后自动执行,无须人为的干预和第三方监管。

3.1.2　混合共识机制

共识机制作为区块链的核心技术,能够保障区块链数据库的一致性和正确性[19]。为了满足第三方支付系统的安全性、可靠性和高效性要求,本文设计了一种混合共识机制,结合了 PoC 和 PBFT 机制。这种机制可以更好地适应现实应用场景的需求。

薛腾飞[13] 基于工作量证明(proof of work, PoW)提出了 PoC 共识机制。PoC 共识机制是对 PoW 共识机制的扩展,能够结合奖励、惩罚机制维护区块链网络的稳定性和公平性。在混合共识机制中 PoC 共识机制作用于 PBFT 机制中的主节点选取过程。

符号定义如表 1 所示。

对于不同节点,根据其对系统的贡献量计算奖励系数,进行主节点竞争时相应地降低目标难度。奖励系数 α 的计算如式(1)所示:

$$\alpha=\begin{cases}\dfrac{1}{m+\mathrm{e}^{\frac{-(c-\mu)}{\gamma}}}, c\geqslant 1\\ 1, c=0\end{cases} \tag{1}$$

衡量一个节点是否为诚实节点,需要利用该节点参与记账的历史记录来计算该节点的可信概率 P,即:

$$P=\begin{cases}\dfrac{c}{s}, s\geqslant 1\\ 0.5, s=0\end{cases} \tag{2}$$

表 1　符号定义

Tab. 1　Symbol definitions

符号	含义
α	奖励系数
c	成功记账次数
s	记账次数
m	奖励最大倍数系数
μ	曲线均值系数
γ	收敛系数
P	节点可信概率
P_{n-1}	竞争到第 $n-1$ 次记账权的节点的可信概率
D	全网目标难度
D_n	节点竞争第 n 次记账权的目标难度
D_{new}	调整后的目标难度
D_{old}	调整前的目标难度
t_0	自上一次调整难度起至第 2 016 个区块生成经历的时间
n'	自上一次调整难度起系统中生成的孤块数量
n_0	常数 2 016
S_{n_0}	常数 2 016 × 10 min

为了激励网络节点进行诚实记账,系统将对诚实节点进行奖励,通过调节竞争记账的目标难度 D_n,延长其记账时间从而使其获得更多的交易手续费,即:

$$D_n=D\cdot\alpha^{-1}\cdot P_{n-1} \tag{3}$$

全网目标难度 D 由全网算力共同决定,并定期调整。与比特币系统不同的是,本系统在调整难度时会考虑到网络中潜在的自私挖矿节点,系统产生的孤块也将成为系统调整难度的参考对象,这样能充分反映出系统中的真实算力[20]。调整后的目标难度 D_{new} 计算如式(4)所示:

$$D_{\text{new}}=D_{\text{old}}\cdot\frac{(n_0+n')t_0}{S_{n_0}} \tag{4}$$

运行混合共识机制时,第一步是确定主节点,通过计算工作量证明最快的节点成为主节点,其他节点成为从节点。主节点和从节点使用 PBFT 机制实施交易信息的接收、验证以及上链操作。PBFT 的工作流程如图 2 所示[21]。

在这个协议中,有客户端 C,还有服务节点 $N_0\sim N_3$,其中包括主节点 N_0、从节点、故障节点 N_3。令故障节点数量为 f,整个服务节点数量为 $|R|=3f+1$。协议具体操作如下。

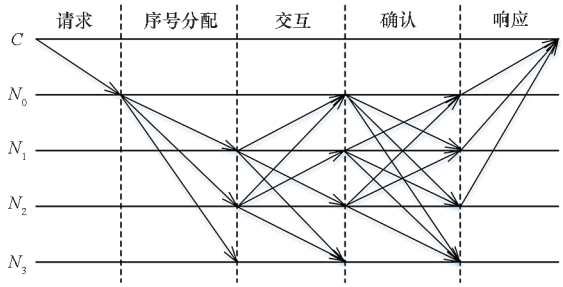

图2 PBFT共识流程

Fig. 2 PBFT consensus process

1)客户端发送交易请求消息 m,触发主节点的服务操作;

2)序号分配阶段,主节点产生序列号 n,并将其分配给 m,接着把 PRE-PREPARE 消息广播给其他节点;

3)交互阶段,接收到节点的 PRE-PREPARE 消息后,借助主节点的公钥验证消息的真实性,验证通过后,向其他服务节点广播 PREPARE 消息;

4)序号确认阶段,当所有节点都收到 $2f+1$ 个 PREPARE 消息后,广播 COMMIT 消息,并执行客户端的请求,然后对客户端进行响应;

5)客户端等待来自不同节点的响应,把 $f+1$ 个相同的响应结果当作请求的处理结果。

该区块链系统采用了混合共识机制,结合了 PoC 和 PBFT,因此区块结构也需要相应的设计,如图3所示。具体地,系统使用了2条链:PoC 链和 PBFT 链,分别用于记录竞争区块和交易区块。在区块的内容设计上,需要注意2条链中的 Hash 值相互引用,实现了双重确认,从而使数据的完整性以及安全性得到进一步提高。

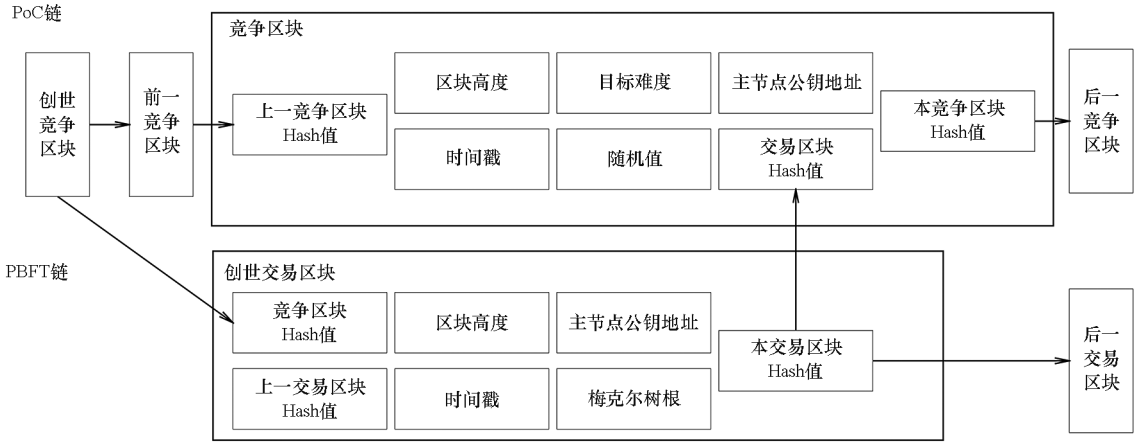

图3 区块结构

Fig. 3 Block structure

3.1.3 密态账本

密态账本技术是一种将账本信息以密文形式在区块链节点间进行存储和验证的技术。每个节点在区块链网络中都保留着一份加密过的完整账本,而且每个节点都有独特的密钥,这样设计可以降低账本信息泄露的风险。密态账本采用时空证明(proof of space time,PoST)的方式进行实现,通过时空证明可以验证该时间段内节点存储了相应的账本数据[22]。实现 PoST 需要采用一种特殊的可验证时延加密(verifiable time-delay encoding function)算法,满足加密时间长、解密时间短且证明与验证过程高效的特性,因此该系统通过 BLS12-381 加密算法[23]进行加密。各节点之间会定期实施轮询操作,借助时空证明来确保各节点数据的完整性。

3.1.4 支付子系统

支付子系统负责向用户提供支付相关的操作接口,针对现实应用场景中各种复杂的情况,在此模块中设计实现了即时支付、延时支付和分期支付三种支付方式。

1)即时支付模块。即时支付是指用户创建一笔合法交易后,交易立即被区块链系统确认生效。具体过程为:

①用户创建交易信息,并用自己的私钥进行签名,保证其真实性和完整性。

②该交易在区块链系统中被广播。

③矿工节点确认后交易立即生效。

2)延时支付模块。延时支付是指用户创建一笔合法交易后,交易会被区块链系统挂起,延时结束后确认生效,其间用户可以取消交易。此类支付方式主要用于大额交易,以防止交易误操作的情况发生。具体过程为:

①用户创建智能合约,并填入交易信息。借鉴以太坊 Gas Limit[3]的设计理念,合约中设

置 Gas 值,延时越长,Gas 值越大。其中 Gas 是以太坊中的工作量成本单位,用于计量在以太坊区块链上执行操作所需的计算、存储资源和带宽。

②若延期时间内用户对该笔交易无异议,则时间到后智能合约自动执行,发送交易,并将未消耗的 Gas 返还给付款方。若延期时间内用户发现交易有问题,需要取消交易,则向智能合约发送预先设定的取消命令,智能合约瞬间进入死循环,将 Gas 消耗完,合约失效,交易未发送。

3)分期支付模块。分期支付是指用户创建一笔合法交易后,交易会按照约定的方式被区块链系统分多次确认生效。具体过程为:

①用户创建智能合约,并填入分期交易信息。但是分期支付的智能合约没有预设的取消接口,一旦发布将不能取消,直到还款完毕。

②根据约定的还款日期,智能合约自动执行还款交易操作。

3.1.5　信用借贷

用户可向银行节点(Bank)提出信贷请求,并提供自己的公钥地址(Original Address)和身份信息。Bank 会根据链上信息推算该地址的财富总量以及资金流动情况,同时 Bank 向联盟链上的其他银行节点查询该申请人的信用状况,据此提供给申请人相应的额度。

审核后 Bank 会生成一个贷款专用公私钥对,同时颁发给申请人一张许可证(License),并使用 Bank 的私钥进行签名认证。未来,许可证将包含每次交易的 Hash 值,以便进行对账。在进行信用支付时可使用 Bank 返回的贷款专用公钥地址 Private Address 作为付款账户。

假设 User 从 Bank 获得信用额度后,期望在 Store 购买某件商品。考虑到现实场景,支付过程分为两种情况,即 Bank 在线和离线,具体支付流程如图 4 所示。

1)Bank 在线情况下的支付过程。Bank 在线情况下的支付流程图,如图 4 上半部分所示,具体流程如下:

①User 构造一个包含 License、支付金额、Store 收款地址、私钥签名的数据包发送给 Store。Store 借助 Bank 的签名来验证 License 的真实性。通过 License 中的 Original Address 验证 License 没有被冒用。然后查找区块链中 User 的 Private Address 中的最近一笔交易与 License 中的记录是否一致,验证 License 剩余数额的真实性。

②Store 将 User 发送的数据包转发给 Bank。

③Bank 会首先核对 Store 发送的 License,以确认与自身记录的一致性。如果 License 与银行记录不一致,表示 User 在上次支付后进行过离线支付。Bank 将要求 User 出示票据以供核对。之后,Bank 会检查 License 中的剩余额度是否足以支付本次交易。如果足够,Bank 会先将款项转入 Private Address,接着再从 Private Address 向 Store 支付这笔款项。

④Bank 会在 License 中增加该笔交易信息,然后重新签名,修改后的 License 也会被返回给 User。

2)Bank 不在线情况下的支付过程。Bank 离线情况下的支付流程图,如图 4 下半部分所示,具体流程如下:

①此步骤与 Bank 在线支付相同,不再赘述。

②Bank 不在线时,Store 会综合考虑 Bank 和 User 的信用度,决定是否接收该支票(Cheque)。

③Store 将 Cheque 广播到区块链网络,同时创建智能合约,一旦 Bank 上线,智能合约自动提醒 Bank 完成该交易。

④User 在支付完成后会将该交易记录至 License 中并进行签名。

⑤Bank 上线后,当合约通知 Bank 完成支付时,Bank 通过查询区块链,找出尚未兑现的 Cheque。然后依据 Cheque 在区块链中的先后顺序向 Store 付款。

⑥Bank 向 User 索要 License 进行交易核对。核对后对 License 进行签名。

User 需在有效期(Duration)内进行还款。User 也可向 Bank 申请延期还款,并支付服务费。延期时间与申请额度的关系如式(5)所示。

$$B = 15 + \log_2 A \tag{5}$$

其中,B 的单位为天,A 的单位为元。期满时,若借款人仍未还款,Bank 会在借款人的信用记录里记录一次逾期未还款的情况。借款人在还清欠款时,需要支付一笔滞纳金作为惩罚。这个滞纳金 P 的计算考虑了借款人的信用情况、欠款金额 A 以及迟还时间 D。P 的计算如式(6)所示:

$$P = \beta \times D \times r \times A \tag{6}$$

其中,β 为正比例系数,r 为利率。β 的计算如式(7)所示:

$$\beta = \begin{cases} \dfrac{x}{x+y} \times a, y \neq 0 \\ b, y = 0 \end{cases} \tag{7}$$

其中,x 表示 User 成功还款的次数,y 表示 User 逾期未还的次数,a、b 为正比例系数。

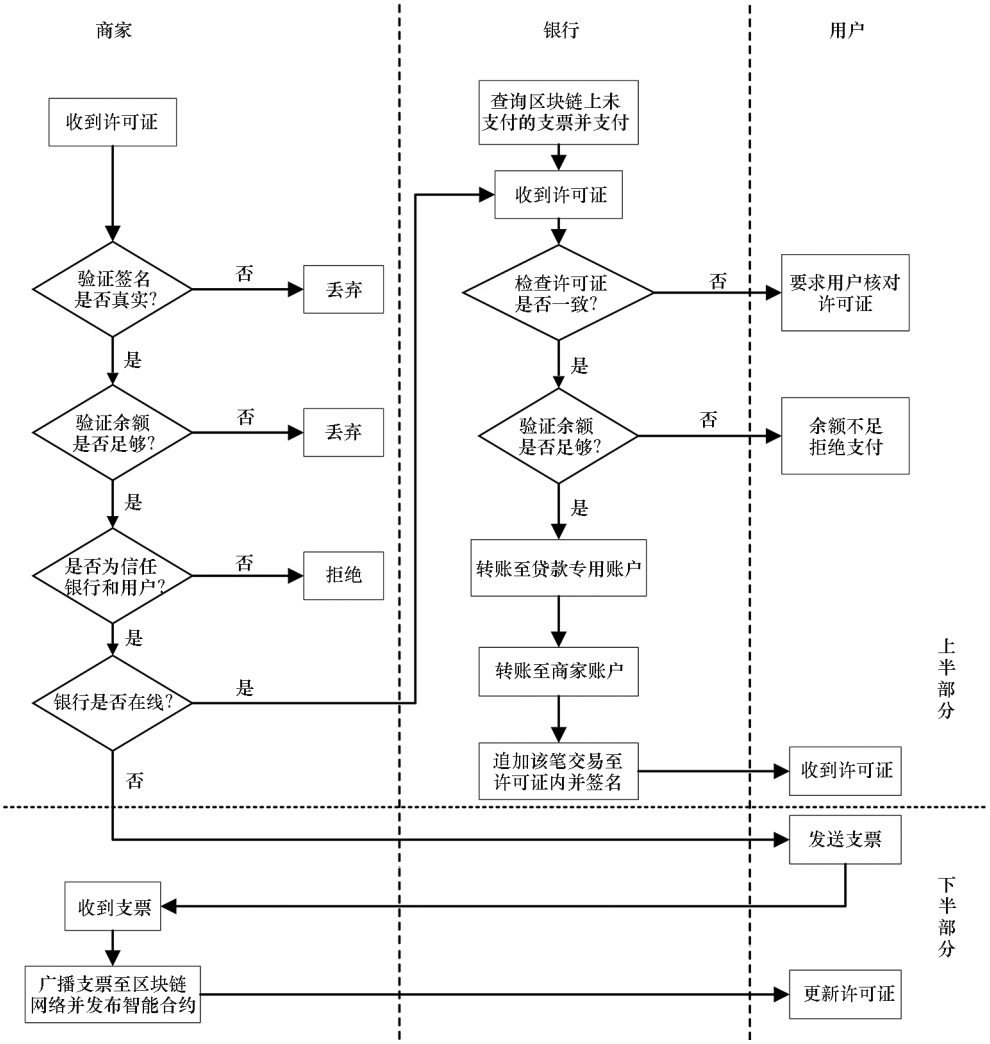

图 4　信用支付流程

Fig. 4　Credit payment process

3.2　系统特色

系统采用联盟链技术设计了安全数据存储系统和联盟链准入标准,使得节点的安全防护能力变得相对较强。除此之外,系统在多功能支付与信用借贷、混合共识机制、信任与弹劾机制等方面进行了创新优化。

1)多功能支付与信用借贷。系统通过构建模型,不仅实现了多功能支付,还实现了信用借贷功能。通过计算借方信用积分建立借贷信息库,再通过实现借贷双方的操作算法完成信用借贷功能。

2)混合共识机制。系统采用 PoC + PBFT 的混合共识机制进行区块共识,结合了 PoC 高安全性和 PBFT 高效性的优点,在满足高安全性的前提下大幅提高了交易吞吐率。若要完成系统攻击,不仅要掌握全网 51% 的算力,还要掌握全网 1/3 的节点,这在联盟链环境下基本不可能实现。

3)信任与弹劾机制。系统采用了信任与弹劾机制,有效地提高了系统的容错度。每个节点都会维护一张全网节点的信用表,若当前主节点的总处理错误率小于某个阈值,全网节点将认定该主节点为诚实节点,并提高 PoC 机制中的当前难度目标值,从而赋予当前主节点更多的交易认证时间。若当前主节点本次交易处理错误率大于 50%,全网节点将认定该节点为恶意节点,全网从节点将会降低 PoC 机制中的难度目标值,瞬间完成主节点的切换。此为本系统应用的弹劾机制。

3.3　系统对比

采用对比分析方法将本系统与比特币[2]、以太坊[3]、Hyperledger Fabric[4]、ByzCoin[24] 和 Algorand[25] 等数字加密货币系统进行横向比较,测试环境如表 2 所示,对比结果如表 3[26] 所示。

通过对本系统在不同节点数量情况下的综合表现可以看出,随着节点数量的增加,区块链网络规模和复杂程度显著提高,单笔交易在网络中的

表 2　测试环境

Tab. 2　Test environment

节点数量	系统	CPU	内存/GB	网络带宽/(Mbit/s)
20	Windows 10	Inter I5 8500 3.0 GHz	16	100
100	Windows 10	Inter I5 8500 3.0 GHz	16	100
500	Windows 10	Inter I5 8500 3.0 GHz	16	100

表 3　系统对比

Tab. 3　System comparison

系统	强共识	共识算法	敌手模型	吞吐率/(Tx/s)	时延/s
本系统(20 节点)	√	PoC + PBFT	$n=4f+1$	1 000	2
本系统(100 节点)	√	PoC + PBFT	$n=4f+1$	1 100	2.3
本系统(500 节点)	√	PoC + PBFT	$n=4f+1$	1 300	4
比特币	×	PoW	$n=2f+1$	7	600
以太坊	×	PoW/PoS	$n=2f+1$	20	60
Hyperledger Fabric	√	BFT	$n=3f+1$	3 000	0.8
ByzCoin	√	PoW + PBFT	$n=4f+1$	974	25
Algorand	√	PoW + BFT	$n=3f+1$	≈1 000	<60

传播时间和确认时延随之增加,因此需要调整好吞吐率、时延和节点数量之间的平衡。

根据对比结果可以看出,本系统在交易吞吐率和交易时延上要明显优于比特币等支付系统,在去中心化方面要优于 Hyperledger Fabric 等采用单一共识机制的分布式账本平台。

4　安全性分析

4.1　形式化安全性证明

基于区块链技术的支付系统面临的安全风险主要体现在验证交易真实性上,而数字签名是验证交易真实性的重要手段,因此本小节重点对数字签名方案进行安全性分析。

本文采用的 ECDSA-SM2 数字签名方案[27]。对于任一数字签名方案(SignGen, Sign, Vrfy),敌手 A 有如下 4 个(伪造级别依次增加)目标:

1)存在性伪造(existential forgery):敌手以不可忽略的概率成功伪造签名,但其伪造的签名所对应的消息很可能无意义。

2)选择性伪造(selective forgery):敌手成功伪造部分自己选择明文的有效签名。

3)一般性伪造(universal forgery):敌手在不知道私钥的情况下伪造任意消息的签名。

4)完全破译(total break):敌手找到私钥。

敌手 A 的两类攻击:未知消息攻击和已知消息攻击。后一种情况中最强的攻击是"适应性选择消息攻击",即 A 可以向签名方询问除预伪造消息以外的任何消息的签名,因而可能根据以前的答案适应性地修改随后的询问[28]。

一个数字签名方案,如果在任何多项式有限时间内,敌手 A 在适应性选择消息攻击下的优势是可以忽略的,则称该方案在适应性选择消息攻击下具有存在性不可伪造性(existential unforgeability against adaptive chosen messages attacks, EUF-CMA),简称为 EUF-CMA 安全。

设 H 是一个随机预言机(random oracle),如果与 GenSM2 相关的椭圆曲线离散对数问题(elliptic curve discrete logarithm problem, ECDLP)是困难的,则 ECDSA-SM2 方案是 EUF-CMA 安全的。

具体来说,假设存在一个 EUF-CMA 敌手 A 以 $\varepsilon(\kappa)$ 的优势攻破 ECDSA-SM2 方案,A 最多进行 q_{H} 次 H 询问,那么一定存在一个敌手 B 至少以 $Adv_{\mathrm{B}}^{\mathrm{E}}(k)\geqslant\frac{\varepsilon(\kappa)}{\mathrm{e}q_{\mathrm{H}}}$ 的优势解决 ECDLP 问题,其中 e 是自然对数的底[29]。

对 EUF 游戏进行如下描述:

1) 挑战者通过 $G_{\mathrm{enSM2}}(\kappa)$ 生成 (Q,d),其中 Q 是公钥,d 是私钥。选取一个随机函数 H。敌手 A 获取公钥 Q。

2) 敌手 A 能够对挑战者请求 $H(\cdot)$ 以及对消息的签名,挑战者在收到请求后向 A 返回 $\sigma=\mathrm{Sign}_d(H(M))$,$\sigma$ 分为 (r,s) 两部分。

3) A 输出一个消息,即签名对 (M,σ),其中消息 M 的签名没有经过请求。如果 $V_{\mathrm{rfyQ}}(\sigma)=H(M)$,则攻击成功。

下面证明 ECDSA-SM2 方案可归约到 ECDLP 问题。

敌手 B 已知 (Q,y^*),其中 y^* 是 $\mathbb{Z}_n^*$ 上均匀随机的。以 A(攻击 ECDSA-SM2 方案)作为子程序,目标是计算 $\mathrm{Sign}_{Q^{-1}}(y^*)$。

分析:B 若能得到某个 σ,使得 $y^*=V_{\mathrm{rfy}Q}(\sigma)$,则 $\sigma=\mathrm{Sign}_{Q^{-1}}(y^*)$。由 $y^*=V_{\mathrm{rfy}Q}(\sigma)$ 知,若 y^* 是某个消息 M 的 Hash 函数值,则 σ 为

这个消息的签名。(M,σ)通过敌手 A 生成,但是 $H(M)$通过 B 生成,B 可设 $H(M)=y^*$。当 B 把 y^*当作某个消息的 Hash 值时,并不知道 A 对哪条消息伪造了签名,因此 B 需要进行猜测(A 的第 j 次 H 询问对应着 A 最终的伪造结果)。

归约过程如下:

1) B 将公钥 Q 给 A 且随机选择 $j\leftarrow_R\{1,2,\cdots,q_H\}$。$j$ 是 B 的一个猜测值:A 的第 j 次 H 询问对应着 A 最终的伪造结果。

2) H 询问(最多进行 q_H 次)。B 建立一个 H^{list},初始为空,元素类型为三元组(M_i,σ_i,y_i),表示 B 已经设置 $H(M_i)=y_i$,$V_{rfyQ}(\sigma_i)=y_i$。当 A 发起第 i 次询问(设询问值为 M_i)时,B 回答:

①如果 $i=j$,返回 y^*。

②否则,选取一个随机值 $\sigma_i\leftarrow_R\mathbb{Z}_n^*$,计算 $y_i=V_{rfyQ}(\sigma_i)$,以 y_i 作为对该询问的应答,并在表中存储(M_i,σ_i,y_i)。

3) 签名询问(最多进行 q_H 次)。当 A 请求消息 M 的一个签名时,设 i 满足 $M=M_i$,M_i 代表第 i 次 H 询问的询问值。B 会做出如下回应:

①如果 $i\neq j$,则 H^{list}中有一个三元组(M_i,σ_i,y_i),返回 σ_i。

②如果 $i=j$,则中断。

4) 输出:A 输出(M,σ)。若 $M\neq M_j$,B 中断;否则若 $M=M_j$ 且 $y^*=V_{rfyQ}(\sigma)$,B 输出 σ。

当 B 猜测正确时,A 在上述归约中的视图与其在真实攻击中的视图是同分布的。原因如下:

1) A 的 q_H 次 H 询问中的每一个都是用随机值来回答的:

①对 M_j 的询问是用 y^* 来应答的,其中 y^* 在 $\mathbb{Z}_n^*$ 上是均匀分布的。

②对 $M_i(i\neq j)$的询问是用 $y_i=V_{rfyQ}(\sigma_i)$来应答的,其中 σ_i 是从 $\mathbb{Z}_n^*$ 上均匀随机选取的,y_i 在 $\mathbb{Z}_n^*$ 中也是均匀分布的。在真实攻击中,H 被视为随机预言机。所以 A 的 H 询问的应答和真实攻击中的应答是同分布的。

2) A 对 $M_i(i\neq j)$的签名询问得到的应答 σ_i 满足 $V_{rfyQ}(\sigma_i)=y_i=H(M_i)$,是有效的。所以 A 在上述归约中的视图与其在真实攻击中的视图是同分布的,即 B 的模拟是完备的。如果 B 的猜测是正确的,并且 A 成功输出一个伪造签名,那么 B 就解决了给定的 ECDLP 实例。B 成功的条件取决于以下三个事件:

α_1:B 在 A 的签名询问中不中断。

α_2:A 产生一个有效的消息,即签名对(M,σ)。

α_3:α_2 发生且 M 对应的三元组(M_i,σ_i,y_i)中下标 $i=j$。$\Pr[\alpha_1]=\left(1-\frac{1}{q_H}\right)^{q_H}$,$\Pr[\alpha_2|\alpha_1]=\varepsilon(\kappa)$,而 $\Pr[\alpha_3|\alpha_1\alpha_2]=\Pr[i=j|\alpha_1\alpha_2]=\frac{1}{q_H}$。所以 B 的优势为:

$$\begin{aligned}\Pr[\alpha_1\alpha_3]&=\Pr[\alpha_1]\Pr[\alpha_2|\alpha_1]\Pr[\alpha_3|\alpha_1\alpha_2]\\&=\left(1-\frac{1}{q_H}\right)^{q_H}\frac{1}{q_H}\varepsilon(\kappa)\approx\frac{1}{eq_H}\varepsilon(\kappa)\end{aligned}$$

4.2 常见攻击分析

本系统为提高安全性能,采用了区块链、贡献量证明与实用拜占庭容错相结合的混合机制、联盟链应用环境和智能合约等技术,与传统互联网支付系统相比,安全性能大大增强。

1)在交易数据防篡改方面,应用 PoC + PBFT 的混合共识机制能有效避免此类攻击。如果攻击者想篡改一笔已经存储在区块链中的交易数据,类似于双花攻击。一种思路是构造一个与目标区块具有相同 Hash 值的虚假区块对系统进行欺骗攻击,从而替换原始区块。这种方式成功的前提是区块链系统使用了抗碰撞性较弱的 Hash 函数,如:MD5[30]和 SHA-1[31]等。由于本系统使用了 SM3 Hash 函数,学界目前尚未提出针对该算法可行的碰撞方案,因此可以认为构建 Hash 碰撞是不可行的。另一种思路是进行区块链分叉,使得恶意链长度大于主链长度。假设诚实节点和攻击者发现下一个区块的概率分别为 p 和 q,攻击者的潜在进展符合泊松分布,其期望值为 $\lambda=z\frac{q}{q}$(其中 z 表示攻击者落后诚实网络的区块数),攻击者使区块链分叉的概率 P 如式(8)所示:

$$P=\min\left\{1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}[1-(q/p)^{(z-k)}],1\right\}\tag{8}$$

攻击者篡改成功的概率同攻击者控制的计算能力之间存在关系,见图 5。可以看到,就算敌手掌握了系统中 1/4 的算力,只要适当选取延时确认的区块时间(如延迟 10 个区块确认信息)就依旧可以把攻击成功的概率压缩到 1%。在现实环境中,敌手通常只能掌握较有限的算力,因此敌手攻击成功的概率可以忽略不计。综上所述,可以认为方案中系统整体的安全性满足设计要求。

2)在联盟链方面,采用适当的节点准入机制可有效提高系统的整体安全级别。仲盛等[32]指出,对于公有链的区块链应用,攻击者可以利用大

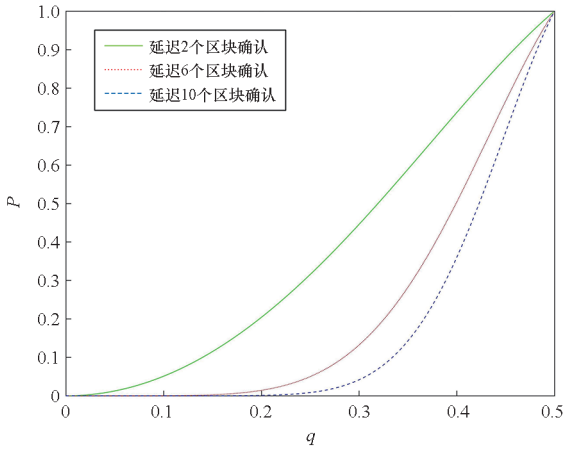

图 5　P 与 q 的关系

Fig. 5　Relationship between P and q

数据分析,描绘用户行为特征,再根据特定的数据定位到现实中的个人,导致隐私泄露。因此本系统采用了联盟链应用环境,数据通过特定的 API 函数进行脱敏后对外开放,有效降低了敏感数据泄露风险。在使用严格的身份认证机制后,恶意节点加入联盟链的概率将大大降低,也可以有效地避免隐私数据泄露问题。

3)在抵御自私挖矿方面,对全网挖矿难度进行合理的动态调整能够有效地控制自私挖矿对系统产生的不良影响。Eyal 等[33]提出当节点拥有 25%算力时,结合日蚀攻击即可完成自私挖矿。检测自私挖矿行为有三个指标,分别是孤块个数、连续区块发布时间、连续区块发布者。在 PoW 中攻击者每次公布新区块时会使用不同的地址接收奖励,这将导致"连续区块发布者"这一指标失去实际意义。但在本系统中的 PoC 机制,节点的难度奖励是基于地址的,攻击者倾向于使用相同的地址,这样可以有效地提高挖矿效率,但同时其攻击行为也更容易被检测。如果攻击者为了避免被检测使用不同的地址,这样会损失算力奖励带来的额外收益。同时本系统将孤块纳入难度调整规则中,使得目标难度更加符合系统的实际算力,从而提高了发动自私挖矿攻击的门槛,保障了系统的公平性和稳定性。

5　结论

基于区块链技术设计了智能安全可靠支付系统。在混合共识机制、密态账本、多功能支付和信用借贷等几个方面进行优化创新。系统将区块链技术、国密算法与互联网支付相结合,给传统互联网支付系统提供一个更加安全的保障。采用混合共识机制提高了交易吞吐率,优化权限管理保证数据的私密性,提供信用借贷促进资金的流动性,同时满足用户的个性化需求。系统对比传统互联网支付系统,在安全性上能够抵御黑客攻击,同时能保证用户信息不被泄露。通过对比比特币、以太坊等电子货币系统,本文系统拥有更强的交易吞吐率,能够实现交易货币的实时到账,能适应当下的市场环境。

系统在设计实现上还存在一些不足之处,需要进一步完善安全保障机制,增强原有系统的安全性能。进一步优化现有系统,提高节点间交互的性能。研究更完善的支付体系,以支持各种用户需求。

参考文献(References)

[1] 魏松杰, 吕伟龙, 李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报, 2022, 33(1): 324 - 355.
WEI S J, LYU W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1): 324 - 355.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2020 - 11 - 03)[2021 - 12 - 28]. https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf.

[3] BUTERIN V. A next-gen-eration smart contract and decentralized application platform [EB/OL]. [2021 - 12 - 28]. https://finpedia.vn/wp-content/uploads/2022/02/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[4] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EUROSYS Conference, 2018: 1 - 15.

[5] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation(NSDI'16), 2016.

[6] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Proceedings of Annual International Cryptology Conference, 2017: 357 - 388.

[7] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: a secure, scale-out, decentralized ledger via sharding[C]//Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), 2018: 583 - 598.

[8] WANG J P, WANG H. Monoxide: scale out blockchain with asynchronous consensus zones[C]//Proceedings of the 16th USENIX Conference on Networked Systems Design and Implementation, 2019: 95 - 112

[9] BIKTIMIROV M R, DOMASHEV A V, CHERKASHIN P A, et al. Blockchain technology: universal structure and requirements[J]. Automatic Documentation and Mathematical Linguistics, 2017, 51(6): 235 - 238.

[10] 陈曦, 田有亮, 马卓, 等. 商业银行移动支付安全研究[J]. 通信学报, 2014, 35(Z2): 131 - 139.
CHEN X, TIAN Y L, MA Z, et al. Research on security of mobile payment for commercial bank [J]. Journal on

Communications, 2014, 35(Z2): 131 – 139. (in Chinese)

[11] 谢辉, 王健. 区块链技术及其应用研究[J]. 信息网络安全, 2016(9): 192 – 195.
XIE H, WANG J. Study on block chain technology and its applications[J]. Netinfo Security, 2016(9): 192 – 195. (in Chinese)

[12] 孙毅, 范灵俊, 洪学海. 区块链技术发展及应用: 现状与挑战[J]. 中国工程科学, 2018, 20(2): 27 – 32.
SUN Y, FAN L J, HONG X H. Technology development and application of blockchain: current status and challenges[J]. Strategic Study of CAE, 2018, 20(2): 27 – 32. (in Chinese)

[13] 薛腾飞. 区块链应用若干问题研究[D]. 北京: 北京邮电大学, 2019.
XUE T F. Research on several issues in blockchain applications[D]. Beijing: Beijing University of Posts and Telecommunications, 2019. (in Chinese)

[14] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445 – 457.
OUYANG L W, WANG S, YUAN Y, et al. Smart contracts: architecture and research progresses[J]. Acta Automatica Sinica, 2019, 45(3): 445 – 457. (in Chinese)

[15] 陈腾. 浅谈区块链防伪溯源[J]. 互联网经济, 2018(12): 26 – 31.
CHEN T. Talking about blockchain security traceability[J]. The Internet Economy, 2018(12): 26 – 31. (in Chinese)

[16] MAYMOUNKOV P, MAZIÈRES D. Kademlia: a peer-to-peer information system based on the XOR metric[M]// DRUSCHEL P, KAASHOEK F, ROWSTRON A. Peer-to-Peer Systems. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 53 – 65.

[17] BENET J. IPFS-content addressed, versioned, P2P file system[EB/OL]. (2014 – 07 – 14)[2021 – 12 – 28]. https://arxiv.org/pdf/1407.3561.pdf.

[18] SZABO N. Formalizing and securing relationships on public networks[J/OL]. First Monday, 1997, 2(9). [2022 – 01 – 01]. https://firstmonday.org/ojs/index.php/fm/article/view/548.

[19] 谭敏生, 杨杰, 丁琳, 等. 区块链共识机制综述[J]. 计算机工程, 2020, 46(12): 1 – 11.
TAN M S, YANG J, DING L, et al. Review of consensus mechanism of blockchain[J]. Computer Engineering, 2020, 46(12): 1 – 11. (in Chinese)

[20] GRUNSPAN C, PÉREZ-MARCO R. On profitability of selfish mining[J]. [2021 – 12 – 28]. https://arxiv.org/pdf/1805.08281.pdf.

[21] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999: 173 – 186.

[22] 董天一, 戴嘉乐, 黄禹铭. IPFS 原理与实践[M]. 北京: 机械工业出版社, 2019.
DONG T Y, DAI J L, HUANG Y M. Principles and practices of IPFS[M]. Beijing: China Machine Press, 2019. (in Chinese)

[23] ARANHA D F, PAGNIN E. The simplest multi-key linearly homomorphic signature scheme[C]//Proceedings of 6th International Conference on Cryptology and Information Security in Latin America, 2019: 280 – 300.

[24] KOKORIS-KOGIAS E, JOVANOVIC P, GAILLY N, et al. Enhancing Bitcoin security and performance with strong consistency via collective signing[C]//Proceedings of the 25th USENIX Conference on Security Symposium, 2016: 279 – 296.

[25] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles, 2017: 51 – 68.

[26] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密码学报, 2019, 6(4): 395 – 432.
LIU Y Z, LIU J W, ZHANG Z Y, et al. Overview on blockchain consensus mechanisms[J]. Journal of Cryptologic Research, 2019, 6(4): 395 – 432. (in Chinese)

[27] 陈建华, 祝跃飞. SM2 椭圆曲线公钥密码算法 第2部分: 数字签名算法 GM/T 0003.2—2012[S]. (2012 – 03 – 21)[2021 – 12 – 28]. https://std.samr.gov.cn/hb/search/stdHBDetailed?id=8B1827F1DF22BB19E05397BE0A0AB44A.
CHEN J H, ZHU Y F. Public key cryptographic algorithm SM2 based on elliptic curves: part 2: digital signature algorithm: GM/T 0003.2—2012[S]. (2012 – 03 – 21)[2021 – 12 – 28]. https://std.samr.gov.cn/hb/search/stdHBDetailed?id=8B1827F1DF22BB19E05397BE0A0AB44A. (in Chinese)

[28] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743 – 1756.
FENG D G. Research on theory and approach of provable security[J]. Journal of Software, 2005, 16(10): 1743 – 1756. (in Chinese)

[29] 杨波. 密码学中的可证明安全性[M]. 北京: 清华大学出版社, 2017.
YANG B. Cyberspace security[M]. Beijing: Tsinghua University Press, 2017. (in Chinese)

[30] WANG X Y, FENG D G, LAI X J, et al. Collisions for hash functions MD4, MD5, HAVAL – 128 and RIPEMD[EB/OL]. (2004 – 08 – 17)[2021 – 12 – 28]. https://eprint.iacr.org/2004/199.pdf.

[31] WANG X Y, YIN Y L, YU H B. Finding collisions in the full SHA – 1[M]//Advances in Cryptology-CRYPTO 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 17 – 36.

[32] 仲盛, 黄欣沂. 区块链应用中的安全隐私专题简介[J]. 中国科学: 信息科学, 2020, 50(3): 461 – 462.
ZHONG S, HUANG X Y. Brief introduction of security and privacy topics in blockchain application[J]. Scientia Sinica (Informationis), 2020, 50(3): 461 – 462. (in Chinese)

[33] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[J]. Communications of the ACM, 2018, 61(7): 95 – 102.