·区块链专题· 文章编号: 1000-3428(2019)05-0001-12 文献标志码: A 中图分类号: TP399

区块链技术综述

张 亮[a,b,c],刘百祥[a,b,c],张如意[a,b,c],江斌鑫[a,b,c],刘一江[a,b,c]

(复旦大学 计算机科学技术学院 a. 上海市区块链工程技术研究中心; b. 上海市智能信息处理重点实验室;
c. 复旦-众安区块链与信息安全联合实验室,上海 200433)

摘 要: 基于区块链整体架构介绍技术栈层级,以比特币为例分析区块链工作原理,从分布式账本的角度描述区块链账本存储模型和账本分类情况。区块链中的数据通过共识算法在全网传播、达成共识并存储。在不存在可信第三方的情况下,利用智能合约实现交易、事务及分布式应用的独立运行,保证区块链数据的完整性、安全性及合法性。同时将哈希算法与默克尔树相结合降低区块链存储空间,基于数字签名算法为区块链参与者提供匿名身份证明,并使用加解密技术进一步保护区块链数据隐私。针对区块链安全、隐私保护、钱包管理等问题对当前研究的不足和未来的研究方向进行分析和展望。

关键词: 区块链; 密码学; 共识机制; 智能合约; 隐私保护

开放科学(资源服务)标志码(OSID):

中文引用格式: 张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程,2019,45(5):1-12.

英文引用格式: ZHANG Liang,LIU Baixiang,ZHANG Ruyi,et al. Overview of blockchain technology[J]. Computer Engineering,2019,45(5):1-12.

Overview of Blockchain Technology

ZHANG Liang[a,b,c],LIU Baixiang[a,b,c],ZHANG Ruyi[a,b,c],JIANG Binxin[a,b,c],LIU Yijiang[a,b,c]

(a. Shanghai Blockchain Centre of Engineering and Technology; b. Shanghai Key Laboratory of Intelligent Information Processing; c. Fudan-Zhongan Blockchain and Information Security Joint Lab, School of Computer Science and Technology, Fudan University, Shanghai 200433, China)

【Abstract】 Based on the blockchain overall architecture, the technology stack hierarchy is introduced. Bitcoin is used as an example to analyze the blockchain working principle. The blockchain ledger storage model and ledger classification are described from the perspective of distributed ledger. The data in the blockchain is spread across the network through consensus algorithms, reaches a consensus and is stored. In the absence of a trusted third party, this paper uses smart contracts to achieve independent operation of transactions, bussinesses and distributed applications to ensure the integrity, security and legitimacy of blockchain data. It combines the hash algorithm with the Merkel tree to reduce the blockchain storage space, provide anonymous identity proof for the blockchain participants based on the digital signature algorithm, and further protect the blockchain data privacy by using encryption and decryption technology. In view of blockchain security, privacy protection, wallet management and other issues, the deficiencies of the current research and the direction of future research are analyzed and forecasted.

【Key words】 blockchain; cryptography; consensus mechanism; smart contract; privacy protection

DOI: 10.19678/j.issn.1000-3428.0053554

0 概述

区块链概念自2008年在比特币白皮书[1]中被提出以来,引起全世界广泛关注,采用去中心化基础架构与分布式存储共识技术。从记账的角度出发,区块链是一种分布式账本技术或账本系统;从协议的角度出发,区块链是一种解决数据信任问题的互联网协议;从经济学的角度出发,区块链是一个提升合作效率的价值互联网。近年来,区块链逐渐从加密数字货币演变为一种提供可信区块链即服务

基金项目: 国家自然科学基金(61672166);上海市领军人才项目(16XD1400200);上海市科技创新行动计划(16JC1402700)。

作者简介: 张 亮(1989—),男,博士研究生,主研方向为区块链、密码学;刘百祥,工程师、博士;张如意、江斌鑫、刘一江,硕士研究生。

收稿日期: 2019-01-03 修回日期: 2019-02-20 E-mail: briliasm@gmail.com

(Blockchain as a Service,BaaS)的平台,各行各业均对区块链青睐有加,积极探索“区块链+”的行业应用创新模式。区块链包含社会学、经济学和计算机科学的一般理论和规律,就计算机技术而言,包含分布式存储、点对点网络[2]、密码学[3]、智能合约[4]、拜占庭容错(Byzantine Fault Tolerant,BFT)[5]和共识算法等一系列复杂技术。由于跨学科融合支撑,使得区块链构建了一个在数字世界中自治理、可信赖、可溯源的系统。

比特币作为加密数字货币,是区块链最原始、本质的应用。在比特币系统中,每个节点复制保存所有账户“币”的状态,每生成一个块,所有节点就迁移至另一个新的状态,并记录所有交易的迁移过程。为支持更多的自定义状态,一些区块链采用图灵完备的状态机模型,而图灵完备的状态机模型是可运行应用的必要条件。2013 年底,以太坊项目[4]立项,并实现了图灵完备的以太坊虚拟机,率先使得去中心化的应用成为现实,即在以太坊虚拟机上运行智能合约。由于区块链的无中心、可验证、无法篡改等特性,也受到了某些私有领域的欢迎,例如银行、金融、跨企业合作等。区块链技术可以改善内外审计工作方式,审计员可以对数据进行实时核实,按天审查公司数据,而不是按季度或按年。区块链可以支持更频繁的审计检查,从而减少人为的腐败问题,使得经济能够更健康稳定的发展。区块链的可靠性保证了经济交易的准确性,其透明性解决了搜集被审资料耗时耗力的问题。

根据开放程度,区块链可划分为公有链和联盟链,任何人都可以自由加入公有链,而只有拥有特定权限的个人或组织才可以加入联盟链。相比传统的中心化技术架构,联盟链中的金融机构能够更好地解决企业间的效率和信任等合作问题。Hyperledger 项目 是一个旨在推动区块链跨行业应用的开源项目,在 2015 年 12 月由 Linux 基金会主导发起,成员包括金融、银行、物联网、供应链、制造和科技行业的多个知名企业,其中最著名的为 Hyperledger Fabric[6]联盟链。

区块链从数字货币职能仅能完成货币转移和在线支付到区块链智能合约的实现,以及完成智能资产和金融领域的延展,再到区块链技术向非金融领域的进一步渗透,使得物联网、防伪溯源[7]、供应链等领域可有机地与区块链技术融合。尽管区块链技术受到广泛关注和研究,但目前其基础设施仍处于探索阶段。同时,区块链还存在一系列需要优化和改善的地方,比如性能低、扩容方案能力有限、隐私保护、存储效率、钱包管理等。本文从分布式记账角度出发对共识算法、智能合约进行分析,总结密码学的基础原理及区块链的安全问题,并对区块链技术的现状和发展方向进行探讨。

1 相关技术

1.1 区块链平台架构

区块链平台整体上可划分为数据层、网络层、共识层、智能合约层和应用层 5 个层次,如图 1 所示。数据层采用合适的数据结构和数据库对交易、区块进行组织和存储管理;网络层采用 P2P 协议完成节点间交易、区块数据的传输;共识层采用算法和激励机制,支持拜占庭容错和解决分布式一致性问题;智能合约层通过构建合适的智能合约编译和运行服务框架,使得开发者能够发起交易及创建、存储和调用合约;应用层提供用户可编程接口,允许用户自定义、发起和执行合约。

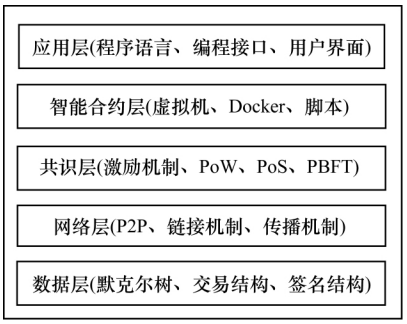

图 1 区块链平台架构

1.2 区块链工作原理

以比特币为例,区块链工作原理具体如下:

1) 节点构造新的交易,并将新的交易向全网进行广播。

2) 接收节点对收到的交易进行检验,判断交易是否合法,若合法,则将交易纳入一个新区块中。

3) 全网所有矿工节点(网络中具有对交易打包和验证能力的节点)对上述区块执行共识算法,选取打包节点。

4) 该节点通过共识算法将其打包的新区块进行全网广播。

5) 其他节点通过校验打包节点的区块,经过数次确认后,将该区块追加到区块链中。

比特币系统的数据结构如图 2 所示,比特币中的交易被组织成为默克尔树[1]结构。交易均被存储在默克尔树的叶子节点上,通过两两合并哈希直至得到根节点。根节点的哈希值作为一个区块头的元素,除此之外,区块头还包括时间戳、Nonce 和前一区块哈希值等。Nonce 是矿工完成工作量证明算法时的输入,也是矿工获取奖励的凭证。区块头包含前一区块的哈希值,使得每一个区块逻辑上以链的方式串联起来。默克尔树结构可使得在仅有部分节点的情况下,快速验证交易的有效性,并大幅减少节点的存储空间。

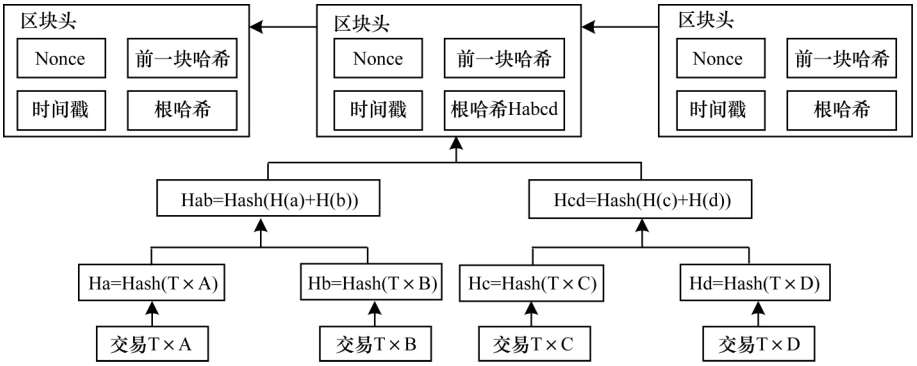

图 2　比特币系统的数据结构

2　分布式账本

尽管分布式账本技术(Distributed Ledger Technology,DLT)常被认为是区块链技术的同义词,但分布式账本是指可以在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。从计算机技术的角度看,账本是一系列包含交易和信息的数据结构,账本可以记录多方资金的往来记录、物品交换记录等。在区块链系统中,交易被组织成块,然后块被组织成逻辑上的链,因此区块链是一本不断增长的账本。账本可以完全公开,例如比特币系统和以太坊系统,也可以在联盟内公开,例如 Hyperledger Fabric。

2.1　账本存储模型

UTXO(Unspent Transaction Output)模型[1]中每个交易都由交易输入和交易输出组成,交易输入和交易输出可以有多项,表示一次交易可将先前多个账户中的比特币合并后转给另外多个账户。每个账户的余额是由该账户下所有 UTXO 总和得到。图 3 显示了 UTXO 模型交易的工作原理,其中,交易 1 中包含 1 个输入和 2 个输出,交易 2 中包含 3 个输入和 2 个输出。

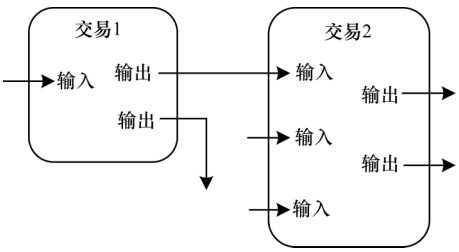

图 3　比特币 UTXO 模型交易原理

账户模型相对于 UTXO 模型更符合人类思维的认知,可直接读出账户的相关信息。智能合约也更适合建立在账户模型上,以太坊采用账户模型,并且将账户分为外部账户和合约账户。

键值对模型中的区块链技术在某些场合下是为了作为分布式账本而存在,存储模型常借鉴键值对数据存储模型,在该模型下数据存取简单。Hyperledger Fabric 致力于解决企业间的合作问题,通常在一种联盟环境下基于共享数据库的方式应用键值对模型。

2.2　加密货币与数字资产

加密货币是指在密码学建立的安全基础上构建虚拟货币,用于充当一般等价物的货币。数字资产是指以数字化存在的各种形式且归属权明确的可用数据或文件。数字资产可以是电子文档、图片、音视频文件等。加密货币是数字资产的一种特例,由于金融安全、技术安全等原因,目前我国并不承认比特币等加密货币的合法性。

以太坊等系统表明区块链可以作为一种具备可编程的开放服务平台,区块链上的应用以一个或多个智能合约的方式体现。以太坊的意见征求稿(Ethereum Request for Comment,ERC)提出了很多数字资产相关的标准。例如,2017 年底风靡全球的谜恋猫正是采用了 ERC721 标准,ERC20 标准常用于首次代币发行众筹(Initial Coin Offering,ICO)。一般数字资产特指排除加密货币等非法资产在内的资产。区块链常作为数字资产的存证和追溯平台,例如 BigchainDB[8] 和 Corda[9]。

2.3　账本分类

根据区块链系统的构建目标,账本会呈现出不同的形态,本节从账本所有权和账本个数的维度介绍账本的特点,具体分析如下:

1) 账本所有权: 在比特币等公有链系统中,所有用户均对账本具有查看权,在共识算法前提下,特定的节点对区块链具有写入权。而在 Fabric 等系统中,仅某通道(Channel)中的节点对该通道中的账本具有所有权,对账本的操作同样需要在共识机制下完成。

2) 账本个数: 区块链系统中可以含有一个或多个账本,例如 Fabric 致力于解决企业级的合作问题,

大企业间通常伴随多种合作业务，因此多账本相当常见。值得注意的是，账本之间相互隔离，但是同一个节点或组织可以同时处在多条 Channel 中，从而通过读写多个账本完成多个账本数据的互通。常见分布式账本对比结果如表 1 所示。

表 1 常见分布式账本对比结果

名称	应用场景	数据模型	账本数量
比特币	加密货币	UTXO	1 个
以太坊	分布式应用	账户	1 个
Fabric	分布式应用	键值对	多个
莱特币	加密货币	UTXO	1 个
BigchainDB	数字资产	UTXO	1 个

3 共识算法

区块链系统的节点可自由加入组织，具备自治性，为更好适应区块链系统，大多系统采用 P2P 网络进行数据传播。P2P 网络中的每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能。为驱使区块链中的节点有效参与共识过程，区块链的共识算法包括设计合理的经济激励机制和公平选取特定的打包节点。

在传统分布式系统中，评价系统采用 CAP[10] 标准，分别评价系统的数据一致性、数据可用性和分区容错性。对应到区块链系统中，有研究人员提出“不可能三角”的评价标准，包括去中心化、可扩展性、安全性。然而对于任意的区块链系统，不能同时满足以上3 个方面。去中心化主要描述参与共识的节点个数，参与共识的节点越多去中心化程度越高。可扩展性主要看吞吐量的大小，考察其是否适用于多种应用场景。安全性考虑其规则被破坏的经济成本，破坏规则的成本越高安全性越高。安全性由多方面保证，包括共识算法的确定性，确定性包括绝对性确认和概率性确认。绝对性确认是指一旦交易被包含在区块中并添加到区块链上，该交易就会被立即视为最终确定；概率性确认是指包含交易的区块的后续区块越多，该交易被撤销的可能性越低。

3.1 共识算法分类

传统共识算法一般称为分布式一致性算法，主要面向分布式数据库操作且大多不考虑拜占庭容错问题，这些算法包括 Paxos[11]、Zab、Kafka 等。在区块链中，尤其是公有链，采用一系列拜占庭容错类共识算法，如 PoW、PoS[12]。

区块链的共识算法由于其容错能力、打包节点选取方式和一致性程度等特点不同，因此可以区分共识算法类别的维度也不同。文献[13]指出可以按照选取打包节点方法的不同分为选举类、证明类、随机类、联盟类和混合类。选举类多见于传统的共识算法；PoW 和 PoS 均是证明类，不同的是 PoW 证明的是矿工的算力，PoS 证明的是参与者占系统虚拟资源的权益；Algorand[14] 和 PoET 是通过依赖随机数选取打包节点，属于随机类；以 DPoS[15] 为代表的“民主集中式”轮流获得打包权属于联盟类算法；还有很多系统采用 PoW + PoS 的共识机制，属于混合类的共识算法。

3.2 常用共识算法

3.2.1 PoW 算法

PoW 算法最早在比特币中使用，其核心思想是通过节点的算力竞争来选取打包节点。比特币系统中的各节点基于各自的计算机算力相互竞争来共同解决一个求解复杂但是验证容易的 SHA256 数学难题，最快解决该难题的节点将获得下一区块的记账权和系统自动生成的比特币奖励。PoW 在比特币中的应用具有重要意义，其奠定了比特币系统的虚拟货币发行、流通功能，并保障了系统的安全性和去中心化的特性，有效防止了女巫攻击。然而，PoW 也存在明显的缺陷，其矿工重复和循环的算力消耗造成巨大资源浪费，而且长达 10 min 的交易确认时间使其不适合小额交易的商业应用。

矿工通过不断尝试随机数使得计算得到的区块哈希值小于难度值，当找到合适的随机数后，广播该随机数和对应区块，随后其他节点验证该区块的合法性，因此算力越高得到记账权的几率越大。基于 PoW 的区块链(如比特币)的去中心化程度较高，节点可以自由进出系统，基于算力竞争的共识算法可以最多抵抗 50% 攻击。但是，PoW 共识会消耗大量的能源，对系统的可持续发展造成较大影响。比特币每秒最多能够处理 7 笔交易，可用性较低。而且 PoW 方式容易造成矿工联合成集中式的矿池，背离了原来去中心化的初衷，也提升了矿工集体合谋进行 51% 攻击的可能性。PoW 中区块是概率确定的，如果追加在区块上的区块数越多，那么该区块的确定性越高，比特币系统认为有 6 个区块确认才能认为该区块是确定的，也就是一笔交易的确认需要至少 1 h 的时间。

3.2.2 PoS 算法

PoS 算法的提出是为了解决 PoW 巨大能源浪费的问题。PoS 由系统中具有最高权益而非最高算力的节点获得记账权，其中权益体现为节点对系统虚拟资源的所有权，Peercoin[12] 是币龄或币天数。Peercoin 中的挖矿难度由币龄决定，拥有更多币龄的用户有更高的概率决定下一个区块并获得出块的奖励，在成功出块后相应的币龄会清空，这样可以保证区块链的有效性由具有经济权益的用户来保障，同时避免 PoW 的大量能源消耗。以太坊的下一阶段的共识将采用 PoS 的共识算法，即 Casper。Casper FFG 版本将采用 PoS 与 PoW(以太坊使用 ethash 基于内存困难的 PoW 算法)混合的方式作为过渡阶段

来减少挖矿能源的消耗,在后续 Casper TFG 版本中将使用纯粹的 PoS 共识算法来保证区块链的有效性,不再使用 PoW 的方式挖矿出块。

PoS 共识算法中的权益一般指用户在区块链上的虚拟资源,常用持有 token 数量或持有 token 时间来衡量。根据用户持有权益的大小决定该用户挖矿的难度,权益越高,挖矿的难度就越低。通过权益的大小来决定记账权可以有效避免资源浪费,进而缩短出块时间和交易的处理时间。PoS 可以通过提高区块链系统的每秒事务处理量(Transactions Per Second,TPS)提高可用性。PoS 共识算法的去中心化程度较高,节点可以方便加入或者退出区块链系统。基于 PoS 的系统仍然需要进行挖矿,且区块的确定性也是概率型的,需要其他多个节点对区块确认后完成最终确定。

3.2.3　BFT 算法

在 BFT 算法[16]中,当拜占庭节点不超过总节点数的 1/3 时,拜占庭将军问题才能解决。原始的 BFT 算法分为口头协议和书面协议。在口头协议中,节点之间需要将接收到的"命令"相互传输,最终根据得到的各个节点的信息确定最终结果。书面协议需要对传输的信息进行签名验证,该协议可以防止拜占庭节点随意更改接收到的信息,使最终结果更加可靠。实用拜占庭容错(PBFT)算法[17]的提出解决了原始 BFT 算法信息传输复杂度较高的问题。PBFT 主要包括 3 个阶段: 预准备,准备,提交。该算法可以较快达到最终结果,但是 PBFT 不适用于大规模的公链场景,因为节点越多,通信时间越长,共识成本较高,所以 PBFT 适用于节点较少的联盟链或者私链,例如 Hyperledger Fabric。

PBFT 主要解决原始 BFT 共识算法效率较低的问题,将通信复杂度从指数级降低到二次方级别,使其能够在实际系统中使用。当系统中的拜占庭节点个数少于总数的 1/3 时,BFT 共识算法就可以正确运行并保证区块链系统的可靠性。

3.2.4　DPoS 算法

文献[15]提出 DPoS 算法。DPoS 共识的基本思路类似于"董事会决策",即系统中每个节点可以将其持有的股份权益作为选票授予一个代表,希望参与记账并且获得票数最多的前 N 个代表节点将进入"董事会",按照既定的时间表轮流对交易进行打包结算并且生产新区块。如果说 PoW 和 PoS 共识分别是"算力为王"和"权益为王"的记账方式的话,DPoS 则可以认为是"民主集中式"的记账方式,其不仅能够较好地解决 PoW 浪费能源和矿池对去中心化构成威胁的问题,也能够弥补 PoS 中拥有记账权益的参与者不希望参与记账的缺点,其设计者认为 DPoS 是当时最快速、高效、去中心化和灵活的共识算法。DPoS 共识算法可与 PBFT 一起使用,先通过 DPoS 的方式在区块链系统中选取一定数量的出块者,当出块者生成一个区块后,用 PBFT 算法在所有出块者中进行区块共识,当 PBFT 共识过程结束才能将区块记录在账本中。

在 DPoS 共识算法下,用户通过抵押一定数量的权益成为记账候选人,其他用户利用投票结果来确定记账候选人的排名,得到票数最多的几个节点拥有某个时间片的记账权,例如 EOS 设置票数最多的 21 个节点为记账节点。投票排名会在一段时间后更新,重新选择出块者。DPoS 共识因为共识节点数量较少,节点间的通信速度快,可以快速完成区块打包、广播以及验证,显著提升系统 TPS,增强平台应用的可用性。DPoS 算法中参与记账的节点大幅减少,因此其是通过牺牲去中心化为代价而实现 TPS 的提升。

3.3　共识算法对比

基于共识算法评价标准,表 2 对 PoW、PoS、DPoS、PBFT 的性能、去中心化程度、容错节点比例、确定性和资源消耗方面进行性能对比。

表 2　常用共识算法性能对比结果

指标	PoW 算法	PoS 算法	DPoS 算法	PBFT 算法
性能效率	低	较高	高	高
去中心化程度	高	高	低	低
容错节点比例/%	50	50	50	33
确定性	概率性	概率性	绝对性	绝对性
资源消耗	高	低	低	低

在"不可能三角"的评价体系中,任何的共识算法都无法达到 3 个特性的最好状态,需要在3 个特性中进行权衡。PoW 选择了去中心化和安全性,但可用性较低。PoS 相对于 PoW 节约能源,但是不够灵活。PBFT 算法保证了去中心化和安全性,但存在大规模节点时可用性较差。DPoS 算法选择了高可用性和安全性,但是去中心化程度较低。

目前的区块链系统中还没有各方面性能都最优的共识算法,只能通过权衡系统需求达到特定的目标。在保证区块链系统安全性的同时,要不断提升可用性以适用于大规模应用,同时在满足一定的去中心化程度的情况下中的用户能积极参与到共识中,并使所有参与投票、共识、验证的节点能够从中获利,所以共识算法的经济激励也是不可或缺的一部分。只有充分使系统中的资源流通以及用户交互、参与,才能实现区块链系统的稳固运行。

4　智能合约

智能合约[18]是一套以数字形式定义的承诺,包括合约参与方可以在其上执行这些承诺的协议。这些承诺指的是合约参与方同意的权利与义务,并且在智能合约中定义了实施办法。由此可见,智能合

约不一定需要使用区块链技术，只是因为区块链技术能够较好地支持智能合约。简言之，智能合约是传统合约的数字化版本，在区块链上是可执行程序。与传统程序一样，区块链智能合约拥有接口部分，接口可以接收和响应外部消息，并处理和储存外部消息。

4.1 区块链上的智能合约

区块链上的智能合约是一段沙盒环境中的可执行程序，与传统程序不同，智能合约更强调事务，智能合约本身也是一项事务产生的程序。智能合约的输入、输出、状态变化均存在于区块链中，也就是需要在节点间共识算法的基础上完成。然而，智能合约只是一个事务处理和状态记录的模块，既不能产生智能合约，也不能修改智能合约，只是为了让能够被条件触发执行的函数按照调用者的意志准确执行，在预设条件下，自动强制地执行合同条款，实现“代码即法律”的目标。

智能合约在共识和网络的封装之上，隐藏了区块链网络中各节点的复杂行为，同时提供了区块链应用层的接口，使得区块链技术的应用前景广阔。智能合约也是区块链的一项重要功能，它标志着区块链不仅是加密货币，而且可以形成基于区块链的服务，即 BaaS。智能合约使得区块链可以承载可编程的程序、运行去中心化的应用和构建需要信任的合作环境。

4.2 从脚本到智能合约的演化过程

在比特币以前，智能合约由于缺少可信的运行环境，并没有在实际生产中实现和运用。比特币通过提供一种栈式的编程环境，即比特币脚本，以支持 UTXO 的模型和完成比特币的转账逻辑。比特币脚本从功能上完成账户之间的转账和转账有效性校验。比特币脚本具有一定扩展性，可以增加额外的指令以实现更多的交易类型和隔离见证等。但脚本处于交易的数据字段，逻辑部分与数据部分耦合，缺乏灵活性，指令扩展容易造成系统安全隐患，脚本的指令功能为图灵非完备。图 4 是比特币中支付到公钥哈希(Pay to Public Key Hash，P2PKH)交易类型的栈结构(从左至右)代码。<sig>指使用者的签名，<PubK>指使用者的公钥，DUP 是指复制<PubK>并压栈命令，HASH160 指对<PubKHash>哈希运算，<PubKHash>指公钥的哈希值，EQUALVERIFY 命令指比对<PubKHash>和使用者的<PubKHash>是否相等，CHECKSIG 指验证<sig>是否正确。

<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

解锁脚本 锁定脚本

图 4 比特币 P2PKH 交易类型

比特币平台并不支持智能合约，通过借鉴比特币的指令设计思路，同时满足图灵完备性和支持交易之外的任意信息交换，以太坊设计了具有独立运行环境和编程语言的虚拟机 EVM。Hyperledger Fabric 使用 Docker 作为沙盒环境和采用 Golang 和 Java 等常见高级编程语言。另外，以太坊中摒弃了 UTXO 模型，而采用人类容易理解的账户模型。在 Hyperledger Fabric 中称智能合约为 chaincode。

4.3 运行原理

在加密货币中，类似智能合约的功能为：1) 验证交易中的签名是否正确；2) 验证交易的输入和输出金额是否匹配；3) 更新输入和输出账户的余额状态。以比特币为例，比特币只有不到 200 种操作命令，通过栈式脚本语言完成上述动作，实现转账功能。

受到加密货币的脚本语言的启发，具备图灵完备的运行环境的区块链系统的智能合约通常是定义若干合约，这些合约包含若干初始状态、转换规则、触发条件以及对应的操作。然后通过提交事务，经过共识算法后，合约安装部署到区块链上。区块链可以实时监控整个智能合约的状态，当某一新的事务满足一定条件时触发合约对应的条款执行，新的事务经过共识后，该事务的输入输出和合同内的状态变化均记录在区块链上。以以太坊为例，首先以太坊的账户分为外部账户和合约账户，外部账户只能以交易的形式发送消息，从而产生事务，这种事务可以是普通的交易，创建一个合约或调用某一合约。如果事务是创建一个合约，那么会产生一个合约账户；如果事务是调用某一合约，对应的合约条款即代码将会被激活执行，代码对状态的操作变化将被记录在区块链上。

外部应用需要调用智能合约，例如去中心化应用，并依照合约执行事务和访问状态数据。外部应用与智能合约的关系可以对比传统数据库应用与存储过程的关系，存储过程在数据库管理系统中运行，访问关系数据库数据，而智能合约在区块链系统中运行，访问区块和状态数据仍待优化和发展。图 5 显示了智能合约的运行机制。

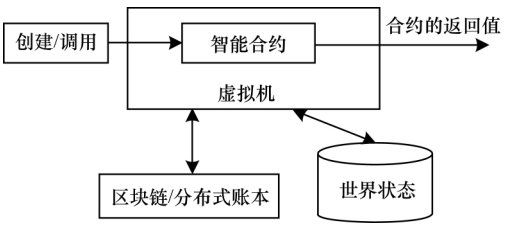

图 5 智能合约运行机制

4.4 运行环境

智能合约不是直接运行在区块链节点已知的环境中，因为合约代码如果直接操作区块链，尤其是写区块链的数据，会导致合约不受管制，破坏区块链数据结构，威胁区块链节点的安全，所以智能合约必须

在隔离的沙箱环境中运行。合约运行环境和宿主系统之间、合约与合约之间通过沙箱环境有效隔离,这既符合解耦合的设计,也提升了智能合约的安全性。目前,主流区块链平台对沙箱的支持主要包括虚拟机和容器,它们都能有效保证合约代码在沙箱中独立执行。以太坊使用自定义的以太坊虚拟机作为沙箱,合约主要由 Solidity、Serpent 等语言编写,经过 EVM 编译和运行。Hyperledger Fabric 使用轻量级的 Docker 容器作为沙箱,Docker 在工程上常用来提供隔离的 Linux 运行环境,同样可以有效隔离合约环境、宿主机环境以及不同合约的运行环境。值得注意的是,Hyperledger Fabric 使用 Docker 容器中的合约仍能访问互联网,而 EVM 没有网络接口。

以太坊环境下的智能合约采用高级程序语言实现。在 solidity 编程语言中,contract 关键字定义了一份合约,合约由一组代码和数据组成,合约数据的共享规则由合约制定者设置。在下文的代码中,SimpleStorage 是一份合约,storedData 是该合约中的一个字段,set 和 get 函数规定了该合约的 storedData 字段会被区块链上任意一个人读取和修改。

```
contract SimpleStorage {
    uint storedData;
    function set( uint x) {
        storedData = x;
    }
    function get( ) constant returns ( uint retVal) {
        return storedData;
    }
}
```

在以太坊中,solidity 语言对应的合约将被编译成二进制字节码,作为以太坊虚拟机的输入,以太坊根据沙盒机制保存智能合约和暴露合约相应的调用接口。

5　密码学

为保证账本的完整性、公开性、隐私保护、不可篡改、可校验等一系列特性,区块链技术高度依赖密码学。正是密码学的一些理论研究和技术特性,使得公有链的所有节点能一定程度上达到公平、安全、可信赖。例如,在比特币系统中,哈希使得工作量证明算法成为全网的共识算法。基于椭圆曲线的公钥密码学的签名验签功能使得仅私钥拥有者可自由支配该账户,从而发起交易。

5.1　相关理论

5.1.1　哈希函数

哈希函数[3]是指将任意长度的字符串映射到固定长度为 l 的字符串,记为 $H:\{0,1\}^{*}\rightarrow\{0,1\}^{l}$。哈希函数 $H(x)$ 可以认为是在映射集合中查找 x 对应的值,如果 x 不在该映射集合中,那么计算数 y,并且在上述映射集合中将 y 赋值给 $H(x)$。一个有效的哈希函数通常具有以下特点: 1) 抗修改性,改动 x 任意一位时,$H(x)$ 变动较大; 2) 不可逆性,已知 $H(x)$,得到 x 的概率较低; 3) 抗碰撞性,对于任意 x 和 x',$H(x)=H(x')$ 的概率极低。

5.1.2　加解密

加解密贯穿于密码学中,公钥密码学又叫非对称密码学[3],是相对对称密码学而言。在对称密码学中,加解密使用相同的密钥。在非对称密码学中,使用公私钥对完成加解密。常用大数分解和离散对数困难问题的求解原理产生非对称密码学的公私钥对。通常,公钥对外公布,私钥私有。为安全起见,区块链中常用椭圆曲线选取群,进而根据求解离散对数困难问题来构造非对称密码学的公私钥。

5.1.3　数字签名和验签

在公钥密码技术中,为保护隐私,通过签名和验签完成权属证明过程[3]。在加解密过程中发送者用私钥加密(签名),接收者公钥解密(验签); 在签名验签过程中常用私钥签名,公钥验签。签名验签具体来说是指私钥持有者对消息 m 进行哈希运算得到 $H(m)$,并用私钥对 $H(m)$ 加密生成签名 s,将消息 m 和签名 s 发送给其他人,其他人用公钥对签名 s 解密,得到 $H'(m)$,对消息 m 进行哈希运算 $H(m)$,然后通过对比 $H'(m)$ 与 $H(m)$ 是否一致判断验签是否成功。

5.2　身份管理

公钥或公钥哈希被视为用户在区块链中的身份。比特币系统直接使用公钥哈希表明用户身份,在交易过程中用户不需要提供其他信息,并且用户可以在交易中使用不同的公钥地址来增加隐私性,因此比特币具有一定的匿名性。比特币系统采用椭圆曲线数字签名算法(ECDSA)[3]产生用户的公私钥对,然后用公钥的哈希作为用户的身份,该身份作为接收数字货币的地址。用户通过其私钥签名可完成对该交易输出的确权,或者授权使用该交易输出。

私钥对于区块链系统至关重要,但从用户的角度来看,私钥是一串杂乱无章的字符串。这就为私钥管理带来了困难,尤其是当用户拥有很多个区块链地址。分层确定性钱包是指在没有私钥参与的前提下,通过公钥直接分散出子公钥,并且分散的子公钥可以由子私钥认证。分层确定性钱包一方面只需要通过备份一次私钥管理多个无关联的子公钥; 另一方面,通过多个无关联的子公钥管理多账户,从而实现多账户私钥管理和隐私保护。

另外,文献[19]提出基于 LPN 的抗擦除攻击认证协议,用于构建移动端可信钱包。文献[20]比较

了 6 种比特币的私钥管理方式: 本地存储方式,密码保护方式,离线方式,离线可计算方式,自主生成密钥方式和托管方式,并对这 6 种私钥管理方式做了详细分析和对比,认为这些方法同样存在各种问题。

5.3 隐私保护

区块链系统要实现隐私保护,离不开密码学的支撑。无论是采用 UTXO 模型,还是采用账户模型,在许多区块链系统中所有的交易数据是公开保存的,通过追踪和分析地址间的交易记录,可以推测出用户身份。为了提高区块链技术的匿名性,保护用户的身份隐私,多种区块链隐私保护方案被提出。

在混币协议[21]中,不同用户被要求同时将相同金额发送到混合服务器,服务器对交易内容混合处理后,将比特币发送到用户新地址。资金经过混合处理后,隐藏了交易输入、输出地址的直接联系,使得攻击者对交易内容的分析变得困难,从而保证用户的隐私。文献[22]提出 Blindcoin 盲签名[23]解决方案。文献[24]采用链式混合及盲化技术实现混币过程。

门罗币[25]、零币[26]、零钞[27]等均基于加密协议实现隐私保护。门罗币基于 CryptoNote[28]协议,通过环签名和隐蔽地址的方式来隐藏输入输出地址之间的关联,环签名技术保证了交易的隐私。文献[26]提出一种基于零知识证明的加密协议,即零币。零币是比特币的一种扩展协议,比特币用户可以通过该协议将比特币转化为零币,从而隐藏交易的输入、输出地址。其他用户只能知道零币是否被花费,而无法获取其余的交易信息。文献[27]在零币的基础上提出了零钞,将加密技术提高到了更高的层次。零钞使用了 zk-SNARK 技术,该技术可以使零知识证明更加简洁。与零币相比,零钞中的交易金额也是保密的,并且可以将不同面值的币铸造成多个等值的币。

由于区块链交易的速度原因,因此一些依赖第三方的链下达成交易方案被提出,这些方案也称为安全通道协议。在安全通道协议的技术框架下,Lightning Network[29]、Sprites[30]、Bolt[31]、TumbleBit[32]等技术致力于解决存在第三方时的隐私安全问题。常见隐私保护技术的性能对比结果见表 3。

表 3 隐私保护技术的性能对比结果

名称	核心技术	特点	结构	隐私保护效果
比特币	签名验签	公钥作为身份,私钥私有	去中心化	差
门罗币	环签名	采用环签名的方式实现地址隐私保护	去中心化	好
零币	零知识证明	隐藏交易信息	去中心化	好
零钞	零知识证明	隐藏交易信息、交易金额	去中心化	好
盲币	盲签名	匿名性取决于第三方混币服务	中心化	好
EOS	多签名	通过多签名可以起到投票的作用	半中心化	好

6 区块链安全

区块链在设计之初就从不同的维度解决安全问题,例如其利用非对称加密保证了支付可靠性,使用哈希和签名的唯一性保证了数据无法被篡改,通过去中心的分布式设计防止数据丢失等。即便如此,随着区块链规模逐渐扩大,仍出现了越来越多的安全问题。

6.1 51% 攻击

工作量算法是首先应用于区块链的共识算法,算力攻击也一直是研究的热点。在比特币的工作量证明机制中,节点挖块的概率与其算力成正比,若算力越大,则其计算正确哈希值的速度就越快,更可能掌握打包权。因此,不同节点希望联合起来成为“矿池”以挖掘更多的块,获得更大的利益。一旦矿池总算力足够大,超过全网 51% 的计算能力,可以破坏整个区块链系统,导致安全问题[33-34]。

1) 修改交易数据,可能导致双重支付攻击[35-36]。

2) 阻止区块部分确认或者全部交易。

3) 阻止矿工开采任何可用的区块。

2018 年 5 月,一名恶意的矿商获得了至少 51% 的网络哈希算力,使得其成功控制了区块链,对比特币黄金网络实施了双重攻击,从交易所窃取超过 388 200 个比特币黄金,价值高达 1 860 万美元。

6.2 硬分叉

分叉是指当区块链系统升级时,共识规则中的新协议也发生了变化,一部分矿工还没来得及升级。对节点来说,已经升级的节点是新节点,没有升级的节点是旧节点。当新节点的算力超过 51% 时,出现遵循不同机制产生的分叉。这种分叉类型又分为 2 种,硬分叉和软分叉。

软分叉意味着当系统开始升级时,引入了新版本或新的协议,它与以前的版本兼容,新的节点出产的区块可以被旧的节点接受。当网络发生了软分叉时,一开始旧节点产生的区块中的交易不被新节点认同,会产生一个短暂分叉,但是新版本的分叉会超过旧版本的分叉成为最长链。因此,网络中的节点不需要同时升级新协议,允许逐步升级。软分叉不会影响节点升级时系统的稳定性和有效性。

硬分叉意味着系统达到新版本或新协议时,不

兼容以前的版本,旧节点不接受新节点出产的区块,因此新旧节点会开始在不同的区块链上运行,1 条链变成了 2 条链。虽然新的节点计算能力比旧节点强,但是旧节点仍将继续维持其认为正确的链。在未得到几乎所有生态中的参与者同意的情况下,硬分叉可能会导致整个区块链生态的分裂,所以,这是一个极具争议和风险的安全问题。一旦发生硬分叉,区块链作为可信平台的信任度将会降低。

6.3　智能合约安全

智能合约本质是一段运行在区块链网络中的代码,完成用户设定的业务逻辑,规范相互不信任的参与者行为,其中最突出的框架是以太坊。但是只要是人为编写的程序,就可能出现错误与缺陷,而不同于传统程序,智能合约以无法逆转的形式存在,一旦出现漏洞将可能带来致命损失。以太坊智能合约中的一些漏洞已经在实践开发以及对合约的静态分析中发现,这些漏洞被人利用并对以太坊的智能合约实施攻击,造成大量的资产损失。

目前,以太坊上智能合约的漏洞根据攻击位置主要分为 3 类,包括 Solidity、EVM 二进制编码、Blockchain[37]。表 4 是对以太坊 3 类漏洞的部分罗列。

表 4　以太坊部分漏洞

类别	产生漏洞原因
Solidity	未知调用
	无 gas 调用
	顺序异常
	类型转换
	重入攻击
	私有变量
EVM	不可修改的 bug
	代币永久丢失
	栈空间受限
Blockchain	未知状态
	随机数生成
	时间限制

6.4　欺诈攻击

欺诈攻击是以一种创造性的方式,使得没有达到 51% 算力的攻击者仍能干扰区块链的正常工作,下面列举 2 个欺诈攻击实例进行说明。一种是“自私的矿工”。攻击者挖到新区块后藏起来不公布,其他诚实矿工因为不知道新区块的存在,还是继续在旧区块基础上挖矿,等到攻击者挖到第 2 个区块后便会同时公布手中藏着的 2 个区块,这时出现区块链分叉。只要攻击者比诚实矿工多挖 1 个区块,攻击者所在的分叉就是最长链: 根据比特币的共识机制,矿工只在最长链后面挖矿。原本诚实矿工们所在的那条链,因为比攻击者的分叉短,便作废。此时,攻击者挖到 2 个新区块而获得相应收益,而诚实矿工的分叉被废弃。另一种是日食攻击[38]。区块链上的节点必须保持不间断通信才可以比较数据。日食攻击是其他节点实施的网络层面攻击,其攻击手段是囤积和霸占受害者的点对点连接时隙,将该节点保留在一个隔离的网络中。在针对比特币网络的日食攻击中,攻击者可以控制足够数量的 IP 地址来垄断所有受害节点之间的有效连接。然后,攻击者可以征用受害者的挖掘能力,并用它来攻击区块链的一致性算法或用于“重复支付和自私挖矿”。针对以太坊的日食攻击,攻击者可以垄断受害节点所有的输入和输出连接,从而将受害节点与网络中其他正常节点隔离。然后,攻击者可以诱骗受害者查看不正确的以太网交易细节,使卖家在交易还没有完成的情况下将物品交给攻击者。

6.5　钱包安全

在区块链中,资产管理也是一个较大的安全问题。区块链具有无中心结构,用户通过公开地址与密钥来宣示资产所有权,一旦密钥丢失,由于区块链的不可篡改特性,意味着不可能通过修改区块链记录拿回资产,因此盗币事件经常发生,其主要是通过交易平台监守自盗、交易所遭受黑客攻击、用户交易账号被盗等手段。2017 年 3 月,韩国比特币交易所 Yapizon 被盗 3 831 枚比特币,相当于该平台总资产的 37%,价值 5 700 万美元; 2017 年 6 月,韩国数字资产交易平台 Bithumb 被黑客入侵,受损账户损失数十亿韩元; 2017 年 7 月,BTC-e 交易所被盗 6.6 万枚比特币,价值 9.9 亿美元; 2017 年 11 月,Tether 宣布被黑客入侵,价值 3 100 万美元的比特币被盗。黑客一旦盗币成功,利用混币等手段进行洗白,几乎无法被追回。

7　发展与展望

7.1　共识机制

共识机制常被认为解决了区块链环境中的两大问题,一是区块打包权的公平选择,二是激励机制。近年来,共识机制的研究受到了广泛关注和投入。总体来说,共识机制的研究方向包括改进 PoW 算法、改进 PoS 算法、PoW 和 PoS 的结合算法、改进传统分布式的一致性算法[13]。

由于原生 PoW 消耗资源多、共识速度慢,Bitcoin-NG[39] 系统将时间分片,OmniLedger[40] 系统优化跨分片交易处理,PoET 和 PoL[41] 采用英特尔可信执行环境 SGX,解决资源浪费问题,但需引入可信第三方。原生 PoS 共识算法存在“无利害关系”问题,Tendermint[42] 将 PBFT 和 PoS 结合并通过保证金机制解决上述问题,以太坊 Casper 中的 TFG 版本是基于链的 PoS 设计,FFG 版本是基于链和拜占庭容错的 PoS 设计解决上述问题。权益速度证明

(PoSV)[42]、燃烧证明(PoB)、行动证明(PoA)均将PoW和PoS结合,同时解决PoW资源消耗问题和PoS安全风险问题。AlgoRand[14]采用密码抽签技术和BA*拜占庭容错协议完成共识。

7.2 跨链技术

区块链的热潮下出现了众多的区块链平台,跨链技术是指将孤立的区块链平台互联互通,使得数字资产能够在链间无障碍流通,其价值巨大。以太坊创始人在《链的互操作性》中指出常用的跨链技术包括:1)公证人机制;2)侧链/中继技术;3)基于哈希的锁定技术。近年来,还有第4种分布式私钥控制技术。公证人机制通过引入第三方可信机构,作为跨链资产的保管人。侧链/中继技术通过去中心化的方式完成链间状态交互,BTC-Relay通过以太坊智能合约实现以太坊与比特币的信息互联;Cosmos将所有区块链看作zone,通过Hub实现中继功能。哈希锁定技术将哈希原象作为秘密,通过分时间段控制和条件支付技术可在无第三方情况下完成原子交换。分布式私钥控制技术通过分布式密钥生成算法和门限签名技术实现资产锁定和解锁操作,Fusion项目采用该技术实现跨链。

7.3 隐私保护

攻击者可通过获得网络中节点IP的相关信息关联个人,以及追溯交易对其进行大数据处理可以得到很多有价值的信息,由于用户使用不当会造成DAPP的隐私泄露,可见隐私保护问题亟待加强。在第5节介绍了一些密码与隐私保护相关的问题,如用零知识证明解决交易隐藏的问题,用环签名实现地址隐蔽和交易隐蔽。同态加密是指对经过加密的数据进行处理得到一个输出,将该输出进行解密,其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的,这就为密文搜索提供了技术保证,对于交易隐私保护有借鉴意义。安全多方计算解决了一组互不信任的参与方之间保护隐私的协同计算问题,同时不泄露各输入值给参与计算的其他成员。其他形式的零知识证明等密码算法有待进一步实现区块链技术各环节中的隐私保护。此外,基于身份的密码[43]、基于属性的密码[44]以及分层确定性钱包技术等用于用户身份信息的隐私保护也值得研究和关注。

7.4 性能优化

比特币和以太坊的交易吞吐量分别约为7TPS和15TPS,Hyperledger Fabric的交易吞吐量不超过2 000TPS,远低于现有数据库。在区块链系统中,交易会被打包成块,然后再写入区块链。在打包前需要在网络中传播,打包时需要对所有交易进行验签和防止"双花",打包后需要将块广播,其他节点需要多次确认达成共识,才能永久写入区块链,因此区块链系统性能相对较差。未来区块链作为平台提供服务,性能将是智能合约运行的瓶颈。性能优化是多种角度的,可以从上述各环节进行性能参数优化,实现全新的共识机制,例如EOS的DPoS机制,分片或使用有向无环图(Directed Acyclic Graph,DAG)等新的交易数据存储结构,优化点对点网络的通信模型提升速度,通过安全通道协议提高线下交易速度。

7.5 多链和侧链

多链是使一个区块链平台具有多条并行的链,使互不相关的交易实现分片存储和并发执行。多链设计方案既可简化架构,降低数据处理压力,又可提高系统可拓展性。同时,链间隔离也在一定程度上解决了隐私泄露问题。以太坊中的分片、Hyperledger Fabric中的多通道以及Cosmos中的zone都是多链技术的应用。侧链是为解决数字资产在不同区块链之间转移的问题而提出的一种技术。侧链可以是一个独立的区块链,有自己按需定制的账本、共识机制、交易类型、脚本和合约等。侧链的核心原理在于能够冻结一条链上的资产,然后在另一条链上产生。以比特币的侧链为例,可以通过支持与比特币系统的锚定来引入一定数量的比特币。当比特币在侧链流通时,主链上对应的比特币会被锁定,直到比特币从侧链回到主链。侧链机制可以在对比特币系统本身不进行改动的基础上,拓展其功能。例如,闪电网络作为比特币的一种侧链,允许"小额支付渠道"跨越多个比特币交易安全执行,并且不影响主链;RSK是一个智能合约平台,其包含图灵完备的虚拟机系统,为比特币拓展了智能合约的功能。

7.6 区块链数据库

如果BigchainDB等平台用作数字资产的存证和追溯,那么在实际应用中,尤其是大规模应用和存取频繁时,区块链作为数据库,这部分的效率就可能受到较大影响。无论是以太坊还是Fabric,目前区块链在数据处理上表现都较差,远不如传统意义上的数据库,一方面体现在速度性能上,另一方面表现在对复合形式的查询语句支持上。虽然区块链涵盖了传统意义上没有的安全和拜占庭容错功能,但在性能优化方面,区块链还有很多地方可以借鉴传统数据库。交易从打包至区块链再到区块验证,最后写入区块链等过程与共识算法类似,均需要较大开销。文献[45]提出4种针对区块链数据存储效率的优化方向:细化分层、各自优化,充分发挥硬件的优势,分片,支持声明式语言。

7.7 安全与自主可控

本文从已有系统和未来发展趋势上提到隐私保护的问题,涉及身份信息隐藏和交易信息隐藏等技术。然而,为了保护区块链使用者的权益和降低风险,需要考虑KYC和AML问题。ChainAnchor通过在受限的区块链上添加身份认证和隐私保护层,使得任何人可以读和认证交易,并且只有匿名身份认

证过的交易才能被处理。2018 年 9 月中国信息通信研究院和中国通信标准化协会推出《区块链安全白皮书》,鼓励“区块链 + 网络安全”应用模式的探索,鼓励自主可控的区块链平台和应用开发,使得区块链中的加密算法国产化。

7.8　分布式可验证随机数生成器

文献[46]提出分布式可验证随机数生成器的概念。近年来,由于区块链系统的盛行和日趋成熟,分布式可验证随机数从理论和实践方面均得到了广泛关注,并且有了实质性进展。分布式可验证随机函数生成器一般在允许有拜占庭节点的情况下,具有连续产生的可用性、随机数产生前的不可预测性、产生时的无偏性和产生后的公开可验证性。分布式可验证随机数生成器应用于共识协议中,将有效解决 PoW 中的能源消耗问题和 PoS 中的节点离线问题。分布式可验证随机数生成器还可以被智能合约使用,实现公平公正的投票、选举和游戏等场景。文献[47]将使用区块链系统(即比特币)作为分布式可验证随机数生成器,但过于依赖比特币系统且存在扣块攻击风险。文献[48]采用“提交-展示”协议实现分布式可验证随机数生成器,但其模型条件过于苛刻。Ouroboros[49]、RandHound[50]、RandHerd[50]、HydRand[51]等系统基于公开可验证密码共享方案(Publicly-verifiable Secret Sharing,PVSS)[52]实现分布式可验证随机数生成器,这些系统均依赖复杂的交互过程。Dfinity[53]使用 BLS[54]签名体制实现分布式可验证随机数生成器,但其安全性仍需进一步证明。

8　结束语

区块链技术是指通过分布式存储,基于点对点网络,使数据达到一致性,并在此基础上提供应用服务的一项计算机技术。在没有第三方权威机构的情况下,区块链技术通过联合密码学、经济学和社会学等学科,保障数据内容安全,并降低合作成本及提升合作效率。尽管目前仍有一些技术难关需要攻克,但区块链技术将与各行各业结合,加快推进智能城市建设步伐。

参考文献

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2018-12-08]. https://bitcoin.org/en/bitcoin-paper.

[2] MILOJICIC D S, KALOGERAKI V, LUKOSE R, et al. Peer-to-peer computing: HPL-2002-57R1 [R]. HP Laboratories, 2003.

[3] KATZ J, LINDELL Y. Introduction to modern cryptography [M]. 2nd ed. Boca Raton, USA: Chapman and Hall/CRC, 2008.

[4] BUTERIN V. A next-generation smart contract and decentralized application platform [EB/OL]. [2018-12-08]. https://github.com/ethereum/wiki/wiki/White-Paper.

[5] 李剑锋. 基于拜占庭容错机制的区块链共识算法研究与应用[D]. 郑州: 郑州大学, 2018.

[6] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [EB/OL]. [2018-12-08]. https://www.colabug.com/3052594.html.

[7] 陆尧, 文捷. 基于比特币技术的供应链管控与溯源方案[J]. 计算机工程, 2018, 44(12): 85-93, 101.

[8] MCCONAGHY T, MARQUES R, MULLER A, et al. BigchainDB: a scalable blockchain database [EB/OL]. [2018-12-08]. http://blockchain.jetzt/wp-content/uploads/2016/02/bigchaindb-whitepaper.pdf.

[9] BROWN R G, CARLYLE J, GRIGG I, et al. Corda: an introduction [EB/OL]. [2018-12-08]. https://gendal.me/2016/08/24/corda-an-introduction/.

[10] GILBERT S, LYNCH N. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant Web services[J]. ACM SIGACT News, 2002, 33(2): 51-59.

[11] LAMPORT L. The part-time parliament [J]. ACM Transactions on Computer Systems, 1998, 16(2): 133-169.

[12] KING S, NADAL S. PPCoin: peer-to-peer crypto-currency with proof-of-stake [EB/OL]. [2018-12-08]. http://www.doc88.com/p-0788912122970.html.

[13] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.

[14] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling byzantine agreements for cryptocurrencies [EB/OL]. [2018-12-08]. https://blog.csdn.net/sanganqi_wusuierzi/article/details/78872360.

[15] LARIMER D. Delegated Proof-of-stake(DPoS) [EB/OL]. [2018-12-08]. http://bitsharestalk.org/index.php?topic=4009.60.

[16] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem [J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[17] CASTROM, LISKOV B. Practical Byzantine fault tolerance [EB/OL]. [2018-12-08]. http://www.pmg.lcs.mit.edu/bft/.

[18] SZABO N. Formalizing and securing relationships on public networks [EB/OL]. (1997-09-01) [2018-12-08]. https://ojphi.org/ojs/index.php/fm/article/view/548.

[19] 曾艾婧, 文捷, 刘百祥. 基于 LPN 的抗擦除攻击认证协议[J]. 计算机工程, 2019, 45(1): 122-128.

[20] ESKANDARI S, BARRERA D, STOBERT E, et al. A first look at the usability of bitcoin key management [EB/OL]. (2015-02-07) [2018-12-08]. https://arxiv.org/abs/1802.04351v1.

[21] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes [C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2014: 486-504.

[22] VALENTA L, ROWAN B. Blindcoin: blinded accountable mixes for bitcoin [C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2015: 112-126.

[23] CHAUM D. Blind signatures for untraceable payments [C]// Proceedings of Advances in Cryptology. Berlin, Germany: Springer, 1983: 199-203.

[24] DUFFIELD E, DIAZ D. Dash: a privacy centric crypto currency [EB/OL]. [2018-12-08]. https://cryptorum.com/resources/dash-whitepaper-privacy-centric-cryptocurrency.10/.

[25] NOETHER S, MACKENZIE A, CORE M. Improving obfuscation in the cryptonote protocol [EB/OL]. [2018-12-08]. https://www.docin.com/p-2122152949.html.

[26] MIERS I, GARMAN C, GREEN M, et al. Zerocoins: anonymous distributed E-cash from bitcoin [C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2013: 394-411.

[27] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin [C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2014: 459-474.

[28] NOETHER S, NOETHER S, MACKENZIE A. A note on chain reactions in traceability in cryptonote 2.0 [EB/OL]. [2018-12-08]. https://www.docin.com/p-2088809162.html.

[29] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments [EB/OL]. [2018-12-08]. https://download.csdn.net/download/vinsuan1993/10272806.

[30] MILLER A, BENTOV I, KUMARESAN R, et al. Sprites: payment channels that go faster than lightning [EB/OL]. [2018-12-08]. https://arxiv.org/abs/1702.05812v1.

[31] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies [C]//Proceedings of 2017 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2017: 473-489.

[32] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: an untrusted bitcoin-compatible anonymous payment hub [EB/OL]. [2018-12-08]. http://cs-people.bu.edu/heilman/tumblebit/.

[33] COURTOIS N T, BAHACK L. On subversive miner strategies and block withholding attack in bitcoin digital currency [EB/OL]. [2018-12-08]. https://www.docin.com/p-2122153184.html.

[34] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable [C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2014: 436-454.

[35] KARAME G O. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin [EB/OL]. (2018-12-08) [2018-12-08]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.400.6276.

[36] ROSENFELD M. Analysis of hashrate-based double spending [EB/OL]. [2018-12-08]. http://www.oalib.com/paper/4043738.

[37] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on Ethereum smart contracts (SoK) [C]//Proceedings of International Conference on Principles of Security and Trust. Berlin, Germany: Springer, 2017: 164-186.

[38] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin's peer-to-peer network [C]//Proceedings of Usenix Conference on Security Symposium. Berkeley, USA: Usenix Press, 2015: 129-144.

[39] 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 Press, 2016: 45-59.

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

[41] MILUTINOVIC M. Proof of luck: an efficient blockchain consensus protocol [EB/OL]. [2018-12-08]. https://arxiv.org/abs/1703.05435.

[42] REN L. Proof of stake velocity: building the social currency of the digital age [EB/OL]. [2018-12-08]. http://www.reddcoin.com/papers/PoSV.pdf.

[43] BONEH D, FRANKLIN M. Identity based encryption from the weil pairing [C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 2001: 213-229.

[44] SAHAI A, WATERS B. Fuzzy identity based encryption [C]//Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2005: 457-473.

[45] DINH T T A. Untangling block-chain: a data processing view of blockchain systems [EB/OL]. [2018-12-08]. https://arxiv.org/abs/1708.05665.

[46] RABIN M O. Transaction protection by beacons [J]. Journal of Computer and System Sciences, 1983, 27(2): 256-267.

[47] JOSEPH B, CLARK J, GOLDFEDER S. On Bitcoin as a public randomness source [EB/OL]. [2018-12-08]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.738.2393&rep=rep1&type=pdf.

[48] POPOV S. On a decentralized trustless pseudo-random number generation algorithm [J]. Journal of Mathematical Cryptology, 2017, 11(1): 60-64.

[49] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol [C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 2016: 357-388.

[50] SYTA E, JOVANOVIC P, KOGIAS E K, et al. Scalable bias-resistant distributed randomness [C]//Procedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2017: 22-26.

[51] PHILIPP S. HydRand: practical continuous distributed randomness [EB/OL]. [2018-12-08]. https://uk.makemefeed.com.

[52] SCHOENMAKERS B. A simple publicly verifiable secret sharing scheme and its application to electronic voting [C]//Proceedings of CRYPTO'99. Berlin, Germany: Springer, 1999: 1-6.

[53] HANKE T, MOVAHEDI M, DOMINIC WILLIAMS D. DFINITY technology overview series, consensus system [EB/OL]. [2018-12-08]. http://arxiv.org/abs/1805.04548.

[54] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]//Proceedings of ASIACRYPT'01. Berlin, Germany: Springer, 2001: 1-5.

编辑 陆燕菲