区块链关键技术探析

郝鹏宇[1] 季国华[2] 杨 琴[3] 杨瑞青[4] 魏彩颖[5]
硅湖职业技术学院，江苏 苏州 215000

[摘要]区块链技术起源于数字货币，近些年来，随着比特币的兴起受到了世界各地的广泛关注和热议。区块链具去中心化、高度自治、可追溯、不可篡改等特性，颠覆了传统中心化的数据治理模式,具有极为广阔的发展前景。文章以区块链为研究对象，围绕区块链的链式结构、安全机制、智能合约、共识算法、跨链机制等核心要素展开了讨论，同时总结和梳理了相关技术的特点。
[关键词]区块链；密码学；共识机制；智能合约；跨链
DOI：10.33142/sca.v5i1.5552 中图分类号：TP393.08 文献标识码：A

Analysis of Key Technologies of Blockchain

HAO Pengyu [1], JI Guohua [2], YANG Qin [3], YANG Ruiqing [4], WEI Caiying [5]
Silicon Lake Vocational & Technical Institute, Suzhou, Jiangsu, 215000, China

Abstract: Blockchain technology originated from digital currency. In recent years, with the rise of bitcoin, it has attracted extensive attention and hot discussion all over the world. Blockchain has the characteristics of decentralization, high autonomy, traceability and non tampering. It subverts the traditional centralized data governance model and has extremely broad development prospects. Taking blockchain as the research object, this paper discusses the core elements of blockchain, such as chain structure, security mechanism, smart contract, consensus algorithm and cross chain mechanism, and summarizes and combs the characteristics of related technologies.
Keywords: blockchain; cryptography; consensus mechanism; smart contract; cross chain

引言

区块链作为一种全新的去中心化自治系统，其设计理念可谓十分精妙，如：链式结构、安全机制、智能合约、分布式共识算法、跨链机制等均是区块链系统不可或缺的要素，发挥着至关重要的作用，区块链很好地解决了复杂环境中参与方之间的信任构建和隐私保护问题，在金融、供应链、电子政务等领域中都得到了广泛的应用[1-3]。

1 链式结构

链式结构是区块链的基本特征，本质是一个以区块为元素的链表，交易都存放在区块中，每个区块分为两部分：区块头和区块体，从图 1 中可以发现，区块体中负责存储交易内容，区块头包含了版本号、时间戳、随机数、Merkle 根以及前置哈希等信息，区块间凭借前置哈希相关联，构成链式结构。

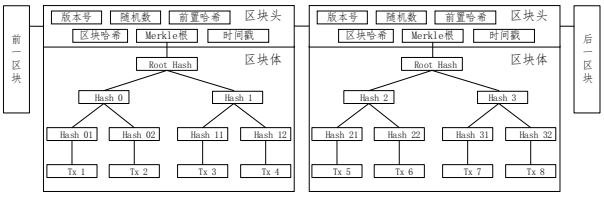

图 1 区块链链式结构

2 安全机制

安全机制是区块链系统的基石，涉及身份认证、隐私保护、加密通信等相关议题，区块链系统中应用了几类典型的密码学技术具体包括：哈希算法、对称加密算法、非对称加密算法。

哈希函数可以把任意长度的输入映射成固定长度的输出，即散列值，所以也被称为安全散列函数。常见的哈希算法包括：MD5、SHA1、SHA256 和 SM3，如表 1 所示。

表 1 哈希算法对比表

对比项	MD5	SHA1	SHA256	SM3
运算速度	快	中	较 SHA1 略低	较 SHA1 略低
输出大小/位	128	160	256	256
安全性	低	中	较高	高

对称加密算法中，参与方使用同一套秘钥对信息进行加密与解密操作，常见的对称加密算法包括：SM4、DES、3DES、AES，如表 2 所示。

表 2 对称加密算法对比表

对比项	SM4	AES	DES	3DES
算法结构特征	基本轮函数加迭代、含非线性变换	轮函数加迭代、含非线性变换	标准的算术和逻辑运算，不含非线性变换	标准的算术和逻辑运算，不含非线性变换
计算轮数	32	10/12/14	16	48
秘钥长度/位	128	128/192/256	64	128
有效密钥长度/位	128	128/192/256	56	112
实现难度	易于实现	略难于 SM4	易于实现	易于实现
安全性	高于 3DES	高于 3DES	低	较高

非对称加密依赖于两个秘钥，其中公钥可以公开，而私钥需要秘密保存，一般被用数据加密和数字签名。常见的非对称加密算法包括：SM2、RSA、ECC，如表 3 所示。

表 3　非对称加密算法对比表

对比项	SM2	ECC	RSA
算法结构特征	基于椭圆曲线	基于椭圆曲线	基于特殊的可逆模幂运算
计算复杂度	指数级	指数级	亚指数级
相同性能下密钥长度	较少	较少	较多
密钥生成速度	较 RSA 快百倍	与 SM2 相近	慢
加密解密速度	快	快	一般

3 智能合约

智能合约大大增强了区块链技术的灵活性，合约的执行环境是一个相对封闭、具有约束性的沙盒，合约代码在内部执行并且对外隔离[4]。常见的合约执行环境分为容器和虚拟机两类，如表 4 所示。

表 4　合约运行环境

序号	智能合约安全计算环境	代表系统	合约语言
1	EVM 虚拟机	Ethereum	Solidity，Serpent，LLL 等
2	Docker 容器	HyperledgerFabric	Golang，Java 等
3	JVM 虚拟机	Corda	Kotlin，Java 等
4	NeoVM 虚拟机	NEO	C#，Java，Kotlin，Python，Golang 等

由于各区块链的底层结构不同，每个系统中关于智能合约的运行机制也略有差异，一般而言，如图 2 所示，当节点收到交易请求时会在本地沙箱调用对应的合约代码，若符合触发条件，则根据合约规则执行并同步更新状态数据库，继而将交易打包放入区块，最后，区块经共识环节确认有效无误后方可“上链”。

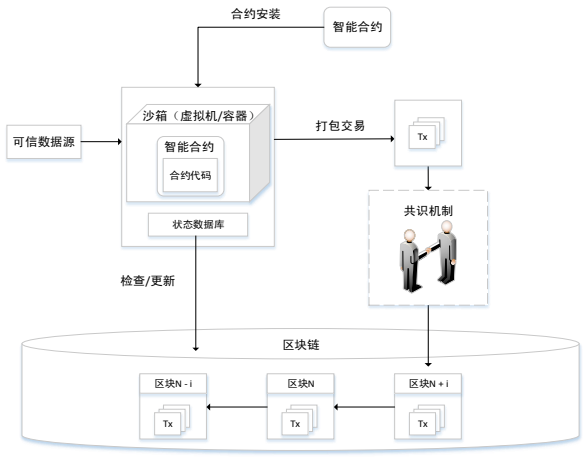

图 2　合约执行机制

4 共识算法

共识算法是一种解决分布式节点如何达成“一致性”问题的策略。不同的共识机制在可用性方面存在一定差异，常见的共识机制有：Paxos/Raft、PoW、PoS、DPoS、PBFT 等，如表 5 所示。

Paxos 与 Raft 类似，在 Raft 共识中每个节点最开始的身份均为 Follower，待进入共识阶段，节点切换到 Candidate，并发起选举请求。当 Candidate 状态的节点，接收到超过半数的赞成票，则升级为 Leader。Leader 向所有 Follower 节点广播事务，如果 Leader 收到超过半数的响应，则会先提交本地事务，并接着向全网广播提交通知，各 Follower 节点收到该消息后，随即在本地执行事务提交操作，最终达成集群数据一致。PoW 本质是借助算力找出某个随机数参与哈希运算并使得结果满足难度要求，该机制需要大量的算力，资源消耗最高。PoS 共识中股权的多少代表了各参与方权益的大小，通过寻找权益较大的节点来竞争出块权，若权益越大，其挖矿难度系数就越低，否则反之。DPoS 是指将持有一定资产的节点视为股东，各股东按照自身资产实际情况做出适量的投票，选出若干节点作为股东代理人，由股东代理人负责轮流生成区块，并赚取一定量的报酬。PBFT 共识略显复杂，每个节点会经历 Pre-prepare/Prepare/Commit 三个环节，每个回合都会有一个特定的节点被选为主节点，首先，在 Pre-prepare 环节由主节点广播消息并通知其他副节点进入共识流程。其次，在 Prepare 环节每个副节点会将接收到的消息分发给其他节点，所有节点会根据所收集到消息的数量是否足额、内容是否一致等情况来共同决定能否进入下一阶段，若进入下一阶段，各节点会再次向其他节点进行广播，发送确认消息。最后，在 Commit 环节各节点会对确认消息的数量进行统计，在收到足额的确认消息后（代表大多数节点都好了执行请求的准备），并向其他节点广播提交通知，各节点会执行事务提交操作，结束这一回合。

PoW 去中心化特性非常显著，具有较好的安全性，但是资源浪费巨大，相较而言，PoS 在一定程度上能降低 PoW 对计算资源的消耗，但是在去中心化方面的表现则不如 PoW。DPoS 在 PoS 的基础之上做了进一步修正，通过削弱去中心化程度，来提升吞吐率。PBFT 具有较好的效能，但是随着共识节点数量的增加，PBFT 共识的共识时间及通信复杂度也会急剧增加，不太适用于含有大规模节点的场景。Paxos 与 Raft 算法应用范围非常局限，基本不具备对恶意节点（拜占庭节点）的防御能力，常见于没有拜占庭错误的分布式系统中[5-6]。

5 跨链机制

跨链技术是实现区块链间数据迁移、互联互通的重要手段。常用的跨链技术包括：（1）公证人机制；（2）分布

表 5 共识机制对比表

对比项	PoW	PoS	DPoS	PBFT	Paxos/Raft
适用场景	公链	公链/联盟链	公链/联盟链	联盟链	故障容错分布式系统
代表系统	BitCoin	Cosmos	EOS	Hyperledgerfabric	Etcd
故障容错率	小于 1/2	小于 1/2	小于 1/2	小于 1/3	小于 1/2
拜占庭容错率	小于 1/2	小于 1/2	小于 1/2	小于 1/3	0
缺点	资源消耗大，且交易确认时间长	易形成寡头	易形成联合垄断局面	确认环节复杂，且节点数量不宜过多	不具备恶意节点的防御能力，只能容错故障节点

表 6 跨链技术对比表

对比项	公证人机制	哈希时间锁定机制	分布式私钥控制机制	侧链/中继机制
跨链交易	支持	支持	支持	支持
安全性	低	中	中	中
交易速度	中	中	中	慢
实现难度	中	易	中	难
典型案例	Interledger	LightingNetwork/ZcashXCAT	Fusion	Cosmos/Polkadot

式私钥控制机制；（3）哈希时间锁定机制；（4）侧链/中继技术。如表 6 所示。

公证人机制通过引入权威机构或者可信群体作为第三方中介，负责资产托管与冲突仲裁，实现资产跨链转移。哈希锁定技术是指通过哈希锁将发起方的 Token 锁定，如果另一方能够在约定时间内提供相匹配的密码学证明，并且与之前约定的哈希值一致，即可将 Token 成功解锁[7-8]。分布式私钥控制技术本质是将密钥分配给不同参与方，各参与者保存一个密钥份额，当所收集的密钥份额达到一定数量时，即可实现密钥恢复，从而完成资产解锁操作。侧链/中继技术的思想是“以链治链”，通过特殊的区块链作为中间方连接多条交易链，以去中心化的方式完成链间数据迁移。

6 结束语

区块链作为新一代解决信任问题的普适性基础设施，具有去中心化、高度自治、不可篡改、可追溯等特性。目前，区块链的发展尚处于探索阶段，仍有一些本质性的问题需要深入研究，相信随着区块链各类基础理论和底层技术的日趋成熟与完善，区块链系统也将展现出更高的价值，迎来更广阔的发展空间。

[参考文献]

[1]章峰，史博轩，蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报，2018，4(4)：22-29.
[2]单进勇，高胜. 区块链理论研究进展[J]. 密码学报，2018，5(5)：484-500.
[3]斯雪明，徐蜜雪，苑超. 区块链安全研究综述[J]. 密码学报，2018，5(5)：458-469.
[4]贺海武，延安，陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展，2018，55(11)：2452.
[5]于鸿源，叶雄兵，张立韬，等. 基于 Ripple 共识机制的分布式作战资源分配方法研究[J]. 信息工程大学学报，2019(6)：1.
[6]范捷，易乐天，舒继武. 拜占庭系统技术研究综述[J]. 软件学报，2013(6)：1346-1360.
[7]李芳，李卓然，赵赫. 区块链跨链技术进展研究[J]. JournalofSoftware，2019(6)：1649-1660.
[8]张诗童，秦波，郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全，2020，9(11)：1.
作者简介：郝鹏宇（1989-）男，江苏苏州人，助教，硕士；研究方向：区块链技术，信息安全。