区块链原理及其核心技术

蔡晓晴[1] 邓 尧[1] 张 亮[1] 史久琛[1] 陈 全[1),2)] 郑文立[1]
刘志强[1] 龙 宇[1] 王 堃[3)] 李 超[1] 过敏意[1),2)]

[1)](上海交通大学计算机科学与工程系 上海 200240)
[2)](上海交通大学上海先进通信与数据科学研究院 上海 200240)
[3)](南京邮电大学物联网学院 南京 210023)

摘 要 随着第一个去中心化加密货币系统——比特币系统自 2009 年上线成功运行至今,其背后的区块链技术也受到广泛关注.区块链技术独有的去中心化、去信任的特性,为构建价值互联平台提供了可能.在比特币白皮书中,区块链的概念十分模糊,而现有的一些介绍区块链的文章中,也多从抽象层次进行介绍,对于更深入的后续研究提供的帮助十分有限.本文首先将区块链技术从具体应用场景中抽象出来,提取出其五层核心架构,并就其中数据、网络、共识三层基础架构作详细说明.这三层架构包含了区块链系统中的三大核心技术:密码学、共识算法、网络.文中介绍这三种技术的研究现状,能够使读者迅速了解区块链技术的发展状况,并能根据自己的需要进行深入阅读.最后,介绍了区块链目前的应用现状和技术展望.

关键词 区块链;比特币;密码学;共识算法;P2P 网络;区块链应用
中图法分类号 TP311 **DOI 号** 10.11897/SP.J.1016.2021.00084

The Principle and Core Technology of Blockchain

CAI Xiao-Qing[1)] DENG Yao[1)] ZHANG Liang[1)] SHI Jiu-Chen[1)] CHEN Quan[1),2)] ZHENG Wen-Li[1)]
LIU Zhi-Qiang[1)] LONG Yu[1)] WANG Kun[3)] LI Chao[1)] GUO Min-Yi[1),2)]

[1)](*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)
[2)](*Shanghai Institute for Advanced Communication and Data Science, Shanghai Jiao Tong University, Shanghai* 200240)
[3)](*College of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing* 210003)

Abstract While the first decentralized cryptocurrency system, Bitcoin, has run successfully since it was launched in 2009, the underlying technology, blockchain, now draws increasing attention. Based on the unique decentralization and trusted features of blockchain, it is possible to build a value-connected platform. However, the Bitcoin white paper does not provide a rigorous definition of blockchain. Meanwhile, prior related work mainly introduces high level concepts in blockchain, ignoring the important technique details. To provide an in-depth introduction of blockchain, this survey first extracts the blockchain technology from specific application scenarios, breaks the blockchain architecture into five core layers, and elaborates on the data, network, and

收稿日期:2018-09-14;在线发布日期:2019-12-19.本课题得到国家重点研发计划项目(2018YFB1004800)、国家"九七三"计划项目(2015CB352403)、国家自然科学基金项目(61872240,61602301,61632017,61702329,61832006,61702328)、上海市科技创新行动计划(19511101403)资助.**蔡晓晴**,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为区块链.E-mail:cai-xq@sjtu.edu.cn.**邓 尧**,硕士研究生,中国计算机学会(CCF)学生会员,主要研究方向为区块链.**张 亮**,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为分布式系统、数据流、区块链.**史久琛**,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为分布式系统、区块链.**陈 全**,博士,特别研究员,中国计算机学会(CCF)会员,主要研究领域为分布式计算、计算机体系结构、区块链.**郑文立**,博士,特别副研究员,中国计算机学会(CCF)会员,主要研究方向为分布式系统、云计算、区块链.**刘志强**,博士,副教授,中国计算机学会(CCF)区块链专委会委员,主要研究方向为区块链、信息安全与密码学.**龙 宇**,博士,副教授,主要研究方向为密码学、区块链.**王 堃**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为区块链、能源互联网、边缘计算.**李 超**,博士,特别研究员,中国计算机学会(CCF)会员,主要研究领域为面向新应用新技术的体系结构.**过敏意**(通信作者),博士,教授,中国计算机学会(CCF)会士,主要研究领域为并行计算、分布式系统、大数据、区块链.E-mail:guo-my@cs.sjtu.edu.cn.

万方数据

consensus layers. More specifically, we introduce state-of-the-art techniques of three main components of a blockchain system: cryptography, consensus algorithm, and network in detail. We firstly introduce basic cryptographic tools involved in blockchain systems, such as hash calculation, Merkle tree, digital signature, elliptic curve digital signature algorithm (ECDSA), ring signature algorithm, zero-knowledge proof, and anti-quantum cryptographic algorithm. We then summarize the mainstream consensus processes involved in the existing systems and refine the consensus framework. Users can choose different consensus components to build their own consensus models according to the characteristics of the application scenarios. The end of the consensus section introduces the methods for modeling consensus algorithms abstractly and the two approaches used to formally prove and analyze the essential features of consensus models. Further, we introduce the network topologies and common network protocols adopted in blockchain systems. In addition, we introduce three hot issues related to blockchain, which are privacy protection, common attack schemes and capacity expansion. The paper analyzes the existing research results on the anonymity of Bitcoin, and then introduces three options to enhance its privacy: mixed currency, ring signature and zero knowledge proof. The existing attack schemes are divided into two categories in the paper, one based on the consensus model adopted by the system, and the other based on the network. We summarize the existing blockchain expansion schemes as single-chain extensions and cross-chain extensions, and analyze the two types in detail. At last, the current application situation and technical prospects of blockchain are introduced. We introduce three phases of the development of blockchain application, namely the digital currency, smart contract and new extensions in other areas. We compared different digital currencies in terms of purpose, distribution method, consensus algorithm and other aspects. We select three typical systems, Ethereum, Hyperledger and Enterprise Operation System (EOS), as the examples to show how to build smart contracts. Blockchain has made significant impact on the innovation and evolution of various fields, especially in the areas of Internet of Things, medical and public key infrastructure. Compared with other blockchain surveys, this survey summarizes and refines the papers in the blockchain field rather than a simple combination of prior work. For example, in the introduction to the consensus module, we extract a general framework from many existing consensus models. We split the consensus instances in different systems according to the hierarchy of the framework, and extract the components that are necessary for building a consensus model. Based on this survey, readers are able to understand the development of blockchain quickly and can explore in depth according to their respective needs.

Keywords　blockchain; Bitcoin; cryptography; consensus algorithm; P2P network; blockchain application

1　引　言

区块链技术起源于比特币，后者是目前最成功的数字货币. 数字货币的概念在 1983 年被第一次提出[1]，此后随着互联网的大规模发展，其应用场景越来越广泛，社会对于货币数字化的需求也越来越急切. 从字面概念来看，相比于物理形式，以数字化形式存在的货币就是数字货币，也可以被称为电子货币. 不过，数字货币通常不包括仅在形式上数字化的，由各国银行发行的数字化法币. 基于这个前提，按照不同的目的，数字货币可以分为两种：虚拟货币和流通货币. 虚拟货币是由其开发者控制的，是一种对价值的数字化体现，并且在特定的社区环境下使

万方数据

用①.在设计之初,虚拟货币主要被用于游戏社区,现在其应用更加广泛,但是依然受限于特定环境.另外一种数字货币则用于流通,其初衷即成为价值交换的中介.根据其是否利用密码学原理,可以分为密码货币和非密码货币,二者区别在于是否利用密码学原理保障了交易的安全性和控制新币的发行②.

交易的形式和内容越来越复杂,表征着价值交换的种类越来越丰富,随之而来的一个显著问题就是交易信息本身的价值保护问题.除了交易参与方之外,交易本身应该是透明、对外不可见的.而现存的交易系统通常需要无关第三方的介入,因而无法实现这一目标.在这种需求下,密码货币诞生了.密码货币的诞生是对非密码货币的一种改进和提升,它的设计初衷即成为独立的货币系统,而不是附属货币系统.表 1 介绍了不同的数字货币.

表 1 密码货币与非密码货币举例

种类	名称	创建时间	发行机构(发明人)	主要特征
非密码货币	E-gold③	1996	Gold & Silver Reserve Inc.	一种网络货币,与黄金等值兑换,提供收付款的中介平台
	Digital Monetary Trust④	1999	James Orlin Grabbe	提供匿名账户平台,在用户与银行间交互
密码货币	Hashcash⑤	1997	Adam Back	提出工作量证明机制
	B-money⑥	1998	Wei Dai	匿名,分布式电子现金系统
	Bit Gold⑦	1998	Nick Szabo	去中心化货币机制

密码货币的意义除了将货币形式改变之外,更深层的愿景在于能安全地简化价值交换过程,去除中心化架构中无关第三方的介入.比特币作为密码货币的一个典型实例,其设计思路正是如此.比特币以去中心化、去信任为核心目标,其架构与运作机制也贯彻这一设计思路.在没有中心机构做背书的情况下,账本数据通过分布式节点进行多处备份,而每次对账本的更新需要付出相应代价,从而阻止恶意节点对账本的破坏.整个系统由奖惩机制驱动,节点付出的合理代价被验证即可获得奖励,驱动系统进行良性循环.

比特币所依赖的底层技术并不是一种完全新的技术,而是根据比特币系统需要的特性将已有的技术结合起来,如密码学、分布式系统、P2P 网络、博弈论等.比特币的发明过程借鉴了 Adam 在 Hashcash⑧ 中设计的工作量证明机制、Haber 和 Stornetta[2] 提出的用于保证数字文件安全的时间戳方法、Dai 在 B-money⑨ 中设计的奖惩机制.迄今为止,比特币系统已经上线成功运行 10 年时间,显示了高度的稳定性和可靠性.随着比特币大获成功,其底层技术也越来越受到关注,即本文陈述的对象——区块链技术.

区块链这一概念首次出现在比特币白皮书[3]中,但是该白皮书并未对区块链做出精确定义.虽然近年来区块链的潜力被逐渐挖掘并应用到货币系统之外的诸多领域,但由于其技术本身还不够完善,变体也有很多,所以截至目前依然没有一个确切的定义.现有的成熟区块链系统,如比特币、以太坊等,其顶层应用主要完成价值交换的功能,因此也常将区块链技术称为分布式账本技术.虽然被称为账本技术,但其本质只是一种抽象概念,是一种以区块形式组织成的数据库.理解成特殊形式的数据库后,则可以摆脱金融应用场景的局限性并找到其他适用领域,凡需要全局性、历史性地记录数据的场景都可以使用区块链技术.总体而言,区块链技术是以数据库作为数据存储载体,以 P2P 网络作为通信载体,依赖密码学确定所有权和保障隐私,依赖分布式系统共识框架保障一致性,旨在构建价值交换系统的技术.

虽然区块链的概念出现已经有十年时间,然而前期的关注重点主要在于比特币系统是否安全可靠,对于区块链技术总体的提炼总结较少.而随着以太坊、EOS 等平台的发展,人们逐渐认识到区块链技术不仅局限于比特币,还可以应用于产地溯源、物流跟踪、物联网记录等更多场景.本文将区块链技术从特定的应用场景中抽象出来,客观地归纳总结区块链本身所包含的技术内容,使读者对技术本身有更清晰的认识.在目前已经发表的区块链论文,如 Zheng 等人[4]、Lin 等人[5]、Li 等人[6]、袁勇等人[7]、何蒲等人[8]、邵奇峰等人[9]、陈伟利等人[10]的工作中,都只抽象、概括性地介绍了区块链技术中的几项核心技术,大多着重于介绍,而没有从理论、形式化的证明中展现出各项技术的发展情况.

尽管区块链技术的热度越来越高,然而作为新兴的技术,还有很多不足之处.区块链最初以应用的

① Bank E C. Virtual Currency Schemes—A Further Analysis. February 2015. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

② Greenberg A. Crypto currency. APR 20, 2011. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#26f0bb81353e

③ E-Gold. https://en.wikipedia.org/wiki/E-gold

④ Grabbe J O. The Digital Monetary Trust. https://web.archive.org/web/20080905150703/ http://www.orlingrabbe.com/dmt1.htm

⑤ Back A. Hashcash. 1997. http://www.hashcash.org/

⑥ Dai W. Bmoney. http://www.weidai.com/bmoney.txt

⑦ Szabo N. Bit Gold. 2005. https://nakamotoinstitute.org/bit-gold/

⑧ Back A. Hashcash. 1997. http://www.hashcash.org/

⑨ Dai W. B-money. http://www.weidai.com/bmoney.txt

万方数据

形式诞生于比特币，关于其相关技术理论分析的综述文章还很少.本文选取了逾百篇区块链技术的相关文章进行分析、总结、对比，深入详细地介绍了区块链中密码学、共识算法、网络三大核心技术的重要意义和丰富内涵，包括在密码学的相关部分中介绍了对于比特币安全性的数学论证及提出的解决方案，在共识算法的相关部分中介绍了区块链共识算法与传统分布式系统共识算法的区别与联系、现有共识算法 POW，POS，DPOS，POC，POL，PBFT，RAFT 的核心步骤及算法之间的差异和联系，在网络相关部分中介绍了区块链系统中使用的网络协议与网络攻击方式.除此之外，本文对于各项核心技术的设计原理进行了分析和解释，使读者能获得对各项技术更为立体多维的理解，也便于读者找到自己的兴趣点进行更深层次的研究.

本文对区块链的介绍主要分为 6 节：第 1 节介绍区块链的发展背景；第 2 节介绍区块链系统的核心概念和基本运作机制；第 3 节介绍区块链系统中的三大核心技术（密码学、共识算法、网络）；第 4 节介绍区块链领域中的热点问题，包括隐私、安全和性能三个方面；第 5 节介绍区块链技术在各领域的应用，并介绍区块链系统目前存在的技术挑战及展望；第 6 节总结全文.

2　运作机制

2.1　概述

本节将介绍区块链系统的基本运作机制和核心概念.为了便于理解，本节首先以比特币为例进行介绍，再从中提取出区块链的核心技术，阐述区块链系统是如何运作的.

2.2　比特币系统运作机制

2.2.1　比特币的核心数据结构——账本

在介绍比特币系统的运作机制前，首先要了解其基础结构.对于任何金融系统来说，最核心最基础的数据结构就是记录交易的账本.账本的由来已久，最早可以追溯到 1494 年，目前主要使用的记账系统是一种复式记账系统，最早由意大利数学家 Pacioli 制定[11].复式记账法对每一笔账目同时记录来源和去向，首次将对账验证功能引入记账过程，提升了记账的可靠性[11].比特币中的账本也是一种可以对账验证的账本.与物理账本类似，比特币账本可以划分为不同的粒度，交易、区块、区块链（这里是一个狭义含义，仅表示一种数据结构），分别对应于物理账本中的一条记录、包含多个记录的一页、包含多页的完整账本.

（1）交易

比特币系统中的交易记录与物理账本中的交易记录类似，每一条交易记录需要记录输入、输出地址以及转让的数目，简单来说就是类似于账户 A 转向账户 B 转移多少比特币的记录.比特币中交易的输入来源于（之前某笔其他交易中的输出）未被使用的交易输出（Unspent Transaction Output，UTXO），注意该概念不等同于用户的账户余额.UTXO 是不可再分割，参与交易的基本单位.UTXO 本身不能被拆分，但是可以通过调整输入输出完成指定交易.比如，如果 UTXO 小于目标值，可以添加多个 UTXO 作为输入；如果 UTXO 大于目标值，可以添加自己的地址作为找零输出，完成交易.在每笔交易中，都会消耗已有的 UTXO，并产生新的 UTXO，价值的转移就是通过 UTXO 的变化完成的，如图 1.

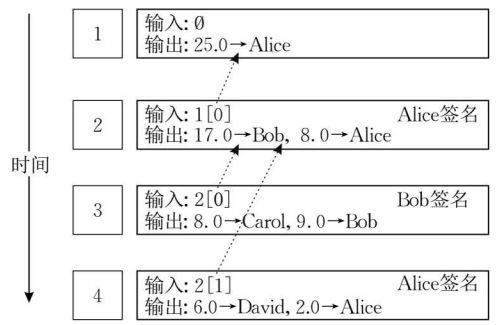

图 1　UTXO 的转移过程

UTXO 的生产和使用是由密码学中数字签名保障的.产生 UTXO 即产生交易输出时，需要使用锁定脚本将比特币锁定到指定账户地址中；使用 UTXO 即产生交易输入时，需要使用有正确签名的解锁脚本（使用用户私钥签署）才能解锁指定地址中的比特币.

比特币中脚本语言是一种基于逆波兰表示的堆栈执行语言.用于计算的栈结构提供的功能十分有限.通常不提供循环或者其他复杂流控制，这种设计能防止恶意控制流的攻击.脚本执行的结果通常是可以预见的，并不因执行者身份不同或者执行地点不同或者其他原因改变，因此一定程度上保证了交易的客观性和正确性.目前比特币系统中支持的交易脚本语言主要有 P2PKH，P2PK，MS（限 15 个密钥），P2SH 和 OP_Return 等[12].

（2）区块和区块链

比特币账本中的区块可类比物理账本中的一页，区块记录一段时间内的交易，由一个包含元数据

万方数据

的区块头和许多条交易记录组成.区块头包括了很多数据,如父区块的哈希值、时间戳、Merkle 树根(用于有效总结区块中所有交易的数据结构)和区块高度等.区块头可连接前一区块,使得区块中的每笔交易都是可追踪、有据可查的.通过区块头哈希值和区块高度可以区分不同区块,区块的哈希值能够唯一标识区块.将这些区块根据区块头中的哈希指针链接成一个链就是一个完整的账本了,也就是狭义的区块链.区块链的整体结构如图 2 所示.

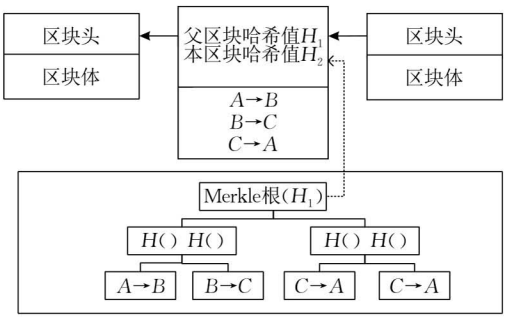

图 2 交易、区块和区块链的关系

2.2.2 比特币运作机制

比特币系统的运作机制就是其完成记账的过程.这里需要区分的是,发起交易和交易记账是两个不同的过程.发起交易是用户相关的过程,而交易记账则是货币系统中的过程,记账操作对用户来说是透明的.

在中心化系统中,账本的记账权属于账本所有者,比如,银行的账本由银行控制记账权,商店的账本由商店控制记账权.而在比特币系统中,其目标是去中心化去信任,因此账本的记账权不能控制在某个中心或是单一机构中.所以比特币采用分布式系统实现去中心化,将记账权下放到分布式系统中的节点中.具体每笔交易由哪个节点记到账本上并不确定,需要各个节点参与竞争选取.这个竞争过程需要各个节点付出一定的代价以防作恶,各节点只有诚实遵守规则付出代价才会受到系统的奖励,恶意破坏系统将会得不偿失.信任就是在这个过程中建立的,在比特币中该过程也可以叫作挖矿,各个节点则被称为矿工.

在解决记账权从属问题后,应该考虑其他节点应如何同步更新,也就是分布式系统中如何保障一致性的问题.数据一致性的保障,和记账权的确立一样,也由系统中共识算法决定.共识算法中的最长链规则,使得各个节点在接收到新区块的数据时,必须停止当前的挖矿工作,并立刻对新区块进行验证.否则节点就无法保证自己之后的工作是基于最长链的,其他节点将不认同他挖出的区块.

万方数据

比特币系统中的消息传播方式由其网络结构决定.比特币中构建的分布式系统是一个松散的系统,系统中的节点以 P2P 网络连接通信,并且系统中的节点无需身份验证,因此系统中节点可以自由参与或退出.

整个运作机制可以简述为:首先由客户端发起一笔交易,将该交易发送到比特币网络中任意节点.节点在收到交易后验证交易是否正确,如果验证不通过,节点将拒绝该交易,并向发送者返回交易被拒绝的消息.如果验证通过,节点将收到的交易放入自己的交易池中,并向网络中继续传播.各节点从各自交易池中打包交易,并通过加入随机数进行计算.最先计算出符合要求哈希值的节点打包的区块有效,即该节点获取了所打包交易的记账权.之后该节点将自己通过计算得到的区块广播到区块链网络中,其他节点接收到新区块后,会立即验证该区块的正确性.验证成功后将新区块连接到自己的链中,同时删除自己交易池中已经被打包的交易记录,再重新开始新一轮的生产区块过程.上述过程可以概括为图 3 中所示流程.

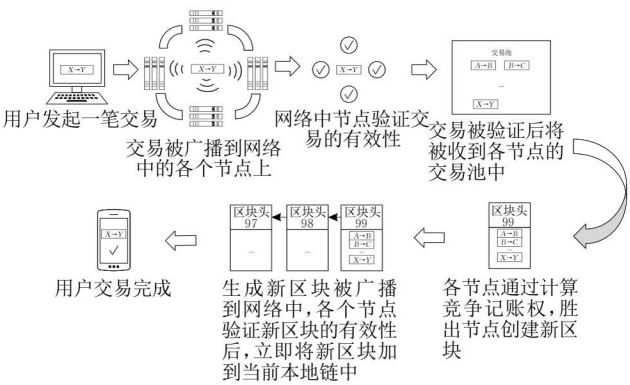

图 3 比特币系统运转流程

2.3 区块链系统运作机制

上文简单介绍了比特币系统中的核心数据结构和运作机制,本节将剥离比特币中的货币属性,提取区块链技术中的核心数据结构和工作机制.

2.3.1 核心数据结构

区块链概念来源于比特币,因此最初的区块链系统也大多沿袭了比特币中的链式结构.随着研究的深入,出于性能、安全性等不同方面的考虑,新的区块链数据结构被提出,如树状结构和图状结构,下面将分别介绍上述三种结构.

2.3.1.1 链式结构

在链式区块链系统中,核心组件与比特币中相似,也可以划分成三级粒度,分别是一条数据记录、包含多条记录的区块、由哈希指针链接的区块链.在

链式结构中，除了第一个区块和最后一个区块外，其他区块都只有一个前驱区块和一个后继区块. 在多个矿工共同挖矿过程中，可能出现不同矿工在同一个父区块上挖出不同子区块的情况，但是最终只会有一个子区块得到确认，并被最终连接入主链.

区块中的数据记录可以根据不同的应用场景，设计不同的字段. 如比特币中的数据记录——交易，一般需要包括输入、输出、时间戳，见图 4. 输入附带的脚本包含用户的私钥签名，输出附带的脚本使用对方的公钥锁定. 输入输出脚本是数字签名机制的具体实现形式，用于保障用户的所有权. 以太坊中平台能够运行更加复杂的智能合约，因此其交易字段的设计更加复杂，可以增加“data”字段记录需要调用的代码函数及传入参数等. 如果链中记录的是医疗、物联网数据等，则可以为不同时间点需要上链的数据.

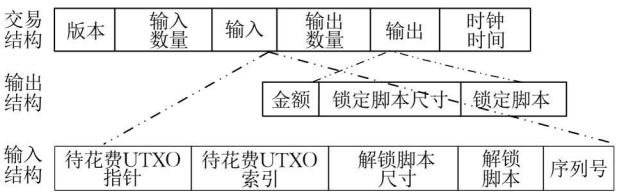

图 4　比特币中交易结构

区块由一个包含元数据的区块头和一组具体的数据记录组成. 区块对于数据记录的组织主要体现在区块头中的 Merkle 树根. Merkle 树也可以称作哈希树，其叶子节点为数据记录，非叶子节点是其对应子节点串联字符串的哈希值. 由于 Merkle 树是通过哈希值组织起来的树，对于交易记录的任何一点改变都能体现在 Merkle 树根值上，因此能够容易地验证数据是否被恶意篡改过. 在不同系统中，可根据具体需求对 Merkle 树进行改造. 如以太坊中使用 Merkle Patircia 树(MPT)进行记录，记录系统的状态、交易、收据. 因此以太坊区块头中包括三棵树，分别为状态树、交易树、收据树.

除了 Merkle 树根值外，区块头中通常还记录用于表明区块身份的信息(如 ID、哈希值等)以及该区块被合理生成的证明. 区块被合理生成的证明指的是矿工参与共识竞争记账权付出代价的证明，不同共识算法矿工需要提交不同的证明信息. 如在比特币、以太坊系统中，是矿工多次尝试找到满足某一条件的随机数. 一些轻量级节点验证数据记录时，只需要区块头的数据即可，无需下载所有的完整区块. 区块头中的父哈希用于连接各个区块，也可以看成是哈希指针. 各个区块依次连接形成区块链，其结构见图 5.

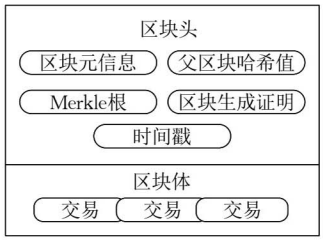

图 5　区块结构和区块头结构

2.3.1.2　树状结构

树状结构与链式结构的区别主要在于区块的组织形式，区块内容类似. 树状结构中，创世区块为根区块，只有后继区块而没有前驱区块. 其余区块可能有多个后继子块，有一个父前驱，可能有多个叔前驱. 如图 6，创世区块为 G，A_1，A_2，A_3 均为 G 的子区块. B_1 为 A_2 的子区块，A_2 是 B_1 的父前驱，A_1，A_3 为 B_1 的叔前驱. 树状结构包含了链式结构中的分支区块，一定程度承认了叔区块的合理性. 但需设计协议对叔区块进行选择，防止恶意分叉，如 GHOST 协议[13]. 区块头中除包含父区块的哈希值，可能还需包含叔区块的哈希值，从而链接成完整的账本.

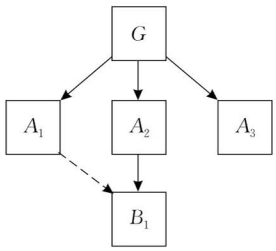

图 6　树状区块链结构示意图

树状结构提升了系统对于分叉的包容性，降低孤块率，并在保障诚实节点利益的同时，一定程度提升了系统的吞吐量. 然而，此方案对于性能的提升较为有限.

2.3.1.3　图状结构

图状结构的典型代表是基于有向无环图(Directed Acyclic Graph，DAG)设计的区块链账本，如图 7 所示. 在图论中，如果一个有向图从任意顶点出发无法经过若干条边回到该点，则这个图是一个 DAG[14]. 将 DAG 应用于区块链的想法最初于 2013 年在 bitcointalk 论坛上出现，旨在提高比特币交易处理的可拓展性，后续也不断有学者利用 DAG 的拓扑结构来改善区块链的效率等问题. 到了 2015 年，Lerner① 提出了 DAG-Chain 的概念，这极大地

① Lerner S D. DagCoin：A Cryptocurrency without Blocks. 2015. URL http://bitslog. wordpress. com/2015/09/11/dagcoin

万方数据

促进了 DAG 结构在区块链系统中应用的步伐. 后来 IOTA① 和 Byteball② 项目的诞生,使得 DAG 区块链得以真正落地.

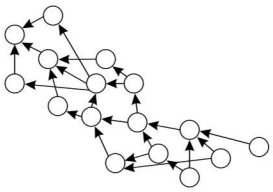

图 7 DAG 图式结构

在此结构中,将交易组织为 DAG,摒弃原本链式结构中的区块设计. 将交易看做为一个个区块,减少了将交易打包的过程. 每一笔交易直接参与全网排序,由交易组成一个有向无环图网络,实现了去区块效果.

相比于之前的链式结构,DAG 图式结构不需考虑区块链扩容问题,且处理速度快,很大程度上提升了区块链网络的效率. 此外因为矿工无需挖矿、交易费用为零,交易吞吐量增加,可以避免链式结构中的大型矿池优势,增强了网络中的去中心化特性. 然而,DAG 区块链系统中使用图作为账本,其数据结构负载复杂度高,对于编码要求较高,需要更大的存储空间进行管理和备份.

2.3.2 区块链系统角色

区块链系统中的角色按功能分为两类,分别为参与节点和维护节点. 参与节点为使用系统的客户端节点,该类节点用于与用户交互,用户在客户端节点发起自己的请求,并广播到网络. 维护节点就是维护系统数据记录的节点,该类节点用于验证用户请求、创建区块、生成区块链和保存区块链,是区块链系统中核心角色. 节点间通过 P2P 网络连接,如图 8 所示. 系统中各类节点之间地位平等,不存在“特殊节点”,整个系统的成功运转是每个节点共同作用的结果. 根据不同场景需求,节点包含功能可选,如可只参与验证转发,不参与维护记录.

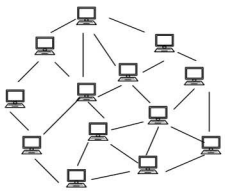

图 8 节点连接方式

2.3.3 区块链运作机制

区块链运作机制如下:

(1)当一个用户节点发起一笔交易时,该节点把交易广播到相邻节点;

(2)当一个节点接收到一笔交易时会进行一系列核验,决定是否接受并转发这个交易,核验内容如下:

(a)检查双花;

(b)检查输出额不能超过输入额;

(c)通过对交易运行核验脚本,确保脚本的返回值都是 TRUE;

(d)检查这笔交易是否被本节点接收,节点会把通过核验的交易放入其交易池,并转发该交易.

(3)产生区块:一个区块的产生代表着对账本的一次状态更新,记账权的归属需要通过特定的领导者选取(leader selection)机制决定,比如 POW,POS 等. 最终拥有记账权的矿工将打包交易的区块广播出去;

(4)当一个节点接收到一个新区块时,也会进行相应核验,决定是否接受并转发这个区块.

上述过程即为以下几个步骤:客户端发起请求、各节点将用户请求在网络中扩散、网络中参与记录的节点验证请求数据、各节点根据共识算法完成用户请求并将多个请求打包生成区块、节点将新区块广播、非区块生成节点验证新区块并更新原有链. 互联网被称为信息互连,区块链被称为价值互连,类似地,对照着 TCP/IP,数据记录、区块和区块链可以看作存储层,节点、网络看作网络层,共识算法、分布式机制、奖励机制等可以看作共识层,这三部分是区块链的基础层次,这是区块链 1.0 中典型架构. 在此基础上的扩展,主要有以区块链 2.0 为代表的智能合约,可以在此基础上扩展合约层. 再进行扩展,还有以区块链 3.0 为代表的可编程社会,因此还可扩展一层应用层,整体框架如图 9[7].

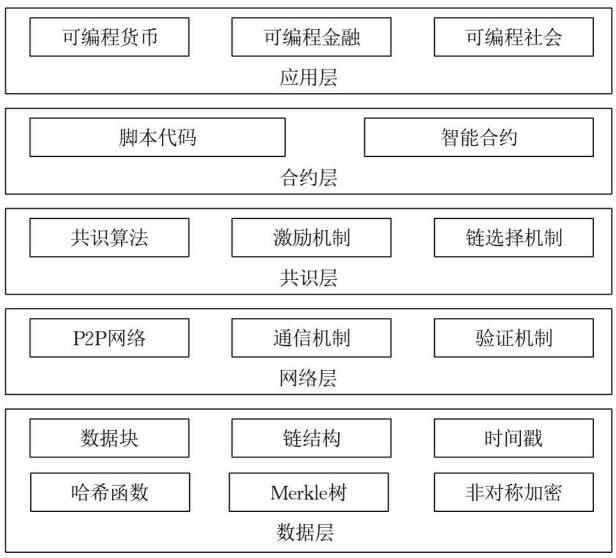

图 9 区块链架构

① Iota. https://www.iota.org/

② Churyumov A. Byteball: A Decentralized System for Storage and Transfer of Value. URL https://byteball.org/Byteball.pdf 2016

万方数据

2.3.4　区块链分类

系统的运转围绕区块链账本的记录和维护过程展开.因此,按照记录权利的归属,区块链系统可以分为公有链、联盟链和私有链.公有链可以由任何节点参与记录维护,联盟链则由预先确定的节点参与记录维护,私有链由单一的节点参与记录维护.这些链的访问权限由区块链的维护者决定,通常用户可以访问公有链,用户能否访问联盟链由链中参与节点决定,私有链一般不对外部用户开放.公有链是完全对外开放的链,私有链不对外开放,联盟链则介于二者之间.表 2 比较三类区块链系统.

表 2　3 种区块链对比

	公有链	联盟链	私有链
访问权限	公开读写	受限读写(预先定义节点)	受限读写(通常为单一节点)
性能	慢	快	快
共识算法	证明类共识算法(POW,POS,POC 等)	传统共识算法(Raft,PBFT 等)	传统共识算法(Raft,PBFT)
身份	匿名、假名	已知身份	已知身份
举例	比特币、以太坊	Fabric	R3 Corda

3　核心技术

第 2 节介绍区块链的基础组件和运作机制等.本节将具体介绍区块链领域中的三大基础核心技术——密码学、共识机制和网络.

3.1　区块链密码学

3.1.1　概述

区块链对密码学的直接需求主要基于两方面的考虑:确定所属权、保护数据隐私.由于电子数据易于复制,数字形式载体的资产(资产表明蕴含价值的东西)无法像物理形式载体的资产较容易地证明所属权.因此需要使用密码学中的数字签名技术来证明数字资产的所属.区块链系统中的账本由网络各节点共同维护,账本数据公开透明.这些公开的数据记录可能会造成隐私泄露,因此,需要借助密码学相关技术匿名化处理交易信息.除了上述主要的两方面外,一些用于生成随机数的密码学工具,可被用于共识方案.

数字签名技术可用于确定所属权.在中心化系统中,向唯一的中心提交身份认证,即可确认对个人资产的所有权.在去中心化环境中,账本由网络各节点共同维护,因此,用户需向网络各节点证明身份,利用大多数节点的共同认可来保证身份的有效性.交互的沟通成本过高,导致原有中心化交互式确认的方法不再适用.数字签名提供一种新的解决思路,用户将私钥保存在自己手中,将自己的公钥分发到网络节点上.用户使用私钥生成签名,其余节点可使用公钥验证签名的正确性.相反,如果没有私钥,用户是无法伪造签名的.

由于账本数据公开透明,如果信息采用明文上链,用户个人隐私难以保障.此外,由于账本中的部分记录蕴含了账户间的关联关系,如果被恶意节点利用也会泄露用户隐私.使用密码学中的工具如非对称加密、环签名、零知识证明等,可对交易进行一些匿名化处理.比特币中采用的一个简单方案是将用户的公钥哈希计算映射为地址,将用户信息匿名化.

3.1.2　区块链密码学核心技术

本节将介绍区块链中所用密码学算法和概念:哈希函数、Merkle 树、数字签名、椭圆曲线签名算法、环签名算法、零知识证明、抗量子密码算法.

哈希函数是将任意长度的消息映射成一个较短的输出定长消息的函数,其主要形式为 $h=H(M)$,其中 M 为变长的消息,h 是定长的哈希值.哈希函数的目的是为文件、报文或其它的分组数据产生"数字指纹".区块链一般使用密码哈希函数(Cryptographic hash function),区块链利用哈希函数的抗碰撞性保障了已有数据的不可篡改性.

它一般满足三个性质:

(1)单向性.对于给定的 y,寻求 x 使得 $H(x)=y$ 成立在计算上不可行;

(2)弱抗碰撞性.对于给定的 x,找到另一个 x',使得 $H(x')=H(x)$在计算上不可行;

(3)强抗碰撞性.寻求不相同的 x 和 x',使得 $H(x')=H(x)$成立在计算上不可行.

Merkle 树[15]是一种用哈希函数建立的二叉树结构,最底层的叶子节点是数据块,每个非叶节点的内容等于其子节点串联起来后的哈希值,以此类推,最终得到一个 Merkle 树根.利用哈希函数的抗碰撞性,只要 Merkle 树根确定,那么所有的数据块都不可被篡改.在区块链中,每个数据块都是一笔交易,得到的 Merkle 树根保存在区块头中.

数字签名[16]是手写签名的数字模拟,主要包含密钥生成、签名、验证签名三个过程.公钥与私钥是通过密钥生成算法得到的一个密钥对,公钥是密钥对中公开的部分,私钥则是非公开的部分.密钥生成算法保证了仅通过公钥来计算私钥是非常困难的,这在很大程度上保证了用户私钥的安全性.在区块

万方数据

链中,公钥即是账户地址,一个人可以拥有多个公钥,每个公钥均为与用户真实身份无关的随机数字,他人无法通过公钥推导出用户的真实身份,从而保护了用户隐私.一个被验证通过的〈消息,签名〉对能够保证:该消息是该公钥的所有者发送的——消息源身份认证;该消息没有被任何人篡改过——消息内容的完整性;该公钥的所有者无法否认他发送过该消息——消息内容不可否认性.

数字签名具体算法如下:

(1)密钥生成.通过算法生成公钥 vk 和私钥 sk,公钥对所有人公开,私钥由签名者自己秘密保存;

(2)签名算法.签名者利用私钥 sk 生成对消息 M 的签名,然后把〈消息,签名〉对公布出去;

(3)验证算法.所有人都可以利用签名者的公钥 vk 对该〈消息,签名〉对进行验证,验证结果为通过或不通过.

椭圆曲线签名算法(ECDSA)为比特币中使用的数字签名算法.该算法在有限域上的椭圆曲线中进行运算,设私钥、公钥分别为 k、$K(K=kG)$,其中 G 为椭圆曲线的基点.使用私钥签名和使用公钥验证签名的过程如下:

私钥签名:

(1)选择随机数 r,计算点 $rG=(x,y)$;

(2)根据随机数 r、消息 M 的哈希 h、私钥 k,计算 $s=(h+kx)/r$;

(3)将消息 M 和签名 $\{rG,s\}$ 发给接收方.

公钥验证签名:

(1)接收方收到消息 M 和签名 $\{rG=(x,y),s\}$;

(2)根据消息 M 求哈希 h;

(3)使用发送方公钥 K 计算 $h/sG+x/sK$ 并与 rG 比较,如相等即签名验证成功.

2001 年,Rivest 等人[17]首次提出了环签名算法.在环签名中,签名人首先选择一些其他成员,用其他成员的公钥与签名人自己的公钥组成公钥环.签名人利用自己的私钥和公钥环上的公钥进行签名,见图 10 中每个交易输入都借助一些与无关用户的公钥生成环签名.环中的其他成员可能并不知道自己被包含在其中.环签名可以让用户隐藏在一群用户中.验证者可以确定签名者是环成员之一但不知道他的真实身份.签名者所在的环构成了他的匿名集.图 10 中展示一笔使用了环签名算法生成数字签名的交易,输入部分除了签名者公钥,还包含了其他无关用户公钥.

万方数据

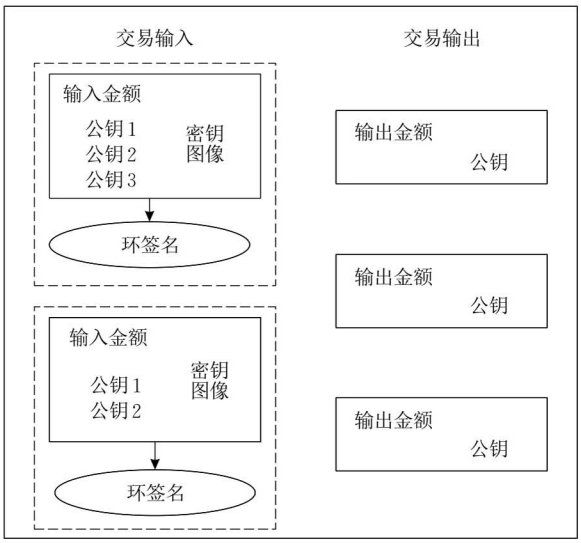

图 10 利用环签名提升交易安全性

一般而言,环签名的安全性质包括:

(1)完备性.利用环上任意一个公钥的私钥所执行的签名,能够被任何人利用环公钥来验证签名的有效性;

(2)无条件匿名性.指攻击者无法通过环签名及环公钥确定签名具体是由环上哪一个公钥的私钥持有者签署的.即攻击者正确追踪到签名人的概率为 $1/n$;

(3)不可伪造性.环成员不能伪造其他环成员的签名,环外的人也不能伪造出环签名.

零知识证明[18]定义为:证明者 P 知道问题 Q 的答案 w,希望通过出示某些信息(证明 π),可以向验证者 V 证明"他知道该问题答案"这一事实,但是验证者不能通过所出示的信息增加关于该答案的任何知识.比如 P 向 V 证明自己知道某一方程的解,但不向 V 透露解的信息.为了方便描述零知识证明的一般过程,我们先给出一些符号定义:

P:证明者,V:验证者,Q:问题,w:问题 Q 的答案,π:证明,x:问题 Q 的一些公开参数,A:验证 w 是问题 Q 答案的程序,比如把根代入方程验证等式两边相等的程序,这个程序是公开的.在区块链中常用的是零知识证明的非交互形式,即非交互的零知识证明.

非交互的零知识证明的一般过程如下:

(1)初始化阶段.一个可信第三方根据程序 A 生成零知识证明的初始化参数 CRS(Common Reference String);

(2)证明生成阶段.证明者 P 利用 (x,w,CRS) 生成证明 π;

(3)证明验证阶段.验证者 V 根据 (x,π,CRS)

判断证明是否通过，通过即说明证明者的确知道该问题答案.

量子计算机的出现将对基于传统公钥密码的分布式账本系统形成了非常大的安全威胁，需要及时未雨绸缪，而后量子密码能有效抵抗量子计算. 主流的后量子密码方案包括：基于 Hash 函数的后量子密码，其安全性依赖于抗碰撞的 Hash 函数；基于多变量二次方程的后量子密码，其安全性依赖于有限域上的多变量二次多项式映射；基于编码理论的后量子密码，其安全性依赖于纠错码理论；基于格理论的后量子密码，其安全性基于格上的困难问题. 目前，将后量子密码签名方案应用于分布式账本系统的主要难点在于方案的公钥及签名长度过大，将极大地影响分布式账本系统的性能效率（如交易吞吐量 TPS），并且基于 LWE 的签名方案中采用的 DGS（离散高斯采样）模块易受旁路攻击，需设计安全高效的防护方案.

3.2　区块链共识机制

3.2.1　从中心化到去中心化

对基于互联网的分布式系统而言，价值交换长期以来都是构成其运行机理的重要基础，其具体形式随技术发展不断演进，从简单的物物交换、产权更迭扩展到服务交换、信息交换等等，在云计算产业蓬勃繁荣的今天已成为社会生产活动的主要环节之一. 由于互联网的匿名性，参与价值交换的双方有时可能存在利用欺诈行为恶意窃取对方价值的倾向，因此，一个能够提供背书的可信第三方（例如电商平台、云服务平台等）是十分必要的，用于高效地见证、监督和维护系统的正确运转.

随着业务规模的增长，这些第三方的信用迅速积累，从最初的见证角色转变为这些价值交换系统的监督者、维护者、决策者，位居价值交换的众多参与者之上，成为这些系统实质上的中心，而真正的参与者却只能被动接受第三方制定的规则. 同时大数据技术的出现，使得海量数据中蕴含的知识规律等得以被提炼，并可用于生产新的价值. 然而，价值交换系统中的庞大交易数据基本被中心化的第三方所独占，真正的参与者反而无法获取及运用这些数据. 上述问题已经逐渐成为限制当前价值交换系统与多种互联网＋产业发展的枷锁，因此，减弱第三方对于价值交换的中心化控制是十分有必要的.

本文讨论的“中心化”指逻辑上的中心化，即分布式系统中存在有作为权利中心的节点，这些节点在物理形式上可能运行在一个或多个设备上. 与权利中心化对应的则是权利去中心化，即将见证、监督和决策等权利平等地下放给系统中真正参与价值交换的各节点.

区块链系统通过对见证人身份进行重新选择，使得见证人不再固定于一个中心化身份的实体，而是由多个节点参与见证、监督和决策，系统中涉及的数据记录由这些节点进行维护和生成，从而实现了去中心化. 根据需求，系统中可以存在功能不同的节点（如比特币系统中的全节点和 SPV 节点），但是却不存在享有特权的节点.

区块链是由在物理上和逻辑上都广为分布的多个节点组成的分布式系统. 区块链系统符合分布式系统的典型特性，因此可将区块链系统抽象为分布式系统模型建模分析. 分布式系统包括的内容十分广泛，在不同应用场景下，表现形式和特性也稍有不同. 与大部分传统分布式系统应用不同，区块链系统中面向开放的互联网环境（Permissionless），节点无需信任基础或较弱信任基础. 因此，区块链系统为达成共识，对外显示一致性，需要更严格的共识协议.

3.2.2　分布式系统基础

分布式系统是一组计算机通过网络相互连接传递消息，并在通信后协调它们的行为而形成的系统[19]. 系统中各计算机节点位于不同的物理分布，利用网络通信交互达成共识，从而共同实现一个任务. 由于分布式系统中不存在一个全局时钟，且各个节点可能并发运行，因此，各节点间需要对系统中所有事件进行排序[20]，以便达成共识.

系统中各节点间建立共识过程的两个核心步骤抽象如下：各节点处理各自持有的数据，利用网络和其他节点通信更新数据. 分布式系统共识主要取决于三个因素：节点可靠性、节点立场和网络通信状况. 节点宕机、崩溃、故障造成的错误叫做非拜占庭错误；敌手节点恶意错发或不发消息造成的错误叫做拜占庭错误. 分布式系统中的网络通讯模型（也称时间模型）主要分为三种[21]：同步网络模型（synchronous model）、异步网络模型（asynchronous model）和弱同步网络模型（也称部分同步模型，partially synchronous model）.

（1）同步网络模型. 节点的时钟漂移有上界，网络传输延迟有上界，节点计算速度相同.

（2）异步网络. 节点时钟漂移无上界，网络传输延迟无上界，节点计算速度不同.

（3）弱同步网络. 介于同步网络模型和异步网络模型之间（可根据不同应用场景做不同假设）.

万方数据

尽管同步网络模型没有完全模拟真实环境，异步网络模型更接近于现实世界.但是同步模型因利于建模分析和扩展，仍有重要的研究价值和意义.

1980 年 Lamport 等人[22]提出了分布式计算领域的共识问题.共识问题的定义主要包含三个方面：终止性、一致性和有效性.终止性是活性的保证，一致性和有效性是安全性的保证.更具体地，Lamport[23]、Herlihy 和 Wing[24]陆续提出了顺序一致性、线性一致性.在同步网络中的一致性是可以达到的，而在异步网络中无法实现.FLP 不可能定理[25]给出了证明，在异步网络模型中，即使只有一个单节点失效，也不存在一个算法能够保证非失败进程达到一致性.现实环境的工程实现中，可以通过对消息进行超时限制以满足需求.后续研究中，CAP 原理[26]说明分布式系统无法同时满足一致性(Consistency)、可用性(Liveness)、分区容忍性(Partition)，在设计中往往需要弱化对某个特性的保证，见图 11.

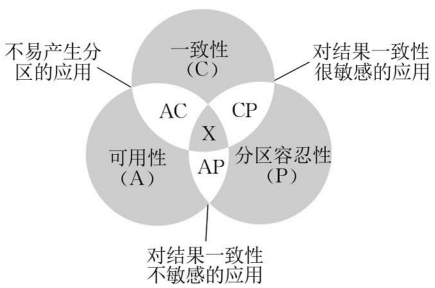

图 11 CAP 原理示意图

早期的分布式系统共识中仅考虑容忍错误节点，代表性工作包括用于分布式数据库的共识协议 Paxos[27]和 Raft[28]等.1982 年，Lamport 等人[29]又提出了“拜占庭将军问题”，从而涵盖了恶意节点.1999 年，Castro 等人[30]提出首个实用的拜占庭容错算法.传统分布式系统共识算法中，采用状态机复制模型实现一致性.其过程为在节点中随机选取一个领导者，为发生的事件确定全局的顺序，其余节点根据领导者广播的消息按序执行操作.由于区块链系统希望降低对信任的要求，无法直接应用上述算法.

3.2.3 区块链共识框架

区块链系统的核心是区块链账本数据的维护，因此，共识的过程是各节点验证及更新账本的过程，共识的结果是系统对外提供一份统一的账本.区块链系统共识基于分布式系统共识，也包含节点数据自处理以及节点间交互的过程，也可以理解为领导者选取和复制的过程.但是由于区块链系统并未对参与系统节点的身份进行限制，因此为防止节点恶意行为，系统要求参与节点付出一定代价参与记账权的竞争.此外，节点间交互过程中，为促使所有节点都不因其他节点改变自己诚实的“初心”，积极正确地维护系统，需要设计一套协议限制节点更新账本的行为.基于以上思路，本文对现有主流系统的共识部分总结、归纳，提炼出区块链系统中的共识框架，如图 12.

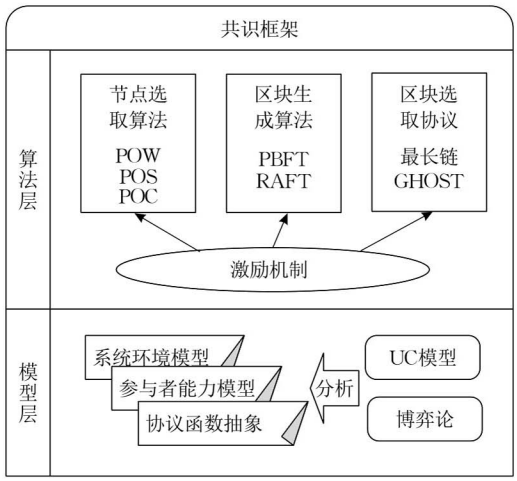

图 12 区块链共识框架

3.2.3.1 记账节点选取算法

选取记账节点与选取领导者节点类似，只不过选取算法的随机性减小，节点参与的主动性增强.不对称性是算法的主要特征，节点参与竞争付出代价较高，其余节点验证付出代价较低.“代价”形式多样，包含物理资源和虚拟资源，如计算资源、存储资源、特殊硬件等.下文将介绍一些主流系统中采用的节点选取算法.

(1) Proof of Work 算法

POW 算法最初被用来抵御拒绝服务攻击(DDOS)[31].以邮件服务为例，在客户端向邮件服务器发起请求之前，客户端需要根据邮件内容以及随机数完成哈希计算.满足预设要求后向服务器发起请求，服务器验证通过后进行响应.该算法能够在为诚实客户端提供服务的同时，有效过滤垃圾邮件.

区块链系统中 POW 算法的常见形式如下[3]，$H(param \parallel nonce) < target$. $param$ 表示与区块信息相关数据，$nonce$ 表示随机数，$target$ 表示目标值(由网络中当前难度值决定).由哈希函数的性质决定，想要找到符合条件 $nonce$，就必须通过穷举 $nonce$ 的方法来实现.最先求得满足上述不等式的 $nonce$ 值的节点获得记账权，其余节点仅需将各参数代入即可验证其正确性.POW 算法通信复杂度为 $O(n)$，

万方数据

节点数可扩展，参与过程无需身份验证. 但是浪费算力资源，效率较低，容易导致算力集中.

(2) Proof of Stake 算法

数字货币除了用于流通外，还蕴含储值价值，作用类似于证券，是一种虚拟资源. 节点持有代币的数量越多，越希望维持币值稳定，越倾向于维护系统正常运转. 因此，节点持有代币的相关信息可用于设计记账节点选取算法，该算法也称为权益证明算法.

POS 这个概念首次出现是在比特币社区 Quantum[①]的帖子中，该概念可以解决 Vandroiy 在论坛帖子中提出的挖矿公地悲剧问题[②]. POS 类算法的核心思想是使用代币相关信息参与计算，但是不同系统提出了不同的算法方案，如 PPcoin[32]，Ouroboros[33]和 Algorand[34]. 其对应的主要密码学工具分别为哈希计算，可验证秘密共享和可验证随机函数.

(I) 哈希计算

最简单的方案是将节点持有代币数目用于哈希计算，该过程类似于 POW，这类系统有 PPC[32]、BLK[③]、NVC[④]、NXT[⑤] 等. 以 PPC 为例，PPC 中提出币龄概念，即持币数量和持币时间的乘积. 其算法为 $H(tx \parallel param) < Coinage \cdot Target$，式中 H 表示哈希函数，tx 为某笔用户未花费交易的相关参数，$param$ 为系统协议设置的相关参数(权益修正因子)，$Coinage$ 表示该笔交易产生币龄，$Target$ 表示目标值. 参与铸币的交易确定时，$Coinage$ 和 $Target$ 越大，节点越容易获得记账权. 当节点成功生成 POS 区块时，其币龄将置零，将得到一笔 *coinstake* 奖励交易. BLK 使用币数代替币龄，以防止离线生成币龄，其算法为 $H(tx \parallel param) < Coins \cdot Target$. 未来币算法中没有使用币龄的概念，其算法公式为 $f(H(tx \parallel param)) < Target \cdot Balance \cdot ElapseTime$，式中函数 f 取哈希函数结果的前 8 个字节，H 表示哈希函数，$Target$ 为目标值，$Balance$ 为账户余额，$ElapseTime$ 表示与上一区块间隔时间.

(II) 基于可验证秘密共享的 G.O.D coin tossing+follow-the-satoshi

该算法[35]的核心思路是根据各节点持有的代币数量随机选取，持有代币数量越多，被选中的概率越高. 该算法的创新点在于随机数的选择. 简单随机数选择协议(coin tossing)用于多方通信场景，通过一个初始伪随机数和多次交互，最终生成一个被多数节点确认的真随机数. 但是如果某节点单方面停止响应，协议无法继续. G.O.D coin tossing 算法在原有 coin tossing 协议中引入了可验证秘密共享(Verifiable Secret Sharing). VSS 方案将秘密切分为一些文件碎片，分发不同节点，在恶意节点数目有限的情况下，大多数节点可根据持有的文件碎片恢复原信息. 将生成的随机数应用到 follow-the-satoshi 算法中，确定出块节点. follow-the-satoshi 算法将所有节点的代币数目作为叶子节点组织成一颗 Merkle 树，根据生成的随机数在左右子树中选择，直至确定出块节点.

(III) VRF

该类算法使用 VRF 函数生成随机数，根据此随机数与持有代币数目选取节点集合. Algorand[34]中的节点分为两种角色，proposer 和 committee. 各节点利用 VRF 函数生成一个哈希值 $hash$ 和一个证明 π. VRF 的性质保证了该 $hash$ 由 sk，$seed$，$role$ 唯一确定，但对于不知道 sk 的其他人该 $hash$ 值与一个随机数没区别. 所有知道公钥 pk 的节点都可以利用 π 来验证该 $hash$ 的正确性. 代币可看做虚拟用户，代币数目则对应于用户持有的虚拟用户的数目. 假设网络中总代币数为 W，用户持有的代币数目为 τ，p 为一个虚拟用户被选为某一角色的概率. $p=\tau/W$，用户持有币数越多，p 值越大，越容易被选为角色. 用户拥有 w 个代币，即可等价于持有 w 个虚拟用户. j 表示 w 个虚拟用户中被抽中的个数(服从二项分布)，由随机生成的 $hash$ 决定(即落在哪个区间)，j 越大代表该用户被选中的优先级越高，即更容易被选中.

(3) Proof of Space 算法

该算法核心在于节点以存储空间(包括内存和硬盘)为代价，竞争记账权. 判断节点是否贡献存储空间的一个直观想法，就是验证者要求证明者存储一个特定文件，并在需要验证时向该证明者发起询问. 如果验证通过则说明节点付出存储代价. 但是上述方法存在较大的通信开销，同时要求验证者也提供一定大小的存储空间. 针对上述问题，Dziembowski 等人[36]利用具有高 pebbling complexity 特性的有

① QuantumMechanic. Proof of Stake Instead of Proof of Work. July 11, 2011. https://bitcointalk.org/index.php?topic%20=27787.0

② Vandroiy. [If Tx Limit Is Removed] Disturbingly Low Future Difficulty Equilibrium. April 22, 2011. https://bitcointalk.org/index.php?topic=6284

③ Vasin P. Blackcoin's Proof-of-Stake Protocol V2. URL: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf, 2014

④ Novacoin. http://novacoin.org/

⑤ NXT. https://www.jelurida.com/nxt

万方数据

向无环图和 Merkle 树构建解决方案.

Dziembowski 等人[36]设计的算法中包含证明者和验证者角色,并由初始化和验证两个阶段组成.初始化阶段,验证者和证明者使用相同输入生成 hard-to-pebble 的有向无环图 $G=(V,E)$,式中 G 表示图,V 表示图中顶点,E 表示图中边,如下图所示.图中每个顶点有一对应标签值 w,证明者按照公式 $w(v)=\mathcal{H}(v,w(\pi(v)))$ 计算每个顶点的标签值,v 表示对应的顶点,$\pi(v)$ 表示顶点 v 的所有前驱节点,即 $\pi(v)=\{v'|(v',v)\in E\}$.如果顶点 v 没有前驱节点,则其标签值 $w(v)=\mathcal{H}(v)$.证明者将各节点的标签值作为叶子节点,生成一棵 Merkle 树,并将 Merkle 根的值返回给验证者.验证通过后,可以进入执行阶段.在执行阶段,验证者随机选取图中某一顶点作为挑战(challenge)发送给证明者,证明者将以该顶点的标签值 w 和在 Merkle 树中该节点生成 Merkle 根路径中的哈希值(该过程为"opening a node")回复(response)验证者.验证者根据证明者返回的值计算图 G 的 Merkle 根,如果与初始化阶段中的 Merkle 根一致,则验证通过.

Hard-to-pebble 图中顶点间互联性很高,为计算某顶点标签值,需已知其所有父顶点标签值,如图 13.存储的标签值越多,越容易计算出所有节点的标签值,尽快完成 pebble 游戏.为了能够在规定时限内响应验证者提出的挑战,证明者需付出存储空间存储足够的标签值.Hard-to-pebble 图的 pebble 复杂性较高,使得恶意节点无法抽取一些值存储,如只存储图中某些节点就能在规定时间内完成 pebble 游戏.因此采用 hard-to-pebble 能够保证证明者付出了相应的存储代价,采用 Merkle 树能够保障验证者能够快速验证.

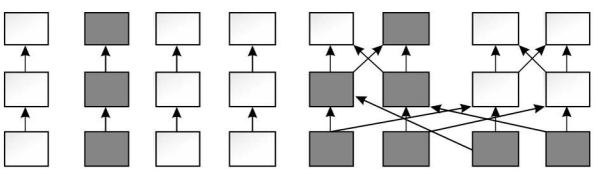

图 13 hard-to-pebble 原理图

(4) Proof Of Retrievability 算法

本算法要求节点贡献存储资源参与竞争,但是与 POC 设计思路略有不同.POC 要求节点贡献存储资源证明自身可靠性,但是存储文件本身并没有特殊含义.POR[37]从实际使用的角度出发,使节点存储一些有意义的数据文件参与记账权竞争.

POR 算法最初用于云存储环境,验证某证明者是否持有某单一文件.通常客户端将一些文件在云空间中托管,POR 算法用于验证云存储供应商是否按照要求存储指定文件,并在客户端需要时完整地恢复原本数据文件.类似算法还有 PDP[38]、proof of storage[39]、proof of ownership[40],初衷都是用于验证远程文件的完整性.尽管和 Ateniese 的 proofs of space[41]重名,但这篇文章的与 POR 算法更类似.

受上述思路启发,可以在区块链系统中构建分布式 POR 算法[42],要求节点存储一些较为重要的数据碎片.节点存储越多文件碎片,其竞争到记账权的概率越高.该算法在公平选择记账节点的同时,还能充分利用网络中空闲的存储资源.算法一共分为初始化(setup)、解密(Scratch-off)和验证(verify)三个阶段.在初始化阶段代理节点(dealer)将文件拆分为 n 份,并将拆分得到的文件碎片组织为一棵 Merkle 树.各节点根据自己的公钥计算出需要存储的文件碎片,其公式为 $\forall i\in[\ell]:\boldsymbol{u}[i]:=H_0(pk\|i)\bmod n$,存储文件碎片标号集为 S_{pk},$S_{pk}:=\{\boldsymbol{u}[i]\}_{i\in[\ell]}$.在 scratch-off 阶段,上一区块数据用于生成本次挑战的参数.节点根据挑战参数代入公式 $r_1:=\boldsymbol{u}[H(puz\|pk\|s)\bmod\ell]$ 得到用于响应挑战的文件碎片编号,并将 $(pk,s,\{\boldsymbol{F}[r_i],\pi_i\},i=1,2,\cdots,k)$ 返回.其他节点收到后,将数据代入公式验证.除了 Permacoin[42]外,Storj[43]、Sia①、Filecoin② 的共识也都基于 POR 算法的思路.

(5) Proof of Luck 算法、Proof of Elapsed Time 算法

这类算法要求节点使用可信硬件环境(Trusted Execution Environment,TEE)[44]参与记账权的竞争.TEE 环境提供一个隔离的执行环境,保证加载到该环境内部的代码和数据的安全性、机密性和完整性.因此,如果节点在 TEE 环境中运行挖矿协议,较难出现恶意行为.现在较成熟的 TEE 环境有诸如 Intel 的 SGX③,ARM 的 Trustzone④,AMD 的 PSP⑤ 等.现有针对 TEE 环境设计的共识算法,主要使用 Intel 的 SGX 框架.

SGX 允许应用中部分程序代码运行在一个称

① Sia. https://assets.coss.io/documents/white-papers/siacoin.pdf
② Filecoin. https://filecoin.io/
③ Intel SGX. https://software.intel.com/en-us/sgx/
④ Trustzone. https://developer.arm.com/ip-products/security-ip/trustzone
⑤ AMD Platform Security Processor (PSP). https://www.amd.com/en/technologies/security

万方数据

作飞地(Enclave)的可信执行环境中，Enclave 在受保护的内存区域(Reserved Protected Memory，RPM)运行，保护程序的执行、控制程序的入口点. 如图 14 所示，用户可将应用程序分为可信和不可信部分，创建 Enclave 时加载需要安全执行的代码、数据等相关信息. 当可信执行函数被调用时，执行会转换到 Enclave 内部进行，保证应用程序代码和数据在运行过程中不受高级别系统软件的攻击(例如特权系统代码、操作系统、BIOS、VMM 等).

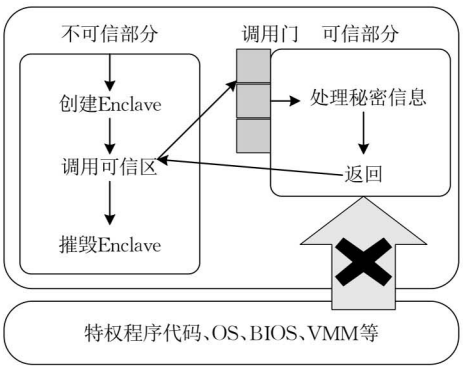

图 14　SGX 可信执行模型

使用支持 TEE 的工作量证明能够回避算力不均的问题. 各节点都有单独的身份证明，且算力平均. 使用这类节点参与挖矿可有效解决算力集中和算力不均等问题，能够有效提升挖矿的公平性.

Sawtooth Lake 项目①基于 SGX 提出 POET 算法[45]，该算法主要包含 *CreateTimer*()和 *CheckTimer*()两个函数. 节点调用 *CreateTimer*()在 Enclave 中为区块创建一个计时器，保障该区块由 Enclave 产生. 该计时器为该节点生成一个随机等待时间，随后节点等待计时结束. *CheckTimer*()用于验证计时器由 Enclave 创建，如果计时器计时结束，将生成一个证明，用于验证节点为竞争记账权已经等待被分配的时间. 最先结束等待时间的节点获得该轮记账权.

Milutinovic 等人[44]基于 SGX 提出 POL 算法，该算法基于将 POW 迁移至 TEE 环境中构建的两个预备算法 POO 和 POT. POT 能够提供防伪时间戳，证明该节点确实能够通过了某一确定时长的时间间隔. POO 算法能够提供可区分的实体身份证明，即节点无法生成虚假身份冒充多个实体. 在这两个预备算法的基础上进行扩展，文中提出 POL 共识算法.

POL 算法主要由两个函数 *PoLRound*()和 *PoLMine*()组成，这两个函数表征了整个算法的两个阶段. 参与者调用 *PoLRound*()，通过当前已知的最新块来准备 TEE 以在特定链上挖掘. 该函数用于限制节点在两次连续挖矿过程中，经历一段时间间隔 *ROUND_TIME*. *ROUND_TIME* 之后，参与者调用 *PoLMine*()挖掘一个新块. 首先使用随机数生成器 *GetRandom*()生成一个[0,1)中的随机值 l，该值服从均匀分布. 将 l 作为参数传入函数 f，$f(l)$的返回值用作 *proof* 表明该 l 的“幸运”程度，用于确定在所有参与者提交的区块中这一轮的获胜块. *PoLMine*()函数的最后执行 *sleep*($f(l)$). 节点越“幸运”则节点的 *PoLMine*()执行时间越短，可以越早将自己这轮生成的区块广播. 若节点执行 *PoLMine*()函数得到结果前就已经收到其他区块，则说明这一轮不够“幸运”. 对于分叉的情况，协议中要求各节点选择幸运值最大的链.

(6) DPOS 算法

委任权益证明 Delegated Proof of Stake(DPOS)算法的核心在于代表的选取和区块的生产. 该算法类似于现代企业董事会制度，通过引入见证人机制解决中心化问题②.

多数节点选取能够代表自己利益的特殊节点获取区块生产权，这些代表(又称见证人)将轮流生产区块. 代表由区块链网络各节点投票产生. 代表集合生成后，各代表轮流获得区块链出块权.

Larmier 等[24]主要从正常流程、少数者分支、未连接的少数者双重生产、网络分片四种情况分析了系统的安全性. 正常流程中，代表轮流获取出块权生产区块. 如果各代表都按照规则在各自负责的时间段生产区块，将产生最长链. 少数者分支指的是，少数恶意节点或故障节点创造了一个分支. 在此情形下，由于诚实节点算力大于少数节点算力，最长链仍然由诚实节点生成. 少数离线多重生产指的是少数者尝试生产多分支影响主链. 然而由于算力比例小，因此分支链比主链短. 网络碎片化时，没有任何分支拥有多数区块生产者，最长链将由有最大的少数者集合维护. 当网络连通性恢复后数量较小的少数者集合将切换到最长链中.

通过选取代表，DPOS 算法消除了交易需要等

① https://sawtooth.hyperledger.org/

② Larimer D. Delegated Proof-of-Stake White Paper. 2014. https://steemit.com/bitshares/@testz/bitshares-history-delegated-proof-of-stake-dpos

万方数据

待的非信任节点验证时间.通过减少待确认要求数量,交易速度得以提高.DPOS 算法可以理解为中心化和去中心化的结合,系统通过选举,使每个人都有可能成为代表绝大多数用户的委托人.并且如果其中有违背协议的节点,这些节点将被取消记账的权利,网络可以重新选举新的节点来代替这个节点.该机制在正常情况、少数分叉、少数离线多重生产、网络碎片化等情况下都能保证正确性①.

目前使用这种共识算法的系统有比特股 Bitshares②,Steem③,EOS④,其见证人的数量分别为 101、21、21,用于选择见证人的票也就是各个系统中流通的代币.

(7) Proof Of Useful Work 算法

POUW 算法要求节点执行某具体任务参与记账权的竞争.POUW 将 POW 中无意义的哈希计算替换为有意义的任务执行.

REM[46] 基于 Intel 的 SGX 框架设计,提出了 Proof of Useful Work 共识算法,节点在 enclave 中执行被分配的任务,将完成任务所需运行的指令条数代入公式 $l \geq 1-(1-diff)^n$ 计算,判断是否符合出块条件.使用 TEE 环境有效降低节点作恶可能,并对于程序执行的入口进行验证,确保节点没有篡改执行的指令条数.节点执行任务所需的指令越多,其成功出块概率越高.

King⑤ 依据素数找寻问题提出了解决方案.寻找素数在数学、密码学领域是一个重要且困难的核心问题.算法要求各节点计算符合三种 Cunningham 链形式之一的质数链,并将结果链的起始元作为除数,该区块的哈希值作为被除数,将得到的商记录在区块头中.使用三种 Cunningham 链形式之一的质数链作为谜题,使得节点挖矿难度可控,参与节点能够以一定概率成功挖矿.其余节点只需进行费马检测(Fermat test)和欧拉-拉格朗日-里夫西兹检测(Euler-Lagrange-Lifchitz test)即可.通过以上检测的素数被称为伪素数,但由于,在以 2 为底条件下找到伪素数的概率比寻找素数概率更低,因此,可以以较大概率相信此验证结果的正确性.

3.2.3.2 区块生成算法

节点参与第一阶段记账权的竞争后,付出了相应代价建立信任,被选入参与出块.部分系统在选择记账节点的同时生成区块.例如,POW 算法中,节点多次试验找到了满足条件的 *nonce* 后,将此证明和交易数据打包,生成区块.而另外部分系统按上述算法选出节点后,或者其系统本身存在一些信任基础,为了提高出块效率,出块过程结合了传统共识算法.大部分区块生成算法都一定程度采用了传统共识算法的思路.

在区块生成算法中,为了便于建模,很多解决方案都引入了时间分片的概念,通常有轮次(round)、阶段(epoch)、时间片(slot)等概念.

(1) PBFT 类

PBFT 算法[30] 中的核心概念有三个部分:视图(view)、副本(replica)、角色(primary,backups).视图表示当前系统的全局状态,系统中参与的节点都成为 replica,而在每个视图中,replica 中的角色分为两类,其中一个副本充当领导者(primary),而其他副本作为备份(backups).假设系统中恶意节点数目为 f,总节点数为 $3f+1$.算法的流程主要分为五个阶段:请求、预准备、准备、提交和回复.在客户端发起请求后,当前视图中的 primary 节点将对请求编号,并通过预准备消息通知各个 backups 节点.如果各个节点认可预准备信息内容,则在准备阶段将各自消息发送到其他节点.各个节点验证自己收到准备信息的数量(至少 $2f$)和内容正确性,验证通过将预准备消息和准备消息写入日志.各个节点完成准备阶段后,向其他节点发起确认消息.各节点验证自己收到确认信息的数量和内容正确性,向客户端发一个回复消息.如果客户收到超过 $f+1$ 个相同回复消息,则表明完成请求,若不满足则重新发起一次请求.其算法过程可概括为图 15.

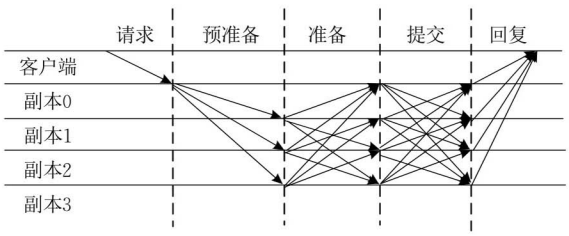

图 15 PBFT 算法流程

将 PBFT 算法应用区块链系统,primary 节点为获取记账权的节点或节点集,客户端请求为交易

① dantheman. DPOS Consensus Algorithm-the Missing White Paper. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
② Bitshares. https://bitshares.org/
③ Steem. https://steem.io/
④ Eosio. https://eos.io/
⑤ King S. Primecoin: Cryptocurrency with prime number proof-of-work. https://assets.ctfassets.net/sdlntm3tthp6/resource-asset-r379/5ad81da96cfdce4043cccad684edf368/b72fce6c-66c4-47e8-8772-f5d7af815450.pdf

万方数据

信息或备选区块，primary 节点依 PBFT 算法组织各节点生成新区块，达成共识.

2016 年，Haithem 等人[47]提出了 HoneyBadger-BFT 协议，该协议相对当时已知最好的异步原子广播协议（Asynchronous Common Subset）进行改进. 包括使用了门限密码体制来消除原协议中过多的冗余，使用基于纠删码的有效可靠广播来优化了异步通用子集（Asynchronous Common Subset）. 从而在异步网络环境下实现了确定性共识. PBFT 和 HoneyBadgerBFT 算法都只能在网络中节点数量已知的情况下进行，且在协议进行过程中无法加入新节点. Duan 等人[48]在 2018 年对 HoneyBadger 的部分模块进行了替换，提出了更为高效的 BEAT 系列协议.

一些系统采用算法混合方案如 POW＋PBFT，POS＋PBFT 中，证明类算法如 POW、POS 被用于竞争记账权，PBFT 算法被用于从备选区块中选择区块或生成区块.

由于 BFT 类算法的高效性，一些方案也将 BFT 算法与 POW 算法结合，既部分提升了区块链共识算法的效率，也同时保证了共识算法的可靠性，如 Cachin 等人[49]、Pass 等人[50]、Min 等人[51].

Algorand[34]系统生成区块的流程如图 16 所示. 系统中包括 proposer 和 committee 两种角色. 首先，所有的用户将自己的代币和想竞选的角色作为输入执行 *VRFsk* 算法. 角色分化后，proposer 成员生成备选区块，如图中所示，B_1、B_2 等，而 committee 成员根据 BA^* 算法从候选区块进行选择，每一轮至多选择一个区块. BA^* 算法中一共分为 *Reduction* 和 *BinaryAgreement* 两个阶段. 在 *Reduction* 阶段，保证所有的诚实节点最多只对一个非空区块达成共识. 在 *BinaryAgreement* 阶段，对 *Reduction* 阶段的输出结果再进行共识，使得所有诚实节点只对该非空块或空块达成共识.

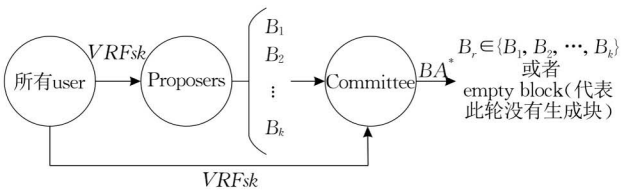

图 16　Algorand 系统区块生成过程

（2）Raft、Paxos

目前使用 Raft 算法出块的区块链主要为联盟链，如联盟链 Quorum① 使用的共识算法就基于 Raft 开发的. 与 PBFT 算法类似，记账节点对应 Raft 算法中的领导者，客户端请求对应于交易或备选区块，领导者节点将交易信息打包成区块，其余节点依赖日志复制同步区块.

Raft 算法中需要两种角色，领导者和跟随者，领导者负责传达指令，而跟随者负责执行命令. 而这两种角色的分化需要一个中间角色来过渡，因此 Raft 系统中节点有三种状态：领导者、候选人、跟随者，三种角色的转换过程如图 17. 推动系统循环往复的是时间元素，通过设置任期的概念防止系统陷入僵局，见图 18，在选民关于领导者意见不统一时，通过设立定时结束僵局，进入下一次选举.

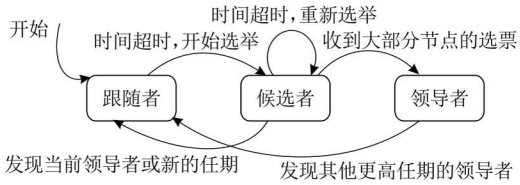

图 17　Raft 算法角色转换图

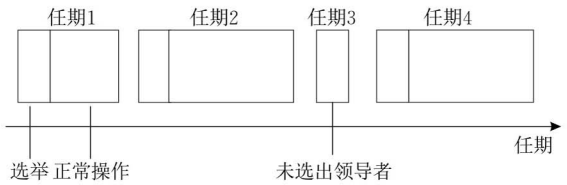

图 18　任期变化示意图

Raft 算法将共识问题拆分为三个核心子问题：领导人选取、日志复制和安全性.

领导者选取：系统通过心跳包触发系统选举. 系统正常运转时，领导者会向追随者发送心跳包，当追随者收不到心跳包时，意味着领导人任期结束，可以开始新一轮的选举. 选举的过程中，参与竞选的节点状态转换为候选人，并向其他节点争取选票，如果获取选票超过半数，则当选下一任期的领导者. 若候选者没有获得超过半数的选票，则此轮选举失败，任期结束，需要等待下一轮选举.

日志复制：保证各节点都执行相同的序列. 当客户端向领导者发起请求后，领导者接收到的数据处于未提交状态（Uncommitted）. 复制的过程分为三步：领导者向追随者节点广播待复制数据，各追随者接收后响应领导者，领导者收集足够追随者响应后向客户端响应. 领导者一旦响应了客户端，则表明此时数据状态更新为已提交（Committed）.

① Quorum. https://www.jpmorgan.com/global/Quorum

万方数据

安全性:防止任期切换造成的不一致.上述过程只保障任期内一致性,当不同任期领导者切换时,前后领导者的日志可能存在冲突情况.以领导者为基础的一致性算法中,领导者最终必须要存储全部已经提交的日志条目,算法中对选举过程中加入限制,以满足这一要求.

(3)分时间片选择

在 Ouroboros 中[33],时间被分为 slot,10 个 slot 为 epoch,每个 slot 至多生成一个区块.整个 epoch 包含 Commitment 阶段,Reveal 阶段和 Recovery 阶段,分别包含 4 个 slot,4 个 slot 和 2 个 slot,对应于生成随机数 VSS 协议的三个阶段,如图 19 所示.每个 $epoch_i$ 初始时,根据 $epoch_{i-1}$ 的历史记录生成 $epoch_i$ 阶段的创世块.该创世块中硬编码了节点公钥、对应的权益和初始的种子 ρ,被用于之后的各 slot 中.各节点在每个 slot 将权益、初始种子和 slot 参数作为输入执行 follow-the-satoshi 算法,确定自己是否被选为出块节点.如果被选为出块节点,则打包交易,生成区块后广播.如果未被选中,则等待其他节点广播,如果超时未收到,则认为该 slot 区块被废弃.重复上述出块过程直到该 epoch 结束,并为下一个 epoch 生成新的随机种子.

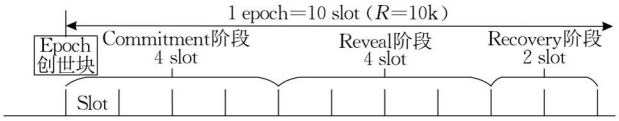

图 19 Ouroboros 协议阶段示意图

Peercoin① 选择区块的协议如图 20 所示,系统中有多种类型的区块.有的包含交易、有的包含权益修正因子,有的包含 coinstake 奖励.矿工选择某区块中一笔未花费交易 tx_1 参与 POS 挖矿,出块时要求 tx_1 币龄最少为 30 天.将 21 天前的权益修正因子代入函数 CreatCoinStake 参与计算.如果成功出块,则将 coinstake 和交易打包生成新区块.

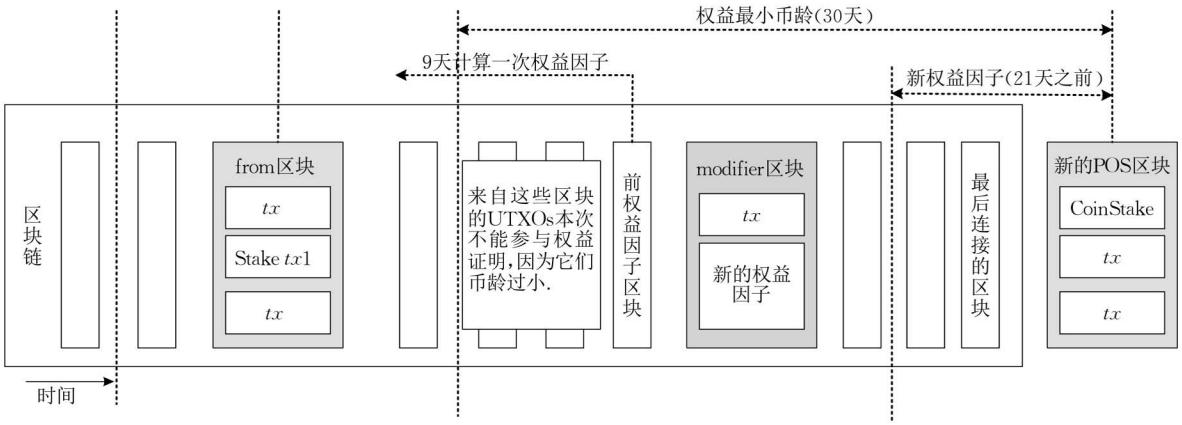

图 20 Peercoin 区块选择流程

(4)混合共识出块

还有一些方案将不同种算法融合使用,POW+POS 等.POW+POS 方案并行使用两种算法,在节点竞争记账权的同时分别生成 POW 区块和 POS 区块.

Bentov 等人[35]提出了一种叫 POA 的共识算法,该算法采用 POW+POS 混合共识出块.POW 挖矿方案采用哈希函数,POS 挖矿采用的方案为 follow-the-satoshi.具体来说,POA 的出块过程主要分为两步,过程如图 21.首先运行 POW 算法,输入区块参数参与哈希计算生成区块头信息,区块体中不包含交易数据.将空区块广播,各节点根据区块头数据应用上述 POS 算法导出参与出块的 N 个随机的节点集合都会验证自己是否属于这些节点中,如果属于就用自己的私钥对区块进行签署.进行到最后一个代币持有者时,他将在区块体中打包交易,扩展空区块头.区块打包成功后,他将广播该区块,

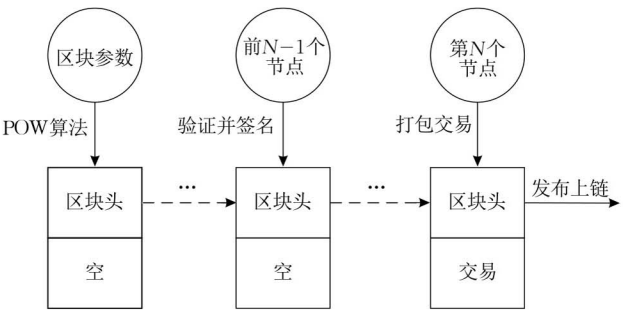

图 21 POA 算法示意图

① Peercoin. https://docs.peercoin.net/#/peercoin-v0-5-proof-of-stake protocol

万方数据

其他节点验证通过后，将新块更新到本地账本. 与单纯的 POS 相比，第一阶段的 POW 保留了挖矿带来的好处，第二阶段加入了 POS 机制选择代币持有者能够一定程度破坏对算力垄断的情况，而且在 POA 中要求代币持有者在线，促进整个系统进入良性循环.

Duong 等人①和 Chepurnoy 等人②提出并行地使用 POW 和 POS，而不是分阶段使用不同的算法. 这种混合出块方式是先由 POW 矿工先挖出来一个 POW 区块，之后再由代币持有者挖一个 POS 的区块，之后再是 POW 区块、POS 区块，并一直这样交替下去. 显而易见，这种情况下，仅仅靠分叉还不足以否认区块链账本的历史，还需要保证能够获得链在一起的 POS 块，才有可能对账本历史进行改写. Alexander 等[3]对这种机制进行了完善，将生成两个链的过程加入难度控制，使整个系统更加稳健.

3.2.3.3　区块选取算法

区块选取算法即组织区块形成账本的协议，其设计目的包括以最大概率承认全网各诚实节点付出，恶意节点难以篡改，促进更多节点参与维护该系统(激励机制). 协议的具体方案与系统中采用的区块链结构相关，下文将分别对应链式结构、树状结构和图状结构进行介绍.

(1) 链式结构

在链式结构中，主要包括两个子协议，分别为最长链原则和激励原则. 最长链原则将网络中最长的链视为正确的链条，要求矿工一直在最长链上挖矿. 矿工在接收一个新区块时，必须停止当前挖矿过程，验证新区块是否有效，否则无法保证自己始终在最长链上工作. 借助最长链原则，保证了每个新区块都会被诚实矿工承认. 激励原则中，最先按规则生成区块的矿工将获得代币奖励和区块中所有交易的交易费. 基于上述两条原则，比特币系统达到一种纳什均衡，能够顺畅运转.

由于网络中的通信时延，链式区块链系统中可能会出现分叉情况. 为了避免分叉造成的不确定性，一般系统在生成新区块 B 后，再等待生成 6～7 个区块后才可确认 B 的有效性. 区块等待的数目是按照概率计算的，随着链条的长度增长，链条被推翻的难度越大. 这种设计能够有效降低系统的孤块率，提升安全性，在更快速的交易确认和更低的分叉概率间作出妥协. 当交易吞吐量较高，实时性较强时，该方案缺陷明显.

(2) 树状结构

如果采用链式结构中的最长链原则，当缩短出块时间，无法避免算力集中作恶的情况. 出块速度提升时，系统将频繁分叉. 大型矿池由于其存在多个物理节点，并且在网络通信过程中具有明显优势，其挖掘区块的所在分叉有极大的可能成为主链，而其他小型计算节点所做的努力在大多数情况下，是徒劳的，不能拿到奖励. 如果缩短了出块时间，还继续沿用最长链原则，对于多数小算力节点是不公平的. 基于以上背景，Sompolinsky 等人[13]提出了将链式结构改良为树状结构，并提出了 GHOST 协议.

该协议修改了节点构建和组织区块链的方式，即承认叔区块的合法性. 区块不仅包含了父块的哈希值，还可以包含叔块的哈希值，被引用的叔块也可以获得一定的奖励. 由于叔块也属于合法区块，是矿工算力的体现，因此在 GHOST 协议中主链的确定采用的是最重子树原则，如图 22 所示. 区块 0 有两个子树，以 $1B$ 为根的子树拥有更多的区块，因此 $1B$ 在主链上；同理 $1B$ 有三个子树，以 $2C$ 为根的子树拥有最多的区块，因此 $2C$ 在主链上. 同理递归，得到 GHOST 规则下的主链为 $0\rightarrow 1B\rightarrow 2C\rightarrow 3D\rightarrow 4B$. GHOST 协议从激励机制上保证了理性矿工会遵守协议的规则进行挖矿. 对 GHOST 规则和最长链规则性能的比较是通过分析每一个主链的增长率来表示的. 在分析了这个增长率的上下界后，利用随机采样的覆盖拓扑来模拟网络，再进行测量得到区块链的增长率.

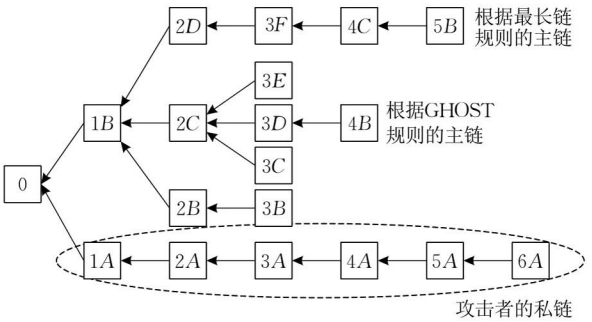

图 22　GHOST 协议与最长链原则对比

(3) 图状结构

在 DAG 区块链网络中，每一个新加入网络中的交易，并非简单选择最长链连接，而需要连接在之前有效节点后. 交易链接多个有效的父交易后，并依次验证其祖先节点交易的有效性. 随着交易的累加，

① Duong T, Fan L, Zhou H S. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. https://eprint.iacr.org/2016/716

② Chepurnoy A, Duong T, Fan L, et al. TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake. https://eprint.iacr.org/2017/232.pdf

万方数据

网络中生成了复杂的 DAG 图结构. 由于图状结构的网络复杂度更高,难以被更改,解决了一个链式结构中存在的隐患,即最终状态为非确定性. 但是,由于网络安全性低,相比于链式结构 51%算力攻击,理论上 34%的算力就可以控制整个网络. 双花攻击等多种攻击方式更易于在 DAG 网络中实现. 现有 DAG 项目多采用见证人主链概念抵御双花攻击,维持一条公认的主链作为凭证,而其他分支只要不和主链冲突都可以视为有效交易.

3.2.3.4 激励机制

激励机制设计的理论基础来自于博弈论. 区块链系统并不限制参与节点的身份,因此需要给予足够的奖励才可以使节点按照既定规则完成. 激励算法使得节点按照规则执行收获比作恶更高的收益,达到一种纳什均衡,因此能够保证系统健康有序的自我约束和发展.

目前比较主流的激励形式就是代币,如比特币每个区块中的 coinbase 奖励交易及手续费、Ouroboros 中的 coinstake 奖励交易及手续费等. 对于奖励数目的大小,各个系统都有自己的设定. 如在比特币中,最初区块的奖励是 50BTC,此后每挖出 21 万个区块,区块奖励就会减半. 以太坊系统中,除了主链中区块将获得 coinbase 奖励交易,分支中的叔区块也将获得 coinbase 奖励交易,该数目比主链稍低. 主链中的区块包含叔区块将有额外 1/32 的区块奖励,但是至多包含两个叔区块. 而一些 POS 代币新星币 NVC①、雅币 YAC②、宇宙币 CMC③ 的年利率分别为 5%、5%、1.5%.

3.2.4 共识框架抽象模型

上一小节介绍了现有区块链系统中共识框架的组成,其中包含多个功能不同的子算法. 本节将介绍如何对共识框架进行抽象建模、分析. 在区块链系统中,各参与者可视为其组件,如客户端、诚实矿工、恶意矿工. 系统中的各种协议则可视为连接各参与者的黏合剂,制定了各方交互的规则.

因此,区块链系统的抽象主要包含三个方面,分别为系统环境模型、各参与者能力的抽象以及对协议的模拟过程.

目前应用较广、认可度较高的两种共识机制分别为基于算力的共识、基于权益的共识. 对于共识机制的抽象建模和分析也集中于这两类共识机制. 尽管各研究中建模的具体细节各不相同,但是分析模型的思路可大致分为两类,博弈论和 UC 模型. 而应用这两种思路分析其他共识机制的安全性,是对研究区块链技术的一个重要方向. 下文主要介绍这两类共识机制的抽象模型.

3.2.4.1 基于算力的共识抽象模型

作为最初且最经典的区块链项目,比特币的安全性一直备受关注. 因此,前期的分析工作均围绕比特币系统展开,分析基于算力挖矿共识框架的安全性. 尽管比特币系统并不能代表所有的区块链系统,但是对其建模的思路和分析的角度仍具深刻的借鉴意义.

系统环境模型包含网络模型、时间模型、账本模型和收益模型. 网络模型指对网络通信模型的假设,如异步网络、同步网络及弱同步网络等. 时间模型指对时间的假设,如时间片(slot)、时期(epoch)、轮次(round)等. 账本模型包括确认交易需要等待的区块数 z(交易验证区块数)、不诚实矿工想要发起攻击的交易具有的价值 v、区块的深度 d 等. 参与者的能力可抽象为持有算力比例或挖矿速率 v 等,若诚实矿工的算力比例为 q,则不诚实矿工的算力比例为 $1-q$. 收益模型中包含矿工参与挖矿的花费 c,矿工挖出区块的奖励 r 和矿工的纯收益 rev.

可从两种角度对构建出的模型进行分析,一种是通过密码学中可证明安全的角度,通过构建通用可复合安全模型(Universally Composable,UC 模型)进行理论证明. 另外一种是从经济学角度,假设系统中的参与者均为理性矿工,目标为自身利益最大化,建模判断系统是否满足纳什均衡的条件,从而确定矿工持有算力大小的阈值.

(1) UC 模型

Garay 等人[52]通过构建 UC 模型分析比特币协议并提炼出两种本质属性:公共前缀和链质量. 这两种性质可被扩展用于分析区块链系统的安全性. 公共前缀属性保证如果 $\frac{t}{n-t}$ 成立,矿工诚实矿工维护的账本记录中,有一个公共的长前缀. 即各诚实矿工去掉本地账本中链尾的一些区块时,余下的链相同. 链质量属性保证任意诚实矿工账本中,由恶意矿工产生区块的比例小于 $\frac{t}{n-t}$. 由于证明的复杂性,文章基于静态假设开展分析,要求同步网络或者弱同步

① Novacoin. http://novacoin.org/
② Yacoin. http://www.yacoin.org
③ Cosmos. https://cosmos.network/

万方数据

网络，玩家数目和网络中总算力确定，POW 的问题复杂度为固定值等. 协议 Π 的执行由环境程序 $\mathcal{Z}$ 驱动，并生成多组实例运行协议 Π. 协议程序 Π 可以被看作可通讯并具有输入输出带的交互式图灵机. 该协议程序有两个功能，能够调用哈希函数计算功能和扩散消息功能. 哈希函数被建模为随机预言机模型(Random Oracle Model)，矿工的算力被抽象为与预言机交互的次数. 账本中的区块被抽象为三元组形式，$B=\langle s,x,ctr\rangle$，$s\in\{0,1\}^{\kappa}$，$x\in\{0,1\}^{*}$，$ctr\in\mathbb{N}$，s 串类比于比特币中上一个区块的哈希值，x 串表示区块值(可类比于比特币中交易)，ctr 表示随机数，q 用于限制随机串 ctr 的长度，同时表示向 RO 模型的请求数目. 根据上述模型，文中对提炼的两种性质进行了论证. 该模型是第一个对比特币系统提供可证明安全的论证，并将底层的数据结构(区块链)与上层应用(交易)分离. 后续构建许多的区块链系统都采用该模型论证其系统的安全性，还有很多研究对该论文从不同角度进行了改进. Garay 等人[53]继 15 年后又在 2017 年提出了对 Bitcoin backbone 的改进分析，允许 PoW 的问题复杂度按照一定规律改变. 2017 年 Pass 等人[54]在具有给定延迟上限的异步网络中重新证明了上述性质. 同年，他们提出了 Sleepy[55]模型，将通用安全假设从“绝大多数节点诚实”降低为“绝大多数在线节点诚实”，进一步细化了协议安全模型. 然而他们所提出的新协议中需要使用到公钥基础设施和公共随机串(Common Random String，CRS)，在无许可区块链环境中实用性不强.

此类共识协议的安全建模尚不完备，目前的最优模型仍然存在不足. 首先最优模型仍未考虑到成员数量变化问题，而总是假设成员数量为固定的. 这并不符合无许可分布式系统的特征. 其次，在现有模型中总是假定攻击者之间的行为是相互独立，若取消此假设，即允许攻击者根据已收集到的信息决定下一攻击步骤，会导致原有的安全分析失效.

(2) 博弈论

公有链系统自发运转来源于矿工对利益的追逐，因此，矿工的行为可使用博弈论相关理论建模分析. 从博弈论角度进行分析，是在不同假设背景下，计算单矿工或矿池采用不同策略所得收益，进而分析系统是否可靠.

Kiayias 等人[56]提出在网络节点完全信息知情情况下，将矿工挖矿时采用的策略分为两种. 第一种策略如比特币，矿工成功挖出区块后，立即广播给其他节点. 第二种策略中，矿工挖出区块后，不广播区块内容. 由于假设各节点信息知情，因此尽管其余节点不清楚区块的具体内容，但仍知道某节点成功挖出新块，需开启新一轮挖矿过程. 文章分别对矿工采用的两种策略场景分析，分析不同策略下系统达到安全性的条件. 在上述两种场景中，均简化为只有两种类型的矿工参与挖矿. 一种执行 FRONTIER 协议，另外一种执行假设优化过的协议. 系统被抽象为一棵状态树，使用二元组 (a,b) 表示系统当前状态，a,b 分别为自系统分叉后，各自链上已有的区块数目，如图 23 所示. 文中构建矿工的收益与系统所处的状态之间的联系，$\hat{g}_k(a,b)=k\cdot\hat{g}^{*}+\hat{\varphi}(a,b)$ 根据纳什均衡成立的条件，计算得出系统安全被保障的情况下矿工算力大小的阈值，并给出了形式化证明.

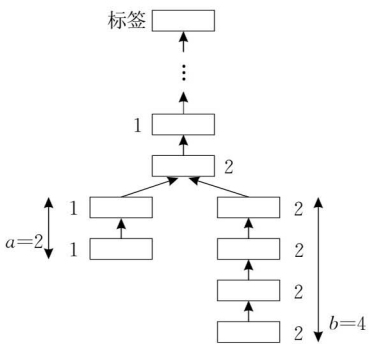

图 23　系统状态树示意图

Kroll 等人[57]对于矿工的挖矿过程进行了建模，对于矿工在何种情况下挖矿可以获得的收益进行了理论分析. C 为矿工挖矿时每秒钟需要耗费的资源的花费，$P=f(C)$ 表示每秒钟矿工可以计算哈希的次数，G 代表解决这个谜题需要计算哈希的次数，V 代表矿工挖到一个区块可以获得的奖励，所以矿工可以挣到 $\frac{PV}{C}$ 的奖励如果他投资 $G<\frac{PV}{C}$. 由于在区块链网络中，不仅仅只有一个矿工，所以现在假设网络中有 N 个矿工，所有矿工每秒钟可以挖出 R 个区块，则 $R=\sum_{i=1}^{N}\frac{P_i}{G}$. 在这里，让 P 代表每秒钟所有矿工可以执行的哈希数，令 $\overline{C}=\sum_{i=1}^{N}C_i$ 代表所有矿工挖矿的花费. 之后，$G=\overline{P}/R$，所以对于单个矿工进入挖矿市场的条件为 $\frac{\overline{P}}{R}<\frac{\overline{P}V}{\overline{C}}\Rightarrow\overline{C}<RV$. 在这里，系统全局纳什均衡的目标为系统中所有矿工每秒的付出和系统每秒给予的奖励相等 $\overline{C}=RV$，C 表示矿工的付出，R 表示每秒生产区块的数目，V 表示每个区

万方数据

块的奖励.文中使用 $S(L)=b^*$ 表示矿工账本的变化,S 表示矿工采用的策略,L 表示当前持有的日志,b 表示根据矿工的策略 S,在日志记录 L 的基础上选择的区块 b^*.文中对于协议的分析多从抽象的理解入手,并未给出形式化证明.

Natoli 等人[58]将区块链系统抽象为一个有向无环图,他们考虑将区块链系统建模为 $G=\langle V,E\rangle$,其中 V 表示区块链系统中的节点集合,E 表示各节点之间建立网络连接的集合.对于可分叉的区块链架构,文章中抽象为有向无环图结构,并用二元组 $l=\langle B,P\rangle$ 来进行表示,其中,B 表示区块链系统中区块的集合,P 是一个指向区块的指针,具体为前一个区块的哈希值.在这种建模下,文章对于区块链系统中不同节点出现分叉时如何达成一致进行了分析,假设系统中存在三个节点 p_1、p_2 和 p_3,并且在某一时刻在三个节点分别达到了不同的三种状态,分别表示为 $l_1=\langle B_1,P_1\rangle$、$l_2=\langle B_2,P_2\rangle$ 和 $l_3=\langle B_3,P_3\rangle$,如图 24 所示.

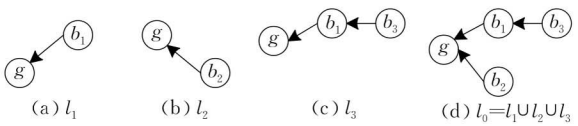

图 24 DAG 结构区块状态图

文章中作者使用有向无环图 $l_0=\langle B_0,P_0\rangle$ 来代表整个区块链网络中不同节点不同状态的集合,其中 l_0 如图 24(d)所示,更加正式的定义为 $\begin{cases}B_0=\bigcup\limits_{\forall i}B_i\\P_0=\bigcup\limits_{\forall i}P_i\end{cases}$.在这种模型定义下,文章中还对于挖矿过程、交易确认过程等进行了模型定义和理论分析并提出了平衡攻击方式.

Sompolinsky 等人[59]对于比特币网络在每一个时刻 t 的状态的最长链模型进行了建模,使用参数 λ 表示区块链网络每秒可以产生的区块数量,将区块链网络在 t 时刻的状态表示为 $\mathcal{C}^t=(C_0^t,C_1^t,C_2^t,C_3^t,\cdots,C_{height(t)}^t)$,$C_0^t$ 代表创世块,$height(t)$ 代表诚实最长链在时刻 t 的长度,区块 b 的高度为其到创世块的距离(其中 $height(C_0^t)=0$).此外,文中假设攻击者拥有占比为 α 的算力大小,则诚实矿工的算力占比为 $(1-\alpha)$,攻击矿工创建区块的速率为 $\alpha\cdot\lambda$,同时诚实矿工创建区块的速率为 $(1-\alpha)\cdot\lambda$.在这种建模下,作者对于接受策略、攻击策略、安全属性等进行了推理和理论分析证明,对于比特币安全保障产生了更加深入的理解,并为希望安全接受交易的矿工提供了安全界限.

Gramoli[60]对于私有链中各个节点之间的通信延迟进行了建模,他们认为存在一个传递消息的通信延迟上限的网络成为同步的,否则是异步的.在一个同步的通信模型中,能够达成共识的条件为:$n\geq 3f+1$,在这里 n 为分布式系统的所有节点数量,f 为存在错误的节点数量.

Kraft[61]针对于难度值控制,对于区块链链式结构建模成了一个具有时间依赖强度的泊松过程,并使用该模型对于各种哈希率场景下的区块时间进行了预测,分析了难度值更新对于区块产生增长的影响,最终提出了一种新的难度值更新方法.

在区块链网络中,在很长的一段时间内,大部分矿工都无法获得区块奖励,同时有很少的一部分矿工可以得到很多的区块奖励,区块链网络中的矿工寻求一种稳定的收入来源并且可以减少奖励的易变性,因此矿池已经成为了现在区块链网络中的主要挖矿形式.在矿池中的矿工可以集中计算力进行挖矿,并且可以分享产生区块的奖励.

Eyal 等人[62]定义每一个节点有一个唯一的 id,并且通过调用 $newTask(id)$ 命令来生成新的 $task$,节点可以在过程中使用 $work(task)$ 命令来做一个任务,$task$ 为进行挖矿的过程.矿工通过 $publish(task,PoW)$ 命令来发布任务和自己已经产生的工作量证明,工作量证明分为部分工作量证明 $pPoW$,和全部工作量证明 $fPoW$,$fPoW$ 为成功挖到区块的矿工产生的证明;$pPoW$ 是没有挖到的矿工的证明,这个证明可以在一次挖矿过程中代表其付出的算力,矿池管理员也会根据这个证明来分配一次挖矿的奖励.此外,区块链网络中的一个节点可以通过 $pay(w,b)$ 命令来给 ID 为 w 的节点发送 b 个比特币.文章中假设矿池的数量为 p,区块链网络中所有矿工的所有计算能力总和为 m,效力于矿池 i 的矿工算力为 m_i.在这种模型定义下,作者定义了矿池之间的一种攻击方式,简单描述可以理解为一个矿池派遣部分矿工去其他矿池进行攻击,只对于被攻击的矿池提供 $pPoW$ 证明来分享该矿池出块奖励,但是其成功挖到区块时,不向被攻击矿池的管理员进行汇报,来分享自己的奖励.作者对于矿池中的扣块攻击方式进行了分析并且对于矿池中扣块攻击的收益收敛性进行了理论证明,得到如果矿池渗透率是常数则矿池收益收敛的结论.在文章中,对于单矿池攻击(两个矿池,只允许一个矿池进行攻击)、双矿池相互攻击(两个矿池,两个矿池之间可以相互攻

万方数据

击)、p 相同矿池攻击(多个矿池之间可以相互攻击)分别进行了建模和分析.文中作者认为,任何一个矿池可通过攻击其他矿池,增加自己利润,但如果他们都选择攻击对方,获得利润要少于都不选择攻击对方的情况,在矿池间可以相互攻击的条件下,存在一种纳什均衡,使得相互进行攻击的收益小于相互不进行攻击的收益.

Lewenberg 等人[63]同样对于使用矿池挖矿的区块链系统模型进行建模.他们讲矿池间交互建模为一个矿工网络,一个矿工网络由 6 元组 $\Gamma=\langle\mathcal{M},S,\mathcal{P},D,d,\lambda\rangle$ 进行表示.其中 $\mathcal{M}=\{1,\cdots,n\}$ 为一组矿工;S 是一些矿工到一些矿池中的划分(S 中的每一个元素是构成单个矿池的矿工集合);$\mathcal{P}=\{p_1,\cdots,p_n\}$ 是每一个代理的算力分布,如果 p_i 是代理 i 的算力比例,则 $\forall i\in\mathcal{M}$,$p_i\in[0,1]$,$\sum_{i\in\mathcal{M}}p_i=1$;$D>0$ 表示不同矿池之间物理机的通信延迟;$d>0$ 是相同矿池中不同物理机之间的通信延迟;λ 是每秒区块链网络期望挖到的区块数量.作者假设每一个矿工 $i\in\mathcal{M}$ 根据泊松分布过程在参数 $p_i\lambda$ 下进行挖矿.没有参与到矿池中的矿工被定义为一个独立的矿工(sole miner).文中假设矿工只可以通过矿池管理者进行通信.作者定义 $\beta=\beta(\Gamma)$ 为每秒钟最长链的区块增长率.对于每一个矿工 i,作者使用 $\gamma_i=\gamma(\Gamma)_i\in[0,1]$ 表示被矿工 i 挖出区块属于最长链的概率.对于每一个矿池 $C_j\in\mathcal{S}$,定义 $\gamma C_j=\sum_{i\in C_j}\gamma_i$.由于只有在最长链上挖出区块的矿工会获得奖励,因此矿工 i 有动力来提高 γ_i.文中之后对于两个理论进行了证明:

(1)令 $\Gamma=\langle\mathcal{M},\mathcal{S},\mathcal{P},D,d,\lambda\rangle$ 是一个有 $|\mathcal{M}|>1$ 矿工,$D>0$ 并且 $d>0$ 的矿工网络,对于每一个独立的矿工(sole miner) i,$\lambda\geq\beta(\Gamma)>p_i\lambda$.

(2)令 $\Gamma=\langle\mathcal{M},\mathcal{S},\mathcal{P},D,d,\lambda\rangle$ 是一个只有一个矿池和没有独立的矿工(sole miners)的矿工网络,则 $\beta(\Gamma)=\dfrac{\lambda}{1+2d\lambda}$.

在这种模型下,文章对于两个矿工的场景、在联合架构中挖矿的场景、作为合作游戏的挖矿的场景分别进行了理论分析,对于矿池奖励和矿池计算能力的非线性关系、矿工会选择加入哪个矿池的博弈行为进行了推理和说明.

3.2.4.2　基于权益证明共识模型的分析

(1) UC 模型

纯 PoS 协议最大的问题在于其安全性一直备受争议.Kiayias 等人在 Crypto 2017 上提出了第一个具有严格安全模型的 PoS 协议 Ouroboros[33],首次证明了 PoS 协议具有理论可行性.然而 Ouroboros 所使用的安全模型与实际的 PoS 模型相差较大.模型中使用了同步通信模型且没有涉及惩罚机制,因而并不具备实际可行性.在 2018 年 Eurocrypt 上,他们又对此工作进行改进,提出 Ouroboros Praos 共识[64],并在半同步网络环境下进行了一致性分析.结果证明此方案可以应对全自适应攻击,但缺点是系统吞吐量受限.其安全性证明基于通用可组合(Universal Composable,UC)模型下前向安全的数字签名和一类新的可验证随机函数.2018 年 CCS 上,他们还提出了 Ouroboros 的动态版本 Ouroboros Genesis[65],协议的安全性分析同样需借助 UC 模型.

Danian 等人提出了 Snow White 协议①并证明了其安全性.此协议通过 BFT 类共识与 PoS 类共识的结合进一步提高了效率,但要求其底层的 PoS 协议自身必须是安全的.

PoS 方面的另一个代表性工作是 MIT 的 Gilad 等人[34]所提出的 Algorand 协议.该协议的最大优点是无分叉,但其不足在于对同步网络环境的依赖性较大,且其模型理论存在不严谨之处.

(2)博弈论

POA 算法的分析从博弈论角度切入,关于系统安全性,Bentov 等人[35]证明了如果网络中有 p 比例的产权,则拥有整个系统 y 比例产权的攻击者需要拥有 $\left(\left(\frac{1}{y}-1\right)\cdot p\right)^N$ 倍的算力才能从系统中获利.目前使用这种共识算法的是 Slimcoin,并且该币依赖 PPC 币.

3.3　共识算法小结

本小节对上述几类共识算法作简单小结,将各算法特性进行对比,见表 3.

3.4　区块链网络

区块链中使用了基于互联网的 P2P 网络架构,见图 8.P2P 网络通常也称对等网络,网络中每个参与节点贡献一部分计算能力、存储能力、网络连接能力.通过网络,这些能力作为共享资源可被其他对等节点直接访问.访问过程中不需要再经过中间实体,所以每个节点既是资源和服务的使用者,又是整个资源和服务的提供者.每个网络节点以“扁平(flat)”的拓扑结构相互连通.整个网络中无特殊地位的节点,每个节点都可对任意对等节点做出响应,提供资源.

① Bentov I, Pass R, Shi E. Snow White: Provably Secure Proofs of Stake. https://eprint.iacr.org/2016/919.pdf

万方数据

表 3 主要共识算法对比

共识机制	POW	POS	DPOS	POL	POC	PBFT	RAFT
中心化程度	去中心化	去中心化	部分去中心化	部分去中心化	去中心化	部分去中心化	部分去中心化
是否抗拜占庭节点	是	是	是	是	是	是	否
是否需要许可	否	否	否	否	否	是	是
系统规模（可允许节点数）	不限	不限	不限	不限	不限	有限	有限
安全性假设	1/2 以上算力诚实	1/2 以上 stake 诚实	1/2 以上股权诚实	1/2 以上 CPU 未损坏	1/2 以上存储空间诚实	1/3 以下恶意节点	1/2 以下故障节点
动态加入与退出	支持	支持	支持	支持	支持	不支持	不支持
适用场景	公有链	公有链	公有链	公有链	公有链	联盟链	联盟链
一致性	弱一致性	弱一致性	弱一致性	弱一致性	弱一致性	强一致性	强一致性
主要资源占用	物理资源（算力）	经济资源（权益、代币）	经济资源（权益、代币）	物理资源（特殊硬件）	物理资源（存储）	物理资源（通信）	物理资源（通信）
算法功能	确定记账权	确定记账权	确定记账权	确定记账权	确定记账权	区块生成	区块生成
理论分析	UC 模型，博弈论模型	UC 模型，博弈论模型	较弱	较弱	较弱	较弱	较弱

除了保障网络连接的基本通信协议之外，针对不同的应用需求，网络层还可以包含其他的协议，区块链本身对使用的网络协议并没有特定的限制，如挖矿过程中用到的网络协议，基于内容进行文件传输的网络协议，矿工使用的高速区块中继网络协议等等. 表 4 介绍了几种用于控制挖矿过程的网络协议，如 Setgenerate 协议、Stratum 协议、Getwork 协议、Getblocktemplate 协议等.

表 4 挖矿网络协议

协议	用途	目的	特点
Setgenerate 协议	CPU 挖矿	控制挖矿	搜索空间大小为 4G
Getwork 协议	GPU 挖矿	使挖矿程序与节点交互	搜索空间大小为 4G
Getblock-template 协议	矿池协议	使矿池与节点交互	区块变动数据通知不及时，算力浪费；每次调用节点均返回数据，频繁调度加重开销
Stratum 协议	矿池协议	使矿池与矿工交互	矿池指派任务与矿工申请任务相结合，有足够的搜索空间，又有很小的交互量

尽管区块链网络中节点由 P2P 协议组织，各个节点间没有主次之分，但是由于不同区块链系统在不同场景下需求功能不同，节点的设计也不同. 总的来说，节点按照功能可以分为全节点、SPV 节点，按照参与共识的身份可以分为客户端、提交者、验证者等，见图 25.

区块链中的节点一般可以包括四个功能：路由通信、账本存储、参与共识、钱包. 在不同的场景下，

图 25 节点类型

可以选择需要的功能组成对应的节点. 如果需要以上四个功能，则组成了全节点；如果仅仅是为了交易，则只需包含与用户相关的账本、钱包、路由通信即可完成简易交易验证，因此这类节点又可以被称为“SPV 节点”；如果节点只是用于实现共识算法，则只需包含参与共识的逻辑即可.

区块链的网络构建过程因区块链种类不同而有所区别. 在无需许可的区块链中，例如比特币、以太坊系统中，当新的网络节点启动后，需要寻找网络中可靠的节点并连接. 寻找的节点可以是比特币系统中一直维持运转的种子节点，也可以是已知的运行节点. 当新节点与网络中运行节点建立连接后，可以将自身地址消息在网络中传播，参与系统运转. 在需要许可的区块链中（包括联盟链和私有链），如超级账本、R3 区块链联盟、ChinaLedger 联盟等，这类区块链系统中，参与运行维护的节点身份信息已知，因此节点在加入到网络中之前需要进行身份的验证，经过验证后节点参与系统运转.

万方数据

节点信息的获取对于分析网络特性也有十分重要的作用，Donet 等人[66]和 Huang 等人[67]分别从不同的侧重点入手提取网络中节点信息，并进行分析. Donet 等人[66]试图解构比特币网络，文中通过数据收集确定了 872 000 多个不同的比特币节点相关信息，如网络大小、节点地理分布、节点中断可用性等，这篇文章提供了分析区块链网络的思路，根据其思路可以研究区块链网络构建的相关参数，其过程可以概述为图 26.

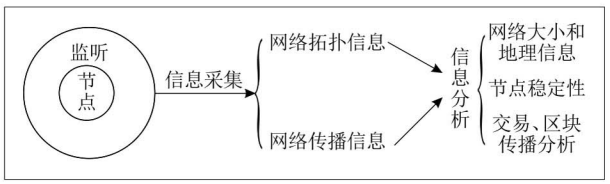

图 26　区块链网络信息提取

比特币网络是一个去中心化、去信任的网络，节点的身份有好有坏，Huang 等人[67]以此为出发点介绍了根据各节点的行为模式自动聚类的方法——BPC 算法，将各节点的交易信息作为核心特征抽象成一个序列表示，并依据序列间的相似程度进行分类.

4　区块链前沿热点

第 3 节详细介绍了区块链框架中的三项最核心且最基本的技术：密码学、共识机制和区块链网络. 随着该技术被广泛应用，关于其隐私性、安全性和性能等方面存在的问题和优化方案备受关注. 本节将介绍在区块链隐私保护、区块链攻击方案和区块链可扩展性三个方面的研究进展.

4.1　区块链隐私保护

如上文介绍，区块链使用数字签名保障用户数据的隐私性，如比特币系统使用椭圆曲线签名算法. 尽管无法直接从公钥地址反推出用户的私钥，但是由于区块链历史数据全网可见，基于这些公开的数据能够分析出用户相关隐私信息，在一定程度上破坏了用户数据隐私性.

4.1.1　比特币匿名性分析

通常，货币类型的应用中，对交易匿名性的要求格外高，因此区块链数字签名部分的技术改良也主要见于一些货币的应用. 此外，比特币是最广泛使用的公有链，历史交易数据丰富，很多研究从不同的角度分析了比特币的匿名性. 分析过程通常是将获取的信息抽象成网络或者图结构(如图 27～图 30)，再将交易的信息汇总，分析其静态动态规律[68-69].

Reid 等人[68]从这些信息中抽象出了交易网络和用户网络. 交易网络是一个有向图，如图 27 所示，顶点表示交易，边表示了一个交易输出作为另一个交易输入的关系. 利用 2009 年～2011 年的交易数据获得交易网络图之后，对交易的累积出入度情况进行分析. 使用统计模型提炼出其静态分布情况并进行动态分析，如交易网络边缘数量、密度和平均路径长度. 用户网络代表了用户之间的比特币流量，如图 28 所示，顶点表示一个公钥地址，边表示公钥地址之间比特币的转移. 由于一个用户拥有大量的公钥地址，因此仅仅利用上述网络是不完整的，不能直观地显示出网络中各用户的比特币流动关系.

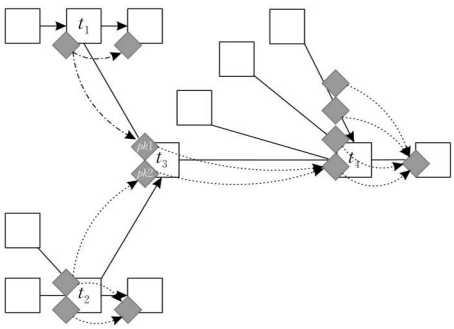

图 27　交易网络抽象图

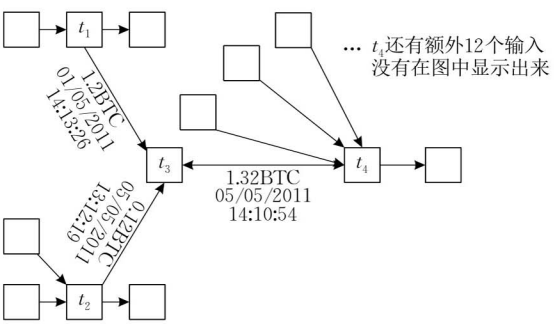

图 28　用户网络抽象图

一笔交易中的多个输入通常来自同一账户，因此可利用这一属性来收缩不完整网络中的顶点子集. 因此文中又构造了一个辅助网络，见图 29，通过找到其中非平凡的最大连通分量来对应到不同用户. 对用户网络使用相同的统计模型进行分析，得到了其静态特征网络累积度的分布情况和动态特征，如用户网络的边缘数量、密度和平均路径长度. 除获取上述信息，还有一些非网络信息，如果能将上述图结构和非网络信息联系起来，则说明比特币网络的匿名性还远远不够. 文中给出了一个简单的例子，利用 the Bitcoin Faucet 网络提供的信息和已经提炼出来的交易网络、用户网络，能够获取一周内接收比

万方数据

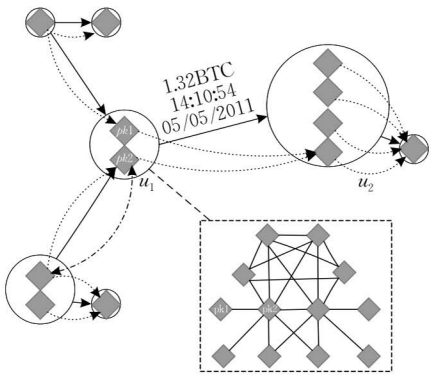

图 29 辅助网络示意图

特币的用户的地理定位 IP 地址的地图.

Fleder 等人[69]构建的图与 Reid 等人[68]构建的图非常类似. 不过它的分析起点不是从交易网络和用户网络图,而是从网络环境(如某些公开论坛). 在网络社交平台中收集一些粗糙的交易信息,再利用这些粗略信息从交易记录中筛选合适的消息. 再结合 Reid 等人[68]方法构建图,可以从中获取用户参与的其他活动,进而标记一些有着大流量的用户节点. 文中已成功将论坛中的账户对应的知名实体 SatoshiDICE 分析出来,表明了比特币及其相似系统中对于用户隐私性的保护还不足够.

Meiklejohn 等人[70]追踪比特币的流动过程. 通过发起重识别攻击以及从网络论坛中采集信息,再使用启发式聚集的方法将这些地址分组,最后再通过重验证的方式确定每组对应的主要机构. 在文中虽然没有以一种图表的形式抽象出所有的交易,但是其使用的聚集方法,一种与 Reid 等人[68]文中相似,根据交易的输入进行聚集,另外一种是扩展,是基于找零的变更地址关系进行聚集. 这篇文章在讨论比特币本身的匿名性强弱的背后,也希望能够一定程度上帮助判断非法交易和维护交易环境.

Barber 等人[71]定性地分析了比特币系统的易受损性和系统中一些常见的攻击方式,并提出了一种减少信任的方法来增强系统的匿名性. 系统中共有三类交易,分别为承诺交易、声明交易、撤款交易,分别用于正常交易和有参与方作恶时. 参与交易的双方分别生成两对公私钥,用于签署不同的交易,保障了不可链接性,见图 30. 这些论文都说明了基于比特币系统提炼出的区块链技术在安全性上还远远不够,比特币系统中的匿名性是通过假名的方式表现的,并不是真正的匿名性,尽管并没有对应到个人的真实信息,但是在有了足够的用户额外信息之后,基于大数据的分析或者其他有针对性的攻击,假匿名性系统无法提供承诺保障.

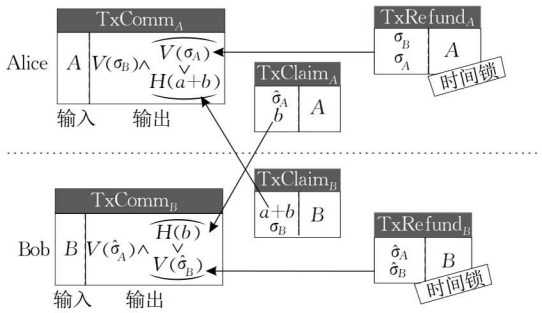

图 30 通过减少信任增强系统匿名性

4.1.2 匿名性提升方案

针对上述问题,很多研究提出了改善区块链系统匿名性的方案,主流方案有三种:混币技术、环签名、零知识证明.

(1)混币技术

混币技术的基本思想是,通过多个标准交易中的多地址合作,切断每笔交易的输入输出之间的联系. 最简单的混币技术通过在系统中增加一些中间可信机构①②来完成零钱兑换等,减少了用户隐私暴露的几率. 显然,这种方式有着较为严重的局限性:运营商可能会窃取资金,追踪货币,或者遭遇了倒闭等情况.

CoinJoin 利用了比特币的多签名脚本,将多个交易合并为一个交易. Dash 引入了主节点,将 CoinJoin 作为协议的一部分. 主节点除了维持网络的安全性之外,还提供 CoinJoin 隐私服务. 用户可以向主节点请求,进行单轮或多轮的混币服务. CoinJoin 的优点是简单高效,与原有比特币的脚本完全兼容;且参与者之间不可能出现窃取他人货币的情况. 但缺点在于参与成员之间可能可以建立输入输出之间的关联. Tumblebit 是基于不可信中介的一类混币技术,关键点在于使用 cut-and-choose、盲签名、多签名和 RSA 加密技术,使得中介只能提供服务,而不能将交易的输入输出建立联系. 缺点在于需要发送方、接收方和第三方进行多次交互.

(2)环签名

门罗币(Monero)是 Cryptonote③ 的一个应用,也是最有名的隐私保护数字货币之一. 门罗币中首先定义了不可链接性(Unlinkability)和不可追踪性

① Bitcoin Fog Company. http://bitcoinfog.info/
② The Bitcoin Laundry. http://www.bitcoinlaundry.com/
③ Cryptonote Currencies—Anonymous 3rd Gen. AUGUST 07, 2014. https://www.ccn.com/cryptonote-more-anonymous-than-bitcoin/

万方数据

(Untraceability)[72]①，后来加入了保密支付来保证交易金额的隐私性.具体而言，门罗币使用了一次性地址来掩盖真实地址，使得发送者无法从接收者的地址中推导出接收者的原地址，从而实现了不可链接.为避免由此所导致的双花攻击，在交易时发送方需要根据自己的一次性地址的私钥来算出一个 Key Image，并将其作为签名的一部分发出去.值得注意的是，这里的签名使用了环签名来实现不可追踪性.这样做的好处是，交易的校验者可以确定这笔交易来自公钥环上的某个私钥的所有者，且该私钥所有者仅能使用该私钥一次.

Kumar 等人[73]对门罗链进行合法性检查，开发并评估门罗币的抗攻击性能，通过实验结果证明了其安全性.Noether 等人②分析了 Cryptonote 应对 plausible 攻击的状况.Macheta 等人③针对 2014.9.4 发生的网络攻击进行分析，并介绍了 Cryptonote 社区和 Monero 社区相处的一些初步的弥补措施.Mackenzie 等人④指出了对 Cryptonote 安全性造成威胁的攻击方式，并提出了能增强其稳定性的改善措施.Noether 等人[74]对现有的加密机制提出改善措施，通过利用 Liu 等人[75]提出的签名方式能够隐藏交易过程中的数额.Noether⑤使用环签名的方式改进了 gmaxwell 的隐私交易，同时还可以应用到 Noether 等人⑥或 Noether 等人[74]中介绍的两种 Monero 系统中，门罗币的主要问题在于由于环签名、环保密交易等，使得交易尺寸膨胀严重.

(3)零知识证明

Zcash[18]是首个具有完全的匿名性的数字货币.借助名为 zk-SNARK 的工具，零币完全隐藏了交易双方的身份、交易的金额以及一切与交易相关的信息，从而实现了完整的隐私保护.具体而言，零币的构造者提出来称为 Decentralized Anonymous Payment(DAP)的机制，并将这个机制搭建在了比特币之上.在 Zcash 中，通过基于承诺的铸币交易(Mint)，可以将比特币铸为零币.接着通过基于零知识证明的花费交易(Pour)，实现了完全匿名和交易金额隐藏的交易.其中零知识证明保证了交易的正确性、平衡性等性质.由于执行 zk-SNARK 需要一个可信的启动过程，这在一定程度上影响了零币的普及.在现实中使用了安全多方计算技术来解决这一问题.该研究后续部分还在继续，致力于减少证明大小和验证时间，提升扩展性和伸缩性.

4.2　针对区块链网络的攻击方式

在区块链网络攻击方式中，大多并不是对于区块链共识算法本身进行攻击，而是通过破坏区块链架构协议平衡或通过网络延迟等其他因素进行攻击.攻击者在网络中造成各个矿工节点的存储数据产生差异，并通过某些方式让网络中的其他诚实矿工可以认证自己做出的恶意行为是正确的.区块链网络的现有防范攻击方式，大多使用矿工攻击的收益和矿工付出代价之间进行权衡，让恶意矿工对于区块链网络攻击所付出的代价要高于攻击付出的收益.在本节中，我们将对于目前区块链网络常见攻击方式分别进行介绍和理论分析，其中包括双花攻击、自私攻击、月食攻击、平衡攻击、扣块攻击.

4.2.1　双花攻击

目前已经耳熟能详的是双花攻击.由于在电子货币系统中，电子货币是易复制的，攻击者可以将同一份电子货币发送给多个其他接收者，即一笔电子货币进行了多次使用.

在比特币系统中，为了抵抗攻击者的双重支付恶意行为，中本聪使用工作量证明机制来验证支付行为，但是在这种方式下，需要在一个区块连接多个区块后才能验证包含支付交易的区块的有效性，这个过程需要平均 10 min 的时间来进行转账交易，这种方法在现代交易系统中是不能被接受的.针对快速支付的场景，Karame 等人[76]对于快速支付下双花攻击的场景进行了分析，认为攻击者可以使用很低的成本对于比特币快速支付进行攻击，并且成功的可能性极大.在文章中，对于成功执行双花攻击的需要满足的三个必要条件进行了分析($\mathcal{V}$ 表示服务提供商，$\mathcal{A}$ 表示恶意矿工，$TR_{\mathcal{V}}$ 表示发送给服务提供商的交易，$TR_{\mathcal{A}}$ 代表双花交易)：

(1) $TR_{\mathcal{V}}$ 加入到 V 的钱包中

$\mathcal{H}$ 代表 $\mathcal{A}$ 一个或者多个帮凶的集合，$T_{\mathcal{A}}$ 代表发送双花交易的时刻，$T_{\mathcal{V}}$ 代表发送普通交易的时刻

① Cryptonote V2.0. https://cryptonote.org/whitepaper.pdf. 2013

② Noether S, Noether S, Mackenzie A. A note on chain reactions in traceability in cryptonote 2.0. https://cryptorating.eu/whitepapers/Monero/MRL-0001.pdf

③ Macheta J, Noether S, Noether S, et al. Counterfeiting via merkle tree exploits within virtual currencies employing the cryptonote protocol. http://cryptochainuni.com/wp-content/uploads/Monero-Counterfeiting-via-Merkle-Tree-Exploits-within-Virtual-Currencies-Employing-the-CryptoNote-Protocol.pdf

④ Mackenzie A, Noether S, Team M C. Improving obfuscation in the cryptonote protocol. https://web.getmonero.org/resources/research-lab/pubs/MRL-0004.pdf

⑤ Ring Ct for Monero. https://pdfs.semanticscholar.org/b9a3/837 3a2fe3f2244 51b07ff3d7664e1b18b2b4.pdf

⑥ Noether S, Noether S. Monero is not that mysterious. https://pic.nanjilian.com/20180716/169c05d0deb630a15f50def3df62b485.pdf

万方数据

($T_{\mathcal{A}}=T_{\mathcal{V}}+\Delta t, t>0$),$\delta t_{\mathcal{V}\mathcal{H}}^{\mathcal{A}}$ 代表 $TR_{\mathcal{A}}$ 从 $\mathcal{V}$ 到 $\mathcal{H}$ 的网络传输时间,$\delta t_{\mathcal{A}\mathcal{V}}^{\mathcal{A}}$ 代表 $TR_{\mathcal{V}}$ 从 $\mathcal{V}$ 到 $\mathcal{H}$ 的网络传输时间. 见式(1):

$$\begin{aligned} t_{\mathcal{V}}^{\mathcal{A}}-t_{\mathcal{V}}^{\mathcal{V}} &\approx \tau_{\mathcal{A}}+\delta t_{\mathcal{V}\mathcal{H}}^{\mathcal{A}}-(\tau_{\mathcal{V}}+\delta t_{\mathcal{A}\mathcal{V}}^{\mathcal{V}}) \\ &\approx \Delta t+\delta t_{\mathcal{V}\mathcal{H}}^{\mathcal{A}}-\delta t_{\mathcal{A}\mathcal{V}}^{\mathcal{V}} \end{aligned} \tag{1}$$

文章中要求满足 $\delta t_{\mathcal{V}\mathcal{H}}^{\mathcal{A}}<\delta t_{\mathcal{A}\mathcal{V}}^{\mathcal{V}}$,假如这样,则 $t_{\mathcal{V}}^{\mathcal{V}}<t_{\mathcal{V}}^{\mathcal{A}}$,则满足了第一个条件.

(2) $TR_{\mathcal{A}}$ 在区块链网络中被确认

文章中将一个在时间间隔$[t_k, t_{k+1}]$区块包含交易 $TR_{\mathcal{V}}$ 的概率建模,见式(2):

$$p_{\mathcal{V}}(k)=\mathrm{Pr}_{\mathcal{V}}^{k}\cdot\prod_{i=0}^{k-1}(1-\mathrm{Pr}_{\mathcal{V}}^{i})=\eta_{\mathcal{V}}^{k}p\cdot\prod_{i=0}^{k-1}(1-\eta_{\mathcal{V}}^{i}p) \tag{2}$$

同样,一个包含交易 $TR_{\mathcal{A}}$ 在同一时间间隔内生成的概率,见式(3):

$$p_{\mathcal{A}}(k)=\mathrm{Pr}_{\mathcal{A}}^{k}\cdot\prod_{i=0}^{k-1}(1-\mathrm{Pr}_{\mathcal{A}}^{i})=\eta_{\mathcal{A}}^{k}p\cdot\prod_{i=0}^{k-1}(1-\eta_{\mathcal{A}}^{i}p) \tag{3}$$

如果在时间 $t=s\cdot\delta t+t_0$(t_0为两个交易 $TR_{\mathcal{V}}$ 和 $TR_{\mathcal{A}}$ 共同存在与网络的时刻,δt 是定义的相等时间间隔)网络中的每个节点已收到至少交易 $TR_{\mathcal{V}}$ 或 $TR_{\mathcal{A}}$,以下模型是适用的,见式(4):

$$\begin{cases} \eta_{\mathcal{A}}^{k}\le\eta_{\mathcal{A}}^{k+1},\ \eta_{\mathcal{V}}^{k}\le\eta_{\mathcal{V}}^{k+1}, & k<s \\ \eta_{\mathcal{A}}^{k}=\eta_{\mathcal{A}}^{k+1}=\eta_{\mathcal{A}}^{s},\ \eta_{\mathcal{V}}^{k}=\eta_{\mathcal{V}}^{k+1}=\eta_{\mathcal{V}}^{s}, & \text{其他} \end{cases} \tag{4}$$

在这里,要求,见式(5):

$$\forall i\ge s,\ \eta_{\mathcal{V}}^{i}+\eta_{\mathcal{A}}^{i}=\eta_{\mathcal{V}}^{s}+\eta_{\mathcal{A}}^{s} \tag{5}$$

计算双花攻击成功的概率,文章中假设,$\forall k$、$\eta_{\mathcal{V}}^{k}$、$\eta_{\mathcal{A}}^{k}$不交换他们新建模块. 这样,正在挖掘 $TR_{\mathcal{V}}$ 的节点生成新块所需的 $t_{g_{\mathcal{V}}}$ 时间与正在挖掘 $TR_{\mathcal{A}}$、$t_{g_{\mathcal{A}}}$ 的节点所需的 $t_{g_{\mathcal{V}}}$ 时间无关. 据此,满足第二个要求的概率 $P_S^{(2)}$ 计算,见式(6):

$$P_s^{(2)}=Prob(t_{g_{\mathcal{A}}}<t_{g_{\mathcal{V}}})+\frac{1}{2}Prob(t_{g_{\mathcal{A}}}=t_{g_{\mathcal{V}}}) \tag{6}$$

即 $P_s^{(2)}$ 由两部分组成,一个对应包含 $TR_{\mathcal{A}}$ 的块首先生成的事件,第二个对应包含 $TR_{\mathcal{A}}$ 和 $TR_{\mathcal{V}}$ 的块同时生成的事件,即,$t_{g_{\mathcal{A}}}=t_{g_{\mathcal{V}}}$. 在后一种情况下,包含 $TR_{\mathcal{A}}$ 的块最终被比特币同行采用的概率是 0.5. 在这里,$Prob(t_{g_{\mathcal{A}}}<t_{g_{\mathcal{V}}})$和 $Prob(t_{g_{\mathcal{A}}}=t_{g_{\mathcal{V}}})$的计算,见式(7)和(8).

$$\begin{aligned} Prob(t_{g_{\mathcal{A}}}<t_{g_{\mathcal{V}}}) &=\sum_{g_{\mathcal{A}}=0}^{\infty}\boldsymbol{p}_{\mathcal{A}}(g_{\mathcal{A}})\cdot\boldsymbol{p}_{\mathcal{V}}(g_{\mathcal{V}}>g_{\mathcal{A}}\mid g_{\mathcal{A}}) \\ &=\eta_{\mathcal{A}}^{0}p(1-\eta_{\mathcal{V}}^{0}p)+\sum_{g_{\mathcal{A}}=0}^{\infty}\eta_{\mathcal{A}}^{g_{\mathcal{A}}}p\cdot(1-\eta_{\mathcal{V}}^{g_{\mathcal{A}}}p)\cdot \\ &\quad\prod_{j=0}^{g_{\mathcal{A}}-1}(1-\eta_{\mathcal{V}}^{j}p)(1-\eta_{\mathcal{A}}^{j}p) \end{aligned} \tag{7}$$

$$Prob(t_{g_{\mathcal{A}}}=t_{g_{\mathcal{V}}})=\sum_{g_{\mathcal{A}}=1}^{\infty}p^{2}\eta_{\mathcal{V}}^{g_{\mathcal{A}}}\eta_{\mathcal{A}}^{g_{\mathcal{A}}}\cdot\prod_{j=0}^{g_{\mathcal{A}}-1}(1-\eta_{\mathcal{V}}^{j}p)(1-\eta_{\mathcal{A}}^{j}p) \tag{8}$$

(3) $\mathcal{V}$ 的服务时间小于 $\mathcal{V}$ 可以检测到双花行为时间

由于服务时间远远小于确认交易的时间,供应商在提供 it 服务之前无法验证 $TR_{\mathcal{V}}$ 是否包含在最近的比特币块中. 此外,即使 $\mathcal{V}$ 的客户端在向 $\mathcal{A}$ 提供服务之前同时接收到 $TR_{\mathcal{A}}$ 和 $TR_{\mathcal{V}}$,在当前的 Bitcoin 实现中也不会向 $\mathcal{V}$ 传播任何消息/警告. 因此,如果需求(1)已经被满足,那么需求(3)在比特币客户端中总是被满足.

此外,他们对于现有快速支付中防止双花攻击的两种方法“Using a Listening Period”和“Inserting Observers in the Network”进行分析,说明其存在的弊端. 最后,他们提出了自己的的解决方法“Forwarding Double-Spending Attempts in the Network”来对抗快速支付场景中的双花攻击.

Rosenfeld[77]研究了典型攻击背后的随机过程及其成功概率,解释了比特币系统的基本架构,对抗双花的对策以及这种保护的破坏方式. 本文推导了一次双花攻击成果的概率,讨论了什么情况下进行双花攻击是经济的,并且证明了等待 6 个确认是绝对安全的或等待时间长度是双花攻击的关键因素是错误的. 在文章中,对于双花攻击成功 a_z 进行了计算,见式(9),并以不同方式列表,讨论了双花攻击的经济性.

$$a_z=\min\left(\frac{q}{p},1\right)^{\max(z+1,0)}=\begin{cases} 1, & z<0\vee q>p \\ \left(\frac{q}{p}\right)^{z+1}, & z\ge 0\wedge q\le p \end{cases} \tag{9}$$

式中,p 表示该区块由诚实矿工发现的概率,q 表示该区块由不诚实矿工发现的概率,z 表示诚实矿工比非诚实矿工多挖的区块.

Bissias 等人[78]提出并验证了一个新的区块链挖矿过程的数学模型,并用它来对所有区块链系统的基础双花攻击进行经济评估. 在文章中用 R 表示攻击者收益、C 表示矿工的花费,根据概率分布,算出其期望,见式(10)和式(11):

$$E[C(X;d,q)]=\frac{qdb}{10}+zBG\left(d;z+\frac{1,10}{q}\right)-\frac{qdB}{10}G\left(d;z,\frac{10}{q}\right) \tag{10}$$

$$E[R(X;d)]=vG(d;z,10/q) \tag{11}$$

式中 X 表示矿工挖出 z 个区块所用的时间,d 表示

万方数据

所给时间期限，q 表示所使用算力比例，B 表示诚实挖矿获得的收益，G 函数与 X 的概率密度相关，v 表示不诚实挖矿获得收益.

当 $R-C=0$ 时，攻击者达到攻击收益平衡点，可以求出平衡点对应的 v 值，利用这个公式可以量化各参数对整个系统的作用. 计算表明交易的安全性随着收到的确认数目提升而提升，并且如果客户强加一个验证的截止期限，攻击者需要使用低于35%的算力和超过 10 个区块验证才能获得收益.

4.2.2　自私攻击

Eyal 等人[79]提出了名为自私挖矿的攻击方式. 在这种攻击方式中，当恶意攻击节点优先于诚实节点挖出区块时，恶意节点不选择立即将挖掘到的区块广播到区块链网络中. 当诚实节点在原有链上挖到新的区块时，恶意节点突然释放之前所保留的区块，增加链的长度，使得区块链网络出现分叉，根据最长链原则，诚实节点挖出的区块无效，即浪费了大量的算力资源. 同时，由于自私链成为了最长链，诚实节点最终也会趋向于在自私链上进行挖矿，严重破坏了区块链系统原有结构.

文章中将自私挖矿的运转流程抽象为状态机，如图 31 所示. 在这个状态机中，每一个状态对应为恶意节点领先的区块数目. “0”领先状态较为特殊，被拆成状态 0 和状态 0′. 0 状态表明只有一个公共链，而 0′状态表明诚实链与自私链长度相同，系统中主链发生分叉. 状态的转移则取决于恶意节点和诚实节点的算力大小，其中 α 与 $1-\alpha$ 分别表示恶意节点和诚实节点的算力比例，γ 表示诚实矿工在自私链上挖矿的比例. 状态 0 时，系统中只有一条公共链，如果算力为 α 的恶意矿工挖出区块，则系统状态变为 1 状态(此时，恶意矿工并不释放自己区块). 如果 1 状态时，诚实矿工节点以算力 $1-\alpha$ 挖出区块，系统转为 0′状态，恶意节点释放之前保留的区块，自私链与诚实链等长，系统出现分叉. 分叉后，系统中节点挖矿的情况将会分为三类，恶意节点在自私链上以算力 α 挖矿，γ 比例的诚实节点在自私链上以算力 $1-\alpha$ 挖矿，$1-\gamma$ 比例的诚实节点以算力 $1-\alpha$ 在诚实链上挖矿. 这三种情况都会消除系统的分叉状态，使得系统变为 0 状态. 其他状态转移类似.

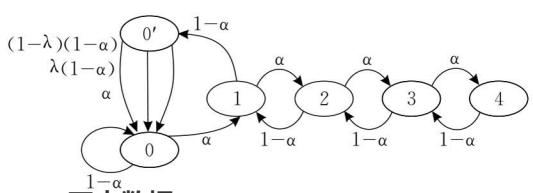

图 31　自私挖矿运转流程图

下述公式中，α 表示恶意节点拥有的算力，γ 表示诚实矿工在自私区块基础上挖矿的比例，p 表示不同状态的概率，R 表示收益.

式(12)表明了每个状态出现的概率，见式(12)：

$$\begin{cases} \alpha p_0=(1-\alpha)p_1+(1-\alpha)p_2 \\ p_{0'}=(1-\alpha)p_1 \\ \alpha p_1=(1-\alpha)p_2 \\ \forall k\geq 2:\alpha p_k=(1-\alpha)p_{k+1} \\ \sum\limits_{k=0}^{\infty}p_k+p_{0'}=1 \end{cases} \tag{12}$$

解方程组得不同状态下的概率，见式(13)～式(16)：

$$p_0=\frac{\alpha-2\alpha^2}{\alpha(2\alpha^3-4\alpha^2+1)} \tag{13}$$

$$p_{0'}=\frac{(1-\alpha)(\alpha-2\alpha^2)}{2\alpha^3-4\alpha^2+1} \tag{14}$$

$$p_1=\frac{\alpha-2\alpha^2}{2\alpha^3-4\alpha^2+1} \tag{15}$$

$$\forall k\geq 2:p_k=\left(\frac{\alpha}{1-\alpha}\right)^{k-1}\frac{\alpha-2\alpha^2}{2\alpha^3-4\alpha^2+1} \tag{16}$$

根据所求概率可计算按此策略自私矿池的收益比例，见式(17)：

$$R_{\text{pool}}=\frac{r_{\text{pool}}}{r_{\text{pool}}+r_{\text{others}}}=\cdots=\frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+(2-\alpha)\alpha)} \tag{17}$$

根据式(17)，可得自私矿池获得大于其付出算力应得收益时 α 的取值范围，见式(18)：

$$\frac{1-\gamma}{3-2\gamma}<\alpha<\frac{1}{2} \tag{18}$$

针对这种攻击方式也有很多论文做了后续补充和优化. Sapirshtein 等人[80]扩展了上述研究成果. 这篇文章在对于自私攻击模型进行一定程度的优化后，发现其盈利攻击所需的最小资源阈值严格低于原方案. 此外，本篇文章深入了解了通信延迟存在的自私挖矿形式，在这种情况下，原先模型的利润阈值不再存在，微小算力矿工甚至也可以进行自私攻击.

在文章中，对于矿工可获得的相对收益 REV 进行了建模，具体内容见式(19). 矿工收益阈值空间见式(20). 式中 π 表示矿工所采用的策略，r 表示矿工的收益，t 表示时间.

$$REV:=E\left[\liminf_{T\to\infty}\frac{\sum\limits_{1}^{T}r_t^1(\pi)}{\sum\limits_{t=1}^{T}(r_t^1(\pi)+r_t^2(\pi))}\right] \tag{19}$$

万方数据

$$\hat{\alpha}(\gamma):=\inf\{\exists\pi\in A\,|\,REV(\pi,\alpha,\gamma)>REV(honest,mining,\alpha,\gamma)\}\quad(20)$$

4.2.3 扣块攻击

扣块攻击最初在 2011 年由 Rosenfeld[81] 提出. 矿池是多矿工共同进行挖矿的一种形式,矿池根据每个矿工付出的计算能力,来按比例分配矿池的挖矿奖励. 扣块攻击的主要思想为加入矿池的恶意节点不发布其成功挖出的区块,但是却共享同一矿池中其他矿工挖出区块的奖励,从而减少了矿池的预期收益. 在这种攻击方式中,虽然恶意矿工不会得到任何额外的收益,但是可以破坏矿池的收益.

Courtois 等人[82] 描述了一种改进的扣块攻击方式,他们改进了文献[7]的破坏攻击,并表明恶意矿工有可能从这样的攻击中获利,与最初的攻击方式不同的是,这篇文章描述了一个具体的实例和一个具体的扣块攻击数值的例子,并分析了可能的变体. 在这篇文章中,用 α 表示恶意矿工算力占比,其中 $\alpha=0.2$,并设定 $\alpha/2$ 的矿工渗透入普通矿池进行作恶. 参加攻击的恶意节点,分享矿池的奖励,但是当恶意矿工挖到区块时,不向矿池进行报告. 对于被恶意矿工渗透的矿池,所有矿工的货币收益将均匀减少为原来应用奖励的 $(1-\alpha)/(1-\alpha/2)=80/90=0.88$. 对于没有参加矿池的 $\alpha/2$ 的恶意矿工,由于其没有参与贡献,其得到的奖励占比高于不进行攻击时获得的 $1-(1-\alpha/2)/(1-\alpha)=13\%$. 总体来说,恶意矿工得到的奖励占比要更大,其中有大约 6%是为了让恶意矿工收益,这是因为他们只有一半的挖矿能力从 13%的高比例奖励中收益,更一般的收益计算,见式(21):

$$\frac{1}{2}\frac{1-\alpha/2}{1-\alpha}+\frac{1}{2}-1=\frac{\alpha}{4(1-\alpha)}\quad(21)$$

此外,也有一些针对不同场景的扣块攻击相关分析工作. Tosh 等人[83] 将区块链应用于云计算环境中,为云计算环境提供不可篡改的证明. 这篇文章在云计算背景下,提出了区块链云中的扣块攻击模式,分别考虑了不同的矿池奖励,针对在矿池挖矿过程中可能发生的扣块攻击问题进行阐述,识别可能的破坏矿池挖矿攻击者所需的哈希能力约束条件.

4.2.4 Eclipse 攻击

Singh[84] 最初提出了 Eclipse 攻击. Eclipse 攻击的核心思想为对于被攻击者的路由表进行攻击,通常通过 Sybil 恶意节点建立虚假身份,使得被攻击者的路由表中大多数为虚假节点. 受到 Eclipse 攻击的节点,被隔离到了正常的区块链网络之外. 而该文中提出的防御方案基于强制节点度限制,要求每个参与节点携带相关证书,并绑定公钥以证明身份. 显然,这种解决方案对区块链网络并不现实. 在 Eclipse 攻击发起时,攻击者使用虚假节点的连接尝试向区块链网络中的某个正常节点不断发送来更新路由表消息. 以这种方法,被攻击节点的路由表中会充满虚假节点的连接建立,进而会影响自己的正常网络通信行为,包括路由查找或资源搜索等[85].

Heilman 等人[85] 详细地分析了在比特币网络中进行 Eclipse 攻击的情况. 在 Eclipse 攻击中,一旦攻击成功,攻击者即可使用远远低于 51%的全网算力来执行 51%攻击. 文章用两个具体方案对于攻击过程进行说明,分别为用低于 51%算力的攻击者攻击和不包含任何算力的攻击者攻击. 在前者中,假设攻击者可以将比特币网络划分为两个部分,第一部分占网络中总体算力的 30%,第二部分占网络中总体算力的 30%,攻击者拥有整体算力的 40%. 攻击者让诚实的两部分矿工不能互相通信,这样攻击者相当于在第一部分和第二部分中分别建立了一个比特币网络,并且在前后两部分中分别拥有 $4/7>50\%$ 的算力. 在这种方案中,攻击者只拥有全网 40%的算力,但是在前后两部分子网络中都用于 50%以上的算力,实现了 51%攻击. 在第二个方案中,假设攻击者可以将区块链网络分为两部分,左侧部分拥有 30%的算力,右侧节点拥有 70%的算力. 攻击者要与某个商人进行数字货币交易,该商人的节点位于左侧部分. 攻击者在左侧子网中向商人发起一个 COIN_0 的交易,而在右侧子网中发起一个 COIN_0 到自身的双花交易. 由于两个部分的区块链网络被阻断,在左右两个子网中的交易都会被最终认可并被打包到区块中. 在左侧网络中的商人,看到转账交易被打包成区块后,认为已经安全,并把商品交给了攻击者. 之后,当两部分的网络恢复通信时,由于右侧网络拥有更多的算力,会生成更长的链,根据最长链原则,左侧网络中新产生的区块被废除,COIN_0 发送给商人的交易也被废除,双花攻击成功.

在文章中,Eclipse 攻击使用“tried”和“new”两个表完成篡改路由的记录,“tried”中记录未经确认请求的 IP 地址,“new”中记录攻击者重写的垃圾地址. “tried”表中假设比例 f 的节点与恶意节点相连,每一轮的攻击时长为 τ_a. 在该假设下,攻击者攻击成功概率见式(22),文章在最后提供了基于 botnet 架构的破解方案.

万方数据

$$q(f,f',\tau_a,\tau_l)=\sum_{r=1}^{\infty}p(r,\tau_a)\cdot f\prod_{i=1}^{r-1}g(i,f,f',\tau_a,\tau_l) \tag{22}$$

本篇文章的作者对于 Eclipse 攻击，也为比特币社区提供了相应的解决方案，其中包括“确定性随机驱逐”、“随机选择”、“更多的桶”等策略. 文章中作者在最糟糕的场景，及“tried”表中存储的均为诚实节点的场景中，部署了这些防御方案，结果发现事实攻击所需的 IP 地址数量从 4600 个提高至 41000 个，攻击成功的概率从 84%降低到 50%.

以太坊作为现代流行区块链系统，同样有可能受到 Eclipse 攻击的破坏，并且由于其允许单个节点在不消耗大量计算资源的情况下创建无上限的公钥地址，其更易受 Eclipse 的影响. 目前，已经有了对于以太坊上执行 Eclipse 攻击的相关研究. Karl 等人① 提出了三个影响以太坊区块链网络和客户端的漏洞，利用区块传播设计实现了 Eclipse 攻击，提出了一个漏洞来迫使一个节点接受比主链更长且总难度更低的链，且概述了以太坊在计算难度值上的一个缺陷. Marcus 等人[86] 提出了针对以太坊的 Eclipse 攻击，并仅仅使用两台主机实现了该攻击. 此外，本篇文章对于以太坊的 Eclipse 攻击漏洞进行了分析，并提出了相应的增强区块链网络抵御 Eclipse 攻击的对策.

4.2.5　其他攻击方式

在 Ghost 协议中，采用“最重子树原则”代替“最长链原则”来选择区块链系统的主链，使得区块链网络中的交易确认时间得到很大程度的提升. Natoli 等人[58,87] 提出了一种针对可分叉区块链系统(Ghost)的新型攻击方式——平衡攻击，此种攻击不以双花已确认的交易为目的，而是以阻止新的交易被确认为目的. 在平衡攻击中，攻击者暂时中断具有相似挖矿能力的子群之间的通信，在此期间，攻击者在一个子群中发送交易，并在另一个子群中挖矿，直到区块子群树的大小超过了交易子群树的大小. 在先前的比特币多种攻击方法中，攻击者必须拥有比诚实矿工更快的速度来获取最长链，平衡攻击的新颖之处在于其可以识别出具有同等挖矿能力的子群，并在他们之间延迟传递消息，而并非追求比诚实矿工更快地开采区块. 相比于平衡攻击，应用到以太坊中的 Eclipse 攻击可以只延迟商家和网络其他部分之间的消息. 然而，这种做法的难度很大. 一个比特币系统中的节点通常连接 8 个逻辑邻居，而以太坊节点通常连接 25 个节点，这使得问题变得更加困难.

Sybil 攻击[88] 是针对点对点网络提出的一种攻击方式，这种攻击方式的特点在于提出了直接身份验证和间接身份验证两种验证方式，破坏了分布式存储系统中的冗余机制，Sybil 攻击方式抽象模型如图 32.

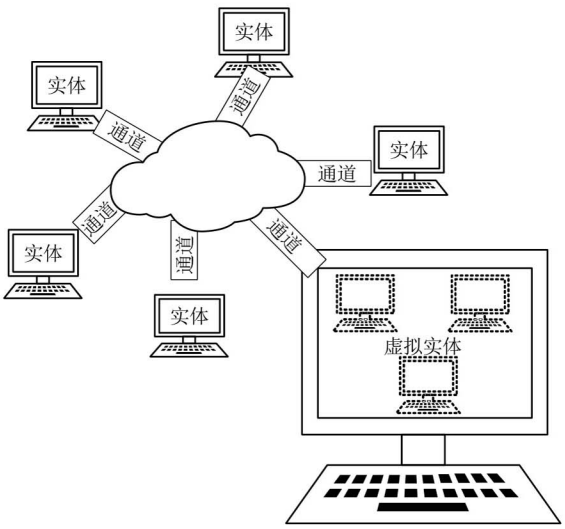

图 32　Sybil 攻击方式抽象模型

Syblil 攻击(女巫攻击)，是指一个恶意节点(Sybil 节点)在利用对等网络中的少数节点创建多个虚假身份. Sybil 攻击可以通过直接通信、间接通信、伪造身份、盗用身份、同时攻击、非同时攻击等不同类型的方式来实现攻击. 在区块链网络中，由于无需验证加入网络节点的身份，因此 Sybil 攻击的攻击者往往利用这一点来发起攻击，首先伪造多个虚假身份并一同加入区块链网络，之后开始向区块链网络中的正常节点发送大量虚假节点信息来控制正常节点的路由表，从而降低区块链网络的节点查询效率，屏蔽正常节点和区块链网络中其他节点的联系. Sybil 攻击的攻击者也可以在网络中传输非授权文件，破坏网络中文件共享安全，消耗节点间的连接资源等，而发起攻击节点本身不受影响.

DDOS 攻击是第三种常见的网络攻击，其攻击方式在于搭建攻击平台并发起大规模攻击. 但是 DDOS 攻击对于中心化服务非常有效，而对于区块链这种分布式系统，其攻击效果被大幅削弱. 由于网络中节点数目多，获取所有节点控制权的代价过高，得不偿失. 因此区块链技术也被应用于抵抗 DDOS 攻击.

重放攻击(Replay Attacks)是指攻击者拦截目

① Ethereum eclipse attacks. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/121310/eth-49728-01.pdf

万方数据

的主机已经接收并确认的数据包，并重复使用这个数据包发送给目的主机，虽然攻击者不能知道已经加密的数据包内容，但是可以对于目的主机进行欺骗来达到攻击的目的. 在区块链系统代码发生改变或者协议升级之后，系统中会出现硬分叉的情况，硬分叉的两条链，拥有共同的公钥和私钥产生算法以及相同的交易格式. 重放攻击基于上述背景发起，使用一条链上的合法交易向另一条链进行发送，导致在两条链上有相同的两笔交易. 因此在硬分叉前，需要做好重放保护，即发生在一条链上的交易，在另一条分叉链上重放就会失效.

Kroll 等人[57]提出了一种想要摧毁比特币的攻击方式，而不仅仅是想利用攻击获取利益的攻击方式，也被称为金手指攻击. 此外，通过分析交易图表发现了一些“匿名化”攻击.

4.3 区块链拓展架构

4.3.1 单链拓展

由于比特币系统并非对于所有类型的交易都适用，因此由比特币衍生出来的区块链有时需要对功能进行拓展，甚至改变架构. 其拓展方式有两种：一种是以比特币区块链为核心，对于一些特殊类型（不适用于区块链的）的交易则由其它支付中心处理或在线下执行，这种方式叫做链下拓展（off-chain scaling）；另一种是提升区块链本身的性能使其有能力处理所有类型的交易，这种方式叫做链上拓展（on-chain scaling）.

4.3.1.1 链上拓展

（1）属性优化

随着实际应用场景中区块链规模的不断增加，其拓展性越来越受到人们的关注. 区块链的可拓展性可以通过两个标准来衡量：事务吞吐量 transaction throughput（区块链能处理事务的最大效率）和延迟 latency（确认一个事务已经包含在区块链上的时间）. 目前，区块链在吞吐量和延迟上出现瓶颈的重要因素就是块大小、出块间隔（inter-block interval）[89]. 显然，想要提高区块链的可拓展性，最直接的方式就是从这两个因素入手.

基于比特币的区块链其最高交易吞吐量被有效地限制在块容量的最大值除以块间隔这个值上. 原有比特币机制中，每 10 min 产生一个区块，每个区块的容量是 1 M，这样计算下来吞吐量的理论值是每秒 7 笔交易. 这个值是远远不能满足现在的经济对电子货币的需求的. 为了提高比特币的拓展性，Bitcoin Improvement Proposals（BIPs）100①，101②，102③ 和 103④ 中都涉及到了对块大小和块间隔的重新参数化. BIP 101 建议用一个随着时间以可预测的速度增长的最大块容量替换固定的 1 MB 的最大块容量. BIP 102 一次性地将一个块中允许的事务数据总量从 1 MB 增加到 2 MB. 这些工作主要在变更块大小的时机、策略（无变更、线性、重复加倍、可选的缩减）以及触发变更的矿商持股比例上进行相应的调整.

除针对 bitcoin 中区块链的属性做出更改提高其可拓展性，有部分研究人员也试图在一般区块链上做出优化. Dennis 等人[90]从资源的有限性角度考虑如何解决当前区块链规模指数增长的问题，进而提出了一种时间“滚动”区块链. 这种策略使得区块链的规模维持在一个恒定的大小，从而不会让区块链的拓展性受到资源容量的限制.

（2）范式优化

虽然对区块链属性的调整可以在一定程度上改善性能，但想要大幅度提高区块链的可拓展性则需要重新设计区块链范式（这里的范式指节点间达成共识的不同方法）. 如图 33，区块链原有的共识范式是每选举出一个首领，达成共识后将一个块上链，这种方式严重限制了记账速度和拓展性. 从共识范式的角度看，Bano 等人[91]将链上拓展的方法分为以下几类：单首领多块范式（Multiple Blocks per Leader）、组合首领范式（Collective Leaders）、并行范式（Parallel Blockchain Extension）和分片交易范式（Sharding Transactions）.

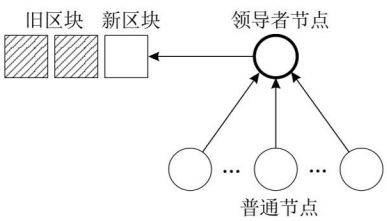

图 33 比特币区块链共识范式

（I）单首领多块范式（Multiple Blocks per Leader）

Bitcoin-NG[92]的信任模型与 Bitcoin 相同，区别在于它将领导人选举与事务串行化解耦. 简单来说，比特币原有的机制是选取一次领导人产生一个块，

① Making Decentralized Economic Policy. http://gtf.org/garzik/bitcoin/BIP100-blocksizechangeproposal.pdf

② Increase Maximum Block Size (BIP 101). https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki

③ Block Size Increase to 2 MB (BIP 102). https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki

④ Block Size Following Technological Growth (BIP 103). https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki

万方数据

现在 Bitcoin-NG 将时间划分为片段. 如图 34，每一个片段中，都有一个单独的首领来负责序列化状态机器转换，为了促进状态传输，首领会生成多个区块. 协议介绍了两种类型的区块：用于首领选择的关键区块和包含账本记录的微区块. 每一个区块都有一个数据头，该数据头包含上一个区块的唯一引用，也就是上一个数据头的密码学哈希值. 该协议的安全性来自激励参与者遵守规则的激励兼容性. 但是由于链结构的原因，Bitcoin-NG 的可伸缩性依赖于随着交易量的增加微块的大小要随之减小，否则就会导致其他矿工交易量不足. 当然，微块太小也是不切实际的(目前公开的 Bitcoin-NG 的交易量可扩展为 Bitcoin 的 5 倍).

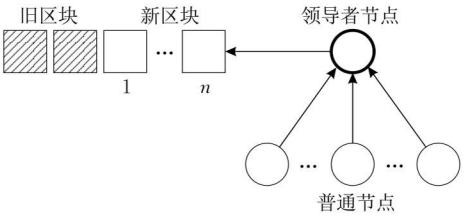

图 34　单首领多块共识范式

(II) 组合首领范式(Collective Leaders)

为了防止 Bitcoin-NG 中领导者在任期间出现恶意重写历史或重复支付的行为，ByzCoin[93] 更改了其生成关键块的方式：将原来只有一个领导者修改为一组领导者共同决定是否将某个块上链，如图 35. 领导小组是根据矿工的状态动态更新的，其投票权与其挖矿数量成正比. 在这样的机制下，拜占庭链能够确保每个微块都是不可逆地提交的，而且能够保证新的 leader 构建在最新的微块之上.

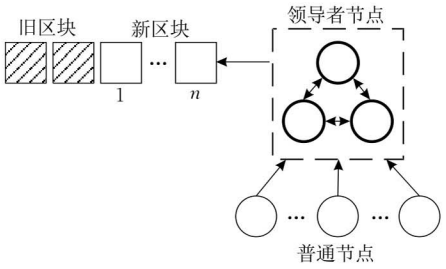

图 35　组合首领范式

(III) 并行范式(Parallel Blockchain Extension and DAG)

对于传统区块链来说，其线性验证和赢家通吃的特性导致了不可压缩的延迟. Boyen 等人[94] 打破了这种传统，他们完全放弃了“区块”和“链”的概念，基于交叉验证交易图构建了一个真正的分布式分类账系统. 在该系统中，每个事务包含一些负载(如加密货币)和有效工作量证明，并需要验证两个父事务. 在这种图结构下，不同的矿工可以并行地拓展交易图的不同分支，如图 36. 虽然这种协议不是基于领导选举，但也不是绝对公平的，因为网络延迟会导致诚实节点之间的冲突而使部分节点无法获得收益.

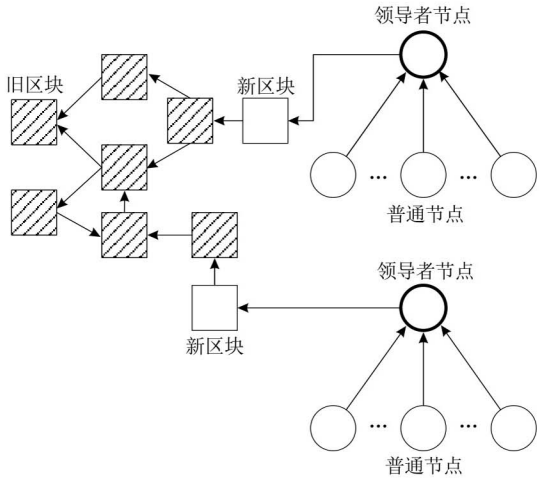

图 36　并行范式

(IV) 分片交易范式(Sharding Transactions)

分片技术来源于数据库领域，它将大型数据库分成更小的部分以便于管理数据. 在区块链的情景中，网络上的交易按照一定的策略分成若干个碎片，这些碎片被划分给小组独立处理. 这里的小组是由网络中的节点按照指定策略划分的，每个小组内部执行一致性协议，其数量随着网络节点的增加而线性增长，如图 37. 由此可见分片技术可以实现区块链水平扩容，这也是引入该技术的最主要原因. 围绕分片技术展开的研究有很多，它们在交易及小组划分策略、小组内部采用的一致性协议、使用场景等方面不尽相同.

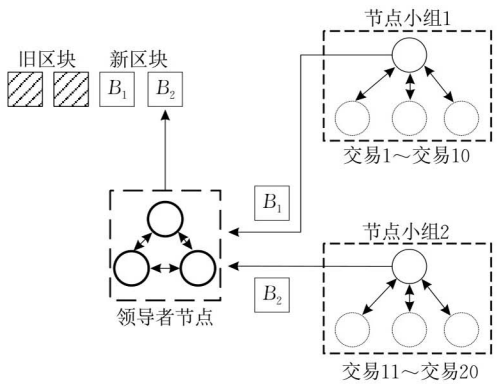

图 37　分片交易范式

PBF[51] 针对联盟链应用分片技术使其可以支持电子商务场景下的即时交易和海量数据，并保持

万方数据

较高的可信度. RSCoin[95]则是基于分片技术的一种加密货币框架. 它在传统的央行集中控制下引入分散的权威机构来监督其交易变动,提供了强大的透明度和可审核性保证. RSCoin 中的每个小组内执行两阶段提交协议,但是这种工作模式不能容忍拜占庭式的错误,还可能会遭到双花攻击. 后续有很多研究对此进行了改进.

ELASTICO[96]是针对开放的公有链提出的一种协议,它可以让没有预先建立身份或是没有公钥的节点参与交易并实现交易吞吐量随节点数增加的线性拓展. 在 ELASTICO 协议中,上面提到的小组被定义成"committee",每个 committee 运行一个经典的拜占庭共识协议来并行地决定他们所商定的交易集,一个 leader shard 验证所有签名并创建一个全局块. 但 Elastico 也存在一些问题:首先,小组成员规模较小,在存在 1/4 的竞争对手时,每个块每个分片有 2.76%的失败率,这在 PoW 系统中是不够安全的;其次分片策略具有一定的倾向性(bias-resistant),且不能确保分片时的交易原子性;最后就是验证器在分片中间不断切换导致必须存储全局状态,从而导致性能下降,以及交易确认的延迟与 Bitcoin 持平,这都导致其实用性大大降低.

针对上述这些问题,Kokoris-Kogias 等人[97]提出了 OmniLedger,它使用抗偏倚的公共随机性协议来选择大规模的具有代表性的小组来处理交易,同时引入了高效的交叉切分提交协议来处理跨多个分片的交易以保证其原子性. 除此之外,OmniLedger 还优化了小组内部的交易并行处理,实现了低延迟的交易验证及通过集体签名状态块来对账本进行剪枝. 实验结果表明 OmniLedger 可以实现吞吐量的线性拓展并支撑 Visa 级的负载,性能有了很大提高.

从上述这些研究中不难发现,现有的基于分片的区块链协议其通信量仍然与参与者数量呈现线性关系,而且它们或者具有较小的故障恢复能力,或者具有较高的故障概率,总之其拓展性和安全性都有待提高. 在这样的背景下,RapidChain[98]出现了,它使得区块链的拜占庭错误容错率达到了 1/3,是第一个不需任何可信设置即可对交易的通信、计算和存储开销进行完全切分的针对公有链的协议. RapidChain 对小组内部的一致性算法、组间路由、跨片交易等部分都进行了优化,从而使吞吐量达到了 7300 tx/s,将交易确认延迟降低到了 8.7 s,系统故障时间延长到了 4500 年(overwhelming time-to-failure).

万方数据

4.3.1.2 链下拓展

链下拓展的主要思路就是取长补短,区块链的吞吐量有限,那么我们就可以试图将交易记账的操作转移,从而减少区块链记账的压力. 减少区块链链上交易数有两种方式:一种是离线交易;一种是合并交易后上链. 下面分别阐述这两种交易方式的原理及相关研究.

离线交易简单来说就是想要交易的两个人没有在公链上记录下一笔交易而是私下向对方提供私钥. 这种方式可以很大程度降低交易记账成本,并可以大幅提高单位时间内交易数量. 但为了防止提供私钥的人保留私钥副本,这种 offchain 的方式就需要建立在双方有一定程度的信任的前提下.

目前基于离线交易思路而开发的平台中最著名的就是 NEM 了,它是一个可以定制化使用区块链的智能资产系统. NEM 智能资产系统由四部分组成:地址"容器"、"固定的"马赛克、个性化的命名空间和交易. 在区块链中,NEM 地址是资产的容器,通过"多重签名"控制可以实现在链上多方之间以各种方式共享地址资产的所有权. 马赛克是存储在 NEM 块上的固定资产. 用户可以通过命名空间在 NEM 块上为自己的业务或资产创建唯一标识,而交易的形式则可以是地址间马赛克的传输或者地址所有权的传输和配置. 这里的转换地址所有权的概念其实就是离线交易的另一种形式,可以极大程度上提高区块链的灵活性和拓展性.

合并交易后上链则更好理解一些,就是将一些规模比较小的交易在主链外合并后再记录到区块链上. 这种想法最早可追溯到 20 世纪 90 年代,为了降低交易记录的成本,Wheeler 和 Rivest 提出了概率支付概念. 概率支付后来演变为微支付通道,用于现在的电子支付场景. Pass 等人[99]提出了一种基于彩票的微支付方案,可以在不改变现有基础设施的情况下用于任何基于账本的交易系统,实现每秒处理数千个支付请求的性能.

有了上述对于微支付通道的研究基础,当比特币遇到拓展性问题时自然会有相应的研究,其中最具代表性的就是闪电网络①. 闪电网络由两种类型的交易合约组成:序列到期可撤销合约(RSMC)和哈希时间锁定合约(HTLC),前者解决了通道中比

① The bitcoin lightning network: Scalable off-chain instant payments. https://www.bitcoinlightning.com/wp content/uploads/2018/03/lightning-network-paper.pdf

特币单向流动问题，后者解决了跨节点传递问题. 这两种协议都依赖于微支付通道来进行交易，使得网络价值的转移发生在链外，再配合其它技术的应用使得无需信任对方或第三方即可进行实时、海量的交易成为现实.

基于比特币闪电网络的思路，以太坊也提出了自己的链下微支付通道解决方案：雷电网络(Raiden Network). 用户可以在链下发送任意数量的交易，而在链上只需要锁定通道金额和关闭通道两个操作就可以达成链上交易金额转移，进而结算完成. 这种将交易和智能合约的执行放在链下执行只在必要时候才公开上链的想法给区块链带来了吞吐量、确认时延、隐私保护等多方面的提升.

但是现有的支付通道也存在一些缺陷，一个支付通道开启后就无法在不执行链上交易的情况下退还. 当用户之间的总交易值大于支付通道容量时，就必须退还该通道重新申请，这就至少会产生两次链上交易，从而产生多余的资源消耗. 为了解决这一问题，Khalil 等人[100]提出了 REVIVE，它允许网络中的任意一组用户根据所有者的实际需求在支付通道之间安全的转移余额. 但是由于存款的总金额一定，所以该方法的平衡调整也有一定的限制.

当然，微支付通道的想法也被应用到其它电子货币上，Bolt[101]就是部署到货币 ZCash 上的一种轻量级匿名支付通道技术. 该技术支持安全的、即时的和隐私支付进而减少网络的存储负担.

4.3.2　跨链拓展

随着区块链技术的不断成熟，其优势不断显现，这就促使越来越多的行业开始着手应用这一热门的技术. 但是目前成熟的区块链社区往往都是针对一个特定的行业，而类比于现实生活，不同行业之间一般都存在着频繁的沟通与交流，这就给区块链的互通性带来了挑战. 在此背景之下，跨链技术就成为了区块链向外拓展和连接的重要桥梁.

目前跨链技术的应用场景可以概括为五个方面：(1)资产(原子)交易；(2)资产跨链转移和使用；(3)跨链数据预言机；(4)资产留置或抵押；(5)通用跨链合约①. 在如此多样的应用需求驱动之下，不同的跨链技术应运而生，且在不断推陈出新. 现在主流的跨链技术已经从原来的三种(公证人机制、侧链/中继、哈希锁定)拓展为五种，新增了分布式私钥控制和混合技术(公证人＋侧链)两种类型.

公证人机制的原理是在两个互不信任的链之间引入第三方中介来传递消息，在不同账本之间完成跨链交易的转换状态过程如图 38. 这种机制虽然简单合理，但是与区块链本身去中心化的理念相互矛盾，大多出现在跨链技术的早期. 代表项目有瑞波 Interledger 协议②和 Corda③.

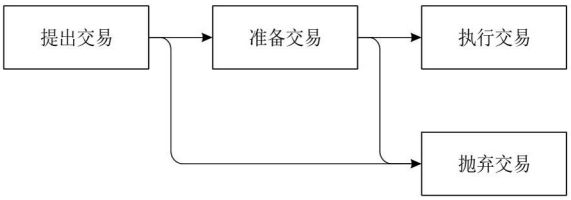

图 38　跨链交易状态转换过程

侧链机制最早由 Blockstream 公司于 2014 年提出④，侧链技术流程如图 39，它通过在侧链与主链之间建立双向挂钩(Two-way peg)并结合简单支付验证(SPV)来实现资产(或比特币)在侧链上的流通，同时保证主链上是冻结状态. 这就可以将一些定制化或是高频交易转移到链外执行，从而拓展比特币的底层协议，衍生出了商业化应用 Liquid⑤. 后来 Blockstream 又于 2017 年提出了联合挂钩(Federated Pegs)[102]来促进资产的去中心化跨链流动，有效减少了交易延迟并降低了对市场参与者的资金需求，增强了 Liquid 在金融市场上的应用可靠性. 中继链技术其实本质上也可以归结为侧链，最

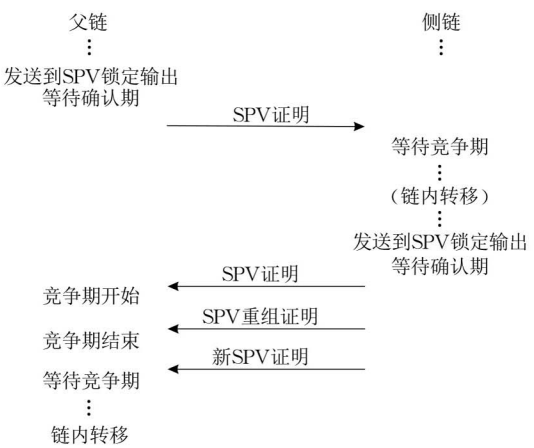

图 39　侧链技术流程示意图

① Buterin V. Chain interoperability. R3 Research Paper, 2016. https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf

② Thomas S, Schwartz E. A Protocol for Interledger. Paymentshttps://interledger.org/interledger.pdf

③ Brown R G, Carlyle J, Grigg I, et al. Corda: an introduction. https://docs.corda.net/releases/release-M7.0/_static/corda-introductory-whitepaper.pdf

④ Back A, Corallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains. http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains

⑤ Liquid. https://www.liquid.com/

万方数据

具代表性的应用就是 Polkadot[①]. 它将原有链上的 token 转入类似多重签名控制的原链地址中对其进行暂时锁定,在中继链上的交易结果则由这些签名人投票决定其是否生效.

一般来说,侧链和中继链并不做明显的区分,这一类技术的原理相通,实现难度高,但可以完成资产的跨链转移、交换与抵押等任务. 与这两项技术相关的应用还有 RootStock[②],Cosmos[③],BTC Relays[④],Aergo[⑤] 和 Bumo[⑥].

哈希锁定技术起源于比特币闪电网络的 HTLC (Hashed TimeLock Contract)[⑦],其初衷是让比特币通过微通道技术达到小额快速支付的效果,后来这一技术被拓展用于跨链. 哈希锁定是通过锁定一段时间猜 *hash* 原值来兑换支付的一种机制. 交易双方 AB 将资产锁定到智能合约中,其中 A 计算一个随机数的 *hash* 值发送给 B,若 B 在规定的时间内能提供该随机数的值则可以拿走被 A 锁定的资产,反之亦然. 若在规定时间 B 不能提供正确的密钥值,则资产将退回给 A. 哈希锁定的好处在于可以在彼此不信任的前提下实现跨链资产交换,但是却没有真正做到资产的跨链转移.

分布式私钥技术应用于跨链的实现原理是将私密资产通过分布式私钥生成与控制技术映射到基于协议的内置资产模板区块链上,然后根据跨链交易信息部署新的智能合约来创建新的资产. 分布式私钥就是将私钥经过密码学算法分到 n 个节点控制,只有集齐其中 k 个节点的私钥分片,才能恢复完整私钥,解锁账户. 这使得用户始终对自己的资产有控制权,但私钥的生成和分片工作也需要一个强信任的中心来完成,这一点上还有待优化. 目前采用这种技术实现跨链交易的代表项目有:Wanchain[⑧] 和 Fusion[⑨].

除了上述 4 个主流的跨链技术外,也有人创新性的将侧链和公证人机制进行融合,以达到灵活性和可信任性的双赢,最具代表性的就是 Ether Universe(基于第三代区块链平台 EOS. IO[⑩] 构建的跨链服务平台). 它通过第三方"连接器"和"验证器"连接以太坊网络、EOS 网络和其它网络,如图 40,其中"连接器"由分布式节点充当,不需额外的信任机制,而"验证器"通过加密算法运行,不会直接看到交易的详情. 网络间的通信则采用侧链技术,生成逻辑子链来与其它主链进行双向锚定实现 ETU(Ether Universe 平台的 token)的通信. 这种混合技术在性能上有天然优势,交易速度可以达到 1 万笔/s,而且费用低廉,特别适合商业应用场景.

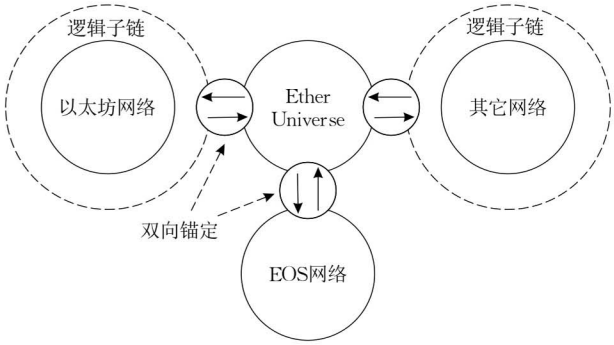

图 40 Ether Universe 技术原理图

5 区块链应用

本节介绍一些已经较为成熟的应用项目. 区块链最初是从比特币中提出的,随着比特币系统的稳定运行,越来越多的用户看到了其背后技术——区块链的潜在价值,并将区块链技术提炼并应用到不同的场景下. Swan 在《区块链:新经济蓝图》[103] 一书中将区块链的应用定义为三个层级,区块链 1.0~3.0. 区块链 1.0 对应的经济形态是以比特币为代表的虚拟货币,应用和货币相关,例如货币转移、汇兑和支付系统等. 区块链 2.0 对应的经济形态 Fusion 是智能合约主导的去中心化应用,其应用场景更加丰富,但仍偏向经济领域,涵盖例如股权、债券、信贷等场景. 区块链 3.0 将区块链应用的领域扩展到现实场景中,与物联网等其他技术相结合,覆盖人类社会生活的各个方面,在各类社会活动中实现信息的价值证明与保障,不再依靠某个第三方或机构获得信任或建立信用,实现信息的共享,例如医疗健康、知识产权、物联网、社会管理、慈善公益等.

5.1 区块链 1.0——数字货币

在区块链 1.0 时代,主要的应用对象为货币,实现的常用功能为货币转移、汇兑和支付等. 其系统架构可以抽象为图 41. 数据层、网络层、共识层都是

① Polkadot. https://polkadot.network/
② Rootstock. https://www.rsk.co/
③ Cosmos. https://cosmos.network/
④ Btc Relay. http://btcrelay.org/
⑤ Aergo. https://www.aergo.io/
⑥ Bumo. https://bumo.io/
⑦ The bitcoin lightning network: Scalable off-chain instant payments. https://www.bitcoinlightning.com/wp content/uploads/2018/03/lightning-network-paper.pdf
⑧ Wanchain. https://www.wanchain.org/zh/homepage/
⑨ Fusion. https://www.fusion.org/
⑩ Eosio. https://eos.io/

万方数据

区块链技术的基础结构，应用层的抽象表明用于表征货币转移的账户和交易. 下面将介绍几种常见的数字货币.

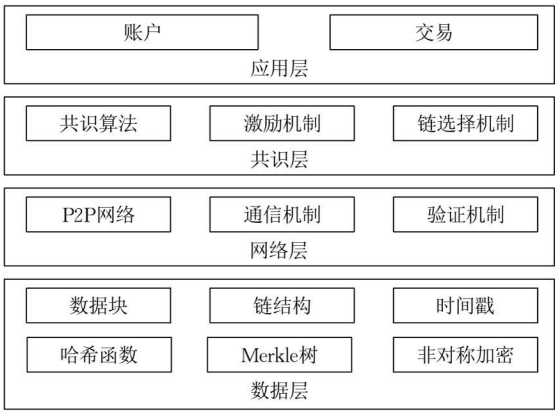

图 41　区块链 1.0 架构

比特币是最早实现去中心化的加密货币，在 2009 年作为开源软件发布. 它使用一种全新的分布式记账技术，使交易过程去中心化. 交易无需通过任何权利机构监督或服务器验证，而由网络中节点决定付款是否合理. 除了比特币平台自身，还可以基于比特币平台创建其他数字货币或应用. 可使用多种方法在区块链上创建代币，如直接在账本内部构建，或利用分叉母链创建新的代币.

2011 年，莱特币出现，是早期一种比特币替代币. 比特币挖矿需要越来越专业和昂贵的硬件，普通人挖矿变得越来越困难. 莱特币在技术原理上与比特币基本相同，但是一种更轻量的数字资产. 莱特币算法降低硬件成本，使得普通计算机能够参与挖矿.

瑞波币与比特币差异较大. 本质上瑞波网络是一种针对其他货币或其他价值体的全球性的结算网络，比如美元、欧元、英镑、比特币和飞行里程、商品等. 该系统试图实现一个灵活的货币流动体系，它的核心是债务关系. 瑞波网络担任中间转手人，帮助两个用户完成不同价值体的兑换. 用户只需和转手网络建立信任关系，用户间无需信任，能够提升兑换效率. 如果想要进行这样的结算，需要使用瑞波币(XRP)来付一定的手续费. 尽管瑞波币可以在加密货币市场上交易，但是瑞波币的根本作用是协助体系内货币流通.

达世币是一款支持即时交易，以保护用户隐私为目的数字货币，基于比特币开发. 达世币本质上是对比特币在两个主要领域做出改善：一个是交易速度，另一个是匿名性. 它通过匿名技术，使得交易无法被追踪查询. 达世币是基于比特币的，有独特的双层网络，既有“矿工”，又有“主节点”，帮助达世币拥有了更加全面和高级的功能. 达世币的即时支付技术可以让交易几乎在瞬间完成，并且通过币种混合技术来保证交易的私密性.

未来币是全新设计和开发的第二代去中心化虚拟货币. 未来币是第一个纯 POS 币，使用透明锻造的方式生产新区块. 未来币不再通过消耗大量的资源挖矿产生新货币，而是通过现有账户的余额去“锻造”区块，并给与成功“锻造”区块的账户交易费用奖励. 未来币目前支持资产交易、任意消息、去中心化域名、帐户租赁等多种功能. 它已经通过 IPO 的方式完成了所有币的分发. 表 5 对上述几种区块链加密货币系统进行对比.

表 5　5 种区块链加密货币对比

	比特币	以太币	莱特币	瑞波币	达世币	未来币
目的	去中心化货币系统	提供智能合约	改进比特币	货币清算	保护用户隐私	使用POS共识算法
发行方式	通过挖矿产生比特币	通过挖矿产生以太币	通过挖矿产生莱特币	预挖矿方式	通过挖矿产生达世币	IPO 方式
区块时间	10 min/块	15 s/块	2.5 min/块	5 s/块	2.5 min/块	60 s/块
总量	2100 万	无上限	8400 万	1000 亿	2200 万	10 亿
共识算法	POW	POW＋POS	POW	OpenCoin 原创算法	POW＋POS	POS
加密算法	SHA256	Ethhash	Script 加密算法	RTXP	X11 超级安全哈希运算	curve 25519
挖矿硬件	ASIC	GPU	GPU，ASIC	无	GPU，ASIC	无

5.2　区块链 2.0——智能合约

区块链构建了一个分布式的数据库，这个数据库的真实性由网络中的众多节点进行维护，每个节点对每条记录都有决定权. 如果记录的内容是各用户间来往的交易，则这个数据库就是一个账本，这就实现了比特币系统的功能. 如果记录内容为更复杂的约定或事件，则此数据库能发挥更大作用，帮助监督更复杂的逻辑实现. 在区块链中，该过程可以抽象为数据的可信记录和可信执行，其中可信的特性由共识机制保障. 在密码货币中，记录为链上的交易历史数据，执行过程为利用堆栈运行加解密脚本. 链上记录通常为固定格式，且可视为常量. 如果能够扩展

万方数据

上链数据(如代码)并允许更加复杂的执行操作(循环判断等),则区块链能够处理蕴含复杂逻辑的交易过程.如果将生活中的交易过程抽象建模,并以代码形式在区块链中记录、执行,可以实现诸如公证、产权证明等.

区块链 2.0 以以太坊为代表实现了更复杂的分布式合约记录——智能合约.合约记录在区块链中,一旦满足了合约的触发条件,预定义的代码逻辑能够自主执行,执行后的结果上链不可更改.早在 1994 年,密码学家 Szabo 就提出了"智能合约"的概念[104].理想状态下的智能合约,可看做一台图灵机,是一段能够按照事先的规则自动执行的程序,不受外界人为干预.但是智能合约的概念提出时缺少可信的执行环境,没有被纳入应用.区块链系统提供去中心化去信任的环境,使得智能合约的概念得以实现.各用户对规则协商一致后创建合约代码,并将该合约代码上链.一旦满足触发条件,合约代码将由矿工按照预设规则执行.区块链 2.0 系统架构可以抽象为图 42.

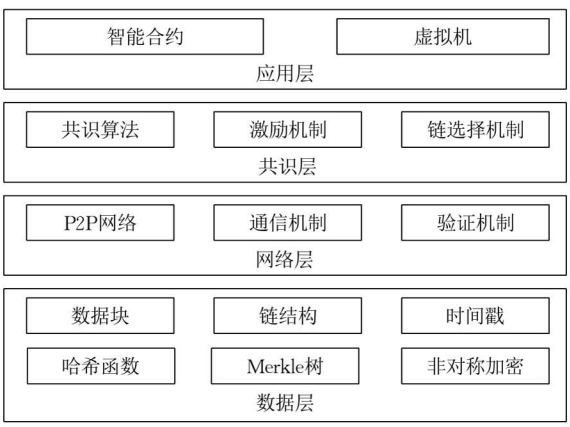

图 42 区块链 2.0 架构

智能合约使得受复杂条件限制的价值转移成为可能.多方用户参与智能合约创建后,将合约发布到区块链中,触发预设条件后,合约代码自动执行,并将执行后合约状态打包进区块,该过程如图 43 所示.触发条件形式上可以为用户发起一笔交易,传参调用合约中函数.矿工节点验证交易合理性,执行被调用函数,并将执行后合约状态打包进区块,各矿工节点经共识验证后各自上链.上述描述中的用户发起交易与合约代码自动执行并不矛盾,交易发起只是触发合约状态改变的一种形式,该交易也可由提供客观事实的机构发起,也可利用设置时间条件限制等因素.而自动执行重在强调执行过程发生的必然性,矿工根据调用执行链上的合约代码.由于链上数据公开且存储在分布式系统中,因此更改攻击少数矿工的执行并不会影响最终结果,这是由区块链的共识特性保障的.

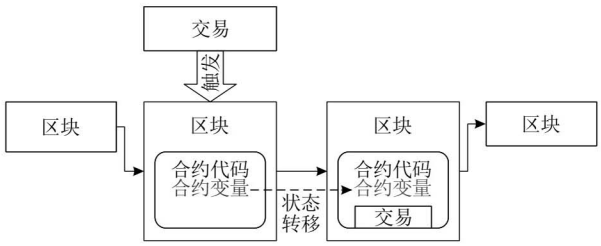

图 43 智能合约区块链架构

长铗等人[105]对智能合约运行机制定义如下:"基于区块链的智能合约包括事务处理和保存的机制,以及一个完备的状态机,用于接受和处理各种智能合约;并且事务的保存和状态处理都在区块链上完成.事务主要包含需要发送的数据;而事件则是对这些数据的描述信息.事务及事件信息传入智能合约后,合约资源集合中的资源状态会被更新,进而触发智能合约进行状态机判断.如果自动状态机中某个或某几个动作的触发条件满足,则由状态机根据预设信息选择合约动作自动执行".

智能合约系统依据事件描述信息中包含的触发条件判断,当触发条件满足时,从智能合约自动发出预设的数据资源,以及包括触发条件的事件;整个智能合约系统的核心就在于智能合约以事务和事件的方式经过智能合约模块的处理,执行后仍是一组事务和事件;智能合约只是一个事务处理模块和状态机构成的系统,它不产生智能合约,也不会修改智能合约;它的存在只是为了让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志,正确执行.

5.2.1 以太坊平台

目前,以太坊是一个较为成熟的智能合约平台,其核心改进是以太坊虚拟机(EVM),该虚拟机支持的语言图灵完备,因此能够执行复杂的控制逻辑.以太坊是以交易为基础的状态转移系统,而以太坊中的分布式账本除了要记录交易数据还要记录全局账户的总状态,其结构如图 44 所示.在以太坊中,有两种类型的账户,分别为外部账户和合约账户.外部账户与比特币系统中的账户概念相同,记录账户余额等信息,而合约账户主要用于记录合约代码.二者的结构相同,都包含四个字段,在使用过程中根据所用字段不同来进行区分,其结构如图 45 所示.两种账户的变化都需要通过交易触发,交易对外部账户的影响通常是账户余额的变化,而交易对合约账户的

万方数据

影响通常表现在代码执行. 无论哪种状态的变化，该过程都需要通过矿工挖矿来记录. 账户的变化只需要矿工对交易进行验证，而合约账户的变化也就是合约代码的运行则需要矿工节点在各自的以太坊虚拟机上运行来验证. 合约代码的运行需要花费一定代价，这样防止账户恶意消耗平台资源，一旦合约账户中资金不足矿工就停止代码执行.

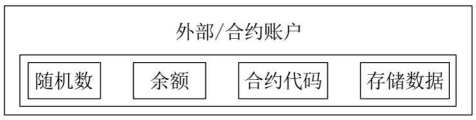

图 44　以太坊账户结构

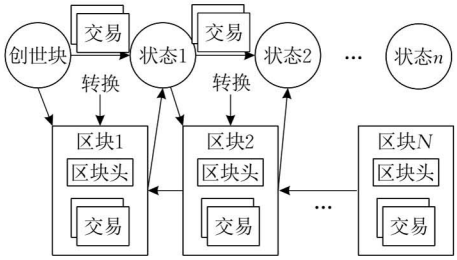

图 45　以太坊系统架构图

账本的维护靠区块链技术中的共识算法，在以太坊中对于交易和全局账户状态的记录需要系统中半数以上节点达成一致才有效. 以太坊目前使用的共识算法是 POW 与 POS 相结合，其资料显示后续将转换为 POS. 如果把区块链技术比作电脑硬件，以太坊则可以看做操作系统. 在以太坊平台上，用户无需关心底层区块链的实现细节，可以根据自己的需要设计合约，还可以开发去中心化应用.

5.2.2　HyperLedger 平台

以太坊是公有链中提供智能合约平台的代表，尽管相较比特币，以太坊的性能有了大幅提升，然而其安全问题、交易效率仍然需要经过更长时间的检验，因此，目前还不能满足商业应用的需求. 在此情境下，Hyperledger① 项目应运而生，旨在打造联盟链，建立关于区块链技术的开源规范和标准，为相互合作的企业构建一个透明、公开、去中心化的开发平台. 该项目的目标是发展一个跨行业的开放式标准以及开源代码开发库，允许企业创建自定义的分布式账本解决方案，以促进区块链技术在商业当中的应用.

Hyperledger 主要包括三大账本平台项目和若干其他项目. 三大账本平台项目主要有 Fabric、SawToothLake 和 Iroha. 整个社区主要是由技术委员会、管理董事会、Linux 基金会共同管理.

Fabric② 是三大项目中活跃度最高的项目，该项目实现了一个可插拔式模块化联盟链框架，该框架由三个核心组件构成，分别为身份认证服务、区块链账本服务和合约链码服务. 身份认证服务可提供对客户端以及矿工节点的认证；区块链账本服务主要为储存交易历史，账本、世界状态更新等服务；合约链码服务则是对账本服务的扩展，以容器方式运行复杂应用业务逻辑.

系统中 CA 用于验证多种身份，逻辑上可分为普通客户端、矿工节点. 其中矿工节点可细化为三类：背书节点、排序节点和确认节点. Fabric 中交易过程如图 46 所示：客户端向 CA 请求身份验证的签名；客户端用此签名向背书节点发送交易请求；背书节点验证交易的合法性并生成背书结果；客户端收集背书并验证数量及合法性；验证通过后将此交易发送给排序节点；排序节点根据交易次序构造区块，并发送到确认节点；确认节点对区块、交易、背书等内容进行验证，验证后记录上链并更新数据库中世界状态. 交易既可以为普通交易，也可以为合约调用（又为作链码调用），若为合约调用，则验证节点将验证该调用是否满足相应背书策略. 由于 Fabric 中节点身份已知，采用基于传统共识算法扩展的 Solo、Kafka 及 SBFT 三类算法实现共识，节点无需付出高昂算力竞争出块权，提升了系统的吞吐量，使得商用区块链成为可能.

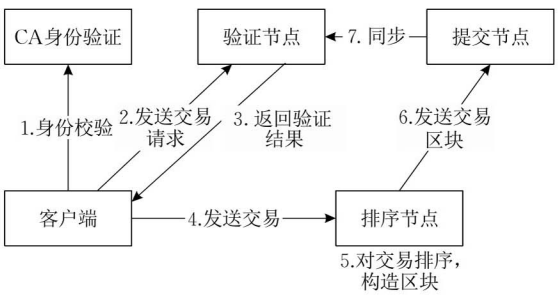

图 46　Fabric 交易流程

此外，Fabric 采用通道机制使得不同应用可根据需要各自生成链. 节点可参与到不同通道中，每个通道与绑定的配置及数据（包括交易、账本、链码和成员身份等）共同组成一条完整的链，见图 47. 图中节点 1，3 参与了通道 1，则二者将保存实线链；图中节点 1、2、3 参与了通道 2，则三者将保存虚线链. 通道之间数据相互隔离与保密，通道外成员无法访问.

① Hyperledger. https://www.hyperledger.org/
② Fabric. https://hyperledger-fabric.readthedocs.io/en/release-1.0/

万方数据

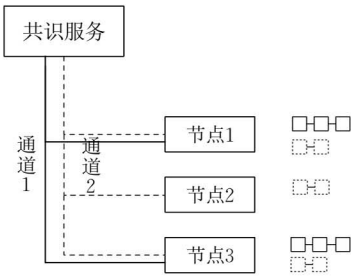

图 47 Fabric 通道机制

5.2.3 EOS

以太坊和 Hyperledger 平台都为探索区块链技术的应用场景提供一种解决思路，通过增加智能合约层允许更复杂条件的价值交换成为可能. 分析二者的设计架构可以看出，以太坊提供的平台适合运行简单逻辑的智能合约，无法支撑大量访问需求，且对发起合约方有较高编程能力的要求，其使用对普通用户并不友好. Hyperledger 作为联盟链，其对于复杂合约的支持能力也十分受限，其受众也更倾向于企业.

因此，EOS[①] 旨在创建一个区块链操作系统，作为底层架构向合约层提供服务，开发商可根据需要开发合约或更为复杂的去中心化应用(DAPP).

DAPP 可视为智能合约的扩展，与中心化应用 APP 相比，DAPP 将代码及应用运行过程中产生的用户数据上链，保障了程序的可信执行(与智能合约自动执行类似)和用户应用数据中蕴含的价值(可限制用户数据的访问权限). EOS 的设计也考虑了用户友好性. EOS 系统面向应用开发商，开发商可基于 EOS 底层链开发自己的上层应用，而具体运行过程对使用 DAPP 的用户透明.

EOS 具有提供帐户、身份验证、数据库、异步通信以及在数以百计的 CPU 或群集上的程序调度等特性. 其目标服务对象为应用开发商，网络中参与挖矿矿工的资源用于为应用开发商部署应用. 系统中代币为 EOS，应用开发商通过持有 EOS 访问对应比例的资源. 为了满足应用中必需的高吞吐访问，EOS 采用了 DPOS 的共识算法，通过见证人高效生成区块. EOS[②] 的架构如图 48，采用 C/S 架构，共有 4 个核心模块，分别为 cleos、keosd、nodeos 和 wallets 模块. Cleos 为客户端命令行工具，可与节点(nodeos)的 REST 接口通信，是用户或开发者与节点交互的工具. Keosd 为本地钱包管理工具. Nodeos 为节点进程，可根据需要配置插件. Wallets 为钱包模块.

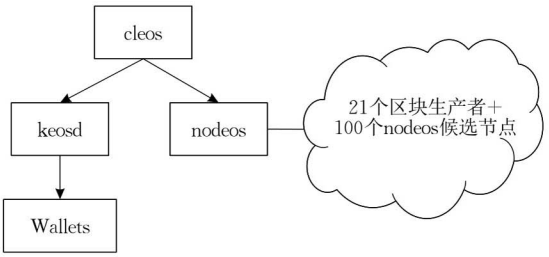

图 48 EOS 系统架构

EOS 系统的运转过程如图 49 所示. 客户端 cleos 创建合约并向节点 nodeos 申请部署；nodeos 将合约代码上链；cleos 调用合约中函数，cleos 将解析收到的数据并从相应合约地址中调取代码并执行；执行结束后将结果上链，并返回给客户端，客户端将结果返回给用户.

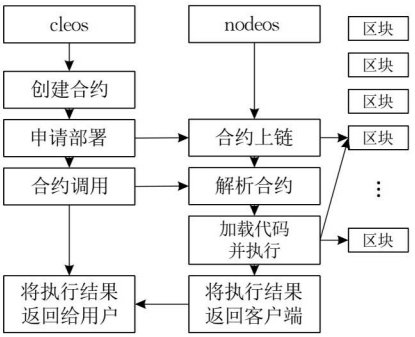

图 49 EOS 系统运转流程

5.3 区块链 3.0——扩展的发展领域

目前，区块链技术已经渗透到各行各业，不断有新的创新型应用问世. 这里我们选取了几个具有代表性的行业来说明人们是如何结合区块链的优势解决各自行业痛点的.

区块链技术源于比特币，那么就免不了与金融行业密切相关. 传统的支付系统起到的作用是安全的存储仓库和交换中心，而区块链的数字化安全反篡改特性可以在达到同等功效的同时省去大量中间成本. 换句话说，区块链技术可以创建更直接的支付流，可以在国内甚至跨国实现超低费率的瞬时支付. 鉴于这些优势，围绕交易与支付展开的研究层出不穷. Peters 等人[106] 分析区块链技术对银行业的冲击并讨论了在银行业中开发分布式账本需要考虑的关键性问题，而另一些人则“迫不及待”着手开发了不同场景下的金融交易或支付平台. 还有一些研究者做出了新的尝试，他们基于区块链技术建立自己的购物系统架构[107]、开发租用物品平台[108] 及采用电

① EOS. https://eos.io/
② EOS. https://developers.eos.io/eosio-home/docs

万方数据

子货币进行薪酬支付[109]，这些努力为区块链的未来发展提供了更加广阔的思路.

物联网是近年来广泛流行的学科，它可以理解为一种通过传感器等装置将物理世界的事物连接成可以相互通信的网络，其优势在于可以实现高力度的信息收集，目前被广泛应用于生活的各个领域.但随着人们对个人隐私的逐渐重视，初代物联网产品的安全性已无法满足要求.事实上，物联网的几大固有特性(缺乏中心控制、异构设备、多攻击面、风险上下文感知和庞大的规模)给其安全和隐私保障带来了巨大挑战.而区块链是由不可信的匿名节点组成的非中心化分布式网络，其特性刚好可以弥补物联网在安全方面的缺陷.将区块链用于物联网是一项极具吸引力的研究，但需要面临以下几个问题：(1)物联网设备资源受限影响采矿；(2)出块速度慢，无法满足物联网应用的低延迟需求；(3)区块链的拓展性无法适应逐渐增多的节点.此外，不同的物联网应用场景也有相应的特性，需要调整区块链的部分架构才能彼此契合.目前，应用到区块链的物联网领域主要有智能家居[110-111]、智慧交通及车辆互联、智能电网及资源分配、设备通信及维护[112-113]，当然也有将区块链用于构造物联网的网络安全模型及电子商务模型[114]的相关新兴研究.

众所周知，不可篡改和可追溯是区块链的重要特性，存有交易的区块在共识机制下按时间顺序加到链的尾部从而使修改区块数据成本极高甚至是不可能完成，进而保障链上数据可靠性，让攻击者“不可抵赖”.这种特性不仅可以用于传统的供应链溯源[115-116]，更使得个人数据也具有了产权属性，可以实现数字资产确权.在社交媒体领域，该特性可以用于追踪用户的声明及发言[117]，迅速追责，从而有效维护网络环境的安全有序.而在商业领域，区块链技术可以用于搭建商家信誉反馈系统[118-119]，从而保障消费者权益；也可以用于保险领域，有效避免欺诈骗险等不诚实行为，维护商家利益[120].除此之外，电子政务也和区块链有着密切关联.政府工作受公众监督，其政务信息[121]、贷款信息[122]、文献信息[123]等需要做到公开透明易维护，项目招标需要做到公平公正易实施.区块链技术可以在不受信任的竞标者之间形成信任共识，并可以通过合约保障项目进度，又可以向公众保证信息的透明性和不可更改性，有效促进政府透明化管理理念的落实.

如果说不可篡改和可追溯性保证了链上数据的安全可靠，那么匿名性则保护了链上节点的权益和用户的隐私.利用到区块链匿名性的应用领域主要是电子医疗和用户数据管理与隐私保护.在医疗领域，一方面患者对于病历记录的保密性要求较高，但不同医疗机构间的分散记录给其安全性和实用性带来了极大的困扰；另一方面，医院、科研单位及医疗企业间的数据共享有利于精确的诊断与治疗，甚至是降低医疗成本.电子医疗记录呈现出的这种矛盾在使用区块链技术后得到了有效缓解.因为区块链利用密码学里的一些技术(哈希运算、非对称加密、私钥、公钥等)使得在数据公开的前提下私人信息的安全得以保证，同样的原理还可以用于用户数据及权限的管理，从而提高数据交易的安全性.

物质世界中，我们有身份证、护照、驾驶证等可以证明身份的物品，但在互联网中，可以进行数字身份认证且安全可靠的平台却少之又少.原因在于数字身份无国界，我们很难找到一个跨全球范围的一致同意的监督实体[124].区块链技术则为这一问题提供了另一种思路，因为它不需要受信任的中央机构，从而绕开难点.目前已有部分研究和项目将这一思路落实，比较有代表性的是 ShoCard① 和 Uniquid②，前者为用户提供交易场景下保护隐私的数字身份，而后者则填补了实体与数字身份之间的鸿沟，允许对设备、服务及人员进行身份验证.与之类似的还有公钥基础设施(PKI)系统，区块链的非中心化不可篡改同样适用于这一场景.PKI 系统允许用户注册唯一的用户名和关联的公钥，并可以存储用户名的附加数据.这种公钥系统不需要任何中央机构或是受信任的一方就可以做到安全可靠的运行.

一般大公司的运行都离不开业务流程管理(BPM)，但在执行过程中不同参与者之间的信任缺乏阻碍了业务的统筹规划.区块链技术提供了一种不同参与者之间无信任也能可靠执行的流程管理方式，同时通过特定的共识算法和激励机制促进节点的进程，有效加快业务流程.此外，区块链的分布式特性还可以用于数据存储与计算平台的搭建.前者主要是利用去中心化特性免除中间商的代理，从而实现点对点的服务或设备资源租用以及数据的分布式(冗余)存储；后者则主要利用区块链的安全性来规避多方计算时数据所有者的隐私泄露问题.

经历了区块链 1.0 和 2.0，区块链技术的认可度越来越高，而且其自身属性与很多领域需要的解

① Shocard. https://shocard.com/
② Uniquid. https://uniquid.com/

万方数据

决方案契合，因此，区块链 3.0 也走入了我们视野中. 区块链的核心在于提供了一个安全、自建信任的数据库. 因此，针对不同领域的处理，实际是这个数据库应该如何设计、管理、维护的问题. 在表 6 中列举了不同领域中的应用实例，从各篇文章中，对于区块链的改造主要集中在账本和共识算法设计中. 账本的设计根据场景选择不同的数据结构. 而共识算法则可以根据场景选择有意义的代价作为建立信任的依据，无需一成不变地使用 POW 进行无意义计算，如在 Storj 系统中节点通过贡献存储资源作为证明，而节点贡献的存储资源解决了系统的存储需要，这样的设计能够与场景完美契合，是理想的设计思路. 表 6 中举例说明了在不同领域中是如何使用区块链技术解决行业痛点的.

表 6 区块链在不同领域的应用

领域	论文	概述	切入点
交易与支付	Peters 等人[106]	分析区块链颠覆银行业的潜力，讨论使用分类账技术需要考虑的若干关键问题	利用区块链的安全反篡改特性，省去传统支付或交易系统的中间成本，实现瞬时支付等功能
	Dilley 等人[102,125]	利用区块链技术记录金融交易流程的方法或平台	
	Cachin[126]	通过识别和实现跨行业的分布式账本开放标准平台，推进区块链技术的应用，从而改变全球业务交易的方式	
物联网	Dorri 等人[110-111]	搭建基于区块链技术的智能家居物联网架构，维护终端设备安全和用户的隐私权益	传统物联网架构由于缺乏中心控制、设备异构等因素导致安全性不足，而这些不足恰好与区块链的去中心化、匿名性等优势契合，两者可互补
	Sharma 等人[127-128]	将城市交通管理系统抽象为分布式网络架构进而与区块链相结合，实现交通运输管理	
	Dorri 等人[129]	将车辆自组网与区块链公钥基础设施相结合，保证车辆间通信的隐私安全	
	Christidis 等人[130]	在智能电网中建立电力交易模型，从而实现电力均衡；在物联网的设备之间建立服务市场，促进资源共享	
	Biswas 等人[112]	围绕物联网环境中的安全问题提出基于区块链的分布式物联网框架、通信框架或固件更新方案	
	Zhang 等人[114]	一个基于区块链技术的物联网电子商务模型	
电子政务与教育	Gerstl[122]	利用区块链记录政务信息、文献信息和贷款信息，从而实现公开透明	利用区块链的不可篡改特性来记录信息，保证其公平公正
	Sharples 等人[131]	结合区块链技术搭建教育信息存储及评估系统	
确权溯源与信誉防诈	Chakravorty 等人[117]	确认并追踪电子文档或媒体数据的所有权，利用区块链技术解决供应链溯源难题	共识机制等技术保证链上数据的高度可靠性，从而应用于对信誉或所有权要求较高的领域
	Carboni[118]	互联网环境中交易平台的分布式信誉反馈系统，依靠区块链的不可篡改性保证反馈信息的安全可靠，有效避免欺诈行为	
医疗	Mettler[132]	介绍区块链在医疗服务领域的影响，并从公共卫生管理、医药领域用户导向、医学研究、药品假冒四方面为例说明	区块链提供对数据权限的控制，量化数据信息的价值并保个人数据隐私安全
	Yue 等人[133]	构建了基于区块链技术的医疗数据网关架构，使患者能够安全管理个人健康护理数据	
	Azaria 等人[134]	构建基于区块链技术的电子病历管理系统，并借助该平台为第三方医疗利益相关者以矿工身份提供参与途径	
隐私数据管理	Fukumitsu 等人[135-136]	将用户个人数据加密拆分并存储到不同的节点，使得攻击者无法在线检测目标用户数据，让使用者拥有对自己数据的安全操控权	利用区块链中的密码学技术保证用户数据隐私与权益
	Xu 等人[137]	利用区块链特性对网络媒体产生的数字内容进行生产、版权、交易管理，有效维护用户权益	
密钥管理及身份验证	Matsumoto 等人[138-139]	利用区块链中自带的账本属性解决公钥基础设施中主要节点失效问题或设计基于区块链的 PKI 增强功能(IKP)	数字世界中身份及密钥管理
	Wilson 等人[140]	绕过数字身份认证需要全局一致信任监督实体的难点，利用去中心化匿名可信特性提供身份验证，保护隐私	
数据存储与计算	Wilkinson 等人[43,141-142]	免去代理商的中间成本，实现点对点的设备租用或数据存储	省去数据存储成本，加强数据计算的安全性
	Zyskind 等人[143]	针对传统计算平台多方计算时的隐私泄露问题，搭建基于区块链的安全计算平台	
	Leiding 等人[144]	实现透明、自我管理、分散的系统	
业务流程管理	Mendling 等人[145-146]	分析业务流程管理中区块链技术应用的可能性，确定区块链技术与业务流程管理生命周期上下文关联	流程数据透明化、公开化，提升数据处理效率
	García-Bañuelos 等人[147-148]	探究区块链技术在商品交易及云服务环境下的业务流程优化	

自比特币 2009 年上线运行，其成功背后也暴露出各种各样的问题，如安全隐私的保障、交易网络的吞吐量、账本的大小、共识算法的稳健性、高效性、在不同领域应用的扩展性.

目前区块链的发展已经有了长足进步，但现在对区块链的应用还远没有达到理想的规模. 究其原因，区块链饱受诟病的问题主要为：技术漏洞、交易吞吐量小、大量数据存储问题、隐私安全性、跨链协议、法律法规尚不规范等.

(1) 技术漏洞

现存主流的区块链平台，仍然存在大量技术漏洞. 在短短几年的发展过程中，区块链技术仍然显示出了不够成熟的显著特点. 这种特点导致区块链部署的过程中可能会出现许多无法预见的问题，这些

万方数据

问题甚至会导致一些区块链项目直接走向失败. 例如，现在流行的以太坊平台，其智能合约编写语言 Solidity 不支持使用小数点，并且对于编写代码使用的堆栈空间都有不同程度的要求. 这种情况给编程人员的开发过程带来了一定的困难，并且在实际应用程序的部署过程中可能会带来一些无法预见的技术漏洞.

(2) 交易吞吐量

影响交易吞吐量的环节主要有：广播通信、信息加解密、共识机制、交易验证. 其中最关键的环节就是共识机制. 由于区块链的去信任特性，区块链对于正确性和唯一性的保证就需要通过各个节点付出足够的代价(工作量)，表征自己的可靠性，自己消息的真实性. 在证明的过程当中，往往需要消耗大量的时间和算力，因此处理的速度就受到了限制. 目前，也有很多相关的研究者和公司在努力改善这种状况. POW 算法尽管解决了双花问题，但是浪费的资源太多，并且验证时间过长，很多文章在这方面做了一些探索. Min 等人[51]提出了一个提升吞吐量和减少延迟的基于 POW 的优化框架. Eyal 等人[92]提出一种新的可扩展的块链协议来克服 Bitcoin(块大小和间隔 vs 延迟和稳定性)中出现的可扩展性问题. Joseph 等①提供了另一种可扩展性的替代方案，该方法利用脱钩交易，同时使用分布式账本维护从事非关联交易的各方之间的合同. Meredith[149]采取关键步骤，找到一种方法来解释和测试一个假设，利用线性证明为块链接的可扩展架构提供了基础. Joseph 等人[89]讨论了比特币的可扩展性限制，但是没有量化较小的区块间隔或大的区块间隔对系统安全性的影响. 为了改善比特币的交易确认时间，可以采用叔区块②或将区块切分成微块和宏块[92].

(3) 不适合大量数据存储

区块链技术的底层本质是分布式存储技术，根据区块链的特性，所有交易等数据都会存储在区块中，并且这些数据是“单次写入，多次读取”的. 通过分布式系统的不同节点备份，能够有效防止账本被恶意篡改. 在区块链账本中，不允许对已有数据进行更改，如果想对于账本进行更改，只能通过链接新的区块进行声明来达到目的. 随着区块链网络中参与节点数的增多、交易量的增加，区块大小会迅速膨胀，对于每个分布式备份节点所需要进行数据存储的空间也会越来越大. 区块扩容、使用轻量级节点目前还不能彻底解决这种问题. 不仅仅是存储数据量的膨胀，随着区块容量的提高，网络传输代价也会随之变大. 因此，区块链系统的数据存储也是目前一个值得关注的问题.

(4) 隐私安全性

区块链的分布式账本由网络中节点公开维护，信息透明. 节点的参与和退出十分自由，无需身份验证，因此，可能存在恶意节点截取链上记录作恶. 链上的交易记录与网络中某些不相关信息关联可能会造成隐私泄露的风险，更有可能使用户陷入被攻击的被动局面. 在大数据技术的辅助下，区块链的加密技术确实被证实可能存在风险，其加密技术能够实现的可能仅仅是一种假名的现象，一些刻意的攻击仍能造成威胁. 不同地址之间的关联交易也可能暴露用户的隐私信息，这对于商业用途是十分致命的. 再加上随着量子计算的发展，密码学本身的安全性也受到了威胁，因此需要不断地更新其中的技术才能保证区块链的安全性.

(5) 跨链协议问题

随着区块链技术的发展，各种以区块链为底层技术的公链相继浮现，这些公链应用在了不同的行业领域，实现着自己不同的经济价值. 然而，每一个公链的出现即意味着产生了一种新的数字货币，各个公链平台之间，无法相互进行数字货币的流通，没有统一协议作为支撑. 区块链技术构建了一个价值互联网，在这个网络中，链接的有效节点越多，产生的经济价值越大，而不应该仅仅将经济价值局限于各个公链自身之中. 在这种场景下，跨链协议的统一标准显得尤为重要. 在跨链协议中，对于“以什么作为统一的各公链之间的兑换标准”这一问题的思考非常重要.

(6) 法律法规尚不规范

区块链技术以其去信任的特性赢得各行业的广泛关注，但是该领域尚缺乏明确法律法规，对区块链技术的治理、监管和标准等仍不健全. 使用区块链技术作恶的例子不在少数，如使用区块链的概念作为噱头开发空气币或恶意集资等金融欺诈问题，以及恶意参与方使用区块链平台或技术为违法犯罪案件提供便利. 这些问题也严重限制了区块链技术在各领域中的大规模应用. 由于区块链系统中并无确定负责中心，因此需要协议规定问责对象. 明确监管区

① The Bitcoin lightning network: Scalable off-chain instant payments. https://www.bitcoinlightning.com/wp content/uploads/2018/03/lightning-network-paper.pdf

② Sompolinsky Y, Zohar A. Accelerating Bitcoin's transaction processing. Fast money grows on trees, not chains. https://pdfs.semanticscholar.org/4016/80ef12c04c247c50737b9114c169-c660aab9.pdf

万方数据

块链的政策法规，才能够促进区块链企业间良性竞争和区块链行业应用的蓬勃发展.

6 结 论

区块链诞生于比特币系统，发展于人们的想象力，区块链将会带给我们多少惊喜还未可知. 本文对区块链技术进行了完整的梳理，抛开比特币的光环，更加客观全面地审视这种技术. 对区块链系统的构成，运转原理做了简单的介绍. 其后详细说明了区块链中三种核心技术：对于安全有至关重要作用的密码学原理，对于去中心化不可或缺的共识机制，能够使整个网络运转的纽带 P2P 网络. 此外还对比了现有的较为成熟的区块链技术的应用，能够使大家对区块链技术有着更为直观的了解和认识. 最后，介绍了区块链的挑战、机遇与探索. 尽管已经吸引了许多目光，现阶段的区块链技术仍处在萌芽阶段，现有平台发展情况良莠不齐，还未形成统一的规范标准. 从研究角度来看，对于区块链的安全性、算法性能和可扩展性的探索还远远不够，需要更多的理论支持论证，区块链技术的无限潜力还有待我们继续发掘.

参 考 文 献

[1] Alabi K. Digital blockchain networks appear to be following Metcalfe's Law. Electronic Commerce Research and Applications, 2017, 24: 23-29

[2] Haber S, Stornetta W S. How to time-stamp a digital document//Proceedings of the Conference on the Theory and Application of Cryptography. Berlin, Germany, 1990: 437-455

[3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008

[4] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 2018, 14(4): 352-375

[5] Lin I C, Liao T C. A survey of blockchain security issues and challenges. International Journal of Network Security, 2017, 19(5): 653-659

[6] Li X, Jiang P, Chen T, et al. A survey on the security of blockchain systems. Future Generation Computer Systems, 2017, 8: 274

[7] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)
(袁勇，王飞跃. 区块链技术发展现状与展望. 自动化学报，2016, 42(4): 481-494)

[8] He Pu, Yu Ge, Zhang Yan-Feng, et al. Survey on blockchain technology and its application prospect. Computer Science, 2017, 44(4): 1-7(in Chinese)
(何蒲，于戈，张岩峰等. 区块链技术与应用前瞻综述. 计算机科学，2017, 44(4): 1-7)

[9] Shao Qi-Feng, Jin Che-Qing, Zhang Zhao, et al. Blockchain: Architecture and research progress. Chinese Journal of Computers, 2018, 41(5): 969-988(in Chinese)
(邵奇峰，金澈清，张召等. 区块链技术：架构及进展. 计算机学报，2018, 41(5): 969-988)

[10] Chen Wei-Li, Zheng Zi-Bin. Blockchain data analysis: A review of status, trends and challenges. Journal of Computer Research and Development, 2018, 55(9): 1853-1870 (in Chinese)
(陈伟利，郑子彬. 区块链数据分析：现状、趋势与挑战. 计算机研究与发展，2018, 55(9): 1853-1870)

[11] Pacioli L. Summa de Arithmetica geometria proportioni: Et proportionalita. Venice: Paganino de paganini, 1494

[12] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. Sebastopol, USA: O'Reilly Media, Inc., 2014

[13] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in Bitcoin//Proceedings of the International Conference on Financial Cryptography and Data Security. San Juan, Puerto Rico, 2015: 507-527

[14] Leiserson C E, Rivest R L, Cormen T H, et al. Introduction to Algorithms. Cambridge, USA: MIT Press, 2001

[15] Merkle R C. A digital signature based on a conventional encryption function//Proceedings of the Conference on the Theory and Application of Cryptographic Techniques. Amsterdam, The Netherlands, 1987: 369-378

[16] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[17] Rivest R L, Shamir A, Tauman Y. How to leak a secret: Theory and applications of ring signatures. Theoretical Computer Science. Berlin, Germany: Springer, 2006: 164-186

[18] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from Bitcoin//Proceedings of the 2014 IEEE Symposium on Security and Privacy. Berkeley, USA, 2014: 459-474

[19] Coulouris G F, Dollimore J, Kindberg T. Distributed Systems: Concepts and Design. 5th Edition. London, UK: Pearson Education, Inc., 2012

[20] Lamport L. Time, clocks, and the ordering of events in a distributed system. Communications of the Association for Computing Machinery, 1978, 21(7): 558-565

[21] Lynch N A. Distributed Algorithms. Amsterdam, Netherlands: Elsevier, 1996

[22] Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults. Journal of the ACM, 1980, 27(2): 228-234

[23] Lamport L. How to make a multiprocessor computer that correctly executes multiprocess programs. IEEE Transactions on Computers, 1979, C-28(9): 690-691

万方数据

[24] Herlihy M P, Wing J M. Linearizability: A correctness condition for concurrent objects. ACM Transactions on Programming Languages and Systems, 1990, 12(3): 463-492

[25] Fischer M J, Lynch N A, Paterson M. Impossibility of distributed consensus with one faulty process. Journal of the ACM, 1985, 32(2): 374-382

[26] Fox A, Brewer E A. Harvest, yield, and scalable tolerant systems//Proceedings of the 7th Workshop on Hot Topics in Operating Systems. Arizona, USA, 1999: 174-178

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

[28] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm//Proceedings of the Annual Technical Conference (USENIX ATC 14). Philadelphia, USA, 2014: 305-319

[29] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401

[30] Castro M, Liskov B. Practical Byzantine fault tolerance// Proceedings of the USENIX Symposium on Operating Systems Design and Implementation. New Orleans, USA, 1999: 173-186

[31] Dwork C, Naor M. Pricing via processing or combatting junk mail//Proceedings of the Annual International Cryptology Conference. Berlin, Germany, 1992: 139-147

[32] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper, 2012, 19

[33] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2017: 357-388

[34] Gilad Y, Hemo R, Micali S, et al. Algorand: Scaling byzantine agreements for cryptocurrencies//Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai, China, 2017: 51-68

[35] Bentov I, Lee C, Mizrahi A, et al. Proof of activity: Extending Bitcoin's proof of work via proof of stake//Proceedings of the International Association for Cryptologic Research. Santa Barbara, USA, 2014: 452

[36] Dziembowski S, Faust S, Kolmogorov V, et al. Proofs of space//Proceedings of the Annual Cryptology Conference (CRYPTO). Santa Barbara, USA, 2015: 585-605

[37] Juels A, Kaliski Jr B S. PORs: Proofs of retrievability for large files//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 584-597

[38] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 598-609

[39] Ateniese G, Kamara S, Katz J. Proofs of storage from homomorphic identification protocols//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Tokyo, Japan, 2009: 319-333

[40] Halevi S, Harnik D, Pinkas B, et al. Proofs of ownership in remote storage systems//Proceedings of the 18th ACM Conference on Computer and Communications Security. Chicago, USA, 2011: 491-500

[41] Ateniese G, Bonacina I, Faonio A, et al. Proofs of space: When space is of the essence//Proceedings of the International Conference on Security and Cryptography for Networks. Amalfi, Italy, 2014: 538-557

[42] Miller A, Juels A, Shi E, et al. Permacoin: Repurposing Bitcoin work for data preservation//Proceedings of the 2014 IEEE Symposium on Security and Privacy. Berkeley, USA, 2014: 475-490

[43] Wilkinson S, Boshevski T, Brandoff J, et al. Storj: A Peer-to-Peer Cloud Storage Network V2. 0. Citeseer Press, 2016

[44] Milutinovic M, He W, Wu H, et al. Proof of luck: An efficient blockchain consensus protocol//Proceedings of the 1st Workshop on System Software for Trusted Execution. Trento, Italy, 2016: 2

[45] Chen L, Xu L, Shah N, et al. On security analysis of proof-of-elapsed-time (poet)//Proceedings of the Citeseer Press International Symposium on Stabilization, Safety, and Security of Distributed Systems. Boston, USA, 2017: 282-297

[46] Zhang F, Eyal I, Escriva R, et al. REM: Resource-efficient mining for blockchains//Proceedings of the Citeseer Press Security Symposium (USENIX Security 17). Vancouver, Canada, 2017: 1427-1444

[47] Miller A, Xia Y, Croman K, et al. The honey badger of BFT protocols//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 31-42

[48] Duan S, Reiter M K, Zhang H. BEAT: Asynchronous BFT made practical//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 2028-2041

[49] Cachin C, Vukolić M. Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873, 2017

[50] Pass R, Shi E. Hybrid consensus: Efficient consensus in the permissionless model//Proceedings of the International Symposium on Distributed Computing (DISC 2017). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. Vienna, Austria, 2017, 39: 1-16

[51] Min X, Li Q, Liu L, et al. A permissioned blockchain framework for supporting instant transaction and dynamic block size//Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA. Tianjin, China, 2016: 90-96

[52] Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: Analysis and applications//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria, 2015: 281-310

[53] Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol with chains of variable difficulty//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 2017: 291-323

万方数据

[54] Pass R, Seeman L, Shelat A. Analysis of the blockchain protocol in asynchronous networks//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Paris, France, 2017: 643-673

[55] Pass R, Shi E. The Sleepy model of consensus//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Hong Kong, China, 2017: 380-409

[56] Kiayias A, Koutsoupias E, Kyropoulou M, et al. Blockchain mining games//Proceedings of the 2016 ACM Conference on Economics and Computation. Maastricht, The Netherlands, 2016: 365-382

[57] Kroll J A, Davey I C, Felten E W. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries//Proceedings of the WEIS. Washington, USA, 2013: 11-32

[58] Natoli C, Gramoli V. The balance attack or why forkable blockchains are ill-suited for consortium//Proceedings of the Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Denver, USA, 2017: 579-590

[59] Sompolinsky Y, Zohar A. Bitcoin's security model revisited. arXiv preprint arXiv: 1605.09193, 2016

[60] Gramoli V. On the danger of private blockchains//Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16). Washington, USA, 2016: 1-4

[61] Kraft D. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413

[62] Eyal I. The miner's dilemma//Proceedings of the 2015 IEEE Symposium on Security and Privacy. San Jose, USA, 2015: 89-103

[63] Lewenberg Y, Bachrach Y, Sompolinsky Y, et al. Bitcoin mining pools: A cooperative game theoretic analysis//Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. Istanbul, Turkey, 2015: 919-927

[64] David B, Gaži P, Kiayias A, et al. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tel Aviv, Israel, 2018: 66-98

[65] Badertscher C, Gaži P, Kiayias A, et al. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 913-930

[66] Donet J A D, Pérez-Sola C, Herrera-Joancomartí J. The Bitcoin P2P network//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2014: 87-102

[67] Huang B, Liu Z, Chen J, et al. Behavior pattern clustering in blockchain networks. Multimedia Tools and Applications, 2017, 76(19): 20099-20110

[68] Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system. Security and Privacy in Social Networks. New York, USA: Springer, 2013: 197-223

[69] Fleder M, Kester M S, Pillai S. Bitcoin transaction graph analysis. arXiv preprint arXiv: 1502.01657, 2015

[70] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins: Characterizing payments among men with no names//Proceedings of the 2013 Conference on Internet Measurement Conference. Barcelona, Spain, 2013: 127-140

[71] Barber S, Boyen X, Shi E, et al. Bitter to better—How to make Bitcoin a better currency//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2012: 399-414

[72] Okamoto T, Ohta K. Universal electronic cash//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1991: 324-337

[73] Kumar A, Fischer C, Tople S, et al. A traceability analysis of Monero's blockchain//Proceedings of the European Symposium on Research in Computer Security. Oslo, Norway, 2017: 153-173

[74] Noether S, Mackenzie A. Ring confidential transactions. Ledger, 2016, 1: 1-18

[75] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups//Proceedings of the Australasian Conference on Information Security and Privacy. Sydney, Australia, 2004: 325-335

[76] Karame G O, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin//Proceedings of the 2012 ACM Conference on Computer and Communications Security. Raleigh, USA, 2012: 906-917

[77] Rosenfeld M. Analysis of hashrate-based double spending. arXiv preprint arXiv: 1402.2009, 2014

[78] Bissias G, Levine B N, Ozisik A P, et al. An analysis of attacks on blockchain consensus. arXiv preprint arXiv: 1610.07985, 2016

[79] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 2018, 61(7): 95-102

[80] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 515-532

[81] Rosenfeld M. Analysis of Bitcoin pooled mining reward systems. arXiv preprint arXiv: 1112.4980, 2011

[82] Courtois N T, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. arXiv preprint arXiv: 1402.1718, 2014

[83] Tosh D K, Shetty S, Liang X, et al. Security implications of blockchain cloud with analysis of block withholding attack//Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. Madrid, Spain, 2017: 458-467

[84] Singh A. Eclipse attacks on overlay networks: Threats and defenses//Proceedings of the IEEE International Conference

万方数据

on Computer Communications (INFOCOM). Barcelona, Spain, 2016: 1-12

[85] Heilman E, Kendler A, Zohar A, et al. Eclipse attacks on Bitcoin's Peer-to-Peer network//Proceedings of the Security Symposium (USENIX Security 15). Washington, USA, 2015: 129-144

[86] Marcus Y, Heilman E, Goldberg S. Low-resource eclipse attacks on ethereum's Peer-to-Peer network//Proceedings of the International Association for Cryptologic Research. Arequipa, Peru, 2018: 236

[87] Natoli C, Gramoli V. The balance attack against proof-of-work blockchains: The R3 testbed as an example. arXiv preprint arXiv: 1612.09426, 2016

[88] Douceur J R. The Sybil attack//Proceedings of the International Workshop on Peer-to-Peer Systems. Cambridge, USA, 2002: 251-260

[89] Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains//Proceedings of the International Conference on Financial Cryptography and Data Security. Christ Church, Barbados, 2016: 106-125

[90] Dennis R, Owenson G, Aziz B. A temporal blockchain: A formal analysis//Proceedings of the 2016 International Conference on Collaboration Technologies and Systems(CTS). Orlando, USA, 2016: 430-437

[91] Bano S, Al-Bassam M, Danezis G. The road to scalable blockchain designs. Winter, 2017, 42(4): 31-36

[92] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable blockchain protocol//Proceedings of the Symposium on Networked Systems Design and Implementation (USENIX NSDI 16). Santa Clara, USA, 2016: 45-59

[93] Kogias E K, Jovanovic P, Gailly N, et al. Enhancing Bitcoin security and performance with strong consistency via collective signing//Proceedings of the Security Symposium (USENIX Security 16). Washington, USA, 2016: 279-296

[94] Boyen X, Carr C, Haines T. Blockchain-free cryptocurrencies. A rational framework for truly decentralised fast transactions. IACR Cryptology ePrint Archive, 2016, 2016: 871

[95] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. arXiv preprint arXiv: 1505.06895, 2015

[96] Luu L, Narayanan V, Zheng C, et al. A secure sharding protocol for open blockchains//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 17-30

[97] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. Omniledger: A secure, scale-out, decentralized ledger via sharding//Proceedings of the Symposium on Security and Privacy(SP). San Francisco, USA, 2018: 583-598

[98] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 931-948

[99] Pass R. Micropayments for decentralized currencies//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 207-218

[100] Khalil R, Gervais A. Revive: Rebalancing off-blockchain payment networks//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 439-453

[101] Green M, Miers I. Bolt: Anonymous payment channels for decentralized currencies//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, USA, 2017: 473-489

[102] Dilley J, Poelstra A, Wilkins J, et al. Strong federations: An interoperable blockchain solution to centralized third-party risks. arXiv preprint arXiv: 1612.05491, 2016

[103] Swan M. Blockchain—Blueprint for a new economy. Sebastopol, USA: O'Reilly Media, 2015

[104] Szabo N. Smart contracts: Building blocks for digital markets. The Journal of Transhumanist Thought, 1996, 18(16): 2

[105] Chang Jia. Blockchain: From Digtital Currency to Credit Society. Beijing: CITIC Press Corporation, 2016(in Chinese)
(长铗. 区块链：从数字货币到信用社会. 北京：中信出版集团股分有限公司，2016)

[106] Peters G W, Panayi E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Banking Beyond Banks and Money. New York, USA: Springer, Cham, 2016: 239-278

[107] Frey R M, Vuckovac D, Ilic A. A secure shopping experience based on blockchain and beacon technology//Proceedings of the 10th ACM Conference on Recommender Systems(PosterRecSys 2016). Boston, USA, 2016(1608): 1-2

[108] Bogner A, Chanson M, Meeuw A. A decentralised sharing app running a smart contract on the ethereum blockchain//Proceedings of the 6th International Conference on the Internet of Things. Stuttgart, Germany, 2016: 177-178

[109] English S M, Nezhadian E. Conditions of full disclosure: The blockchain remuneration model//Proceedings of the European Symposium on Security and Privacy Workshops (EuroS&PW). Paris, France, 2017: 64-67

[110] Dorri A, Kanhere S S, Jurdak R, et al. Blockchain for IoT security and privacy: The case study of a smart home//Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Kona, Big Island, USA, 2017: 618-623

[111] Dorri A, Kanhere S S, Jurdak R. Towards an optimized blockchain for IoT//Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. Pittsburgh, USA, 2017: 173-178

[112] Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology//Proceedings of the International Conference on High Performance Computing and Communications; International Conference on Smart City; International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Sydney, Australia, 2016: 1392-1393

[113] Lee B, Lee J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. The Journal of Supercomputing, 2017, 73(3): 1152-1167

万方数据

[114] Zhang Y, Wen J. The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994

[115] Kim H M, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, Finance and Management, 2018, 25(1): 18-27

[116] Wüst K, Gervais A. Do you need a blockchain?//Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT). Zug, Switzerland, 2018: 45-54

[117] Chakravorty A, Rong C. Ushare: User controlled social media based on blockchain//Proceedings of the International Conference on Ubiquitous Information Management and Communication. Beppu, Japan, 2017: 99

[118] Carboni D. Feedback based reputation on top of the Bitcoin blockchain. arXiv preprint arXiv:1502.01504, 2015

[119] Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain//Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST). London, UK, 2015: 131-138

[120] Nath I. Data exchange platform to fight insurance fraud on blockchain//Proceedings of the 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW). Barcelona, Spain, 2016: 821-825

[121] Ølnes S. Beyond Bitcoin enabling smart government using blockchain technology//Proceedings of the International Conference on Electronic Government. Guimarães, Portugal, 2016: 253-264

[122] Gerstl D S. Leveraging Bitcoin blockchain technology to modernize security perfection under the uniform commercial code//Proceedings of the International Conference of Software Business. Ljubljana, Slovenia, 2016: 109-123

[123] Jabbar K, Bjørn P. Growing the blockchain information infrastructure//Proceedings of the CHI Conference on Human Factors in Computing Systems. Denver, USA, 2017: 6487-6498

[124] Shrier D, Wu W, Pentland A. Blockchain & infrastructure (identity, data security). Massachusetts Institute of Technology-Connection Science, 2016, 1(3): 1-19

[125] Lundbaek L N, D'Iddio A C, Huth M. Optimizing governed blockchains for financial process authentications. arXiv preprint arXiv: 1612.00407, 2016

[126] Cachin C. Architecture of the hyperledger blockchain fabric//Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Washington, USA, 2016, 310: 4

[127] Sharma P K, Moon S Y, Park J H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. Journal of Information Processing Systems, 2017, 13(1): 184-195

[128] Yuan Y, Wang F Y. Towards blockchain-based intelligent transportation systems//Proceedings of the International Conference on Intelligent Transportation Systems (ITSC). Rio de Janeiro, Brazil, 2016: 2663-2668

[129] Dorri A, Steger M, Kanhere S S, et al. Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 2017, 55(12): 119-125

[130] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access, 2016, 4: 2292-2303

[131] Sharples M, Domingue J. The blockchain and kudos: A distributed system for educational record, reputation and reward//Proceedings of the European Conference on Technology Enhanced Learning. Lyon, France, 2016: 490-496

[132] Mettler M. Blockchain technology in healthcare: The revolution starts here//Proceedings of the International Conference on e-Health Networking, Applications and Services (Healthcom). Munich, Germany, 2016: 1-3

[133] Yue X, Wang H, Jin D, et al. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 2016, 40(10): 218

[134] Azaria A, Ekblaw A, Vieira T, et al. Medrec: Using blockchain for medical data access and permission management //Proceedings of the International Conference on Open and Big Data (OBD). Vienna, Austria, 2016: 25-30

[135] Fukumitsu M, Hasegawa S, Iwazaki J, et al. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain//Proceedings of the International Conference on Advanced Information Networking and Applications (AINA). Taipei, China, 2017: 803-810

[136] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data//Proceedings of the Security and Privacy Workshops. San Jose, USA, 2015: 180-184

[137] Xu R, Zhang L, Zhao H, et al. Design of network media's digital rights management scheme based on blockchain technology//Proceedings of the International Symposium on Autonomous Decentralized System (ISADS). Bangkok, China, 2017: 128-133

[138] Ali M, Nelson J, Shea R, et al. Blockstack: A global naming and storage system secured by blockchains//Proceedings of the Annual Technical Conference (USENIX ATC 16). Denver, USA, 2016: 181-194

[139] Matsumoto S, Reischuk R M. IKP: Turning a PKI around with blockchains. IACR Cryptology ePrint Archive, 2016, 2016: 1018

[140] Wilson D, Ateniese G. From pretty good to great: Enhancing PGP using Bitcoin and the blockchain//Proceedings of the International Conference on Network and System Security. New York, USA, 2015: 368-375

[141] Vorick D, Champine L. Sia: Simple Decentralized Storage. Nebulous Inc., Technical Report, 2014

[142] Watanabe H, Fujimura S, Nakadaira A, et al. Blockchain contract: A complete consensus using blockchain//Proceedings of the Global Conference on Consumer Electronics (GCCE). Osaka, Japan, 2015: 577-578

万方数据

[143] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint arXiv: 1506.03471, 2015

[144] Leiding B, Memarmoshrefi P, Hogrefe D. Self-managed and blockchain-based vehicular ad-hoc networks//Proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. Heidelberg, Germany, 2016: 137-140

[145] Mendling J, Weber I, Aalst W V D, et al. Blockchains for business process management-challenges and opportunities. ACM Transactions on Management Information Systems, 2018, 9(1): 4

[146] Weber I, Xu X, Riveret R, et al. Untrusted business process monitoring and execution using blockchain//Proceedings of the International Conference on Business Process Management. Rio de Janeiro, Brazil, 2016: 329-347

[147] García-Bañuelos L, Ponomarev A, Dumas M, et al. Optimized execution of business processes on blockchain//Proceedings of the International Conference on Business Process Management. Barcelona, Spain, 2017: 130-146

[148] Rimba P, Tran A B, Weber I, et al. Comparing blockchain and cloud services for business process execution//Proceedings of the International Conference on Software Architecture (ICSA). Gothenburg, Sweden, 2017: 257-260

[149] Meredith L G. Linear types can change the blockchain. arXiv preprint arXiv: 1506.01001, 2015

CAI Xiao-Qing, Ph. D. candidate. Her research interest is blockchain.

DENG Yao, M. S. candidate. His research interest is blockchain.

ZHANG Liang, Ph. D. candidate. Her research interests include distributed system, data flow, blockchain.

SHI Jiu-Chen, Ph. D. candidate. His research interests include distributed system, blockchain.

CHEN Quan, Ph. D., tenure-track professor. His research interests include distributed computing, computer architecture and blockchain.

ZHENG Wen-Li, Ph. D., tenure-track associate professor. His research interests include distributed system, cloud computing and blockchain.

LIU Zhi-Qiang, Ph. D., associate professor. His research interests include blockchain, information security and cryptography.

LONG Yu, Ph. D., associate professor. Her research interests include blockchain and cryptography.

WANG Kun, Ph. D., professor. His research interests include blockchain, energy internet and edge computing.

LI Chao, Ph. D., tenure-track professor. His research interests include architecture for new applications and new technologies.

GUO Min-Yi, Ph. D., professor, IEEE Fellow. His research interests include parallel computing, distributed system, big data and blockchain.

Background

The blockchain technology draws increasing attention for its unique decentralization and trustless features. Since blockchain initially starts from Bitcoin, a currency system, the focus of blockchain in the early stage is mainly on the application level, not on the technical level. What's more, there are no unified specifications and standards for blockchain, making it difficult to explore in-depth. As a result, a comprehensive survey on blockchain is necessary. Blockchain is a completely new concept, existing introduction surveys are high level, aiming at explanation more than technical analysis. It's unhelpful for readers to find their interests in subsequent research. The paper introduces three core technologies in detail from a technical perspective. The paper breaks blockchain architecture into five core layers, and elaborates on the data, network, and consensus parts. It provides blockchain enthusiasts a convenient and comprehensive index map. They can spend their time on something more meaningful than looking for information. This work is partially sponsored by the National Key R&D Program of China (No. 2018YFB1004800), the National Basic Research 973 Program of China (No. 2015CB352403), the National Natural Science Foundation of China (Nos. 61872240, 61602301, 61632017, 61702329, 61832006, 61702328), and the Shanghai Science and Technology Innovation Fund (No. 19511101403).

万方数据