计算机工程与应用
Computer Engineering and Applications
ISSN 1002-8331,CN 11-2127/TP

《计算机工程与应用》网络首发论文

题目：区块链关键技术及存在问题研究综述

作者：刘双印，雷墨鹭兮，王璐，孙传恒，徐龙琴，曹亮，冯大春，郑建华，李景彬

网络首发日期：2021-11-02

引用格式：刘双印，雷墨鹭兮，王璐，孙传恒，徐龙琴，曹亮，冯大春，郑建华，李景彬．区块链关键技术及存在问题研究综述[J/OL]．计算机工程与应用．https://kns.cnki.net/kcms/detail/11.2127.TP.20211101.1727.005.html

网络首发时间：2021-11-02 14:42:53
网络首发地址：https://kns.cnki.net/kcms/detail/11.2127.TP.20211101.1727.005.html

区块链关键技术及存在问题研究综述

刘双印[1,2,3,4,6]，雷墨鹭兮[1,3,4,6]，王璐[1,3,4,6]，孙传恒[5]，徐龙琴[1,3,4,6*]，曹亮[1,3,4,6]，冯大春[1,3,4,6]，郑建华[1,3,4,6]，李景彬[2]

(1. 广州市农产品质量安全溯源信息技术重点实验室， 广州 510225；2. 石河子大学机械电气工程学院， 石河子 832000；3. 仲恺农业工程学院 智慧农业创新研究院， 广州 510225；4. 广东省高校智慧农业工程技术研究中心， 广州 510225；5. 国家农业信息化工程技术研究中心，北京 100097；6. 广东省农产品安全大数据工程技术研究中心， 广州 510225）

摘 要：区块链是基于数字加密货比基础上发展而来的分布式数据库技术，区块链系统具有去中心化、不可篡改、高度自治、分布共识等特点，为无需第三方监管实现分布式一致性问题提供了解决方案。随着区块链技术快速发展，区块链在弱信任平台应用领域更加普及，但也面临着自身系统漏洞和安全攻击的挑战。本文从区块链研究背景及漏洞发展趋势入手，总结分析了区块链关键技术原理及其优缺点、区块链系统存在的技术漏洞和安全攻击，并对技术漏洞和漏洞攻击类型进行归纳分类，指出语法错误、环境配置和图形界面错误是区块链系统中排前三的漏洞缺陷，漏洞攻击对区块链系统构成极大的安全威胁，务必加以重视和防范，以期对未来区块链技术改进发展提供参考与借鉴。

关键词：区块链；共识机制；去中心化；智能合约；漏洞攻击

文献标志码：A **中图分类号**：TP391 doi：10.3778/j.issn.1002-8331.2107-0404

Survey of Blockchain Key Technologies and Existing Problems

LIU Shuangyin[1,2,3,4,6], LEI Moyixi[1,3,4,6], WANG Lu[1,3,4,6], SUN Chuanheng[5], XU Longqin[1,3,4,6*], CAO Liang[1,3,4,6], FENG Dachun[1,3,4,6], ZHENG Jianhua[1,3,4,6], LI Jingbin[2]

(1.Guangzhou Key Laboratory of Agricultural Products Quality & Safety Traceability Information Technology, Guangzhou 510225, China

2.College of Mechanical and Electric Engineering Shihezi University, Shihezi, 832000, China

3.Academy of Intelligent Agricultural Innovations, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China;

4.Intelligent Agriculture Engineering Technology Research Center of Guangdong Higher Education Institutes, Guangzhou 510225, China

5.National Engineering Research Center for Information Technology in Agriculture, Beijing 100097, China

6.Guangdong Provincial Agricultural Products Safety Big Data Engineering Technology Research Center, Guangzhou 510225, China）

Abstract：Blockchain is a distributed database technology developed on the basis of digital encryption and comparison. The blockchain system has the characteristics of decentralized, non-tampering, high autonomy, distributed consensus, etc., and achieves distributed consistency without third-party supervision. The problem provides a solution. With the rapid development of blockchain technology, blockchain has become more popular in the application field of weak-trust platforms, but it also faces the challenges of its own system vulnerabilities and security attacks. This article starts with the research background of the blockchain and the development trend of vulnerabilities, summarizes and analyzes the key technical principles of the blockchain and its advantages and disadvantages, the technical

基金项目：广州市重点研发计划项目（202103000033）；广州市创新平台建设计划项目（201905010006）；广东省重点领域研发计划资助（2020B0202080002）；国家自然科学基金项目(61871475，61471133)；广东省科技计划项目（2019B020215003，2017B0101260016）；广东普通高校工程技术研究中心(2017GCZX0014)；北京市自然科学基金项目（4182023）；广东省农业技术研发项目（2018LM2168）

作者简介：刘双印（1977-），男，博士，教授，CCF 会员，主要研究方向区块链溯源、机器学习、人工智能、大数据和智能信息处理等。Email：hdlsyxlq@126.com;雷墨鹭兮（1997-），女，硕士研究生，CCF 学生会员，主要研究方向区块链与安全、区块链溯源。

vulnerabilities and security attacks that exist in the blockchain system, and summarizes and categorizes the types of technical vulnerabilities and vulnerability attacks. Pointed out that grammatical error, environmental configuration and graphical interface errors are the top three vulnerabilities in the blockchain system. Vulnerability attacks pose a greatest security threat to the blockchain system. We must pay attention and prevent them in order to protect the future blockchain system. Provide reference and reference for technological improvement and development.

Key words: blockchain; consensus mechanism; decentralized; smart contact; vulnerability attacks

在当今信息大爆炸的时代，时刻产生海量数据难以安全可靠传输，数据安全已严重影响人们的生活，如何有效保证系统数据安全成了如今迫在眉睫的问题之一[1]。每个人都是数据的生产者和使用者，但企业往往为保护隐私导致数据共享性差，甚至出现数据孤岛等问题。虽然数据共享技术不仅可解决信息的封闭性和单一性问题，也有效实现数据增值，但同时存在上述数据安全和隐私泄漏的缺陷。2018 年 Facebook 遭黑客攻击，8000 余万条用户信息被泄漏；2019 年多个公司大量用户数据被盗，黑客私下交易 8.7 亿条个人数据；2020 年万豪国际集团 520 万客人信息被泄漏等，这些被泄漏的身份信息常被不法分子用于非法活动。因此，研究新一代技术防止黑客攻击，确保数据安全具有重要的现实意义。

区块链是一种在密码学、统计学、经济学和计算机科学等多学科交叉基础上发展起来的新技术，以其去中分布式存储、匿名性高、数据一致性等优点被广泛应用于信息安全、金融、证券、数字确权、溯源等领域，实现数据的分布式存储和有效利用。区块链与隐私保护的结合可以降低第三方监管不严的风险，在一定程度上保证数据安全有效，具有更广阔的应用价值。区块链系统的安全性对系统本身意义重大，为了避免恶意节点的攻击，使交易有序进行，区块链工作者改进共识机制、优化智能合约、对网络监管进行加强，让区块链能应用到各个领域。但由于区块链技术还处在发展阶段，其在核心技术领域并不完善，导致区块链系统本身存在一些缺陷，甚至在改善的过程中产生了一些新的技术漏洞，因此本文在分析区块链关键技术的基础上，主要针对区块链现存的一些问题进行分析总结，概括了目前区块链的几项关键技术，旨在总结出区块链系统现阶段存在的问题，并给出了基于这些关键技术存在的安全问题。通过详细阐述区块链系统现存问题：a)可以作为区块链系统开发者的参考，了解和避免常见的陷阱;b)可以作为研究人员的指导，以促进区块链技术的分析和验证技术的发展。以期为未来的区块链发展提供更强有力的理论和现实支撑，为能更快的发现问题解决问题。因此，本文对区块链系统现存问题和安全漏洞的分析对区块链技术的发展具有极为重要的意义。

1 研究背景

1.1 区块链研究背景

“区块链”概念于 2008 年在《比特币：一种点对点电子现金系统》中被首次提出[2]，并在比特币系统的数据加密货币体系成功应用，已成为政府、企业和学者等重点关注和研究热点。英国政府于 2016 年 1 月发布了《分布式账本技术：超越区块链》报告[3]，指出英国政府正积极的评估区块链技术潜力，并旨在更好的用来处理领导、协作和治理之间的关系；同年 11 月，微软发布 Azure 区块链。我国于 2016 年 10 月发布了《中国区块链技术于应用发展白皮书（2016）》[4]，预示着我国正式进入了前所未有的区块链高速发展时代；同年 2 月 IBM 公司正式推出区块链应用平台；2019 年 10 月，习近平总书记指出区块链作为自主创新的新兴技术，将成为国家级战略部署关键技术之一。截止到 2019 年底，我国已经发布了 25 项与密码模块相关的国家标准，阿里、腾讯、京东及百度等大型互联网公司陆续推出自己的区块链服务平台；Facebook 公司成立 Libra 协会，美国已有 28 个州推出区块链的相关政策，且其政府部门共提出了 22 项区块链相关法案[5]。2020 年我国成立区块链专委会，招商银行、农业银行和工商银行等国内金融机构纷纷推出区块链金融项目，为促进区块链快速发展奠定坚实基础。

区块链技术具有去中心化存储、隐私保护、防篡改等特点，提供了开放、分散和容错的事务机制，成为新一代匿名在线支付、汇款和数字资产交易的核心，被广泛应用于各大交易平台[6]。同时也给金融、监管机构、科技创新、农业以及政治等领域都带来了深刻的变革[7-9]。以可编程社会为目标，区块链技术将同 20 世纪互联网技术一样，创造 21 世纪技术革新的新纪元[10-12]。

1.2 安全漏洞研究背景

据国家信息安全漏洞共享平台[13]统计，自 2016 年到 2020 年的低危、中危和高危漏洞分布对比，如图 1 所示。中危漏洞发生频率最高，虽然在 2018 年有所减少，但是总体处于增长状态；高危漏洞的发生频率仅次于中危漏洞，2017 年下降明显，但随后几年又呈快速增长趋势；低危漏洞发生率最低，但逐年不断增长。总体来看，漏洞总量仍然处于不断上升的势态，应用程序、操作系统及数据库的安全性依然存在极大威胁。

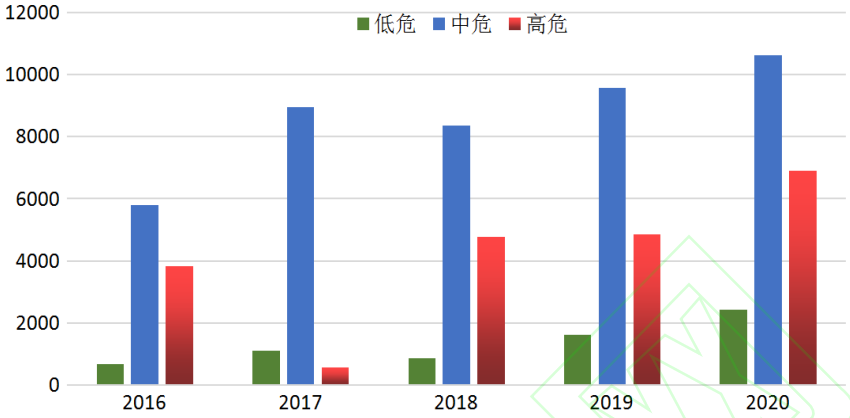

图 1　近五年漏洞分布对比

Fig.1　Comparison of vulnerability distribution in the past five years

1.3系统漏洞

同时漏洞严重危害着区块链系统的安全，为了进一步分析区块链漏洞危害，文献[14]从区块链系统角度进行分类，总结概括分为以下 6 类漏洞：

由表 1 可以看出，第一类漏洞主要由语义设置造成，由于开发人员对程序的不透彻理解导致引入错误语义，且语义错误一般特定于应用程序，即使后续使用智能检测工具也很难自动检测出来。具体的可以分为执行错误、异常处理错误、特征缺失以及输入输出错误。例如 cpp-ethereum 系统中回退功能不属于外部合约估算；go-ethereum 系统中，在函数中 GET&POST 延长截止日期请求陷入超时会导致最后期限延长。第二类为环境和配置漏洞，由于区块链系统应用环境较为宽泛，且不同的环境驻留在不同的硬件或操作系统上，安装许多不同版本的库会影响依赖库的功能；即便安装相同版本的库，由于用户的各种自定义操作，也会使库的配置信息与环境不匹配，导致底层操作系统执行错误。第三类是 GUI 漏洞，主要表现为用户图形界面的设置不规范。例如在 Windows 下，比特币系统的界面会因为主机自身设置的原因显得过大；在 dogecoin 系统中，客户端的启动画面时，徽标与文字重叠；ethereum 系统中，点击新的窗口加载器屏幕不显示框架等诸如此类情况的发生。第四类是并发漏洞，在大型系统中，高线程或进程并发极易出现错误从而造成系统错误。在 cpp-ethereum 系统中，如果多个客户同时创建交易，以太坊默认设置无法可靠使用，因为任何客户端都可以随时更改它，因此以太坊交易在创建合同时返回的地址不能保证是否是合同实际目标地址。第五类为安全漏洞，由于系统脆弱性导致软件上的信息和软件提供的服务被破坏，极易遭受各种漏洞攻击的危害。第六类为性能漏洞，主要体现在系统不能高效执行系统任务而造成事务延迟，致使进程死锁等现象。例如 go-ethereum 系统中高速读取磁盘时进程死锁导致任务中断甚至数据丢失等的情况发生。

表 1　漏洞分类

Table 1　Classification of Bugs

分类 Classification	描述 Description	占比 Percentage
语义 Semantic	与程序员意图不符或与上述条件不一致 Inconsistent with the programmer's intention or inconsistent with the above conditions	67.23%
环境和配置 Environment and Configuration	影响功能的依赖库、底层操作系统和非代码中的漏洞 Vulnerabilities in dependent libraries, underlying operating systems, and non-code that affect functionality	11.42%
图形界面 GUI	图形用户界面漏洞，包括不正确字体、对齐方式和按钮大小 Graphical user interface vulnerabilities, including incorrect font, alignment, and button size	6.98%

并发 Concurrency	并发任务间的同步、数据竞争和死锁问题导致漏洞 Synchronization, data races and deadlocks between concurrent tasks lead to vulnerabilities	4.44%
安全 Security	系统脆弱性导致软件、软件上的信息和软件提供的服务被破坏 System fragility leads to the destruction of software, information on the software, and services provided by the software	1.90%
性能 Performance	系统在正常工作负载下响应能力和稳定性方面表现异常的漏洞 Vulnerabilities where the system performs abnormally in terms of responsiveness and stability under normal workloads	1.48%

2 区块链概念

自中本聪[2]提出区块链之后，国内外学者从不同的角度对区块链概念提出了自己的见解。如 Sookhak 提到区块链是一个分散的、无信任的、防干扰的、分布式的账本[15]。Daniel 认为区块链是一种新型的软件开发架构，以一种仅附加的形式使用独特的数据结构将数据连接成链，并将哈希函数作为映射数据的工具以保证数据的安全[16]。王芳将区块链定义为利用加密链式区块结构来验证与存储数据、使用分布式节点共识机制(Consensus Mechanism)来生成和更新数据，并通过智能合约(Smart Contracts)来编程和操作数据的一种去中心化的基础架构与分布式计算范式[17]。袁勇、张奥将区块链理解为是一个随着时间序列不断增长的去中心化的分布式数据库，其本质是基于非对称加密算法的分布式账本技术[6,18]。Yu 认为区块链是电子货币帐簿系统的一种点对点技术实现，它是由参与者来维护的，可以在网络系统中没有中心服务器的情况下记录每个比特币交易记录[19]。Halamka 解释区块链是由一组不可变的分布式数字账本组成，它们负责跟踪交易并将其记录在数字块上，区块链架构中所有节点相对应地服务且不依赖中心网络服务器，因此区块链中心故障点无懈可击[20]。Yang、魏晓旭认为区块链是采用密码学的方法将数据块连接在一起并可以进行可行性交易的分布式数据库技术，具有防篡改、可追溯、多方维护的功能，它为了实现不同各方之间的信息共享和信息监督，任何一方必须按照约定事先得到其他各方的同意[21-22]。综上所述，区块链概念可以理解为以非对称加密算法为基础，以改进的默克尔树（MerkleTree）[23]为数据结构，使用共识机制、点对点网络、智能合约等技术结合而成的一种分布式存储数据库技术。

区块链分为公有链（Public Blockchain）、联盟链（Consortium Blockchain）、私有链（Private Blockchain）和混合链（Hybrid Blcokchain）[24]四大类。公有链是网络中任何人都可以随时访问的区块链系统，通常被认为是完全去中心化、匿名性高和数据不可篡改的区块链。联盟链为若干企业或机构共同管理的区块链，参与者要事先进行注册认证，因此相对于公有链来说，联盟链的参与节点较少。数据由认证后的参与者共同记录和维护，这类节点拥有读取数据的权限。私有链是一种由某个组织或某个用户控制的区块链，控制参与节点个数规则严格，因此交易速度极快，隐私等级更高，不容易遭受攻击，相比于公有链系统有更高的安全性，但去中心化程度被极大削弱。从接入类型来看，区块链分为非许可链和许可链[14]。非许可链不需要获得允许即可接入区块链系统，公有链就是一种典型的非许可链，所有节点都可以自由参与链上的交易。许可链包括联盟链和私有链，对于接入节点有严格的标准和控制，系统内的数据访问权只授权给经过认证的节点。相对于非许可链来说，许可链牺牲了一定的去中心化特性[25]，以换取链上数据更高的安全性保护。混合链是公有链和私有链的混合体，结合了共有链和私有链的特性。混合链允许用户决定区块链的参与成员，以及交易是否可以被公开，因此混合区块链是可定制的，所以它的混合架构通过利用私有区块链的限制访问来确保隐私，同时保持了公共区块链的完整性、透明度和安全性。

3 区块链关键技术分析

区块链技术包括密码学、默克尔树（MerkleTree）、对等节点（Peer-to-Peer，P2P）、共识机制以及智能合约[26]，其区块链关键技术栈如图 2 所示。

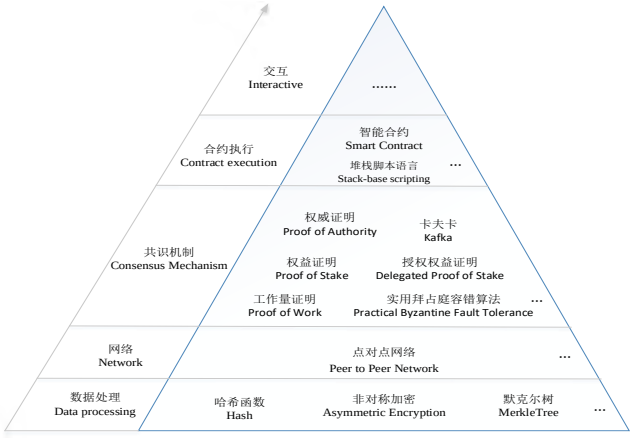

图 2　区块链关键技术栈

Fig.2 Stack of Blockchain key technology

区块链中密码学原理主要涉及到加密和签名，其中加

密是由发送方利用接收方的公钥加密，接收方收到信息后用自己的私钥解密即可得到信息内容；签名是由发送方用自己的私钥签名，接收方用发送方的公钥验证其信息发送者的身份；两种方式皆采用非对称加密算法。默克尔树利用哈希指针构成树形数据结构，将处理后的数据连接汇总为一串哈希值，节点间的算法一致性保证了哈希指针的准确性。对等节点（P2P）组网运行在区块链系统的网络层，用于控制消息和数据之间的传输可以直接在节点之间完成，有利于各个节点监听网络发布区块以及验证信发布交易的合法性，允许数据以快速和安全的方式存储、维护和分发[27]。共识机制则保证了区块链中所有用户的共同参与，是实现去中心化管理的重要协议，从公知机制提出至今已有一系列的公式算法投入使用。智能合约在区块链基础上得到进一步的完善，由开始的单一堆栈脚本语言到如今可自动控制交易完成度的合约协议。

从结构来看，区块包含区块头（BlockHeader）和区块体（BlockBody）两部分，区块头中的关键信息包括当前版本号（Version）、前区块哈希值(PreviewsHash)、时间戳（Timestamp）、随机数(Nonce)以及默克尔树（MerkleTree）的哈希值（MerkleHash）等信息[28]。前一个区块存储后一个区块的哈希值，并按生成的时间顺序进行连接，物理上是块与块之间的连接，逻辑上是链上信息的关联，构成了一个外表为链内在是数据关联的账本形式，如图 3 所示。区块链的关键技术加密算法、默克尔树、共识机制、智能合约详细分析如下。

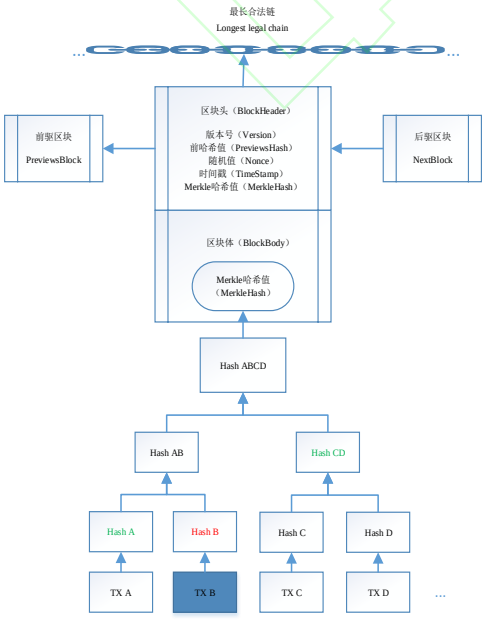

图 3　区块链内部结构图

Fig.3　Structure of Blockchain internal diagram

3.1 哈希算法

哈希函数是一种将可变长度数据映射到固定长度摘要的函数，对输入数据的任何更改都会导致哈希列中发生不可预测的变化。区块链中使用 SHA-256（Secure Hash Algorithm 256）哈希函数对任意长度的交易数据进行哈希运算，即将源数据加工得到一串 256 位的字符，便于数据统一管理和存储，再将统一格式的字符打包存进区块，在减少存储空间的同时最大程度保证数据安全性。哈希函数具有三大经典特性：单向性（Hiding）、抗碰撞性（Collision resistance）、结果不可预测性（Puzzle friendly）。其中单向性：已知输入可以得到输出，但是已知输出无法逆推出输入。抗碰撞性：由于哈希函数拥有 2^{256} 个输入空间，计算量趋于无限大，想要构造一个输入使其结果为当前值几乎不可能。结果不可预测性：对于已经公布的交易或是随机值，要推测得到特定特征的输出也是不可能的。在区块链的交易过程中为了保证数据的安全，如图 4 交易签名过程，首先对所有产生的交易数据都取哈希值 Hash（M）；其次将得到的哈希值与交易明文拼接得到最终发送内容 *S*；然后将 *S* 用发送方自己的私钥进行数字签名，最终将数字签名写入区块。该数字签名利用非对称算法的计算安全性，保证了信息的完整性和不可抵赖性，例如 A 给 B 发起交易，A 声称自己是 A，但 B 无法确定消息的正确性以及 A 的身份，因为 B 的公钥是公开的，任何人都可以使用 B 的公钥向其发送消息，而数字签名不仅能够确保 A 的身份和数据的完整性，还能够防范双花攻击[29]，减少分叉的可能。

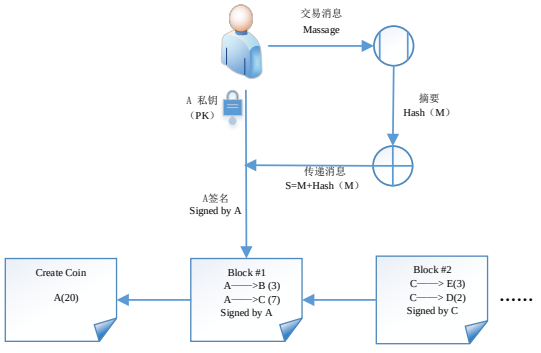

图 4　交易签名

Fig.4　Signature of transaction

3.2 MerkleTree

从广义上来看，区块链是在密码学的基础上，对数据的一种分布式存储技术。首先对数据进行预处理：区块链对数据进行加密取哈希、摘要处理，得到符合区块要求的数据格式，在减少存储空间的同时最大程度的保证了数据的安全性。存储：即将得到的不同数据哈希值打包放进区块。在计算机领域中，MerkleTree[30]是一种树形数据结构，如图 3 所示。区块分为区块头和区块体，两部分使用 MerkleTree 的数据结构进行存储连接，叶子结点的交易（transaction，TX）两两得到的哈希值是上一层的叶子结点，这样逐层往上递进，将区块体中全部交易迭代得到的根哈希值打包存储在区块头中。在打包交易时再添加交易时间戳、随机数等关键值。MerkleTree 可以实现大量数据的快速存储和读取，有利于数据的高效验证。

作为区块链数据存储的关键结构，MerkleTree 主要用于完整交易的存在性检查[31]。MerkleTree 中将网络节点分为全节点和轻节点。全节点中保存着链上交易中所有的信息，而轻节点则负责验证交易合法性，如比特币钱包。其主要步骤为：

1）轻节点计算出 TX B 的 Hash B，并向链中全节点发送请求，请求一个能够证明蓝色交易 TX B 被包含在 MerkleTree 里面的默　克尔树根哈希值（Merkle proof）。

2）全节点收到请求，将上一层绿色的 Hash A 发送给轻节点进行计算验证。

3）轻节点得到 Hash A，与自己的 Hash B 进行哈希运算得到 Hash AB 值，全节点再将另一个分支上绿色的 Hash CD 传给轻节点。

4）轻节点将自己的 Hash AB 与得到的 Hash CD 进行哈希运算最终得到 Hash ABCD。

5）最后将 4）的结果与本地存储的根哈希值进行比较，验证该交易的存在性。

3.3 共识机制

共识机制是指在动态交易的过程中使节点对分布式数据库中的内容达成一致的过程，区块链使用共识机制令节点对交易达成一致性共识，从而弱化中心化监管体系的功能。从最开始的工作量证明（Proof of Work, PoW）、实用拜占庭容错算法（Practical Byzantine Fault Tolerance, PBFT）、权益证明（Proof of Stake, PoS）到后来的授权权益证明（Delegated Proof of Stake, DPoS）、权威证明（Proof of Authority, PoA）和 Kafka 等一系列共识机制[32-34]。共识机制一直在不断完善，对应着领域要求的不同向不通的方向演进。作为区块链的核心技术，共识机制能有效对区块链中各节点的数据达成共识，快速完成交易数据处理，保证了数据的一致性和可靠性。其典型的共识机制详细分析如下。

工作量证明（Proof of Work，PoW）：Cynthia 于 1993 年首次提出用工作量证明思想，通过计算出某个数学难题来提高垃圾邮件发送者成本[35]。1999 年首次在论文中引出 PoW 共识机制，这也为后世中本聪提出在比特币中使用的共识机制奠定了基础[36]。工作量证明是区块链共识机制中最典型的算法之一，如比特币中的挖矿过程。“矿工”通过不断尝试计算出符合挖矿难度（Difficulty）的随机数 N，来获得一定的比特币奖励，如公式 1 所示。难度值属于 2^{256} 个输入空间中极小的一部分目标值域（Target），如公式 2 所示。在区块链系统中区块会在某个周期内（每 2016 个区块，约两周时间）动态调整阈值的难度，如公式 3 所示，当系统挖矿难度（target）不变时，实际挖矿的难度大于预期挖矿的难度，等号右边大于 1，目标阈值增大，同时挖矿难度减小，挖矿难度与目标阈值难度成正比。当挖矿人数增多导致区块产生速度明显加快时，系统就会提升挖矿的难度，使区块的产生速度趋于平衡（一般情况下每 10 分钟产生一个区块）。1999 年 Liskow 等提出使用拜占庭容错算法（Practical Byzantine Fault Tolerance, PBFT），应用于吞吐量不大但要处理大量事件的数字资产平台，在原始拜占庭算法的基础上提高了效率[37]。PBFT 算法规定全网至少需要部署 $3f+1$ 个节点，最多可容忍 f 个恶意节点，若出现拜占庭故障，整个系统的状态由 $2f+1$ 个节点决定，即在保证系统活性和安全性前提下，在全网恶意节点数少于 1/3 时达成共识。但著名科学家 Eric 教授在报告中提出分布式系统在一致性、安全性、分区容错性三者中最多只能同时满足两种，PBFT 算法亦不能满足当时的生态系统。2012 年，权益证明（Proof of Stake, PoS）首次在点点币（Peercoin）中出现，其使用“币龄”的概念将矿工手中的货币量加以控制，并规定持币者必须有一定时间期限，时间越久币龄越长，如公式 4 所示

[38-39]。为了保证系统的公平性，矿工的币龄越高则挖矿的难度越低，在一定程度上可以削减用户被攻击的可能性。PoS 的出现改善了 PoW 中算力消耗过大的现象，并在一定程度上缓解了之前由于出块时间过慢造成效率低下的情况，增加了吞吐量的同时加快了处理速度，但若系统中首富现象突出，会造成中心化集中问题[40]。

$$H(\text{BlockHea der}) \leqslant \text{target} \tag{1}$$

$$\text{T arg } et = t \arg et * \frac{actualtime}{\exp ectedtime} \tag{2}$$

$$\text{Di}fficulty = \frac{difficulty \parallel t \arg et}{T \arg et} \tag{3}$$

币龄=货币量×持有时间 （4）

其中，actualtime 和 expectedtime 分别为实际挖矿难度和期望挖矿难度；target 和 Difficulty 分别为系统的目标阈值难度和挖矿难度；Difficulty ‖ target 为系统设置实际挖矿难度值，最小为 1，Target 为目标阈值。

授权权益证明（Delegated Proof of Stake, DPoS）[41]：DPoS 基于民主投票的形式，由节点选举出 N 个成员成为系统中的“代表团”，拥有代币数量越多的节点成为“代表”的概率越大。团中的“代表”节点负责收集信息、打包交易以及验证交易和新生产的区块，如下授权权益证明工作流程图。由时间片轮流分配时间给“代表”节点处理事物，若出现恶意“代表”，该节点将会被撤销出块权利并取消“代表”资格，再推选出新的“代表”。DPoS 的出现减少了算力和电力的浪费，也提升了交易处理速度和区块吞吐量，但同时不可避免的削弱了去中心化工作模式的能力。

权威证明（Proof of Authority, PoA）：以太坊创始人 Gavin 于 2017 年首次提出权威证明共识机制。PoA 共识机制主要用于声誉积累，验证者需要验证用户的身份，而不是用户所持有的货币[42]。想要验证交易的用户要首先确认其身份，将身份链接到所执行的验证，并存储在区块链上。当交易被验证时，验证者的身份将通过某种协议在链上得到确认。该身份只有由一小群验证者来确定，从而提高了共识协议的效率和安全性。PoA 不需要高计算成本，也不需要积累大量代币，但它仅适用于私有区块链和联盟区块链网络。同年 7 月，Hyperledger 社区正式发布 Fabric 1.0，其中出现的共识机制打破了以往以证明为主的共识机制印象，形成了以背书节点（Endorsing peer）、排序节点（Orderers）和提交节点（Committing Peer）三类节点为主的 Fabric 共识机制[43]。超级账本共识流程如图 5 所示，其主要步骤如下：

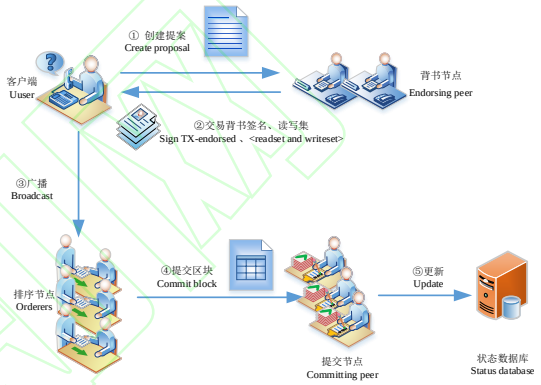

图 5　超级账本共识流程

Fig. 5　Process of hyperledger fabric consensus

步骤一：客户端（Client SDK）创建提案，根据所选择的背书策略（Endorsement policy）将提案发送给相应的背书节点。提案中包含了用户编号（ClientID）和所调用的链码函数（BlockchainCoin Function）及其参数、时间戳（Timestamp）和客户端签名（ClientSig）等信息[44]。

步骤二：背书节点会验证客户端签名，确保提案是由已认证的客户端发出。背书节点所模拟的交易请求是根据提案中链码执行的，背书节点的签名（Sign TX-endorsed）附加在生成的执行结果中，即背书过程。模拟执行的结果是一组基于当前世界状态（State Database）的读写集（Readset and WritesetSet），背书后将背书签名和读写集发送给客户端。

步骤三：客户端验证背书结果的签名，确保其来自合法的背书节点，客户端可以检查背书节点签名的有效性以及从不同背书节点接收到的读写集之间的一致性，如果一

致则根据背书结果生成交易并广播给排序节点。在验证阶段后期客户端可以施行强制检查，目的是可以帮助在事务流程早期阶段检测事务故障，以降低开销。

步骤四：在 Hyperledger Fabric 中使用 Kafka 模式对交易进行排序。排序节点将收到的交易交给 Kafka 集群排序，同时会按照一定的规则从 Kafka 集群中读取一定数量的有序交易并打包成块。排序服务对区块签名后，将区块分发给提交节点。

步骤五：提交节点收到区块后，即可对区块进行验证，其中主要是验证交易中的读写数据集是否与世界状态的数据版本一致。提交节点使用读写集合的读集部分来检查交易的有效性，然后将所有验证通过的交易中读写集中写部分写入世界状态，同时提交节点会使用写集更新状态数据库即账本。若验证失败，已中止和已提交事务的验证块将附加到分类帐中，将记录每个事务的提交或中止状态。

除了以上介绍的六类主流共识机制，还存在一些应用于各大区块链平台的共识算法，文章对它们的特征、优缺点、参与系统以及在自身基础上所提出的改进算法整理如下表 2 所示：

表 2　共识机制分类

Table 2 Classification of consensus

名称 Name	特征 Feature	优缺点 Advantage/disadvantage	参与系统 System	改进算法 Improved
工作量证明（PoW，Proof of Work）	由中本聪在其论文中提出，用于建立分布式无信任共识并识别“双重支付”（double spend）问题。	自测试以来就得到广泛应用； 速度慢、耗能大，易受“规模经济”影响。	Bitcoin Ethereum Litecoin	PoS PoSV
权益证明（PoS，Proof of Stake）	PoS 作为 Pow 的替代技术被提出，PoS 中不支持一次性消耗所有算力。	节能，增加了攻击者的攻击代价，不受“规模经济”的影响；受“无利害关系（Nothing at stake）”攻击影响。	Ethereum Peercoin Nxt	Ouroboros PoSV PoActivity
授权权益证明（DPoS，Delegated Proof-of-Stake）	权益持有者可以选举领导者（或称为见证人，Witness）。经权益持有者授权，这些领导者可进行投票。该机制使得 DPoS	节能高效；略为中心化，拥有高权益的参与者可投票使自己成为验证者。	BitShares Steemit EOS Lisk Ark	Casper DPoS dBFT
e）	要快于正常的 PoS。			
权威证明（PoA，Proof-of-Authority）	基于 PoA 的网络、事务和区块，是由一些经认可的账户认证的，这些被认可的账户称为“验证者”（Validator）。	节能高效；略为中心化，虽然可用于公有区块链，但是通常用于私有区块链和许可区块链。	POA.Network Ethereum Kovan testnet VeChain	
所用时间证明（PoET，Proof of Elapsed Time	PoET 用于许可区块链网络，它可决定网络中获得区块者的挖矿权利，它的实施需要确保两个重要因素 1）参与节点在本质上自然选取某个随机时间，而非某个参与者为胜出而刻意选取的较短的时间。2）胜出者的确完成了等待时间。	高效去中心化，对于参与者更易于验证领导者是否通过合法选举产生，且选举过程与获得价值成正比； 需使用特定的硬件，无法大规模采用，不适合公有区块链。	HyperLedger Sawtooth	PoSV PoWeight
空间证明（PoSpace，Proof of Space）	PoSpace，也称为 PoC，通过分配一定数量的内存或磁盘空间用于解决服务提供者所提供挑战的方式。此概念由 Dziembowski 等在 2015 年提出。	使用空间代替计算因此环境友好，可用于恶意软件检测，防范拒绝服务（DoS）攻击；激励机制存在问题。	Burstcoin Chia SpaceMint	
权益流通证明（PoSV，Proof of Stake Velocity）	PoSV 是作为 PoW 和 PoS 的替代方法被提出，是为了提高 P2P 网络的安全性，进而用于确认 Reddcoin （一种加密货币）交易。	高效节能，安全性提高；作为 PoS 的改进	Reddcoin	
实用拜占庭容错（PBFT，Practical Byzantine Fault Tolerance）	PBFT 使用了较少的预选定将军数，因此运行非常高效。	高交易通量和高吞吐量；略中心化，用于许可网络。	Hyperledger Fabric Stellar Ripple Dispatch	dBFT DPoS-BFT
联邦拜占庭协议（FBA，FederatedByzantine Agreement）	FBA 的通用理念是每个拜占庭将军负责自身的链、消息一旦到来，通过排序建立事实。因吞吐量优于所有共识机制被广泛使用。	吞吐量极高，交易开销低和网络扩展性好；只用于私有网络和许可网络		
授权拜占庭容错算法（dBFT，Delegated Byzantine Fault Tolerance）	dBFT 可为具有个共识节点的共识系统提供\(f = {{n-1} \over 3}\)容错。这种容错也涵盖了安全性和可用性、不受将军和拜占庭错误影响，并且适合任何网络环境。	快速可扩展；每个人都争相成为根链。其中可能存在多个根链。	Neo	

RAFT	Raft 提供一种在计算系统集群中实现分布状态机的通用方式，确保集群中每个节点在同一组状态转移上取得一致，且具有一系列的开源参考实现。不可容忍拜占庭错误。	模型比 Paxos 更简单，提供了同等的安全性，有多种语言可实现； 用于私有网络和许可网络。	IPFSPrivate Cluster Quorum	
有向无环图（DAG，Directed Acyclic Graphs）	每个区块和交易只需数个前期区块得到确认，就可并行地添加到区块和交易中。	高度可扩展，快速节能； 只能通过使用 Oracle 实现智能合约。	Iota HashGraph Byteball RaiBlocks/Nano	Tangle ByteBall Hashgraph 等

3.4 智能合约

智能合约（Smart Contract）[45]由 Szabo 在 1994 年首次提出，它是一段可以自动执行的计算机程序，在区块链中应用复杂的可编程语言和工程操作对区块链的执行步骤做约束，当账户触发特定条件时合约自动执行。其目的是为了保证合约双方不能恶意篡改合约内容，并能够在没有中心管理者的监管下确保合同有效实施，其代码具有自动执行和跟踪协议条款和条件的能力，因此，智能合约是自我验证、自我执行和不可逆的，智能合约被认为是区块链革命的第三代产品[46]。

智能合约的雏形是基于比特币系统的堆栈脚本语言（Stack-base scripting）[47-48]，该语言不支持内部循环，缺乏图灵完备性（Turing completeness）。比特币中的智能合约只能支持有限的计算逻辑，是基于交易的账本模式（Transaction-based Ledger），故通常只能用于识别用户身份。以太坊使用图灵完备的智能合约对交易进行识别、处理和验证，调用函数对以上过程进行操作。超级账本（Hyperledger）旗下的 Fabric 子项目采用多种通用语言编写“链码（Chaincode）”，Fabric 更偏向于企业级应用开发，功能强大，共识机制可插拔，基于复杂的业务逻辑触发执行，开发过程快速便利。

智能合约的执行流程[49]如下图 6 所示，智能合同通常由一个可以识别的执行代码和状态集合的特定地址组成。两方发起交易，合约由开发人员（Developer）进行开发，通过使用不同编程语言（如 Python 或 Solidity[50]）中的特定条件语句进行编译，将编译得到的字节码（Bytecode）在以太坊虚拟机（EVM）里执行，并由矿工共识（Miners Consensus）强制执行智能合约，不同的交易触发各自对应的合约条款。提交包括智能合约功能所需参数的交易给区块链，同时矿工们要负责核实该交易的合法性并将事务存储到区块中，目的是创建一个用来调用智能合约的唯一地址。之后，区块链用户可以通过将事务传输到合约来调用合约代码触发事件（Event），合约将由状态变量和外部可信数据集进行检查。交易事件触发成功合约自动执行支付（Payment）操作，最后广播全网由矿工们进行验证（Verification）。

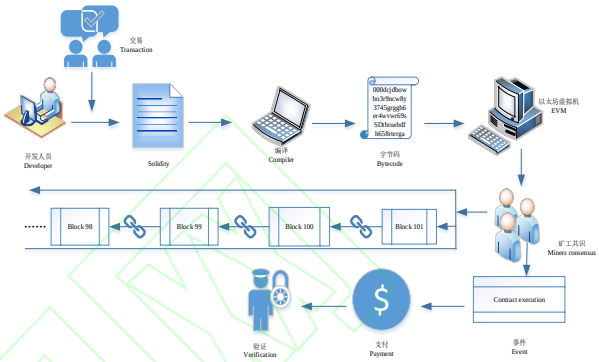

图 6　智能合约执行流程

Fig. 6　Working of smart contract

智能合约的调用只能由外部用户发起，合约用户不能主动发起交易。以以太坊为例，创建交易时，接收地址为要调用的智能合约地址，调用的函数及其函数的编码填写在合约的 DATA 域中。

代码 1：构造函数

构造函数仅在合约创建时调用一次，并准备好新合约的唯一地址：

代码 1: 构造函数

```
1 Constructor(time，address)
2   Public{
3            Address=address;      // 地址=当前合约地址
4            endtime=time;         // 事件终止时间=实际时间
5            bytes solution;
6 }
```

代码 2：合约函数

在智能合约中，使用 event 定义一个事件，emit 调用该事件。外部函数调用合约函数，此处假设外部账户已触发合约：

代码 2: 合约函数

```
1 contract X{
```

```
2   event A(string str)
3   Function foo(string str) return (uint){
4           emit A(str);
5           return 123;
6   }
7 }
8 contract Y{
9   uint z;        //z 为 x.foo("call foo directly")的返回值。
10          Function callXFooDirectly(address adr) public{    //调用 X 合约，该函数的参
数是合约 X 的地址
11          X x=X(adr);
12              z=x.foo("call foo directly")
13          }
14 }
```

用户交易由外部账户 W 发起，首先调用合约 Y，再由 Y 调用合约 X 继续执行。若用户交易调用的合约发生错误，会导致发起调用的合约立即回滚，即若合约 X 执行过程中出现异常，合约 Y 调用失败。

为了确保采矿网络计算消耗工作的公平，以太坊需向矿工支付与所需计算成比例的交易费。即以太坊字节码中的每个指令都具有预先指定数量的 gas，当用户发送交易调用合同时，用户须首先指定自身愿意为此次合约执行提供多少 gas 以及每个 gas 单元的价格（gasprice），区块中的矿工随后会收到交易费[49]，如公式 5。如果某些执行需要的气体超过 gas 限额（gaslimit），则执行终止，区块状态将恢复到初始状态，但作为保护机制，发送方仍必须向矿工支付所有的 gaslimit，这是对抗资源耗尽攻击的一种有效措施。

$$TX - fees = gasprice * gaslimit \quad (5)$$

以下将智能合约分为三类：

表 3　智能合约分类

Table 3　Classification of Smart Contract

类型 type	优点 advantage	缺点 disadvantage
智能法律合约 Smart legal contract	由国家法律严格编写而成的具有法律追索权的合同 A contract with legal recourse that is strictly compiled by national laws	国家之间的法律界限分明，缺乏对现行智能合约框架的支持 The legal boundaries between countries are clear, and there is a lack of support for the current smart contract framework
去中心化自治组织 Decentralized autonomous organization[61]	由社区自治化管理，资金由用户众筹所得，所有人都可以参与社区交易 Managed by community autonomy, funds are raised by users crowd-funding, and everyone can participate in community transactions	存在递归调用漏洞，导致短时间内大量资金流向攻击者，致使 DAO 不得不分叉 Existing a recursive call vulnerability, which causes a large amount of funds to flow to the attacker in a short period of time, causing the DAO to fork
应用逻辑合约 Application logic contract	适用于物联网领域，可以和链上其他智能合约还有程序协同工作 Applicable to the field of Internet of Things, it can work with other smart contracts and programs on the chain	多功能智能合约大多在一个管理程序下，不便于管理 Multifunctional smart contracts are mostly under one management program, so it's not easy to manage

与传统的智能合约相比，前者具有公开透明、内容不可篡改以及永久运行的能力，还具有去中心化和高效的特点。但由于其不可篡改性致使合约一旦部署便再无更改的可能性。同时由于匿名性，在目前网络法律立法还不完善的情况下，若任一方违约都将造成极大损失。最后，智能合约仍存在许多安全上的隐患亟待解决。

4 存在的问题

区块链顺应潮流发展，同时也存在很多问题制约和阻碍其推进。为了更好的分析区块链技术发展存在问题，本节将从区块链的数据存储与交互、隐私保护、资源分配、漏洞攻击四个方面进行概括总结。

4.1 数据存储与交互

区块链作为分布式数据库在数据存储和读取方面有一定的优势，但是随着数据的增多，大部分节点无法高效存储数据，出现多形式数据存储、数据更新以及跨链时延等问题。多形式数据存储：区块链最大的优势之一是对非关系型数据的一次存储多次读取，在密集的点对点网络（P2P）体系中随机部署节点进行数据 Hash 存储。对于合法用户而言，他们可以查询到自己或他人的交易额、内部系统信息或黑名单信息，但所有的数据都是以字符串的形式呈现，若交易数据是视频、音频或者图片，随着网络需求的增加，网络时延使数据传输失帧，分布式账本无法保证分布式一致特性。数据更新：由于区块链的序列化特性上链的每一条数据都需要进行排序连接，因此区块交易极其缓慢。比特币交易时长平均 10 分钟一个区块，每秒约 3 到 4 笔交易，以太坊出块时间约为 15 秒，每秒约 20 笔交易。相比之下，Visa 支付平台每秒可处理 6.5 万笔交易，支付宝每秒处理 8.9 万笔交易，它们的交易速率是比特币和以太坊的近千倍。

缓慢的交易速率极不利于数据快速存取和交互，若缩短出块时间则能最大化减少分叉产生带来的数据更新后的不一致。跨链时延：区块链结合了去中心和匿名等特点，在此基础上的加密数字货币可以在全世界范围内流通。作为一种点对点支付系统，对于跨国交易的操作比传统的支票和汇款更加方便快捷，除去人工的奔波耗时，降低了人为操作带来的失误率，同时提高了不同国家之间汇率的透明度。但随之而来的是手续费的增加，由于各个国家之间地域的跨度，造成数据传输时延大，在传输过程中更容易遭受恶意攻击，且交易确认等待时间长，因此区块链交易账本的分布式存储还需要考虑数据传输的安全性和可扩展性。

4.2 隐私保护

隐私保护指的是通过技术手段对个人或企业的隐私信息进行维护和保护的过程。以下主要将隐私保护分为用户隐私保护和企业隐私保护两大类别。1）用户隐私保护：对用户来说，隐私保护就是保护用户不愿意被公开的数据信息。匿名化使区块链与现实世界相隔绝，用户在使用区块链时很难做到使自己的身份、IP 地址、联系方式、公私钥以及姓名之间没有关联，攻击者对大量的用户交易地址使用流量分析等方式进行网络攻击。倘若所使用的账户地址没有高安全等级防护，私钥一旦泄漏，区块链没有任何更改机制，交易账户只能会遗弃。2）企业隐私保护：区块链上交易的每一个流程都是开放且透明的，但对企业而言，数据完全透明并不意味全是优势。例如股票交易所，每一笔交易都要求实时的数据操作，所有的用户都能看见其他节点的交易数据，易造成不法分子盗用用户隐私导致财产损失，使得企业失去广大用户的信任。

4.3 资源分配

区块链具有去中心化和防篡改的特性，因此账本上的数据对于系统来说容易存在事务排序依赖、数据高冗余、不可持续发展和算力浪费等问题。事务排序依赖：以太坊中，支付以太币越多，事务排序优先级越高，处理速度越快。即当两个节点同时提交事务，花费以太币较多的节点事务优先得到处理，致使花费较少的节点一直排序等待，并且后续支付较多的节点无需等待就可加入队列优先执行事务，造成进程堵塞，进度拖欠，导致资源分配极度不均。数据高冗余：区块链依赖分布式账本这一优势，对数据进行分布式存储。但随着要记录的数据越来越多，信息呈现爆炸式增长，每个节点为保证账本高度一致，实时复制、同步、更新造成数据高度冗余，且每个节点存储容量有限，这可能使得我们在未来面临着如何处置这些数据的困境。不可持续发展：纸币之所以流通是因为它具有重复使用、可交换及市场调节等功能。但是对于虚拟货币而言，币的数量是有限的，不能随着市场经济的变化而调控，由于币的固定性，其本身无法作为货币流通。其次，每次交易过程中都会收取交易费，随着剩下区块的数量越来越少，对应的区块奖励也随之不断减少，未来交易费将成为区块产生的驱动力，无论是对经济发展还是科技进步都是不利的。算力浪费：工作量证明是一种基于计算机算力争夺记账权的共识机制，在比特币中表现为“挖矿”的方式，这是一个天然的“赏金漏洞”——参与的人越多越民主，数据越安全，公众参与度增高，问题在于减少成本的同时被攻击的可能性也随之增加。这极大的暴露了代币机制的弊端，即记账权完全由算力决定，挖矿设备专业化驱使人们花重金购买性能更高的 ASIC 芯片进行算力争夺，导致芯片的算力越高获得记账权的机率越大，最后争夺记账权和芯片高算力成正比。使用 ASIC 芯片进行大量哈希计算造成巨大能源消耗，据统计，区块链高速发展时期，每年用来挖矿的电力相当于几个核电站的总电力输出。

4.4 漏洞攻击

黑客利用系统漏洞对其进行监听、拦截、重放甚至破坏的行为被称为漏洞攻击，因此，由于区块链系统自身漏洞造成的黑客攻击防不胜防，本节将其漏洞攻击类型分为分叉攻击、基于共识机制攻击、基于智能合约攻击以及其他攻击。

4.4.1 分叉攻击

分叉攻击在区块链系统中较为普遍，且危害极大，分叉攻击有主要分为系统自身产生分叉导致被攻击和攻击者主动制造分叉进行攻击两大类。系统自身产生分叉导致的分叉：首先，区块链在弱共识的前提下，因系统时间顺序产生区块的特性，会同时产生多个区块（State fork），因而极易成为攻击者的攻击目标；其次，由于区块链系统内部协议的更新，例如软件升级，弱共识无法要求整个系统中所有节点同时更新，就有可能产生硬分叉或软分叉[52]。硬分叉中旧节点不承认新节点，只要旧节点不更新系统分叉就不会消失。软分叉则相

反，只要一直沿着新节点增加区块即可消除分叉威胁。

攻击者主动制造分叉进行攻击：其一是女巫攻击（Sybil Attack），它是一种基于 P2P 网络的一种攻击类型，会由攻击服务器生成超过系统 51%的傀儡账户参与投票选举造成，它可以击败分布式存储系统的冗余机制，还会对传感器网络中的路由机制构成威胁[53]。其二是双花攻击（Double spending）[54]，它利用了比特币数字加密货币的传输特性，使一笔钱“花费两次”，除非接受方在交易发起时就立即验证每一笔代笔的来源，否则就将造成巨大损失，在比特币中使用交易签名的方式防范双花攻击，许多区块链硬件也会使用防篡改的模式。其三，以太坊为了防止双花攻击，对区块使用多数据集生成 hash 值，但是由于网络延迟，会产生重播攻击（Replayattack）[55]，即以太坊系统中重复使用同一请求，一笔钱“收两次”，与“双花攻击”恰好相反。其四是私自挖矿攻击[56-57]，主要指的是恶意矿池挖出区块隐瞒不发，而是继续在隐藏链上挖矿，当恶意矿池挖出的隐藏链比诚实节点所维护的合法链更长时，恶意矿池发布分叉链，由于诚实矿工都会选择最长链为合法链，因此分叉攻击实施成功。

4.4.2 基于密码学攻击

区块链中对于数据的安全保护基于密码学纯数学计算方式。所使用的密码学算法有 MAC 函数、HASH 函数以及 RSA 公钥加密体制和 ECC 椭圆曲线加密体制等[58-60]。这些算法在目前理论上是安全的，且密钥的产生需要特殊的随机元，一个好的随机元生成的密钥对的安全系数相比于较差的随机元的安全系数更高，能直接避免和其他账户生成重复的密钥对。针对密钥对的破解，最通用的密码爆破方式为字典攻击：通过构造常用的密码组合模式的脚本来自动执行匹配账户密码的步骤，但这样的脚本所构造的密码组合较为单一，对于复杂的账户密码无从下手。被动攻击[61]是基于攻击者对截取到的数据 PDU 进行的流量分析，数据包累计回应，攻击者可得到数据的长度、频度、特性甚至破解信息内容。由于区块链系统节点众多，对于认证的参与者无法完全确定其是否诚实，同样的，侧信道攻击[62-65]普遍存在于任何区块链系统，服务器硬件存储密钥信息，若私钥被盗，即可锁定私钥对应的账户，系统中私钥被盗将无法找回，重新生成同一私钥在计算上不能成立，若有报道称某加密货币被偷则意味着私钥被盗，由于区块链数据无法更改，一旦罪犯偷了一把私钥并将相关资金公开转移到另一个账户，这笔交易通常无法撤销。目前主流的 SHA-256 算法的输入空间 $2^{256} \approx 10^{77}$，虽是普通计算机昼夜不停两年的计算量，但若使用量子计算机，计算速率将成指数倍增长，因此，随着量子计算机[64,65]的兴起，现有密码体制将直接面临被攻破的威胁。

4.4.3 基于共识算法攻击

基于共识算法的攻击有 51%算力攻击、长程攻击、DDOS 攻击、区块截留攻击以及渗透博弈攻击。其中 51%算力攻击指的是 PoW 通过算力比拼以竞争区块记账权，若恶意节点拥有 51%的哈希算力，便可以发动攻击[66]。长程攻击是指从创世区块就开始创造另一条与主链完全不同的链，试图替换原主链，其中的交易和用户也不完全一致，由于节点的弱主观性，长程攻击成了 PoS 最大的威胁[67]。DDOS 攻击是指攻击者旨在利用庞大的 IP 群体对目标主机发送大量无效请求，导致目标主机接收不到真实请求，有时甚至造成系统瘫痪，致使共识效率极低，如在 Hyperledger Fabric 中极少数的背书节点就容易成为攻击目标[68]。区块截留攻击则指的是恶意矿工通过丢弃所有成功答案，而只向矿池管理员提交部分答案，造成矿池亏损。虽然区块截留不会对区块链造成很大的伤害，但是会降低矿池和诚实节点的收益，且以极低的代价让矿池不再受诚实节点的信任。渗透博弈[69]的原理源自博弈树，即攻击者选择对区块节点进行渗透，一般出现在矿池间的恶性竞争，于是在受攻击的节点上形成博弈状态，各方都为了自己的利益最大化[66]。

4.4.4 基于智能合约攻击

虽然智能合约是一段自动执行的程序代码，但它只是一套固定的规则逻辑在经过编写和审计之后得到多方用户签署再部署到分布式系统中，实际开放平台中还是存在合约构造不合理、代码不严谨、确认时间长以及事件调用依赖情况严重等不足，极易隐含漏洞成为被攻击的对象。

the DAO[51]是区块链史上众所周知的黑客攻击事件，因为系统代码漏洞，攻击者可间接递归调用漏洞函数，旨在系统中强行创建分支，并在每个分支上都获取以太币，the DAO 攻击造成了 6000 万美元的金额损失。时间戳依赖攻击[71]：在以太坊中设定节点之间需保持时间“大致相同”而并非完全保持一致，前驱区块的哈希值和区块数是已知的其他的合约变量，如导致产生随机

数的原因也是已知的。因此，矿工就可以预先计算和选择时间戳，矿工可以随机产生一个有利于他的结果，而攻击者利用这偏差来左右时间戳的设置并发动攻击。调用堆栈深度攻击：智能合约中规定，当外部用户调用合约用户时，合约堆栈自动增加一位，当栈满时会有溢出异常。在以太坊中，智能合约规定栈最大为 1024 位，攻击者在发动攻击之前，事先生成一个将满的堆栈，当再次调用目标合约时堆栈溢出就会抛出异常，导致系统崩溃轻。交易排序依赖攻击[72]：一个区块中包含的两个交易同时调用了一个合约导致用户不知道他们单独调用时合同处于哪种状态，因此用户打算调用的合约状态与执行时发生的实际状态存在差异，所以只有负责开采的矿工能决定合约的最终状态即交易的执行顺序。恶意用户可以利用合约的交易排序依赖来获得更多的利润，甚至可以窃取用户的钱。代码漏洞：在运算过程中当计算结果无法放置在整型数据类型中时，会产生整数溢出（Integer overflow）[72]。例如以太坊使用的 solidity 语言就具有该严重漏洞，会导致攻击者获得未经授权的数字资产，且 solidity 语言无法支持小数点，这可能使得一个区块链项目因数据格式不一致或精度不匹配而半途夭折。还有路由更改攻击，即攻击者利用 BGP 动态变化的路由更改自己的网络前缀伪装成其他节点，并对目标节点进行定向流量拦截，引导数据流向原本错误的路线。

4.4.5 其它攻击

除了以上四类基于区块链系统的漏洞攻击，还存在一些基于网络、社工或物理设备的漏洞攻击，攻击者可以利用它们从系统之外对数据进行窃取或破坏。分布式系统使物理上分隔的用户得以网络交互，而日蚀攻击可以阻止目标用户与外界进行数据通信。病毒攻击：现阶段区块链平台的广泛应用，没有统一的标准进行规范化约束，攻击者想要植入病毒或木马很容易，这会严重威胁到用户的财务状况[73]。供应链攻击：大多数的企业会把自家的大型业务外包给其他的技术公司或者是多家企业联合业务，但很多时候这种潜在的危险就是合作方，他可能是流氓企业，也可能有流氓雇员，在系统的产生过程中就已经存在漏洞。中间人攻击：攻击者对网络中传输的信息进行截取、偷听甚至篡改，但不会惊动通信双方的攻击方式。重放攻击：即将上一次传输的信息与当前传输的信息进行合并再发送，以达到欺骗系统和阻碍认证的目的。社会工程学分析[74-75]：对某些账户的交易数据进行流量分析，联系他在现实中的生活轨迹得到用户的真实身份。恶意软件攻击：攻击者通过向用户发送恶意软件骗取用户登陆信息，以盗取账户信息和节点私钥等。侧信道攻击：攻击者对链下支持区块链运行的物理设备进行的攻击甚至破坏，导致服务器硬盘损坏数据丢失等。虽然攻击者达到了破坏区块链分布式账本的完整性，但对于攻击者本身并没有多大益处。除以上所列出的各类攻击，还有各种各样的攻击类型。

5 分析与讨论

综上所述，导致全球区块链安全事件的原因包括两个方面：一方面是其共识机制、私钥管理、智能合约等存在的技术局限性所面临的安全问题；另一方面是区块链去中心、自治化的特点给现有数据存储、隐私保护、资源分配等技术手段带来了新的挑战。文章从目前区块链现存问题入手，其一从系统内部结构和逻辑意义两方面总结了技术局限所面临挑战的可能解决方案，其二提出检测技术、身份管理和法律法规三方面提出合理建议，共同维护区块链系统的安全性。

5.1基于分叉攻击与密码学攻击的安全分析总结

存在于区块链系统内部结构的两类攻击类型是基于分叉机制攻击和基于密码学攻击。在区块链系统中，分叉尤为常见，它易导致最长合法链不一致、系统无法同时更新软件、伪造节点投票和发动双花和重播攻击，或者私自屯块覆盖最长合法链等操作。因此为了有效缓解区块链遭到以上分叉攻击造成的影响，对应的解决方案如下：需要提升共识效率，增加出块速率；更新换代时定期查看日志，提醒用户及时更新；参与工作量证明机制，同时对每个节点身份进行验证；增加采矿过程的复杂性，每个用户增设 UTXO 集合，对于新产生的块延迟确认，在 6 个区块产出（约一小时）之后，被篡改概率指数下降；使用随机数和时间戳同时对数据包进行实时标记，对每一笔交易都有签名；定时查看 CPU 占用率高的进程，查看内部网络和主机的安全防护设备告警和日志信息，查找异常。基于密码学的攻击主要分为四类：较简单的字典攻击、由链外产生的被动攻击、基于物理逻辑的侧信道攻击以及复杂的量子密码攻击。字典攻击使用数学公式的排列组合或弱口令即可破解，世纪中叶非对称密码问世之后字典攻击只能对付对称密码。被动攻击主要是通过分析大量数据包得到信息来

破坏数据的保密性和完整性，因此使用 HASH 函数计算得到的固定值再 MAC 函数取摘要,HASH 函数与 MAC 函数相结合可以得到对消息以及消息发送者的同时验证。区块链系统中密钥管理的安全性允许节点自己生成密钥对，以促进网络中节点之间的安全通信，侧信道攻击主要针对存储有密钥的服务器或缓冲区，现有文献[76]提出了基于区块链的边缘计算密钥管理方案，并且提出以公开审计的方式对密钥进行保护。量子密码是目前最复杂的密码之一，量子计算机是一种利用物质和能量的物理特性进行计算的新技术，因此一个足够强大的量子计算机将使许多种形式从密钥交换到加密再到数字认证都处于危险之中。针对数据和流量分析以破解交易地址的攻击，Meiklejohn[77]提出更完善的“找零地址”，以确保用户账户的安全性。由密钥管理技术发展而来的，为保证系统中私钥管理的安全性，软件钱包、硬件钱包、托管钱包和门限钱包技术相继出现[78]。文献[79]提出量子密钥协议使远程参与者能够根据他们的私人输入公平地建立一个安全的共享密钥。同时随机密钥预分配机制[80-81]也开始流行。

5.2基于共识机制攻击与智能合约攻击的安全分析总结

区块链系统基于关键技术的逻辑意义，且可插拔的两类攻击类型是基于共识机制攻击和基于智能合约攻击，共识机制主要以分布式系统本身和所使用网络两方面改进，智能合约作为可插拔的自动执行程序，具有极强的可塑性，因此解决方案主要从已有的攻击类型和对应的可能解决方案，如表 4 所示：

表 4 基于共识机制和智能合约攻击防护措施分类

Table 4 Protection measures of attacks based on consensus mechanism and smart contracts

分类	名称	定义	防范机制	文献
基于共识机制攻击	51%攻击	一个具有更多计算资源的单个矿工节点比其他网络节点（51%）主导着事务的验证和审批。	检测技术，对加入的节点采用多重身份认证技术	66,81
	长程攻击	由于 PoS 中矿工挖矿需要付出的代价极低，具有权益优势的节点有可能从创世块开始产生一条完全不同的区块链分叉。	从创世区块开始产生的最长合法链，加强对节点身份的认证。	67
	DDos 攻击	攻击者设法得到互联网上的大量主机的用户账号，然后设法秘密地在这些主机上安装从属程序（slave program），并在同一时间发起攻击使主机迅速瘫痪。	基于机器学习的解决方案，能够检测流量中的异常请求；基于统计数据的解决方案，旨在通过分析和收集与流相关的统计数据来保护网络。	68,82,83,84
	区块截留攻击	通过委派部分矿工加入到目标矿池贡献无效的工作量，分得目标矿池的奖励,以追求矿池整体获得更高的奖励。	用零行列式策略（Zero-determinant，ZD）的子策略：设定策略、敲诈策略和宽容策略，优化困境中矿池收益并优化矿池策略选择，从而缓解攻击.	85,86
	渗透博弈攻击	两个节点之间，恶意节点考虑到所有进攻的可能性并切断诚实节点的后路。	节点之间采用有向图博弈，增加信息流的流通。	64,87,88
基于智能合约攻击	The DAO	合约调用时进程停止产生中间状态，攻击者利用该状态重入调用合约发起攻击。	硬分叉是目前区块链唯一可行的重构方式。	51,89
	时间戳依赖攻击	攻击者通过时间戳的产生偏差来控制智能合约的执行结果	增加一位随机值的设置位，将时间戳与随机数相结合的实时传输验证，削弱仅时间戳自身误差造成的漏洞。	
	调用堆栈深度攻击	攻击者故意突破调用栈深度限制，使得合约执行异常。	同一节点的调用合约次数加以控制，设置触发器并记录日志名单。	46,47 49,66
	代码漏洞	智能合约中规定了整数的范围，难以避免变量、中间计算结果越界，导致整数溢出。程序中仅保存异常结果，影响智能合约的执行。	开发人员在开发过程中需严格按照开发规则，合约设计初期与专业法律人士深入讨论敲定方案。MySthril 是一个开源工具，它利用符号执行技术来确定代码中的错误。	
	交易顺序依赖	攻击着故意改变智能合约以改变交易顺序，控制所产生的不同结果。	使用MythX安全分析服务，它可以扫描基于 EVM 的智能合约的漏洞。MythX 通过三个阶段来分析智能合同代码。首先，它需要开发人员提交他们的代码；其次，需要激活一套完整的分析技术；最后，它生成一个分析报告，以显示是否存在任何错误。	10,67
	路由更改	基于 IP 地址的路由更改攻击，	网络协议的设置按照严格的 NIST 网络安全框架执行。或者采用新型路由协议进行传输数据（AODV 路由算法、PIHNSPRA 路由算法）	90，91

5.3未来研究趋势

区块链问世以来一直面临着各种各样的监管问题，无论是自我监管还是第三方协同管理都存在弊端，因此经研究分析得以下三条建议：

检测技术：现存的机器学习和数据挖掘算法可能会侧

重于检测基于区块链交易中的欺诈和发现入侵者的新型应用，通过对人们的交易历史进行分析、监控和检测行为模式，监督机器学习方法，如深度学习神经网络，支持向量马赫数网络和贝叶斯信念网络可能有助于检测离群值行为。

法律法规：各机构、立法者和立法机构应了解、调查和审查区块链技术的机制和影响，并合作开发和实施法律、政策和法规管理程序，以管理区块链技术的使用，这样做可能会催生创新商业模式的新兴点对点经济的安全性和运作。NIST 网络安全框架明确规定区块链网络环境安全，尽管该框架不是专门为区块链技术设计的，但其标准足够广泛，足以涵盖区块链技术，并帮助机构开发识别和控制影响区块链技术的风险的管理系统和流程。

广泛应用：在此提出一种新的思想，除非得到大多数社会技术的广泛接受和采用，否则该技术中固有的任何机制和保护都不能发挥作用。虽然只有一小部分交易发生并记录在区块链中，但攻击者、恶意分子和罪犯仍然可以通过其他渠道获得想要的信息。因此，将区块链广泛应用于各大领域对成功地预防各类型的攻击至关重要。

6 总结与展望

随着区块链技术快速发展，区块链具有数据去中心化管理、不可篡改和安全性高等优点，使区块链引起了政府、企业和学者的广泛关注，并在一些领域得到成功应用。但是区块链为去中心化平台提供技术的同时，自身系统漏洞所带来的安全问题也越演越烈。本文基于以上问题，从区块链关键技术和漏洞分类分析入手，通过文献分析和综合研究得到以下结论：

总结了区块链自发展以来的国内外研究现状以及漏洞演变趋势，发现应用程序、操作系统及数据库的安全问题依然严重，通过分析研究文献对目前区块链系统存在漏洞的分类得出实例分析。接着归纳了区块链的概念，同时对密码学、默克尔树、对等节点（P2P）、共识机制以及智能合约等区块链关键技术进行深入分析，总结了各自的工作原理及其优缺点。尤其是对目前众多平台主流的区块链共识算法应用效果进行对比分析，总结各种关键技术适宜的应用场景，以方便用户参考借鉴。

对区块链的数据存储与交互、隐私保护、资源分配、漏洞攻击等四个方面进行分析总结，归纳并指出了区块链系统在安全方面存在的亟需解决的问题，对区块链系统的漏洞攻击进行归纳，指出分叉攻击、基于密码学攻击、基于共识算法攻击、基于智能合约攻击以及从系统之外发起的攻击等五类可被利用的漏洞攻击，并对区块链系统存在的安全漏洞攻击进行分类，从大量文献中归纳分析得出各个攻击的类别定义以及可能有效的解决方案，为用户提高区块链安全性指明方向。以上存在的四个方面问题对区块链系统存有极大的安全威胁，务必加以重视和防范。

结合以上问题，本文建议在未来系统设计的过程中需更加完善安全体系，从算法到系统整体提升区块链系统的安全性，其中对于数据的存储效率还需要进一步的提升，毫秒级的交易额数量直接影响着区块链系统的性能，因此需要提供更高效的共识机制，对隐私数据的保护需要增加访问控制的功能以防止第三方恶意入侵，以及系统对资源的分配可采用云端服务器或 IPFS 技术，因此未来还需对区块链内部系统做进一步完善，为区块链技术发展和平台开发提供更加准确、安全、标准的技术，以防止各类漏洞对区块链系统的攻击，进而提升区块链系统的工作效率。

参考文献

[1]刘敖迪，杜学绘，王娜，等.区块链技术及其在信息安全领域的研究进展[J]. 软件学报,2018,29(7):2092-2115.

Liu Ao-Di, Du Xue-Hui, Wang Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, **29**(7):2092-2115 (in Chinese)

[2] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].available: https://bitcoin.org/bitcoin.pdf, 2009.

[3]Walport M. Distributed ledger technology: beyond blockchain[EB/OL]. available:https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain,October 5, 2018.

[4]Ministry of Industry and Information Technology. Chinese blockchain technology and application development white paper 2016 [EB/OL]. available: http://www.fullrich.com/Uploads/article/file/2016/1020/580866e374069.pdf, October 5, 2018.

[5]赛迪报告：《2019-2020 中国专利白皮书》.[EB/OL].https://baijiahao.baidu.com/s?id=1684115088555403329&wfr=spider&for

=pc.

[6]袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016,42(4): 481-494.

Yuan Yong, Wang FeiYue. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.(in Chinese)

[7]Creydt M, Fischer M. Blockchain and more – Algorithm driven food traceability[J]. Food Control, 2019, 105: 45 – 51.

[8]Olsen P, Borit M. The components of a food traceability system[J]. Trends in Food Science & Technology, 2018, 77: 143 – 149.

[9]Yuan Y, Wang F Y. Blockchain and cryptocurrencies: model, techniques, and applications[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9):1421−1428.

[10]Z. Wan, D. Lo, X. Xia, et al. Bug Characteristics in blockchain systems: A large-scale empirical study[C]. 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), Buenos Aires, Argentina, 2017, 413-424.

[11]Maesa D D F , Mori P . Blockchain 3.0 applications survey[J]. Journal of Parallel and Distributed Computing, 2020, 138:99-114.

[12]钱建平，吴文斌，杨 鹏. 新一代信息技术对农产品追溯系统智能化影响的综述[J]. 农业工程学报，2020，36(5)：182 – 191.

Qian Jianping, Wu Wenbin, Yang Peng. Review on agricultural products smart traceability system affected by new generation information technology[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2020, 36(5): 182 – 191. (in Chinese with English abstract)

[13]国家信息安全漏洞共享平台.[EB/OL].（2020）. https://www.cnvd.org.cn

China national vulnerability database. [EB/OL].（2020）. https://www.cnvd.org.cn

[14]Wan Z , Lo D , Xia X , et al. Bug characteristics in blockchain systems: A large-scale empirical study[C]// IEEE/ACM International Conference on Mining Software Repositories. ACM, 2017.

[15]Ms A,Mrj B,Nss C,et al. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues[J]. Journal of Network and Computer Applications, 2021,178(1):10-29.

[16] Wong D R, Bhattacharya S,Butte A J. Prototype of running clinical trials in an untrustworthy environment using blockchain [J]. Nature Communications, 2019, 10(1):1-8.

[17]王芳，赵洪，马嘉悦,等. 数据科学视角下数据溯源研究与实践进展[J]. 中国图书馆学报, 2019, 45(5):79-100.

WANG Fang，ZHAO Hong，MA Jiayue，et al. Research and practice progress of data provenance from the perspective of data science[J]. Journal of Library Science in China, 2019, 45(5): 79-100.(in Chinese)

[18]张奥,白晓颖.区块链隐私保护研究与实践综述.软件学报[J], 2020,31(5):1406−1434.

Zhang A, Bai XY. Survey of research and practices on blockchain privacy protection[J]. Ruan Jian Xue Bao/Journal of Software, 2020,31(5):1406−1434.(in Chinese)

[19]Ruiguo Yu,JianrongWang,Tianyi Xu,et al. Authentication with block-chain algorithm and text encryption protocol in calculation of social network[J].2017,vol. 5, 24944-24951.

[20]Halamka,J.D.,Lippman,A., et al. The potential for blockchain to transform electronic health records. Harv. Bus. Rev. 2017，3 (3), 1–5, [EB/OL]. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

[21]X. Yang, M. Li, H. Yu, et al. A trusted blockchain-based traceability system for fruit and vegetable agricultural products[J]. IEEE,2021, vol. 9, 36282-36293.

[22]魏晓旭，郑佳. 我国区块链研究现状及热点分析[J]. 高技术通讯, 2019, 29(11):1116-1123.

Wei Xiaoxu，Zheng Jia. Research status and hot spot analysis of block-chain in China[J].Chinese High Technology Letters,2019, 29(11):1116-1123.(in Chinese)

[23] Liu Y , Wang K , Yun L , et al. Light chain: A lightweight blockchain system for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6):3571-3581.

[24]D Team. Blockchains Tutorials. Accessed: Aug. 10, 2020. [EB/OL]. Available: https://data-flflair.training/blogs/types-of-blockchain/

[25]Melo C , Dantas J , Pereira P , et al. Distributed application provisioning over Ethereum-based private and permissioned blockchain: availability modeling, capacity, and costs planning[J]. The Journal of Supercomputing, 2021:1-27.

[26]S. A. Bhat, I. B. Sofi and C. -Y. Chi. Edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities[J].IEEE, 2020,vol. 8,205340-205373.

[27]王学龙,张璟. P2P 关键技术研究综述[J]. 计算机应用研究, 2010, 27(3):801-805+823.

Wang X L, Zhang J. Survey on peer-to-peer key technologies[J]. Application Research of Computers, 2010，27(3):801-805+823.

[28]W. Zheng, Z. Zheng, X. Chen, et al. NutBaaS: A blockchain-as-a-service platform[J].IEEE Access,2019,vol. 7, 134422-134433.

[29]P. R. Nair and D. R. Dorai, Evaluation of performance and security of proof of work and proof of stake using blockchain[C].2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, 279-283.

[30]黄根,邹一波,徐云.区块链中 Merkle 树性能研究[J].计算机系统应用,2020,29(9):237-243.

HUANG Gen, ZOU Yi-Bo, XU Yun. Performance analysis and research of merkle trees with blockchain[J]. Computer Systems & Applications.2020,29(9):237−243.(in Chinese)

[31]Ray P P , Kumar N , Dash D . BLWN: Blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare[J]. IEEE Systems Journal,2020, PP(99):1-12.

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

Yuan Yong, Ni Xiao-Chun, Zeng Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011−2022.(in Chinese)

[33]Nguyen G T , Kim K . A survey about consensus algorithms used in Blockchain[J]. Journal of Information Processing Systems, 2018, 14(1):101-128.

[34]郭上铜,王瑞锦,张凤荔.区块链技术原理与应用综述[J].计算机科学,2021,48(2):271-281.

GUO Shang-tong,WANG Rui-jin ZHANG Feng-li, Summary of principle and application of blockchain[J].Computer Science, 2021,48(2):271-281.(in Chinese)

[35]Dwork C, Naor M. Pricing via processing or combatting junk mail[C]. Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA: Springer-Verlag, 1992. 139−147.

[36]Jakobsson M, Juels A. Proofs of work and bread pudding protocols (extended abstract)[J]. Secure Information Networks. Boston, MA, Germany: Springer, 1999. 258−272.

[37]Castro M, Liskov B. Practical Byzantine fault tolerance[C]. Proceedings of the 3rd Symposium on Operating Systems Design and Implementation[C]. New Orleans, USA: USENIX Association, 1999: 173−186.

[38]Proof of stake [EB/OL]. available: https://en.bitcoin.it/wiki/Proof of Stake, April 11, 2018.

[39]Sunny K,Scott N.PPcoin：Peer – to – Peer CryptoCurrency with Proof-of-Stake [EB/OL].https://decred.org/research/king2012.pdf,2012-8-19.

[40]A. Gervais, G. O. Karame, K. Wüst, et al. On the security and performance of proof of work blockchains, in Proc[C]. ACM SIGSAC Conf. Comput. Commun. Secur., in Computer and Communications Security. New York, NY, USA: Association for Computing Machinery, 2016, 3–16.

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

[42]I. T. Javed, F. Alharbi, T. Margaria, et al. Qureshi, PETchain: A blockchain-based privacy enhancing technology[J]，IEEE, 2021，vol. 9, 41129-41143.

[43]孟吴同,张大伟.Hyperledger Fabric 共识机制优化方案[J/OL].自动化学报,2020, 46: 1-14.

Wu-Tong M, Da-Wei Z. Optimization scheme for hyperledger fabric consensus mechanism[J]. Acta Automatica Sinica, 2020, 46: 1-14.(in Chinese)

[44] Androulaki E, Manevich Y, Muralidharan S, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//the Thirteenth EuroSys Conference, 2018.

[45]S. Wang, C. Huang, J. Li, et al.Decentralized Construction of knowledge graphs for deep recommender systems based on Blockchain-powered smart contracts[J].IEEE, 2019,vol. 7,136951-136961.

[46]Vacca Anna et al. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges[J]. Journal of Systems and Software, 2021: 110891-110909.

[47]Loi Luu, Duc-Hiep Chu, Hrishi Olickel,et al. Making smart contracts smarter[C]. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 254–269.

[48]王璞巍，杨航天，孟佶,等. 面向合同的智能合约的形式化定义及参考实现[J]. 软件学报, 2019, 30(9):44-55.

Wang PW, Yang HT, Meng J, et al. Formal definition for classical smart contracts and a reference implementation[J]. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2608−2619.(in Chinese)

[49]S. Sayeed, H. Marco-Gisbert and T. Caira. Smart contract: attacks and protections[J]. IEEE, 2020,vol. 8, 24416-24427.

[50]ETHEREUM. Solidity[EB/OL].[2021-04-09]. https://docs.soliditylang.org/en/latest/

[51]Liu L , Zhou S , Huang H , et al. From technology to society: an overview of blockchain-based DAO[J].IEEE Open Journal of the Computer Society, 2021,1-11.

[52]Mccorry P , Heilman E , Miller A . Atomically trading with roger: Gambling on the success of a hardfork[C]//European Symposium on Research in Computer Security International Workshop on Data Privacy Management Cryptocurrencies and Blockchain Technology. 2017.

[53]Newsome J , Shi E , Song D X , et al. The sybil attack in sensor networks: analysis & defenses[J]. IEEE, 2004,259-268.

[54]Karame G O , Androulaki E , Capkun S . Double-spending fast payments in Bitcoin[C]//Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[55]Giuseppe Franzè,Francesco Tedesco,Domenico Famularo. Resilience against replay attacks: A distributed model predictive control scheme for networked multi-agent systems[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(3):628-640.

[56]Moustapha B A . The effect of propagation delay on the dynamic evolution of the Bitcoin blockchain[J]. Digital Communications and Networks, 2020, 6(2):157-166.

[57]Yizhong Liu, Yiming Hei, Tongge Xu, et al. An evaluation of uncle block mechanism effect on ethereum selfish and stubborn mining combined with an Eclipse attack[J],2020,vol. 8, 17489-17499.

[58]Kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems[C]//Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 1999.

[59]Habib M , Mehmood T , Ullah F , et al. Performance of WiMAX Security Algorithm (The Comparative study of RSA Encryption Algorithm with ECC Encryption Algorithm)[M]. IEEE, 2009,108-112 .

[60]杨波.现代密码学[M].北京：清华大学出版社，2017.

[61]Abulkasim, H., Mashatan, et al. Secure multiparty quantum key agreement against collusive attacks[J]. Scientific Reports,

2021,11,1-8.

[62]万武南, 陈豪, 陈俊,等. 区块链的椭圆曲线密码算法侧信道安全分析[J]. 应用科学学报,2019, v.37(2):57-66.

Wan W N, Chen H, Chen J, et al. Side channel security analysis of elliptic curve cryptography of blockchain[J]. Journal of Applied Sciences, 2019,37(2),57-66.

[63]Gobin L. A refined power analysis attack on elliptic curve cryptosystems[C]//Proceeding of Public Key Cryptography, Springer-Verlag, 2003: 199-211.

[64]Aleksey K. Fedorov, Evgeniy O. Kiktenko,et al. Quantum computers put blockchain security at risk[J]. Nature, 2018, 568, 465-467.

[65]Raussendorf R, Briegel H J. A One-way quantum computer[J]. Physical Review Letters, 2001, 86(22):5188-91.

[66]C. Ye, G. Li, H. Cai, Y. Gu and A. Fukuda, Analysis of security in blockchain: Case study in 51%-attack detecting[C]. 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 2018,15-24.

[67]Motter A E , Nishikawa T , Lai Y C . Range-based attack on links in scale-free networks: are long-range links responsible for the small-world phenomenon?[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2002, 66(6):065103.

[68]Mirkovic J , Prier G , Reiher P . Attacking DDoS at the source[C]//IEEE International Conference on Network Protocols. IEEE Computer Society, 2002:312-321.

[69]约翰·范本特姆, 刘奋荣. 图博弈的设计与模态逻辑的发展[J]. 清华大学学报(哲学社会科学版), 2019, 34(2): 131-139.

Johan van Benthem，Liu Fenrong.Interaction Between Graph Game Design and Modal Logics[J].Journal of Tsinghua University (Philosophy And Social Sciences), 2019, 34(2): 131-139. (in Chinese)

[70]王甜甜, 于双元, 徐保民. 基于策略梯度算法的工作量证明中挖矿困境研究[J]. 计算机应用, 2019, 39(5):1336-1342.

WANG Tiantian, YU Shuangyuan, XU Baomin. Research on proof of work mining dilemma based on policy gradient algorithm[J]. Journal of Computer Applications, 2019, 39(5): 1336-1342.(in Chinese)

[71]韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报 , 2019, 45(1): 206-225.

Han Xuan, Yuan Yong, Wang Fei_Yue. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225.(in Chinese)

[72]Giliazov R.R. Blockchain Protocol Study[J]. Sovremennye informacionnye tehnologii i IT-obrazovanie=Modern Information Technologies and IT-Education. 2019,15(1):190-199.

[73]Xu, Jennifer J. Are blockchains immune to all malicious attacks?[J]. Financial Innovation, 2016, 2(1):1-9.

[74]Furnell S M, Bakhshi T, Papadaki M, et al. Social engineering: assessing vulnerabilities in practice[J]. Information Management & Computer Security, 2013, 17(1):53-63.

[75]Zeng S, Ni X C, Yuan Y, et al. A bibliometric analysis of blockchain research[C]. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV 18). Changshu, China:IEEE, 2018: 102−107.

[76]武继刚, 刘同来, 李境一,等. 移动边缘计算中的区块链技术研究进展[J]. 计算机工程, 2020(8):1-13.

WU Jigang,LIU Tonglai,LI Jingyi. Research progress on blockchain technology in mobile edge computing[J].Computer Engineering. 2020(8):1-13.

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

[78]张中霞，王明文.区块链钱包方案研究综述[J].计算机工程与应用，2020，56（6）：28-38.

ZHANG Zhongxia, WANG Mingwen. Survey on blockchain wallet scheme[J]. Computer Engineering and Applications, 2020, 56（6）：28-38.

[79]W. Du, J. Deng, Y. S. Han,et al. A pairwise key pre-distribution scheme for wireless sensor networks[J].In ACM CCS 2003,2003, 42-51.

[80]L. Eschenauer,V. D. Gligor. A key-management scheme for distributed sensor networks[J]. In Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002, 41-47.

[81] Sri P, Bhaskari D L. Blockchain technology for secure medical data sharing using consensus mechanism[J]. Materials Today: Proceedings, 2020.1-8

[82] Eliyan L F, Pietro R D. DoS and DDoS attacks in software defined networks: A survey of existing solutions and research challenges-science direct[J]. Future Generation Computer Systems, 2021, 122:149-171.

[83]A. Shoeb, T. Chithralekha, Resource management of switches and Controller during saturation time to avoid DDoS in SDN[J], in: Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016, 2016, 152–157.

[84]K. Giotis, G. Androulidakis, V. Maglaris.A scalable anomaly detection and mitigation architecture for legacy networks via an OpenFlow middlebox[J], Int. J. Appl. Eng. Res. 2015, 9, 1958–1970.

[85]刘子州，程晓荣，王治博．区块链中区块截留攻击的研究与分析．计算机工程与应用.2020.1-17.

LIU Zizhou, CHENG Xiaorong, WANG Zhibo.Research and analysis of block withholding attack for blockchain[J]. Computer Engineering and Applications.2020.1-17.

[86]张茹．基于博弈论的区块截留攻击缓解策略的研究[D].内蒙古大学, 2019.

Zhang R. Research of block withholding attack mitigation strategy based on game theory[D].Inner Mongolia University，2019.

[87] Zhao C, Wang Q, X Liu, et al. Reinforcement learning based a non-zero-sum game for secure transmission against smart jamming[J]. Digital Signal Processing, 2021, 112(12): 103002.

[88] Cai X, Wang B, Cao Z, et al. Game control of attack and defense in cyber physical system[J]. Procedia Computer Science, 2021, 187(10):488-494.

[89] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (SoK)[C]//International Conference on Principles of Security & Trust. Springer, Berlin, Heidelberg, 2017.

[90] Kumar A, Varadarajan V, Kumar A, et al. Microprocessors and Microsystems xxx (xxxx) xxx Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm[J]. Microprocessors and Microsystems, 2020, 80.

[91] Rajendran N, Jawahar P K, Priyadarshini R. Cross centric intrusion detection system for secure routing over black hole attacks in MANETs[J]. Computer Communications, 2019, 148(Dec.): 129-135.