计算机科学
COMPUTER SCIENCE

**区块链技术的研究及其发展综述**

傅丽玉，陆歌皓，吴义明，罗娅玲

引用本文

傅丽玉，陆歌皓，吴义明，罗娅玲. 区块链技术的研究及其发展综述[J]. 计算机科学, 2022, 49(6A): 447-461.

FU Li-yu, LU Ge-hao, WU Yi-ming, LUO Ya-ling. Overview of Research and Development of Blockchain Technology[J]. Computer Science, 2022, 49(6A): 447-461.

---

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210600214

# 区块链技术的研究及其发展综述

傅丽玉　陆歌皓　吴义明　罗娅玲
云南大学软件学院　昆明 650000
(2276215853@qq.com)

**摘　要**　区块链被称为下一代的价值互联网,是一种去中心化新兴加密货币的基础系统架构。自2008年中本聪提出区块链一词以来,区块链因其本身的不可篡改、可溯源、去中心化等特性而逐渐受到人们的广泛关注,其中的两个典型代表为比特币区块链系统和以太坊区块链系统。但是在目前已有的文献资料中,大多是将已有的区块链技术应用到实际生活中,而对区块链的底层的实现介绍较为模糊,应将区块链从实际的应用中抽离出来,并通过比特币区块链系统和以太坊区块链系统的设计思想及其关键技术来了解区块链的工作原理。文中主要从区块链设计的密码学原理、共识算法、数据存储结构等方面来详细介绍区块链技术的基础架构,并针对比特币白皮书和以太坊黄皮书中较模糊的概念进行了补充,从而为后面的读者提供更加深入的研究参考。最后,介绍了区块链目前的应用现状和展望。

**关键词**:区块链;比特币;智能合约;分布式共识;区块链应用;工作量证明;权益证明
**中图法分类号**　TP309;TP311.1

## Overview of Research and Development of Blockchain Technology

FU Li-yu,LU Ge-hao,WU Yi-ming and LUO Ya-ling
Software College,Yunnan University,Kunming 650000,China

**Abstract**　Blockchain is called the next-generation Internet of Value,which is a basic system architecture for emerging decentralized cryptocurrencies. Since Satoshi Nakamoto proposed the term blockchain in 2008,it has gradually received widespread attention due to its immutability,traceability,and decentralization features. Two of the representatives are the Bitcoin block Chain system and Ethereum blockchain system. However,in the current literatures,most of the existing blockchain technology is applied to real life while the introduction of the underlying implementation of the blockchain is relatively vague. To this end,the blockchain should be separated from the actual one,and the working of the blockchain can be understood through the design ideas and key technologies of the Bitcoin blockchain system and the Ethereum blockchain system. The article mainly introduces the infrastructure of blockchain technology including the cryptographic principles,consensus algorithms,data storage structure and other aspects. Further the supplements about ambiguous concepts in the Bitcoin white paper and the Ethereum yellow paper are presented as well,which can provide more deeply research for readers later. Finally,the current application status and prospects of blockchain are discussed.

**Keywords**　Blockchain,Bitcoin,Smart contracts,Distributed consensus,Blockchain applications,Proof of work,Proof of stake

## 1　引言

早年,Diffie W 和 Hellman M 两位密码学界的大师发表了论文《密码学的新方向》[1],该文讨论了现代密码学的两个发展方向,即加密和认证。其覆盖了未来几十年密码学所有可能的新的进展领域,包括非对称加密、椭圆曲线算法、哈希等手段,奠定了迄今为止整个密码学的发展方向,也对区块链的技术和比特币的诞生起到了决定性作用。在同时期发生了另外一件看似完全不相关的事情——哈耶克发表了他人生中最后一本经济学方面的专著:《货币的非国家化》[2-3],其中心思想可以概括为"货币如果可以完全地实现市场化会更好"。作者认为允许个人发行货币,可以形成一种竞争优胜劣汰,而不是由国家垄断。货币的非国家化提出的非主权货币、竞争发行货币等理念,可以说是去中心化数字货币的精神指南。

区块链作为下一代的价值互联网[4],是比特币的核心以及技术基础。2008年11月1日,中本聪(Satoshi Nakamoto)发表了《比特币:一种点对点的电子现金系统》[5]以后,区块链一词进入人们的视野并受到人们的广泛关注。区块链技术从它诞生之日起通过一些分布式共识算法及密码技术,使其不需要可信第三方便可实现系统的稳健运行[6-9],区块链自2009年起在没有认可超级管理员和专门的系统维护人员的情况下稳定运行至今,可证明其安全性和稳定性。

目前已有不少的研究学者投身于区块链的建设中,并在不同领域取得了不错的成就,如将区块链技术应用于金融领域,这也是区块链一词最早被提出的领域,也是区块链技术发展时间最长、最成熟的一个领域。比特币的上线使大家熟知了区块链这种去中心化的账本[10],在不需要专门的管理机构介入的同时仍然能够有条不紊地运行。但比特币的一个致命的弱点就是交易发布到区块链上的时间过长,一个合法交易要想成功发布在区块链上形成全网的共识至少需要10min。

通信作者:陆歌皓(glu@ynu.edu.cn)

这对于实体世界的交易而言非常不现实，这就将比特币的发展限制在了网络世界中。为了缓解这一矛盾，随之诞生了以太币、莱特币等一系列数字货币。去中心化的特性指区块链技术具有不可篡改的特性，在这个信息化的时代这个特性正好可以解决一些其他领域的冲突，例如，将区块链技术与现代的医疗结合进行医疗信息的资源共享、区块链技术与物联网结合实现产品采购生产以及物流的溯源等。但是这些都只是将区块链技术直接应用于实体世界，对于一些区块链底层的技术实现并没有关注。因此，本文将区块链从实际的应用中抽离出来，从区块链的底层的原理以及实现来对区块链技术进行剖析。

本文第 1 节介绍本文的背景、动机和目的；第 2 节提到区块链发展的概述；第 3 节分析区块链所涉及的相关技术；第 4 节介绍区块链在目前的一个应用前景；最后总结全文并展望未来。

## 2 区块链概述

区块链一词最早出现在中本聪发表的《比特币：一种点对点的电子现金系统》一文中，为了解决在现实社会中进行点对点技术实现的电子现金系统中，需要通过可信第三方的金融机构来保证交易的安全可靠，中本聪在论文中指出，在目前已有的技术手段中，可以通过数字签名的方式解决需要可信任第三方金融机构去保证交易的安全可靠这一问题，但是数字签名并不能保证在进行支付时不发生双重支付，区块链的产生正是针对这一问题而提出的解决方案。在区块链中，通过随机的散列对全部交易加上时间戳，并将它们合并在一个不断延伸的基于随机散列的工作量证明的链条中作为交易记录，除非重新完成所有的交易的工作量证明，否则形成的交易记录将不可更改。其中，最长的区块的链条不仅被认为是提交交易记录发生时间先后顺序的证明，而且被看作是来自 CPU 计算能力最大的池[11]，只要网络中的大多数节点没有联合起来进行攻击，那么诚实的节点就一定会比恶意的节点生成的链条更长，即可以保证在区块链中交易的不可篡改。由此诞生了以中本聪为核心人物的区块链，在 Swan 等[12]的论文中称此时的区块链为区块链 1.0。区块链 1.0 被称为可编程货币，主要是以比特币为核心。它主要围绕比特币区块链展开诸多业务及周边服务，如钱包、工具、交易所、挖矿、矿机业务等。在 1.0 时代，人们过多地关注建立在区块链技术上的虚拟货币，关注它们的价值、获得比特币的途径以及利用比特币进行交易的方式。随着越来越多人关注比特币，使用比特币作为支付手段产生的交易也越来越多。因为在比特币的系统中区块的大小固定，并且产生一个区块的时间固定在 10 min 左右，导致利用比特币转账的速度越来越慢，再加上比特币只用于支付、流通等功能，使得比特币不能被更广泛地应用到生活当中，带来了些许不便。针对此问题，人们在区块链 1.0 的基础上增加了一套系统，即可以自动执行一系列操作标志着这套系统为“智能合约”。智能合约的产生，标志着区块链进入了以以太坊区块链为代表的区块链 2.0 时代。

区块链 2.0 时代是指智能合约开发和应用，智能合约与电子货币结合，也给金融领域提供了更加广泛的应用场景。2.0 时代是通过分叉比特币区块链或构建另一套基于区块链技术而创建的更广泛的协议并生成内在的新的代币。智能合约是一套数字形式定义的承诺，合约的参与方可以在上面执行这些承诺的协议。区块链 2.0 时代以以太坊区块链为代表，以太坊区块链建立了一套更为灵活而通用的框架系统，在协议层面和应用层面的创新使开发者能够轻松地在一个全新的应用程序集上创建新的协议，使用智能合约在其区块链上构建新的功能。以太坊区块链的核心与比特币区块链系统本身没有本质区别，不同之处在于以太坊区块链智能合约的实现，使得以太坊区块链的编程是图灵完备的，以太坊区块链支持了合约的编程，使得区块链技术不仅仅用于发行代币和转账交易，而且可以提供一些商业的和非商业的应用场合，如进行网上拍卖等；其次，以太坊区块链的出块规则和奖励机制也有所不同，我们将会在后面进行详细的介绍。

未来的区块链 3.0 可能不仅仅局限于金融领域，而是一个生态的、多条链构成的网络，覆盖人类社会生活的方方面面，包括在司法、医疗、物流等各个领域。目前，我们并未有一个准确的规则去划分区块链 3.0 时代。区块链 3.0 并没有像比特币和以太坊区块链这样的典型代表，因此无法像区块链 2.0 一样以智能合约为核心代表去划分区块链 3.0。总的来说，区块链 3.0 是为了解决各行各业相互信任的问题与数据在传输过程中安全技术的落地与实现。

## 3 核心技术

### 3.1 区块链

#### 3.1.1 比特币的密码学原理

比特币被称为加密货币，但是实际上加密货币并不是加密的，比特币的交易信息在区块链中是完全公开的。所有的交易记录、转账金额、用户的账户地址等都被公布在区块链上，即所有的用户都可以登录网站去查看区块链上的任何信息。因此，为了实现区块链的安全性，在设计区块链时应该考虑以下 3 个方面的问题。

(1)抗哈希碰撞

哈希碰撞指将两个不同的输入值，经过哈希函数计算得到的哈希值相同，即有两个数 $x$ 和 $y$，其中 $x!=y$ 经过哈希计算得到 $H(x)=H(y)$。在区块链中采用的哈希算法是 SHA256，即输出空间为 $2^{256}$，虽然输入空间是无限大的，根据鸽笼原理可知，必然存在两个不同的输入会映射到同一个输出的情况，但是，我们并没有一个高效的算法人为地去制造哈希碰撞。通过蛮力去暴力地制造哈希碰撞，在现有的计算机的计算能力的条件下是不可行的。因此采用哈希 SHA256 的算法可以抵抗哈希碰撞。此性质在区块链中可以用于验证区块链中区块是否被篡改，对所有的交易信息取哈希形成信息摘要。当验证这些信息是否被修改时可以对这些交易信息再取哈希，将两次的哈希结果进行对比，从而判断交易是否被修改。

(2)原哈希值隐藏

哈希函数的另一个重要的性质就是可以隐藏原哈希值，即哈希函数是单向的。当输入的空间足够大并且输入空间的取值分布均匀时，假设有一个消息 $x$，消息 $x$ 通过哈希函数计算得到消息摘要 $H(x)$。这个过程非常容易，若想要由 $H(x)$ 去获得原消息的值 $x$ 则非常困难，即 $P(x\rightarrow H(x))\rightarrow 1$，$P(H(x)\rightarrow x)\rightarrow 0$。在实际的应用中，输入的空间可能有限，在输入结果有限的情况下可以在其后面增加一个伪随机数，

使输入空间足够大，这样便可以避免使用暴力的方法去得到某一哈希摘要的原哈希值。

(3)相关性不可预测

给定一个散列函数 $H$，它从用户那里获取一些输入 $x$，并产生输出 $H(x)$，一个好的“Puzzle friendly”算法不会显式输入 $x$ 和输出 $H(x)$之间的任何可预先确定的相关性。也就是说，你不能选择某个 $x$，寄希望于返回某个 $H(x)$。在实际的区块链网络中，接受低于某个域值的块，需要此块的哈希值满足当前网络难度的域值。这时用户不应该根据任何类型的预期的输出值来选择输入，整个输入值范围应该有相同的机会返回所需的输出，否则，用户可能会区分某些范围内的输入值，从而缩小他们的搜索范围，并增加他们找到有效输出的机会。允许用户进行“有根据的猜测”将破坏 POW 加密货币所需的功能。

### 3.1.2 比特币的数据结构

区块链在本质[13]上是一个由区块构成的链表。每一个区块都包含当前区块的前一个区块的哈希指针，最后一个区块的哈希指针保存在系统中，以备后面产生的新区块使用。这样做的一个好处在于只要有最后一个区块的哈希指针的值，便可以验证该区块链中整条链的哈希值从而验证数据的正确性。其形式如图 1 所示。

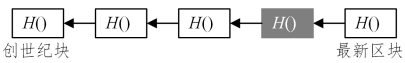


图 1 区块链结构示意图

Fig. 1 Blockchain structure diagram

基于以上性质，区块链中的节点可以不保存整个区块链的所有内容，当需要验证某一交易是否存在或者有效时，只需要通过当前的哈希值向前进行验证即可。如果存在恶意节点，那么验证哈希值是不会通过的，这是由区块链抗哈希碰撞的性质所决定的。

区块链中所有的交易记录的存储会形成一棵 Merkle 树[14]。Merkle 树和普通的树的结构唯一的不同点在于，Merkle 树使用的是哈希指针而不是普通指针。哈希指针不仅存储了与普通指针一样的结构体的起始地址，还存储了当前的哈希值。这样做的好处是可以根据根哈希值去验证整棵树中所有交易信息的正确性。在比特币中，每个区块与区块之间是通过哈希指针连接在一起的，每个区块由两部分组成，分别为区块的块头和区块的块体。区块头包含当前块的根哈希值、随机数 nonce、难度值 target 等；区块体则包含交易列表以及交易的哈希指针构成的 Merkle 树。其具体形式如图 2 所示。

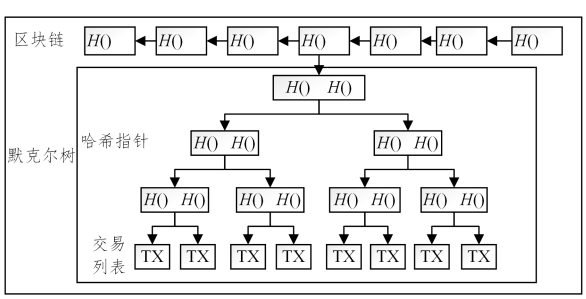


图 2 Merkle 树的数据结构

Fig. 2 Merkle tree data structure

当某个用户想要证明某一交易信息确实存在区块链的 Merkle 树中，可以从根节点逐步往上去验证哈希指针的值是否正确，如果哈希指针的值并无异常则说明该交易确实在区块链中。值得注意的是，如果想要证明某一交易不在 Merkle 树中，那么它的时间复杂度会是线性级别的，因为事先我们不能确定某一交易会存在哪个位置上，所以需要遍历一整棵 Merkle 树才能肯定某个交易不存在，而遍历整棵 Merkle 树的时间复杂度是线性级别的。一种解决的办法是对 Merkle 树中的交易进行一定规则的排序，通过排序 Merkle 树去查找某个交易是否存在时，可以确定该交易所处的范围，从而从根节点逐个验证，这样查找的时间复杂度是对数级别的。其中，哈希指针与普通指针相比具有如表 1 所列的优势。

表 1 哈希指针的优势

Table 1 Advantages of hash pointers

| pointers | Traverse the tree | Link other pointers | Check data |
|---|---|---|---|
| hash pointers | Yes | Yes | Yes |
| ordinary pointers | Yes | No | Yes |

### 3.1.3 比特币的协议

数字货币在本质上是一个文件，文件拥有者可以进行任意的复制和转发。在现实生活中，一张有效的被大家认可的货币是由权威机构也就是由央行发行并带有防伪标识的货币[15]。它的有效性是因为权威机构作为可信第三方被全社会的人认可，在进行商品交易的过程中的价值交换可以得到保证。防伪标识能够使货币的真实性得到保证，使其不能通过非法手段获得。因为实体货币在现实生活中是一个实实在在的东西，其不能进行任意的复制然后使用。在比特币中，我们可以类比现实中的货币，通过权威机构的私钥签名的方法，实现某一个电子货币的有效性。当货币的接收方接受到货币时，我们便可以使用权威机构的公钥进行签名的验证。若验证成功，则说明该货币是由权威机构发行的货币，是一个有效的货币。但是，由于数字货币可以任意的复制和转发的性质人们可以将一份真实有效的货币进行复制，然后分别在不同的场合进行支付，因为该货币是有权威机构签名的有效的货币，所以在不同的场合进行验证时该货币仍是有效的，故都会被接纳。这就会带来一个严重的问题，即一个货币被多次使用。不同于实体货币的是，实体货币在完成一次交易时，持有者手里的货币已经以一定的形式将手中的货币给了服务的提供者，此时用户手中并没有货币了，所以并不存在一个货币被多次使用的情况。为此，我们可以为每个货币添加一个编号，即使复制多份，但编号一样的货币会被认为是同一个币。

基于此就需要权威机构去维护一张巨大表，用于记录每一个货币的编号以及持有者的信息。一旦货币的持有者将自己手中的货币用于交易花出去以后，权威机构需要去更新该货币持有者的信息。这样便可以防止某一货币出现双花甚至多花的情况产生。但是这样会带来的问题是，因为在每一时刻有很多用户会产生许多的交易信息，这样会导致维护这个巨大的表所需要的成本巨大，而且更新的信息太快可能会导致系统超负荷而崩溃。这是一个中心化的方案，其在理论上是可行的。

比特币的目标是实现一个去中心化的数字货币系统[15]。但在去中心化的货币体系中，没有权威机构去管理和维护货币的发行量、辨别货币的真伪以及货币是否被花出去过，因此

需要利用区块链的性质来解决比特币面临的这些挑战。在区块链中，比特币的产生是通过矿工挖矿产生的，每当矿工通过不断尝试随机数得到符合当前网络难度要求的区块时，矿工便获得了铸币权也称为出块奖励，这是区块链系统中，比特币产生的唯一来源。在区块链系统中为了防止比特币双花甚至多花的情况，在每一笔交易中都需要指出该交易中使用的比特币的来源，以及该笔比特币接受方公钥的哈希值即地址。这样当矿工进行打包交易时，便可以通过哈希指针去查看某一比特币的来源，以及该比特币在传输的过程中是否已经被使用过了。具体如图 3 和图 4 所示。

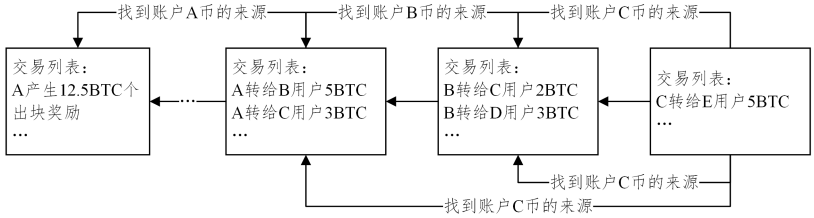


图 3 正常交易处理过程

Fig. 3 Normal transaction processing

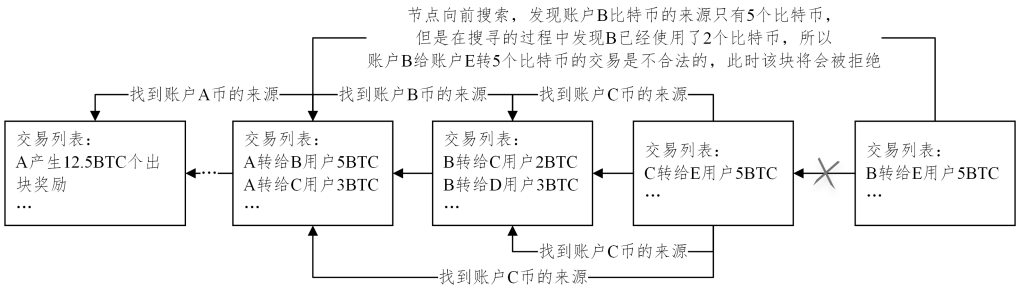


图 4 异常交易处理过程

Fig. 4 Abnormal transaction processing process

由图 3、图 4 可知，基于区块链的比特币可以防止一个币出现双花的可能。传统货币与数字货币的区别如表 2 所列。

表 2 传统货币与数字货币

Table 2 Traditional currency and digital currency

| currency | Copy | Whether to hold if it has been spent | Savetable |
|---|---|---|---|
| digital currency | Yes | Yes | Yes |
| traditional currency | No | No | No |

在区块链中，账号通过随机产生公私钥对的方式产生。账号的注册是随机的，并不需要权威机构去授权，每个合法账户都可以发布交易。那么在区块链的诸多交易中，怎样才能将交易打包进区块链中并被所有的节点接受。目前使用的分布式共识协议有 Paxos 协议，该协议一旦达成共识便是全部节点的共识。在区块链系统中，假设大多数的节点都是好的节点，要实现节点的共识，一种想法就是进行投票，因为在区块链中大多数的节点都是好的节点，所以我们可以通过投票的方式确定哪个区块可以加入到区块链中，其中的交易被全网承认是真实有效的；又因为，区块链中的账户是用户通过随机产生公私钥对的方式独立产生的，所以，如果有恶意节点大量的产生账户并参与区块链的投票，当账户的数量达到一半及以上时，恶意节点就可以操控投票结果，使区块链中的投票结果失去意义，这被称为“女巫攻击”[16]。为此，区块链设计了一种通过工作量证明(Proof of work)的方式，去产生新区块。矿工通过不断地尝试一个随机数，使该随机数和当前区块的信息一起取哈希值，得到的哈希值的结果满足当前网络的难度要求，即得到一个满足要求的区块。该满足要求的区块便可以发布到区块链中并对发布新区块的矿工给予一定的奖励。

当有两个矿工同时得到一个满足要求的区块并发布到区块链中，这时便会产生一个短暂的软分叉的情况。当软分叉产生时，区块链便继续等待下一个区块的产生，直到有一条链成为最长的链，称为区块链中的最长合法链。原来的分叉中败出的链中的区块将会被舍弃，所有的矿工在更新本地的区块链时便会遗弃该块，只承认最长合法链上的区块。这样一来，每次有新区块产生时，其他的矿工节点只需要验证新区块并更新本地的区块链，便可以形成全网的共识。其中，遇到软分叉时的形式如图 5 所示。

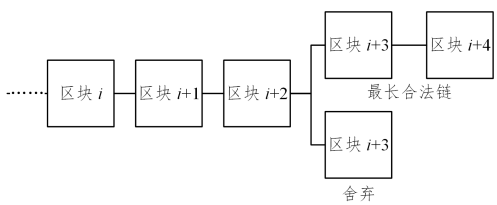


图 5 最长合法链规则

Fig. 5 Longest legal chain rule

### 3.1.4 比特币的实现

区块链被称为去中心化的账本，而比特币则是基于交易的去中心化的账本模式，所以在比特币区块链系统中没有账户，系统并不能显式地显示某一账户上有多少余额。当用户需要进行转账交易时，由于比特币没有账户，因此在进行交易之前需要查找区块链中的全节点，查看当前转账用户中的余额是否满足转账的要求。如果发现余额不足，则该交易是一个非法的交易，将不会打包到区块中，否则打包进区块即完成转账操作。在比特币区块链系统中，每个全节点都需要去维护一个未消费交易输出(Unspent Transaction Outputs，UTXO)集合[17-18]，用于记录所有没有被消费的比特币的来

源，其中一个交易可能有多个输出，故在未消费交易输出集合中需要给出产生交易的哈希值以及是第几个输出，这样可以快速地检测双花攻击。其次，在区块链中比特币一旦被使用，则该比特币的原未消费交易输出应从未消费交易输出集合中删除，表示该比特币已经被使用了。在比特币区块链系统中，假设某条未消费交易输出含有 5 个比特币，但是在实际的交易过程中只使用了 3 个比特币，系统并不是将 5 个比特币直接减去 3 个比特币，而是直接删除 5 个比特币的未消费交易输出记录，然后产生一条 2 个比特币的未消费交易输出存入未消费交易输出集合中。其实现过程如图 6 所示。


图 6 交易处理

Fig. 6 Transaction processing

在比特币区块链系统的交易[19]中，每个区块所有交易金额的输入总是大于或等于所有交易金额的输出，其中存在小部分的差额为矿工在挖矿打包区块时的交易费。这在一定程度上可以防止某些自私的节点只打包与自己相关的交易的情况，可以鼓励矿工在合理的区块大小的范围内尽可能地打包合法的交易到区块链中，实现区块链的稳定运行。

在比特币区块链系统中，实现交易打包到区块链中实际上是一个矿工不断尝试不同的随机数，使得新生成的区块的哈希值满足当前网络难度要求。其中尝试随机数以计算哈希值的过程是一个伯努利实验的过程，在计算过程中表现为无记忆性，即每次计算块的哈希值是否满足当前网络难度值时与之前计算过多少次难度值没有关系，每次算出正确的哈希值的概率是一样的，这样可以保证区块链中的不同计算能力矿工之间的公平性。如果计算哈希值时与计算次数有关，那么计算能力强的矿工在一定程度上会形成不成比例的优势，这会导致计算能力强的矿工挖矿越来越容易，而计算能力弱的矿工挖矿越来越难，并且，出块时间也是服从指数分布的，因为指数分布的无记忆性有利于将出块时间稳定在 10 min 左右。挖矿对于维护比特币的系统安全至关重要。在比特币区块链系统中大部分计算能力掌握在诚实的矿工手中，但是在比特币区块链系统中仍然存在不诚实的节点掌握记账权的情况。假设不诚实的节点想要强制地将不合法的交易写入区块链中，那么诚实的节点将不会接受该节点而从该区块的上一个区块继续挖矿去寻找下一个区块。例如，不诚实的节点发动双花攻击，此时，挖矿便可以通过这种验证的方式，使得不诚实的节点在发布区块时不被其他节点接受，即该节点是无用的节点，发布区块的不诚实的节点将不能获得区块奖励。这里需要注意的是区块的零确认，即用户已经将交易发布到比特币区块链网络中，但是在比特币区块链系统中并没有产生下一个区块，此时交易并没有写入区块链中只是全节点监听到了该交易，此时发动恶意的攻击是比较容易的。

### 3.1.5 比特币的网络

比特币区块链系统的实现过程可以简单地看成是用户将交易发布到比特币区块链网络，矿工将用户的交易打包进区块链的一个过程。在这个过程中比特币区块链系统是运行在应用层的，底层是一个 P2P 的拓扑网络，用于运行比特币协议，在该网络中所有的节点都对等，没有超级节点或者主节点。当矿工想要连接到网络时，只需要知道一个种子节点，即可通过种子节点网络中的其他节点进行通信，向旁边的节点获取自己所需要的信息。各节点之间通过 TCP 协议进行通信，有利于节点之间通信穿透防火墙。想要退出网络时，只需要关闭客户端或浏览器，一段时间后网络没有检测到某一节点的任何活动时该网络会自动忽略该节点。这种网络的特点是简单、鲁棒强，但是并不高效。

交易在比特币区块链网络中传播是通过节点之间的转发实现。当某个节点第一次收到一条交易信息时，它会将该交易信息传播给邻居节点，并记录该节点的信息，表示已经接收过这条交易信息，当再次接收到该交易信息时，节点会自动忽略该交易信息而不会转发给邻居节点，这实现了交易的全网络广播并且防止了同一交易的重复转发导致数据阻塞。等待写入区块链中的交易会被存入全节点的等待写入区块链交易集合中，每次全节点收到一个未打包的交易时，全节点都会将该交易存入区块链的交易集合中，并把交易转发给邻居节点。如果这个交易已经被写入区块链中，则在验证新区块、更新本地全节点数据时将该交易的信息从区块链的交易集合中删除。由于交易在网络的广播过程中存在网络延迟，因此比特币对于区块大小有 $1\times10^6$ 字节的限制，原因是区块在网络上传播需要一定的时间。其次在比特币区块链网络中全节点会先接受先到达该节点的交易，因此存在两个有冲突的合法交易在网络中被不同的全节点接受的情况。这时，这两个有冲突的交易中一旦其中的一个交易被写入区块链中，那么该交易就会从存储该交易的全节点删除并且将存储其冲突交易的全节点中删除。因为，一旦其中一个交易被打包进区块链，那么另一个有冲突的交易将会被视为非法交易，永久不会被打包进区块链中。例如，当发现自己的转账交易出现错误时，可以立即再发布一个与该交易有冲突的转账交易，这有一定的概率挽回自己的损失。

### 3.1.6 比特币挖矿难度的调整

比特币区块链系统采用的哈希算法是 SHA256，故搜索空间的大小为 $2^{256}$。矿工挖矿就是矿工不断的去尝试随机数，使得块头的哈希值满足当前网络的难度阈值的过程。只有块头的哈希值满足当前网络的难度阈值，该区块发布到区块链中才能被全网的矿工节点所接受形成全网共识，矿工才能获取出块的奖励。在比特币区块链系统中平均的出块时间为每 10 min 出一个区块，但是随着现有计算机的计算能力不断增强，每分钟平均可计算的哈希值的次数也不断增加。如果不调整网络中的出块的难度阈值，将会导致出块时间越来越短，因此，挖矿难度应与目标阈值成反比，其中挖矿难度最小为 1，此时的目标阈值是一个趋于无穷的数。它们的关系如下式所示：

$$mining\_difficult=\frac{target}{real\_difficult} \tag{1}$$

其中，$mining\_difficult$ 表示挖矿难度；$target$ 为挖矿难度等

于1时的目标阈值；*real_target* 表示当前网络的目标阈值。

挖矿难度的动态调整有利于稳定系统的出块时间，提高系统的安全性和稳定性。因为，计算机的计算能力不断增强，所产生的矿工出块时间越来越短，将会导致区块链中矿工在同一时刻发布一个区块的概率增大，即区块链中更容易出现软分叉。因为每一个区块都是满足要求的区块，所以这些区块都会被诚实的矿工接受。新区块在比特币区块链网络中传播，由于网络延迟的存在，将会导致不同的矿工可能收到的第一个区块不尽相同。每个新区块都是合法的区块，所有收到新区块的矿工就会沿着他收到的区块的链去继续寻找下一个区块，这样便会分散比特币区块链系统中诚实矿工节点的计算能力，当恶意节点想要发动分叉攻击时，它可能并不需要51%以上的计算能力便可以攻击成功。恶意节点可以集中计算能力去沿着某一条恶意区块链继续寻找下一个区块，而诚实的节点沿着不同的分叉去继续挖矿，在一段时间后恶意节点最终会成为一条最长的合法链，使其攻击成功。因此稳定系统的出块时间有利于比特币区块链系统的安全，实现比特币区块链系统的稳定运行。

在实际的比特币区块链系统中，每2016个区块将会调整一次目标阈值，大概14天调整一次，其调整方式为：

$$target\_threshold=\frac{real\_time}{expect\_time} \tag{2}$$

其中，target_threshold 为目标阈值；real_time 表示最新产生的2016个区块期待花费的时间；expect_time 表示产生2016个区块期待花费的时间。

其中，产生2016个区块期待花费的时间是一个固定值即 $2016*10=20160$ min。当最新产生的2016个区块所花费的实际时间大于20160 min时，即当前的网络阈值太小，挖矿的难度太大，需要调整比特币区块链系统的挖矿难度。调整过程为，通过上面的公式得到一个大于1的目标阈值，再代入式(1)中，除以一个大于1的值，此时比特币区块链网络的难度阈值减小。反之，得到一个小于1的目标阈值，再代入式(1)中，除以一个小于1的值，此时比特币区块链网络的难度阈值增大。在实际的应用中，不管是上调或者下调目标阈值都有一个4倍的上下限，这是为了防止比特币区块链网络因为某些原因而导致比特币区块链网络出块时间出现异常波动的情况。并且这些原则是写入了区块链的代码中，所以在比特币区块链网络中所有的矿工节点都会遵守该规则。

#### 3.1.7 比特币中挖矿

在比特币区块链系统中，矿工挖矿的过程实际上是一个不断尝试随机数的过程。通过不断的去尝试随机数，使得当前区块的块头的哈希值满足当前网络的难度要求，即成功挖到一个区块。矿工全节点便可将区块发布到比特币区块链网络上形成全网共识，最后获得出块奖励。在尝试随机数的过程中全节点需要不断的监听网络上是否有新区块产生，如果没有，那么全节点继续去尝试随机数，使得自己组装的区块的块头的哈希值满足当前网络的难度阈值，当得到满足要求的随机数时，即该矿工挖矿成功，将区块发布到比特币区块链网络中，其他的矿工节点验证区块的合法性，最后形成全网的共识，矿工获得出块奖励。如果全节点监听到比特币区块链网络中有新区块时，应立即重新组装一个新的区块再进行挖矿。因为如果矿工不重新组装区块，可能某些交易已经打包进区块链了，此时再将该交易打包进区块中会造成双花，导致交易不合法。其次，上一个区块块头的哈希值已经改变，最长合法链也已经改变，如果沿着之前的链继续往下挖矿，会被诚实的矿工节点认为是不合法的区块而拒绝。最后，挖矿计算哈希值是一个无记忆的过程，所以放弃当前区块和继续挖区块挖出的概率是一样的。目前，挖矿的一个趋势是挖矿设备逐渐走向专业化，由一开始的CPU挖矿转变为GPU挖矿，目前的矿工基本上是通过ASIC矿机去挖矿。

随着挖矿设备的不断专业化，挖矿成本不断提高。矿工的收入变得极度不稳定，这将会动摇比特币区块链系统中矿工的挖矿热情，但大型矿石地出现很好的解决了这一问题的出现。对于单个全节点挖矿的矿工而言，他需要自己去维护一个全节点的所有职责，这不仅会给矿工增加存储的负担也会分散矿工更新全节点和计算随机数时的计算能力，对于矿工而言非常不友好。大型矿石的出现使每个矿石都有一个矿主，在该矿主下面会分布很多的矿工，矿主只需要计算区块块头的哈希值而不需要去履行全节点的其他职能，这样可以减轻矿工节点的压力，保证稳定的收入，在一定程度上对于比特币区块链网络的发展有积极的作用。但由此产生的一个问题是，一个矿石得到的出块奖励应该如何分配给不同的矿工。在一个矿石中，矿主将不同的任务分配给不同的矿工，并设置一个低于比特币区块链网络难度值的目标阈值，矿工根据矿主给出的任务去尝试不同的随机数的值，并将满足矿主要求的区块提交给矿主作为自己的工作量证明，在分配出块奖励时矿主根据不同矿工提交的区块的数目进行利益的分配。因为矿工挖到矿的概率取决于矿工尝试随机数的数目，尝试的随机数的次数越多产生满足矿主要求的区块的数量就会越多，获得出块奖励分配的比例也会越大。每个矿工计算的区块都是由矿主分配的，里面有矿主账户的哈希地址，所以不存在不诚实的矿工节点在得到正确的区块时不提交给矿主，而自己发布到比特币区块链网络中获利的情况。

#### 3.1.8 比特币的分叉

在比特币的网络中，区块链只有一个区块的块头哈希不指向前一个区块和一个区块的块头没有后继的区块。如果在某一时间内，存在两个不同的区块块头的哈希指向前一个区块，这时我们称为区块链的分叉。分叉产生的原因有很多，例如，当有两个矿工同时发布两个合法的区块到比特币的网络中，这时这两个区块都将会被比特币的网络接受，形成临时的分叉；恶意节点想要篡改比特币的网络中的交易，进行分叉攻击，而比特币的网络中的协议发生改变，有一些节点没有更新该协议等等都有可能产生分叉。在区块链中有两种比较典型的攻击方式是分叉攻击和数据的篡改。但是这两种攻击方式几乎不可能成功。

基于区块链的系统中的交易以块的形式进行，由矿工来挖矿生成区块确定，交易一旦由某个矿工打包到区块链中，其他的矿工节点便会执行该块，并更新本地的Merkle树来达到所有节点的共识。当有恶意的节点想要修改区块链中某一块的信息时，因为区块链的规则是最长合法链规则，所有的矿工节点只承认最长的合法链即只有在最长合法链中的数据才会被所有的矿工承认，里面打包的交易才会被认为是合法的。所以当矿工想要发动攻击时，例如在发动一个分叉攻击时，攻击者只有在其攻击的分叉的链路上形成最长合法链，让所有

的矿工承认攻击者发动攻击的这条链是最长合法链，攻击才能成功。而这需要攻击者掌握系统至少 51％的计算能力才有可能实现，但是区块链中的矿工节点大多数是好的节点，因此，发动此攻击基本上是不可能实现的，如图 7 所示。

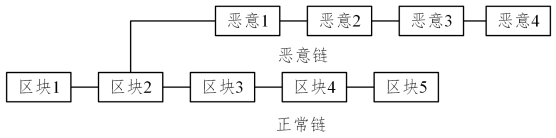


图 7　分叉攻击成功

Fig. 7　Fork attack succeeded

其次，当恶意节点只是想要去篡改某一块上的数据，而不是发起分叉时，攻击者在修改当前区块的交易信息后，还需要修改当前块的哈希值。因为区块链中的块都有一个块头，块头记录了当前交易的根哈希值，通过根哈希和随机数来计算难度域值，只有符合当前网络难度域值合法的块才会被认为是一个合法的区块，所以当交易的 Merkle 树的根哈希发生变化时，需要重新计算这个难度域值。后面的区块头部信息中又包含前一个区块的根哈希值的信息，当前一个区块信息发生变化时，相应的也需要修改后面区块的根哈希信息。以此类推，从当前修改的区块开始，后面的所有区块都需要修改根哈希信息。区块链中的块，一般需要等待至少 6 个块的确认信息才会被认为是安全的，因此攻击者至少需要修改 6 个块的块头信息，该交易才会被认为是一个合法的区块，这在实际的生活中几乎是不可能实现的，如图 8 所示。

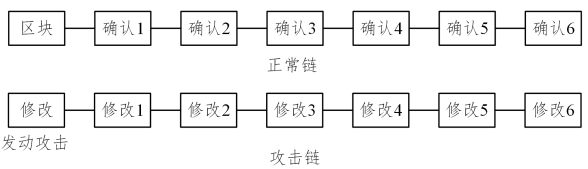


图 8　恶意节点修改区块信息

Fig. 8　Malicious nodes modify block information

综上所述，区块链中每一个块都依赖于上一个块的信息，所以区块链在实际的应用中有一个很好的特性即可溯源性。

3.1.9　比特币的匿名性

在比特币区块链系统中所有的交易都是在网络上公开传播的并且不可篡改，网络上所有的用户都可以查看这些交易的信息，随之引发的问题是用户的隐私如何得到保证[20-22]。比特币区块链系统中，同一用户的不同账户可能会产生关联性：首先，同一笔交易中，由于一个账户的余额不够，因此使用两个子账户中的比特币来支付一笔交易。因为比特币的账户是通过私钥来控制，故这两个账户私钥的同时交易可能是来自同一个人；其次，在一笔交易中的输出中产生的小额输出可能是付款账户的找零账户。换句话说，账户所有者在使用比特币区块链系统中进行交易时，相应的该账户所有者也在现实世界中以这些账户中所持有的比特币作为交易金额进行交易，我们可以通过分析大量的现实世界中的交易记录与比特币区块链系统之间的联系，从而知道该账户的所有者是谁，从而泄露该用户的个人信息。

为了解决比特币账户之间的关联性，首先应该保证比特币区块链系统在网络层的匿名性[20]。常用的一种方法是通过多路径转发的方式，来实现账户关联的隐藏。比特币区块链系统在应用层实现匿名性，是通过将不同用户的比特币混在一起，然后分配给不同的用户来实现。目前有一些专门的网站可以提供混币的服务，这些提供服务的网站通过提供这种混币服务向比特币用户收取一定的服务费。在线钱包以及比特币的交易所也天然地具有混币服务的性质，因为在这些平台中比特币用户将比特币提交给这些机构，在不同用户提出比特币时，机构将你刚刚提交的比特币给了别的用户。当自己需要提取比特币时，提取的可能是别人提交的比特币，所以比特币交易所具有天然的混币的功能。

在比特币区块链系统中，每一笔转账交易都需要比特币账户私钥的签名，表示该比特币账户对于该账户具有操作的权限，能够使用该比特币账户上的比特币，这样的交易矿工节点在验证其合法性时才可能通过。零知识证明是指一方（证明者）向另一方（验证者）证明一个陈述是正确的，而无需透露除该陈述是正确的以外的任何信息。其中，比特币的零知识证明指比特币账户去证明某一比特币账户是属于自己，但是比特币账户并不会告诉矿工节点比特币账户的私钥，因为比特币账户的公钥在比特币区块链系统中是公开的，所以，全节点只需要用比特币账户的公钥去验证其签名是否正确便可以验证某一交易的合法性。同态隐藏，即如果 $x$，$y$ 不同，那么它们的加密函数值 $E(x)$ 和 $E(y)$ 也不同，即加密函数值不会出现碰撞，如果 $E(x)$ 等于 $E(y)$，则 $x=y$。给定 $E(x)$ 的值，很难反推出 $x$ 的值；给定 $E(x)$ 和 $E(y)$ 的值，可以很容易地计算出某些关于 $x$ 和 $y$ 的加密函数值。同态加法，即通过 $E(x)$ 和 $E(y)$ 计算出 $E(x+y)$ 的值。同态乘法，即通过 $E(x)$ 和 $E(y)$ 计算出 $E(x*y)$ 的值。通过加法和乘法便可以扩展到多项式。同态隐藏特性在比特币区块链系统中是实现零知识证明的数学基础。

## 3.2　以太坊

3.2.1　以太坊概述

随着计算机的发展，互联网已经连接到了世界上的大部分的地方，全球信息共享的成本越来越低。比特币区块链网络通过共识机制和自愿遵守的社会合约，实现了一个去中心化的价值转移系统且可以在全球范围内自由使用，这样的技术改革体现了它的巨大力量。但是在比特币区块链系统中仍然存在每个区块发布的时间长、基于交易的管理模式用户查询余额时存在许多不便、脚本语言实现简单且只能进行简单的转账交易等局限。故以太坊区块链尝试使用一个通用性的技术项目，以构建任何基于交易的状态机。而且以太坊区块链致力于为开发者提供一个紧密整合的端到端的系统，智能合约的产生正是区块链进入 2.0 的标志性事件。在比特币中进行挖矿是通过不断的尝试哈希值得到符合当前网络难度要求的哈希值，即在比特币区块链系统中挖矿比拼的是计算机的算力。在以太坊区块链的系统中，为了抵抗挖矿设备的不断专业化，其在设计共识协议时对内存有一定的要求。其次，新增的对智能合约的支持使以太坊区块链从工作量证明转向权利证明提供了前提和基础。

比特币实现的是一种去中心化的货币，而以太坊区块链的一个显著特点就是去中心合约的支持[23-24]。相比于现实社会中的合同，在现实社会中参与方之间签署的合同的有效性需要政府或者一些司法手段来维护。并且现实中的合同有一个明显的弊端，即当合同的参与方各自在不同的国家，他们就没有一个公共的司法管辖权，那么要去签署合同形成共识

是一件非常困难的事情，同时如果合同的签署方不按照要求执行合同时，要对其采取强制措施也非常困难。对比上述现实中合同的难题，我们设想是否可以通过编程的方式，将合同固化成一个大家公认的程序代码并且一旦签署合约不管结果好坏都不能更改合约的内容和否认执行。智能合约是将合同里面的内容通过编程的方式写入以太坊区块链网络中，一旦该合约被打包进区块链中，其合约的内容将不可更改，合约的签署方也必须按照合约的内容进行执行。这样可以保证合约参与方从开始就按照合约的内容去执行，且不存在否认或者不执行的情况。

### 3.2.2 以太坊账户

在区块链中比特币区块链系统是基于交易的模式，在这种模式下每个用户并不能显式地知道自己账户上比特币的余额多少，在每次使用比特币进行交易时需要去查询余额。其次，在比特币使用的过程中，收到的一笔比特币在使用时必须一次性花出去，当消费金额小于总的比特币数额时，就必须使用一个用于接受差额的地址，否则这部分的差额就会被认为是矿工的交易费而全部转给矿工。这对于比特币用户而言是非常不友好的。以太坊区块链最重要的一点是它支持智能合约，因此以太坊区块链在设计时要求合约参与方需要有比较稳定的身份。以太坊账户与普通银行账户的异同点如表 3 所列。

表 3 以太坊账户与银行账户

Table 3 Ethereum account and bank account

| account | Check balance | The address to receive the balance | Spend all your money at once |
|---|---|---|---|
| Ethereum account | Yes | Yes | Yes |
| Bank account | Yes | No | No |

以太坊区块链是基于账户模式的区块链，在进行转账交易时只需要验证以太坊区块链账户上的余额是否充足，而不需要说明以太坊区块链账户上以太币的来源。由于以太坊区块链账户是基于账户的模式，因此在进行转账时并不需要一个接受差额的地址，在使用以太坊区块链进行支付时直接在账户上扣除即可。在比特币区块链系统中，因为没有确切的账户，所以防范双花攻击的方式是去查验当前使用的比特币是否已经被使用。以太坊区块链系统是基于账户的模式，当以太坊区块链用户在使用以太币进行交易时，就从该用户的账户上扣除相应的以太币，所以以太坊区块链系统可以天然地防止双花的攻击。但是在该模式下，因为检测到有转账交易便会直接去扣除某一账户上的金额，所以可能存在恶意的收款方恶意地将转账交易进行重复发布的情况，因为交易是一个合法的交易所以当该交易再次被打包到以太坊区块链中时，付款方的账户会再次被扣除相应数额的以太币。为此，在以太坊区块链交易中每个账户发起的交易都会有一个相应的编号，用于记录该笔交易是当前账户发起的第几笔交易。以太坊区块链矿工在进行打包交易时只需要去验证当前交易的编号和用户账户状态所维护的交易的编号是否匹配，便可以防范恶意节点的重放攻击。

以太坊区块链的账户可分为两类账户：一类账户为外部账户，另一类账户为合约账户。外部账户记录着该账户的账户余额、该账户当前已经发布的交易的数目等。外部账户通过公私钥对账户进行控制，外部账户可以主动发起一个交易并调用某些合约账户。合约账户不能主动发起一个交易，所有的交易都必须由外部账户发起。当进行不同合约账户之间的调用时，需要通过外部账户发起一个交易，并通过该交易调用内部的合约账户，再通过内部的合约账户去调用其他的合约。合约账户是通过合约账户的地址去调用合约。合约账户需要保存合约的相关代码，账户相关的状态以及变量的取值等，如图 9 所示。

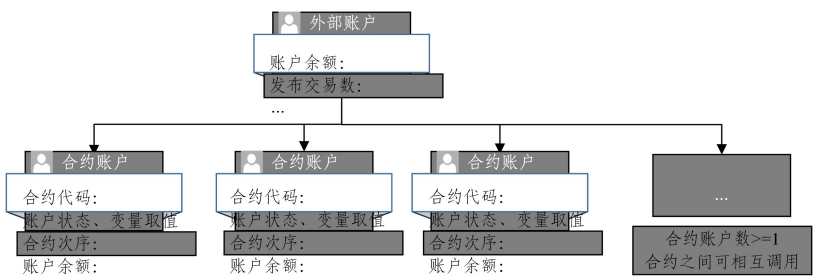


图 9 以太坊区块链账户模型

Fig. 9 Ethereum blockchain account model

### 3.2.3 以太坊的状态树

在比特币区块链网络中，矿工去验证交易是否合法时，只需要向前搜索该交易中使用的比特币是否合法以及交易是否有合法的签名。但是以太坊区块链基于账户模式的账本并没有显式地记录该账户上的以太币的来源。验证以太坊区块链中交易是否合法便不能与比特币相同，故在以太坊区块链中需要设计一种满足以太坊区块链网络的状态树。验证交易的合法性，关键在于将交易信息与用户的账户状态信息关联，通过交易去搜索到相关的账户然后验证交易的合法性。最直观的一种想法是构建一张哈希表，它记录着每个账户的信息以及对应的账户状态信息。因为哈希表是线性的，故在验证交易有效性时只需要去查找哈希表即可，它的时间复杂度是线性级别的。目前，不管是比特币区块链网络还是以太坊区块链网络，在发布一个区块时都需要提供工作量证明。利用哈希表去验证交易是否合法时，进行工作量证明需要将整个哈希表中的内容组成一棵 Merkle 树，将 Merkle 树的根哈希值存在区块的块头节点中，在验证交易是否合法时只需要验证 Merkle 树中的根哈希值是否正确便可以知道当前状态下哈希表中数据的正确性。但是，以太坊区块链中每时每刻都有交易发生，每时每刻都有用户的状态在不断发生改变，所以每当有新的交易发生时，系统所维护的哈希表的内容就会发生改变，全节点需要重新去构建一棵新的 Merkle 树。每次发生变化的账户相比以太坊区块链总的账户数而言是非常小的，所以每次更新 Merkle 树所要

花费的代价太大，在实现上不可行。

Merkle 树的作用是维护各个全节点状态的一致性以及查询账户余额。在使用哈希表在进行工作量证明时，如果哈希表中的内容发生改变就需要重新构建 Merkle 树，那么我们设想是否可以直接使用 Merkle 树而不使用哈希表，每当有交易发生时只去修改与该交易相关的 Merkle 树的节点，从而实现全节点的共识。在当前已有的算法中并没有一个高效的算法可以快速查找和更新 Merkle 树，并且，对于非排序的 Merkle 树，相同的交易集合中不同的矿工组成的 Merkle 树的方式可能不同，这样计算出的根节点的哈希值不同，不利于以太坊区块链系统的全网共识实现。如果将交易插入到排序的 Merkle 树的中间部位时，由于后面的交易排序与前面的顺序相关，将新产生的交易插入到排序 Merkle 树中时就需要更新大部分的 Merkle 树，这在真正的系统实现上也不可行。

基于上述不足，以太坊区块链系统使用了压缩前缀 Merkle 树（Merkle Patricia Tree，MPT）的结构来存储账户的状态。因为以太坊区块链账户的地址长度是固定的，且长度为 160 位二进制数，即 40 位 16 进制数。如果采用前缀树的方式来存储以太坊区块链的账户，构成的状态树的节点最多只有 17 个分支，其中 16 位为十六进制的编码再加上一个结束标志位。以太坊区块链账户的查找效率只与状态树的高度有关。在树型结构中，不同的键值所对应的分支也不同，所以使用前缀树来构建以太坊区块链的状态树一定不会发生哈希碰撞。当以太坊区块链网络中产生新的交易时，即使不同的矿工打包交易的顺序不同，但是每个交易可按照其地址编码去寻找对应分支的叶子节点，所以当打包交易顺序不同时，形成的前缀树的根节点还是一样的，满足了以太坊区块链网络中全网共识性质的要求，当需要更新树中的某些账户时，只需要找到对应账户的叶子节点，然后修改与该交易有关的路径上的值即可，而不需要更新整棵树。为了防止以太坊区块链系统中用户生产地址时产生哈希碰撞，地址空间一般设置地会比较大。而在实际的应用系统中，用户的实际账户地址数目与以太坊区块链的总的账户地址数目相比微乎其微，这就会造成存储空间的极大浪费和增加查找账户的时间，因为可能存在大量的节点只有一个分支一脉相承的情况，故我们可以将这样的节点进行压缩，形成压缩前缀树。最后将树中的普通指针改成哈希指针，便形成了以太坊区块链的状态树的数据结构，压缩前缀 Merkle 树使树的高度变小，提高了查找账户的时间效率，并且从叶子节点向根节点去验证压缩前缀 Merkle 树，便可以得到账户的状态以及账户的余额。压缩前缀 Merkle 树可以验证该状态树是否被修改。通过地址搜寻压缩前缀 Merkle 树可以很容易证明某个账户是否存在，这是普通的 Merkle 树不能实现的。以太坊区块链状态树的具体结构如图 10 所示。

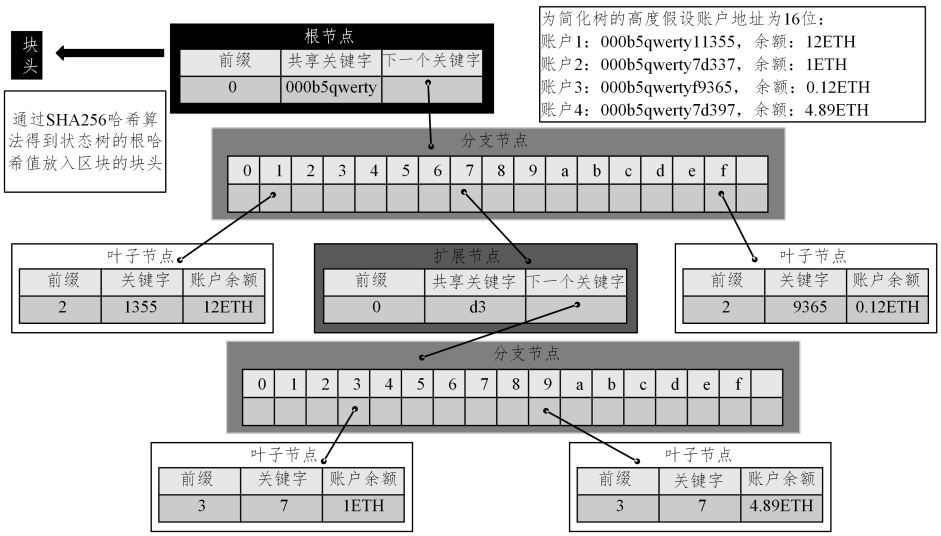


图 10 以太坊区块链状态树结构

Fig. 10 Ethereum blockchain state tree structure

其中 0 表示在扩展节点中有奇数位空键值，1 表示在扩展节点中有偶数位空键值，2 表示在叶子节点中有奇数位空键值，3 表示在叶子节点中有偶数位空键值。在实际的以太坊区块链系统中账户的状态并不只是账户的余额，还有发布交易次数、合约内容、随机数等。比特币状态树与以太坊状态树区别如表 4 所列。

表 4 比特币状态树和以太坊状态树

Table 4 Bitcoin state tree and Ethereum state tree

| Tree | Traverse | New tree | Compressed storage | Block link |
|---|---|---|---|---|
| Bitcoin state tree | Yes | Yes | Yes | No |
| Ethereum statetree | Yes | No | No | Yes |

当全节点监听到以太坊区块链网络中有新的交易产生时，更新状态树并不是将整棵树进行重建，而是新建一棵包含新产生的交易的状态树，而那些状态没有发生变化的地方不需要再次构建，只需将当前新产生的区块的状态树的节点指向前一个区块的状态树即可。其修改过程如图 11 所示。

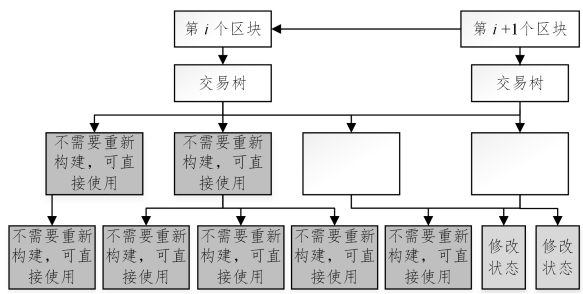


图 11 修改状态树

Fig. 11 Modify the state tree

以太坊区块链中设置的出块的时间间隔非常短，所以产生分叉非常常见，分叉的区块中的交易需要进行交易的回滚也比较困难。所以在修改状态树时，不能只生成与状态发生变化的交易相关的状态树，同时也需要将指针指向未发生变化的节点，以便在发生分叉时，方便交易的回滚。

#### 3.2.4 以太坊的交易树和收据树

在以太坊区块链网络中，每个矿工节点都可以打包以太坊区块链网络中的交易信息，这些交易信息会被矿工节点打包成一个区块的形式最终发布到以太坊区块链网络上。而这些交易信息所形成的交易结构被称为以太坊区块链网络的交易树，其中，每个交易执行完以后会形成一个收据，用来记录交易执行的具体内容以及相关信息。每一条交易信息都会形成一条收据信息，并且它们在组织形式上也是一样的，我们称这种数据的数据结构为以太坊区块链的收据树。在以太坊区块链网络中，智能合约的执行及其调度过程比较复杂，保存交易树和收据树有利于快速查询执行的结果。在以太坊区块链系统中，状态树、交易树和收据树采用的是相同的数据结构，这样有利于区块数据的管理，并且使用压缩 Merkle 树可以实现快速查找。例如，在状态树中可以使用用户的账号快速查找与该账户相关的状态信息，在交易树和收据树中，可以通过该交易在区块中的序号来查找。交易树和收据树与状态树的不同点在于交易树和收据树只存储了当前区块的一部分信息，而状态树则是保存了整个以太坊区块链网络中所有账户的状态信息。在以太坊区块链网络中每个区块的交易树和收据树是相互独立的，区块之间不共享节点；而状态树中，区块之间的不变的用户状态是可以共享的。

在实际的使用过程中，想要进行默克尔证明，证明某个交易的执行结果或者查找在某个时间段内与某个交易或者账户有关的交易信息，例如，查找在过去十分钟内与某个智能合约有关的交易信息，一个最直接、简单的方法就是扫描十分钟内新生成区块的所有交易信息，去查找与该智能合约相关的交易信息，但是该查找方法的效率非常低下。所以在实际的应用中，以太坊区块链系统提供了一个布隆过滤器(Bloom Filter)的数据结构[25]，它可以在一个大的集合中计算出一个非常紧凑的摘要信息，通过该摘要信息可以快速定位和验证某一交易信息是否存在。在该集合中，一开始先对所有元素的初值都赋值为 0，当某一交易信息进行消息摘要后映射到该集合中的某一位置时，将该位置的信息赋值为 1，表示交易存在。弊端是存在哈希碰撞的可能，所以当进行查找时，发现该位置的元素为 1 时，并不能说明某一交易一定存在，还需要进一步去检查交易树的信息，但是该数据结构一定可以确定某一交易不存在，所以通过该性质可以快速过滤一些无关的区块。其次，该数据结构并不支持删除操作，因为存在哈希碰撞的可能，在删除时可能把另一个交易的交易信息一起删除，所以为了系统的稳定，该数据结构并不支持删除操作。在以太坊区块链系统中每个收据都保存了一个布隆过滤器记录用于交易类型、地址等信息。并且会在块头形成一个总的布隆过滤器的并集。其中布隆过滤器的数据结构如图 12 所示。

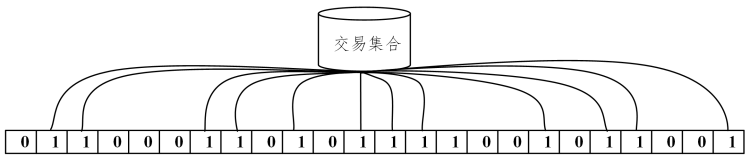


图 12 布隆过滤器数据结构

Fig. 12 Bloom filter data structure

每次查找交易记录时，只需要先验证区块的块头的信息，如果区块的块头中布隆过滤器集合元素中没有该交易的信息，那么在这个区块的块体里面一定没有该交易信息。如果存在该交易信息，则继续查找该区块的区体中的具体的交易，去验证该记录是否存在哈希碰撞的可能。

#### 3.2.5 GHOST 协议

在设计以太坊区块链系统时，为了改善比特币区块链系统出块时间太长导致的工作效率不高的问题，在设计时将以太坊区块链网络的出块时间缩减到了十几秒。但是在现实生活中，数据在网络上的时间延迟最少也需要十几秒，所以，在以太坊区块链系统中出现临时性分叉非常常见，这不利于以太坊区块链网络中所有的节点形成一个共识，破坏了系统的稳定性和安全性。在比特币区块链系统中，一些不在最长合法链上的区块将被视为无效的区块而被丢弃，系统也不会给发布该区块的矿工任何的出块奖励。但是，在以太坊区块链系统中存在大量的临时性的分叉，如果也将没有在最长合法链中的区块丢弃，将会有大量的矿工发布的区块被丢弃，这会打消矿工挖矿的热情，这会对以太坊区块链系统的安全造成威胁。最后，比特币区块链系统中的方式对于大型矿石而言会形成一个不成比例的优势，因为大型矿石的计算能力较强，大型矿石会沿着自己发布的区块继续计算随机数的值，并且，大型矿石在网络中的接口较多，所以大型矿石发布的区块更容易传播到网络的其他节点中，使得一些个人矿工去接受大型矿石发布的区块。在这种恶性循环下，大型矿石最终会形成一个不成比例的优势。大型矿石不断地累积自己的优势，最终可能出现区块链被某个大型矿石控制的情况，这对于区块链安全来说是致命的，也是不能容忍的。

为了解决以上难题，以太坊区块链系统采用了 GHOST 协议作为它的共识协议。该协议将一些不在最长合法链上的分叉的区块称之为叔父区块。它的一个核心思想是对于最终没有成为最长合法链上的区块也会给予一定的出块奖励，并且对于包含这些叔父区块的新发布区块也给予一定的额外奖励，鼓励新产生的区块尽可能地包含这些不在最长合法链上的叔父区块。每个新区块最多可以包含 2 个叔父区块，每包含一个叔父区块矿工节点便可以获得当前网络出块奖励的 1/32 倍的额外奖励。这样有利于激励新区块尽可能地包含叔父区块，有利于以太坊区块链系统出现分叉后及时地合并这些分叉，维护系统的稳定。在以太坊区块链系统中，从当前节点开始的往前七代的分叉的区块都被认为是叔父区块，这样可以防止某一时刻出现的分叉的区块的数目大于两个时，有些叔父区块将不能被包含在以太坊区块链网络中或者有些

恶意的矿工节点有意不将叔父区块打包进以太坊区块链网络中的情况。在以太坊区块链网络中的两种分叉情况及其具体出块奖励的计算过程如图 13 所示。

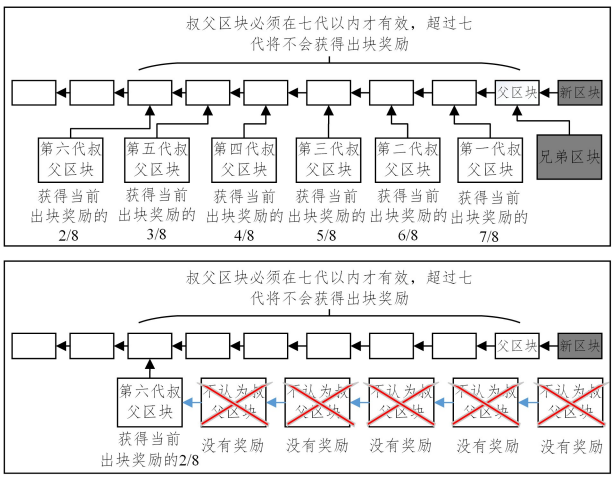


图 13　叔父区块的出块奖励

Fig. 13　Uncle block's block reward

叔父区块被新区块包含时，新区块并不需要验证叔父区块的交易信息的合法性。但是新区块需要去验证叔父区块是否符合当前网络的难度要求。它们的奖励机制计算式如下：

$$unclereward=\frac{8-Unclegenerations}{8}\times target \tag{3}$$

$$reward=unclecounts\times\frac{1}{32}\times targetreward+targetreward \tag{4}$$

其中，*uncle reward* 为叔父区块奖励；*Uncle generations* 为叔父区块的代数；*target* 为当前网络的难度阈值；*reward* 为新发布的一个区块的出块奖励；*uncle counts* 为当前区块叔父区块的数目；*targetreward* 为当前网络的出块奖励。以上共识协议只将分叉中的第一个区块视为合法的叔父区块，可以提高分叉攻击时的代价，在以太坊区块链的网络中大大减少了以太坊区块链的分叉，提高了系统的安全性和稳定性。

### 3.2.6　挖矿算法

在以太坊区块链系统中，矿工节点也是通过不断的尝试随机数的值来计算一个哈希值是否符合当前网络难度要求的方式去挖矿。但是以太坊区块链系统在设计之初将如何抵抗挖矿设备的专业化和进行从工作量证明转向权益证明做了准备，以太坊区块链的挖矿算法针对这两点要求设计了一个和比特币区块链系统完全不同的挖矿算法。首先，在以太坊区块链系统中有两种不同大小的数组，其中较小的数组大概在 $16\times10^6$ 左右，我们称之为缓存数组，主要的作用是用于轻节点去验证交易的合法性以及生成矿工挖矿时需要保存的大的数组。

缓存数组的生成方式为：1）计算一个随机种子的哈希值，得到缓存数组的第一个元素；2）通过数组的第一个元素计算哈希值得到该缓存数组的第二个元素；3）以此类推，直到整个数组的元素填充完成；4）数组每隔 3000 个区块会进行一次更新操作。工作量证明数组的生成方式为：1）计算一个伪随机数的哈希值，得到对应缓存数组中的元素的位置；2）按照伪随机的顺序，在缓存数组中进行 256 次查找得到 256 位的一个数；3）利用该数去计算哈希值，便可以得到工作量证明数组的第一个元素；4）后面的元素按照同样的方式依次生成。数组生成过程如图 14 所示。

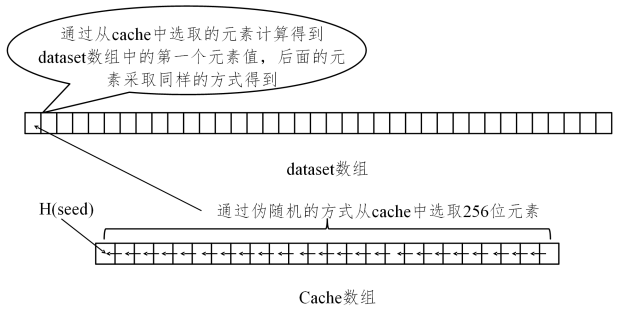


图 14　以太坊验证数组生成方式

Fig. 14　Ethereum verification array generation method

在进行验证时，矿工节点通过区块的块头信息和随机数的值计算哈希值得到第一个元素的位置信息。取该位置元素以及和它相邻的元素的值，以同样的方式进行 64 次取值得到一个 128 位的元素，计算该元素的哈希值是否符合当前网络的难度要求。如果满足当前网络的难度要求，则表示找到该随机数的值；若不符合当前网络的难度要求，否则继续去计算下一个随机的值。

### 3.2.7　难度调整

在比特币区块链系统中，为了维持系统的稳定，每隔 2016 个区块便会调整一次当前网络的难度阈值，从而将系统的出块时间维持在 10 min 左右。而以太坊区块链系统中，当前网络的难度阈值是动态变化的，下一个区块的挖矿难度与当前的父区块有密切的联系。其具体的以太坊区块链系统的难度调整算法如下所示：

$$D(H)=\begin{cases}D_0, H_i=0 \text{ 且 } D_0\geqslant 1\,317\,072\\ \max(D_0, P(H)_{Hd}+x\times\delta_2)+\varepsilon, \text{其他}\end{cases} \tag{5}$$

其中，$D(H)$ 是当前区块的难度，$D_0$ 为创世纪块的出块难度且 $D_0$ 的最小值为 1 317 072，即整个以太坊区块链系统的难度是大于或等于 1 317 072 的。以太坊区块链的难度调整是将基础部分 $P(H)_{Hd}+x\times\delta_2$ 和难度炸弹部分相加得到。基础部分的 $P(H)_{Hd}$ 为父区块的难度，每个新区块的难度都在父区块的难度基础上进行调整；$x\times\delta_2$ 主要用于调节出块难度，维持系统的出块速度；$\varepsilon$ 是难度炸弹，难度炸弹的设置主要是为了将来从工作量证明转向权益证明的过渡做准备。为了防止有些矿工拒接从工作量证明转向权益证明而导致当前的以太坊区块链出现硬分叉的情况，可以利用难度炸弹这个特殊的参数将以太坊的工作量证明的难度设置地非常大。如果矿工节点不转向权益证明，那么该矿工将无利可图，所以难度炸弹为工作量证明向权益证明转变做准备。

将上式各参数展开可写为：

$$H_{i'}\equiv\max(H_i-3\,000\,000, 0) \tag{6}$$

$$\varepsilon\equiv\left\lfloor 2^{\lfloor H_i'\div 100\,000\rfloor-2}\right\rfloor \tag{7}$$

$$\delta_2\equiv\max\left(y-\left\lfloor\frac{Hs-P(H)_{Hs}}{9}\right\rfloor, -99\right) \tag{8}$$

$$x\equiv\left\lfloor\frac{P(H)_{Hd}}{2048}\right\rfloor \tag{9}$$

其中，$x$ 是调整单位，由每次调整的单位的父区块的出块难度除以 2048 向下取整得到；$\delta_2$ 是调整的系数，它与父区块相关联。其中 $y$ 表示父区块中叔父区块的数目，如果父区块中包含了叔父区块，则 $y$ 设置为 2；如果父区块中没有包含叔父

区块，则 $y$ 设置为 1。这样做的主要目的是为了保持货币发行量的稳定，因为如果父区块包含了叔父区块，那么该区块所获得的出块奖励将会大于当前网络的出块奖励，因此在挖下一个区块时会相应地增加挖矿难度。$Hs$ 为当前区块时间戳，$P(H)_{Hs}$ 为父区块的时间戳，他们相减得到先后两个区块出块的时间间隔。如果时间间隔小于 9 s，表示当前出块的时间太短，当前网络的难度较低，向下取整为 0 故整个网络的出块难度将会上调。如果时间间隔大于 9 s 小于 18 s，表示当前出块的时间符合系统的难度要求，向下取整为 1 故整个网络的出块难度将不会改变。如果时间间隔大于 18 s，表示当前出块的时间太短当前网络的难度较高，向下取整为 2 故整个网络的出块难度将会下调。但是，整个难度系数的调整应不超过 99 个单位。这是为了防止黑客攻击和其他意想不到的黑天鹅事件。ε 是一个 2 的指数函数，每产生 100 000 个区块便会增大一倍，所以后期将会增加地非常快，这也是难度炸弹的由来。$H'$ 为假的区块号，因为在拜占庭阶段[26-27]以太坊区块链系统的难度已经变得非常高，但是转向权益证明的准备还不充分所以不得不进行一次区块序号的回调。$H_i$ 为真正的以太坊区块链的块号。

### 3.2.8 权益证明

比特币和以太坊目前使用的挖矿算法是工作量证明，以这种方式进行挖矿的一个弊端是会消耗大量的电力资源，在一定程度上会造成资源的浪费和环境的污染。所以以太坊区块链系统在设计时，便考虑要采用将工作量证明逐渐转向权益证明的方式来进行挖矿。权益证明的核心思想是，通过每个矿工手中所持有的以太币的数量来决定该矿工在这次投票过程中所占的权重，同时也是在利益分配时的权重。并且，采用工作量证明的系统的安全并不是闭环的；因为在工作量证明进行挖矿时，每个矿工发布一个区块实际上是在进行计算机算力的比拼。计算机的算力是可以通过实体世界的货币买入大量的挖矿设备来得到，故只要有足够的财力便可以聚集超过 51%的算力来发动攻击[15]。而使用权益证明的系统中，决定系统中区块的发布是通过矿工手中所持有的以太币决定的。当某个恶意的矿工节点想要发动攻击时，必须要有足够的以太币才能成功。在大量买入以太币的过程中，必然会导致以太币价格的上涨，所以说采用权益证明设计的系统其安全性是闭环的。但是，权益证明和工作量证明这两种方式并不是互斥的，例如，矿工可以用自己手中持有币的多少去降低挖矿难度。矿工将自己手中的币投入到这种混合系统中，系统将矿工投入的币锁定并减小矿工的挖矿难度。当矿工挖到一个区块并发布到网络上时，矿工在系统中锁定的币不能直接提取出来，而是要等达到一定数目的区块后才能进行提现继续使用。

在早期，为了使工作量证明向权益证明转变，使用的权益证明的协议为 Casper FFG 协议[28-29]，用于为工作量证明提供最终证明。交易一旦写入，那么该交易将不会被回滚。其具体的实现过程为：矿工投入一定的保证金，使得该矿工节点成为验证者具有一定的投票权，可以决定哪一条链是最长合法链。其中，投票的权重是由矿工投入的保证金的多少决定的。投入系统的保证金将会被系统锁定，当有矿工节点获得投票权但是却不作为，系统将会扣除该矿工节点一定的保证金。如果矿工节点进行恶意投票，即在两个有冲突链上都进行投票，那么系统将会扣除该矿工节点的所有保证金，回收的保证金将会直接被销毁。在区块链中，每发布 100 个区块作为一个纪元。在每个纪元中矿工节点都需要进行两轮的投票，分别成为预投票和确认投票。在这两轮投票中都必须有 2/3 以上的验证者验证通过才能通过。每个验证者都有一定的任期，在任期结束后等待一段时间，验证者便可以取回自己当初投入的保证金和得到相应的奖励。在改进后，将前一个纪元的 50 个区块作为先验消息，后一个纪元的 50 个区块作为确认消息。这样每个验证只需要进行一栏的投票即可，可提高系统的效率，其具体过程如图 15 所示。

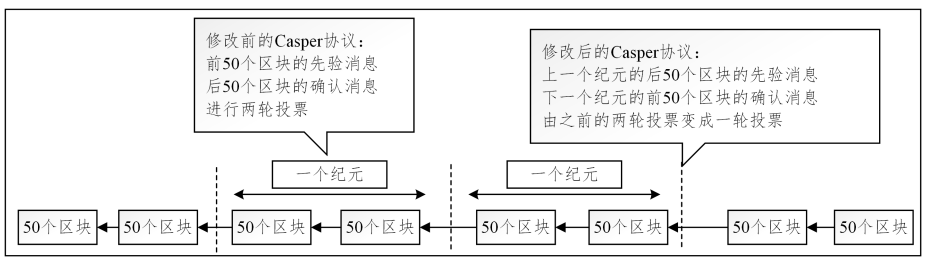


图 15 权益证明工作过程

Fig. 15 Proof of equity work process

### 3.2.9 智能合约

智能合约的本质是运行在区块链上的代码序列，代码逻辑定义了合约内容，智能合约的账户保存了合约当前的运行状态，例如账户当前的余额、交易次数、合约代码等。它的存储方式为一棵压缩的 Merkle 树的结构。创建一个智能合约是通过一个外部账户发起一个转账交易到 0×0 的地址。其中转账金额为 0，但是要支付汽油费，合约代码放在数据域里面。以太坊中的交易具有原子性，一个交易要么全部执行完，要么回退到交易的初始状态。所以，在智能合约的运行过程中，如果出现错误交易会自动回滚到初始状态，但是在执行智能合约过程中消耗的汽油费则不会退回到发布交易的账户。为了防止矿工为了获得大量的汽油费一次性打包很多交易，在以太坊区块链系统中对一个区块的汽油费进行了限制。但是这并不是固定的，每个矿工可以在上一个矿工发布的区块的基础上做出一定的微调。

当一个全节点打包交易时，有一些交易是对智能合约的调用，那么全节点应先执行完智能合约后再进行挖矿。智能合约在执行过程中，任何状态的修改都只是对全节点本地的状态树的修改，只有当该全节点获得记账权发布一个区块时才能获得汽油费，其他节点不获得汽油费，并且全网的矿工节点必须更新自己本地的全节点的状态信息，最终形成全网共识。与比特币区块链的不同点在于，以太坊区块链中发布到区块链中的交易不一定都可以成功执行，因为执行交易需要一定的汽油费，可能存在汽油费不足的情况，导致交易执行

错误。汽油费只有将交易成功发布到区块链上形成全网共识后才收取，所以执行错误的交易也是可以发布到区块链上。通过收据树和交易树中的状态域查看当前交易是否成功执行。

智能合约的另一个特点是不支持多线程，因为在以太坊区块链系统中输入一组交易时，必须要有一个确定的输出，而多线程中的多个核对内存访问的顺序不同，得到的结果有可能不同，从而破坏全网的共识。

### 3.3 共识协议对比

共识，顾名思义即大家都接受的观念或规则。如，你约了一群人出去玩游戏，玩游戏需要制定一个规则，在玩之前事先规定好游戏的输赢以及奖惩措施，在游戏开始之前需要每个参与游戏的人都同意这个游戏规则并达成一致意见，这样才能保证整个游戏的公平性。而在这个游戏中，这个游戏规则就是游戏的共识。同样地，在区块链系统中也需要这样一个共识，使得区块链系统在工作过程中可以公平有序地进行。对区块链系统而言，共识是一个决策的过程，它的目标是确保所有参与者在添加新数据块后，能就其当前状态达成一致。换言之，共识协议是为了确保一条链的正确性，并为做出贡献的参与者提供激励措施。共识协议对区块链来说非常重要，它可以防止一个人单独控制整个系统，并确保每个人都遵守网络规则。以比特币区块链为例，虽然中本聪创造了比特币区块链，但他对这条链并没有所有权，比特币区块链完全是透明和开放的，网络中的每个节点都是平等的。总的来说，一个协议就是一套人为制定的规则，它应该有利于确保在线交易的可行性、消除双重损毁的可能性、确保参与者不作弊、确定性的逻辑规则、以加密技术和密码学作为安全基础、使网络协议得以延续等。目前行业中有多种区块链协议，我们分析了几种共识协议的使用场景以及优缺点，如表5所列。

表5 共识协议对比

Table 5 Consensus agreement comparison

| | 工作原理 | 使用范围 | 使用案例 | 优点 | 缺点 |
|---|---|---|---|---|---|
| Proof-of-Work (PoW) | 容易检测结果的正确性，但是很难找到反向找到解决方案 | 公有链 | 比特币、以太坊、莱特币 | 能够保证两个互不信任的参与者在同一个网络中工作，任何人的加入不需要任何许可 | 交易的成本高并且处理效率低 |
| Proof-of-Stake (PoS) | 抵押的资源越大，网络允许这个验证者创建块的概率就越高 | 公共/私有区块链 | Cosmos，Tezos，Ethereum也正准备从PoW转向PoS | 能够保证两个互不信任的参与者在同一个网络中工作，任何人的加入不需要任何许可，并且交易的处理效率比PoW高的多 | 目前实现较为困难 |
| Delegated-Proof-of-Stake(DPoS) | 参与者将新块的生产委托给被选出来的、数量固定的验证者 | 公共/私有区块链 | Eos、Bitshares | DPoS通过减少验证者的数量来提高交易速度以及创建块的速度，与PoS相比，DPoS更快更公平 | 在一定程度是一个完全的去中心化的系统 |
| | 工作原理 | 使用范围 | 使用案例 | 优点 | 缺点 |
| Proof-of-Activity (PoA) | PoW和PoS的混合 | 公共区块链 | Decred | 结合了PoW和PoS协议，在一定程度上PoA协议为矿工和普通网络成员之间提供了平衡 | 多个协议共同工作，系统更为复杂 |
| Proof-of-LocaTIon (PoL) | 使用信标记录特定的GPS位置，可查看处于同步状态的节点，然后用临时标记来标记其存在 | 公共区块链 | FOAM、PlaTIn | 依赖于BFT信标，它在区块链中记录地理位置和时间标记，从而防止系统中断和欺诈 | BFT信标的质量会影响系统的质量 |
| Proof-of-Importance (PoI) | 和PoS类似，增加了一个影响力排名的附加条件 | 公共区块链 | NEM | 同PoS | 目前实现较为困难 |
| Proof-of-Elapsed-TIme(PoET) | 块是在相同的时间里以及受信任的环境中创建的 | 私有/联盟区块链 | IntelLedger | 该系统类似于工作证明，但使用的电力较少 | 是一个具有中心化性质的系统 |

## 4 区块链的应用

本节介绍了区块链技术中一些较为成熟的应用项目。区块链最早是在比特币系统中被提出，随着比特币系统的稳定发展，越来越多人意识到区块链背后的技术具有潜在的价值，并且将这一技术进行提炼并应用在不同的领域中。Swan在《区块链：新经济蓝图》[9]一书中将区块链的应用定义为3个层次，区块链1.0－3.0。区块链1.0是以比特币为代表的虚拟数字货币，进行最简单的转账操作。区块链2.0是以以太坊为代表的智能合约的时代，它扩展了比特币的简单模式，将区块链技术应用到金融领域，如股权、债券、信贷等。区块链3.0则是将区块链扩展到了一些非金融领域中，覆盖人类生活的方方面面，使人类在日常生活中可以不依靠可信的第三方或机构而建立信任，实现信息共享，如医疗健康、知识产权等。

### 4.1 货币金融领域

比特币是最早实现去中心化的加密货币，它使用一种全新的分布式记账技术，使得交易过程去中心化。它无需可信第三方或者机构来保证交易的合法性，而是通过网络中所有节点的公共监督和维护来保证。目前，除了比特币平台自身，还衍生出了许多基于比特币平台创建的其他代币。随着比特币逐渐受到人们的关注，在比特币中获取利益的越来越多，导致了比特币的挖矿越来越难，挖矿设备不断走向专业化。莱特币(Litecoin，LTC)是早期比特币的一种代币。它在技术原理上与比特币基本相同，但是实现了一种更为轻量的数字资产。因为算法降低了硬件成本，使得普通的计算机也能进行挖矿。而后又有瑞波币的发行，瑞波币与比特币之间存在较大的差异。瑞波币在其设计上试图实现一个灵活的货币流动体系，主要是处理一些债务关系。它在其中扮演一个货币的中间转手人，帮助两个不同价值体系的货币实现兑换，并从中收取一定的手续费。达世币是基于比特币开发的一款支持即时交易的以保护用户隐私为目的的数字货币。它针对比特币出块时间长和在全网公开交易的情况做了进一步的改进：一是提高了交易速度；二通过匿名技术，使得交易无法追踪查询。达世币中交易基本上都是瞬间完成，并且通过混币服务，

在交易过程中保证用户交易的隐私性。未来币是一种全新开发和设计的第二代去中心化虚拟货币，也是第一个完全基于权益证明的第一代数字货币。在未来币中挖矿不再需要消耗大量的计算资源和电力资源，每个用户可以根据自己账户上的余额去发布新区块，最后根据余额所占的比例来进行利益的分配。表 6 是针对以上几种货币系统进行对比的结果。

表 6 区块链的 6 种加密货币对比

Table 6 Comparison of six cryptocurrencies of blockchain

| | BTC | LTC | XRP | DASH | ETH | NXT |
|---|---|---|---|---|---|---|
| 目的 | 去中心化货币 | 进比特币 | 货币兑换 | 隐私保护 | 提供智能合约 | 使用 POS 算法 |
| 发行方式 | 挖矿 | 挖矿 | 预挖矿 | 挖矿 | 挖矿 | IPO 方式 |
| 时间 | 10 min/块 | 2.5 min/块 | 5 s/块 | 2.5 min/块 | 15 s/块 | 1 min/块 |
| 货币总量 | 2100 万 | 8400 万 | 1000 亿 | 2200 万 | 无上限 | 10 亿 |
| 共识机制 | POW | POW | OpenCoin | POW+POS | POW+POS | POS |
| 加密算法 | SHA256 | Script | RTXP | X11 | Ethash | Curve25519 |
| 挖矿设备 | ASIC | GPU, ASIC | 无 | GPU, ASIC | GPU | 无 |

### 4.2 扩展的其他领域

目前区块链已经参透到了各行各业，不断有创新性应用问世。区块链技术源于比特币，因此我们最直接想到的一个应用就是在金融领域。传统的货币支付体系的作用主要是安全地存储货币和提供货币交换的中心。将区块链技术应用到传统的货币支付系统中，因为数字化货币具有不可篡改的特性所以可以达到与传统货币相同的功能，并且在中间省去了大量的成本。换句话说，区块链技术可以实现更加直接的支付，甚至在跨国交易实现超级费率的支付。鉴于这一优势，围绕跨国转账的代币也兴起。William 等[30]分析了区块链对传统银行业的冲击，并且讨论和分析了银行业中开发分布式账本需要考虑的问题。一些研究者也基于区块链技术去搭建属于自己的购物系统架构[31]、开发租用物品平台[32]、以及考虑使用电子货币来进行薪资的支付[33]。这些都是区块链在金融领域的扩展。

众所周知，区块链的两个最为重要的特性就是不可篡改性和溯源性。交易在区块的共识机制下按照时间的顺序添加到区块链的尾部，想要修改其中的信息所需花费的代价是极高的也几乎是不可能的。这种特性在一些需要进行溯源的场景中非常重要，比如在产品的供应过程中，需要保证自己的产品是否已经被人替换。个人数据的知识产权保护，可以通过区块链技术实现数字资产的确权。我们无时无刻不在接触社交媒体，在社交媒体上进行言论发布所需的成本也非常低，通过区块链的该特性，可以迅速追踪用户的声明和发言，对于一些危机国家安全或可能造成社会动荡的一些不当言论进行快速追责。除此之外，将区块链技术应用于保险领域，可以有效防止骗保、骗险等恶意行为，从而维护商家的利益。政府[34]的工作受到公众的监督，其政务信息、贷款信息、文献信息等[35]都需要做到公开公正。政府项目的招标需要公平公正，区块链技术可以在一个不信任的环境中在竞标者之间形成一个共识，例如把自己的竞标价格的哈希值发布到区块链上，当竞标结束时可以通过区块链中的数据作为自己竞标时的依据。这样既保证了消息的公开公正，也减少了在一个不信任环境中形成共识所需要花费的成本代价。

物联网[36-39]是目前比较流行的一个学科分支，由物联网衍生出许多的技术也被应用在生活的各个方面。但是物联网主要是通过传感器将物理世界与网络世界连接在一起，这就不可避免地带来了许多安全隐患，最为直观的就是物联网上缺乏中心控制、设备异构，信息执行容易被篡改。其中区块链技术正是在一个不信任环境中建立的安全机制，其去中心化的分布式网络正好弥补了物联网的这一缺陷，例如将区块链技术应用到智能家居、智慧交通、智能电网、基础设施以及一些通信资源[40-45]的分配等。

最后，将区块链技术应用到医疗等对数据保密性要求较高的领域[46-48]也是目前比较常见的。医疗数据的共享可以极大地促进医疗事业的发展，但是医疗数据都是患者的隐私数据，对于这类数据一般都有较高的保密要求，这对不同机构之间分享数据来提高精准诊断与治疗，甚至是降低医疗成本都是一个巨大的挑战。面对电子医疗技术的挑战，将区块链技术引入后便可缓解冲突。因为区块链技术使用密码学的一些技术例如哈希运算、非对称加密等使得数据在公开后仍能确保安全。其次，在药品溯源方面引入区块链技术，用户可以通过互联网查询药品的来源，预防非法机构将一些伪劣的药品以次充好。

### 4.3 未来展望

受市场需求的影响，不断产生了一些具有更高计算能力、更高效的计算机。量子计算也从基础的理论研究逐渐转向现实应用的研究。这对经典的密码学造成了极大的冲击和挑战。此外，Grover 算法也有可能会影响到对称加密和哈希算法，但目前我们并不知道如何获得相比传统计算机更多的二次加速。而区块链实现的匿名性、自治性、开放性、可溯源性等优良性质，是通过公钥加密和哈希函数提供的。量子计算的快速发展使得目前的共识协议在不久的将来被成功攻击的可能性增大，从而降低了区块链的安全性。如何预防区块链的量子攻击，重新设计区块链，将会是未来的一个发展趋势。利用能够抵御量子攻击的密码系统，从而创造出被称为后量子、量子证明、量子安全或抗量子的密码的区块链系统也是当前亟需解决的一个问题。但是总的来说，区块链与量子计算的较量中，目前是区块链更胜一筹，因为量子计算机离真正的商用还有一段距离。

**结束语** 自 2009 年比特币系统上线以来，其不仅扩展了支付形式，促进了金融领域的发展，也在各个领域都取得了一定的成就。但是其成功的背后也暴露了一定的问题，如技术的漏洞、交易中浪费资源和跨链的协议问题。现在比较流行的以太坊平台，其用于编写智能合约的 Solidity 语言并不支持小数点的使用，而且编写代码对使用的堆栈空间都有不同程度的要求。这些情况都会给程序编写人员带来一定的不便，而且在实际的程序的实现过程中，可能存在着一些还无法遇见的技术漏洞。目前的两大主流数字货币比特币和以太币使用的挖矿技术主要是工作量证明，这将会消耗大量的电力

资源，也给区块链技术的扩展带来了一定的限制。最后，随着区块链技术的发展，区块链技术会应用到不同领域，这些不同的公链在各自的领域实现着不同的价值。然而，一个公链的产生就意味着一种新的数字货币的产生，怎样实现这些不同币种的流通，没有一个统一的协议作为支撑。故在这种场景下，怎样实现跨链协议的统一标准也显得尤为重要。

## 参 考 文 献


[1] DIFFIE W，HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory，1976，22(6)：644-654.

[2] WANG C. Academic Debate about the Nature of Hayek's Monetray Theory and Its Logic Its Combing and Discrimination[J]. Foreign Frontier Journal of Social Sciences，2021，2(820)：75-87.

[3] VON HAYEK F，YAO Z Q. The denationalization of currency [M]. Rising Star Press，2007：99-110.

[4] MIN X，LI Q，LEI L，et al. A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size[C]// 2016 IEEE Trustcom/BigDataSE/ISPA. IEEE，2016，90-96.

[5] NAKAMOTO S. Bitcoin：A Peer-to-Peer Electronic Cash System[J/OL]. https：//bitcoin. org/bitcoin. pdf.

[6] SHEN X，PEI Q Q，LIU X F. Survey of block chain[J]. Chinese Journal of Network and Information Secuiity，2016，2(11)：11-20.

[7] CAI X Q，DENG Y. The Principle and core Technology of Blockchain [J]. Chinese Journal of Computers，2021，44(1)：84-131.

[8] YU G，NIE T Z. The Challenge and Prospect of Distributed Data Management Techniques in BlockChain Systems [J]. Chinese Journal of Computers，2021，44(1)：28-54.

[9] SAPRA R，DHALIWAL P. Blockchain：The new era of Technology[C]// 2018 Fifth International Conference on Parallel，Distributed and Grid Computing(PDGC). 2018：495-499.

[10] WOOD G. Ethereum：A secure decentralised generalised transaction ledger [J]. Ethereum Project Yellow Paper，2014，151：1-32.

[11] DDV，ANISH J. Bitcoin mining acceleration and performance quantification[C]// IEEE Canadian Conference on Electrical and Computer Engineering. 2014：1-6.

[12] SWAN M. Blockchain-Blueprint for a new economy[M]. O'reilly Media，2015：1-9.

[13] LI M，SONG W P，HAO H，et al. IEEE Standard for Data Format for Blockchain Systems[J]. Institute of Electrical and Electronics Engineers，2020，2(2418)：1-32.

[14] ZHANG W B. Constructing blockchain world state Merkle Patricia Trie subtree：USA，10929374[P]. 2021-02-23.

[15] HONG S，KIM H. Analysis of Bitcoin Exchange Using Relationship of Transactions and Addresses[C]// 2019 21st International Conference on Advanced Communication Technology (ICACT). 2019：67-70.

[16] YANG X，CHEN Y，CHEN X. Effective Scheme against 51% Attack on Proof-of-Work Block-chain with History Weighted Information [C] // 2019 IEEE International Conference on Blockchain(Blockchain). 2019：261-265.

[17] CHEN H，WANG Y J. A Lightweight Scalable Protocol for Public Blockchain[J]. Journal of Computer Research and Development，2020，57(7)：1555-1567.

[18] ZHU J，LIU P，HE L. Mining Information on Bitcoin Network Data[C]// 2017 IEEE International Conference on Internet of Things(iThings) and IEEE Green Computing and Communications(GreenCom) and IEEE Cyber，Physical and Social Computing(CPSCom) and IEEE Smart Data(SmartData). 2017：999-1003.

[19] HOU B，CHEN F. A Study on Nine Years of Bitcoin Transactions：Understanding Real-world Behaviors of Bitcoin Miners and Users[C]// 2020 IEEE 40th International Conference on Distributed Computing Systems(ICDCS). 2020：1031-1043.

[20] ZOLA F，EGUIMENDIA M，BRUSE J L. Cascading Machine Learning to Attack Bitcoin Anonymity[C]// 2019 IEEE International Conference on Blockchain(Blockchain). 2019：10-17.

[21] LU T，YAN R，LEI M，et al. AABN：Anonymity assessment model based on Bayesian network with application to blockchain [J]. China Communications，2019，16(6)：55-68.

[22] DIAMOND B. Systems and Methods for Side-Chainnel-Secure Blockchain Anonymity Using：I2P：WO2 021 113 732[P]. 2021-06-10.

[23] HUANG Y，WANG B，WANG Y. MResearch on Ethereum Private Blockchain Multi-nodes Platform[C]// 2020 International Conference on Big Data，Artificial Intelligence and Internet of Things Engineering(ICBAIE). 2020：369-372.

[24] MA F C，REN M，FU Y，et al. Security reinforcement for Ethereum virtual machine[J]. Information Processing and Management，2021，4(58)：1709-2022.

[25] KUMAR K，XU J，JIA W，et al. Space-Code Bloom Filter for Efficient Per-Flow Traffic Measurement[C]// Infocom Twenty-third Joint Conference of the IEEE Computer & Communications Societies. IEEE，2006：2327-2339.

[26] ETHAN B，KWON J，MILOSEVIC Z. The latest gossip on BFT consensus[J]. arXiv：1807. 04938，2018.

[27] JALALZAI M M，BUSCH C，RICHARD G G. Proteus：A Scalable BFT Consensus Protocol for Blockchains[C]// 2019 IEEE International Conference on Blockchain(Blockchain). 2019：308-313.

[28] BUTERIN V，REIJSBERGEN D，LEONARDOS S，et al. Incentives in Ethereum's Hybrid Casper Protocol[C] // 2019 IEEE International Conference on Blockchain and Cryptocurrency(ICBC). 2019：236-244.

[29] BUTERIN V，GRIFFITH V. Casper the Friendly Finality Gadget [OL]. https：//www. researchgate. net/publication/320626951_Casper_the_Friendly_Finality_Gadget.

[30] WILLIAM P G，EFSTATHIOS P. Understanding Modern Banking Ledgers Through Blockchain Technologies：Future of Transaction Processing and Smart Contracts on the Internet of Money[J]. SSRN Electronic Journal，2015：239-278.

[31] FREY R M，VUKOVAC D，ILIC A. A Secure Shopping Experience Based on Blockchain and Beacon Technology[C] // 10th ACM Conference on Recommender Systems(RECSYS 2016). ACM，2016：1-2.

[32] BOGNER A，CHANSON M，MEEUW A. A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain [C]// International Conference. 2016：177-178.


（下转第 666 页）

[6] WEI S, GUO Y, WANG D M, et al. Research on CBR Algorithm Based on Ontology and Its Application to CAPP [J]. Machine Design & Research, 2013, 29(3): 43-47.
[7] PAN X W, GU X J, QIU Y F, et al. Knowledge Modeling Techniques for Knowledge Management [J]. Computer Integrated Manufacturing Systems, 2003(7): 517-521.
[8] LIU S N, ZHANG Z M, TIAN X T, et al. Knowledge discovery method for typical process sequence based on clustering analysis [J]. Computer Integrated Manufacturing Systems, 2006(7): 996-1001.
[9] LIU J F, WU J, ZHOU H G, et al. Method of reusing process information based on machining feature [J]. Computer Integrated Manufacturing Systems, 2017, 23(4): 791-798.
[10] DUAN Y, HOU L, LENG S. Building and application of metal cutting knowledge graph [J]. Journal of Jilin University (Engineering and Technology Edition), 2021, 51(1): 122-133.

**WANG Yu-jue**, born in 1997, master. Her main research interests include knowledge graph and ontology construction.

**ZHU Deng-ming**, born in 1973, Ph.D, associate researcher, master supervisor, is a member of China Computer Federation. His main research interests include virtual reality and human computer interaction.

(上接第 461 页)

[33] ENGLISH S M, NEZHADIAN E. Conditions of Full Disclosure: The Blockchain Remuneration Model[C]// 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2017: 64-67.
[34] JAGRAT C, PCHANNEGOWDA J. A Survey of Blockchain Based Government Infrastructure Information[C]// International Conference on Mainstreaming Block Chain Implementation (ICOMBI). 2020, 1-5.
[35] JABBAR K, BJORN P. Growing the Blockchain Information Infrastructure[C]// CHI Conference on Human Factors in Computing Systems. ACM, 2017: 6487-6498.
[36] DORRI A, KANHERE S S, JURDARK R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]// The International Conference on Pervasive Computing and Communications Workshops (PerCom Workshop). 2017: 618-623.
[37] DORRI A, KANHERE S S, JURDAK R. Towards an Optimized BlockChain for IoT[C]// The second IEEE/ACM conference on Internet of Things Design and Implementation (IoTDI 2017). ACM, 2017: 173-178.
[38] SINGH S, HOSEN A, YOON B. Blockchain Securi-ty Attacks, Challenges, and Solutions for the Future Distributed IoT Network[J]. IEEE Access, 2021, 9: 13938-13959.
[39] DING H, CHEN X F, LIN D Z. IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management [J]. Institute of Electrical and Electronics Engineers, 2021, 1(2144): 1-20.
[40] SPATARU A L, PUNGILA C P, RADOVANCOVICI M. A high-performance native approach to adaptive blockchain smart-contract transmission and execution[J]. Information Processing & Management, 2021, 58(4): 102561.
[41] KAMANASHIS B, MUTHUKKUMARASAMY V. Securing Smart Cities Using Blockchain Technology[C]// IEEE International Conference on Smart City. IEEE, 2016: 1392-1393.
[42] LEE B, LEE J H. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment [J]. Journal of Supercomputing, 2017, 73(3): 1152-1167.
[43] CHAKRAVORTY A, RONG C. Ushare: user controlled social media based on blockchain [C]// International Conference on Ubiquitous Information Management & Communication. 2017: 1-6.
[44] LNES S. Beyond Bitcoin Enabling Smart Government Using Blockchain Technology[C]// International Conference on Electronic Govern-ment and the Information Systems Perspective. Springer International Publishing, 2016: 253-264.
[45] GERSTL D S. Leveraging Bitcoin Blockchain Technology to Modernize Security Perfection Under the Uniform Commercial Code[M]. Springer International Publishing, 2016: 109-123.
[46] ZHU H, HOU M. Research on an Electronic Medical Record System Based on the Internet[C]// 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA). 2018: 537-540.
[47] INDUMATHI J, SHANKAR A, GHALIB M R, et al. Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unl-imited Health Care Services (BC IoMT U6 HCS) [J]. IEEE Access, 2020(8): 216856-216872.
[48] POONGUZHALI N, GAYATHRI S, DEEBIKA A, et al. A Framework For Electronic Health Record Using Blockchain Technology[C]// 2020 International Conference on System, Computation, Automation and Networking (ICSCAN). 2020: 1-5.

**FU Li-yu**, born in 1997, postgraduate. Her main research interests include blockchain and distrbuted system.

**LU Ge-hao**, born in 1977, double master. His main research interests include blockchain and software engineering.