区块链技术综述

沈鑫[1]，裴庆祺[1]，刘雪峰[2]
（1. 西安电子科技大学通信工程学院，陕西 西安 710071；
2. 西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘　要：区块链是一种广泛应用于新兴数字加密货币的去中心化基础架构，随着比特币的逐渐被接受而受到关注和研究。区块链技术具有去中心化，区块数据基本不可篡改、去信任化等特性，因此受到企业尤其是金融机构的追捧。阐述了区块链技术的核心技术原理，探讨了区块链技术的应用以及所存在的监管问题、安全问题，旨在对区块链技术的相关研究提供帮助。

关键词：区块链；数字货币；去中心化；分布式；共识机制
中图分类号：TP319
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2016.00107

Survey of block chain

SHEN Xin[1], PEI Qing-qi[1], LIU Xue-feng[2]
(1. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China;
2. School of Cyber Engeering, Xidian University, Xi'an 710071, China)

Abstract: With the wide spread of Bitcoin, block chain serving as the building block of digital currency becomes a hot spot in industry and academia. Due to the decentration of network, the unforgeability of block data, etc., block chain has attracted more and more attentions from financial institutions. The essential theory and core technique of block chain were surveyed, and the issues of management and security problems of block chain based applications were discussed. To help improve the block chain techniques is the goal.

Key words: block chain, digital currency, decentralization, distribution, consensus mechanism

1　引言

区块链是比特币的基础支撑技术，首次出现在中本聪（Satoshi Nakamoto）发表的《比特币：一种点对点式的电子现金系统》[1]，文中详细描述了如何建立一套全新的、去中心化的、不需要信任基础的点到点交易体系的方法，其可实现性已经被自 2009 年运行至今的比特币所证明。区块链技术的突出优势在于去中心化设计，通过运用加密算法、时间戳、树形结构、共识机制和奖励机制，在节点无需信任的分布式网络中实现基于去中心化信用的点到点交易，解决了目前中心化模式存在的可靠性差、安全性低、高成本、低效率等问题。虽然近几年比特币快速发展，但其交易的匿名性和作为货币的发行权无法被掌握，多数国家机构不承认其货币属性，而区块链凭借其独特的优势，吸引众多目光，相关研究和应用一时之间呈现井喷的趋势。区块链技术更是被认为是继大型计算机、个人计算机、互联网、移动社交之后的第 5 次颠覆式计算范式，是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第 4 个里程碑[2]。广义的区块链技术有望彻底重塑人类社会活动形态，为金融、科技、文化、政治等领域带来深刻的变革。

收稿日期：2016-07-15；修回日期：2016-10-11。通信作者：沈鑫，shenxinzh@gmail.com

截至 2016 年 9 月, 有关区块链的学术研究成果仍然寥寥无几[3~18]，相关知识产权和专利也是一片空白，区块链领域更是呈现出技术和产业创新驱动的发展趋势[19~27]。本文系统地梳理了区块链技术的相关内容，包括区块链的起源、发展现状、基本原理、核心特点、相关应用及其存在的问题，为以后的研究提供启发和借鉴。

2 区块链概述

文献[1]中所描述的区块链是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构，并以密码学方式保证不可篡改和不可伪造的分布式去中心化账本，能够安全存储简单的、有先后关系的、能在系统内进行验证的数据[5]。区块链的出现解决了数字货币的两大问题：双重支付问题以及拜占庭将军问题[28~33]。双重支付问题是同一笔钱被使用了超过一次，是在原有的以物理实体（纸币）为基础的传统金融体系中自然可避免的问题。在区块链出现之前的数字货币，都是通过可信任的中心化第三方机构来保证，以前是银行，现在是支付宝、微信支付等。区块链技术通过共识机制和分布式账本，不需要可信第三方就可以解决双重支付的问题是数字货币的一大突破。拜占庭将军问题（Byzantine generals problem）[15]是现实世界问题的模型化，适用于分布式网络的简单抽象为“在缺少可信中心节点的情况下，分布式节点怎么达成共识建立互信的问题”。区块链使用“工作量证明”（PoW，proof of work）及“权益证明”（proof of stake）或其他的共识机制，再加上加密技术，使一个不可信网络变成可信的网络，所有参与者可以在某些方面达成一致，而无需信任单个节点。

区块链具有去中心化、网络健壮、灵活性、安全可信等特点。首先，区块链采用纯数学的方法建立分布式节点间的信任关系，形成去中心化的可信分布式系统，产生交易、验证交易、记录交易信息、进行同步等活动均是基于分布式网络完成的，是彻彻底底的去中心化。其次，区块链采用独特的经济激励机制来吸引节点完成工作（如挖矿），促使节点提供算力或其他资源，保证整个分布式网络的顺利运行。整个分布式网络所容纳的节点越多，其健壮性越强，除非一半以上的节点同时出现问题，否则分布式网络将会一直安全运行。再次，区块链提供用户可编程的脚本系统，大大增加了区块链应用的灵活性。在比特币中，脚本不是很成熟，多用于交易的用途；而在以太坊（Ethereum）中，更加完备、功能更加强大的脚本系统智能合约，使更为复杂更为高级的分布式应用得以实现[34]。最后，区块链的安全性是加密技术所保证的，整个分布式网络所提供的算力是非常惊人的, 想要篡改区块链中的数据，不仅只是在理论上可行，而且所花费的电力、设备等成本也是得不偿失的。

下面通过描述比特币的工作过程来一窥区块链的全貌。比特币网络的全节点无时无刻不在进行数学运算（挖矿、工作量证明），每个节点贡献自己的算力来竞争解决一个动态可调整的数学问题（进行 SHA256 运算的结果小于某个值），成功解决该数学问题的节点将获得一定数量的比特币（初始 50 比特币，每挖出 210 000 个区块减少一半）以及该区块的记账权，该节点将当前时间段的所有交易打包计入一个新的区块，获得基于自愿原则的交易手续费，所有的交易都会经过算法处理（SHA256），并且经过验证，产生一定格式的区块（按一定格式计算出的包含前一区块信息的块头，由树形结构组织的交易数据构成块体），最后将该区块链接到主链上。整个比特币网络周而复始，比特币网络顺利运行。“挖矿”是所有节点通过数学运算达成共识的过程，由于非对称算法 SHA256 的性质，理论上保证记账权获得的随机性。一笔交易数据经全部节点验证通过后，进行 SHA256 运算，与其他交易两两匹配，再进行 SHA256 运算，直到最后剩下一个“树根”，矿工将上一区块的散列值（SHA256 运算结果）、时间戳、本区块的计算难度值、一个随机数和本区块的“树根”（Merkle 树根）打包成块头，加上“交易树”（Merkle tree）作为块体，形成完整的区块添加到区块链上。由于每个区块都带有前一区块的特征，想要篡改一个区块的交易记录，必须要重新计算该块之后的所有区块，需要修改时间越久的区块，所花费的算力越大，一般来说，一个区块后面有 6 个区块，就无法被修改了（根据比

特币网络算力以及现有计算设备综合考虑)。

3　区块链架构与关键技术详解

本节使用比特币和以太坊的区块链架构为实例，详细描述区块链技术的基础架构、基本原理以及核心技术。比特币和以太坊是 2 种具代表性的区块链技术应用，一个是区块链技术的起源，另一个是区块链 2.0 的代表应用，市面上其他使用区块链技术的数字货币大都与之雷同，所以，比特币和以太坊的基础架构是研究学习区块链技术的重要实例。

比特币和以太坊的基础架构如图 1 所示。图 1 中虚线表示的是以太坊与比特币的不同之处。总体来说，数字货币的区块链系统包含底层的交易数据、狭义的分布式账本、重要的共识机制、完整可靠的分布式网络、网络之上的分布式应用这几个要素。底层的数据被组织成区块这一数据结构，各个区块按照时间顺序链接成区块链，全分布式网络的各个节点分别保存一份名为区块链的分布式账本，网络中使用 P2P 协议进行通信，通过共识机制达成一致，基于这些基础产生相对高级的各种应用。在该架构中，不可篡改的区块链数据结构、分布式网络的共识机制、工作量证明机制和愈发灵活的智能合约是具代表性的创新点。

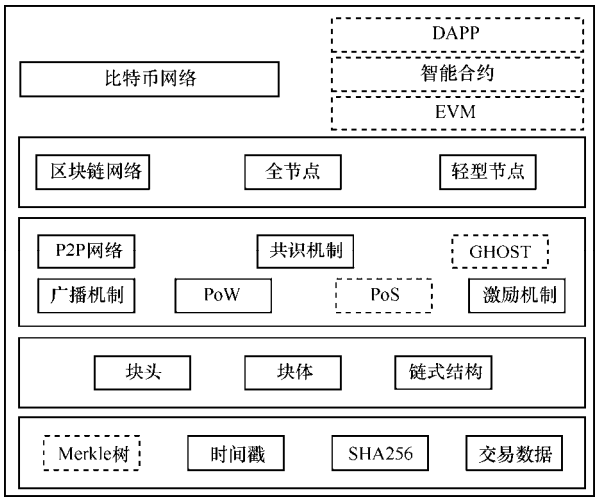


图 1　区块链基础架构

3.1　底层数据

在区块链系统中，底层数据并不是存储在区块链中的数据，这些原始数据需要进一步加工才能被写入区块内。底层数据最根本的是交易记录，其他的数据只是为了对消息记录进行封装。

交易数据：交易数据是带有一定格式的交易信息，以比特币为例，一条比特币交易信息应包含以下字段：4 B 的版本信息，用来明确这笔交易参照的规则；1~9 B 的输入计数器，表示被包含的输入数量；变长字节的输入，表示一个或多个交易输入（地址）；1~9 B 的输出计数器，表示被包含的输出数量；变长字节的输出，表示一个或多个输出（地址）；4 B 的时钟时间，表示一个 UNIX 时间戳或区块号[35]。

时间戳：时间戳被用来加盖在区块头中，确定了区块的写入时间，同时也使区块链具有时序的性质，时间戳可以作为区块数据的存在性证明，有助于形成不可篡改不可伪造的分布式账本。更为重要的是，时间戳为未来给予区块链技术的互联网和大数据增加了时间维度，使通过区块数据和时间戳来重现历史成为可能[5]。

SHA256 算法：区块链不会直接保存明文的原始交易记录，只是将原始交易记录经过散列运算，得到一定长度的散列值，将这串字母与数字组成的定长字符串记录进区块。比特币使用双 SHA256 散列函数，将任意长度的原始交易记录经过 2 次 SHA256 散列运算，得到一串 256 bit 的散列值，便于存储和查找。散列函数具有单向性、定时性、定长性和随机性的优点。单项性指由散列值无法反推得到原来的输入数据(理论上可以，实际几乎不可能)，定时性指不同长度的数据计算散列值所需要的时间基本一样，定长性指输出的散列值都是相同长度，随机性指 2 个相似的输入却有截然不同的输出。同时，SHA256 函数也是比特币所使用的算力证明，矿工们寻找一个随机数，使新区块头的双 SHA256 散列值小于或等于一个目标散列值，并且加入难度值，使这个数学问题的解决时间平均为 10 min，也就是平均每 10 min 产生一个新的区块。

Merkle 树：Merkle 树是区块链技术的重要组成部分，将已经运算为散列值的交易信息按照二叉树形结构组织起来，保存在区块的块体之中。Merkle 树的生成过程：将区块数据分组进行散列函数运算，将新的散列值放回，再重新拿出 2 个

数据进行运算，一直递归下去，直到剩下唯一的“Merkle 根”。比特币采用经典的二叉 Merkle 树，而以太坊采用了改进的 Merkle Patricia 树。Merkle 树的优点：良好的扩展性，不管交易数据怎么样，都可以生成一颗 Merkle 树；查找算法的时间复杂度很低，从底层溯源查找到 Merkle 根部来验证一笔交易是否存在或合法，时间复杂度为 lb N，极大降低运行时的资源占用；使轻节点成为可能，轻节点不用保存全部的区块链数据，仅需要保存包含 Merkle 根的块头，就可以验证交易的合法性。

3.2 分布式记账本

这里使用分布式记账本来代替区块链，是为了区别狭义的区块链和广义的区块链技术，前者是分布式记账本这一时序链式数据结构，后者是个完整的带有数学证明的系统框架。狭义的区块链结构如图 2 所示，每个区块分为块头和块体两部分，所有区块按照时序相链接，形成狭义上的区块链。

区块头：区块头的内容有上一区块头的散列值、时间戳、当前 PoW 计算难度值、当前区块 PoW 问题的解（满足要求的随机数），以及 Merkle 根。以比特币为例，具体的数据格式为：4 B 的版本字段，用来描述软件版本号；32 B（256 bit）的父区块头散列值；32（256 bit）字节的 Merkle 根；4 B 的时间戳；4 B 的难度目标；4 B 的 Nonce（随机数，问题的解）。区块头设计是整个区块链设计中极为重要的一环，区块头包含了整个区块的信息，可以唯一标识出一个区块在链中的位置，还可以参与交易合法性的验证，同时体积小（一般不到整个区块的千分之一），为轻量级客户端的实现提供依据。

区块体：区块体包含了一个区块的完整交易信息，以 Merkle 树的形式组织在一起。如图 2 所示，Merkle 树的构建过程是一个递归计算散列值的过程，以图中为例，交易 1 经过 SHA256 计算得到 Hash 1，同样算得 Hash 2，将 2 个散列值串联起来，再做 SHA256 计算，得到 Hash12，这样一层一层地递归计算散列值，直到最后剩下一个根，就是 Merkle 根。可以看到，Merkle 树的可扩展性很好，不管交易记录有多少，最后都可以产生 Merkle 树以及定长的 Merkle 根。同时，Merkle 树的结构保证了查找的高效性，N 个叶子节点的 Merkle 树最长查找路径长度为 lb N，这种高效在大交易规模中异常明显。

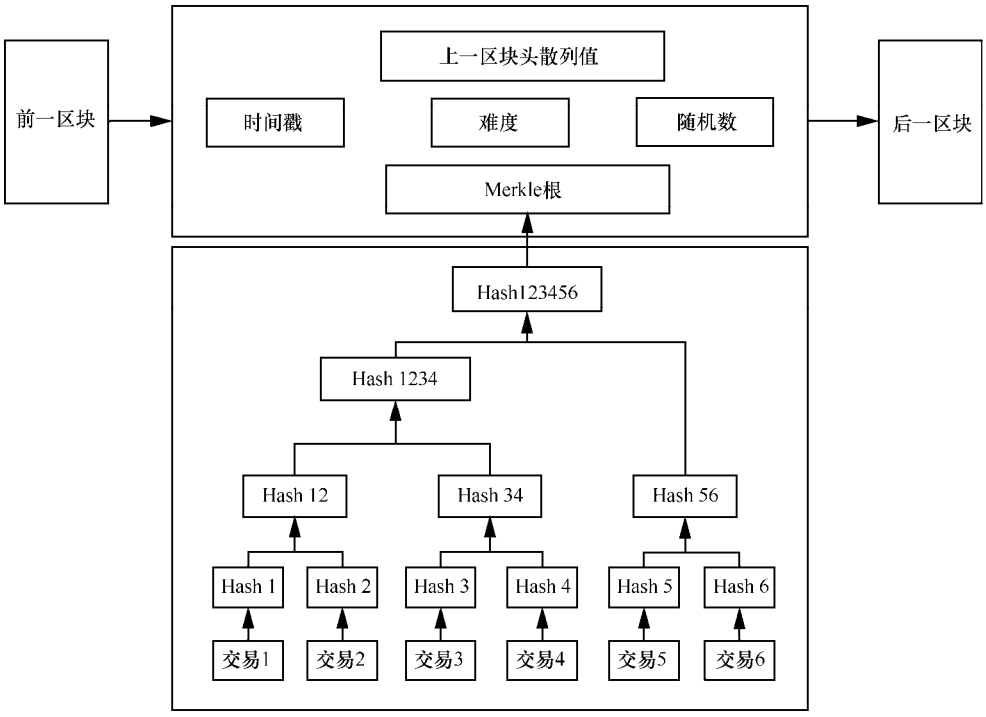


图 2 分布式记账本模型

链式结构：除了创世区块以外，所有区块均通过包含上一区块头的散列值的方法构成一条区块链。同时，由于包含了时间戳，区块链还带有时序性。时间越久的区块后面所链接的区块越多，修改该区块所花费的代价也就越高，这里借用一个形象的比喻，区块链就好比地壳，越往下层，时间越久远，越稳定，不会轻易发生改变。区块链在增加新区块的时候，有很小的概率发生“分叉”现象，即同一时间挖出 2 个符合要求的区块。对于“分叉”的解决方法是延长时间，等待下一个区块生成，选择长度最长的支链添加到主链，“分叉”发生的概率很小，多次分叉的概率基本可以忽略不计，“分叉”只是短暂的状态，最终的区块链必然是唯一确定的最长链。

创世区块：每一个区块链都有一个特殊的头区块，不管从哪个区块开始追溯，最终都会到达这个头区块，即创世区块。这里不得不提到比特币的创世区块，它在北京时间 2009 年 1 月 4 日 02:15:05 被中本聪生成，是比特币诞生的里程碑，也是数字货币的新纪元。中本聪在比特币创世块中留下了一句话“The Times 03/Jan/2009 Chancellor on brink of second bailout for bank”，是当天的头版文章标题。中本聪的引用，既是对该区块产生时间的说明，也是对旧有银行系统面对金融危机脆弱表现的冷嘲[36,37]。

3.3　组网方式和核心机制

狭义的区块链，即分布式账本的内容上面已经介绍完毕，将这个账本用起来才是区块链技术的关键所在。基于分布式账本之上的区块链网络，采用对等式网络——P2P 网络（peer-to-peer network）将所有节点连接在一起，设计 PoW 或其他共识机制使无信任基础的双方在不需要第三方的情况下建立互信，使用广播的方式传播交易信息，加上激励机制来保证节点提供算力以维持整个网络的顺利运行。

P2P 网络：区块链网络的去中心化来自于采用 P2P 组网方式，网络中每个节点均地位对等且以扁平式拓扑结构相互连通和交互，不存在任何中心化的特殊节点和层级结构，每个节点均会承担网络路由、验证交易信息、传播交易信息、发现新节点等工作。

广播机制：区块链网络公布交易信息的方式是广播，生成交易信息的节点先将信息广播到相连接的节点，节点验证通过后就会再进行广播，信息会以极快的方式被全网中的节点接收。实际上，并不需要全部节点都保留这条交易信息，只要保证大多数（51%）节点接收到，就可以认为交易通过。如果这条交易信息有问题，如交易者的余额不足以支付，接收到错误消息的节点验证不通过，就会废弃该交易数据，不会对它再进行广播。新区块的生成也是通过广播来确认的，找到满足条件的随机数后进行广播，记过验证后确认新区块的记账权，生成新的区块，全网进行同步，将该块添加到主链上。

共识机制：分布式网络的核心难题是如何高效地达成共识，就好比现有的社会系统，中心化程度高的、决策权集中的社会更容易达成共识，像独裁和专制，但是社会的满意度很低；中心化程度低的、决策权分散的社会更难达成一致，像民主投票，但是整个社会的满意度更高。“任何基于网络的数据共享系统，都最多拥有以下 3 条中的 2 条：1) 数据一致性（C）；2) 对数据更新具备高可用性（A）；3) 能容忍的网络分区（P）”，即 CAP 理论[38]，分布式网络已经带有了 P，那么 C 或 A 只能在两者中选择一条。如何在一致性和可用性之间进行平衡，在不影响实际使用体验的前提下还能保证相对可靠的一致性，是研究共识机制的目标。早期的比特币采用高度依赖节点算力的 PoW 机制来保证比特币网络分布式记账的一致性，随着各种竞争币种的发行，更多相似的共识机制得以出现，PoS 就是一种基于 PoW 并且进行改进的共识机制。

PoW 共识机制：PoW 机制是由中本聪所设计的适用于比特币系统的共识机制，其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。在比特币中，所有参与“挖矿”的节点都在遍历寻找一个随机数，这个随机数使当前区块的区块头的双 SHA256 运算结果小于或等于某个值，找到符合要求的随机数的节点获得当前区块的记账权，获得一定数额的比特币作为奖励。另外，引入动态难度值，使求解该数学问题所花费的时间在 10 min 左右。PoW 共识机

制具有十分重要的意义，将比特币的发行、交易和记录完美地联系起来，同时还保证了记账权的随机性，确保比特币系统的安全和去中心化。

GHOST（Greedy Heaviest Observed Subtree）协议：GHOST 协议是为了解决比特币使用 PoW 算力竞争引起的高废块率带来的算力浪费问题。废区块指的是在新块广播确认的时间里“挖”出的符合要求的区块。GHOST 协议提出在计算最长链时把废区块也包含起来，即在比较哪一个区块具有更多的工作量证明时，不仅有父区块及其祖先区块，还添加其祖先区块的作废后代区块来计算哪个块拥有最大的工作量证明。在以太坊中，采用了简化版 GHOST 协议，废区块只在五代之间参与工作量证明，并且废区块的发现者也会收到一定数量的以太币作为奖励。

PoS 共识机制：PoW 共识机制有明显的缺点，算力资源被过多地浪费掉，PoS 共识机制是为了解决 PoW 的缺陷而提出的替代方案。PoS 本质上是采用权益证明来代替 PoW 的算力证明，记账权由最高权益的节点获得，而不是最高算力的节点。权益证明就是资源证明，拥有最多资源的节点挖矿的难度最小。以太坊目前采用的仍然是 PoW，但是正在开发的下一版本将会转为 PoS 共识机制。

激励机制：激励机制是区块链技术中的重要一环，以比特币为例，开采出新的区块的节点会得到一定数量的比特币和记账权，记账权使节点在处理交易数据的时候得到交易费用。比特币的交易费用基于自愿原则，提供交易费用的交易会被优先处理，而不含交易费用的交易会先放在交易池中，随时间的增加而增加其优先级，最终还是会被处理。激励机制保证了整个区块链网络的保持向外扩张，促使全节点提供资源，自发维护整个网络。以比特币为例，目前整个比特币网络的算力已经达到 800 000 000 Gh/s，超过了全球 Top 500 超级计算机的算力总和，想要对整个比特币网络做出影响几乎不可能。

3.4 区块链节点

在最初的区块链网络设计中，不存在任何中心化的特殊节点和层级结构，每个节点完全对等，承担着网络路由、验证交易信息、传播交易信息、发现新节点等工作。但是实际上物理设备是存在明显性能差距的，以比特币网络为例，可作为节点的设备有个人计算机、服务器、专为比特币挖矿设计的矿机，以及移动端，它们提供的算力相差了几个数量级，并且存储空间也不同。目前市面上可见的移动端存储空间最大不过 100 GB 左右，而存有全部数据的区块链数据总量已经超过 60 GB，想要将移动端作为全节点无疑是不现实的。于是有了全节点和轻型节点，全节点是传统意义上的区块链节点，包含有完整的区块链数据，支持全部区块链节点的功能。全节点通常是高性能的计算设备，比特币刚面世时依靠 CPU 来提供算力，后来使用 GPU，发展到现在是专门设计将 SHA256 算法固化到硬件的矿机，算力成几何增长趋势。轻型节点是依靠全节点存在的节点，不用为区块链网络提供算力，只保存区块链的区块头，由于区块头包含了 Merkle 根，可以对交易进行验证。轻型节点多为移动端，如智能手机、平板电脑、移动计算机等。

3.5 智能合约

区块链技术的智能合约是一组情景——应对型的程序化规则和逻辑，是部署在区块链上的去中心化、可信息共享的程序代码。签署合约的各参与方就合约内容达成一致，以智能合约的形式部署在区块链上，即可不依赖任何中心机构自动化地代表各签署方执行合约[5]。智能合约具有自治、去中心化等特点，一旦启动就会自动运行，不需要任何合约签署方的干预。

智能合约的运行过程如下。智能合约封装预定义的若干状态、转换规则、触发条件以及对应操作等，经过各方签署后，以程序代码的形式附着在区块链数据上，经过区块链网络的传播和验证后被记入各个节点的分布式账本中，区块链可以实时监控整个智能合约的状态，在确认满足特定的触发条件后激活并执行合约。

智能合约对区块链有重要的意义，智能合约不仅赋予了区块链底层数据可编程性，为区块链 2.0 和区块链 3.0 奠定了基础；还封装了区块链网络中各节点的复杂行为，为建立基于区块链技术的上层应用提供方便的接口，拥有了智能合约的区块链技术前景极为广阔。例如，对互联网金融的股权招募，智能合约可以记录每一笔融资，在

成功达到特定融资额度后计算每个投资人的股权份额，或在一段时间后未达到融资额度时将资金退还给投资人。还有互联网租借的业务，将房屋或车辆等实体资产的信息加上访问权限控制的智能合约部署到区块链上，使用者符合特定的访问权限或执行类似付款的操作后就可以使用这些资产。甚至与物联网相结合，在智能家居领域实现智能自动化，如室内温度湿度亮度的自动控制、自动门允许特定的人进入等。

现有水平的智能合约及其应用本质逻辑上还是根据预定义场景的“ IF-THEN ”类型的条件响应规则，能够满足目前自动化交易和数据处理的需求。未来的智能合约应具备根据未知场景的“ WHAT-IF ”推演、计算实验和一定程度上的自主决策功能，从而实现由目前“ 自动化 ”合约向真正“ 智能 ”合约的飞跃[5]。

3.6　上层应用

前文系统地介绍了区块链技术，有了一个比较全面的系统性概念之后，可以更为深入地研究基于区块链技术的上层应用。目前的区块链应用都具有相似的架构，各家的重心在于研发不同的上层应用。比特币是经典区块链应用，所使用的区块链技术十分具有研究学习价值。然而，比特币本身作为一种数字货币来说存在局限性，虽然可以用很低的成本开发出其他的数字货币（实际市面上存在很多类似的竞争币），但是很难开发出除了数字货币之外的应用。以太坊是另一个使用区块链技术的产品，不仅在底层解决了区块链原有的一些问题，更是把区块链技术进行封装，降低区块链和具体上层应用的耦合性。以太坊提供功能强大的智能合约语言来进行上层应用的设计，开发者们通过部署智能合约可以方便快捷地开发区块链应用。以太坊的最终目标是将所有节点连接起来，成为一台拥有恐怖算力的虚拟机，虚拟机上运行着各种各样的分布式应用，彻底改变现有的网络架构。

4　区块链技术存在的问题

毋庸置疑任何技术都存在局限性，虽然区块链技术有自身的独特优势，但也不是解决所有问题的灵丹妙药。区块链技术还处在发展初期，存在诸多问题。本节从各个角度描述目前区块链技术有待解决的问题。

4.1　效率问题

效率是区块链技术可用性的保证，目前区块链的效率问题表现为以下几点。

分布式记账本数据量问题。分布式记账本记录了整个区块链网络从诞生到当前时间节点的一切交易记录，在保证区块链数据不可篡改的同时，带来了存储和同步的问题。上文提到过，目前比特币的数据量已经超过了 60 GB，数据量巨大，更令人头疼的是比特币从诞生到现在才不过短短 7 年，按照比特币愈发活跃的走势来看，账本过大是一个急需解决的问题。

同步时间问题。截至目前为止，比特币网络已经有 43 万个区块被开采出来，新添加进网络的节点同步账本所花费的时间就长达几天。如果没有改进的方案，时间越往后增加，新节点的代价就越大，甚至会阻碍区块链网络的扩张。

交易效率问题。以比特币为例，一秒只能处理 7 笔交易，而确定交易则要等待下一个区块产生，平均为 10 min。这种交易效率远远无法满足需求，虽然现在有了些研究成果，如闪电网络（lightning-network）[39]，但仍然缺少全面解决效率问题的方法。

4.2　中心化问题

算力证明导致节点的不对等。理论上，在区块链网络中每个节点被平等地对待，但是为了挖矿获得经济回报，开始进行硬件竞赛，导致节点之间的不对等（使用矿机的节点自然比使用 CPU 的节点更容易挖到矿）。目前，使用 CPU 挖比特币，理论概率几乎等于 0。区块链记账权的随机性受到破坏，违背了设计初衷。

算力证明导致的产业化趋势。同样，也是为了挖矿获得经济收益，产生了矿池。矿池指的是产业化规模化挖矿，通常在地理位置上选择靠近水电站的地区，在硬件上选择专门用于挖矿的矿机，几千上万台机器集群，试图用较低的成本来挖矿获得收益。以比特币为例，据统计，有约 60% 的算力来自中国的矿池，比较有名的三大矿池是 F2Pool、BTCChina Pool 以及 Huobi Pool。算力的集中破坏了分布式设计，并且带来了著名的“ 51%

攻击”威胁。

51%攻击问题。简单地说，就是在投票制中掌握了半数以上的选票，可以使任何提案得到通过，放在比特币环境下就成为实现双重支付的手段，一笔交易只要半数以上的节点通过，那么对整个网络来说就是合法有效的。虽然理论上掌握分布式网络的大多数算力是几乎不可能的事，但是矿池的出现使“51%攻击”具备了实施的可能，并且算力的集中破坏了去中心化，带来种种安全隐患，所以开发新的共识机制是目前区块链研究的一个主要方向。

中心化趋势。分布式网络的中心化趋势也是一大问题，前面所说矿池的出现不仅带来了“51%攻击”的威胁，也影响了整个分布式网络的稳定性，如果一个矿池发生问题（如停电、火灾等），整个网络都会受到影响，削弱了分布式网络的优势。

4.3 隐私和安全问题

虽然区块链技术采用密码学相关技术，具有很高的安全性，但是整个区块链网络在隐私和安全方面仍然存在薄弱环节。

数据隐私问题。以比特币为例，比特币使用地址进行交易，具有匿名性，但是交易记录却完全公开，一个地址的所有交易记录全部都可以被查到，一旦将地址与真实身份联系起来，后果十分严重。

使用安全问题。区块链技术本身的安全性很高，采用非对称密钥机制，保证了安全性和有效性。但是对私钥的使用和保存状况却令人堪忧，即使 256 bit 的私钥表现成 50 个字符长度形式，依然难以记忆，使用其他软件进行辅助交易是必然的选择，但这类软件的安全性就值得商榷，交易网站或者个人的比特币被盗的消息络绎不绝，使用安全问题需要引起人们的重视。

4.4 公有链、联盟链和私有链的问题

根据区块链网络中心化程度的不同，分化出 3 种不同应用场景下的区块链。1) 允许任何节点都可以加入区块链网络，查看区块链上任意信息的区块链被称为公有链，最初的区块链都是公有链，如比特币。2) 允许授权的节点加入网络，可以根据权限查看信息，往往被用于几个公司或机构之间的区块链被称为联盟链或行业链。3) 所有网络中的节点都被掌握在一家公司或机构手中，被称为私有链、不管是公有链，联盟链还是私有链都是区块链技术在不同场景下的应用，还处于发展初期的区块链技术在发挥其独特优势的同时，也带来了诸多挑战。公有链的问题在上面已经简要描述过，在此不再赘述。

联盟链的问题。联盟链作为一种带有权限机制的区块链，需要考虑的问题有很多。首先，是准入权限问题，一个节点如何被通过允许加入区块链，是人工鉴别还是采用身份验证机制；其次，是区块链数据的查阅权限问题，很明显企业和机构的数据都是存在保密等级的，拥有不同等级权限的节点只能看到本层及本层以下的数据，如何进行查阅权限的分配和数据保密等级的划分是主要问题；再次，联盟链中是否应该存在一种机制，保证等级较低的节点无法直接与等级高的节点进行交易，就像在生活之中，普通人去银行办业务，只会去找柜员而不是去找行长一样，一旦出现这种跨等级的交易，应该有特别措施进行处理；最后，是匿名性和数据透明性以及审计便利性的综合问题，如果需要保留匿名性，各个公司的审计就无法开展。如果为了方便审计不保留匿名性，就需要降低数据的透明性（毕竟一个公司并不想其他公司知道自身的准确数据），如将交易数据进行加密，但这样就增加了审计的工作量，总之是一个需要综合考虑的问题。

私有链的问题。私有链多用于一个公司或机构的内部，也存在与联盟链类似的问题。首先，是细粒度的可视权限分配问题，即对数据的访问权限要细化到每一个账户，跟联盟链的查阅权限类似；其次，是效率问题，私有链的节点都是被掌握的可信节点，自然不需要 PoW 共识机制，不仅浪费算力，还不够高效，考虑使用其他高性能分布式一致性解决方法；最后，是私有链本身的安全问题，过于集中的私有链抵御攻击的能力跟前 2 种区块链相比差很多，尤其是如果攻击来自内部，修改“理论上不可篡改”的区块链也是可以做到的。

5 结束语

自 2009 年到 2016 年，区块链技术已经走过

了 7 个春秋，经历了区块链 1.0 时代，目前处于区块链 2.0，正在向区块链 3.0 稳步迈进。区块链 1.0 更适合被称作狭义区块链技术的时代, 其代表为比特币；区块链 2.0 是功能强大的智能合约时代，可以实现更为高级更为复杂的功能，大大扩宽区块链技术的应用场景；至于区块链 3.0，是将区块链技术的去中心化和共识机制发展到新的高度、影响全人类意识形态的时代。

目前，受到较多关注的研究方向是去中心化自治社会（DAS, decentralized autonomous society），这是一个从去中心化应用（Dapp, decentralized application）逐渐发展到去中心化自治组织/公司（DAO/DAC, decentralized autonomous organization/decentralized autonomous corporation），最后实现 DAS 的发展方向[40,41]。区块链技术天然契合分布式社会系统的概念，其中每个节点都将作为分布式系统中的一个自治的个体，随着区块链生态体系的逐步完善，自治节点通过更为复杂的智能合约参与各种 Dapp, 形成特定组织形式的 DAO 和 DAC，最终形成 DAS[42]。

区块链技术也许是实现人工智能的一个途径，智能合约被设计得越来越自动化，智能化和复杂化，考虑将现有的研究成果移植到区块链上来，使其得到进一步发展。

本文系统性地介绍了区块链技术的原理技术和应用，是对目前区块链技术研究成果的一个总结。目前，区块链技术的基础理论和技术研究还处于起步阶段，虽然出现了很多使用区块链技术的商业产品，但缺少理论研究，无法对产品进行支撑，不利于区块链技术的长远发展。希望本文能为未来的研究提供参考与启发。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoi n.pdf.

[2] SWAN M. Blockchain: blueprint for a new economy[M]. USA: O'Reilly Media Inc, 2015.

[3] 赵赫, 李晓风, 占礼葵, 等. 基于区块链技术的采样机器人数据保护方法[J]. 华中科技大学学报(自然科学版), 15, 43(Z1): 216-219.
ZHAO H, LI X F, ZHAN L K, et al. Data integrity protection method for icroorganism sampling robots based on blockchain technology[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015,43(Z1):216-219.

[4] 丁未. 基于区块链技术的仪器数据管理创新系统[J]. 中国仪器仪表, 2015 (10): 15-17.
DING W. Block chain based instrument data managementsystem[J]. China Instrumentation, 2015, (10): 15-17.

[5] 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 Y, WANG F Y. Block chain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016,42(4): 481-494.

[6] SWAN M. Block chain thinking: the brain as a decentralized autonomous corporation[J]. IEEE Technology and Society Magazine, 2015, 34(4): 41-52.

[7] DAVIDSON E. Hive mentality or blockchain bloat?[J]. New Scientist, 2015, 228(3043):52.

[8] ANONYMOUS. New kid on the blockchain[J]. New Scientist, 2015, 225(3009): 7.

[9] GODSIFF P. Bitcoin: bubble or blockchain[C]//The 9th KES International Conference on Agent and Multi-Agent Systems: Technologies and Applications (KESAMSTA). 2015, 38: 191-203.

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

[11] WILSON D, ATENIESE G. From pretty good to great: enhancing PGP using Bitcoin and the blockchain[C]//The 9th International Conference on Network and System Security, New York. 2015,: 368−375.

[12] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing privacy: using blockchain to protect personal data[C]//The IEEE Security and Privacy Workshops (SPW 2015). 2015:180-184.

[13] KYPRIOTAKI K N, ZAMANI E D, GIAGLIS G M. From Bitcoin to decentralized autonomous corporations: extending the application scope of decentralized peer-to-peer networks and blockchains[C]//The 17th International Conference on Enterprise Information Systems(ICEIS2015). 2015: 284-290.

[14] ANDRYCHOWICZ M, DZIEMBOWSKI S. PoW-based distributed cryptography with no trusted setup[C]//Advances in cryptology—CRYPTO. 2015:379-399.

[15] SWAN M. Blockchain thinking: the brain as a decentralized autonomous corporation [J].IEEE Technology and Society Magazine, 2015, 34(4):41-52.

[16] ELDRED M. Blockchain thinking and euphoric hubris [J]. IEEE Technology and Society Magazine, 2016, 35(1):39-39

[17] GOBEL J, KRZESINSKI A E, KEELER H P, et al. Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 2016.

[18] YUE X, WANG H J, JIN D W, LI M Q, JIANG W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical System, 2016, 40(10): 1-8.

[19] Factom white paper 1.0. Business processes secured by immutable audit trails on the Blockchain[EB/OL]. https://www.factom.com/devs/docs/guide/factom-white-paper-1-0.

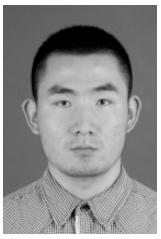
[20] Colored coins introduction [EB/OL]. https://github.com/Colored-Coins/Colored -Coins-Protocol-Specification/wiki/Introduction.

[21] Antshare white paper[EB/OL].https://github.com/AntShares/ AntShares.wiki.git.

[22] Nasdaq LINQ. Building on the Blockchain[EB/OL].http://business.nasdaq.com/Docs/Blockchain%20Report%20March%202016_tcm

5044-26461.pdf .
[23] R3CEV[EB/OL].https://r3cev.com/.
[24] Maidsafe white paper. MaidSafe.net announces project SAFE to the community[EB/OL].https://github.com/maidsafe/Whitepapers/blob/master/Project-Safe.md.
[25] Hyperledger. Project Charter[EB/OL]. https://www.hyperledger. org/about/charter.
[26] Microsoft azure baaS[EB/OL]. https://azure.microsoft.com/zh-cn/solutions/blockchain.
[27] IBM blockchain[EB/OL]. http://www.ibm.com/blockchain/.
[28] The Byzantine Generals problem[EB/OL].http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf.
[29] FAN J, YI L T, SHU J W. Research on the technologies of Byzantine system[J]. Journal of Software, 2013, 24(6):1346-1360
[30] NELSON M. The Byzantine General's problem:an agreement protocol for distributed system[EB/OL]. http://www.drdobbs.com/cpp/the-byzantine-generals-problem/206904396.
[31] LAMPORT L. The weak byzantine generals problem[J]. Journal of the ACM (JACM), 1983, 30(3): 668-676.
[32] FEDOTOVA N, VELTRI L. Byzantine generals problem in the light of P2P computing[C]// The International Conference on Mobile & Ubiquitous Systems: Networking & Services. 2006:1-5.
[33] REISCHUK R. A new solution for the byzantine generals problem[J]. Decision Support Systems, 1985, 1(2):182.
[34] Ethereum white paper. A next-generation smart contract and decentralized application platform[EB/OL].https://github.com/ethereum/wiki/wiki/WhitePaper.
[35] ANTONOPOULOS A M. mastering bitcoin: unlocking digital cryptocurrencies[M]. USA:O 'Reilly Media Inc., 2014.
[36] Bitcoin Sourcecode[EB/OL].https://github.com/bitcoin/bitcoin/.
[37] Bitcoin Website [EB/OL]. https://bitcoin.org/.
[38] NANCY L, SETH G. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services[J]. ACM SIGACT News, 2002, 33(2): 51-59.
[39] POON J. The Bitcoin lightning network[EB/OL]. https://lightning.network/lightning- network-paper-DRAFT-0.5.pdf.
[40] VIGNA P, CASEY M J. The age of cryptocurrency: how Bitcoin and the blockchain are challenging the global economic order[M]. St. Martin's Press. 2015
[41] HODSON H. Bitcoin moves beyond mere money[J]. New Scientist, 2013, 220(2945):24.
[42] The Economist. The DAO of accrue: a new, automated investment fund has attracted stacks of digital money [N].2016.

作者简介：



沈鑫（1994-），男，陕西宝鸡人，西安电子科技大学硕士生，主要研究方向为区块链安全。

裴庆祺（1975-），男，广西玉林人，西安电子科技大学教授、博士生导师，主要研究方向为信任管理、无线网络安全、区块链安全。

刘雪峰（1985-），男，安徽亳州人，西安电子科技大学讲师，主要研究方向为云计算安全、区块链安全、物理层安全。