区块链技术研究与发展综述*

游玲 李陶深** 葛志辉

广西大学计算机与电子信息学院，南宁，530004

摘 要 区块链是一种非常强大的工具，致力于改变世界是如何移动资产、保护系统、建立数字身份。我们需要了解区块链是如何工作的，以及怎么更好地利用这一技术，因为它们将在不久的将来融入到许多日常在线交互中。针对区块链技术络这一研究领域，本文分别从区块链技术组成、区块链共识协议、区块链中的信任、区块链应用 5 个方面综述近些年的研究现状与相关结论，旨在为区块链技术的研究发展提供参考。

关键字 区块链，智能合同，共识协议，信任

Blockchain Technology: A Review of Recent Advances

You Ling Li Taoshen Ge Zhihui

School of Computer, Electronics & Information
Guangxi University
Nanning 530004,China
tshli@gxu.edu.cn

Abstract—Blockchain is a very powful tool dedicatd to changing how the world moves assets, protects systems, and establishes digital identities. We need to understand how blockchain works and how to make better use of this technology, because they will be integrated into many daily online interactions in the near future. Aiming at the new research field of blockchain technology, this paper summarizes the research status and relevant conclusions recently from four aspects: blockchain technology composition, blockchain consensus protocol, trust in blockchain and blockchain application. This paper provides reference for the research and development of blockchain technology.

Key words—Blockchain, smart contract, consensus algorithm, trust

1 引 言

区块链技术被认为是计算机革命的“第五次进化”，在互联网以一种去中心化的方式建立信任层。许多人认为，它是对 2007 年美国房地产泡沫破裂后几年银行系统腐败的一种反应[1]。由于它提供了一种创新的分布式数据库与开源网络的结合，近年来区块链技术得到了越来越多的关注[2]。

区块链之所以广受欢迎的一点是可以在没有信任基础的双方之间进行价值转移，且许多复杂的应用程序可以建立在这个创新基础上，它是一种能够确保交易安全、具有潜在应用性的工具[3]。

粗略地说，区块链技术指的是通过加密，在公共数据库中系统地永久记录曾经发生的每笔交易，网络中的所有相关参与者都可以验证信息和事务的合法性，保证透明公开。这种去中心化组织方式引起了人们的关注[3]。从本质上来说，区块链技术伴随着数字货币比特币产生,是一个具有全网一致性共识、去中心化、可编程和安全防篡改等特点的分布式数据账本[4]。它将社会使用了数千年的旧式模型与分布式数据库合并并在线上推广，可在数百万种设备上运行，并向所有人开放，目前在数字金融货币领域的应用最为广泛。

区块链的核心是允许不同的实体合作和协作，而不需要信任对方的数据安全或业务流程。 从历史上看，受信任的中间人或企业财团促成了这种情况的发生，但它们的间接费用很高，而且只是将信任转移到另一方。区块链将信任转移到一个客观的第三方网络上，最终转移到数学上。区块链使用数字信任系统，使用被称为节点的计算机网络来验证交易，并永久的记录保存交易历史记录。这样可以缩短交易的时间，提高数据准确性，降低成本。区块链不仅仅可以安全、匿名地移动、存储和管理数据信息，还包括任何其它有价值的事物，如头衔、契约、身份，甚至是选票。当数据是永久的和可靠的数字格式，你可以在网上处理交易，这些在过去都只能线下办理。所有保持模拟

*基金资助：本文得到广西科技计划项目（桂科 AD20297125）资助。
**通讯作者：李陶深，教授，tshli@gxu.edu.cn

的东西，包括产权和身份，现在都可以在网上创建和维护。缓慢的商业和银行流程，如货币线和基金结算，现在几乎可以立即完成。其中的信任是通过代码建立的，而不是通过可靠的中介机构（如政府和银行），消除了对中介机构的需求。

区块链技术的另一个关键特征是没有必要让可信的第三方提供系统的状态，系统中的每个用户都可以验证系统的完整性。要向区块链添加新区块，所有节点必须随着时间的推移达成共同协议；但是，允许出现一些暂时的分歧。该数字分类账本通过点对点网络将信息发送给所有用户，无论何时在其中添加新的交易块，都会为用户自动更新，因此，世界各地的节点都会收到完整的区块链副本。

与传统的数据库相比，区块链具有以下优势：

(1) 数字化。区块链用户可从世界任何地方访问，不受实际地点限制。

(2) 透明、可审计。每个用户都可访问相同的区块链，从而提高透明度和可审计性。

(3) 去中心化。区块链不受中央机构的控制，由网络中的所有节点进行决定。

(4) 不可变性。每个唯一链都是输入到该特定链的数据的永久历史，无论该数据代表什么，这些历史被锁定在一个无法被操纵的秩序中，当一个事务已经创建和发布时，它不能被删除或操作。

(5) 安全加密。区块链融合了加密学，所有数据都被安全地存储和加密，安全性得到保障。

2 区块链技术组成

每个基于区块链的网络都是一个复杂的系统，由许多独立的组件相互交互，以确保整个系统的运行。区块链技术的运作基于确定性功能和由此产生的可预测性，这是由于它们依赖哈希函数和公私密钥加密的数学特性，以及一些计算机科学机制和记录保存概念（如分类账）的混合。

2．1 节点

区块链是一个点对点的系统，没有中央权限管理数据流。在保持数据完整性的同时去中心化的关键方法之一是拥有一个由独立的用户/服务器组成的大型分布式网络。这意味着构成网络的计算机位于多个位置。这些计算机通常被称为节点，即节点是与运行和维护区块链网络的计算机。

区块链网络由“全节点”组成。这些节点自愿以“管理员”身份加入区块链。每个节点都有一个事务分类账本，它们不断检查要添加到链中的新事务是否有效。每个节点都包含了在该区块链中曾经记录过的所有交易的完整记录。

节点不受位置、身份限制，位于世界各地，可以由任何人操作。然而操作一个完整的节点需要消耗计算机资源，这个过程是困难、昂贵和耗时的，所以底层区块链算法会通过奖励去激励用户操作一个节点，奖励通常是价值令牌或加密货币，就像比特币一样。

2．2 事务

事务代表交易双方的交互。例如，对于加密货币，事务表示区块链网络用户之间加密货币的传输。不同区块链上事务包含的数据可以是不同的，但事务交易传输过程大致是相同的。区块链中一个节点向另外一个节点发送数据，可以包括相关标识符、发送节点的公钥、数字签名、事务输入、事务输出等[7]。

区块链中的每个块可以包含零个或多个事务。单个事务最少要包括输入和输出：输入通常是要转移的数字资产的清单。输出通常包括要接收数字资产的账户以及可接收的数字资产额。每个输出都指定了要转移到新节点的数字资产额、新节点的标识以及新节点要使用该资产所要满足的条件。如果发送节点提供的资产剩余，则发送回给发送节点。

事务除了用来转移资产，还可用来传送数据。例如，在应用了智能合同的区块链网络中，事务可以用来发送数据、处理数据、存储相关结果。事务通常由发送方用私钥进行数字签名，并且可在任意时间用相关的公钥进行验证，所以确定事务的真实性和有效性是十分重要的，真实性可确定发送节点可以访问这些数据，有效性保障事务满足区块链上各种协议的要求。

2．3 块

块是记录到分类账中的交易清单，由事务交易组成。区块链网络用户通过软件（桌面应用程序、智能手机应用程序、数字钱包、网络服务等）向区块链网络提交候选事务。软件将这些事务发送到区块链网络中的一个节点。一旦一个等待的事务被分配到节点上，它就必须在队列中等待，直到它被一个发布节点添加到区块链中。当一个发布节点发布一个块时，事务将被添加到区块链中，按块分组在一起，其他完整节点将检查已发布块中所有事务的有效性和真实性，如果包含无效事务，则不接受块；经过验证后的有效块，被附加到已确认的块链上。

一个块中包含块头和块数据。块头包含此块的元数据，即块号（在一些区块链网络中也称为块高）、前一个块头的哈希值（该数据块数据的一种散列表示法）、时间戳、块大小。块数据则包含提交到区块链网络的已验证的和真实的交易的列表，同时也可能还

存在一些其他的数据，包括交易的来源、接收对象和发送的金额。

区块链的第一个块叫“创世块”，通常被称为块 0，包含所有未来区块建立基础的协议，这是整个区块链的起源和基础。理论上讲，区块链可以包含无限数量的区块。每个区块通过包含前一个块的块头的哈希值把每个块链接在一起，按线性结构、时间顺序，从而形成区块链。随着越来越多的块被添加到链中，每个区块都可追溯起源到创世块。

2．4 加密技术与加密函数

区块链技术使用非对称密钥加密技术，也称为公钥加密技术。这种技术通过提供一种机制来验证事务的完整性和真实性，同时允许事务保持公开，从而使不知道或相互信任的用户之间能够建立信任关系[8]。

区块链上使用安全哈希算法对事务进行加密[9]，因为它创建了一个无法解密的单向函数。哈希函数创建一个数学算法，它将任何大小的数据映射到固定大小的比特字符串。一个位字符串通常长32个字符，表示被散列的数据。它允许个人独立地输入数据，散列该数据，并输出相同的结果，证明这个过程中数据没有变。SHA-256就是其中的一种类型，它可以生成一个几乎唯一的、固定大小为256位（32字节）的哈希[10]。许多计算机在硬件上支持这种算法，使它快速计算。

2．6 智能合约

智能合同于 1994 年由 Nick Szabo 提出，旨在于满足像付款条件、留置权、保密性以及合同执行等之类的常见合同条件，尽最大努力避免恶意条款和事故，减少合同双方对第三方中介的依赖[11]. 智能合同是一种执行合同条款的计算机化交易协议，是区块链网络中应用加密数字签名事务的代码和数据的集合，本质上是一串计算机代码，当满足特定的预定条件时，这些代码会自动执行，而无需任何进一步的行动[12]。智能合同特性是满足条件就自动执行，一旦执行，不可逆转，而自动执行确保了合同的执行不受法律中介人的监管。这是一项重要的计算机创新，因为它们允许不认识或不信任对方的个人进行合作，而不必担心对方不会按照双方商定的条款行事[13]。

智能合同由区块链网络中的节点按照预设计执行，并将结果记录在区块链中。智能合同是确定性的，定会基于给定的输入产生相同的输出。此外，执行智能合同的所有节点都同意在执行合同后的新状态。智能合同具有匿名性，交易双方可保持匿名交互，无需像传统纸质合同一样依靠第三方验证交易是否正确。

由于智能合同编码在去中心化区块链中，允许两个或多个交易方在任意时间、地点完成交易，不受位置限制。区块链网络用户创造事务，智能合同根据用户提供的数据，选择合适的方法执行服务，此时，代码作为可信任的第三方，保证数据的可靠和透明，节省完成交易的时间，降低成本。

引入智能合同后，国际贸易市场将会发生彻底的变化，交易速度极速提高，书面纸质工作大幅度减少，完成交易时间成本更低、效率更高。去中心化应用、去中心化自治组织、智能财产等的实现依赖于智能合同的引入，这也为自动化金融应用揭示了美好前景。

2．7 分布式分类帐本

分布式分类账本是一个共享和同步的数据库，是事务交易的集合。事务以块的形式组合在一起，并按链状的线性结构按时间链接在一起，创建一个不可改变的分布式分类账本。

分布式分类帐本可以存储各种数据，包括事务和智能合同，并由网络中的每个节点独立创建和维护，基于不同的共识机制进行操作。从本质上讲，分布式分类账是去中心化的，可被任何地点的任意用户访问。公众可审计、透明公开的特点在一定程度上增加了安全性，也是其它数据库所不具备的功能。此外，区块链建立在分布式分类账上，即该技术建立在点对点网络上，不需要中央机构对其进行控制和维护，节点之间的直接交互可节省时间和成本。

区块链技术支持使用分布式所有权和分布式物理架构的这种方法。人们对分类账分布式所有权的兴趣越来越大，这是由于与集中式数据库相比，分布式分类账提供更高的安全性，因为黑客必须攻击网络中所有节点才有可能成功，这都涉及相关的可能信任、安全和可靠性问题

3 区块链的共识机制

什么是共识机制？共识机制就是一个容错结构，区块链用来在分布式处理或多交易系统中就单个数据和网络整体存储数据达成某种共识，并维护分类账内容在整体网络中保持一致。换句话说，区块链共识机制是一种规则集，它决定了什么是有效的区块，进入的事物和什么链应该被信任[14]。

区块链技术的一个关键方面是确定哪个节点发布下一个块。每个发布节点很可能都是出于自身对经济利益的渴望，而不是由于其他发布节点、甚至是网络本身的福祉。为什么用户会传播另一个用户试图发布的块？当多个节点在大致相同的时间发布一个块时，谁来解决冲突？ 为了使这一工作有效，区块链技术使用共识机制，使一群相互不信任的用户能够一起工作。

每个区块链都有自己的算法，用于在其网络中为正在添加的事务创建协议。有许多不同的模型来创建共识，因为每个区块链都在创建不同类型的事务。 一

些区块链是交易价值，另一些是存储数据，另一些则是保护系统和合同。目前在各种区块链上主要使用了以下几种主要的共识机制。

3．1 工作量证明共识协议

工作量证明共识协议（Proof of Work Consensus Model）是比特币最初所使用的共识协议，针对系统用户之间几乎不信任的情况设计的。协议要求服务请求者进行某种类型的工作，通常是解决复杂数学方程式的计算机处理时间长短的形式。采矿软件使用复杂的算法来生成哈希，该哈希被用于该区块，即每个块都包含一个由“矿工”生成的有效哈希，这就是工作量证明协议要求的工作，当提出有效哈希时，将验证该区块并将其添加到区块链中。

工作量证明协议的工作原理是对第一个解决特定区块内密码难题的“矿工”给予块的奖励。“矿工”在完成工作后，就将有效块发送到区块链网络中的完整节点，然后继续计算下一个难题。难题的难度已由网络验证且难度可调整。这是一种减慢发布新块速度、防止恶意节点损害区块链的机制，因为任何想要试图篡改区块链都需要重新计算后面所有的块，这是一个庞大且很难做到的工程。这个机制的一个重要方面是待解决的难题是独立的，解决正在计算的难题不会影响节点解决未来出现的难题的可能性。

工作量证明协议的几个特点[15]：

（1）非对称难题：工作量证明是解决“难解决、易验证”证明的有效解。“矿工”解决难题很难，但是验证很容易，只需做一个散列来检查是否解决了难题。

（2）工作量远超工作质量：任何“矿工”都可以参与到解决难题之中，唯一优势纯粹是计算能力，这与计算机硬件设备相关。

（3）难题参数可调整：区块链网络提高或者降低难题的难度取决于“矿工”解决难题的时间长短。如果计算时间不在设定的参数范围内，计算就会做出相应调整。这种调整是为了保持这个难题的计算难度，从而维护网络的核心安全机制，旨在于确保任何节点都不能独占块生产，但此计算需要大量的资源消耗。

围绕工作量证明协议的一个主要关注是它在解决难题中消耗能量。目前没有可解决难题的快捷方式，反复试验的过程意味着，“矿工”必须使用大量设备和精力来运行软件并生成正确的哈希值。对于工作证明区块链，他们拥有的用户越多，使用区块链作为服务的成本就越高，系统越慢。另外一个存在的问题是PoW 区块链很容易受到 51%的攻击，其中大多数挖掘能力是由少数个人产生的，然后他们可以破坏区块链历史上写的记录。

3．2 股权证明共识协议

股权证明共识协议（Proof of Stake Consensus Model ）机制是基于每个节点在区块链中的拥有的货币数量（即其股份）[16][17]。即用户对系统的投资越多，他们就越希望系统正确操作运行，也就越不希望系统遭受颠覆。换句话说，区块链网络的股权证明使用用户的股份数量作为发布新数据块的决定因素。

股权证明协议首先由 Peercoin 区块链实现，用来减少工作量证明所带来的高成本，有了这个共识模型，就不必要进行 PoW 时需要的资源计算（涉及时间、电力和处理能力），潜在的矿工基础就得到了极大利用。在股权证明协议中，算法会随机选定一个“验证人”，被选择的这个节点拥有发布新块的权利，当节点拥有的加密货币越多的时候，被算法选择的概率就越大。在这个协议中，矿工因其拥有的股份或者所有权而得到回报，而不是计算机的计算工作能力。

区块链网络如何使用这些股份的方法可能会有所不同，主要有随机选择、多轮投票和选举系统。

（1）随机抽样（chain-based proof of stake）：区块链将关注网络中持有股份的所有用户，并根据他们的股份（即存储的加密货币总体数量）的比率在其中进行随机选择。因此，如果一个用户拥有整个区块链网络股份的 60%，他们将有 60%的概率被选择；那些拥有 5%的人被选择的概率就是 5%。

（2）多轮投票（Byzantine fault tolerance proof of stake）：区块链网络将选择几个节点作为发布下一个块的候选人，然后所有的持股用户都会投票给其中一个提议候选人，最终达成一致。在决定一个新区块之前，可能会进行几轮投票。此方法允许所有持股用户在选择哪个节点生产新块的过程中拥有发言权。

（3）选举系统：与传统选举类似，网络中的节点投票让被投的节点成为发布新块的节点，即获得最多票数的节点成为发布节点，可以验证和发布新块。区块链网络用户的投票权重与他们拥有的股权成正比，股权越大，投票所占权重就越大。可连续投同一个节点产生新块，这样可激励节点为保持发布节点的地位，而不产生恶意发布无效块的行为。

股权证明(POS)区块链通过要求正在处理事务的节点“入股”一些加密货币来创建信任，如果它们被抓到诈骗网络，这些加密货币可能会被没收。但 PoS 系统有自己的问题：少数团体可以汇总网络上的大部分价值并占有它。

3．3 轮循环共识协议

在轮循环共识协议（Round Robin Consensus Model）中，所有节点循环轮流创建发布块。为了防

止节点在可发布块期间无法发布块，系统设置了时间限制，在此段时间内，无权发布块的节点无法打断当前节点发布新的块[16][17]。

此协议可确保没有一个节点可以创建大部分的数据块。特点是直接、不用计算难题、较低功耗要求。缺点是仅适用于某些私有区块链。在节点彼此之间缺少信任的情况下，此模型不太适用于公共区块链网络。因为恶意节点可以在循环轮流产生块时不断添加其它节点，以增加其发布新数据块的可能性；甚至可以颠覆整个区块链。

3．4 权限/身份证明共识协议

权限证明也称为身份证明，其共识模型依赖于对发布节点现实身份的部分信任[16][17]。发布节点必须在区块链网络中证明和验证其身份的真实性。发布节点在区块链网络中的行为造成的影响与其声誉相关，所拥有的同意呼声高则声誉也高，不赞成呼声高则声誉低，声誉越低的节点能发布节点的可能性也就越低。

3．5 股权证明共识协议

失效时间证明共识协议（Proof of Elapsed Time Consensus Model）在失效时间证明(PoET)共识协议内，每个发布节点从其计算机系统内的安全硬件时间源请求等待时间，安全的硬件时间源将生成一个随机的等待时间，并将其返回给发布节点软件[16][17]。发布节点在给定的随机时间内空闲。一旦发布节点从空闲状态唤醒，它就会创建并发布一个块到区块链网络，提醒其他节点产生了新的块；其他仍处于然空闲状态的发布节点都会停止等待，整个过程就会重新开始。

该协议需要确保使用随机时间，因为如果没有随机选择等待时间，恶意发布节点只会等待默认情况下支配系统的最小时间；此模型还需要确保发布节点没有提前开始。这些问题可通过在一些计算机处理器上找到的可信执行环境中运行软件得到解决。“失效时间证明”算法可以在计算机主处理器的安全区域内运行，称为受信任的执行环境(TEE)。PoET 利用 TEE 的安全性来证明时间已经通过时间戳的交易而过去了。

3．6 中心化的共识协议

中心化的共识协议（DPOS）的算法允许令牌持有者通过投票系统选择块生产者[16][17]。DPOS 每 0.5 秒产生一组事务。这些区块分 126 轮生产，21 个当选的生产者每轮生产 6 个区块。所有块生产者都可以用相同的时间戳签署所有块，但同时签署的块生产者不能超过一个。当 15 个区块生产者签署后，该区块被视为不可更改。这种结构允许在平均 0.25 秒内确认事务。对于区块链技术来说，这是非常快的。如果块生产者承诺生成块，但未能这样做，则跳过该生产者，在 EOS 区块链中创建至少 0.5 秒的间隙。如果块生产者错过了它的块，并在 24 小时内没有生产任何块，则删除生产者。

在 DPOS 上的节点不像工作证明区块链上的节点之间是竞争关系，在 EOS 上，他们合作生产区块。如果一个区块生产者被抓住采取非利益行动，它将被淘汰。较少的节点，只有 21 个，意味着它非常集中，并且具有安全风险。

下面的表格 1 总结对比了各共识协议的优缺点。

表 1 多种共识算法优缺点

共识协议	目标	优点	缺点
工作量证明共识协议（PoW）	以计算难题的形式为新块的发布提供一个障碍。	向任何有硬件的人开放来解决这个难题。	计算消耗资源、能量高； 有可能会造成51%的攻击。
股权证明共识协议（PoS）	通过“流动民主”建立更有效的共识模型，参与者投票选择	计算强度比 PoW 小； 向任何希望持有加密货币的人开放。	利益相关者控制系统； 少数团体可以汇总网络上的大部分价值并占有它。
轮循环共识协议	提供一个系统，用于在信任的发布节点之间发布块。	需要的计算能力较低； 容易理解。	在发布节点之间需要大量的信任。
权限/身份证明共识协议	创建一个中央集权的共识进程以最小化块的创建和确认率。	快速确认； 允许块生产速率为动态的；	基于当前验证节点没有被破坏的假设； 导致集中的故障点；给定节点的声誉可能会受到高风险的影响。
失效时间证明共识协议（PoET）	为了给区块链网络提供一个更经济的共识模型，而牺牲了与 PoW 相关的更深层次的安全保证。	计算成本比 POW 更便宜。	硬件要求获取时间。
去中心化共识协议（DPOS）	许令牌持有者通过投票系统选择块生产者	产生块的速度快	较少的节点，只有 21 个，意味着它非常集中，并且具有安全风险

4 区块链中的信任

区块链的重要性在于它允许在交换有价值和隐私的信息这方面具有新的效率和可靠性，这些曾经需要靠第三方去促进，例如资金的流动和身份的真实性。

因为我们的社会和经济的大部分结构都是围绕建立信任，在信任破裂时强制信任，以及促进信任的第三方。而区块链可以提高信任度和透明度，这点是很重要的。

普遍认为在区块链网络是基于无信任建立的，没有“受信任的第三方”。以传统的角度看待这种方式，区块链在正确运行时，不需可靠的第三方持有交易双方或多方的账户，减轻了如道德、逃避等委托代理问题，实现了直接交付，可认为区块链网络没有具备信任关系的特征，是一种“无信任的技术”。

文献[18]中提出了一个不一样的观点：区块链不一定是一个无信任、去中心化的，其所提倡的信任与传统意义的组织形式有所区分，区块链所体现的信任是算法权威信任和对组织结构信任的融合。算法信任关注技术能力和透明度层面，对组织结构的信任则是涉及到社会层面的相关利益群体。例如在比特币区块链中，就已经开始将传统的信任理论数学化，将信任转移到第三方网络上，并最终转移到数学上。区块链的驱动力—共识协议的种类多样更是强调了这种新形式信任的重要性。在这种环境下，用户不仅需要信任算法权威，还需要信任软件开发人员开发、维护区块链。

在文献[19]中将对区块链技术的信任的讨论嵌入到关于信任和信心的更广泛的社会学和哲学讨论中，认为区块链技术不是一种“无信任的技术”，而是一种“信心机器”。作者从经济参与者（采矿池、采矿场）、核心开发人员和开源社区贡献者、加密货币和令牌持有者、监管机构四个不同角度出发，分析区块链技术将减少信任这些个体参与者中的任何一个的需要，但是它并没有完全消除对信任的需要。基于区块链的系统旨在产生对特定系统的“信心”，以最大限度地提高对系统的信心，作为间接减少信任需求的一种手段。

简而言之，基于区块链的网络被看作是“无信任”技术在很大程度上是存在误导性的。区块链网络不仅仅只是由代码、函数、数学理论组成，网络中还包括很多参与者，信任只是被转移，而不是被消除。

5 常用区块链

5．1 比特币区块链

比特币区块链的概念最初在 2008 年秋季作为白皮书引入，是世界上历史最悠久、规模最大的区块链之一，几乎所有区块链都借鉴了它的框架[20]。比特币区块链的提出旨在于解决拜占庭将军的问题，填补数字信任的窟窿，通过在网络中记录无法被删除的数据与信息重新构建信任。它是一个点到点的系统，数据是结构化的，每个完整的节点（在网络中运行的计算机）都包含网络中的所有数据。用户之间可以直接发送比特币，网络在这里充当受信任的第三方的角色。对于比特币，任何了解比特币协议的人都可以确信，网络将在特定条件下（每当矿工发现新区块）和特定速度（平均 10 分钟内）生成特定数量的新比特币（12.5 个比特币），而无需依赖于集中权力机构。

比特币区块链的特点是数据信息被永久记录，不可更改，而保持其稳健性的关键是去中心化。比特币区块链中数据块大小受到限制，处理事务的数量也受到限制，这些限制被编码到比特币协议中，有助于确保网络保持去中心化。它的核心特征之一是“没有人需要被信任“，“没有人可以假装是值得信任的一方”。

4．2 以太坊区块链

基于比特币区块链协议的附加应用程序在扩大规模上存在问题，且其没有能力编写像智能合同这样的脚本，对比特币区块链核心代码的升级超出了现实可能的范围，Vitalik Buterin 认为比特币需要一种脚本语言来促进新应用程序的开发，建议开发一种新平台，以支持更通用的脚本语言（以太坊）。

以太坊的白皮书于 2013 年发布，它是一个去中心化的开放软件区块链平台，运行在智能合同上，允许去中心化应用程序在其上运行[21]。以太坊区块链是有史以来最复杂的区块链之一，它可以做任何常规编程语言做的事情；具有文档和用户友好界面，可快速启动和运行，开发时间短，小应用程序更安全；应用程序之间交互能力强，是构建去中心化应用程序的最佳场所。以太坊区块链的创建将区块链的世界推向了不仅仅是交易数据；但是也面临着可扩展性限制，随着以太坊上庞大的应用程序的进行，会出现瓶颈，例如：需要验证的大量的积压事务会在平台高活跃期弹出。

5．3 Waves 区块链

Waves 区块链是由 Sasha Ivanov 在 2016 年创建[22]。当时大多数区块链软件是为终端用户创建，常使用命令行及其计算机终端，Waves 区块链则可供普通人使用，简单且直观。Waves 区块链是具有不同能力的相对新的区块链，将多个技术合并于一个简易且用户友好的界面（例如：多资产钱包、去中心化交易所、加密货币创建工具），能给公共区块链提供很快的速度，且用户不需要掌握如何编码就可从 Waves 区块链中有所收获。它是一个可供普通人使用的最简单、但最强大的区块链应用程序，非常方便用户、易于学习。

Waves 区块链与其它区块链不同在于它是基于股权证明协议的公共区块链平台，完全去中心化、透明、可审计；任何人都可以使用该平台，可在平台上推出、分发和交易货币；与其它区块链奖块励机制保护系统不同，该区块链通过现有账户的余额来“锻造”区块来保护网络，“锻造者”被给予交易费，而不是被奖励块。该区块链平台实现了去中心化的点对点交换、投票系

统、聊天系统、去中心化的域名系统。许多区块链都有一两个这些特性，而 Waves 区块链在一个新的网络模型上拥有所有这些特性。

5．4 Factom 区块链

Factom 是一个发布平台，核心是发布和验证任何数据，为构建在它之上的应用程序而创建，因可扩大区块链规模而被保留。Factom 协议旨在解决其他区块链的成本和容量限制，主要目标是确保数据和系统的安全[23]。 由于这一目标，Factom 通常被描述为发布引擎。它不同于其他公共区块链，具有独特的特性，使其成为发布数据流和创建安全系统的理想选择。Factom 软件正在被构建成管理人和事物的身份和安全的系统。

Factom 区块链允许用户将数据写入其分类账，并收取少量费用。事务大小仅限于 10 个 kibibytes，并且具有固定成本，与使用工作证明的区块链相比，它的成本更低，并且具有更大的交易量能力。将数据输入 Factom 的固定成本也是 Factom 的一个独特特征。

Factom 与其它区块链很好的集成，可以用于智能合同创建一个数据库，允许比存储证明系统更低的成本引用其它永久数据。而且链允许在子链中构造数据，这些数据可以单独解析，以证明任何事务的有效性，从而应用程序只从 Factom 块链中提取他们感兴趣的数据，而不需要下载完整的数据集。

此外 Factom 特别擅长获取信息，是在云解决方案中存储大型文件的理想方法，可用 Factom 中的指针为应用程序定位这些文件；Factom 还具有与大多数公共区块链不同的一个功能，通过在其它多个公共区块链中每十分钟发布一整个区块链的散列，采取其它措施确保网络安全；Factom 区块链也将自己扩展到安全的网络中，防止数据腐败，数据腐败是防止构建区块链的服务器无法检测到重写历史，防止服务器向不同的人显示两个不同的版本。

5．5 EOS 区块链

EOS 是一个较新的区块链，允许其用户编程能够执行广泛功能的智能合同[24]。EOS 既具有区块链技术的透明性，又具有创建智能合约的能力，并增加了帐户功能、身份验证、数据库、异步通信以及跨许多中央处理单元(CPU)核心的应用程序调度。EOS 的体系结构可以扩展到每秒数百万个事务，降低用户费用，并允许更容易地部署去中心化应用程序(Dapp)。

EOS 开创了一种新的系统，称为委托股权证明(DPOS)。EOS 区块链上的令牌持有者可以通过投票选择块生产者。任何人都有可能成为块生产者，只要他们能说服令牌持有者。

EOS 期望使用去中心化的共识算法 DPOS 去解决面对的一些核心问题：（1）区块链技术必须能够支持数千万活跃的日常用户，就像谷歌、Facebook、Twitter 和亚马逊每天所做的那样，而不会增加成本或崩溃系统；（2）区块链技术必须能够大幅降低成本，以接管所有类型的应用程序和这些应用程序信任的系统；（3）区块链软件必须允许非政治性升级和漏洞恢复，避免像比特币和以太坊那样因核心开发商的内斗和矿工的财政压力而陷入发展停滞；（4）正在构建应用程序的区块链开发人员需要多功能性来增强他们的应用程序的新特性，同时仍然允许区块链软件的安全性。

6 区块链的应用

区块链起初最常用于金融经济中，并已经迅速扩展到其它领域。由于区块链技术还是比较新颖的技术，所以如何应用这项技术是人们普遍比较关注的问题。如果系统需要诸如：参与者人数多且需要是分布式、不想依赖可信的第三方、事务是流动性的、需要去中心化服务、需要密码安全加密、需要与参与者共享完整的事务历史记录，就可以考虑应用区块链技术。

在决定是否使用区块链时，必须考虑到多种因素，并确定这些因素是否限制了一个人使用区块链或特定类型区块链的能力。美国国土安全部(DHS)科学和技术局一直在调查区块链技术，并创建了一个如图 1 所示流程图，以帮助人们确定开发倡议是否需要区块链。

结合区块链独有的特点，未来将有极大可能在以下行业中应用区块链技术[2][5][12][14][24]：

（1）金融。在对区块链的研究探索中，最先应用这项新技术的就是金融行业。区块链技术在数字支付、智能合同、金融交易、物联网金融等多个方面有着广阔的使用前景。例如：区块链的分布式特点使其对国际和跨境支付特别有用。较低的交易成本，更高的透明度和更快的结算时间，使得基于区块链的支付比传统的支付方式更为可取。

（2）游戏。区块链其中包含的技术去中心化、智能合同、货币交易等，可有助于保护游戏用户的隐私问题，对游戏中的虚拟游戏货币能维持其保值，在另外一种意义上实现用户和游戏开发公司的价值共享。

（3）隐私。区块链在社交领域方面最值得重视的价值就是对隐私的保护。大数据背景下，网络用户的隐私安全问题往往得不到保障，区块链的可匿名性以及数据历史不可更改、去中心化特点，可以使用户最大限度的让管理自己数据的权利把握在自己手上。

（4）医疗。区块链技术可以用于像医疗这种数据存储和传输非常重要的行业。区块链这种分布分类账

本非适合医生与患者共享医疗记录、各医院进行的临床实验数据等等。

（5）慈善。区块链在慈善领域的应用点在于能保持数据的透明公开、可审计。对于慈善事业，这将有助于善款捐助人清楚地知道每一笔资金的具体流向。

（6）旅游业。使用区块链技术可以帮助和促进旅游业的发展，它可以通过向到某些地方旅游的游客提供积分来激励旅游。它可以使用智能合约来促进奖励。

（7）交通运输。可以使用区块链技术来改善运输和物流。具体的研究应用旨在帮助地区参与者就如何交换商品进行合作。智能合约将被用作合规和结算问题的解决方案。

（8）商业登记管理。可以使用区块链技术进行商业登记。可以通过 flex Desk 程序简化身份验证。

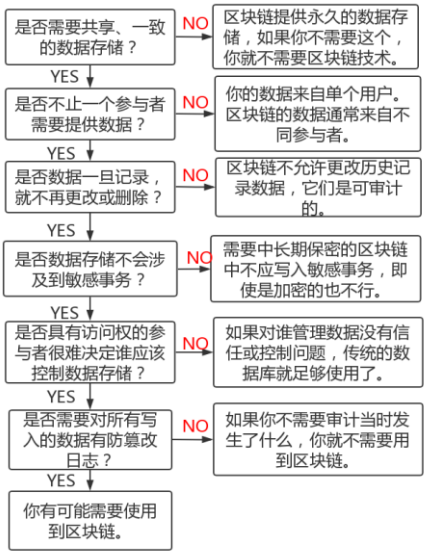

图 1 是否需要区块链技术流程图

7 结束语

本文介绍了区块链技术的技术概念，对比讨论了区块链网络的共识协议和几种常见的区块链，简要论述了区块链中对信任问题，并对区块链的应用方向做了展望。

目前对区块链技术的应用仍然处于起步阶段，但它是建立在被广泛理解和健全的密码原则之上，有许多被提议的用途。通过计算机网络验证的分布式账本，区块链网络更安全、迅速快捷、成本低，从金融市场、支付系统到供应链，几乎所有行业都开始应用区块链。展望未来，预计区块链将有可能在预测、网络和物联网、保险、私人运输和乘车共享以及慈善事业都有所涉及，区块链技术将会成为另一个可以使用的工具。随着越来越多的行业应用区块链技术，将在未来改变现实生活的所有领域，我们也将会进入安全、隐私、去中心化的新世界。

参 考 文 献

[1] F Casino, T K Dasaklis, C Patsakis, A systematic literature review of blockchain based applications: current status, classification and open issues [J]. Telematics Inform. 2019, 36 : 55－81

[2] 毛瀚宇,聂铁铮,申德荣等. 区块链即服务平台关键技术及发展综述[J].计算机科学,2021,48(11):4-11

[3] 庞微波.关于区块链的网络安全技术综述[J].网络安全技术与应用,2021,(11):21-23

[4] J Sidhu. Syscoin: A peer-to-peer electronic cash system with blockchain-based services for E-business[C]// 2017 26th International Conference on Computer Communications and Networks, IEEE Press, 2017: 1-6

[5] 曹傧,林亮,李云等.区块链研究综述[J].重庆邮电大学学报(自然科学版), 2020,32(1):1-14

[6] W Zhao. Blockchain technology: Development and prospects [J]. Source: National Science Review, 2019, 6(2):369-373

[7] A K Shrestha, J. Vassileva.Bitcoin Blockchain Transactions Visualization[C]//2018 International Conference on Cloud Computing, Big Data and Blockchain, IEEE Press, 2018:

[8] 张多宝.加密技术在电子商务安全中的应用探讨[J].网络安全技术与应用,2016,(2): 64

[9] 高泽龙, 姚顺, 孔立伟.哈希用于区块链存证和反垃圾信息的原理解析[J].网络空间安全,2021,12(Z1):27-31

[10] M Kammoun, M Elleuchi, M Abid, et al. HW/SW Architecture Exploration for an Efficient Implementation of the Secure Hash Algorithm SHA-256[J]. Journal of Communications Software and Systems, 2021,17(2):87-96

[11] M P J Kelsey, J Shook. Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness[]. 2017.

[12] 林诗意, 张磊, 刘德胜.基于区块链智能合约的应用研究综述[J]. 计算机应用研究,2021,38(8):2570-2581

[13] Yaga, Dylan J., et al. Blockchain Technology Overview.NIST Interagency/Internal Report (NISTIR) - 8202, 2018.

[14] 夏清,窦文生,郭凯文等.区块链共识协议综述[J].软件学报, 2021,32(2):277-299

[15] X Yang, Y Chen, X Chen. Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information[C]//2019 IEEE International Conference on Blockchain (Blockchain), IEEE Press, 2019:

[16] 柏语蔓,于莲芝.区块链权益证明共识机制综述[J]. 信息安全与通信保密,2021,(8):68-81

[17] 刘懿中, 刘建伟, 张宗洋等.区块链共识机制研究综述[J].密码学报,2019, 6(4):395-432

[18] Chetan Chawla,Trust in blockchains: Algorithmic and organizational,Journal of Business Venturing Insights,Volume 14,2020,e00203,ISSN 2352-6734

[19] Primavera De Filippi, Morshed Mannan, Wessel Reijers,Blockchain as a confidence machine: The problem of trust & challenges of governance,Technology in Society,Volume 62,2020,101284,ISSN 0160-791X

[20] 牛玉坤, 魏凌波, 张驰等.基于比特币区块链的公共无线局域网接入控制隐私保护研究[J].网络与信息安全学报, 2020, 6(2):56-66

[21] 聂梦飞, 庞晓琼, 陈文俊等.基于以太坊区块链的公平可搜索加密方案[J].计算机工程与应用,2019,56(4):69-75

[22] Motta G A,Tekinerdogan B,Athanasiadis I N. Blockchain Applications in the Agri-Food Domain: The First Wave[J]. Frontiers in Blockchain,2020,3()

[23] 朱昱锦, 姚建国,管海兵.区块链即服务:下一个云服务前沿[J],软件学报,2019,31(1):1-19

[24] 温啸林,李长林,张馨艺.基于 DPoS 共识机制的区块链社区演化的可视分析方法[J],计算机科学,2021,48(12)