关于区块链技术的研究综述

A summary of Blockchain Technology

林小驰 胡叶倩雯

摘要：区块链技术是一种去中心化、去信任的集体维护数据库技术，其本质是一种互联网协议。区块链技术拥有显著的应用优势：去中心化的分布式结构应用于现实中可节省大量的中介成本，不可篡改的时间戳特征可解决数据追踪与信息防伪问题，安全的信任机制可解决现今物联网技术的核心缺陷，灵活的可编程特性可帮助规范现有市场秩序。

关键词：区块链 去中心化 信任机制

Abstract: Blockchain Technology is one kind of collective database maintenance technology with the features of decentralization and deTrust. It is an Internet Protocol in essence. Blockchain technology has significant application advantages. The decentralization distribution structure can be used to save huge intermediary costs. The non-modifiable timestamp feature can solve the data tracking problems and ensure information security. The safe trust mechanism can compensate for the core defect of our current Internet Technology. Its programmable feature can also help to regulate the current market order.

Keywords: Blockchains, Decentralization, Trust Mechanism

区块链的来源：为什么会有区块链的创新？

未来世界的趋势是去中心化的

“看不见的手”是对市场去中心化本质的一个很好概括。

林小驰系中信证券股份有限公司研究部财务与估值组首席分析师；胡叶倩雯供职于中信证券股份有限公司研究部。本文仅代表作者个人观点，与所在单位无关。

两点之间直线最短，人们之间沟通的最好方式也是直接沟通，无论从哪个角度切入，去中心化的市场本质都是无可辩驳的。

目前来看，TCP/IP协议已经成为全世界人们之间的“牵手协议”。它将之前人们一直渴望的“去中心化、分布式”理念变成了一种可执行化的程序，互联网世界由此派生出了更多的类似协议。

那么为什么会出现中介？这是因为人们在活动的过程中需要交流，而交流是以信息为基础的，中介随之诞生。中介搜集了人们渴望知道的信息，在与需求方交换信息的过程中收取相应的中介费。这样一种中心化、高成本且低效率的市场体系持续运营了许多年。

这种中心化的体系存在很多不容忽视的问题：首先，在中心化的体系内，价值分散在各中心手中，由于各中心的系统不同，各中心的互通成本非常大；其次，由于少数中心化的机构掌握了多数的价值，因此价值的流通受制于中心化机构的体系要求，造成了一种高成本、低效率的运作现状；最后，由于所有数据均存储于中心化机构中，更容易遭恶意破坏者的篡改。

第一代互联网成功实现了信息去中心化，然而无法建立全球信用

目前来看，TCP/IP协议已经成为全世界人们之间的“牵手协议”。它将之前人们一直渴望的“去中心化、分布式”理念变成了一种可执行化的程序，互联网世界由此派生出了更多的类似协议。

然而，回顾互联网技术的发展后发现，这一代互联网技术成功实现了信息的去中心化，但却无法实现价值的去中心化。换句话说，互联网上能去中心化的活动是无需信用背书的活动，需要信用做保证的都是中心化的、有第三方中介机构参与的活动。因此，无法建立全球信用的互联网技术就在前进中遇到了很大的阻碍——人们无法在互联网上通过去中心化的方式参与价值交换活动。

从信息互联到价值互联

随着互联网技术的发展，这种基于信用而存在的第三方中介机构（如银行、结算结构）的运营成本已经大到无法忽视。于是，现今的人们开始尝试新的技术：这种技术在无法保证人们互相信任的前提下，还可以从事价值交换的活动，从而做到真正的去中心化、去第三方中介机构，实现从信息互联网到价值互联网的转变——区块链技术应运而生。

区块链技术解决了拜占庭将军问题①

延伸到互联网生活中，当需要与不熟悉的对手方进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗、迷惑从而做出错误决策。进一步将拜占庭将军问题延伸到技术领域中来，其内涵可概括为：在缺少可信任的中央节点和可信任的通道的情况下，分布在网络中的各个节点应如何达成共识。区块链技术解决了该问题——它提供了一种无需信任的单个节点、还能创建共识网络的方法。

区块链是什么?

区块链：一种数据结构

从数据的角度来看，区块链是一种几乎不可能被更改的分布式数据库（或称为分布式共享总账，Distributed Shared Ledger），这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（由系统参与者来集体维护）。区块链能实现全球数据信息的分布式记录（可以由系统参与者集体记录，而非由一个中心化的机构集中记录）与分布式存储（可以存储在所有参与记录数据的节点中，而非集中存储于中心化的机构节点中）。从效果的角度来看，区块链可以生成一套记录时间先后的、不可篡改的、可信任的数据库，这套数据库是去中心化存储且数据安全能够得到有效保证的。

区块链是一种把区块以链的方式组合在一起的数据结构。它适合存储简单的、有先后关系的、能在系统内验证的数据，用密码学保证了数据的不可篡改和不可伪造。它能够使参与者对全网交易记录的事件顺序和当前状态建立共识。

区块链技术：一种去中心化、去信任的集体维护数据库技术

如今的区块链技术概括起来是指通过去中心化和去信任的方式集体维护一个可靠数据库。其实，区块链技术并不是一种单一的、全新的技术，而是多种现有技术（如加密算法、P2P文件传输等）整合的结果，这些技术与数据库巧妙地组合在一起，形成了一种新的数据记录、传递、存储与呈现的方式。过

区块链能实现全球数据信息的分布式记录（可以由系统参与者集体记录，而非由一个中心化的机构集中记录）与分布式存储（可以存储在所有参与记录数据的节点中，而非集中存储于中心化的机构节点中）。

① 又称两军问题，由莱斯•兰伯特提出的点对点通信中的基本问题。指在信息可能丢失的不可靠信道上，试图通过信息传递的方式达成一致性，这是不可能的。

区块链技术重新定义了网络中信用的生成方式。在系统中，参与者无需了解其他人的背景资料，也不需要借助第三方机构的担保或保证，区块链技术保障了系统对价值转移的活动进行记录、传输、存储，其最后的结果一定是可信的。

去，人们将数据记录、存储的工作交给中心化的机构来完成，而区块链技术则让系统中的每一个人都可以参与数据的记录、存储。区块链技术在没有中央控制点的分布式对等网络下，使用分布式集体运作的方法，构建了一个点对点的自组织网络。通过复杂的校验机制，区块链数据库能够保持完整性、连续性和一致性，即使部分参与人作假也无法改变区块链的完整性，更无法篡改区块链中的数据。区块链技术涉及的关键点包括：去中心化、去信任、集体维护、可靠数据库、时间戳（Time stamp）、非对称加密（Asymmetric Cryptography）等。

区块链技术：不信任参与者，但信任结果

区块链技术重新定义了网络中信用的生成方式。在系统中，参与者无需了解其他人的背景资料，也不需要借助第三方机构的担保或保证，区块链技术保障了系统对价值转移的活动进行记录、传输、存储，其最后的结果一定是可信的。

区块链技术实际上是互联网上出现的一种技术，类似于互联网上的一项应用协议。现在广为人知的协议有HTTP协议和SMTP协议，区块链技术所达成的协议与这两种协议类似。HTTP和SMTP的协议传递的是信息，区块链也能传递信息，但区块链传递的信息内涵更为广泛。

区块链技术原理详述

设想一下，如果要在互联网世界中建立一套全球通用的数据库，那么会面临三个亟待解决的问题，这也是设计区块链技术的核心所在。

问题一：如何建立一个严谨的数据库，使得该数据库能够存储海量的信息，同时又能在没有中心化结构的体系下保证数据库的完整性?

问题二：如何记录并存储下这个严谨的数据库，使得即便参与数据记录的某些节点崩溃，仍能保证整个数据库系统的正常运行与信息完备?

问题三：如何使这个严谨且完整存储下来的数据库变得可信赖，使得可以在互联网无实名背景下成功防止诈骗?

针对这三个核心问题，区块链构建了一套完整的、连贯的数据库技术。此外，为了保证区块链技术的可进化性与可扩展性，区块链系统设计者还引入了“脚本”的概念来实现数据库的可编程

性。以下四大技术构成了区块链的核心技术。

核心技术1：区块+链

关于如何建立一个严谨数据库的问题，区块链的办法是将数据库的结构进行创新，把数据分成不同的区块，每个区块通过特定的信息链接到上一区块的后面，前后顺连来呈现一套完整的数据，这也是“区块链”这三个字的来源。

区块。在区块链技术中，数据以电子记录的形式被永久储存下来，存放这些电子记录的文件我们就称之为“区块（block）”。区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的所有价值交换活动，所有区块汇总起来形成一个记录合集。

区块结构。区块中会记录下区块生成时间段内的交易数据，区块主体实际上就是交易信息的合集。每一种区块链的结构设计可能不完全相同，但大结构上分为块头（header）和块身（body）两部分。块头用于链接到前面的块并为区块链数据库提供完整性的保证，块身则包含了经过验证的、块创建过程中发生的价值交换的所有记录。

区块结构有两个非常重要的特点：第一，每一个区块上记录的交易是上一个区块形成之后、该区块被创建前发生的所有价值交换活动，这个特点保证了数据库的完整性。第二，绝大多数情况下，一旦新区块完成后被加入到区块链的最后，则此区块的数据记录就再也不能改变或删除。这个特点保证了数据库的严谨性，即无法被篡改。

顾名思义，**区块链**就是区块以链的方式组合在一起，以这种方式形成区块链数据库。区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。

顾名思义，区块链就是区块以链的方式组合在一起，以这种方式形成区块链数据库。区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。

由于每一个区块的块头都包含了前一个区块的交易信息压缩值，这就使得从创世块（第一个区块）到当前区块连接在一起形成了一条长链。由于如果不知道前一区块的“交易缩影”值，就没有办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。

“区块+链”的结构为我们提供了一个数据库的完整历史。从第一个区块开始，到最新产生的区块为止，区块链上存

储了系统全部的历史数据，提供了数据库内每一笔数据的查找功能。区块链上的每一条交易数据，都可以通过“区块链”的结构追本溯源，一笔一笔进行验证。

区块+链=时间戳，这是区块链数据库的最大创新点。区块链数据库让全网的记录者在每一个区块中都盖上一个时间戳来记账，表示这个信息是这个时间写入的，形成了一个不可篡改、不可伪造的数据库。时间戳可以证明一个活动/一项发明的最先提出者/创作者是谁：只要先驱者的活动/发明在区块链中盖上时间戳再发布，则所有在其后发表的均为转载；时间戳可以证明某人曾在某天确实做过某件事情，由于信息记录和时间戳的存在，这个“存在性”的证明就变得十分简单。

核心技术2：分布式结构——开源的、去中心化的协议

有了区块+链的数据之后，接下来就要考虑记录和存储的问题。在现如今中心化的体系中，数据都是集中记录并存储于中央电脑上。但是区块链结构设计精妙的地方就在这里，它并不赞同把数据记录并存储在中心化的一台或几台电脑上，而是让每一个参与数据交易的节点都记录并存储下所有的数据。

关于如何让所有节点都能参与记录的问题，区块链的办法是构建一整套协议机制，让全网每一个节点在参与记录的同时

区块链结构设计精妙的地方就在这里，它并不赞同把数据记录并存储在中心化的一台或几台电脑上，而是让每一个参与数据交易的节点都记录并存储下所有的数据。

也来验证其他节点记录结果的正确性。只有当全网大部分节点（或甚至所有节点）都同时认为这个记录正确时，或者所有参与记录的节点都比对结果一致通过后，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。

关于如何存储下“区块链”这套严谨数据库的问题，区块链的办法是构建一个分布式结构的网络系统，让数据库中的所有数据都实时更新并存放于所有参与记录的网络节点中。这样即使部分节点损坏或被黑客攻击，也不会影响整个数据库的数据记录与信息更新。

区块链根据系统确定的开源的、去中心化的协议，构建了一个分布式的结构体系，让价值交换的信息通过分布式传播发送给全网，通过分布式记账确定信息数据内容，盖上时间戳后生成区块数据，再通过分布式传播发送给各个节点，实现分布式存储。

分布式记账，会计责任的分散化（Distributed accountability）。从硬件的

角度讲，区块链的背后是大量的信息记录储存器组成的网络，这一网络如何记录发生在网络中的所有价值交换活动呢？区块链设计者没有为专业的会计记录者预留一个特定的位置，而是希望通过自愿原则来建立一套人人都可以参与记录信息的分布式记账体系，从而将会计责任分散化，由整个网络的所有参与者共同记录。

分布式传播，每一次交换都传播到网络中的所有节点。区块链中每一笔新交易的传播都采用分布式结构，根据P2P网络层协议，消息由单个节点被直接发送给全网其他所有的节点。

分布式存储，数据信息的可容错性极高。区块链技术让数据库中的所有数据均存储于系统所有的电脑节点中，并实时更新。完全去中心化的结构设置使数据能实时记录，并在每一个参与数据存储的网络节点中更新，这极大提高了数据库的安全性。可以说，区块链技术构建了一套永续系统——只要不是网络中的所有参与节点在同一时间集体崩溃，数据库系统就可以一直运转下去。

核心技术3：所有权的信任基础——数学

有了一套严谨的数据库，也有了记录并存储这套数据库的可用协议，当将这套数据库运用于实际社会时，要解决最核心的一个问题：如何使这个严谨且完整存储下来的数据库变得可信赖，使得我们可以在互联网无实名背景下成功防止诈骗？

对于这一问题，区块链设计者使用了密码学的方式来解决共识机制。这个共识机制的运作原理就是“非对称加密数学”。简单而言，它让我们在“加密”和“解密”的过程中分别使用两个密码，两个密码具有非对称的特点：一是加密时的密码（在区块链中被称为“公钥”）是公开全网可见的，所有人都可以用自己的公钥来加密一段信息（信息的真实性）；二是解密时的密码（在区块链中被称为“私钥”）是只有信息拥有者才知道的，被加密过的信息只有拥有相应私钥的人才能够解密（信息的安全性）。

在区块链技术中，所有的规则事先都以算法程序的形式表述出来，人们完全不需要知道交易对手方的品德，更不需要求助中心化的第三方机构来进行交易背书，而只需要信任数学算法就可以建立互信。

从信任的角度来看，区块链实际上是数学方法解决信任问题的产物。在区块链技术中，所有的规则事先都以算法程序的形式表述出来，人们完全不需要知道交易对手方的品德，更不需要求助中心化的第三方机构来进行交易背书，而只需要信任数学算法就可以建立互信。区块链技术的

区块链技术的信任机制建立在数学（非对称密码学）原理基础之上，这就使得区块链系统中的人们可以在不需了解对方基本信息的情况下进行可信任的价值交换，信息安全的同时保证了系统运营的高效率与低成本。

背后，实质上是算法在为人们创造信用，达成共识背书。

核心技术4：可编程的智能合约——脚本

脚本可以理解为一种可编程的智能合约。如果区块链技术只是为了适应某种特定的交易，那脚本的嵌入就没有必要了，系统可以直接定义完成价值交换活动需要满足的条件。然而，在一个去中心化的环境下，所有的协议都需要提前取得共识，那脚本的引入就显得不可或缺了。有了脚本之后，区块链技术就会使系统有机会去处理一些无法预见的交易模式，保证了这一技术在未来的应用中不会过时，增加了技术的实用性。

一个脚本本质上是众多指令的列表，这些指令记录在每一次的价值交换活动中，价值交换活动的接收者（价值的持有人）如何获得这些价值，以及花费掉自己曾收到的留存价值需要满足哪些附加条件。通常，发送价值到目标地址的脚本，要求价值的持有人提供以下两个条件，才能使用自己之前收到的价值：一个公钥，以及一个签名（证明价值的持有者拥有与上述公钥相对应的私钥）。脚本的神奇之处在于，具有可编程性：它可以灵活改变花费掉留存价值的条件，例如脚本系统可能会同时要求两个私钥、或几个私钥、或无需任何私钥等；它可以在发送价值时附加一些价值再转移的条件。

区块链的特点、应用优势与目前需要关注的问题

区块链技术的特点

区块链技术最初是伴随比特币的设计而出现的，其后人们才渐渐发现了技术本身的价值。

纯数学方法建立信任关系，去中心化结构——高运作效率、低运营成本。区块链技术的信任机制建立在数学（非对称密码学）原理基础之上，这就使得区块链系统中的人们可以在不需了解对方基本信息的情况下进行可信任的价值交换，信息安全的同时保证了系统运营的高效率与低成本。

数据信息完整透明——符合法律和便于追踪。由于区块链将从创世块以来的所有交易都明文记录在区块中，且形成的数据记录不可篡改，因此任何交易双方之间的价值交换活动都是可以被追踪和查询到

的。这种完全透明的数据管理体系为现有的物流追踪、操作日志记录、审计查账等提供了可信任的追踪捷径。

分布式记账与存储——高容错性。由于区块链的记账与存储功能分配给了每一个参与的节点，因此不会出现集中模式下的服务器崩溃风险问题。分布模式使得区块链在运转的过程中具有非常强大的容错性功能，即使数据库中的一个或几个节点出错，也不会影响整个数据库的数据运转，更不会影响现有数据的存储与更新。

智能合约可编程——没有负担的进化模型。区块链技术基于可编程原理内嵌进了脚本的概念，这就使得今后基于区块链技术的价值交换活动变成了一种智能的可编程模式。

全球一个数据库——高包容性业务模式。基于区块链技术建立起来的数据库是一个全球范围内的超级大数据库，所有的价值交换活动（包括开户、登记、交易、支付、清算等）都可以在这个数据库中完成，业务模式具有极高的包容性。

透明世界背后的匿名性——保护隐私。区块链的信任基础是通过纯数学方式背书而建立起来的，能让人们在互联网世界里实现信息共享的同时，不暴露在现实生活中的真实身份。区块链上的数据都是公开透明的，但数据并没有绑定到个人。透明世界的背后具有匿名性特点。

区块链技术的核心应用优势

了解区块链的技术原理及特点后，可以发现区块链技术的核心价值所在，在不需要系统内各节点互信的情况下，系统确保一切数据的记录都是真实的，从而形成一个诚实有序的去中心化分布式的数据库，而且人们对系统内参与交换的价值还可以灵活地编程。

去中心化的分布式结构：现实中可节省大量的中介成本。由于区块链技术能成为人与人之间在不需要互信的情况下进行大规模协作的工具，所以其可被应用于许多传统的中心化领域中，处理一些原本由中介机构处理的交易。

基于区块链技术建立起来的数据库是一个全球范围内的超级大数据库，所有的价值交换活动（包括开户、登记、交易、支付、清算等）都可以在这个数据库中完成，业务模式具有极高的包容性。

不可篡改的时间戳：可解决数据追踪与信息防伪问题。在当今社会中，大量伪造的信息与数据充斥着我们的生活。而区块链技术为我们的数据追踪与信息防伪领域打开了一扇大门。由于区块链中的数据前后相连构成了一个不可篡改的时间戳，就能为所有的物件贴上一套不可伪造的真

实记录，这对于现实生活中打击假冒伪劣产品及整顿信息纪律等都大有帮助。

安全的信任机制：可解决现今物联网技术的核心缺陷。传统的物联网模式是由一个中心化的数据中心来收集所有信息，这样就导致了设备生命周期等方面的严重缺陷。区块链技术能在无需信任单个节点的同时创建整个网络的信任共识，从而能很好地解决物联网的一些核心缺陷，让物与物之间不仅相连起来，而且能自发活动起来。

灵活的可编程特性：可帮助规范现有市场秩序。在现今社会里，由于市场秩序不够规范，在转移自己的资产时，根本无法保证其能在未来发挥应有的价值。假如将区块链技术的可编程特性引入，在资产转移的同时编辑一段程序写入其中，可以规定资产今后的用途与方向。

区块链技术可能需要面对的问题

从区块链技术面世之初发展到现在，有越来越多的人对技术本身提出了一些疑问，问题主要集中于落地到现实应用时的技术细节问题。区块链技术想要全面应用于现实社会中，解决高耗能、数据存储空间、大规模交易处理及安全性保障问题就变得十分关键。

高耗能问题。数字货币经济学中也存在“不可能三角”，即不可能同时达到“去中心化”、“低能耗”和“安全”这三个要求。区块链是否在节约中心化成本问题的同时又过度使用了电子能耗成本呢？技术的应用要考虑其系统的整体性，也许区块链技术的应用过程就是一个权衡成本收益后让技术效用最大化的过程。

在现今社会里，由于市场秩序不够规范，在转移自己的资产时，根本无法保证其能在未来发挥应有的价值。假如将区块链技术的可编程特性引入，在资产转移的同时编辑一段程序写入其中，可以规定资产今后的用途与方向。

数据库存储空间问题。区块链数据库记录了从创建开始发生的每一笔交易，因此每一个想参与进来的节点都必须下载存储并实时更新一份从创世块开始延续至今的数据包。如果每一个节点的数据都完全同步，那区块链数据的存储空间容量要求就可能成为一个制约其发展的关键问题。

处理大规模交易的抗压能力问题。目前的区块链技术还没有真正处理过全世界所有人都共同参与进来的大规模交易，目前已投入使用的区块链系统中的节点总数规模仍然很小。一旦将区块链技术推广到大规模交易环境下，区块链记录数据的抗压能力就无法得到保证。

安全性问题。目前的区块链技术是基于非对称密码学的原理，但随着数学

研究和量子计算机技术的进一步发展，这些非对称加密的算法能否被破解呢？对于这个问题，市场中目前正在整合更强的加密原理。

本文认为，区块链技术不会因为上述问题而停滞不前。随着人们对区块链技术优势的认识越来越深刻，越来越多的资本、人才、资源正在源源不断的被投入到相关技术的研究中，区块链技术的上述缺陷得到解决相信只是时间问题。

区块链应用的发展历史

区块链这一概念首次出现在比特币的论文中。然而发展到今天，人们关注区块链技术已远超于关注比特币本身了。Melanie Swan在其著作*Block Chain: Blueprint for A New Economy*中将区块链的应用范围划分成三个层面，分别称其为区块链1.0、2.0和3.0。本文借用其分类来梳理区块链应用的发展历史脉络。

区块链1.0：可编程货币

可编程货币的出现，使得价值在互联网中直接流通成为了可能。区块链构建了一种全新的去中心化的数字支付系统，随时随地的货币交易、毫无障碍的跨国支付以及低成本运营的去中心化体系都让这个系统变得更具潜力。

区块链2.0：可编程金融

受到数字货币的影响，人们开始将区块链技术的应用范围扩展到其他金融领域。基于区块链技术可编程的特点，人们尝试将“智能合约”的理念加入区块链中，形成了可编程金融。有了合约系统的支撑，区块链的应用范围开始从单一的货币领域扩大到涉及合约功能的其他金融领域，让区块链技术得以在包括股票、清算、私募股权等众多金融领域崭露头角。目前，许多金融机构都开始研究区块链技术并尝试将其运用于现实。

可编程货币的出现，使得价值在互联网中直接流通成为了可能。区块链构建了一种全新的去中心化的数字支付系统，随时随地的货币交易、毫无障碍的跨国支付以及低成本运营的去中心化体系都让这个系统变得更具潜力。

区块链3.0：可编程社会

随着区块链技术的进一步发展，其“去中心化”功能及“数据防伪”功能在其他领域逐步受到重视。人们开始认识到，区块链的应用也许不仅局限在金融领域，而是可以扩展到任何有需求的领域中去。于是，在金融领域之外，区块链技术又陆续被应用到了公证、仲裁、审计、域名、物流、医疗、邮件、鉴证、投票等其他领域中来。在这一应用阶段，人们试图用区块链来颠覆互联网的最底层协议，并试图将区块链技术运用到物联网中，让整个社会进入智能

互联网时代，形成一个可编程的社会。

区块链的现状

数据库技术现状：数据库正在从集中式走向分布式。近年来，随着互联网的高速发展，网络中的数据量也急剧膨胀，传统的集中式数据库越来越无法处理高速增长的电子数据。因此，数据库开始由集中式向分布式结构转变。然而，现有的分布式数据库都只是基于中心化结构基础上的多重存储、多重备份数据库，一旦中心节点出现问题，所有的分布节点数据就会停止更新。

区块链技术处于理论阶段，尚需实践。国内外对于区块链技术的投入使用都已经逐渐展开，但目前尚未有完全落地的应用性成果。从发展的角度来看，区块链技术目前仍然处于理论阶段，今后的技术转换尚需一段很长时间的实践。

区块链技术现状：多元化区块链共同发展。经过了近几年的发展与实践，人们对区块链技术的了解越来越深入，许多领域试图在比特币区块链的基础之上对其做进一步的改进。目前，区块链已经从比特币完全去中心化的公共区块链，发展出了依附于公有链之上的侧链以及非完全去中心化的私有区块链等。

公共区块链（public blockchain）是区块链的最初形态，是一种完全去中心化的分布式存储数据库。任何人都可以访问公共区块链上的数据，并在其上进行价值交换，信任机制的建立通过密码学技术来保证。

侧链（side-chain）是公共区块链的延伸，是一种基于公共区块链所开发出的新技术，可以实现公共区块链上价值与其他账簿上价值在多个区块链间的转移。在用公共区块链辅助证明信用的同时，侧链技术能支持更为复杂的数据结构及操作。

私有区块链（private blockchain）是公共区块链更进一步的变形，参与的节点只有用户自己，数据的访问和使用有严格的权限管理。

区块链技术处于理论阶段，尚需实践。国内外对于区块链技术的投入使用都已经逐渐展开，但目前尚未有完全落地的应用性成果。从发展的角度来看，区块链技术目前仍然处于理论阶段，今后的技术转换尚需一段很长时间的实践。

区块链的启示：从技术到市场，再到整个社会

从底层技术的角度看：数据管理方式有望转型，互联网底层协议将被颠覆

作为互联网领域的底层技术，区块链有望促进数据记录、数据传播及数据存储管理方式的转型。BaaS（Blockchain as a

区块链技术有望将法律与经济融为一体，改变原有社会的监管模式。由于区块链技术能达成互联网中的全网校验、全网信任共识，我们就有理由相信，未来基于区块链基础之上的社会对监管的需求会大幅下降。

Service，区块链即服务）将是未来一个非常重要的趋势。

区块链本身更像一个互联网底层的一个开源式协议互联网时代到来之前，人们的信息传递是严重受阻的；第一代互联网TCP/IP协议的建立让整个社会的信息实现了自由传递；而现在的区块链技术，正拥有着让整个互联网信息实现从自由传递到自由验证、过程的强大力量。

从市场应用的角度看：平台机构已成过去，公司模式重心转移

区块链能成为一种市场工具，帮助社会削减平台成本，让中间机构成为过去。区块链在去中心化的情况下构建了一个基于数学的全球信用体系，其技术现在已被用来挑战各行各业中成本高、耗时长的中间商业务。随着区块链技术的发展和应用的普及，中间商将会遭到极大的冲击，未来的市场将是一个建立在互联网去中心化信用体系之上的区块链市场。

区块链能促使公司现有业务模式重心的转移，有望加速公司的发展。去除了中间商的市场是一个自由、开放且透明的市场，许多公司的传统业务模式都将面临颠覆式挑战。区块链正在悄然改变市场中人们交易的方式。区块链技术有望打破现有的利润体系，将更多利润分配给那些真正能为社会创造价值的公司中去。另一个改变是，在区块链的环境下，公司传统的品牌形象建立、融资、审计等一系列漫长过程都将加快，区块链能帮助市场更快地淘汰落后企业和筛选优秀企业，公司发展将步入一个新时代。

从整个社会结构的角度看：法律经济可成一体，组织形态发生改变

区块链技术有望将法律与经济融为一体，改变原有社会的监管模式。由于区块链技术能达成互联网中的全网校验、全网信任共识，我们就有理由相信，未来基于区块链基础之上的社会对监管的需求会大幅下降。由于信息更加透明、数据更加可追踪、交易更加安全，整个社会用于监管的成本会大为减少，法律与经济将会自动融为一体，“有形的手”与“无形的手”将不再仅仅是相辅相成、而是逐渐趋同的态势。N

文字编辑：卢超群