区块宝
qukuaibao.com

2017年区块链行业年度特别报告

区块宝研究院

2017年12月31日

区块宝简介

区块宝创办于 2015 年，以区块链技术服务为核心，为全球的用户提供区块链的产品和行业解决方案，满足不同用户的场景化服务需求。

区块宝公有云是专业可信赖的区块链基础云平台，定位于为行业用户提供区块链即服务（BaaS）平台，在此平台上构建可信赖、可扩展的区块链应用基础平台产品，集成相关领域的基础产品功能，帮助企业快速搭建区块链应用场景；

区块宝企业云是区块宝为企业用户提供的个性化、差异化、定制化的区块链解决方案，覆盖资产、股权、版权、保险、医疗、征信等多个领域，基于用户的不同需求及对安全和数据隔离的考虑，提供定制化的区块链行业解决方案；

区块宝研究院致力于区块链与数字资产行业研究，建立了庞大的区块链商业信息数据库，为政府、企业、投资机构提供决策依据；

区块宝《范范而谈》是记录数字世界的新媒体平台，关注数字资产和区块链企业家、创业者、投资人、监管者，以视频、直播、音频等多层次产品形态，打造前沿、专业、有趣的数字资产和区块链垂直领域新媒体平台。

前言

在之前的报告中，区块宝研究院曾将 2016 年列为区块链元年，2017 年为区块链“合规元年”。实际上，2017 年不仅是区块链“合规元年”，也是区块链“应用元年”。

2017 年，我们见证了很多，区块链行业经历了很多。我们见证了美国内华达州立法为区块链免除赋税；见证了中国人民银行成立数字货币研究院；见证了全球多地为引领金融科技的发展而设立监管沙盒；见证了多国政府为规范区块链行业稳健发展而遏制投机行为；见证了以太坊如期成功步入大都会（Metropolis）阶段；见证了区块链技术在金融、农业、法律、艺术、能源、医疗、物流、电商等领域的相继落地。

在区块链的发展史上，2017 年注定是要被载入史册的一年，是永远不会被忘记的一年。因为 2017 年，是区块链行业产业生态链初步成型的一年，是区块链行业产业价值获得全球广泛认可的一年，是区块链技术在商用中上下求索的一年，是区块链从概念走向商业应用的关键一年。

自区块链技术诞生以来，伴随着国内外研究机构对区块链技术的研究和应用，区块链的应用前景受到各行各业的高度重视，区块链被认为是继大型机、个人电脑、互联网、移动/社交网络之后计算范式的第 5 次颠覆式创新，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，是从信息互联网时代过渡到价值互联网时代的引擎。

经过近几年的商用实践，业界对区块链的认识更加透彻的同时，对区块链的商用价值、定位也更加明确。随着区块链技术的进一步成熟与更大范围、更多行业的普及，未来的区块链应用将更大程度的脱虚向实，更多的行业、企业将使用区块链技术来降低成本、提升协作效率。

目 录

图表目录

第一章 区块链技术概述

1.1 区块结构基础

1.1.1 区块链概念

区块链本质上是一个对等网络（peer-to-peer）的分布式账本数据库。区块链本身其实是一串链接的数据区块，其链接指针是采用密码学哈希算法对区块头进行处理所产生的区块头哈希值。每一个数据块中记录了一组采用哈希算法组成的树状交易状态信息，这样保证了每个区块内的交易数据不可篡改，区块链里链接的区块也不可篡改。

狭义上讲，区块链技术是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改、不可伪造的分布式账本。

广义上讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

1.1.2 区块结构相关概念

区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合与创新，从而实现以前未实现的功能。其关键技术包括：P2P 动态组网、哈希函数、非对称加密算法、共识机制、智能合约等。只是如果没有中本聪那一篇开创性的关于比特币的白皮书，这些强大的技术，都还只是埋藏在学术论文堆里。

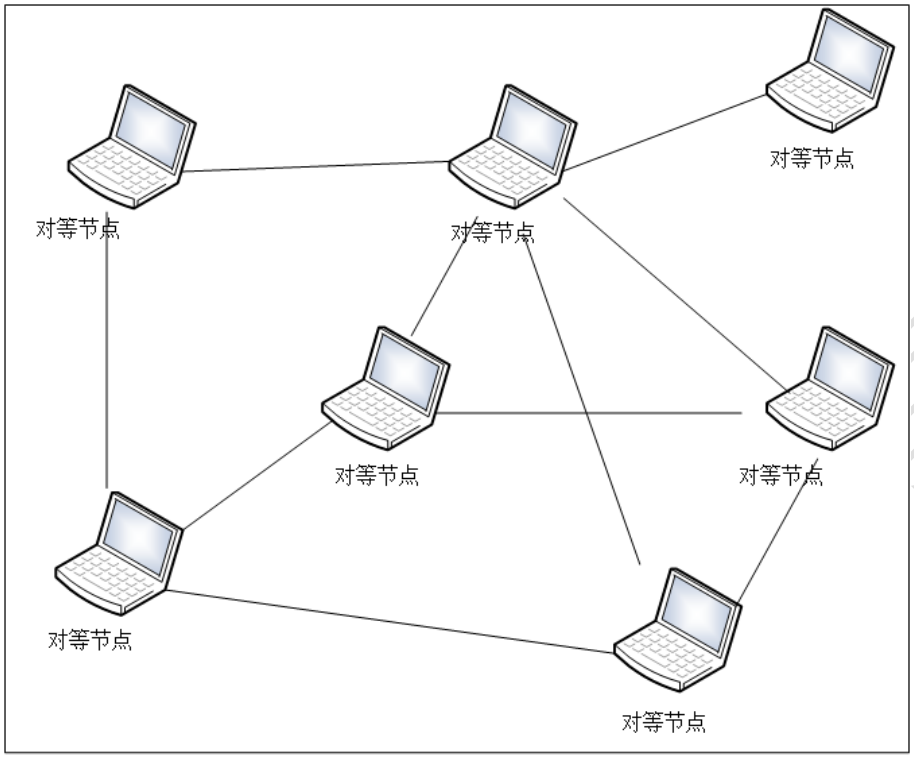
因为这些技术单独使用，并不能解决商业问题，但这一系列技术的结合，出人意料地形成了一个系统的可实践的解决方案。但是，在探讨区块链行业的产业发展动态之前，在探讨区块链的整体架构之前，仍然有必要先探讨区块链的区块结构细节及一些细节技术。

P2P 网络

P2P 网络（peer-to-peer network，对等网络）是一种在对等者（peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。

区块链系统是建立在 IP 通信协议和分布式网络的基础上的，它不依靠传统的电路交换，而是建立于网络通信之上，完全通过互联网去交换信息。网络中所有的节点具有同等的地位，不存在任何特殊化的中心节点和层级结构，每个节点均会承担网络路由、验证数据区块等功能。

图表 1：P2P 网络



制图：区块宝研究院

网络的节点根据存储数据量的不同，可以分为全节点和轻量级节点：

全节点——全节点存储了从创始区块以来的所有区块链数据，全节点的优点是进行数据校验时不需要依靠别的节点，仅依靠自身就可以完成校验更新等操作，缺点是硬件成本较高。

轻量级节点——轻量级节点只需要存储部分数据信息，当需要别的数据时可以通过简易支付验证方式（Simplified Payment Verification，SPV）向邻近节点请求所需数据来完成验证更新。

在比特币出现之前，P2P 网络计算技术已被广泛用于开发各种应用，如即时通讯软件、文件共享和下载软件、网络视频播放软件、计算资源共享软件等。P2P 网络技术是区块链技术架构的核心技术之一。

分布式数据库

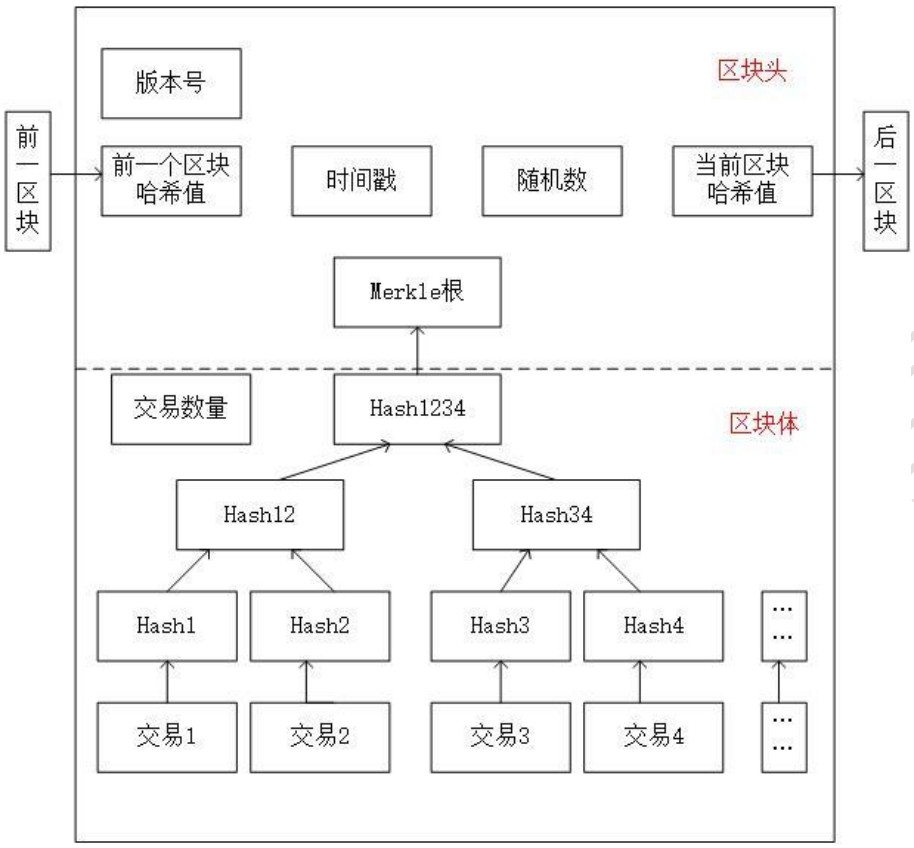
比特币系统中的区块就像一个记账本一样，记录了比特币系统中发生的这段时间内的所有交易信息。每一个比特币用户的比特币收支情况都被永久地嵌入数据区块中以供别人查询。

这些数据区块中的交易数据存放在每一个比特币用户的客户端节点中，所有的这些节点组成了比特币及其坚韧的分布式数据库系统。任何一个节点的数据被破坏都不会影响整个数据库的正常运转，因为其他的健康节点中都保存了完整的数据库。

数据区块

比特币的交易记录会保存在数据区块之中，每个数据区块一般包含区块头（Header）和区块体（Body）两部分。如图 1 所示：

图表 2：区块结构



制图：区块宝研究院

区块头——区块头封装了当前的版本号（Version）、前一区块地址（Pre-block）、时间戳（Timestamp）、随机数（Nonce）、当前区块的目标哈希值（Bits）、Merkle 树的根值（Merkle-root）等信息；区块头的大小为 80 字节，由 4 字节的版本号、32 字节的上一个区块的哈希值、32 字节的 Merkle 根哈希值、4 字节的时间戳（当前时间）、4 字节的当前难度值、4 字节的随机数组成。

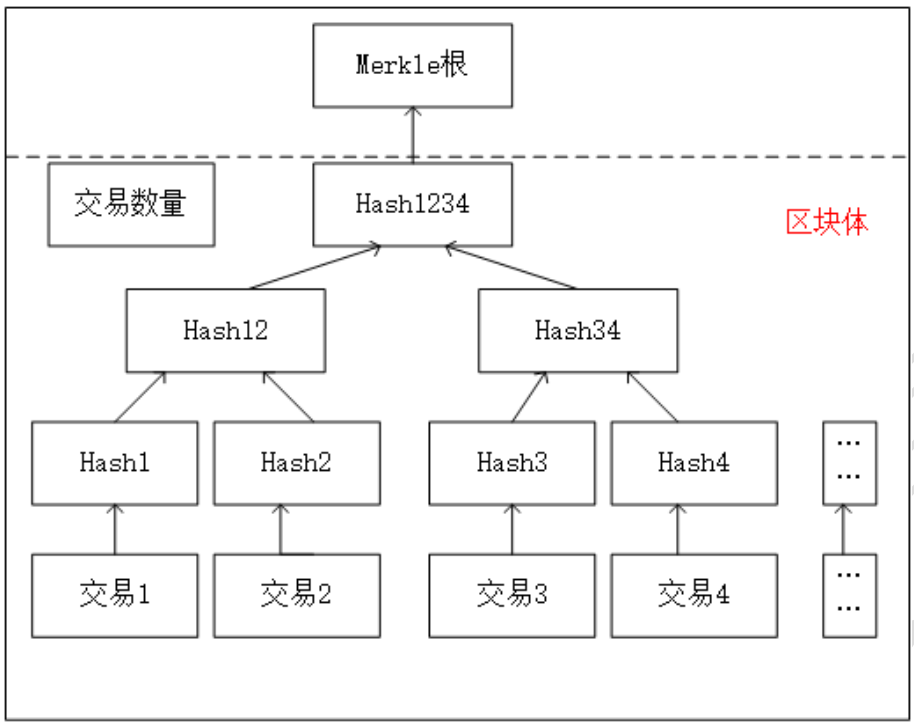
区块体——区块体中主要包含交易计数和交易详情。交易详情就是比特币系统中的记账本，每一笔交易都会被永久地计入数据区块中，而且任何人都可以查询。区块体中的 Merkle 树会对每一笔交易进行数字签名，以确保每一笔交易都不可伪造且没有重复交易。所有的交易将通过 Merkle 树的 Hash 过程产生一个唯一 Merkle 根值记入区块头。

Merkle 树

Merkle 树是数据结构中的一种形式，可以是二叉树，也可以是三叉树，它具有树结构的所有特点。比特币区块链系统中采用的是 Merkle 二叉树，它的作用主要是快速归纳和校验区块数据的完整性。

它会将区块链中的数据分组进行哈希运算，向上不断递归运算产生新的哈希节点，最终只剩下一个 Merkle 根存入区块头中，每个哈希节点总是包含两个相邻的数据块或其哈希值。

图表 3：区块中的 Merkle 树



制图：区块宝研究院

在比特币系统中使用 Merkle 树有诸多优点：

首先是极大地提高了区块链的运行效率和可扩展性，使得区块头只需包含根哈希值而不必封装所有底层数据，这使得哈希运算可以高效地运行在智能手机甚至物联网设备上；

其次是 Merkle 树可支持“简化支付验证协议”（SPV），即在不运行完整区块链网络节点的情况下，也能够对交易数据进行检验。所以，在区块链中使用 Merkle 树这种数据结构是具有重要意义的。

时间戳

时间戳是指从格林威治时间 1970 年 01 月 01 日 00 时 00 分 00 秒起至现在的总秒数，通常是一个字符序列，唯一地标识某一刻的时间。在比特币系统中，获得记账权的节点在链接区块时需要在区块头中加盖时间戳，用于记录当前区块数据的写入时间。每一个随后区块中的时间戳都会对前一个时间戳进行增强，形成一个时间递增的链条。

时间戳本身并没有多复杂，但在区块链技术中应用时间戳却是一个重大创新，时间戳为未来基于区块链的互联网和大数据增加了一个时间维度，使得数据更容易追溯，重现历史也成为可能。同时，时间戳可以作为存在性证明（Proof of Existence）的重要参数，它能够证实特定数据必然在某特定时刻是的确存在的，这保证了区块链数据库是不可篡改和不可伪造的，这也为区块链技术应用于公证、知识产权注册等时间敏感领域提供了可能。

UTXO 交易模式

UTXO（Unspent Transaction Outputs）是未花费的交易输出，它是比特币交易过程中的基本单位。

除创世区块以外，所有区块中的交易（Tx）会存在若干个输入（Tx_in,也称资金来源）和若干个输出（Tx_out,也称资金去向），创世区块和后来挖矿产生的区块中给矿工奖励的交易没有输入，除此之外，在比特币系统中，某笔交易的输入必须是另一笔交易未被使用的输出，同时这笔输入也需要上一笔输出地址所对应的私钥进行签名。

当前整个区块链网络中的 UTXO 会被储存在每个节点上，只有满足了来源于 UTXO 和数字签名条件的交易才是合法的。所以，区块链系统中的新交易，不必追溯整个交易历史，就可以确认当前交易是否合法。

这些技术并不是新技术，而是已有的技术，正是这些已有的技术，形成一个完整的区块链系统后，使得区块链在无中心的网络上形成了运转不息的引擎，为区块链的交易、验证、链接等功能提供了源源不断的动力。同时，也带来了提高社会效率、促进和谐发展的一种新的可能。

1.1.3 区块结构的链接

区块链虽然是一个新兴的概念，但它依赖的技术都是很成熟的，正是这些已经非常成熟的技术组成了严谨的区块链。

区块链技术是一项新兴技术，不是指其组成技术新，而是其组合呈现的方式新；区块链技术的强大，不在于其单项基础技术的作用强大，而在于其配套形成的账本系统功能强大。比如：时间戳本身并没有多复杂，但在区块链技术中应用时间戳，就相当于为未来基于区块链的互联网和大数据增加了一个时间维度，使得数据更容易追溯，重现历史也成为可能；分布式账本、共识算法都是已经存在很久的技术，但是分布式账本和共识算法的结合，解决了集体维护分布式账本的历史难题；具有公钥和私钥体系的数字签名，也是一项很成熟的技术，将数字签名引入分布式账本中应用，则实现了去中心化身份管理，保障了区块链的隐私性和准匿名性；时间戳、UTXO 和数字签名的组合使用，完美地避免了双重支付（双花）问题。

可以这么说，区块链更像是一门交叉学科，区块链技术是巧妙地结合了 P2P 网络、UTXO、数字签名、哈希函数、非对称加密算法、共识算法等等技术，构建成的一个新技术。

1.2 区块链基础架构

1.2.1 基础架构解析

架构设计一般要考虑灵活性和稳定性的两个方面。

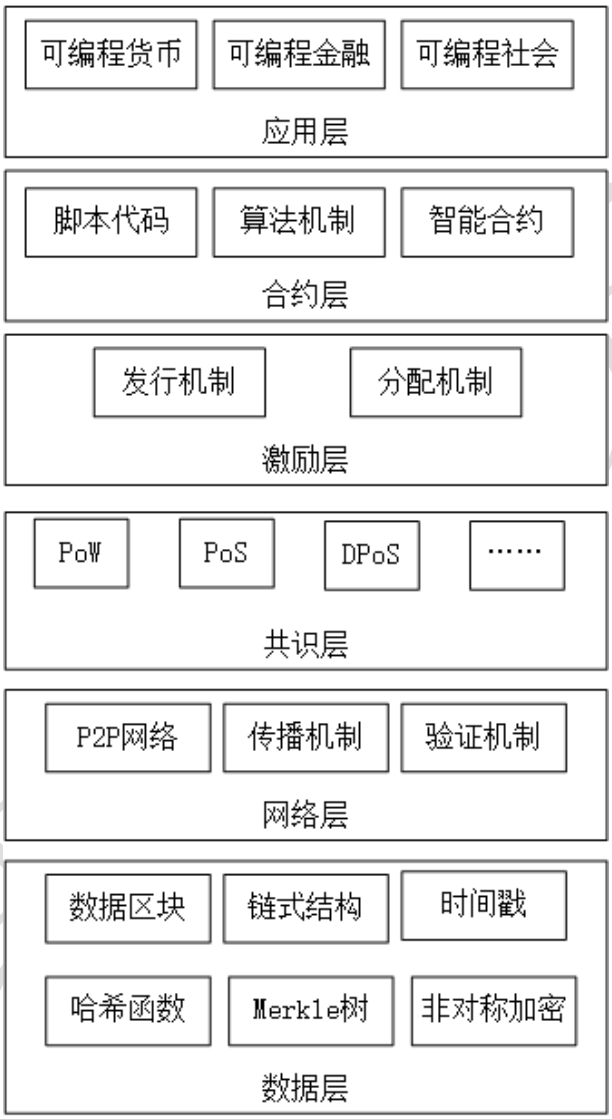
一个有长久生命力的系统都有一个设计高明的架构，其精髓在于架构能支持系统功能的变化、发展、演化，允许系统功能不断变化，也就是架构必须提供的灵活性；而系统在易用、安全、稳定和各

种功能等方面则应该具备稳定性。

关于区块链的基础架构，已有不少学者和专家进行过阐述，经区块宝研究院甄别，其中比较有代表性的是发表于 2016 年《自动化学报》的文章《区块链技术发展现状与展望》。

该文首次将区块链的框架划分为六层架构，认为区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。

图表 4：区块链基础架构模型



制图：区块宝研究院

数据层：封装了底层数据区块以及相关的数据加密和时间戳等技术；

网络层：包括分布式组网机制、数据传播机制和数据验证机制等；

共识层：主要封装网络节点的各类共识算法；

激励层：将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；

合约层：主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；

应用层：封装了区块链的各种应用场景和案例。

区块链基础架构的设计，经过区块链行业多年实践的考验，已经充分证明了其可靠性。对区块链基础架构的这套解析是比较合理的，既能体现区块链架构中底层基础的稳定性，也能兼顾因应用场景不同而有不同架构的灵活性。

1.2.2 基础架构特点

在这一套基础架构下，构建了区块链技术的去中心化、时序数据、集体维护、可编程、安全可信、准匿名性等特点。

去中心化

区块链数据的记账、验证、存储、传输等过程均基于分布式系统结构，采用纯数学方法，而不是中心机构来建立分布式节点之间的信任关系，区块链网络中的所有参与节点都具有同等的权利和义务，从而形成去中心化的可信任分布式系统。

时序数据

区块链采用带有时间戳的链式区块结构存储数据，从而为数据增加了时间维度，具有极强的可追溯性。

集体维护

区块链系统中的数据区块由整个系统中所有具有记账功能的节点来共同维护，任一节点的损坏或失去都不会影响整个系统的运作。并通过共识算法来选择特定的节点将新区块添加到区块链中。

可编程

区块链技术可提供灵活的脚本代码系统，支持用户创建高级智能合约、货币或其他去中心化应用。最典型的是以太坊（Ethereum），以太坊平台提供了图灵完备的脚本语言，以供用户来构建任何可以精确定义的智能合约或交易类型。

安全可信

区块链技术采用非对称加密算法对交易进行签名，使得交易不能被伪造；同时利用哈希算法保证交易数据不能被轻易篡改；最后借助分布式系统各节点的共识算法形成强大的算力来抵御破坏者的攻击，保证区块链中的区块以及区块内的交易数据不可篡改和不可伪造，因此区块链具有极高的安全性。

准匿名性

由于节点之间的交换遵循固定的算法，其数据交互是无需信任的。用户只需要公开地址，不需要公开真实身份，而且同一个用户可以不断变换地址。因此，在区块链上的交易不和真实身份挂钩，只是和用户的地址挂钩，具有交易的准匿名性。

1.3 区块链核心技术

区块链除了构建了强大的区块链基础架构以保证区块链系统的灵活性和稳定性之外，为保证存储于区块链中的信息的安全与完整，还使用了一些强大的密码学核心技术。

区块及区块链的定义和构造中使用了包含哈希算法（哈希函数）、非对称加密算法（公钥密码算法）和共识算法（共识机制）在内的多种核心技术。

区块链技术采用非对称加密算法对交易进行签名，使得交易不能被伪造；利用哈希算法保证交易数据不能被轻易篡改；借助分布式系统各节点的共识算法形成强大的算力来抵御破坏者的攻击。

1.3.1 哈希函数

哈希函数，也称为哈希算法。哈希函数是一种密码学算法。在区块链中的作用是：为信息加密，用于为原始信息添加“密码语言”。

哈希函数是一类数学函数，可以在有限合理的时间内，将任意长度的消息压缩为固定长度的二进制串，其输出值称为哈希值，也称为散列值。哈希函数在现代密码学中扮演着重要的角色，常用于实现数据完整性和实体认证，同时，也构成多种密码体制和协议的安全保障。

在比特币系统中使用了两个密码学哈希函数，一个是 SHA256，另一个是 RIPEMD160。SHA256 算法的一个主要用途是完成 PoW（工作量证明）计算，RIPEMD160 则主要用于生成比特币地址。

哈希函数的三个性质：

① 碰撞阻力

碰撞是与哈希函数相关的重要概念，体现着哈希函数的安全性。所谓碰撞是指两个不同的消息在同一个哈希函数作用下，具有相同的哈希值。哈希函数的安全性是指在现有的计算资源（包括时间、空间、资金等）下，找到一个碰撞是不可行的。

举例：如果无法找到两个值，x 和 y，x≠y，而 H（x）＝H（y），则称哈希函数 H 具有碰撞阻力。

哈希函数的碰撞阻力是指寻找两个能够产生碰撞的消息在计算上是不可行的。值得注意的是：找到两个碰撞的消息在计算上不可行，并不意味着不存在两个碰撞的消息。由于哈希函数把大空间上的消息压缩到小空间上，碰撞肯定存在。通过简单的计数论证，是可以证明碰撞的确存在的。

哈希函数的输入空间包含所有长度的任意字符串，但输出空间则只包含特定固定长度的字符串。因为输入空间比输出空间大（输入空间是无限的，而输出空间是有限的），一定会有输入字符串映射到相同的输出字符串，也就是说，碰撞是存在的。

打个比方：输入 100 个值，经哈希函数 H 之后，输出仅 80 个值。因为输出的数量小于输入的数

量，我们可以确定，某个输出肯定对应多个输入。

也就是说存在 x≠y，而 H（x）＝H（y），存在碰撞；但在计算上，找不出来 x 和 y 这两个值，所以称哈希函数 H 具有碰撞阻力。

哈希函数的碰撞阻力特性常被用来进行完整性验证。完整性是信息安全的 3 个基本要素之一，是指传输、存储信息的过程中，信息不被未授权的篡改或篡改后能被及时发现。如果原消息在传输过程中被篡改，那么运行哈希函数后得到的新哈希值就会和原来的哈希值不一样，这样就很容易发现消息在传输过程中完整性受损。

在区块链中，某个区块的头部信息中会存储着前一个区块的信息的哈希值，如果能拿到前一个区块的信息，任何用户都可以比对计算出来的哈希值和存储的哈希值，来检测前一个区块信息的完整性。

SHA256 是一个主要被比特币世界采用，并且效果还很不错的哈希函数，而且 SHA256 还获得了**安全哈希算法**的美名。但是，我们必须谨记，在理论上来讲，世界上是没有哈希函数具有坚不可摧的碰撞阻力的。我们实践中使用的安全哈希算法（SHA256），仅仅是人们经过不懈努力之后，暂未成功找到碰撞的函数。

如果有一天，我们最终找到了 SHA256 哈希函数的碰撞，那么，就如之前的 MD5 哈希函数一样，在找到 MD5 哈希函数的碰撞之后，该函数在实践应用中被逐渐淘汰。

② 原像不可逆

原像不可逆，通俗地说，是指知道输入值 x，很容易通过哈希函数 H 计算出哈希值 H（x）；但是知道哈希值 H（x），却不能通过哈希函数 H 计算出原来的输入值 x。

为什么哈希函数会具有这个特性？因为 x 的取值来自一个非常广泛的集合（输入空间是无限的）。

原像不可逆的应用是承诺方案（Commitment Scheme），承诺方案被认为是密码学领域中一类重要的密码学基本模型，承诺具有隐藏性和约束性。

承诺模型可以看做一个密封信件的数字等价体。如果 Tom 想承诺某个信息 m，则他可以把 m 放进一个密封的信封内，无论什么时候他想公开这个信息，则只需要打开信封。这个过程要求数字信件能够隐藏信息，即承诺的隐藏性，同时 Tom 也不能改变 m；而通过承诺的打开，任何人都能验证他所得到的 m 其实就是 Tom 最初承诺的信息 m，即承诺的约束性。

利用哈希函数的碰撞阻力和原像不可逆两个特性，承诺的隐藏性和约束性均能成立：

隐藏性——如果仅仅知道承诺函数的输出，就如同只看到信封并不能得到信中的内容；

约束性——这就确保了 Tom 一旦承诺信封内的内容，就不能再改变主意。

③ 谜题友好

通俗地说，难题友好性指的是没有便捷的方法去产生一满足特殊要求的哈希值。也就是说，如果有人想通过锁定哈希函数来产生一些特殊的输出 y，而部分输入值以随机方式选定，则很难找到另外

一个值，使得其哈希值正好等于 y。

哈希函数的难题友好特性，构成了基于工作量证明的共识算法的基础。例如，给定字符串“blockchain”，并在这个字符串后面连接一个整数值串 x，对连接后的字符串进行 SHA256 哈希运算，要求得到的哈希结果（以十六进制的形式表示）以若干个 0 开头的。按照这个规则，由 x＝1 出发，递增 x 的值，我们需要经过 2688 次哈希计算才能找到前 3 位均为 0 的哈希值，而要找到前 6 位均为 0 的哈希值，则需进行 620969 次哈希计算。也就是说，没有更便捷的方法来产生一个满足要求的哈希结果。这样通过哈希运算得出的符合特定要求的哈希值，可以作为共识算法中的工作量证明。

正是因为哈希函数具备这三个核心性质，使得哈希函数具备“保证交易数据不能被轻易篡改”的功能。

1.3.2 非对称加密算法

非对称加密算法，也叫公钥密码算法。非对称加密算法也是密码学算法，在区块链中的作用是：为交易加密，用于对交易发起、确认、签名、验证。

公钥密码算法是现代密码学发展过程中的一个里程碑。这类密码学算法需要两个密钥：公开密钥和私有密钥。因为加密和解密使用的是两个不同的密钥，另外，私钥可以推导公钥，而公钥不能倒推私钥，所以这种算法也叫做非对称加密算法。

（1）非对称加密算法的特点

加密和解密使用的是两个不同的密钥；公钥是全网可见的，私钥只有信息拥有者才知道；私钥可以推导公钥，公钥不能倒推私钥。

（2）非对称加密算法的用途

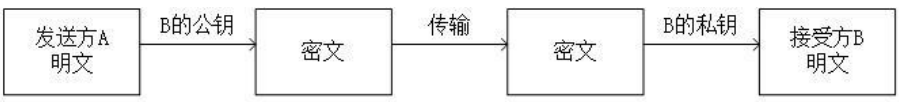
非对称加密算法主要有两个用途：一是在发送信息过程中使用公钥加密私钥解密，二是在数字签名过程中使用私钥签名（加密）公钥验证（解密）。

发送信息过程：

公钥加密：发送方 A 用接收方 B 的公钥对信息加密，并将该加密后的信息传输到区块链网络。

私钥解密：接收方 B 用其独有的私钥对信息解密，从而确保信息获得传递的同时还保证信息的真实性。

图表 5：非对称加密解密过程



制图：区块宝研究院

数字签名过程：

私钥签名：信息发布者用私钥对交易进行签名。用户发起交易时，用私钥对交易信息签名（加密），表明对交易具有所有权，并对真实性负责。

公钥验证签名：矿工用公钥对信息发布者的签名进行验证。矿工收到信息后，用公钥对签名进行验证（解密），若验证通过，则说明：第一，该信息是由特定的私钥的拥有者“签名”的；第二，该信息在签名后没有被改变过。那么，该信息可予以记录到区块链。

在比特币系统中，生成比特币地址的流程中也会用到公钥和私钥。

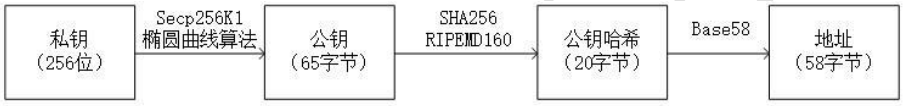
（3）生成比特币地址流程：

①比特币系统随机产生一个随机数为私钥；

②私钥通过 Secp256k1 椭圆曲线算法生成公钥；

③公钥通过双哈希运算+Base58 处理生成比特币地址。

图表 6：生成比特币地址流程



制图：区块宝研究院

私钥生成公钥过程所使用的 Secp256K1 椭圆曲线算法是一种单向加密函数，公钥生成比特币地址的过程中所使用的也是单向加密哈希函数。基于这些数学函数的密码学，使得生成数字密钥和不可伪造的数字签名成为可能。

（4）非对称加密算法的种类

非对称加密算法主要有以下几种：

图表 7：非对称加密算法种类

名称	简写	备注
椭圆曲线加密算法	ECC	生成比特币密钥的过程中
椭圆曲线数字签名算法	ECDSA	比特币的签名算法
RSA 公钥加密算法	RSA	使用最广泛的公钥加密算法
Elgamal 算法	Elgamal	基于公钥密码体制和椭圆曲线加密体系
Diffie-Hellman 算法	D-H	只是生成可用做对称密钥的秘密数值，不是一般意义上的加密算法。

制表：区块宝研究院

非对称加密算法在区块链中的使用，具有重大意义。区块链系统中，所有权验证机制的基础是非

对称加密算法。从信任的角度来看，区块链实际上是用数学方法解决信任问题。在区块链系统中，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的对手是“君子”还是“小人”，更不需要求助于中心化的第三方机构来进行交易的信用背书，区块链通过严谨的数学算法就可以建立互信。区块链技术的背后，实质上是算法在为人们创造信用，达成共识背书。

1.3.3 共识机制

共识机制，也称为共识算法。在区块链中，共识机制更多的是体现为：一种确保记账一致性的措施、机制。

利用区块链构造基于互联网的分布式账本，需要解决的首要问题是如何实现不同账本节点上的账本数据的一致性和正确性。这就需要借鉴已有的在分布式系统中实现状态共识的算法，确定网络中选择记账节点的机制，以及如何保障账本数据在全网中形成正确、一致的共识。

区块链中常用的共识机制主要有以下几类：

①PoW：工作量证明机制

简单地说，PoW（Proof of Work）就是一份确认工作端做过一定量工作的证明。PoW 机制的主要特征是计算的不对称性。工作端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查工作端是不是做了相应的工作。

PoW 机制的用例：比特币。

②PoS：权益证明机制

PoS（Proof of Stake）机制在创始区块内写明了股权分配比例，之后通过转让、交易的方式，逐渐分散到用户手里，并通过“利息”的方式新增货币，实现对节点的奖励。PoS 机制使用一个确定性算法以随机选择一个持币者来产生下一个区块，该算法中账户余额决定了节点被选中的概率。

简单地说，就是一个根据用户持有代币的数量和时间（币龄），发放利息的一个制度。类似于股票或者银行存款，如果用户想要获得更多的代币，那么就要打开客户端，让它保持在线，这样就能通过“利息”来获益，同时保证网络的安全。

PoS 机制的用例：未来币。

③PoW+PoS：PoW 发行新币，PoS 维护网络安全

PoW+PoS 结合的机制是指，采用工作量证明机制 PoW 发行新币，采用权益证明机制 PoS 维护网络安全。

这种共识机制最早是于 2012 年 8 月，由一个化名 Sunny King 的极客推出 Peercoin 时采用。

该机制中，区块被分为两种形式：PoW 区块及 PoS 区块。在这种新型区块链体系中，区块持有

人可以消耗他的币龄获得利息，同时获得为网络产生一个区块和用 PoS 造币的优先权。

在 PoW+PoS 机制下，只要是持币人，不论持币的数量是多少，都可以挖到数据块，而不用采用任何的矿池导致算力集中；同时，由于多采用币龄生成区块，而不是算力，所以降低了资源消耗，解决了单纯 PoW 机制在维护网络安全方面的先天不足。

PoW+PoS 机制的用例：Peercoin。

④DPoS：授权股权证明机制

PoS 面临的挑战是如何通过及时而高效的方法达成共识。为了达到这个目标，每个持币节点可以将其投票权授予一名代表。获票数最多的前 100 位代表，按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块，所有的代表将收到等同于一个平均水平的区块所含交易费 1%作为报酬。如果一个平均水平的区块含有 100 股作为交易费，则 1 名代表将获得 1 股作为报酬，这样可以大大提高共识效率，这就是 DPoS（Delegated Proof of Stake）的核心思想。

这 100 位代表可以理解为 100 个“矿池”，这 100 个“矿池”之间的权利是完全相等的。如果这些代表提供的算力不稳定、计算机宕机、或者试图利用手中的权利作恶，那么，那些手里握着代币的用户可以通过投票的方式随时更换这些代表，后备代表则可以代替他们。

DPoS 机制的用例：比特股。

⑤其他分布式一致性算法

除了以上详列的 PoW、PoS、PoW+PoS、DPoS 等共识机制外，还有一些分布式一致性算法，比如：PBFT、Paxos 和 Raft 等。

这类分布式一致性算法常用于联盟链、私有链。而这些分布式一致性算法又分为解决拜占庭将军问题的拜占庭容错算法（PBFT）和非解决拜占庭问题的分布式一致性算法（Paxos、Raft）。

图表 8：共识机制汇总

算法名称	适用环境	用例
PoW	公有链	Bitcoin
PoS	公有链	Nextcoin
PoW+PoS	公有链	Peercoin
DPoS	公有链	Bitshares
PBFT	联盟链、私有链	IBM Hyperledger fabric
Paxos	联盟链、私有链	Chubby lock
Raft	联盟链、私有链	CITA
RPCA	公有链、联盟链	Ripple

PoET	公有链、联盟链	Hyperledger Sawtooth

制表：区块宝研究院

这些共识机制各有优劣。例如 PoW 共识机制在安全性和公平性上比较有优势，也依靠其先发优势已经形成成熟的挖矿产业链，但也因为其对能源的消耗而饱受诟病。而 PoS 和 DPoS 等则更为环保和高效，但在安全性和公平性方面比不上 PoW 机制。

在设计了共识机制的区块链网络中，每个节点只有保持诚实记账，才能获得网络中的奖励。本质上，共识的达成，是基于人类的趋利避害的本能。一般而言，各种共识机制并没有严格意义上的优劣之分，只是分别适用于不同的环境。

第二章 区块链行业概述

2.1 区块链产业生态链

区块链技术是具有普适性的底层技术框架，可以为金融、经济、科技甚至政治等各个领域带来深刻变革。以区块链技术为核心的区块链行业，已经形成了一个比较完整的产业生态链。

狭义的产业生态链可以理解为产业链，比如：数字货币矿机行业，上游是芯片厂商、各种硬件供应商等，中游是矿机的研发、生产、加工、组装等厂商，下游是各大矿场及个人矿工。

广义的产业生态链是指遵循开放、有序、合作、共赢的原则，为区块链技术及区块链行业的发展创造更好的生态环境，让身处其中的各个元素共存共荣，最终实现整个产业链条及系统和谐发展的一个生态环境。

自区块链技术诞生以来，随着区块链技术在各行各业应用场景的逐步落地，区块链产业生态链已经初具雏形。

区块链产业生态链中的各个元素在 2017 年都呈现出一个高速发展、百花齐放的形势。开源社区、产业联盟、骨干企业、初创公司、投资机构、金融机构、监管机构等各司其职，在区块链行业的发展过程中积极扮演着区块链行业内的各种角色。

开源社区

开源社区是区块链技术的发源地，区块链技术诞生于开源社区。开源社区是区块链产业生态链中非常重要的一个节点，也是区块链技术保持持续发展、突破的源泉。

开源社区一般由拥有共同兴趣爱好的人组成，根据相应的开源软件许可证协议公布软件源代码，由于开放源码是由散布在世界各地的编程者共同开发，开源社区就成了他们沟通交流的必要途径。以 Github 社区为例，大批周边扩展服务被建立起来，构成了一个极具活力的生态圈，开发技术人员不仅可在 Github 上参与开源项目，更可建立社交圈子，促成开放的分布式协作模式。

开源社区的最主要特征是：团队协作、个体平等、主动贡献。这也是开源精神的主要内涵。开源社区具备很强的利他主义（Altruism）精神，参与到开源软件开发并把源代码开放给大家共享的开源社区成员，一般称之为贡献者（Contributor）。贡献者通过参与开源社区的开发，一方面得到了锻炼成长的机会，也有助于解决自身工作中遇到的技术问题，另一方面开源项目也有机会产生较大的商业价值，而商业化进程中就又需要这些贡献者担任顾问以推进技术落地。

最早的区块链开源社区是比特币社区，此后区块链领域几乎所有重要的技术革命和突破也均诞生于建立在开放、自由、共享理念之上的各开源社区与开源项目。如图灵完备的智能合约平台以太坊的开源社区，以联盟链的形式将区块链技术大规模商用的 IBM 等机构建立的 HyperLedger 开源社区等。

产业联盟

区块链行业的产业联盟，是助力区块链技术快速商用的重要推手。国内外知名区块链产业联盟主要有 2015 年成立的 R3 区块链联盟、Hyperleder，2016 年成立的中关村区块链产业联盟、China Ledger 联盟，2017 年成立的俄罗斯区块链联盟等。

产业联盟往往能够聚集政、企、学三界力量共同发力，在促进区块链技术的商业落地方面发挥着重要作用，在建立区块链行业标准方面也扮演着重要角色。

骨干企业

区块链行业内的骨干企业，往往是区块链技术商用方向的风向标。所谓骨干企业，是指在行业内起重要支撑作用的企业，对促进行业发展起主要作用的企业。由于区块链技术是一项新兴技术，区块链行业是一个新兴行业，因此，区块宝研究院对区块链行业的骨干企业的界定，并不参考纳税额，更多的是考虑其在区块链技术商用探索过程中是否具备风向标作用。

近几年来，已经有一些企业在区块链行业中崭露头角，比如：

微软：提供 BaaS（Blockchain as a Service）的微软 Azure，是微软区块链技术方案的后盾，支持众多分布式账本技术。Azure 的 BaaS 旨在基于微软全球领先的云系统技术支持下，进行深入研究新的业务流程；

Coinbase：Coinbase 成立于 2012 年 6 月，先后多轮次获得国际知名投资机构投资，Coinbase 制定了通过“比特币钱包+数字货币交易平台+开发者工具平台+商户支付应用”四大产品线创建自我增强的生态系统的强大战略，通过提供不同产品和服务全面聚拢交易用户、开发者用户、企业用户等多种力量。尤其在拓展企业用户及合作伙伴方面表现出突出的执行力。

无论是数字货币交易平台出身的 Coinbase，还是做 BaaS 业务的微软，他们在区块链领域的商业布局，值得区块链行业内外的企业关注和思考。

初创公司

区块链行业初创公司的稳步发展，是做强区块链产业生态链的着力点。初创公司的专业化程度，会影响区块链产业生态链的匹配度，行业内产业链上中下游企业的协同发展，大中小企业的错位发展，才能实现区块链产业生态链的做大做强。

区块链行业初创公司的繁荣发展，也是区块链推动时代的巨轮从信息互联网到价值互联网的必要条件。区块链作为一项底层技术，必须结合各个行业的具体应用场景，唯有在各个行业的应用场景中落地实施，区块链才能发挥更大的影响力。所以，区块链初创公司在区块链产业生态链中同样具有非常重要的作用。

目前已经初具影响力的领域包括：金融领域的支付汇款、智能债券、资产发行与交易后清结算等；

非金融领域的数字存证、物联网、供应链、医疗、公益、文化娱乐等。此外，还有一些为区块链开发者提供开发平台的技术性初创公司也发展得比较好。

投资机构

投资机构是行业发展的内在推手，也是区块链行业中承担风险的先锋。区块链技术是一项新兴技术，区块链技术的应用场景的落地商用还处于早期的探索阶段，毫无疑问，投资机构是区块链行业中最早一批承担风险的机构。

国际知名的区块链行业内的投资机构有很多，比如：投资了 Ripple Labs、Coinbase、21 Inc、TradeBlock、OpenBazaar 等区块链公司的 Andreessen Horowitz，投资了 Circle、Coinbase、Koinify、Ripple Labs 等区块链公司的 IDC。

2015 年以前，主要的投资主要集中在与比特币相关的企业中，比如矿机芯片、交易平台、支付汇款、钱包服务等相关企业。随着区块链技术的发展，越来越多的资金投入在了区块链技术研发及行业应用上，包括交易后清结算、智能合约、供应链、物联网、医疗、身份认证、数据存储、数据分析等。

金融机构

金融机构有助于区块链稳健发展，将引领区块链产业生态链走向繁荣。芝加哥商品交易所已于 2017 年 12 月 10 日推出首款比特币期货合约，期货合约具有套期保值功能，比特币在实际贸易中是有一些应用场景的，市场对比特币期货的套期保值功能有市场需求。许多使用比特币作为交易媒介的商家，为了抵御比特币价格波动的风险，需要金融机构提供这种套期保值的金融产品。

众所周知，硅谷是科技的代名词，华尔街是金融的代名词，在区块链方面，华尔街表现出来的热情比硅谷更高。究其原因，金融机构是区块链行业的重要建设者之一。

自 2015 年以来，全球主流金融机构纷纷开始布局区块链，以高盛、摩根大通、瑞银集团为代表的银行业巨头纷纷成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。

监管机构

监管机构在区块链行业也扮演着重要角色，一方面是引领作用，另一方面是规范作用。在区块链的发展过程中，区块链技术的无中心、分布式、匿名性等特点，曾经一度被不法分子利用。监管机构在区块链行业的发展过程中与时俱进，一方面，采取了不少先进的“监管科技”，打击了不法行为；另一方面，也设立了“监管沙盒”，引领区块链行业的稳健发展。

整体而言，以区块链技术为核心的区块链行业，已经形成了一个配套开源社区、产业联盟、骨干企业、初创公司、投资机构、金融机构、监管机构等一系列角色的区块链产业生态链。

2.2 区块链产业价值链

与其他行业不同，区块链行业的产业价值链的呈现方式比较特别。因为区块链技术具备传递价值的功能，研究区块链行业的产业价值链时，我们会发现，有一条特殊的价值传导通道，在一定程度上体现了区块链产业的价值传导过程。

在《区块链：价值互联时代的引擎》报告中，区块宝研究院首次提出“区块链是推动时代的巨轮从信息互联网时代向价值互联网时代前进的引擎”的论断。区块宝研究院当时提出这个论断是基于非常充足的论据，包括“区块链技术表现在加密数字货币方面可以实现价值转移”、“区块链技术的追本溯源、不可篡改等特点使互联网传递的大量信息仍然有价值”等。

因为区块链技术可以实现价值转移，所以在研究区块链行业的产业价值链时，有一个特殊的价值传导过程，是有别于其他行业的。

区块链行业的产业资产价值，主要呈现下图的传导过程：

图表 9：区块链行业价值传导图

制表：区块宝研究院

芯片作为数字货币矿机的核心部件，芯片厂商是矿机厂商最重要的供应商，芯片厂商也就成了区块链产业价值链上的第一个获利环节。在早期，使用一般电脑的 CPU 就能非常轻松的制造新的区块而挖到比特币；之后，矿工们开始使用高端 GPU 显卡参与矿池挖矿；再然后，有了半定制化的 FPGA 矿机，运算能力又比高端 GPU 显卡高很多；最后，半定制化的 FPGA 矿机在算力功耗方面又迅速被定制化的 ASIC 矿机超越。这种定制化 ASIC 比特币矿机专为比特币挖矿算法设计，只能用于挖矿，ASIC 比特币矿机的出现使得显卡挖矿成为历史。

区块链产业价值链的第二个获利环节，当数矿机厂商。国际上知名的比特币矿机厂商有 Butterfly Labs、GAW Miners、KnCMiner、BitFury Group、21 Inc 等，国内的比特币矿机厂商有 Canaan-creative、Bitmain、ASICMiner 等。

再然后，就是在区块链行业发展过程中扮演了重要角色的矿场、矿工。最初全世界只有两个矿工，除了中本聪之外，另一个叫哈尔·芬尼，他是密码圈成名已久的大牛，也是第一笔比特币转账的接收者，早期只有他和中本聪两个人测试比特币网络。因为越来越多人知道挖矿有利可图，全网算力持续

上涨，比特币挖矿难度持续提升，个人挖矿就没有优势了，于是矿场（矿池）也就登上了历史舞台。所谓矿池，就是把大家的算力集中起来，挖到比特币之后收益大家一起分。比特币挖矿趋于集约化的现象，对于实现区块链的去中心、分布式账本的初衷是不利的。掌握着全网多数算力的矿场在 2017 年的许多举措，已经动摇了区块链发展的初衷，这个态势值得区块链技术和区块链资产爱好者引起重视。

数字货币交易所也是区块链产业价值链的重要环节，数字货币交易所是区块链资产的中转站，是区块链资产的贸易中心。数字货币交易所对于区块链行业的发展也有积极的促进作用，数字货币交易所的存在给了区块链产业生态链的众多参与者一个便捷变现的机会，也给普通的区块链资产爱好者、区块链产业投资者提供了一个便捷的入场渠道。另外，数字货币交易所往往还直接或间接地对接着看似处于这条产业价值链之外，但同样处于区块链产业生态链中上游的区块链项目方。

数字货币投资者，既是区块链产业投资者，也是区块链产业受益者。数字货币投资者是区块链产业价值链的下游，也是区块链产业发展最坚实的基础。同时，数字货币投资在区块链产业价值链中参与门槛和变现门槛也最低。

区块链具有价值传递的功能，这个特点使得区块链行业具有特殊的魅力。在一般行业，普通投资者是无法直接进入到产业价值链环节中的，但是区块链技术的价值传递功能解决了这个难题。区块链技术，让更多普通投资者，能够参与到一个产业的投资中来；让更多普通投资者，像投资机构一样，能够伴随着区块链产业的壮大、发展，分享产业蓬勃发展带来的丰厚利润，而且能够便捷地将投资变现。

鉴于区块链产业生态链的繁荣发展，区块链产业价值链也将呈现出集点、线、面、网于一身的发展态势，贯穿区块链产业价值创造、传递、分配的全过程。区块链产业生态链的多元化发展，会促进区块链产业价值链的发展与完善。

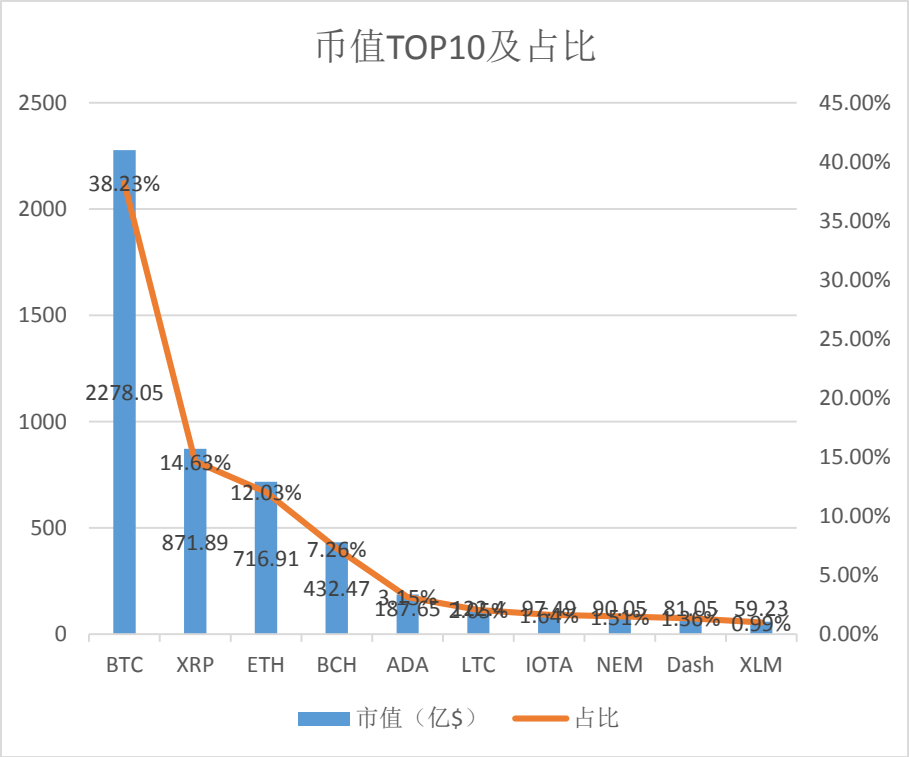
2.3 区块链数字资产统计

鉴于区块链技术具备价值传递功能的特殊属性，区块链数字资产的发展现状及趋势是研究区块链行业发展趋势时不可忽视的一方面，区块链数字资产也是反映区块链行业发展现状的一个视角。

2.3.1 数字资产总市值

据区块宝研究院统计，全球数字货币种类已经多达 1372 种。截至 2017 年 12 月 31 日，全球数字货币总市值已经达到 5958.77 亿美元。币值排名前 10 的数字货币市值数据及其占全球数字货币总市值的比重情况，如下表所示：

图表 10：币值 TOP10 及占比



制图：区块宝研究院

全球数字货币市值分布，呈现高度集中化的现象。全球 1372 个数字货币中，仅 BTC 一个币的市值占比就高达 38.23%，排名前 10 的数字货币市值占全球数字货币总市值的占比高达 82.86%，全球数字货币市值高度集中。

2.3.2 比特币市值分析

区块链行业的数字资产，主要体现在比特币市值上，因此有必要对比特币的市值及财富分布情况进行重点分析。

比特币市值情况

以 2017 年 12 月 31 日 23:59 的比特币价格为统计基础：

① 比特币总市值

比特币设计发行总量为 2100 万枚，按目前市场价 13581 美元，比特币总市值为 2852.01 亿美元。

② 已产出比特币市值

截至 2017 年 12 月 31 日 23:59，比特币区块高度为 501905，已产出比特币总量为 16773812.5 个，那么，目前已产出比特币市值为 2278.05 亿美元。

③ 实际流通比特币市值

据数字取证公司 Chainalysis 的研究报告，大约有 278 万至 379 万个比特币已经永远消失，这个数

字相当于比特币总量的 17%至 23%。

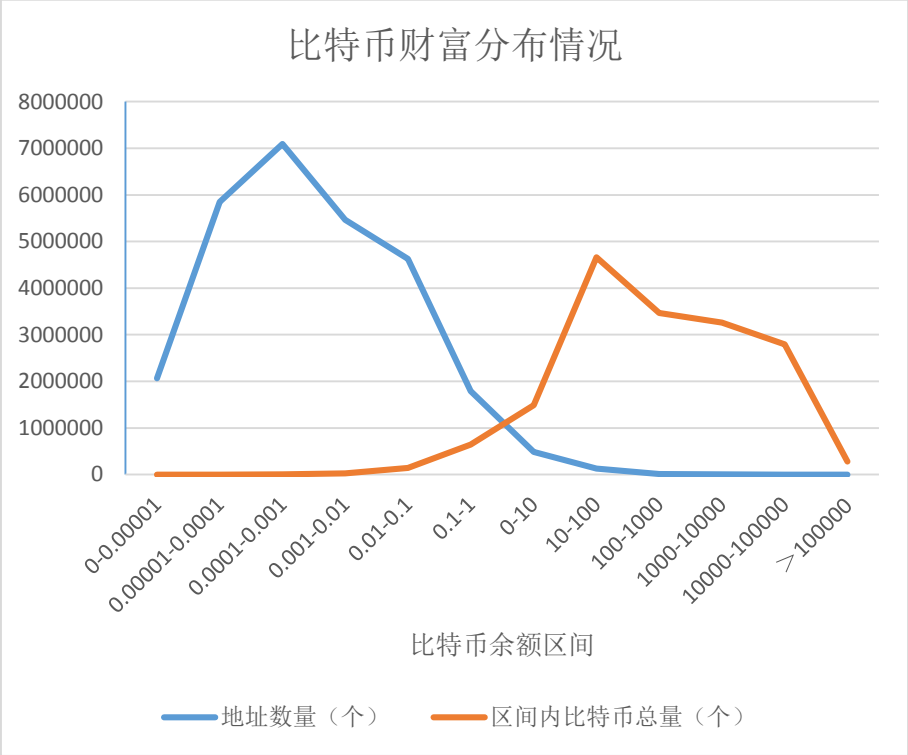
所谓消失，是指永远沉睡。沉睡的比特币不是在各个交易所被盗的比特币，事实上被盗之后，这些比特币还是在网络中。沉睡的比特币主要是 2009 年-2010 年早期的一些挖矿者无意间遗失的。

已产出的比特币总量为 16773812.5 万个，减去消失的比特币数量，目前市场上能流通的比特币大概 1350 万个，实际流通比特币市值大概为 1833.44 亿美元。

比特币财富分布情况

据区块宝研究院统计，截至 2017 年 12 月 31 日，已经产出的比特币地址数量分布情况及区间内比特币总量分布情况，如下表：

图表 11：比特币财富分布情况



制图：区块宝研究院

上表统计 16767681 个 BTC。截至 2017 年 12 月 31 日 23：59，BTC 的区块高度是 501905，已经挖出的 BTC 总数为 16773812.5 个。排除一些无法统计到的数量，数据基本属实。

2016 年年末瑞信研究院（Credit Suisse Research Institute）曾公布一份《2016 年全球财富报告》，该报告指出：全球 0.7%的人口掌控者全球近一半的财富；而处于财富金字塔底部 37%的人口，每人拥有的财富不到 1 万美元。

在比特币的世界里，也就是在所有比特币持有者的世界里，比特币的贫富两极分化的现象更加严重：全球 0.51%的钱包地址占据了 86%的 BTC 数量，全球 2.27%的钱包地址占据了 95%的 BTC 数量；全球 54%的钱包地址合计仅拥有 2964 个 BTC，即 56%的钱包地址合计仅占 0.018%的 BTC 数量；全球 74%的钱包地址合计仅占 0.17%的 BTC 数量。

因为区块链资产的匿名性，做区块链资产分布统计的时候，无法像传统富豪排行榜的统计一样具体到个人或企业，区块链资产的统计只能以钱包地址为单位。默认一个钱包地址对应一个单位，实际情况可能是多个钱包地址都是属于同一个单位。也就是说，实际区块链资产的集中度可能比统计情况更严重。

第三章 2017 年回顾

3.1 政策保驾护航：各国政府纷纷出台专项政策

区块链行业作为一个新兴行业，离不开国家政策的引导和规范。随着区块链的应用价值逐步获得认同，部分国家相继出台了一些区块链相关的政策，但全球各国针对区块链出台的政策都比较零散，不具备系统性，大多数是没有配套框架的扶持性的专项政策。

图表 12：各国区块链政策摘要

国家	内容
美国	2016 年 6 月，美国国土安全部对 6 家致力于政府区块链应用开发的公司发放补贴，推动政府数据分析、连接设备和区块链的研究发展。
	2017 年 3 月，亚利桑那州将基于区块链的签名和智能合约置于州法律内。4 月，通过了禁止利用区块链追踪枪械的议案。
	2017 年 6 月，内华达州参议院通过了第 398 条法案，免除了区块链技术使用的相关赋税和管制。
	2017 年 7 月，特拉华州通过一项修正法案，明确允许在区块链上进行股票交易的权利。
俄罗斯	2017 年 1 月，关于“合法化”区块链技术的发展路线图提交总统批准。
韩国	2016 年 2 月，韩国央行在报告中提出鼓励探索区块链技术。
德国	2016 年，德国联邦金融监管局对分布式账本的潜在应用价值进行探索，包括在跨境支付中的使用，银行之间转账和交易数据的存储。
加拿大	2016 年 6 月，加拿大央行展示了利用区块链技术开发的 CAD-Coin，即电子版加元。
英国	2016 年 1 月，发布白皮书《分布式账本技术：超越区块链》，第一次从国家层面对区块链技术的未来发展应用进行全面分析并给予研究建议。
	2016 年 5 月，英国金融行为监管局（FCA）正式启动“监管沙盒”，为区块链等金融科技企业在监管政策不确定的情况下提供了一个安全创新的环境。
新加坡	2016 年 6 月，新加坡提出监管沙盒机制，并于 11 月发布《金融科技

	监管沙盒指引》文件。
澳大利亚	2016 年 12 月，澳大利亚 ASIC 发布《金融科技产品及服务测试》监管指引文件，澳大利亚的沙盒不需要公司申请许可，ASIC 直接在监管指引文件中发布了监管豁免条款，只要符合特定条件并告知 ASIC 即可开启测试服务。
马耳他	2017 年，马耳他首相宣布国家支持区块链技术，高度评价了区块链技术的不可更改和去中心特点在储存和处理敏感数据的优势。并于 9 月成立了区块链咨询委员会，汇集了一些专家，专门就其国家区块链战略提供建议。
中国	2016 年 12 月 15 日，国务院印发的《“十三五”国家信息化规划》中，区块链技术被定义为战略性前沿技术。
	2016 年 12 月 31 日，贵阳市人民政府发布《贵阳区块链发展和应用》白皮书。
	2017 年 5 月，央行成立金融科技委员会，旨在加强金融科技工作的研究规划和统筹协调。
	2017 年 8 月，国家互联网应急中心发起成立的国家互联网金融安全技术专家委员会官网发布《合规区块链指引》。
	2017 年 10 月，深圳市人民政府向各区人民政府、市政府直属各单位引发《深圳市扶持金融业发展若干措施》，其中提到“设立金融科技（Fintech）专项奖，重点奖励在区块链、数字货币、金融大数据运用等领域的优秀项目。”

制表：区块宝研究院

全球区块链政策中，对区块链技术的扶持力度最大的当属美国内华达州通过的第 398 条法案。2017 年 6 月，内华达州参议院通过了第 398 条法案，免除了区块链技术使用的相关赋税和管制。该法案旨在为新兴的技术公司创造一个良好而非敌对的环境，也首次认可了智能合约的合法性和法律约束力。该法案禁止：

州政府：（一）对使用区块链征收税费；（二）使用区块链需要获得证书、执照和许可证；（三）对使用区块链强加其他任何要求。

虽然全球各国出台的区块链相关政策尚属零散，但这些扶持性政策的出台，意味着多数国家政府已经认识到区块链技术的巨大应用前景。国务院印发的《“十三五”国家信息化规划》中，将区块链

技术列为战略性前沿技术，意味着政府已经开始着手从国家战略发展的层面考虑区块链的发展道路。

3.2 监管引领规范：多个地方政府引入监管沙盒

监管在区块链行业发展过程中，一方面具有引领发展的功能，另一方面具有规范发展的功能。

根据区块链的应用层划分，区块链划分为区块链 1.0 可编程货币、区块链 2.0 可编程金融、区块链 3.0 可编程社会三个阶段，区块宝研究院曾在《区块链：价值互联时代的引擎》中判定当前处于 1.0 成熟，2.0 拓展，3.0 探索的阶段。非常时期用非常手段，针对金融科技的特色监管方式——监管沙盒，也就在这个阶段诞生。

监管沙盒（Regulatory Sandbox）的概念由英国政府于 2015 年 3 月率先提出。先后获得英国、新加坡、澳大利亚、中国、马来西亚、阿联酋等国采用。

图表 13：全球监管沙盒的用例

国家	内容
英国	2016 年 5 月 9 日，英国 FCA 率先启动监管沙盒机制。
新加坡	2016 年 6 月，新加坡提出了监管沙盒机制。
澳大利亚	2016 年 12 月，澳大利亚 ASIC 发布了一份指引文件，允许符合条件的金融科技公司在向 ASIC 备案后，无需持有金融服务或信贷许可证即可测试特定业务。
中国	2017 年 7 月 9 日，中国赣州区块链金融产业沙盒园暨地方新型金融监管沙盒在北京正式启动。
	2017 年 7 月 25 日，中国贵阳发布“区块链 ICO 沙盒计划”。
	2017 年 9 月 29 日，中国香港证监会也推出了监管沙盒，为合资格企业提供一个受限制的监管环境，以便其使用金融科技来进行受规管的活动。
马来西亚	2016 年 10 月，马来西亚政府正式宣布推出监管沙盒计划。
阿联酋	2016 年 6 月，阿布扎比酋长国的金融服务监管部门（FSRA）为区块链初创企业提供沙盒环境，初创公司可以在灵活的监管架构下运行长达两年时间的方案。
	2017 年 10 月，阿布扎比接受第二批企业入驻监管沙盒。

制表：区块宝研究院

中国地方政府主要在 2017 年相继推出监管沙盒，是对金融科技领域的创新的鼓励和引领。

目前国际上金融科技的监管模式大致可以分为两类：

一类是一些相对小型开放的经济体并且是国际金融中心，比如英国、新加坡。这些国家由于自身市场比较小，金融科技发展产生的风险隐患并不是很突出，同时肩负着国际金融中心发展的使命，会采取一些鼓励措施，包括引入监管沙盒；

另一类是一些大型经济体且金融市场特别大，比如美国。美国发展金融科技在技术上具有一些领先优势，并且在金融科技穿透式监管、功能监管方面比较突出。

从国际经验看，监管沙盒实施对象是一些初创型企业，金融科技自我发展动力不足，需要鼓励发展。而我国市场比较大，金融科技机构相对而言比较容易盈利，自身发展动力强。

中国人民银行金融研究所所长孙国峰指出，中国金融科技监管要将微观功能监管与宏观审慎管理相结合。微观功能监管采取穿透式监管，根据金融科技的金融特征，按照相关业务的类别由相关监管当局进行监管，实现监管全覆盖，避免监管空白；宏观审慎管理是把金融科技纳入到宏观审慎管理框架当中，完善支付机构客户备付金集中制度。

监管沙盒在中国采用相对较晚，截至目前也仅仅在赣州、贵阳、香港等局部地区试行，实施时间还不长。监管沙盒机制是否适合中国土壤、能否产生良好效果目前尚未可知，但中国多个地方政府在2017年相继设立监管沙盒，足以说明政府对金融科技领域、对区块链行业的重视。

另外，2017年9月4日，中国政府七部门联合发布《关于防范代币发行融资风险的公告》，督促行业远离乱象回归理性，共同维护正常的金融秩序。这个举措对于区块链行业而言意义非凡，将区块链行业发展从盲目、投机、炒作中拉回到理性地探索区块链技术应用场景落地的道路上。

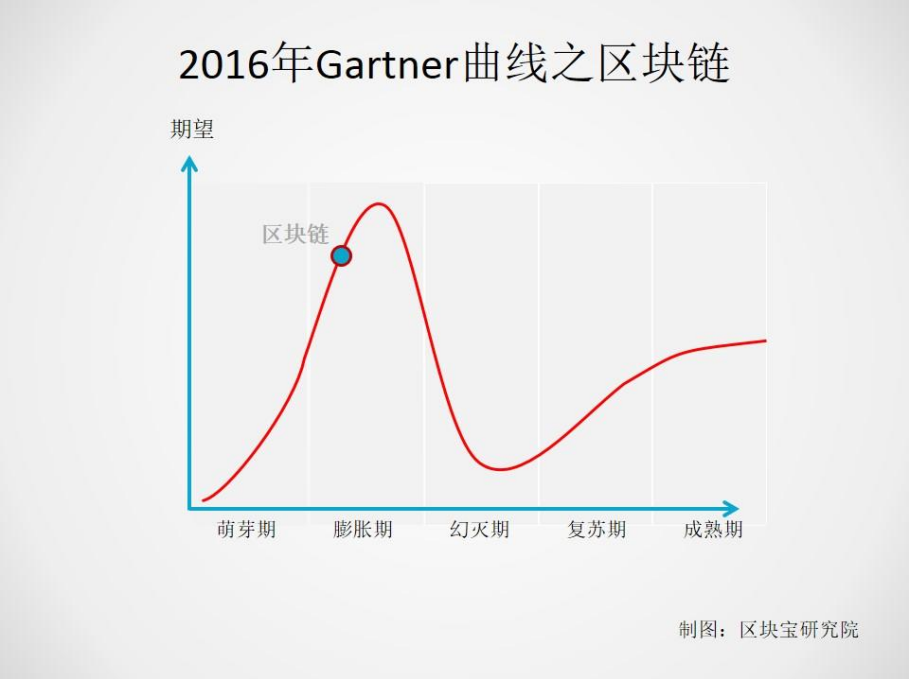
3.3 行业上下求索：前路漫漫，道阻且长

2016年是区块链元年，2017年是区块链的“应用元年”。其实，2017年也是区块链的“问道”之年。

区块链技术连续两年位列Gartner公司发布的Gartner新兴技术成熟度曲线：

2016年，区块链技术位列Gartner新兴技术成熟度曲线的期望上升阶段末期，并且已经进入期望膨胀期，Gartner公司认为区块链技术的成熟时间需要5-10年。

图表 14：2016 年 Gartner 曲线之区块链



2017 年，区块链技术再次位列 Gartner 新兴技术成熟度曲线，但此时区块链技术已经处于期望膨胀期末期，并且已经处于期望下降阶段初期即将进入幻灭期，Gartner 公司依旧认为区块链技术的成熟时间需要 5-10 年。

图表 15：2017 年 Gartner 曲线之区块链

Gartner 认为，区块链概念正在得到人们的认可，未来它将改变行业的经营模式。区块链在多个行业获得应用落地的实例表明其初步价值，但还需要进一步的验证。未来，我们将看到区块链在金融服务业、制造业、政府、医疗和教育行业得到更快的认可和应用。

区块宝研究院认为，Gartner 公司提出的区块链技术正在得到人们的认可，未来将改变行业的经营模式是正确的。但是，我们认为区块链行业在逐渐获得人们认可的同时，其实也在不断地重新自我

认识。区块链行业仍然是在上下求索的道路上，前路漫漫，道阻且长，区块链行业的参与者、建设者们仍需不忘初心，砥砺前行。

2017 年，区块链行业发生了很多特别重大的事情，对推动区块链行业的发展影响深远：

① 埃森哲专业服务提供商获得“可编辑的区块链”的技术专利

2017 年 9 月底，埃森哲（Accenture）专业服务提供商获得了一项与“可编辑的区块链”技术相关的专利。该专利许可的区块链将使各方能够在错误或欺诈的情况下编辑数据。

埃森哲的“可编辑的区块链”概念旨在解决如何在出错时解决问题的问题，以及将技术推向“成熟”的一种方式。

“可编辑的区块链”增加了一系列的选择，特别是对链上的数据结构，埃森哲发明这项专利的初衷是：利用 DLT 创新，使区块链技术能够用于企业 IT 使用。

埃森哲公司主张“在区块链系统上，允许企业解决人为错误，适应法律法规的要求，解决恶作剧和其他问题，同时保留密钥加密特性。”

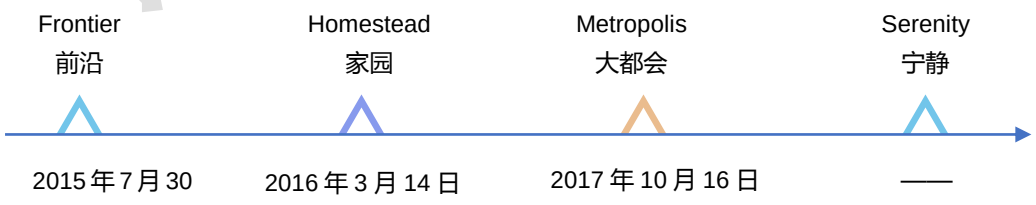
埃森哲公司的这项专利，是有违区块链技术最初设计的。区块链技术的“不可篡改”特性，虽然无法保证记录在区块链账本中的信息是诚实的，但是却可以记录下一切不诚实的行为和历史记录。

对于是否要反对埃森哲的这项专利技术用于区块链，是否要坚定保持区块链的“时序性”和“防篡改性”，区块宝研究院认为，仁者见仁智者见智。区块链的技术方案，具有诸多优点，不同商业场景使用区块链技术的核心目的不同，只要使用区块链技术后能够达到所想要的效果，使用区块链技术后能够实现降低成本、提升协作效率的目标，能够让世界更美好，并不一定要将区块链技术的所有优点汇集，毕竟不同商业场景使用区块链技术的核心目的不同。只是，区块宝研究院希望区块链行业的建设者和区块链技术的研发者，不要把区块链行业和区块链技术变成自己曾经讨厌的模样。

② 以太坊进入大都会阶段，开始向 PoS 证明机制转变

2017 年 10 月 16 日，以太坊网络在 4370000 区块高度成功进行拜占庭硬分叉，以太坊正式进入大都会（Metropolis）阶段。此次拜占庭硬分叉后以太坊使用的是 Casper 共识算法，以太坊将是一个 PoW 和 PoS 共存的系统，每 100 个区块将有一个采用 PoS 协议挖出。

图表 16：以太坊的规划路线



制图：区块宝研究院

以太坊在设计之初，提出了 PoW 转 PoS 的明确方案，以太坊最终采用 PoS 的设计理念主要目的

是节约能源。为了能够坚定的实现从 PoW 向 PoS 的转换，以太坊设计了一个以太坊冰河期（ICE AGE）。

以太坊的冰河期实际上是以太坊的 PoW 机制对难度的调整策略。不同于比特币里 PoW 对难度的调整策略（根据平均 10 分钟出一次块动态调整，可调大可调小），以太坊里 PoW 对难度的调整将随着区块高度不断增加，而且这个增加是指数级的，算力发展的速度将远跟不上难度增加的速度。

以太坊的 PoW 机制对难度的调整策略的结果：一方面，平均出块时间将不断增加；另一方面，当区块增长到一定高度，PoW 的难度值将大到矿工们无法在合理的时间里打包出区块。（这种现象称为“难度炸弹”）

所以，以太坊务必在出现难度炸弹之前进行升级，以防进入冰河期。

以太坊进入冰河期的时间并没有一个明确的红线，一般认为当区块高度达到 480 万左右，平均出块时间将会严重影响到以太坊系统正常运转。因此，为了以太坊网络的正常运转，不能让以太坊进入冰河期。故而，以太坊决定在第 437 万个区块高度开始从“家园”向“大都会”的升级。

根据 2015 年公布的计划，以太坊从“家园”向“大都会”的升级将分为两个阶段：

第一阶段——拜占庭硬分叉；

第二阶段——君士坦丁堡。

北京时间 2017 年 10 月 16 日 20 点-21 点进行的就是第一阶段的拜占庭硬分叉。

以太坊进入大都会后，主要有以下四个方面的变化：

第一，zk-Snarks。“大都会”最大和最重要的特性就是执行 zk-Snarks（简明非交互零知识证明），zk-Snarks 基于“零知识证明”。

第二，PoS 早期实施。以太坊的 PoS 协议使用的是 Casper 共识算法，它不仅能激励诚实的矿工还能惩罚不诚实的矿工。Casper 共识算法下，以太坊将是一个 PoW 和 PoS 共存的系统，以太坊将开始从单纯的 PoW 向 PoS 转变。

第三，以太坊将更加体现其“去中心的应用平台”的作用，而不仅仅是一种数字货币。以太坊平台将会引入 9 大关键改进协议（EIP），这将使以太坊平台更加轻巧高效，还能提高交易速度和智能合约的安全性、隐私性、灵活性、稳定性。

第四，抽象账户。所谓抽象账户就是量子级别的安全账户。现在的以太坊有两类账户——外部账户和合约账户，外部账户由私匙控制，合约账户由创建者编写的代码控制。以太坊进入“大都会”后，将模糊二者的界限。通俗地说，抽象账户是一个方便人们使用的人性化且具备量子级别安全性的以太坊账户。

③ 崛起中的亦来云：区块链驱动的智能万维网

亦来云（elastos）致力于将互联网打造成为智能经济生态圈，不仅具备以太坊的智能合约功能，还解决了以太坊网络的几个弊端。例如：

从连接用户日常场景的角度来看，以太坊 EVM 存在两个主要问题：第一，单主链结构，计算能力有上限，无法扩容；第二，区块链作为存储和计算空间，无法支持用户日常生活场景，无法应用数字内容。

对于第一个问题，亦来云采用主链+侧链的弹性区块链设计结构。主链只负责基本的交易和转账支付；侧链执行智能合约支持各种应用和服务，每条区块链都是一台服务器。现实软件方案里，当服务器性能无法突破上限时，通常的做法不是去研发超级服务器，而是增加更多的服务器分流负载。在区块链项目上也同样，亦来云通过弹性侧链的方式让不同应用、服务共享一条侧链或分别部署在不同侧链，从而满足多样的需求。

在 2017 年推出的 CryptoKitties 的火爆，导致以太坊堵塞的事实已经证明，单靠一条主链想运行所有智能合约是很难的。而亦来云的主链+侧链的弹性设计解决了这个难题。

对于第二个问题，亦来云通过 Elastos Runtime 将 App 运行在相互隔离的进程、通信受阻的沙箱环境中。所有网络数据必须通过安全、可信、可识别身份的通道发送，这些身份识别和鉴权都来自于区块链身份 ID。这样就让区块链的可信传递到 Elastos Runtime。而 Elastos Runtime 可以有多种形态：可以是独立 OS，可以是 VM 虚拟机，可以是结合原生 App 的 SDK。

总而言之，以太坊的智能合约在区块链行业里当时是一个首创，以太坊的智能合约是一个非常好的概念、想法；而亦来云则是试图基于以太坊的设计理念，对以太坊的弊端进行改善的一个将“概念”进行商业化，可能实现商用，具备商业价值的项目。大多数行业都会经过不断地试错、改善的过程，而后才产生越来越完美的应用，逐步具备商业价值。

④ 比特币频繁硬分叉，且比特币分布高度集中

2017 年 8 月 1 日比特币硬分叉产生 Bitcoin Cash（BCH），BCH 支持 8M 大区块，不需要 Segwit，BCH 挖矿算法和矿机与 BTC 一样。BCH 分叉成功后，支持 BTC 大区块的机构都转向 BCH，币价一度高达 19000 元人民币。

BCH 币价的表现，成了比特币当今频繁硬分叉的导火线。自从 BCH 硬分叉获得极大成功后，诸多团队纷纷发行比特币分叉币。据区块宝研究院统计，影响较大的比特币分叉币已经多达九种。

图表 17：比特币分叉币统计表

代码	中文名	分叉高度	分叉时间	总发行量（万）
BTC	比特币	——	——	2100
BCH	比特现金	478559	2017 年 8 月 1 日	2100
BTG	比特币黄金	491407	2017 年 10 月 25 日	2100
BTX	比特币土叉	494784	2017 年 11 月 17 日	2100

BTD	比特币彩钻	494784	2017 年 11 月 17 日	0.21
BCD	比特币钻石	495866	2017 年 11 月 24 日	21000
SBTC	超级比特币	498888	2017 年 12 月 12 日	2121
BCX	比特无限	498888	2017 年 12 月 12 日	21000000
BTW	比特世界	499777	2017 年 12 月 17 日	21000000
BCK	比特币王者	499999	2017 年 12 月 19 日	2100
BTP	比特支付	500000	2017 年 12 月 23 日	2100

制表：区块宝研究院

比特币频繁发生硬分叉的现象，表明区块链行业的发展仍不成熟，行业内分歧仍然大量存在，共识依旧没有形成，投机的思想还是比较严重。

另一方面，比特币的分布情况，也反映出严重的集中性。全球 0.51%的钱包地址占据了 86%的 BTC 数量，全球 2.27%的钱包地址占据了 95%的 BTC 数量；全球 54%的钱包地址合计仅拥有 2964 个 BTC，即 56%的钱包地址合计仅占 0.018%的 BTC 数量；全球 74%的钱包地址合计仅占 0.17%的 BTC 数量。

⑤韩国比特币交易所 YouBit 遭黑客攻击破产，安全仍然堪忧

2017 年 12 月 19 日，韩国比特币交易所 YouBit 称遭“黑客入侵”，自行宣布破产。三年前，当时世界最大比特币交易平台 Mt Gox 也因黑客攻击宣布破产，破产后投资者无处索赔。时隔三年，区块链资产的安全问题仍然堪忧。

2017 年是区块链的“问道”之年。区块链曾经以“不可更改”的特点著称，而今埃森哲的“可编程的区块链”专利技术却能够在许可的区块链中让各方能够在错误或欺诈的情况下编辑数据；区块链曾经以“去中心化”的特点著称，而今以太坊进入大都会正式开启 PoS 证明机制，权益证明机制的马太效应极可能导致中心化的结果，然而作为 PoW 机制的践行者，比特币的实际分布情况，却也反映出“去中心化”方面的失败；区块链曾经以“安全可信”的特点著称，而今比特币的频繁硬分叉，比特币交易所一再发生重大资产丢失，令人对区块链资产的安全问题担忧。好的现象是，区块链行业一直在探索中前进，区块链技术的商用价值仍在逐步验证。

对于区块链行业，中长期趋势良好，新兴技术，大有可为；短周期存在挑战，前路漫漫，道阻且长。曾经高喊着去中心的，如今成为了新的中心。作为新兴技术的区块链技术，在走向成熟的同时，却也可能变成自己曾经讨厌的模样。值得期待的是，区块链行业的项目仍处于不断改善中。还是衷心地希望区块链行业的建设者们，不忘初心，砥砺前行！

第四章 2018 年前瞻

1714 年发明的打字机用了 150 年才被普遍运用，1836 年发明收割机用了 100 年时间才得以推广，而 1920 年左右发明的吸尘器、冰箱只用了 34 年时间就已全球普及，1939 年以后发明的电视机等电器只用了 8 年时间就已行销全球。区块链的发展，又会在何时推动时代的巨轮全面进入价值互联网时代？

这是一个让人眩晕、迷茫的变化速度，唯一的选择——除了变革，还是变革；这也是一个让人激动、兴奋的变化速度，极大的可能——价值互联，未来已来。

2017 年是区块链行业的“问道”之年，2018 年有望成为区块链行业的“整合”之年。根据诸多方面的信号，区块宝研究院认为，2018 年区块链行业有望呈现三个主要趋势：联盟链/私有链成为主流、跨链需求增多、行业资源整合趋势明显。

4.1 企业应用是主战场，联盟链/私有链将成为主流

在企业级应用中，企业更关注区块链的强身份许可、安全隐私、高性能、海量数据、监管合规等元素；另外，大多数企业使用区块链技术的主要目的是降低成本和提升协作效率。因此，联盟链/私有链这种强管理的区块链部署模式，更符合企业在应用场景落地中的需求，将成为企业级应用的主流技术方向。

目前在商业应用中定位比较清晰，作用比较明确的多数是联盟链。呈现方式多数是某个行业的上下游，或者一些核心企业联合起来，一起构建一个半公开化的区块链，以便共同将业务规模做大，最终实现共同发展。例如 R3、Hyperledger 等。

4.2 跨链需求增多，互联互通的重要性凸显

如前所述，行业级、企业级用户的主流方向是联盟链。随着区块链应用的深化，支付结算、物流追溯、医疗病例、身份验证等领域的产业链或企业，都将建立各自的区块链系统。

受吞吐量、网络孤立性、监管、伸缩性等因素的制约，目前的区块链项目并不能很好的服务于商业应用。在区块链所面临的诸多制约因素中，网络孤立性阻碍了不同区块链之间的协同操作，极大限制了区块链在商业应用中的发挥空间。

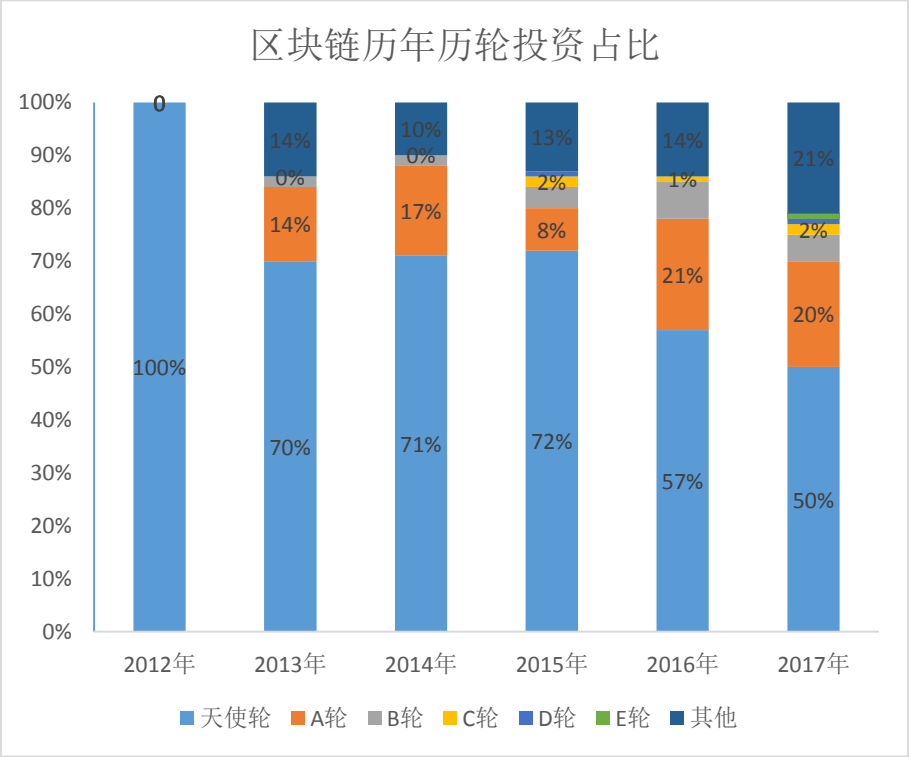
如果说共识机制是区块链的灵魂核心，那么对于区块链特别是联盟链及私有链而言，跨链技术就是实现价值互联网的关键，它是把联盟链从分散单独的孤岛中拯救出来的良药，是不同区块链之间拓展和连接的桥梁。

区块链从技术层面而言，是带有时间戳的分布式账本技术；从商业层面而言，则是价值网络。在这个网络中，连接的有效节点越多、越分布，可能产生的价值就会越大。区块链是价值互联网时代的引擎，区块链的应用不应该只局限于单个行业内的联盟之间的价值互联，区块链的发展需要跨链技术，以便对不同区块链进行连接和扩展，构建庞大的价值互联网。

4.3 整合趋势即将呈现，龙头地位越发明显

据区块宝研究院统计，区块链行业年度全球融资交易各轮次投资份额如下表所示：

图表 18：区块链历年历轮投资占比



制图：区块宝研究院

由上表可以比较直观地观察到，自 2012 年以来，区块链行业的天使轮投资份额在近两年呈现出较为明显的下降趋势。早期股权交易份额的稳步下降，一方面表明有相当数量的早年创立的区块链项目已经开始逐步走向成熟；另一方面也表明，区块链行业和其他新兴技术行业一样，正经历着从创造到拥挤，再到整合的演变过程。

据区块宝研究院统计，2013 年至 2014 年间，有 103 家区块链公司获得最初的种子轮或天使投资，但只有 28%的公司在之后继续获得 A 轮及之后轮次的投资。相比其他科技行业，区块链行业获得后续轮次投资的公司占比明显更小。这个现象表明，区块链公司比其他领域的科技初创公司失败的比例更高。基于此，区块宝研究院判断，区块链行业的整合趋势可能会比其他行业来得更快。

《区块链：价值互联时代的引擎》中，区块宝研究院曾指出，每一次时代的变迁，都是机遇的来

临，也会成就伟大的公司。区块链领域的独角兽，也有望随着区块链+应用场景的逐步落地、发展而诞生。根据目前区块链行业内骨干企业和创业公司的发展情况来看，区块链行业内各个细分领域龙头企业的龙头地位将更加明显。

免责声明

本研究报告由区块宝研究院撰写，研究报告中所提供的信息仅供参考。报告根据国际和行业通行的准则，以合法渠道获得这些信息，尽可能保证可靠、准确和完整，但并不保证报告所述信息的准确性和完整性。

本报告不能作为投资研究决策的依据，不能作为道义的、责任的和法律的依据或者凭证，无论是否明示或者暗示。区块宝研究院将随时补充、更正和修订有关信息，但不保证及时发布。对于本报告所提供信息所导致的任何直接的或间接的投资盈亏后果，本公司及研究人员不承担任何责任。

区块宝研究院对于本免责申明条款具有修改权和最终解释权。

参考文献

【1】《中国区块链技术和应用发展白皮书（2016）》，中国区块链技术和产业发展论坛，2016年10月18日

【2】《关于防范代币发行融资风险的公告》，中国人民银行、中央网信办、工业和信息化部、工商总局、银监会、证监会、保监会，2017年9月4日

【3】《合规区块链指引》，国家互联网金融安全技术专家委员会，2017年8月1日

【4】《区块链 参考架构》，中国电子技术标准化研究院，2017年5月16日

【5】《十三五国家信息规划》，国务院，2016年12月15日

【6】《贵阳区块链发展和应用》，贵阳市人民政府，2016年12月31日

【7】《深圳市扶持金融业发展若干措施》，深圳市人民政府，2017年10月9日

【8】袁勇，王飞跃 《区块链技术发展现状与展望》，自动化学报，2016,42（4）：481-494