2017 年度信息技术行业研究

区块链剖析

研究要点

- 通常意义上，我们口中所讲的区块链指代两种意思：一是支持比特币或其他任何问世或未问世的虚拟货币的区块链技术形式；另一是达成区块链最终目的（去中心化、去信任、不可逆等）所代表的技术手段，这个区块链可能是私有的、部分公开的或是完全公开的；

- 区块链的爆发离不开比特币的崛起。纵观区块链的历史，我们可以 2008 年中本聪的《比特币白皮书》作为节点，对区块链从技术积累到被人熟知进行时间划分；

- 2015 年，我国集成电路市场达到 1760 亿美元，涨幅达 3.7%（60 亿美元）；同时，全球集成电路市场经历了 0.9%（20 亿美元）的下滑。此起彼伏致使我国 2015 年集成电路市场占据全球市场的 64%。在过去十年中，我国 IC 需求总共增长了 1290 亿美元，而全球市场仅仅增长了 830 亿美元；

- 区块链的核心是共识机制。共识机制解决了分布式存储和通信中的最大难点，即谁来记账的问题；

- 分布式的无中介性为企业节省成本和时间，并降低了风险。在传统业务网络中，所有参与者都维护着自己的账本，这些账本之间的重复和差异会导致争议、更长的结算时间，而且因为需要中介，还会导致相关的间接管理成本。但是，通过使用区块链，交易在通过共识性验证并写入账本后，就不能再更改，这样企业就能节省时间和成本，同时减少风险；

- 目前我国对区块链如何应用尚不明朗，发布区块链相关公告的 A 股上市公司均处于研究阶段，还未能转化成实际业务和收入。大部分 A 股上市公司主营业务并非区块链，那么区块链的研究主要方向将会是弱中心化甚至私链为主。

基石基金 CORNERSTONE CAPITAL

基石基金投资部

鲁翰

电话：18515474546

电子邮件：lh@bjjsfund.com.cn

相关研究

1.《区块链技术的回顾与展望》-Zaker 数据观

2.《共识-价值互联的不变协议》-毕马威

3.《全球区块链十大应用趋势》-中国信息通信研究院

4.《区块链前瞻之从基础到应用》-中原证券

目录

图表目录

一、区块链的来龙去脉

通常意义上，我们口中所讲的区块链指代两种意思：一是支持比特币或其他任何问世或未问世的虚拟货币的区块链技术形式；另一是达成区块链最终目的（去中心化、去信任、不可逆等）所代表的技术手段，这个区块链可能是私有的、部分公开的或是完全公开的。目前，除了本身作为法币替代品的虚拟货币区块链之外，基于区块链技术的应用始终无法摆脱“数字货币”这一限制，这就涉及到了区块链从结构上设计的难点。本文不对虚拟货币的投资价值进行判断，而是通过对区块链技术本身的发展、目前形势、潜在应用等方面进行研究和阐述。

1.1 区块链历史

区块链的爆发离不开比特币的崛起。纵观区块链的历史，我们可以 2008 年中本聪的《比特币白皮书》作为节点，对区块链从技术积累到被人熟知进行时间划分。

1.1.1 比特币之前的区块链技术积累

1976 年，Bailey W. Diffie、Martin E. Hellman 发表了论文《密码学的新方向》，覆盖了未来一段时间内密码学所有新的进展领域（非对称加密、椭圆曲线算法、哈希等），奠定了整个密码学的发展方向，正式开启了密码学，对区块链的技术的诞生起到决定性作用。1977 年，Ron Rivest、Adi Shamir、Leonard Adleman 三人一起提出 RSA 算法。RSA 算法是一种非对称加密算法，是《密码学的新方向》的自然延续研究

图表 1 1976 年-1998 年关键技术

成果。1980 年，Merkle Ralf 提出了 Merkle-Tree 数据结构和算法。该算法被用于校验分布式网络中数据同步的正确性，也是比特币采用的同步校验方法。值得一提的是，当时哈希算法、分布式网络还尚未出现，作为《密码学的新方向》编写的主要参与者之一，Merkle Ralf 的研究成果具有极高的前瞻性和超前性。1982 年，Lesile Lamport 等人提出拜占庭将军问题，象征分布式记账的可靠性理论和实践进入实质性阶段。同期，David Chaum 提出 Ecash。Ecash 是一种密码学支付系统，是密码学货币的先驱者之一，标志着密码学开始在货币、支付领域展开应用。

1985 年，著名的椭圆曲线加密算法（ECC）由 Neal Koblitz 和 Victor Miller 分别独立提出。相比 RSA 算法，ECC 使用短得多的密钥得到相同的安全性，处理载荷显著减少，从而在公钥密码应用领域的实用性大大提高。1997 年 Adam Back 提出 Hashcash 算法，一开始是主要用于反垃圾邮件。在随后发表的论文里，Hashcash 具体的算法和机制就已经完全涵盖了比特币所使用的 POW 机制了。到了 1998 年，Wei Dai 提出 B-money。B-money 被认为是比特币的精神先驱，甚至之后的以太坊的计量单位都以“Wei”来表示。同一时期，传奇密码学家 Nick Szabo 提出 bitgold 以及一些列密码学、去中心化的货币思路。尽管 Nick Szabo 不会

编程，但是其 bitgold 提纲与 10 年之后中本聪的比特币论文所列出的特性十分接近，让人一度怀疑他就是中本聪本人。而在早些年，Nick Szabo 提出了智能合约的概念，所以他也被称为智能合约之父。可以说，1998 年是密码学货币思想大功告成的一年，只剩相关互联网技术手段出现、发展和完善。

在随后几年时间里，区块链相关的领域又有了几次重大进展：首先是点对点分布式网络，1999 到 2001 的三年时间内，Napster、EDonkey 2000 和 BitTorrent 分别先后出现，奠定了 P2P 网络计算的基础。NSA 于 2001 年发布了 SHA-2 系列算法，其中就包括 SHA-256 算法，即比特币最终采用的哈希算法。总的来看，到了 2001 年，比特币或者区块链技术诞生的所有的技术基础在理论上、实践都被解决了，比特币呼之欲出。

1.1.2 区块链的认知爆发

投资者和企业对于区块链技术的理解与认可、大众对于区块链技术的关注是与比特币的由小众到火爆息息相关的。到 2018 年为止，区块链发展过程可以分为如下四个阶段：

1.1.2.1 技术实验阶段

比特币创始人-中本聪（化名）从 2007 年开始探索用一系列技术创造一种新的货币。2008 年 10 月 31 日中本聪发布了《比特币白皮书》，2009 年 1 月 3 日比特币系统开始运行。比特币体系主要包括分布式账本、非对称加密、哈希函数、POW 机制等技术与概念。这些技术并非中本聪发明，而是被合理应用在其比特币体系里。2007 年到 2009 年底，比特币处在一个极少数人参与的技术实验阶段，相关商业活动还未实质开展。

1.1.2.2 极小众阶段

2010 年 2 月 6 日，第一个比特币交易所诞生了；5 月 22 日有人用 10000 个比特币购买了 2 个披萨。2010 年 7 月 17 日首家比特币交易所 Mt.Gox 成立，这标志着比特币真正进入了市场。这一时期，了解比特币并进入市场中参与比特币交易的主要是互联网技术极客。这批早期活跃者在 Bitcointalk.org 分享技术和经验，在 Mt.Gox 交易比特币，也用自己的私人电脑进行挖矿。此时，矿场并不存在，算力大致平均的分配在各个个人计算机中，去中心化的理念得到了贯彻。在这些互联网技术狂热者中，有一部分人在之后的几年里因为持有比特币而成为了亿万富翁。

1.1.2.3 市场酝酿阶段

2013 年初比特币价格为 13 美元。前半年因为塞浦路斯政府关闭银行和股市，比特币价格飙升至 4 月份的最高 266 美元。下半年一些政府机构，比如德国政府、美国参议院听证会、明确了比特币的合法性和货币地位。因此，11 月 19 日，比特币达到 1242 美元新高。然而，中国银行体系的遏制、Mt.Gox 的倒闭触发了比特币的一波大熊市，价格暴跌至 200 美元以下。原先飙升的价格包含了过于乐观的预期，于是当出现范围较广的负面信息时，比特币市场直面了一次洗牌，许多企业倒闭。不过活下来的企业实力却因此变得更强。对于大众来说，比特币和区块链开始逐渐进入视野，尽管大部分人不愿意或者没能力理解。此时的比特币还远远没有被普遍认同。

1.1.2.4 主流阶段

2016 年全球发生了几件黑天鹅事件。6 月 23 日英国公投宣布脱欧，9 月朝鲜第五次核试验，11 月 9 日特朗普当选美国总统等事件，让世界经济处于不稳定状态。比特币的法币替代能力使其成为了一种新型的 safe heaven，即避险货币。比特币的市场开始复苏，交易规模快速扩大。尽管中国市场仍严厉遏制，但日本、韩国、拉美等市场快速升温，开启了 2016-2017 年的大牛市，价格从 16 年初的 400 美元上升到 2017 年

底的 20000 美元。如此高速的增长造成了比特币网络拥堵，而后者又带动了其他虚拟货币以及各种区块链应用的大爆发。2017 年第四季度芝加哥商品交易所上限比特币期货交易使得比特币正式进入主流投资品行列。

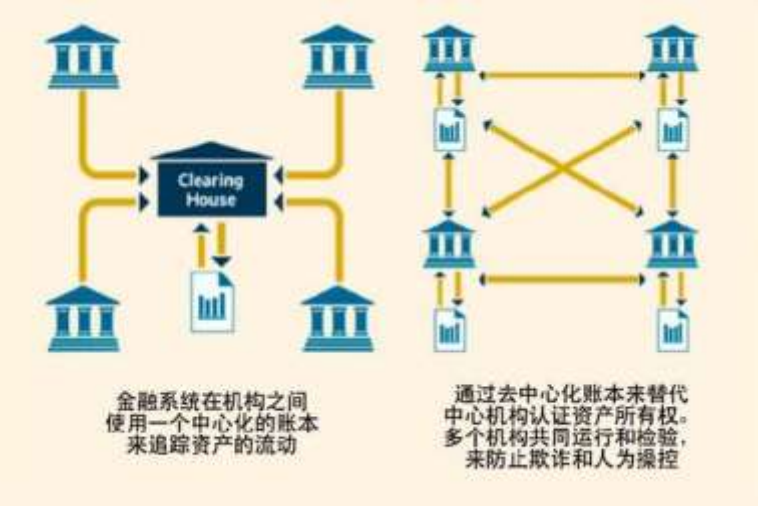
1.2 区块链的特点

需要说明的是，区块链本身是一系列技术的集合，而不是一个特定的技术或者产品，所以用区块链的特点来描述并不恰当，准确的说应该是运用区块链所能带来的优势。

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式，也有很多人也把它定义为分布式记账的一种技术。区块链之所以受到如此热捧，因为其有如下几个**优点：**

1.2.1 去中心化

分布式存储数据库早已出现，但是使用区块链技术就再也无需管理员、中心服务器、中心。以金融领域为例，所有的汇款、支付等都要通过相应的人民银行系统或者其他支付和清算中心，而运用区块链，没有这样的支付和清算中心也能够安全的实现。



图表 2 中心化清算和去中心化

1.2.2 开放性

区块链体系是开放的，除了交易各方的私有信息被加密外，区块链的数据对其他所有使用者公开：任何使用者都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。区块链体系是开放的，除了交易各方的私有信息被加密外，区块链的数据对其他所有使用者公开：任何使用者都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

1.2.3 去信任（自治性）

区块链采用基于协商一致的规范和协议使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对人的信任改成了对机器的信任，即在规范和协议的限定下通过计算机自动完成，人无法干预。

1.2.4 信息不可篡改（不可逆）

一旦信息经过验证并添加至区块链，就会永久的存储起来。同时，后一区块链的某些信息、数据是根据前一区块而来，除非能够同时掌握算力网中超过 50%的算力，否则对数据库的修改是无效的。而掌握区块链算力网中 50%以上的算力在现实中几乎不可能实现，因此区块链的数据稳定性和可靠性极高。

1.2.5 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(区块链中的程序规则会自行判断活动是否有效)，因此交易对手无须通过公开身份的方式让对方自己产生信任。

区块链将人与人之间的信任问题以一种开放、不可逆、去中心的方式解决了。然而，区块链在近年来的发展过程当中也暴露了许多**缺陷**：

1.2.6 安全性

区块链技术一大特点就是不可逆、不可伪造，但前提是私钥是安全的。私钥是用户生成并保管的，没有第三方参与。私钥一旦丢失，便无法对账户的资产做任何操作。随着量子计算机等新计算技术的发展，未来非对称加密算法具有一定的破解可能性，这也是区块链技术面临的潜在安全威胁。

1.2.7 数据确认延迟

在金融区块链中，数据确认的时间相对较长。拿比特币举例，当前产生的交易有效性受网络传输影响，比特币交易每次的确实时间大约 10 分钟，6 次确认的话需要一个小时。因此区块链的交易数据是有延迟性的。

1.2.8 监管

区块链的去中心、自治化的特点淡化了国家监管的概念。然而所有的创新，都需要符合监管的要求。区块链的监管，在某种程序上是促进区块链的商业应用，更好的提供合规性保护。另一方面监管部门对这项新技术的法律和制度建立上存在滞后，也可能会毁掉区块链，需要把握好尺度。

1.2.9 能源浪费

以比特币为例，比特币的共识机制决定他存在的价值就是比特币价格高于挖矿所消耗的电能，否则就不会有人去参与挖矿，也就不会有人去记账。在比特币产生初期，挖矿的人数较少，比特币价格也低，但是很容易得到；而在大量算力转移到比特币挖矿的现在，挖矿难度根据比特币内置的难度调整而变得极大，耗费大约 3000 到 7000 美元电费才能得到一个比特币。但是由于参与者众多，也就将比特币价格抬到 1 万美元以上，因而比特币就是“有价值”的。

图表 3 天嘉网络的芭蕉溪水电站“矿场”

摩根士丹利在近期发布的一份研究报告中估计，2017 年比特币的挖矿业务共消耗了 36 太瓦时的能源，这与卡塔尔一年的能源消耗量相当。报告指出，2018 年比特币的电力需求量将增至三倍以上，耗电量可能会超过 125 太瓦时，这与阿根廷整个国家一年的能源消耗量相同。

1.3 区块链技术解析

1.3.1 区块链的区块、链和 Hash

区块链（BlockChain），顾名思义是一个个块（Block）形成的链（Chain）。每次写入数据，就创造一个区块，区块中有表头和内容，区块头（head）：记录当期区块的元信息，即连接信息。区块体（Body）：记录实际数据（Data）。具体如下：

字段名	含义	大小(字节)
Version	版本号	4
hashPrevBlock	上一个block hash值	32
hashMerkleRoot	上一个block产生之后至新block生成此时间内，交易数据打包形成的Hash	32
Time	Unix时间戳	4
Bits	目标值，即难度	4
Nonce	随机数	4

图表 4 字段名及其含义

- Version，版本号，很少变动，一般用于软件全网升级时做标识
- hashPrevBlock，前向 Block Hash 值，该字段强制多个 Block 之间形成链接

- hashMerkleRoot，交易 Hash 树的根节点 Hash 值，起校验作用，保障 Block 在网络传输过程中的数据一致性，有新交易加入即发生变化
- Time，Unix 时间戳，每秒自增一，标记 Block 的生成时间，同时为 block hash 探寻引入一个频繁的变动因子
- Bits，可以推算出难度值，用于验证 block hash 难度是否达标
- Nonce，随机数，在上面数个字段都固定的情况下，不停地更换随机数来探寻

所谓 Hash，即哈希函数。计算机利用哈希函数，可以对任意内容，映射出或者简单说计算出一个长度相同的特征值，实现索引和对应的功能。区块链的 Hash 长度是 256 位，这就是说，不管原始内容是什么，最后都会计算出一个 256 位的二进制数字。而且可以保证，只要原始内容不同，对应的 Hash 一定是不同的。

区块头里面内容包含当前时间、上一个区块的 Hash、此区块的 Hash 等信息。在区块头里面包含了上个区块的 Hash，以此来连接区块，每个区块都连接上一个区块，因而得名“区块链”。这意味着如果当期区块的内容变了，或上一个区块的内容变化了，一定会使当前区块的 Hash 变化，如果有人修改了一个区块，该区块 Hash 变化，那么相应的就必须修改后面所有的区块，否则就是无效的。只有当某人或者某组织的算力大于剩余其他全部算力总和，即占大于全网 50%的算力时，才可以篡改信息。这种联动性保证了区块链的可靠性。

1.3.2 区块链的核心-共识机制

区块链的核心是共识机制。共识机制解决了分布式存储和通信中的最大问题：谁来记账？ 计算机算法里面著名的拜占庭容错问题（BFT），说的是拜占庭罗马帝国在军事行动中，采取将军投票的策略来决定是进攻还是撤退。每一个将军离其他将军的距离很远，必须得通过书信的方式进行交流。但是军队中如果有叛徒或者奸细，如何保证投票的结果真正反映了忠诚的将军的意愿？拜占庭将军问题反映到信息交换领域中来，可以理解为在一个去中心的系统中，有一些节点向外界广播错误的信息或者不广播信息，在这种情况下如何验证数据传输的准确性。

图表 5 毕马威区块链研究

目前比较流行的五种共识机制：

- Proof of Work（POW）工作量证明：比特币在 Block 的生成过程中使用了 POW 机制，一个符合要求的 Block Hash 由 N 个前导零构成，零的个数取决于网络的难度值。要得到合理的 Block Hash 需

要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的 Block Hash 值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理 hash 是一个概率事件。当节点拥有占全网 n%的算力时，该节点即有 n/100 的概率找到 Block Hash。

- Proof of Stake(POS)股权证明：类似于财产储存在银行，这种模式会根据用户持有数字货币的量和时间来分配相应的利息。 在股权证明 POS 模式下，有一个名词叫币龄，每个币每天产生 1 币龄，比如某人持有 1000 个币，总共持有了 10 天，那么此时币龄就为 10000。如果持有者发现了一个 POS 区块，币龄就会被清空为 0。每被清空 365 币龄，持有者将会从区块中获得 0.05 个币的利息（假定利息为年利率 5%），那么在这个案例中，利息=10000*5%/365=1.37 个币。
- Delegated Proof of Stake（DPOS）委任权益证明：原理是让每一个持股的人进行投票，由此产生 101 位代表，我们可以将其理解为 101 个超级节点或者矿池，而这 101 个超级节点彼此的权利是完全相等的。如果代表不能在轮到他们时生成区块的责任，他们会被除名，网络会选出新的超级节点来取代他们。DPOS 的出现最主要还是因为矿机的产生，大量的算力在不了解也不关心比特币的人身上。DPOS 缩小参与共识节点数量，大幅缩短共识时间，达到秒级共识验证
- Practical Byzantine Fault Tolerance（PBFT）实用拜占庭容错算法：PBFT 是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。PBFT 可以最小延迟处理大量的直接点对点（或分布式）信息。这意味着程序员可建立安全和适应性强的私人分布式网络。
- Pool 验证池：基于传统的分布式一致性技术，加上数据验证机制；是目前行业链大范围在使用的共识机制。在分布式一致性算法基础上实现秒级共识。不需要代币也可以工作，没有因为代币存在而导致的一系列社会问题。不过去中心化程度不及比特币。

1.3.3 新区块生成过程

下面以比特币为例，描述新区块是如何生成的：

1. 节点监听全网交易，通过验证的交易进入节点的内存池(Tx Mem Pool)，并更新交易数据的 Merkle Hash 值；
2. 更新时间戳；
3. 尝试不同的随机数(Nonce)，进行 hash 计算；
4. 重复该过程至找到合理的 hash；
5. 打包 block：先装入 block meta 信息，然后是交易数据；
6. 对外部广播出新 block；
7. 其他节点验证通过后，链接至 Block Chain，主链高度加一，然后切换至新 block 后面挖矿。

大约每 10 分钟，比特币会生成一个新的区块。

1.3.4 区块链的类别

区块链因其应用场景不同，导致共识机制也有变化，进而使得不同场景下的区块链有很大区别。目前，区块链大致可以分为三类：公有链、联盟链、私有链。

1.3.4.1 公有链

以比特币为代表的虚拟货币都是公有链。

公共区块链是指全世界任何人都可读取的、发送交易且交易能获得有效确认的、都能参与其中共识过程

的区块链。作为中心化或者准中心化信任的替代物，公共区块链的安全由“加密数字经济”维护——“加密数字经济”采取 POW、POS 或 POW+POS 等方式，将**经济奖励**和加密数字验证结合了起来，并遵循着一般原则：**每个人从中可获得的经济奖励**，与对共识过程作出的贡献成正比。这些区块链通常被认为是“完全去中心化”的。

1.3.4.2 联盟链

以 IBM 的 Hyperledger（超级账本）、R3 等为代表。

联盟区块链是指共识过程中的节点是预先选择好的一类区块链，即采取 DPOS 或者 PBFT 机制。假设有一个 10 个政府组织组成的团体，这其中每一个政府组织都拥有一个内部的节点。根据不同的确认原则，比如（2/3）确认，来落实新区快的生成。联盟链的内部性导致其写入权只能局限在这些预先确定的节点，即新区块的生成完全有这些节点掌控。但是读取端未必只受限于此团体，可以延伸到全世界任何人。这就表明联盟链只能达到部分去中心化，或者说是弱中心化。

1.3.4.3 私有链

数据库管理、审计等应用场景下可能会使用私有链。

私有链是指写入权完全掌握在某个单节点，而读写权既可对外开放也可不开放（或受限）的区块链。私有链属于完全中心化的区块链。目前尚未看出有任何意义，因为私有链能做的事情，传统数据库都可以做到。很多区块链项目和公司自称使用的是区块链，但实际上并无太大价值。

1.3.5 目前区块链的设计局限

共识机制的选择决定了区块链的性能。事实上，一个区块链不管采用哪种共识机制，都无法同时满足能效、安全和去中心化这三点。基于 POS 和 POW 的共识机制可以满足去中心化和安全的需求，但效率极低。以比特币为例，比特币只支持每秒 7 笔交易，同时能耗极高。DPOS 属于弱中心化机制，基于多数投票或者说多数“股权” 就可以达成共识；在联盟链中用的较多的 PBFT 同样也只是节点间的公平，达不到完全的去中心化，但是效率和安全性有所保障。而完全以 P2P 传输的项目而言，中心化不成问题，但是为了达到高效，必须在安全性上有所取舍。

“能效-公平-安全”是目前区块链的不可能三角。公有链的公平程度最高，安全性较强但能效最差，这种形式在主要的商业模式中是无法应用的；联盟链去中心化能力一般，但能效率有大的提升；而私有链完全是中心化数据库。

然而区块链本身是一种集合众多已有技术的模式创新。虚拟货币的出现，其实是对于记账问题的一种妥协。因为如果没有虚拟货币，人们也就没有动力去记账。而在不需要人们记账的环境下，往往是中心化的机构来代劳。在未来，也许我们可以看到新的区块链共识机制、新的技术、亦或是两者的结合来克服区块链的不可能三角，达到这项技术的完全体状态。

二、区块链技术的应用

比特币和其他加密货币在 2017 年“大放异彩”之后，2018 年大家的注意力开始转向了支撑这些虚拟货币的基础技术-区块链。市场普遍看好区块链在各产业的应用，因为区块链绝不仅仅只是比特币的燃料，“区块链+”的时代是可以预见到的。

分布式的无中介性为企业节省成本和时间，并降低了风险。在传统业务网络中，所有参与者都维护着自

己的账本，这些账本之间的重复和差异会导致争议、更长的结算时间，而且因为需要中介，还会导致相关的间接管理成本。但是，通过使用区块链，交易在通过共识性验证并写入账本后，就不能再更改，这样企业就能节省时间和成本，同时减少风险。

分布式账本的统一性减少了错误。区块链共识机制提供了经过整合的、一致的数据集的优势，减少了错误，拥有近实时的引用数据，而且参与者能够灵活更改其拥有的资产的描述。

去中心化使信息可信度和完整性更高。因为没有参与成员拥有共享账本中所含信息的来源，所以区块链技术会提高参与成员之间的交易信息流中的可信度和完整性。

区块链的不可逆性降低了审计和合规性成本，增加了透明性。而且在使用区块链技术的业务网络上，合约得以智能、自动化执行并最终确认，所以企业会获得更高的执行速度、更低的成本和更少的风险，所有这些使企业能构建新收入流来与客户交互。

图表 6 区块链催生多元化应用

如果说比特币等加密数字货币代表的是区块链 1.0，以太坊的区块链基础设施和智能合约功能是区块链 2.0 的话，那么抛开技术不谈，思维方式的转变将会是影响接下来区块链发展的绝对因素。如何组合各种已有技术，将去中心化等大家需要的特性融入到或取代目前已有模式，这是区块链进化的核心问题，也是区块链的精神所在。

2.1 区块链技术在金融领域的应用

- **国际支付：**区块链在国际支付和汇款领域会有较大作用。Banco Santander 银行对区块链在支付领域的潜力非常感兴趣。这是因为作为一家大型商业银行，Santander 拥有众多零售客户，这些客户将从更加高效、更加便宜的付款中受益，这在国际转账领域尤其明显。这是因为银行手动结算交易的成本明显高于使用区块链的成本。尽管区块链目前还未实际应用到国际支付和汇款，但是相关从业人员大都对此持积极看法。
- **资本市场：**Santander 银行同样认为资本市场也可以因为区块链的普及而受益。然而，这些解决方案比支付领域的解决方案复杂得多，所以距离区块链在资本市场的应用还有一段相对更长的路要去探索。瑞士信贷也开始在资本市场和企业金融方面寻求使用区块链的机会。目前已经有很多资本开始流入这个应用方向，比如 Axoni，一家纽约的初创企业，在 2016 年底就获得了高盛和摩根大通的 1800 万美元 A

轮融资。

- **贸易金融：**2016 年 9 月，巴克莱银行与现场客户进行了首次基于区块链的贸易金融交易。该笔交易使用的是巴克莱银行与以色列 Fintech Wave 合作开发的系统。巴克莱银行在该笔交易中，根据买方的请求，用区块链开出了一张给卖方的信用证。使用信用证完成贸易金融通常比较费事，还需要纸质文件支撑。相同的交易通常需要一周的时间才能完成，但是巴克莱银行的系统能够在 4 个小时内完成交易。

  区块链对于贸易金融来说是一件值得期待的技术。全球贸易金融总量大约为 10 万亿美元。传统处理贸易金融的方式非常缓慢，甚至会导致企业中断业务，或是使企业无法掌控自身现金流动性，可以说是已然成为了痛点。巴克莱银行的这次成功的交易，展示了区块链是如何简化贸易金融交易，也提供了一个绝佳的技术服务于金融的案例。
- **合规与审计：**区块链的安全性使其可以完美融入会计和审计工作。它可以使工作过程中错误发生的概率显著降低，也可以确保记录的完成性，因为一旦区块被建立，就算是区块链所有者也无法进行任何修改。不过，区块链有可能会改变整个审计行业的生态-会计、审计有可能会被完全取代。
- **反洗钱：**区块链可以有效地打击洗钱活动。每一笔交易对象都会被永久记录。
- **保险：**对于保险领域的应用最大可能性是通过智能合约来达成的。以区块链技术为基础的智能合约能够保证客户与保险公司之间的索赔透明且安全。所有合同和索赔都可以在区块链上记录并通过网络进行验证，从而消除无效索赔。比如，区块链不会承认同一起事故中的多重索赔。
- **P2P 交易：**P2P 交易目前是有一定局限性的。比如，有些交易根据地理位置限制交易，另一些会收取一定的手续费。大多数 P2P 的安全性十分脆弱，这也使得很多想要使用 P2P 交易的潜在用户望而却步。区块链是有可能解决这些问题的。

2.2 区块链技术在商业领域的应用

- **2.2.1 供应链管理：**区块链的不可逆性同样非常适合追踪货物在供应链里的流转。美国初创企业 Skuchain 和 Factom 已经开始提供基于区块链技术的供应链管理解决方案。
- **2.2.2 卫生保健：**在卫生保健领域里，挑选何种健康数据适合使用区块链来记录是非常重要的。适合的数据包括一般信息，比如年龄、性别，也可能包括基本病史、免疫史或者生命体征等不能识别特定病人的信息。这是因为这些数据，在未来实际应用中，很可能会被保存在公链里，而公链里所有的信息都可以被任何人读取。如果使用可以识别特定病人的数据，可能会引起隐私问题。

  我们处在一个专业的互联医疗设备变得越来越普遍，并且越来越与人的健康记录相关联的时代。区块链可以将这些设备生成的数据保存在卫生保健区块链中，在人们需要使用这些信息的时候，准确、无误地传达给医务人员。区块链正是链接这些孤岛的绝佳方案。
- **2.2.3 房地产：**在发达国家，普通人平均每 5-7 年就会出售一套房子，一生当中会搬家 12 此左右。作为一种中短期的、涉及到大量信息交换、大额的交易活动，房屋买卖对区块链将会有较大的需求。区块链技术的应用会通过快速确认财务状况、无欺诈确认房屋信息等特性高效安全地利好房地产行业。
- **2.2.4 传媒：**媒体公司已经开始采用区块链技术。7 月，区块链内容分发平台 Decent 宣布推出 Publiq，允许作家和其他内容创作者通过区块链传播作品并取得即时付款。Comcast（康卡斯特）的高级广告组开发出一项基于区块链的新技术，允许公司通过广播和 OTT 电视购买广告。
- **2.2.5 能源：**据 PWC 称，区块链不仅可用于能源供应方面的交易，更可以进一步服务于能源计量、计费和清算流程。其他潜在应用包括记录所有权、资产管理、原产地保证、排放配额和可再生能源证书等。

2.3 区块链技术在政府的应用

- **2.3.1 记录/档案管理：**几乎在世界任何地方，政府机构都要维护个人档案或记录。管理这些数据

是一件比较困难的事情，尤其目前还有很多档案是以纸质形式存在的。通常，民众需要亲自前往当地政府办公室更改他们的记录，而这个过程其实是费时且不必要的。利用区块链可以更有效率更安全的替代现有流程。

- **2.3.2 身份认证管理：**通过区块链上的足够信息，人们只需提供最低限度（例如出生日期）就足以证明其身份。
- **2.3.3 选举：**投票的公平公正透明是民主社会最重要的组成部分。而区块链可以保证每个有访问权限的节点绝对公平，投票的过程不可更改，不会被破解，每个选票都可追溯其来源。如果选票丢失、正在运输或被修改，选民可以在选举结束之前就发现并维护他们的权力。
- **2.3.4 税收：**报税是一件流程繁琐并且容易出现人为错误的工作。区块链技术可以使其变得更加高效。
- **2.3.5 非盈利组织：**最近的民意调查显示，公众对慈善组织的信任度处于历史最低水平。 但是区块链可以通过向捐助者表明慈善组织实际上是按照预期使用他们的资金的。此外，区块链技术可以帮助这些非营利组织更高效地分配这些资金，更好地管理资源，并提高其跟踪能力。
- **2.3.6 法律/标准/监督：**今年早些时候，爱尔兰基金，德勤，北方信托和华尔街就一个项目进行了合作，试验区块链如何通过他们所谓的“RegChain”来加强监管报告。他们证明区块链可以识别交易，通过智能合约功能管理报告，并增强合规性。根据该试验的结果，使用区块链提高了过程的透明度和数据存储的安全性。

2.4 区块链技术在其他领域的应用

- 2.4.1 财务管理/会计：如果企业使用区块链来进行财务管理工作，那么对于监管机构来说，就无需再为企业做假账等问题烦恼。
- 2.4.2 股东选举：纳斯达克在 2016 年进行了一次试验，其与区块链初创公司 Chain 合作开发了一个数字资产显示投票权的系统。该系统使用的区块链是以传统方式记录 CSD 报告的证券所有权，并根据这些证券所有权的持有量，为每个股分配布投票权代币。如果用户拥有投票权代币，那么他们可以用代币在每一个会议议程中参与投票。
- 2.4.3 信息安全：区块链在网络安全方面的最大优势是消除了单点故障的风险。区块链技术还提供端到端的加密和隐私。
- 2.4.4 大数据：网络上每台计算机都在不断验证存储在其上的信息。这个现状，加上区块链的不可变性，使区块链成为存储大数据的绝佳工具。
- 2.4.5 数据存储：大数据的相同原则也适用于数据存储。
- 2.4.6 物联网：区块链有望改变多个物联网领域的做法，其中包括：
  供应链：跟踪货物运输的位置，并确保它们保持在指定的条件下；
  资产跟踪：监控资产和机器，记录它们的活动，作为云解决方案的替代选择；
  医疗保健：通过多种权限，允许众多利益相关者之间记录和共享医疗数据。

三、区块链技术现状

3.1 国际

3.1.1 监管

3.1.1.1 欧美

美国虽然没有关于数字货币的统一监管法规，而且各州之间有差异，但对数字货币和 ICO 都有各种监管文件和具体措施。美国金融犯罪执法网络(FinCEN)、美国国税局(IRS)、美国商品期货交易委员会(CFTC)、美国金融消费者保护局(CFBP)、美国司法部(DOJ)等都对数字货币的界定、应用以及犯罪预防、消费者权益保护等发布了相关报告和指引。其中，纽约州金融服务局(NYSDFS)更是率先对数字货币的业务监管建立了规范框架。美国将比特币界定为一类特殊的虚拟货币，将从事比特币交易的平台、支付中介等视为资金传递者(money transmitter)纳入监管范畴。围绕“资金传递者”这一核心，从市场准入、资金转移、反洗钱以及消费者权益保护等方面实施监管。

时间	态度
2014.03	美国 IRS（Internal Revenue Service）国税局在税务系统中将这种虚拟货币视作资产，适用股票和易货交易的相关规定，而不会将其认定为货币。
2017.04	俄罗斯财政副部长表示 2018 年俄罗斯可能会承认包括比特币在内的加密数字货币。
2017.04	华盛顿州规定数字货币交易所需要申请牌照，同时要求独立第三方审核。
2017.07	美国 SEC 表示 ICO 受到联邦证券法的管制。
2017.09	美国 SEC 成立专注于区块链技术的网络部门，希望加强对网络安全和散户投资者的保护。
2018.01	包括法国经济部长、德国央行、英国首相在内的欧洲国家呼吁采取更大的加密货币政策。预计具体的政策有可能在今年春天会公布。
2018.02	美国禁止信用卡进行数字货币兑换。
2018.03	英国央行行长表示应该对数字货币交易所实施更严格的规定。
2018.03	美国 SEC 证券交易委员会对多家在区块链/加密货币领域开展业务的创业企业展开调查
2018.03	美国 SEC 证券交易委员会发表声明《关于潜在的非法数字资产交易平台》

美国 SEC 近期多项措施，监管问询从事区块链的公司，对数字货币交易所的未审核和注册风险进行提示。3 月 7 号 SEC 的声明写到依照联邦法律的标准，数字资产属于证券范畴，因此交易平台必须在 SEC 注册或获得注册豁免。许多平台自称“交易所”，可能会误导投资者，认为他们受到监管或符合国家证券交易所的监管标准。实际上，SEC 并未审查过这些平台上提供的数字资产和交易协议，平台所谓的标准也不等同于国家证券交易所的标准，因此投资者在交易之前应谨慎考虑。现有的数货币交易平台都未经 SEC 审核过。SEC 的声明只是相当于风险提示，但也预示着之后对数字货币交易所的监管将要到来。

欧洲各国对数字货币的态度都相对友好，但也在探索监管的道路上并有严加监管的趋势。监管的态度主要集中在数字货币交易和 ICO 的无序性上，各国央行行长和财长基本都有表示加强监管的意图。

3.1.1.2 日韩

时间	态度
2016.03	日本内阁通过投票将比特币和数字货币均视为数字等价货币。

2017.04	日本实施了《支付服务法案》，正式承认比特币是一种合法的支付方式，对于数字资产交易所提出了明确的监管要求。
2017.07	日本新版消费税正式生效，比特币交易将不再需要缴纳 8%的消费税。
2017.09	韩国金融服务委员会 FSC 宣布将如何对数字货币，比如比特币，以太币进行监管。韩国加大监管力度，对于洗钱非法融资和其他数字货币非法交易进行调查。
2017.09	日本金融厅（FSA）发布了首批得到许可的日本“虚拟货币交易所”名单。首批获得牌照的日本境内虚拟货币交易所包括 Bitflyer、Zaif、BTCBOX、GMO、QUOINEX、BitBank、Bitpoint 等在内的 11 家交易所，这是全球范围内首批正式获得政府批准的虚拟货币交易所。
2018.01	韩国税务局突击检查韩国第二大比特币交易所 Coin 呢，要求交易所披露文件和加密货币交易信息。
2018.01	韩国政府宣布将对数字货币交易所征收 22%的企业税以及 2.2%的地方所得税。
2018.01	韩国政府规定从 1 月 30 日起，在数字货币交易中禁止使用匿名银行账户。

韩国对于比特币的监管比较严格。相对而言，日本的监管态度好得多，没有太过限制数字货币的发展。日本政府也是首个认可数字货币交易所的政府，日本政府认可后的监管主要在保护客户账户安全、反洗钱上和对交易所进行合规性审查。具体有：

第一：分离客户账户。首先，交易平台用户资产和平台资产要分开记账，分别管理。

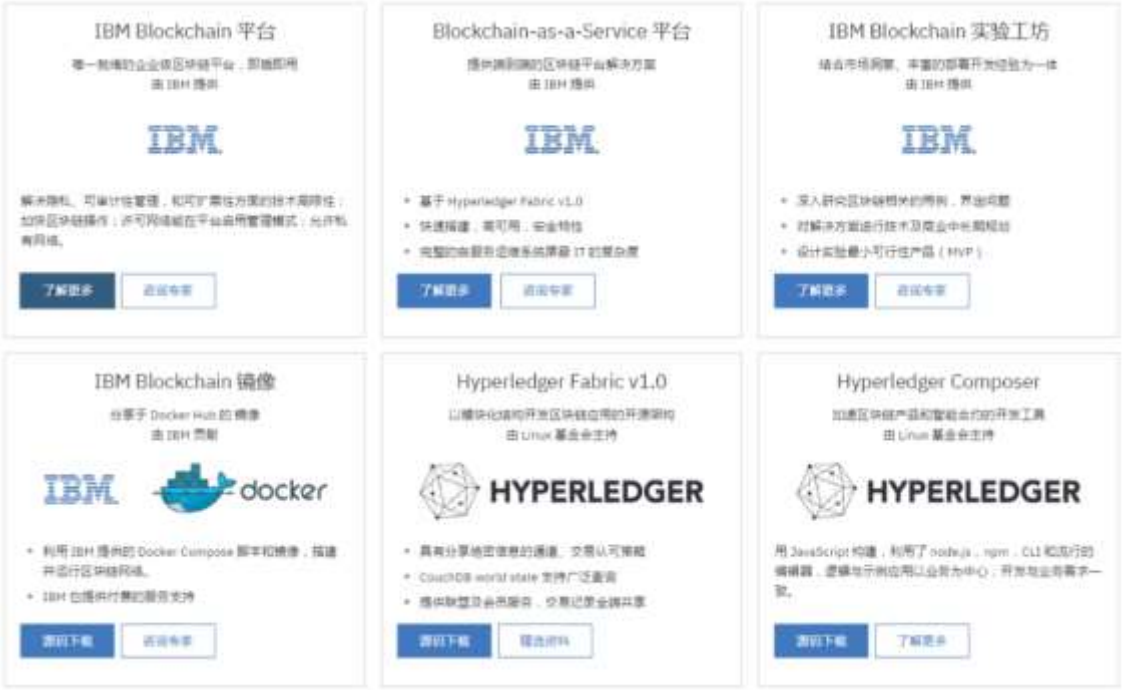
第二：反洗钱。每个交易所被要求必须进行严格的 KYC，各国用户需要提供能代表身份的信息。常规身份认证结束之后，交易所会给用户寄出一封信，核实用户现居住地址。用户只有确认本人收到信件之后才能通过认证开始交易，如果信件非本人签收，或者被返退回至交易所，用户的账户将一直处于冻结状态。

第三：系统安全管理。日本金融厅 FSA 需要对这些交易所的内部系统进行评估，评判其保护客户资产的能力，必要时会进行现场视察。在政府的一系列“有形的手”的监管之下，如今的日本比特币交易量，不仅超过中国跃居世界首位，在最高时还接近了全球交易总额的一半。

3.1.2 国外实际应用

3.1.2.1 IBM 区块链平台

IBM 在区块链技术上有 27 项专利，并开发了众多区块链在不同领域的解决方案，联合沃尔玛将供应链透明，使食品安全科追溯；跟中国邮储银行合作基于区块链的资产托管计划；为 Everledger 钻石公司提供“开放账本”抑制黑市行为和欺诈交易等等。



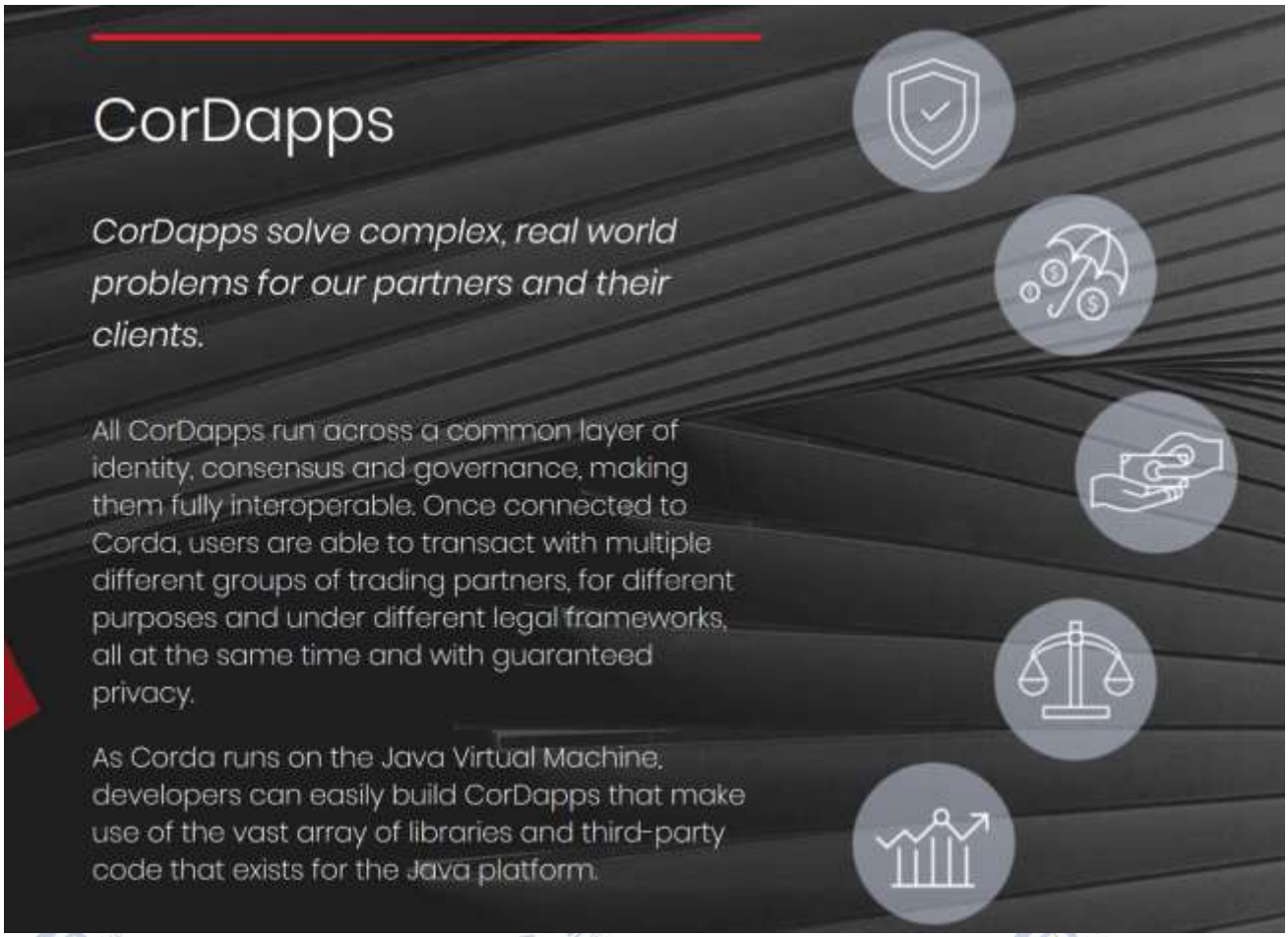
图表 7 IBM 区块链应用-IBM 官网

3.1.2.2 Hyperledger（超级账本）

Hyperledger 是 Linux 基金会主办的一个全球合作项目，参与者包括金融、银行、物联网、供应链、制造和技术领域的领导者。130 多名成员和 8 个正在实施的项目（包括 Hyperledger Fabric 和 Hyperledger Composer）携手合作，旨在创造一个开放、标准化、企业级的分布式账本架构和代码库。它采用模块化架构，使共识服务和成员服务等组件可以即插即用，保证了商业区块链解决方案的机密性、灾备能力、灵活性和可扩展性。在中国，IBM 已经与中国银联和邮储银行进行了合作。

3.1.2.3 R3 联盟

R3CEV 是一家总部位于纽约的区块链创业公司，由其发起的 R3 区块链联盟，至今已吸引了 100 家巨头银行的参与，其中包括富国银行、美国银行、纽约梅隆银行、花旗银行、德国商业银行、德意志银行、汇丰银行、三菱 UFJ 金融集团、摩根士丹利、澳大利亚国民银行、加拿大皇家银行、瑞典北欧斯安银行（SEB）、法国兴业银行等。国内平安银行也早早加入了联盟。R3 开发专门用于金融机构的分布式记账凭证的 Corda。官网显示 R3 在九个国家有超过 2000 名技术人员、金融和法律的专家，并在近期完成 A 轮 1.07 亿美元融资。



图表 8 Cordapps-R3 官网

然而，最近包括高盛在内的 R3 成员不断退出，同时 R3 也宣布放弃区块链，认为区块链不适合其 Corda 平台。R3 董事董事 Clemens Wan 表示，R3 已经从“区块链初创公司”转变为“受区块链启发的初创公司”了。R3 的研究方向是私有链，而如上文所讲，私有链其实和加密数据库并没有太大区别。

3.1.2.4 Ripple（瑞波）

Ripple 是一个开放的支付网络，主要用于货币兑换和汇款；网络内使用的 XRP 币（瑞波 币）是一种 Ripple 内的原生货币。Ripple 网关是 Ripple 网络的重要组成部分，是通过 Ripple 网络交易的关键所在。

Ripple 基于分布式数据库（公开的），可实现即时清算，成本低廉。传统系统要 3-5 天的处理，Ripple 只需 4 秒。Ripple 共识机制要求 UNL 子网（不是整个系统）中 80%的绝对多数节点同意验证某项交易。这意味着交易可在数秒内发生，不像工作量证明（Pow）系统需花上 10 分钟或更长时间。

图表 9 Ripple 支付优势-Ripple 官网

3.2 国内

3.2.1 政策

3.2.1.1 国家层面

目前国务院、工信部针对区块链的推动政策如下：

时间	政策
2016 年 10 月	工业和信息化部发布《中国区块链技术和应用发展白皮书(2016)》，总结了国内外区块链发展现状和典型应用场景，介绍了国内区块链技术发展路线图以及未来区块链技术标准化方向和进程。
2016 年 12 月	“区块链”首次被作为战略性前沿技术写入《国务院关于印发“十三五”国家信息化规划的通知》。
2017 年 1 月	工信部发布《软件和信息技术服务业发展规划(2016-2020 年)》，提出区块链等领域创新达到国际先进水平等要求。
2017 年 5 月	工信部发布《区块链参考架构》。《区块链参考架构》是区块链领域重要的基础性标准，对推进国内区块链应用具有重要作用。通过对区块链的用户视图和功能视图的阐述，对区块链的主要参与者和核心功能组件进行了详细规定，系统描述了区块链的生态系统，帮助业界建立对区块链的共识，对各行业选择、开发和应用区块链具有重要的指导和参考价值。
2017 年 8 月	国务院发布《关于进一步扩大和升级信息消费持续释放内需潜力的指导意见》提出开展基于区块链、人工智能等新技术的试点应用。
2017 年 10 月	国务院发布《关于积极推进供应链创新与应用的指导意见》提出要研究利用区块链、人工智能等新兴技术，建立基于供应链的信用评价机制。
2018 年 3 月	工信部发布《2018 年信息化和软件服务业标准化工作要点》，提出推动组建全国信息化

	和工业化融合管理标准化技术委员会、全国区块链和分布式记账技术标准化委员会。

我国就区块链发展和应用问题，在政策层面持积极态度。但是，基于我国国情，区块链，尤其是公链，不可能采取完全去中心化模式，弱中心化区块链必然是未来我国主要应用模式。在弱中心化的大前提下，区块链因为目前已经可以在不使用数字货币、用目前已有的共识机制开始试验、应用，所以我国对去数字货币公链的研究大概率会减缓，甚至抛弃这个方向，并在此方向上与外国持续拉开差距。不过，政府在弱中心化中的出现，也许在许多领域会提高弱中心化的公信力（相比选择其他组织、企业作为编写节点），使弱中心化区块链加速落地。

3.2.1.2 地方层面

就各地区而言，我国地方性区块链政策推动力度不一。主要地区和推进力度较大的地区如下：

地区	总体态度	时间	相关推进
北京	虽然未出台针对区块链产业发展的专项政策，但一直保持高速发展状态。	2016 年 8 月	北京市金融工作局发布了《北京市金融工作局 2016 年度绩效任务》，为推进北京市金融发展环境建设，推动设立了中关村区块链联盟。
		2016 年 12 月	北京市金融工作局与北京市发展和改革委员会联合下发《北京市“十三五”时期金融业发展规划》的通知，将区块链归为互联网金融的一项技术，鼓励发展。
		2017 年 4 月	北京市发布首个对区块链企业予以资金支持的政策《中关村国家自主创新示范区促进科技金融深度融合创新发展支持资金管理办法》。开展人工智能、区块链、量化投资、智能金融等前沿技术示范应用，按照签署的技术应用合同或采购协议金额的 30%给予企业资金支持，单个项目最高支持金额不超过 500 万元。
		2017 年 9 月	由北京市金融工作局、北京市发展和改革委员会、北京市财政局、北京市环境保护局等联合下发《关于构建首都绿色金融体系的实施办法的通知》再次提到区块链，发展基于区块链的绿色金融信息基础设施，提高绿色金融项目安全保障水平。
上海	在区块链政策上相对保守，只在金融区块链试点上出台多项指导政策。	2017 年 3 月	上海市宝山区人民政府办公室发布《2017 年宝山区金融服务工作要点》通知。提到跟踪服务庙行区块链孵化基地建设和淞南上海互联网金融评价中心建设。
		2017 年 4 月	上海市互联网金融行业协会发布《互联网金融从业机构区块链技术应用自律规则》，包含系统风险防范、监管等 12 条内容，这也是国内首个互联网金融行业区块链自律规则。
广州	紧密对接国家“区块链+”发展战略，针对区块链产业多个环节给予重点扶持，出台目前国内支持力度最大、模	2016 年 12 月	广州市委书记任学锋关于五年工作主要工作任务的讲话中曾提到要发展区块链等前沿技术。
		2017 年 10 月	深圳市人民政府向各区人民政府，市政府直属各单位印发《深圳市扶持金融业发展若干措

	式突破最强的区块链扶持政策。		施》，其中提到“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，年度奖励额度控制在 600 万元以内。
		2017 年 12 月	广州出台第一部关于区块链产业的政府扶植政策《广州市黄埔区广州开发区促进区块链产业发展办法》，整个政策共 10 条，核心条款包括 7 个方面，涵盖成长奖励、平台奖励、应用奖励、技术奖励、金融支持、活动补贴等。预计每年将增加 2 亿元左右的财政投入。
深圳	为确保在区块链产业国际化竞争中走在前列，积极扶持重点企业与重点项目，出台长期配套发展资金。	2016 年 11 月	深圳市金融办发布《深圳市金融业发展“十三五”规划》，提到，支持金融机构加强对区块链、数字货币等新兴技术的研究探索。
		2017 年 9 月	深圳市下发《深圳市人民政府关于印发扶持金融业发展若干措施的通知》，鼓励金融创新，设立金融科技专项奖，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，年度奖励额度控制在 600 万元以内。
		2018 年 3 月	深圳市经济贸易和信息化委员会发布文件《市经贸信息委关于组织实施深圳市战略性新兴产业新一代信息技术信息安全专项 2018 年第二批扶持计划的通知》，区块链属于扶持领域之一，按投资计算，单个项目资助金额不超过 200 万元，资助金额不超过项目总投资的 30%。
重庆	对区块链产业发展高度重视，在引进专业人才、凝聚产业力量以及营造良好的产业生态环境等方面加大投入和支持力度。	2017 年 11 月	重庆市经济和信息化委员会发布《关于加快区块链产业培育及创新应用的意见》，提出到 2020 年，力争全市打造 2-5 个区块链产业基地，引进和培育区块链国内细分领域龙头企业 10 家以上、有核心技术或成长型的区块链企业 50 家以上，引进和培育区块链中高级人才 500 名以上，初步形成国内重要的区块链产业高地和创新应用基地。
浙江	浙江是国内最早重视区块链技术的省份之一，2016 年初就有相关人士指出，希望浙江成为全国区块链技术开发应用高地。2018 年更是提出把区块链打造成未来产业，对区块链的重视程度非常高，发布诸多政府文件中都提及区块链。	2016 年 12 月	浙江省人民政府办公厅发布《关于推进钱塘江金融港湾建设的若干意见》，为推进钱塘江金融港湾建设，将积极引进区块链企业入驻。
		2017 年 5 月	西湖区人民政府金融工作办公室发布《关于打造西湖谷区区块链产业的政策意见(试行)》
		2017 年 5 月	宁波市经济和信息化委员会发布《宁波市智能经济中长期规划(2016-2025)》，其中提到加大区块链、人工智能等技术的推广应用。
		2017 年 6 月	杭州市人民政府发布关于推进钱塘江金融港湾建设的实施意见，支持金融机构探索区块链等新型技术。
		2017 年 11 月	《浙江省人民政府办公厅关于进一步加快软件和信息服务业发展的实施意见(代拟稿)》中提及需要加快云计算、大数据、区块链等前沿领域

			的研究和产品创新。
江苏	目前国内在政府文件中提及区块链最多的省份之一，江苏软件产业发达，科教资源丰富，具备区块链技术发展与应用的良好环境，在政策扶持上制定了针对区块链领域的人才扶持及产业创新的优惠政策，先后成立一批区块链相关的研究机构，致力于推动区块链技术应用、发展。	2017 年 2 月	南京市人民政府下发《市政府办公厅关于印发“十三五”智慧南京发展规划的通知》，明确提出要使区块链等一批新技术形成突破并得以实际应用。
		2017 年 3 月	南京市政府印发的《南京市“十三五”金融业发展规划》中，强调要以大数据、云计算、人工智能及区块链技术为核心，推进金融科技在征信、授信、风险控制等领域的广泛应用。
		2017 年 5 月	首届中国(无锡)物联网与区块链产业发展高峰论坛上，无锡软件行业协会区块链专业委员会暨物联网与区块链联合实验室正式对外揭牌。
		2017 年 9 月	2017 世界物联网新技术新产品成果发布会上，《中国区块链与物联网融合创新应用蓝皮书》发布。
		2017 年 10 月	南京发布“互联网+政务服务+普惠金融便民服务应用协同区块链支撑平台项目方案”。该方案利用区块链技术解决了政府各部门政务系统与各银行业务系统的打通。
		2017 年 12 月	苏州高铁新城向社会开放首批 15 个区块链应用场景，并发布 9 条扶持政策，吸引区块链企业和人才落户。
贵州	国内最早占据区块链发展风口，率先制定出区块链发展战略规划、发展区块链产业的地区之一。在推动区块链产业迅速发展的同时，也形成了国内较为完善的区块链产业生态。	2016 年 12 月	贵阳市政府新闻办举行了《贵阳区块链发展和应用》白皮书新闻发布会，白皮书计划 5 年建成主权区块链应用示范区。
		2017 年 2 月	在贵州省大数据发展领导小组印发的《贵州省数字经济发展规划(2017-2020 年)》的政府报告中，提道了“建设区块链数字资产交易平台，构建区块链应用标准体系”等目标。
		2017 年 5 月	贵阳国家高新区推出促进区块链技术创新及应用十条政策措施(试行)，在入驻、运营、成果奖励、人才、培训、融资、风险、上市十个方面提供政策支持。
		2017 年 6 月	贵阳市人民政府下发支持区块链发展和应用的试行政策措施，主要在主体、平台、创新、金融和人才五方面对区块链产业提供政策扶植。
山东	设立区块链产业发展年度专项资金，连续执行五年。	2017 年 6 月	山东省青岛市市北区发布了关于加快区块链产业发展实施意见，发布了区块链技术在政府管理、跨境贸易、供应链管理、供应链金融、大健康产业、公示公证、城市治理、社会救助、知识产权产业化、工业检测存证等十大领域的转化应用。
		2017 年 6 月	山东省市北区人民政府印发了《关于加快区块链产业发展的意见(实行)》，力争到 2020 年，形成一套区块链可视化标准，打造一批可复制推

			广的应用模板，引进和培育一批区块链创新企业。
		2017 年 9 月	青岛发布了“链湾”白皮书，计划成立全球区块链中心，建设青岛“全球区块链+”创新应用基地。同时通过税收优惠、房租补贴等吸引区块链企业入驻。
		2017 年 12 月	青岛国际沙盒研究院在崂山区发布了全球首个基于区块链的产业沙盒“泰山沙盒”。

整体上看，北京、广州、深圳、重庆、浙江、江苏、贵州、山东等地对区块链支持力度相对较大，政策将会吸引区块链企业加速在这些地区落地生根。由于区块链属于基础性综合技术，并且会对于现有各行业模式带来较大变化，所以一旦应用模式落地并得到认可，将会快速辐射全国。

3.2.2 监管

对于区块链的监管主要集中在数字货币。区块链本身并不属于极其深奥或难以理解的事物，但是由于“区块链”三个字本身让人无法立刻理解其意义，加上民众对无法立刻使用的新事物普遍抗拒学习和理解，所以给很多人行骗的机会。诸如前段时间火热的 ICO 数字代币融资，就是利用了人们对比特币的不理解，认为任何数字货币都是有价值的，来骗取大众数以亿计的财产。

国内对数字货币交易所和 ICO 监管态度非常严厉。2017 年 9 月，央行联合七部委联合推出《关于防范代币发行融资风险的公告》，公告指出，“ICO 本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。”并要求即日停止各类代币发行融资活动，已完成代币发行融资的组织和个人应当做出清退等安排等，叫停 ICO 并且在 9 月 30 号之前关闭境内数字货币的交易所。受此影响，火币网和 OKCoin 等知名交易网站都已迁出国内。

主体	时间	态度
中国互联网金融协会	2018.01	《关于防范变相 ICO 活动的风险提示》
中国人民银行/中央网信办、工信部、工商总局/银监会/证监会/保监会	2017.09	《关于防范代币发行融资风险的公告》
上海金融信息行业协会	2017.08	《关于 ICO 的风险提示》

2018 年 1 月，中国互联网金融协会发布关于防范变相 ICO 活动的风险提示。中国互联网金融协会指出，随着各地 ICO 项目逐步完成清退，以发行迅雷“链克”（原名“玩客币”）为代表，一种名为“以矿机为核心发行虚拟数字资产”（IMO）的模式值得警惕，存在风险隐患。从国内的监管政策看，对于数字货币和 ICO 的打击本质上是打击金融乱象，但是对区块链技术本身并无恶意，央行早已经在 2017 年 1 月份正式成立数字货币研究所，对新技术是探索和谨慎的态度。

3.2.3 国内实际应用

3.2.3.1 腾讯企业级 TrustSQL 区块链平台

TrustSQL 跟 IBM 的区块链平台类似，都是 BAAS（Blockchain-as-a-service）。底层平台分为四个部分：

图表 10 腾讯 TrustSQL 区块链平台底层服务-腾讯官网

用户管理：负责所有区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理以及用户真实身份和区块链地址对应关系维护等，并且在授权的情况下，监管和审计某些真实身份的交易情况。对数字资产等金融交易类的应用，还提供了风险控制的规则配置，以保证系统交易安全。

基础服务：基础服务部署在所有区块链的节点上，用来验证业务请求的有效性，并对有效请求完成共识后记录到存储上。对一个新的业务请求，基础服务先对接口适配解析，鉴权处理，然后通过共识算法将交易或者合约加上签名和加密之后，完整一致的存储到共享账本上。共识机制可自适应，在网络和节点都正常情况下具有高并发性，网络异常或者节点欺骗的情况下具有强容错性。

智能合约：负责合约的注册发行以及合约的触发和执行。用户通过某种编程语言定义合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户签名或者其他的事件触发执行，完成交易结算等合约的逻辑。

运营监控：负责产品发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态可视化的输出，如：告警、交易量、网络情况、节点健康状态等。

3.2.3.2 国内上市公司区块链布局

上市公司	股票代码	公告
易见股份	600093.SH	（1）2017 年 4 月，易见股份携手 IBM 中国研究院联合发布了国内首个区块链供应链金融服务系统---“易见区块”。（2）易见股份 2017 年 9 月 12 日公告，公司拟与云南信托、浙江浙银泓万资产管理有限公司采用有限合伙企业形式，发起设立易见浙银区块链投资基金（有限合伙），基金总规模拟定 7.6 亿元，公司出资 2.5 亿元。
安妮股份	002235.SZ	为加速新媒体版权保护创新模式研究，提升公司转化区块链技术在版权领域的能力，公司加入工信部中国区块链技术和产业发展论坛并担任理事单位职务，加入 Linux Foundation 基金会全球会员，加入超级账本 Hyperledger 会员。同时，公司积极与厦门大学知识产权研究院、Hyperledger 开源社区等机构开展学术合作。
新晨科技	300542.SZ	2018 年 1 月 18 日公告，表示公司认为区块链业务及技术尚处于探索阶段。
远光软件	002063.SZ	在基于区块链技术的电子证照、基于区块链的资金管理创新应用、基于分布式能源的区块链交易、结算平台、基于区块链的数据安全共享技术以及区块链理论研究方面均有涉足。
飞天诚信	300386.SZ	飞天诚信澄清公告：公司推出的产品产品仅是区块链虚拟货币的安全存储设备，属于区块链产业链中的终端辅助产品，且尚未形成销售收入。
恒生电子	600570.SH	公司运用区块链技术实现基于联盟链的数字票据系统。和关联法人共同设立鲸腾网络公司（筹），鲸腾网络正式设立后，将负责处理涉及行情服务、支付中心、

		开放平台、仿真产品及 FTCU（金融业务协作区块链联盟平台）的业务。
赢时胜	300377.SZ	公司将于 2018 年 3 月初上线保理区块链 SAAS 系统，未来将陆续上线供应链代采购及票据区块链 SAAS 系统。
金证股份	600446.SH	2016 年 5 月 31 日，金融区块链合作联盟（深圳）成立大会暨第一次成员大会在深圳正式召开，公司为大会发起成员之一。公告称，截至目前公司区块链业务处于培育期和探索期，尚未形成相关技术，目前研究仅是课题研究，没有实质性成果。
广电运通	002152.SZ	公司 FINTECH 研究院围绕智能视频分析、智能语音识别、区块链、人机交互等人工智能前沿技术不断取得突破。
海联金汇	002537.SZ	联动优势一直专注于金融科技服务领域相关技术研究和产品的创新，尤其在区块链技术的改进和应用上不惜投入，对以太坊和超级账本方面均有很深的研究，对超级账本的底层区块链技术做出了改进，此改进针对金融行业场景提供生产级的技术优化和服务支持，目前有多个区块链项目产品正在实施中。
恒宝股份	002104.SZ	公司公告，目前公司区块链技术尚处于前期技术研发和应用探索阶段，还未签订正式合同，未产生业务收入。2018 年公司将根据经营需要适度加大对区块链技术的研发和应用投入，为公司未来的物联网应用项目做好技术储备。
新国都	300130.SZ	2017 年 7 月 4 日公司在互动表示，公司去年成立了区块链研究中心，跟踪区块链技术发展方向。公司的区块链研究中心会聚焦于实际应用，主要是公司所在领域的商业应用及产业战略方面的研究探索。
四方精创	300468.SZ	2017 年 12 月 7 日晚间公告，公司与 IBM 合作开发的产品 MVP(Minimum Viable Product)首个转化为实际应用的项目，“CCBA Blockchain for Bancassurance Project”在中国建设银行(亚洲)股份有限公司成功实施。该项目是区块链技术在银行保险业务的应用，项目的成功实施可以实现保险政策数据的实时共享，优化银行保险业务。
浙大网新	600797.SH	浙大网新参股杭州趣链科技有限公司。16 年 10 月，趣链科技发布全球首个成熟商用的联盟区块链平台 Hyperchain。
用友网络	600588.SH	2017 年 1 月份，公司拟出资 168 万元受让博晨技术 5.2366%的股权。受让完成后，公司占博晨技术总股本的 5.2366%。博晨技术是一家定位于区块链技术标准与解决方案的研究，开发，区块链应用系统的部署及运营的创新企业，核心团队拥有一定的区块链领域研究积累及开发经验。
高伟达	300465.SZ	2016 年 8 月公司公告与中信集团正式签订《战略合作协议》，就互联网、物联网、大数据、云计算、区块链等领域建立深度战略合作关系，共同推动业务模式的系统化创新，支撑和引领中信集团产业互联网战略规划的落地和发展，合同为期限三年。根据公告，第一阶段双方具体合作内容包括但不限于集团和子公司物联网和区块链应用开发。
御银股份	002177.SZ	2016 年 4 月 13 日公司在互动表示，区块链技术由于最近互联网金融和在支付行业的应用得以引起广泛关注，相对于集中模式，它能够更加快速、有效、低成本解决信用认证的问题，目前公司有组织团队进行研究，希望将利用区块链技术在信息安全及身份识别领域的应用机会来提高公司产品的安全和效率。
中元股份	300018.SZ	2018 年 1 月 22 日晚回复深交所关注函称，公司全资子公司世轩科技正探索区块链技术在医疗领域的实践和运用，目前已在《世轩互联网医院软件 V1.0》项目中研究区块链技术的应用，但尚未形成独立产品和服务对外销售。
海联金汇	002537.SZ	2018 年 2 月 10 日在互动平台表示，公司 2017 年自主研发了区块链底层平台名为优链（英文名称:UChains），同时通过了中国信息通信研究院的可信区块链预测试，该产品为公司独有研发。

视觉中国	000681.SZ	公司互动平台上表示，区块链技术作为互联网底层技术，只有与数字版权的全流程业务场景相结合才能真正落地。区块链技术在视觉中国的主营业务中具有丰富的业务应用场景，公司会继续研究区块链技术对数字版权产业的积极方面，并在全流程的业务场景中应用相关技术，将它们更好地运用在服务中。
深科技	000021.SZ	公司为国内知名比特币挖矿机产品制造商之一，2018 年 1 月产量约 15 万台左右。
卫士通	002268.SZ	公司在 2016 年成立了研究小组，小组成员 20 人，在区块链平台开发建设、隐私保护、智能合约编程等方面开展了研究。截止目前，区块链技术没有直接产生业务收入，也不对公司经营构成实质性影响。

目前我国对区块链如何应用尚不明朗，发布区块链相关公告的 A 股上市公司均处于研究阶段，还未能转化成实际业务和收入。大部分 A 股上市公司主营业务并非区块链，那么区块链的研究主要方向将会是弱中心化甚至私链为主。结合 3.2.1.1 的论述，在大方向上，我国区块链未来不太可能会采取完全去中心化的模式。