

2016-6-16

行业研究(深度报告)

 评级 **看好** 维持

信息技术行业

区块链报告之一：基础篇——具备优质特征，应用场景丰富

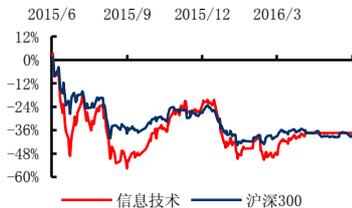
分析师 马先文
 ☎ 862765799815
 ✉ maxw@cjsc.com.cn
 执业证书编号：S0490511060001

分析师 王懿超
 ☎ (8621)68751569
 ✉ wangyc8@cjsc.com
 执业证书编号：S0490516050003

联系人 杨靖凤
 ☎ (8621) 68751636
 ✉ yangjf@cjsc.com.cn

行业内重点公司推荐

公司代码	公司名称	投资评级
------	------	------

市场表现对比图(近12个月)


资料来源：Wind

相关研究

《长江电子日观点荟萃(2016.06.15)》2016-6-15

《数据流量爆发下的确定性机遇》2016-6-15

《长江计算机“七日谈”(20160614)一级市场动态：互联网金融回归初心，互联网征信有望加速》2016-6-14

报告要点
■ 多节点参与记账维护，去中心化的大账本

区块链衍生于比特币，是哈希密码、时间戳和 P2P 传输创造性组合的产物，其原理是使用全新的加密认证技术和去中心化的记录生成机制，所有参与者共同记录、维护（而不是某一中心记录）一个包含全部记录的大账本。

■ 可靠可追溯、去中心化信任、智能合约

区块链采用非对称加密，同时多节点参与记账、核对，使得其记录具有高可靠性，加上时间戳和区块之间的数据指纹使用，具备良好的可追溯性；参与记账的各节点是独立的，而共识机制的设计使得各个节点正确记账获得奖励，刻意错记或篡改记录不被认可或面临极高的成本而不具有经济性，因而可以在没有权威中心的条件下达到去中心化信任的效果；最后，区块链自带智能合约的属性，大量合约之间自动执行大幅降低监督和执行成本，并为物联网价值交换提供坚实基础。

■ 降低信任成本，应用场景广泛

区块链具有广泛的应用场景，如国家数字货币、非国家数字货币、支付与清算、金融资产发行与交易、权属证明与交易、自组织物联网、内部流程审计与优化。这些领域目前均存在可靠性不足、获取信任成本高昂，区块链的应用一方面降低也有业务的成本，一方面衍生出新的业务。

■ 技术有望快速突破，应用将逐步落地

区块链在记账效率、存储成本、开发难度等方面还存在一些问题，监管上也有着不确定性。但我们认为在核心的算法和共识机制创新、开发平台的成熟等带动下，技术层面将持续突破；多个国际大型金融机构表现出极大重视；监管方面的态度也出现了较大转变，行业正处于快速发展阶段。在应用落地方面，将沿着金融和非金融两条路径推进，我们看好非金融领域的权属证明与交易、自组织物联网等细分市场机会，及金融领域的非高频、监管相对缓和、痛点较多领域的快速发展，如跨境支付、票据交易、区域股权市场。

目录

创造性组合的产物，去中心化的大账本	4
区块链是创造性组合的产物	4
所有节点共同参与记账的大账本	5
公有链、联盟链、私有链形式多样	6
具备可靠可追溯、去中心化、智能合约特征	8
非对称指纹+多节点账本：可靠、可追溯	8
高可靠性+节点独立记账：去中心化信任	10
高可靠性+可编程：合约智能化	12
狙击多处痛点，应用领域广泛	12
非央行数字货币	13
央行数字货币	13
支付与清算	13
金融资产发行与交易	13
权属证明与交易	13
自组织物联网	13
内部流程优化与审计	14
技术有望持续突破，应用逐步落地	16
技术有望持续突破，央行关注提升	16
共识机制和算法持续创新	16
中心化和去中心化寻求平衡	16
平台化趋势助力应用快速开发	17
央行态度从谨慎到重视	18
非金融领域前景广阔，金融领域从低频细分突破	20
贯通技术、场景和法规，方能一显身手	20
非金融领域具备广阔前景	20
金融领域从低频细分切入	20
有望成为价值互联的基础框架	20
附录：比特币挖矿	21

图表目录

图 1：区块链研究框架	4
图 2：比特币是多个技术创造性结合的产物	5

图 3: 区块链最大的特点是去中心(多中心)的记录和存储.....	6
图 4: 区块链通过大量的哈希算法和时间戳使得篡改记录难度极大.....	9
图 5: 传统记账机制的信任中心是权威机构.....	10
图 6: 区块链记账的信任中心是一套共识算法.....	10
图 7: 智能合约属于法律相关行为.....	12
表 1: 区块链按参与对象范围和关系的不同可分为公有链、联盟链、私有链.....	7
表 2: 区块链具有可靠可追溯、去中心化信任及智能合约属性.....	8
表 3: 区块链具有高度防篡改特性.....	9
表 4: POW、POS、DPOS 比较.....	11
表 5: 区块链具备解决多个领域痛点的潜力.....	14
表 6: 区块链开发平台逐步丰富.....	17
表 7: 国家或地区对比特币的监管态度总体偏谨慎.....	18
表 8: 多家央行或重要金融机构对区块链较为重视.....	19
表 9: 比特币区块头结构.....	21

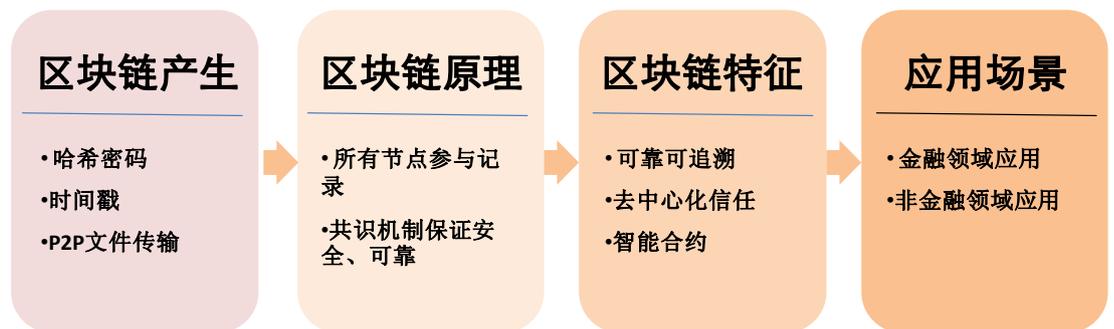
在前期报告中，我们结合专家的观点对区块链做了全景性的介绍和梳理，本篇这是我们区块链系列报告的整体框架，在后续报告中我们将主要探讨区块链的应用及重点领域的专题研究。

创造性组合的产物，去中心化的大账本

区块链是创造性组合的产物

2015 年开始，“区块链”在国内开始受到较高的关注，吹捧质疑声音皆有，加之和比特币有着纠缠不清的关系，更增加其神秘色彩。其实，关于区块链大多数争论和误解都是围绕其应用于数字货币领域展开，因为货币作为宏观经济最重要的变量，本身就具有相当的复杂性，这增加了对区块链认识的难度。我们认为，更好的认识区块链需要以其产生的历史背景为起点、了解其原理为基础，在深入理解区块链技术特征的基础上，探讨其可能的应用场景下的价值，并结合技术进展、行业特征和商业模式探讨区块链的发展路径。

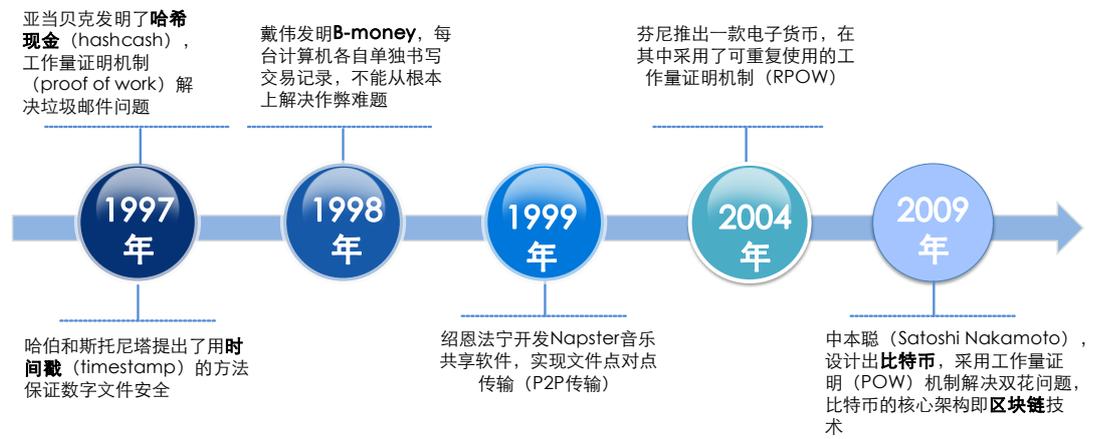
图 1：区块链研究框架



资料来源：长江证券研究所

区块链源于比特币，即比特币是基于区块链架构的第一个应用，并规定了区块链技术的一些基本要素。总体而言，区块链是哈希密码、时间戳、P2P 文件传输创造性组合的产物，在比特币之前有过较长时间的艰辛探索和技术突破。数字货币的吸引力由来已久，然而，一款优秀的数字货币方案要解决安全性、防双花和实现价值的灵活转移，这使得数字货币的实现在很长时间内还停留于理论。比特币将已有技术创造性的组合，并对技术细节进一步补充和完善，诞生了第一款真正意义上的数字货币，也为区块链奠定了可靠可追溯、去中心信任、智能合约等重要属性，并引爆网络空间价值去中心化转移领域的持续创新。

图 2: 比特币是多个技术创造性结合的产物



资料来源: 互联网, 长江证券研究所

所有节点共同参与记账的大账本

在当前, 货币或者其他价值转移一般是依靠权威的第三方来记录, 比如刷卡时银行负责金额转移记录、购房时政府负责产权转移登记、天猫购物则是支付宝和银行等负责资金转移账本, 记账人无一例外都具有权威和中心化的特征。

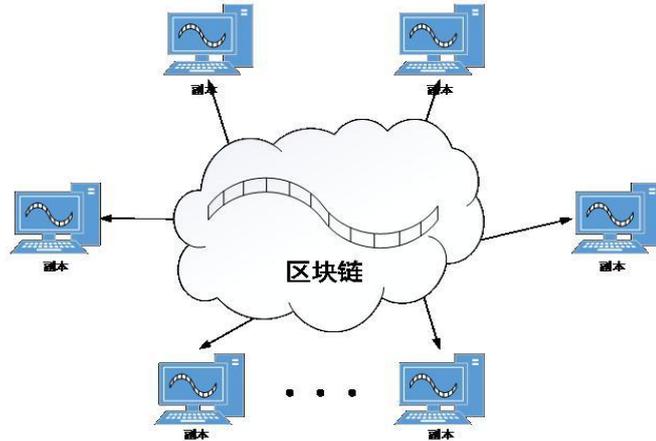
- 权威: 记账人的信任要么是政府信用, 要么是影响力足够大的第三方, 能获得全体参与人的信任。
- 中心化: 记账人的个数极少, 所有价值转移都经过记账中心确认。如天猫所有买卖都会通过支付宝进行支付确认, 刷卡消费会通过银行和银联确认资金转移。

在历史上和现阶段, 价值转移经历了非中心化—中心化的变化, 这与作为价值载体的货币形式的演化伴随发生, 比特币的诞生则标识着去中心化价值转移路程的开启。

简单而言, 区块链就是所有参与交易 (活动) 的对象都参与记录交易的结果, 并共同保管记录。具体而言, 区块链技术是使用全新的加密认证技术和去中心化的记录生成机制, 共同维护一个所有记录的大账本。区块链最大创新在于解决了去中心化条件下因记账角色不可信而导致的价值转移受阻, 即在没有一个可信任的权威机构 (如支付宝和银行) 参与下, 实现对交易结果可靠的记录, 并且能做到防篡改和完全可追溯。区块链对于实现比传统技术更加安全和可靠的记录具有重大意义。

一种典型的情况是, 参与交易的所有对象在自己终端都会保存一个完整的账本 (每个人的账本都是完全相同的), 这一账本记录了从系统开始运行到上一次记账的所有交易记录。当有新的交易记录时, 每个对象都暂时记录下来, 把从上一次记账结束到现在这段时间的交易记录汇总, 并加上一些附加验证信息就构成一个区块, 把区块加入原有的账本并和前一个区块通过一定的关联唯一联系起来就构成区块链的记录主体。

图 3: 区块链最大的特点是去中心(多中心)的记录和存储



资料来源: 互联网, 长江证券研究所

比特币区块链实例:

- 1、某一个时点, 所有参与比特币交易的对象的客户端都有一份完整的从比特币诞生以来的完整交易记录。该记录分区块存储, 每一个区块的内容是某个小段时间的交易记录(如 10 分钟)、上一个区块的指纹、区块生成时的时间(时间戳)和其他附加信息。
- 2、A 要把一个比特币转账给 B 时, 他将向整个网络广播, 但只有 A 用上特有的私钥才能顺利接收转账, 每一个接收到广播的参与对象均记录这一交易过程。
- 3、一段时间后找到了一个合格的记账者 X (X 因为解决了一个数学难题而获得记账权限), 他把上个区块的指纹, 该段时间所有交易记录、当前时间和其他一些附加信息打包记录下来向整个网络广播。
- 4、网络中所有其他人验证 X 是否有记账权限及他对账目的记录是否正确, 当其他对象都(大部分)都认为正确时, 新的区块生成, 并加入到每一个对象账本的末尾, 账本增加一个区块。若 X 的记账结果没有获得全网大多数参与者的承认, 则重复步骤三, 直到新的区块产生, 并回到步骤 1。

公有链、联盟链、私有链形式多样

最早的比特币区块链(交易记录文件)是所有参与比特币交易的对象都会在客户端获得一个完整的历史交易记录, 任何人都可以使用运行客户端的联网设备接入比特币网络。随着理念和技术创新, 其他区块链对参与记账的对象的进入门槛和范围有了一些变化。按参与对象范围的不同, 区块链可粗略区分为公有链、联盟链和私有链。划分的标准不是参与节点的多少, 而是整个系统中记账节点的门槛和记账权的分散度。公有链参与对象广泛, 每个参与者均参与记录和保管记录, 比特币是典型的公有链; 联盟链节点参与者是开展相似业务或有着共同需求的群体, 如数十个国际大银行共同参与运作的 R3 CEV; 私有链则不仅节点更少, 其更本质的特征是所有节点可能最终都是由一个实体控制, 一个公司内部的区块链系统可以是典型的私有链。

表 1: 区块链按参与对象范围和关系的不同可分为公有链、联盟链、私有链

	参与对象	方案价值	适用领域	优点
私有链	单独的个人或实体	不完全解决区中心化信任问题, 但改善可审计性; 具备智能合约属性	公司、政府内部审计和测试, 政府主导的产权登记等	容易部署, 能实现较好的控制
联盟链	预先设定或特定发起的组织	多中心化, 大幅改善信任问题、降低成本、提高效率	银行或国家清算、结算,	控制权易设定、扩展性较好、可提供较快的交易频率
公有链	任何对象都可以参与	去中心化, 去信任化	广泛应用于支付、金融资产交易、存在性证明等	灵活性大, 能部署丰富的应用程序

资料来源: 互联网, 长江证券研究所

公有链、联盟链和私有链并无简单的优劣之分, 而是分别适用于不同的场景。

私有链的优点: 私有区块链不完全解决去中心化信任问题, 但保留可靠可追溯特性, 具备其他诸多优点。

- 和现有法规兼容。例如将区块链用于房地产登记, 在目前国内背景下, 政府部门放弃房地产登记主导地位的可能性不大, 而由房地产登记部门主导搭建一个私有区块链登记平台, 发挥区块链安全、可追溯、可编程优点的同时, 可以使登记权可控和符合现有法规;
- 效率高、成本低。私有链所有节点背后控制人为同一个, 基本不存在伪造和双花攻击, 布局数个到数十个节点即可保证足够的安全可靠, 在记账的共识机制方面也可以采用 DPOS 等一些效率较高的方案, 实现高效率低成本的登记。

联盟链的优点:

- 联盟链参与对象主要为某一特定行业企业, 其具有相似的行业属性, 依托联盟链可高效率地实现行业既有标准或制定并执行复杂的新标准;
- 整个区块链系统是多中心化的, 具备良好的可靠可追溯特征, 能实现去中心化信任, 解决行业内部成员之间因信任缺乏导致的效率低下;
- 每一个节点是事先确认或者事后申请加入的, 节点可控性强, 因而, 联盟链在共识机制选择上具有更大的灵活性, 不用花太多精力放在诸如 51%攻击等难题上面, 有助于效率提升和成本降低。

公有链优点:

- 可以做到最大程度的去中心化。比特币和其他数字货币底层所使用的区块链技术是典型的公有链, 即每一个节点都有参与记账的权利, 这种类型的公有链在节点达到一定数量时有着足够的稳定性, 可以完全忽略新接入节点的特征, 然而其共识机制往往需要设计得相当复杂从而避免恶意节点的攻击。
- 节点足够独立情况下, 少量节点即可获得最大程度去中心化信任效果, 从而实现公有链的特征。去中心化的程度不一定需要大量的节点, 只要这些节点是互相独

立的，或者说代表不同的利益方。如基于区块链的投票系统，并不需要每个选民都要一个节点，只要数十个节点分别属于不同的利益团体即可保证足够的可靠性和去中心化信任。

- 稳定性好。当奖励机制合理，从而有大量节点参与记账时，完全去中心化的系统具有极高的稳定性，如比特币区块链久经考验仍稳定运行。

具备可靠可追溯、去中心化、智能合约特征

随着区块链关注度越来越高，市场关于区块链的文章数量呈爆发性增长，然而大部分文章并没有深入地分析区块链具有的优质基因和应用领域之间的关系。我们认为，只有深入理解区块链最重要的特征，并结合应用场景分析才能更好认识区块链的价值。

区块链技术主要有三大重要特征，每一个应用场景都或多或少用到各个特征，在不同的应用场景下，对其中一两个特征更为倚重。其中：

- 不可篡改、可追溯特征可用于不动产登记、商品防伪、知识产权等领域；
- 可靠性+记账节点的独立性实现去中心化信任，这是非中心化的数字货币（非央行数字货币）、金融资产发行与交易、自组织物联网及很多中心化信任缺失或者实现中心化信任承受极高的成本的场景实现价值传输的利器；
- 可靠性+可编程属性使得智能合约变得容易实现，衍生出广泛的应用场景，如央行数字货币、金融资产交易、数字知识产权登记交易、物联网等。

表 2：区块链具有可靠可追溯、去中心化信任及智能合约属性

区块链特征	实现原理
可靠、可追溯	前后区块通过记录指纹唯一联系+时间戳+保存全部历史数据：实现记录的不可篡改（篡改成本极高）、可追溯
去中心化信任	高可靠性+每个节点独立记账，所有节点参与核对
合约智能化	高可靠性+多个交易的连接可听过事先编程、实现自动执行

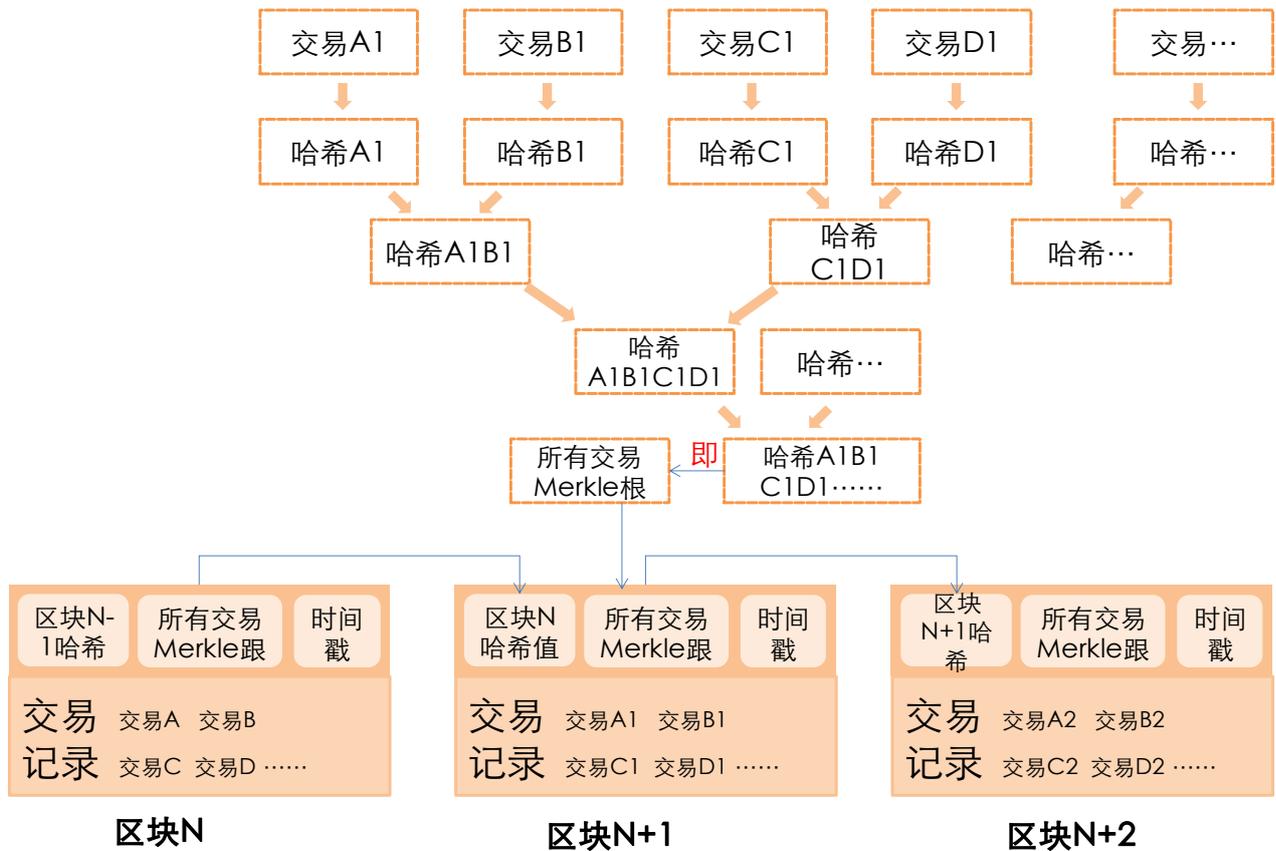
资料来源：长江证券研究所

非对称指纹+多节点账本：可靠、可追溯

可靠是指篡改数据很难、摧毁系统很难，可追溯是指价值传递过程可追溯，进而可追溯价值传递过程背后对应的实体关系。

典型的区块链记账方法会生成每一次交易的指纹（哈希值），并再次生成指纹的指纹（两个哈希值合并字符串的哈希值），通过层层哈希得到最后一个指纹，即所有交易的 Merkle 根。由于哈希算法的特性，任何单笔交易的微小篡改都会使得最终的 Merkle 根面目全非。区块链技术会将第 N 个区块整个记录包通过哈希算法生成的数据指纹放在第 N+1 个区块链当中，第 N+1 个区块的指纹放在第 N+2 个区块链当中，通过指纹的依次传递实现上下区块之间的唯一联系。若篡改其中一个区块，则意味着需要篡改记账网络中全部节点上该区块以后的所有区块，难度极大。

图 4：区块链通过大量的哈希算法和时间戳使得篡改记录难度极大



资料来源：互联网，长江证券研究所

多节点账本是参与记账的每一个节点保存一份从系统开始运行到目前的所有历史交易的账本，故理论上而言只要有一个节点保存有一份完整的记录数据就不会丢失。此外由于节点保存所有历史记录，理论上可追溯一个项目（如一笔资金）自系统运行以来的所有流转过程，这对于审计、供应链追踪、所有权转让具有重要作用。

表 3：区块链具有高度防篡改特性

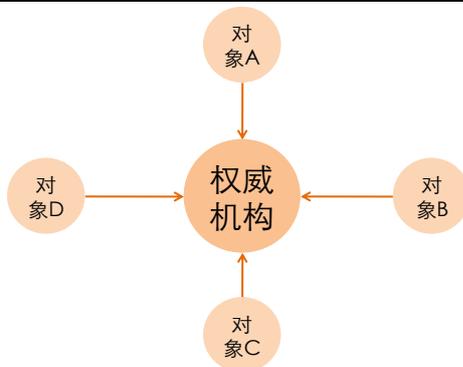
	区块链	互联网	社交网络	传统数据库
主要用途	储存信息、交易记录等	发送和接收信息	沟通交流	储存信息
去中心化	是	是	否	否
高度防篡改	是	某些情况下	否	否
是否在线	是	是	是	否
适合私人使用	私有链适合	有时是	否	是

资料来源：Deloitte，长江证券研究所

高可靠性+节点独立记账：去中心化信任

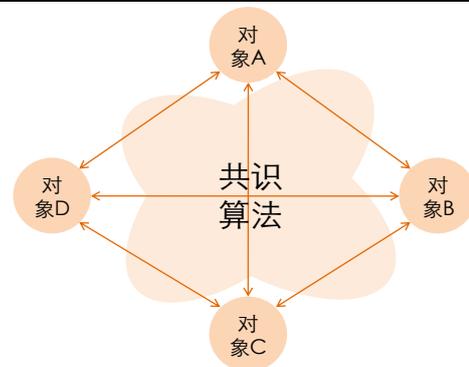
目前，价值交换需要的可信任的中心化平台基本都是由某一权威部门提供。中心化信任是将记录权交给政府部门、银行等权威机构，而典型的区块链（公有链）是去中心化信任，其本质是将记账权交给一套算法。传统的货币、资产、所有权等价值交换的过程都离不开见证人，见证人由获得各方信任的机构或个人担当，充当记账人的角色。但这种机制远非完美。在业务不太复杂时，主要的问题是中心的信任问题和可靠性问题，这包括两个层面，其一是记账角色可能是不值得信任的，例如在法制不健全的社会，中心记账人具有极大的操纵特权；其二是中心记账人是否可靠，即我们虽然确定中心记账人是公正的，但他可能不具有很好的记录交易和保存账本记录的能力，其记录过程可能出错，账本可能丢失或者被其他人篡改，如跨境支付清算因为可靠性导致的信任问题而付出极高的成本。总体而言，传统信任的是位于中心的权威机构，区块链信任的是无处不在的一套算法（共识机制），而算法比某一特定的中心更加可靠。

图 5：传统记账机制的信任中心是权威机构



资料来源：,长江证券研究所

图 6：区块链记账的信任中心是一套共识算法



资料来源：长江证券研究所

进一步而言，区块链通过没有特权的、平等的多方同时记账、同时核对账本及每个节点保存一个不可篡改的账本而很好的实现去中心化信任。并且，由于多方参与记账，可以做到所有记录的公开透明。去中心化信任是区块链具有广泛用途的最重要的技术属性。目前大量中心化的业务由于获取各方信任而面临极高成本，例如跨境结算、股票的发行和交易；为保证中心节点的可靠（经常不可靠），需要付出高昂的成本，并且参与各方的业务往来都要通过中心节点协调，效率低下。区块链的去中心化技术属性则直接越过中心机构实现点对点的可信任的价值交换。

去中心化信任主要针对公有链和联盟链。典型的公有链环境下，每个独立的节点均参与记录及所有节点参与核对记录。区块链技术设计一种合理的机制使得：

- 1、正确记录会获得一定的收益；
- 2、单个节点故意或非故意的错误记录不能获得系统大多数节点认可，从而启动自动纠错机制，最终实现正确记录；
- 3、联合其他系统大多数节点恶意作假或篡改记录会使得成本极高，甚至远高于作假记录和篡改的收益，从而不具有可行性。

在联盟链环境下，记账节点需要事先审核，本身没有造假动机或造假成本极高，如银行联盟链中的某个银行做假账的成本就高到不可承受，所以在联盟链下，共识机制的设计可以更加灵活。

记账人的随机分配和鼓励正确记账需要一个对应的选择记录人的过程及奖惩机制。目前比较常见的机制有 POW、POS、DPOS 等。这些机制都还有一定的缺陷，记录人选择算法的设计和保证记录的可靠性是区块链技术突破很重要的重要方向。

- **POW (Proof of Work, 工作量证明):** POW 机制是首个区块链应用比特币采用的共识机制，基于非对称加密原理，节点需要花费很大的算力解决一个数学难题（每个节点解决的数学难题的初始条件不同，但难度相同）才获得记账权限，而且其他节点可以很轻松地验证试图记账的节点的答案是否正确（POW 机制解决的数学难题具有难求解、易验证的特点）。此外，算法会评估每个节点的算力，并根据算力分配投票权限，某节点想要作弊时，必须获得系统 51%票数，因此需要有系统 51%算力，因而需要花费极高的成本。
- **POS (Proof of Stake, 权益证明):** 该机制背后的思想是，系统出问题，持币越多的人面临的潜在损失越大，因而持币越多作弊的动机越小，从而给与其更多的记账机会，但在每一次记账后则减小其相应的下次记账概率，一段时间没有记账则增加其记账概率。
- **DPOS (Delegate Proof of Stake 股份授权证明):** 在 POS 机制基础上向前一步，首先是投票选出一批代表性的节点（如 101 个），然后这些代表性的节点再选出一个节点负责记录，其他节点核对记录，更大程度提高记账的效率。

表 4: POW、POS、DPOS 比较

	原理	优点	缺点	案例
POW	通过算力暴力枚举解答数学难题获得记账权利，同时记账节点获得相应奖励	成熟、稳定、容易获得所有节点认可	能耗高、算力集中趋势	比特币
POS	通过消耗币天数获得记账权，同时获得相应奖励	效率较高、能耗较低	初始阶段可能需要 POW 等机制配合，可能一定程度造成穷者愈穷富者愈富	未来币
DPOS	投票产生适当数量的代表，在代表中随机选择记账人，记账人获得相应奖励	效率高、能耗低，解决 POW 共识机制中算力集中的问题。	整个共识机制还是依赖于代币	比特股

资料来源：互联网，长江证券研究所

总体来看，目前多种共识机制及团队之间的争论主要限于数字货币，区块链真正产业化和大规模应用可能需要根据不同场景而选择不同共识机制，只要合适的机制能保证记录的可靠可追溯、不同节点具有相对平等的权利，则机制的不同并不改变区块链的本质。共识算法的创新将是推动区块链产业化的重要力量。

高可靠性+可编程：合约智能化

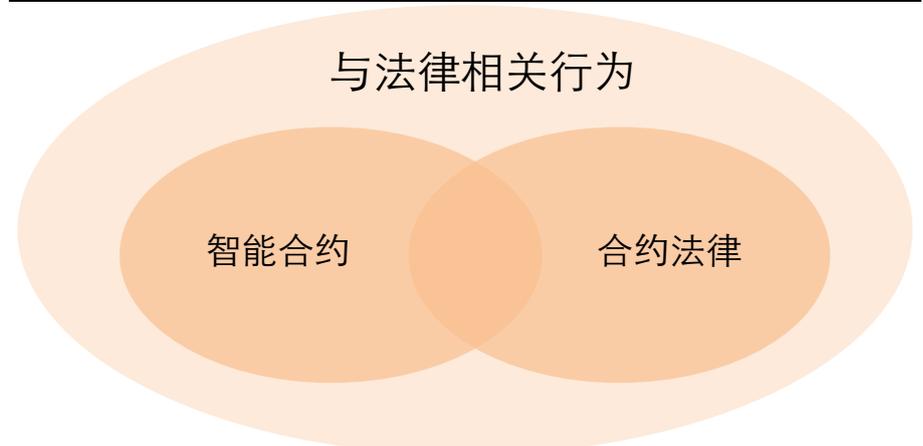
智能合约是存储在区块链账本上的一段代码，其能对外界特定的信息作出回应，从而自动实现预先设定的功能。

在区块链系统中，由于非对称加密（公钥、私钥）的引入和自带可编程的属性，使得合约可以实现智能化，即可以设定一些包含条件的合约，当这些条件都成立时，合约自动执行。例如，民政部门对于生活困难的 A 先生每月发放一定补助，在其去世时发放一次较大的补助。在现行的做法中经常遇到的一个情况是，从 A 先生去世到民政部门更新 A 去世的信息有很长一段间隔，或者家人故意延迟上报从而获得更多补助。应用区块链技术，可以设计一个智能合约，每月发放补助时扫描死亡信息库，如果没有 A 的名单就发放补助，如果 A 已去世，则发放一次性大额补助给 A 指定的接收人，并把 A 调出补助名单。整个过程是自动执行的，省去了传统做法中大量人员的配备，并有着完美的精确性。

一般而言，可编程属性可用于交易对象和交易流程的控制，比如央行在区块链上发行数字货币有望实时监测流通中的货币状态，提取流通关键参数，也可精准控制货币流向；涉及时间或条件生效的合约也可自动执行，比如居民向金融机构抵押住房所有权贷款，在贷款还清的同时，抵押自动取消。

可编程属性降低执行成本和监督成本。一旦交易的初始条件设定清楚，后续事项将在条件成就时自动执行，减少大量不必要的纠纷。将区块链的智能合约属性应用于物联网，则可以在物联网中实现区中心化的、完全无人工干预的、复杂的价值交换。

图 7：智能合约属于法律相关行为



资料来源：互联网，长江证券研究所

狙击多处痛点，应用领域广泛

我们认为区块链的可靠、可追溯，去中心化信任和智能合约属性将带来广泛的应用场景，对现阶段的价值传递流程进行重塑，在多个领域具备极大的应用价值。我们看好区块链在非国家数字货币、国家数字货币、支付与清算、金融资产发行与交易、权属证明与交易、自组织物联网、金融机构内部流程优化与审计等领域的巨大应用价值。

非央行数字货币

比特币是区块链的起源，自推出以来，虽价格波动较大，仍以其稳定性和广泛的认可度征服了大量参与者。目前比特币产业链发展已相对完善，其他数字货币仍呈现旺盛活力，非央行数字货币是区块链的重要创新来源。我们认为，抛开比特币表面存在的诸多争议，其区块链设计机制、技术和背后的理念在去中心化价值转移中有着较大的价值。

央行数字货币

货币从实物形态到纸币再到数字货币是一较为确定的趋势。区块链安全、可追溯的优质基因获得多国央行密切关注。自 2015 年 7 月以来俄罗斯、英国、欧洲央行均表示正着手研究区块链技术，中国央行也在大力推进数字货币，并认为区块链技术是可供选择的技术方案之一。我们认为央行发行货币的数字化是历史趋势，而区块链诸多技术特点能较好满足可靠、可追溯，且有助于执行精准的货币政策的潜力，后续更多央行的研究及尝试值得期待，一旦央行推出基于区块链的数字货币，将对现行金融体系产生广泛而深远的影响。

支付与清算

支付与清算领域存在很多痛点，首当其冲是安全问题频出和成本高昂，在跨境支付、机构间清算（跨境清算）领域更为常见。区块链的特性可有效弥补现在支付清算领域的不足，在该领域，一批行业先驱进行了较为成功的尝试，我们预计未来这一块应用将大有可为。

金融资产发行与交易

常见的金融资产，如股票、债券、期货发行时为克服信息不对称需要付出极高的代价；在交易过程中，造假影响及为保证安全付出的成本极其高昂。区域股权市场、票据造假等领域影响最为突出，区块链技术在金融资产发行与交易领域有望显著降低成本，大有用武之地。

权属证明与交易

在某些国家，权属登记中心信任度不够；一些诞生于互联网的版权缺乏权威登记机构；另外一些权属交易市场则混乱或缺失。区块链记录具有的可靠可追溯的优势天然适合于权属的登记与交易，配合智能合约和物联网，将产生新的巨大市场。

自组织物联网

现阶段，物联网的广泛应用仍存在较多问题，主要为海量联网设备给物联网信息处理中心带来极大的负荷，同时通讯的可靠性较差，物联网设备一旦和中心通信出现故障则可能造成灾难性的后果（如无人驾驶汽车和信息中心交互出现故障）。区块链技术有助于物联网设备间去中心化的通信和去中心化的信任的建立，从而形成去中心化的自制系统，极大程度提高物联网的稳定性和可靠性。同时，区块链的智能合约属性也能使物联网设备之间达到去中心化价值交换，将物联网设备之间的联系推进到新的层级，如无人驾驶的新能源汽车通过充电桩购买电能。

内部流程优化与审计

大型银行等金融机构内部的部门和人员之间存在大量的信任问题，现阶段只能设计复杂的流程减少风险的产生，这带来效率的损失和成本的增加，且不能完全避免（如频繁发生的巨额存款丢失）。区块链应用于大型银行或其他金融机构内部，有助于重塑信任链条，提高效率、降低成本，同时区块链拥有的可靠可追溯的特性也会给后续的内部可审计性带来极大的改善。

表 5: 区块链具备解决多个领域痛点的潜力

应用领域		痛点	区块链切入点	效果	现有项目或研究计划
非国家数字货币		-	可靠性、去中心化信任、智能合约	-	比特币、Coinbase、Abra
国家数字货币		央行只能控制基础货币供应或利率，不能控制货币流通速度，不能控制货币特定流动方向，对整个经济体系货币分布只有粗略认识	可靠可追溯、智能合约	控制货币供应量、控制货币流向、精确把握整个经济体系货币分布；央行发行的数字货币也能将国家关于货币发行的法律内嵌其中（如货币主义者的一些理念）	英国央行、欧洲央行、中国央行、日本金融厅、巴巴多斯
支付与清算	跨境支付	跨境支付网络是分散和孤立的，支付网络之间缺乏通用信任机制，造成了高成本、漫长的结算时间以及较差的客户体验	去中心化信任、智能合约	实时跨境支付、大幅降低成本、提升安全性	Ripple、SWIFT、Align Commerce、Circle
	银行间清算	银行之间，特别是跨境银行之间缺乏权威的信任机构或者清算效率低下	去中心化信任	引入联盟链，共识机制作为强信任主体大幅提高清算效率	R3CEV
金融资产发行与交易	区域股权证券发行	区域 OTC 市场证券发行透明度差，加之交易流程复杂造成流动性差	可靠可追溯、去中心化信任	用户可自主发行股份，并基于区块链自主交易，整个过程可以做到完全透明	纳斯达克 Linq、Chain
	金融资产交易	流程复杂、清算效率低下、造假风险	去中心化信任、智能合约	交易即清算，方便地实现复合式交易	DAH、Chain

	票据交易	全国性市场缺失, 供需对接不畅; 票据涉及的多个环节独立风控, 成本高且难以杜绝虚假交易	可靠可追溯、智能合约	可靠可追溯, 杜绝虚假票据; 区块链技术构建无限扩展的市场; 和交易关联的智能合约降低交易成本; 可追溯特征便于了解票据来龙去脉	R3 CEV
内部流程优化与审计	银行等复杂机构内部流程	银行业务繁杂, 很多环节不能做到绝对可靠, 只能通过复杂的授权机制降低风险, 导致业务效率低下	可靠可追溯, 去中心化信任	区块链能确保记录可靠可追溯; 高可靠性使得人工验证环节可大大减少, 提高效率; 去中心化信任使得对单个节点和人员可靠性依赖度大幅降低	巴克莱、高盛、花旗、汇丰、摩根大通、瑞银集团
	公司审计	采用抽样方式审计企业业务耗时费力, 效率低下	可靠可追溯	区块链技术自带的可追溯性特征显著提高账目的课审计性	德勤
权属证明与交易	数字知识产权登记与智能交易	由于具有拷贝特征, 具有知识产权的数字作品技术过关而经济的版权保护手段乏善可陈, 特别是单价相对较低的作品(如个人在网络上发布的摄影作品)	可靠可追溯、智能合约	数字产品哈希值+时间戳完美解决归属问题, 嵌入智能合约可无缝对接各种形式的交易	Mediachain、Ascribe
	不动产登记	一些政府部门处理能力差, 不够重视, 存在丢失可能; 为防止差错, 引入复杂的处理流程, 效率低下; 质押转让极不方便	可靠可追溯、智能合约	快速登记, 可靠记录, 智能合约属性使其质押转让及其他复杂操作极其方便	Factom
自组织物联网		维护成本过高、可靠性不足、中心节点脆弱、物联网设备之间价值交换缺失	可靠、去中心化信任、智能合约	去中心化稳健的物联网大幅降低维护成本, 通过智能合约实现物联网设备间的完全自治	IBM、Slock

资料来源: 互联网, 长江证券研究所

技术有望持续突破，应用逐步落地

技术有望持续突破，央行关注提升

区块链技术尚处于早期探索阶段，在实际应用中存在较多不足，我们认为区块链膨胀、记录低效率、复杂项目开发缓慢和标准缺失是在现阶段较为突出的问题。

- **区块链膨胀：**区块链的机制使得每一个交易都需要完整的记录下来，随着时间的推移，存储的数据会越来越大。而且，区块链网络中每一个节点都要保存完整的区块链数据库，整个网络中数据存储量巨大，带来极大的成本开支。如比特币交易记录，在2016年一月的时候已经达到53GB，若区块扩容将导致更快的膨胀速度，此外海量的存储也可能带来搜索的低效率。
- **记录生成的低效率：**在区块链网络中每一笔交易发生时通知所有节点，在需要把一段时间的交易记录下来时首先要通过一定的共识机制选择一个记账者，然后把记录的结果发送到每一个节点确认，这样能保证新的区块的可靠性，但也带来了较低的效率。
- **项目开发难度大：**区块链开发还没有成熟的平台，一个新的区块链的应用基本要从头开始搭建，而且区块链应用需要IT人员、行业专家协作，使得开发和优化效率低下。
- **缺乏统一标准：**目前，关于区块链的技术优劣还没有达成共识，基本规范还缺乏统一的标准，导致整个应用开发领域较为混乱，增加了开发和应用的难度。

虽然存在各种大大小小的问题，但我们认为区块链技术会呈现快速进步趋势，一批小范围的应用有望在近两年推出，五年内某些项目达到商业推广阶段。在此过程中，共识机制和算法的创新将带来效率的突破式提升；去中心化理念和中心化的平衡有助于记账效率的提升和应用的快速落地；平台化、云计算降低开发成本、带来更快的开发速度，技术瓶颈将逐步突破。而在政府态度方面，也有望迎来持续改善的监管环境，促进区块链技术的落地。

共识机制和算法持续创新

在以比特币为代表的公有链中，其记账人的选择采用POW机制，并被认为是去中心化的核心保证，然而记录生成的效率较低；点点币采用POW+POS机制，记账成本下降，效率大幅提升；比特股DPOS机制、以太坊的POA机制、摩根大通在超级账本项目上推出Juno原型、英特尔PoET和Quorum Voting机制等都有不同程度的创新，后续新的突破值得期待。机制的持续改进将带来记账效率的提高。在存储内容方面，不降低安全可靠前提下某种形式的精简算法及存储压缩算法的突破则有望逐步解决区块链膨胀问题。

中心化和去中心化寻求平衡

区块链衍生于比特币，而中本聪设计的比特币是采用的完全去中心化理念，所以在一些早期的区块链尝试中记录和存储也采用完全去中心化，区块链甚至被一部分人贴上完全去中心化的标签。随着认识的深入，业界有了新的认识：去中心化的实现并不依赖于大量的节点，只有每个节点拥有独立的记录和验证权，并且有一种合理的机制使得这些节点合谋作弊不能实现或成本不可承受即可。所以，在联盟链中，去中心化容易实现；在

私有链中，节点的独立性主要用于保证系统的高可靠性；在大部分公有链中，也不需要所有节点都参与记录和记过保存即可达到去中心化的效果。在各个应用场景中，去中心化和中心化不同程度的平衡有助于应用的快速落地。

平台化趋势助力应用快速开发

区块链涉及较多技术，从 0 开始研究和开发区块链并非易事。利用现成的区块链平台或区块链公有云作为开发和测试环境可减少底层开发所需要的大量的软硬件投入、资金投入，从而将开发重点聚焦于应用本身。类似 PC、智能手机应用的快速丰富离不开高效的开发平台，目前区块链的开发平台正逐步形成，为区块链应用的丰富奠定基础。平台开发难度大，对技术实力要求极高，一般需要业内巨头和具有强大技术创新基因的公司参与，IBM 的超级账本、微软及万象区块链实验室的 BAAS (Blockchain as a service)、以太坊智能合约平台等项目快速推进使区块链平台出现了从无到有的飞跃，平台推进的标准出台、共识机制和算法的突破、功能的强化和接口的丰富将助力区块链应用的加速落地。我们认为随着平台的成熟，区块链落地项目的数量和质量有望迎来新的阶段。

表 6: 区块链开发平台逐步丰富

时间	参与公司	平台概况	合作对象/应用案例
2014 年	以太坊	提供智能合约开发平台，目前基于以太坊的智能合约应用快速增加	KYC-Chain、Eth-Tweet、WeiFund
2015 年 11 月	微软	与 ConsenSys 达成合作，在其 Azure 环境里面提供 Ethereum 区块链即服务 (EBaaS)，该服务将让客户和合作伙伴能够在一种现成的开发/测试/生产环境下试用、学习和快速开发，成本低廉。2016 年 4 月，与 R3 联盟结成合作伙伴，帮助分布式总帐在 R3 成员当中的推广	R3CEV、Ripple、Factom
2016 年 2 月	IBM	合作推出“开放账本项目” (Open Ledger Project)，开发企业级的区块链软件结构，推动区块链技术的商用，通过 IBM 云计算平台的 Bluemix 和 API 基础架构来支持外部数据的对接。可使用 IBM 在 Bluemix 上可用的新的区块链服务，开发人员就可以访问完全集成的开发运维工具，在云端创建、部署、运行和监控区块链应用	-
2016 年 3 月	万向集团	提供的 BaaS (Blockchain as a Service) 平台为区块链技术的开发和应用提供了便捷的路径。提供便捷的 BaaS 服务，致力于降低区块链开发门槛、减少开发者重复性工作，为区块链创业公司降低开发与部署成本。目前支持 Bitcoin Blockchain、Ethereum Blockchain 以及 Factom，未来将会接入更多的区块链开发环境	以太坊、Factom

2016年4月	英特尔	平台由‘交易家族’执行数据模式和交易语言，以反映账本用户的需求。该系统使用了两种共识机制，PoET 和 Quorum Voting，目前该项目还在试验阶段	超级账本参与者、推出梦幻体育市场游戏 (fantasy sports marketplace game)
2016年5月	亚马逊	与 Digital Currency Group (DCG) 合作，向 DCG 投资的公司提供区块链即服务，想众多区块链公司提供高集成度的区块链开发测试环境	与区块链投资公司 DCG 合作

资料来源：互联网，长江证券研究所

区块链是分布式存储、加密算法等技术的创新组合，基础技术的创新、组合方式的创新都有助于区块链的发展。我们认为随着对区块链应用认识的深入，快速增加的研发的投入、IT 巨头的参与、初创公司的丰富，技术瓶颈将逐步突破，使区块链安全可追溯、去中心化信任、智能合约的特征应用于更加广阔的场景。

央行态度从谨慎到重视

在比特币发展早期，其背后的区块链技术的价值并没有为大家所认知，比特币作为一种脱离政府和监管的类货币形态受到了多个国家地区和央行的关注，虽然也有较为支持的态度，总体而言，在 2015 年以前，央行对比特币的风险和法律地位持谨慎态度，比特币不时受到监管风险的影响。

表 7：国家或地区对比特币的监管态度总体偏谨慎

国家或地区	监管态度
欧盟	评估比特币等类似的数字货币，是否会被用作恐怖主义和洗钱
美国	在 2013 年 11 月 18 日参议院听证会上，伯南克表示：美联储无权直接监管虚拟货币，认为比特币等虚拟货币拥有长远的未来，有朝一日或许能成为更快、更安全、更有效的支付体系
中国	曾两度下发防范比特币风险的通知，在 2014 年对以比特币为代表的数字货币进行了较为严格的监管，但是在 2015 年并未有进一步明确表态
中国香港	香港政府官方发表声明称“比特币对金融体系不构成显著威胁”，没有必要监管比特币
中国台湾	在比特币监管问题上保持中立
美国加州	2015 年 3 月，加州众议院批准了一项名为 AB 1326 的法案，要求以类似银行的监管方式对数字货币公司进行监管，例如比特币
俄罗斯	比特币兑换卢布者，可能判处四年有期徒刑 “俄罗斯央行已表示会采取反对的措施，将会把使用比特币视为不当的行为
厄瓜多尔	禁止比特币，建立国家数字货币
玻利维亚	禁止所有数字货币
德国	2013 年 8 月，承认比特币的合法地位，已经纳入国家监管体系，成为世界首个承认比特币合法地位的国家
加拿大	承认比特币的“货币地位”，世界首个比特币 ATM 机在温哥华投入使用
泰国	买卖比特币、用比特币买卖任何商品或服务，与泰国境外的任何人存在比特币的往来，在泰国都被视为非法

印度	相关机构表示，虚拟货币给监管、法律以及运营风险带来挑战，将继续关注比特币的发展
韩国	拒绝承认比特币的货币地位，比特币不是真正的投资，不会对比特币征收资本所得税
荷兰	发布声明警告比特币风险，质疑比特币存储无法保障，不是由政府 and 央行发行
以色列	不承认比特币为官方货币，但是政府正在考虑对比特币的盈利征税，认为比特币的赚钱者需要缴税

资料来源：互联网，长江证券研究所

随着区块链的价值得到越来越充分的认识，多个国家央行的态度开始出现逐步的转变。新加坡央行较早行动，其于 2015 年 7 月即出资支持一个基于区块链的记录系统项目，此后，俄罗斯央行、澳大利亚央行、英国央行、韩国央行等动作不断，2016 年 2 月，中国央行也提出区块链是数字货币一项可选技术。最近的 2016 年 6 月，国际货币基金组织、国际清算银行、包括美联储和中国央行在内的 90 个国家的央行及监管层代表在金融业政策挑战国际大会上对区块链进展表现出前所未有的关注，充分显示其对区块链技术可能的应用突破抱有厚望。

表 8: 多家央行或重要金融机构对区块链较为重视

时间	国家	区块链方面动作
2015 年 7 月	新加坡央行	出资支持一个基于区块链的记录系统项目
2015 年 9 月	俄罗斯央行	俄罗斯正在研究数字货币及比特币的区块链技术，将与支付公司 QIWI 合作，建立国家数字货币体系。俄罗斯已决定研究一个新的国家数字货币——BitRuble（比特卢布），可能由俄罗斯国家中央银行系统负责监管
2015 年 12 月	澳大利亚央行	澳大利亚中央银行——澳大利亚储备银行行长格伦·史蒂文斯（Glenn Stevens）表示支持澳大利亚国内银行对分布式总账技术（区块链技术）的探索，利用区块链技术的优势
2016 年 1 月	英国央行	英国央行（BoE）将制定基于英镑结算基础设施现代化发展蓝图，以满足分布式账本技术（DLT, Distributed ledger technology）和其他技术创新的需要。英国财政大臣表示，区块链将会帮助英国重新回到全球金融中心
2016 年 2 月	韩国央行	韩国银行（韩国央行）一份最新的报告中建议，央行需要监测区块链技术的发展，甚至需要对该项技术展开自己的研究
2016 年 2 月	中国央行	央行行长周小川表示数字货币终将取代纸币，区块链技术是一项可选的技术
2016 年 2 月	欧洲央行	欧洲央行（ECB）已经表示，它正在调查如何运用区块链技术，关于区块链技术如何运用于该地区的证券与支付结算系统，以及如何可以改善它们，央行正在研究区块链应用如何可以改善或阻碍这些市场的基础设施
2016 年 2 月	巴巴多斯	宣布正式发行基于区块链的法币
2016 年 2 月	日本金融厅	考虑将数字货币划入“具有货币功能”的类别
2016 年 3 月	荷兰央行	致力于开发名为“DNBCoin”的内部区块链货币，出于谨慎，暂没有具体说明其用途
2016 年 6 月		国际货币基金组织、美联储、国际清算银行及包括中国代表在内的来自 90 个国家的央行及监管层代表在美联储总部参加为期三天的金融业政

策挑战国际大会，区块链技术为最重要的议题之一

资料来源：互联网，长江证券研究所

非金融领域前景广阔，金融领域从低频细分突破 贯通技术、场景和法规，方能一显身手

区块链落地和发展需要技术方案能真正解决痛点；应用场景和商业模式带来有效需求；和现有法律法规和行业规则不发生冲突。考虑到目前区块链效率瓶颈还没有很好的解决方案，加之法律框架的影响，我们预计区块链技术有望率先在非金融领域取得大突破，对于金融领域，离散、流程复杂、获取信用成本高、非高频的应用场景应用也有望较快落地。中长期来看，去中心化的金融资产发行业务与交易系统、国家数字货币、物联网有望大展拳脚。

非金融领域具备广阔前景

金融行业一般具有高风险、对社会影响巨大的属性，因此各国行业普遍实行较为严格的监管。与金融领域相比，其他领域技术创新和对商业模式限制明显较少，监管相对宽松，价值转移在这些领域的传递也处于相对低频的状态，但这些场景也存在中心化信任不足和获得信任成本较高的现状，有可能成为区块链技术率先落地的沃土。

- 权属证明与交易：包括数字知识产权登记与基于智能合约的交易；不动产和其他权属登记及基于登记的证明；
- 自组织物联网：如车联网，医疗健康领域的联网设备；
- 存在性和公正性证明：如商品追踪与溯源，贵重物品认证。

金融领域从低频细分切入

区块链在金融领域有着丰富的应用场景，由于区块链存在的记账效率较低和监管因素，我们预计在金融领域其在非高频交易、监管相对宽松或不明确、痛点较多的领域有望获得突破，如跨境支付、银行间清算、区域股权市场等。

- 支付与清算：跨境支付与清算；银行间清算；场外市场交易清算；
- 金融资产发行与交易、区域股权市场股票发行、金融资产（票据）交易；
- 非央行数字货币：该领域区块链应用较多，一些技术创新和突破有可能在该领域发生，此外，从长期来看，一个稳定的非国家数字货币或有其存在的价值。

有望成为价值互联的基础框架

TCP/IP 协议开启了信息的去中心化传输，使信息的双向交互效率大幅提升，P2P 理念的蔓延衍生出 Airbnb、Uber 等众多新兴商业模式。区块链诞生标识网络空间价值去中心化传输成为可能，区块链理念的推广和技术的突破或将带来价值去中心化传输趋势的逐步兴盛，而区块链基本原理和理念则有望成为价值互联网的基础框架。

附录：比特币挖矿

比特币挖矿即比特币网络中的节点通过竞争获得记账权、并实现比特币收益的过程。

比特币“挖矿”算法大致流程如下：

第一步：找到区块版本号 version。

第二步：找到上一个区块的 hash 值：prev_hash。

第三步：输入记录交易的 hash 树的根节点 hash 值：root_hash。

第四步：更新的时间 :time。

第五步：全网当前难度 :difficulty

第六步：自己找一个随机数 random

把以上 6 个参数作为输入，做二次 SHA256 运算，形似于

SHA256(SHA256(version , prev_hash , root_hash , time , difficulty, random))

最终得到结果 result。最后把结果 result 提交给系统，有系统判断这个计算结果是否有效。若判定结果为有效，就产生了一个新的区块，并会告知全网。

表 9：比特币区块头结构

数据项	目的	更新时间	大小(字节)
Version 版本	确定区域版本号	更新软件后，它指定了一个新版本号	4
前一区块的 HASH 值	记录前一个区块的数据指纹	新的区块进来时	32
所有交易的 Merkle 根	记录新区块时间段内所有交易的数据指纹	接受到一个交易时	32
Time 时间戳	记录当前区块生成的时间。从 1970-01-01 00:00 UTC 开始到现在，以秒为单位的当前时间戳	实时更新	4
Bits 当前目标 HASH 值	记录当前区块的生成难度	挖矿难度调整时（两周一次）	4
Nonce 随机数	记录生成的哈希值对应的随机数，（从 0 开始的 32 位随机数）	产生 HASH 时 A(每次产生 HASH 随机数要增长)	4

资料来源：互联网，长江证券研究所

算法规定：一个新的区块的第一笔交易必须将 25 个比特币发到某个地址，当然这个地址肯定会设成挖矿人自己的比特币地址，从而获得系统的比特币奖励。系统是如何判断你的计算结果是有效的呢？系统获取你的计算结果 results，然后把计算结果与目标值 target 进行比较。当 results < target 时，系统判断你找到了正确值，从而生成区块。

系统根据全网的难度设置目标值 target，target 值越小难度越大。从而实现控制出块时间，让出块时间稳定在 10 分钟。

风险提示： 技术进步不及预期，监管不确定性加大，短期投资过热

投资评级说明

行业评级	报告发布日后的 12 个月内行业股票指数的涨跌幅度相对同期沪深 300 指数的涨跌幅为基准，投资建议的评级标准为：
看好：	相对表现优于市场
中性：	相对表现与市场持平
看淡：	相对表现弱于市场
公司评级	报告发布日后的 12 个月内公司的涨跌幅度相对同期沪深 300 指数的涨跌幅为基准，投资建议的评级标准为：
买入：	相对大盘涨幅大于 10%
增持：	相对大盘涨幅在 5%~10%之间
中性：	相对大盘涨幅在-5%~5%之间
减持：	相对大盘涨幅小于-5%
无投资评级：	由于我们无法获取必要的资料，或者公司面临无法预见结果的重大不确定性事件，或者其他原因，致使我们无法给出明确的投资评级。

联系我们

上海

浦东新区世纪大道 1589 号长泰国际金融大厦 21 楼 (200122)
电话：021-68751100 传真：021-68751151

武汉

武汉市新华路特 8 号长江证券大厦 11 楼 (430015)
传真：027-65799501

北京

西城区金融大街 17 号中国人寿中心 606 室 (100032)
传真：021-68751791

深圳

深圳市福田区福华一路 6 号免税商务大厦 18 楼 (518000)
传真：0755-82750808, 0755-82724740

重要声明

长江证券股份有限公司具有证券投资咨询业务资格，经营证券业务许可证编号：10060000。

本报告的作者是基于独立、客观、公正和审慎的原则制作本研究报告。本报告的信息均来源于公开资料，本公司对这些信息的准确性和完整性不作任何保证，也不保证所包含信息和建议不发生任何变更。本公司已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，不包含作者对证券价格涨跌或市场走势的确定性判断。报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可升可跌，过往表现不应作为日后的表现依据；在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告；本公司不保证本报告所含信息保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司及作者在自身所知范围内，与本报告中所评价或推荐的证券不存在法律法规要求披露或采取限制、静默措施的利益冲突。

本报告版权仅仅为本公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用须注明出处为长江证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。刊载或者转发本证券研究报告或者摘要的，应当注明本报告的发布人和发布日期，提示使用证券研究报告的风险。未经授权刊载或者转发本报告的，本公司将保留向其追究法律责任的权利。