主题策略

2016 年 03 月 22 日

区块链技术：颠覆式创新

——区块链和数字货币系列报告之一：入门指南（上）

相关研究

证券分析师
谢伟玉 A0230512070007
xiewy@swsresearch.com
王胜 A0230511060001
wangsheng@swsresearch.com
联系人
王洋阳
(8621)23297818×7386
wangyy2@swsresearch.com

本期投资提示：

- **区块链本质上是一个去中心化的巨大分布式账本数据库。**作为比特币的底层技术，区块链是一串使用密码学相关联所产生的数据块，每一个数据块中包含了多次比特币网络交易有效确认的信息。随着加密交易不断产生，矿工不断解密验证交易，创造新的区块来记录最新的交易，这个帐本就会一直增长和延长。新的区块按照时间顺序线性地被补充到原有的区块末端，就构成了区块链。区块链上保留有每个节点比特币的余额信息，并随着自身的延长向各个节点进行自动更新。

- **区块链技术具有多重优点，各种形式演变为其赋予颠覆式创新可能。**区块链具有分布式去中心化、去信任化、不可篡改、数码加密安全等特点，从而可解决“双花”和“拜占庭将军”问题。目前最大区块链比特币链存在费用增加、容量限制、确认时间变长、能耗走高的缺点。但例如 Ripple、以太坊等另类区块链，以及公共、私有、联盟链等多种形式的涌现将区块链在多领域造成颠覆式创新变成可能。

- **区块链技术在支付、智能合约、金融交易、物联网等多领域存在广大应用潜力。**支付方面，不同于传统“拉式”模式，区块链技术采用“推式”模式，大幅改善安全性，自动化强降低支付成本并缩短处理时间，去中心化开放特点有助于平台内创新。智能合约作为区块链延伸核心技术打开区块链各种领域互联智能的应用空间。金融交易领域，区块链技术可将结算审核时间从小时级降低至秒级，自动化强大幅降低中间成本，结合智能合约将数字证券自动发行交易变为可能。对于物联网，区块链技术在数量呈指数级增长的智能设备之间建立了低成本的互相直接沟通桥梁，同时又通过去中心化的共识机制提高系统的安全私密性。区块链叠加智能合约技术可将智能设备变成可以自我维护调节的独立个体，这些个体可在事先规定或植入的规则合约基础上执行类似和其他个体交换信息或核实身份等功能。

- **发达国家积极布局区块链，支付、金融交易、数据安全、物联网多点开花。**随着比特币的局限性开始显露，区块链技术结合智能合约的应用空间打开、优点开始展现，产业内投资重点已从比特币挖掘硬件转向区块链技术相关应用。目前最高估值区块链公司已超过 1 亿美元，且众多初创公司雄心勃勃正进行支付、交易、风控等多领域布局。金融机构例如高盛、花旗、纳斯达克等积极探索区块链在金融领域的应用，并大力布局金融交易清算相关区块链技术公司，先行者纳斯达克已开始利用区块链技术进行私有股权发行交易；物联网和网络安全相关公司则得到政府和大型机构投资者青睐；支付领域得到银行和电商的垂青。

- **中国相关机构产业内投资力度较小，后期有望突破。**我国过往相关投资较重视挖矿，以及报价等信息提供业务和咨询。有深入研究并有一定规模的应用项目比较匮乏。目前行业内开始呈现向区块链多元化应用和深度发展的发展投资趋势，但体量较小且缺乏大型金融机构政府支持。万向集团下的区块链实验室是少有的大型机构支撑的研发项目。随着央行对区块链重视加深以及来自国外最新科技进展的溢出效应，伴以区块链应用的更加成熟和可投资投标的增加，区块链有望成为“互联网+”后的下一个热捧对象。这将激发创业者和应用者的热情，从而形成我国区块链发展的良性循环。产业内动态值得跟踪关注。

主要风险：

- 区块链技术发展放缓
- 各国对区块链技术监管加严

申万宏源研究微信服务号

目 录

图表目录

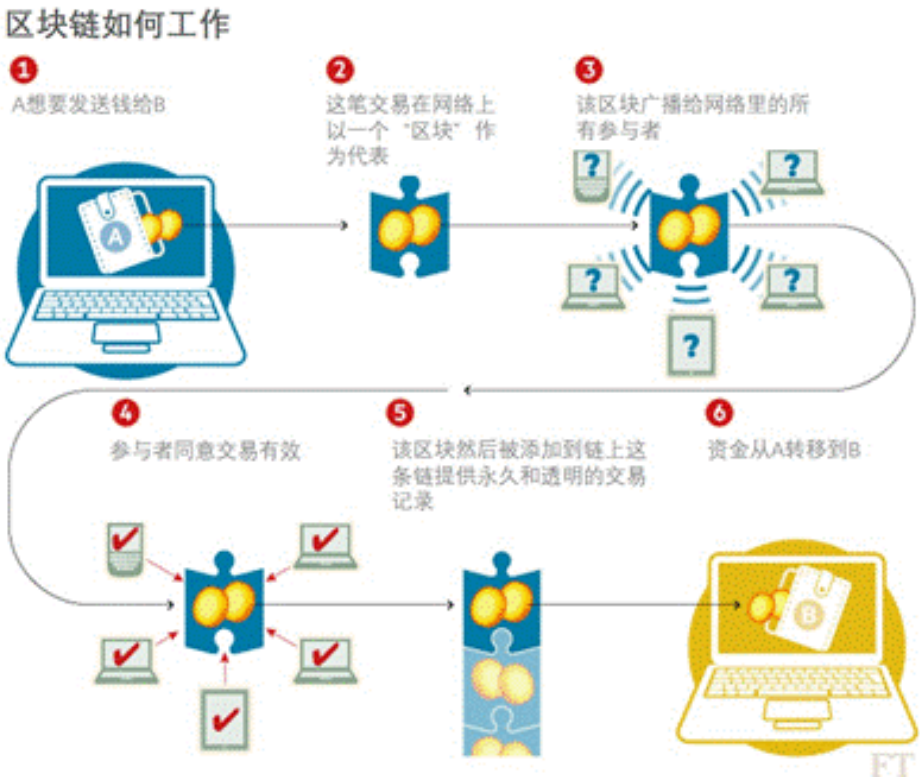
1.区块链：去中心化时代的新兴技术

1.1 区块链技术的工作原理

区块链本质上是一个去中心化的巨大账本数据库，作为比特币的底层技术，区块链是由一串使用密码学相关联所产生的数据块组成，每一个数据块中包含了多次比特币网络有效确认（一次有效交易检验被称为一次确认）的信息。随着交易不断产生，矿工不断验证交易创造新的区块来记录最新的交易，这个帐本会一直增长延长。这些区块按照时间顺序线性补充到原有的区块链上。每一个节点（每台通过钱包的客户端口连接到区块链网络上的电脑）都有一份完整的已有区块链备份记录，而这些都是通过进行数据验证算法解密的矿工网络自动完成。区块链上保留有所有关于每个节点和节点上比特币余额的信息，这些信息也被记录在完整的区块链上。公共式区块链帐本完全对外公开，这意味着区块链信息可以通过特定地址在区块链浏览器上（例如www.blockchain.info）进行查询。

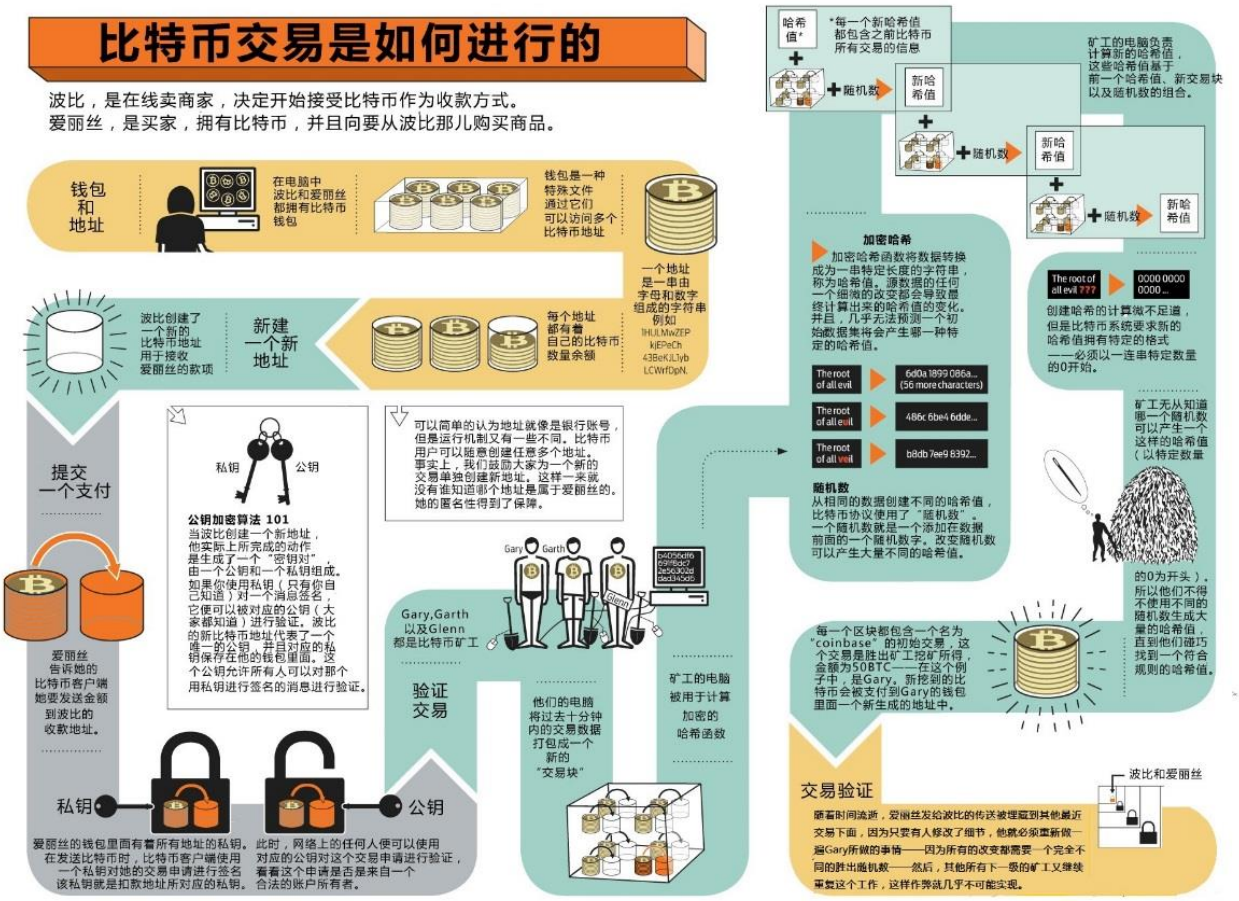
与其千言万语解释区块链的工作原理，不如几张流程图来的简单直接。下图用一个比特币交易的例子，系统性地说明了区块链技术的工作原理：

图 1：区块链交易的简易流程示意



资料来源： FT，申万宏源研究

图 2：比特币区块链交易的具体流程示意



资料来源：Karlssonwilker Inc.，申万宏源研究

1.2 区块链的技术特点

自 2009 年中本聪提出比特币概念，比特币起初因为其高度的隐蔽性和不可追踪性受到了“黑市丝绸之路”用户的青睐，后期又频繁被当作赎金来使用。虽然博得了眼球，但比特币至今仍没有成为一种主流货币，过高的波动性和各国监管层对其复杂的态度抑制了比特币的发展。但其背后的数据结构—区块链却得到了快速的的发展。作为一种基于开源软件和建构上的 P2P 网络，在和货币相关的例如交易支付等领域，相比传统网络的支持方式，区块链可以为这些领域带来多种优秀特点。**这些优点包括：去中心化、无须信任系统、去中介化、不可篡改、加密安全性。**这些优点的叠加可以解决两个长期存在于加密数字货币行业的问题：“双花”问题和“拜占庭”将军问题。

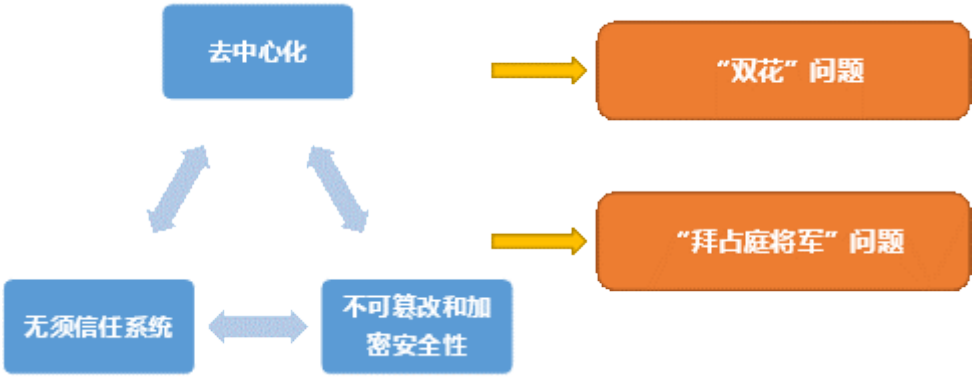
去中心化：区块链是一个由各矿工节点记账维持，并储存在全球范围内各个去中心化节点的公开账本，因为每个节点和矿工都必须遵循同一记账交易规则，而该规则基于密码算法而非信用，同时每笔交易需要网络内其他用户的批准，所以不需要一套第三方中介结构（比如说银行）或信任机构背书。在传统的中心化网络中，对一个中心节点（例如支付中介第三方）实行有效攻击即可破坏整个系统，而在一个去中心化

的例如区块链的网络中，攻击单个节点无法控制或破坏整个网络，掌握网内 50%的节点只是获得控制权的开始而已。

无须信任系统：区块链网络中，通过算法的自我约束，任何恶意欺骗系统的行为都会遭到其他节点的排斥和抑制，因此其不依赖中央权威机构支撑和信用背书。传统的信用背书网络系统中，参与人需要对于中央机构足够信任，随着参与网络人数增加，系统的安全性下降。与之相反，区块链网络中，参与人不需要对任何人信任，但随着参与节点增加，系统的安全性反而增加，同时数据内容可以做到完全公开。

不可篡改和加密安全性：区块链采取单向哈希算法，同时每个新产生的区块严格按照时间线形顺序推进，时间的不可逆性导致任何试图入侵篡改区块链内数据信息的行为很容易被追溯，导致被其他节点的排斥，从而限制了相关不法行为的产生和施行。

图 3：区块链解决了经典的“双花”和“拜占庭将军”问题



资料来源： 申万宏源研究

“双花”问题：加密数字货币和其他数字资产一样，如同可以将一个文件以附件形式保存并发送任意多次，具有无限可复制性的缺陷。如果没有一个中心化的机构，我们无法确认一笔数字现金或资产是否已经被花掉或提取。为了解决“双花”问题，可以信赖的第三方需要保留交易总帐从而保证每笔现金或资产只被花费或提取过一次。在区块链中，每一个区块都包含了上一个区块的哈希值，从创始区块开始连接到当前区块从而形成块链。每一个区块都要确保按照时间顺序在上个区块之后产生，否则前一个区块的哈希值是未知的。同时，由于区块链中所有交易都要进行对外广播，所以只有当包含在最新区块中的所有交易都是独一无二且之前从未发生过，其他节点才会认可该区块。因此在区块链中，“双花”变的非常困难。

“拜占庭将军”问题：拜占庭问题的核心问题是当战场上多个将军互相并不信任彼此（存在叛徒）时，互相相隔甚远无法碰头，但却要保证进攻时间一致，所以某种分布式远程协调沟通机制尤为重要。如果每个将军向其他九个将军派出一名信使，也就是 10 个将军每个派出了 9 名信使，即为总计 90 次的传输，每个将军会分别收到 9 条信息，可能每一封都附着不同的进攻时间。此外，部分将军会答应超过一个的攻击时间，故意背叛发起人，所以他们将重新广播超过一条的信息链。这个系统迅速变成不可靠信息和攻击时间相互矛盾的混合体。区块链通过为发送信息加入了成本，也

就是基于计算一个随机哈希算法得到遗传 64 位的随机数字和字母组成的字符串的“工作量证明”，并加入了一个随机元素以保证在一个时间只有一个将军可以进行广播，解决了这个问题。

在历经 5 年以上的发展后，目前比特币区块链为应用最广泛的数字货币区块链。截止至 2016 年 3 月，比特币区块链的市值已经达到了 62.9 亿美元并仍处于稳步增长的趋势中，较大的市值确保了其较充沛的流动性。但是如同各种新兴技术一样，比特币也面临着诸如挖矿费用不断增加、容量需不断膨胀但面临限制、更长的确认时间、越发高企的能量消耗等限制。

1．**费用增加**：虽然目前用户可以将信息保存到最小额的比特币交易中，但用户仍需向进行确认工作和交易打包进区块链的矿工交付交易费用。目前最少的交易费用是 0.0001BTC—大约 0.04 美元，其将随比特币价格上涨而增加，高频率的记录会大幅提高成本。

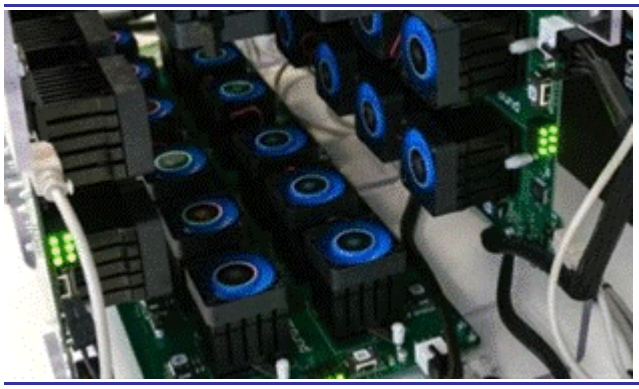
2．**容量限制**：比特币区块链设计之初人为将一个区块的容量设置为 1MB，而后期随着比特币发行量的增加和相关应用类型的增多，比特币区块链网络开始逐渐达到 1MB 的上限，交易开始时不时被迫推迟，扩容成为迫切的需求。近期，比特币核心开发者 Gavin Andresen 提出了最新的从 Bitcoin Core 切换至硬分叉链 Bitcoin XT 的区块扩容方案，将区块从 1MB 扩容至 8MB，之后每两年翻倍，而若要变动生效，需要 1000 个连续区块中的 750 个区块包含矿工的变更批准信息。比特币社区开始分裂。Andresen 提出，因为容量的限制，比特币的处理量太小，这样的限制会严重削弱比特币的未来扩展。目前，作为中国比特币社区中的代表性声音，中国三大比特币矿池 F2Pool、BTCChina Pool 和 Huobi Pool 针对 Andresen 的新方案采取等待跟随的策略。“关于 Gavin 的提议，我们将等待其他核心开发人员的看法。但我们肯定是不会切换到’Bitcoin’ XT 这种竞争币上的。如果我们这样做了，它会开启一个极坏的先例，无论你是谁，你不能制造一个新的币，并宣称它就是‘比特币’，因为你还没有得到其他核心开发者的同意”— F2Pool 的管理员如是说。后续事件如何发展，我们拭目以待。

3．**确认时间长**：目前比特币需要平均 10 分钟才能确认交易并将交易记录到区块链中。比特币网络每个区块只能容纳 4,096 笔交易，无法处理超过每秒 7 次的交易，相比于类似 Visa 这样每秒能够处理 2,000 笔交易、最多可以允许 10,000 笔每秒峰值交易的支付系统，显得力不从心。根本原因在于比特币区块链是通过工作量证明（Proof of Work）系统（POW）来确保系统的安全性和运作，而工作量证明的形式一般是让计算机来解决一个数学问题，当工作量达到峰值、计算机的极限又较固定时，运算时间会放缓。有时为了安全性，对于大额交易甚至要花费更长时间来处理，以抵御例如“双花”攻击带来的风险，而 VISA 只需要 1 秒。

4．**能量消耗高**：算力在比特币区块链的挖矿中尤其重要，早期估计全球比特币区块链网络每天在挖矿中花费 150 万美元，一年将近 5.3 亿美元。目前随着矿机算

力的提高，消耗的能量和金额水涨船高，根据 Coindesk 的测算，在全网算力达到 110,000,000GH/S 的今天，目前整个网络每日需要耗电 80,666 千瓦，相当于 707,120,500 千瓦时/年。按照每兆瓦 100 美元计算，这些电力一年需要消耗 7,071.2 万美元，而为了达到 110,000,000GH/S 的算力，大约需要 36,670 台海王星矿机(每台售价 9,995 美元)，如果一年需要更新支出 2 次，一年内算力投资的费用就需要 7.33 亿美元，所以一年下来总消耗将近 8 亿美元，同时整个网络会释放 42 万吨的二氧化碳。虽然相比黄金币制比特币能量消耗更低，相比信用纸币制更加安全，但如果比特币区块链希望得到更广普及达到更大规模，能量消耗是必须要克服的瓶颈。

图 4：海王星是全球主流的矿机之一



资料来源：KnCMiner，申万宏源研究

图 5：ASIMINER PRISMA，单机算力 1.4T，功耗 1050W，能量消耗不算低

资料来源：网络资料整理，申万宏源研究

图 6：位于香港的大规模矿场、定制的 ASIC 芯片被垂直摆放以用来集成挖矿

资料来源：网络资料整理，申万宏源研究

图 7：屋顶摆放的水冷散热系统，为室内芯片散热，矿主透露每个月支付电费达到约 5 万美元

资料来源：网络资料整理，申万宏源研究

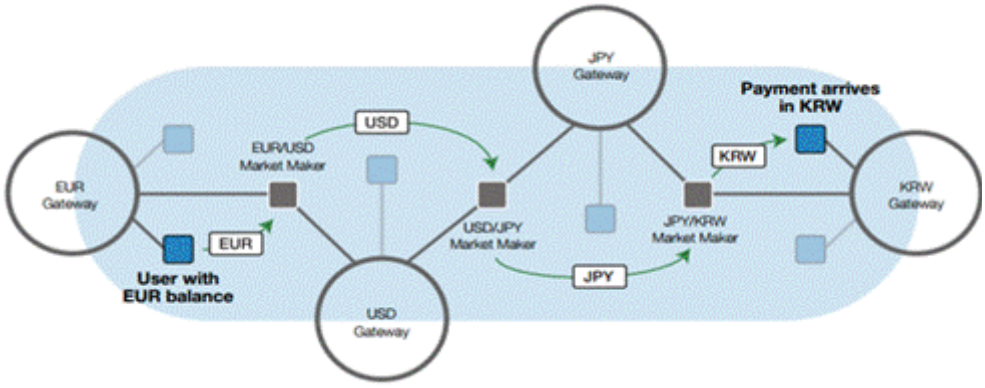
1.3 区块链技术目前已有多种策略演变

为了弥补比特币区块链存在的缺陷并在其基础上进行改进，多种另类区块链模式应运而生。这些区块链模式几乎完全独立于比特币区块链，并在诸如更快的交易时间、更大的交易容量、不同的节点共识机制、多等级匿名性和假名使用、更复杂的授权特征等方面有着一定的改善。目前行业内最重要的三个子区块链分别为另类区块链

(Alternative Blockchain)、彩色币区块链(Colored Coin Blockchain)、以及侧链（Sidechain）。

1. 另类区块链（竞争币）：另类区块链旨在利用区块链技术提供比特币以外的数字货币应用，例如瑞波（Ripple）币、狗币等等。这些另类区块链旨在改进比特币区块链所存在的问题或拓展比特币区块链的应用范围。

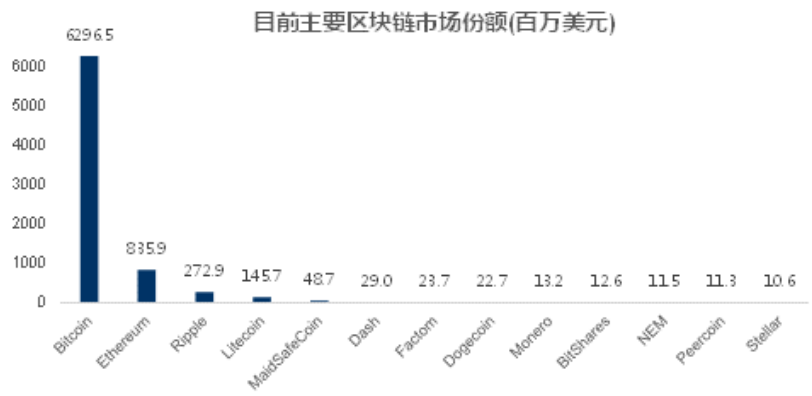
图 8：瑞波网络内的汇兑示例，瑞波的智能化可以帮助汇兑者找到最合适的汇兑路径，实现快速汇兑



资料来源：比特币之家，申万宏源研究

例如，作为世界上第一个开放的支付网络，Ripple 技术基于比特币区块链，但其体系目的又和比特币区块链有很大不同。**如果说比特币试图挑战的是国家的铸币权或各大央行的货币发行权，那么 Ripple 技术挑战的则是全球银行汇款和支付系统。**Ripple 系统中的核心是基于比特币区块链去中心化思想基础之上的 Ripple 支付协议，从而挑战传统的银行间 SWIFT 系统，造成颠覆。在 Ripple 系统中，比特币等虚拟货币、以及美元、欧元、人民币等实体货币皆可流通并受到系统支持。Ripple 币作为 Ripple 系统的载体，主要在两方面起到作用：（1）通过引入网关（Gateway）系统，Ripple 在自身网络中建造了资金进出的大门。类似于传统货币的存取和兑换机构，网关允许人们把法定货币或虚拟货币注入或抽离 Ripple 网络，并可以充当支付双方的桥梁。网关相当于 SWIFT 协议中的银行，使 Ripple 币之外的转帐可以在陌生人之间进行。由于 Ripple 协议的开源性，恶意攻击者可以制造大量的垃圾账目，导致网络速度严重下滑或瘫痪。为了防止此种类型状况的发生，Ripple Lab 要求每个 Ripple 网络上的账户都要至少有 20 个 Ripple 币，每进行一次交易即会销毁十万分之一个 Ripple 币。对于正常交易者来说，销毁额度非常小可以忽略不计，但对于制造大量虚假交易信息的恶意交易者来说，Ripple 币销毁量会呈指数性上升，同时成本将随之急速上升。（2）Ripple 币作为中介桥梁货币，可以成为各种货币兑换中的中间物，加快货币流通速度，降低流通难度。

图 9：比特币区块链目前处于大幅领先的地位

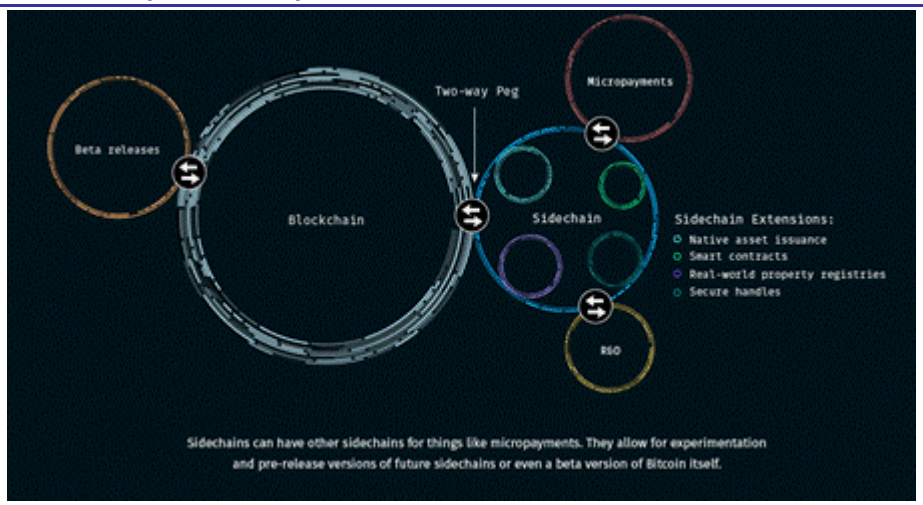


资料来源：比特币之家，申万宏源研究

以目前的情况来看，另类区块链目前的货币使用比较小众，其面临的最大问题是无法战胜比特币区块链自身强大的网络效应。鉴于比特币已成为了最大的区块链数字货币，众多区块链衍伸创新会倾向将比特币作为载体。同时，比特币区块链自身也存在后续变革，以吸收新兴另类区块链优点，同时改进自己的不足的可能。直至今日，尚未有一种另类区块链可以在规模、成交量等货币市场重要指标上和比特币区块链所抗衡。但是，例如 Ripple 和 Ethereum（以太坊）的创新性体系，将金融支付、汇率兑付、去中心化智能合约应用基于区块链上的改善变成了可能。其中以太坊作为后起之秀，其运营模式本文会在智能合约部分中做具体的描述。

2．彩色币：彩色币区块连旨在利用比特币区块链提供除数字货币以外其他类型资产的应用。这些其他类型的资产包括公司股权、债券、商品证书、智能财产、彩票等。彩色币的优点在于直接利用比特币区块链目前较佳的网络规模效应，在网络中可以直接完成存储、发行、或交易等行为，同时彩色币可以在未来直接受益于比特币区块链技术发展带来的各种技术突破。目前关于彩色币最大的质疑在于其会加大目前已承重负的比特币区块链的负担。

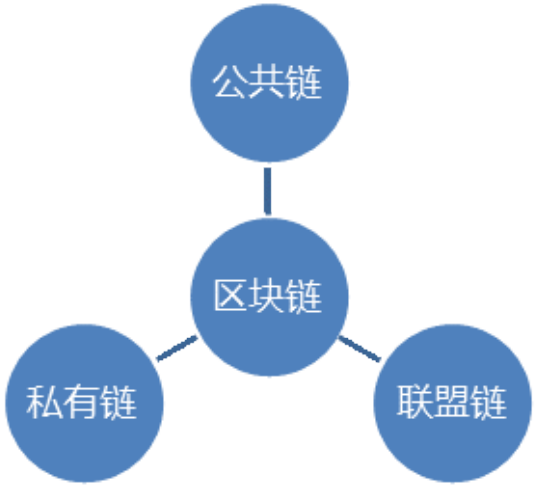
图 10：区块链(Blockchain)、侧链（Sidechain）之间联系的图解



资料来源：比特币之家，申万宏源研究

3．侧链：侧链旨在实现比特币和其他数字资产在多个区块链间的转移。由于目前比特币区块链的区块容量和传送运算速度都面临较大的挑战，侧链提供的双向挂钩如同一座桥梁，将比特币区块链以及其它区块链相互连接在一起，从而实现比特币的快速扩展。形象地说，比特币区块链和侧链之间的关系就如同黄金和和黄金挂钩的金本位货币之间的联系。同时，侧链为创新提供了更好的环境和更多的可能，创新者可以在侧链内进行基于比特币上的智能合约、智能商业模式等方面的创新，但不会影响到核心比特币区块链的关键代码和运营。如果侧链得到了快速的发展，其势必会对众多另类区块链（竞争币）造成较大的冲击。但是侧链若想取得和比特币区块链双向挂钩的联系，其必须要获得核心比特币区块链内超过 50%节点的认可。

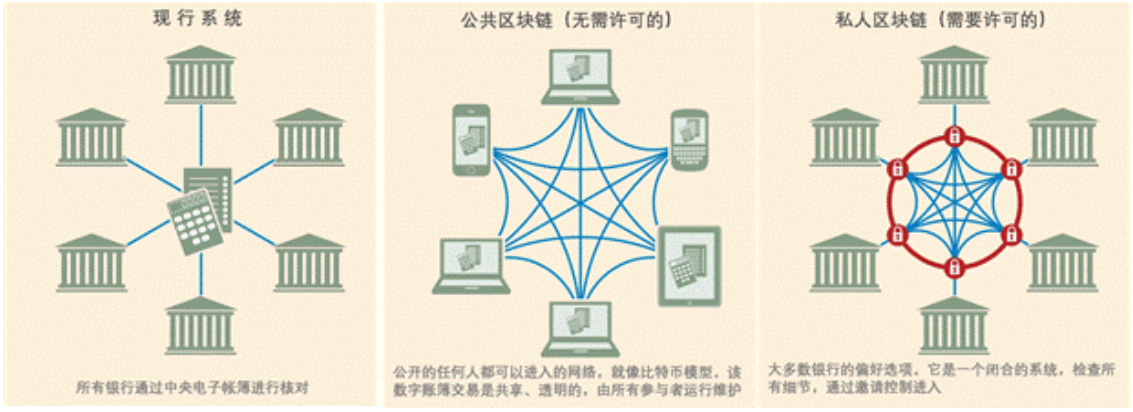
图 11：区块链部署方式分为公共链、私有链、联盟链三种



资料来源：申万宏源研究

除去另类区块链、彩色币、以及侧链，区块链领域同时还发生了部署方式上的革新。和完全开放、无许可必要的的比特币公共链（Public Blockchain）不同，联盟链和私有链在信息公开程度和中心控制力度方面有所限制，这些限制可以帮助区块链满足不同类型的应用需求。

图 12：私人区块链是大部分银行的偏好区块链选项



资料来源：FT，申万宏源研究

公共链：公共链是真正意义上的去中心化分布式区块链，系统安全性由工作量证明或权益证明机制来保证，容易进行应用程序部署，全球范围可以访问，不依赖于单

个公司或者辖区。公共链参与者往往匿名性强，任何参与者都可以在其中写入、读取、并参与交易验证，比特币区块链即是公共链最好代表。

联盟链：联盟链采取多中心式，参与成员为预先根据一定特征所设定（例如纳斯达克内的市场参与者，各券商的策略分析师等）。系统内交易确认的节点一般也是事先所设定，并通过共识机制确认。取决于联盟链内部的信任程度和相关需求程度，虚拟数字货币可以选择匿名或非匿名。联盟链容易进行控制权限设定，拥有更高的应用可扩展性，对于跨产业或跨国家的清算、结算、审计等有很大应用价值。联盟链可以大幅降低异地结算成本和时间，比现有的系统更简单，效率更高，同时继承去中心化的优点，减轻垄断压力。

私有链：私有链没有去中心，但具有分布式特点。中心控制者指定可以参与和进行交易验证成员的范围。对于私有链内的成员，系统不需虚拟货币提供奖励。私有链对公司政府内部的审计测试、以及同联盟内银行机构的交易结算有很大价值。

2.区块链在多个领域存在颠覆式应用价值

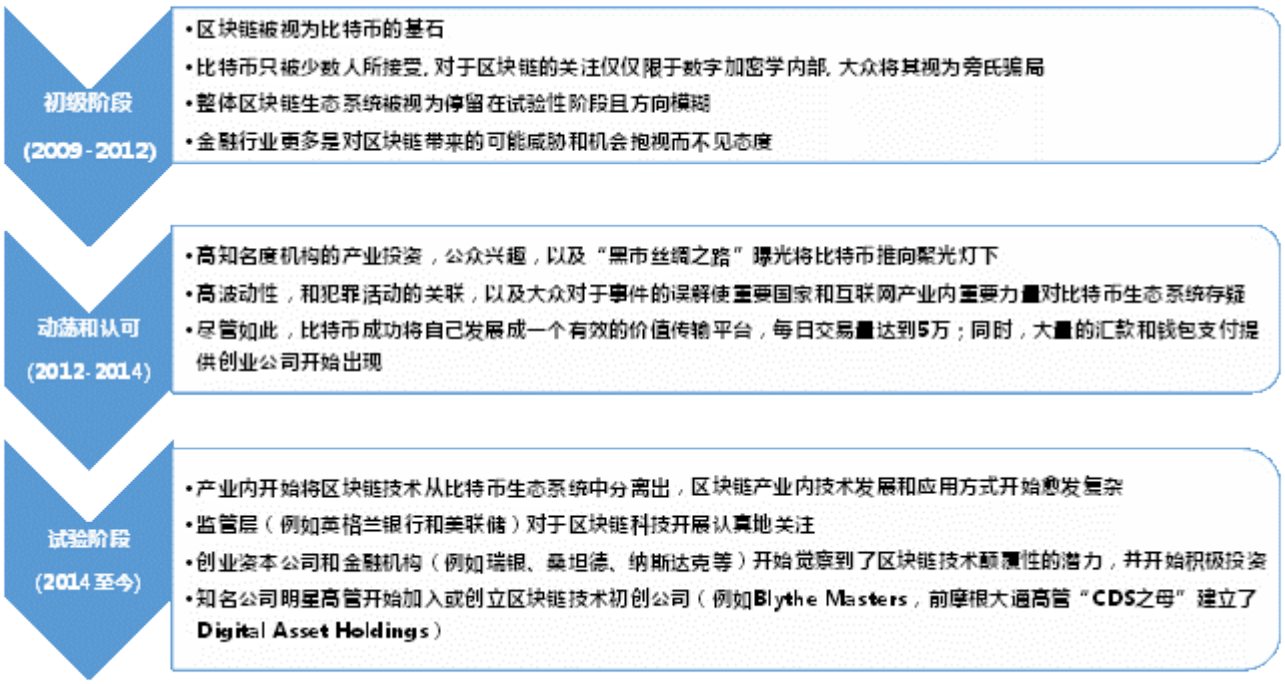
图 13：发达国家普遍对于比特币持较宽容的态度，但并非鼓励

资料来源： CoinDesk，申万宏源研究

经历多年的发展，区块链技术发展日新月异，区块链已经超越了数字货币领域，在多个方面都拓展出了其独特的应用价值，并且已经表现出了可以重塑社会各个方面及运作方式的潜力。根据区块链科学研究所(Institute for Blockchain Studies)创始人 Melanie Swan（梅兰妮.斯万）的观点，目前由区块链技术所带来的已有和将有的革新主要分为三类：区块链 1.0、2.0、以及 3.0。1.0 对应的是数字货币，这方面的应用和现金有关，包含例如货币转移、汇兑和支付系统等。2.0 对应的是智能合约，这方面的应用主要在经济、市场、金融领域等，但其可延伸范围比简单的现金转移要宽广，可以涵盖例如股票、债券、期货、贷款、按揭、产权、智能合约和智能合约等。

3.0 则对应的是超越货币、金融、市场以外的应用，主要在政府、健康、科学、文化和艺术方面。[1]

图 14：经历多年发展后产业已将关注从比特币等数字货币转移至区块链技术

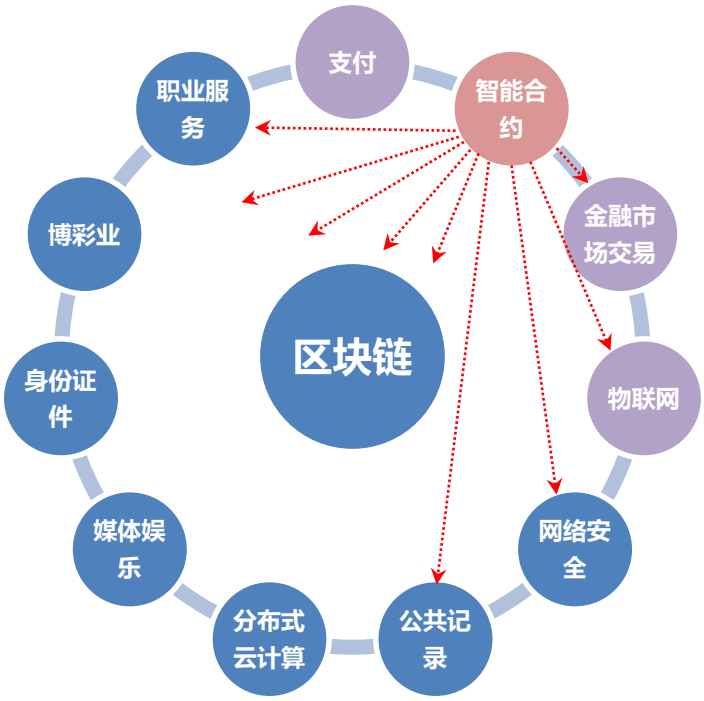


资料来源：麦肯锡咨询“Beyond the Hype: Blockchains in Capital Markets”，申万宏源研究

比特币所需颠覆的是央行的货币发行权和主权国家对货币的控制权，我们认为货币发行替代官方货币方面，比特币区块链会面临不可逾越的限制。同时因为隐蔽性强、不可追踪的特点，比特币往往和外汇转移、恐怖组织融资、逃税等有紧密联系。这种联系也让各国监管层对其颇为警惕。从创立初至今比特币持续的高波动性也不利于其成为一种稳定的储蓄性货币。但我们认为，基于比特币区块链上衍生出的货币转移、汇兑和支付等 1.0 技术，因为可以解决目前很多现有相关运营模式的痛点，会在政府监管下获得持续发展，甚至被政府所采用以提升效率。同时，各大咨询公司的分析和产业内投资的趋势表明，近年来产业内已经将区块链技术和比特币分离，投入了更加独立的关注、分析、发展、和推广。智能合约相关技术的发展更是迅速，成为了业内公认区块链通往未来颠覆性创新的钥匙。**区块链 2.0 应用的核心在于智能合约**，随着智能合约的发展加快，区块链技术在物联网、金融市场交易、网络安全、公共记录、金融市场等多个领域会大显身手，改进目前各个领域的服务流程，甚至颠覆这些行业内的传统商业模式。每一个领域区块链的应用方式和产业趋势都值得一篇深度分析的研报，在此我们先就**支付、智能合约、金融市场交易、物联网四大重要应用**做一下简短的介绍。

图 15：区块链应用广泛，多方面前景广阔，智能合约是关键

[1] 梅兰妮斯万，《区块链：新经济蓝图及导读》。



资料来源：申万宏源研究

表 1：超越货币领域的部分区块链应用

分类	实例
一般	托管交易、保税合同、第三方仲裁、多方签名交易
金融交易	股票、私募股权、集资、债券、共同基金、衍生工具、年金、养老金
公共交易	土地和产权证、车辆登记、营业执照、结婚证、死亡证
证件	驾驶证、身份证、护照、选民登记
私人记录	借据、贷款合同、投注、签名、遗嘱、信托、中介
证明	保险证明、权属证明、公证文件
实物资产	家宅、酒店客房、汽车租赁、汽车使用
无形资产	专利、商标、版权、保留权益、域名

资料来源：Ledra Capital Mega Master，《区块链，新经济蓝图导读》，申万宏源研究

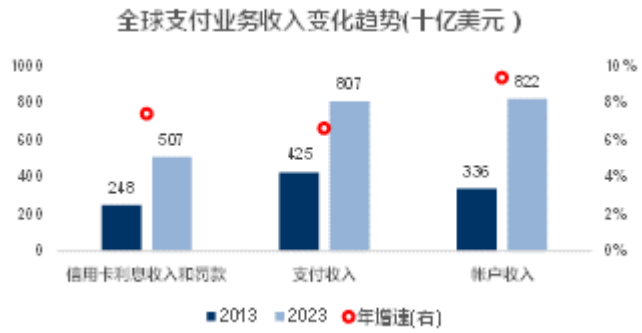
2.1 基于区块链的支付系统更快、更安全、性价比更高

根据波士顿咨询(BCG)的统计，在 2013 年，支付业务收入达到 4,250 亿美元，而到 2023 年，全球支付业务收入预计将会达到 8,070 亿美元。基于区块链技术的汇兑和支付属于区块链的 1.0 应用版。**区块链技术可以在安全性、交易时间、消耗费用上对传统支付业务进行颠覆式改进。**自从区块链技术推出以来，平均每日的交易数量、金额总量、以及平均每笔金额皆稳步大幅上升，从运营能力上证明了其替代现有传统支付业务的能力。

安全性上，基于区块链技术的支付系统采用的是分布式“推式（Push）”支付，而非传统的集中式“拉式（Pull）”支付。“推式”支付中，用户将付款金额发送至商家，过程中不用提供自己的私人银行帐户信息。而传统“拉式”支付中，用户将私

人银行帐号等信息提供给商家，商家在过程中保存用户的私人银行帐号信息并使用信息完成提款。“拉式”支付中商家积累的用户银行帐号和交易信息极易成为黑客和不法分子供给窃取的目标。**因此，对于用户，基于区块链技术的支付系统可以大大改善网络商业环境的安全性。**

图 16：全球支付市场成长迅速，潜力巨大



资料来源：申万宏源研究，BCG

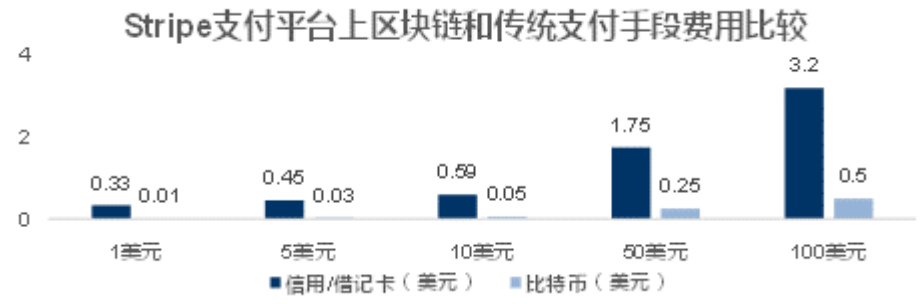
图 17：但随之而来的信息盗窃风险越发严重

公司	受影响卡数（百万张）
Home Depot	56
Target	40
Michael's	2.6

资料来源：申万宏源研究，网络资料整理

近期宣布进入中国市场的 Apple Pay 和海外得到广泛应用的 Google Pay 以及 PayPal 在安全性上无疑走在了电子支付系统的前列。和区块链系统类似，Apple Pay 和 Google Pay 并未采用传统“拉式”支付方式，用户不用将个人银行帐号信息等提供给商家，但和区块链技术不同的是，Apple Pay、Google Pay、Paypal 是将用户金融信息保存在自身系统内，每个用户的信息对应了一个加密的令牌，而该令牌在每次交易后自动作废，新令牌重新被系统加密。虽然这种支付方式避免了交易方卖家存储个人金融信息的可能性，并大幅降低了信息被盗窃的可能性，但相比区块链系统，核心风险仍存—也就是 Apple，Google，以及 PayPal 这些第三方其本身，一旦对于这些第三方的信息窃取攻击成功，后果将会更加不可设想。

图 18：比特币区块链在支付新秀 Stripe 平台上性价比优势尽显



资料来源：Stripe，申万宏源研究

对于商家来说，基于区块链技术的支付系统可以大幅帮助他们降低交易成本。相比传统的信用卡/借记卡，区块链技术可以帮助商家节省约 80%到 90%的交易费用。目前的信用卡/借记卡每笔交易商家手续费通常是 3%，远高于几乎可以忽略不计的区块链技术支付系统手续费。例如，使用 Coinbase 提供区块链技术的美国的新兴急速上升支付公司 Stripe 对于常规付费方式一般会向商家在 30 美分的固定费用基础上另收交易额的 2.9%作为手续费，但是对于使用比特币的交易，100 万美元交易额之

内不收取手续费，100 万美元交易额作为门槛多出的部分收取 1%作为手续费。Stripe 之所以有降低费率的本钱，根本原因还是在于区块链技术中分布式算法不依赖第三中心方所带来的自动化成本优势。

相比传统支付方式，基于区块链技术的支付方式可以大大缩短支付时间。对于传统信用/借记卡交易来说，一天以上的处理时间非常常见，跨境支付更是需要两三天的时间。而区块链支付短则几秒，长也不过几个小时的速度对于交易双方的吸引力明显。处理时间的缩短对于某些特殊交易类型有着不一般的意义。对于大笔跨境支付来说，传统交易中所需要的两三天处理时间，实际上是让交易金额在一段时间内被迫处于了冷冻的状态。对于公司之间的大宗交易来说，两三天的投资机会成本是巨大的，区块链技术因为其更短的处理时间，可以将机会成本大大降低。同时，更快的处理也降低了交易时间拉长存在的风险。此外，处理速度的提升还可以造成跨境支付的竞争局面，将现有的传统技术中交易成本降低，造成正面外部效应。

区块链技术可以让支付交易变的更加“碎片化”，从而达到满足用户日益灵活的付费需求。传统的支付（尤其是跨境支付）因为一般所需的手续成本较固定，支付金额降低时，边际平均成本迅速上升。基于区块链技术的支付方式固定手续成本低，可以满足更低、更碎片化的支付金额。同时，区块链和网络可以紧密结合的特点，或会颠覆现有众多网络商业的模式。例如，未来视频网站或会打破“试看-订阅”的模式，而利用区块链支付技术根据用户实际观看流量进行实时推进式收费。用户在观影的过程中，所需付金额直接挂钩流量。通过这种方式，视频公司可以捕捉到处于初次浏览但不愿订阅（价格弹性高）和死忠订阅用户（价格弹性低）之间的中性用户，同时给客户更好的性价比体验。此外，**区块链去中心化，开放的特点有助于更多平台内的创新，进一步提升支付效率。**

2.2 区块链智能合约技术打开应用空间

作为“去中心化应用”的基本构件，智能合约（smart contract）是一个包含价值，当特定条件满足会被自动打开的加密“箱子”。合约中包含的商业逻辑在区块链云上（不需要服务器）执行，在多方之间自动执行给定协议的条款。在区块链的环境中，合约或智能合约的发展意味着区块链交易将远不局限于简单的买卖货币这些交易，更加广泛的指令可以嵌入到区块链中，当预先设定的条件被满足后，指令就自动会被系统执行。同样是双方同意或不同意做某事，智能合约的特点就是，协议双方无需再事先信任彼此，这是因为智能合约不仅是由代码来进行定义，同时也是由代码所强制执行。智能合约可以如此操作主要是因为三点：自治、自足、和去中心化。自治指的是合约一旦启动后就运行，不需要发起者做任何干预。其次，智能合约可以自主获得资源，通过提供服务或发行资产来获得资金，以备不时之需。同时智能合约并不依赖某个单中心化的服务器，而是采用分布式网络节点来自动运行，规避了第三方操纵风险。

最简单的一个智能合约的例子可以用自动贩卖售货机来说明，当用户塞钱进入机器并做出对应选择后，被选择的物品会自动弹出同时根据情况找零。基于区块链技术上的智能合约可以大大降低合约“创造-执行-强迫实施”流程中所需要的人力资源（例如律师和会计等），降低成本的同时，可以提升执行和强迫实施的效率。

以太坊于2015年7月上线以来的迅速崛起是基于区块链技术上进行智能合约应用开启无限可能性的代表案例。作为另类区块链中的优秀改进，以太坊致力于打造一个提供超强图灵完备脚本语言的优秀底层协议。在该协议的基础上，用户可以创建任意的高级智能合约、众筹协议、货币、投票、公司管理或其他去中心化应用。以太坊的设计遵循简洁、通用、模块化、无歧视原则。简洁方面，以太坊运行速度快，每个区块产生时间只需17秒，大幅领先比特币所需的10分钟，而且每个区块没有尺寸限制，更加灵活，对于并行处理的支持可以保证后期运算交易速度的持续性提升。以太坊采用权益证明以替代传统比特币区块链采用的工作量证明，克服了比特币区块链中容易逼近运算峰值后系统速度下降的缺点。权益证明中，系统根据每个节点持有的虚拟货币数量进行交易确认，而非采用竞争性节点（矿工）工作量验证。通用性方面，以太坊包容系统内编程，以支持系统内智能合约的生成。模块化方面，以太坊的不同部分被设计为尽可能模块化和可分的，在开发过程中可以让协议端做小幅改动的同时应用层却可以不加改动地继续正常运行。无歧视原则上，图灵完备保证协议不会主动试图限制或阻碍特定的目的或用法并反对特定的不受欢迎的应用。以太坊甚至支持一个无限循环脚本的运行，只要用户愿意为其支付按计算步骤计算的交易费用。和比特币区块链为造币而造币的模式不同，以太币扮演双重角色，为各种数字资产交易提供主要流动性，并提供了了支付交易费用的一种机制。

一个简单的例子可以展示不远的未来，带有智能合约的类以太坊区块链将如何改变我们的生活以及其将打开的市场空间潜力实为广大。近期，德国莱茵集团（RWE）建立了一个内部工作小组来评估如何通过区块链技术，降低有关能源传输的费用，以帮助企业削减成本。集团目前正在探讨利用区块链智能合约对用户进行认证和管理开票程序。公司准备在以太坊区块链上进行概念论证，并将充电站作为顾客认证点和付款处理点。在原型机上，用户通过在以太坊网络上生成智能合约，和充电站建立合同关系。充电前，用户在网上进行存款，在交易完成后存款会被扣除。用户按照充电过程中所消耗的电量进行相应付费，而非根据汽车与充电站连接的时间长短进行传统式付费。通过这次试验，集团试图论证用户使用小额交易可以节省开支，同时通过这种方式可以对电力进行更有效的部署。在这种商业模式下，用户将能够通过智能合约与机器直接签订合同，而非与人或者公司。

上述的事例只是近期众多相关应用的一项。智能合约和以太坊的崛起已经吸引了非技术人员的关注，主要即因其在各种经济领域的应用潜力，例如后文所要介绍的在金融市场和物联网上的应用。智能合约是打开区块链技术2.0应用空间的关键要素。下表罗列了智能合约的部分应用领域，供读者参考。

表 2：智能合约可以在多种场合得到应用

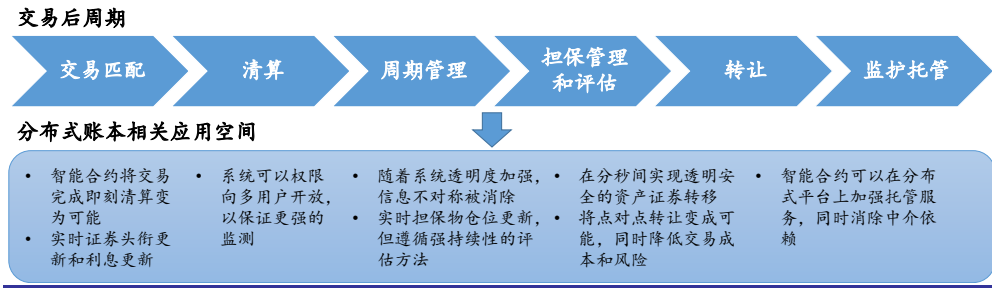
应用领域	具体内容
电子商务	智能合约的自动性和纪律性可以帮助加快网络上贸易和商务，同时凭借将人力介入程度最小化来减少交易成本
物联网	智能合约在机器间交流互联中可以起到关键作用，使得基于预定义标准上的机器自主互动变成可能。例如，在智能合约式的程序指引下，一辆自动无人驾驶汽车可以在乘客下车后自动支付停车费用。
权限控制	利用智能合约技术，在获得了付款后，离出租房屋很远的 Airbnb 房主可以给住户远程提供房屋的数码钥匙。同时房主可以利用智能合约技术设定数码钥匙的执行条件，如果用户滞留时间超过所付期限，数码钥匙会自动失效同时房屋内停止供电。
赌博业	基于区域区块链技术的赌场可以使用智能合约技术来根据赌局结果自动给赢家提供奖励，减少人工费用和错误几率。
遗产计划	生者可以将遗嘱以智能合约形式进行设计，在生者过世后自动给相关方根据先前设定的遗嘱进行财产分配。
数字资产	相关方可以利用智能合约来加速特定内容资产（例如艺术品）的传送和特许。

资料来源：网络资料整理，申万宏源研究

2.2 区块链技术可以全方位改善金融市场环境

除了为比特币数字货币提供交易平台以外，区块链技术可以大幅改善，甚至颠覆现有数字货币以外的各种资产交易系统，在例如金融衍生品、外汇、私人股权、能源信用挂钩投资品等资产的清算结算等交易后市场程序中大显身手。**区块链技术可以为这些市场程序带来更快的速度，更短的结算周期，更低价的费用，以及更强的安全性。**

图 19：区块链将全面提升金融市场交易后周期的效率

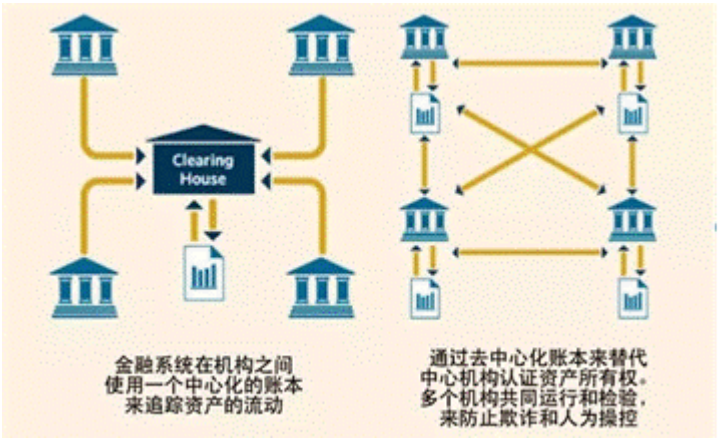


资料来源： Santander " The Fintech 2.0 Paper: Rebooting Financial Services"，申万宏源研究

（1）更快的速度方面，目前美国证券市场内普遍的结算审核所需时间是 2 到 3 天，区块链技术的应用有望将结算审核时间从小时级降低至分钟级、甚至是秒级，从而将结算风险降低 99%，同时降低资金成本和系统性风险。区块链中交易确认和结算为同时进行，节点交易受系统确认后自动写入分布式账本，并同时更新其他所有节点对应的分布式账本，自动化的运作机制可以大幅缩短结算所用周期。（2）更低的费用上，在目前的结算机制下，要想达到更短的结算周期，大幅增加的结算成本和初始投入开支是必须。根据美国托管信托和清算公司（DTCC）和波士顿咨询（BCG）

的测算，如果将美国证券市场内交易所结算常规周期从 T+3 变为 T+2，初始投资需要 5.5 亿美元，3 年的投资周期内部收益率为 18%。如果将结算周期从 T+3 变成 T+1，初始投资需要 17.7 亿美元，5 年的理想化（交易量持续增加）投资周期内部收益率为 14%。区块链技术的出现为更加效率快速缩减结算周期提供了可能。缩减交易中间程序方面，根据奥纬（Oliver Wyman）的估算，目前数字证券（例如 OTC 权益）全球每年交易流程各种中间人程序加总要浪费 650 到 800 亿美元，区块链可以大幅省去类似中间程序，从而节省大笔费用，而这笔巨额费用就是相关区块链产业的市场空间。（3）安全性方面，除了更快的处理速度，更短的清算周期降低了风险以外，区块链技术融入智能合约技术，可以程序化处理复杂的衍生品交易，将清算变的更为标准化、自动化。区块本身时间线形堆进的特点可以帮助监管层鉴别发现违规操作，同时智能合约可以将合规检查变自动化，从清算之初就将违规的可能性降为最低。区块链技术 24 小时不间断运转的特点也可以将泛州间交易所数据互换处理变得更为稳定和值得信赖。近日，韩国交易所（KRX）宣布将创建一个使用区块链技术的场外交易平台(OTC)，交易所代表称，“交易所希望这个系统有助于场外交易商节约成本和减少寻找交易对手的精力花费，从而让交易更便捷。”

图 20：区块链分布式的特点可以防止交易结算内的欺诈和人为操控



资料来源：FT，申万宏源研究

除了证券交易结算以外，区块链还可以用来注册并发行数字资产拥有权。目前，纳斯达克正在和 Chain 进行紧密的合作，利用区块链技术建设私有公司股权交易系统，发行和转移私有公司的股票份额。之所以选择从私有股权交易系统开始，主要是因为私有股权的发行和交易目前仍主要依赖于人工（律师）的手动处理（Excel），区块链技术可以大幅提升程序自动化。智能合约则可以将众多复杂的衍生品交易条款写入区块链技术支持的注册发行程序中，当交易发生时区块链网络可以迅速地进行正确执行。许多其他交易所，例如纳斯达克的竞争对手纽交所目前也对区块链技术表达出了浓厚的兴趣。“区块链技术，不断重新定义的不仅仅是发行交易领域的运作方式，同时还有整个全球金融经济体系。纳斯达克的目标是在这一转折点式的发展机遇中，充当重要角色”— 纳斯达克 CEO Bob Greifeld 如是说。2015 年 11 月，纳斯达克和 Chain 合作的区块链技术新项目 Linq 已利用基于区块链的发行交易平台完成了第一笔私募股权交易。

图 21：区块链技术可以有效提升发行交易效率

资料来源：财新观点，申万宏源研究

除了交易发行业务，区块链在会计的应用前景近期吸引了大量业内人士的关注。会计、审计和编纂对于全球企业和四大会计事务所成本巨大，基于区块链技术上的自动化会计可以大幅削减相关成本。公司不需要招聘专门审计人员来公司内部审核账本，所有交易可以集中记录储存在内部区块链，由于区块链具有不可逆性和时间邮戳功能，四大会计事务所等外部审计人员和监管机构通过跟踪这些区块链可以实时监控公司账本，同时机构可以借此大幅减少对于审计员审核金融交易的依赖，将审计业务变得更有效率。商业模式一旦有明朗趋势，产业内各种试验便迅速跟上。2015 年 7 月，德勤便透露其正在尝试将区块链技术应用到客户端的自动审核。至今，德勤已推出软件平台 Rubix，其允许客户基于区块链基础设施创建各种应用。德勤官网罗列了该软件的四个应用方面，其中包括实时审计功能、贸易合作伙伴关系跟踪、土地登记功能、以及忠诚度点数维护。同时，从审计延伸至外，德勤还看到了区块链技术在咨询方面的应用机会，通过 Rubix 平台，德勤有潜力通过 P2P 众包平台（公司以自由形式外包给非特定大众网络）提供大范围咨询服务。顾客可以在区块链上进行咨询，然后区块链可以针对顾客独特问题匹配合适公司来帮助解决问题。德勤先行，其竞争对手也不甘落后。今年 1 月，普华永道宣布公司组建了一个 15 人的区块链专家小组，为客户提供咨询服务，并计划在年底将队伍扩大到 40 人。

2.4 区块链技术让物联网更智能自主

物联网无疑是互联网技术的下一个大风口，近年来领域内迅猛的发展趋势反映了人们对于智能服务的需求，我们正在目睹亿万智能设备互联演变成千亿智能设备互联的过渡，迅速的发展对于智能设备的管理和运营水平提出了更高的要求。传统的中心式计算模式，例如云计算，在安全性、隐私保护、融通性等物联网重要属性方面可能并非最佳选择。目前智能设备之间的连接和计算基本上是基于对数据处理过程的信任（第三方），而随着智能设备数量呈现指数性增加，摆脱这种信任所带来的不确定性是必然趋势。**区块链对于物联网的最大意义在于在海量的智能设备之间建立了低成**

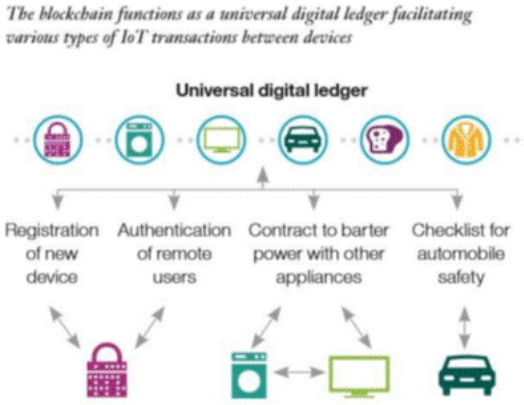
本的互相直接沟通的桥梁，同时又通过去中心化的共识机制提高了系统的安全性和私密性。同时基于区块链技术的智能合约技术又将智能设备变成了可以自我维护和调节的独立个体，这些个体可以在事先规定或植入的规则合约基础上执行类似和其他设备交换信息或核实身份等功能。

图 22：物联网领域的发展趋势，区块链主导的开放分布网络将成为未来趋势

资料来源：Veena Pureswaran and Paul Brody, Device Democracy, IBM Institute for Business Value，申万宏源研究

安全性和隐私保护强度方面，随着用户将汽车、手环、手机等数据节点完成相互连接，用户每日的起居行动产生大量数据。如果使用得当，这些数据为企业进行产品分析和性能改造，科研部门进行社会健康研究等正面效应活动提供了可能。但目前大量产生的数据为中心化系统或子中心储存，为不法分子、黑客、网络恶意攻击者等提供了集中窃取和攻击的可能。同时，由多个中心化系统组成的物联网错误成本偏高，随着连接中心的智能设备呈现指数增加，一个子中心系统数据处理的错误会导致所有其连接的智能设备数据出现错误。区块链散布式去中心化的特点可以大幅提升其系统内流通数据的安全性。从融通性角度来看，各个子中心系统也容易各自为营，在利用不同标准的情况下导致不同子中心数据之间的数据流通处理出现障碍。区块链系统则可以在相关问题上取得突破，让智能设备之间做到真正的互联互通。例如，设定好的智能合约可以让智能设备根据能耗分析，自动在网络内和其他智能设备进行交流，以重新分配能耗。

图 23：区块链技术在物联网领域的应用广泛



资料来源： Veena Pureswaran and Paul Brody, Device Democracy, IBM Institute for Business Valu，申万宏源研究

区块链技术也可以大幅改善物联网的操作完整性，提高智能设备的自主更正性抗御力。随着各种智能设备的智能程度越发提高，适用领域越发广泛，如果遭受网络攻击，设备或会做出和常规功能模式不同的行为，从而造成大程度危害。例如，在面临带有特定意图攻击时，你搭乘的智能汽车的刹车系统或会失灵、乘坐的飞机仪表可能会显示比你实际所处高度高出 1000 米的数据，你所处地区电站产生系统错误从而导致地区性电力瘫痪，你住所的安防系统或被远程解除。2010 年 6 月，震网（Stuxnet）病毒被首次检测出，作为第一个专门定向攻击真实世界中基础（能源）设施的蠕虫病毒，其引起了互联网安全专家和国家基础设施专家的高度重视和担忧。根据一位德国计算机高级顾问的表示，“震网”病毒让德黑兰核计划拖延了两年，此恶意软件 2010 年反复以伊朗核设施为目标，通过渗透入“Windows”系统，对其进行重新编程以破坏。基于区块链技术的安全公司 Guardtime 创建了无钥签名基础设置(KSI，Keyless Signature Infrastructure)，可以内置在工业级区块链中，对系统内任意数据或者全部数据进行签名，并且就历史上任一时间、地点和真实性进行独立验证。Guardtime 的首席技术官 Matthew Johnson 称，“Guardtime 可以持续监控平台的完整性，让那些对于管理软件访问权限操作者们可以实时观察系统全局，并且能够纠正未经批准的配置调整，这样可以确保没有恶意软件在应用程序中运行，以及让配置好的数据负责任的运行。”[2] Guardtime 对于物联网安全性的贡献已经获得了一定认可，为了避免类似德黑兰状况的发生，英国专注于智能城市创新的公司 Future Cities Catapult 已经和 Guardtime 签订合作协议，授权使其保护英国核电站、防洪系统和电网等基础设施免受网络攻击。近日，美国国防巨头洛克希德马丁和雷神也和 Guardtime 签订协议，确保其防御系统的操作完整性和抗攻击性。目前 Guardtime 已经在通信、国防、金融市场、保险、政府服务、数字营销方面取得应用进展。但 Guardtime 其实也只是众多物联网相关区块链技术公司的一家，市场广大，已吸引了诸如 IBM 的产业巨头积极布局，同时多家初创公司已经开始进行探索。

图 24：Guardtime 区块链技术已在通信、国防、金融市场、保险等六大方面提供物联网安全服务

电信
区块链支持的大数据安全系统可以帮助电信运营商在竞争中脱颖而出

国防
Guardtime为国防航天工业提供下一代防篡改硬件，并使用智能合约技术来帮助设备自动探测并抵御网络攻击

金融市场
Guardtime利用区块链合约技术可以减少先进技术支持的数据威胁，自动进行合规检查，探查数据污染并上传至云

保险公司
Guardtime利用区块链合约技术提供KSI解决方案，方案可以帮助保险公司提供更好的网络安全相关产品

智能政府
KSI技术使得政府内部知情人和外部监管审计人员都可以实时跟踪政府网络内情况，同时保证政府网络安全。这将提升政府的透明和可信度

数字营销
Guardtime提供的解决方案可以清除恶意软件，实时核实广告库存，利用区块链技术智能合约技术对广告数据实行收集，跟踪和分析，从而摆脱网页植入性Cookies

资料来源： Guardtime，申万宏源研究

[2] http://www.ibtimes.co.uk/uk-nuclear-power-plants-protected-cyberattack-by-guardtime-blockchain-technology-1533752.

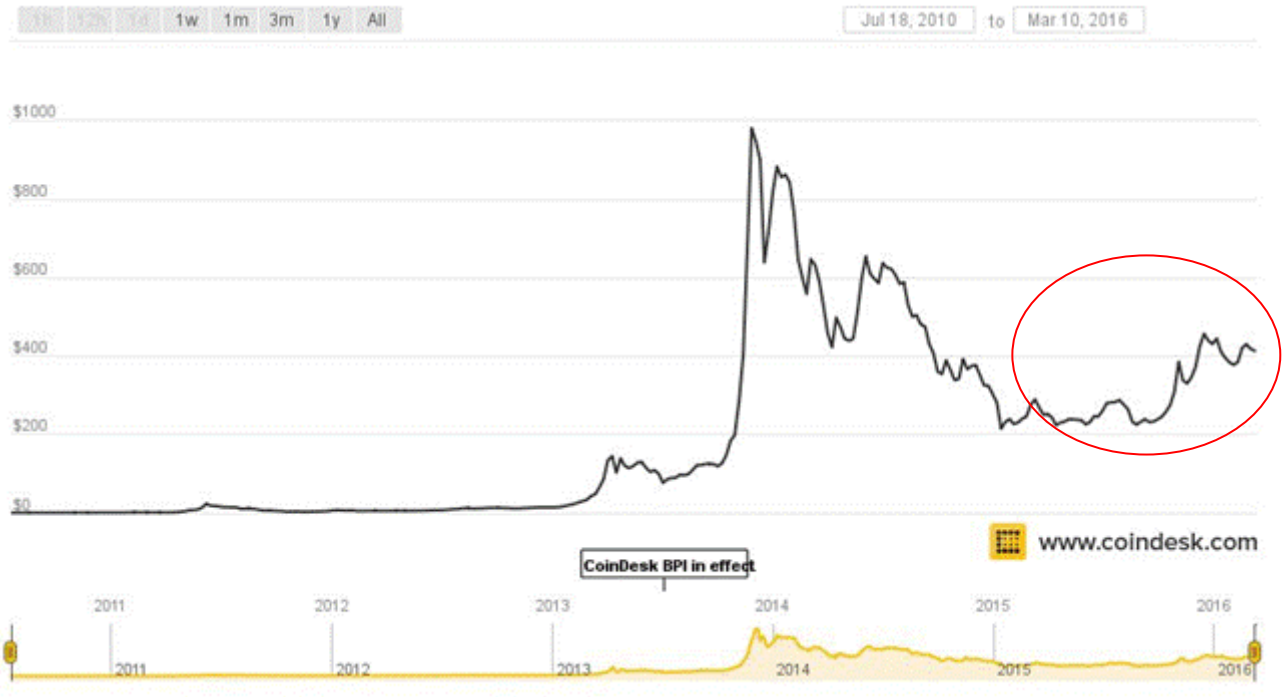
区块链技术可以提升物联网上各个节点设备运营的长久性。目前偏中心化的物联网顺利和持久运作对于各个中心节点（例如设备制造商、数据运营商等）其实是提出了较高要求。为了保持运作，各中心节点需要付出大量的营运费用，同时一旦中心节点不再运作或者退出市场，大量相关设备将面临瘫痪的局面，会给用户直接造成影响。大量营运费用的必要性也为试图进入物联网有潜力成为中心节点的公司创造了较高门槛，影响了网络内的创新活力速度。对于设备制造商来说，将物联运作外包给区块链网络可以减少运营的费用负担，从而将更多的精力放在产品本身创新上，同时提升运营持续性，有效增强用户信心。

3.区块链技术迎来拐点，产业内跃跃欲试

3.1 发达国家发展迅速多点开花

2015 年在区块链产业内标志着拐点。2015 年区块链内的交易量和交易地址数量开始大幅上升。同时，在经历了 2014 年的一路下跌后，受益于一系列利好比特币的政策或事件的发生，比特币价格也有所反转。相关事件包括（但不限于）：2014 年 10 月，纽约金融监管方面提出对于新成立的比特币公司给予宽松政策；2015 年 8 月，巴克莱银行成为英国首家接受比特币的银行；2015 年 11 月，巴巴多斯考虑添加比特币作为外汇储备；2015 年下半年人民币贬值导致部分人民币以比特币形式流出；2016 年 2 月，日本监管机构宣布考虑将把比特币视为法定货币；2016 年 3 月大型贵金属交易商 JM Bullion 开始支持比特币支付等。

图 25：近期比特币价格近日大幅上涨，反映了一系列的事件利好和区块链技术推进的溢出效应



资料来源：申万宏源研究，CoinDesk

图 26：区块链的平均每日交易数量大幅增加

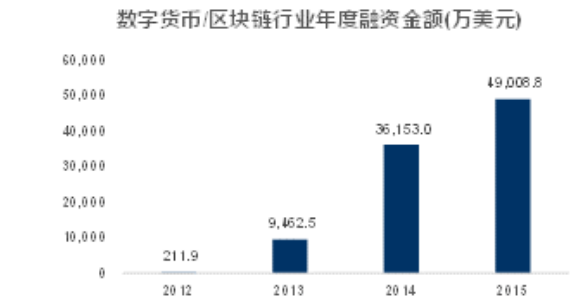
资料来源：blockchain.info，申万宏源研究，

图 27：区块链平均每日单一网络地址数量大幅增加

资料来源： blockchain.info，申万宏源研究

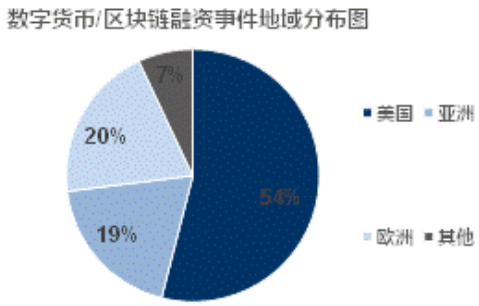
但我们需要注意的是，随着 2015 年产业内将区块链技术从比特币中抽离出来对待的趋势逐渐明显后，大量投资开始涌入区块链技术，区块链技术应用的广泛化和深入化，也间接促进了比特币的上涨。通过分析产业内投资方向，我们发现美欧日发达国家主导的区块链/数字货币投资中，挖矿类硬件造币投资比例大幅下降，交易所、智能合约商家应用等偏区块链技术应用投资比例大幅上升，资本的方向标明了产业内未来最明朗的方向。同时，用图灵完备脚本语言将智能合约和区块链技术整合的以太坊自 2015 年 7 月上线以来，吸引了大量创业公司项目在其平台上开发应用，呈现出爆发式增长，不到一年时间之内市值已经达到 10 亿美元，跻身于独角兽行列，并明显拉近了和比特币之间的差距。龙头公司之间竞争的进程也标明了产业内的发展趋势。

图 28：数字货币/区块链融资上升迅速



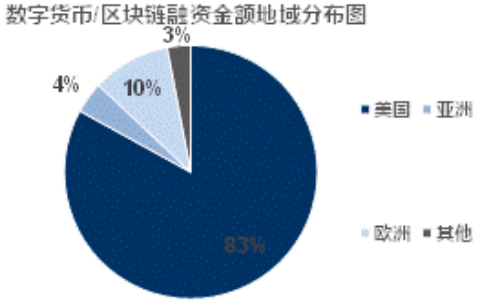
资料来源：8btc.com，申万宏源研究

图 29：美日欧等发达国家地区占投资数量主导



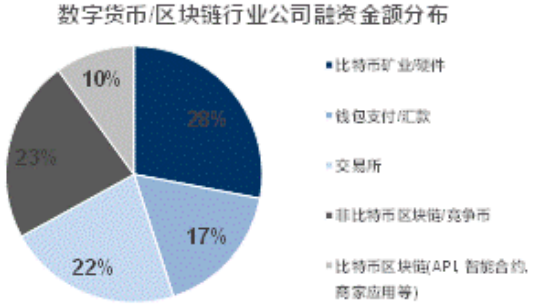
资料来源：8btc.com，申万宏源研究

图 30：美日欧等发达国家地区占投资金额主导



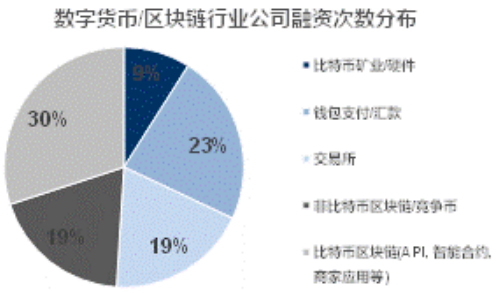
资料来源：8btc.com，申万宏源研究

图 31：虽然矿业和硬件仍是融资规模最大部分



资料来源：8btc.com，申万宏源研究

图 32：但融资次数上，区块链技术应用已经开始取代造币成为投资新方向



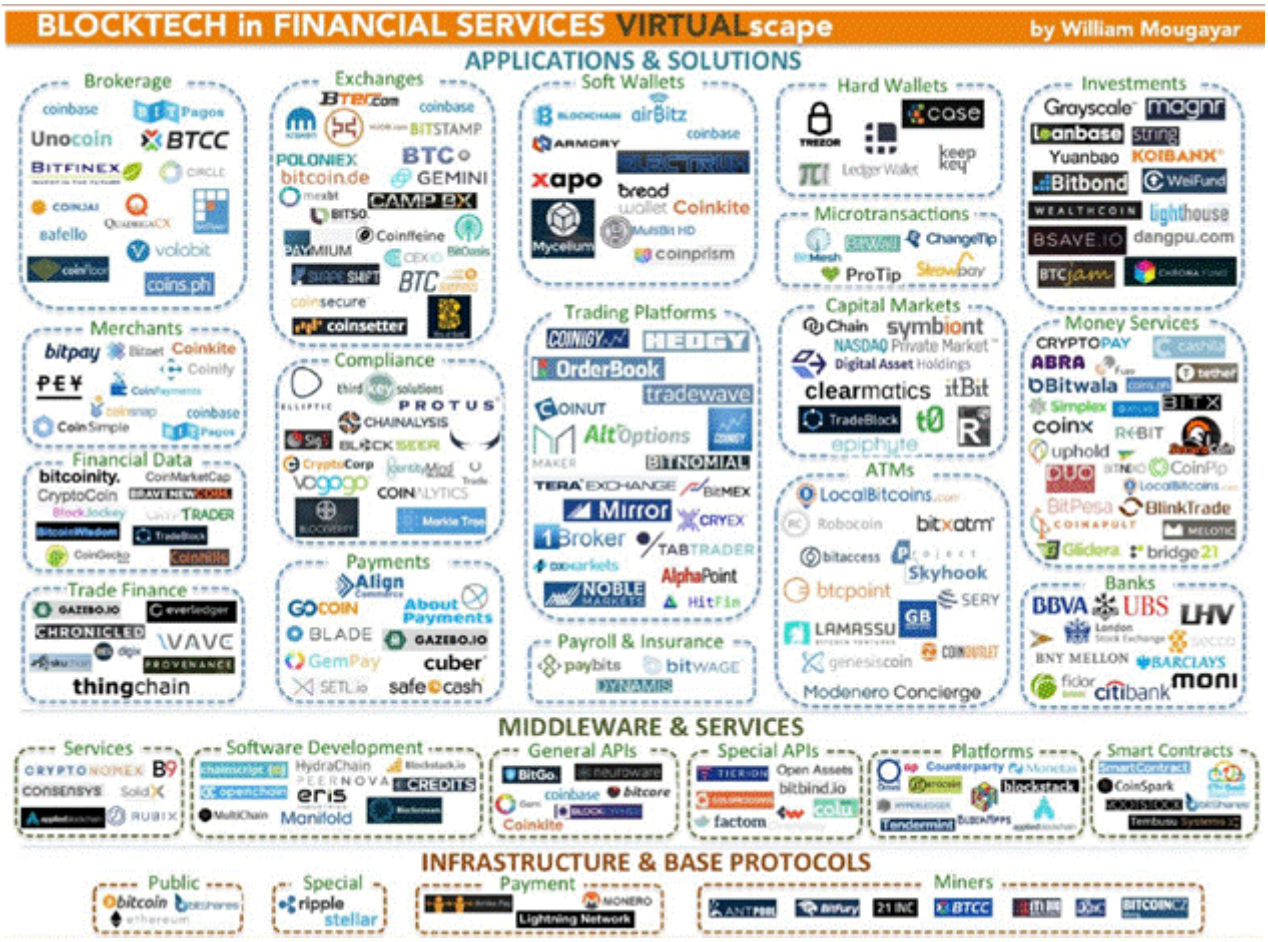
资料来源：8btc.com，申万宏源研究

图 33：同时，产业内开始出现 B 轮和 C 轮融资公司

资料来源：8btc.com，申万宏源研究

随着区块链技术的日益成熟和应用的扩展，各发达国家的区块链创业公司如雨后春笋般涌现。例如 Andreessen Horowitz、Fortress Investment Group 等有远见的专业机构投资者，以及例如杨致远、Max Levchin, Yuri Milner 等知名互联网科技产业内部人士积极进行投资，表达了对于产业长远发展的看好。

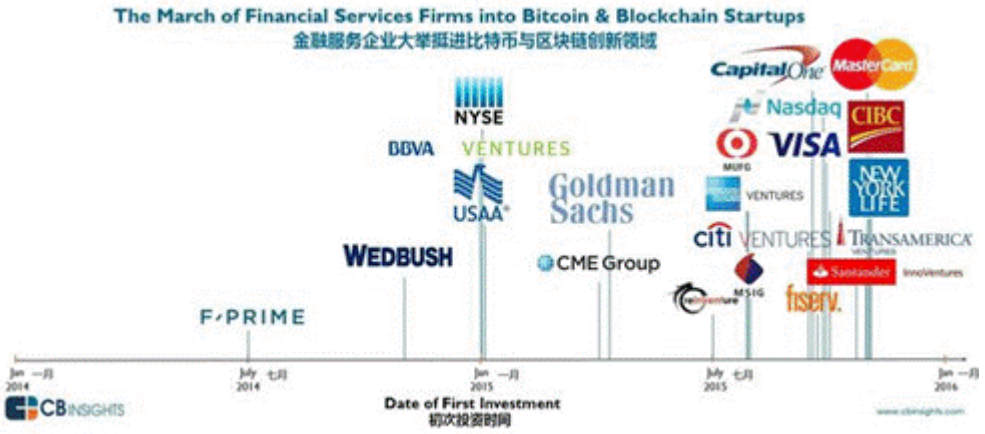
图 34：区块链技术金融相关创业公司不断涌现



资料来源：申万宏源研究，William Mougayar

附表 1 中展示了目前全球领先的区块链公司，我们发现这些公司覆盖领域普遍集中在交易、支付、清算、物联网等痛点业务，也是本文聚焦介绍的区块链技术四大应用行业。一些公司已经取得了一定的规模，并已经发展出了比较清晰的商业模式，同时多个公司业务在区块链产业链实现延伸，涵盖支付、交易、风控等，充分利用多点协调效应。通过对于投资者结构方面，我们发现了诸如 Goldman Sachs、NYSE、CME、BBVA、Santander、Capital One、JP Morgan、Citi 等金融企业积极投资清算交易等金融功能初创企业的倾向，以进行对自身金融服务的提升和扩展。同时我们发现了例如 Rakuten 等电子商务贸易企业对于支付领域进行投资的趋势，以探索并改进自身服务提供效率和扩大客户覆盖面。

图 35：各国大型金融企业和交易平台开始大举挺进区块链领域



资料来源：申万宏源研究，CB Insights

图 36：各国大型金融企业在区块链领域展开积极探索

CBW BANK	• 位于堪萨斯州的韦尔小型社区银行（CBW）已和Ripple Labs建立了合作伙伴关系，以推出其实时支付系统—One Card • 此技术和其竞争者区别在于其可以为实时结算提供便利，使得客户可以随时取回资金
BNY MELLON	• 纽银梅隆已在尝试比特币技术，着重用于提高金融交易的效率。把比特币的去中心化、点对点模型集成到银行的客户服务系统 • 纽银梅隆还推出了一种供公司内部使用的员工酬劳系统 BK Coins，这个BK Coins可用于兑换礼品卡，优惠券以及其他津贴
Westpac	• 澳新（ANZ）、西太平洋（Westpac）、澳大利亚联邦银行（CBA）正试验Ripples Labs的区块链分类帐户系统 • 澳新银行和西太平洋银行正调研使用瑞波系统来跟踪支付，而澳联邦银行则把该系统用于其附属机构之间的支付结算 • 在试验中，西太平洋银行的工作人员已经完成了向两个国家进行小额国际支付的尝试 • 2015年6月底，西太平洋银行通过旗下的风投基金 Reinventure 投资了Coinbase
BARCLAYS	• 巴克莱加速器”——一个为期三个月的导师计划，已经选出了三个区块链相关的初创公司Safello，Atlas Card和Blocktrace，这三家初创公司将加入到巴克莱银行的金融科技孵化器中 • 2015年6月份，巴克莱银行与比特币交易所Safello达成协议，将探索区块链技术如何加强金融服务业 • 巴克莱在探索可以改变银行运作方式的技术上可谓乐此不疲。在2015年4月的SWIFT论坛上，巴克莱银行的首席数据官 Usama Fayyad 表达了对区块链技术的兴趣，他相信区块链技术最终将会与传统银行业基础设施结合在一起
UBS	• 瑞士联合银行(UBS)正打算在伦敦设立一个技术实验室，以探索区块链在金融服务中的应用，尤其是对区块链技术如何使金融交易变得更高效这方面颇感兴趣
Goldman Sachs	• 高盛联手其他投资公司向Circle注资5000万美金。作为Circle的主要投资者，这一举动表明高盛认为区块链技术可能会改变现有的交易方式
ABN·AMRO Bank	• 荷兰银行(ABN Amro)，荷兰安智银行(ING bank)和荷兰合作银行(Rabo bank) 正调查区块链技术应用于它们现有银行支付系统的可能性 • 荷兰安智银行认为，区块链技术除了能够使银行的资金流动速度加快之外，还可以让银行24全天候运营，具有较强的吸引力
citibank	• 银行业巨头花旗集团，已开发了3条区块链，并在上面测试运行了一种名为“花旗币”（Citicoin）的加密货币

资料来源：巴比特，申万宏源研究

3.2 中国相关机构产业内投资力度较小，后期有望突破

我国过往相关投资主要重视挖矿和硬件投资，以及报价等信息提供业务和咨询。有深入研究并有一定规模的应用项目比较匮乏。目前行业内开始呈现向区块链多元化应用和深度发展的投资趋势，但体量较小且缺乏大型金融机构政府支持。万向集团下的区块链实验室是少有的大型机构支撑的研发项目。IDG 和数贝投资则是国内比较重要的区块链投资机构。

我们认为，随着央行对区块链重视加深和来自发达国家的技术溢出效应逐渐明显，我国相关发展会加快。根据以太坊创始人 Vitalik 的观察，中国目前区块链发展迅速，2015 年 10 月上海万向举办的区块链峰会中，300 多名与会者中不乏大公司或政府代表，且众多公司表示了希望与以太坊合作的意向。未来随着区块链应用的更加成熟和可投资投标的增加，区块链有望成为“互联网+”后的下一个热捧对象。这将激发创业者和应用者的热情，从而形成我国区块链发展的良性循环，产业内动态值得关注。

4. 核心假定的风险关键投资建议

区块链技术发展放缓

各国对区块链技术监管加严

5. 附表

附表 1：全球领先区块链公司一览

公司	领域	状态	总部	总融资（MM$）	融资阶段	投资公司	公司简介	公司近况
Guardtime	数据安全、物联网	私有	爱沙尼亚塔林	不明	不明	不明（或获得美国军方支持）	公司旨在利用区块链科技开发数字加密应用，以确保物联系统的系统完整性和安全性。Guardtime 主要是为数据提供签名授权、签名时间以及完整性验证。无论数据存储于磁盘中，在网络中移动，还是在云计算中使用，都可以在全球范围内保证它的可靠性和完整性。	Guardtime 的技术已经经历过长达 5 年的实战考验，众多政府和金融机构已经开始使用 Guardtime 作为系统泄露的早期探测和预防措施。
Coinbase	交易、钱包、支付、平台	私有/创业资本支持	美国加州	106.7	C 轮：75MM$	Andreessen Horowitz, BBVA Ventures, NYSE 等	公司业务主要包括比特币钱包和交易平台，让商家和消费者可以用新的数字货币比特币进行交易。公司的交易所将为个人和机构提供比特币交易服务，并实时监控这种虚拟货币的价格变动。该交易所将为比特币带来一定的合法性，这种货币并未获得美国中央政府的支持，但将为包括纽约、加州在内的 25 个州提供交易服务。这意味着 Coinbase 已获得美国多个州监管机构的合法执照。	USAA 宣布扩大其比特币整合范围，开始允许所有账户持有者链接到他们的 Coinbase 账户，并能从 USAA 的官网直接查看 Coinbase 的账户余额；公司在美国正式推出借记卡支付方式。其欧洲客户现在也可以使用借记卡和信用卡两种方式进行支付。

							Coinbase 表示，公司已购买了保险，因此可以为交易者提供一定的资金保障。	
Circle	支付、钱包	私有/创业资本支持	美国波士顿	76	C 轮：50MM$	Accel Partners, General Catalyst Partners, IDG Capital, Goldman Sachs 等	一家为消费者开发使用比特币的工具的公司，公司基于互联网提供消费者金融服务和零售消费银行产品。公司的愿景是让网络上发送和接收货币如同传送图片一样容易，同时利用区块链技术提供无以伦比的安全性。公司着力于全球拓展其商业模式。	近日，摩根大通的一位前高管已加入比特币初创公司 Circle Internet Financial；近日，其数字货币平台正式上线，平台将支持超过 160 种不同的货币；近日，公司已从纽约州监管机构那里拿到了第一张数字货币许可证 BitLicense，这意味着该公司将可在纽约州持证提供数字货币服务。
BitFury	交易处理	私有/创业资本支持	美国加州	60	B 轮：20MM$	DRW Trading Group, Georgian Co-Investment Fund, iTech Capital 等	BitFury Group 2011 年创立于俄罗斯，在旧金山和阿姆斯特丹设有管理部门，在冰岛和格鲁吉亚共和国设有数据中心和私人矿池。早期是一个 ASIC 比特币矿机芯片研发团队，现在转型做区块链基础数据服务和交易处理服务，拥有全球 15%的比特币交易处理份额。BitFury 的管理团队和董事会成员由经验丰富的业内资深人士组成，他们都有半导体工程、企业发展和公司投资的管理经验。	根据高盛投资公司近期的报告，大约 80% 的比特币交易数量来自人民币，交易量第二为美元，欧元排第三。除了巨大的比特币交易规模之外，中国因具有电费低廉、基础设施成熟而且硬件制造商成本低的优势，已经成为世界比特币开采中心。今年 BitFury 计划会为中国市场发布专用服务。
Digital Asset Holdings	清算结算、软件、私有和公共区块链	私有	美国纽约	52	A 轮：52MM$	ASX, CME, JP Morgan, ICAP, Accenture, BNP Paribas, Citi 等	公司旨在允许所有的参与者，在同一个数据库中进行实时的资产交易，同时利用 Cryptocurrency 区块链技术确保交易实时性和安全性。公司同时还提供企业辛迪加贷款、国债回购、股票交易结算等解决方案。	公司 CEO 为前摩根大通高管“CDS 之母”Blythe Masters；近期赢得一份来自澳洲证券交易所的合同。
Chain	清算、联盟链、平台、软件	私有/创业资本支持	美国加州	43.7	B 轮：30MM$	Capital One, Citi Ventures, Nasdaq, Orange, Visa 等	Chain 帮助机构与企业定制部署区块链基础设施，尤其是帮助金融企业建立系统网络，以摆脱对于中介的依赖。公司业界内非常知名。	近日，Chain 已使用纳斯达克的私募市场区块链解决方案 Linq，发行了本公司的股份。
Xapo	钱包、支付、平台	私有/创业资本支持	美国加州	40	A 轮：20MM$	Fortress Investment Group, Max Levchin, Yuri Milner, 杨致远等	公司大概率是全球最大的比特币托管人。公司提供比特币快捷和安全的储存方式，公司在瑞士阿尔卑斯山下有一个大型深度冷藏库服务器用以加密存储受托管比特币。同时公司提供将现金转换为比特币等数字货币的服务，用户不需银行帐户，即可以直接用平台进行数字货币交易。	比特币公司 XAPO 宣布计划济将总部搬迁到瑞士苏黎世，主要是看中了瑞士中立且稳定的环境。XAPO 公司注重的是比特币安全服务，从三个月前就已经开始很据客户要求转型。

Ripple	支付、结算、私链、软件、外汇、平台	私有/创业资本支持	美国加州	38.4	A 轮：32MM$	IDG, CME, Santander 等	公司是世界上第一个开放的支付网络，通过这个支付网络可以转帐任意一种货币，简便易行快捷，交易确认在几秒以内完成，交易费用几乎是 0，没有所谓的跨行异地以及跨国支付费用。Ripple 是开放源码的点到点支付网络，可以使客户轻松、廉价并安全的把金钱转帐到互联网上的任何一个人，无论其在世界上哪个地方。因为 Ripple 是 P2P 软件，没有任何个人、公司或政府操控，任何人都可以创建一个 Ripple 帐户。	公司于 2015 年末对外公布了其“InterLedger”协议项目，该项目的目标就是打造全球统一支付标准，创建统一的网络金融传输的协议。这一倡议也得到了微软（Microsoft）和万维网（World Wide Web）的支持。
Bitpay	支付、平台	私有/创业资本支持	美国佐治亚	32.7	A 轮：14.5MM$	AME Cloud Ventures, FelicisVentures, Horizon Ventures	BitPay 一直被称作 Bitcoin 上的 PayPal，它是面向收取 Bitcoin 商户的支付解决方案，商户收到消费者的 Bitcoin（必须是使用 Bitcoin 的个人消费者），通过 BitPay 把钱转成自己使用的货币，向 BitPay 支付 0.99%作为手续费。	美国著名贵金属销售商 JM Bullion 宣布与比特币支付处理器 BitPay 达成合作协议，为消费者提供比特币付款方式。BitPay 近日宣布与区块链服务供应商 Bloq 进行合作，为了提供更好的服务和新的功能
itBit	交易、清算、私链、软件、平台	私有/创业资本支持	美国纽约	32.5	A 轮：25MM$	Blockchain Capital, Raptor Capital Management, RRE Ventures, Solon Mack Capital 等	公司的愿景是成为全球型的可以处理任何资产、24 小时、全地理方位的交易平台。公司的 Bankchain 平台针对金融机构希望打造成一个更快、价格更低廉，更全面的清算和交易平台。	公司 2015 年获得了纽约州的信托牌照，这意味着 ItBit 开始受到纽约金融服务部门（NYDFS）的监管。对于该公司来说，其业务可以合法地扩大到美国地区，其合法地位已经和 Northern Trust，BNY MELLON 等平起平坐。
BLOCKCHAIN	钱包、平台、支付	私有/创业资本支持	英国伦敦	30	种子轮：30MM$	Lightspeed Venture Partners, Wicklow Capital 等	在相对年轻的比特币生态系统中的老字号钱包提供商和软件开发公司，目前已经拥有超过 450 万用户，每日完成 65 万交易，每周公司增加 7 万钱包。因为始终坚持虚拟货币的匿名性和去中心化的最初理念，而在该行业备受尊重。	最近公司收购了 RTBTC，后者提供实时的多个比特币兑换交易所的交易平台。最近公司收购了 ZeroBlock，后者提供关于比特币的实时数据和新闻。
VOGOGO	风控、支付	加拿大上市（TSX V: VGO）	加拿大卡尔加里	21	B 轮：12.5MM$	Beacon Securities, Clarus Securities 等	Vogogo 成立于 2008 年，起初业务包含设计，建造，并推出了基于网络的支付处理技术，并且同时扩大其在软件开发，支付，风险管理，合法化和相关金融的服务。	公司近日宣布，将与世界上曾经最大的比特币交易所—Bitstamp 进行整合，使其拥有专有的合法性和风险管理能力。公司正在与 Bitstamp 达成几个全球性倡议，并且大力支持 Bitstamp 的扩张进入美国和加拿大市场，以及增加欧洲的一些汇率。

Uphold	支付、外汇、钱包、平台	私有/创业资本支持/众筹	美国加州	20	众筹股权：9.9MM$	不明	公司是全球增长最快的基于区块链技术的金融平台。自 2014 年 11 月成立以来，公司已成功协助完成了超过 6.8 亿美元的交易。Uphold 数以万计的会员来自全球 170 个市场，交易超过 24 个币种和 4 种贵金属。通过整合其开源的应用编程接口 Uphold Connect，开发人员可以使用免费和即时的金融储存，为业务客户交换和转让资金。	公司今日宣布，即日起接受来自中国银联-中国最大的银行卡联合组织的在线服务。自今日起，中国 Uphold 会员可使用银联卡为其 Uphold 数字钱包充值。充值成功后，会员将享有即时、安全和免费的 P2P(点对点)支付服务，以及安全持有资金并获得国际支付的能力。
Bitnet	支付、平台	私有/创业资本支持	爱尔兰贝尔法斯特	14.5	A 轮：14.5MM$	Highland Capital Partners, Rakuten 等	Bitnet 提供顾客使用比特币支付的平台，然后在收取顾客的比特币后，折算付给商家现实的本地货币。据 Bitnet 称，每笔交易将收取最高不超过 0.9%的服务费用，而随着交易数额的变化，Bitnet 的收费大致相当于信用卡优惠利率的三分之一。由于比特币支付是不可逆的，Bitnet 接受其中的意外风险和贬值风险，他们拥有一个这样的风险承担系统：Bitnet 里存在着一个第三方托管代理，这个托管代理将分别、单独的与顾客和电商签订并执行交易，如果有任何一方没收到货币或者商品，托管代理将直接进行赔偿。	公司推出“即时交易’服务，减少商家等待比特币交易的时间。通过“即时交易”，与 Bitnet 合作的商家不再需要等待 2 到 6 个确认，只需几秒钟就能完成比特币交易。
ABRA	支付	私有/创业资本支持	美国加州	14	A 轮：12MM$	Arbor Ventures, Carthona Capital, First Round, RRE Ventures	Abra 是一款采用“比特币区块链+人体 ATM”组合技术的移动应用，基于 IOS 和 Android 平台的现金钱包和转帐应用，希望借此绕过中间商，降低用户昂贵的交易费用，从而进军 5500 亿美元的汇款市场。这款应用主要依靠“出纳员”网络运行，当用户想要存钱到他们的帐户中，他们既可以直接使用借记卡转帐，或者直接拿出手机，打开 Abra，应用会显示出附近的“出纳员”的坐标地图，同时还会显示根据其他用户以及其本身的费用而确定的评级。用户可以在众多出纳员中挑选一位，然后和他面对面交易，用现金换取“电子现金”。电子现金随后会被发送到用户手机，此过程靠区块链来完成确认。但是，所有存款皆以美元为保证，在存款后三日内，用户钱包里的存款额不会随着比特币价值而波动。用户看到的都是以美元计价的交易，而 App 后端使用比特币。只要用户的帐户里有钱，他们就可以完成给任何海外	近期获得了来自美国运通公司和印度塔塔集团名誉董事长——Ratan Tata 的战略投资

							汇款。收款人会被告知他们收到一笔汇款，随后他们便可以寻找附近的“出纳员”把钱取出来。	
BitGo	钱包、平台	私有/创业资本支持	美国加州	14	A 轮：14MM$	Blockchain Capital，Redpoint Ventures 等	BitGo 是一家比特币安全平台，近日其宣布推出第一个自动化的开源代码密钥恢复服务软件（Key Recovery Service 简称 KRS），该软件可生成、保护和存储私钥备份。	为了应对全球的比特币盗窃风险，BitGo 同 XL Group 保险公司达成协议。这是全球第一个比特币公司通过一个全球 A 级保险公司发行政策。
Filament	物联网、工业网络	私有/创业资本支持	美国内华达	6	A 轮:5MM$	Bullpen Capital，Samsung Ventures 等	公司是一个使用比特币区块链的去中心化的物联网软件堆栈，能够使公共分类总账上的设备持有独特身份。通过创建一个智能设备目录，Filament 的物联网设备可以进行安全沟通、执行智能合同以及发送小额交易。	近期，公司计划开发 2 个硬件单位： Filament Tap，一个传感器装置，允许装置与周边 10 英里以内的电话、平板电脑和计算机进行沟通；Filament Patch，用来延伸该技术的硬件，可以实现硬件项目的定制。通过利用基于区块链技术的堆栈，企业可以更好地管理物理采矿作业或农业灌溉，不需要再使用效率低下的中心化云方案或文件式的老方案。
BLOCKCYPHER	平台、软件基础设施	私有/创业资本支持	美国加州	3.1	种子轮：30MM$	500 Startups，AME Cloud Ventures，Blockchain Capital 等	BlockCypher 是一家区块链软件基础设施公司，其可以帮助公司使用简单的网络 API 搭建应用程序。	公司计划后续在多方面取得合作，包括网络开发商、成熟区块链公司、和大型金融机构等。
Factom	数据管理	私有	美国德州	1.1	种子轮：1.1MM$	First Step Partners，Resonant Venture Partners 等	公司提供基于区块链技术层级来记录和储存信息。公司的软件解决方案最大特点在于在区块链上存储各种尺寸的哈希加密信息，以创造不可逆的审计记录。对于有严格合规需求的公司，该方案吸引力较强。	近期，洪都拉斯政府开始和 Factcom 开展合作，以解决政府传统中心化记录所带来的腐败问题（例如，有权限访问并修订政府中心数据的官员利用制度漏洞篡改数据，为自己获得额外资产。）

资料来源：申万宏源研究，公司资料整理，互联网资料整理

附表 2：中国区块链创业项目一览表

项目名称	项目介绍	项目创始人（包括投资人）	技术创新
万向区块链实验室	专注于区块链技术的非营利前沿研究机构，就技术研发、商业应用、产业战略等方面进行探讨，为创业者提供指引，为行业发展和政策制定提供参考，促进区块链技术服务与社会经济的进步发展	肖风 Vitalik Buterin 沈波	行业技术交流和基础理论研究，区块链技术培训认证及推广、区块链丛书出版

布比	专注于区块链技术和产品的创新，以去中心化信任为核心，致力于打造开放式价值流通网络。目前已获得百万美元级天使轮投资	蒋海	在可证明安全性、交易验证共识、业务可拓展性等方面优势显著，既能满足互联网级开放式平台的要求，也可应用于各类企业级场景
莱特币	是一种基于“点对点”技术的网络货币，也是MIT/X11许可下的一个开源软件项目	李启威	在工作量证明算法中使用Colin Percival首次提出的Scrypt算法，因此相对比特币，在普通计算机上挖掘莱特币更容易
OKCoin比特币交易平台	中国最专业的比特币交易平台，采用ssl、冷存储、gslb、分布式服务器等技术，确保比特币交易的安全、快捷、稳定。目前，TradeBlock XBX、Coindesk Index、NASDAQ Europe ET三家机构已分别在价格指数中使用OKCoin比特币的价格	徐明星	1.策略交易，首创冰山委托、时间加权委托等策略交易工具；2.业内首创实时动态风控体系，实行多级动态风控标准，根据市场动态对账户和仓位进行分级管理；3.全球多市场，综合比特币指数，针对比特币波动大、交易所不稳定，定制多级权重管理体系，保证指数平滑的基础上，将全球主要市场纳入指数成分中
好有钱APP	专注熟人借贷的社交金融产品。熟人借贷即利用社交关系发展债权关系，但具有熟人信任的属性。F2F模式充分释放借款人和放贷人之间的社交关系价值，将借贷风险控制到最低。具有零风控、手续简单、借贷速度快等优势	徐明星	1.借鉴比特币去中心化的理念，发力熟人借贷，打破传统P2P的集中式系统风险；2.六维安全保障体系，保障借款人和放贷人的资金安全；3.结合比特币区块链技术，应用加密解密手段，在区块链上形成电子合同；4.应用移动互联技术让人和人之间信任关系更和谐
小蚁	基于区块链技术的股权登记、管理和交易系统。用电子签名签署股权转让协议，用区块链保存交易记录，是带自动执行功能的电子合同签署系统	达鸿飞 张铮文	结合国际电联X.509标准和《电子签名法》，设计具备法律效力的区块链身份认证方案；以双方签署电子合同的形式完成股权转让，符合《公司法》《合同法》要求；超导交易机制是交易所成为纯粹的信息撮合者，传统“用户+资金托管+证券托管+交易所+清算中心”简化为“用户+信息撮合者”模型
太一系统	可以方便发行多种数字货币，多种数字货币、数字资产管可以共享太一区块链。	邓迪	全球第一的有法币制成的数字货币，多资产共享区块链，降低发行成本
BTCC	最初以“比特币中国”创立于2011年，中国第一个比特币交易所，全球运营历史最长的交易所。提供数字货币交易所、矿池、支付网关、用户钱包、区块链刻字等服务	李启元 杨林科 黄啸宇	在高安全性和用户方便性上取得最佳平衡，创造一站式解决用户对比特币生态圈各个环节需求的模式
Goopal	基于区块链技术开发的全球移动数字积分系统，塑造公正、公开、透明的特性，同时使Goopal技术在更广泛的场景应用	孙江涛 崔萌 徐伟	采用DPOS股份授权证明机制；出块速度不超过10s；支持多种数字资产发布
WeSUCH	引入SAK支付系统，以“蜜悦APP”为依托，利用“流支付”思想解决实时、多方、碎片化的利益分配难题，发挥“粉丝经济”效应，服务人们生活	王东	利用DAC思想创造性地构建了一个能够自己发展壮大的平台规则体系，是各个参与方获得长期利益回报，并促进WeSUCH平台持续发展壮大
BitSE	于2013年在上海成立，提供全球最强壮的区块链及其侧链为基础，打造全球区块链服务平台，提供算力管理、数字资产管理与交易、物联网、防伪、IP注册等服务	钱德君	首次提出Blockchain As A Service，结合知识产权防伪检验的痛点，利用区块链及侧链的智能合约技术，以区块链安全芯片及区块链物联网芯片为核心提供服务
精灵天下	针对当前电子资产的版权认证不方便、取证难、认证难、交易繁琐等问题剔除新型模型	李贝宁	在附加区块链网络上面设计一层版权记录、认证、交易的协议，此协议能很好地对电子资料作Hash和附加信息的记录
安存正信	提供数据的真实性、有效性、证据化的基础性服务，以区块链的时间戳为基础，关联用户的线下真实身份提供存在性证明。	高航	在国内司法体系对电子证据认可的基础上，叠加基于区块链的存证技术，以“存证”为切入点

BitBank	立足于虚拟货币银行，为虚拟货币提供投资理财服务，前身为聚啊，累计理财超过 20 万 BTC、150 万 LTC，世界最早的虚拟货币理财平台、世界最大的虚拟货币银行。巨额投资 bw.com 公司到中国第一款 14nm 芯片的矿机中；技术上创新众多，投资重量级全冷钱包技术公司。	花松秀 郭宏才	提供虚拟货币挖矿理财，拥有比特币云算力理财
BitShares	基于 DPOS 区块链技术，达到工业级交易速度的开源去中心化交易所解决方案，无须任何技术知识就可以发行或交易数字货币、法币、金融衍生品，并收取自定义资产的交易佣金	Daniel Larimer 李笑来 沈波 龚鸣	首个全球范围商业化运作的交易平台解决方案，类 LMAX 交易引擎让区块链交易速度达到新高峰。能突破许多地区法律管辖限制，实现绝对公开透明的方式交易已存在或自定义金融产品
CertChain	以去中心化、纯粹数学算法的方式提供匿名且安全的存在证明。可根据用户需求便捷和极低成本的证明某个人对任意类型文件的所有权	龚鸣	无须透露任何鉴证内容给第三方就完成鉴证过程，公开、透明且免费。区块链使海量微信息的微公证成为可能，且使用数学算法让鉴证结果没有国界限制
DAI Bond	贷券是首个基于以太坊技术、可转让、等价可互换的加密债券。参与者无须事先认证，同时确保借贷行为低风险	Nikolai Mushegian Rune Christensen 龚鸣	价值与美元等法币实现 1:1 绑定。任何以太坊地址可持有贷券，也可自由发送给其他地址
ViewBTC	面向数字加密货币的独立第三方产业研究和咨询机构，三大业务包括维优指数、维优行业研究、维优数据分析，是 ViewFin 的数字货币方向分支项目	初夏虎	维优指数、维优行业研究、维优数据分析
RichFund	业务涉及比特币挖矿芯片、比特币矿机、矿场、对冲套利、量化及高频交易、场外交易、比特币相关项目投资和孵化	赵国峰	全球著名数字货币对冲基金
智能坊	第二代数字货币系统，提供图灵完备的 C/C++语言作为合约开发语言，拓宽应用领域，降低去中心化应用开发难度	石玮松	去中心化智能合约应用平台
BTSFair	P2P 比特资产兑换平台	郑浩	实物资产和虚拟资产链接的桥梁，提高比特币流动性、接受度、用户友好度
比太钱包	官方推荐钱包，为比特币企业提供安全的企业级钱包解决方案	文浩	基于 SPV 轻钱包模型，支持 HD 模型和多重签名技术，创新的冷热钱包模式，独创的极随机解决方案
币看	主营比特币和其他加密货币 APP，提供价格、咨询、交易功能，获几百万天使投资	刘爱华	通过 Web 和手机 App 提供比特币行情和咨询服务，并可以通过 app 介入比特币交易市场或个人进行交易
比特币交易网	支持人民币、美元、澳元、日元等与比特币交易的比特币交易平台，日交易金额最高超过 10 亿人民币	张寿松	全资收购聚币网
BitExchange 和闪电矿机	与 BitExchange 合作在全球建立比特币生态系统，连续推出多款矿机	廖翔	提供比特币硬件：矿机、Atm、硬件钱包、矿场部署
火币网	虚拟货币交易平台	李林 杜均	全产业链布局；首家实现比特币投资 A 股；一站式交易最完善
区块链中国	区块链技术门户网，行业搜索引擎	索剑伟	一站式解决区块链技术问题，提供外包服务、受理创业基金申请
Tilepay	为物联网行业提供去中心化的人到机器或机器到机器的支付解决方案。基于区块链技术开发微支付平台，并建立全球化的数据交易市场	Shawn David Kennedy Carol Duranleau	通过区块链技术重构物联网架构，隐去物联网设备的真实 ID，增加 mesh 网络安全性

		帅初	
币富网	数字货币数据分析和投资建议网站，以数据为出发点，结合行业热点分析判断数字货币发展趋势	潘国力 周朝晖	首创社会化情绪指数指导数字货币交易
ENS	区块链顶级名称注册的名称系统，管理以太坊区块链上的顶级域名	Nikolai Mushegian Rune Christensen Ryan Casey 鲁斌 杨仲东	可以永久地将以太坊区块链上的任何数据和名称关联起来

资料来源：《区块链，新经济蓝图导读》，申万宏源研究

信息披露

证券分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉的职业态度、专业审慎的研究方法，使用合法合规的信息，独立、客观地出具本报告,并对本报告的内容和观点负责。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

与公司有关的信息披露

本公司隶属于申万宏源证券有限公司。本公司经中国证券监督管理委员会核准，取得证券投资咨询业务许可，资格证书编号为：ZX0065。本公司关联机构在法律许可情况下可能持有或交易本报告提到的投资标的，还可能为或争取为这些标的提供投资银行服务。本公司在知晓范围内依法合规地履行披露义务。客户可通过 compliance@swsresearch.com 索取有关披露资料或登录 www.swsresearch.com 信息披露栏目查询从业人员资质情况、静默期安排及其他有关的信息披露。

机构销售团队联系人

上海	陈陶	021-23297221	18930809221	chentao@swsresearch.com
北京	李丹	010-66500610	18930809610	lidan@swsresearch.com
深圳	胡洁云	021-23297247	13916685683	hujy@swsresearch.com
海外	张思然	021-23297213	13636343555	zhangsr@swsresearch.com
综合	朱芳	021-23297233	18930809233	zhufang@swsresearch.com

法律声明

本报告仅供上海申银万国证券研究所有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。客户应当认识到有关本报告的短信提示、电话推荐等只是研究观点的简要沟通，需以本公司 http://www.swsresearch.com 网站刊载的完整报告为准，本公司并接受客户的后续问询。本报告首页列示的联系人，除非另有说明，仅作为本公司就本报告与客户的联络人，承担联络工作，不从事任何证券投资咨询服务业务。

本报告是基于已公开信息撰写，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。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、价值及投资收入可能会波动。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。

客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为作出投资决策的惟一因素。客户应自主作出投资决策并自行承担投资风险。本公司特别提示,本公司不会与任何客户以任何形式分享证券投资收益或分担证券投资损失，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。市场有风险，投资需谨慎。若本报告的接收人非本公司的客户，应在基于本报告作出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告的版权归本公司所有，属于非公开资料。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。