



证券研究报告
2016年1月29日

主题研究：热门美股

泡沫启示录：区块链，从革新金融到构建自治社会

观点聚焦

移动互联网也近十年之痒，下个平台是什么？

移动互联网从2007年苹果推出iPhone算起，已近“十年之痒”，业界和投资者纷纷布局下一个计算平台。正如我们在《泡沫启示录：科技投资的胜者为王》中阐述，人们往往高估技术的短期影响而低估长期影响，每一次平台轮替都会创造更大的财富，催生新的巨头，但只有少数卓越公司可以成功跨越。我们无法确知下一个平台是什么，但Blockchain、机器人/人工智能、VR/AR和物联网等皆有可能。

区块链异军突起

比特币因其剧烈的价格波动和与犯罪相连的坏名声，2009年诞生至今仍远未进入主流。作为比特币背后的架构协议，区块链却越来越受到广泛关注。区块链就是具有分布式、去中心化、去信任化、不可篡改、加密安全性等特征的账本。基于对比特币区块链种种缺点的修正，后来兴起的第二代区块链，如Ripple、以太坊等，将区块链推向了实际应用。就如TCP/IP协议支撑了互联网和信息经济，在区块链架构之上，或许能搭建起更高效、更透明、更个体自治的新社会。

Fintech 2.0，革新金融业基础架构

正如我们在《硅谷挑战华尔街》中所言，Fintech创业公司凭借的往往只是用户体验优化、市场定位细分和监管套利，却远远没有触及金融行业的底层架构。但区块链有望改造金融基础设施，释放存量市场的活力。当前开始商用或测试的应用领域包括跨境支付、证券交易结算和证券发行等，今年或将看到更大规模的商业化。华尔街对区块链的主动拥抱也将深化Fintech 2.0的影响，清算所、存托所、交易所、投资银行、商业银行、经纪商等金融机构的职能将被取代或转型。对于监管者而言，区块链有利于实现原本互不相容的两个目标：降低系统风险和减少监管负担。

社会帮助物联网落地，实现智慧政府，构建自治社会

区块链可为物联网中数以亿计的设备之间建立低成本的、P2P直接沟通桥梁，使智能设备成为自我维护的自治个体，又保证了信息的安全性和私密性，可使流行多年的物联网概念真正落地。对于国家能力尚不健全的发展中国家，区块链提供了跳跃式发展的可能，帮助政府完善公共服务、分配公共资源。此外，区块链对信息安全、云存储、共享经济、产权保护、媒体传播、预测研究等也将具有重要意义。而由区块链带来的效率节约和信任重构，将有利于促进消费者利益，限制权力腐败，构建社会自治。

中国机遇

中国金融机构也应尽早开始区块链实验。以太坊等开源平台提供了技术便利，还需决策层的战略眼光、机构之间的配合协作，以及监管支持。万向和石基信息在区块链方面较为积极。参见同日报告《区块链：改变金融业基础架构》。

分析员

何玫，CFA

SAC 执证编号：S0080512090005
SFC CE Ref: AVJ148
mei.he@cicc.com.cn

分析员

毛军华

SAC 执证编号：S0080511020001
SFC CE Ref: AMJ527
junhua.mao@cicc.com.cn

联系人

颜少彬

SAC 执证编号：S0080115030005
shaobin.yan@cicc.com.cn

相关研究报告

- 泡沫启示录：人工智能，魔鬼还是忠仆？(2015.11.23)
- 泡沫启示录：虚拟/增强现实，梦想照进现实(2015.10.20)
- 泡沫启示录：科技投资的胜者为王(2015.09.15)
- 美国科技观察周报：网络电视高歌猛进，区块链异军突起(2016.01.24)
- 美国科技观察周报：创投市场感受加息寒意，区块链革新金融业(2015.12.20)
- 独角兽启示录：硅谷挑战华尔街(2015.06.11)
- 热门美股：LendingClub，全球最大的P2P网贷平台(2014.09.19)



目录

区块链异军突起	4
区块链源于比特币，但走得更远	4
硅谷和华尔街合力打造，推动金融创新、物联网落地和智慧政府	5
Fintech 2.0，革新金融业基础架构	13
Fintech 2.0，从根本上革新金融业基础架构	13
开始商用或测试的应用领域包括跨境支付、证券交易结算和发行等	16
将冲击或改造金融机构商业模式	23
帮助物联网落地，实现智慧政府，构建自治社会	24
帮助物联网落地	24
实现智慧政府	27
构建自治社会	29
附录：虚拟货币概要	35

图表

图表 1：区块链是比特币的底层技术	6
图表 2：2014 年以来，区块链概念得以与比特币分开，受到广泛重视	7
图表 3：其本质就是一个账本，由数据块组成链条	7
图表 4：但具有 P2P	8
图表 5：...分布式、去中心化	8
图表 6：...不可篡改、加密安全性高等特点，从而解决双重支付问题和拜占庭将军问题	9
图表 7：比特币区块链有一些缺点，如区块大小限制	9
图表 8：...确认时间长、损耗能量等	10
图表 9：因此产生了其他区块链协议	10
图表 10：部署方式可分为公共链、私有链和联盟链	11
图表 11：创投活跃，已累计 10 亿美元 VC 投资	11
图表 12：不仅创业企业涌现	12
图表 13：传统金融机构也纷纷以内部研究、外部结盟和投资的方式，布局区块链	12
图表 14：区块链将大幅提高金融市场效率，到 2020 年可节约 150~200 亿美元金融机构中后台成本	15
图表 15：而在区块链之前，缩短结算周期需要大量初始投入	15
图表 16：虽然目前大多处在概念验证、内部测试阶段，预计 2016 年以后将竞相商业化	16
图表 17：预计 2016 年以后将竞相商业化	16
图表 18：Ripple 为金融机构提供跨境支付和外汇做市的解决方案	20
图表 19：...比现有系统速度更快、成本更低	20
图表 20：纳斯达克开始用基于区块链的 Linq 平台，交易私有股权	21
图表 21：除了与纳斯达克 Linq 合作以外，Chain 还提供国债回购解决方案	21
图表 22：Digital Asset Holdings 提供企业辛迪加贷款、国债回购、股票交易结算等解决方案	22
图表 23：高盛开发了金融资产交易交割系统 SETLcoin，并申请专利	22
图表 24：智能合约是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值	26
图表 25：区块链将使物联网形成点对点的高效低成本连接，使亿级智能设备成为自我维护的独立个体	26
图表 26：IBM ADEPT 物联网方案	27
图表 27：Agora Voting 基于区块链开发的安全高效匿名公正的投票系统	29
图表 28：微软 Azure 推出 Ethereum Blockchain as a Service	30
图表 29：德勤推出的 Rubix 是一站式区块链软件平台	30



图表 30: Everledger 钻石“护照”和智能合约方便钻石交易	31
图表 31: DocuSign 和 Visa 合作推出基于区块链的汽车交易租赁平台	32
图表 32: Ujo Music 以 P2P 方式销售歌曲 Tiny Human	33
图表 33: Augur 预测市场	34
图表 34: 虚拟货币是一种电子货币，但不是任何机构或个人的负债，且无官方担保	35
图表 35: 目前最大的虚拟货币是比特币	35
图表 36: 比特币价格依然波动剧烈	36
图表 37: 比特币依然没能形成主流	36
图表 38: 各国政府对比特币的态度以限制或禁止为主	37
图表 39: 比特币及其 colored coins 的创业公司分为基础设施、钱包、支付、交易所、金融服务、挖矿等类别 ..	37
图表 40: 在支付体系中推广虚拟货币依然困难重重	38



区块链异军突起

区块链源于比特币，但走得更远

比特币因其剧烈的价格波动、高度的匿名性和与犯罪相连的坏名声，2009 年诞生至今仍未进入主流。然而 2014 年以后，作为比特币背后的数据结构，区块链（Blockchain）却越来越受到广泛关注。Marc Andreessen 等知名风投认为，**区块链将重新定义互联网**，IMF 和英格兰银行认为，**区块链将极大革新金融业**。

从本质上说，**区块链就是一种巨大的账本（ledger）**，由一串密码学方法产生的数据块组成，每一个数据块包含了一次比特币网络交易的信息，用于验证其信息的有效性和生成下一个区块。区块链具有分布式（Distributed）、去中心化（Decentralized）、去信任化（Trustless）、不可篡改（Immutable）、加密安全性（Cryptographically secure）的特征，从而解决了双重支付（Double spend）问题和拜占庭将军问题（Byzantine Generals' Problem）。

- ▶ **去中心化：**这是比特币发明的最大创新之处。按照中本聪（Satoshi Nakamoto）的白皮书所说，比特币“基于密码学原理而不基于信用，使得任何达成一致的双方，能够直接进行支付，从而不需要第三方中介”。去中心化的衡量标准就是需要攻击多少个地方，才能破坏整个网络。
- ▶ **去信任化：**参与整个系统中的每个节点之间进行数据交换是无需互相信任的，整个系统的运作规则是公开透明的，所有的数据内容也是公开的。因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其他节点的。
- ▶ **加密安全性和不可篡改性：**每个节点因预先设置的协议而生成，也是由协议约束而参与到执行环节，准确的承载着数据和信息。构成区块链的算法则“哈希算法”通过单向数学函数来检验是否有人试图篡改信息。因每个节点及形成的函数“散列”都是独一无二的，且每个节点都能获得一份完整数据库的拷贝，任何试图入侵破坏或篡改区块链数据的行为都会变得显而易见。除非能够同时控制整个系统中超过 51% 的节点，否则单个节点上对数据库的修改是无效的，也无法影响其他节点上的数据内容。
- ▶ **解决双重支付问题：**普通数字货币是通过中心化的银行来解决双重支付问题。而在比特币区块链中，所有的交易都是公开宣布的，当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性。
- ▶ **解决拜占庭将军问题：**“拜占庭将军问题”由几个 SRI International 科学家于 1982 年提出。它以假想的数支拜占庭军队联合攻城为情形，讨论如何使分布的节点达成共识，避免内部叛徒出卖或外部攻击。比特币区块链以工作量证明的机制，解决了这个问题。工作量证明机制的本质则是一 CPU 一票。“大多数”的决定表达为最长的链，因为最长的链包含了最大的工作量。如果大多数的 CPU 为诚实的节点控制，那么诚实的链条将以最快的速度延长，并超越其他的竞争链条。如果想要对已出现的区块进行修改，攻击者必须重新完成该区块的工作量外加该区块之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。

比特币区块链是第一个、也是目前最大的区块链，但实际用途有限。2015 年 12 月 31 日时，比特币市值 64.5 亿美元，总流通量 1,502.8 万。然而，比特币区块链具有区块容量限制、确认时间长、能量消耗大等缺点，一度成为其商业化应用的主要限制。

- ▶ **区块容量限制：**中本聪设计比特币区块链时，人为设置了每个数据块 1MB 的大小限制。随着比特币发行量的增多和应用的推广，目前比特币网络已经接近了这个上限，使交易时间延长，甚至高峰时一些交易请求无法成功（这一问题又因为 50% 以上的比特币矿工在中国防火墙以内而更加恶化）。针对是否应该提高区块容量上限的问题，比特币社区已经发生了严重分歧，分出来 Bitcoin Core 和 Bitcoin XT 两派，Mike Hearn 等知名比特币开发者宣布退出比特币社区。



- ▶ **确认时间长：**比特币区块链通过工作量证明（Proof of Work）来确保系统的安全性。工作量证明就是让电脑计算出一个数学问题，当电脑的计算能力为某个有限值的情况下，需要运算一定时间才能解决。因此每个新区块的生成平均需要 10 分钟。再加上区块大小的限制（每块最多可以容纳 4,096 笔交易），比特币网络每秒只能处理 7 笔交易，远远低于 Visa/Master 网络每秒 4.7 万笔交易的能力。
- ▶ **能耗高：**比特币矿工目前的“挖矿”设备已经由 300MH/秒的 CPU 升级到了 5TH/秒的 ASICs。据估计，目前比特币网络处理一笔交易的耗电量相当于美国一个家庭一天的耗电量，而碳排放是 534 吨每日或 825 万吨每年。

近年来开发出其他区块链协议，才使区块链有机会在金融业和其他行业中得到实际应用。以太坊（Ethereum）、Ripple、Stellar、Eris、Tendermint、HyperLedger 等替代区块链，往往以权益证明（Proof of Stake）、股份授权证明 DPOS（Delegate Proof of Stake）等机制取代了费时费力的比特币工作量证明机制，从而提高了交易速度，降低了能耗。

例如，作为开源平台的以太坊，每个区块产生时间只需要 17 秒，采用权益证明取代工作量证明（不是让各个节点竞争性的完成工作量，而是根据各个节点已有的虚拟货币数量来进行交易确认），没有区块大小限制，图灵完备（可以实现任何可以想象的计算，包括无限循环），具有并行处理的可扩展性（未来可达 10 万次交易每秒），可编程（适合生成智能合约）。其目标是成为下一代智能合约和去中心化应用平台。目前正在开发的许多金融和非金融的原型项目都以以太坊为基础协议。

在实际部署时，区块链又根据中心控制力度和信息公开度，分为公共链、私有链和联盟链。

- ▶ **公共链：**任何人都可以往区块链中读取、写入，参与交易的验证，真正的分布式和去中心化。其系统安全性由工作量证明或权益证明机制来保证。参与者往往是匿名的。由隐含的虚拟货币为参与者提供激励。比特币区块链就是公共链。
- ▶ **私有链：**私有链具有分布式的特点，但却不是去中心的。它由中心控制者指定可以参与的成员、进行交易验证的成员。不需要虚拟货币提供激励。私有链往往是内部研发测试时使用，真正成熟商业化以后将变成公共链或联盟链。
- ▶ **联盟链：**其实是多中心式，参与主体是预先设定的、具有特定特征的成员（如某组织的成员、某公司的客户等），交易通过共识机制确认，确认交易的节点也是事先选定的。虚拟货币的必要性由该联盟链内部的信任程度决定。可以匿名也可以不匿名。联盟链或许将是区块链行业应用的主要形式，比如某种证券的市场参与者就可以组成联盟链来进行交易和结算。

硅谷和华尔街合力打造，推动金融创新、物联网落地和智慧政府

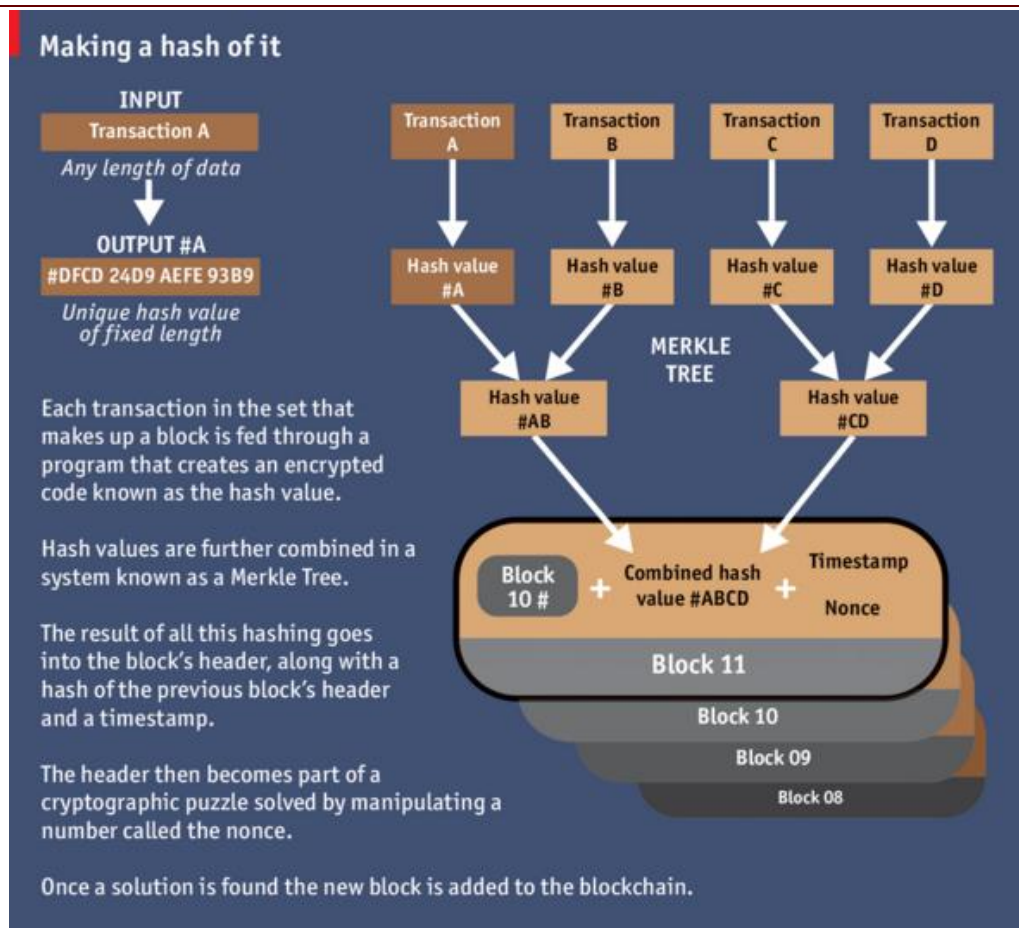
区块链意义深远，推动金融创新和物联网落地。因其去中心化、加密安全性的特征，区块链不仅可以支持比特币等虚拟货币（Virtual Currencies），也将在金融、互联网、政府事务、商业、媒体、医疗等方面有广泛的应用，使原本严重依赖中介机构的活动和行业，极大的简化流程、提高效率，也将有助于打破垄断。此外，区块链衍生出的智能合约，还将成为物联网落地的关键技术。

创投活跃，华尔街积极布局。据统计，截止 2015 年 12 月 1 日，投向比特币和区块链的风投资金合计达 10 亿美元。此外，与其他新技术以硅谷为中心不同，区块链因其在金融领域潜在的革新力量，纽约华尔街也积极投身区块链的研发。美国和欧洲所有大型金融机构，每家都有 10~20 个区块链项目进行内部开发和评估。此外，金融机构也以联盟和对外投资的方式布局生态系统。例如，R3 CEV 已吸引了 42 家金融机构成员，创业公司 Digital Asset Holdings 获得了摩根大通、花旗、美国存管信托和结算公司（the Depository Trust & Clearing Corporation, DTCC）等的投资。区块链初创企业也多以服务（而非“颠覆”）金融机构为任务目标。硅谷和华尔街的合作创新（collaborative innovations）可能使区块链所代表的 Fintech 2.0 比 Fintech 1.0 收获更多、影响更大。



监管环境宽松。与比特币相比，区块链的监管环境大为宽松。比特币有可能成为洗黑钱、恐怖组织融资、逃税、躲避资本管制等违法犯罪活动的工具，且监管定义不清（物产、货币、大宗商品、证券皆有可能），各国政府大多将比特币设为限制或禁止的对象。但对于区块链多以支持为主。美国 CFTC（the Commodity Futures Trading Commission）主席 Timothy Massad 表示，区块链将帮助实现原本不可调和的两大监管目标——控制系统性风险和减少监管干预。英格兰银行称区块链是 Internet of Finance 的首次尝试。IMF 表示，独立于虚拟货币以外的区块链，因其往往由受监管的金融机构在有限的范围内使用，因此不会引起太多监管风险。国际清算银行则呼吁各国央行持续跟踪和分析虚拟货币及其区块链技术，在支付及支付以外金融活动中的影响。

图表 1：区块链是比特币的底层技术



资料来源：Economist "The great chain of being sure about things"



图表 2：2014 年以来，区块链概念得以与比特币分开，受到广泛重视

Five years of blockchain development, leading to new applications

Early days	Turbulence and recognition	Experimentation
		2014 – present
2009-2012 Blockchain regarded exclusively as backbone to Bitcoin Bitcoin only adopted by marginal number of users Overall ecosystem seen as experimental and obscure Awareness limited largely to cryptographic community Broader perception of digital currencies as fad or Ponzi scheme Pronouncements by financial industry dismissing potential threats and opportunities	2012-2014 High-profile investments, public interest, “Silk road” effect put Bitcoin in the spotlight High volatility, criminal associations and mis-conceptions make the Bitcoin ecosystem suspicious for important players Nevertheless, Bitcoin establishes itself as a legitimate value-transfer vehicle, averaging 50,000 transactions per day worldwide Multiple remittance payment and wallet provider start-ups emerge	Dissociation of blockchains from Bitcoin for many players and increasing sophistication in approach to technology Serious interest from regulators (Bank of England, Fed) towards the technology (not just currency) Venture capital firms and financial institutions see potential disruptive effect of the technology and invest (e.g., UBS, Santander, Nasdaq) High-profile executives join and found start-ups Announcements of prospective consortia collaborating to find common protocols for adoption

资料来源：McKinsey “Beyond the Hype: Blockchains in Capital Markets”

图表 3：其本质就是一个账本，由数据块组成链条

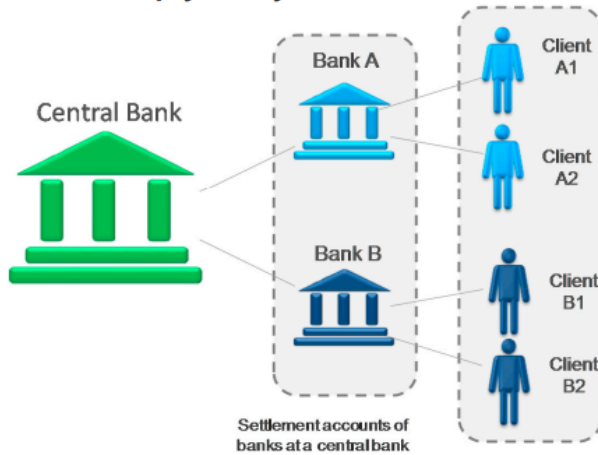
区块链数据块示意	
Block	#125552
BlockHash	00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
# of Transactions	4
Height	125552 (Mainchain)
Block Reward	50 BTC
Timestamp	May 21, 2011 1:26:31 PM
Merkle Root	2b12fcf1b09288fcff797d71e950e71ae42b91e8bdb2304758dfcfc2b620e3
Previous Block	125551
Difficulty	244112.48777434
Bits	1a44b9f2
Size (bytes)	1496
Version	1
Nonce	2504433986
Next Block	125553

资料来源：Vermont State Government “Blockchain Technology: Opportunities and Risks”



图表4：但具有P2P...

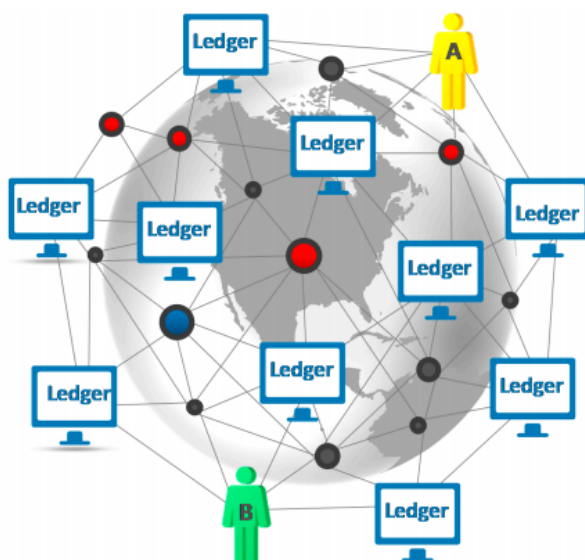
A centralized payment system



Payment from A1 to B1:

- Money is deducted from A1's account in bank A.
- The central bank moves money from bank A's settlement account to B's.
- The central bank maintains central record (ledger) of interbank transactions, by validating transactions and safeguarding against double-spending and counterfeit.
- Bank B adds money to B1's account.
- Banks A and B maintain the ledger of transactions for their clients A1 and B1 respectively.

An illustrative example of distributed ledger system similar to Bitcoin (Blockchain)

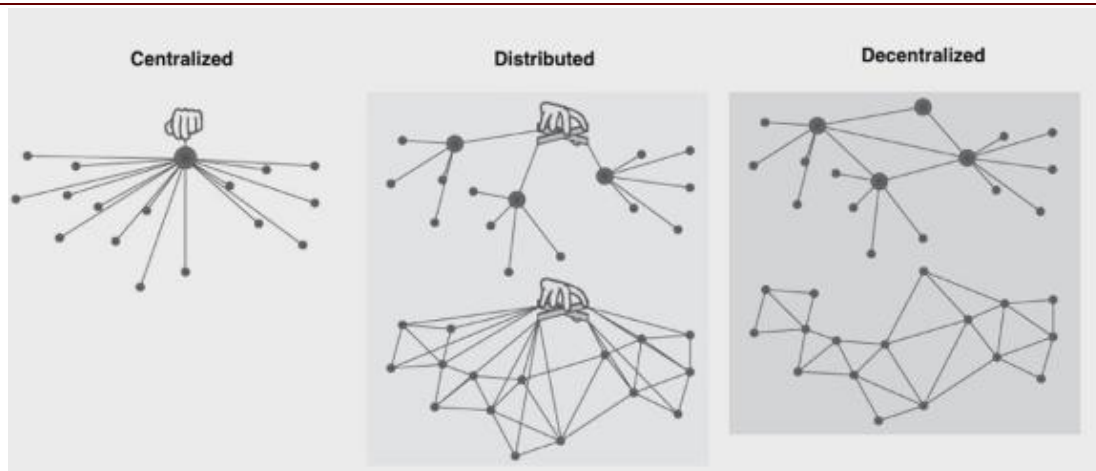


Payment from A to B:

- Copies of transaction records (ledgers) are kept in multiple computers in the network and visible to anyone.
- The transaction is settled by a multitude of individual nodes (miners), providing computing resources to the network.
- Miners solve a cryptographic puzzle as part of validation process. Miners need to show proof of doing this work to the network (called a "proof-of-work" system), which is costly (computing and energy resources).
- Only the miner who finds the solution faster than any others receives newly minted Bitcoins as reward for their service.
- "Trust" is created by making tampering attempts prohibitively expensive. If a miner wants to record a false transaction, she needs to compete against other miners who are acting honestly (or trying to fake a different transaction).¹

资料来源：IMF "Virtual Currencies and Beyond: Initial Considerations"

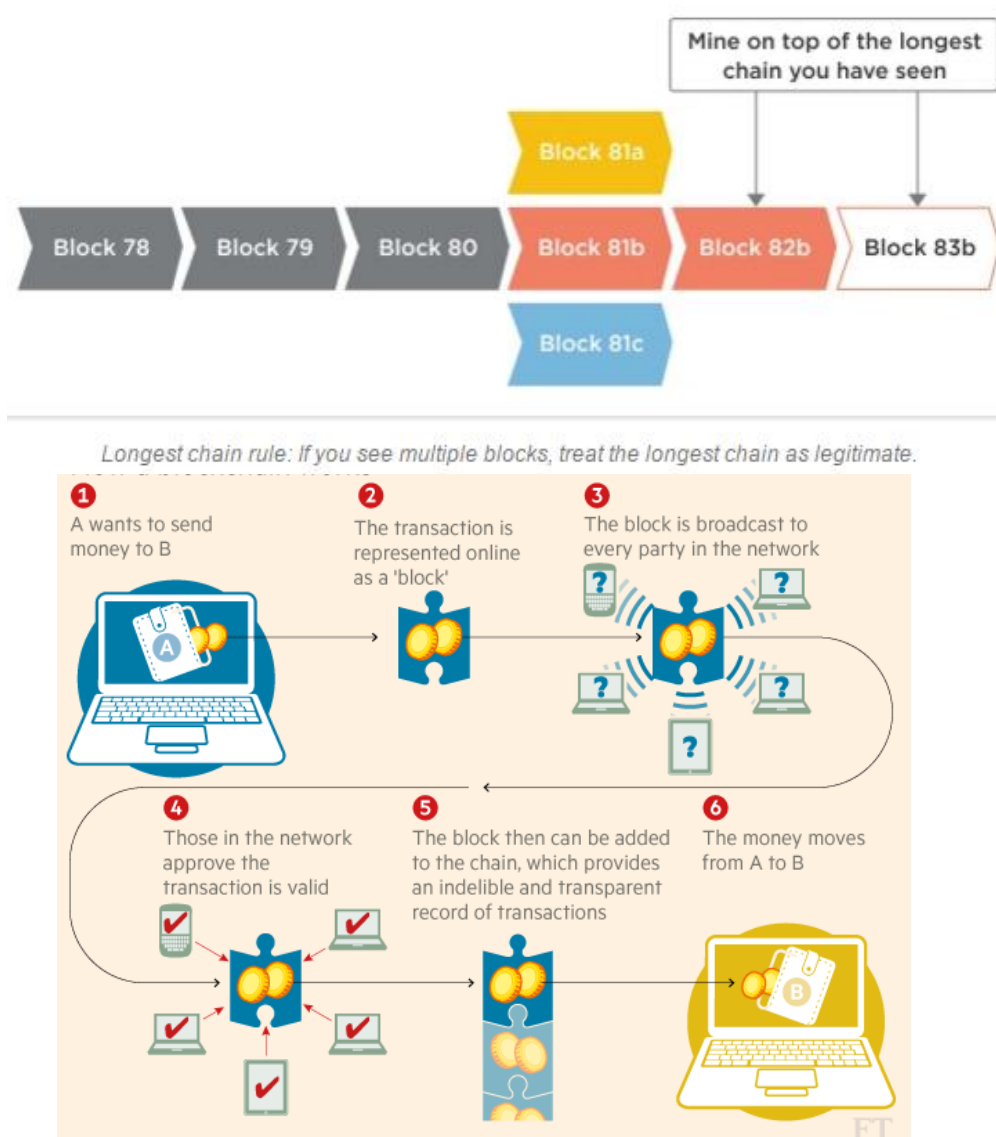
图表5：...分布式、去中心化...



资料来源：okTurtles Foundation

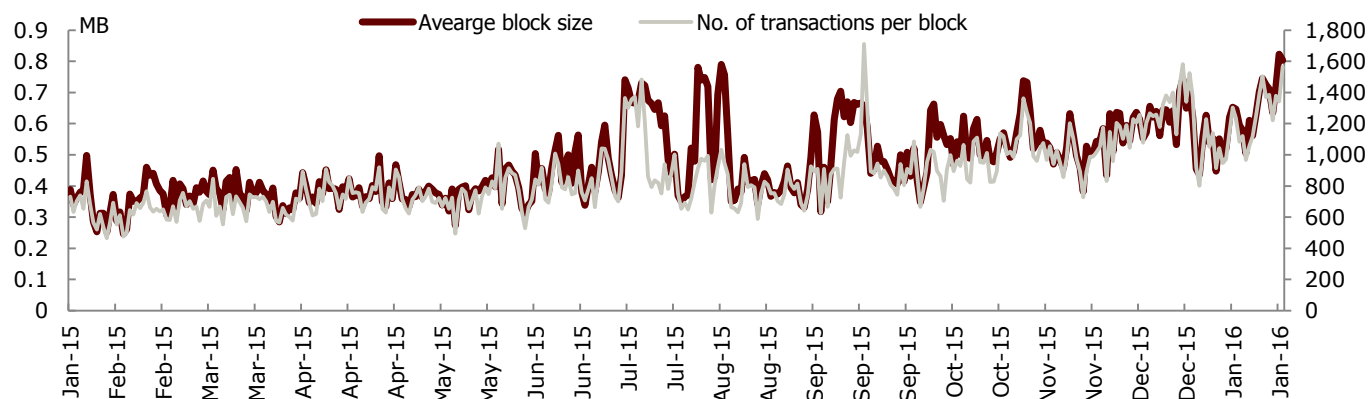


图表 6: ...不可篡改、加密安全性高等特点，从而解决双重支付问题和拜占庭将军问题



资料来源: Antony Lewis, Financial Times

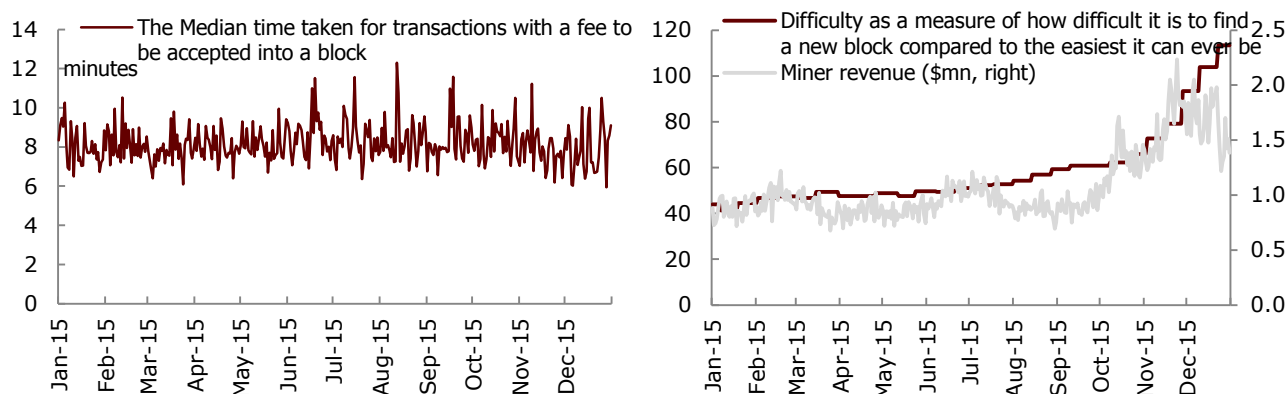
图表 7: 比特币区块链有一些缺点，如区块大小限制...



资料来源: blockchain.info



图表 8: ... 确认时间长、损耗能量等



资料来源: blockchain.info

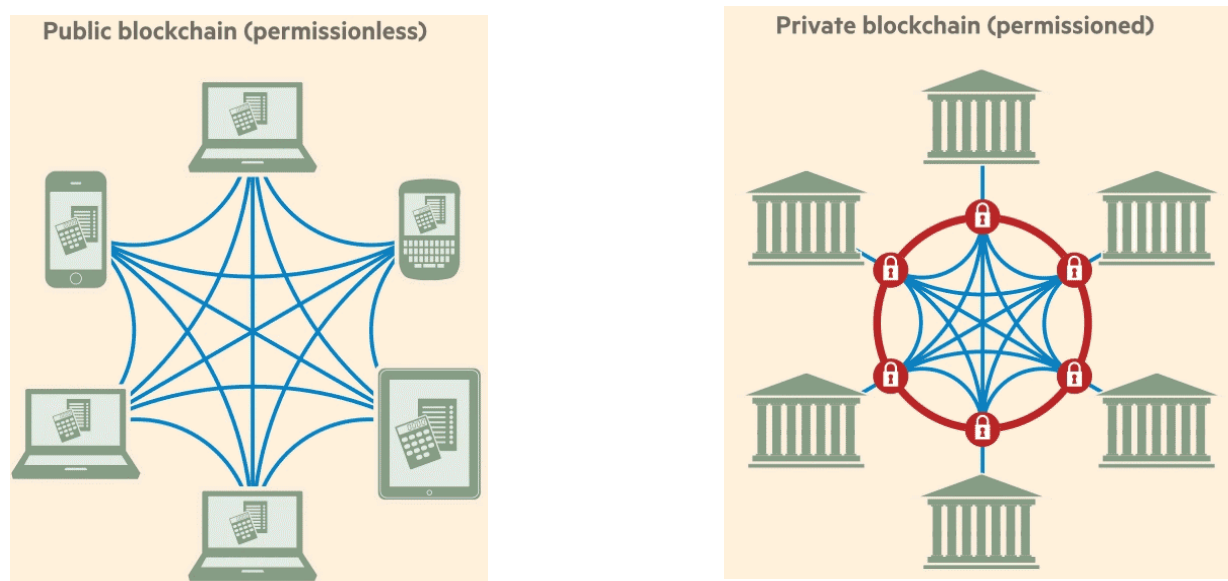
图表 9: 因此产生了其他区块链协议



资料来源: Simon Janin, 公司网站

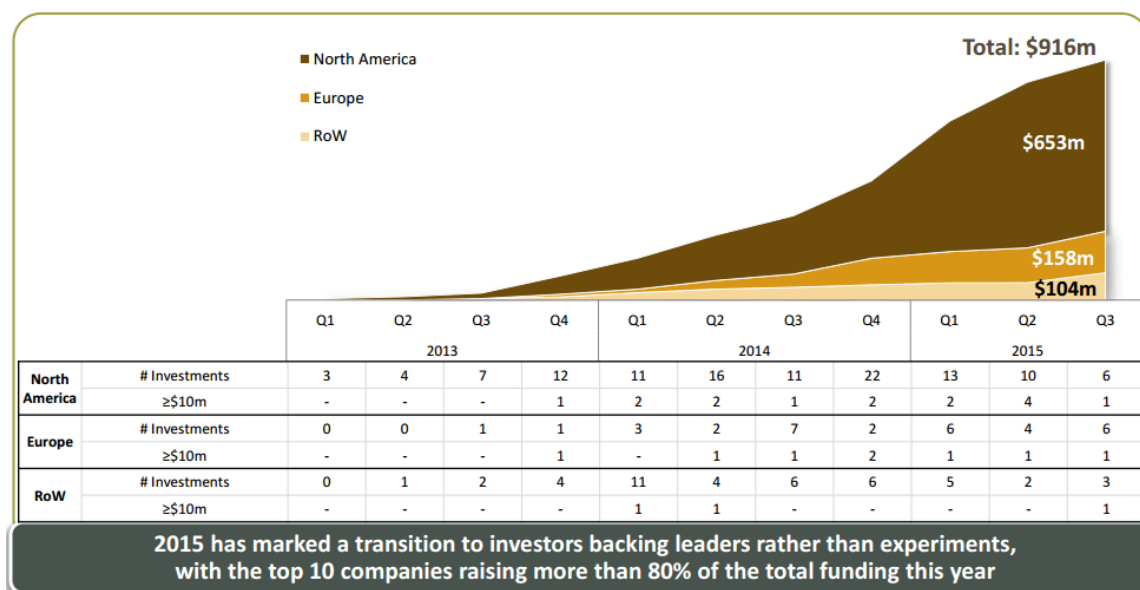


图表 10：部署方式可分为公共链、私有链和联盟链



资料来源：Financial Times

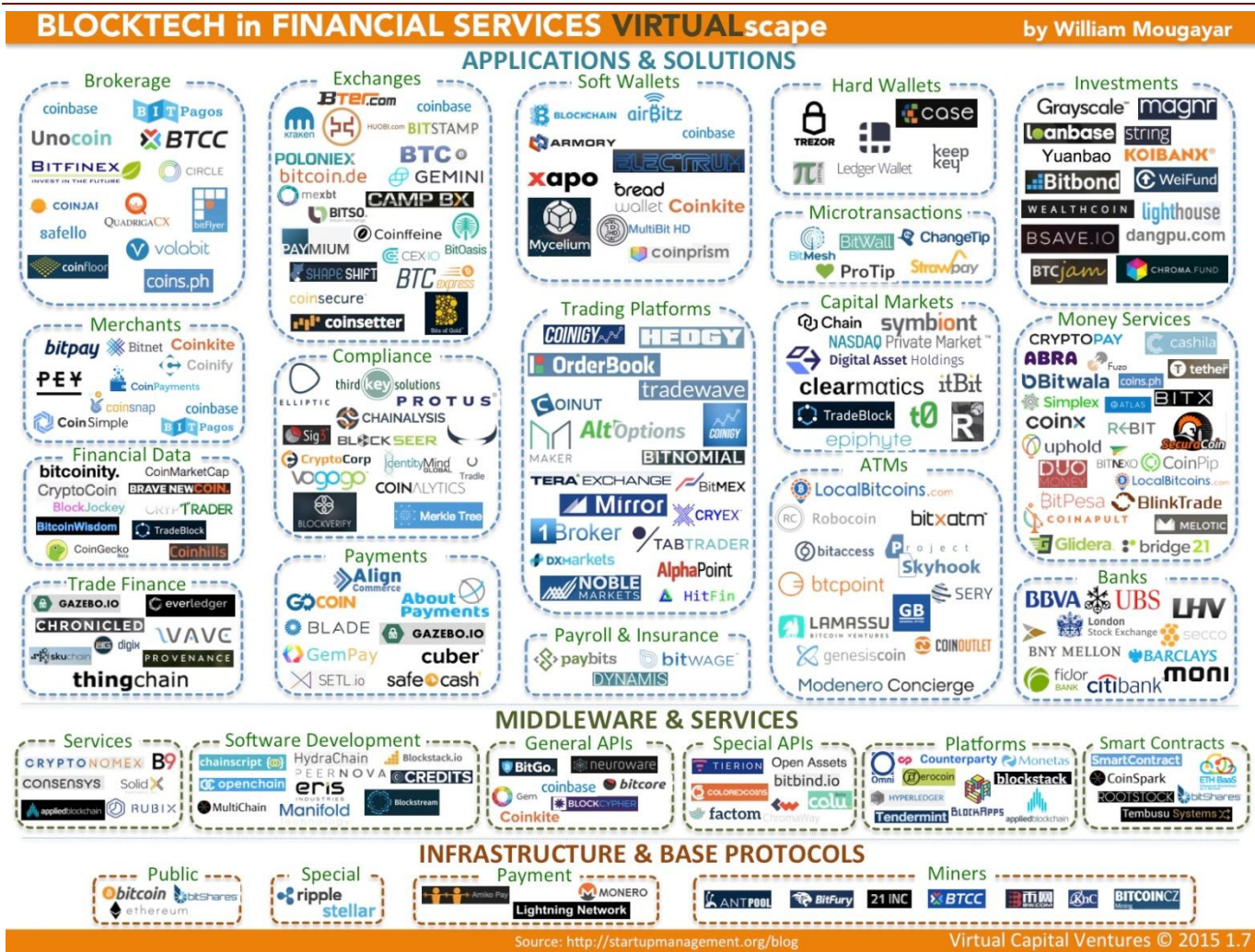
图表 11：创投活跃，已累计 10 亿美元 VC 投资



资料来源：Magister Advisors



图表 12：不仅创业企业涌现...



资料来源：William Mougayar

图表 13：传统金融机构也纷纷以内部研究、外部结盟和投资的方式，布局区块链

Company	Description	Financial Institution Investors
Digital Currency Group	Digital currency asset management firm, OTC trading and start up investor	MasterCard, New York Life Investment, TransAmerica Ventures, CIBC
Ripple	Cryptocurrency-based payments system	Santander InnoVentures, CME Ventures
Digital Asset Holdings	Developer of Distributed Ledger Technology for the financial services industry	JPMorgan, Citi, BNP Paribas, ABN AMRO, Santander, ASX Limited, CME Venture, The Depository Trust & Clearing Corporation (DTCC), PNC Financial Services Group
Consortium	Description	Financial Institution Members
Open Ledger Project	Led by Linux Foundation, to develop an enterprise grade, open source distributed ledger framework	J.P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group, State Street, Wells Fargo, DTCC, SWIFT, ANZ Bank
R3 CEV	To design and develop commercial products and financial-grade distributed ledger solutions that incorporate various open source technologies and standards	Banco Santander, Bank of America, Barclays, BBVA, BMO Financial Group, BNP Paribas, BNY Mellon, CIBC, Commonwealth Bank of Australia, Citi, Commerzbank, Credit Suisse, Danske Bank, Deutsche Bank, J.P. Morgan, Goldman Sachs, HSBC, ING Bank, Intesa Sanpaolo, Macquarie Bank, Mitsubishi UFJ Financial Group, Mizuho Financial Group, Morgan Stanley, National Australia Bank, Natixis, Nomura, Nordea, Northern Trust, OP Financial Group, Scotiabank, State Street, Sumitomo Mitsui Banking Corporation, Royal Bank of Canada, Royal Bank of Scotland, SEB, Societe Generale, Toronto-Dominion Bank, UBS, UniCredit, U.S. Bancorp, Wells Fargo and Westpac Banking Corporation
Post Trade Distributed Ledger Working Group	Exploring how blockchain could be used to run post-trade processes	London Stock Exchange, LCH.Clearnet, Societe Generale, CME Group, UBS, Euroclear

资料来源：公司网站



Fintech 2.0，革新金融业基础架构

Fintech 2.0，从根本上革新金融业基础架构

在区块链受到重视以前，金融业已经迎来了一次不小的互联网革命。然而，正如我们在《独角兽启示录（3）：硅谷挑战华尔街》中所言，Fintech 创业公司凭借的往往只是更优化的用户界面（如 Stripe 和 Square）、细分的市场定位（Wealthfront 和 Transferwise）、有利的经济环境和监管套利（LendingClub 和 OnDesk），却远远没有触及金融行业的底层架构和基础设施。

但区块链有望改造金融基础设施，释放存量市场的活力。美欧金融市场的 IT 架构都为上个世纪的遗留，因此中间程序复杂、迟滞时间长。例如，银行间小额国际汇款的手续费是 7.68%，而区块链可以使其下降到 1% 以下。美国国库券交易的结算周期是 T+1，而股票、公司债券、共同基金份额等证券的结算周期是 T+3。全球资本市场每年花在交易以后的中后台交割结算成本是 650~800 亿美元。根据 Santander 的研究，区块链的应用在 2020 年就可节约 150~200 亿美元的交易中后台成本。

区块链也可以服务发达和欠发达地区尚未享受现代金融服务的人群，发掘增量市场。FDIC 报告称在美国有 5,000 万成年人没有银行账户，6,800 万成年人金融需求没有得到充分满足。而在肯尼亚和菲律宾已经发展出了以比特币为桥梁的国际汇款工具，使没有银行账户的人们，通过手机 App 就能跨境收发当地货币的款项。IMF 报告认为区块链对扩大金融共享（financial inclusion）大有帮助。

具体而言，对于改造金融基础设施，区块链的好处包括：

- ▶ **更快的结算周期，降低对手风险。**区块链的机理使交易确认与结算是同时进行的，无需交易双方（或多方）在交易确认后还需要各自核对账目。在交易通过 POW 或 POV 验证之后，新的区块将写入分布式账本，所有节点的账本将同时更新，所有节点依然共享完全一致的账本。在区块链以前，DTCC 和 BCG 的 2012 年报告曾经估算过，将美国股票结算由 T+3 改成 T+2 需要花费 5.5 亿美元的初始投入，3 年回收期。而改成 T+1 需要 18 亿美元投入，10 年回收期。目前业界正在讨论往 T+2 改变。DTCC 近期报告肯定了区块链在加快结算周期上可以起到的作用。
- ▶ **去中介化。**区块链使 Delivery versus Payment（DVP）更加方便，无需中介机构确保“交钱的人有钱，交货的人有货”和“一手交钱，一手交货”。
- ▶ **标准化的交易验证过程，可使用不同复杂程度的金融产品。**基于区块链构建的交易结算系统具有广泛的适应性，其交易验证过程是标准化的，既可用于简单的现券交易，也可用于复杂的衍生品交易。
- ▶ **减少人工，提高自动化。**许多金融交易目前还以人工为主，区块链则完全通过网络和结算能力实现交易中交易后的全过程。例如，纳斯达克对区块链的实践首先从未上市的私有公司股权交易开始，就正是由于此前这类交易都只能通过律师手工完成，手工在简易的 Excel 里记录。此外，以区块链为基础延伸的智能合约（Smart Contracts，运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值），又能把交易前的步骤自动化。智能合约可以把许多复杂的金融衍生品合约条款（往往以外部事件为触发点）写入计算机程序，进行自动执行。
- ▶ **降低系统性风险。**金融危机的爆发往往从金融机构的短期流动性危机开始。而容易出错的人工操作、冗长的结算周期和各家银行分散的账本记录（在对 08 年金融危机的事后调查中发现，万亿美金的 CDS 市场是各银行手写单据、传真机传送进行交易和记录的）无疑增加了流动性风险。区块链不仅可以缩短结算周期、提高自动化，以区块链发行、交易、结算的电子证券（digital securities）还可以实时定价，自动计算保证金要求，甚至在条件触发时自动终止平仓。



- ▶ **降低系统遭到攻击而被破坏的可能性。**目前防止系统宕机的主要方式是多处备份和多套系统（redundancy）。而区块链分布式的特点自动满足了这一安全性要求。
- ▶ **保存监管记录和审计痕迹。**每一个区块记录都包含有完整的时间戳，可以满足金融监管中记录存档要求，以及内外审计中的留痕要求。英国监管部门 Financial Conduct Authority (FCA) 甚至表示，区块链的应用将有助于减少监管负担，是所谓的 RegTech 创新，即技术创新为监管提供了新的工具。金融危机后，金融机构和监管机构的负担大大加重，文件处理量也大量增加。而区块链智能合约里可以在代码层面实现合规，而不再只是事后检查。
- ▶ **可以 7*24 小时运转。**

当然在实际应用中，现有的区块链还存在一些问题，需要相应改进：

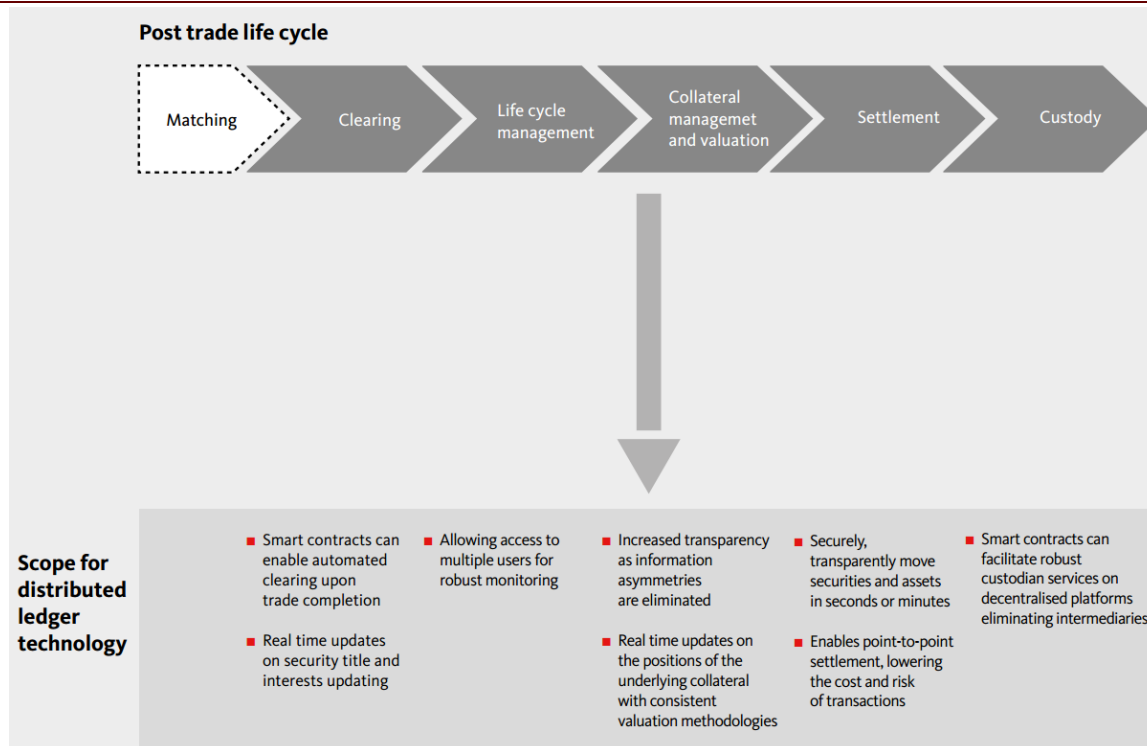
- ▶ **事后不可追索。**不可篡改是区块链的一大好处。但在实际应用中，却造成了无法事后追索的问题。一旦区块写入，就不能修改或取消，而一定需要进行新的一笔逆向交易。因此在构建区块链的交易结算系统中，需要预先设置追索机制和例外机制。
- ▶ **无法以净头寸结算。**DTCC 和 NSCC (the National Securities Clearing Corporation) 都是以每日交易各方的净头寸进行清算交收的，区块链 P2P 的特点需要对每笔交易进行结算，可能增加交易者的资本金和抵押品要求。目前许多以金融交易为目标市场的区块链创业公司已经正在解决这个问题。
- ▶ **无法融券。**区块链在解决双重支付问题时会验证交易者的物权完整性。但许多金融资产的交易原本允许融券交易（如卖空）。目前这个问题也正在解决中。
- ▶ **缺乏互换性（Fungibility）。**第一个基于区块链的公开股票发行已由美国电商公司 Overstock.com 完成。但其 SEC 文件的风险项中列有“该股票不能与公司的其他传统股票互换”。Overstock 是把其按传统方式发行和交易的股票，与以区块链发行和交易的股票分在了不同等级。未来区块链的数字证券发行也有可能解决这个问题。
- ▶ **交易令牌以及实际资产的匹配。**区块链上交易的或许是数字化/令牌化后的真实资产，在需要实物交割的场景下，区块链的优点将大大下降。
- ▶ **智能合约自动执行可能影响金融稳定。**与高频交易类似，智能合约也可能会有自我反馈循环（self-reinforcing feedback loop）的特点，会放大价格波动。

综合以上优缺点，区块链在各项金融业务的适用性和潜在影响的大小可以通过以下条件判断。DTCC 近期也发布报告称，区块链特别适用于证券发行和后续服务、清算、交收结算、复杂金融合约的交易、记录和对照，抵押品管理等。

- ▶ 资产是否可以电子化？
- ▶ 是否需要互无信任基础的多方参与，而原来需要可信任的中介机构？
- ▶ 是否不同交易之间存在关联？例如，后一笔交易需要前一笔交易完成后（利息本金的偿还在借款之后，赎回在发行之后）。
- ▶ 是否需要接近实时的结算，但又允许一定的延迟（latency）？
- ▶ 合约是否复杂？是否隐含较大的对手风险？
- ▶ 是否原来是劳动密集、资本密集？
- ▶ 是否需要共享记录？

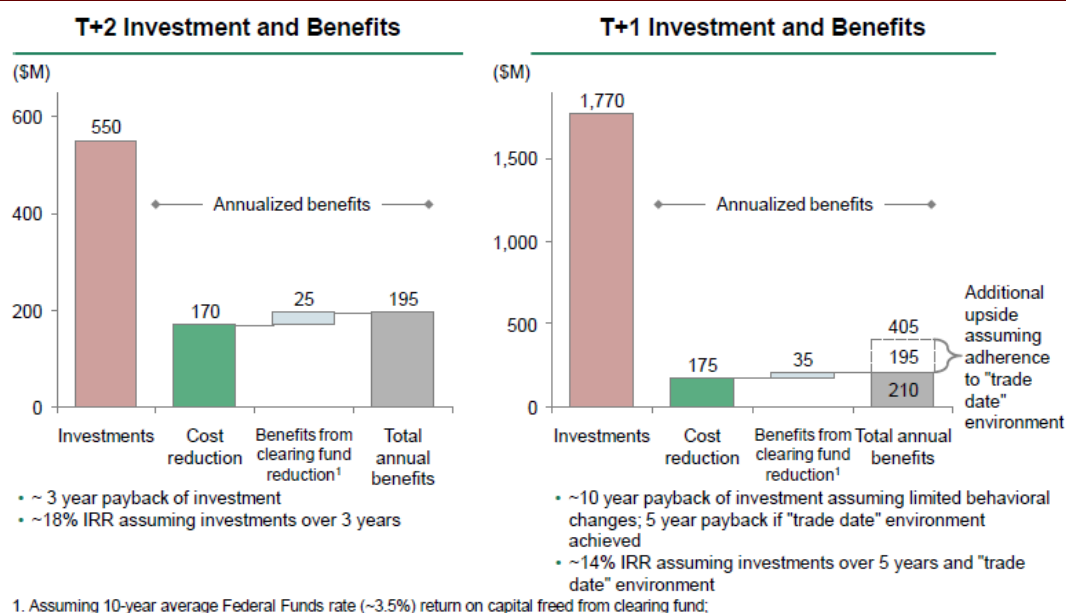


图表 14：区块链将大幅提高金融市场效率，到 2020 年可节约 150~200 亿美元金融机构中后台成本



资料来源：Santander “The Fintech 2.0 Paper: Rebooting financial services”

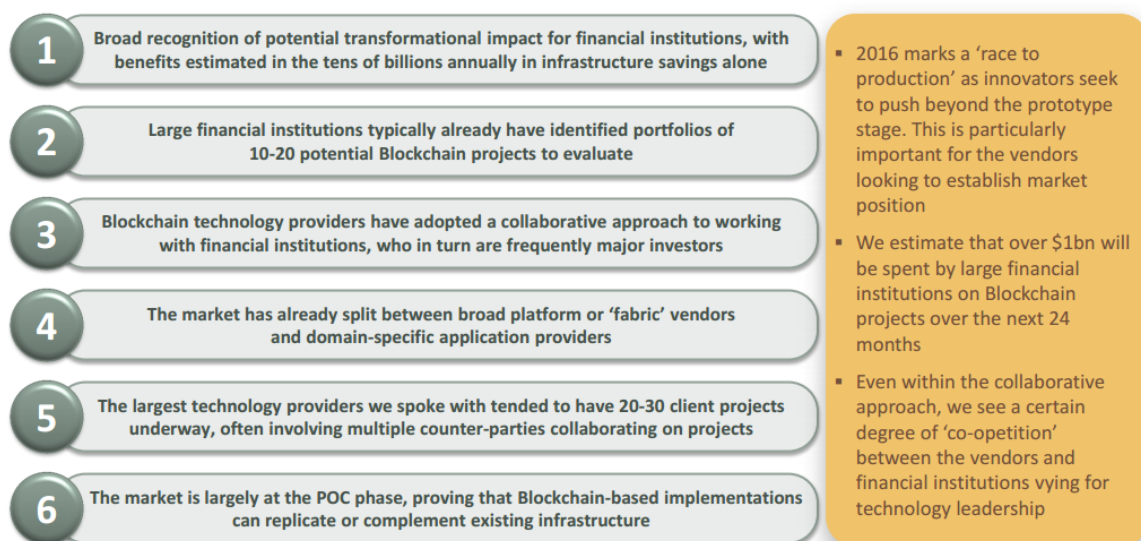
图表 15：而在区块链之前，缩短结算周期需要大量初始投入



资料来源：DTCC & BCG “Cost benefit analysis of shortening the settlement cycle”

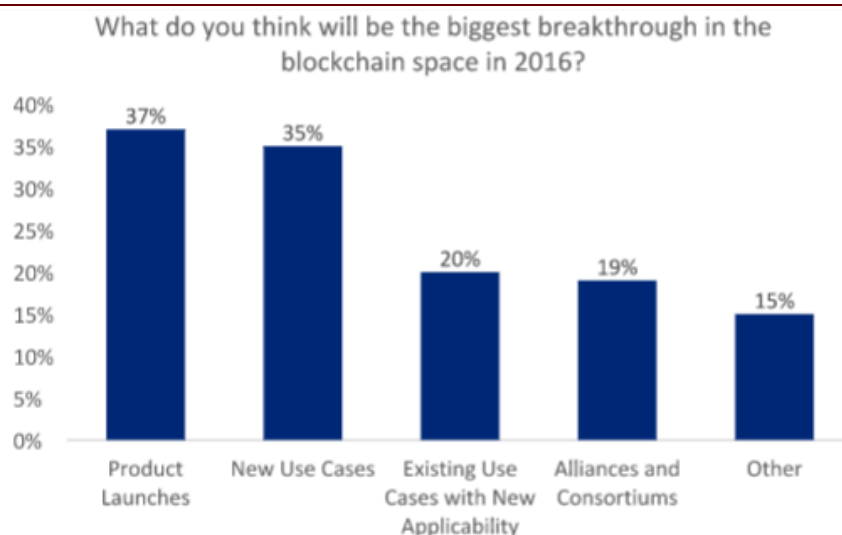


图表 16：虽然目前大多处在概念验证、内部测试阶段，预计 2016 年以后将竞相商业化



资料来源：Magster Advisors

图表 17：预计 2016 年以后将竞相商业化



资料来源：Deloitte

开始商用或测试的应用领域包括跨境支付、证券交易结算和发行等

从云计算到开源软件到第二代信息安全技术，我们其实看到，华尔街在新技术应用、推广甚至研发上，越来越紧跟前沿。而有鉴于区块链的潜在影响，金融机构也已开始主动研发。几乎所有欧美大型金融机构当前各自都有 10~20 个项目在开发测试中，对外投资和联合也不遗余力。即使是理论上会受到区块链影响的 DTCC，不仅参与了 Open Ledger Project 联盟，投资了 Digital Asset Holdings，还发表研究报告，宣称自身可以在这次金融设施革新中发挥组织者的作用。从初创企业来看，Ripple 等一些原来尝试 2C 虚拟货币的创业企业，也把战略聚焦于为金融机构提供 2B 服务之上。

虽然目前大多数的应用案例都还处于测试阶段（prototype, proof of concepts），尚没有任何一个区块链网络进入了大规模商用。但今年我们将会看到更多商业化的实践。此外，行业联盟还会继续推进，以拟定统一的行业标准，保证各自系统的互联互通性。



当前已经商用或测试的应用领域包括跨境支付、证券交易结算和证券发行等。而证券交易结算中又以自动化程度较低、复杂度较高的私有股权、辛迪加银行贷款、ABS、国债回购为先行尝试。

Ripple: 为金融机构提供跨境支付和外汇市场做市的区块链解决方案

Ripple 专注于跨境支付领域，主要为银行和其他金融机构提供基于区块链协议的外汇转账方案。目前已公布的银行客户有 3 家，并正在和另外 80 多家银行深入洽谈。Ripple 主要通过其开发的“InterLedger”协议项目，在保持银行等金融机构的各自不同的记账系统的基础上，打造一个全球统一的网络金融传输协议。其系统特点包括：

- ▶ **Interledger 协议建立不同记账系统沟通桥梁。**在 Interledger 协议系统中，两个不同的记账系统可以通过第三方“验证端”来互相自由地传输货币。目前，Ripple 为不同银行提供 Connect 软件，接入 Ripple 网络，进行货币传输。不同银行不需要采用统一的记账系统，可以保持原有的记账系统，同时银行间的交易可以隐藏起来，“验证端”是通过加密算法来进行，不会看到交易的详情，只有银行自身的记账系统可追踪交易的详情。这保证了银行的私密性和安全，而银行只要做小小改变就可使用该协议。
- ▶ **分布式记账系统提供去中心化支付。**在传统模式下，不同银行之间的支付转账，为了减少资金流动，必须通过中央结算系统作为交易对手进行记账和净额结算，因为需要中央结算系统作为信任中心。在 Ripple 网络中，统一的分布式记账系统通过许多节点以共识机制来验证交易并记账，不需要任何信任中心。通过这样分布式的网络，可以：1) 支付 7 天 24 小时全天候进行；2) 支付更加实时，一般几秒就可完成，改变传统需要几天的延误；3) 减少支付准备金（传统需要多个准备金账户，而 Ripple 只需一个），从而减少资金占用。
- ▶ **做市商为跨货币支付提供流动性。**在传统的模式下，往往除了同货币汇款所需的环节，还需要一个中间银行 correspondents 的角色，该中间银行拥有不同的货币账户，协助双方进行货币兑换，导致了跨货币处理更慢同时成本更高。在 Ripple 网络下，由银行、货币兑换商等金融机构扮演做市商，只要有足够的做市商，便能为 Ripple 网络提供足够的流动性，从而实现点到点的直接支付。做市商网络可以带来以下好处：1) 减少成本，汇款银行可以选择自己信任的做市商，只要做市商足够多，理论上会提供具有市场竞争力的汇率水平，同时 Ripple 网络也通过算法寻找最优汇率水平；2) 加快效率，做市商网络能随时随地为跨境支付服务。
- ▶ **基础货币充当安全卫士和桥梁货币。**在 Ripple 网络中，将存在美元、欧元、人民币等各种法币和比特币等各种电子代币，而 Ripple 的基础货币 XRP 则充当黄金和美元曾经在传统金融货币体系中的角色，与所有货币建立联系，这样一个货币只要能与 XRP 建立联系，就能与其他任何一种货币建立联系。瑞波币还担任着网络的安全卫士，瑞波币固定为 1,000 亿个，每个 Ripple 账户要求至少持有 20 个瑞波币（约为 0.1 美元），每次交易需销毁 0.00001 个瑞波币，但外界进行额外攻击时，系统会识别到交易量的持续大幅提升，“验证端”会形成销毁币数增加的一致意见，从而导致需销毁的瑞波币快速上升，迅速消耗攻击者的瑞波币，导致攻击的成本极高。

纳斯达克 Linq: 私有股权的区块链交易平台

纳斯达克通过与区块链初创企业 Chain.com 合作，已正式上线了用于私有股权交易的 Linq 平台。

此前未上市公司的股权融资和转手交易多是律师通过 Excel 表格手工完成，出错率高，又难以留下审计痕迹。成立于 2014 年的 Nasdaq Private Markets 主要提供未上市公司股权的转手交易。近年来，独角兽数量的增多（参见报告《独角兽，本轮科技泡沫的显著特征和可能收场》）使此类私人股权交易活动日益活跃。



而 Linq 平台不仅帮助私人股权的交易交收，还提供了界面优化的数据分析工具 Equity Timeline View，使发行公司可以看到详细的资本结构表（Cap table），可以按日期、投资人名称进行检索，可以点击查看某一张股权证明的细节等。

去年 12 月 30 日，Linq 平台完成了首次交易，由 Chain.com 公司向某未具名投资人发行了股份。目前 Linq 平台上发行公司还有 ChangeTip、Peernova、Synack、Tango 和 Vera 等。扩大用户群的主要难点在于帮助发行公司完成股权的电子化和向新系统的迁徙。

除了纳斯达克以外，初创公司 Symbiont 也于去年 8 月在其 Smart Securities 平台上发行了股权。澳大利亚交易所 ASX 也刚刚委托初创公司 Digital Asset Holdings 开发交易结算系统。

Overstock tØ: 首次用区块链发行债券和股票

Overstock 创建了 tØ 区块链交易平台，证券无需通过纳斯达克等交易平台，直接在区块链上完成交易。2015 年 7 月，Overstock 向 FNY 资本的子公司销售首个区块链上的加密债券，10 月，有 5 个客户通过该平台借出股票。2015 年 12 月，美国证券交易委员会（SEC）已批准在 Overstock 通过区块链来发行本公司的股票。

高盛：SETLcoin 专利，用于证券交易结算

高盛以比特币区块链为蓝本，开发了通过加密货币进行证券交易结算的系统，称之为 SETLcoin（Settle + Coin）。高盛于 2014 年 10 月 30 日向美国专利商标局递交专利申请，后者于 2015 年 11 月 19 日将专利申请文件公开。

除高盛以外，美洲银行、摩根大通、万事达等都有关于加密货币和区块链的专利申请。其中美洲银行已经公开的专利申请就有 20 项之多，涵盖基础设施、电子钱包、风险识别、加密安全等等。

就高盛的 SETLcoin 而言，SETLcoin 的交易通过钱包软件来进行，并利用 SETLcoin 代币来代表特定的证券。交易者将他们的资金放于各自的虚拟钱包当中，通过 SETLcoin 系统实现开放式的证券交易。在经过核查和验证之后，SETLcoin 的所有权立即传送到新的所有者手中，保证了几乎瞬时的执行和结算。交易中的核查验证通过两阶段承诺协议（two phase commitment protocol）和一对公开和私密钥匙（public/private keys）进行。这套系统同样也可以用于虚拟钱包与非虚拟钱包之间的 P2P 交易。

UBS: Smart Bonds 债券发行和交易平台，并无偿捐助 HIV 研究

UBS 于去年 9 月完成测试并推出了 Smart Bonds 系统，用于各类债券的发行和交易。今年 1 月公司宣布将这一系统的代码无偿捐献伦敦的一家区块链初创企业 Finclusion。后者将在 Smart Bonds 代码的基础上为 HIV 研究机构 HEAL Alliance 发行 25 年期的 100 亿美元债券，为 HIV 研究和社区治疗中心的发展募集资金。这套系统将于 1 月 21 日到 4 月 20 日进行测试，并受到英国 FCA 的支持。

此外，德意志银行也于去年 12 月完成了一个内部测试，用区块链模拟完成了公司债发行、利息支付和赎回的全过程。公司认为，这样的系统未来 2 年内一定会商业化。



Digital Asset Holdings: 金融区块链创业企业明星

Digital Asset Holdings 成立于 2014 年，由前 JP Morgan 高管、被誉为 CDS (Credit Default Swap) 的发明者的 Blyth Masters 创立，因而备受业界关注。今年 1 月公司获得了来自 DTCC、JP Morgan、花旗、ASX 等 13 家金融机构 5,000 万美元投资，并被澳大利亚交易所 (ASX) 委任开发股票中后台交收结算系统。公司的核心技术来自于此前收购的 Hyperledger，并已将其开源，贡献给由 Linux Foundation 牵头的 Open Ledger Project。

Hyperledger 是带有客户 API 接口的企业级的区块链服务器。Hyperledger 采用只能追加的金融交易日志，复制分享于多个金融机构，而无需中心控制。它是由在金融机构工作数十年的团队，按照企业架构的要求建立的，在代码和运行上拥有高度模块化的设计，以便与遗留系统集成。它虽然采用与比特币区块链同样的 UTXO/script 脚本，但以拜占庭容错共识取代了工作量证明机制，使其可以兼容更多应用。

Digital Asset Holdings 正在研发的金融业解决方案，除了股票结算以外，还包括国债回购、辛迪加贷款等。

劳合社：将区块链容纳进保险市场的现代化改造计划

老牌保险按组织劳合社 (Lloyd's of London) 于去年开始了名为 Target Operating Model 的现代化计划。而区块链被劳合社视为可以将保险市场脱离纸张、去中心化的重要工具，纳入现代化计划的一部分。目前劳合社开展的实验包括由区块链驱动的交易室和以代币为桥梁的保险市场联盟链。由区块链驱动的交易室可以使远在千里之外的国际保险公司参与分保、再保交易，可以安全的分享文件，也不需要中立的中间方进行记录。

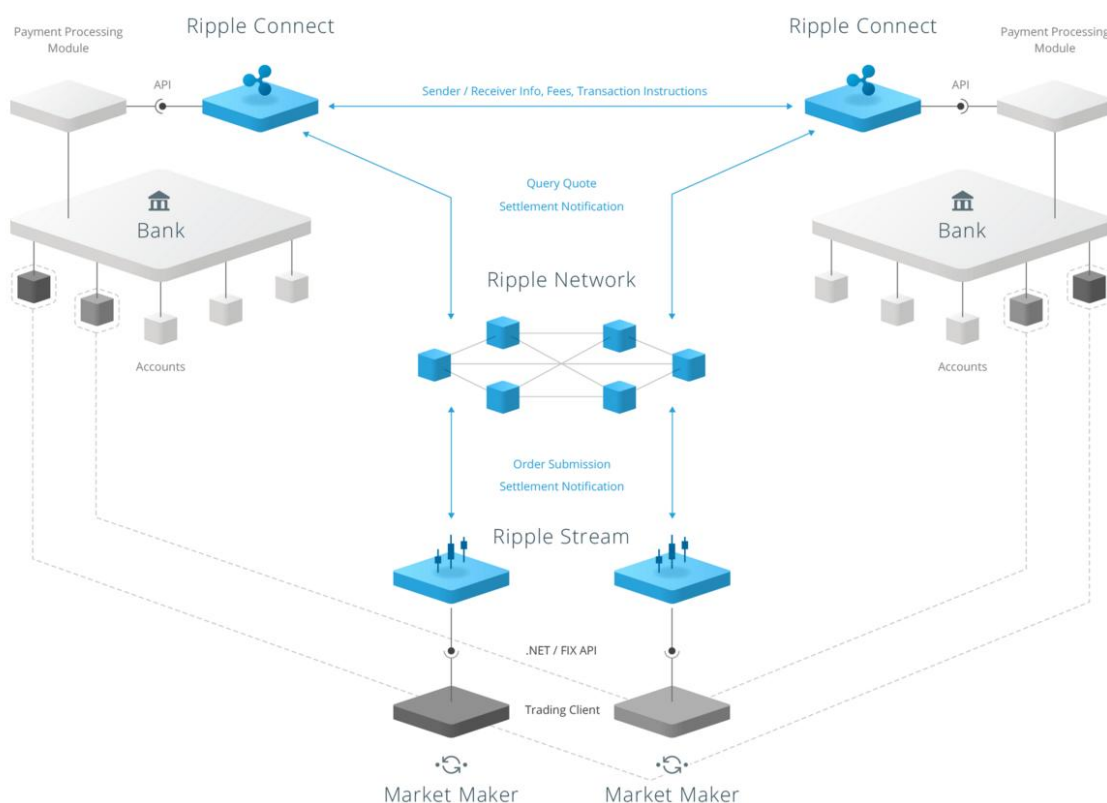
埃森哲的一份报告认为，区块链在保险上的应用会晚于银行，因为用途还不够明确。但是，区块链还是可以用于投保物追踪、产权保险、个性化保险合同，以及智能合约自动执行等。

Hedgy: 智能合约交易比特币衍生品

Hedgy 是一家比特币衍生品初创公司，开发了全球首个基于区块链技术的智能合约平台。该平台取代传统柜台交易模式，将合约创建、资金临时监管、合约签署和合同清算一系列程序智能化。Hedgy 一直努力研发比特币衍生产品和工具，是全球第一个推出能够为矿工解决比特币价格波动性的商业对冲工具，此后利用 Multi Signature Technology 设计了比特币价格预测、锁定等衍生工具。2015 年 4 月公司宣布完成 120 万美元融资，此次融资包括此前来自 Boost VC Tribe 4 的 76 万美元，其他资金来自由 10 名投资者组成的团队，包括 Draper Fisher Jurvetson 合伙人 Time Draper、Salesforce CEO Marc Benioff 和 Sand Hill Ventures 等。

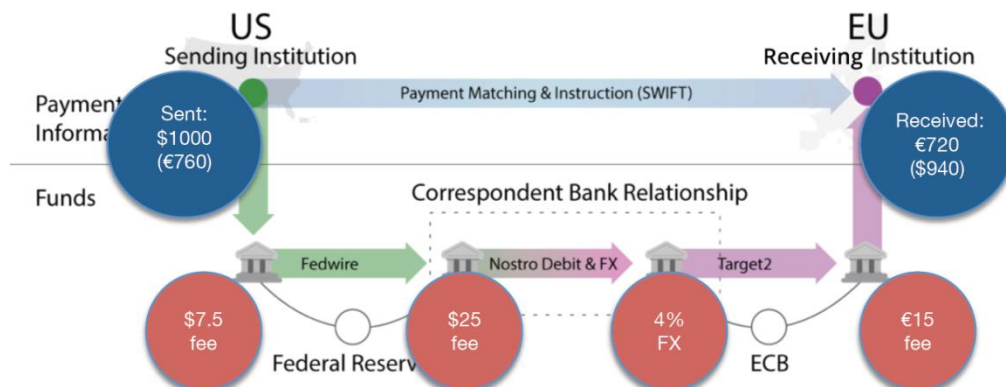


图表 18: Ripple 为金融机构提供跨境支付和外汇做市的解决方案



资料来源: Ripple 公司网站

图表 19: ...比现有系统速度更快、成本更低

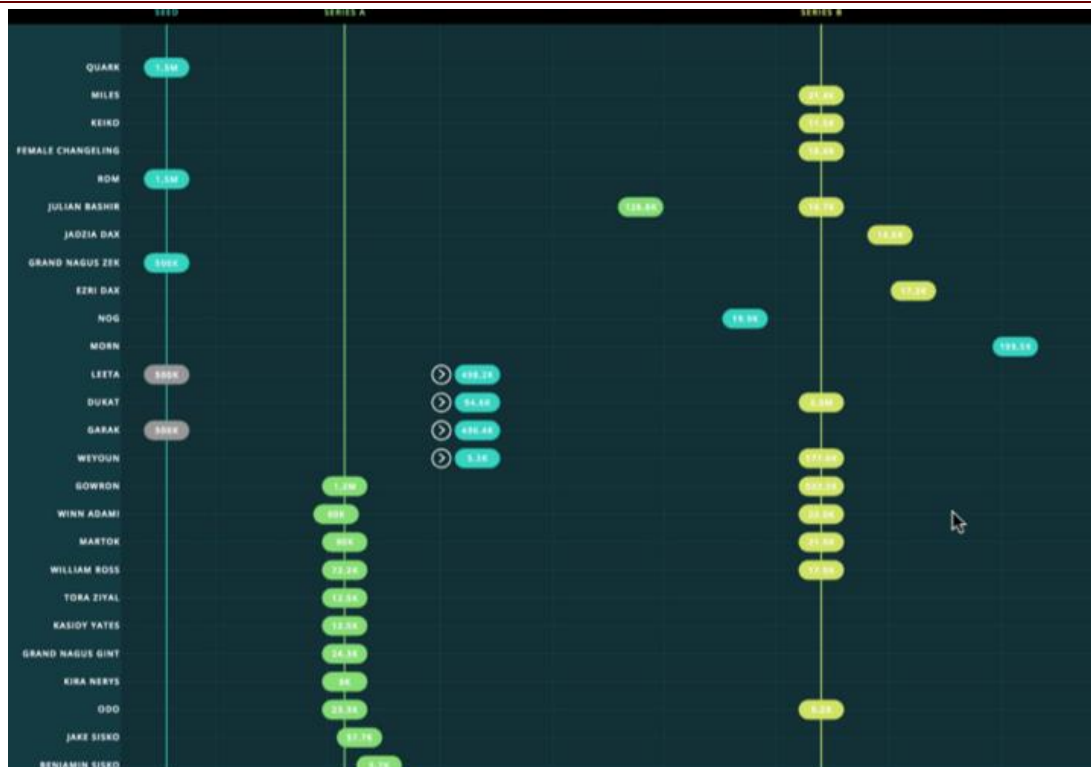


	SWIFT	Bitcoin	Ripple
Architecture	Centralized	Decentralized	Decentralized
Settlement Process	Batch clearing & settlement	Proof of Work	Consensus
Speed	2+ business days	10 - 60 minutes	3 - 6 seconds
Peak Volume	19mm Messages/Day ¹	600,000 Transactions/Day ²	86mm Transactions/Day [RL Est.]
Currency	Fiat currencies	BTC only	Universal
Transaction Cost	Operator fees	Mining fee	Security Cost

资料来源: The Ripple Protocol: A Deep Dive for Finance Professionals

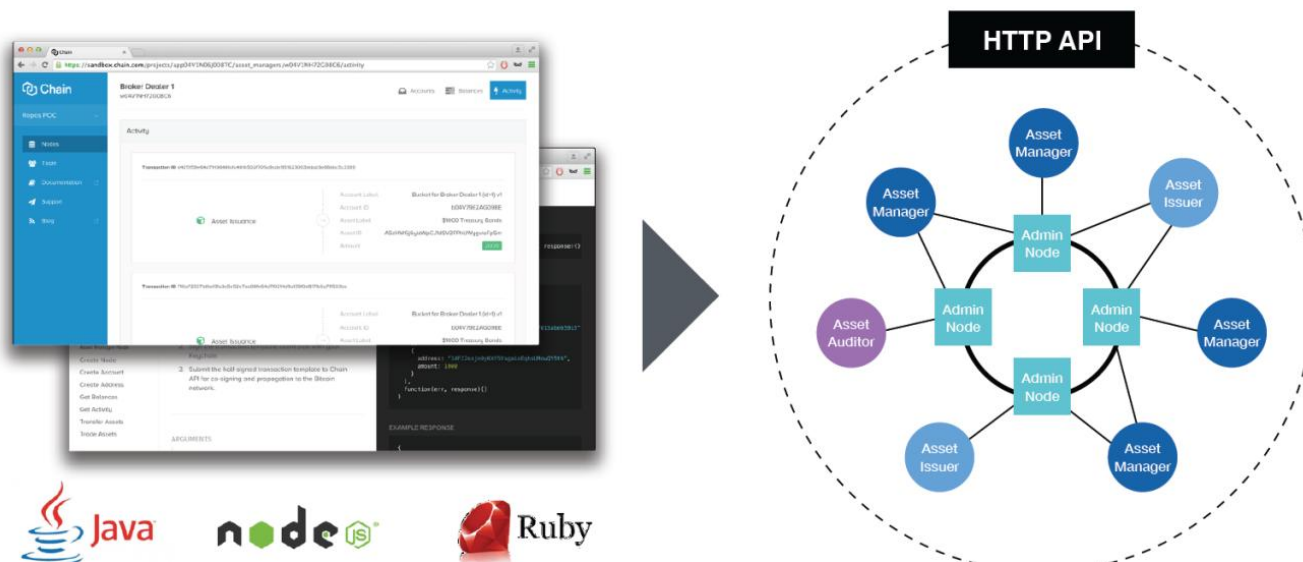


图表 20：纳斯达克开始用基于区块链的 Linq 平台，交易私有股权



资料来源：CB Insights

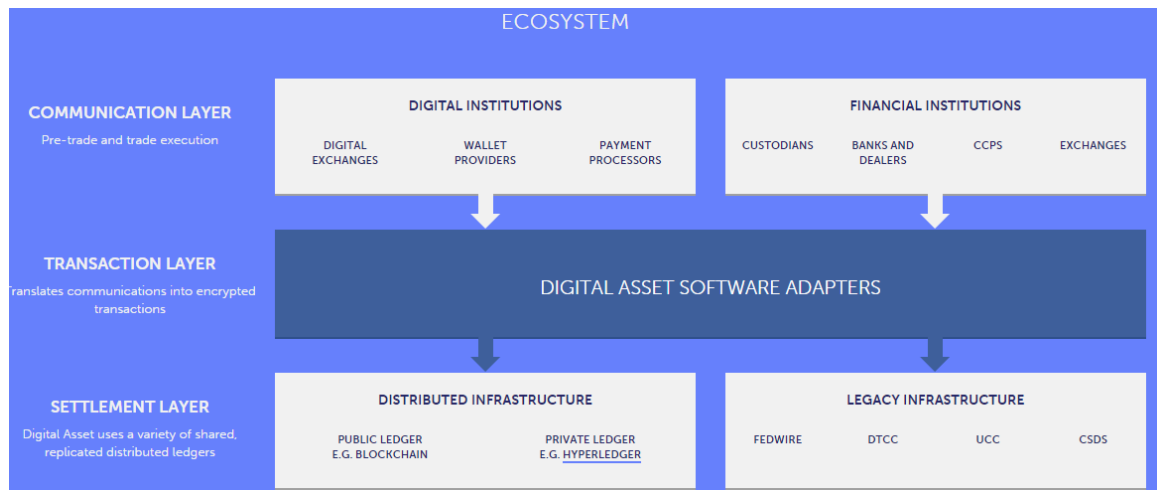
图表 21：除了与纳斯达克 Linq 合作以外，Chain 还提供国债回购解决方案



资料来源：Chain 公司资料

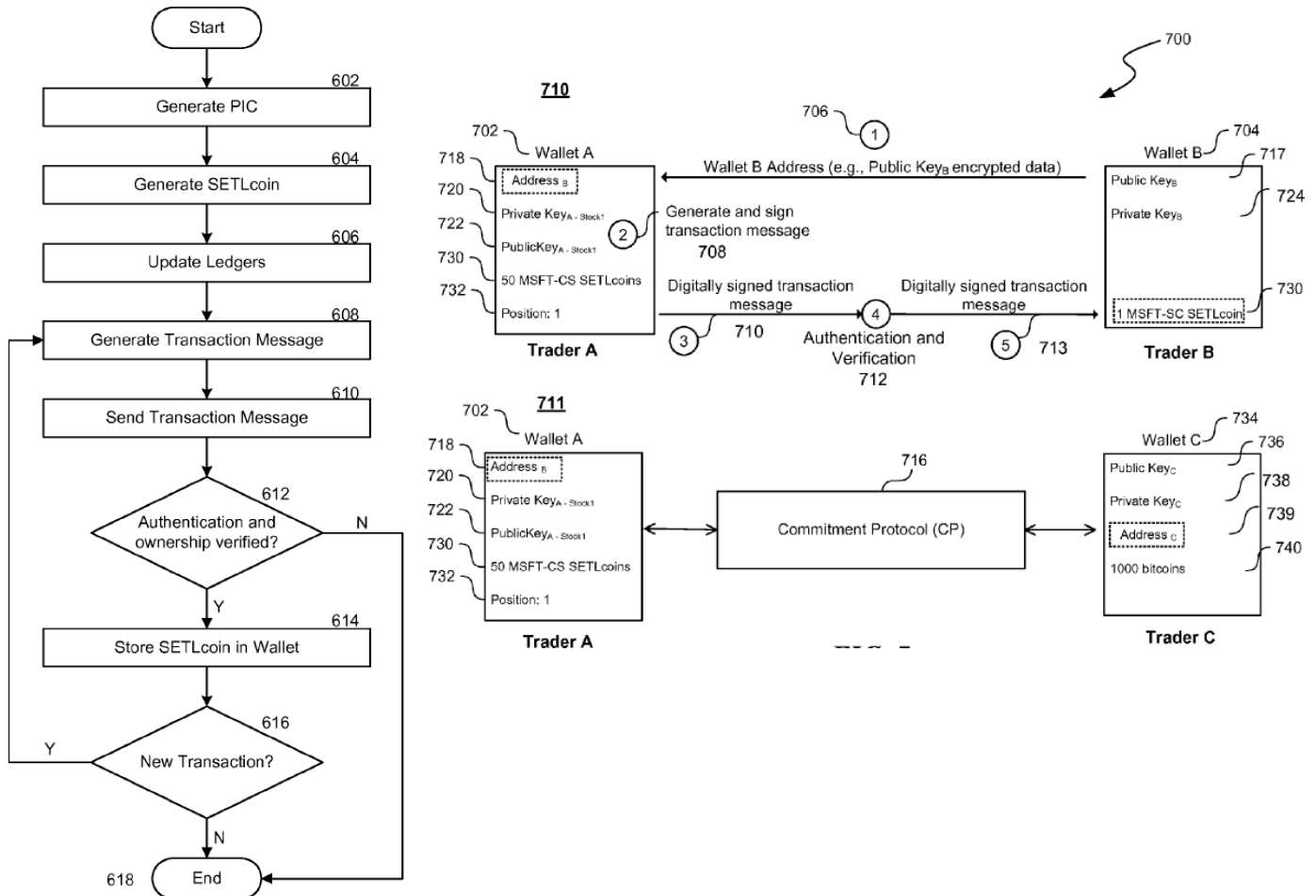


图表 22: Digital Asset Holdings 提供企业辛迪加贷款、国债回购、股票交易结算等解决方案



资料来源: Digital Asset Holdings 公司网站

图表 23: 高盛开发了金融资产交易交割系统 SETLcoin, 并申请专利



资料来源: 高盛专利申请文件



将冲击或改造金融机构商业模式

区块链的广泛应用在提高效率、降低成本的同时，也会对金融机构的商业模式提出挑战。一些机构的职能将被替代，转型，或者强化。

- ▶ **清算所在过渡时期作用重大：**区块链去中心化的机制，会最终取代清算所的现有职能。但是在渐进式发展中，清算所将依然会起到独立清算的作用。而在许多金融衍生品市场上，清算所目前是所有市场参与者的交易对象，保证市场的流动性和有效性。在智能合约充分成熟之前，清算所这一职能还不容抹杀。美国 DTCC 也正积极参与区块链的讨论，认为其自身 40 多年的经验、独特的所有权和管治结构，需要在这次资本市场基础设施革新中发挥领导作用。
- ▶ **存托所功能强化：**区块链的推行可能使更大量的资产数字化，会使存托所的功能受到强化。而且存托所可能还需要在将区块链中的代币与真实资产同步交易的过程中充当角色。
- ▶ **交易所面临差异化竞争：**区块链虽然使交易执行点对点和自动化，将催生更多的交易场所和卖方主导的拍卖交易，但交易所具有的价格发现和交易匿名两个功能是区块链无法实现的。此外，目前比特币区块链和以太坊区块链都没能达到算法交易所要求的毫秒级交易。
- ▶ **投资银行承销业务受到影响：**区块链将便于发行公司以拍卖的方式发行股票或债券（谷歌 IPO 就是公司自己进行拍卖），会打击投行的承销佣金业务。然而，投行在兼并收购、资本中介等其他方面的业务不会受到影响。
- ▶ **商业银行提高效率：**商业银行的贷款业务和支付业务都可能因为使用基于区块链的解决方案而降低成本，提高效率。然而，目前关于国家中央银行发行虚拟货币的讨论越来越多，一旦付诸实践，商业银行在由央行主导的 Fiatcoin/Fedcoin 支付体系中的职能地位尚不明确。
- ▶ **主办经纪商部分职能被弱化，但其他职能被强化：**Prime brokers 一般为对冲基金公司提供信用中介、资产托管、融资融券等一揽子服务。区块链应用之后，资产托管和信用中介职能将被取代，但融资融券的职能却可能被强化，利好资产负债表强劲的 prime brokers。
- ▶ **交易执行经纪商效率提高，但也面临新的竞争：**Executing brokers 会因为区块链带来的结算周期缩短、交易系统稳定而享受到效率提高的好处。然而可能会有新的公司以自有区块链技术参与进来，为买方提供更快捷的服务，使 executing brokers 的做市商交易（principle trading）业务面临新的竞争。
- ▶ **投资者/资产管理公司手续费下降，中后台简化：**作为资本市场的买方，资产管理公司应该能享受到市场基础设施升级的好处，包括对手风险下降、手续费下降、流动性风险降低等。当然，资产管理公司自身的中后台流程也会得到简化，相关部门受到影响。



帮助物联网落地，实现智慧政府，构建自治社会

帮助物联网落地

物联网的概念虽然已流行多年，但实际应用依然很少，普及依然很低。而区块链以及其基础上构建的智能合约，有望解决物联网应用中的一些难题，实现效率和规模化，帮助物联网落地。

- ▶ **设备无法互联互通，或者联网成本高：**物联网的价值就在于智能设备在需要时共享数据，完成操作。但目前不同厂商设备之间的连接性依然存在问题。而且长远来看，目前中心化的网络虽然可以适应十亿级别的移动互联网设备，但对于百亿甚至万亿级别物联网设备来说，速度和成本都难以支持。
- ▶ **物联网硬件产品维护成本过高：**从大型机到智能手机，在硬件出售后，都会由厂商或关联方提供售后维护支持。然而，百亿甚至万亿的智能设备的维护支持成本过高，后市场缺乏商业模式支持。
- ▶ **网络安全性、隐私性：**智能家居、车联网等普及的另一障碍就是消费者所担心的网络安全和隐私。

区块链对于物联网的意义就在于，为物联网中数以亿计的设备之间**建立低成本的、P2P 直接的沟通桥梁**，又通过去中心化的共识机制保证了信息的**安全性和私密性**，但同时又做到开放和透明化的数据管理。IBM 预计 2025 年之后，物联网将摆脱对中央控制系统的依赖，实现设备之间的实时交流，无需担心原本中心化架构中政府、工程师、设备制造商、服务提供商等各个环节参与者所带来的数据信息安全问题，同时还能大幅降低物联网信息交互、存储和管理产生的成本。

智能合约对于物联网的意义在于，**使智能设备成为自我维护、自我调节的独立个体**，能够自主的与其他设备核实身份、交换信息，并按照事先拟定的规则合约，执行相应的动作。

- ▶ 当一个物联网设备从生产线上完成最后的组装成为成品时，制造商就会在区块链上登记产品出厂信息，赋予该产品“生命”。一旦产品售出，消费者可以在区域区块链上再次登记产品，那么该产品就会拥有属于自己独特的身份识别。
- ▶ 设备运行出现故障时便会自动在区块链系统中查看出问题的部件是否在保修期，自行向服务提供商下单购买更换的部件。
- ▶ 设备还能够根据能耗分析，自动与其他设备进行交涉，重新分配能耗。若洗衣机运行时用户电视机处于关闭状态，可要求降低电视机能源分配，而电视机同样具有能耗分析，根据数据信息，若预知用户将使用电视，电视机具有自主拒绝其他设备提出的降低能耗要求。

IBM 去中心物联网模型 ADEPT

IBM 和三星合作开发了基于区块链技术的物联网去中心化网络概念 ADEPT，将物联网当下依赖于中心数据处理和管理的架构转换成去中心化 P2P 自动遥测架构。ADEPT 项目于 2015 年 CES 大会上发布，由三种架构协议组成，包括文档分享 BitTorrent、智能合约 Ethereum 和 P2P 信息交流工具 TeleHash。

ADEPT 根据设备的性能和设备之间的信任级别将物联网设备划分为 Light Peers（轻量级对等体）、Standard Peers（标准对等体）和 Peer Exchanges（交互对等体），这样的分类组成了 ADEPT 的基本架构。其中 Light Peers 指那些低存储空间的小型传感器和辅助型设备，其主要职责是传递信息辅助区块链中文件分享；Standard Peer 指那些在接下来几年中生产成本低但性能较强，可以满足区块链后台计算要求的物联网设备部件；Peer



Exchange 指具有高存储和计算能力的高端设备，在 ADEPT 架构中主要由商业和机构实体操作运行，往往具有承载市场的能力，允许大量价值交换、支付交易、提供分析解决方案、审查欺诈行为、对接供需、迎合法律及合规标准等活动。目前 ADEPT 主要针对门锁、可穿戴设备、长时间连接的设备（如洗衣机）等设备进行可行性研究，前两者属于 Light Peers，后者属于 Standard Peers。

三星正在与 IBM 合作，将 ADEPT 理念用于实际产品中。例如，三星 W9000 洗衣机可以探测清洁剂余量，自动向指定零售商购买清洁剂。从创建订单到完成安全支付都通过实现编程好的智能合约自动执行。而另一端的零售商，也可以查证与该台洗衣机的合约，收取交易金额，完成订单。一旦订单确认，用户即会在手机上收到确认信息和快递信息。

Filament 工业物联网方案

成立于 2012 年 Filament 是一家以物联网为目标市场的区块链公司。Filament 所创立的架构本质与 IBM 和三星打造的 ADEPT 项目类似，只是 Filament 更专注于工业物联网，解决工业市场的效率问题，包括油气开采、制造业、和农业等行业。该公司于 2015 年 8 月完成 A 轮 500 万美元融资，投资者有 Bullpen Capital、Verizon Venture 和三星风投。

为了实现物联网去中心化，Filament 首先推出了两种硬件设备。Filament Tap 是一个可以使电话、电脑、移动智能设备在 10 英里范围内交流，同时具备监控基础设施能力的传感器；Filament Patch 可以用来定时硬件项目，是前者的延伸技术硬件。

公司建立了囊括 5 种协议（Blockname、P2P 信息交流工具 Telehash、智能合约、小额交易技术 Pennybank 和文件分享 BitTorrent）的区块链架构。Filament 希望帮助工业企业更好的管理并提高工业生产效率。它给每一个物联网设备在去中心化的公共分布式记账本上设立特有的身份，从而使设备进行安全高效的沟通、执行智能合同，甚至交易付款。

目前存在的主要问题是，物联网支付能力尚处于早期研发阶段，小额交易技术 Pennybank 现在可以做到为两个物联网设备建立托管服务，当两者均在线时，才可以进行小额交易结算。未来还需要研发适用于工业支付的方式，满足工业企业对安全、快捷、实时支付的要求。

Slock.it 基于物联网的共享经济

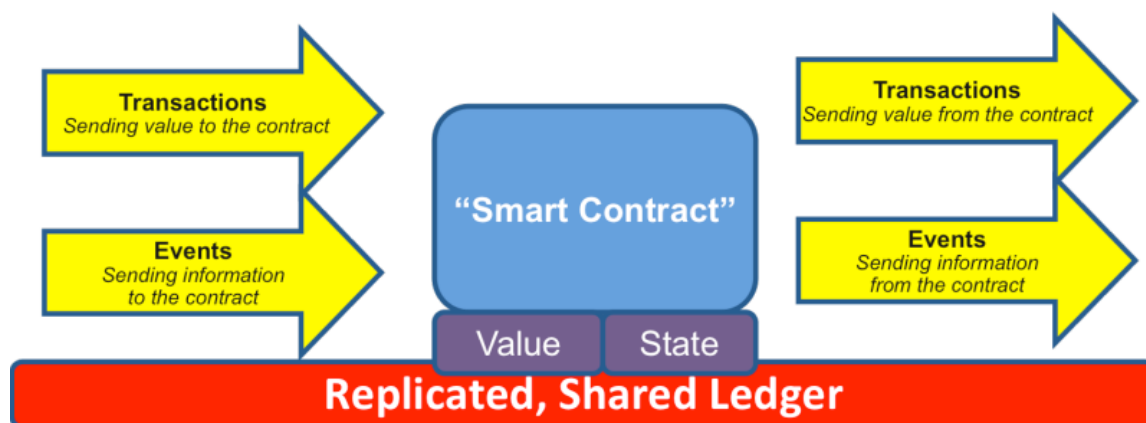
成立于 2015 年 6 月，Slock.it 是一个建立在以太坊之上的新共享经济平台，也是一个物联网基础设施架构，欲取代 Airbnb、Uber 等作为中心调度站的角色，实现完全自动化。

Slock.it 是全球首个 DAO 架构平台（Decentralized Autonomous Organization，去中心化的自治组织），具有透明、完整、简单、高效的特性。DAO 架构中智能合约，可以保证用户在移动应用上，随时随地追踪、控制出租或使用中的物品，且在每次共享完结时，可以准确、即时的收取费用、分配收入、给予分享者回报。

Slock.it 开发的首个硬件产品以太坊计算机，是一款迷你、预先配置好的家庭服务器，可以运行各种去中心化应用，例如 Web3 身份仓库、物联网 Slock 网关等。Slock.it 同时还提供 P2P 直接付款、存款、保险等服务。该公司计划于 2016 年早些时候开始预售 Slock.it 密码器，2017 年平台正式上线。未来他们还计划打造适用于物联网的小额支付和其他智能合约应用。

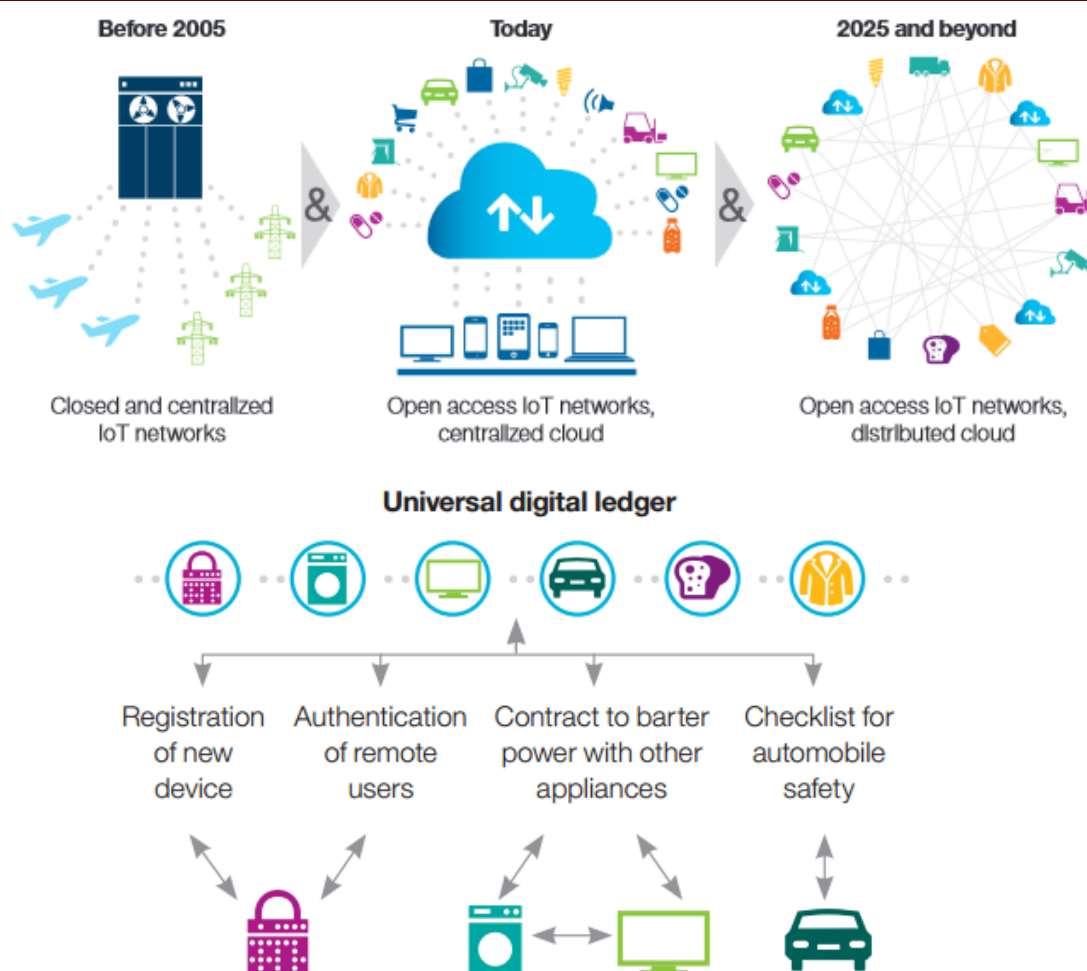


图表 24：智能合约是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值



资料来源：Richard G. Brown

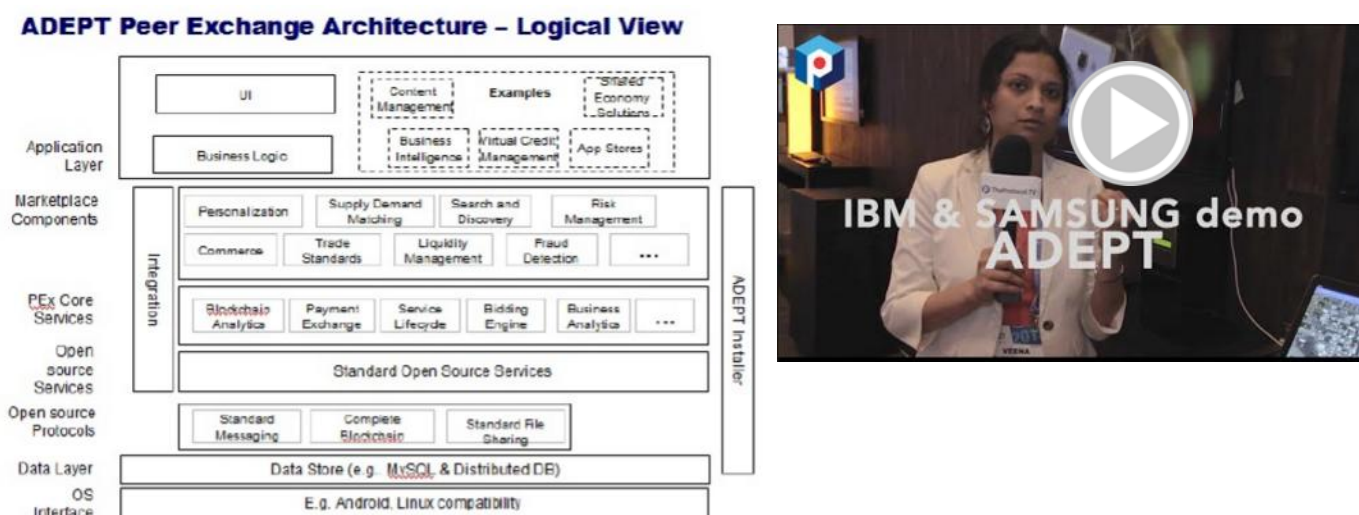
图表 25：区块链将使物联网形成点对点的高效低成本连接，使亿级智能设备成为自我维护的独立个体



资料来源：IBM "Device Democracy"



图表 26: IBM ADEPT 物联网方案



资料来源: IBM, ADEPT "An IoT Practitioner Perspective"; YouTube 视频链接地址 <http://v.qq.com/page/o/v/f/o0181iblgvf.html>

实现智慧政府

分布式账本在政府公共事务管理中可以发挥重要作用。英国政府科学办公室就已发表报告，推荐英国政府探索和试验分布式账本技术。分布式账本有潜力帮助政府收集税收、传递福利、签发护照、记录土地注册、保证商品供应链，确保政府记录和服务的完整性。目前，已经有一些国家政府开始了区块链实践。

对于国家能力（**state capacity**）尚不健全的发展中国家，区块链或许提供了跳跃式发展的可能，帮助政府完成公共事务管理的信息化，完善公共服务，分配公共资源。东欧小国爱沙尼亚（人口约 130 万）就是使用加密技术（爱沙尼亚 LHV Pank 银行是世界上第一个发行加密存单的银行）和公钥基础设施最积极的国家。而一些非洲国家开始尝试用区块链进行土地登记。

区块链对于限制权力腐败，提供政府公信力也有帮助。不可更改的公共账本便于政府审计和公民监督。智能合约还可以使一些可电子化、可编程的行政过程自动化，避免人为干扰。

爱沙尼亚公民和企业身份信息管理

自 2013 年，爱沙尼亚政府便采用了 Guardtime 公司开发的 KSI 无钥签名区块链架构，用于公民身份信息和企业信息管理。爱沙尼亚是全球使用国家级公钥基础设施（Public Key Infrastructure, PKI）最多的国家。使用 PKI 身份证，居民可以领取处方药、选举投票、登录网上银行、在线查看子女教育记录、申请政府福利、报税、提交遗嘱、申请入伍等多达 3,000 项功能。除了公民以外，企业也在 PKI 上建立了企业身份信息，可用于申请执照、递交财报、发行股权文书等。政府官员也使用 PKI 身份证明，加密文件以便内部传阅，审核批准申请文件等。就连部长级官员召开内阁会议时，也用 PKI 投票表决、阐述立场和审阅会议纪要。因此爱沙尼亚每人每年产生 39 个电子签名，且这一数字仍在攀升。

不断扩大的公钥基础设施需要区块链技术将其完善。区块链能够将公钥基础设施上的身份和认证信息进行加密保护。KSI（无钥签名）可以保证数据真实性。任何信息的修改都需要不只一方的认证。从公民角度来讲，任何人在区块链上查看了公民的信息和资料，该公民都能知道被人查看的原因、时间和对方身份。此外，与其他使用非对称加密的 PKI 不同，KSI 使用区块链散列（hash）使其不被量子算法攻击，并具有很好的规模性，可以 1 秒钟写入 1 个 EB（exabyte, 10 的 18 次方）数据，而只消耗微小的电量和网络流量。这种去中心化的公共区块链架构使得公共管理完全自动化，摒弃对某一管理机构的依赖。



区块链在欧洲能源零售市场发挥的作用

欧洲能源署近年来提出了“能源联盟”的概念，致力于寻找一种新机制使得公民在能源零售市场中发挥更大的作用。通过分布式发电、智能电网和储能技术，居民得以参与能源的生产和销售，降低电费开支。然而，虽然智能电网等技术已经成熟，但居民真正参与能源零售市场，依然面临很多障碍。例如，如何在一体化的能源市场上为居民提供及时的成本和需求数据使他们可以做出正确的决策；如何鼓励居民积极参与能源市场，简化能源供应合同的切换，如何管理因需求而动态变化的能源价格；如何保证不同市场的互联互通性，使自我生产、自我消费的能源用户真正获得收益。为此欧洲能源署正在研究区块链的作用，具体可以有以下两种方式：

- ▶ **Micro-Generation Energy Market:** Micro-Generation 指的是社区或家庭为单位自行发电。若将该种产量市场化，把生产者和消费者对接，便形成了市场。区块链在此起到的作用一方面是将产销两端直接对接，另一方面是将这种新型市场上的交易规范化。智能电表可以直接把生产消费者（proconsumer）产生的电量记录在分布式记账本上，便于进行市场交换。与原来生产消费者与某家电力公司签订双边合同不同，由分布式记账本管理的能源市场，增加了生产消费者的选择权。自行消费之后的多余电量不仅可以存于电池备用，或返回给电网，还可以出售给网络里出价最高的买家，甚至异地赎回（如给在外行驶的电动车充电）等。
- ▶ **Energy Contract Ledger:** 此前消费者更换能源供应商时，需要进行程序繁琐的解约和新签约过程。能源公司也需要因此配备中后台人员。而在区块链支持下，能源合约可以数字化、智能化。消费者只需在电脑或手机上点击几次，就可以更换供应商。

Agora Voting 公司的投票软件

西班牙公司 Agora Voting 成立于 2014 年，是一款基于区块链技术而建立的免费投票 SaaS 软件，致力于将传统耗时且存在作弊风险的投票方式电子化，保证投票选举的公正、公开和民主。该软件可以支持几百人甚至几千人进行安全、可靠、专业的在线投票。投票类型包括公开预选、机构内部选举、公共协商和普通投票等。为保证每次投票都是由注册用户本人操作，软件提供了多种验证身份的方式，例如认证码、政府签发证件、智能卡片、电子身份证、密码器、邮件和短信动态验证码等。

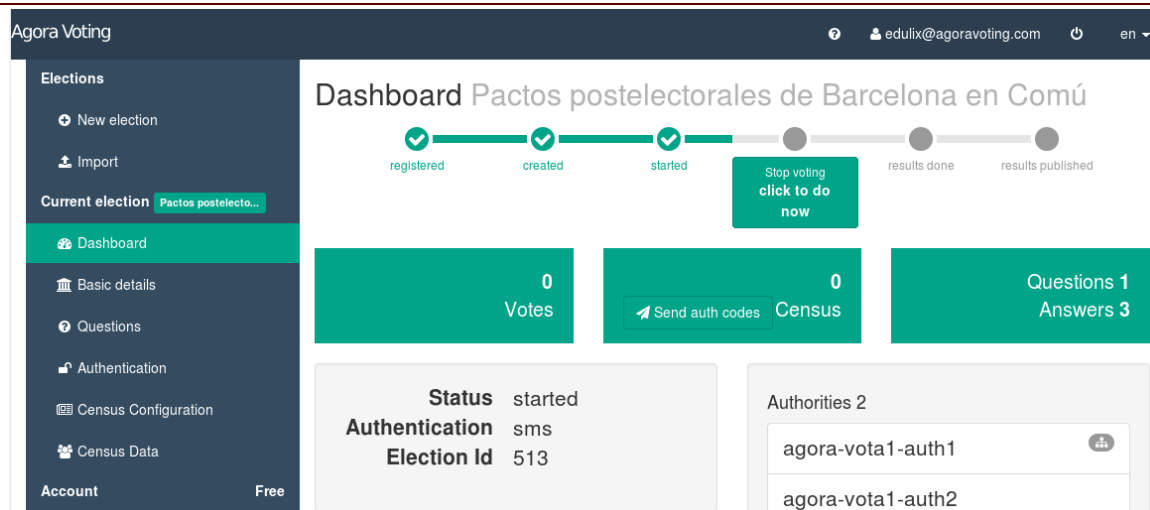
由于区块链本身的特性，Agora Voting 所提供的投票解决方案最大的亮点便是高级别的安全性。投票人的每个投票环节都受到端到端的加密保护。从投票人进入虚拟投票站，所持有的选票信息就会被系统层层加密上锁，且在投票提交前，加密的选票会被自动截取快照以备后续验证选票使用。这一系列的程序仅在投票人电脑上便可完成，并不通过远端服务器。所有提交的选票都将会被存储在 Digital Ballot Box（数字选票盒）中，任何一个选票官都没有单独打开查看投票结果的权限。因为选票的加密是在个人终端完成的，而服务器只有验证和核对选票证书的职能。接下来的计票过程是在完全可验证的流程下进行，待所有选票汇总在 Digital Ballot Box 中，系统才一起提交给选票官们。在不打开选票的情况下，系统开始执行解码、混合和打乱选票等程序，保证每一张选票是匿名，且不可识别的。只有当所有选票官联合向投票人获取解码批准后，才能正式执行计票。而系统最终的计票结果和相关分析数据还会自动核对每个投票人电脑终端的原始投票内容，以确保线上公布的投票结果准确无误。此外，整个流程采用的加密保护和编码都有留痕，可供后续任何人进行审核查验。

Agora Voting 另一大优点在于以较低花费向人们提供了可定制的投票流程。针对大型、专业，甚至政府官方投票，Agora Voting 可以根据用户的特殊要求进行投票功能和流程定制。根据投票人数、对安全保护的要求、选举时间长短，软件的收费标准和提供的安全级别有所不同，以 1,000 人的普通投票为例，每个选票收费 0.39 欧元、每条短信息收费 0.2 欧元，享受一级安全保护，加上税费合计 590 欧元。

软件推出后获得了来自政府、教育机构等青睐，目前已获得注册用户超过 15 万，主要机构用户包括西班牙 Lugo 市政府、西班牙 Podemos 党、西班牙远程教育大学、西班牙工会 CCOO 工会等。



图表 27: Agora Voting 基于区块链开发的安全高效匿名公正的投票系统



资料来源: Agora Voting 公司网站

Factom 公司的产权登记系统

Factom 是一家专门利用区块链技术管理数据和保持档案记录的公司，适用于审计系统、医疗档案、供应链管理、投票选举、产权等领域应用，受到企业和政府机构的青睐。其中最值得关注的是，Factom 努力与发展中国家政府讨论使用区块链技术帮助建立和完善产权的登记和维护。公司目前正在和加纳政府商议，合作建立产权登记系统。此前还与洪都拉斯政府有过计划，但由于当地政治因素，洪都拉斯项目目前处于停滞状态。

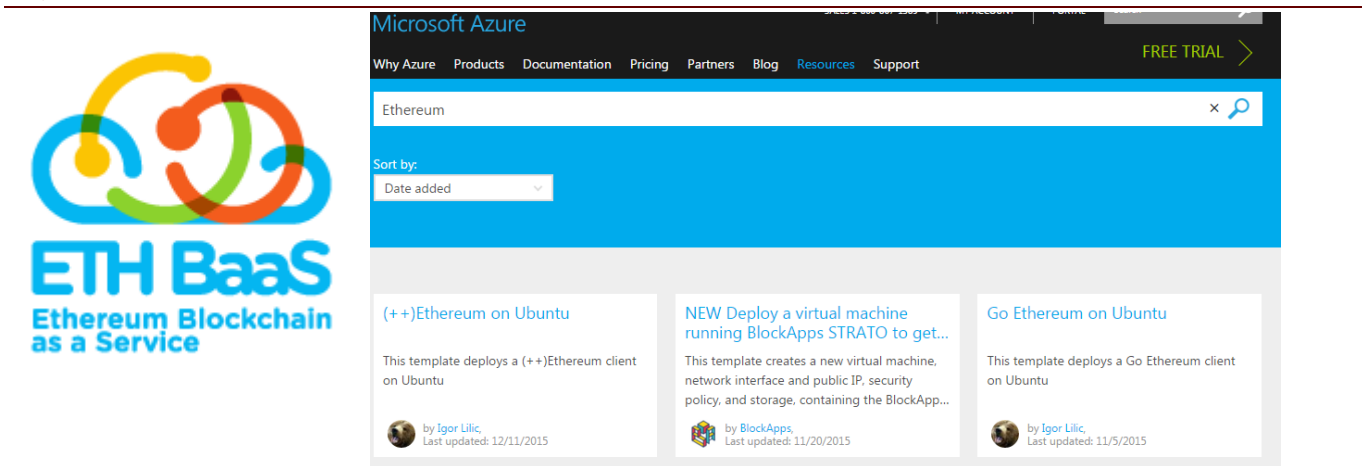
构建自治社会

除了金融、物联网和智慧政府以外，区块链在信息安全、云存储、实物资产登记和交易、文件验证、媒体等方面也有广泛的用途。当然，这些应用目前还处于萌芽阶段。近期一些工具平台的推出，或将有助于区块链的普及。微软与初创公司 Consensys 联合于去年 11 月推出以太坊区块链云平台（Ethereum Blockchain as a Service），使 Azure 用户可以廉价、迅速的下载相应套件，创建私有链或智能合约。德勤于去年 7 月推出“一站式区块链软件平台”Rubix，帮助客户开发区块链应用，其目标也是成为区块链领域的 AWS，同时也为客户提供相应的咨询服务。

从长远来看，区块链可能为社会经济组织形式的演化提供条件，在减少对中心化组织（不仅是政府，也包括原先起中介作用的商业机构）的依赖的同时，又提高效率，还能促进消费者利益，完善公民自治。就如 TCP/IP 协议支撑了互联网和信息经济，在区块链架构之上，或许能搭建起更高效、更透明、更个体自治的新社会。

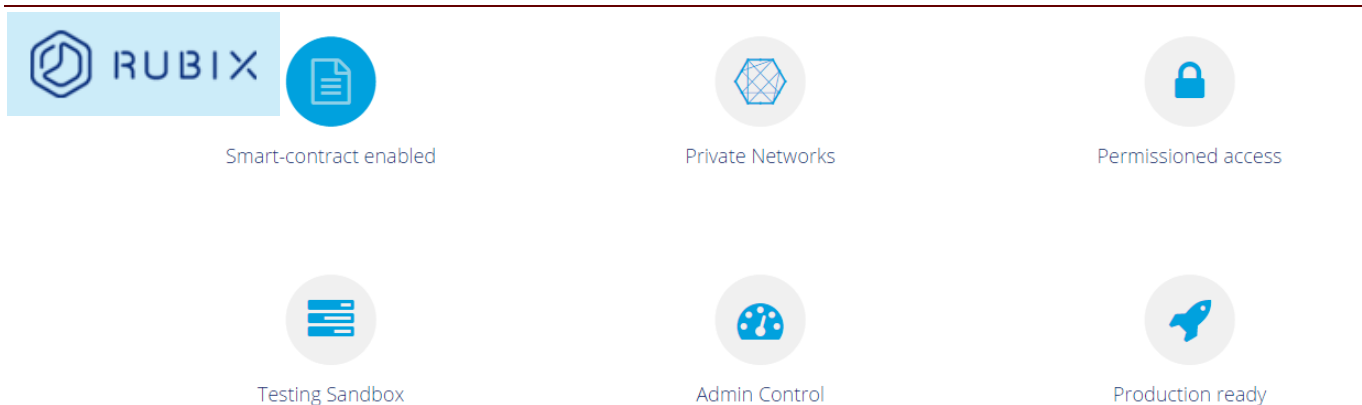


图表 28：微软 Azure 推出 Ethereum Blockchain as a Service



资料来源：微软 Azure 网站

图表 29：德勤推出的 Rubix 是一站式区块链软件平台



资料来源：德勤 Rubix 网站

信息安全：Guardtime 公司

区块链去中心化和加密安全性的特征，使区块链网络与传统网络相比，在防范黑客攻击方面更加有效。一些创业公司正在以区块链为核心，打造新一代信息安全产品。

2006 年成立于爱沙尼亚的 Guardtime 就是一家致力于利用区块链技术为金融、电信服务提供商、国防、航空航天、保险和政府等客户提供网络安全解决方案的公司。公司主要由密码员、网络架构师、硬件工程师、软件开发者和安全架构师等 100 多人组成，在荷兰阿姆斯特丹、美国加州欧文市、爱沙尼亚塔林市和塔尔图市设有办公室。2007 年，因创造了 Keyless Signature Infrastructure（无钥签名）专利技术而名声大噪，其他产品还包括 Black Lantern Security Appliance、KSI Security Manager 和 KSI 相关服务等，为企业所提供的解决方案涉及关键基础设施保护、企业安全、Hadoop Big Data Lakes、数据泄漏管理、Inside Threat Mitigation 内部威胁缓解、Object Store WORM、DevOps、云广播网络、Advertising Attribution、云担保、电子政务、物联网、车联网等。

Guardtime 开创的无钥签名专利技术 KSI，与传统的非对称密钥不同，采用哈希函数加密方式，依托于区块链平台，可验证和证明海量的电子数据的签名时间、签名起源和数据完整性。这项技术的出现改进了传统区块链在规模和交割时间方面的两大弱点，同时还提高了区块链在工业规模上的可用性。首先，传统区块链是基于交易数量这一变量而成直线增长，每发生一笔交易就会生成一个相关区块，相较之下 KSI 技术独立于交易数量，以时间为变量建立区块从而实现直线成长的模型。假设以每秒作为每个区块生成的单位标准，那么在这秒内发生的所有交易都会被记录在同一个区块上。其次，KSI 限定了其区块链上的参与者数量，可以做到在一秒内使 KSI 上各个节点达成一致协议，从而削减了交割所需的各种繁琐的审批环节。



分布式云存储：Storj 公司

Storj 是一个带有分布式应用套件的云存储平台。允许用户以安全的、去中心化的方式通过自动网络出租额外的硬盘空间，使用密码学来进行安全加密。Storj 公司开发小规模系统，名为 Metadisk 的拖放文件托管 App，公司也已经开源 Metadisk 的 API，使更多需要云存储平台的用户在其自己的 App 和网页中添加 Metadisk。该公司团队还会继续开发类似 DriveShare 的 App 使用户可以出租自己的硬盘空间，最终形成一个更完整的去中心化存储平台。

Storj 的去中心化存储成本只有中心化存储成本的 1/100 到 1/10 左右。目前 Dropbox 租用 100GB 存储空间的费用为 99 美元年费加每月 9.99 美元的管理费，如果用户使用量低于 100GB，而 Storj 租用 100GB 存储空间的年费仅为 1.96 美元。而且用户可以在 Storj 平台上出租未使用的额外硬盘空间，获取利润。

如果 Storj 这样的分布式云存储获得发展，将威胁 Box/Dropbox 等传统云存储的发展空间。因为即使中心化云存储的存储媒介成本每年减半，运营成本，包括数据中心的租金、维护费用和法律费用等固定费用仍会逐年增加，限制了中心化云存储服务的竞争能力。

实物资产登记：Everledger 公司的钻石“护照”

上线于 2015 年的 Everledger 由英国知名连环创始人 Leanne Kemp 创立，是全球首个基于区块链技术的钻石数字账本。钻石因其体积小、稀有、价值高、易转移等特性，常常成为犯罪活动价值交换的“货币”。虽然人们早已广泛使用纸质防伪认证证书，但仍不能完全解决证书被篡改、伪造的难题，而且现今仍有些国家缺少健全的法律监管。因此，Everledger 创立的使命就是为了给每一颗钻石创建独一无二的数字“护照”，用电子指纹将钻石的产地、净度、切割工艺，以及所有权转移信息等连接到分布式账本中。截至去年 6 月，该公司已经记录了 280,000 个钻石。所有的主要钻石认证中心都已成为 Everledger 的合作伙伴，4 家保险公司成为客户。

这套体系的建立主要分为三个环节：1) 建立带有钻石属性和镭射激光序列码的电子身份验证；2) 赋予可用于记录、监管交易历史、转移和来源的电子护照；3) 侦查和监管非法和欺诈活动。假设一颗 5 克拉的钻石，它的序列号、切割、净度、组成钻石的 40 个数据点和角度等属性，都会被记录在区块链。该记录就是这个钻石唯一的身份证件，可用于海关、保险、警察执法、交易买卖等。例如，当钻石被盗窃时，警察可以根据区块链上的数据进行调查，并把追回的赃物与记录核对。保险公司可以根据区块链的数据来判断客户的索赔是否合理，防止索赔欺诈。如果钻石找回，保险公司还可弥补损失。Everledger 的系统还具备智能合约功能，方便钻石交易、购买保险、抵押借款等。

而除了钻石之外，Everledger 的技术还可以广泛适用于其他所有具有独特唯一、难以被篡改复制的标识的实物资产上。近期，Everledger 加入了德国安联集团的创新孵化期，以便研究开发进一步的解决方案，为保险公司防范保险欺诈提供帮助。

图表 30：Everledger 钻石“护照”和智能合约方便钻石交易

TRANSACTIONS	BLOCK INFO	# TXS	HEIGHT	BROADCASTED
30863a72e40c0a2ed79f4217f107ec54ad...	082df5335f...	1297	393742	8 days ago
ba526363c7eb0f9a034703e8caacd66dafa...	851dcc20de...	795	393741	8 days ago
3349d5916d3af4cc8cac59b69bf3b684fba...	e86d54f2d1...	2547	393740	8 days ago
7f8099e57fe742d10f498a158587c9730e4...	004290a471...	1010	393739	8 days ago
cb5bae9bd78f95a9f37fdb749326b8170c...	f5653891f3...	915	393738	8 days ago
000434e0411f8e85447fb7723001950d2d8...	ca8c8d5122...	1647	393737	8 days ago
911d2264869e7c22f918236726cbd1ac452...	287be754d0...	2976	393736	8 days ago
95541fe959cf5645df8e8b378bc98a217af...	2ad8de0778...	1	393735	8 days ago
a041024681a0b8d51e2373154b734695063...	033598f272...	1300	393734	8 days ago
8605fe4b2c2fd0ceb5d5ac9efc4c72a562cd...	0b709d0abe...	1921	393733	8 days ago

资料来源：Everledger 公司网站



文件验证：BitProof 公司的学历记录

BitProof 公司是一家利用区块链技术进行文件验证的公司，该公司在教育领域有所建树，使用区块链来记录学历，颇受招聘公司赞赏，据背景调查公司 HireRight 统计，约有 86% 的受访公司表示他们曾经发现应聘者有学历造假的行为。区块链的可验证、防篡改特性解决了学历造假问题。目前 BitProof 已经与加州一所软件工程师培训学校 Holberton School 合作，未来将会有更多学校加入进来。

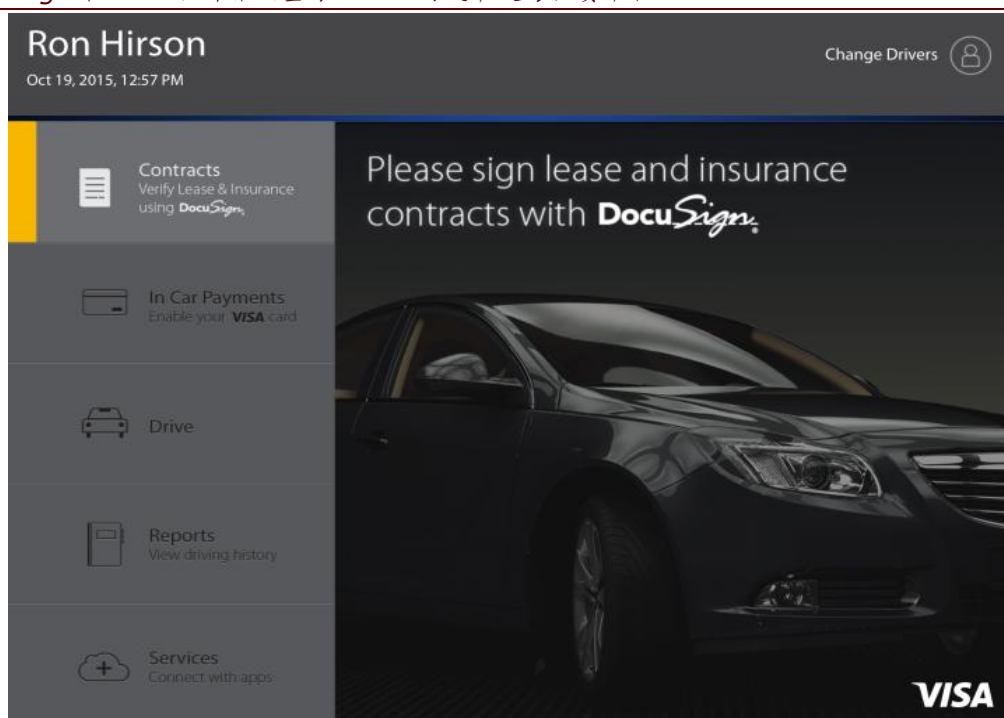
区块链还能简化海量的学历信息归档、整理、查询环节，节省大量人工和时间成本。Holberton School 称，在建立了这套体系后，企业雇主 Merkle 在调查本校学生背景时，通过在线免费的区块链浏览器，仅花费了几秒钟便获得了这名学生的学历证书等信息。

汽车：Visa 和 DocuSign 合作推出汽车交易和租赁平台

2015 年 10 月，数字交易管理公司 DocuSign 旗下的 DocuSign Lab 和 Visa 公司的 Visa Innovation Lab 合作计划利用区块链技术打造一个汽车交易和租赁平台。两家公司的愿景是将汽车和汽车交易信息完全透明、公开化，同时将汽车买卖和租赁流程简化到“点击查看、签署合同、提车”这三个步骤。从顾客选择车辆和交易类型，到随后的合约签署和汽车保险的购买都将会自动在区块链上记录和更新。而汽车购买租赁原来需要的复杂繁琐的保险评估、贷款申请等，将被完全数字化，在移动终端上就能全部完成。在这一计划当中，Visa 和 DocuSign 将分别在支付和合同签署两个环节发挥自身优势。

依赖于区块链技术本身的优势，两家公司还计划与车辆管理处实现信息联网，将服务内容扩张至车辆的登记和管理、驾驶数据的收集和记录。此外，例如公路收费站付款、汽车养护、泊车、下载音乐、外带食物等消费都有可能被囊括于这一平台。

图表 31: DocuSign 和 Visa 合作推出基于区块链的汽车交易租赁平台



资料来源：DocuSign 公司网站



共享经济：La'Zooz 的 P2P 共享出行

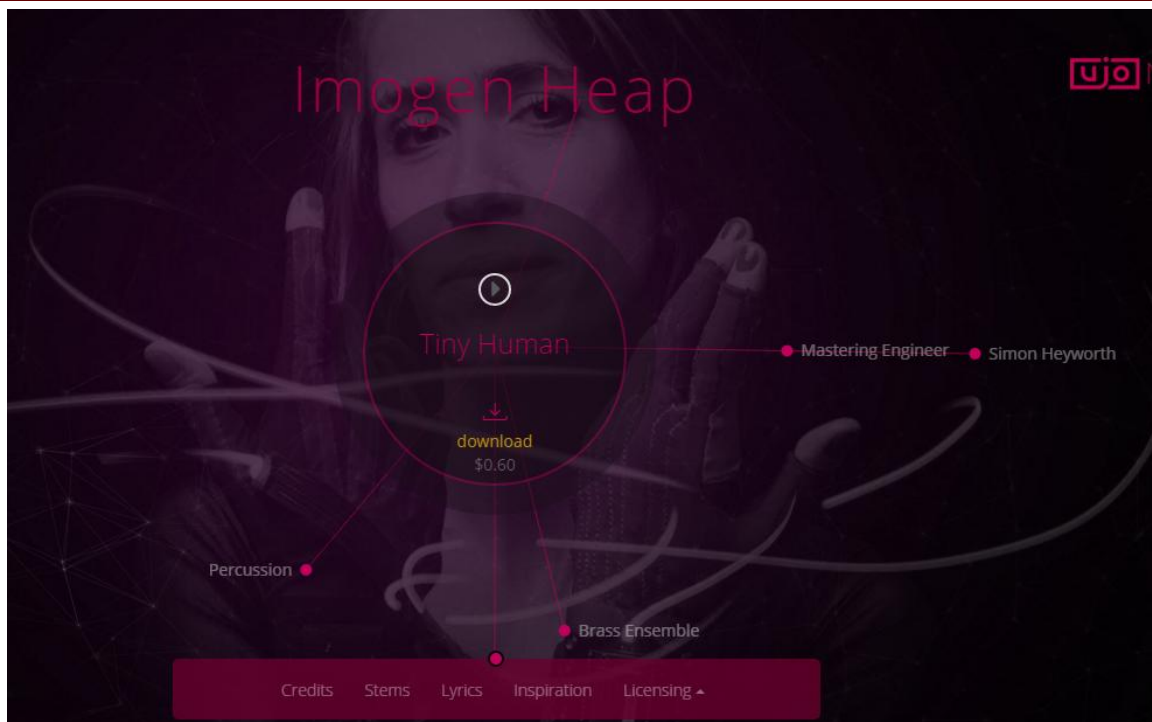
与当下备受关注的共享出行公司 Uber 的运营方式背道而驰，来自以色列的初创公司 La'Zooz 致力于利用区块链架构将共享出行去中心化，取代像 Uber 这样的调配中心角色。2013 年，公司发明了一套虚拟货币 Zooz 和相关体系。用户通过允许该应用程序追踪自己所在位置，便可以获得 Zooz。同时为了鼓励更多的服务提供者加入，自愿提供乘车服务的司机可以获得 Zooz 以示奖励。供需两端的对接不需要调配中心，用户自行在 La'Zooz 上寻找目的地相近的人而获得行程，用 Zooz 支付打车费用。La'Zooz 团队认为这种去中心化的共享出行解决方案向人们展示了“社区责任”理念，更有效的帮助城市改善交通拥堵、合理分配资源等。

媒体：Ujo Music 的数字音乐销售

区块链技术对音乐行业的颠覆主要表现在版权保护、支付方式这两方面。由英国音乐创业者 Phil Barry 领头的 Ujo Music 致力于重塑音乐行业，提高在线音乐分享的公平性、透明度和盈利能力，阻止近年来音乐行业日趋下滑的趋势。基于以太坊区块链（Ethereum）开发的音乐分享平台 Ujo Music，允许音乐创作人发布音乐作品时将作品信息和所有权信息永久自动记录在区块链上，从而保证作品版权的真实性，避免侵权行为的发生。当用户购买音乐时，购买金额会直接付予音乐作品的所有创作人员，省去唱片公司等第三方中介。系统自动通过智能合约，自动执行购买者对版权保护条款和规则的认可。这一流程不仅解决了传统流媒体音乐版权支付问题，更可以帮助音乐人提高收入，与乐迷直接交流互动。

Ujo Music 的测试版在 2015 年下半年时推出，与格莱美奖和艾佛莫诺奖的获得者 Imogen Heap 合作，将其个人新专辑中的 Tiny Human 歌曲作为测试版的推广曲目。测试版为每一个作品打造了完整、自足的歌曲信息生态系统，用户可以清楚的了解歌曲创作人、音乐类型、版权等信息，以及歌曲单笔收入向每个创作人员的分配情况。Ujo Music 计划在下一个更新版本中添加信用卡支付功能，使平台支付方式更多元化，避免目前只能单一使用虚拟货币以太币（Ether）支付的情况。

图表 32: Ujo Music 以 P2P 方式销售歌曲 Tiny Human



资料来源：Ujo Music 公司网站

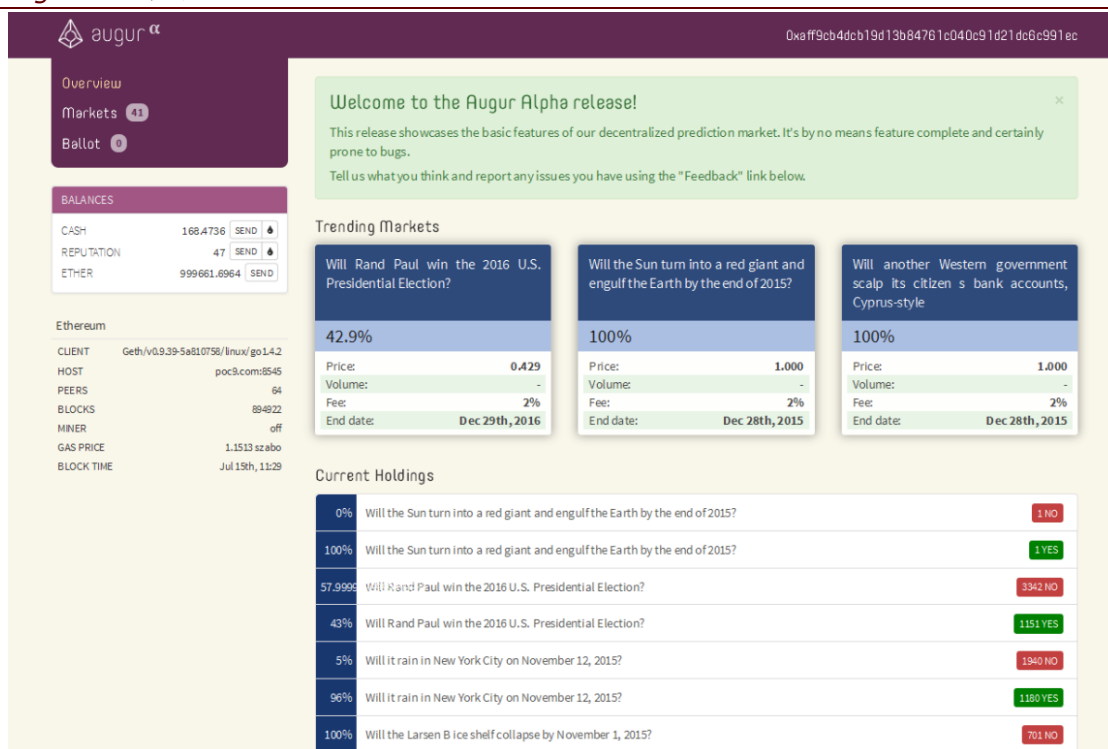


预测：Augur 的预测市场

区块链技术的出现对研究、分析、咨询和预测产生重大影响和改变，通过在线众筹大众智慧的方式，成立于2014年9月的初创公司 Augur 计划于2016年推出全球第一个基于 Ethereum 以太坊的预测市场平台。预测市场指的是人们买卖某一事件结果的“股票”，即事件发生概率的市场价值，集合尽可能多人的智慧来评估某一事件的发生概率，这样的共识往往能够比所谓专家评论得到更为准确的结果预测。而准确预计了事件结果的人可以在市场上获得相应股票价值的回报。假设，就“希拉里是否能赢得2016年美国总统大选”这一事件在预测市场提问，若“她能赢”的股票价格为每股60美分，那么意味着市场预测希拉里有60%的机会赢得大选。假设预测正确，那么就可以获得相应金额奖励，减去买入预测时的成本就是最终获得的收益。相比此前就有的预测市场模式，区块链机制有效的消除了来自于对手和中心化服务器的风险。

Augur 所创建的平台去中心化体现在，处在世界各地任何人都可以发起任意感兴趣的预测市场，而区块链保证了这一庞大的、动态变化的市场运作时的交易安全性和信息公开、透明。Augur 运用自己发明的信誉（REP）作为其系统的虚拟货币来保证交易流通。REP 类似比特币可以分割和交易，由复杂的密码构成。该平台的去中心化还体现在，事件结果不是由某个人或组织得出，而是通过 Augur 构建的去中心化报告机制，由 REP 持有者进行报告。REP 持有者需要针对事件的真实结果，做出事件发生、没有发生、不知道其中一种选择。如果出现不诚实报告，Augur 后台分析法将扣除 REP 持有者一定信誉，分配给其他诚实的持有者以示惩罚，这同时意味着 REP 数量高的持有者产生的报告具有很高的可信度。目前该平台测试版已经上线，而正式版还在积极开发当中。

图表 33: Augur 预测市场



资料来源：Augur 公司网站













附录：虚拟货币概要

图表 34：虚拟货币是一种电子货币，但不是任何机构或个人的负债，且无官方担保

Feature	Bitcoin	USD (home currency)	Euro (foreign currency)	Commodity (bullion)	Commodity currency (coin)	Gold Standard	U.S. Greenback Era (1861-78)
Economic demand factors							
Intrinsic Value	None	None	None	Yes	Yes	None	None
Claim to issuers?	No	Yes	Yes	No	No	Yes	Yes
Legal tender	No	Yes	No (in the U.S.)	na	na	Mixed	Yes (no) to public note (private)
Used as medium of exchange	Small, but rising especially in online retail	Yes	Limited (in the U.S.) possibly more for cross-border trade	Yes	Yes	Yes	Yes
Used as a unit of account	No	Yes	No (in the U.S.)	Yes	Yes	Yes	Yes (all notes shared "dollar" unit)
Used as store of value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk	Yes, subject to foreign exchange risk	Yes, subject to commodity price risk/cycle	Yes, subject to dilution of quality (inflation/devaluation)	Yes, subject to devaluation risk	Yes, subject to inflation risk
Supply Structures							
Monopoly/decentralized	Decentralized	Monopoly	Monopoly	Decentralized Private/public mining	Mixed	Mixed	Decentralized
Supply source	Private	Public	Foreign Public	Mixed	Mixed	Mixed	Public and Private
Supply quantity	Inflexible	Flexible	Flexible	Inflexible	Inflexible	Inflexible	Flexible
Supply rule	Computer program	Rule-based (inflation target)	Rule-based (inflation target)	Opportunity Cost for mining	Tied to commodity in bullion	Tied to commodity by reverse ratio	Private not subject to reserve requirement
Supply rule change (by issuers) possible?	Yes with agreement of majority miners	Yes	Yes	No	Quality of minted coins can be diluted	Reverse ratio can be changed and economized	No for private banks
Cost of production	High (electricity consumption for computation)	Low	Low	Very high (mining)	Medium	Low	Low

资料来源：IMF

图表 35：目前最大的虚拟货币是比特币

	Market cap (\$)	Price (\$)	Available supply	Trading volume (\$, 24hrs)
 Bitcoin	5,726,185,536	378.89	15,113,175 BTC	88,516,300
 Ripple	171,373,970	0.00511	33,537,439,933 XRP	359,715
 Litecoin	134,656,765	3.05	44,165,398 LTC	3,547,950
 Ethereum	113,373,113	1.48	76,456,740 ETH	1,657,800
 Dash	31,484,402	5.11	6,162,260 DASH	1,096,200
 Dogecoin	17,520,383	0.00017	102,775,122,567 DOGE	488,938
 Factom	9,220,923	1.05	8,753,819 FCT	853,256
 Peercoin	9,108,807	0.397224	22,931,159 PPC	45,167
 Stellar	8,210,397	0.001697	4,837,356,606 XLM	28,445
 BitShares	7,624,633	0.003003	2,539,022,231 BTS	156,142

资料来源：<http://coinmarketcap.com/>



图表 36：比特币价格依然波动剧烈



资料来源：彭博资讯，中金公司研究部

图表 37：比特币依然没能形成主流

	Quarterly				Year Ago	
	December-15	September-15	Q4/Q3Δ	Q3/Q2Δ	Q4 2014	Δ
Commerce						
Wallets (EoQ)	12,768,681	11,051,719	16%	18%	7,396,772	2x
Transaction Volume (BTC)	384,835,478	350,286,741	10%	7%	291,817,718	1x
Merchants' annual revenue (\$bn) (EoQ)	197	\$190	4%	0%	180	1
ATMs (EoQ)	536	475	13%	12%	342	2x
Price						
Price (EoQ)	430	236	82%	-10%	320	1x
Exchange trading volume (BTC)	150,025,305	28,615,261	424%	17%	40,041,026	4x
Bitcoin market capitalization (\$bn) (EoQ)	7	3	86%	-8%	4	1x
Industry						
All-time VC investment (\$mn) (EoQ)	949	\$923	3%	10%	459	2x
Number of VC-backed startups (EoQ)	127	120	6%	6%	90	1x
Media						
Mainstream media mentions	521	411	27%	11%	508	1x
Blockchain						
Number of blockchain companies (EoQ)	5	42	29%	40%	14	4x
Technology						
Network hashrate(billion/second) (EoQ)	743,604,444	457184328	63%	30%	313,142,289	2x

资料来源：Coindesk



图表 38：各国政府对比特币的态度以限制或禁止为主

Jurisdiction	AML/CFT: warning and regulating (existing and new)	Tax Treatment	Consumer Warnings and Advisories	Licensing/Registration of VC Intermediaries	Financial Sector Warnings and Bans	Bans on Issuance/Use
Argentina	Warning on the ML/TF risks		Consumer Warning		Warning on reporting entities	
Bolivia						Yes
Canada	Amending existing regulations	Clarified tax treatment	Consumer Advisory			
China					Ban	
France	Applications of existing regulations	Clarified tax treatment	Consumer Warning			
Germany	Applications of existing regulations					
Italy			Consumer Warning		Warning	
Japan	Plan to introduce new regulations		Consumer Warning	Plan to introduce new regulations		
Russia	Applications of existing regulations		Consumer Warning			Yes-draft law
Singapore	Plan to introduce new regulations	Clarified tax treatment	Consumer Warning			
South Africa			Consumer Warning			
U.K.	Applications of existing regulations	Clarified tax treatment				
U.S.	Applications of existing regulations (Federal)	Clarified tax treatment (Federal)	Consumer Warning	State licensing regimes (for example, NY BitLicense)		

资料来源：IMF

图表 39：比特币及其 colored coins 的创业公司分为基础设施、钱包、支付、交易所、金融服务、挖矿等类别



资料来源：Coindesk



图表 40：在支付体系中推广虚拟货币依然困难重重

爱沙尼亚最大银行 LHV Pank 是全球首个发行受加密保护存单的银行，发行金额为 10 万欧元。随后 LHV Pank 创办了 CUBER (Cryptographic Universal Blockchain Entered Receivable) 子公司，专注于比特币虚拟货币和区块链技术，先后推出了 CUBER 证券和 Cuber Wallet。



CUBER 证券就是被记录在区块链上的存款证明。以欧元计价，具有价值储藏、交易媒介、信托和托管、利息支付等功能，甚至可以用于物联网中机器与机器的交易。

CUBER 钱包是首款移动 P2P 支付软件，为个人与个人之间提供免费快捷的转账，也商户与个人之间提供了低成本的转账。用户端不需要下载所有交易相关数据，而只载入区块头，便可自动发起用户命令的转账交易，避免数据过于庞大的问题。该系统将比特币作为数据的载体，将比特币与爱沙尼亚法定货币关联，商户接受 CUBER 钱包，就像接受信用卡支付一样。

有 LHV Pank 银行为母公司，使 CUBER 得以方便的在传统银行账户和 CUBER 钱包之间进行转账。但作为银行的子公司，CUBER 又需要接受银行业的监管。例如欧洲反洗钱条例就要求在银行开户必须本人持有效证件亲自到柜台面对面验证，才能办理开户，类似这样的监管对于在线金融服务的便捷性产生很大限制。因此，CUBER 面临着两难选择，或者接受银行业严格监管，或者脱离银行母体及其提供的各种方面。可以看到，**在传统银行和加密货币之间建立一个简单、安全、合规的桥梁依然是十分困难的。**

资料来源：UK Government Chief Scientific Advisor "Distributed Ledger Technology: beyond block chain"



法律声明

一般声明

本报告由中国国际金融股份有限公司（已具备中国证监会批复的证券投资咨询业务资格）制作。本报告中的信息均来源于我们认为可靠的已公开资料，但中国国际金融股份有限公司及其关联机构（以下统称“中金公司”）对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供投资者参考之用，不构成所述证券买卖的出价或征价。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专业财务顾问的意见。对依据或者使用本报告所造成的一切后果，中金公司及/或其关联人员均不承担任何法律责任。

本报告所载的意见、评估及预测仅为本报告出具日的观点和判断。该等意见、评估及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，中金公司可能会发出与本报告所载意见、评估及预测不一致的研究报告。

中金公司的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。中金公司没有将此意见及建议向报告所有接收者进行更新的义务。中金公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

本报告由受香港证券和期货委员会监管的中国国际金融香港证券有限公司于香港提供。香港的投资者若有任何关于中金公司研究报告的问题请直接联系中国国际金融香港证券有限公司的销售交易代表。本报告作者的香港证监会中央编号已披露在报告首页的作者姓名旁。

本报告由受新加坡金融管理局监管的中国国际金融（新加坡）有限公司（“中金新加坡”）于新加坡向符合新加坡《证券期货法》及《财务顾问法》定义下的认可投资者及/或机构投资者提供。提供本报告于此类投资者，有关财务顾问将无需根据新加坡之《财务顾问法》第 36 条就任何利益及/或其代表就任何证券利益进行披露。有关本报告之任何查询，在新加坡获得本报告的人员可向中金新加坡提出。本报告无意也不应，以直接或间接的方式，发送或传递给任何位于新加坡的其他人士。

本报告由受金融市场行为监管局监管的中国国际金融（英国）有限公司（“中金英国”）于英国提供。本报告有关的投资和服务仅向符合《2000 年金融服务和市场法 2005 年（金融推介）令》第 19（5）条、38 条、47 条以及 49 条规定的人士提供。本报告并未打算提供给零售客户使用。在其他欧洲经济区国家，本报告向被其本国认定为专业投资者（或相当性质）的人士提供。

本报告将依据其他国家或地区的法律法规和监管要求于该国家或地区提供本报告。

特别声明

在法律许可的情况下，中金公司可能会持有本报告中提及公司所发行的证券头寸并进行交易，也可能为这些公司提供或争取提供投资银行业务服务。因此，投资者应当考虑到中金公司及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。投资者请勿将本报告视为投资或其他决定的唯一参考依据。

与本报告所含具体公司相关的披露信息请访问 http://research.cicc.com/disclosure_cn，亦可参见近期已发布的相关个股报告。

研究报告评级分布可从 <http://www.cicc.com.cn/CICC/chinese/operation/page4-4.htm> 获悉。

个股评级标准：“确信买入”（Conviction BUY）：分析员估测未来 6~12 个月，某个股的绝对收益在 30% 以上；绝对收益在 20% 以上的个股为“推荐”、在 -10%~20% 之间的为“中性”、在 -10% 以下的为“回避”；绝对收益在 -20% 以下“确信卖出”（Conviction SELL）。星号代表首次覆盖或者评级发生其它除上、下方向外的变更（如*确信卖出 - 纳入确信卖出、*回避 - 移出确信卖出、*推荐 - 移出确信买入、*确信买入 - 纳入确信买入）。

行业评级标准：“超配”，估测未来 6~12 个月某行业会跑赢大盘 10% 以上；“标配”，估测未来 6~12 个月某行业表现与大盘的关系在 -10% 与 10% 之间；“低配”，估测未来 6~12 个月某行业会跑输大盘 10% 以上。

本报告的版权仅为中金公司所有，未经书面许可任何机构和个人不得以任何形式转发、翻版、复制、刊登、发表或引用。

V150707
编辑：杨梦雪



北京

中国国际金融股份有限公司
北京市建国门外大街1号
国贸写字楼2座28层
邮编: 100004
电话: (86-10) 6505-1166
传真: (86-10) 6505-1156

深圳

中国国际金融股份有限公司深圳分公司
深圳市福田区深南大道7088号
招商银行大厦25楼2503室
邮编: 518040
电话: (86-755) 8319-5000
传真: (86-755) 8319-9229

上海

中国国际金融股份有限公司上海分公司
上海市浦东新区陆家嘴环路1233号
汇亚大厦32层
邮编: 200120
电话: (86-21) 5879-6226
传真: (86-21) 5888-8976

Singapore

China International Capital Corporation (Singapore) Pte. Limited
#39-04, 6 Battery Road
Singapore 049909
Tel: (65) 6572-1999
Fax: (65) 6327-1278

香港

中国国际金融（香港）有限公司
香港中环港景街1号
国际金融中心第一期29楼
电话: (852) 2872-2000
传真: (852) 2872-2100

United Kingdom

China International Capital Corporation (UK) Limited
Level 25, 125 Old Broad Street
London EC2N 1AR, United Kingdom
Tel: (44-20) 7367-5718
Fax: (44-20) 7367-5719

北京建国门外大街证券营业部

北京市建国门外大街甲6号
SK大厦1层
邮编: 100022
电话: (86-10) 8567-9238
传真: (86-10) 8567-9235

上海德丰路证券营业部

上海市奉贤区德丰路299弄1号
A座11楼1105室
邮编: 201400
电话: (86-21) 5879-6226
传真: (86-21) 6887-5123

南京汉中路证券营业部

南京市鼓楼区汉中路2号
亚太商务楼30层C区
邮编: 210005
电话: (86-25) 8316-8988
传真: (86-25) 8316-8397

厦门莲岳路证券营业部

厦门市思明区莲岳路1号
磐基中心商务楼4层
邮编: 361012
电话: (86-592) 515-7000
传真: (86-592) 511-5527

重庆洪湖西路证券营业部

重庆市北部新区洪湖西路9号
欧瑞蓝爵商务中心10层及欧瑞
蓝爵公馆1层
邮编: 401120
电话: (86-23) 6307-7088
传真: (86-23) 6739-6636

佛山季华五路证券营业部

佛山市禅城区季华五路2号
卓远商务大厦一座12层
邮编: 528000
电话: (86-757) 8290-3588
传真: (86-757) 8303-6299

宁波扬帆路证券营业部

宁波市高新区扬帆路999弄5号
11层
邮编: 315103
电话: (86-0574) 8907-7288
传真: (86-0574) 8907-7328

北京科学院南路证券营业部

北京市海淀区科学院南路2号
融科资讯中心A座6层
邮编: 100190
电话: (86-10) 8286-1086
传真: (86-10) 8286-1106

深圳福华一路证券营业部

深圳市福田区福华一路6号
免税商务大厦裙楼201
邮编: 518048
电话: (86-755) 8832-2388
传真: (86-755) 8254-8243

广州天河路证券营业部

广州市天河区天河路208号
粤海天河城大厦40层
邮编: 510620
电话: (86-20) 8396-3968
传真: (86-20) 8516-8198

武汉中南路证券营业部

武汉市武昌区中南路99号
保利广场写字楼43层4301-B
邮编: 430070
电话: (86-27) 8334-3099
传真: (86-27) 8359-0535

天津南京路证券营业部

天津市和平区南京路219号
天津环贸商务中心(天津中心)10层
邮编: 300051
电话: (86-22) 2317-6188
传真: (86-22) 2321-5079

云浮新兴东堤北路证券营业部

云浮市新兴县新城镇东堤北路温氏科技园服务
楼C1幢二楼
邮编: 527499
电话: (86-766) 2985-088
传真: (86-766) 2985-018

福州五四路证券营业部

福州市鼓楼区五四路128-1号恒力城办公楼
38层02-03室
邮编: 350001
电话: (86-591) 8625 3088
传真: (86-591) 8625 3050

上海淮海中路证券营业部

上海市淮海中路398号
邮编: 200020
电话: (86-21) 6386-1195
传真: (86-21) 6386-1180

杭州教工路证券营业部

杭州市教工路18号
世贸丽晶城欧美中心1层
邮编: 310012
电话: (86-571) 8849-8000
传真: (86-571) 8735-7743

成都滨江东路证券营业部

成都市锦江区滨江东路9号
香格里拉办公楼1层、16层
邮编: 610021
电话: (86-28) 8612-8188
传真: (86-28) 8444-7010

青岛香港中路证券营业部

青岛市市南区香港中路9号
香格里拉写字楼中心11层
邮编: 266071
电话: (86-532) 6670-6789
传真: (86-532) 6887-7018

大连港兴路证券营业部

大连市中山区港兴路6号
万达中心16层
邮编: 116001
电话: (86-411) 8237-2388
传真: (86-411) 8814-2933

长沙车站北路证券营业部

长沙市芙蓉区车站北路459号
证券大厦附楼三楼
邮编: 410001
电话: (86-731) 8878-7088
传真: (86-731) 8446-2455



CICC
中金公司

