火星区块链

数字金融应用探索中的机遇和挑战

2020年7月

出品方

火星区块链

联合出品

分布式资本 · 欧科云链 · 币安中国区块链研究院 · 标准共识 STANDARD & CONSENSUS

NGC ventures · IOSG Ventures · LONGHASH 用数据读懂区块链 · 共识实验室

出品方：

火星区块链

联合出品：

分布式资本　欧科云链研究院　币安中国区块链研究院　标准共识
NGC Ventures　IOSG Venture　LongHash　共识实验室

CONTENTS

目录

导语　什么是我们所理解的数字金融　01

第一部分　区块链技术驱动金融　01

1.1　区块链技术的本质和核心价值　02

1.1.1　区块链技术发展简述　02

1.1.2　从比特币到以太坊　05

1.2　金融是区块链天然适合的应用领域　09

第二部分　区块链应用落地：赋能金融创新　13

2.1　区块链对传统金融的改造　14

2.1.1　供应链金融　16

2.1.2　支付清算　18

2.1.3　保险　23

2.1.4　征信管理　25

2.1.5　资产数字化　27

2.2　区块链创造新金融物种的诞生　29

2.2.1　DeFi　29

2.2.2　Staking 经济　42

2.2.3　数字通证衍生品　45

CONTENTS

第三部分　区块链技术演进：重塑金融未来　47

3.1　跨链　48
3.2　以太坊 2.0　51
3.3　商业级金融公链　54
3.4　零知识证明　56

第四部分　数字金融创新与全球监管政策　59

4.1　区块链产业政策　60
4.2　沙盒监管　61
4.3　金融标准化建设　65

结语：面向未来的数字金融　67

致谢　70

参考资料　71

导语

什么是我们所理解的数字金融

今天，我们正处在一个新时代的十字路口。

以互联网为底层构架的数字技术经过几十年的发展，缔造了全新的数字世界，并诞生了腾讯、阿里巴巴、Facebook、亚马逊等互联网时代的霸主。

数字世界的进化和迭代的速度远远超过了传统现实世界的发展，区块链技术就是在这样的大背景下应运而生。区块链技术作为集合了密码学、计算机科学等多学科技术革新的集合应用模式，已经被越来越多的人相信，它将是互联网之后最具颠覆性的技术变革。

随着计算机和通信技术的融合，将全部资产数字信息化，并应用在区块链上，达到货品或服务的生产、交易、供货等流程的数字化改造，使得传统常规行业转型成为新数字化产业，这会引起新一轮的社会经济模式的变革，开创一种新的经济体系。

金融是经济体系繁荣兴盛的血液和重要支撑。由于区块链技术特点与金融业务的天然契合，其诞生初期就具备极强的金融属性，区块链也被不少人看作是数字金融的基础设施，是实现价值互联网的关键所在。

然而，对于数字金融的定义，业界尚未形成统一认识，有的观点认为，数字金融是传统金融机构与互联网公司利用数字技术实现融资、支付、投资和其他新型金融业务模式[①]；也有观点认为，数字金融是网络技术与金融的渗入和融合，是将互联网“开放、平等、协作、分享”精神渗透入传统的金融行业，在金融上所表现出的新特征、新技术、新平台、新模式和新形式[②]；也有观点认为，数字资产是数字金融的核心命题；以资产数字化为特征的数字金融创新，是一个全新的体系，或将重构传统金融运行方式、服务模式乃至整个生态。[③]

综合以上观点，在我们看来，**数字金融是以区块链技术为底层驱动的全新一代的金融业务模式，加密数字资产、基于区块链技**

① 黄益平，黄卓，《中国的数字金融发展：现在与未来》，北京大学经济学（季刊），2018 年第 17 期

② 西南财经大学互联网金融研究中心，《中国数字金融发展报告》，2018 年 8 月

③ 引自中国证监会科技监管局局长姚前 2019 年 9 月在第五届区块链全球峰会上的公开发言

术改造的传统金融业务和创新金融业务，都是数字金融重要的应用落地场景。本报告也将围绕数字金融的这一定义，展开细述和论证。

以支付清算为例。在目前金融机构之间、支付机构与银行开展支付结算的过程中，是透过中心节点来处理数据，后台业务的处理需要特定的时间、特定的程序才能成功实现，有些繁琐的交易必须手工注册和核实，在跨境商品交易之后，资金不能与商品同时到位，造成清算资金的时滞，这妨害了清算支付的效率。而要提高支付清算系统体系的支付效率和体系的稳妥性，必须对支付结算系统体系实行系统结构优化，区块链技术为之提供了一条可行之路。通过建立一种网络支付清算平台，以区块链分布式架构为基础，可以提高清算效率，大大降低支付机构的经营费用，借助该平台为公司与机构间的支付清算提供相同划一、公共的交易支付清算方式来实现；交易的清算便可在链上同步完成，参与者共同享有，更新及时，支付清算生态系统的清算效率将会大幅改善。

回眸历史，76 年前的 1944 年，在助推美元击败英镑成为全球货币的布莱顿森林体系中，其中关键的因素就是美元与黄金挂钩，其他货币与美元挂钩。如今，金融市场的基础设施正在逐渐被区块链重构。试想一下，在未来的数字金融世界里，基于区块链的加密数字货币能否引发全球货币新的主导权之争？中国如何获得全球数字金融的领先地位和话语权？如何去构建更加先进、开放和高效的数字金融体系？如何让数字化的资产具备更高的流通性……都是需要我们不断思考和实践的问题。

普林斯顿大学计算机系教授阿尔文德·纳拉亚南（Arvind Narayanan）等著的《区块链：技术驱动金融》一书中提到，长达 10 年的全球金融危机、全球货币与资产价值的不稳定，就是数字货币和区块链技术被国内外众多金融机构和个人追捧的一个重要背景，而区块链技术创造了一个用“共信力”来解决公信力的途径。

可以预见，在澎湃的区块链浪潮下，以区块链为“创造信用”引擎的数字金融将重塑整个世界的金融体系，甚至开创一个全新的金融世界。

我们和你一样，期待和见证着数字金融新时代的到来！

火星区块链产业研究院
《数字金融应用探索中的机遇和挑战》报告编委会
2020 年 7 月

PART 1

第一部分

区块链技术驱动金融

1.1 区块链技术的本质和核心价值

在过去十年的数字经济发展浪潮中，区块链技术成为最受人瞩目的技术之一。区块链技术利用非对称加密，共识算法等技术，凭借公开透明、不可篡改等优势，在金融经济、民生政务等领域都有广泛的应用。

1.1.1 区块链技术发展简述

从技术角度看，区块链技术并不是一种单一的技术，而是通过巧妙方式将原有技术（如非对称加密，时间戳，工作量证明等）组合而形成的技术。区块链技术强调的是制度设计的革新，而非基础技术的原创。

在整个区块链技术体系中，最重要的是非对称加密算法[①]，其诞生于上世纪 70 年代，但在开始时，加密技术主要运用在国防外交领域。直到 1983 年，大卫·乔姆（David Chaum）提出可以将加密技术运用于电子现金上，同时为了防止出现“双花（Double Spending）问题”[②]，乔姆提出了一个创造性的

大卫·乔姆（David Chaum），阿姆斯特丹数学与计算机中心密码组的负责人。1982年提出匿名的密码学网络支付系统，被认为是区块链设计思想的雏形。

亚当·贝克（Adam Back），英国的密码学家，1997年发明了哈希现金（Hashcash），其中用到了工作量证明系统，后来成为比特币区块链的核心要素之一。

戴维（W DAI）在1998年发明了B-money。强调点对点的交易和不可更改的交易记录，以及保持对交易的追踪。其分布式思想是区块链的重要灵感来源。

尼克·萨博（Nick Azabo），2005年提出比特金的设想。此外萨博还发表多篇关于《合同法》在网络安全实现的文章，这些思想被视为智能合约的起源。

图：区块链技术的重要贡献者

① 非对称加密算法：一种密钥的保密方法，通常需要两个密钥：公开密钥（publickey，公钥）和私有密钥（privatekey，私钥）。如果用公钥对数据进行加密，只有用对应的私钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。

② 双花（Double Spending）：即双重支付，指的是在数字货币系统中，由于数据的可复制性，使得系统可能存在同一笔数字资产因不当操作被重复使用的情况。

解决方案“盲签技术（Blind Signature）”[①]，这是第一个真正意义上的电子货币方案，虽然它还必须要有一个受大家信任的中心化服务器。

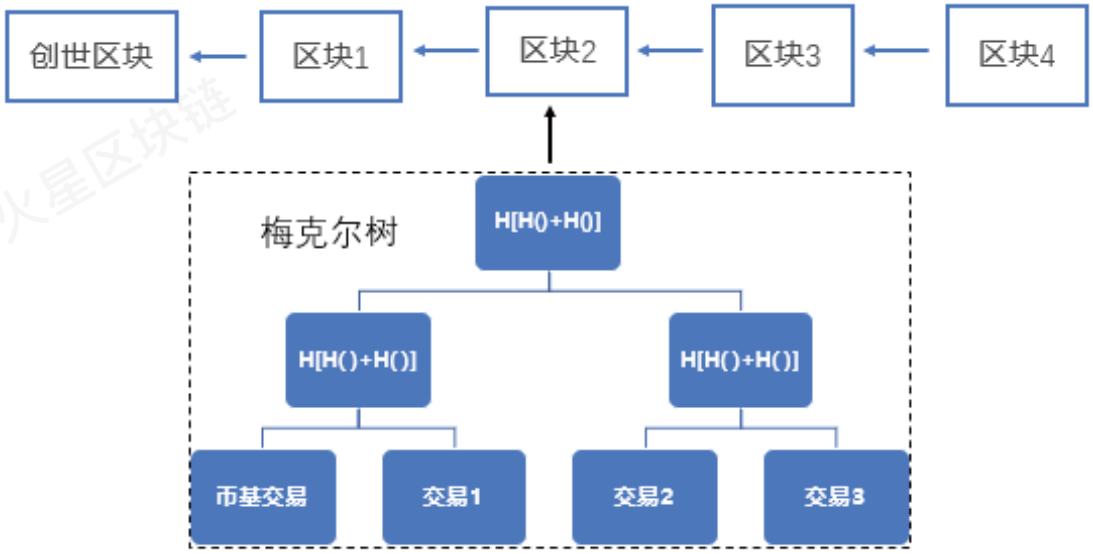
1997 年，亚当·贝克（Adam Back）发明了哈希现金，其中用到了工作量证明技术。该技术由密码学家新提亚·沃克（Cynthic Dwork）和摩尼（Moni Naor）在 1992 年提出，主要用来解决垃圾邮件问题，后来成为区块链技术最重要的基础之一，用于解决加密数字货币的发行问题。

区块链的另一个关键技术是时间戳，该理论基础最早可以追溯到哈勃（Haber）和斯托尔内塔（Stornetta）1991 年发表的一系列论文。他们指出，可以利用时间戳来记录文件创建的时间，利用时间和指针作为签名，以防止数据被更改。随后他们还在另一篇论文中提出了一个提升效率的方案：不必链接每个文件，而是把它们集合成块，然后在一条链中链接整个块；在每个块里，文件通过树状结构的方式相连，这样减少了查找特定文件所需的工作量。

这一特殊的数据结构，形成了区块链最原始的框架结构，即人们理解的狭义区块链。

随后，戴维（W DAI）在 1998 年发明了 B 币（B-money），尼克·萨博 (Nick Szabo) 在 2005 年提出比特现金的设想，这两项发明均运用了时间戳技术来保障数据的完整和不可篡改，但遗憾的是他们都没有解决分布式条件下数据的一致性问题，即著名的“拜占庭将军问题”。

为了解决这个问题，兰伯特提出了 OM



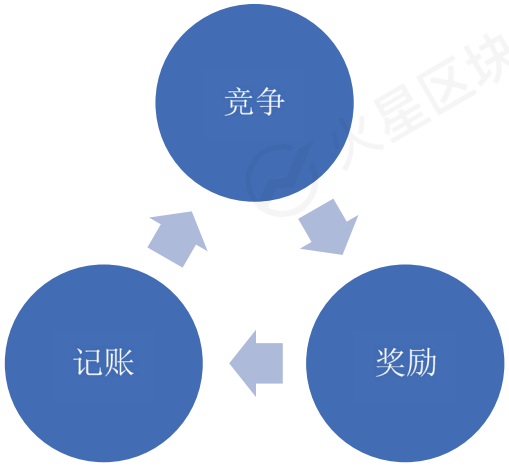
图：高效的时间戳框架

① 盲签（Blind Signature）：是一种数字签名的方式，在消息内容被签名之前，对于签名者来说消息内容是不可见的。

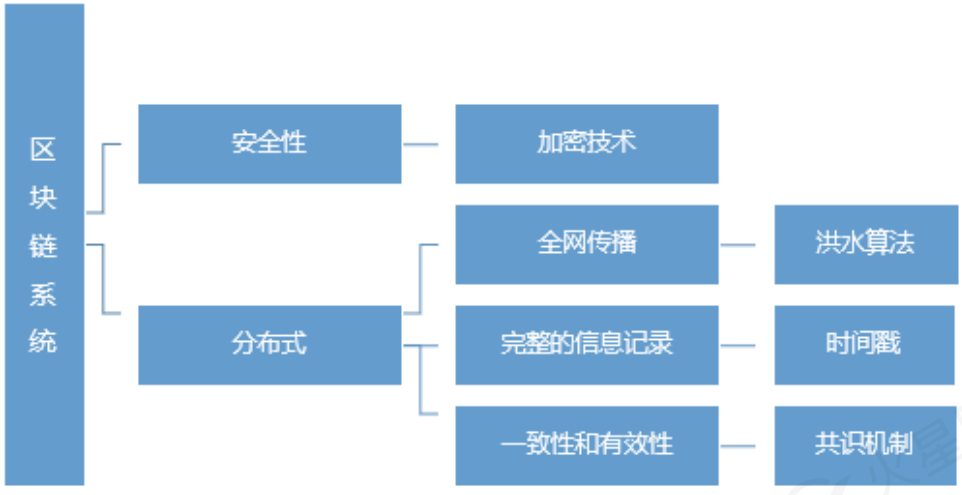
算法，在这种情况下，只有当问题计算机的总数不超过计算机总数的 1/3 时，才能实现最终的一致行动。更为著名的是“Fischer-Lynch-Paterson 结论”，该理论认为在一个多进程异步系统中，只要有一个进程不可靠，那么就不存在一个能保证有限时间内使所有进程达成一致的协议。

之后，中本聪（Satoshi Nakamoto）在比特币区块链系统中设计了一个精巧的共识机制，从而打破了原有分布式理论中的“不可能性结论”，完美地应用经济思维解决了技术科学上的难题。

事实上，当前所有的公有链共识机制，均是遵从中本聪设计的竞争记账框架构建的。基本原理图如下图所示，系统上所有的节点通过竞争选出优胜者，优胜者拥有记账权，而通过记账能获取加密数字货币作为奖励，这反过来又激励节点参与新的记账竞争。这套系统将维护账本的唯一性和一致性与数字货币的发行完美地结合到一起，在引入竞争的同时，解决了去中心化货币系统发行的难题，这非常类似于去挖掘金矿并将黄金注入到货币流通领域，因此被形象地称为“挖矿”，由此形成了一个完美的经济系统。只不过，在竞争中 POW 使用的是“工作量证明”，POS 使用的是“权益证明”（根据权益的大小来决定竞争记账的获胜者），DPOS 使用的是“股份授权证明”（类似股东大会选举产生董事会的制度，是一种选举投票竞争）。



图：基于竞争记账框架的共识机制



图：区块链系统技术

从大卫·乔姆的盲签技术，到沃克的工作量证明，再到哈勃的时间戳，一代代先驱在电子现金上的探索，累积了大量的技术基础，而中本聪接过了最后一棒，站在这些先驱的肩膀上，用经济学的思维，通过POW机制完美解决了“拜占庭将军问题”，最终形成了目前我们所熟知的区块链技术。

“智能合约”的概念早在1994年就由计算机科学家、加密大师尼克·萨博(Nick Szabo)于《智能合约》(Smart contracts)一文中正式被提出。智能合约的概念虽更早提出，但限于缺少可落地的执行方案使其长期没有得到真正应用（在区块链之前，主要的是自动售货机形式的“智能合约”应用）。直到区块链技术出现以后，基于区块链的智能合约开始被广为认知，也开始了大规模的应用研究和开发。

区块链技术的去中心化、去信任、规则透明、集体维护、不可篡改等特性，恰好为智能合约提供了安全可靠的记录载体和执行环境。

首先，区块链技术采用纯数学的方法，在不牺牲隐私性，也无第三方信用机构参与的条件下，可以对所有过去、当前的数字事件（如行为、资产等），建立分布式的一致性表达；其次，区块链提供了可供用户进行编程的脚本系统，进一步增强了区块链应用的灵活性，如在以太坊中，具备图灵完备、功能强大的脚本系统，使得基于智能合约的更为高级的分布式应用得以实现。

1.1.2 从比特币到以太坊

2008年美国次贷危机爆发，并陆续引发全球范围的金融危机。当时的民众普遍把责任归结为以华尔街为代表金融资本业的贪婪以及政府的不作为。

2009年1月3日，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了比特币的第一个区块——创世区块（Genesis Block），并获得了首矿奖励——50个比特币。在创世区块中，中本聪写下这样一句话：The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.（财政大臣处于第二次援助银行的边缘）。而这句话是英国《泰晤士报》当天的头版文章标题。

根据《比特币白皮书：一种点对点的电子现金系统》内容，比特币提出了一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。

比特币是去中心化思维的最新产物，用不可攻破的数学原则来规制人的行为，从而免去复杂的政府系统的保护。其目的是解决金融交易中的信息不对称、搜索成本高、匹配效率低等问题。伴随着互联网和计算机技术的发展，人们可以借鉴一个更具优势的去中心化模式，来解决现行金融体制中存在的许多问题。

比特币对于现行金融体制的启发与借鉴，主要体现在以下方面：

类别	传统金融业	比特币
记账方式	中心化的重复记录	信息全网自动同步
信息传递	渠道闭塞，缺乏透明	渠道开放、公开透明
监管成本	强力监管导致成本高昂	匿名性使保管数据成本降低
数据安全	中心化记录者数据丢失的风险	掌握51%算力后的双花攻击风险

图：比特币与传统金融业的主要区别

（1）中心化的重复记录与比特币的自动广播

现有的金融体系采取的是中心化记录方式，这存在明显的弊端，最为突出的就是记录的重复性。首先，主流的复式记账法要求同时记录资产和负债两个项目，这意味着一笔商业银行的交易，需要被两个独立的系统记录两次，这样的系统繁琐且维护成本昂贵；其次，因为这笔交易只在交易双方的银行中得到了有效的记录，但商事交易是一个庞大的体系，这两家银行还需要保证其他各方银行和金融机构对这笔交易的记录是一致的，因此需要多方对账，这种大规模的对账体系需要花费大量成本。

在比特币去中心化的系统中，借助区块链技术，每笔交易完成之后自动广播给其他所有节点，使得整个区块链信息是全网自动同步，交易网络能够自动记录和存储交易数据，并自动完成交易，而这正是金融机构青睐区块链技术的重要原因。同时，通过数据自动记录与同步促成的去中心化的交易，金融市场也更加贴近自由市场模式，运行效率更高，系统更稳定。

（2）信息闭塞与比特币信息的开放透明

现行的金融体系中，大多数投资者往往只能通过间接融资市场、直接融资市场、结构性融资等进行金融交易，且投资者往往缺少话语权，只能作为资金的提供者。因此，对于投资者而言，获取投资的信息渠道较为闭塞，交易信息不够透明。

比特币系统的开放，改善了传统金融中最为严重的信息不对称和逆向选择[①]问题，并提供最大化的信用公示系统，由此大大削减交易或借贷双方为获取信息而产生的事前、

① 逆向选择，指市场的某一方如果能够利用多于另一方的信息使自己受益而使另一方受损，倾向于与对方签订协议进行交易。

事中与事后的成本。尤其是对于小微金融和普惠金融领域，信息的不确定带来了极大的金融风险与交易成本，而比特币和其背后的区块链系统让这些企业的“自金融”市场模式体系健全化、自由竞争化成为可能。

（3）监管的弊端与比特币的匿名性

信息不对称会导致当前市场普遍处于失灵模式，最直接的解决办法就是通过强力的监管，要求所有信息必须进行公开，出具各种质量要求和质量标准。如此大范围的监管包括了固定成本、设备投入和可变成本及耗费的电费、人力等，这些成本汇集在一起形成了巨大的资源浪费。

比特币的匿名性体现在其背后的区块链是一种“推式”技术，而非传统金融业一般使用的“拉式”技术。“拉式技术”要求交易的银行或金融机构主动抽取用户储存在各类繁杂账户中的无序信息，再一一进行整合，这样的拉取过程非常耗时耗力。而在比特币交易中，用户只需要在交易时将交易的相关信息“推送”给网络，也即将该笔交易推送到整个区块链系统中，由矿工对该笔交易进行记录。这样可以保护无需存储用户的个人信息，从而避免被黑客攻击或被中心打包出售、出租或流入其它非法途径，并且可以进一步降低保管数据的费用。

（4）中心化记账风险与比特币分布式记账的安全性

财产不被侵犯是每个用户最需要被保护的权利，而安全性也是中心化记账的重要因素。如前文所说，虽然中心化的金融体制不断进行技术更新，但是中心化记录者数据丢失的风险从未消除，其中中心化节点的数据一旦丢失，就很难再恢复。

对此，比特币系统通过数字和代码构建出的分布式记账法，提供了更高的安全性。比如，比特币账户的唯一性及不可盗用性，是通过密码学的哈希函数实现的，加密后的哈希函数有着诸多特性，比如碰撞阻力[①]等。哈希函数的这一特性使比特币账户生成的地址是唯一的，且无法通过地址逆向反推出密钥值，因此比特币的账户具有唯一性和不可盗用性的特点，这也是整个分布记账法运行的基础之一。

当然，比特币系统也存在一定的安全风险，最值得关注的是“双花攻击”，即通过制造两笔交易，将假的交易纳入最长的区块链中，再利用区块链账本只识别最长链的特点，以完成比特币两次花费的目的。但“双花攻击”往往需要攻击者拥有全网 51% 的算力，这对于造假者而言无疑是一个巨大的成本，实施难度极大。

比特币开创了去中心化加密数字货币的先河，构造了全新的货币传输体系——比

① 碰撞阻力：如果有两个不同的值 X，Y，H(X)=H(Y) 成立，则称哈希函数 H 产生了碰撞。而碰撞阻力是指无法找到两个不同的值 X，Y 使得 H(X)=H(Y)。

特币网络。然而比特币并不完美，如：协议的扩展性不足，在比特币网络里只有一种符号——比特币；另外，比特币协议里使用了一套基于堆栈的脚本语言，该语言虽然具有一定灵活性，使得像多重签名这样的功能得以实现，然而却不足以构建更高级的应用。

受到比特币的启发，2013 年末，以太坊创始人 Vitalik Buterin 发布了以太坊初版白皮书，正式启动了以太坊项目。而以太坊设计初衷，就是为了解决比特币扩展性不足的问题①。

Vitalik Buterin 将以太坊比作“世界计算机”，在他看来，区块链应当是一个功能类似于计算机的整体，它有一个硬盘驱动器，存储着所有的账户，同时还存储了所有智能合约的代码，以及所有这些智能合约存储的信息。

以太坊致力于实施全球去中心化且无所有权的数字技术计算机，并执行点对点合约。简单讲，以太坊是一个你无法关闭的“世界计算机”。利用以太坊可以创建去中心化的程序、自治组织和智能合约，其加密架构与图灵完整性的创新结合将促进大量产业创新出现。

由以太坊引入智能合约融合后的区块链技术，对于现行金融体制的启发与借鉴，主要体现在以下方面：

（1）降低金融交易成本尤其是跨境交易成本。

智能合约不受地域限制适用于全球任何区域的交易行为处理，使得可信的资产和金融工具自由流通，减少第三方机构的介入和因此产生的费用，在状态判断、条款执行、资产处理、信息核对等方面比受限于具体辖区的传统合约具有明显的低成本优势。

（2）保障金融交易安全和效率。

智能合约一旦确定，相关资金就会按照合约执行，任何一方不能控制或者挪用资金，确保交易安全。记录在区块链上的智能合约具备不可篡改和无需审核的特性。

（3）有助于金融机构对交易的监管。

区块链上创建的分布式账本，记录上链的资产、交易和所有权情况，区块链上嵌入的智能合约也是公开透明的，这样会方便金融机构的监管。

（4）协助实现央行可编程货币功能。

国家央行利用区块链技术发行数字货币，最终目的是实现可编程货币，即央行可以对区块链上的任何资产写入代码，嵌入智能合约。一旦实现，则当央行需要实施量化宽松政策或者发行特定金额到制定账户，即可把发行目标、账户、批次、时间等信息以代码形式事先编写好，满足触发条件后就会自动执行，极大增强央行的管控能力的同时提高

① Vitalik Buterin 在《以太坊白皮书》中提到：“基于比特币的方法存在缺陷，因为它继承不了比特币的简化支付验证（SPV）功能”，“比特币实验的另一部分，可以说是更加重要的部分——是作为分布式共识工具的底层区块链技术，关注正在迅速转移到比特币的其他方面。”

透明度。

在 2019 年 4 月底上线的新版以太坊官网首页上，以太坊官方修订了以太坊的定位，特别强调了以太坊在去中心化金融方向的愿景。以太坊联合创始人 Joseph Lubin 更是为以太坊提出一个更为务实的远景——去中心化的全球结算层。

Joseph Lubin 认为，当我们对世界进行通证化的时候，资源丰富的金融机构和交易者依旧会不遗余力地操纵市场，以获取利益或政治优势。但是我们不希望下一代经济中流动性强的代币市场（通证市场）同样脆弱，我们必须选择一个最为去中心化的基础作为全球经济的基本结算层。

Vitalik Buterin 曾断言，金融行业很可能是第一个被区块链颠覆的行业。从“世界计算机”到“全球结算层”的转变，意味着以太坊的使命可能会越来越集中于服务于金融创新。

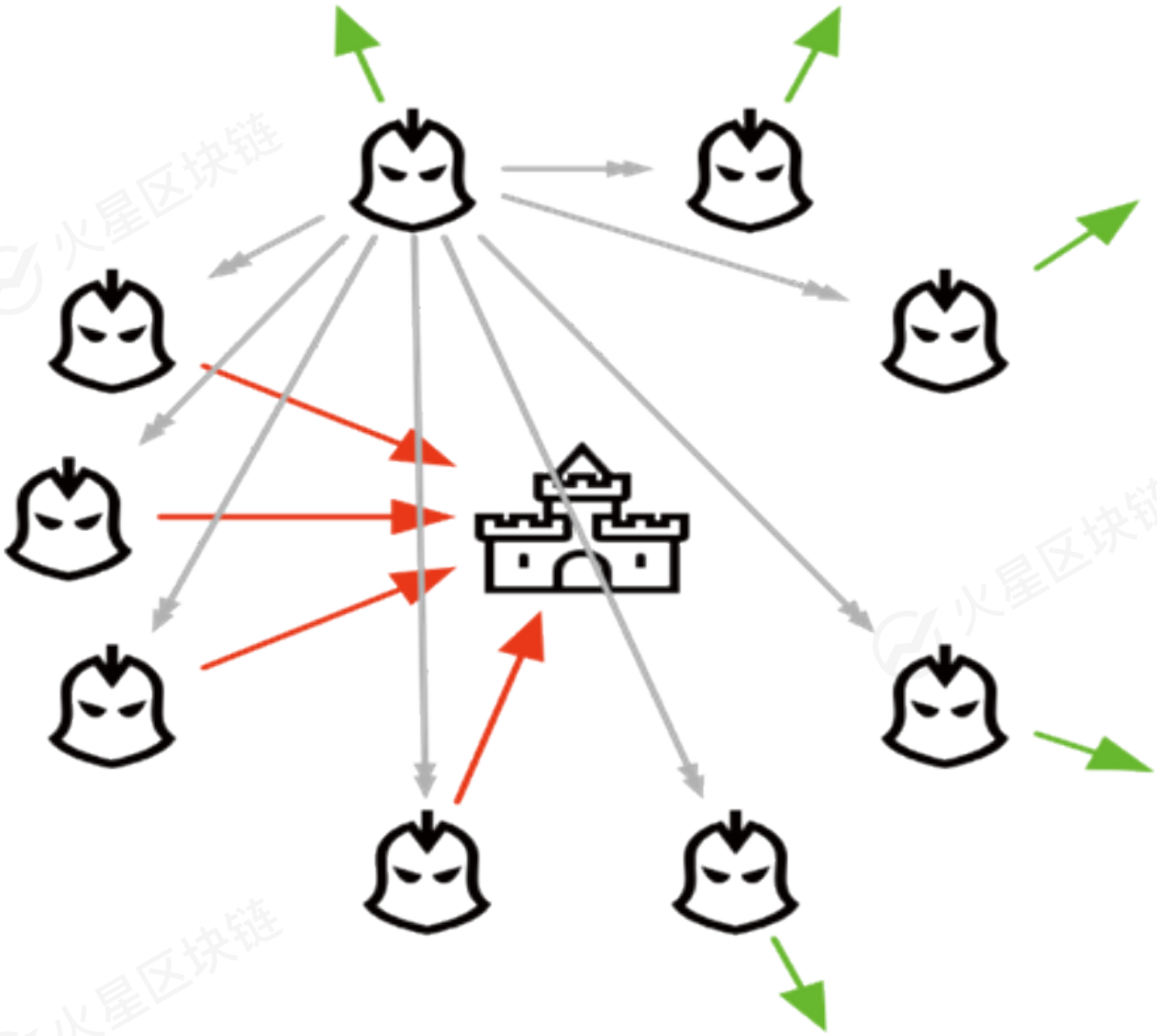
1.2 金融是区块链天然适合的应用领域

信息的真实性，即信息不对称问题，是现代金融理论研究的一个重要问题。区块链技术之所以能够得到金融科技界的广泛关注，主要是其解决了信息传递中的信用问题，也称“拜占庭将军问题（Byzantine Failures）”。

拜占庭将军问题由 Leslie Lamport 最早提出。拜占庭帝国（东罗马帝国）国土辽阔，驻守边疆的各支军队距离远，将军间依靠信差传递消息。根据规定，只有在所有将军和副官达成共识的情况下，才能攻打敌人。但是，由于军队内部存在叛徒和间谍，其发出的错误信息可能会影响出兵决定。“拜占庭将军问题”就是在已知存在叛徒的情况下，忠诚的将军如何不受影响，形成正确共识的问题。

金融科技领域迫切需要拜占庭将军问题的解决方案，以应对分布式系统的信息交互问题，即当网络中任意节点都无法相互信任时，如何防范信息被篡改并形成共识，以进行安全的信息交互。

而区块链技术的特点可以有效解决拜占庭将军问题。共识机制使得一段时间内只有一个节点发送消息，其他节点验证即可。由于区块链消息全网广播，故各个节点接收到的消息是一致的。非对称加密技术保护消息内容，同时让消息接收方确定发送方的身份。A 发给 B 的消息通过 B 的公钥加密，B 通过私钥解密。若 A 想申明自己的身份，只需要将消息使用自己的私钥进行签名即可，B 收到消息后就可以使用 A 的公钥验证消息的来源。由此，一个不可信的分布式网络变成了一个可信的网络，所有的参与者可以在某件



图：拜占庭将军问题示意图

事达成一致。

在一个互不信任的市场中，要想使各节点达成一致的充分必要条件是每个节点出于对自身利益最大化的考虑，都会自发、诚实地遵守协议中预先设定的规则，判断每一笔记录的真实性，最终将判断为真的记录记入区块链之中。换句话说，如果各节点具有各自独立的利益并互相竞争，则这些节点几乎不可能合谋欺骗你，而当节点们在网络中拥有公共信誉时，这一点体现得尤为明显。

共识机制是区块链节点就区块信息达成全网一致共识的机制，可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。可以说，共识机制是解决拜占庭将军问题所引发信任缺失的重要保障。

现今区块链共识机制主要类别包括工作量证明（Proof of Work，POW）、权益证明机制（Proof of Stake，POS）、股份授权证明机制（Delegate Proof of Stake，DPOS）等。

区块链技术正是运用一套基于共识机制的数学算法，在机器之间建立“信任”网络，从而通过技术背书而非中心化信用机构来进行全新的信用创造，解决了金融业一直以来存在的信任缺失的问题，为金融业创造一种“自信任”的全新生态提供了更多可能性。

从区块链技术的特点看，其在金融领域中的应用存在巨大潜力，包括证券的发行与交易、清算结算等各流程、各环节都可以通过区块链技术被重新设计和简化，从而带来一系列潜在的优势，包括提高效率、缩短处理时间、加大透明度、降低成本和确保安全。可以说，金融领域是区块链天然适合的应用领域，两者之间具有非常高的契合度。

（1）**交易效率**。

在金融交易中，前台系统承担着撮合交易的功能，后台系统则负责交易的清算与交收，两个系统流程和环节较多，使得各交易所处理交易的时间与资金成本过高；同时，不能在交易当日完成实时结算的制度给资本也带来了潜在的风险。区块链能够简化、自动化冗长的交易流程，实现证券发行人与投资者的直接交易，减少前台和后台交互，节省大量的人力和物力。

图：区块链主流共识机制的类型

（2）信息记录。

区块链中的数据信息是不可篡改的，配合“时间戳”等技术，区块链将系统成立以来的所有交易全部记录在数据区块中，所有的交易活动都可以被追踪和查询到，并且形成的数据记录不可篡改。这便于对金融交易活动进行追踪，可以有效解决交易验证和交易后续纠纷等问题。

（3）系统安全。

传统金融市场以交易所为中心，交易所的交易系统保证全部交易的正常进行，一旦交易系统被攻击或出现故障，就可能导致整体网络瘫痪，交易暂停。区块链技术利用许多分布式节点和高性能服务器来支撑点对点网络，整体运作不会因部分节点遭受攻击或出现问题而受影响。

（4）隐私保护。

区块链技术可以确保金融交易信息的机密性和安全性。区块链的信任基础是通过数学的代码方式而建立起来。区块链技术利用公钥地址代替用户的身份信息，从而能够有效实现匿名性，使人们在互联网世界里实现信息透明共享的同时，不会暴露自己的真实身份信息，极大地保护参与者的个人隐私。

PART 2

第二部分

区块链应用落地：赋能金融创新

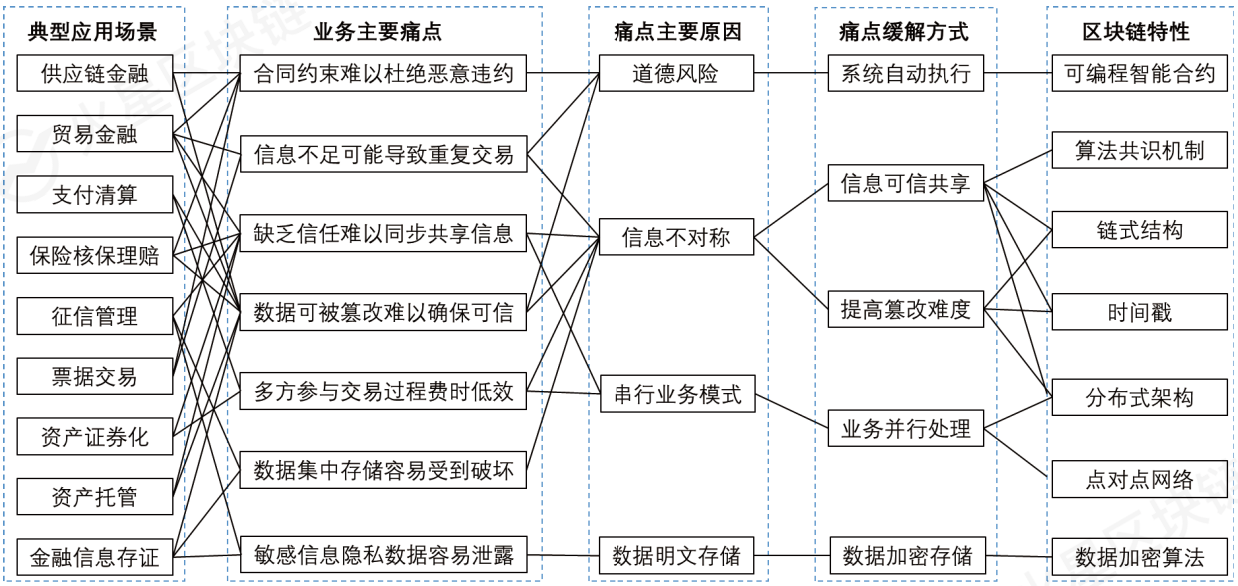
2.1 区块链对传统金融的改造

区块链技术具有数据不可篡改、可追溯等数据存储的特点，是结合去中心化实现维护数据库可靠性的方案，改变了数据记录和共享的模式，减少了交易双方信息不对称、效率低下等传统金融存在的主要问题。

从具体适用领域看，区块链技术的分布式架构、链式结构、共识机制、时间戳提升了数据的不可篡改性，能够实现信息可信共享，解决金融领域的信息不对称问题；加密算法的应用，很好地降低金融领域的数据泄露风险；智能合约的引入，则有助于实现复杂业务流程的自动执行，提高了业务处理效率，有效降低了金融业务的道德风险和操作风险。

因此，区块链技术为传统金融创造了一个交易成本更低、效率更高、安全性更好的业务模式。区块链技术与金融业相结合，必然将会创造出越来越完善的业务模式、服务场景和金融产品。

从我国实际情况看，区块链技术逐渐在金融领域实现一定规模的落地应用，截至2019年8月，已有近30家银行500余家网点业务实现上链运行，业务总量超500亿元人民币。各大金融企业也基本实现了区块链技术在其业务领域的落地。



图：区块链技术在典型金融应用场景的应用

表：全球主要金融机构区块链实践 ①

		数字货币	资金管理	贸易金融	供应链金融	支付清算	风控	数字资产	其他
国内	中国银行			区块链福费廷交易平台 海区贸易金融区块链平台 中国贸易金融跨行交易区块链平台		中国银联区块链跨境汇款服务平台	区块链抵押贷款估值系统	区块链债券发行系统	
	中国农业银行			跨境 e 链 中国贸易金融跨行交易区块链平台	e 链贷				
	中国工商银行		雄安征拆迁资金管理区块链平台 贵州脱贫攻坚基金区块链管理平台	中欧 e 单通 中非 e 链通 中国贸易金融跨行交易区块链平台	工银 e 信网络融资金融服务平台				
	中国建设银行			BCTrade2.0 区块链贸易金融平台 海区贸易金融区块链平台 中国贸易金融跨行交易区块链平台	基于区块链的再保理业务平台				
	中国交通银行			中国贸易金融跨行交易区块链平台				链交融	
	平安银行			"资企链"融资平台 区块链福费廷交易平台 海区贸易金融区块链平台 中国贸易金融跨行交易区块链平台				金融壹账通 ALFA（阿尔法）智能 ABS 平台	
	香港交易所					区块链交易结算系统			
国际	美国银行						申请区块链相关专利 53 件，涉及风险检测、交易验证、可疑用户警报等		
	摩根大通	JPM Coin				基于 Quorom（自建区块链平台）的银行间信息网络(IIN)		基于 Quorom 测试债券发行	
	汇丰银行			voltron 平台		FX Everywhere 平台			
	花旗	Citicoin（已放弃）				与纳斯达克合作使用分布式账本开发一体化自动交易结算支付解决方案	参与 IBM LedgerConnect 试运行		
	高盛	SETLcoin							
	摩根士丹利					BDS360 区块链平台，用于处理交易备份交易结算记录			
	纳斯达克					私有股权交易平台 LinQ 与花旗合作使用分布式账本开发一体化自动交易结算支付解决方案			区块链投票和代理委托应用 eVoting
	澳大利亚交易所					区块链交易结算系统			
	洲际交易所					数字资产平台 Bakkt			
	伦敦证券交易所					成立跨行业组织，探索区块链清算结算		证券发行数字化	
	德意志交易所								区块链证券借贷
	AXA								Fizzy 区块链保险系统

	基础平台	资金管理	供应链金融	贸易融资	支付清算	数字资产		
						ABS	票据	其他
工商银行	√	√	√	√		√	√	
农业银行			√					
中国银行		√			√	√	√	
建设银行		√	√					
交通银行						√		
邮储银行		√		√				
招商银行				√	√	√		
平安银行	√		√	√				√
浦发银行							√	
度小满	√					√	√	√
蚂蚁金服	√				√		√	
微众银行	√		√		√			
京东数科	√		√			√		

图：国内金融企业区块链应用落地情况

① 参考资料：中金公司、币安中国区块链研究院

2.1.1 供应链金融

全球著名债券评级机构穆迪曾给出过127个区块链案例，从积分到交易清算，从文件存证到供应链管理，从跨境支付到供应链金融，各种应用层出不穷。而在如此众多的应用当中，又属供应链金融领域最受瞩目，商业化落地的进展较快。

供应链金融（Supply Chain Finance），是指将供应链上的核心企业以及与其相关的上下游企业看作一个整体，以核心企业为依托，以真实贸易为前提，运用自偿性贸易融资的方式，对供应链上下游企业提供的综合性金融产品和服务。根据融资担保品的不同，金融机构将供应链金融分为在应收账款类、预付类和存货类融资，其中应收账款类的规模尤为巨大。

图：供应链金融基础业务模式①

（1）区块链如何解决供应链金融的痛点

痛点1：供应链上的中小企业融资难，成本高

由于银行依赖的是核心企业的控货能力和调节销售能力，出于风控的考虑，银行仅愿意对核心企业有直接应付账款义务的上游供应商（限于一级供应商）提供保理业务，或对其下游经销商（一级供应商），提供预付款或者存货融资。这就导致了有巨大融资需求的下游供应商/经销商的需求得不到满足，供应链金融的业务量受到限制，而中小企业得不到及时的融资易导致产品质量问题，会

① 参考资料：苏宁金融研究院相关资料

伤害整个供应链体系。

区块链解决方案：供应链生态整体电子化，并在底层有区块链支持，使供应链的资金流、物流、商流、信息流四流合一，生态各方及中立第三方共同形成联盟链，在上发行应收帐款的凭证，这种凭证由于背后有四流来进行确权，以保障其真实性，并可以在公开透明、多方见证的情况下进行随意的拆分和转移。这种模式相当于把整个商业体系中的信用将变得可传导、可追溯，为大量原本无法融资的中小企业提供了融资机会，极大地提高票据的流转效率和灵活性，降低中小企业的资金成本。

痛点 2：作为供应链金融的主要融资工具，现阶段的商业汇票、银行汇票使用场景受限，转让难度较大

商业汇票的使用受制于企业的信誉，银行汇票贴现的到账时间难以把控。同时，如果要把这些债券进行转让，难度也不小。因为在实际金融操作中，银行非常关注应收账款债权“转让通知”的法律效应，如果核心企业无法签回，银行不会愿意授信。据了解，银行对于签署这个债权“转让通知”的法律效应很谨慎，甚至要求核心企业的法人代表去银行当面签署，显然这种方式操作难度是极大的。

区块链解决方案：银行与核心企业之间可以打造一个联盟链，提供给供应链上的所有成员企业使用，利用区块链多方签名、不可篡改的特点，使得债权转让得到多方共识，降低操作难度。当然，系统设计要能达到债券转让的法律通知效果。同时，银行还可以追溯每个节点的交易，勾画出可视性的交易流程图。

（2）区块链公司如何切入供应链金融业务

在市场选择上，我们认为区块链初创公司应选择天花板足够高，供应链较长且上下游小而多的细分领域，比如家电、服装、汽车等。这些行业一方面市场广阔，另一方面对供应链管理以及供应链金融的需求较大。总体上看，区块链公司切入供应链金融主要有两种模式：

第一种模式，直接与核心企业 / 平台合作，为其提供区块链底层解决方案，在积累足够多数据之后，通过搭建联盟链，对接资金方提供金融服务。获得核心企业的支持可以有效解决获客的问题，因为一家大型核心企业一般都会有很多家的各类供应商。目前，国内的区块链公司从核心企业切入的包括布比、网录科技等，布比推出了一个专为供应链金融打造的联盟链“布诺”，将银行、核心企业、保理公司等都链接起来，布比立足广州深圳，辐射东南区业务，深挖供应链金融领域。

第二种模式，从提供供应链管理服务入手，比如溯源、追踪、可视化等，将资金流、物流、商流、信息流整合到一起，在此基础之上从事金融服务。这种模式相当于用区块链搭建起了一个应用场景。比如 VeChain 提供一种防伪溯源的方法，通过给每个商品植入一个 NFC 芯片，将商品注册到区块链上，

使其拥有一个数字身份，再通过共同维护的账本来记录这个数字身份的所有信息，达到验证效果。目前 Vechain 产品已经对接了多家行业标杆客户，数百万个 ID 运行在链上。

（3）区块链技术在供应链金融领域应用的实现路径

从实现路径来看，区块链在供应链金融领域的应用，可以通过三个步骤来实现：

作为前提，我们需要先打造一个区块链 + 供应链金融的联盟，联盟的参与者包括供应链金融平台，核心企业、专业的金融中介机构、资金方、保理机构等。每个参与者都需要承担相应的义务，比如平台负责提供供应链信息，客户信息这些类似水电的基础服务，而核心企业了解行业状况，对供应链上的企业具有掌控力，负责风险控制。

专业的金融中介机构可以对平台信息进行整合分析，提供定制化的供应链金融产品，比如个性化的区块链电子票据。资金方包括银行、互联网金融机构等负责对接相应风险偏好的客户。

联盟链搭建好之后，就可以开始三步走战略：第一步，数据上链，将供应链联盟里的数据放到链上，利用区块链的特性使其不可篡改，并提供数据的确权，溯源等服务。第二步，资产数字化，把仓单、合同、以及可代表融资需求的区块链票据都变成数字资产，且具有唯一、不可篡改、不可复制等特点。第三步，数字资产的交易，供应链金融平台将将转变成一个金融资产交易所，将非标的企业贷款需求转变成标准化的金融产品，对接投融资需求，进行价值交易。

最终，区块链技术将能有效地增强供应链金融资产的流动性，调动新型的融资工具和风控体系帮助覆盖中小企业融资的长尾市场，催生供应链金融即服务。

案例：腾讯金融科技的微企链平台

微企链是腾讯 + 联易融共同打造的“供应链金融 + 区块链 +ABS 平台”，于 2018 年成立，通过第三方强信任背书的资产网关，实现资产真实上链的操作；引入多签名，实现多主体多种资产的相互转让；用资产模型（UTXO）做一对多的资产映射；最后，在兑付环节引入腾讯财付通的资金清算能力，面向用户开发 APP 来实现线上的处理。从中小微企业来看，通过引入核心企业的贷款额度，实现比较低的融资利率，引入过桥基金，实现秒级放款。从核心企业来说，实现对供应链企业的知情权和全链条健康安全的管控，核心企业可以改善现金流与负债表，提升供应链效率。对金融机构来说，很多银行以前都是给核心企业贷款，引入中小微企业后，提升了他们的获客能力，通过自主定价，提升相关收益。

2.1.2 支付清算

作为核心金融基础设施中的一部分，支付清算将彼此独立的不同金融模块连接成有机的整体，促使其正常运转。在现代金融体系中，随着金融产业规模的扩大，支付体系的地位逐渐凸显，向下有利民生，降低社会

上交易的摩擦成本，向上提高经济运行效率，促进经济稳定发展。

（1）区块链在境内支付结算领域的应用

自 2002 年 10 月 CNAPS（中国现代化支付系统）在北京、武汉两地投产后，在接下来十多年内，第二代 CNPAS 和 CIPS（人民币跨境支付体系）逐渐建立并完善，共同构成中国支付清算系统。境内支付方面，根据中国支付清算发展报告（2019）提供的数据，可以看到 2018 年全国银行业金融机构共办理非现金支付业务 2203.12 亿笔，金额 3768.67 万亿元，同比分别增长 36.94% 和 0.23%。

支付清算呈现以下特点：票据业务总量下降、结构分化；银行卡发卡量保持稳步增长；贷记转账等其他结算业务量有所下降；电子支付尤其是移动支付业务延续快速增长势头，境内电子支付成为支付领域的主要增长点。

根据 2019 年 11 月 28 日中国人民银行副行长范一飞在第八届中国支付清算论坛的讲话，可以发现境内支付清算市场目前仍然存在不少问题：首先，商户资质审核不严，准入管理流于形式，随之而来的就是伪造、编造交易，使得交易信息的真实性、完整性都受到影响。其次，核心业务外包，但管理能力较差，导致外包业务出现大量纰漏。第三，受理终端管理不严密，挪用支付机构买卖终端，一机多码、一机多户的现象频繁出现。第四，为非法活动提供支付服务，一些商户利用虚假商户和和终端为网络赌博、黑灰产业提供支付渠道。另外，不同于小额批量支付系统若干笔交易打包统一处理，批量发送，定时清算，央行在大额支付过程中的实时逐笔清算模式，只在工作日 8:30 到 17:00 运行，周末、节假日关闭，导致了到账时间的延后。

所以，部分支付机构为特约商户提供大额资金当日结算服务，也就是说支付机构的利用自有资金或银行间授信资金提前将资金结算给予用户，而不是经过跨行清算，收单清算，异地转账涉及分行和总行的清算等一系列清算过程。而这种行为本质上涉及到信贷服务，容易滋生很多风险隐患，比如说银行套取的短期授信资金投资于高风险资产，产生严重的期限错配；甚至还利用信托、券商层层嵌套，抬高金融杠杆率，导致风险扩张。

区块链技术通过共识机制、哈希函数和数字签名等技术保障历史记录不会被篡改新型账本模式，具备交易即结算，可编程性、去信任化等特点。

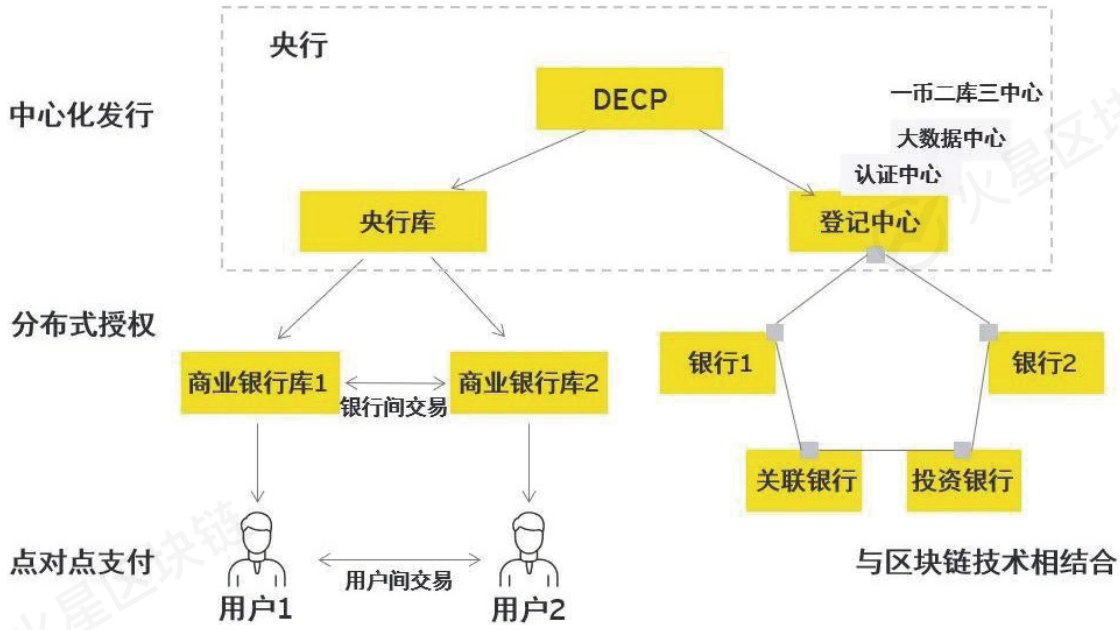
基于区块链底层的 DCEP 系统，从目前人民银行领导和相关负责同志的讲话和论文中，可以推断具备以下特点：数字通证替代了账户模型，以数字货币的表现形式完成确权，同时具备可编程性；遵循以传统的中央银行 - 商业银行二元模式运行框架，对 C 端用户采用 DID[①] 身份体系；采用密码学技术

① DID：即 Decentralized IDs，分布式数字身份标识符，由字符串组成的标识符，用来代表一个数字身份，它是一种去中心化可验证的标识符，实体可自主完成 DID 的注册、解析、更新或者撤销操作，不需要中央注册机构就可以实现全球唯一性。

和中心化登记中心、认证中心和数据分析中心完成对数字货币的监控。根据这几个特质，可以发现 DCEP 在支付系统中与目前最为火热的第三方电子支付可以相互替代。

终端和商户审核的问题是核心。由于数字货币的确权属性和衍生的 DID 身份体系，线上冒充商户进行伪造、编造交易将会基本杜绝，而登记中心和数据分析中心的存在将会对网络赌博、黑灰产业进行封锁。

但是由于支付过程中涉及到很多线下的场景，区块链系统主要是在线上系统内对此类风险予以排查和封锁，从线下绕过这类安全体系仍然存在一定可能性，所以 C 端支付方面区块链能做的依然有限。不同于 C 端支付，银行间支付和清算已经完成电子化，在这方面区块链能更好提供效用。



图：DCEP 采用的混合架构 ①

在传统支付清算过程中，转账和汇款涉及银行账户操作，较为麻烦的是跨行转账，除了调整交易双方在各自开户银行的存款账户余额以外，还涉及两家开户银行之间的结算，也就是需划拨中央银行的存款准备金账户余额。这相当于是在三个不同的账户体系内进行流转。更麻烦的是涉及到第三方支付机构的收单清算，这其中可能出现屡禁不止的二清风险，结算过程也就更为复杂。在大额资金划转中由于银行和支付机构为吸引顾客可能会使用前文所述的大额资金当日结算服务更加剧了清算过程中的风险。在 DCEP 系统中，这部分风险或许可以利用数字货币的可编程性实现。

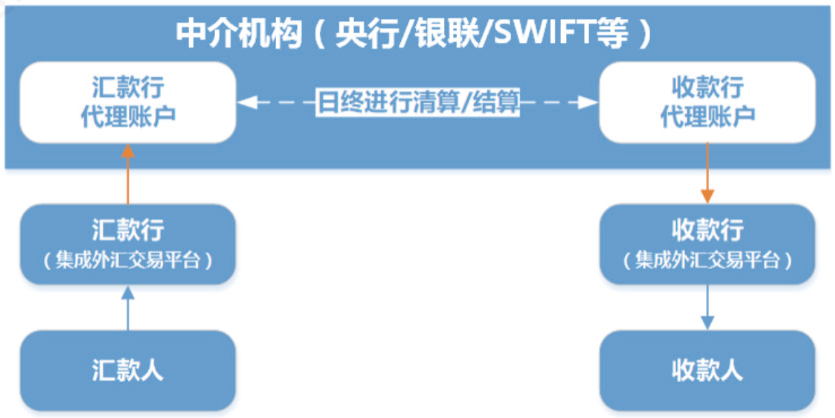
① 参考资料：安永 wavespace《中国央行数字货币 DCEP 如何重构未来商业形态》

可编程性的具体体现是智能合约，智能合约是一种无需中介、自我验证、自动执行合约条款的计算机交易协议。其运行方法简单来说如下：在多方共同协定、各自签署后随用户发起的交易提交，经 P2P 网络传播、矿工验证后存储在区块链特定区块中，用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约。矿工或联盟链参与者受系统预设的激励机制激励，将贡献自身算力来验证交易，在收到合约创建或调用交易后在本地沙箱执行环境中创建合约或执行合约代码，合约代码根据可信外部数据源和状态的检查信息自动判断当前所处场景是否满足合约触发条件。在交易验证有效后交易结果被打包进新的数据区块，新区块经共识算法认证后链接到主链，从而使所有更新生效。可以发现智能合约体系可以利用自动执行的代码封装节点复杂的金融行为以提高自动化交易水平。在理想化的央行区块链系统中，在验证资金后，用户 A 可以通过预设智能合约直接向用户 B 转账，其中的各项清算只需要在通过银行内、银行间的智能合约完成，交易延迟可以控制在几个区块的产生时间内，其中的资金流向也在链上清晰可见，无需担心资产证券化的风险。

当然，这其中仍然存在着结算完成前违约风险、流动性风险、智能合约漏洞风险等问题，但不失为目前清算系统问题的破局之道。

（2）区块链在跨境支付结算领域的应用

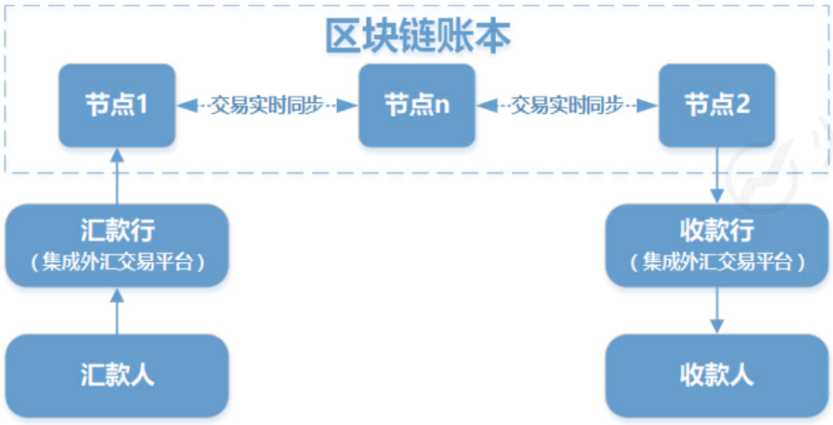
目前主流的跨境支付结算的方式包括银行电汇、汇款公司、国际信用卡组织和第三方支付，其中电汇是最主流的方式。传统跨境支付结算模式，主要依靠的是支付机构之间通过协议以及账户、备付金建立起来的信任链条，整个流程是链式结构，从汇款人到收款人中间可能经过 N 个中间机构，依托这些机构建立的一对一对的信任关系将资金流传递下去。



图：传统跨境支付简化模型 ①

① 参考资料：腾讯云《区块链商用调查》

传统支付结算的信任机制，是以线下备付金账户和合作协议为基础搭建起来的，但这种模式受地域、时间、监管等因素影响巨大，导致信任链条建立的成本居高不下，总体来看存在四大问题[①]：一是周期长。由于涉及到多中间机构的划转，跨境汇款从资金汇出到收妥可能需要三到五个工作日甚至更长的时间；二是费用高。以目前全球最大的国际支付和结算组织 SWIFT 为例，从美国汇款到中国，汇款手续费为汇款金额的千分之一，另外还需要承担货币兑换成本；三是支付和结算流程复杂。传统的支付结算平台要接入的金融机构数量太多，造成后续资金清分过程就变得复杂冗长；四是控制权过于集中。目前的绝大部分的汇款都会通过 SWIFT 平台，但美国及其盟友占据了 SWIFT 董事会的大部分席位，在货币、组织和数据方面有绝对话语权。



图：传统跨境支付简化模型[②]

在跨境支付结算中引入区块链技术，其重要意义在于：建立高效点对点支付高效支付网络，解决传统跨境支付方式清算时间长的问题。排除第三方机构的中间环节，全天候支付、即时收款、轻松取现、满足跨境电子商务支付结算服务的便捷需求。低成本建立全球一体化的基础跨境支付信任平台，消除跨境支付欺诈造成的跨境资金风险。

依托现有区块链的共识机制和智能合约，搭建一个全球化、低成本的信任中心，支持跨境支付业务的可信开展。改变跨境支付格局推动全球经济融合，利用区块链可以极大的降低跨境支付的信任、时间、金钱成本，进而从更深层次，推动全球经济的低成本融合。

① 参考资料：硅谷洞察《区块链在跨境支付、清算结算领域的应用分析》
② 参考资料：腾讯云《区块链商用调查》

案例：支付宝 AlipayHK 跨境汇款

2018 年 6 月 25 日，全球首个基于区块链的电子钱包跨境汇款服务在香港上线。港版支付宝 AlipayHK 的用户可以通过区块链技术向菲律宾钱包 Gcash 汇款。在区块链技术的支持下，跨境汇款从此能做到像本地转账一样，实时到账，省钱、省事、安全、透明。区块链通过分布式共享账本与智能合约将其升级为并行，实现了交易信息的实时共享，节省了大量的传递时间和对账结算成本，使得实时到账、低成本、汇率优成为可能。此外，因为区块链具有账本不可篡改和智能合约等技术特点，使得跨境汇款的各参与方有了实时、可信的信息验证渠道，汇款有迹可循，更加安全。同时，因为在联盟链采用隐私保护模型，用户的信息能得到更全面的保障。区块链技术还能降低风险，使跨境汇款能实现更透明的监管和更高效的风控。香港和菲律宾的监管机构可以对个人跨境汇款链路进行实时、全程监测，极大地提高了时效性和有效性。

2.1.3 保险

保险与银行、证券并称为金融业的三大支柱。保险是普通民众保障人生财务的基本工具，是市场经济条件下风险管理的基本手段，其在金融及社会保障体系中发挥着重要支撑作用。

2020 年初，保险行业受新冠疫情影响明显下滑。按照险种分类来看，寿险由于保险代理人人均产能下降及代理人留存率低收新冠疫情影响较重。由于寿险行业主要为代理人驱动型市场，在疫情防控情况下，居民被要求居家隔离，减少出行，代理人减少了和客户的面对面交流，从而导致了人均产能下降，间接导致代理人留存率下降，在多米诺骨牌的效应下，对整个寿险行业有着不小的打击。产险方面，车险作为产险的大头，由于疫情影响，新车销量大幅下滑，根据汽车业协会数据，2020 年第一季度单月同比下滑显著，尤其是 2 月份下滑了 80%。而健康险方面，由于疫情冲击，大众的健康意识显著增强，在互联网保险的加持下，促进了疫情期间健康险保费大幅增长。

从以上简单的疫情影响分析可以看出，传统寿险由于靠代理人驱动，在中国互联网普及率快速增长的情况下，互联网保险的份额将会显著上升，通过互联网保险来提高保险渗透率；健康险方面，互联网保险对其渗透率的提升在疫情期间有显著的帮助。

综上，市场对互联网保险的需求慢慢在增加。虽然借助着互联网技术，保险的渗透率得以上升，险企本身的执行效率也显著增加，用户也有了更好的体验，但是传统的互联网技术依旧不能够改善，抑或是增加了新的行业痛点。

首先，在互联网保险的快速发展下，数据不透明的问题被严重暴露出来。许多民众对保险业大量的负面印象来自于保险理赔纠纷问，而在很多情况下，保险公司也是受害者，用户报案内容往往不属于或是超过合同

的约定内容。其根本问题在于保险双方的信息不透明及不对称，定责本身会花费大量的时间精力，且还会有是否信任第三方定责结果的问题。最终导致保险公司运营成本上升，而用户则因理赔不及时或者是理赔结果不公正削弱了用户体验。

其次，在传统保险行业中，保险公司将大量的资金用于资金管理而非保险产品本身，大量的分销渠道赚取了绝大部分利润，导致保险本身价格升高而理赔费用并没有特别大的改善。在互联网金融的发展下，保险经纪人也在慢慢失业，但是其中很多传统保险经纪公司实际上也在转型成为线上分销平台，由于经纪人的交易信息不能够公开透明，保险信息存在数据孤岛，中间商收取高额费用的问题依旧存在。

再次，互联网保险还面临所有互联网企业都存在的数据安全泄露的问题，虽然传统保险同样存在这类问题，但是随着信息数字化的加持下，数据泄露的问题则被进一步放大，用户信息得以批量出售给多数第三方，增加了违法效率并降低了成本。

以上谈到的三点问题其根本还是在于保险数据本身的问题，针对这些数据方面的问题，区块链技术能够作为有效的解决方案。

在区块链保险中，借助分布式存储技术，保险信息能够被上链共享，直保公司，再保公司，经纪公司甚至是第三方定责机构之间的数据能够公开透明并且公正的反应在网上，保险数据的公开公正能够大大减少理赔纠纷问题。

此外，区块链技术中的数字证书能够解决身份所有权问题，避免了身份伪造，也同样可以防止重复保险多重索赔等伤害保险公司利益的行为。

另一大区块链的特色技术——智能合约，还能够有效减少保险公司的运营成本，提高用户体验。当所有数据上链后，通过可靠的预言机技术，当某些线上数据达到特定的值后智能合约就能够自动触发理赔，可以有效减少传统的理赔摩擦。

例如，在航空延误险这块，用户在购买基于智能合约的保险后，一旦飞机延误就能够快速收到理赔，而不用再像原来一样，经理及其繁琐的理赔过程，提交各类保单身份证明等东西。保险经纪人数据的公开透明能够更进一步让客户获得对称信息，减少暴力空间保障用户利益。

另外，数据安全泄露的问题也能够通过区块链上的数据权限控制来有效保护用户的数据问题。目前在大数据及人工智能技术的加持下，很多互联网保险公司开发了很多基于大数据的保险产品，通过用户提供的个人数据及用户自定义的理赔条件提供经济的报价。在寿险中用户会提供各类历史健康信息，而在车险中用户会提供各种驾驶习惯及汽车硬件数据，这类数据都能够为用户带来更好的报价。相对传统保险，基于大数据的保险

产品的数据泄露会给普通用户带来更加恶劣的影响。市面上还慢慢出现很多基于M2M[①]的数据保险，例如基于自动驾驶数据开发的数据保险，此类数据的安全泄露问题将会是企业级别的问题。通过区块链中的密码学技术能够有效保障用户及企业在数据共享的情况下保留必要的隐私。

案例：华为区块链保险业防欺诈解决方案

2020年6月26日，华为发布区块链保险业防欺诈解决方案，基于区块链的去中心化、唯一性、可溯源、不可篡改等特征，构筑保险行业联合反欺诈解决方案，来预防保险欺诈、骗保、反复理赔等欺诈行为的发生。华为区块链保险防欺诈解决方案通过联盟链构建“会员、保险公司、公估机构、资金管理方、第三方支付平台、会员代表方”通过“分布式共识”让用户的每一个环节都与区块链应用紧密结合，保证信息上链，组织上链，从参与社群、做到透明、安全、可追溯，进而识别欺诈风险。

2.1.4 征信管理

金融体系是由资金流和数据流组成，而数据流即代表了征信情况，是金融体系中风控的核心。根据中国人民银行征信中心定义，征信是指依法收集、整理、保存、加工自然人、法人及其他组织的信用信息，并对外提供信用报告、信用评估、信用信息咨询等服务，帮助客户判断、控制信用风险，进行信用管理的活动。

近年来，随着我国社会信用体系的建设和征信体系的完善，征信领域得到了迅速发展，潜在市场空间达到千亿级别。征信重要度不可替代，大数据与征信深度融合。

截至2019年中，国内征信系统累计收录了9.9亿自然人、2591万户企业和其他组织的有关信息，已成为世界上收录人数最多、数据规模最大、覆盖范围最广的征信系统。征信系统被广泛应用于金融机构的贷前审批、风险定价和贷后风险管理等环节，在防范金融风险、促进金融业发展方面发挥了不可替代的重要作用。根据问卷调查统计，仅2018年，21家全国性银行机构应用征信系统，在贷前审查环节拒绝高风险客户申请9117亿元，在贷后预警高风险存量贷款13028亿元，清收不良贷款1594亿元。

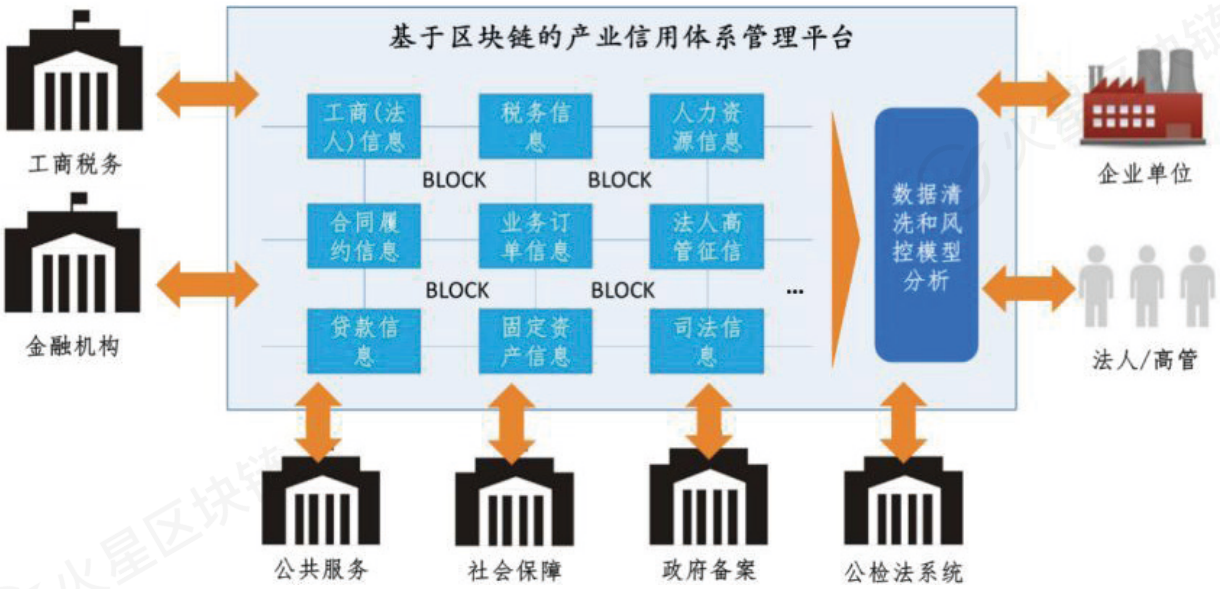
征信的本质其实是大数据。大数据与征信结合可以从全面、多元、高效三个特点来完善征信体系，包括覆盖更多的征信主体和征信数据、更多元的方式获得征信信息和形成征信结果，从而提高征信系统的全面性、可靠性、实时性和授信效率。但从目前的情况来看，已经获取到的征信数据依然存在许多问题。

首先是缺乏足够的数据。就目前的情形来看，政府仍然掌握着维度最全面、价值最高的有效信息，受隐私安全保护，这部分信

① M2M：即Machine to Machine，是指数据从一台终端传送到另一台终端，也就是机器与机器的对话。

息往往不会被共享。一些互联网大数据公司希望通过相关技术对用户个人行为进行更深度的挖掘，进而间接判断征信情况，但效果并不理想。此外，大量的有效数据无法在各个平台之间流通，于是出现了窃取征信数据的现象，有业内人士测算，中国“网络黑产”从业人员已经超过150万，形成了一条从信息需求、盗取、交易的成熟产业链，消费者的征信隐私得不到保障，同时，越来越多的消费者不愿意公开提交个人的有价值征信数据。

区块链被誉为“信用机器”，其核心价值在于将相互之间不信任的节点连接在一起实现信任机制的传递，并具有不可篡改、可追溯、隐私保护等特性。区块链网络作为底层架构，可以通过接口与应用层对接，从而实现数据的交互。



图：基于区块链的产业信用体系管理平台[①]

如果将区块链技术应用在征信领域，可能会对征信领域产生以下这么几方面的影响：

第一，在充分保护用户隐私的前提下，实现机构间的征信数据共享。当不同的机构以节点身份将用户信用数据上传时，区块链网络会对其明文数据进行加密，在没有获得用户授权的情况下，机构是无法对他方的数据进行查看或其他操作的，保证用户数据隐私不被侵犯。

第二，保证征信数据的不可篡改性以及可追溯性。链上各金融机构作为节点共同参与记账，且各节点的账本有且唯一，可有效

① 参考资料：佛山市禅城区《“区块链＋产业”白皮书》

防止对征信数据的篡改，而且链上数据可以追溯，提高了机构或个人的违约成本。

第三，提高征信机构的积极性，更好的丰富征信数据。当各金融机构将其所拥有的征信数据上传至区块链网络后，可在没有中心化后台的情况下，利用智能合约实现自动化、公平化的激励机制，对数据所有方进行激励，从而鼓励各机构积极共享和更新数据。

通过引入区块链技术，有效解决了机构共享数据意愿差、更新慢和人工采集信息耗时长、成本高等问题，降低了接入门槛，使得数据来源的维度得以丰富，且各行业平台还可以根据本行业的特定需求，定制化的开发大数据分析功能，灵活地满足机构对于风控的要求。

如何在保证合法合规的情况下，在机构间通过区块链底层网络的形式，共享征信数据是各企业需要与监管部门去共同探索。

从目前来看，数字证书（CA）是其中一种可行性比较大的解决方案。据公开资料，国家商用密码管理办公室已经许可了 40 余家 CA 机构提供具备法律效力的电子认证服务。这些 CA 机构用自己的证书为个人或公司颁发一份认证其身份的数字证书。证书内包含该个人或公司的真实身份信息以及证书持有者与颁发机构两者的电子签名。未来，如果在区块链上进行要求实名的交易时，双方互相提供 CA 机构颁发的数字证书即可，并且保证了身份信息只向对方披露。不参与交易的第三方不会获得这些数字证书，也就无法得知双方的身份信息。不想进行实名认证的用户也可以继续使用匿名的账户，但是无法参与到对方要求实名的交易中去。

案例：公信宝区块链数据交易所

公信宝于 2016 年将区块链技术结合到征信行业中，深度研发基于区块链技术的“公信宝数据交易所”。公信宝数据交易所是一个通用的数据交换平台，底层是基于区块链（公链）打造的一条联盟链，面向的典型客户为互联网金融企业、政府部门、银行、保险等。公信宝主要通过数据爬虫产品负责在用户授权下抓取用户数据，覆盖泛金融、泛电商、泛社交、个人身份等多种维度数据，为各大银行、互联网金融公司等机构提供征信基础数据服务，交易过程中公信宝会对交易双方进行匿名处理，并实现数字资产的所有权认证以及有效遏制数据交换中的造假问题。

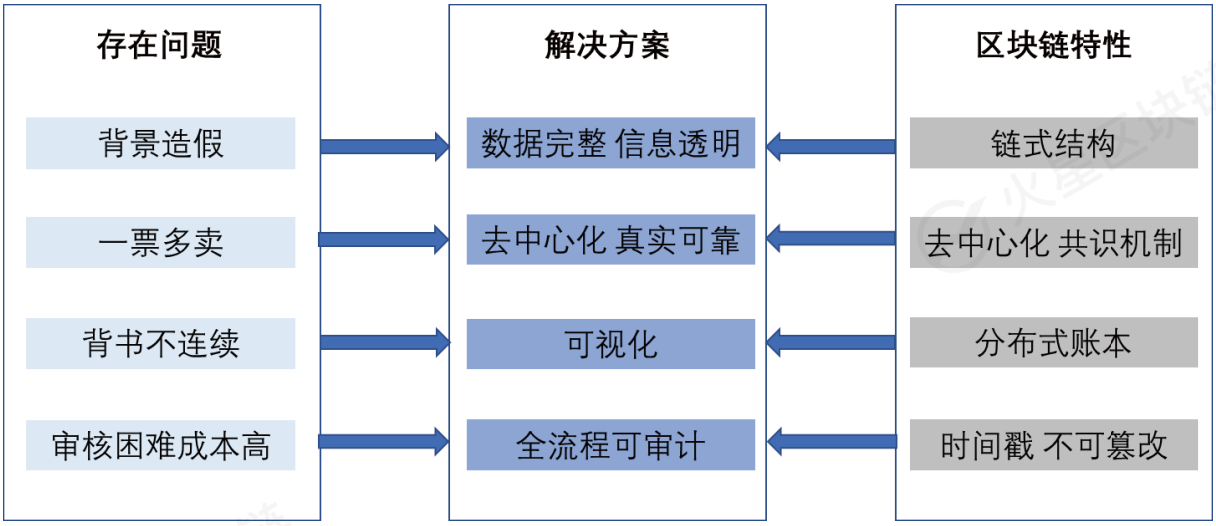
2.1.5 资产数字化

传统资产流通均依靠信用中介结构的中心化服务系统进行交易，这将导致更低效率的流通过程，更高的交易费用，降低了资产的流通性。通过区块链技术构建的资产数字化平台，将能够实现资产的登记、发行、交易、结算全部上链，保证了资产流通数据的完整性，并且区块链技术的不可篡改性和可追溯性将实现对数据安全性的保证，保证资产的可信度，有效减少了资产交易过程中的信息不对称问题。

目前，资产数字化项目最为集中的领域为：数字票据和资产证券化。

（1）数字票据

在传统票据市场交易中，交易背景造假、交易不透明、违规交易、一票多卖的现象时有发生，因此对票据的防伪防篡改有很高的要求，其只能通过中心化交易系统来保证交易的安全可靠。而区块链技术应用于票据系统所形成的数字票据，将构建出更安全、便携的票据交易平台，完美解决票据交易中的痛点，具有多种交易优势。区块链技术使得任何交易都能实现可追踪可查询，实现对票据流转过程的控制，有效把控其中的风险；智能合约的可编程性则具备了对票据的限制性和可控性；同时，数字票据系统的搭建省去了中心应用系统搭建的成本，减少了中心化带来的风险。



图：区块链技术与票据业务的融合

案例：央行区块链数字票据交易平台

2018 年 1 月 25 日，根据中国人民银行的安排部署，由上海票据交易所、数字货币研究所牵头，中钞信用卡产业发展有限公司杭州区块链技术研究院承接，同 4 家商业银行研发的“基于区块链技术的数字票据交易平台”实验性生产系统成功上线试运行，系统顺利完成了基于区块链技术的数字票据的签发、承兑、贴现、转贴现业务。该平台采用联盟技术，央行、数字票据交易所、商业银行以及其他参与机构以联盟链节点的形式经许可后接入数字票据网络。不同的节点在接入时可以根据角色不同和业务需求授予不同的链上操作权限，包括投票权限、记账权限和只读权限等。数字票据发行后以智能合约的形式登记在联盟链上，并在链上进行交易撮合，结算则通过数字票据交易所连接联盟链之外现有的基于账户的支付平台完成。在央行的数字票据系统中，实现了传统票据生命全周期的功能，包括出票、背书转让、

贴现、转贴现、托收等。

（2）资产证券化

在传统的资产证券化过程中，通过把缺乏流动性的资产打包，然后进行结构化设计，变成可在金融市场出售和流通的证券，项目收益主要依赖于企业优质资产产生的现金流。然而 ABS 业务参与方多、环节多、链条长，包括基础资产的转让出表、基础资产的打包发行、为 ABS 提供担保等，同时由于缺乏资产穿透的手段，对于投资者来说，底层资产的不透明使得难以进行有效的信用评估，资产现金流回款情况也难以进行监管，ABS 底层资产的存续管理十分复杂。传统 ABS 业务存在的诸多问题导致底层资产质量只能与公司信用挂钩，中小企业仍然存在融资难的问题。

而区块链技术中的分布式存储，可追溯和不可篡改性将能有效解决 ABS 业务中的环节多、流程复杂、底层资产透明度问题，有以下显著优势。首先通过全流程数据上链，将看到资产的全生命周期，提高了底层资产的透明度和真实性；其次，区块链的不可篡改性将保证业务流程中信息数据的安全和统一；最后区块链使得投资者对底层资产的回款情况、资金分配状况的掌握成为了可能。

案例：交通银行区块链资产证券化系统“链交融”

2018 年 12 月 20 日，交通银行依托区块链技术打造的国内首个资产证券化系统——“链交融”正式上线。“链交融”平台将原始权益人、信托、券商、投资人、评级、会计、律师、监管等参与方组成联盟链，有效连接资金端与资产端，利用区块链技术实现 ABS 业务体系的信用穿透，从而实现项目运转全过程信息上链，使整个业务过程更加规范化、透明化及标准化。在此基础之上，“链交融”正在打造一套智能应用，涵盖智能资产筛选、智能估值定价、智能监管、智能风险监控等功能。“链交融”建立了一套可配置的产品模板，已支持信用卡分期、住房抵押贷款、应收账款、不良贷款、对公贷款等主流资产证券化产品的快速发行。

2.2 区块链创造新金融物种的诞生

2.2.1 DeFi

DeFi，Decentralized Finance 的简称，即去中心化金融。借助区块链技术，来解决传统及中心化金融存在的天然短板，如金融体制不平等、审查流程繁琐、缺乏透明性和潜在的交易风险等。

DeFi 最初是为了以太坊生态内的各种代币搭建金融基础设施，MakerDAO[①] 成为引爆 DeFi 的第一大应用，之后，EOS、Cosmos、Polkadot、Nervos 等项目纷纷在 DeFi 应用领域开展布局，赋予了 DeFi 更大的想象空间。截至 2020 年 7 月 2 日，DeFi 行业的总锁仓价值为 18.1 亿美元，较 2019 年 1 月 1 日的 3.02 亿美元，一年半时间增长了近 270%b。随着以太坊 2.0、跨链等区块链技术不断突破，DeFi 市场容量和用户数或出现爆发性增长。

当前，DeFi 最值得关注的三个应用领域[③]：稳定币、加密数字资产借贷、去中心化交易所。

2.2.1.1 稳定币

稳定币是指与法币的兑换比例保持相对稳定的类似“货币”的一般等价物。稳定币最早起源于 2014 年 Bitfinex 组建的泰德公司（Tether Limited）发行的 USDT，通常被认为是一种具有稳定价值的加密货币，其价值锚定法定货币或其他资产，旨在避免其它完全由市场驱动价格的加密货币所固有的波动性。

（1）稳定币的分类

在 Tether 的迅速发展下，越来越多形式的稳定币也纷纷涌现出来。目前，稳定币主要分为以下类别：

分类 1：根据抵押形式划分

——链下资产抵押型稳定币。由“常规”法定货币（例如美元或欧元），贵金属或其他现实世界资产支持的稳定币。它需要信任不透明且集中的第三方来持有抵押品。目前法币背书的稳定币主要有 USDT、USDC、PAX、GUSD 等。贵金属背书的稳定币主要有 DGX、OGC 等。

——链上资产抵押型稳定币。由区块链和智能合约支持，抵押数字资产并发行稳定币，大部分该类稳定币目前都基于以太坊构建。主要包括 DAI、Celo 等等。

——算法型稳定币。依靠算法和智能合约的组合模拟来维持价格平衡。主要包括 Terra、Ampleforth 等等

分类 2：根据发行主体划分

——传统巨头公司。2019 年各大企业巨头在稳定币方面动作频发，其中以 Facebook 发布天秤币（Libra）白皮书最为轰动。除此之外，摩根大通推出摩根币（JPM Coin）；零售业巨头沃尔玛向美国专利商标局提交了一份稳定币专利申请等。

——加密货币交易所。2019 年，加密货

① MakerDAO：成立于 2014 年，是以太坊上自动化抵押贷款平台，同时也是稳定币 Dai 的提供者。MakerDAO 通过智能合约来质押用户的数字资产，再借给用户同等金额的稳定币 Dai 供他们自由使用。

② 数据来源：DAppTotal.com

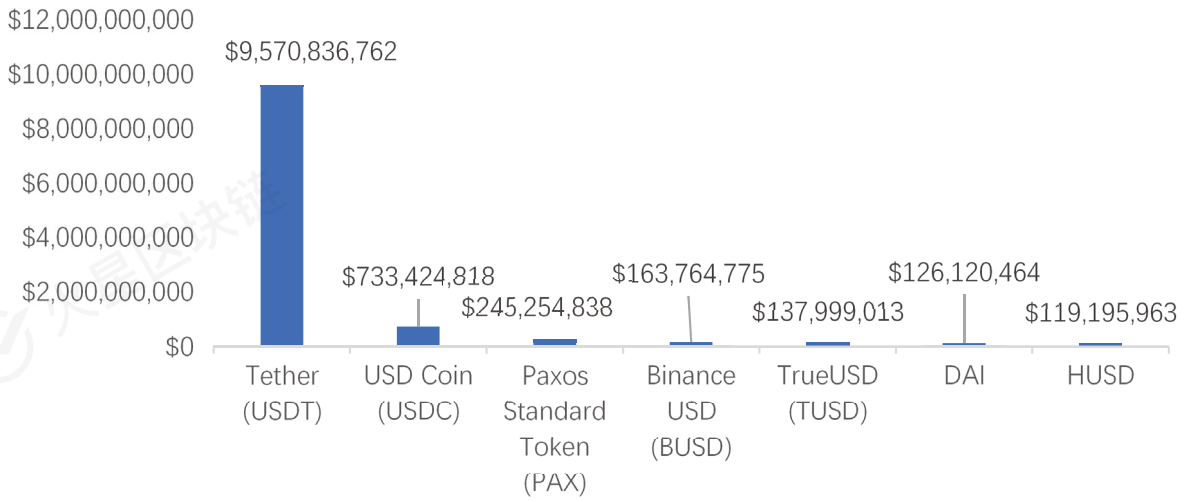
③ 说明：本报告主要聚焦去中心化的稳定币、借贷及交易所的应用场景，但内容同时也涵盖了中心化相关应用的数据统计和分析。

币交易所 OKEx、币安、火币已经陆续入局稳定币市场。6 月 3 日，OKEx 宣布全球首发上线稳定币 USDK。9 月 15 日，币安宣布与 Paxos Trust 联合推出与美元挂钩的稳定币 BUSD，并获得纽约州金融服务局（NYDFS）的批准。火币的稳定币 HUSD Token 是由火币资本投资的 Stable Universal 与 Paxos Trust 合作发行的合规美元稳定币。

——合规金融机构或政府。PAX 是由纽约州信托机构 Paxos Trust Company 于 2018 年发行的美元稳定币，受纽约金融服务部（NYDFS）的监管。TUSD 由 Trust Token 于 2018 年发行，受美国法律监管，是全球首个由政府担保发行的稳定币。USDC 是由 Centre 联盟于 2018 年发行的美元稳定币，Centre 联盟由满足监管、合规、储备、审计等要求的金融机构组成，目前联盟成员包括 Circle 和 Coinbase。

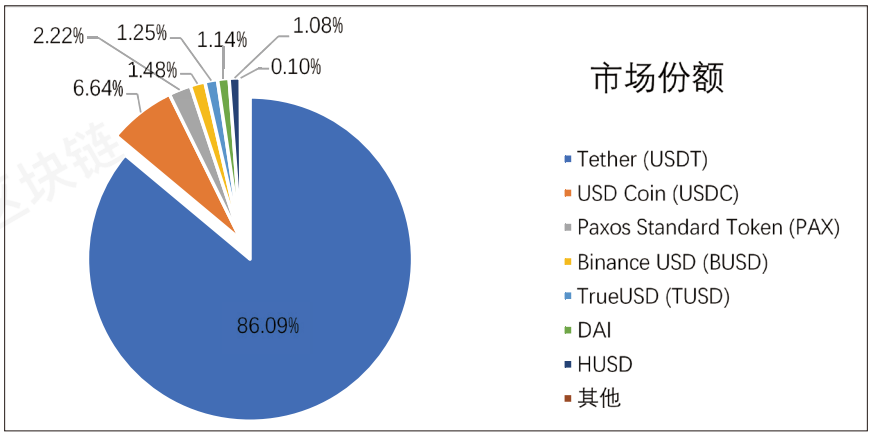
（2）稳定币的市场现状

随着市场的发展，稳定币在加密货币中扮演越来越重要的角色。截至 2020 年 6 月 16 日，所有稳定币市值加总高达 112.5 亿美元，占加密货币整体市值的 5% 左右。USDT 始终在稳定币市场拥有最大话语权，目前占领着 86.1% 的稳定币市场份额，且长期处于增长态势。USDC 处于第二，占领了 6.6% 的市场份额。



图：主流稳定币市值[①]

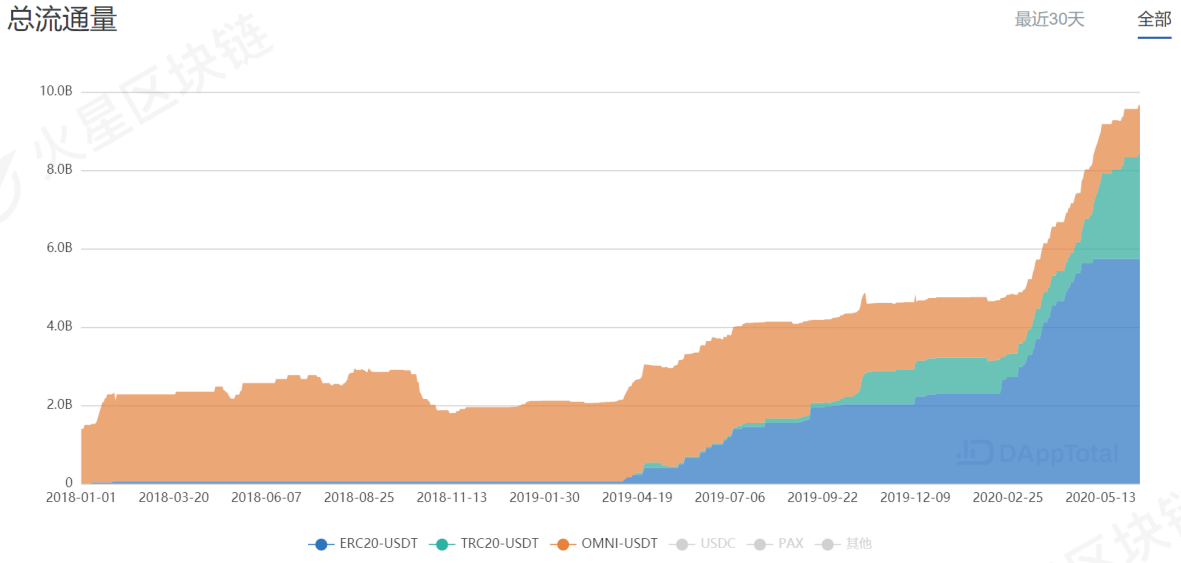
① 数据来源：stablecoinindex.com



图：各主流稳定币的市场份额

——中心化稳定币项目代表：USDT

USDT 最早于 2014 年由 Tether 公司发行，与 Bitfinex 交易所的母公司均为注册地为香港的 iFinex 公司。USDT 的发行逻辑很简单：每个 USDT 都由 Tether 储备的美元支持，以 1:1 锚定美元，并且可以通过 Tether 平台赎回。USDT 最早发行与 Onmi 区块链上，现在也流通于 Ethereum、TRON 等网络中。以 TRON 为例，2019 年 4 月，Tether 公司宣布在波场上发行了基于 TRC-20 协议的 USDT，并承诺在波场上转账 USDT 不收手续费，目前基于波场的 USDT 市值已经超过波场本身市值。



图：USDT 总流通量变化[①]

① 图表来源：https://dapptotal.com/stablecoins

——去中心化稳定币项目代表：DAI

DAI 是去中心化的加密资产抵押型稳定币，其发行组织 MakerDAO 是以太坊最早的去中心化自治组织之一，创建于 2014 年，经过 3 年开发于 2017 年 12 月上线。在 Maker 体系中有两种主要代币，第一种是稳定币 DAI，第二种是管理型代币 MKR。简单来说，用户只需要向 Maker 协议中提供 ETH、BAT 或者 USDC 作为抵押物就可以参与发行美元稳定币 DAI。但是需要用 MKR 支付一定的稳定费，这部分稳定费的定价由 MakerDAO 治理投票来决定。2019 年 11 月 18 日，MakerDAO 团队宣布正式启动多抵押 DAI。原来的单抵押品产生的 DAI 将更名为 SAI。2020 年以来，MakerDAO 内的资产锁仓量也在逐步提升。但是，DAI 应用场景的缺失以及去中心化金融本身的门槛，依然制约着 DAI 市值的进一步扩大。

图：DAI 总锁仓量统计 ①

——新兴稳定币项目代表：Libra

2019 年 6 月，Facebook 宣布发行一个名为 Libra 的稳定币，引起加密货币圈不小的震动。Libra 由 Libra Association（Libra 协会）组织管理发行，该组织由 Facebook 发起，由数十家机构参与运行。Libra 的白皮书写到：“Libra 的使命是建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。”而一个在全球拥有近 30 亿用户的公司确实也有实力实现这个愿景，不过这也大大挑战了现有的政府和金融体系。2019 年 9 月后，PayPal、Visa、Mastercard、Stripe、eBay、Mercado Pago 和 Booking 七家公司先后宣布退出即将正式成立的 Libra 协会。

尽管监管压力重重，Libra 还是在努力推进。2020 年 2 月，电商巨头 shopify、投资公

① 数据来源：DeBank

司淡马锡等相继宣布加入 Libra 协会。2020 年 4 月 16 日，Libra 白皮书 2.0 版发布，主要宣布新增锚定单一币种的稳定币，并进一步推进合规。2020 年 5 月 6 日，Libra 协会任命汇丰银行首席法律官斯图尔特·利维（Stuart Levey）为首任首席执行官。Libra 计划于 2020 年底正式推出。

（3）稳定币的发展趋势

——价格稳定机制是内核。不管采用中心化或者去中心化的机制，价格稳定始终是稳定币最核心的功能。中心化稳定币中，存款银行的风控能力、发行主体的信用风险等都会对稳定币的稳定程度造成影响；去中心化稳定币中，协议的安全性、抵押资产的波动率等等都会对稳定币的稳定程度造成影响。

——应用场景进一步扩大。稳定币主要有交易工具、避险资产、支付手段等功能，主要应用于中心化交易所、理财产品、跨境结算等场景。随着未来区块链和数字货币的发展，其应用场景也会随之扩大。比如去中心化借贷、做市商等都给稳定币增加了新的应用场景。

——进一步追求合规。USDT 因先发优势在没有那么合规和透明的情况下占据了主要市场，但这并不是各类法币稳定币可复制的模式。目前，还是有许多稳定币在进一步寻求合规。比如 Libra，在已经拥有大量用户群体的基础下，走通合规后，确实有机会成为一个新型的稳定币巨头。

2.2.1.2 加密数字资产借贷

加密数字资产借贷是增长最为迅速的加密数字货币金融市场。金融服务公司一直在寻求发行信贷和债务，数字资产借贷行业被证明是在加密生态系统中为用户提供有形价值的首批突破性的应用场景之一。

按照资产是否托管在中心化组织为划分标准，其主要分为中心化金融借贷和去中心化金融借贷两种模式[①]。中心化金融贷款服务就像典型的金融服务公司一样。他们使用内部风险管理程序来匹配借款人和贷方、评估信誉度、确定利率并保管资产；去中心化金融借贷项目则使用开源协议和智能合约，来自动化贷款发起流程旨在完全消除收费中介。

根据 2019 年 Bloomberg 报告，从 2018 年至 2019 年，加密数字资产借贷市场规模已经增长至 50 亿美元，而且增长势势头依然强劲；Coinbase 报告指出，目前加密数字资产借贷市场规模达到 130 亿美元。以主要面向机构的纽约加密数字资产借贷商 Genesis Capital 为例，其业务量呈现陡峭的增长曲线。据该公司披露，截止到 2020 年第一季度，其在贷余额约为 6.5 亿美元。

① 目前，主流的中心化金融借贷机构包括：Genesis Capital、Celsius Network、Lendingblock、Unchained Capital 和 BlockFi、贝宝金融等；主流的去中心化金融借贷协议包括 MakerDAO、Compound、Aave 和 Balancer 等。

图：Genesis Capital 加密数字资产借贷业务增长情况[①]

（1）加密数字资产借贷市场现状

加密数字资产借贷市场早期阶段，主要需求来自矿工。但是随着加密金融期权和期权市场的迅速发展，对加密数字货币流动性的需求越来越大，套利借贷的增长速度上升很快。目前驱动加密数字资产借贷市场高速增长的主要因素有：

——资金周转需求。早期加密数字货币的借贷需求主要来自矿工、矿场和持币用户。对矿工和矿场而言，需要不断支出电费和矿场运营成本，而他们的收益是比特币或者其他加密数字货币。在没有借贷之前，矿工们的通常做法是在市场上卖掉加密数字货币，换回现金，满足支出和开销需求；当加密数字资产借贷服务出现之后，矿工们在卖币之外多了一项选择，可以选择通过抵押比特币来获得现金。

——做空做多套利需求。做空和做多是投资者增加回报或对冲风险（尤其是高度波动期）的重要机制。由于加密数字资产市场的特征之一是高波动性，意味着大量的套利机会。比如，当比特币现货和期货价格之间出现大的差异，就代表着投资者可以通过在现货和期货之间，通过借入或借出比特币进行交易来进行套利，有时年化可达 40-50%。

在 2019 年之前，来自矿池、矿场的运营需求是加密数字资产借贷的主要增长动力，但随着 2019 的下半年比特币衍生品市场的快速发展，套利需求带来的加密数字资产借贷业务正在占据越来越大的规模。

2020 年，以 Compound、Balancer 等为代表的、基于以太坊的去中心化加密货币借贷平台的通证价格和借贷量出现大幅上涨，引发市场对“借贷即挖矿”“流动性挖矿”等加密数字资产借贷新模式的高度关注。

Compound 是一个基于以太坊的 DeFi 协议，主要实现的业务类似于银行的“抵押借贷”，用户可以将自己的资产抵押在协议中获

① 参考资料：Genesis Capital 2020 年第一季度报告

得年化收益，而资产借出方则需要支出相应利息。2020 年 6 月 16 日，Compound 向用户分发其治理通证 COMP。COMP 通证激励模型的实质是用股票补贴借贷双方，让 lenders 拿到更高的收益，让 borrower 拿到更低的利率[①]。截至 7 月 2 日，COMP 总市值约 35 亿美元，Compound 平台锁定的通证总价值飙升至约 6 亿美元，在半个多月时间内涨幅超 500%，跃居 DeFi 类借贷平台首位[②]。

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Compound	Ethereum	Lending	$595.6M	-0.95%
2.	Maker	Ethereum	Lending	$481.8M	6.89%
3.	Synthetix	Ethereum	Derivatives	$308.8M	7.43%
4.	Balancer	Ethereum	DEXes	$134.6M	7.21%
5.	Aave	Ethereum	Lending	$125.8M	9.56%
6.	WBTC	Ethereum	Assets	$80.9M	1.22%
7.	InstaDApp	Ethereum	Lending	$51.6M	0.86%
8.	dYdX	Ethereum	Lending	$36.2M	2.46%
9.	Bancor	Ethereum	DEXes	$18.5M	7.05%
10.	Uniswap V1	Ethereum	DEXes	$18.2M	-0.53%

图：DeFi 借贷类项目排行榜[③]

Balancer 是一个非托管的通用自动做市商（automatic market maker）协议，任何人都可以创建一个 Balancer 池，并为协议增加流动性。从本质上讲，Balancer 池就像自我平衡的指数基金，但不会向用户收取费用，而实际上向贡献流动性的用户支付报酬。2020 年 6 月 1 日，Balancer 正式开始向用户分发其治理通证 BAL。

（2）影响加密数字资产借贷市场发展的因素

——比特币价格。从数据统计看，加密数字资产借贷业务量增长和比特币的短期价

① 参考资料：数字资产研究院副院长孟岩《对 COMP 通证经济模型的一般性评价》
② 数据来源：defipulse.com、AICoin
③ 来源：Defipulse，统计截至 2020 年 7 月 2 日

格走势（特别是波动率）呈正相关关系。原因是，在比特币币价大幅下跌的时期，矿工们由于运营的需要，对借贷的需求上升。当币价脱离低价区间时，专业机构和高净值个人（单客户业务往来大于 100 万 USDT 等值）的套利和投机需求上升，即不同价格周期，借贷市场的客户群体会发生变化。

图：比特币价格波动与加密数字资产借贷市场关系 ①

——基础设施的完善程度。许多加密数字货币投资者期待传统金融机构的进入这一市场，但是，基础设施的完善程度不足，依然是目前的最大障碍，这包括监管政策的不确定、基本设施不足等。具体而言，传统金融机构若要投资比特币，内部必须经过严格合规，而目前各个国家和市场的监管对比特币存在一定模糊性，市场上也缺乏足够可信的托管机构，使得一般机构很难从技术上实现对比特币直接投资。这也是 Gray scale 等资产管理公司的信托基金始终存在一定溢价的重要原因。

（3）加密数字资产借贷市场的发展趋势

——市场规模继续扩大。根据数据分析公司 Cryptocompare 报告，2020 年 5 月，加密数字货币衍生品交易量增长 32%，规模达到 6020 亿美元。此外，随着加密数字货币矿业进一步机构化和专业化，提高了参与者对金融产品的接受度，运用借贷等加密数字货币的相关金融产品，进行风险和现金流管

① 参考资料：《2019 贝宝金融年度报告》

理的需求将会逐渐上升。

#	名称	可存币种	可贷币种	锁仓额	总资产*	资产增幅
1	Compound	9种	9种	¥54.85亿	¥129.39亿	-1.37%
2	Maker	1种	1种	¥72.12亿	¥73.74亿	-1.55%
3	Aave	17种	17种	¥25.56亿	¥36.81亿	+7.69%
4	dYdX	3种	3种	¥2.6亿	¥4.14亿	-1.19%
5	bZx	11种	11种	¥114.07万	¥2430.1万	-5.34%
6	Nuo	12种	12种	¥1291.07万	¥1260.71万	-0.96%
7	DDEX	6种	5种	¥1984.2万	¥1246.83万	+0.97%

图：DeFi 类借贷项目排行榜（截至 2020 年 7 月 30 日）[①]

——机构竞争和合作增强。由于借贷业务良好的现金流回报，很多拥有一定流量的平台，包括交易所、钱包、矿池都在觊觎这一市场，必然会带来这个市场竞争的加剧。但借贷业务需要独特的金融专业能力，而一般平台往往不具备足够的金融产品和风险控制能力，也带来加密借贷平台与其他机构的合作机会。

——更加重视安全和风险管理。加密数字资产借贷平台与交易所、钱包、托管等其他加密数字货币金融服务机构的最大不同，在于其需要一套完整的金融风险管理能力。这也是 2020 年“312”黑天鹅事件的最大教训之一。不具备金融风险管理能力的借贷平台，就会遭遇巨额损失，甚至被淘汰出局。

2.2.1.3 DEx

分布式交易平台（英文 Decentralized Exchange，简称 DEx），又名去中心化交易所、分散式交易平台，是基于区块链创造的不依赖第三方信任的数字信息交换方式，提供了一种全新的信用机制和价值交换模式。

从全球范围来看，关于分布式交易平台的探索分为两大阵营：

一是以自治社区（DAO）[②] 为主的 DEx。

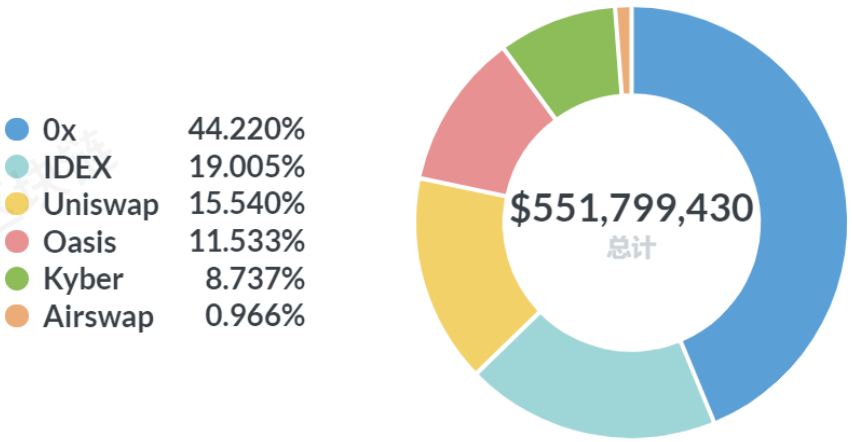
① 图表来源：QKL123

② DAO：全称是 Decentralized Autonomous Organization，即分布式自治组织，一种将组织的管理和运营规则以智能合约的形式编码在区块链上，从而在没有集中控制或第三方干预的情况下自主运行的组织形式。

	中心化交易所	分布式交易所
安全	单点故障会影响所有人交易，对黑客吸引力高	单点故障无影响，对黑客吸引力低
控制	中介机构完全控制资金	用户完全控制资金
速度	中心化服务器可实现高吞吐量 （数万至数十万 TPS）	区块链节点的分布意味着低吞吐量 （数十到数千 TPS）
费用	0.02% ~ 5% 不等	非常低，甚至不收费
个人资料	必需	可以不需要
流动性	流动性好，利于高效的价格发现	流动性有限，不利于价格快速发现
功能性	易于使用，适合所有交易者	复杂的界面，适合经验丰富的交易者
可扩展性	低	高

图：中心化交易所和分布式交易所对比

DEx 大多运行在无需准入许可的公有链上，目前日均交易量超过 100 万美元的 DEx 有十家左右；排名前 7 的 DEX 在 2020 年前 5 个月的交易量达到了 25 亿美元，已经超过了 2019 年全年的交易量总和，其中，2020 年 5 月同比 2019 年 5 月增长 144%。



图：主流 DEX DApp 交易量统计（2020 年 7 月）[①]

二是以各大传统证券交易所为主的、基于区块链的交易基础设施的探索。主要包括：纳斯达克的 LINQ、德意志证券交易所、澳大利亚证券交易所、新加坡交易所、泰国证券交易所、俄罗斯莫斯科交易所等，不过目前尚未有项目进入大范围应用推广阶段，并

① 数据来源：DappRadar

且这些探索主要利用区块链在证券交易后流程优化，在交易层面仍然更多是中心化的。前者基于无需准入许可但公有链建立，后者大多基于需要准入许可的联盟链或私有链；前者的产品设计大多面向所有人，而后者暂时更多针对机构间（批发）使用场景。

相关研究和案例证明，区块链技术可以使得电子金融交易流程变得更加公开、透明，通过区块链结构，使得原本高度依赖中介和集中式处理的传统交易、结算模式变为点对点的自组织网络交易模式，这不仅使参与者的范围更广、服务更便捷、效率更高、成本更低，也可以赋予监管、风控和合规更加智能化和自动化的空间。

表：区块链在交易平台相关业务链的应用[①]

	业务环节	主要局限	区块链应用
交易前	公司研究分析 风险管理	信息可获取性、传递效率、及有效性	可追溯、穿透至底层资产，自动验证归属，信息有效性、不可篡改、可追溯，条件触发自动处置
交易中	订单执行及撮合	运营时间限制、处理结算	全天候、实时处理跨机构、跨行业、跨境
交易后	清算交收	对手方风险、机会成本、融资成本	消除一对一风险降成本，高效、实时、无缝处理资产转移和变动
	托管 资产管理	操作成本高需 要人工处理及确认	交易流不可篡改，无需第三方保管账目自动执行合规，减少操作成本

（1）分布式交易平台的工作方式

传统的证券交易分为可交易前流程，如询价、报价、订单匹配等，以及交易后流程，支付与交付（DvP）、平仓与结算等。受到基础公链的架构和性能制约，目前不少分布式交易平台将“交易前流程”放在链下完成，仅在链上实现 DvP 和结算，而交易前订单簿和交易撮合结算完全在链上的 DEx 较少。

相对于以上两种订单簿模式，还有一种没有订单簿的储备库模式，由一个储备管理机构提供 token 储备，通过智能合约来进行快速结算，如 Kyber 和 Uniswap。此外还有一种模仿荷兰式拍卖的协议，通过这种古老的博弈模式，促成最终成交价向市场公允价格靠拢，典型的用例是 DutchX 协议。

以订单簿和交易撮合结算完全在链上的 DEx 为例，不需要用户将其资产转移到交易所账户或任何智能合约，用户不需要进行 KYC，所以 DEx 理论上可以降低黑客盗窃交易所用户资产的风险。此外由于 DEx 挂单撤单手续费以及所有记录透明等特点，可以防止刷量交易量或价格操纵。

需要注意的是，在高并发的交易环境中，并不是每个信息输入都是有用的、合法

① 资料来源：上海证券交易所、币安中国区块链研究院

的，每一次信息写入都需要验证，尤其在区块链里每一次验证是有“代价”的，所以针对交易专门研发、建立一条区块链可能是有必要的。

以币安链 Binance Chain（BC）上的分布式交易平台为例，在 2019 年初发布的版本中，为了交易的高效流畅，BC 没有做支持智能合约二次开发的图灵完备公链，而是仅使要该链有发行 Token、链上撮合和交易的功能，这样的设计保证了 2000+ 的 TPS，满足了交易上链中高速、高频、低手续费的需求。随后在 2020 年发布的币安智能链（BSC）中加入智能合约层，成为 Binance Chain 的并行链。两条链通过智能链中继器和语言及中继器相联，无需第三方信任。这样的双链架构为开放金融的创新应用提供了更加高性能的基础架构。

图：币安链和币安智能链架构

（2）分布式交易平台的金融创新

——缩短结算时间，增加传统证券业的流动性。

传统证券交易清算涉及多个主体，包括银行、证券公司、交易所、中央结算对手方等，各个机构有着不同的 IT 系统、账本、工作流程，相互对账时间完成最终证券结算约在 1 ~ 3 天左右。区块链架构下点对点的交易平台可以大幅加速结算时间，使证券结算间隔从缩短至几小时甚至几秒钟，从而增加证券的流动性。

不过，这种优势的前提是需要假设区块链能够处理证券和款项的所有权转移。客观来说，目前标准化证券交易依旧强调权威登记、审查，区块链架构无法绕过证券监管流程，在解决场内交易痛点方面优势并不明显。此外，券商负责客户审查和服务、交易所负责交易撮合、证券登记结算公司负责过户、银行负责资金清算，“四权分立”的模式如何与区块链的分布式架构做到统一协调，仍有待探讨。

——提高交易效率，促进非标准交易市场的发展。

考虑到场外（OTC）存在的大规模交易的需求，基于区块链的分布式交易平台大有广阔天地。因为 OTC 产品往往是非标准化合约或非集中交易产品，例如场外期权、保险、非上市公司股权、私募基金份额、非标债权 /

商品等等。这些产品的交易、结算场景与区块链的技术特征天然匹配，区块链架构有利于改善 OTC 市场的组织运行模式，显著降低交易对手方风险和确权审查成本，提高市场效率与透明度的同时，也有利于加强监管和系统性风险的防范。

例如，上海证券交易所 2019 年已进行了名为“百川”的概念验证项目，将区块链技术应用于场外交易及结算，实验显示智能合约可以提供自动或半自动执行复杂衍生品的功能，降低合约执行成本，简化交易后业务环节降低合约执行，同时便于监管穿透、追踪交易。上交所认为应充分重视区块链技术价值，明确将其作为上交所金融科技重要发展方向。

综上，DeFi 无需准入和代码驱动的优势，在稳定币、借贷、数字资产交易等领域已取得突破进展。目前，除了以太坊之外，基于比特币的 DeFi 基础设施正在建设当中，如原子互换（Atomic Swaps）、跨链桥、侧链、闪电网络、DLC's(离散对数合约) 、代币化 BTC 等，未来，将会有越来越多的数字资产应用于新的 DeFi 金融应用中。正如百度旗下度小满分布式技术金融白皮书中所提到：数字化经济有多庞大，资产化规模有多快，DeFi 的应用空间和潜力就有多大。

2.2.2 Staking 经济

Staking 是 POS 共识机制下的一个验证过程。由于 PoS 机制中的所有节点通过质押 token 的方式参与共识，其网络中的验证者同时也是 token 持有者。由于 token 的价值直接被抵押，激励机制的作用开始出现。一般来说，质押者必须将他们的 token 锁定为抵押品。作为交换，他们有获得验证区块和挖矿奖励的权利。这个过程通常被称为“ Staking ”或“验证”。简而言之，Staking 是指通过自己的权益证明（Token），如投票或者是单纯锁仓，来获取收益或分红的行为。

生活中类似 Staking 的行为其实也很常见，比如我们通过持有股票获得定期分红，就是很典型的 Staking。现实世界中，通过自己的权益（投票权）换取收益其实也很常见，比如美国各地选议员，尽管议员候选人不能直接承诺给投票者金钱回报，这在绝大地方都构成贿选，但当选者在当选之后通过施政给大家带来更好的生活，本质上也是另一种形式的回报。

Staking 经济是一种商业模式，Stake 持有人通过质押、投票、委托和锁定等行为获取交易费、区块奖励以及分红等收益。它最初由 2019 年初 Stake.us 获 Coinbase（美国首家合规比特币交易所）、Pantera Capital（美国最大的加密货币对冲基金之一）等机构的 450 万美元投资引燃，之后，EOS、以太坊 2.0、Dfinity、Polkadot、Harmony 则进一步将 Staking 推向大众视野。

2019 年以来，Staking 经济迎来了爆发式增长的一年。根据 StakingRewards.com 统计，截至 2020 年 6 月，全球共有 111 只加密资产支持 Staking，Staking 总市值已达到 170 亿美金。按照总体平均 11.08% 的年化收益率粗略

计算，Staking 为持币者每年创造的收益可达 7.5 亿美元。

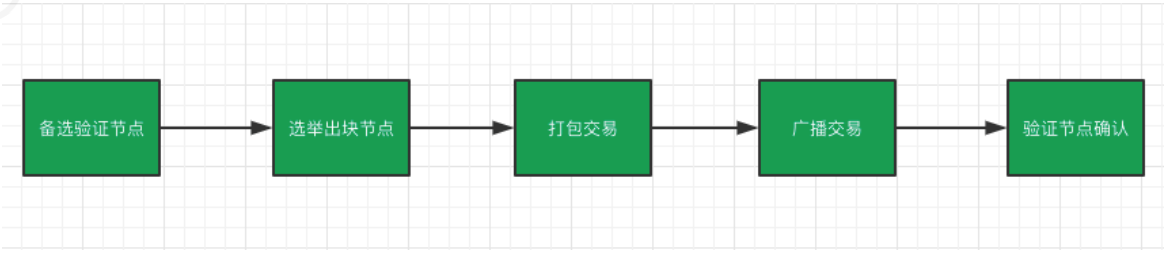
Staking 显示了加密金融原始的创新能力。它通过通胀奖励的方式将一部分通胀收益转移给加密资产持有人，减轻了持币者资产被稀释的风险，但是它又是矛盾的——过度的激励可能带来不受约束的高通胀，不仅对加密资产二级市场的价格形成抛压，也可能令加密项目内部形成恶性循环。

图：2019-2020 年 Staking 市场抵押资产规模

Staking 市场的参与方主要有两种节点：验证节点和代理节点。

（1）验证节点

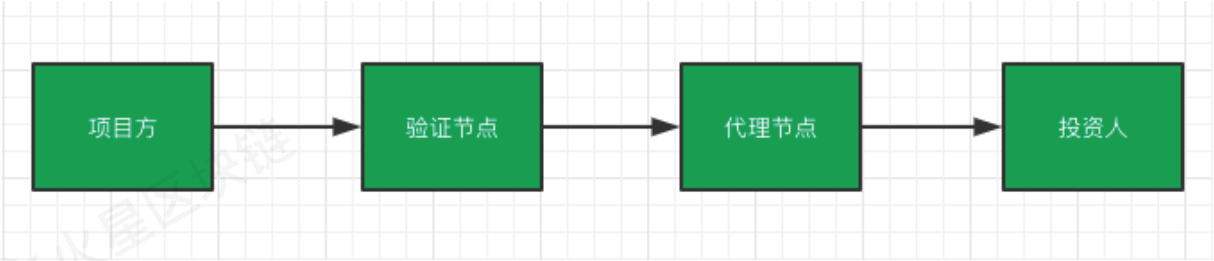
验证节点在每个项目中的名字也许会有不同，例如全节点、超级节点等等。以 EOS 为例，在 EOS 项目中，验证节点被称为超级节点。他们是从 100 个备用节点中，经过所有持币用户投票选举诞生的最终获得记帐权的 21 个节点。验证节点首先是网络中的全量节点（Full Node），并通过私钥签名发送广播投票参与节点间的一致性投票。验证节点在区块链中产生新的区块并获得出块收益。节点必须参与投票社区治理的提案。验证节点的权重取决于他占有的股份权益（Stake）。



图：选举验证节点的主要流程

（2）代理节点

代理节点可以理解为一个二级经销商。在整个业务链条中，代理节点起到一个收集投资人的投票权给某个验证节点的作用。而作为奖励或报酬，验证节点会给与一定的佣金作为收集投票权的报酬。



图：代币传递过程

本文着重对处于 PoS 机制金字塔尖的超级节点作为案例进行分析。目前为止，超级节点主要类型为以下几种：钱包、矿池、交易所、社区节点以及投资机构。

——钱包。钱包最基础的功能就像它的字面意思一样，即存储各类数字资产的地方，能转账就行；对于那些喜欢尝试各类 DApp 的朋友来说，钱包可能更像是一个浏览器；但是不管钱包怎么演进，它本质上一直在默默无闻的做着一件事情——架起人与区块链沟通的桥梁。

节点类型	服务商
矿池	Huobi Pool、OKEX、bitfish、SPARK POOL、stake-fish、ANTPOOL、币印
交易所	BINANCE、gate.io、BITTREX、Huobi、coinbase
钱包	imToken、In Math We Trust !
投资机构	POLYCHAIN CAPITAL、CoinFund、DIGITAL CURRENCY GROUP、GALAXY DIGITAL
专业服务机构	StakeWithUs、coinbase Custody、HashQuark

图：staking 超级节点主要类型

——矿池。矿池起源于比特币挖矿时期，在全网算力提升到了一定程度后，过低的获取奖励的概率，促使一些极客开发出一种可以将少量算力合并联合运作的方法，使用这种方式建立的网站便被称作“矿池”(Mining Pool)。在此机制中，不论个人矿工所能使用的运算力多寡，只要是透过加入矿池来参与挖矿活动，无论是否有成功挖掘出有效资料块，皆可经由对矿池的贡献来获得少量比特币奖励，也就是多人合作挖矿，获得的比特币奖励也由多人依照贡献度分享。

——交易所。交易所即为各种项目方代币交易中心。PoS 机制下，Staking 对于交易所来说有两大好处。首先，Staking 可以带来额外收益。额外收益来自于交易所使用交易所内用户的存币进行 Staking，同时运行节点，享受每年增发的收益，将成为交易所除了交易手续费及上币费之外的额外收益。我们并不清楚是不是大部分交易所都已经开始这么做了，但表面上看，实际分享出收益给用户的交易所非常少。

——投资机构。投资机构主要指那些天使及风险投资机构。由于他们所投资的项目以代币形式发放给投资机构本身，导致投资机构持有大量项目代币。通过 Staking 的形式，投资方能够获取额外收益，这也是他们参与 Staking 的驱动力。

——社区节点。社区节点通常是那些密切关注项目发展，且对项目治理作出积极贡献的群体，他们可以通过参与节点的方式，更进一步的影响到项目的发展方向，并获得项目增发的收益。

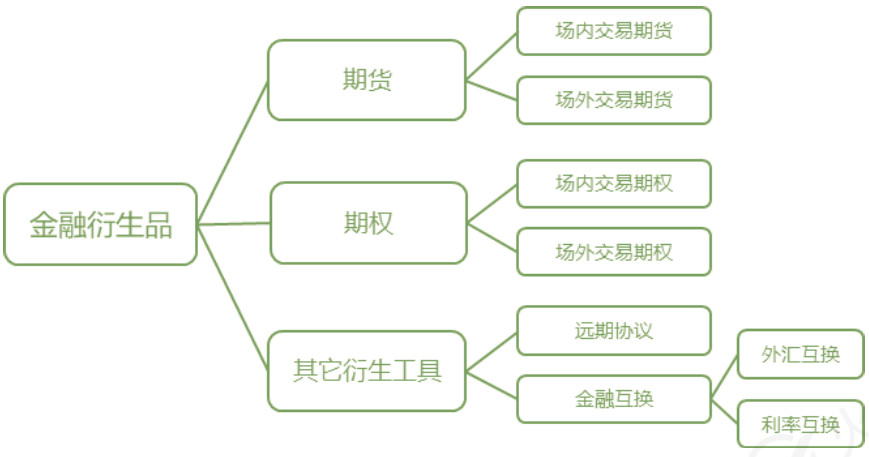
未来，Staking as a Service 将成为 Staking 经济和生态的商业模式的核心，钱包、交易所、加密资产托管机构、PoS 矿池借助其先天优势成为 Staking 的天然入口；此外，数据研究、安全服务、应用开发……更多领域的参与者将加入 Staking 生态，为加密金融市场继续繁荣提供新的动力。

2.2.3 数字通证衍生品

传统金融衍生品是以金融市场上的资产或指数作为标的资产的金融合约，主要包括远期、互换、期权等衍生金融工具。随着全球金融市场的不断发展，金融工具的种类逐渐增加，能够实现高杠杆交易、套期保值、风险对冲以及投机交易等功能的金融衍生品逐渐开始发展，用来满足不同投资者的需求。

与传统金融工具类似，在以区块链为基础技术的加密数字货币广泛发展的今天，加密数字货币也已经成为很多投资者的另类投资标的，满足投资者的资产配置选择。加密数字货币合约规定了投资者拥有在未来按照约定价格交割一定数量数字货币的标准化合约。通过交割合约，可以实现对数字货币的做多或者做空，满足了对数字货币持有不同预期投资者的需求。

随着以加密数字货币合约为主要代表的数字通证衍生品交易市场的不断发展，越来越多的投资者进入这个市场，逐渐在发现衍生品的套期保值、风险对冲和资产负债管理等其他作用。



图：传统金融衍生品市场的主要类型

本文重点研究的数字通证衍生品市场，主要以永续合约、交割合约和期权合约为主。

加密数字货币永续合约与交割合约存在一定区别，永续合约没有到期时间，而是通过资金费用机制，以实现合约价格紧跟标的价格，利用标记价格来计算投资者账户的未实现盈亏；期权合约赋予了投资者在未来某一约定的时间以约定的价格进行交易的权利，投资者可以选择四种不同的头寸，买入看涨期权、卖出看涨期权、买入看跌期权、卖出看跌期权，买入合约的投资者在付出一定的权利金后便享有了到期买卖数字货币的权利，卖出合约则可获得暂时的期权费收益，但却承担着未来买卖数字货币的义务。

交易所	期货合约	永续合约	期权合约	现货杠杆
Huobi	√	√		√
OKEx	√	√	√	√
Binance	√	√	√	√
BitMEX	√	√		√
Bitfinex	√	√		
CoCoCoin		√		
HBTC		√	√	

图：部分主流数字货币交易所支持的合约类型 ①

2019 年，数字通证衍生品交易呈现爆发式增长，2019 年 12 月 31 日，市场交易金额达到了 124 亿美元，是 2019 年 1 月的日均成交金额（接近 50 亿美元）的 2 到 3 倍，并且还有不断增加的趋势。随着加密数字货币衍生品种类的不断增加，预计 2020 年的数字通证衍生品交易量将继续呈现爆发式增长态势。

虽然数字通证衍生品市场仍处于早期发展阶段，且衍生品合约的开发和投资门槛较高，但其吸引了越来越多投资者的关注，为投资者提供了更多数字资产配置的选择，市场将进入高速发展阶段，推动数字资产交易及管理市场更加成熟化。

① 数据统计截至 2020 年 6 月

PART 3

第三部分

区块链技术演进：重塑金融未来

3.1 跨链

跨链是不同链间可以执行原子性交易，交易涉及的数据可以被访问、验证以及使用，实现互操作性。跨链可以按照交换信息的种类拆分为加密资产互操作与状态事件互操作。简单来说，跨链或者区块链互操作性的技术是为了提供两个区块链交换信息的方法。

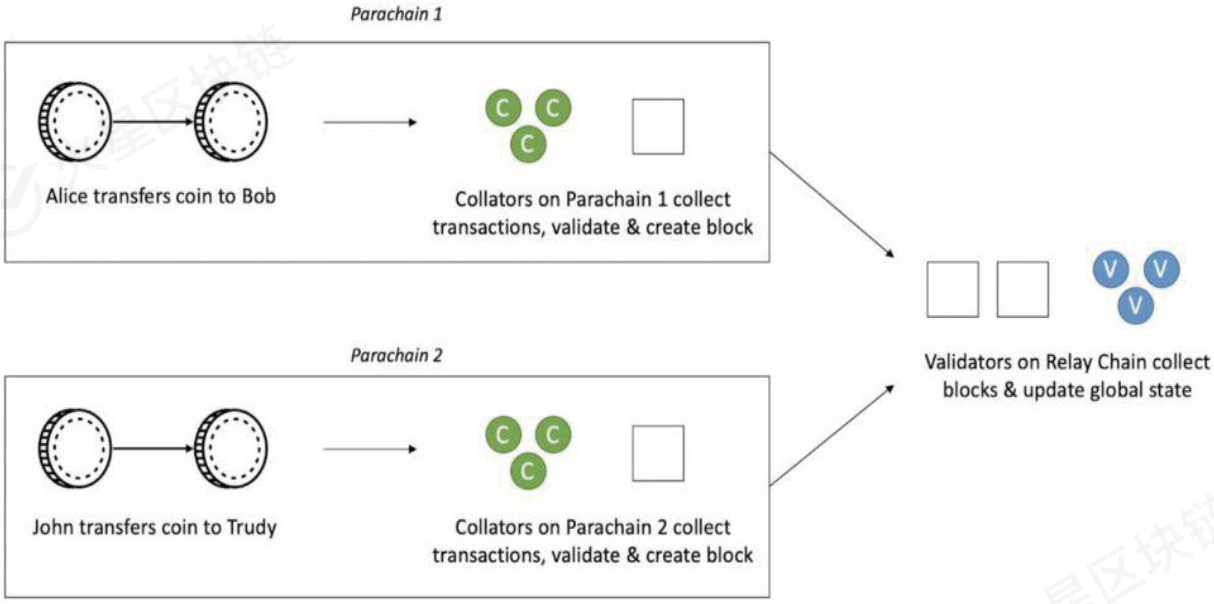
早期，跨链技术更多关注的是资产转移，典型项目包括 Ripple（瑞波）、BTC Relay 等；如今，跨链技术更多关注的是跨链基础设施，尝试建立一套多链的架构，让所有接入此架构的区块链，能更好的完成互相之间的信息和价值交互。跨链技术确保了区块链之间的互操作性，是实现价值互联网的关键。

（1）跨链技术的主要类型

——多链架构的互操作性解决方案

代表项目：Polkadot、Cosmos

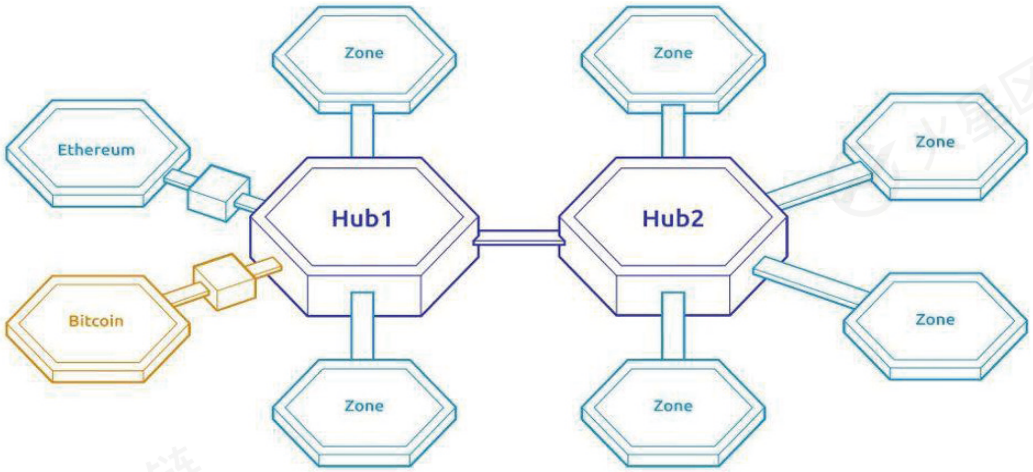
Polkadot 项目创立的初衷是试图规避以太坊在围绕分片、超级立方体模型（hypercubes）和 Casper 的研究变得越来越复杂时所面临的挑战。Polkadot 的方案是通过允许相同区块链的多个「迭代」（即平行链 + 中继链的方案），在彼此之间实现互操作，从而最大化可组合性。Polkadot 的中继链类似于以太坊的信标链的枢纽角，将多个平行链连接在一起。



图：Polkadot 网络架构

为了最大化多链架构的可组合性，Polkadot 创建了开发框架 Substrate，任何人都可以基于 Substrate 去做自己的区块链项目，即使与 Polkadot 毫无关联也并不影响，Substrate 框架开源后是中吸引一大批开源社区的开发者使用，其核心组件包括：数据库（简单键值存储并实现 PatricaMerkle Tree 以支持轻量级客户端之间的无需信任的交互）、网络连接、交易队列和共识引擎。

Cosmos 网络由不同的独立、平行区块链组成，其中的每条区块链都通过例如 Tendermint 这样的经典拜占庭容错共识运行。Cosmos 上的区块链称为“分区（zone)”。其中的一些分区又称为“枢纽（Hub）”，而不同的分区可以通过共享的枢纽来互相通信与互操作。Cosmos 网络上的第一个分区就是 Cosmos 枢纽（the Cosmos Hub）。



图：Cosmos 网络架构

所有跨分区的代币转移都需要通过 Cosmos 枢纽进行，因此代币可以安全、迅速地在分区之间转移。分区之间无需具有直接的汇兑流动性，而只需通过 Cosmos 枢纽来追踪记录每个分区持有的代币总量，并确保所有分区的代币总量不变。在此，Cosmos 枢纽起到了一种类似中央银行结算功能的作用。

——公证人模式（中间商）

代表项目：Ripple—Interledger Protocol (ILP)

见证人是一种多中心或弱中心的模式。与中心化方案对一方的信任相比，见证人模型选择相信多方信任。它选择一个多方委员会，只要大多数验证者都同意，就可以执行跨链消息，换句话说就是相信大多数验证者的安全。跨链流程资产由多个见证人移交。相对于中心化的解决方案，资产跨链安全性和透明度的见证模型得到了极大的改进。而且它对交易双方更加友好，并且实现相对简单。因此，该模型已被广泛使用。但从本质上讲，它仍然取决于对人的信任。此外，还计划在这种模式下进一步分散和保密证人的规模，以进一步提高权力下放的程度，但同

时也带来了更好的复杂性。

相对于中心化模式下的信任，去中心化模式要求消除人为中介，并努力利用去中心化技术来承担中介角色，强调对密码学安全的信任。

——哈希锁定

代表项目：lighting network

哈希锁定是一种原子交换技术。它通过哈希时间锁定来实现交易双方的资产锁定和托管。其实现模式要求交易双方都严格遵守参与流程，严格的时间锁定要求以及端到端通信要求。但是，交易双方完成了交易过程，并且跨链资产立即被原子交换。它是完全去中心化的，安全的，透明的，并且没有第三方的参与。

原子交换作为资产跨链中最简单的技术，跨链的过程直接由交易双方执行，从而完全消除了第三方的信任并完全消除了交易对手的风险。资产交换成功或失败，并且用户资产始终是安全的。

从技术上讲，原子交换通常基于哈希时间锁定技术或多签名技术，并且需要同时具有两条链，例如相同的哈希算法和哈希时间锁定支持。因此，它通常只能应用于同构链之间。原子交换是完全分散的，并且高度安全，但是它们在易用性方面非常差，难以大规模商业化。

——轻节点式侧链中继

代表项目：BTC-Relay、POANetwork

所谓轻节点是指一种验证方法，可以通过输入少量数据和少量计算资源来获得安全正确的反馈。资产跨链领域的应用主要用于跨链区块头和交易证书的验证。这个方案资产跨链的两侧主要埋在彼此的轻节点中，中继用作通信桥以提供双向通知。正是由于双向光节点的不信任信任验证功能，中继才可以被信任。在轻节点的实现中，使用与原始链一致的一致性验证算法来验证原始链的所有块头，并通过交易根和交易签名来验证数据安全性。在资产跨链过程中，用户资产也托管在轻型节点上。如果没有第三方的参与，则无需信任第三方，从而可以实现原始链的最高安全性。锁发，销毁和解锁的过程通过跨链认证完全实现，并且完全不受信任。

（2）加密资产互操作的商业价值

资产跨链流通、自由交互在商业上给网络和用户带来了三个显著的价值：

——资产交换。资产跨链给资产交换带来安全和透明。用户可以基于链上匿名身份，在加密世界自由进行资产交换，不需要KYC、不需要中心化审核、不需要信任第三方、不会买到假资产、资产也不会被挪用占用，资产控制权永远掌握在用户手里。

——扩展协作。链和链之间可以有所分工，各自专注于专业化和垂直化，以独特功能服务好用户。彼此之间通过跨链的方式进行协作互补，从全面竞争转向开放协作，全面提升网络价值和网络效应。譬如BTC发挥数字黄金作用，流入其他链作为基础货币发挥价值存储作用，Libra可以进入其他链平台发挥交易媒介作用，Zec可以帮助其他链增强隐私功能等等。

——开放金融。基于跨资产的融合将会带来开放金融应用更广阔的前景。当下开放金融应用被认为是区块链最具备爆发力的场景之一，但当前受限与链与链之间割裂，开放金融应用受困于单资产和单一用户群，无法低摩擦进行扩展。举例，在以太坊的 MakerDAO 应用中，当前受限于只能使用 ETH 或 ERC20 Token 作为抵押物，并且只能服务以太坊用户。由于 BTC 无法支持智能合约，所以 MakerDAO 无法部署于 BTC。另外为了服务 EOS 用户，MakerDAO 需要再在 EOS 链上重新部署一套 MakerDAO 智能合约。这个是完全隔离的世界。如果有资产跨链，这一切就会变得非常不一样。通过资产跨链，一个应用只需部署一次，可以使用所有资产，同时为所有链的用户提供服务。

3.2 以太坊 2.0

根据以太坊的规划，共分为四个阶段：边境（Frontier）、家园（Homestead）、大都会（Metropolis）和宁静（Serenity）。目前以太坊已经走过了前三个阶段，以太坊 2.0，或称 Serenity（宁静），是以太坊开发的第四阶段。

图：以太坊 2.0 路线图

以太坊 2.0 的核心是实现以太坊网络大规模应用，大幅提升网络扩容性。以太坊 2.0 计划在 2019 年至 2021 年间，分四个阶段发布。2019 年 4 月，Vitalik 表示，为了在现有以太坊网络上改善扩展性问题，以太坊 2.0 带来的变化大致有两种：将 PoW 算法变更为 PoS，以及 Sharding（分片技术）。

以太坊 2.0 并不是对现有以太坊网络的升级，而是一次全面的修订和重新设计。并且整个更新计划将持续很多年，直至完成最终的规划目标。

（1）ETH2.0 的技术变迁

——共识机制由 PoW 转移为 PoS，这将是备受关注的创新型 PoS 共识 Casper FFG 算法的首次落地实现。

——在 PoW 共识机制下，以太坊只有一条最长的链作为主链，而以太坊 2.0 网络则拥有一条信标链和 1024 条分片链，以实现扩容。这些不同的分片链可以互相通信，并统一由主链信标链进行控制和验证。

——ETH2.0 链上的数字资产为 BETH，原来的 ETH 将在新的主链上无法使用。ETH 的持有者只能通过销毁的方式，将 ETH 按照 1:1 方式兑换 BETH。原来的 ETH 将被销毁，从而产生新的 BETH。这个兑换机制由以太坊 1.0 上的智能合约完成，并受 ETH 2.0 信标链的监控。

——Staking 将是 ETH 2.0 的重大功能之一，即用户可以通过质押 32 BETH，成为 ETH 2.0 信标链的验证人。

-	以太坊1.0	以太坊2.0
架构	单链	多链（分片）
后端开发	Solidity (类似JavaScript), Vyper (类似Python)	Solidity (类似JavaScript), Vyper (类似Python)
执行环境	单VM	多同质分片
可组合性	智能合约可互相同步调用	智能合约可在同一个分片中互相同步调用，也可在分片之间互相异步调用
治理	Off chain	Off chain
共识机制	Ethash（PoW）	Casper (PoS)
项目执行费	每次调用以gas进行计价	每次调用以gas进行计价
状态（截至2019年11月）	2015年上线至今	预计2020年Q1发布阶段0，之后分阶段推出

图：ETH 1.0 与 2.0 对比

（2）ETH 2.0 的设计目标

根据以太坊 2.0 白皮书，其设计目标如下：

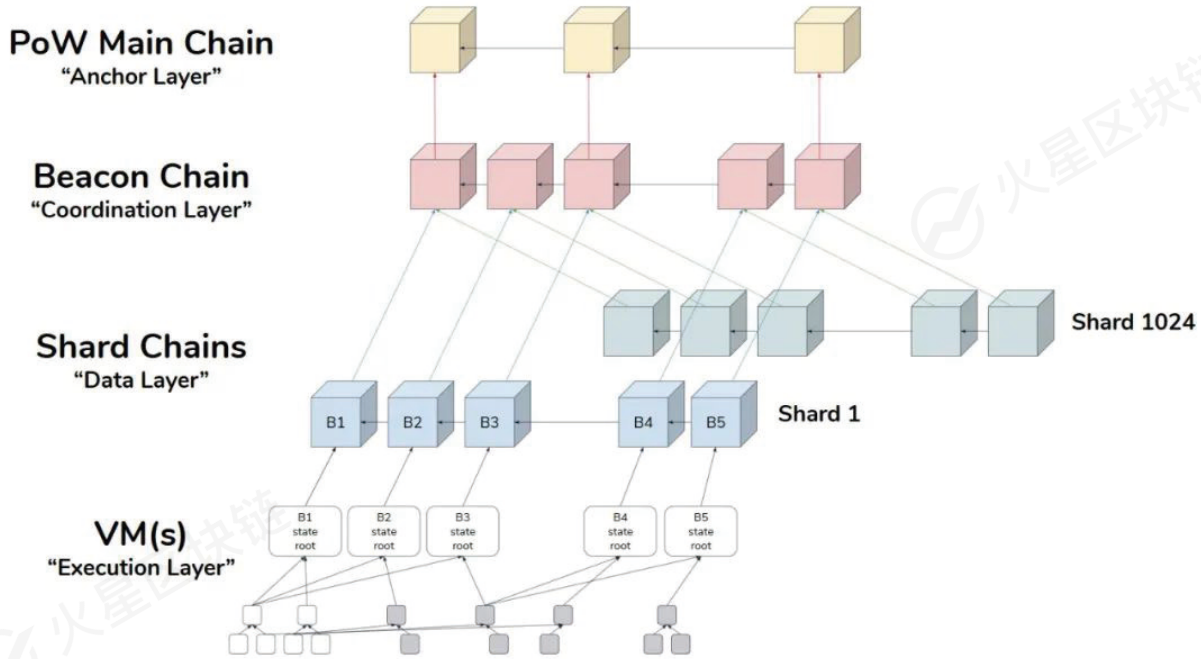
——**简洁性**。最大程度地降低复杂性，哪怕会导致效率有所下降。

——**强韧性**。在主网分区之后，大部分节点离线之时，整个系统依旧能够运行。

——**持久性**。选用的组件要能够抵抗量子计算，或是选用可替换型组件直到可用的抗量子计算组件出现。

——**安全性**。通过密码学技术和设计技术提高验证者的总人数和单位时间内的参与者数量。

——**去中心化**。允许处理能力达 O(C) 的消费级笔记本电脑处理 / 验证 O (1) 个分片（可能是系统上任何一层的验证，如信标链）。



图：ETH 2.0 路线图

（3）以太坊 2.0 的技术升级和创新

——共识机制 POW 转 POS：提升效率，解决耗能问题

在以太坊 1.0 中，使用工作证明（Proof of Work，PoW）作为共识机制，并借此产生新的区块。基于 POW 算力的共识，所有的节点同时只能做一件事，整个网络能够处理的任务量是非常有限的，严重受制于网络中单个节点所能处理任务的上限。即使对区块大小进行扩容，由于存在全网共识，效率提升的作用也是有限的。因此，为了要减少工作证明产生新区块时所花时间过长，以及需要大量算力造成资源浪费的问题，以太坊 2.0 将改为权益证明（Proof of Stake，PoS）作为产生新区块的共识机制。

——分片（Shards）：提升网络性能和

容量

物理空间上，分片是将公链网络中的所有节点划分为不同的分组，每一个分组叫做一个分片。原本公链中所有节点所做的任务是完全相同的，现在将任务进行分组，分配给不同的分片，各个分片处理不同的任务。原来公链网络的性能瓶颈取决于网络中节点的性能，进行分片后，单个分片内的节点仅需承担全网的部分工作，各个分片并行工作，从而提升整个网络的承载能力。假设分片数为 n，则每个节点需要承担的的工作量为全网工作量的 1/n。同理，全网容量也将变为原来的 100 倍。分片是区块链扩容最佳方案，它能在没有提高节点硬件要求且没降低去中心化程度的情况下，实现网络性能和容量的大幅提升。

——由 eWASM 代替 EVM：提升智能合约的兼容性和执行效率

以太坊团队提出使用 eWASM 替代 EVM，eWASM 是 WASM (WebAssembly) 代码的 Ethereum 版本，相比于 EVM，eWASM 具有更好的性能以及更好的扩展性，可支持 Solidity，C++，Rust，AssemblyScript 等多种编程语言，开发合约会更容易，也将可能在 ETH2.0 上支持智能合约、账户、状态等。

以太坊 2.0 如果顺利完成升级，将极大地促进区块链技术整体向前发展，特别是解决了当前公链最大的难点扩容问题。但是，也必须认识到以太坊 2.0 更新整体跨度的时间比较久，技术创新度高且难度大，是否能够能够实现稳定、安全的新一代底层公链目标尚存在较大的不确定性。

3.3 商业级金融公链

与传统架构相比，区块链架构具有防止篡改、易于审计、透明度高、可靠性强、智能合约可自动执行等优势，被越来越多的人认可其是构建新一代金融市场的重要基础设施。根据参与者准入程度不同，金融区块链在公有链、联盟链、私有链、混合链的架构上可以产生不一样的价值。很多金融应用场景已经拥有了完备、低成本的信用体系的情况下，在什么环节上使用区块链、使用什么样的区块链架构成为探索“金融公链”应用的前置问题。

目前商业中大多数区块链用例都是“许可链”，显示企业需要更可靠的系统和有效的协作，但必须在同一生态链的成员内部。因为这些数据不适合公开，且必须防止受到网络攻击。此外，与无许可的公链相比，保留在少数或公司的内的联盟链需要的计算能力更低，并且由于其限制性而往往带来了更大的可扩展性。

对于公链而言，最显而易见的优势是通

过建构一个开源、多元的生态系统，但金融行业的创新往往需要遵从监管层的意见，须要置于国家主权范畴下、法律与监管下考虑，并且始终将安全可靠性作为第一要求，公链天然具有的无边界、弱身份验证属性，使得法律监管成为大规模商用的首要障碍。除此之外，软硬件性能、产品设计、资产创造等方面的问题金融公链在大规模应用也亟待突破。

理想中的商业级金融公链的特征，一方面具备金融应用场景中的 TPS 等硬指标，以满足交易上链中高速、高频的需求；另一方面还要支持智能合约，以实现在合约上链时的复杂交易、业务合约、金融合约、逻辑和验证内容。

下一阶段，商业级金融公链可能在以下几个方面实现新的突破：

（1）公链性能提升将显著扩展金融应用场景

在传统金融行业中，对交易系统运行的效率具有很高要求，以证券交易为例，传统证券交易主要包括报单、撮合、清算、结算等步骤，交易所完成撮合即视为交易完成，TPS 高达数十万。而性能问题是目前限制公链大规模商用的最大阻碍之一，十位数甚至个位数的 TPS 导致比特币和以太坊这两个最大的公链网络经常出现拥堵现象，性能问题直接导致区块链网络交易费用高昂、基于公链开发的应用用户体验差，完全限制了公链在高并发场景以及复杂业务场景中的应用。

目前已有多种公链的扩容方案提出，如链上扩容、链下扩容以及第零层扩容等众多解决思路，具体解决方案如分片、状态通道等。经过一段时间的探索，部分区块链扩容项目已经测试实现了千位数的 TPS。未来随着区块链扩容相关技术的不断深入，公链性能有望达到传统金融系统应用的基本要求。

（2）公链的产品设计门槛逐渐降低

目前基于公链的交易平台的主要产品对新手来说，使用门槛较高。一个新用户在正式开始交易之前需要至少经历六个步骤：下载钱包 app/ 插件——创建密码——抄写保存助记词——按顺序确认助记词——购买数字资产并转账进入钱包——钱包绑定 DEx。尽管事实上这个流程可能花费时间不会超过 10 分钟，但关于助记词、复杂的区块链地址、不同于银行的转账系统、需要缴纳 Gas 费等等新事物会大大增加用户的理解负担。

对于完全去中心化但分布式交易平台，改善用户体验是大规模应用的关键瓶颈。目前一种创新的解决方案是通过智能合约来管理资产，用户账户的资产不只由一个私钥完全控制，而是通过提前写入规则的智能合约管理，包括设置管理权限、账户恢复，转账限额等，使得用户即便泄露或遗失记录私钥的物理装置，也有办法保证不会丢失所有资产。

（3）更多高质量、高流动性资产即将上链

链接投资人和资产是所有交易平台的本质功能。受限于目前主流 DEx 上的资产多以 utility token（实用型通证）为主的现状，utility token 的使用场景尚未大范围铺开、价

值捕获较模糊，导致其交易流转的需求及用户数受限。

随着区块链升级至中国的国家级战略，将带来一轮新型数字资产的诞生，像供应链金融、知识产权、用户数据等等，市场空间极为广阔。有分析机构预测，仅供应链金融资产上链就有望在三年之内达到3.6万亿人民币，这将超过现有所有数字货币的总市值，届时分布式交易平台架构可能因为更多高质量数字资产的流转需求而变得普及。

（4）底层硬件系统发展实现突破

公链实现商业级的应用，面临的天花板不只是软件系统，硬件的发展也带来不容忽视的水桶效应，如：区块链系统由于采用分布式存储，每个节点都要复制信息，对带宽供应速度提出很高要求；其次，交易需要验证，对CPU的计算能力有要求；另外，所有的交易记录要保存下来，因此对硬盘的I/O速度也有要求。随着计算机硬件设备的不断升级，区块链底层硬件系统将实现新的突破，为商业级金融公链的发展提供硬件支撑。

3.4 零知识证明

零知识证明的概念于20世纪80年代初由麻省理工学院研究人员S.Goldwasser、S.Micali及C.Rackoff提出。简单来说，零知识证明是一种技术，可证明使论述为真的证据的存在，而不用暴露证据本身，例如，人们可以证明自己拥有符合审计的证据，而不需要披露证据本身的细节。这项技术具有三个特性：完整性（Completeness）、可靠性（Soundness）、零知识性（Zero-Knowledge），三者必须同时满足才能完成零知识证明。

举例，某证明者(P)向某验证者(V)宣称：他们知道洞穴后面密门的密码，而且希望在不透露密码的情况下，向验证者(V)证明这件事。证明者沿着A或B任一条路径走进去。假设他们一开始选择A路径，然后到达后方的密门。接着，验证者来到洞口，并要求看到证明者从B路径出现。（这时候验证者并不知道证明者选择哪一条路径走进洞穴。）上述验证必须进行多次以保证没有运气成分，如果证明者每一次都能出现在正确的路径上，那么证明者就能向验证者证明他的确知道密门密码，同时验证者无法得知密码到底是什么。

在上述示例中，零知识证明的三个特性同时满足：完整性：因为该论述是真实的，诚实的证明者(P)可以说服诚实的验证者(V)；可靠性：如果证明者(P)不诚实（即其实他们不知道密码），他们也无法在多次实验下欺骗验证者(V)。即便证明者(P)很幸运，运气也总有耗尽的一天；零知识性：验证者

(V) 自始至终都不知道密码是什么，但他会被说服证明者 (P) 拥有密码。

（1）主流零知识证明技术

零知识证明最有代表性的两个技术为 ZK-SNARKs 以及 ZK-STARKs。

ZK-SNARKs 的代表项目是 Coda，它是第一个具有简洁区块链的加密货币协议，它克服了下载验证区块链的所有事务的要求，使得加密货币对每个人都是可访问的。Coda 协议的核心在于 SNARK 的递归组合。SNARK 递归组合是指为多个 SNARK 证明创建一个 SNARK 证明，可将这些 SNARK 证书以递归结构链接在一起，实现了让区块链保持约 20kB（SNARK + 尾部 Merkle 路径）的恒定大小。这使得开发在浏览器中本地运行的用户友好型加密应用程序变得异常容易，并实现了更具包容性和可持续性的共识。

ZK-STARKs 的代表项目是 StarkWare，它对零知识证明算法作了改进，提高区块链的可拓展性和隐私性，并且该算法能够抵抗量子计算的攻击。

（2）零知识证明的金融场景应用

应用场景 1：隐私交易

代表项目：Zcash

Zcash 代表了 zkSNARKs 的一个应用方向：隐私。隐私有不同的程度，Zcash 的隐私交易指的是隐藏交易的发送方，接收方以及交易金额。Zcash 已经经历过三个版本：Sprout，Overwinter，Sapling。这三个版本本质上都没有太大的变化，只是支持的功能更多，生成证明更快，体验更好。Zcash 目前的特点以及可以实现的功能有：低成本交易（成本接近 0.0001 ZEC）、交易地址隐私、加密备忘录（可应用于银行保密法的 Trave Rules）、密钥揭示、付款披露。

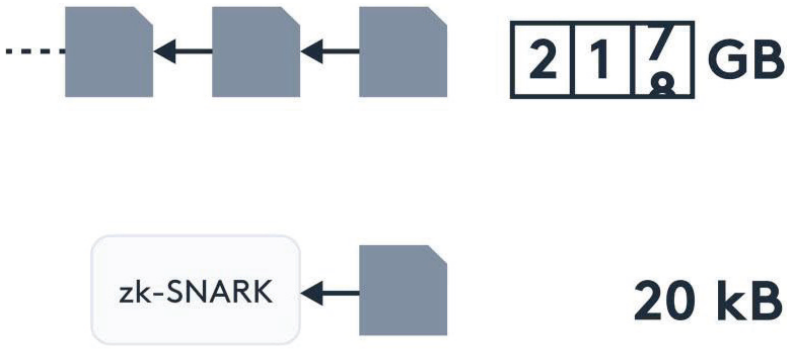
其它类似技术应用到隐私场景的项目，如 EYBlockchain (EY，安永)，Quorum (JPMorgan)。

应用场景 2：链上数据压缩

代表项目：Coda，Filecoin

Coda 通过零知识证明 ZK-SNARKs 技术将区块链数据压缩到固定字节大小。由于目前区块链全节点数据容量非常大，并且有继续变大的趋势，让全节点的网络同步以及存储变得很困难，Coda 通过零知识证明的不断递归，能将目前几十 GB 的区块链账本压缩到 20k，从而使得移动端也可以即时同步区块链数据。

Filecoin 作为一个去中心化的存储项目，首先面对的核心问题就是如何证明存储提供方真实有效的存储了指定的数据。对此，Filecoin 是通过 PoREP 以及 PoST 算法实现的（其中就包括零知识证明）。PoREP 算法是通过零知识证明证明数据已经正确处理，并提供了处理后数据形成的 Merkle 树的树根。而 PoST 则每隔一段时间随机抽选一个叶子数据，需要存储提供者在一定的时间内提供从该叶子数据到 Merkle 树根的路径证明。如果处理完的数据没有保存在一个可靠的存储上，无法在合理时间内重建整个 Merkle 树，也就无法提供证明。



图：Coda 通过 zk-SNARK 压缩区块链账本 ①

应用场景 3：链上交易平台扩容

代表项目：Loopring DEX 3.0

从 2017 年，路印从“环路撮合”的最初设计，经过了 1.0，2.0 以及 3.0 的三个大的版本的协议升级。1.0/2.0，相对来说，受限以太坊本身性能的限制，交易流程复杂，体验和中心化交易所相比，有较大的差距。2.0 协议之前，采用的是“链下撮合，链上记录“的方式，链下主要由 Relay 维护订单（Order Management）和完成订单的撮合（Settlement Engine），完成撮合的订单，需要在链上记录（由链上的智能合约实现）。路印协议 3.0 所有的撮合逻辑仍然在链下完成，但 3.0 采用零知识证明技术 zkSNARK 的 Groth16 算法，每一笔撮合都会生成证明并提交到链上，证明链下的撮合正确无误。

总的来说，路印协议 3.0 通过零知识证明技术，在 zk Rollup 的基础上，结合 DEX 的业务场景开发设计，兼顾去中心化和交易性能。

① 资料来源：Coda Whitepaper

PART 4

第四部分

数字金融创新与全球监管政策

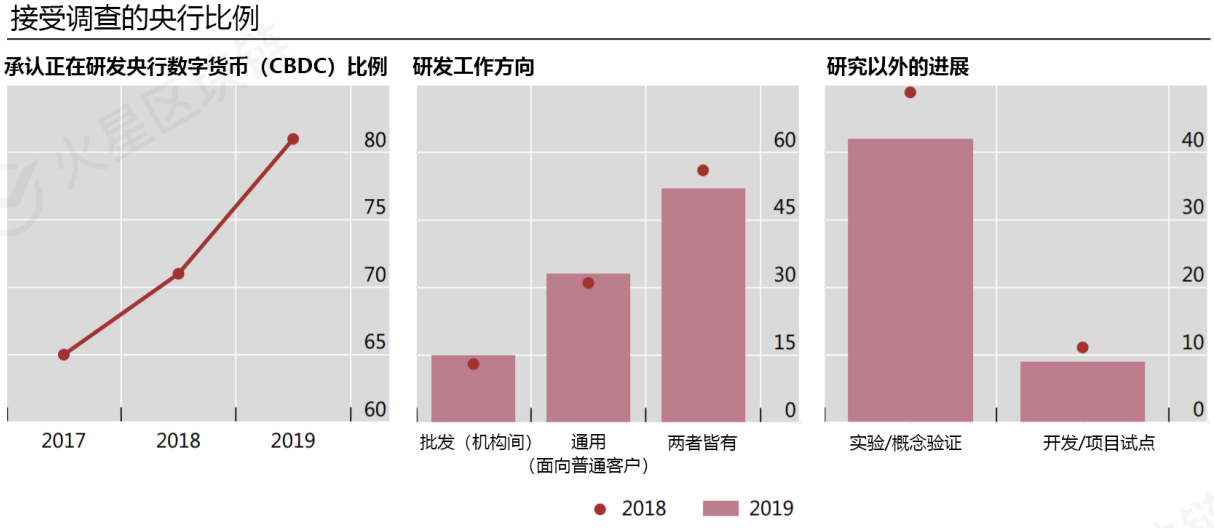
4.1 区块链产业政策

（1）区块链已成各国必争之地，多国制定总体战略

——多国制定区块链产业总体战略。2019 年 Libra 项目白皮书的发布引发全球广泛关注，将全球关于区块链技术应用与监管的讨论推向新的高潮。澳大利亚、韩国、德国、荷兰、塞浦路斯、阿联酋、马耳他等多个国家制定了区块链产业总体发展战略，2019 年 9 月，德国发布《德国国家区块链战略》，2020 年 2 月，澳大利亚公布国家区块链战略路线图，区块链技术俨然已经成为各国下一个必争之地。

——各国积极研发央行数字货币（CBDC）。根据国际清算银行对 66 个国家（地区）央行的调查，2019 年约 80% 的央行正在研发央行数字货币，相比 2017 年增加了 15 个百分点，同时 10% 的项目已经进入试点阶段。2020 年 2 月，瑞典央行开始电子克朗测试，2020 年 5 月，法国央行宣布完成了对数字欧元的首次测试，韩国等国家公布了央行数字货币测试计划。

此前否定央行数字货币的美国和日本态度近来也出现了转变，2020 年 2 月，美联储理事莱尔·布雷纳德表示正在研究发行数字美元的可行性，日本也已经开始研究央行数字货币。



图：各国研发央行数字货币的不完全调查统计 ①

① 资料来源：国际清算银行 (BIS)、临港区块链技术产业研究院

（2）中国高度认可区块链技术，密集发布支持政策

——区块链上升到国家战略高度。2016年10月，工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》；2016年12月，国务院印发《“十三五”国家信息化规划》，首次将区块链技术列入国家级信息化规划内容；2019年10月24日中央明确把区块链技术作为核心技术自主创新的重要突破口，加快推动区块链技术和产业创新发展。

——各级政府单位密集发布扶持政策。据《中国区块链年度发展报告》，2019年全球82个国家、地区、国际组织发布区块链相关政策超过600项，其中中国发布267项，占全球总数的45%。2020年4月20日，国家发改委明确“新基建”范围，区块链技术被纳入其中，北京、上海、广东等20多个省份都将区块链写入了2020政府工作报告，表明中央及地方对于区块链技术作为新一轮科技和产业变革驱动力的认可，政策东风下，政府区块链项目采购迅速增长。2019年政府区块链采购项目数量同比增长210%，2020年前5个月，政府区块链项目采购较2019年上半年增长67%。

（3）政策环境不断明朗，加速区块链研发应用落地

——政策环境明朗，加速区块链研发应用落地。定调区块链为核心技术，以及各类鼓励扶持政策的推出，一方面充分肯定了区块链技术的发展潜力，为区块链发展创造了明朗的政策环境，另一方面也有助于解决目前区块链行业存在的资金人才不足、产业集聚不强等现实问题，加速区块链的技术研发以及与产业的结合。

目前金融领域是区块链技术应用场景探索最多的领域，区块链的应用环节及应用逻辑相对明晰，各类支持政策的推出，将进一步加速区块链在金融及更多领域的应用落地。

——基础理论和关键技术研究支持有待加强。国家和地方已经出台了大量鼓励区块链发展的政策，但是缺乏统筹规划和顶层设计相关政策文件，下一步应尽快出台区块链发展总体规划，强化产业体系化布局。此外当前的区块链扶持政策多从企业角度进行鼓励，对于基础理论和关键技术研究的支持有待进一步加强。

4.2 沙盒监管

（1）沙盒监管契合区块链，成金融创新监管新趋势

沙盒监管由英国首创，已成为国际金融创新监管新趋势。随着金融科技的迅速发展，英国首创的监管沙盒制度吸引了新加坡、中国香港等众多国家和地区的探索尝试，截至

2020 年 2 月，全球已经推行沙盒监管的国家和地区超过 25 个，计划推行沙盒监管的国家和地区超过 18 个，地区性以及全球性监管沙盒也在推进。

各国监管沙盒理念一致，具体实施存在差异。沙盒监管的基本理念是通过法规豁免或限制性授权的方式，为申请者提供一个相对宽容的试错平台，各国（地区）的沙盒监管在监管主体、适用对象、准入标准、运作模式等方面存在不同程度的差异。

以英国为例，其监管沙盒由金融行为监管局（FCA）主导进行，由于未对业务类型

<table>
<tr><td rowspan="2">实施主体</td><td>负有金融监管职能的中央银行或货币当局</td><td colspan="2">中央层面单个或多个金融监管机构</td><td>地方层面金融监管机构</td><td>其他组织</td><td rowspan="2">沙盒监管部门多样化，多为对金融业进行统一监管的最高权责机构</td></tr>
<tr><td>新加坡、印度等</td><td colspan="2">英国、澳大利亚、日本、韩国、印度尼西亚、泰国等</td><td>加拿大等</td><td>美国等</td></tr>
<tr><td rowspan="3">适用对象</td><td colspan="3">领域</td><td colspan="3">机构 / 项目</td></tr>
<tr><td>聚焦某一领域</td><td colspan="2">未限制业务类型及规模</td><td>机构</td><td colspan="2">项目</td></tr>
<tr><td>加拿大、泰国、日本等</td><td colspan="2">英国、新加坡、澳大利亚等</td><td>英国、新加坡、澳大利亚等</td><td colspan="2">加拿大、印度尼西亚等</td></tr>
<tr><td>准入标准</td><td colspan="6">多数国家（地区）监管沙盒都制定了明确的准 0 入标准，主要包括创新性、提升消费者福利、对现有法律法规存在突破需要等
多数国家（地区）对持牌机构和非持牌机构同时开放，部分国家（地区）允许非持牌机构单独申请</td></tr>
<tr><td rowspan="2">评估主体</td><td>内部评估</td><td>开放式评估</td><td colspan="4" rowspan="2">多方参与的评估专家委员会机制，具有主体来源多元化、专业综合化匹配等优势</td></tr>
<tr><td>英国、新加坡等</td><td>韩国等</td></tr>
<tr><td rowspan="2">风险防控机制和消费者保护</td><td colspan="2">监管部门</td><td colspan="2">测试机构或项目</td><td colspan="2">消费者</td></tr>
<tr><td colspan="2">构建风险防控机制，在风险可控的阈值内放宽 / 豁免监管规则</td><td colspan="2">充分披露相关信息，制定风险防控方案，建立消费者赔偿机制</td><td colspan="2">提前了解沙盒测试信息，评估风险偏好和承受能力，参与合格投资者测试</td></tr>
<tr><td rowspan="3">退出安排</td><td colspan="2">通过测试</td><td colspan="2">未通过测试</td><td colspan="2" rowspan="3">监管机构需做好沙盒退出前的把关，防止风险扩散</td></tr>
<tr><td>限制性牌照授予</td><td>不设市场限制</td><td>直接退出沙盒</td><td>调整后申请重新测试</td></tr>
<tr><td>英国、澳大利亚等</td><td>新加坡、加拿大等</td><td>澳大利亚、日本、印度等</td><td>新加坡等</td></tr>
</table>

图：主要国家（地区）金融沙盒监管概况[①]

① 资料来源：北京大学数字金融研究中心，京东数字科技研究院，币安中国区块链研究院

和规模进行限定，因此适用范围很广，传统金融机构及金融科技创新机构均可进入；测试产品或服务必须满足具有突破性创新、能够明显使消费者受益等条件；测试流程主要包括申请、审核、确定测试方案（包括测试要求、适用范围等）、测试（FCA 全程监测）及评估。

沙盒监管与金融改革逻辑一致，更加契合区块链等金融科技的发展特点。沙盒监管的基本理念与中国内地的金融改革试点类似，不同之处在于“监管沙盒”是一种相对常态化的安排，且沙盒监管的综合授权、不限定地域更加契合区块链等金融科技的跨行业、跨地域特性，不限定测试内容更加契合区块链等金融科技的多元性发展。

（2）中国试点沙盒监管，区块链监管创新未来可期

中国大陆监管沙盒启动，已扩大至六市（区）。2020 年 1 月 14 日，央行营业管理部（北京）公示了首批 6 个金融科技创新监管试点应用，这一金融科技创新监管试点被称为中国版的“监管沙盒”。2020 年 4 月，试点范围扩大到上海、重庆、深圳、雄安、杭州、苏州等六市（区）。

监管沙盒试点标志着中国金融科技监管理念的重大转变，有助于促进区块链创新发展，实施灵活监管。早在 2017 年内地就已出现政府主导的沙盒试点，但随着监管收紧无疾而终。如今沙盒试点再次推出标志着大陆在金融科技监管方面迈出了关键的一步，利用沙盒监管能在有效防控风险的前提下鼓励创新，降低区块链公司的合规成本，减小监管不确定性带来的负面影响。另外监管部门通过与行业及项目的沟通交流，能够适时调整条款，实施灵活监管。

图：金融科技监管困境 ①

① 资料来源：临港区块链技术处产业研究院《鼓励金融科技创新的监管工具：国际实践中的创新中心与监管沙盒》

沙盒监管模式尚未成熟，仍有一定局限性。沙盒监管作为一种创新监管工具，目前还处于探索阶段，没有成熟的经验可借鉴，实操中也存在一定的局限性。例如授权难题和参与测试的成本问题仍有待解决，监管沙盒提供的测试环境与真实环境存在一定距离，加上沙盒评估标准的主观性和局限性等因素，导致沙盒监管测试难以作为判断真实市场效果的全部依据，同时也对监管部门提出了更高的要求。

借鉴国际经验，促进监管沙盒与改革试点融合创新。目前内地沙盒试点刚刚起步，未来要不断借鉴国际沙盒实践的经验，避免国际沙盒监管实践中暴露出的问题。另外鉴于沙盒监管与改革试点逻辑理念上的一致性，可以充分吸收改革试点的优点，在适应中国国情的同时，保持沙盒监管的特色，使沙盒监管成为高效透明的容错监管机制。

	美国证监会	英国金融行为监管局	澳大利亚证券和投资委员会	新加坡金融管理局
数据收集				
应用程序接口	√		√	
数据输入法			√	
数据提取法		√	√	
机读监管		√		√
云计算	√	√	√	
聊天机器人		√		
数据分析				
大数据	√	√	√	√
人工智能	√	√		√
自然语言处理	√	√	√	√
机器学习	√	√	√	√
监督学习	√	√	√	
无监督学习	√	√	√	
主题建模	√	√		
随机建模	√	√	√	
图像识别		√		
神经网络	√			

图：全球资本市场科技监管现状[①]

① 资料来源：临港区块链技术处产业研究院《全球资本市场科技监管发展现状》

加载监管科技，提升沙盒监管效率。在科技创新的推动下，越来越多的国家开始探索利用新技术开展科技监管，通过科技赋能实现事前预防和事中监控，从而监管更加积极主动，更有效率。目前科技监管的探索实践美国相对领先，英国、澳大利亚紧随其后。国内证监会已经成立科技局，未来在监管科技的加持下，监管部门的监管能力将进一步提升，沙盒监管的效率也将大大提升。

4.3 金融标准化建设

（1）中国区块链标准化起步较早，已颁布多项标准

国际标准化组织积极开展区块链标准化研究。目前，国际标准化组织（ISO）、电气和电子工程师协会（IEEE）和国际电信联盟（ITU）三大标准化组织在区块链方面均已提出多项标准。

中国区块链标准化起步较早，积极参与区块链国际标准制定。中国的区块链标准化工作于2016年底启动，与国际标准化基本同步，同时中国积极参与三大国际标准化组织区块链国际标准的制定。2017年，国内首个区块链标准《区块链参考架构》发布。2020年2月，央行发布《金融分布式账本技术安全规范》，为国内金融行业首个区块链标准。截至2020年6月10日，国内共发布27项区块链团体标准、5项区块链地方标准。

（2）标准化建设层层加码，助力区块链规模化应用

标准化建设有利于区块链规模化应用。区块链规模化应用，离不开完善的标准体系。目前，区块链金融乃至整个区块链行业都未形成区块链标准体系，异构跨链对接等技术难题导致产业生态兼容性较差，拖延了区块链的商业布局。在推动核心技术突破的同时，推进标准化有助于规范区块链金融产品市场，加速区块链在不同业务领域的规模化应用和推广。

国内区块链标准化仍有提升空间。国内区块链标准化具有良好的发展基础，但仍有较大提升空间，主要存在体系化程度不够、缺乏统一协调机制、标准研制进度及更新速度较慢等问题需要解决。另外区块链技术本身迭代迅速，很多关键技术还在发展阶段，也给标准化工作带来了困难。

2019年10月24日习总书记的讲话强调，加强区块链标准化研究，提升国际话语权和规则制定权，此后中国区块链标准化建设不断提速。2017年首个国家区块链标准立项，2020年以来已有2项新的国家区块链标准获批立项，5项地方标准及9项团体标准发布。针对区块链标准化缺乏统一协调机制

问题，国家区块链标准化委员会正在组建。2019 年 11 月，国家标准委宣布新建区块链和分布式记账技术标准化技术委员会，2020 年 5 月已完成委员名单公示。

区块链标准化关乎话语权之争，国际竞争异常激烈，未来中国应进一步加强区块链标准化人才培养，有重点地加速推进区块链标准化建设；选择重点领域开展应用示范，推进产业良性发展；积极跟踪国际区块链标准化进展，积极参与区块链国际标准制定。

结语
面向未来的数字金融

2015 年，英国《经济学人》杂志首次报道区块链，并将其喻为“制造信任的机器”(The trust machine)。如今，在经历了市场信心的快速膨胀、冷却再到理性的起伏之后，区块链依靠密码学和经济激励手段进而有效实现信任的共识，已经渐入人心。

区块链技术特点与金融业务需求天然契合，加之区块链与人工智能、物联网、云计算、大数据等前沿科技的碰撞融合，在不远的将来，借助区块链，我们或将迎来一副更加开放、更加自由的数字金融新图景：

可信协议、模块化与可组合性，数字金融的基础设施日益夯实。

首先是可信协议。区块链影响金融未来的方式之一就是通过一组组协议来完成征信、授信，实现资金 / 资产在不同主体之间的自由流动，而不需要像银行、信用卡公司、支付宝、微信这样的中介。这不仅是区块链作为信任机器的最直接显现，也意味着，区块链突破了信息互联网的限制，还同时实现了价值互联网和货币互联网。协议的价值也将因此得以放大。协议本是计算机用来通信的消息格式，没有协议，计算机之间无法通讯，网络也就不复存在。协议如此重要，但在互联网的价值分配中，应用占大头，协议只占一小部分。区块链将让协议胖起来。“胖协议”不仅是协议本身更加功能化，而且在价值分配上的所得也更为丰厚。

再来看模块化与可组合性。传统的金融产品本质上是由单一的服务提供商设计的封闭生态系统，如今基于区块链技术的去中心化金融（DeFi）产品却是组合使用的。MakerDAO、Uniswap、Compound 等不同协议既可以单独使用，也可以组合使用。这种模块化金融的方式代表着未来，也是未来开放式金融系统最重要的特征。当然，模块化组合也增大了去中心化金融本身的的系统风险，Lendf.me 丢币、bZx 闪电贷攻击、MakerDAO 零出价拍卖事件都表明，我们的探索仍有大量问题需要解决。

智能合约的自动化执行，数字金融的运行成本将大幅降低。

智能合约是区块链技术的伟大发明，它通过代码对资产和行为赋值并赋予规则，决定了网络中相关资产运作的地点和方式。所有的合约将不依赖于人的意志，按照预定标

准自动执行。因此，区块链不仅是一种技术，更是一种制度安排。这或许是对现代金融体系最大颠覆。它以区块链可编程技术为基础，带来可编程的货币、可编程的资产乃至可编程的生产关系。

更现实一点，聚焦于时间稍短一点的未来，智能合约将使我们避免繁杂冗余的法律关系。例如，自动执行的借贷合同如果已经经过法律的认证和审核，就不需要再经过法院执行。

此外，借助智能合约，区块链可以实现监控比简单付款（包括期权和其他衍生工具）更复杂的金融产品的生命周期。由于它们的衍生性质，无论是场外交易还是场内交易，都要求实时地对市场状况进行监视和跟踪。跟踪数百或数千种产品会消耗大量资源，并且需要大量对账工作。智能合约将使这一些化繁为简。

如今，对智能合约的探索也正与未来的金融科技监管进行融合。监管的灵活性、透明度和监管的要求有望通过智能合约达到形式和实质的统一。

数字资产的被标记化，数字金融的价值流通将更加高效。

当整个世界发生不可避免的数字化，所有的资产也将被数字化。数字化的重点是是资产能够被标记。资产标记化是一个过程：用一个数字标记来表示一个真实的资产或它的一部分，这个数字标记可以追溯到原始资产。

未来的的金融世界将因为所有资产都可以被标记化而实现资产的极大充盈，这包括数万亿流动性极差的房地产市场，也包括古董、艺术品等等，甚至“人”本身也可以作为独特的要素被标记。今年 1 月，NBA 篮网球星丁威迪发起了“个人代币的革命”，通过区块链 Token 发行平台 Securitize 基于以太坊发行了 100 个个人债券代币，每个代币价值 15 万美元，总价值是 1500 万美元，大约相当于他未来 3 年合同总收入 3440 万美元的 40% 左右。

一切只不过刚刚开始。区块链技术的特征将保证被标记的数字资产是真实有效，可分割、可确权的。也能保证整个过程的透明与安全。Securitize、Polymath、tZero…… 许多区块链创业者都已经开始了这场伟大的尝试。

面对区块链驱动的数字金融的未来，才刚刚开始。

尽管许多可能性已经出现，但今天人们还是会被各种各样的名词缠绕，以太坊 2.0、跨链、互操作性、隐私计算……这些词汇终将成为技术黑箱的一部分，所有的技术都将被封装到产品和服务当中，用户只需要按规程操作便可得到预期的输出。

《技术的本质》作者布莱恩 • 阿瑟提出的收益递增理论认为，首先发展起来的技术往往具有占先优势，再通过规模效应降低单位成本，并利用普遍流行导致的学习效应和许多行为者采取相同技术产生的协调效应，致

使它在市场上越来越流行，人们也就相信它会更流行，从而实现自我增强的良性循环。而区块链要变得流行，需要尽快建立属于自己的良性循环。

在区块链驱动金融变革的旅途中，引爆点将在何时、何地以何种面貌出现？

文字仅仅是一些思考和畅想，仍需要我们共同去寻找更多引爆的火种。

致谢

《数字金融应用探索中的机遇和挑战》报告由以下机构共同参与编写：

第一章：区块链技术驱动金融，分别由欧科云链研究院、火星区块链研究院共同起草；

第二章：区块链应用落地：赋能金融创新，分别由分布式资本、Longhash、欧科云链研究院、NGC Ventures、币安中国研究院、标准共识共同起草；

第三章：区块链技术演进：重塑金融未来，分别由 IOSG Venture、标准共识、币安中国研究院、IOSG Venture、共识实验室联合起草；

第四章：数字金融创新与全球监管政策，由币安中国研究院主要起草。

报告编委会成员包括（按首字笔画排序）：王峰、邓鹏、任铮、江金泽、谷涛、李炼炫、陈怀远、肖锐、杨钰莹、林锦周、姜陆洋、徐江、黄凌波、夏晴天、蔡彦等。

在此，向以上机构的大力支持和各编委会成员的辛苦付出，一并表示最诚挚的感谢。

火星区块链产业研究院

《数字金融应用探索中的机遇和挑战》报告编委会

2020 年 7 月

参考资料

［1］ *Bitcoin: A Peer-to-Peer Electronic Cash System Nakamoto*，Satoshi，2008

［2］ *A Next-Generation Smart Contract and Decentralized Application Platform*，Vitalik Buterin，2013

［3］《比特币的技术：原理与经济学分析》，凌清，复旦大学，2014 年

［4］《比特币的理论、实践与影响》，贾丽平，国际金融研究，2013 年

［5］《区块链技术驱动金融：数字货币与智能合约技术》，阿尔文德·纳拉亚南（Arvind Narayanan），约什·贝努等，中信出版社，2016 年

［6］《区块链金融》，深圳前海瀚德互联网金融研究院，中信出版社，2016 年

［7］《区块链：重塑新金融》，赵增奎，宋俊典，庞引明，张绍华，清华大学出版社，2017 年

［8］《FinTech+：金融科技的创新、创业与案例》，王阳雯，经济管理出版社，2018 年

［9］《数字金融：数字科技创造金融服务新价值》，京东数字科技研究院，中信出版社，2019 年

［10］《中国的数字金融发展：现在与未来》，黄益平，黄卓，北京大学经济学（季刊），2018 年

［11］《数字化金融：人工智能、区块链、云计算、大数据与数字文化》，约翰·贝斯特（John Best），人民邮电出版社，2019 年

［12］《区块链金融：技术变革重塑金融未来》，刘洋，北京大学出版社，2019 年

［13］《区块链新时代：赋能金融场景》，巴曙松，科学出版社，2019 年

［14］《数字化信任—区块链的本质与应用》，赵刚，电子工业出版社，2020 年

［15］《金融基础设施、科技创新与政策响应——周小川有关讲座汇编》，杨燕青，周徐，中国金融出版社，2019 年

［16］《中国数字金融发展报告》，西南财经大学互联网金融研究中心，2018 年

［17］《鼓励金融科技创新的监管工具：国际实践中的创新中心与监管沙盒》，法伊基什彼

得（Fykiss Pter），金融与经济评论，2019 年

［18］《区块链供应链金融》，段伟常，电子工业出版社，2018 年

［19］《基于区块链的智能合约技术与应用综述》，贺海武等，《计算机研究与发展》，2018 年 11 月

火星区块链

火星区块链以激励人人创造价值及分享价值为理念，聚焦区块链技术和产业创新发展，面向区块链从业者，专业从事区块链技术与应用资讯、行情数据、数字矿业、数字金融服务及区块链应用研究，力图将区块链信息服务与金融服务相结合，打造面向未来的数字经济基础设施。

目前，火星区块链旗下拥有火星财经、火星云矿、火星交易大师三大产品及服务，覆盖媒体资讯、算力服务及投资顾问工具等业务，现已服务用户数量超300万，连接国内区块链技术及应用型企业超6000家。共识实验室系火星区块链生态旗下的专业投资及研究平台。

火星区块链现有员工技术及产品岗位占比超45%，内容及运营岗位占比约35%。团队核心管理成员来自腾讯、华为、IBM、摩托罗拉及金山等知名公司，大多拥有计算机、软件、金融、经济及传媒等相关专业背景，研究生及以上学历占比超40%。

公司由蓝港互动（HK.8267）创始人王峰先生于2018年2月发起成立，现已获得IDG资本、策源资本、泛城资本等多家知名机构投资。2019年9月，火星财经获币安、Matrixport投资，估值达2亿美元。

火星财经
区块链信息资讯
服务平台

火星云矿
一站式实体矿机算力
服务平台

火星交易大师
数字资产管理及投资
服务平台