中国区块链发展回顾与前瞻（2019）

作者：姚前 YaoQian出版时间：2019 年 08 月

摘要：

本报告从现代密码学的演进脉络追溯数字货币的发展过程，回顾区块链技术的缘起，指出非对称密码算法解决了开放系统中密钥大规模分发的问题，并带来独特的认证功能；而哈希函数具有快速收敛、不可逆、无须耗费巨大计算资源等优势，两者为数字现金的加密、签名和自主开户奠定了基础。比特币则是通过分布式共享账本与工作量证明机制的创新设计，防止去中心化条件下数字现金的“双花”，开创了价值交换技术——区块链技术。本报告还从系统架构、会计学、账户、资产交易、组织行为学、经济学六个维度，对区块链技术进行解读，指出区块链技术具有难以篡改、自由开放、数据高度可信任、容错性强优秀特质，但存在性能问题、隐私保护、安全问题、治理缺失、互操作性问题的不足。本报告最后从共识机制与性能、跨链、治理机制、身份管理、隐私保护、数字钱包、智能合约与自组织商业模式、与其他科技的融合八大方向，对区块链技术的未来发展进行前瞻思考。

关键词： 加密货币区块链非对称加密哈希算法

Abstract：

This Article first examines the root of the blockchain technology from the perspective of the historical development of modern cryptography. Foundations of the encryption，signature and independent access features of digital currencies could be found in developments in asymmetric cryptographic algorithm，which gave rise to new solutions to large-scale key distribution in open systems as well as distinctive verification functions，and hash algorithms，which brought benefits in rapid convergence，irreversibility and low energy consumption. Bitcoin successfully achieved the prevention of double spending in decentralized environments by integrating the Proof-of-Work consensus mechanism to a shared distributed ledger and thereby gave birth to the blockchain technology. The Article then moves on to analyze the blockchain technology from system architecture，accounting，account system，asset transaction，organizational behavior and economics perspectives，and identifies its main benefits （tamper-proof，open access，high data trustworthiness，high fault tolerance） and shortcomings （performance，privacy protection，security issues，lack of sound governance and low interoperability）. Last but not least，the Article looks at what blockchain would look like in the future in terms of consensus mechanism and performance，cross-chain interoperability，governance，identity management，privacy protection，digital wallet，smart contract and Decentralized Autonomous Corporation （DAC） models as well as blockchain’s interaction with other emerging technologies.

Keywords： BlockchainCryptocurrencyAsymmetric CryptographyHash Algorithms

自 2009 年比特币问世以来，数字货币[1]的数量不断增长，从主流币到稳定币，热点不停地切换。根据 Coinmarketcap 的数据统计，截至 2019 年 5 月底，全世界共有 2212 只数字货币，总市值为 2650 亿美元。其中，比特币的市值占比最高，在 2017 年初一度达到 90%，随后由于其他数字货币爆发式增长以及比特币价格下跌，比特币的市值占比下滑，但至今基本维持在 50%的水平。接着为以太币、瑞波币、比特币现金等其他数字货币。在一定程度上，数字货币总市值与比特币价格呈正相关关系。如果按照融资额来统计，数字货币融资额在 2018 年占全球股票首次公开发行融资额的 9%以上。比特币价格与加密资产

市值的走势见图 1。各类加密资产的数值占比见图 2。ICO 融资规模见图 3。基于不同货币的比特币成交额见图 4。

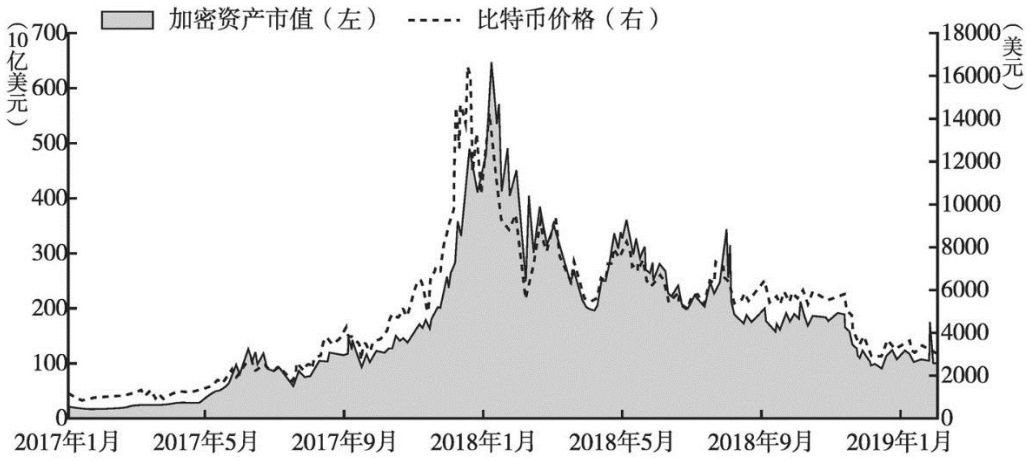

图 1 比特币价格与加密资产市值的走势

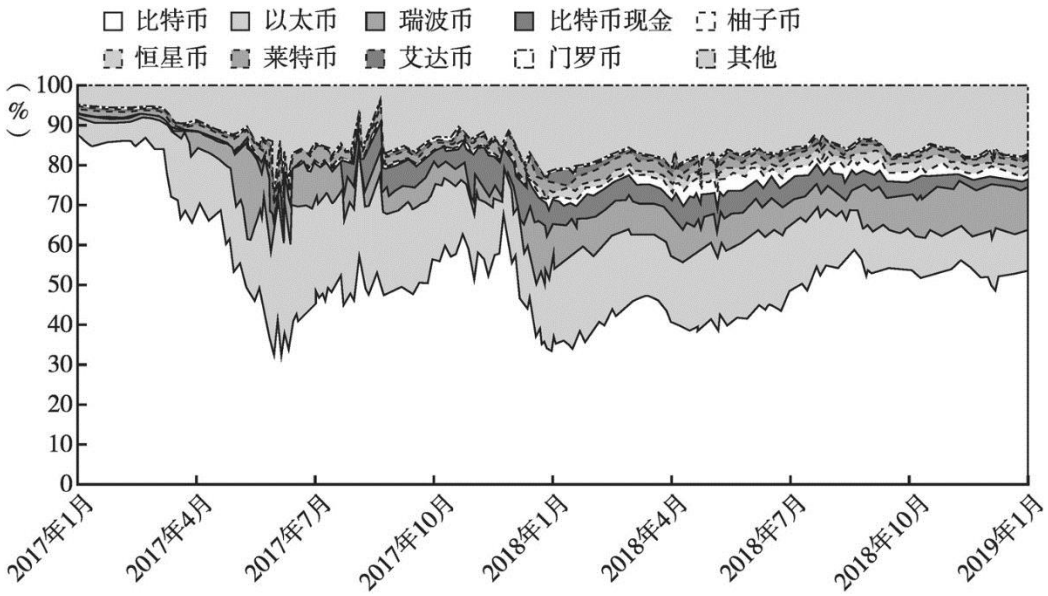

图 2 各类加密资产的数值占比

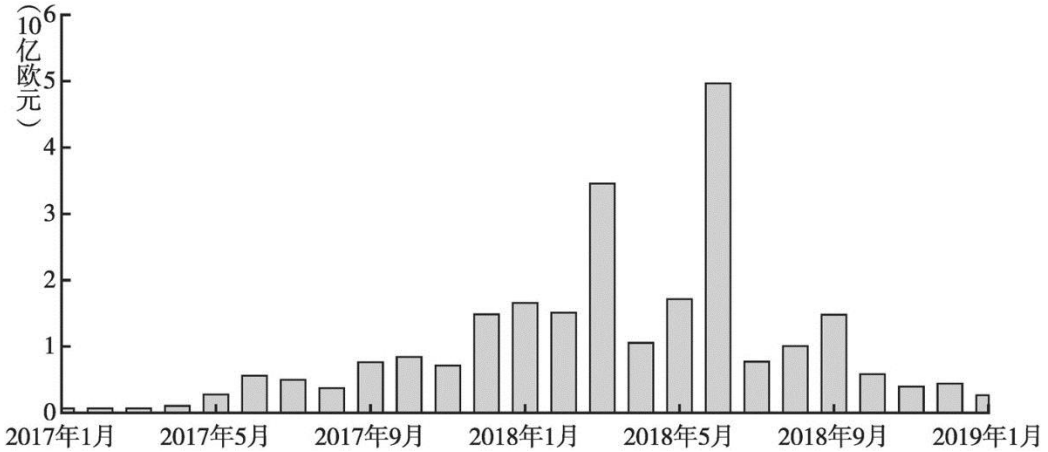

图 3 ICO 融资规模

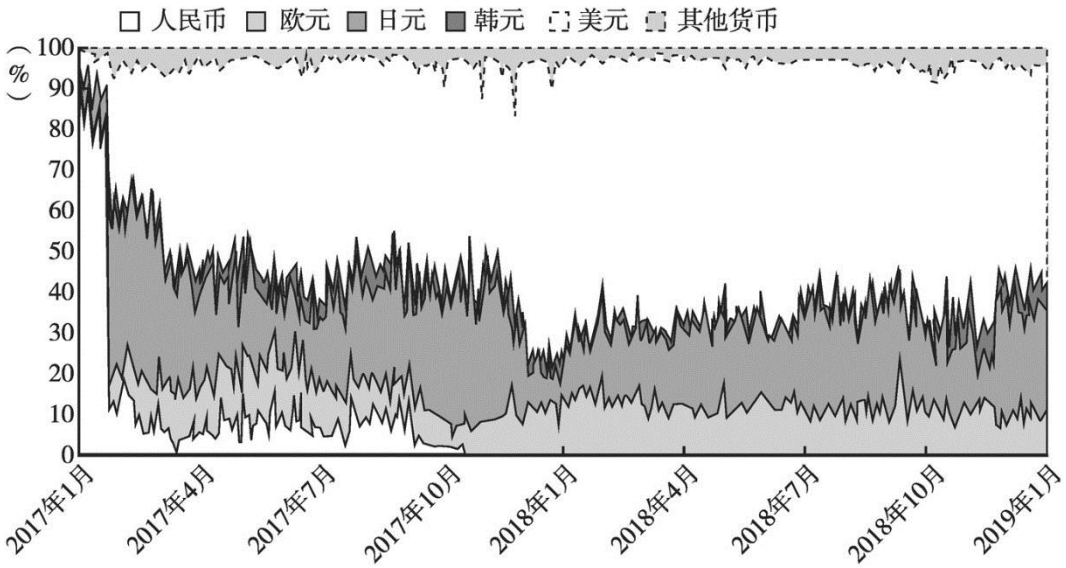

图 4 基于不同货币的比特币成交额占比

当前，各国对数字货币的本质并未形成一致的看法，有的将其视作货币或者支付工具，有的将其界定为特殊的商品，也有一些国家倾向于将其界定为证券。但无论如何，各国对于数字货币的底层技术——区块链技术的发展潜力高度重视。有人认为，区块链技术是继大型机、个人电脑、互联网、移动互联网之后计算范式的第五次颠覆式创新，是新一代云计算的雏形，有望像互联网一样彻底重塑人类社会活动形态，实现从目前的信息互联网向价值互联网的转变[2]。

本报告将从现代密码学的演进脉络追溯数字货币的发展过程，回顾区块链技术的缘起，提出理解区块链技术的六个维度，并剖析区块链技术的优秀特质与不足之处，最后对其未来发展方向进行前瞻思考。

一 现代密码学演进

罗马非一日建成。想准确理解区块链技术的缘起，我们需要回到 40 多年前以研究现代密码学的发展历史。现代密码学的一个革命性突破是解决对称密码算法无法在大规模的信息加密传输中普及的问题。对称密码算法是指加密和解密共用一个密码，也称单钥密码算法。它的最大缺陷是，信息发送方必须和每个接收方约定好对称密钥，这样在密钥的大规模分发过程中，无法有效防止密钥被窃取或者被人攻击，也不太容易去管理那么多的密钥。

对此，1976 年，Diffie（迪菲）和 Hellman（赫尔曼）提出了新的思路，他们将原来的一个密钥分成一对密钥，一个密钥用于加密，另一个密钥用于解密。加密密钥公开，称为公钥。解密密钥不能公开，唯独本人秘密持有，不能让别人知道，称为私钥。如果张三想给李四发信息，张三要用李四的公钥对信息进行加密，那么只有李四的私钥才能解开，其他任何人都解不开。同样，李四想给张三发信息，要用张三公开的公钥进行加密，而只有

张三手上有的那把私钥才能解开加密后的信息。这样的思路就很好地解决了单密钥体系下的密钥大规模分发的问题。这就是非对称密码机制的思想。1978 年，Rivest（李维斯特）、Shamir（萨莫尔）和 Adleman（阿德曼）提出著名的 RSA 密码算法，首次实现了非对称密码算法。

非对称密码算法除了解决开放系统中密钥大规模分发的问题外，还带来原来对称密码体制不具备的功能，那就是非常独特的认证功能。比如，如果张三想给别人发信息，那么张三不仅用别人的公钥对报文进行加密，同时还可用张三的私钥进行签名，这样别人就可以用张三的公钥进行验签，判定报文是不是由张三发出的。认证功能的出现使信息加密传输形式发生革命性的变化：信息既可以加密，也可以签名，就像支票一样，信息的加密传输有了抗抵赖的功能。所以说，非对称密码机制的实现是密码学的一次重大革命，密码学的应用因此从军事领域走向民用领域。

哈希算法是现代密码学的又一个飞跃。它也叫“安全散列函数”，最早的 SHA 哈希算法由美国国家安全局设计，于 1993 年发布。2010 年，中国国家密码管理局公布中国商用密码哈希算法标准：SM3 密码哈希算法。

哈希算法又称信息摘要，众所周知，文章摘要是对文章内容的概括总结。通过文章摘要，我们就能理解文章的大部分意思。哈希算法也有这样的功能，它可以把任意的信息集，用非常简单的信息予以描述。它是一个特别的数学函数：给定输入很容易得到输出，但是从输出计算输入不可行。这就像从全文得出摘要很容易，但要根据摘要把全文再重写一遍就很不容易了。此外，哈希算法还有一个有意思的特性，只要原始信息稍微发生变化，摘要就变得完全不一样，这一特性非常有用。

与对称加密算法和非对称加密算法不同，哈希函数是一种快速收敛的算法，从输入到输出的计算非常快，迅速收敛数值，无须耗费巨大的计算资源，而从输出倒推输入又几乎不可行。基于这样优秀特质，哈希函数得到广泛的应用，我们习以为常的人民币冠字号码即由哈希算法产生。在数字货币领域，哈希算法常常被当作数字货币交易挖矿、交易区块链接以及钱包地址压缩生成的工具，得到广泛的应用。

二 数字货币的中心化与去中心化：区块链技术的缘起

长期以来，密码学家有个想法，既然邮件能够加密、签名发送出去，那么手里的现金能不能像邮件一样，加个数字信封，进行加密和签名后，从一端发送到另外一端？这就是最早的数字现金思想的由来。随着现代密码学的发展，数字现金的技术实现逐渐成为可能，引起许多密码学家的广泛兴趣。

1982 年，David Chaum（大卫·乔姆）在顶级密码学术会议——美密会议上发表了一篇论文《用于不可追踪的支付系统的盲签名》。论文中提出了一种基于 RSA 算法的新型密码协议——盲签名。利用盲签名构建一个具备匿名性、不可追踪性的电子现金系统，这是最早的数字货币理论，也是最早能够落地的试验系统，得到了学术界的高度认可。

但 Chaum 当时建立的还是传统的“银行、个人、商家”中心化模式。每个使用过的 E-Cash 序列号都会被存储在银行数据库中，且每次交易系统都要验证 E-Cash 序列号的唯一性，因此系统会维持一个已交易序列号的数据库。随着交易量的上升，该数据库就会变得越来越庞大，验证过程也会越来越困难。

面对中心化数字货币模式的缺陷，2008 年，中本聪发表了经典论文《比特币：一种点对点的电子现金系统》，提出了一种全新的去中心化的电子现金系统，其核心思想之一就是通过对等网络方式消除单个中心化依赖，实现点对点交易；同时，将已花费的数字货币序列号（UTXO）数据库转变成未花费的数字货币序列号数据库，控制数据规模，并利用哈希算法，打上时间标记，纵贯相连。这一底层支撑技术就是我们今天热议的区块链技术的来源。当然，也有人提出早在 1990 年到 1991 年，W.Scott Stornetta 和 Stuart Haber 就提出了区块链的想法。为确保数字文档的精确性，他们认为如果不去信任某个人或者机构，“那就去信任每一个人，也就是说，让世界上的每一个人都是数字文档记录的见证者”。就理念而言，这一思想确实与比特币区块链的思路相通：去中心化的本质就是多中心化——既然没有了权威中心，那么大家都成了中心，但各个中心既须自律亦须他律，彼此之间相互验证，相互制衡，以构造严丝合缝的信任机器。

所以中本聪的区块链技术不仅是“分布式”和“共享”的简单理念，它还综合采用了密码学、分布式数据库（大规模数据存储与处理）、点对点通信（P2P 网络）、共识机制（分布式一致性）等技术进行组合创新。狭义的区块链技术是一种按照时间顺序将数据区块以链表的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系的、能在系统内验证的数据。广义的区块链技术则是指利用加密技术来验证与存储数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上的代码，即智能合约，来保证业务逻辑的自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

三 理解区块链技术的六个维度

第一个维度，从系统架构看，区块链技术是一种全新的信息网络架构。从大型机到个人电脑，再到移动智能终端，互联网技术的进步与应用打破了传统信息系统的相对封闭性，可以说传统的中心化架构过于依赖中心节点，极大制约了客户端的自主性和灵活性；区块链技术则通过巧妙的设计，打开了传统中心化系统的围墙，模糊化了客户端和服务器端的边界。各节点既可以是客户端，也可以是服务器端。这使 C 端客户的自主掌控能力及其在系统中的话语权得到极大的增强，信息网络由中心化架构进入以 C 端为主的平权时代。

第二个维度，从会计学角度看，它是一种全新的分布式账本技术，采用了全新的记账方法：每个人都可以参加，只要按照要求，达到选举规则的设定目标，就可以获得记账权，成为新区块的记账人，所有参与者共有、共享账本信息，都能检测、验证账本信息。与传统账本技术相比，DLT 账本技术的优势在于：不易伪造，难以篡改，效率高，可追溯，容易审计；通过交易签名、共识算法和跨链技术保障分布式账本的一致性，自动实时

完成账证相符、账账相符、账实相符；从技术可行性看，基于自动化执行、实时记账又能实现全局一致性的 DLT，瞬时的资产负债表编制或将成为可能[3]。

第三个维度，从账户角度看，它是全新的账户体系，传统上我们所有的金融业务都是围绕商业银行的账户开展的，而现在，私钥本地生成，非常隐秘，从中导出公钥，再变换出钱包地址，自己给自己开账户，不需要中介，这在金融史上是一个非常重大的变化：一是用户可通过数字身份运用安全技术对金融资产进行自主控制；二是用户点对点之间进行金融资产交易，可以独立于任何第三方服务机构；三是用户对数字身份的保管，直接承担交易责任，自金融模式由此应运而生。

第四个维度，从资产交易角度看，它是一种全新的价值交换技术，既可采用 UTXO 模式，通过构造包含解锁脚本和锁定脚本的交易输入和交易输出，完成“未花费交易输出”的转移，也可采用传统的 Account 模式。UTXO 模式和 Account 模式可相互转化，通过聚合归纳（Reduce），UTXO 可转化为账户余额，而对账户余额进行拆分则可得到 UTXO 的结果[4]。基于这一价值交换技术，我们可以创造一种全新的金融市场模式：去中心化资产交易[5]。

第五个维度，从组织行为学角度看，它是一种新型的去组织化的分布式协同生产活动，它通过激励相容的算法规则和契约安排，明确了各方的经济利益，充分调动了各方的积极性，使有效的分布式协同生产真正成为可能，出现了新型的组织形态——自治去中心化组织（DAO）：没有董事会，没有公司章程，没有森严的上下级制度，没有中心化的管理者，去中心化、去权威、点对点平权等，完全颠覆了人们通常脑海里的企业印象。不少人惊叹，企业正在被消解。这是经济活动组织形式的变革[6]。

第六个维度，从经济学角度看，它开创了一种新型的算法经济模式。建立在区块链技术的算法经济以去中心化、开放为特征，强调和尊重市场交易的自愿原则，发挥市场价格的统筹协调机制。在经济自由度上，兼具计划和市场两种机制的优点，是一种更加接近自由市场的经济模式[7]。

四 区块链技术的优秀特质与不足之处

（一）优秀特质

一是难以篡改。以比特币为例，掌握了 50%以上的全网算力，才有可能篡改链上的数据。目前比特币的全节点数目上万个，遍布世界各地，在一定程度上保障了系统的不间断连续运行。

二是自由开放。任何人都可以竞争记账权或者加入某个矿池参与挖矿，只要挖矿成功，谁都可以获得奖励。这在传统的相对封闭的信息系统几乎不可能，比如某人买了一台计算能力很强的服务器，想为腾讯服务，可能吗？不可能，一般机构绝对不可能让其他人随便加入系统，参与它的运行。作为自由开放的体系，比特币欢迎任何人带着算力参与记账权竞争。从技术演进角度看，这是一个重大的进步。

三是数据高度可信任。数据的难以篡改带来了数据的可信，可信的结果是我们可以基于这些可信数据，进行多方面的应用和交易，比如智能合约。实际上，智能合约是区块链数据上的应用小程序，在不能保障数据可信的情况下，这些应用小程序是无法运转的。应该说，区块链技术的出现使智能合约的应用真正变成可能。

四是容错性强。区块链技术通过共识算法保持各节点数据的高度一致，每一个全节点都会维护一个完整的数据副本，如果某个节点遇到网络问题、硬件故障、软件错误或者被黑客控制，则均不会影响系统以及其他参与节点。问题节点在排除故障并完成数据同步之后，便可以随时再加入系统中继续工作。由于整个系统的正常运转不依赖个别节点，因此每个节点可以有选择地下线，进行系统例行维护，同时还能保证整个系统的 7×24 小时不间断工作。

（二）不足之处

一是性能问题。区块链技术的理念之一是分布式共享，但假设近万个节点都要共享数据的时候，速度自然就慢下来，效率不高。目前比特币的成交至少要等 10 分钟，有时候要等 1 个小时以上，这是许多人不能容忍的。

二是隐私保护。比特币的整个账本是公开的，但如果有些人/机构不愿意自己的资金交易被全网看到，尤其是大额交易，那么该如何处理？隐私保护成为区块链技术的一个研究热点，一些解决方案已经出现，比如零币。

三是安全问题。目前，智能合约还处于初级阶段，一旦有漏洞，就会被人攻击，出现重大的风险。比如 The DAO 被黑事件，黑客利用 The DAO 智能合约的安全漏洞，从合约管理的 ETH 中划走 360 万个 ETH。

四是治理缺失。当社区面临重大决策事件时，让社区参与进来，以某种机制形成社区意见，最终在区块链上表达出来。这些决策可能是不同的技术升级提案，也可能针对 The DAO 这样的突发事件，或者有关该区块链某些基础规则的调整。如果缺乏治理机制，就只能通过软分叉或者硬分叉解决问题，最终将导致混乱和分裂[8]。

五是互操作性问题。互联网以通用的 TCP/IP 协议作为基础来实现互联互通，而区块链作为新一代价值互联网并没有通用的协议，目前都还是社区自组织模式，跨链互操作没有统一的规范，在很大程度上限制了应用创新。

五 区块链技术前瞻：八大方向

（一）共识机制与性能

共识协议用于在分布式系统中实现可用性与一致性，是区块链的关键技术，其核心指标包括共识协议的强壮性（容错、容恶意节点的能力）、高效性（收敛速度，也即系统达成一致性或“稳态”的速度）及安全性（协议抽象理论模型的安全界）。代表性协议包括以 PBFT 为代表的 BFT 类共识、以 PoW/PoS 为代表的中本聪共识（Nakamoto Consensus）、新型混合共识等。目前来看，共识协议最大的难题在于如何实现安全性与高效性的平衡。

在保障安全性的前提下，大概有四种提高效能的思路。一是硬件和算力的改进，从CPU、GPU、FPGA 到 ASIC，挖矿设备不断升级，同时计算机整体算力水平也在快速提升，根据 OpenAI 的分析，自 2012 年以来，人工智能训练任务中使用的算力呈正指数级增长，其目前速度为每 3.5 个月翻一倍（相比之下，摩尔定律是每 18 个月翻一倍）。倘若算力突破一定临界点，目前区块链的性能问题可能就不再是问题。二是不改变共识协议的系统改进，代表性方法有缩短区块的产生间隔、增加区块大小、采用双层链结构、引入闪电网络、改变区块+链的基本结构、修剪区块中的数据以及改进算法。三是新型数据结构，比如，采用有向无环图（DAG）数据结构，典型项目有 IOTA 和 ByteBall。四是新型共识协议，比如研究者们提出 PoW 机制的 Thunderella 算法、PoS 机制的 Algorand 协议和 Ouroboros 算法、基于 Sleepy Model 的 PoS 共识、空间证明机制（Proof of Space）等新型算法。

（二）跨链

现在有各种链：公链、联盟链和私有链。公链为大众服务，联盟链局限于一个联盟，私有链仅服务于某一个私人机构。从私有链、联盟链到公链是去中心化的过程，而从公链、联盟链到私有链则是中心化的过程。在这些转变过程中，会出现不同的为私有链、联盟链、公链服务的各种区块链产品。那么，当不同机构之间业务发生交互时，不同的链与链之间怎么交互，则成为很大的难题。目前有三种跨链技术：公证人机制（Notary Schemes）、侧链/中继（Sidechains/Relays）、哈希锁定（Hash-locking）技术。跨链技术是下一步区块链技术发展的重点。

此外，目前私有链存在谁加入谁的博弈难题，彼此都希望对方加入自己的区块链系统。虽然 BaaS（Backend as a Service，后端即服务）能够复用底层的技术平台，但关键是不同业务系统数据和用户的打通，以及业务系统之间的协同工作。倘若不同系统之间没有联通，就无法复用客户、资产、数据等基础资源。解决的思路可能有两种：一是政府或标准化组织推动区块链技术的标准化和规范化，增强不同系统间的互操作性；二是政府建设公共服务平台，比如香港金管局推动的 HKTFP 即为典型，此类模式的优点在于，基于公共利益而建设的平台可以较好地解决建设主体和治理机制的纷争，打通用户、场景和公共服务，实现资源整合，而且也便于政府监管，提升监管效率。

（三）治理机制

由于区块链本身即一种天然投票系统，包含更改验证程序集或更新其自身规则所需的一切逻辑，而且投票结果可自动进行，链上投票机制自然就成为区块链生态系统的首选治理机制。目前有不少链上投票机制探索，比如 EOS、NEO、Lisk 等系统中的委任权益证明（DPOS）机制，通过链上投票来决定运行网络的超级节点由谁操作；或者对协议参数进行表决，来决定以太坊的 Gas 上限；或者用来表决协议升级，如 Tezos。目前链上投票机制存在的不足如下。第一，投票参与度低，这就导致两个问题：一是投票的结果只反映小部分人意见，难以得到普遍认可；二是攻击者只需少量的成本就可左右投票。第二，可能

会出现财阀式的少数人链上治理，损害普通用户利益，目前已有相关事件发生。从技术角度看，如何更好地完善链上治理机制，是下一步区块链技术值得研究的方向。

另外，完全依靠链上治理，尚无法解决区块链生态系统的委托代理问题，还需要法律监管、声誉机制等链下治理的支持。目前，许多国家的监管部门正倾向于将初始代币发行（ICO）的代币界定为证券。为此，证券型代币的区块链系统需要考虑如何将监管部门提出的合规要求内嵌于系统，总体思路是在技术上设置监管接口，为监管者提供客户识别（KYC）、反洗钱（AML）、项目尽调、风险评级、信息披露、风险监测等监管功能。具体实现方案可考虑许可链（服务中心化监管）+公链（支持去中心化应用）的“二元模式”：证券型代币的发行、交易、退出等所有处于监管范围的证券类活动在许可链开展，许可链向相关监管部门注册，接受全面监管；证券型代币的应用则使用公链，开展去中心化商业活动，去中心化应用（Dapp）的创造者自由部署智能合约，并根据自己的选择与其他区块链整合。若有需要，监管者亦可从许可链穿透到公链，管控全局。多链策略既保障了证券型代币的合法合规，同时又不损害去中心化新型经济模式的优势。

（四）身份管理

区块链使自主身份（Self-sovereign Identity）成为可能。它本身可以作为去中心化公钥基础设施（PKI）来使公钥体系更有用和更安全。区块链可被视为去中心化的证书颁发机构，将身份维护映射到公钥。智能合约还可以增加复杂的逻辑，实现撤销和恢复，减轻终端用户的密钥管理负担。这些技术将身份的所有权从集中式服务推向个体之间端到端服务，并使身份本身可控。这被称为自主身份。这种方法分散了数据和计算，并将其推向了每个个体，对于黑客来说，其经济上的价值较低，因为需要大量的努力才能一个接一个地攻击许多个人身份。

在联盟链中，需要对不同节点分配不同的权限，并满足一定的可监管性要求，为此，需要构建安全高效的身份认证与权限管理机制。可采用基于生物特征识别技术的认证机制，或是高效的、生物特征与密码技术有机结合的认证方案；也可采用高效实用的、基于身份/属性的密码方案，实现对节点/用户的细粒度访问控制/权限管理。

（五）隐私保护

在传统的中心化模式下，由于技术不对等，个人用户在企业面前处于弱势地位，企业自身又没有内在激励机制以对个人数据进行“匿名化”处理，从而造成个人与企业在数据权利之间的冲突无法得到真正解决，个人隐私被侵犯事件屡屡发生。区块链技术的出现则创造了一种全新的不依赖中心、多方共享环境下基于密码学、用户自主可控的隐私保护模式：用户无须让渡数据权利，自主可控地对个人数据匿名化[9]。例如，用户自主产生本地公私钥，通过公钥计算发布有效的钱包地址，来隔断钱包地址和钱包持有人真实身份的关联，并通过控制私钥在区块链网络自主完成交易。

基于先进密码学技术的隐私保护方案有：通过采用高效的零知识证明、承诺、证据不可区分等密码学术语与方案来实现交易身份及内容隐私保护（例如：Zcash 中采用了 zk-

SNARK 来实现隐私保护机制）；基于环签名、群签名等密码学方案的隐私保护机制，基于分级证书机制的隐私保护机制也是可选方案（例如：Monero 采用了环签名方案来实现隐私保护机制，Hyperledger Fabric 采用分级证书机制来实现隐私保护机制）；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护（例如：Ripple 通过采用安全多方计算方案来实现交易通道的隐私保护）；还可采用混币机制实现简单的隐私保护。

（六）数字钱包

目前数字钱包都在尝试从单纯的钱包服务转向数字资产生态入口，希望借此获取更大的市场份额，发展更丰富的资产管理服务，主要有资产管理、资产交易、信息聚合、Dapp 分发等方向。其中，资产管理可以细分为挖矿增值、理财增值、资产归集管理等方向；资产交易主要有去中心化数字资产兑换和法币汇兑等；信息聚合主要是交易所信息及项目信息聚合；Dapp 分发类似于小程序商店。尽管不同钱包的切入点和发展路线各不相同，各有所长，但由于彼此间的长远目标是渐进趋同的，各类钱包的增值功能略有重叠。

随着数字资产产业的不断发展，数字生态环境的不断完善，数字钱包的场景功能将越来越重要。其未来发展重点有三个方面：一是保证钱包服务的安全、开放和便捷；二是围绕资产增值需求，搭建数字资产管理平台，为用户提供丰富的金融产品，提高用户转化率；三是打通数字资产与现实世界的连接，丰富数字资产应用场景，构建数字资产生态。

其中安全是根本。软件技术方面可采用无密钥的密码算法（标准算法的白盒化方案或设计新型的白盒密码算法）和代码混淆技术，实现敌手无法提取核心密码和密钥信息；或采用基于口令、身份、生物特征等认证因子的加密算法对密钥进行加密存储；硬件方面则可基于 TEE（可信执行环境）或者 SE（安全环境）安全模块，定制终端设备的技术方案，这是保障数字钱包安全的重要可选方向之一。

（七）智能合约与自组织商业模式

智能合约具有透明可信、自动执行、强制履约的优点。它一旦被部署到区块链上，程序的代码和数据就是公开透明的，无法被篡改，并且一定会按照预先定义的逻辑去执行，产生预期的结果，且契约的执行情况将被记录下来。应该说，区块链技术与其商业应用具有相辅相成、相互促进的关系。建立在智能合约基础上的自组织商业应用，有助于提升区块链技术的价值，使加密经济模式的适用范围和领域不断扩大。虽然从技术角度看，智能合约只是一段编码，但它实质上承载了许多商业逻辑，甚至一个智能合约就代表一个商业模式，具有无限的想象空间。而反过来，自组织商业模式的实现，也需要智能合约的精巧设计，同时还需要性能提升、安全增强、隐私保护等配套相关技术安排。换言之，这既是一个商业模型的创造，又是一个技术系统的设计。

智能合约的安全性至关重要。由于智能合约的开放性，其代码和内容均可通过公开方法获得，在很大程度上可以让黑客进行合约分析并针对弱点进行攻击；一旦攻击成功，将造成重大损失，因此，迫切需要完善智能合约检测技术，在合约上链之前进行检测，定位

并排除漏洞。当前已经出现了不少智能合约检测工具或在线检测站点，但这些检测仍基于经验总结，对于未知合约漏洞则无能为力。形式化验证方法是一个可能的解决思路，通过建立恰当的模型，精确判断程序是否能按照开发者的预期运行。但对于智能合约的形式化验证难度较大，目前还没有找到合适的解决方案，需要进一步深入研究。

在智能合约的应用方面，一方面，需要从法律层面明确智能合约的可执行性；另一方面，由于智能合约具备天然的确定性，不具有普通合同的灵活性和可选择性，因此在特定场景中，需要建立允许代码暂停或终止执行的干预机制。

（八）与其他科技的融合

常说的云计算、大数据、人工智能、区块链技术等，实质上均是“算法+数据”的体现，无非侧重点各有不同。既然本质相通，那么相互之间的融合就是必然了。例如，在资产证券化的场景中，需要对底层资产的信息进行持续的披露，同时还需要实现大规模分布式文件存储。区块链技术可以通过交易签名、共识算法和跨链技术，保证各交易相关方分布式账本的一致性，在保障交易背景真实性的基础上，自动实时完成信息披露，从而实现账证相符、账账相符、账实相符，大大提高可交易产品的信用等级，大幅降低成本，这就使信息使用者可以实时、穿透式获得企业运营的全局信息，而全局信息的获取意味着信息的大规模增长，如何更好地存储与提取信息价值则成为关键[10]。因此，将区块链技术与分布式文件系统、大数据分析、云计算、人工智能等科技进行融合是未来发展的一个重要方向。