来源：cbdio.com

国内外区块链发展几乎同时起步，从全球来看，全球区块链发展正从全面否定与全面推崇的感性认识趋于理性认识，国外内都更加专注于探索区块链潜在的应用价值和商业模式。然而，国内外针对区块链技术的发展重点、部署策略和研发过程都有所不同。

区块链典型关键技术

区块链并不是作为一项全新的技术而存在，相反，它是分布式系统、加密算法、数字签名、共识机制、智能合约等多种技术的集成体。与比特币等加密货币不同，区块链本身的创新之处在于技术融合。当前，区块链技术仍然处于高速发展阶段，技术创新不断实现，技术侧重点主要体现在以下几个方面：

1.分布式账本技术

区块链系统中的区块就像一个个电子账单，记录着所有节点的交易信息。每个区块的数据都存储在各用户的客户节点中，所有节点共同构成了一个安全可靠的分布式账本。即使其中任意节点的数据被销毁，整个系统的账本正确性都不会受到影响。整个系统具有高度的透明性和开放性，除对交易各方的私有信息进行加密外，会将可共享信息面向所有人公开，并可通过开放接口查询到公开数据。

2.点对点传输技术

点对点传输技术也称为对等网络，是TCP/IP的一种通信体系结构。采用点对点传输技术后，相互连接的节点都处于平等地位，节点可直接连接且自由进出，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中的节点来共同维护。

3.密码学应用技术

区块链系统采用多种密码学原理进行数据加密及隐私保护，尤其是非对称加密算法和哈希散列算法（同电子签名的主要技术），有效实现身份认证与数据防篡改。

4.共识机制技术

共识机制又称为共识算法，是区块链系统中各个节点达成一致的策略和方法，所谓共识指，就是指分布式节点在信息传输过程中可以保持常见的有POW、POS、DPOS、PBFT、DAG等数十种算法，系统可根据不同的应用场景、系统情况来灵活选择。

5.智能合约技术

智能合约是运行在区块链数据库上的应用程序，在满足预设条件时可以自动执行。智能合约取代了法律明文，以代码的形式定义了承诺条款的合约，合约内容不能修改。合约的参与双方将达成的协议提前安装到区块链系统中。在双方约定的内容完成后，开始执行合约。其最大的优势是利用程序算法替代人为仲裁和合同执行。

区块链关键技术发展现状

虽然，世界各国都在争相布局区块链，开辟国际竞争的新赛道，抢占新一轮产业创新的制高点以提高自身国际竞争力，但无论是国内还是国外，在区块链发展道路上都是在摸索前行，从区块链底层、中间层、应用层来看：

1.底层关键技术

包括BFT共识算法、原子跨链技术、子链技术等。其中，BFT共识算法：国内未形成自主可控算法，多在开源代码上优化调整。如趣链、井通都采用RBFT算法，但策略略有不同；原子跨链技术：国内外同步探索，虽国内部分企业产品已稳定运行，但性能效率，稳定性、应用性远差于国外同行。如迅雷网欣的Relay中继技术、上海火昱的合约跨链技术；子链技术：国内企业除杭州秘猿、上海链景外，几乎无探索子链技术，国外多采用分层设计思路实，能通过部署高安全性的主链来保障子链安全性，又能用子链来提高主链的处理速度。

2.中间层关键技术

包括哈希锁定、分布式私钥控制、隐私数据授权访问等。哈希锁定：国外研究较早，也有相对成熟的产品出现；国内机构虽也有实现，但没有大规模的应用检验。分布式私钥控制：国外技术相对完善，国内安全性、可靠性稍显不足；隐私数据授权访问：国内企业研究较早，但基于国密的隐私数据授权访问还未在区块链上大规模推广应用。

3.应用层关键技术

包括分布式应用、智能合约等。智能合约：以Solidity、JavaScript、Wasm、Move等为主，都为国外主导的智能合约语言，国内未形成自主智能合约语言。分布式应用：国内DApp、DeFi技术相对成熟，类型远比国外丰富，已关注到电子发票、电子存证、保险、司法等领域。如腾讯科技、东港股份的电子发票、蚂蚁金服的杭州互联网法院等。

区块链关键技术发展总结

综合来说，国内外对区块链的研究、探索和应用几乎同时起步，国外侧重于BFT共识算法、原子跨链、子链等底层关键技术。国际巨头将区块链作为核心战略进行布局，不断提供人财物力，集聚全球资源打造开源社区，输出原创技术和开源产品，影响和主导行业发展方向和路径。国内侧重于哈希锁定、分布式私钥控制、隐私数据授权访问等中间层关键技术，以及分布式应用、智能合约等应用层关键技术。

然而，国内在区块链创新上缺少动力，又欠缺资金投入，且高度依赖国外开源软件产品，虽应用探索多于国外同行，但对于行业影响力不足。区块链涉及的各类关键技术，严重依赖国外开源软件项目，国内虽借鉴并有所创新，但无法影响其技术路线，未形成自主可控算法和技术，且性能效率，安全性、稳定性远差于国外同行，存在较大的安全隐患。

（作者：相里朋，工信部电子五所）