区块链的现状、发展和未来

16340305

郑先淇

区块链在最近两年着实大火了一把。

就在几年前，很多人似乎都还听都没有听过区块链这个概念，短短的两三年，区块链这个词汇就好像插上了翅膀，不管是真正对其有所研究的人，亦或是就是单单听闻过这个词的人，林林总总，说区块链技术现在在IT领域是家喻户晓的，我觉得丝毫不过分。

对于很多人来说，认识区块链的契机可能在于比特币的大火和炒币、挖矿的的盛行吧。

所以这里我们先来讲一下与比特币的一些事情。2008年金融危机，全世界大多数国家都遭遇了重大的挫折，就是在这个时候，一个化名为中本聪的科学家发表了一篇论文： 《比特币：一种点对点的电子现金系统》。但是这篇论文发表的初期，好像并没能够引起人们的关注，在相当长的一段时间里，对比特币感兴趣的人可谓是寥寥无几。但是，从13年起，比特币就慢慢地火起来了，关注的人越来越多，渐渐地也吸引了一些业界的大佬的关注。随着关注的人越来越多，人们对比特币的认识也越来越深刻，这时候作为比特币底层技术支撑的区块链技术引起了人们的重视，人们惊奇地发现，区块链技术相比于比特币，存在着巨大的发展潜力，区块链能带来的，或许是一场能改变当今社会生产关系的巨大革命。

那么区块链是什么呢？简而言之，区块链是一种去中心化的分布式账本数据库，其拥有去中心化、匿名性、可追溯性、稳固性和安全性等特点。当然区块链也并不是完全意义上的去中心化，也有可能是弱中心化、多中心化。为什么说区块链技术能改变的，或许是社会的生产关系呢？个人认为这是由区块链的特质决定的。区块链的特质解决的，是经典的信任问题。退一步说，即便算不上真正完全解决了信任问题，但是至少对于我们当今的生产关系来说，区块链技术对信任问题的解答，无疑是一种极为重大的进步。区块链涉及的技术很多，包括非对称密码学、P2P网络、共识机制等等。本篇文章主要谈论区块链技术的现状、发展和未来，限于篇幅，技术方面并不详细展开，还请读者谅解。这篇文章主要从以下三个方面进行论述，分别是区块链的发展、区块链的应用和区块链的挑战。

区块链的发展可以归结为3个阶段：区块链1.0,、区块链2.0和区块链3.0。区块链1.0的主要特征是可编程数字加密货币体系，最具代表性的是比特币系统；区块链2.0的主要特征是可编程的金融系统，目前尚无代表性应用；区块链3.0以可编程社会为主要特征，目前尚无代表性应用。个人认为，区块链的发展目前处在1.0和2.0阶段，以数字加密货币和区块链平台应用为主。值得一提的是，所谓的1.0、2.0和3.0阶段并不是一个循序渐进的过程，而是三个平行发展的过程。举例来说，虽然目前区块链已经逐渐开始进入2.0阶段，但是区块链1.0阶段仍旧极不成熟，还有很大的发展空间，所以我们说三个阶段是并行发展的过程。

关于区块链的应用，时至今日，区块链落地的应用已经有很多了，并且最近的几年里，区块链的应用将会以井喷方式增加。公有链应用以比特币系统和以太坊为典型代表，比特币是现今范围最广、认可度最高、活跃量最大的数字加密货币体系，而以太坊是现今最成熟的区块链应用开发平台，如今以太坊上已经有上千个区块链应用，例如CryptoKitties、KyberNetwork；企业间的互联、合作主要通过联盟链应用实现，欧洲的某些国家已然使用了联盟链应用实现了银行系统的互联；至于私有链应用，目前还没有比较成熟的发展。

值得重视的是，区块链当今面临着很多很重大的挑战，包含安全、资源、效率等诸多方面。安全方面，基于非对称密码学的加密机制随着量子计算机技术的发展将变得脆弱，其次个人用户的隐私保护也是一个很棘手的问题，尽管区块链中的用户都是匿名的，但是当黑客真正有切实的目的和目标时，这样的安全措施还不能有足够的安全保证。资源方面，比特币系统中基于工作量证明的共识机制使得矿工花费大量的计算资源和电力资源用来挖矿，作为矿机原料的硅也被大量征用，引起了巨大的资源浪费。效率方面，比特币系统中每一笔交易都需要10分钟的时间来确认交易，而且每秒钟能够进行的交易数量最多仅为7笔，这完全无法满足工业化的需求。即便是作为性能改进过的以太坊，每秒钟最多也只能支持几千的交易数量，这同样是远远不够的。显然，不管是从安全方面，还是从资源、效率方面，区块链的还面领着许许多多的问题和挑战，只有解决了这些问题，区块链技术才能真正地应用于实际，才能真正做到为改善人们的生活做出贡献。