区块链综述

1 引言

从去年年初开始，“区块链”这一名词突然进入公众的视野。其实作为一项技术应用模式，区块链的概念早已存在，很早以前听说的比特币就是其衍生物之一。随着其在经济领域所造成的影响日趋扩大，区块链逐渐为公众所知；而近期更是由于央行对于数字货币的大力支持，并出台了一系列相关政策，区块链才一夜之间爆火，甚至成为了人们茶余饭后离不开的话题。

2 区块链发展史

2.1 区块链史前时期

区块链是在密码学基础上，通过一系列机制涉及，实现的一种电子现金。若追根溯源，则可追溯到计算机的诞生、密码学的诞生、货币的诞生……然而在分析事物的因果关系时，不能仅仅只看到“如果不……就不会……”的概率，还要看到“如果是……就一定……”的可能性[1]。

真正起到决定性作用的，是 1976 年 Bailey W. Diffie、Martin E. Hellman 两位密码学的大师发表了论文《密码学的新方向》，论文覆盖了未来几十年密码学所有的新的进展领域，包括非对称加密、椭圆曲线算法、哈希等一些手段，奠定了迄今为止整个密码学的发展方向，也对区块链的技术和比特币的诞生起到决定性作用[2]；1978 年提出的 RSA 算法更是开启了密码学的新时代[3]；在 2001 年，随着 NSA 发布了 SHA-2 系列算法，区块链技术所需的哈希算法也诞生了。这时，区块链已经呼之欲出，它的全部充分条件已经产生，就差一个真正将这些不同领域的技术联系在一起的想法了。

2.2 区块链的诞生

2008 年 10 月 31 日，中本聪发表了论文《比特币：一种点对点的电子现金系统》，在论文中，他提出了一种不断延伸的基于随机散列的链条作为交易记录，从而使现金系统能在点对点的环境下运行，并能防止双重支付。并在 2009 年 1 月 3 日，他用他的第一版软件创建了第一个区块。

2010 年 3 月，第一个比特币交易所上线；同年五月，美国程序员拉兹洛用 10000 个比特币买了 2 个价值 25 美元的披萨，完成了比特币在现实生活中的第一笔交易。这也标志着比特币真正进入了市场[4]。

2.3 区块链日趋成熟

2011 年后，比特币逐渐进从极客圈走向大众，价格快速上涨的同时，比特币的一些弊端也显露出来。黑客盗币事件以及一些使用比特币的非法交易，使得比特币进入寒冬时期。

随后在 2012 年和 2016 年的两次产能减半，以及去中心化应用平台以太坊的出现，使得比特币再次回暖，并且一度价格暴涨。最终因为其对于市场造成的混乱，基于区块链筹款的首次币发行 ICO 在“94 事件”中被叫停。

2017 年 9 月 4 日，以央行为首的七部门出手正式叫停代币发行。通知指出，任何组织和个人不得非法从事代币发行融资活动。数字货币交易所的盘面也因此开始了长时间的大幅下跌。

随着虚拟货币和区块链会在市场、监管、认知等各方面进行了调整，各国开始积极规范代币募资的行为，公众的防范意识也进一步增强，关于区块链技术的讨论也多了起来，2018 年成为了区块链技术的启动元年。随后，在国家大力监管的同时，央行也出台了一系列的鼓励与扶持政策，区块链技术赋能实体经济，越来越受到人们的重视。

近日，习近平总书记更是强调，要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

3 区块链技术简介

区块链这一概念首次出现在中本聪的比特币白皮书[5]中，但是该白皮书并没有对区块链是什么做出一个精确的定义。近年来，随着区块链的各种应用的诞生，不仅仅是应用于数字货币比特币，而且还延伸到了许多货币系统之外的领域，加之技术本身还不够完善，变体也有很多，这使得目前对于区块链仍然没有一个确切的定义。

3.1 比特币运作机制

与现实生活中的账本类似，比特币的账本可以划分为交易、区块、链表等不同的粒度。每一条交易记录都需要交易记录需要记录输入、输出地址以及转让的数目，类似于现实生活中的转账记录。

3.1.1 比特币的记账模式

比特币系统的运作机制，就是其完成记账的过程。交易由用户发起，而记账则是在交易过程中由系统产生。在中心化系统中，账本的记账权属于账本所有者，比如，银行的账本由银行控制记账权，商店的账本由商店控制记账权。而在比特币系统中，其目标是去中心化去信任，因此账本的记账权不能控制在某个中心或是单一机构中。所以比特币采用分布式系统实现去中心化，将记账权下放到分布式系统中的节点中[6]。

3.1.2 比特币的交易模式

一次交易会被全网广播，而记账的人则需要将其打包成块。由于每一个区块都含有前一个区块的哈希值，所以每一个区块都和前一个区块唯一地链接。按照这一规则链接起来的链状区块就是区块链。如果有多个人同时算出了哈希值，那么区块链就会产生分叉，但是因为交易只能进行一次，因此只有一条链是有效的，即最长的一条，其他的链均会是非法链，不会得到全网的认可，即比特币的最长链原则。为保证自己的交易没有被买家多次交易，卖家一半会在自己的交易被收录进链之后再等几个块，才会认为交易完成。

3.1.3 比特币的生产模式

比特币的产生来源于出块奖励，算出一个区块所需的随机数是一个很繁琐的过程。因此，比特币制定了一个鼓励机制，即第一个算出并打包区块的人，就认定他“挖”出了一定数量（最早为 50，之后每 21 万个区块减半，这也意味着比特币的总量会是 2100 万）的比特币。

3.2 区块链运作机制

3.2.1 区块链的结构

区块链的概念来源于比特币，因此最开始，区块链的系统也沿用了比特币中的链式结构。后来又产生了树状结构与图状结构。

链式结构与比特币中类似，不再赘述。

树状结构即采用数据结构中的树作为存储结构，根区块没有前驱区块，只有后继区块；

而其余区块则有一个前驱区块与多个后继区块。树状结构的复杂之处在于每个区块不仅仅要包含前驱区块的哈希值，还要包含所有上层区块的哈希值；同时还要设计专门的协议，防止恶意分叉，如 GHOST 协议[8]。这种结构一定程度上可以提高数据的吞吐量。

图状结构的设计是基于图论中的无环图，与 2015 年由 Sergio 等人提出[9]，并很快投入了应用。这种方法将交易本身看作一个个区块，减少了打包的过程，实现了去区块的效果，在很大程度上提高了区块链网络的效率。但是同时也需要更高的编码要求，以及更大的存储空间，有利有弊。

3.2.2 区块链的功能

按照功能，区块链中的区块分为参与节点和维护节点。参与节点即为用于与用户交互的客户端节点，它可以发起交易请求，并广播到全网；而维护节点则是用于维护系统数据的，用于对用户的请求等操作进行验证。

4 区块链与密码学

4.1 哈希算法

如前所述，哈希算法是区块链系统最根本的技术基础之一。它能够实现数据从一个维度向另一个维度的映射。其原理是基于通过特定哈希函数的不断重复"压缩"输入的一组组数据和前一次压缩处理的结果的过程，直到全部数据都被压缩完毕，最后的输出作为整个消息的哈希值。值得注意的是，到目前为止，并没有严格的理论证明哈希函数是安全的，但并不影响哈希函数在应用密码学中的广泛使用。

在区块链中，区块的链结构是由前一个区块通过指针向后一个区块进行链接的，而这个指针就是采用的哈希指针。其优点在于，后面的区块在计算出新的哈希值的时候，是包含了上一区块的哈希值的，同时由于哈希函数便于验证，这就保证了区块链不宜篡改的特性[10]。

4.2Merkle 树

Merkle 树是一类基于哈希值的结构体，其原理是：将每一个数值进行哈希运算，得到一个哈希指针作为叶节点；非叶节点则是将它的所有子节点哈希值进行组合，然后进行哈希运算得到哈希值；层层迭代，即可得到整个树中每个节点的哈希值。

在交易过程中，节点会将收到的交易数据的哈希值按时间顺序两两合并，再取哈希值，然后把第二层的哈希值继续两两合并取哈希值，如此持续，直到算出一个把所有交易都容纳进去的最终的哈希值，这个过程，从交易内容，到层层的哈希值，到最终的跟哈希值合起来，就组合成了一个二叉的 Merkle Tree，即一个区块体的内容。Merkle 树使得数据的校验非常方便，只需要层层比较即可确定哪个数据被修改过。

4.3 非对称加密算法

对称加密算法是在解密时使用和加密相同的密钥；而非对称加密则是会区分公钥和私钥了。虽然非对称加密算法一般比较复杂，且执行时间相对较长，但是因其不需要考虑密钥分发问题，因此较为安全，也得到了广泛的应用。在区块链中，主要使用的是 ECC 椭圆曲线算法。

在区块链中，非对称加密算法主要应用于信息加密、数字签名和登录认证等过程。信息加密是发送者使用接收者的公钥进行加密，再发送回接收者，用其自己的私钥解密；数字签名是发送者用自己的私钥加密，然后发送给接收者用公钥解密，即可确认发送者；登录认证则是由客户端使用私钥加密登录信息后发送给服务器，服务器再用客户端的公钥解密认证信

息。

5 区块链发展前景

近几年来，国家在高科技领域的自主创新方面投入较多，先后出台了云计算、人工智能等多个领域的产业发展策略，区块链相关的技术和产业发展自然而然也是整体推进产业系统中的一环。从区块链技术、应用及产业发展情况来看，我国和国际先进水平基本上保持平齐，虽然在核心算法（例如加密机制、共识算法、安全体系）等方面还存在一些差距，但我国在技术与产业应用结合上具有天然优势，为区块链技术和应用发展提供了良好机遇[11]。

在社会生产协同方面：区块链技术可改造升级数字金融、物联网、智能制造、供应链管理、数字资产交易等生产领域，通过信任和协作来加快产业发展、发挥市场优势，进一步将创新、应用、价值、协同都建立在基于区块链的信任、透明体系上，实现“一链通”，提升跨企业、跨行业、跨地域多要素协同，形成“化学反应”，降低信用、资金、质量、资源等方面的风险，提高协作效率，培育新的生产关系。

在社会生活方面：区块链与数字政务结合，打通政务体系中的数字孤岛，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。区块链技术可打通并协调教育、就业、社保等方面信息共享，形成更全面、更准确的社会征信体系。区块链与养老、医疗健康、公益、精准扶贫等领域的结合，将进一步加强我国民生工程的效果，减少因为信息沟通和协作不畅带来的地域之间的差异，最终惠及全体群众。

同时我们也应看到，目前位置区块链的应用仍然仅仅限于数字货币领域，要从数字货币转向实体应用，通过这些实体行业的成本减少，来达到使区块链变现的目的，仍然有很长的路要走。

参考文献

[1]韩笑.休谟因果问题与归纳问题浅析[J].重庆科技学院学报(社会科学版),2012(08):26-28.

[2] https://www.zhihu.com/question/265992968

[3]姚前.数字货币的前世与今生[J].中国法律评论,2018(06):169-176.

[4]贾丽平.比特币的理论、实践与影响[J].国际金融研究,2013(12):14-25.

[5]Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.

[6]蔡晓晴,邓尧,张亮,史久琛,陈全,郑文立,刘志强,龙宇,王堃,李超,过敏意.区块链原理及其核心技术[J/OL].计算机学报,2019:1-51[2019-12-26].

[7]段夕华.区块链的原理与机制[J].团结,2019(04):18-21.

[8]He Pu, Yu Ge, Zhang Yan, et al. Survey on Blockchain Technology and Its Application Prospect. Chinese Journal of Computers. 2017, 44(04): 1-7.

[9]Lerner S. D. Dagcoin: A Cryptocurrency without Blocks.2015.

[10]https://www.jianshu.com/p/becd44975081

[11] 何申. 区块链：未来已来[N]. 人民邮电,2019-11-15(007).