问题的提出

不同于元宇宙这一虚无缥缈且难以落实的概念集合，区块链这一概念有明确的范围且有着核心的技术，那么，区块链到底是什么？

回答这一问题有很多层面，本文主要侧重于区块链的核心技术与可能的未来应用，即重点关注这样两个问题：

1.区块链的技术何时成熟？

2.区块链技术成熟后对人类未来生活的改变主要有哪些方面？

区块链的定义

狭义区块链是按照时间顺序，将数据区块以顺序相连的方式组合成的链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

广义区块链技术是利用块链式数据结构验证与存储数据，利用分布式节点共识算法生成和更新数据，利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约，编程和操作数据的全新的分布式基础架构与计算范式。

总结：区块链是一项去中心化的数据形式，主要特征是利用分布式记账使数据不可篡改。

区块链的兴起背景

区块链技术起源于2008 年由化名为\中本聪"(Satoshi nakamoto)
的学者在密码学邮件组发表的奠基性论文《比特币: 一种点对点电子现金系统》。

随着比特币近年来的快速发展, 区块链技术的研究与应用也呈现出爆发式增长态势, 被认为是继大型机、个人电脑、互联网、移动/社交网络之后计算范式的第五次颠覆式创新,
是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第四个里程碑. 区块链技术是下一代云计算的雏形,有望像互联网一样彻底重塑人类社会活动形态, 并实现从目前的信息互联网向价值互联网的转变。

区块链技术的快速发展引起了广泛关注. 2016 年1月,
英国政府发布区块链专题研究报告, 积极推行区块链在金融和政府事务中的应用;

中国人民银行召开数字货币研讨会探讨采用区块链技术发行虚拟货币的可行性,
以提高金融活动的效率、便利性和透明度. 美国纳斯达克于2015 年12
月率先推出基于区块链技术的证券交易平台Linq,
成为金融证券市场去中心化趋势的重要里程碑;
德勤和安永等专业审计服务公司相继组建区块链研发团队,
致力于提升其客户审计服务质量。

区块链的核心技术

一般说来, 区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成.

其中, 数据层封装了底层数据区块以及相关的数据加密和时间戳等技术;
网络层则包括分布式组网机制、数据传播机制和数据验证机制等;
共识层主要封装网络节点的各类共识算法;
激励层将经济因素集成到区块链技术体系中来,
主要包括经济激励的发行机制和分配机制等;
合约层主要封装各类脚本、算法和智能合约, 是区块链可编程特性的基础;
应用层则封装了区块链的各种应用场景和案例. 该模型中, 基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。

区块链技术并不产生实际价值，其本质是一种数据算法，但就像网络的发展一般，这项技术的突破会给人类生活带来巨大改变。

区块链的应用场景

区块链系统具有分布式高冗余存储、时序数据且不可篡改和伪造、去中心化信用、自动执行的智能合约、安全和隐私保护等显著的特点,
这使得区块链技术不仅可以成功应用于数字加密货币领域,
同时在经济、金融和社会系统中也存在广泛的应用场景。

数据存储: 区块链的高冗余存储(每个节点存储一份数据)、去中心化、高安全性和隐私保护等特点使其特别适合存储和保护重要隐私数据,
以避免因中心化机构遭受攻击或权限管理不当而造成的大规模数据丢失或泄露。

数据鉴证: 区块链数据带有时间戳、由共识节点共同验证和记录、不可篡改和伪造,
这些特点使得区块链可广泛应用于各类数据公证和审计场景。

金融交易: 区块链技术与金融市场应用有非常高的契合度.
区块链可以在去中心化系统中自发地产生信用,
能够建立无中心机构信用背书的金融市场, 从而在很大程度上实现了\金融脱媒",
这对第三方支付、资金托管等存在中介机构的商业模式来说是颠覆性的变革。

资产管理: 区块链在资产管理领域的应用具有广泛前景,
能够实现有形和无形资产的确权、授权和实时监控。

选举投票: 投票是区块链技术在政治事务中的代表性应用.
基于区块链的分布式共识验证、不可篡改等特点,
可以低成本高效地实现政治选举、企业股东投票等应用; 同时,
区块链也支持用户个体对特定议题的投票.。

根据实际应用场景和需求, 区块链技术已经演化出三种应用模式, 即公共链(Public blockchain)、联盟链(Consortium blockchain) 和私有链(Privateblockchain).
公共链是完全去中心化的区块链,
分布式系统的任何节点均可参与链上数据的读写、验证和共识过程, 并根据其PoW或PoS 贡献获得相应的经济激励.

比特币是公共链的典型代表. 联盟链则是部分去中心化(或称多中心化) 的区块链,
适用于多个实体构成的组织或联盟, 其共识过程受到预定义的一组节点控制,
例如生成区块需要获得10 个预选的共识节点中的5 个节点确认;
私有链则是完全中心化的区块链, 适用于特定机构的内部数据管理与审计等,
其写入权限由中心机构控制, 而读取权限可视需求有选择性地对外开放。

区块链不产生新的价值，其只能对现实生活进行优化，区块链的最大作用在于其“去中心化”带来的实时监控及不可篡改功能。

区块链的存在的技术问题

安全性威胁是区块链迄今为止所面临的最重要的问题. 其中, 基于PoW
共识过程的区块链主要面临的是51% 攻击问题, 即节点通过掌握全网超过51%
的算力就有能力成功篡改和伪造区块链数据。

区块链效率也是制约其应用的重要因素. 首先是区块膨胀问题:
区块链要求系统内每个节点保存一份数据备份,
这对于日益增长的海量数据存储来说是极为困难的.

PoW 共识过程高度依赖区块链网络节点贡献的算力,

这些算力主要用于解决SHA256 哈希和随机数搜索,
除此之外并不产生任何实际社会价值, 因而一般意义上认为这些算力资源是被\浪费"掉了,同时被浪费掉的还有大量的电力资源。

区块链网络作为去中心化的分布式系统,
其各节点在交互过程中不可避免地会存在相互竞争与合作的博弈关系,
这在比特币挖矿过程中尤为明显. 即去中心化便会带来小节点的权限问题。

区块链的弊端主要在于虽然一方面保护了隐私，但另一方面也带来了不可监管的问题。

区块链的现实影响

一、加密货币的兴起。其带来的影响是巨大的、全方位的。

二、基于区块链技术的智能合同。这更像是对原有合同形式的优化，且其仅能优化不可篡改性与私密性，并付出相应的技术对价。

三、对虚拟财产权的确权。通过区块链技术，可以实现对无形资产的全方位确权，方便民众享有权利和转让相关权利。但也是付出了“难以监管”的对价。

总结

区块链是一项编程技术，并不会给人类社会带来革命性变革，其只能通过影响人类的交往方式影响人类的生活。其核心特征在于去中心化，带来的作用是数据的确定性以及匿名化，同时也带来了难以监管等问题。

参考文献

[1]袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494. DOI:10.16383/j.aas.2016.c160158.

[2]邵奇峰,金澈清,张召,钱卫宁,周傲英.区块链技术:架构及进展[J].计算机学报,2018,41(05):969-988.

[3]何蒲,于戈,张岩峰,鲍玉斌.区块链技术与应用前瞻综述[J].计算机科学,2017,44(04):1-7+15.

[4]沈鑫,裴庆祺,刘雪峰.区块链技术综述[J].网络与信息安全学报,2016,2(11):11-20.

[5]谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2016(09):192-195.

[6]郑戈.区块链与未来法治[J].东方法学,2018(03):75-86.DOI:10.19404/j.cnki.dffx.2018.03.008.