**第一章课后调研报告**

**区块链（blockchain）基本定义和发展现状**

**学 号 3020244294**

**姓 名 石子跃**

**学 院 智能与计算**

**专 业 网络安全**

**年 级 2020**

**2022年 3月 19日**

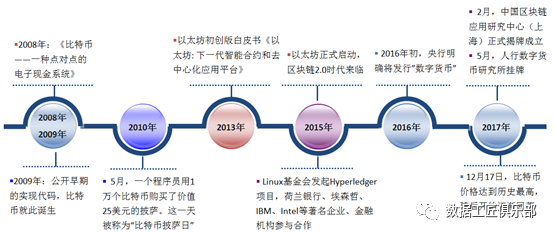
## 区块链基本定义

狭义来讲, 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构, 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。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、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来编程和操作数据的一种全新的分布式基础架构与计算范式。

《华为区块链白皮书》：区块链是一系列现有成熟技术的有机组合，它对账本进行分布式的有效记录，并且提供完善的脚本以支持不同的业务逻辑。

工信部信软司《中国区块链技术和应用发展白皮书（2016）》：区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。

## 区块链技术的发展脉络



从区块链的发展路线为脉络，分为技术起源，区块链1.0，区块链2.0三个部分。

技术起源：哈希算法来自于1997年，哈希之父AdamBack；分布式匿名现金系统最早出现于1998年，WEIDAI提出b-money加密货币系统；点对点技术在1999年就已大范围流行。

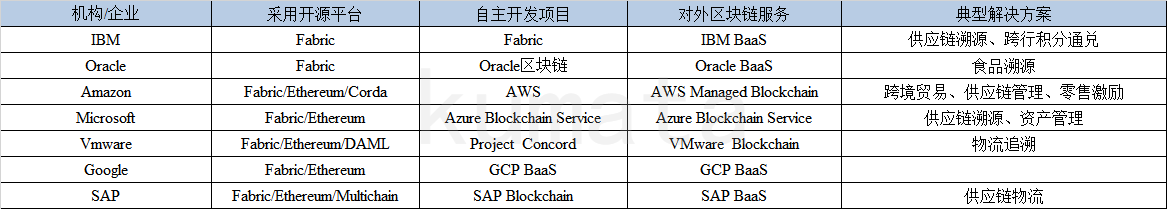
区块链1.0：2008年，名为“中本聪”（Satoshi Nakamoto）的学者发表了一篇奠基性论文《比特币: 一种点对点的电子现金系统》，中本聪将密码朋克的精神与积累注入比特币当中，就像从矩阵当中走出的创世者，意在捍卫公民在数字世界中的权利。由比特币掀开的区块链的1.0时代描绘的是一个不被政府和银行机构控制的货币交易网络。

区块链2.0：基于区块链的可编程金融。数字货币的强大功能吸引了金融机构采用区块链技术开展业务，人们试着将“智能合约”加入区块链形成可编程金融。目前，可编程金融已经在包括股票、私募股权等领域有了初步的应用，包括目前交易所积极尝试用区块链技术实现股权登记、转让等功能；华尔街银行通过联合打造区块链行业标准，提高银行结算支付的效率，降低跨境支付的成本。

区块链1.0、区块链2.0、区块链3.0，也许感觉这是一种递进的演化，但事实上仅仅是应用范围的不同而已，从区块链1.0到区块链3.0都是平行的发展阶段，在各自的领域内发挥应有的作用。

## 国内外区块链的平台

国外：



国内：



普遍采用Hyperledger Fabric（超级账本）和Ethereum（以太坊）。

·从二者的运作模式来看，以太网可以是公共的或私有的，没有任何权限，而Hyperledger是一个私有和许可的网络。

·从二者的共识机制来看，使用以太坊，所有网络参与者（或节点）必须就所有交易达成共识。这与节点是否参与特定交易无关。目前，以太坊通过基于工作证明（PoW）算法的挖掘建立了其共识机制。所有节点必须就共同的分类帐达成一致，并且所有节点都可以访问所有记录的条目。相反，Hyperledger允许节点在No-op（不需要共识）和协议协议（PBFT）之间进行选择，由此两个或多个方可以以影响结果的方式就密钥达成一致。这使得不受欢迎的第三方无法在协议方上强制进行关键选择。因此，Hyperledger对共识和对交易的限制访问进行了细粒度控制，从而提高了性能可伸缩性和隐私性。

·编程语言方面一个关键区别是在以太坊中使用智能合约，用一种名为Solidity的高级的合约导向语言编写。但是，在Hyperledger中，你可以使用术语“chaincode”作为智能合约的同义词。链代码通常处理网络成员同意的业务逻辑，因此可以将其视为智能合约。这些链代码是用Golang编写的，这是一种由Google创建的编程语言。

·加密货币，Hyperledger不需要加密货币进行交易。它没有内置的本地加密货币，如以太坊的token——以太币。因此，根本不需要采矿。这允许可扩展的一致性算法，其能够处理大多数企业应用程序所需的高速率交易。但是，一个硬币有两面（代币），因为以太坊有自己的以太币，在需要加密货币的用例中，它比Hyperledger更有利。由于Hyperledger也是可编程的，因此它可以利用链代码中的嵌入式逻辑来自动化整个网络中的业务流程。如果需要，你还可以通过链码开发自定义代币。

## 常见的区块链应用



·从蚂蚁链看，蚂蚁链连续三年上榜《福布斯》全球区块链50强榜单，成为连续三年上榜的唯一中国企业。以蚂蚁链“浙冷链”防疫溯源系统为例，截止至今，浙江省已平稳处置55起阳性冷链食品事件，溯源倒查350.3吨涉疫食品，在防疫方面发挥了重要作用。

·基于腾讯区块链研发的“至信链”已与腾讯企鹅号、ISUX原创馆等内容生产平台完成对接，已累计存证保护原创作品超过1000万篇，目前每日存证数量超过6万篇。

·百度超级链为百信银行、商户以及电商平台搭建商户清算联盟链，成为了其在金融科技领域的又一重要进展。在教育领域，浙江正元智慧科技股份有限公司基于百度超级链开放网络推出首个智慧校园易校园。

·京东智臻链云签电子合同平台连接互联网法院、公证处等司法机构，提供电子合同发起、签署、管理，风险监控、一键举证等功能，目前已服务超百万份电子合同签约。在政务领域，京东智臻链技术平台还为广州互联网法院“网通法链”提供了区块链底层技术，并通过区块链联盟网络，将智臻链数字存证平台与广州互联网法院“网通法链”建立互信互通。

·平安壹账链则在金融贸易领域大放光彩，其用户包括广东金融局、香港金管局、天津海关试点、招商港口跨链、某国际 跨国组织、多个国家部委及地区政府等多个机构。

·趣链科技国产自主可控底层联盟链平台已服务于中国人民银行、住建部、审计署、工信部、国家市监局、四大行总行、沪深交易所、主流股份制商业银行、国家电网以及地方政府等上百家组织或机构，支撑业务规模达数千亿人民币。

参考文献:

[1]ChainTimes快链.新人必读:万字解析区块链产业发展脉络. <https://www.geekmeta.com/article/4148824.html>

[2]傅一平. 一文读懂～国内外区块链发展现状、趋势和政策. <https://blog.csdn.net/fuyipingwml1976124/article/details/103471407>

[3]中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书

[4]华为技术有限公司. 《华为区块链白皮书》

[5]Kumata.整理分析国内外主流区块链平台.https://www.cnblogs.com/kumata/p/1264279

1.html

[6]国内主流产业区块链平台比较. <https://ytm.ltd/?id=1005>

[7]Prerna. Hyperledger vs Ethereum – Which Blockchain Platform Will Benefit Your Business?. <https://www.edureka.co/blog/hyperledger-vs-ethereum/>