**Day1 区块链的前世今生、前沿技术和未来**

1. **为什么会出现区块链**

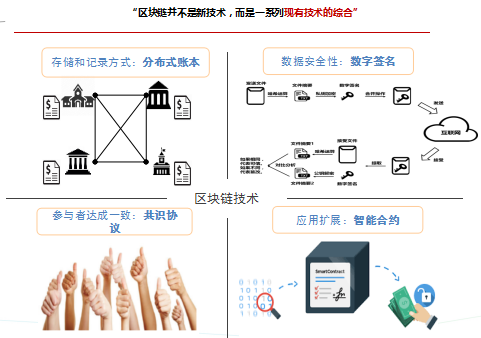
区块链技术的出现是互联网发展到一定高度的必然产物，互联网的TCP/IP协议基本实现了全球信息高速、低成本的传输和共享，但是随着互联网进入到生活的各个层面，我们发现货币这一类需要信任背书的特殊信息，仍然无法在互联网上进行高速传输和共享，其根本原因在于，现有的信息互联网不是价值互联网。货币这一类需要背书的价值信息的传递和分享，必须获得所有参与方的认可，且结果不能受任何一方控制。那么，互联网的下一步发展急需要解决的就是价值转移的问题。

目前“价值转移”行为是通过中介来解决完成，比如银行，支付宝等第三方机构来，这些机构都是通过公司和政府背书的中心化方案来解决，而这种解决方案是建立在对这个中心化的人或者机构的信任上。但系统中往往最不可信任的就是人，为了解决中心化信任问题，需要设置大量繁琐的流程、成本高昂的规则制度、流程和监控手段来部分实现。因此，要真正完成以信任为基础的价值转移，需要一个能取代第三方中介的方式，能够自动运行、且具备数学（算法）和机器信任的机制来完成价值转移。具备这些特点的区块链，因运而生。

1. **什么是区块链**

**区块链是什么？个人认为有以下几个方面的理解**

首先，从技术上讲不是新的技术，是由一系列的已有技术组成：



* **在点P2P网络上构建的不可篡改的分布式账本**：通过区块加链的数据结构确保单一节点账本在结构上不可篡改，P2P网络是区块链的基础计算架构，每个相等地位的节点彼此相连，不依赖于专用的集中服务器，以保障区块链是一个分布式系统，使每个节点共享账本，每个节点拥有区块链的完整备份数据，实现节点间的可信和透明共享。
* **加密等安全技术：**通过密码学来保障交易真实、一致和安全，Hash算法使区块链彼此链接不可篡改，签名算法保证交易不可抵赖，非对称加密、对称加密以及同态加密等保障交易的安全和隐私。
* **共识算法：**是对区块链记账权的集体验证的机制，无须借助第三方机构担保，在不完全信任的环境，使用纯数学的机制建立各方信任关系，用技术来保障共识的结果是可信的。建立信任的成本极低，是区块链的精髓所在。
* **智能合约：**是能够自动执行合同条款的计算机程序，是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。具备自治、自足和去中心化。区块链中所有交易行为通过智能合约触发，所有交易行为对参与方透明可见，杜绝人为因素干扰，所有交易过程和结果存入区块链中，不可篡改。

其次，区块链是一个分布式的共享账本系统，建立了去中心、机器信任、集体维护的分布式共享账本系统，用一个完美的数学解决方案建立了参与各方信任和共识的机制。

版本号

上一区块哈希值

Merkle根节点

时间戳

难度值

随机数

交易数据

区块N

版本号

上一区块哈希值

Merkle根节点

时间戳

难度值

随机数

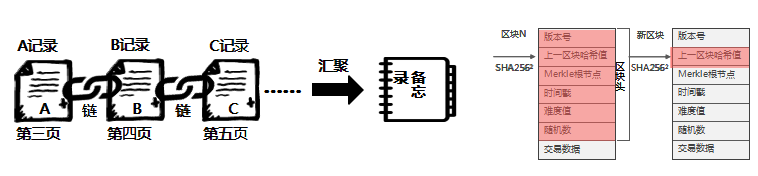
交易数据

新区块

SHA2562

区块头

SHA2562



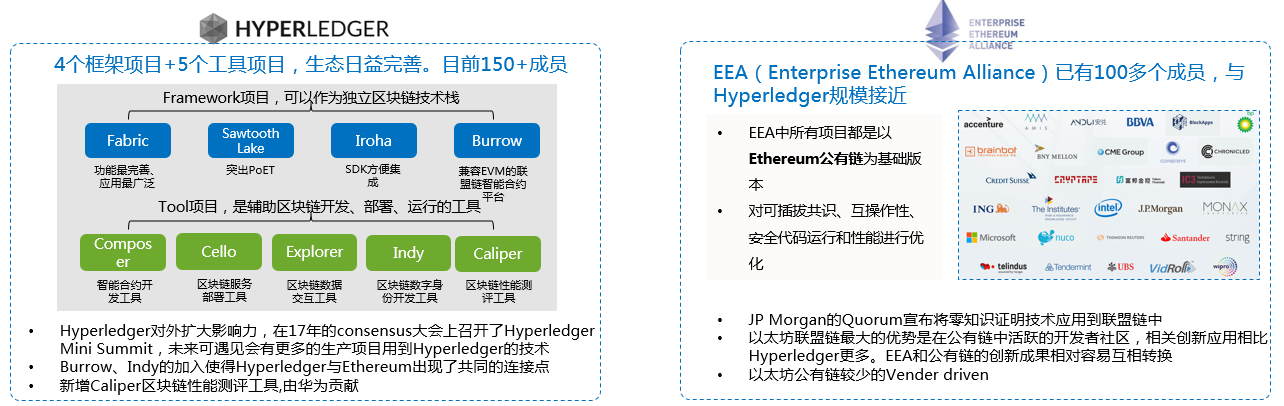
**区块链的特点：**

* **共享开放**：系统对所有参与者开放，都享有知情权，平等享有区块链信息。
* **全员共识**：所有参与者对交易记录顺序和状态建立共识，共同信任区块链机制。
* **公平竞争**：通过算法决定记账权。
* **真实完整**：每个记录在监督下被真实、完整记录，有据可查，证据充分，多方拥有，不可篡改。
* **安全可靠**：数据加密和密码学保证数据不可篡改、不可伪造，复杂的校验和共享机制保证数据的完整性、连续性和一致性。

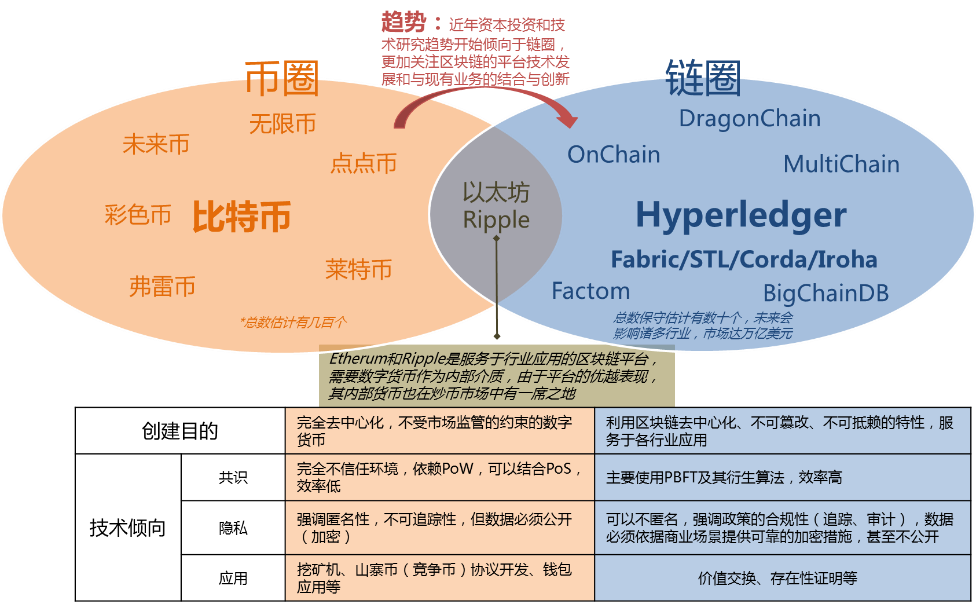
1. **区块链发展历程和现状**

**区块链的类型：公有链、私有链、联盟链和混合链**

* **公有链**：是任何人随时可以加入，任意读取数据，人人都能发送交易和获得有效确认，人人参与共识过程的区块链。通常采用POW，POS和DPOS的共识机制，将经济激励和加密算法验证结合起来，并遵循每个人获得的经济奖励和对共识过程做出的贡献成正比的原则，通常称为完全去中心化区块链。程序员无权干涉用户。但公有链也存在交易性能差、能源消耗巨大，虚拟货币不合法以及交易完全匿名不符合监管等问题。下一代公有链越来越趋向于联盟链的方式如EOS等。
* **私有链**：是指写入账本的权限是由一个组织或者机构控制的区块链，读取权限可以对外开放也可以进行任意程度的限制。从外部看私有链是中心化的，但在内部，它也是由多个点组成的去中心化的区块链系统。它的优势是不需要代币的设计方案，同时在处理速度和账本访问的私密性和安全性上相对于公有链有巨大的优势。
* **联盟链**：是一种许可链，是私有链的对外范围扩大版本，是指共识过程受到预选节点控制的区块链。区块链账本可以将读取权限只限制于联盟成员内部，也可以对外提供读取能力。联盟链基于可信节点共识的机制，使联盟具备出块速度快、交易性能高、安全隐私高等优点，Hyperledger、EEA和R3 CEV就是典型的联盟链系统。联盟链是企业区块链应用的趋势。



* **混合链**：随着区块链技术越来越复杂，技术和架构开始不能简单的被定义为公有链或私有链，他们之间的界限越来越模糊，所有的节点不再是简单的一模一样的权限，而是有不同的分工，角色和权限等级也越来越多，比如DPOS共识算法就能看出这种趋势开始出现。以后的技术发展趋向于这种混合链的方式。



区块链的发展脉络

* 
* **区块链1.0**：以比特币为为代表的可编程货币，是一个全新的数字支付系统，其去中心化、基于秘钥的数字货币交易模式，在保证安全性的同时降低交易成本，使价值在互联网中直接交换成为可能，是区块链技术的起源。但是比特币存在价格波动剧烈、识挖矿消耗能源巨大、交易性能差、交易脚本单一以及合法性存疑等问题，使其只限于虚拟货币。
* **区块链2.0**：基于区块链的可编程社会，主要特点是将智能合约引入区块链使交易功能强大，同时通过提高交易效率和速度，将区块链广泛应用到金融等社会领域，亦可以在点对点交易、信息可信登记、所有权版权等确权和智能管理领域有初步应用。
* **区块链3.0**：价值互联网，随着区块链技术的成熟和发展，区块链底层信任平台与大数据、人工智能等技术相结合，作为互联网的信任和价值传递的基础平台，可以广泛应用到社会各行各业，通过其去中心化、不可篡改、可信共享等特点，提高整个社会的运行效率和整体信任水平。

\*\*这里所说的区块链1.0、2.0和3.0并不是递进的演化，仅仅只是应用范围不同而已，从1.0到3.0都是平行的发展阶段，在各种的领域内发挥自己的应有作用。

1. **区块链未来发展方向**

**区块链目前存在几大技术上的障碍影响其大规模广泛应用。**

* **有限的交易性能和可扩展性**：区块链有限的交易处理能力和交易形成区块的时间缓慢。公有链一般每秒只有几笔到几十笔交易，联盟链和基于石墨烯技术的公有链通常在1000左右TPS，这相对于中心化的架构的处理速度还是有很大差距。

目前有以下几种扩展方案：

* + **分片：**分片背后的概念是区块链整体的状态被分成不同的“片”，分区并行处理。
  + **链下**：将计算和验证过程转移到链下单独的协议中，就能达到交易的高吞吐量，块链只是用作结算层来处理一系列交易的总和——最终交易，包括侧链和闪电链技术。
  + **DAGs（有向无环图）**：DAG，有向无环图的缩写，是一个图形数据结构，由顶点和边组成（顶点是图中的点，边是图中一个点到另一个点的路径）。DAG保证了没有环，即不可能从一个点开始沿着一系列的边在回到这个点，这使得我们能够沿着拓扑顺序获得一个节点（或顶点）序列。以DAG为基础的协议（例如IOTA的Tangle）的前提，是将全局线性区块链排在一起，用DAG数据结构来维护系统的状态。 为了维护网络安全，这些协议依赖于他们自己的新方法，不要求每个节点都以线性方式处理每个交易。这种技术还处于非常基础的阶段。
* **有限的隐私保护**：区块链可以防篡改、去中心化、在非信任的网络运行，但正因为用户的账本对参与组织是透明的，也就是任何组织都可以访问到相同的数据，如果将用户的隐私的数据放到链上将会放大用户隐私泄露的风险。当前在比特币等公有链系统中，所有的交易信息都是公开的 （包括交易金额）。但是，在金融业的交易中，金融交易信息是敏感数据，非业务相关方不能查看，但同时又要满足监管机构的监管要求，而大部分的区块链并没有满足隐私性的要求，需要以下相关安全技术得到突破：
  + **同态加密**：对用户的交易数据用其公钥进行加密保护，交易的时候都是密文运算，最终账本中加密保存，即使节点被攻破，获取到账本记录也无法解密。
  + **零知识证明**：能够在不向验证者提供任何有用的信息的情况下，使验证者来相信该结论是正确的，证明过程中不用向验证者泄露被证明的消息。
  + **可信执行环境**：TEE（Trusted Execution Environment）是主处理器的安全区。它保证内部加载的代码和数据在保密性和完整性方面得到保护。
* **存储的约束**

将信息存储在区块链数据库中意味着数据由网络中的每个全节点存储。由于区块链数据库仅可添加、不可更改，所以数据被无限期地存储。因此，数据存储为分布式网络增加了巨大的成本，每个全节点需要无限期的存储越来越多的数据。从而，对于任何构建在区块链上的现实应用，存储都是一个巨大的障碍。目前有几个公有链的存储方案：

* + 蜂群协议（Swarm）：是 Ethereum 点对点文件共享协议，允许用户将应用程序代码和数据存储在主链下连接到以太坊区块链的 swarm 节点中，接下来用户就可以在区块链上交换这些数据。
  + Storj：是一种数据分片的解决方案，首先对文件和数据进行分片、加密，然后分发到多个节点，从而使每个节点只存储一小部分数据。
  + IPFS：是一种可选的 p2p 超媒体协议，以内容寻址超链接为基础的、提供高吞吐量、内容寻址的块存储模型。从本质上讲，它允许文件以永久和分布式的方式存储，同时提供历史版本的文件，从而删除重复文件。
  + Decent：是一个分布式的内容共享平台，允许用户上传和数字货币化分享他们的工作成果（视频，音乐，电子书等），不依赖于集中化的第三方来进行分享。
  + 在联盟链中可以通过数据归档，区块链运行系统只保留最近数据，历史数据通过归档进行保存。

虽然区块链技术还存在各种技术不完善的约束，但是区块链底层技术的价值已经得到政府和社会的广泛认可，不是一时炒作，是具有划时代意义的，在经济社会的各个领域，已经引起广泛关注。IBM公司研究称，区块链是新一代事物处理应用技术，它建立了信任、问责制和透明度，同时简化了业务流程。未来，一个用于交互的操作系统，将大大减少做事情的成本和复杂性，对于未来区块链具有5大战略意义：

1. 区块链是建立价值互联网的基础平台
2. 区块链是支撑万物互联的基础可信账本
3. 区块链是大数据时代的数据资产流通的关键支撑
4. 区块链是驱动分享经济发展的新引擎
5. 区块链是建立社会治理新体系的创新方法

谢谢大家。