招新，基础入门

1.什么是区块链

对于区块链而言，我认为可以这样理解为一个记账系统。例如对于一个班级内部而言，每一天都会存在支出和收入。那么就会存在记账本这个问题。由于记账涉及到钱的问题。班上就会出现有一个人出来记录每天的支出和收入，但不同于会存在会计这个角色，对于区块链而言，每一个人都可能是会计，每一个人的账本都是同步更新的（去中心化），会有一个叫做共识问题的东西，让大家都可以去记账。

当然啊，记账肯定是有报酬，其他的就会给他钱（区块链存在的奖惩机制，会计就好比某一个区块，都是在不断努力去生成新的“账本”，即区块，通过计算寻找满足特定SHA–256哈希值对应的数值解。这个过程就是比特币中的“挖矿”，而且这个一定要快，一旦其中一个区块计算出来了，就相当于新一天的账本就ok了，那么就可以进行公示，也就是给每个区块进行打包，打包可以获得报酬和系统给予的奖励而赚钱），但是呢，会计的账本必须公开，就是你自己干了什么都要给其他所有的区块声明一下下，所以就会有要求每一个人的消费信息是透明可见的，而且必须要在公示栏上公示出来，免去了每时每刻都在记账的问题，那么每天生成出来的一个账本就相当于是区块，并且会写明每一天的时间（时间戳），那么每一天就会生成一个区块（当然真实的区块不会那么慢），当然，每个人都会去copy这个账本，作为自己的记录。那么就会有人说啊，公示栏离得人有远有近，不一定是每个人都要去查找公示栏来记录，大家完全是在准确的基础上面进行借阅和抄写，也就是的我可以到处抄，这种点对点的一种信息交流，然后用加密方式穿在一起（这就是链），当然，因为是一个链式反应的存在，而导致这个账本非常难以被修改，好比牵一发而动全身，总的来说就是一个互相监督验证，公开，去中心化，带有共识机制，点对点（P2P）难以篡改的分布式账本。

PS；当然上面的基本都是一些基本的底层逻辑罢了。

1. 比如分布式账本基于每个区块的记录，每一个区块相对于而言就是一个公证人，里面存在51%及以上的认可即为系统权威。
2. 哈希函数，好比一个区块我声明了一个我输入了，然后将字符串转化为一堆数字（256二进制的数字），比如666，那么每个人就会在自己账本记上666，那么就可以很好的对账本同时可以保护用户自身的隐私性，并且对于其他的区块，他们都是我的公证人。
3. 某种意义上来说，区块链就是对于分布式账本实现的一个辅助手段，为了给虚拟货币做出一个带有加密性质的保障，当然价值不止于此，更多的在于其他的关于信息交换的应用。.

4.补充，区块链的模型架构

区块链的基础架构一共分为6个，，包括数据层、网络层、共识层、激励层、合约层、应用层

a.数据层

数据层主要描述区块链技术的物理形式。技术人员们首先建立的一个起始节点，之后在同样规则下创建的规格相同的区块通过一个链式的结构依次相连组成一条主链条。之后，新的区块通过验证后不断被添加到主链上，主链也会不断地延长。

b.网络层

网络层的主要目的是实现区块链网络中节点之间的信息交流，一个节点既接收信息，

也产生信息。节点之间通过维护一个共同的区块链来保持通信。区块链的网络中，每一个节点都可以创造新的区块，在新区块被创造后会以广播的形式通知其他节点，其他节点会对这个区块进行验证，当全区块链网络中超过51%的用户验证通过后，这个新区块就可以被添加到主链上了。

c.共识层

共识层能让高度分散的节点在去中心化的系统中高效地针对区块数据的有效性达成共识。区块链中比较常用的共识机制主要有工作量证明、权益证明和股份授权证明三种。

d.激励层

激励层的主要功能是提供一定的激励措施，鼓励节点参与区块链的安全验证工作。比如说比特币的情况，在一定的数量前会对新区块的收取手续费和比特币的给予，如果达到一定数量那么就是只有手续费收取。

e.合约层

合约层主要是指各种脚本代码、算法机制以及智能合约等。我们以比特币为例，比特币是一种可编程的货币，合约层封装的脚本中规定了比特币的交易方式和过程中涉及的种种细节。

f.应用层

应用层封装了区块链的各种应用场景和案例。

2.区块链的分类和自我理解

目前在网上查询到的一共有三种的链。

分别为1.公共链2.私有链3.联盟链

A. 公共链

顾名思义，什么人都可以进来参与。任何人都可以参与（完全去中心化），阅读，交易发送。但是对于用户而言，可以完全免受开发者的干扰，而开发者可以利用这些程序去保护用户（运用代币机制（一种奖励机制）鼓励竞争记账）（你能保他，但不能干他）。

当然，对于应用的方面而言，比如说比特币和以太坊就是公链的应用，也就是意味着你的交易信息就会被公布在网上，你也可以看到所有的交易信息。

当然，对于应用的方面而言，比如说比特币和以太坊就是公链的应用，也就是意味着你的交易信息就会被公布在网上，你也可以看到所有的交易信息。

B. 私有链.

对于私有链而言，就是整个区块链完全被以个人或者组织机构所拥有，会被严格控制参与节点的资格吗，但是呢，私有链往往可以有极快的交易速度、更好的隐私保护、更低的交易成本、不容易被恶意攻击，并且能做到身份认证等金融行业必需的要求。总的来说就是封闭且相对安全，成本低且高效。正因为有这些特点，私有链被广泛运用在，国家机关或者企事业单位对内部数据进行监管和一些金融机构，保证内部数据的安全。主要还是为了保密的应用。

C. 联盟链

联盟链是指有若干个机构共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易，并且共同来记录交易数据。我个人认为是可以理解为若干个私有链的pro。把个个的私有链联合交叉起来，所以相对于私有链，联盟链的权限设计会不同，可能更加开放一点，但也意味着更加复杂。

对于联盟链的应用，比如说经典的超级账本Hyperledger Fabric，还有R3,和蚂蚁金融。

D. 许可链

就是参与到区块链系统中的每个节点都是经过许可的，未经许可的节点是不可以接入到系统中，因此私有链和联盟连都属于许可链。有些许可链是没有代币机制，因为不需要通过代币来鼓励节点竞争记账。然后现在就出现了混合链这一个概念（我就不单独列出来了），实际上，混合链就是公有链和许可链的杂糅，混合链会导致不同的节点会有不同的作用，就是你干你的，我干我的。而且对于信息的保护而言，我可以处于一种平时是保护而必要时放出来给大家看的一种情况。就好比清朝晚期，总体上是封闭的，但是又有着具有和外界沟通的能力，具有很高的灵活性。网上查找到的应用有GMPC。

3.比特币和区块链的关系

个人认为，对于比特币和区块链的关系，好比盖楼，区块链就是地基（比特币的底层技术），那么比特币就是盖在区块链上的一个叫做比特币的大厦（第一个基于区块链技术的应用）。对于比特币而言，它实际上是一种由电脑生成的虚拟货币，而通过区块链技术去来实现价值储存和交易。当然比特币作为一个公有链，应用的技术是开源的，面对所有人开发，就会导致有“挖矿”这种东西，消耗资源。所以总的来说就是比特币这种的加密货币技术是 应用区块链的，但是区块链技术并非加密货币专业。