我是去年的时候接触区块链的，更准确的说是接触比特币原理去中心化的分布式账本技术的。因为工作的公司是金融公司，金融公司对自己的业务很看重，我们又有一个代理记账的小公司，因而也在找寻一套技术体系支撑我们公司只做真账的理念。因此我也关注了区块链技术。

看了初链的白皮书，高性能首先是吸引我的点，因为现在比特币交易时间慢，性能低。如果初链能改变这点也是区块链技术的重大进步。另一个是去中心化技术，这个技术虽然不新颖了，区块链好多领域都用了去中心化分布式账本技术，但是去中心化的最终目的吸引一部分为打造自由平等的互信社会而努力的区块链爱好者。现在的共识算法pow pos dpos 都在不断的迭代更新，如果初链能找到更快更好的混合共识机制算法，让人们认可我想会是一个不小的颠覆性成果。我个人觉得初链除了可以进军保险，医疗，游戏等方面还可以拓新，因为好多行业领域区块链大军正在进军中，区块链云养猫这些好多已经发展的很成熟了，可以从一些解决人的痛点，但是目前还没有人能解决的领域去探索。这仅仅是个人的愚见

其次说说我对区块链的理解和认识，我接触区块链就是为了想做自己的项目，区块链的理念深深吸引我，去中心化，不易被篡改，恰恰是我想要的公平公正。比特币是区块链最成功的应用，但是我相信区块链能应用到更多的场景，我们的想象空间还可以无限放大：

如果将区块链应用于股份的众筹，那我们还会担心众筹发起人跑路吗？

如果区块链应用于银行票据，那银行票据还会被非法贴现吗？

如果区块链应用于医保，社保，还会出现骗保现象吗？

…

区块链还是 21 世纪最具革命性的技术之一，它仍然处于不断成长的阶段，而且还有很多潜力尚未显现。 本质上，区块链只是一个分布式数据库而已。 不过，使它独一无二的是，区块链是一个**公开**的数据库，而不是一个私人数据库，也就是说，每个使用它的人都有一个完整或部分的副本。 只有经过其他“数据库管理员”的同意，才能向数据库中添加新的记录。 此外，也正是由于区块链，才使得加密货币和智能合约成为现实。

首先从 “区块” 谈起。在区块链中，真正存储有效信息的是区块（block）。而在比特币中，真正有价值的信息就是交易（transaction）。实际上，交易信息是所有加密货币的价值所在。除此以外，区块还包含了一些技术实现的相关信息，比如版本，当前时间戳和前一个区块的哈希。哈希计算，是区块链一个非常重要的部分。正是由于它，才保证了区块链的安全。计算一个哈希，是在计算上非常困难的一个操作。即使在高速电脑上，也要耗费很多时间 (这就是为什么人们会购买 GPU，FPGA，ASIC 来挖比特币) 。这是一个架构上有意为之的设计，它故意使得加入新的区块十分困难，继而保证区块一旦被加入以后，就很难再进行修改。本质上，区块链就是一个有着特定结构的数据库，是一个有序，每一个块都连接到前一个块的链表。也就是说，区块按照插入的顺序进行存储，每个块都与前一个块相连。这样的结构，能够让我们快速地获取链上的最新块，并且高效地通过哈希来检索一个块。为了加入一个新的块，我们必须要有一个已有的块，但是，初始状态下，我们的链是空的，一个块都没有！所以，在任何一个区块链中，都必须至少有一个块。这个块，也就是链中的第一个块，通常叫做创世块（**genesis block**）

第二：区块链的一个关键点就是，一个人必须经过一系列困难的工作，才能将数据放入到区块链中。正是由于这种困难的工作，才保证了区块链的安全和一致。此外，完成这个工作的人，也会获得相应奖励（这也就是通过挖矿获得币）。“努力工作并进行证明” 的机制，就叫做工作量证明（proof-of-work）。要想完成工作非常地不容易，因为这需要大量的计算能力：即便是高性能计算机，也无法在短时间内快速完成。另外，这个工作的困难度会随着时间不断增长，以保持每 10 分钟出 1 个新块的速度。**在比特币中，这个工作就是找到一个块的哈希**，同时这个哈希满足了一些必要条件。这个哈希，也就充当了证明的角色。因此，寻求证明（寻找有效哈希），就是矿工实际要做的事情。

第三：持久化存储和命令行接口，本质上，区块链是一个分布式数据库，存储需要数据库的调用

第四：交易（transaction）是比特币的核心所在，而区块链唯一的目的，也正是为了能够安全可靠地存储交易。在区块链中，交易一旦被创建，就没有任何人能够再去修改或是删除它。

由于比特币采用的是 UTXO 模型，并非账户模型，并不直接存在“余额”这个概念，余额需要通过遍历整个交易历史得来。

第五：在比特币中，没有用户账户，不需要也不会在任何地方存储个人数据（比如姓名，护照号码或者 SSN）。但是，我们总要有某种途径识别出你是交易输出的所有者（也就是说，你拥有在这些输出上锁定的币）。这就是比特币地址（address）需要完成的使命。

以上大概是比特币从框架的所有实现交易的步骤，也是我对区块链技术的大体了解另外对DPOS算法的理解是：本质上，所有区块链都是一种由交易驱动的确定性状态机。而共识，是就确定性交易顺序达成一致并过滤无效交易的过程。有各种不同的共识算法都可以产生等效的交易排序，但通过在多个区块链上长年累月的可靠运行，DPOS 已经证明其具备健壮性、安全性和有效性。像所有共识算法一样，块生产者(俗话就是出块人)可能导致的最大损害是审查（censorship）。所有块的有效性必须基于确定性的开源状态机逻辑。

目前正在学习区块链的路上越走越远，从go开始学起，go的并发性好，ETH的底层就是用go语言写的，设计很巧妙，go语言也很灵活。希望初链能越做越强大，把区块链技术推向另一个高潮，我现在更有学习的动力，我始终看好区块链技术，但是并不意味我看好发币，我感觉落实一些实际应用更能造福人类，把区块链技术推向正在的高潮，也能让它成为未来世界最伟大的发明。