我对于区块链的理解就是，这其中并不存在太过复杂的技能树，但首先要把作为底层技术的区块链技术了解透彻。这是了解的第一步，也是很重要的一步。就是说在谈到区块链的时候，一定是要有一个**基础的技术知识**，知道底层是数据库和数据结构市场是什么样子的。如果说望文生义，直接从区块和链这两个事情上去进行自己的衍生想象，去想象去数据库是什么样子，那我觉得这是绝对错误的。

因为我之前是学编程的，所以我想用之前在一本很有名的学习c语言的书里的语句来描述，就是“勿在浮沙筑高台”。这句话对我的启示就是学习一定要把最基础、最关键的东西读懂，比如对区块链的学习，最底层的就是了解它开发的方方面面还有它运行的原理。对于了解运行原理，我推荐的是通读**以太坊的白皮书**，把白皮书作为入门的第一步。因为以太坊相当于是比特币之后最著名的一个区块链，以太坊白皮书中也存在一种文献结构。在看白皮书的时候，你会发现它非常详细的描述了比特币区块链是什么样的、他自身的智能合约是什么样的，所以把以太坊白皮书读清楚，基本上就能对最基础的区块链是如何运行的，它的每个节点和节点之间是怎么衔接的，它中间有什么样的存储数据的结构有所了解。

然后在读的过程中，你会遇到很多**专业的术语**，比如哈希值和默克尔树。当撞上这些专业术语时，你就会顺着这个专业术语一步步去查，一步步去寻找它对应的内容。比如你去看什么是树形结构，你可以看到一些密码学基础的东西，比如什么是哈希值，它的加密原理又是什么。你会去了解这样一些的事情，以以太坊白皮书作为一个主干，同时也是一个约束，然后去**拓展**自己相关的知识。

在你对以太坊白皮书有了一定的了解之后，你可以去读中本聪开始比特币的论文。这篇文章中有不少内容，读完之后会对他**比特币的设计有更进一步的概念**。

**以上这些是最基本的入门**，是关于从0到1的跨越的内容，也是再去了解1到1.2，也就是看明白之后发生的微妙变化所需要的底层逻辑。

想要对比特币有一个更深层、更前沿的理解，我认为还可以去**阅读有关的政策或者相关论文**。

如果你比较关注区块链的应用，那我认为你应该关注一些常见的国内提出来的一些无币区块链及其相关基础应用，就是说它在哪些方面上是把它当成数据库来看。然后以此为基础，从媒体报道等渠道去了解相关的案例。有些书本上也多多少少会有区块链应用的案例。因为区块链有一个特性是难以篡改。在金融里它经常会用到这种特性，比如记账就对无法篡改的特性存在需求。记账可以用在很多地方，供应链金融、各种各样的凭证的发行过程中都会存在这样的需求。

如果你是对其他的方面比如说的**货币属性**感兴趣，那么你可以去关注它的一些定价相关的理论，然后研究对应的宏观政策。比如说它的数字货币，它会对我们的现在的法币体系造成什么样的冲击、要怎样设定上限和下限。这一部分就相对要偏理论一些，但也存在许多值得深究并且很有意思的地方，比如你可以宏观一点看它跟哪些因素有关系。它真的是一个什么数字黄金？是不是真的跟黄金一样有避险属性？它对我们的货币流通有什么作用？对我们整个经济的发展有什么促进作用？微观一点你就可以去看它的交易过程中它跟哪些币发生着关联等等。

数字货币剩下的就是**开发**这一块，即对数字货币的底层进行改进。比如说智能合约，我能不能再给它添加更多的功能？我能不能自己写一个平台？虽然写一个智能合约的平台现在对我们来说太遥远了，这不是一个人能完成的事情，但是在这一块我有一些简单的建议。我们要把自己定位成一个开发者，要去关注当前的数字货币，或者说相关的区块链在技术上发展到了什么样的程度。

这种技术上的发展分为几层。第一层是**加密上的进展**。比如，我们可以思考，是不是还有更好的算法，能让它有更好的性能。

第二层就是**共识层**。我们可以思考共识能不能改变？比特币是对还是不对？近来有很多新的共识产生。例如比特币的POW，以太坊从POW过渡到POS，此外还有DPOS，投票型，激励型。有各种激励，比如说给你提供了多少带宽，给你提供了多少存储空间。还有POSP（PO Space）等。然后包括拜占庭，这是一个大的方向，比如说像Libra的HotStuff这样的一些协议。一般来讲，共识层基本上就是上述这些，我们可以去了解，可以去考虑去开发一个什么样的共识。开发者面对的是区块链的大生态圈，我们不一定从头到尾都要会，我们可以专注于共识。

再往上的第三层，就是它的**网络结构**。网络结构也会对区块链产生影响。网络结构原来可以是线型的，可以是列，也可以是树型，它也可以有其他形状，比如可以是一个图，还可以是个graph。那么，网络结构会发生什么样的改变？这样改变会带来什么样的影响？到底安不安全？他的允许做恶的人群比例是多少？这些东西都是可以研究的。

网络结构再往上的第四层就是**智能合约**。当区块链树结构构造基本完成，再往上就是一些偏应用的层次，比如说它的智能合约的构成，它的语言用什么编写，等等。例如，现在出现了各种各样的语言，如Python和MATLAB这样自成一派的语言。这些语言之间它是存在竞争的，哪个标准被采用最多，说明大众对这一语言的认可度越高。这也是一个研究的角度。在这个层面上，目前我们对语言的研究很少。我们需要提供提供最安全、最方便的智能合约编写。这实际上跟金融也有一定联系。一个语言，如何能够既贴近人的合同语言，又在和计算机打交道的时候不出错，这块其实也是可以研究的。如果有兴趣，你们也可以去找相关的资料，这块我了解的也不是很多。

在学习区块链这一方面，除了我们说的应用项目、去找一些案例，我们至少去读一些项目白皮书，做一些学术研究、编程研究，剩下的还有研究区块链其他相关产业。比如说交易所就是其中之一。如果对这一方面有兴趣的话，你们也可以自己去了解。但是我现在有点说不太清楚这方面的情况，因为区块链的相关产业实际上是附属在一个很大的网络里，或者说，整个以区块链为主体的金融体系里有一些其他的附属结构，例如一些媒体法律机构，像交易所这样的第三方服务机构等等。这块其实也是很大一个生态，或者其实它

可能是由区块链衍生出来的生态，这也很有研究价值。这方面的研究跟区块链应用一样，它实际上也是通过一些案例，通过一些编程，比如说挖矿的编程。这种编程比较细碎，同学们需要依靠自己的兴趣，自己去寻找相关的资料，自己来学习。

区块链的学习现在是一个很新的东西，我觉得我也没法覆盖到方方面面，但是它总量来讲确实就不大，基本上就是一门课32学分差不多就能搞定的事情。

关于书籍或者文章，我最近在写教材，我们和中科院卫星黄老师、几个北工大的老师在写的区块链教材快出来了，如果出来的话可以算作，这个算是夹带私货了。其他的书籍我要推荐的不是很多。其实数字货币的监管这块也是一个很大的东西。这一块其实可能法律那边的老师会更了解一些。

如果想去了解他的**监管**的话，可以研究美国、新加坡、日本、英国这样海洋法系的监管。因为他们和中国这边大陆法系比较文件性质的监管不太一样。

法律方面可以去找邓建鹏老师。他一直在做数字货币相关的一些法律。法律这一块内容我了解不太多。

我们一般来说监管就是两种，一种是金融科技有限公司，穿透式监管；另一种是一块是这个叫监管沙箱或者监管沙盒。监管沙盒新加坡香港做的比较多，因为地方小，出什么乱子也很快就平息了，但是中国地方大，所以一般来讲不敢搞一个太大的沙箱。但是这些年中国也在提监管沙箱，比如说像北京市西城区和深圳试点。

如果是穿透式监管，一般就看美国。因为美国是把你当做证券来监管的，你要符合ABCD各种条件，好几个管理局都会介入。这实际上是美国的一贯特征。比如一个案子，会由 FBI、CIA等同时管理。