北极星|第一期·戴韡老师

###这部分放进一个框里，字小一些

自2008年10月31日“比特币白皮书”发布，区块链技术抽枝发芽，在社会各个领域开放出绚烂的时代之花。**学校小伙伴们对区块链的学习热情非常高涨**。但是，区块链领域发展成一个庞杂丰富的知识体系，从不同的角度出发可以有**截然不同的学习路径**，最终收获不同的成果……

中央财经大学前瞻到了金融科技的重要性，在国内首创“金融科技系”；校内老师、专家迅速跟进，**在区块链领域产出了大量宝贵的优秀研究成果**。因此，我们希望能**代大家向校内专家、老师讨教区块链学习方法**。

我们坚信，“师者，所以传道授业解惑也”。学校老师对学习方法、学习路径的认识一定具有**专业的认识**；不同老师的研究领域也有所不同，因而不同老师对区块链学习也一定具有**独到见解**。

在错综复杂的知识网络中，会有点点明星照亮斗折蛇行，照亮满路荆棘，正如“北极星”……

这便是“北极星”系列访谈。

###

2020年10月23日，“繁星”社社长冯云飞、小助手赵雨桐拜访了**社团指导老师戴韡老师**，向他讨教区块链的学习路径。戴老师首先介绍了区块链领域入门方式，再根据区块链技术层次（加密层、共识层、网络层、智能合约）系统介绍了深入学习的建议。我们为大家整理了和戴老师的访谈记录，希望能对大家的区块链学习有所帮助。

###这里的老师介绍也放进一个框里

戴韡老师：中央财经大学金融学院副教授、清华大学不确定理论实验室成员，清华大学数学专业博士毕业，研究领域包括不确定理论、数字货币等，在相关重要杂志发表数篇文章。

###

我对区块链的理解是：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。这是学习的第一步，也是很重要的一步。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是什么样子的。如果望文生义，直接从区块和链这两个词想象数据库是什么样子，我认为这是绝对错误的。

学习任何一项技术，我希望告诉大家的是，“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**。对区块链学习，**最底层的，就是了解它开发的方方面面还有它运行的原理**。这里，我推荐的是读一些经典项目的**白皮书**，**把白皮书作为入门的第一步**。例如以太坊项目的白皮书，它是比特币之后的项目，因此非常详细地描述了比特币区块链网络是什么样的，他同时也是区块链2.0的先驱，也比较清楚的展示了智能合约是什么样的。因此，把以太坊白皮书读清楚，基本上就能对最基础的区块链运行原理、节点之间的协作、区块链存储数据结构有所了解。



以太坊

在读的过程中，你会遇到很多**专业的术语**，比如哈希值、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。比如去看什么是树形结构，你就可以去看一些算法数据结构的书；比如什么是哈希值，你可以看到一些密码学基础的东西，基础的加密原理等等。**以以太坊白皮书作为一个主干，同时也是一个目录，拓展自己相关的知识。**

对以太坊白皮书有一定了解之后，可以学习中本聪开创比特币的论文。这篇文章中有不少内容，涉及到比特币的分叉建模等，读完之后会**对比特币区块链的设计有更进一步的了解**。

**以上这些是最基本的入门** 。想要对区块链有一个更深层、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**。这是“从0到1”，接下来就是“从1到1.1、1.2”的进阶部分。

如果希望探索**区块链的应用**，我认为应该关注国内提出来的一些无币区块链及其相关基础应用，也就是在哪些领域把区块链当成数据库来看。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。比如记账就对难以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。



戴老师耐心讲解

如果你是对**货币属性**感兴趣，我建议关注一些定价相关的理论，然后研究对应的宏观政策。比如数字货币会对我们的现在的法币体系造成什么样的冲击、私人发行数字货币为什么影响央行货币政策？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，比如宏观一点看它跟哪些因素有关系。比特币真的能做数字黄金么？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影响？对我们整个经济的发展有什么促进作用？微观一点，还可以去了解，交易过程中，它与哪些环节发生着关联等等。例如近期的JOURNAL OF FINANCE就提到了泰达币超发对比特币的通胀影响。

数字货币剩下的就是**开发**，即对数字货币的底层进行改进。比如智能合约，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**加密算法上的进展**。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。

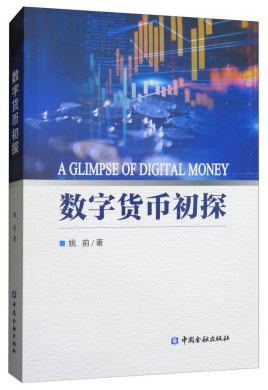
第二层就是**共识层**。我们可以思考，共识能不能改变？近来有很多新的共识产生。例如比特币的POW，以太坊从POW过渡到POS，此外还有DPOS，投票型，激励型。有各种激励，比如说，提供了多少带宽，提供了多少存储空间，还有POSP（PO Space）等，还有拜占庭，还有像Libra的HotStuff这样的一些协议……这是很大的一个方向。一般来讲，共识层基本上就是上述这些，我们可以去了解、维护、开发一个什么样的共识。开发者面对的是区块链的大生态圈，我们不一定从头到尾都要会，我们可以专注于共识。

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，还可以是个有向无环图。例如姚期智团队在推广的conflux等。那么，网络结构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。

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，语言之间是存在竞争的，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。

除了应用项目、案例、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。区块链的相关产业附属在一个很大的网络里，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。这其实也是很大的一个衍生生态，这很有研究价值。这方面的研究跟区块链应用一样，也会侧重一些编码，比如挖矿的编程。这种编程比较细碎，同学们需要依靠自己的兴趣自行学习。

如果想了解**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。他们和中国类似大陆法系下的监管不太一样。一般来说，监管有两种，一种是穿透式监管；另一种是监管沙箱。对于监管沙盒，新加坡、中国香港做的比较多，可以侧重关注。中国幅员辽阔，不倾向实行太大的沙箱。如果是穿透式监管，一般就是关注美国。



《数字货币初探》

关于书籍或者文章，除了刚才提到的白皮书，我还向大家推荐姚前老师的**《数字货币初探》**。另外，我最近和中科院、北工大的老师也在编写区块链教材，马上就要问世了，邀请大家多多关注。



小朋友们与戴老师合影

下期预告：王卯宁老师

整理：李佳阳 袁瑞婕 冯云飞

编辑：