**关于比特币的课堂报告**

各位同学大家好，我是软网1604的马冲，今天我的课堂报告主题是比特币。比特币自从**2008年中本聪在论文《比特币：一种点对点的电子现金系统》**中提出后至今已发展了接近十年，但除了在去年异常火热之外，一直都只是少数极客的玩物。但是到了今年，**区块链**可谓是站在了互联网的风口之上，各种投资公司，各种互联网公司纷纷研究起了区块链，其风头一时超过了2017年的人工智能和大数据。作为即将从业互联网的我们，我觉得不说深入研究区块链，最起码做到了解应该还是有必要的。同样，鉴于绝大部分同学和我一样能力有限，所以本次报告基本**不会涉及比特币具体的技术细节**。我的目的是科普比特币，重点是让大家理解去中心化的概念。过多的技术实现枯燥无味我相信大家也不愿意听，所以会涉及较多的关于比特币和区块链的发展情况。

今天的主要内容可以分为三个方面：比特币的简介、区块链以及比特币带来的思考。

比特币是什么？借用中本聪的话说，是一种点对点的电子现金系统。这个定义的**关键在于系统**，而不是电子现金。很多不了解比特币的人都仅仅认为其是一种数字化的货币，就像是Q币的变种一样。但是实际上往夸张的说，比特币意味的是一种全新的货币系统，其与现有的法币相比，就像是C/S架构与P2P架构的区别一样。

比特币最大的特点是**去中心化**。我希望大家能够记住并认真思考这个词。去中心化的意思是，比特币不会属于任何人任何机构，它的存在只依附于互联网。对此我们可以和法币进行对比：**法币由国家发行**，银行机构进行控制，任何一笔法币之间的交易理论上都与国家相关——国家通过控制法币的发行量来增贬法币的实际价值。你的**每笔交易实际上都依赖于国家——换个词来说叫可信第三方**，学过信息安全概论的同学一定对这个词不陌生。举个极端的例子，**国共内战**期间，万恶的国民党通过无限发行金圆券在不到两个月的时间内，从我们伟大的劳动人民手中强取豪夺了总值超过2亿美元的黄金白银。

另外一个例子是在**二十世纪的美国**。1933年，美国总统罗斯福通过了政府法令：所有美国人持有黄金都是非法的。然后美国政府通过强行用美元交换美国人手中的黄金强行推高黄金价格，从而使美国债务贬值，勉强对抗当时的经济大萧条。直到1975年，美国又恢复了美国人民对黄金的合法拥有权。补充一句，我国是在1982年才能合法拥有黄金的。

以上两个例子虽然极端，但是不可否认的是，即便是国家，有时候也会为了经济利益拉下脸来强取豪夺人民的财产。

然而去中心化的比特币就不存在可信第三方的问题。比特币之间的交易不需要第三方的认可，你的就是你的。就如同网上论坛中所说：**比特币第一次从技术手段上保证了私有财产神圣不可侵犯**。

比特币拥有一种美称：**数字黄金**。比特币的诸多特点均可以看出黄金的影子，因此有人说，如果你觉得比特币不靠谱，那么把你的观点带入到黄金身上看看是否适合。

比特币总量2100万，地球上黄金的储量也有限；

比特币需要耗费电力算力来挖矿，黄金也需要；

比特币虚拟化易携带，但黄金是实体不易携带；

比特币和黄金一样有一定的价值可以存储，也可以依靠价值波动进行炒作。

以上，是**理论中的比特币**的样子，不管你信不信，从客观上来说比特币就被设计成了这样。但是**在现实中的比特币**至少在目前并没有在货币市场起到相当大的作用。现实中的比特币更多的用在了**炒币和非法交易**上。

先说**非法交易**。比特币匿名化的特点使其天然适用于见不得光的产业中。截止目前，比特币真正的发挥其货币作用的地方绝大部分都在暗网的非法交易当中。

比特币之所以会被用来炒完全是因为其**剧烈的价格波动**。大家可以看一下这几幅2013年左右比特币兑换美元的价格图。其价格波动幅度之大，远远超过了任何一种投资商品。因此比特币市场也难免涌入大量不懂比特币却又妄想着暴富的小白，期望能通过炒币来迎娶白富美走上人生巅峰。知乎上也有一个这样的回答。2011年的比特币价格我查了查是31.9美元，而截止我完稿时其价格为6728美元，超过210倍的收益足以说明为什么有这么多人为之疯狂。另外值得注意的一点是，比特币历史最高价是在去年十二月份，超过了18000美元每枚。

除了买卖比特币，虚拟货币市场还有另外一种可以牟取暴利的方式——**ICO**。ICO是初始货币发行的意思。由于比特币的代码是开源的，许多黑心商人假借数字货币的名头简单改几行代码就可以创造出一种全新的数字货币。在其发行之初庄家通过自己倒卖来创造的暴涨假象来诱惑小白大量买入。庄家收钱跑路，小白就只能交点智商税。ICO远比炒币来钱快，所以很快就引起了国家相关部门的注意，**2017年9月，政府终于下令禁止ICO**，连带着关停数字货币交易所。自此，比特币在中国和法币交易的途径已被堵死。

我们可以看到，虽然从理论上来看比特币无比美好，但实际上能够真正用到比特币的地方都不怎么合法。比特币作为一种新型的货币系统还是有很长的路需要走。

接下来说一说**区块链**。所谓的区块链，高度概括来说，就是一种去中心化的数据记录与存储体系。区块链中数据的存储方式类似于**链表**。链表节点——通常称其为**区块**——之间通过哈希值相连而不是指针。**每个区块主要存储当前和上一区块的哈希值、时间戳以及具体的数据记录**。

不同服务器之间通过一定的方式来获得下一区块的**打包权**——你们可以理解为更新数据的权力，然后通过广播的方式来和其他服务器之间同步数据。具体的打包权竞争目前**有POW，POS等算法**。

区块链在目前最主要也是最佳应用的地方就是银行的**支付清算业务**，尤其是在金融方面。大家可以设想一下，很多个银行之间都有转账操作，难道结算的时候就跟笛卡尔乘积一样各自结算？还是说像我国一样由中央银行统一结算？各自结算的成本开销不用多说，而统一结算又使整个系统过于中心化。区块链则无疑是最佳的选择。

至此，关于比特币以及背后的区块链技术的科普基本结束了。最后，我觉得大家有必要来思考一下我全篇都在提的一个词——**去中心化**。

中心化自然有**中心化的好处**。最典型的例子就是中国。中国这几十年的发展完全靠的就是我党统一力量集中建设。但是同样我们也能看到，如果过度的集中势必会在协调上浪费大量的成本，导致效率反而极其低下。这一点在金融方面体现尤为明显。以中央银行作为中心来集中进行结算的成本远远高于各个银行以平等节点的身份运用区块链的技术来结算。

同样在前边的例子中我们也可以看到，**作为中心的节点即便是国家也不一定是可信的**。

从深层次意义上来讲，比特币的意义远比它表面上暴露出来的多。比特币之于金融领域完全可以说是一个新的方向。**从古时以物易物到发明货币可以说是巨大的进步，那由国家这种中心化机构发行的法币到去中心化的虚拟货币同样是巨大的进步。**比特币的出现是**对国家拥有的货币发行权的一种挑战**——民众愿意用什么当货币是民众的权力，不管是贝壳还是比特币，只要民众承认并使用，那它就是货币。然而现实是：国家垄断了货币的发行权，并把其作为一种管控经济的手段，经常通过滥发等手段来间接剥夺大众的财产。这也就是为什么有人说**比特币通过技术手段实现了私有财产神圣不可侵犯**。

网上有的分析认为，**比特币的最高使命是以技术手段来限制政府滥发法币。**换句话说，就是让比特币作为一种新的货币来同法币在市场上竞争，法币的份额越小，则越不敢滥发，否则当大众都使用比特币时，国家的经济命脉就无从保证。

然而，理想是美好的，现实是残酷的。在我看来，不管比特币背负着多么光荣的使命，能不能实现还是个未知数。人人都说共产主义社会好，但它今天也仍未实现不是么？我们也自从初中政治就学过那句“我国正处于并将长期处于社会主义初级阶段”。比特币作为一种新兴的事物，它还**需要时间**进行成长。**不管是真的成为了颠覆金融领域的下一代货币，还是像世界语一样最后无人问津，时间才是检验真理的唯一标准。**

我的课堂报告到此结束，如果大家有什么问题可以提问。