**比特币是骗局吗？**

*作者：浅析 2017.10.22*

很多时候人们论“数字货币”的时候会把它与“法定货币”进行比较。这样其实会产生误导，不利于理解真实状况，因为“数字货币”与传统的货币和证券相似之处很少。所以在这篇文章里面，作者采用“数字资产”替代“数字货币”，这样更利于表述和区分。

有人认为数字资产没有内在价值，政府会摧毁它；也有人认为数字资产将从此会颠覆银行／政府／硅谷科技巨头。其实这两种极端的观念都没有真实的反映现实状况。

现实状况是以下事实同时存在：

\* 当前的数字资产市场处于非理性的狂热状态中；

\* 其中有很多所谓的“创新”，以及骗局；

\* 其中有很多的利益冲突，虚假宣传，刻意的混淆；

\* 主流媒体／金融行业／科技行业／学术界／政府机构，甚至那些正在购买数字货币的人，在这些群体中只有很小一部分人真正理解现在正在发生的改变；

\* 包括作者自己在内，也有很高的可能性不理解现在正在发生的改变

与此同时

\* 银行／政府并没有消失或有消失的趋势

\* 科技巨头／传统公司的组织架构也没有消失或有消失的趋势

所以现在的状况是各种信息混杂一起，既有人为产生的噪音，也有真正指示未来趋势的信号。

在近一步探讨之前，有必要对数字资产做一个定义。

数字资产是一种新的资产类别（new asset class）。就像任何一种资产类别一样，它作为一种收集资源的机制，把获取的资源提供给特定形式的组织，在这里对应数字资产的组织形式称为“去中心化应用”（decentralized applications）

举例：

股票是一种资产类别，它将大众投资提供给上市公司供其经营。

国债是一种资产类别，它将筹集到的资金提供给政府供其进行国防开支／提供公共服务／进行基础设施建设。

房贷是一种资产类别，它将银行贷款提供给购房者供其购买房产。

所以数字资产也是一种（新出现的）资产类别（而已），是为“去中心化应用”这种形式的组织服务。

具体到比特币，它是为了“去中心化的点对点支付应用”服务。

那么什么是”去中心化应用“？

”去中心化应用“是一种运营方式，在这种方式下不需要依靠某一个特定的主体（但还是要有某一个主体）进行运营，却同样可以提供持续稳定的服务。

“去中心化应用”是一种全新的组织架构形态，它从上至下，在生产／融资／运营等方面采用全新模式。目前还很难说这种架构比传统的组织架构更好或者更坏，因为在有些方面“去中心化应用”做了牺牲，以便加强另外的方面。我们只能说这两种架构有很多本质上的区别。

“去中心化应用”中最早出现的比特币是如何运作的？如何做到在不需要第三方中心化机构存在的情况下，进行支付并保存更新交易记录？

比特币的解决方案：让所有网络参与者竞争，胜利者对交易进行验证，确认交易的合法性。这样虽然“每次验证都需要有这样一个机构或个人存在”，但是可以避免“长期对某一个特定机构或者个人”的依赖。

让参与者竞争。听起来很像市场经济，但相比真正的市场经济，似乎还缺少一点什么。

实际上缺少的是一种激励参与者竞争的奖励手段。或者更直接一点来说，一种资产。

这种激励参与者竞争的资产就是比特币，参与竞争并验证交易合法性的人就是矿工，比特币通过代码开源、网络开放的方式让任何人都可以在任何时候参与进来。

怎么样进行竞争？比特币规定，矿工们要根据一定规则去寻找一个随机数字，找到这个随机数字非常困难，需要消耗大量的CPU计算量和电力能源。就像电影《巧克力工厂》里面，富家女买下成千上万的巧克力，寻找可以进入巧克力工厂的“黄金门票”，都是一种暴力搜索的方式。

为什么要通过这种故意设定的，消耗大量能源的方式让矿工进行竞争并验证交易？

数字资产是互联网世界中那只无形的手，比特币是存粹的资本主义，更是存粹的自由主义。

通过这种机制，比特币的设计者一箭双雕：用来激励旷工们耗费真金白银来维护去中心化网络这件事情所能得到的奖励品，与在这个去中心化网络中所使用的货币，是同一个东西，即比特币。从而解决了先有鸡还是先有蛋的哲学问题。

简单来说这就是比特币以及其他“去中心化应用”的运行方式，它能以一种“无需信任”的方式做很多现在用中心化的方式也能做到的事情。例如存储文件Filecoin vs Dropbox。

这是一种奇迹，仅仅只是互联网、开放协议、加上一种新的资产，人们创造并实现了一个可以动态的获取各种必要资源提供各种服务的网络，而这一切是自动自发的，无需一个中心化的机构来运行。

因此很多人认为这就是未来，这将对现在的金融巨头和软件巨头带来极大的挑战。

但是作者不这么认为。因为去中心化应用有自己的问题。去中心化应用对大多数人的用处并不十分清晰。你很难对所有人解释比特币比PayPal能更好的完成支付功能，Filecoin比Dropbox更好的完成存储功能，以太坊比Amazon EC2更好的部署应用服务。

实际上，在绝大多数的方面，去中心化应用要比中心化应用的表现要差：

\* 处理速度慢

\* 运行成本高

\* 可扩展性低

\* 用户体验差

\* 系统管理难度大

……

但是不要误会，存在这些问题并不是因为去中心化应用是新事物，而是从它最初的设计上就已经明确，其他目标都要遵从于最核心的目标：去中心化。哪怕这意味着性能上的妥协。

以比特币为例，最好的描述并不是”去中心化的Paypal”，而是一个“及其低效的电子支付网络”，但是作为交换，这是一个“去中心化的电子支付网络”。

所以中心化应用几乎在所有方面都击败去中心化应用，除了一点。这点不仅仅是去中心化应用优于中心化应用的地方，而且是只能依靠去中心化应用实现的地方。

抵御审核（Censorship resistance.）

抵御审核，意味着不受约束的使用去中心化应用，并且在这些应用中的交易不可逆转和篡改。只要我能连入网络，用数字资产进行结算，没有人能阻止我的比特币交易，没有人能阻止我在以太坊里面执行代码，没有人能阻止我在Filecoin里存储文件。

所以尽管我们不能得出“对所有人来说比特币比VISA要更好”的结论，但是对于某些用户来说比特币的确是唯一的支付方式。

问题是哪些客户？哪些客户可以接受速度慢、费用高、效率低，但是能抵御审核的支付网络？

虽然没有准确的数据，但是去中心化应用的用户大致有两类：

\* 不能接入现有网络的的人群。例如生活在缺乏传统服务基础设施，但是可以有互联网接入的边缘区域的人群。

\* 不愿意接入现有网络的人群。例如不想暴露自己交易信息的人群。

可以进一步的问：

对于谁来说，比特币是最好、唯一的支付方式

对于谁来说，Filecoin是最好、唯一的文件存储方式

对于谁来说，以太坊是最好、唯一的程序执行平台

通过这些问题可以了解去中心化应用的核心价值

有哪些用户会真正使用去中心化应用？这些用户会成为未来市场的主流用户吗？这些问题很难现在预测，因为这不仅部分取决于技术如何发展，更大程度上取决于社会大众如何反应。

一个例子。直到不久之前，加密短信服务仅仅被黑客、间谍、阴谋论狂热份子中使用，丝毫没有在普通人群中爆发的迹象。直到斯诺登事件之后，一夜之间到处是使用Signal、Telegram进行端到端加密通讯的用户。不能否认加密通讯技术的确有了一些进步，但是造成主流用户群体大规模使用的根本原因是社会大众的观念变化。

这是否是一场革命？这能否成为未来经济体系中的关键组成部分？数字资产的价值是否会爆发增长？由于还处在非常早期的发展阶段，以至于现在任何判断都言之过早。正是因为未来很难预测，所以越来越多的资本在这个领域开始投资。聪明的做法是，在早期开始投入并不断观察其发展，避免错过以后可能的重大机会。

长期来说，某种数字资产的价值，由采用这种资产的去中心化应用被人使用的程度来决定。

虽然现在处于早期，但还是有比较充分的理由对目前数字资产做较高的估值（例如比特币5000美元）。因为即使在未来数字资产被大众接受的可能性较小，但是带来的影响力却将十分巨大。

标签：比特币；区块链；以太坊

**注：**

*本文是基于Chain公司创始人Adam Ludwin在10月16日公开发表的，用来回应JP Morgan CEO Jamie Dimon近期对比特币的一系列看法加上作者的理解并整理内容若有不当之处请多指教*。

*相关链接如下：*

[*https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80?from=groupmessage&isappinstalled=0&gi=8ffd154d2e03*](https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80?from=groupmessage&isappinstalled=0&gi=8ffd154d2e03)

【声明：文章为作者独立观点，不代表UNITIMES官网立场。欢迎转载，转载请务必注明来源。如有不当之处请多指教】