每日区块链思考

日期：2018.03.15 Tru.

区块链的本质是一种创造性的分布式的信任模式。所有的交互都需要信任，不过是信任的程度决定交互的深度。基于不同的信任基础设施也有不同的信任模式：

1. 交互双方的直接信任（认证），面对面交易；
2. 基于平台中介的信任，B2C\C2C的网商平台交易；
3. 去中心化（中介化）的信任，P2P模式

区块链的信任模式是基于公共账本的信任，账本本身的公开透明、不可篡改和可追溯特性可实现两个方面的信任。

1. 对于过往交易记录真实性的信任；
2. 对于当前发生的交易会被真实记录的信任；

对于公共账本及其运行机制的信任，使得交互双方不需要直接信任也不需要中介化的信任，可方便地实现交互协作提高效率降低成本。

日期：2018.03.27 Tus.

区块链所表现出来的数据安全和隐私保护特性是由其共享账本式的分布式共识（信任）模式所带来的。

区块链技术中的Hash、签名等安全机制在当前的中心化网络环境下一样可以实现，而且在一定程度上效率更高。（主要是在共识效率上，通过中心化机制可直接达成整个系统的共识，再通过统一的状态复制达成系统所有节点的状态一致。）但其同时也带来了另一方面的安全问题，即：1）中心化节点本身的安全问题；2）中心化管控系统运营状态不公开不透明的信任担忧；3）数据隐私泄露的问题。

而区块链的公开透明，本身就可以增加相互间的信任，相互独立的节点彼此没有直接的利益关联，也增加了非技术层面的安全性。

“共享经济”新生代，基于Token的价值转移可实现不同“信任域”之间的协作。

日期：2018.05.21 Mon.

区块链为解决不同信任域实体之间协作的问题提供了一种可行的思路。

原有体系下各实体属于不同的结构网络，应用不同的规则由各自的中心化节点管控形成了各自不同的信任域。信任域内的节点之间交互协作可通过自身域内中心化管控机构的身份认证、纠纷协调等机制提供保证，实现相互信任完成协作。而不同信任域的实体之间要进行交互协作，则会面临各中心化系统之间不同的规则、不同的机制如何达成信任完成协作的问题。而区块链提供了一种可行的解决方案。

1. 去除彼此的中心化信任机构，打破协作的壁垒；
2. 用统一的规则和不可更改的记录，实现交互协作的公开透明和相互信任；
3. 剪除臃肿的信任机构，提高效率降低成本。

有观点说区块链技术是一次生产关系的变革，会对人类的生产生活产生巨大的推动作用。我觉得有一定的道理，还记得马克思哲学讲到生产力和生产关系的矛盾运动是推动社会不断前进的动力，而在资本主义社会的基本矛盾就是生产资料私有制同社会化大生产之间的矛盾。当前社会发展的现状和区块链所描绘的蓝图恰好反映了这一点。或许区块链真能达到上述评论的高度，但其自身必须要发展完善，而当前区块链的发展还处在初期阶段，还存在诸多问题。

1. 基础链的性能问题，TPS
2. 共识机制的问题，POW\POS\DPOS\PBFT\DAG性能与安全性和区中心化的权衡
3. 区块链存储问题，IPFS\Sia\Storj
4. 智能合约的安全性问题
5. ……

这些问题都是限制区块链发展和应用的关键

日期：2018.07.04 Wen.

6月币圈深处熊市，公链项目的集体爆发，世界杯的主题也没能挽救低迷的行情。被寄予厚望的EOS上线主网后也没了动静反倒是问题连连漏洞不断。突然出现的FCoin成了一大亮点，无论是“交易即挖矿”还是“创业板上币”都赚足了眼球，吸引了大量用户半个月交易量就跻身全球交易所首位。

有人说FCoin是在用传统的互联网思维即通过不可持续的烧钱抢夺用户在谋求发展。也有人说FCoin是真正的交易所的颠覆者，真正让利于普通用户。而对于大多数用户来说根本不关心这些，他们只知道FCoin的“交易即挖矿”能够赚钱。而基于项目热度和社群发展的“上币”规则更是点燃了项目方的热情，疯狂空头发币奖励用户充值，让FCoin的用户数再度激增。

不论FCoin是真心让利于广大普通用户还是吸引用户的各种套路，至少在一定程度上是成功的。归结起来有几点：

1．“交易即挖矿”的创新模式，从08年中本聪发表比特币白皮书算来区块链已经走过了10个年头，各行各业都在说区块链思维模式，但真正理解用好区块链思维的寥寥无几。传统的金融和互联网思维还是深入人心无法轻易跳脱。

FCoin的“交易即挖矿”模式一出引来无数质疑，100%交易费返还外加持币分红80%交易费，另外交易所也会获得相应的收益，怎么算都觉得不对。从用户的角度交易费全额返还持币还有分红绝对的稳赚不赔，从交易所的角度用户交易解锁代币同时还有20%的手续费收入那也是绝对赚钱的买卖。

那么钱从哪儿来，不少人认为FCoin就是“资金盘”以资金购买用户来带动平台增长，玩一场庞氏骗局的游戏。

但细想下来却也不是这样，就像“交易即挖矿”所说将FT的Token发放形式类比挖矿。比特币通过计算哈希贡献算力挖矿奖励btc来抵除费用和赚取收益，而FT通过交易来挖矿奖励FT来抵扣交易费。以交易挖矿的模式来吸引用户进行交易满足不同用户对于币币交换的需求，从这个角度来看这种方式也是合理可行的。

原来的交易是从交易需求的角度来看，用户在交易所进行交易是为了满足自己的需求，交易所提供平台和管理收取费用。而FCoin则鼓励用户交易，用户更多的是各种代币的提供者满足其他用户的需求，完成交易获取相应的代币奖励。

2．“社区化”的经营模式，传统的交易所的经营都是通过收取交易费和上币费来盈利，发行平台币也主要用于抵扣手续费和分红。这种模式下交易所和用户联系并不紧密利益相关性不大，交易所的经营更多的是靠自身的推广营销和运作。

FCoin则是通过一种“社区化”的模式来运营。首先，在平台代币的发行上通过交易获取，平台收取交易币种的手续费按比例兑换FT代币返还给用户。这种另类的代币发行方式，是的交易所的运行和用户的交易紧密联系起来。其次，FT代币的持有者相当于交易所的股东，实际收取的各种币的手续费按比例分红给FT的持有者而且比例高达80%。再次，FCoin白皮书里显示，FT持有者不仅享有收益分配的权利，还享有参与社区治理决策的权利，包括社区委员会的选举等。

相比于传统交易所，FCoin的经营模式更加“社区化”，人人建立社区，人人获得收益。