

井通区块链的哲学思维

在2008年的时候，当华尔街金融精英们导致的全球金融危机席卷大家的生活的时候，中本聪创立的比特币系统也应运而生了。

比特币系统，作为一种点对点（英文P2P Point – To – Point，建基于bitTorrent技术）的电子现金系统，首先要解决的是，剔除金融机构作为第三方验证和保证的角色。

大家不要小看这个设计，因为人类社会的深度分工，离不开金融系统的存在。而我们人类个体或者组织的互相交往之间，在社会分工的综合计价和支付上，都离不开金融系统扮演的第三方验证的角色。

那么中本聪代表的全球技术精英，尤其是美国硅谷的高科技精英，常常有种以天下为己任的自傲心态。当他们和整个社会的实体经济（Main Street）被华尔街金融精英的虚拟经济（Wall Street）所激怒的时候，如何想出一个技术上的解决方法，来达到人类社会，不需要金融机构的参与，应该是一种彻底解决华尔街腐败而绑架全社会的终极方案。

这个也是为啥比特币系统一出现，就先遭到了华尔街代表的银行系统的仇视和封杀。别说是传统银行，关闭任何个人和比特币相关的账号，连Paypal这样的后来者，也对比特币参与的账号，进行封杀。比如我自己的款项，就被Paypal冻结过。

当然，用数字签名（Digital Signature），这个密码学已经发展了多年的公私钥配对（Public / Private Key Pair）来解决第三方验证机构的依赖，前人已经做了不少的先驱工作。其中比较有名的就是美国华裔科学家戴伟，因此今天以太币的最小单位，还是用Wei来命名作为纪念。

但是这个方案，还是不能解决双重支付（Double Spending）。

那么中本聪的杰出贡献，是运用了随机散列（Hash）对全部交易加上时间戳

（Timestamping），将每个一定时间段（10分钟）形成的交易总和，汇聚成一个区块

（block），并将每个区块，通过建立于随机散列的工作量证明（POW，Proof – Of – Work）的链条，串在一起形成了一个区块链（Blockchain）。

那么这样形成的交易不可更改，除非你可以将已经完成的全部工作量重新完成。因此这种方法，导致了对双重交易的禁止。

而通过获得创立新区块的权力的随机散列验证（俗称的矿工挖矿），同时获得了新的比特币的产生的奖励，也同时解决了央行发币的问题。

但是，正是比特币系统，对央行的法币的发币，持有海耶克的浪漫情怀，也导致了各国的金融监管部门和中央银行，对比特币系统的暧昧态度。

一方面政府机构，不会接受对法币系统权威的垄断性提出挑战，另一方面，对比特币的新生事物，其中的技术意涵，也引起了政府的关注。

当然今天看起来，大家都知道区块链成了风口，好像所有人，以及家里的阿猫阿狗，都在讨论区块链。但是回到以前，这个概念还没有被完整提出。

当时，对这个技术非常有看法的先驱人士，包括硅谷著名的安德森，都是用大写的比特币

（Bitcoin）来描述比特币系统，而用小写的比特币（bitcoin）来描述比特币系统底层的区块链技术。

那么我们的井通，也正是在这个时候，开始酝酿和产生的。

在井通产生的同时，在如何用区块链技术来解决实际问题，基本上走了两个不同的路径。

第一个，就是利用比特币系统已经存在的现有架构，对比特币协议里面的部分内容重新定义，从而开发出新的应用。

走这条路子的，包括MetaCoin，ColorCoin，等等。大家要区别以比特币系统建基的支付应用，比如Circle和Coinbase这些，和企图在比特币系统上面，开发出的例如智能合约等等其他的应用。

这种做法的好处是显而易见的，因为你可以依赖比特币系统在底层的支持，而无需自己开发一套可用的底层系统。但是其缺点，也是显而易见，因为如果你应用上的需要，无法简单地进行改动，而需要在底层功能上改进的话，你很可能难以说服比特币技术委员会，来做出符合你需求的变动。目前比特币社区，关于继续保持区块的1MB的规模（只可以每秒钟处理7个交易），和依靠硬分叉来扩张到2MB的争论（Bitcoin Core vs Bitcoin Classic），不光是关于定义比特币系统为一个现金支付系统（中本聪的愿意）和一个交易的清算系统（目前的发展），而且也牵涉比特币系统应该彻底去中心化，还是要向现实妥协，有限的去中心化。

基于这些哲学思维的不同，井通一开始就选择了另一条路子，就是建立自己的底层系统。

这条道路上，井通的同路人，包括瑞波（Ripple）和以太坊（Ethereum）。

当然这些系统的方向，是不应该与拷贝比特币系统的山寨币（莱特币，狗币，元宝币，暗黑币等等）相同并论。毕竟这些系统，建立底层平台的原因，是更好地服务以上的运用。那么在自己建立系统的实践过程中，井通提出了自己的一些哲学思想。

1. 当作为中心化的云计算／大数据兴起的时候，作为其对立面的去中心化的区块链，也正常兴起，正好是中国人思想的阴阳平衡的体现。
2. 因此和我们海外的同行不同，追求替代中心化的极端去中心化路线，我们认为区块链不是云计算大数据中心化的替代，而是补充和平衡。正如老子所言，阴在阳之内，不在阳之对。
3. 我们认为，相对于彻底或者极端去中心化的想法，我们追求的是一种中心化／去中心化的平衡。我命名为“有效去中心化”，也注意到经历了DAO的惨败的事件，行业人士开始了认为“有限去中心化或者成为区块链主流”的认识。对此，我们很自豪地说，有效去中心化，一直就是我们这3-4年的基本方针。
4. 有效去中心化的基本思路，就是如何在保持中心化带来的高效率的优点，又同时避免其带来的可靠性的缺点。我同时认为，这个有效的界定，应该是一个区间，而不是一个优化点。要根据不同行业的实践，来确定这个区间的更精准位置。
5. 有效去中心化，是可以进行量化的。比如首先就是要打败南翔挖掘机，避免一台挖掘机，就可以打败支付宝。
6. 鉴于如此认识，我们井通的共识机制，没有采取比特币的全民直选方式，也反对中心化的寡头决策方式。我们用的是PBFT改进型的新方式，扬弃了传统的POW，POS和DPOS的弊端。这种方式，可以叫做代议制下的全国人民代表大会制度。
7. 井通的智能交易撮合系统，以及智能合约系统，也是通过分层和分级的控制，不会出现以太坊的DAO这种激进的方式。

井通的很多哲学思维，不可能在这样的一篇短文里面全部体现出来，而是我们这3年来，不断进行区块链实践中，获取的点点滴滴的成果。井通欢迎各位有志的同行一起参与建设区块链的实践应用。