区块链已经是一个世人皆知的名词了，有人甚至断言，未来人类社会的一切都将以区块链为基石。但若问区块链究竟是个什么技术，各路“专家”的解释可谓语焉不详：有些堆砌常人不可理解的术语，有些大谈其潜在应用，有些干脆冠之以“第四次工业革命”——至于区块链的本质，大家终究还是不甚了了。

之所以闪烁其词，原因并不难猜。就功能而言，区块链无非是一个特殊方式加密的公共数据库，这种毫不性感的概念是没法用来炒作的。当然，区块链吸睛如斯，其内涵和外延不可能如其功能般缺乏营养。要把它讲清楚，我们需要了解大量技术本体以外的信息，而其中的重中之重便是以比特币为代表的虚拟币。

区块链的痛点

放在五年前，世上并无太多人知道什么是区块链。作为比特币的底层技术，这个系统以数据块（block）的形式进行传输，并以末端追加的方式将数据块连成链状（chain），因而得名区块链（blockchain）。从技术层面看，区块链和之前存在的IT技术之间没有显著的壁垒，并无革新性的进步；但从价值观层面看，它们则有根本性的不同——以前所有的技术都旨在提高效率，而区块链是反其道而行之的。

鉴于比特币是区块链标志性的存在，我们不妨拿它作为样本。

比特币体系内的每一笔交易记账都在全网范围内由无数个用户验证，验证通过后，该次交易才能成立。而第一个成功记账的用户可以得到一定量的比特币奖励。这个信息处理过程俗称“挖矿”。目前比特币系统的活跃用户数约500万人，2017年全年处理量约3000万笔交易。3000万笔是个什么体量呢？2017年11月11日这一天时间里支付宝完成了14.8亿笔交易，约为比特币全年交易量的50倍。

这个差距并不说明太大问题。毕竟比特币的用户数远低于支付宝，应用场景也远少于支付宝，所以交易量有数量级的差别并不奇怪。真正说明问题的，是支持这3000万笔交易所消耗的电量：外媒Digiconomist公布，2017年比特币系统消耗的电能达到了300亿度，占全球耗电量的0.13%，超过数十个国家的全国年用电量。换言之，处理一笔交易，比特币系统平均需要消耗1000度电；以我国居民电价计，相当于每个活跃用户人均承担电费3000元。如此匪夷所思的耗电量意味着巨大的算力配置，这与其渺小的处理功能形成了强烈反差。

“去中心化”的低效，不只体现在算力，还体现在数据存储。

继续以比特币为例，众所周知，比特币（区块链技术）要求用户分布式储存公共账本。其背后的逻辑很奇葩：“去中心化”理念认为中心账本的管理者会作假，故账本的存储必须公共化。目前完整的比特币公共账本大小已经超过150GB，并以每年

数十GB的速度快速递增——仅仅为了支持500万用户每年3000万笔交易。如果有朝一日其处理量与目前的支付宝比肩，那每年比特币账本的大小将增加超过500TB。这相当于把支付宝服务器的存储数据在所有用户的个人电脑上进行备份，其荒谬性是显而易见的。

为了解决这个问题，比特币系统现在允许用户存储不完整的公共账本，即“轻钱包”，但其交易验证仍然依赖网络上其他人的完整账本。我们试想，当公共账本大到绝大多数人都无力完整存储的时候，仅剩的那些完整用户节点不就又成了中心账本吗？

把视野延伸到虚拟币以外的区块链应用（如果存在的话），公共账本需要记录的将不仅仅是纯数字的交易金额，还可能是每一辆车的保险信息、每一个人的信用信息，这些多维度的数据若也要“去中心化”存储在每个用户的终端上，那我们需要的将是天文数字级的存储空间。短时间内，这将是一个不可能解决的难题。

从哲学高度讲，科学的本质是怀疑，宗教的本质是相信。区块链作为科技范畴内的概念，是如何让众人无视诸多悖论、沦为其信徒的呢？答案当然也离不开比特币，这个现世的造富奇迹。

比特币的哲学

不知从何时起，大佬们开始刻意把比特币和区块链作为两个概念割裂开来，众口一词称比特币只是区块链的应用之一。

其中的动机是多样的。

但凡稍有经济学常识的人都知道，比特币不可能成为正常经济体的通行货币。它自带通缩属性，无视货币政策，与现代经济理论八字不合。更重要的原因是，它所挑战的信用货币，实在是过于强大了。全世界除了少数几个失败国家，清一色都是基于政府信用发行货币的。信用货币之所以也被称为法币，是因为绝大多数国家都用法律明确规定，本国货币为国内流通领域“必须接受”的一般等价物。通过这种方式，国家确保信用货币不被拒绝，也同时保证了货币持有人的权利不受侵害。换言之，信用货币并不是凭空发行的，它背后有政府信用背书，有国家机器撑腰。

而比特币的发行机制（也就是挖矿），其用意就是把政府的货币集权“去中心化”，背后则是对政府存在之合理性的质疑。

前面已经提到过，“去中心化”的逻辑出发点是对中心化机构的不信任。比特币原教旨信徒之所以选择用“机器共识”来代替“制度共识”，根本上的理由是认为政

府主导的货币发行制度无法体现公平正义——通胀、贫富不均——这些比特币试图解决的问题，无不指向建制。从这个角度看，比特币低效的共识机制也就有了“效率换公平”的哲学意义。

如果技术的进步终将让损失的效率忽略不计，那是否意味着“不值得信任的”中心化机构就无需存在呢？

这是一个危险的问题，好在我们暂时不必作答——因为比特币的“公平化”尝试已经基本失败了。

比特币设计者的初衷，是希望比特币参与者在同一时期能大致机会均等地获得比特币。为此设计了一个相当精巧而理想化的区块链算法，也就是所谓的PoW（ProofofWork，工作量证明）机制。通过穷举随机数变量，第一个得到特定要求哈希函数值（Hash）的用户将有权记账该轮交易，并获得对应的比特币奖励。基于PoW机制，每个用户获得比特币的概率直接由他贡献的算力决定，投入越多，回报越多，看似合情合理。

当然，事情没那么简单。

一方面，比特币的PoW是极其耗能的，每次生成随机数获得特定要求哈希值的预期概率是1/62^18(不到亿亿亿亿分之一)，所以全体设备需要海量的穷举运算才能决出记账权。比特币高昂的运行成本极大程度上应归功于这个“公平”的激励机制。

另一方面，比特币设计者对算力分布做出了严重误判。他本以为用户会老老实实用CPU运行挖矿程序，而受限于CPU的核心个数和成本，单一用户不太可能集中太多算力。然而后来发生的事情大家都已经了解了，从GPU到矿机，再到大型矿坑，一个旨在去中心化的系统已经近乎寡头化。

比特币之所以会严重背离其理念，原因其实并不偶然。

规模化的生产给“矿业巨头”带来了诸多好处：更强的电费议价能力，更高的固定资产利用效率，更低的综合人力成本，更薄的研发摊销成本。即便是比特币这样的虚拟产品，其生产过程终究还是符合边际成本递减这一朴素的经济学规律，这便是中心化存在的必然性。从自然科学角度看，类似的结论同样成立：一盘散沙的个体是熵值最高的状态，而高熵意味着无能。

有些人认为，是PoW扭曲了比特币理念，降低了效率，诱发了算力竞争，把它废止了问题就能迎刃而解。于是他们设计了PoS、DPoS等新的激励机制。依我愚见，这些努力是不会有结果的，因为在“效率”和“公平”这个跷跷板上，你不可能满足

所有人，甚至不可能满足大多数人。

说得再玄一点：任何一种虚拟币激励机制都是一套经济制度——“死的制度”不可能保证一个动态经济体系稳定运转，只有“活的人”可以。

脱币化的困境

由于比特币的种种问题，圈内的有识之士意识到，继续把区块链和比特币绑定在一起，必将一损俱损，以“技术无罪”的名义切割关系已是当务之急。这不单是应时势，更是遂人愿：比特币的影响已经过于深远，若不把区块链解放出来，后来者的致富空间将被压榨殆尽。

然而，区块链真的可能脱币化吗？

很多不明真相的普通人，甚至一些知名投资者都觉得“真实，不可篡改”的区块链单凭技术本身便存在无限的价值。

对此我要说，这中间误会太大了。

比如银行间结算，即便区块链系统成功完成了记账操作，但某无赖银行拒绝对外打款，区块链能代替法律、保证对手银行权利不受侵害吗？再如产品防伪，即便二维码全程无误，但卖家第一时间在盒子里装的就是次品，区块链能施展魔法、让顾客顺利收到正品吗？事实上，区块链的“真实，不可篡改”，充其量只能作用于虚拟信息，它的触角根本伸不到现实世界。

然而，现在这些概念正被有意无意地滥用。负责任地说，大部分号称前景远大的区块链应用，完全是基于“真实，不可篡改”字面意思的臆想，提出这些应用的人并不理解区块链技术本身，他们找到的只是一些以“真实性”为痛点的应用场景而已——而此类场景当然是无处不在的。然而，最后所有人都会发现，即便克服了低效冗余安全性等众多难题，想象中的区块链需求依旧不会出现。

因为这很大程度上不是个技术问题，而是个经济问题。

区块链的“去中心化”设计意味着系统运行成本会被分摊到每个用户头上，但理性人的天性从来都不是共享和奉献，而是搭便车。以比特币为例，且不讲矿机之类的硬件投资，仅是电费一项，活跃用户人均就要支付每年3000元人民币。如果区块链应用不产生切实的个体收益，就不会有自发的参与者，即便勉强参与了，其可靠性亦会存疑。所以，区块链的商业应用断不能和激励机制脱钩。

说得更深入点，区块链的共识，并不单单是技术上的公共账本共识，更是对区块链价值介质的共识。比如在比特币系统里，如果没有激励机制，抑或比特币一文不值，那就不会有人提供算力，就不会有人提供存储空间，就不会有人传教布道——比特币本身就是系统的价值，理念和技术都只是美好的故事。

现在媒体报道的各种区块链应用，总结起来无非两种：要么就是借题材炒作，在中心化机构的交易中强行套用区块链算法；要么就是纯粹的“展望”，丝毫不考虑实现的方式和难度。出于某些原因，这些媒体在鼓吹区块链的过程中达成了奇妙的默契，绝口不提虚拟币，这对大家产生了严重误导，以为区块链只是一个纯粹的网络技术。事实上，如果确有名副其实的区块链生态出现，那白皮书最后图穷匕见的，必定是虚拟币。

据此，我们不妨重新审视下虚拟币和区块链的关系。

圈内有个说法，称“区块链为本，虚拟币为用”，此话的真伪甚是难辨。

挑明了说，区块链的本质是虚拟币为了建立“公平激励机制”而创造的特定算法，所谓的“区块链为本，虚拟币为用”无异于买椟还珠。在此我们大可断言，一旦失去虚拟币这个灵魂，区块链就不存在价值。

这个论点或让人一时难以接受，但逻辑上并无太多不妥。

所谓“产生价值”，无非三个标准：创造需求，降低成本，重塑公平。从成本看，区块链之于中心化可谓毫无优势；从公平看，宏大的比特币社会实验已然揭开分晓。那么唯一留有悬念的，就是区块链是否“创造需求”了。

这时候币圈人可以跳出来斩钉截铁说，当然有需求，你看这风起云涌的ICO！

ICO的狂欢

ICO，全称InitialCoinOffering，即首次代币发行。简而言之就是把早期项目的特定虚拟币，以比特币等通用虚拟币作价，向公众发售份额的众筹融资行为。所谓的“早期项目”有多早呢？组一个团队再写一个白皮书就够了。如果有闲工夫，顺便做个PPT那算是相当勤奋了。至于尽职调查、财务分析，那都完全不需要，因为大部分项目一分钱营业收入都没有。

“特定虚拟币”这个称呼略有点不专业，在币圈通行的叫法应是token，高雅点的翻译叫“通证”。在白皮书里，项目团队会画出各种大饼，告诉你将来自家通证会有多大“价值”。但你若想知道通证究竟是个什么东西，不好意思，区块链圈子有

一个优良传统，叫“语焉不详”。

出于某些意味深长的原因，大部分ICO的法律文书（LegalDocuments）都是纯英文的，而通证的真实定义其实就藏在其中。几乎所有ICO都在法律文书里作了类似如下的规定：“通证不授予白皮书所规定回报以外的任何权利，且仅在项目成功时方能生效。众筹投资者对项目发展和管理不可施予任何影响。通证不代表投资者对项目拥有任何形式的所有权，亦不可凭此获得项目相关的未来收入和知识产权。”

这段让人瞠目结舌的文字，说白了就是：虽然你出了钱，但你什么都不是。ICO众筹并不是我们过去知道的那个众筹，投资者花钱买到的不是股份，而是筹码，什么时候庄家不玩了，筹码就归为空气——且不讲大多数庄家根本玩不起来。

没有底层资产，没有主体信用，没有商业模式，没有法律保障，这样的虚拟币，卖得出去吗？答案竟然是肯定的。

这一切看似荒谬绝伦，但背后的逻辑其实非常简单：因为很多人通过ICO赚了钱。

建团队写白皮书是ICO产业链的第一环，紧接着要拉大佬站台，到境外“交易所”发币，虚拟币上线了还要操纵币价吸引更多炒家入场，最后看准时机套现离场就算走完了全程。有人在这个游戏中直接实现了财务自由；有些虽然没吃到肉，但也喝到了汤。

面对门槛如此低的造富奇迹，任谁都要心动一下。

但是，如果项目本身无法盈利，那不管如何包装美化，ICO终究还是个零和游戏——如果有人赚得盆满钵满，那肯定有人赔得底裤不剩。这就像我们熟知的传销，所有人都知道接最后一棒会死，但都觉得自己不会接到最后一棒。

那区块链在ICO大潮中究竟扮演了什么角色呢？

众所周知，去中心化、去信用化和公平公正，这些都是区块链标榜的理念。我们反观ICO：若要上线发币，就必须向中心化的交易所支付巨额“上币费”，这是何等的“去中心化”？项目团队欺诈横行、币圈媒体刻意误导、交易账户频遭黑客，这是何等的“去信用化”？庄家大鳄肆意哄抬价格，牟取暴利，倾轧韭菜，这是何等的“公平公正”？事实上，除了提供虚拟币和噱头，区块链在币圈什么都不是。更具讽刺意味的是，很多ICO发行的虚拟币甚至都没有基于区块链技术。

所以，ICO不是区块链创造的需求，而是区块链之耻。

链和币的未来

既然我们已经知道虚拟币是区块链存在的唯一价值，那么对于区块链未来的分析也就有了大致的思路。

法定货币充分电子化的当下，基于区块链技术的虚拟币在正常社会生活中并无太多实用价值。但置于特殊场景，虚拟币却有一个电子法币不可复制的优点，那就是隐私性。

但凡以银行作为支付通道的交易，都是能被监管的，如果当局愿意，他们可以知道你把钱给了谁，这笔交易的背景，发生的时点，一切的一切。所以在比特币问世之前，绝大多数见不得人的交易都是用现金完成的。你只见过黑帮片里提着一大箱子现金去买毒品，绝对看不到带着一个POS机过去的。

而比特币的横空出世，革新了洗钱、贩毒和黑市军火买卖。有了这种完全匿名的货币，不法分子再也不必为一箱箱现金提心吊胆，再也不必为连号的美元支付折价了——比特币就是便携的黄金，正如它的设计理念一样。

所以，比特币及其替代品是不可能被彻底消灭的，因为逃脱监管的需求将永远存在。

只要虚拟币不死，区块链经济就一定有生存的空间，因为虚拟币代表的价值必然需要兑现的途径，而这个途径不可能永远是法币。

这里要插一句，最近区块链和中心化账本的妥协产物，比如雷电网络等，正逐渐露出头角。原理上中心账本能大幅提高处理效率，适应大规模高频次应用，但如果虚拟币核心用户的主要诉求是脱离监管，那么这个功能可能并不会受欢迎。结果如何，不久便知。

另一个大家关心的问题是：风起云涌的ICO会导致虚拟币大爆发吗？答案当然是否定的。

虚拟币不受法律强制保护，所以其公众接受度很大程度上决定了它的价值和前途。在接受法币支付时，我们默认自己得到的法币，别人也同样会接受，其面值在流通过程中不产生任何折价，具有100%的流动性。虚拟币的场合情况就不一样了，由于缺乏流动性量化指标，我们只能根据公众对其接受度的笼统判断，决定是否接受该种虚拟币支付。这种判断方式会形成强大的马太效应，因为公众的选择会迅速趋同。

另一方面，公众自发接受的货币种类也是有上限的。拿共享单车打个比方，我们会给摩拜充押金，会给OFO充押金，心很大的还会给Bluegogo充押金，敢问同时给4种以上共享单车充过押金的人有多少？通常情况下，大众对于同质化功能的接受上限仅有“三个”。在货币的场合，法币第一的位置无法动摇，第二多半是比特币，第三是以太坊——所以很不幸，不出意外其他所有虚拟币都长不大。

有人会说，这是基于公链的判断，我们还有私链和联盟链。

在这里，我们要旗帜鲜明地站定立场：私链就是个中心账本，和区块链理念一点关系都没有。至于联盟链，相关的误解就更多些。比方说，现在很多联盟链的构想是没有token成分的，这便是最大的误解。如之前分析，若没有激励机制，高频应用会变成低频应用搭便车的工具，更差的情况甚至连价值传输的介质都会缺失。另外，如果不同应用间token价值的兑现方式存在区别，联盟内部的套利也将不可避免。总之，联盟链和公链相比，除了隐私性略有提高外，问题只多不少。Token泛用性的差距意味着它只能在公链的阴影下靠底层资产价值苟延残喘。

综上，我们对于未来区块链的应用范围也就有了基本的认识：大部分自然生长的区块链经济，都将基于比特币和以太坊存在。这里说的自然生长，特指与中心化机构强行附会的伪区块链进行区别。无论是银行间结算、产品防伪还是其他任何场景，如果参与主体间的共识和信任早已存在，那所谓的区块链应用充其量只是个数据库，而且不会是最优设计的数据库。

最后一个问题：区块链的热潮什么时候会退去呢？

这是一个很难回答的问题。不过有句话说得好：你可以在一个时间愚弄所有人，也可以永远愚弄一个人，但不可能永远愚弄所有人。

（作者系金融科技研究人士）