（思进注：长久关注我的网友都知道我对比特币的观点，特别是从支付角度而言，对比特币的底层技术——区块链的微言，事实上，从各国央行数字货币的架构选择（如数字人民币就并未完全照搬区块链技术，仅引入了分布式账本技术），就反证了当前区块链技术的不足……再转发下文《为什么虚拟货币难当货币大任？从比特币的底层技术说起》（对这个问题有详谈），和大家分享……）

为什么虚拟货币难当货币大任？从比特币的底层技术说起

作者 | 吴云、朱玮

来源 | 澎湃新闻

比特币真的能够替代现有法定货币体系而担当货币大任吗？我们先来看看两个简单的感性数据，就可以知道这种期望是不现实的：比特币交易验证的平均等待时间是10分钟；迄今为止，比特币在2017年12月发生了历史上最严重的交易拥堵现象，当月一笔交易的平均等待时间是两天两夜！

从系统技术效率的角度，比特币（bitcoin）之于现有的电子支付（如支付宝），犹如马车之于火箭，差别巨大。读者可能会奇怪，在这个比喻里，究竟比特币是马车，还是支付宝是马车？笔者可以负责任地说：“比特币是马车！”实际上，作为支付工具，比特币相比较于支付宝，比马车与火箭的速度差距还要大一百倍。请注意，这里仅是从支付工具的角度讨论，并不否认比特币带来的区块链技术所蕴含的创新性和应用价值。（详细参考笔者文章《虚拟货币：失败的货币实验和成功的技术革新》，2020-08-30，澎湃商学院）。

2009年，比特币的诞生，标志着虚拟货币作为一种现象级事件正式登上了历史舞台。我们一般将比特币这种私人发行的数字货币称为“虚拟货币”，截至2020年3月5日，仅利用以太坊上的ERC20开发的虚拟货币就达到24.55万种。比特币深受私人货币思想的影响，不仅怀有取代现有法定货币还怀有改变现有金融格局的宏大理想。比特币的设计者和创始人“中本聪”在《比特币白皮书》中指出，比特币是“一种纯粹的点对点电子现金，不通过金融机构，可以实现交易对手之间直接的网络支付”。比特币诞生以后，引发了各界广泛的关注，人们曾经对虚拟货币抱有很大的期望，很多人将其视为替代现有支付体系的“高科技武器”，甚至大胆预测比特币所开创的点对点支付手段将会使金融体系彻底摆脱对金融机构的依赖。

记得我们的中学教科书里说过，新生事物的发展是曲折的。这句话用到比特币和众多虚拟货币之上也是合适的。比特币确实提供了一种新型货币和支付体系的思路，但是，至少到目前为止，比特币和各种虚拟货币并没有表现出作为支付手段的任何优势，甚至在关键技术指标上可以说是“落后的”，它们不可能成为公众可以大规

模使用的支付手段。

为什么现实和期望之间有如此巨大的反差？这还要从比特币的底层技术说起。

一、比特币的交易数据构造：交易、区块、链

和传统的电子支付一样，比特币也抛弃了纸钞、黄金这样的实体，但为了在点对点环境下实现可信支付，比特币创造性地使用交易记录作为货币的载体。虽然在比特币名字中有“币”这个字,
但在比特币这个系统中并不存在一枚金光闪闪的“币”。
比特币所构造的模型迥异于传统银行系统的余额制, 当然更不同于古老的金银铸币和纸钞（倒是在流通模式、隐私保护上与金银和纸钞类似）。中本聪设计的比特币，以交易记录的形式出现。你并非拥有一个比特币, 而是拥有别人转比特币给你的一笔记录。这个记录就叫作“未花费的输出”（Unspent Transaction Output，UTXO），可以理解为一张可转让的权利电子凭证。

很多论著或报道告诉我们，区块成链，所以我们把这种技术形象地称为“区块链”。实际上，比特币区块之中的交易通过UTXO记录的形式也勾连成链，形成了连续的交易链条，也即交易成链。我们来具体了解一下“区块”的特点和“链”的形成过程。

“区块”是将多笔交易数据打包在一起形成的数据体。可以将区块理解为一个账本, 账本里记录了多笔交易。单笔交易在最简单的情况下，大小为250字节,
当然实际发生的交易会大于这个数值。每个区块大小被中本聪限定最大为1兆字节（1024千字节）, 那么我们就可以算出来,
一个区块最多可以容纳4096(1024000/250) 笔交易。以账本作比喻,
中本聪限定了一个账本最多只有1024页。而每个最基本的交易要占用四分之一页,
那么一个账本最多就是4096笔交易。

区块成“链”的同时交易也成链。记账人按照规则在账本（区块）上记满了交易后，在封面贴上时间封条，同时在账本封面上记录前一个账本的编号，这样就在账本之间构成了一个首尾相连的账本链条。这样构成的账本链条,
有一个特点：越老的账本,
其中的交易越难以篡改。若要更改2015年高度为363270区块中的一笔交易,
那么就要将自2015年该账本之后的所有账本, 全数改掉, 重新记账才可做到。

如何防止篡改账本呢？比特币创造性使用了工作量证明（POW）机制，矿机通过哈希运算竞争获得记账权，从而防止区块篡改。比特币没有中心服务器，而是由所有节点的矿机自发运行为系统提供算力。矿机通过竞争，以获得记账权，系统会给获

得记账权的矿机以比特币作为奖励。也就是我们常说的“挖矿”。矿机作POW运算就是对“区块头”数据进行两次哈希运算（比特币使用的是SHA256哈希运算），得到了一个256位的哈希值。

算出哈希值只要几秒时间，矿机在瞬间即可完成，因此，比特币给哈希运算提出了要求，也即你必须算出指定要求的哈希值，比如，前19位数都是零。这样，难度陡然增加。矿机要算出指定要求的哈希值，必须用试错的方法，将随机数（专业上称作“被使用一次的非重复的随机数值”，即Nonce）不断代入以运算出小于某个数值的哈希值。因为SHA256的运算结果是非常随机的, 所以,
要想运算出指定的哈希值, 唯一的方法就是不停地尝试 Nonce。因此,
矿机是否能够挖矿成功, 一是依赖矿机的运算速度; 二是依赖运气,
也许第一次改变Nonce的值, 就得到了合乎大小的哈希值, 也许运行几百亿次, 也没有得到。比特币设置了自动调节哈希运算的时间，将其设定为平均十分钟，并动态调整。这个时间设定，是两个方面的平衡，时间太少，消耗算力不够，无法让篡改企图知难而退，且造成网络同步不稳定，而时间太长则交易确认时间过长，矿机体验太差。（哈希运算问题比较复杂，这几个术语我们限于篇幅不作详细解释，有兴趣的读者可以阅读《区块链简史》第四章。）

以上是对比特币的区块链原理的基本解释，对于非技术人员了解比特币的运行效率而言，至关重要的有三个方面：

第一，可以将每一次比特币交易验证过程理解为一次“出块”，就是将很多交易数据文件整理在一起后封装，并盖上数据哈希和时间戳，从此不再更改（前提是在哈希竞赛中胜出并在共识机制中得到足够多的确认）。

第二，比特币区块大小被设定为1兆字节，每个区块理论上只能记载4096笔交易。

第三，出块时间就是矿机们验证交易、区块打包、哈希竞赛的时间，按照比特币代码的设定，比特币哈希竞赛的目标难度值会进行动态调整，使出块时间平均维持在10分钟左右。

二、从单笔交易速度看，比特币“出块”时间被设定为平均十分钟，耗时是支付宝的200倍，无法用于公众日常使用

比特币在底层技术上将“出块”时间设定为平均10分钟，这也即意味着完成“一批”交易的验证时间是10分钟。每次交易的平均确认时间也在10分钟左右。对于公众日常支付，这个速度是无法接受的。试想，你在超市结账，排在你前面的人，用比特币发起支付到商家确认收到比特币，要10分钟，这队应该排到几公里外了。再仔细用简单的数字计算一下：超市的一个收银柜台要10分钟完成一笔收款，一个小时

才6笔，在8个小时的营业时间里只能完成48笔。可以说比特币的这种速度是无法满足公众的日常使用需求。

大家可以回想一下我们日常使用电子支付的时间。生活经验告诉我们，支付宝每笔交易的系统处理时间不超过3秒（仅指系统处理时间，不包括打开App，输入密码等用户操作所耗费时间），网络银行转账也可以几秒之内到账。按照中国银联的技术规范，非接触卡交易时间更是应少于500毫秒。

比特币并发处理速度 4096 笔/10 分钟=6.83 笔/秒

而根据支付宝2017年“双十一”公布的数据，支付宝的每秒交易处理量峰值是25.6万笔。这两者的处理速度差距有多大呢？相差了3.7万倍！而火箭的第一宇宙速度和马车的速度也仅是474倍的差距。

比特币	中国第三方支付
理论上比特币能够处理的最大交易数量： 【每小时】：60 分钟×（4096 笔/10 分钟）≈2.46 万 【每天】：24×每小时交易量≈59 万 【每月】：30×每日交易量≈1770 万 【每年】：12×每日交易量≈2.12 亿 截止 2019 年 11 月 23 日，共有区块 60.5026 万个，那么能够承载的最大交易为 24.78186496 亿笔	支付宝：每秒 25.6 万笔并发交易（2017 年双十一） 中国第三方支付清算量（通过网联）：每日 11.8 亿笔（2019 年第三季度）

比特币系统满负荷运转，理论上每年仅能承载2.12亿笔交易，相当于网联每日清算量的五分之一左右。比特币将近十年的累计历史交易量仅相当于网联清每日清算量的三分之一。