理性认识比特币及区块链风险

□ 梁 睿

今年1月份，曾经风光一时的比特币走出了一波跳水行情，价格从2万美元一度跌至1.1万美元，几近腰斩。此前，一些国家的监管部门已纷纷采取措施，取缔、限制比特币等虚拟货币交易。拥有全球最大的比特币交易所的韩国最近也明确表示，正在准备一项禁止通过交易所进行加密货币交易的法案。而比特币背后的区块链技术概念，在今年年初的A股市场上一度大热后，也在市场的严密监管下归于沉寂。

所谓的区块链，是指分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链本质上是一个去中心化的数据库，也是比特币依赖的底层技术。在比特币区块链中，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性和生成下一个区块。

用术语解释区块链概念有些拗口，这些都不明白也没关系。所谓万变不离其宗，其实只要略懂电脑网络，就能明白其中风险。区块链的运行一离不开电脑实时处理，二离不开网络传输信息。随着比特币等虚拟货币交易次数越来越多，需要传输和处理的信息总量会成指数级增长，其背后需要支撑的硬件配置就会越来越高，导致系统不堪重负。

目前，数据写入大型区块链，要等待10分钟。等所有节点都同步数据，则需要更多的时间。拿比特币举例，当前产生的交易有效性受网络传输影响，比特币交易每次的确认时间大约10分钟，6次确认的话需要1个小时。这么慢的交易速度，连比特币拥趸们都不待见，“北美比特币大会”组织者今年就在其网站上宣布，由于网络拥堵和人工处理速度缓慢，他们停止接受比特币付款购买门票。

随着交易数据量不断增长，区块链数据库将越来越庞大，直到耗尽系统资源，而这一技术风险，目前尚未有完善的解决方案；即使解决了，也会是谁的机器算力强，谁的网络带宽大，谁更占优势，这又与区块链标榜的“去中心化”背道而驰。这一道理，已经被比特币从创始之初的人人都可“挖矿”的相对公平合理设计演变成了谁的算力强谁就能占优所证明。此外，无论电脑还是网络，都有被黑客攻击或操纵风险，一些比特币交易所因为受到黑客攻击而损失惨重甚至关门大吉，就是例证。

区块链难以“小而美”是比特币们的一大硬伤，估值则是比特币们另一大风险。比特币等虚拟货币的价格完全建立在市场买卖的基础上，既没有一篮子货币可锚定，又没有政府信用做背书，也不像金、银等贵金属集价值和使用价值于一身……所以价格必然上蹿下跳，波幅惊人。曾经于2014年高调支持比特币支付的微软，今年初也悄悄取消了微软商店对比特币的支持，原因就在于比特币价格波动太大受不了。

值得警惕的是，市场有一些私募机构大佬对并不成熟的区块链技术和虚拟货币风险视若无睹，不断下重注。当然，你看好，关起门来投，闷声发大财就行了，但出来高调跟大家讲区块链好，我投了，你们快跟，就不大地道了。对投资者来说，还需理性认识比特币及区块链的风险，谨慎对待所谓的投资机会。

我做比特币矿工这一年

作者：云锋金融研究部

编者按 去年9月份，央行等七部门发文叫停各类代币发行融资。此后，国内几大比特币交易所相继关闭场内交易。近日，多地金融管理部门积极行动，综合采取电价、土地、税收和环保等措施，引导虚拟货币“挖矿”企业有序退出。本文以一个比特币矿工的视角，生动记录了比特币生产过程，展现了挖矿产业的畸形一面和投资风险。

长达150米的仓库两侧，密密麻麻地放着超过20000台隆隆作响的机器。

灯光昏暗，只有LED灯在不断地闪烁着绿光。巨大的噪音中，还有鼓风机和空调的声音，是他们确保了仓库不会变成一个桑拿房。然而，闷热烦躁的气氛却怎么也挥之不去。这就是我的工作环境，我是一名比特币矿工。我的工作就是每天巡视一遍仓库里的机器，用手中的笔记本电脑对每一台机器进行测试。如果发现问题，就按照操作手册上说的步骤执行——“重启——重新连接线路板——卸下机器交给技术部门”。

一

矿场墙上贴着一条标语——“时间就是金钱”。

2017年初，第一次走进这个位于内蒙古鄂尔多斯的“矿场”，其实是仓库机房的工作地点时，我被巨大的轰鸣声吓得倒退了三步。刚开始的时候，我并不知道为什么这个地方叫作矿场。

有次休息的时候，看到同事们神秘地围成一圈，对着一个屏幕念叨着什么。我凑上去一看，是一张弯弯曲曲的折线图，最上面写着几个英文字母——Bitcoin。

一位同事告诉我，这些字母翻译成中文叫“比特币”，而这个机房就是用来“挖”比特币的地方，所以被形象地称为挖矿的矿场。可一个虚拟的东西，为什么会用挖这个词呢？我仍然百思不得其解。

同事也解释不清，让我去问带班的组长。戴着黑框眼镜，看起来就像一个技术宅男的组长应该已给很多人解释过，他很耐心地给我讲了这背后的原理：“其实比起挖矿，获取比特币更像是美国和澳大利亚都有过的淘金热。”

“挖矿给人的感觉是一分付出一分收获，但与在河水里淘金不一样。除了纯粹的体力劳动之外，还需要足够的耐心和很好的运气。挖比特币就是这么一种感觉。更确切地说，我们的挖矿是参加一场每10分钟举办一次的‘饥饿游戏’，全世界的矿工都会参与，而游戏的奖品就是比特币。”

组长解释，之所以你看到现在的矿场规模这么大，是因为拿到奖品的难度在与日俱增。

这背后有很多原因，比如参加的矿工越来越多，像我们这里这样的矿场，现在光中国就有百八十个，而新建的矿场大多在冰岛和俄罗斯等的荒无人烟的地方。但同时，单场游戏的奖品却越来越少。这是“中本聪”在创造比特币的时候就强制规定的。2012年之前，每场游戏可以产生50个奖励。之后每4年就会减半，也就是说，现在，每场游戏只会产生12.5个奖励。而且，这游戏还有明确的结束时间，当比特币数量达到2100万枚的时候就会彻底结束。估摸下来，应该也就是2050年前后。

组长告诉我，这还不算，每次游戏的难度也在不断加大。怎么说？因为这游戏从本质上讲就是猜数字为了控制发行速度，正确答案的数字正在变得越来越复杂。矿工们以前可能猜10次就能猜中的数字，现在猜1000次都未必对。

“所以我们矿场的墙上要贴上‘时间就是金钱’，因为时间在这里真的就是金钱——越早尝试，就越可能拿到新的比特币。”说到这里，组长突然停下来看着我。

我还在努力消化他刚才的那些话，突然反应过来，他是在嫌我浪费工作时间了。

回到岗位上我才想到，其实还有一个最重要的问题没问——拿到比特币这个奖品又如何？为什么我们要参加这样一场游戏呢？

二

关于这个问题，在不久后我自己就找到了答案，因为同事教会了我看比特币的价格图。那时还是2017年年初，一个比特币大概值1000美元，也就是6000多元人民币。显然，一场每10分钟就派出巨额奖金的游戏，确实没有不参加的理由。

而且我很快就知道了这场游戏的诀窍——那就是没有诀窍。

所谓的挖矿算法，也就是猜数字的方法，其实是固定而简单的，并不存在什么可以改进的地方。

所以赢得游戏的方法只有一个，那就是寻找在单位时间内能执行最多次算法的硬件。另外，1+1=2，谁拥有这样的硬件数量最多，谁就最有可能赢得游戏。

从同事那里我也知道了，整个比特币的挖矿史其实就是挖矿硬件的迭代史。刚开始的时候，大家都用普通电脑的CPU挖矿，那是一个美好的、个人就能挖矿的时代。

到2010年，有人发现AMD公司出产的GPU芯片有一个特定的计算部件，可以加速猜数字的关键步骤，于是多个GPU组装成的“GPU矿机”迅速淘汰了普通电脑矿机——这也是近几年来为什么显卡和其他电脑硬件不同，价格经常不降反升，而且还老缺货的原因。

再到2011年年末，FPGA（现场可编程逻辑门阵列）矿机横空出世，因为它剔除了GPU中不必要的图像计算硬件单元，所以效率大幅提升。也就是在那时候，出现了第一个矿场Eligius。不过，当年的矿场还只处于萌芽期，矿工依然主要指的是全世界默默挖矿的个人电脑们。

而我现在每天维护的矿机，已经是第四代，也就是ASIC芯片机（一种为专门目的而设计的集成电路）。比起FPGA来说，ASIC芯片牺牲了灵活性，造出来就是为了猜数字挖矿，所以效率再次有了质的飞跃。

如果作个简单的比较，CPU的挖矿速度是1，那么GPU大概就是10；FPGA矿机的速度虽然只是8，但消耗的电能比GPU小40倍；而ASIC的挖矿速度是2000，功耗与GPU相当。

这样也就很容易理解，为什么ASIC芯片一问世，就迅速将其他三类矿机赶出了市场。另外，到了这个阶段，矿场已经成为挖矿的主力。因为一台主流的ASIC芯片矿机，如蚂蚁矿机S9，要卖到1万多元钱。而这时候想要挖到比特币，已经至少要上百台S9日夜不停地运转。

排名前三的矿场迅速成为中国选手的竞技场。前些年中国在IT领域积累起来的强大供应链和制造能力，在此时发挥得淋漓尽致。

以比特大陆为例，因为设计出了比特币挖矿专用的ASIC芯片，于是这家公司迅速成为世界矿机界的领头羊。这两年他家的矿机销量在数十万台以上，每台矿机要用上百颗ASIC芯片，例如一台蚂蚁矿机S9就要使用189个ASIC芯片。听说2017年上半年，这家公司的净利润已经超过10亿元人民币，那么在比特币暴涨的2017年下半年，利润水平该更加惊人吧。

三

时间过得很快，转眼我已经在这个矿场工作了半年。就在庆幸冬去春来，再也不用在北方的寒夜里瑟瑟发抖的时候，组长通知我们，矿场要搬家了。

身边的老员工对此都非常淡定，转身就开始收拾行李，留下我们一帮新人一头雾水，不知道发生了什么。后来我们才知道，像候鸟般迁徙是矿场的惯例，冬天在新疆、内蒙古一带，夏天就会去四川。可几万台机器的搬家可不是件容易的事情，这又是为什么呢？

直到看到四川的矿场新家我才顿然醒悟。新的工作地点就在一个水电站边上，江水在窗外奔流不息。

对于矿场而言，收益＝生产的比特币×币价－矿机成本－电费－维护费及人工成本－矿场折旧费。

万万没想到的是，挖矿开支的大头并不是我觉得很贵的矿机，当然也不会是我们这些廉价的人力，而是电费。事实上，早在鄂尔多斯的时候，我就觉得整个矿场像是一个用电的黑洞。

组长曾在闲聊时提过，我们矿场一个小时要用掉40兆瓦时电，相当于12000个家庭的用电量。尽管当地政府给了很多优惠，但每年还是要缴纳上亿元的电费。而这还是一个电力过剩的地方。还有比那里电费更便宜的地方吗？

有，那就是夏天丰水季节的四川。

沿着301国道开向四川康定的时候，一路上经过的水电站大大小小不下几十个。汹涌的江水给水电站带来了源源不断的电力，在夏天，这些电根本来不及传输出去。然而，当比特币矿场如雨后春笋般出现之后，电力闲置的情况就不复存在了。

我们矿场的新址是一排整齐的蓝色塑钢大棚，依山而建，每个大棚里都有几千台矿机。水电站的发电7×24小时支持了矿机的运转，财大气粗的矿场主往往会包下整个水电站，为的就是确保自家矿机的电力供应。

尽管夏天山区里气温只有20多摄氏度，但每当打开大棚的门，一股热浪还是会扑面而来——几千台矿机24小时不间断运转产生的热能，可比那些普通机房大多了，我几乎每天都会发现几台矿机的电路板被烤出黄斑，无法修理只能更换。

但组长和我们说，这样依然是值得的。因为丰水季节的水电站电费边际成本接近于零，矿场直接用承包的方式买下一个电站的电力，一个月只需要四五百万元人民币，远比在鄂尔多斯的时候便宜。

那到了枯水季节呢？我好奇地问。

组长叹了口气，因为这两个季节水电站的产电量可以差5到10倍，所以电价会在枯水季节往上浮好几倍。这也是为什么一到夏末秋初，矿场们又会不畏严寒向新疆和内蒙古等地迁徙。

四

我的矿工生涯在今年初戛然而止。

去年底，矿场老板把迁徙地定在了新疆。没有想到，就在刚刚过完新年的1月4日，新疆互金办发文，要求各地政府部门排查当地比特币矿场情况。

尽管没有说要直接取缔，但当地政府还是防患于未然地取消了之前以招商引资为由给我们的电价优惠——国家电网标准价是一千瓦时0.4元左右，而之前给矿场的优惠价是0.2元—0.3元之间。

翻了近一番的电价让矿场利润骤减，而比特币价格也结束了单边上涨趋势。尽管我们的莱特币矿机还在赚钱，但老板还是决定见好就收，结束了这项政策风险越来越大的生意。

至于我身边的同事，大多因为买卖各种数字货币赚了些钱，此时就作鸟兽散——有的去了别的矿场，有的干脆彻底投身币圈做职业投资。

我因为进入行业太晚，买币更晚，所以并没有靠这个发财致富。但长期的矿场工作让我落下了耳鸣的毛病，医生说，如果你再在这样的环境下工作两年，听力就会永久受损了。但这也不是我离开矿场的关键理由。事实上，是我意识到，在这里上班根本连矿工都算不上。

我不懂哈希值，不懂默克尔根，区块链和数字签名对我来说只有一个懵懂的概念。我和这个号称“互联网时代的黄金”的比特币之间的联系，只有维修不完的矿机。

中本聪设想的那个“去中心化”“人人平等”“算力民主”的世界并没有到来，站在矿机外的我，和掌控算力的人，差距只在越扩越大。我准备报考明年的研究生考试，重新进入校园学习知识。我要去做真正的极客，而不是一个只知道擦灰的矿工。 **（文章来源：云锋金融微信公众号。本文由云锋金融集团有限公司授权发布，本报有删改。不构成具体投资建议。敬请投资者注意，投资涉及风险）**

财富学堂

比特币的来龙去脉

□ 金 风

2008年，国际金融危机爆发。同年11月1日，在前人的理论和实践基础之上，一位化名中本聪的“神秘人”发表了一篇《一种点对点的现金支付系统》的论文，阐述了他对电子货币的新构想。

2009年1月3日，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了比特币的第一个区块——创世区块（Genesis Block），并获得了首矿”奖励——50个比特币。在创世区块中，中本聪写下这样一句话：The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.（财政大臣处于第二次援助银行的边缘）。这句话是英国《泰晤士报》当天的头版文章标题。

通俗的说，比特币是一种由开源的P2P（点对点）软件产生的电子数据。比特币的初始来源就是中本聪设计的比特币系统给出的奖励。比特币账户间交易很像个人发送电子邮件，先要安装一个比特币客户端，账户就像是个人电子邮箱地址，而密码就像是比特币交易的个人私钥。

在比特币的网络中，每个安装了客户端的节点都拥有一个分布式数据库来管理比特币生产、交易，查询账户余额记录，同时也更新和记录着比特币系统变化的最新记录。当要给朋友发送1个比特币的时候，需要进入比特币个人账户，用个人私钥发出转账信息。周边的节点会检查你的账户是否拥有1个比特币，如果有，则同意这次交易，并且把这条信息广播到附近的节点，一传十，十传百，很快整个网络都会确认这笔交易信息，然后写入到区块中。朋友将会收到这个比特币，交易就算完成了。

区块链是比特币的底层技术，为了保证比特币交易的准确性、公正性和可追溯，需要通过区块链技术记录和确认整个交易过程，就像银行系统准确记录每一笔资金的汇划金额和支付时间、交易对象。比特币交易系统每10分钟就将这段时间内全网所有的交易数据打包，存储在特定的区块文件中，并发送到每个节点，这些区块文件按照时间先后顺次排列，就成为区块链。

由于比特币网络中有许多电脑节点，这些节点就像一个个“账房先生”，如何从中找出那个记账又快有准的“账房先生”来生成唯一被系统认可的区块呢？中本聪创造了比特币的奖励机制，既哪个“账房先生”能够最全搜集前10分钟内的全网交易数据，并且最快猜出特定复杂方程的解并发送到网络上让大家确认，就让他成为这个区块的记账者，奖励一开始是50个比特币，以后每隔4年减半，直到2140年2100万枚比特币全部发完为止。

中本聪设计的这套奖励机制，鼓励各比特币节点努力工作，保证了比特币区块链的正常运转，并不断产生新的区块链，保证比特币的发行和流转。

一开始，比特币不过是区块链技术的一项实践活动，前景如何，谁也不好预测，参与的也是一些计算机网络和密码学爱好者。比特币也不大受待见，一美元能买一大把，接受的人也少，美国一位程序员曾花1万个比特币买了两块总值25美元的匹萨饼，现在来看，这两块匹萨可能成为史上最贵匹萨了。

比特币价格扶摇直上还是有了交易所以后的事。随着比特币总量的增加，以及比特币和法定货币之间交易需求的增加，比特币交易所应运而生。比特币交易所的出现，又使得比特币吸纳了大量的投机资金，价格扶摇直上。2010年，世界上第一个比特币交易所Bitcoin Market（比特币市场）诞生，不过好景不长，由于技术原因，很快就偃旗息鼓。比较著名的是MtGox（门头沟），该交易所于2010年7月份成立于日本东京，在交易高峰期的时候，该交易所处理的比特币交易量一度占所有比特币交易所的70%，但这家交易所也是命不好，因为丢失了85万个用户的比特币而于2014年关门。此后，全球又陆续出现了100多家交所，中国境内的交易所也异军突起，一度占据了全世界交易总量的八成。

比特币交易所通过线上撮合交易大大便利了比特币炒作和变现。毕竟，在交易所交易比特币，只在充值和提现的时候才记录到比特币区块链，而用户间的买进卖出交易则记录在交易所的服务器，并不受系统时间的限制。

要指出的是，在中本聪的比特币系统中，并没有设计交易所这样的一个中心化的市场。由此，我们也可以看出比特币的异化路径。

由于交易所的繁荣，比特币可以大规模地在全球各比特币交所所交易，并转换成各种货币，从而也为资金外逃和洗钱创造了方便之门，这也是各国央行打击的重点。各个国家和地区监管部门对比特币等虚拟货币交易的各项监管措施，基本都出台于比特币和法定货币之间的交易异常繁荣之后。2013年12月5日，中国人民银行等五部门发布关于防范比特币风险的通知，要求各金融机构和支付机构不得以比特币为产品或服务定价，不得从事比特币相关业务，不得直接或间接为客户提供其他与比特币相关的服务等；2017年9月4日，中国人民银行等七部门又联合出台严令，叫停代币交易平台的兑换功能，特别是与法定货币的兑换功能。此后，中国境内比特币交易所全部关停。