

# 八年暴涨了300万倍,连勒索病毒都拿它当赎金 疯狂比特币,大革命还是大忽悠?



本报记者 王昱

## 暴涨： 俩披萨吃掉亿万富翁

今年5月22日,对大多数人来说只是普通的一天,但分布在全世界的比特币玩家们却在庆祝一个别开生面的小众节日——“比特披萨节”。在这一天,他们会吃块披萨,举杯致敬一个叫拉斯洛·汉耶茨的倒霉蛋——他为了了一份披萨,错过了成为亿万富翁的机会。

故事要从2010年讲起。某日,身为程序员的拉斯洛·汉耶茨在网上晒他囤积起来的比特币——在当时,比特币仅仅诞生一年,还只是小圈子里极客玩家们的玩具,在真实世界里买不到任何东西。

于是有人理所当然地提出疑问:“这玩意儿有啥用?”

为了回应这个质疑,汉耶茨在网上向比特币玩家发起挑战,看有没有人愿意接受1万枚比特币,帮他买一份披萨。到了当年5月22日,终于有人接招,花了25美元在Papa John's买了两份披萨,寄给了汉耶茨,并收下了他1万枚比特币的对价。这次交易是人类历史上第一次比特币购买实物的交易记录。

然而,让汉耶茨始料未及的是,比特币后来的故事,不仅打了质疑者的脸,也让他自己后悔不迭:

2011年,阿桑奇领导的“维基解密”宣布接受比特币作为捐款币种,使得这种原本小圈子内使用的虚拟货币第一次进入主流社会的视野。

2012年,美国NBC等主流媒体开始大规模报道比特币,更多的机构开始接受比特币,但美国监管机构也开始盯上比特币。

2013年2月,比特币的结算中心Coinbase宣布,当月比特币以22美元/枚左右的价格突破了1百万美元成交量的大关。从此以后,比特币对美元的价格和交易量都进入突飞猛进的增长期,到2016年底,比特币月交易量已接近一千万美元。

时间进入2017年,比特币迎来了“爆发年”,4月1日,向来以保守著称的日本率先吃螃蟹,日本内阁早前签署的《支付服务修正法案》正式承认了比特币在该国具有“类货币财产”的地位,全日本有26万家商店接受比特币支付,廉价航空公司乐桃甚至宣布接受比特币订购该公司的机票。而韩国、俄罗斯、印度等国也在讨论给予比特币类似的地位。

5月12日晚间,一个名为“想哭”的恶意软件在全球多个国家迅速蔓延,数以十万计的电脑遭受攻击,而后被锁死。黑客将电脑中的资料文档上锁,而黑客索要的赎金,是与300美元等价的比特币。

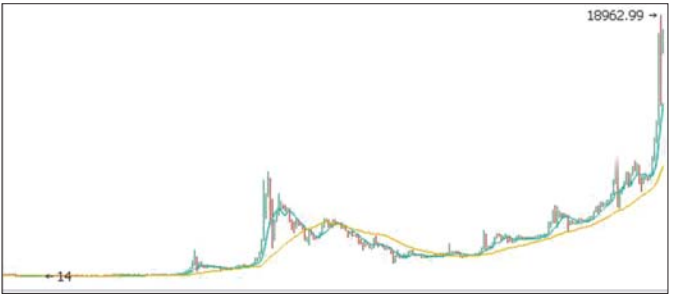
接踵而至的爆炸性消息增加了比特币的曝光度,也开启了比特币的新一轮上涨,在今年5月份的涨幅就累计超过了50%,币值在经历几轮冲高,回



以现在的价格而论,即便把1枚比特币打造为重约50克的金币也是划算的。

现在买什么增值最快?如果你的回答是北京的房子,恭喜你,答错了。正确答案是比特币。最近一段时间,这种虚拟货币的价格屡创新高,甚至一度创下了一比特币兑换2760美元的历史纪录,对比2009年比特币刚刚出现时,1美元差不多可以买到1300枚比特币,在短短八年时间内,比特币已经暴涨了300万倍。

比特币到底是什么?它又经历了什么?更为关键的是,比特币的疯狂暴涨,到底是在宣告一个新时代的来临?还是又一场新的泡沫?



2011年9月以来的比特币走势周线图(据比特币中国官网,单位为人民币)。



比特币发明人 中本聪。

落后,暂时稳定在1比特币兑2200美元左右。有人计算过,如果按现在的比价将比特币“现实化”,可以将其打造成每枚约50克的大金币——此情此景,让当年用1万比特币换回俩披萨的汉耶茨情何以堪?

## 真相： 拿数学题答案当钱花

比特币到底是什么?它凭什么有这么高的价值?

答案也许让不少人大跌眼镜——通俗地说,它其实是一道数学题的答案。

2008年,在一个密码学爱好者的圈子内,一个化名“中本聪”的匿名者发表了一篇论文《比特币:一种点对点的电子货币系统》。这篇论文描绘了一种“去中心化”虚拟货币的前景:这种货币的发行不需要央行,因此也无需担心货币发行总量的控制,免除通货膨胀的风险。神秘的中本聪在2011年比特币曝光度大增后退出江湖,将比特币的管理权交给了

用户平台。经过几次调整和更新,比特币的生产机理如今完全公开透明化了。

本质上,比特币其实就是一堆复杂方程组的若干个“特解”。特解是指方程组所能得到的无限个(其实比特币是有限个)解中的一组,而每一个特解都能解开方程并且是唯一的。而所谓“挖矿”的过程,就是通过只有计算机才能运行的庞大计算量不断地去寻求这个方程组的特解,由于这个方程组被设计成了只有约2100万个特解,所以比特币的上限就是约2100万。

想靠“挖矿”获得一枚比特币,你必须下载专用的比特币运算工具,然后注册各种合作网站,把注册来的用户名和密码填入计算程序中,然后开始运算。当你运算得到新的特解后,该程序将通过P2P分布式网络记录并告知全网,将该特解锁定给你,你于是就获得了这个特解的“专利”。所谓比特币的交易,其实就是对这些特解“专利”进行兑换,而比特币

的每一次交易,都会被程序记录并告知整个网络世界。

把数学算式的答案当钱花,这听上去很匪夷所思,但它很可能正是货币在网络时代的最终存在形态。与传统货币相比,比特币存在如下优势:

首先,伪造可以说是所有货币在互联网时代的梦魇。货币在互联网时代只是银行里的一个数字,理论上讲,一个手段高超的黑客如果能破解银行的防火墙,就能修改这些数字。而比特币由于是一个超复杂方程组的特解,其本身的加密性很好,黑客伪造每枚比特币都需要付出和矿机相等甚至更多的计算量,而由于所有比特币的制造、交易都告知全网,黑客们即便能伪造比特币,想“以假换真”也是不可能的任务。

而比特币的另一大优势,是中本聪当初就提过的——无须担心有中央银行会超发货币。自从货币与黄金等硬通货脱钩以来,中央银行加印钞票导致通货膨胀就时有发生,毕竟印多少纸币,是可以人为控制的事情,而比特币约2100万的总量却是被数学定律所固定的。用比特币拥趸们的话说:“直到宇宙毁灭那一天,只要1+1还等于2,比特币就不会超发一个。”

## 迷思： 看不透,所以炒得嗨

难伪造还不会超发,这样的虚拟货币不就是“数字黄金”吗?可能正是出于这样的思路,“比特币之父”中本聪日前在接受日本《朝日新闻》采访时信心满满地表示,如今比特币的价格只是小意思,比特币的目标是4000美元!中本聪还暗示说,随着货币的数字化,比特币在不远的未来会成为最理想的跨国支付手段。

但是,非常有意思的是,《朝日新闻》在同篇报道中,还意味深长地提到了另一种预期。澳大利亚经济学家约翰·奎根在文中警告正在疯狂购买比特币的日本人,不要被眼下的盛况冲昏了头脑:“比特币是经济泡沫最纯粹的例子。当比特币泡沫破裂时,受到波及的将不仅仅是持有比特币的投资者,与之相挂钩的所有金融市场也将受到巨大冲击。”

约翰·奎根的警告是有道

理的,传统货币虽然有超发、易仿造等诸多缺点,但却有一个优势是比特币难以比拟的——它们的背后都有国家信誉对其购买力给予保证。美元、人民币、日元这些通行全球货币的背后,是美国、中国、日本这些经济强国,除非国家破产,其货币就有购买力。而比特币的背后有什么呢?“除了一群极客什么都没有,”奎根说,“而你无法说服普通公众像爱黄金那样爱电脑里的一串数字。”

比特币另一个遭经济学家诟病之处,恰恰是其发明者所津津乐道的“不会超发”。世界财富总量是增长的,货币总量若被锁死,就势必会造成通货紧缩,随着越来越多产品被产出,钱会变得越来越值钱,这将鼓励人们囤积比特币,而不利于经济加速流通。从经济学的角度看,一种货币如果想要成为全球支付的手段,保证一定的超发空间是必须的,而这一点恰恰是比特币的软肋。

笼罩在比特币头上的另一片阴云,是比特币近年来的价格暴涨所带来的副作用。在设计者原先的理想中,“去中心化”是比特币的一大优势,世界各地的用户分散“挖矿”,比特币平均流通。然而近几年,由于比特币价格暴涨,调用大型计算机进行挖矿成了一门有利可图的买卖,以致出现了“职业矿机”。8年来的数据指出,前4年矿机和CPU算力一直是很分散的,但从2012年底和2013年初开始,矿机和CPU算力迅速集中。截至目前,挖掘和维持比特币的大部分算力都集中在少数“职业矿机”的手上,这意味着大量比特币被少部分人所控制。货币的生命在于流通,一旦一种虚拟货币被少部分人囤积居奇,会造成什么后果呢?没有的人会拱拱手,那就不玩了呗,毕竟它本来就是一串数字。“这个过程将跟17世纪的郁金香泡沫很像。”悲观者们警告说。

不管怎么说,比特币所提出的不易伪造、不会被恶意超发、去中心化的理念,有可能成为未来虚拟货币值得借鉴的理念。而有关比特币所带来的到底是一场革命还是一堆泡沫的争论,依然还在继续着,与之相伴的,是比特币在金融市场上过山车般的价格走势图。

也许,比特币之所以值得投资,正因为多数人还没看明白它的价值。