**【独家】比特币运行原理和金融功能**

*2014-04-15* *韩锋* [郭大刚](javascript:void(0);)



题目：比特币运行原理和金融功能

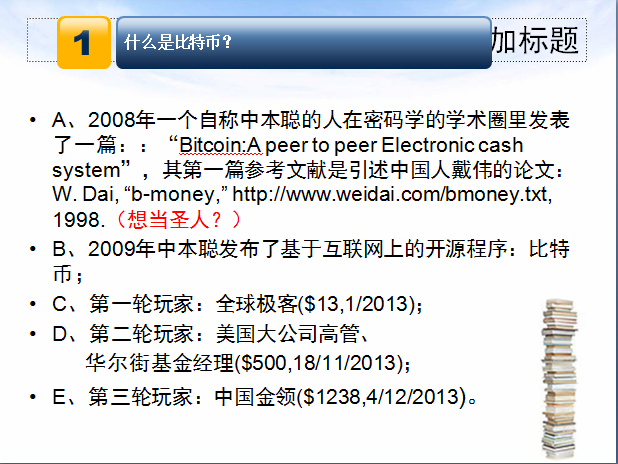
时间：2014年4月8日

韩锋，清华大学博士生，比特币基金会终生会员，曾任清华大学十五规划重点课题“基于网络大数据的创新人才评价和选拔”项目负责人，美国甲骨文教育基金会中国合伙人。

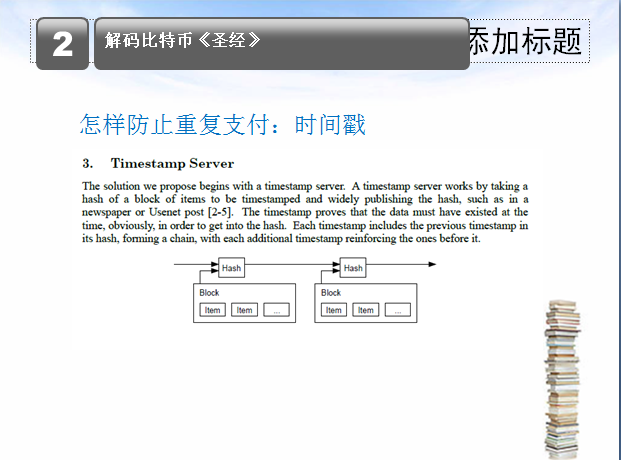
韩锋：大家好！谢谢黄震教授邀请！



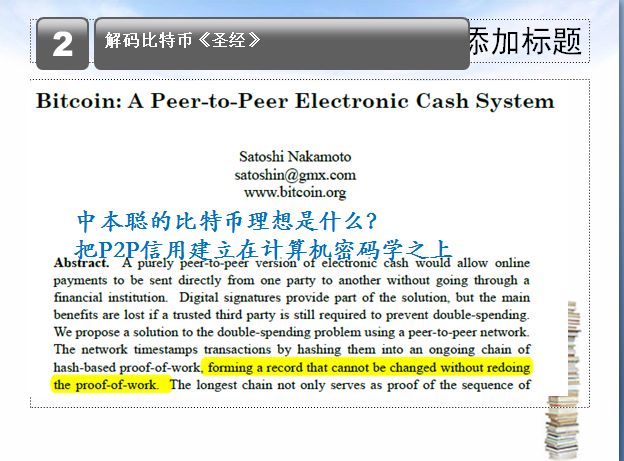




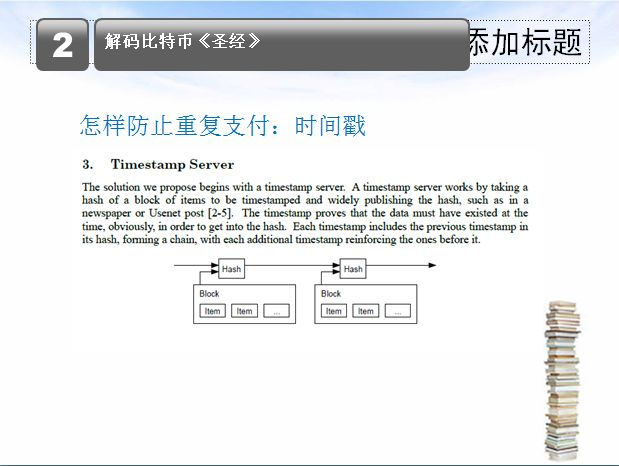
这个过程中有很多传说，中本聪后来也就隐身了。为何隐身？我个人觉得中本聪是想当圣人的，而人类历史中，那些圣人都是死后才真正被认定为圣人，所以他想当 圣人就只能隐身了。2014年，记者报道说在加州发现了他本人，但他现在仍极力否认。后来就派生出很多故事，包括美国有个电视剧也谈到了中本聪的出处。其 中一种说法是比特币是由三个人创造的，其中一个是中国人。这个说法倒也不是空穴来风，因为中本聪的论文中，第一篇引述的就是中国人戴伟的那篇关于电子货币 的方案的论文，这个方案基本架构于P2P、密码学之上已经产生了。所以又有很多人开始演绎，包括有个北大教授说，中本聪这个名字就是戴伟起的，意思是“中 国人本来聪明”。这个说法有点自恋。我们相信中本聪现在就是隐身的状态。比特币自打一产生，第一轮首先是一些极客认为靠着技术，尤其互联网技术，可以改变 世界的现状，尤其改变社会中让人不满的一些情况。所以他们开始把比特币当玩具买来买去玩。最典型的一个故事就是拿1万个比特币买了一张比萨券，并且换成一 个比萨吃了。现在这个比萨估计是人类历史上最贵的一个比萨。到了2013年，应该说是比特币发展元年，很多华尔街高管、基金经理、大公司如 facebook、google等公司的高管也开始参与进来，他们认为比特币在未来金融创新上有很大意义。在他们的推动和努力下，比特币价格出现了实质性 上升，大约达到500美金一个。后来中国玩家大量参与，让比特币价格继续攀升，达到新高峰，最高达到1200美金左右一个。



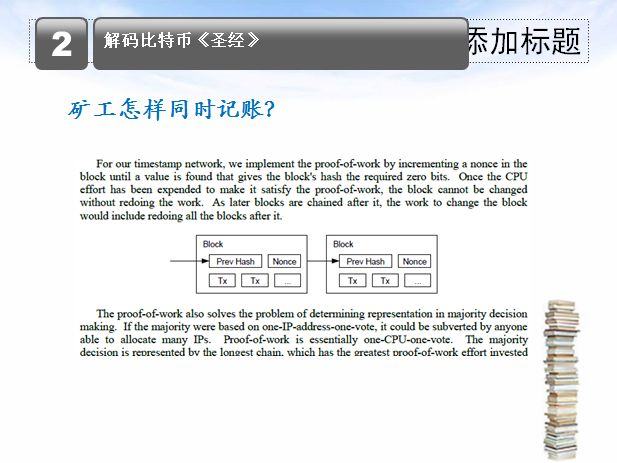
比特币的价格在2013年上升了大约100倍。这样一种社会现象让很多人吃惊，这并不奇怪。因此也出现了很多说法，最典型的是说它是泡沫，类似当年的郁金 香，是一场骗局。我认为我们应该先认真了解比特币运行的原理，它究竟是怎么回事，再来看它是否骗局，是否是郁金香。首先它是泡沫吗？泡沫是肯定的。其实在 早期互联网，大家经历的过程中其实也出现了很多泡沫，股票炒到惊人高度。比如hotmail等。我曾经有缘和李开复讨论过这个问题，当时李开复的观点是， 确实是泡沫，但如果没有早期爆炒的阶段，大家不会大量投资开发互联网应用。恰恰因为互联网有了那么一个阶段，才引起全社会的关注，才开始大量普及，才有了 大量投资和后期的大量应用。我个人认为后来互联网的历史发展证明了李开复博士的判断。所以面对比特币在2013年被爆炒的状况，面对这样一个新生事物，我 觉得如果不想丧失机遇，首先确实应该了解它的运行机制，我们只有在充分理解的基础上，在知识和理性的基础上才能作出正确判断。那么，要想了解比特币的基本 原理，我想，最直接的办法就是研究一下中本聪最早提出比特币的论文。这篇论文之所以在密码学具有划时代的地位，是因为其真正解决了电子货币的重复支付问 题，也就是造假币问题。



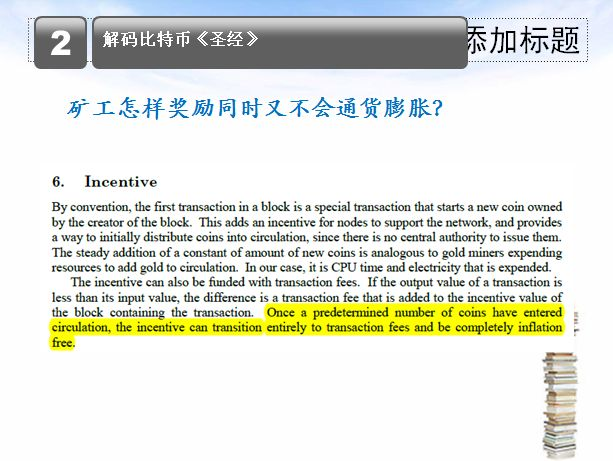
中本聪的理想就是要把人类货币的信用建立在P2P密码学上。他认为传统信用系统都是靠第三方（当然了，现在主要是靠政府）来发行，但他认为第三方成本高、 弊病大，尤其不利于互联网时代的全球贸易。所以他认为应该去掉第三方，信用系统可以建立在密码学的基础上，也就是我后面说的所谓DHC（分布式自治系 统）。这个想法当然是非常创新性的。当然，在中本聪之前，哈耶克（诺贝尔经济学奖获得者）也在上世纪70年代提出，货币应该通过市场竞争起决定性作用。当 然，中本聪想发明一套建立在P2P系统之上的货币，首先当然要解决重复支付问题，也就是造假币的问题。大家知道，纸币（国家主权货币）是靠着强大的法律、 国家暴力系统来惩罚，来控制可能造出的假币。那么比特币靠什么解决这个问题呢？



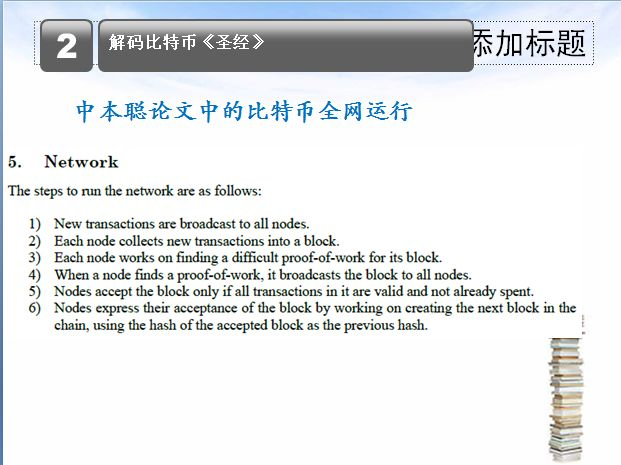
中本聪最大的创造来自于，它是靠着盖时间戳来保证重复支付不可能。也就是任何一笔支付、交易都马上通过盖时间戳记账，保证一笔数字货币不能再被支付给第三 方。按理说数字货币也就是全密码符号，某种意义上说被拷贝是非常容易的。如何保证重复支付呢？就是通过盖时间戳、记账、全网公开，靠着这套机制保证重复支 付不可能。那么大家自然要问，谁来记账？谁来盖时间戳？



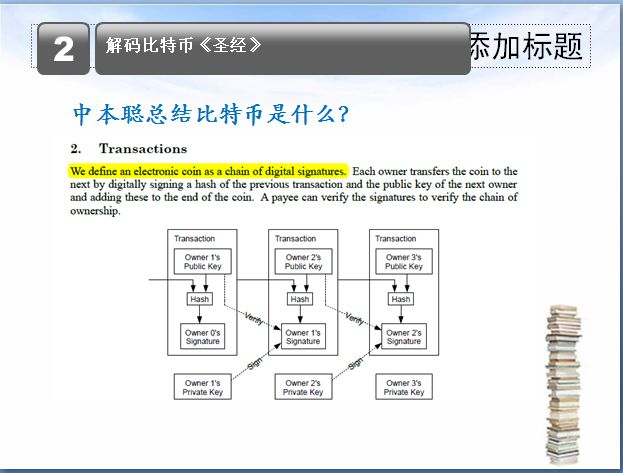
解决这个问题就是比特币最核心的创新，也就是所谓靠矿工的机制。矿工这个词某种意义上并不太准确，他们首先是记账员，要用他的计算机，靠他的算力，来为全 网的比特币交易记账、盖时间戳，保证不会发生重复支付。大家会问，难道这是靠雷锋吗？恰恰相反，中本聪假设人性本恶，人人互相不信任，并不主动做好事，大 家都为利益而来。那么要指望这些算力来给全网记账、盖时间戳，就要保证他们有利益，他们的利益就是可以同时挖矿。那么挖矿就是基于密码学SHA-256基 础之上来进行。实际上就相当于解密码学的方程。谁先解出来，谁先找出哈希值，谁就算挖到了矿。每个block前四年每个奖励50个比特币。四年后是每个 block，十分钟产生一个，每个奖励25个比特币。所以矿工这个名词因此而来。但其实矿工起的最核心作用是盖时间戳和记账。如果没有这些矿工提供他们的 计算机算力，为比特币世界全网记账、盖时间戳的话，那么比特币作为一个支付系统是不成立的。因此，每十分钟挖出一个block，这十分钟之内全互联网所有 比特币交易盖的时间戳都记到这个block里面，然后向全网公开。如果挖矿以后要指望获得25个比特币的奖励，就必须全网承认他的合法性，并且把下一个 block建立在其链条之上。其实比特币就是这样一个从第一个到后面不断挖出的block的链条，所有账都记在这个链条之中。所有比特币钱包也同时下载该 账单，全网确认其正确性，每一笔交易才合法。



那么大家自然会问，比特币的总量有限（中本聪设定为2100万个），理论上在2140年全部挖完，但实际上我算过，2040年已经挖出2050多万个了。 那时剩下的比特币就很有限了。到那会儿如何保证全网的矿工再拿出其算力为整个比特币世界盖时间戳、记账呢？按中本聪的设计，就是给他们付交易费。现在扣每 笔交易费的万分之一，那时会提得更高。那时就不是挖矿了，而是抢着记账，谁抢到了合法的记账权，谁就抢到了交易费。那时就不叫旷工了，而是真正叫记账员。 比特币的系统大概来说是这么设计的，让它这样永远下去，不会导致通货膨胀。所以，比特币的总量有限，是首先吸引很多玩家来参与的重要特征。



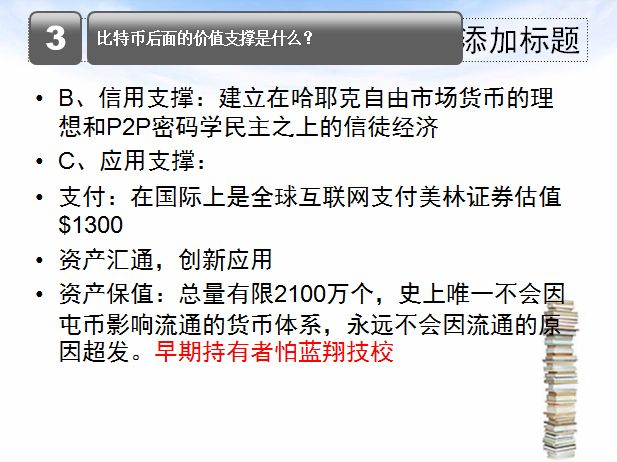
那么中本聪在其论文中，很精辟地总结了整个比特币全网运行的机制。第一，每笔交易都向全网所有节点公开广播。所谓节点是指每个希望挖出block奖励的矿 工的节点。向他们公开，也就是让他们记账，当然了，还关乎谁记的账最后将成为合法的。第二，每个节点，即每个矿工实际上都在不断把新的比特币交易进入他挖 出的block。只有矿工这10分钟之内所有交易都被正确计入block，这个矿工的block才能被承认是合法的，才能获得奖励。那么很多人都在竞争这 个block，竞争记账。谁能最终获得奖励？这就是中本聪发明的工作量证明。只有证明你的算力是10分钟内全网最大的，才能获得block。随着2013 年比特币价格飞升，尤其2013年比特币世界全网算力在飞速成长。那么，只有一个节点真正证明了这十分钟内你的算力是最强的，你才能获得block，并要 向其它节点公开，意味着宣布大家不要再竞争这个block了，要竞争的是这个节点开始的下一个block。那么，全网接受你这个新挖出的block的条 件，是你必须正确记录了全网这十分钟所有的交易，并都盖好了时间戳，否则这个block将不会被全网认定合法，你也不能获得相应奖励。



一旦一个block被全网接受，大家就立刻开始竞争下一个block，下一个block一定要接在这个block之上，也就是绝对不能出现分岔。比特币系 统中一旦出现分岔，就意味着存在造假币的可能，那么这个系统就面临被破坏、崩溃的危险。曾经2013年4月由于系统升级，造成了一次分叉。最后靠比特币基 金会出面协调，所有挖矿退回到起点，从一开始避免了分岔危机，也让大家松了一口气。否则，比特币作为一个支付系统，将会被破坏。那么，中本聪在自己的论文 里，最后总结了一下：所谓比特币系统就是一个数字签名的链条，或者说一个电子记账的链条。只要保证这个链条的正确性、都盖好时间戳，那么这个系统就可以作 为一个完善的支付系统，不会被造假币，不会被破坏，这样完好地运行下去。P2P把信用建立在这个系统之上，前提是大家并不相互信任，这一点是十分重要的。

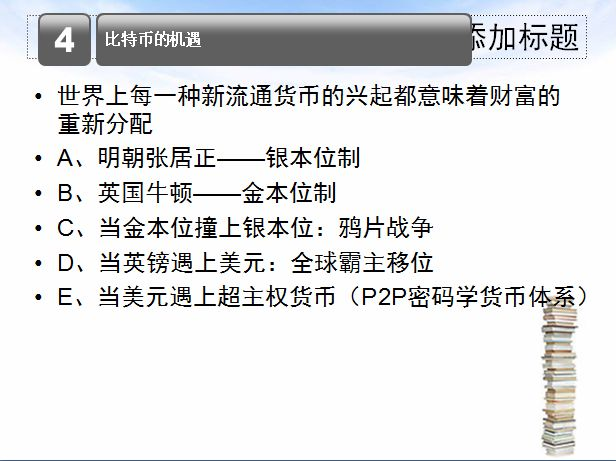


那么，很多朋友在第一次听说比特币的时候，总爱问，法币背后有国家主权，有国家机器去保护，有法律系统，比特币背后有什么？实际上，比特币背后也有很强的 保护，那就是算力。那些全网在挖矿的矿工，他们实际上是记账员，他们当然也是矿工，他们在抢着挖矿。他们实际上是保护着比特币的国防力量，是军队。为什么 这么说？因为比特币系统当然也要防止任何可能的恶意攻击，比如造假币，比如破坏系统让它不按规则运行。中本聪设计的规则是，除非掌握全网算力，即超过 51%的攻击力量，才会造成造假币的可能，才能篡改历史上所有记的账，才有可能对系统造成破坏。按照现在全网算力的成本，现在比特币全网算力的成本已经达 到十几亿美元，当然了这个数字在不断变化。要达到超过51%的攻击力量，至少要达到哈萨克斯坦一年的军费，才能发动这样的攻击。所以比特币系统是靠全网算 力来保护的，比特币的价格某种程度上和其背后的算力也有关。现在一些比特币经济学家在计算比特币可能的合理价格，第一都是要考虑现在全网算力是什么情况。

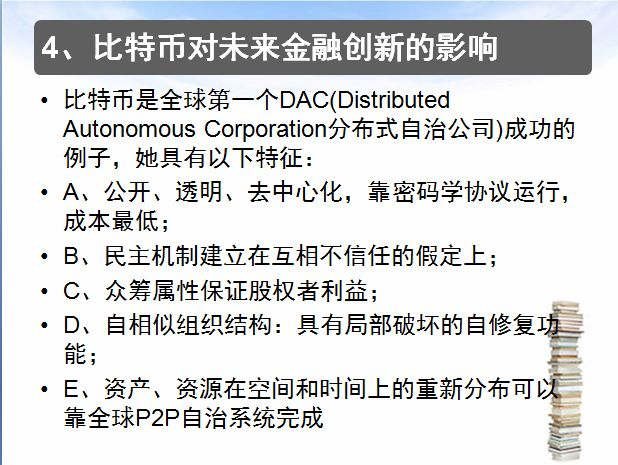


好，我们基本弄清了比特币大概的运行原理后，就能比较理性地分析其价值背后的支撑究竟是什么。我认为比特币背后的支撑，第一是其信用支撑。实际上比特币现 在的价格，我认为很大一部分是靠信徒支撑的，这叫“信徒经济”，有点类似在基督教世界最早期，也是信徒经济支撑了文艺复兴时期欧洲的经济。比如意大利佛罗 伦萨的美第奇家族，据说最早发家也是靠的“信徒经济”。恰恰是有这样的信徒经济，才使得比特币在经历各个政府各种打压的情况下，现在价格还能维持在500 美金以上。我认为绝对是忠实信徒们在维持着比特币价格的基本盘。什么是比特币的信徒？他们相信哈耶克的理念，认为完美的货币应该通过市场自由竞争产生，货 币权或者说金融权应该来自民间。当然了，他们的信仰并不是空穴来风，黄金或白银历史上最早的确都是从民间的信用开始建立的，而后来现在流行的法币其实开始 也是。法币最早往往是靠着黄金或白银的背书才建立起自己的信用体系。所以信用来自民间，或者说在互联网时代来自P2P，不是一个空想的假设，是有历史依据 的。当然了，在信徒经济的基础上，有很多金融机构在分析其可能的价值。比如2013年底，美林证券提出了一个估值，说每个比特币可以值1300美金。我看 了他那篇文献，基本假设是未来全球互联网贸易10%用比特币支付，从而得出比特币1300美金的价值。这也算一家之言吧。我个人认为比特币未来的价值其实 很大程度上在于创新应用，它在于全球资产的汇通，它的速度快，成本低廉，它在交易的时间和空间配置上产生很多创新，我觉得这是它被看好的前景。

当然，很现实地说，现在很多人购买和囤积比特币，是冲着它保值的功能，也就是它总量有限，仅2100万个，大家觉得这个系统从理论上比法币更能保值。因为 法币总量无限，几乎每个法币都超发，最严重的超发到上万亿倍。但是当然也有懂经济的朋友马上会说，只要有人大量囤积比特币，就一定会造成比特币流通的问 题。当然，历史上的确贵金属货币几乎都是因为囤积问题而最后退出了流通领域，因为最简单来说它们不是无限可分的，它们在物理上分到一定程度就无法使用了， 所以不得不退出流通领域，所以它们理论上无法支撑现在全球的经济贸易。但比特币和贵金属货币有一个本质区别在于，它实际上是密码学数字，所以它是几乎无限 可分的，哪怕现在市面上只流通一个比特币，通过小数点后移，也不影响它作为全球支付系统。按照中本聪最原始的设计，可以小数点往后移8位。如果需要，只要 达到全网民主协议同意，小数点还可以继续往后移。那么，有的经济学家就说这会造成通货紧缩。当然，如果世界上只有比特币这一种货币，当然会造成通货紧缩。 但我个人觉得这种情况在可预见的未来是绝对不可能出现的。绝对不可能天下只有比特币这一种货币，而且所有法币都不存在。最后的情况有可能是不同的货币将来 在全球市场上共存。我认为未来比特币保值的功能将会长期存在。比如人们可以用法币购买原材料。而比特币的密码学数学属性保证它在流通领域永远不会稀缺，不 管你囤积得再多。



那么从货币发展历史来看，全球每一次主流货币的变更都相当于财富的重新洗牌。中国最早是明朝张居正确立了银本位，由于当时中国占全球财富的很大一部分，所 以全球的白银都向中国汇集。所谓鸦片战争其实是因为英国当时白银不够，所以要用鸦片作为硬通货和中国进行贸易，而中国当然要拒绝。因此发生了鸦片战争。当 然那一仗打下来我们败了，因此我们退出了世界主流货币的中心，我们因此穷了一百多年。我认为面对比特币这种全新的货币形式的产生，我们一定要抱着参与的态 度，不能冒“在下一次全球支付系统的创新中被边缘化”的风险。我认为这种风险不值得冒。



那么总结一下，比特币究竟是一种什么样的金融创新呢？大家现在公认它是全球第一个DAC的成功案例。针对以上PPT中DAC的主要特征：A、成本比传统公 司成本低得多，邓迪已经讲得很清楚。B、这是西方的一贯传统，从人性恶的基础上开始设计政治机制，不假定要依赖大家的善良和美德，而是假定人有机会都会做 坏事，这样设定，按西方政治学原理，才能最大限度保护每个参与人的权益。C、比特币系统已经证明其有众筹属性，也就是能保证股权者利益，且先入者利益更 多，这是一个合理的经济学系统。我觉得在众筹系统里不能指责先入者利益更大，因为游戏规则就是这么定的。那么比特币系统也就是这样一个DAC系统已经显示 出它有自相似的结构，也就是说局部被破坏，它的自修复功能很强，它可以自相似地再生长。比如一棵大树，砍掉它一边的枝叶，只要整个系统没有被颠覆性地破 坏，那么它会继续生长，而且是按原来的自相似形状修复。那么比特币2014年以来遭到如此多的独立的破坏，尤其还导致了最大交易平台的倒闭，这个系统目前 还能运行，就说明这个系统自修复功能是很强的。总结一下，比特币到目前为止给我们展现的希望就是，所谓未来的金融，也就是资产和资源在空间和时间上的重新 分布，是可以靠全球P2P系统自治完成的，不需要巨大的第三方成本。当然了比特币是第一个试验。不要把比特币说得太大了，什么替代法币那都是不可能的，更 不可能将来比特币一统天下。我觉得除非到了某种恶意才会这样假设比特币，然后来否定它。比特币只不过是一个创新实验，它的本质是DAC。但有这样一个试 验，为未来人类的发展，不光是金融领域，更是为未来在互联网上的创新打开了一个全新的视野和领域，我们值得期待。

【互动环节】

韩锋：圣经云，你看到的东西都是暂时的，你看不到的才是永生的。

沈鸿：比特币就象欧文的乌托邦，设计和愿望是美好，但在现实条件确实艰难的，呵呵。

韩锋：是很难啊，但是有什么真正的创新开始的时候不难吗？

谢涛令：说得太好了！万事开头难嘛。

沈鸿：那为什么打压的国家多？是涉及国家利益吗？

郭大刚：大家还是对新生事物多观察吧，至于是否参与，纯粹个人风险偏好。

韩锋：当然啦，法币占了民众多少便宜大家都清楚，大众想通过数字货币争取自己的权益一定是一个异常艰难的过程。

霍学文：比特币，无中生有，有胜于无。

Q1：请问韩教授，您是把比特币看做货币，还是资产？谢谢。（刘军）

A：有句话我特别欣赏：比特币不是货币，她是货币的互联网。

Q2：能给几篇参考文献吗？（郭大刚）

A：中本聪文献网上很容易查到，建议读英文原版。巴比特和比特币中文网上资料较多。

Q3：请教韩博士对莱特币，狗币等其它电子货币是什么观点？会存在多种电子货币，还是仅会存在一种？（马卫华）

A：我更看好在比特币基础上开发的各种二代系统，不看好仿照比特币开发的所谓山寨币。我相信哈耶克的理论，多种货币并存，让市场来起决定性作用。

Q4：比特币表现出来的一个特性是投机性比较强，但我们可以利用的是其可能会优于法币的保值特性，这样理解是否正确？另外它的价格是完全由交换产生的是么，是套利保持它在不同法币中的兑换价格保持相对稳定性？（马卫华）

A：她的价格我相信目前主要靠信仰、投机和创新扩展。

过当阿狗：人民币一样有炒作的，只是看规模。