本访谈由数字游民生活方式设计教父Tim Ferriss和硅谷天使投资人Naval Ravikant主持。嘉宾Nick Szabo是加密货币领域的先驱，早在1994年提出了智能合约的概念，并在1998年设计创造了Bit Gold，被很多人认为是比特币的前身。三人从加密货币的基本定义聊开，谈论了一系列区块链相关的经典话题，包括密码学、货币起源、智能合约、分布式账本等等。

神聊容易出金句，我们挑几句看看：

1. 现代加密货币像比特币和以太坊等等，是受到密码学里的一个叫默克尔树的结构保护，你可以想象它是被琥珀封存的飞虫。

2. 每个区块就像薄薄一层琥珀，而链有多长，琥珀层就有多厚。

3. 回到货币的起源，会发现这些货币的前身在继承，伤害补偿（像现代社会里打官司，不过没有政府的法庭，大多通过战争讨回公道），陪嫁礼等各种情境下被使用，它们的功能远不止经济学里交换媒介那一条。

4. 比特币可能是人们口袋里或脑海中的瑞士银行。

5. 金钱就是永不破灭的泡沫。

6. 这就是这个概念很疯狂的地方，钱、信息、数学成了同一种东西。我可以用脑袋记住这些信息，每次跨过边界等于是身藏几亿的巨款过境。

7. 干代码就是基于计算机的编码，而湿代码是要人脑理解的，像那些像法律条文。

8. 你可以把智能合约的祖上想象成自动售卖机。

9. 发觉金子值钱不是因为金子有什么奇妙的属性，而是因为它不可伪造的奢侈性（unforgeable costliness），因为它自然的信任最小化的稀缺性。

10. 矿工会是新的银行家，密码学家是新的美联储。

本文由橙皮书特别栏目【硅谷 3 点钟】出品。硅谷 3 点钟，只发布全球最有深度的区块链访谈对话。

正文：

Nick Szabo怎么结识Naval Ravikant的？

Naval：我现在很多好友都是从Twitter上结交的。对我而言，想进行场有质量的对话就会上Twitter，因为这种机会在日常生活范围里一般是找不到的。在Twitter上泡得久了，身边就逐渐聚集起一群优秀而有思想的人。

当初我开始接触加密货币、区块链，在自己探索学习的过程中，不经意间发现了一个名为“Unenumerated（直译为未列举/明示）”的博客，过会Nick说不定可以解释下这博客名的来历。那博客的主题涉猎极广，显然是由一位博学多才的人创作的，我就进去仔细看了里面的内容。之后我就在Twitter上关注了作者Nick，转了他几条推文，有过若干段不超过160字的简短的文字交流。这么一来一往，互相推来推去的就熟悉起来了。

我也一直关注Nick的文章，最近那篇有关社会可扩展性的读完感觉太震撼了。我以为自己很懂加密货币，但那文章帮助我真正重新审视了自己现有认知的架构，升级了我的思维模式。Charlie
Munger提出过不少思维模式，我从Nick那里至少又顺来四、五个，除了Charlie Munger外大概就数他最多了。我在Twitter上发了些那篇文章的节选，然后就有人提议Nick和Naval做个Podcast。以上就是这次访谈的缘起。

什么是加密货币？

Nick：加密货币就像
它的字面意思，是被加密保护了的货币。
现代加密货币像比特币和以太坊等等，是受到密码学里的一个叫默克尔树的结构保护，你可以想象它是被琥珀封存的飞虫。
如果你说：“我开枪射杀了肯尼迪总统。”然后经过默克尔树，私匙签名等一系列流程放到区块链上，它就在那儿了。你就不能事后抵赖：“哦，我没这么说过。”
这种系统下就可以做类似“我给了某人多少比特币”的声明，广播出去等若干个区块产生间隔后（差不多是10分钟生成一个区块），要否认这笔交易或者反悔的难度就成指数倍增长。

Tim：最初为什么会对这方面产生兴趣？

Nick：90年代我们有个叫“密码朋克（Cypherpunks）”的小组，里面有Tim May、Eric Hughes、John Gilmore等等，其中有一部分政治动机的。Tim May想造网络世界的高尔特峡谷，像安·兰德小说《阿特拉斯耸耸肩》里那个创造者和企业家的世外桃源。在书里当然只是幻想设定，Tim认为当时密码学发展已经可以将其变为现实。我基本同意，但觉得还是需要解决合约执行，财产保护之类的问题。然

后我们就开始研究怎么用计算机科学在网络空间里保护交易的进行。

说起密码学，一般人脑海里的第一反应大概是二战电影里出现的恩尼格玛（Enigma）密码机之类。到底什么是密码学？ Nick：密码学的出现原本就是为了守住秘密不被人知道，电影里的纳粹当然没成功。他们密码不够强，最后被图灵破解了，英国人就拿到了情报。类似比特币里用的现代加密方法就要强很多，终结纳粹密码的那种暴力破解法基本不管用，对此大可放心。当然还有别的破解方法，比如盗取别人的私钥。

Naval：密码学可以说是用数学原理保护秘密吧。许多数学领域的突破促进了密码学发展，但理解密码学的关键之一是单向哈希函数加密的概念。

简单来说，如果让一组数据通过这个特殊的函数进行数学变换，另一头出来的结果将很难反过来推导出原始数据，所以说是单向的。以前，如果我要发一些加密信息，我和信息接收者都要有同样的密匙。我先用手上的密匙加密信息发给对方，对方收到后可以用同样的密匙解密得到信息。但是我怎么知道你有的密匙是哪一个？要用什么方式加密？另外，无论是谁截取了密匙就能得到所有信息，因为同一密匙既可以加密又可以解密，所以我们又面临密匙本身传送的安全问题。

之后就有了这样一个创举：把密匙分成公匙和私匙。留在手头的私匙是可以进行加密解密的，而别人可以用公匙为你加密，但不能解密。具体细节可能就不是这次访谈覆盖的内容了，不过值得花点时间去研究下哈希函数、公匙私匙，因为它们是密码学的重要基石。看上去很复杂，实际上没那么可怕。我觉得这是要在现代科技领域立足必备的思维模式之一。

回过头来看加密货币，其实它是在用单向哈希函数来做类似“我给了Tim10美元”的声明。传统模式下，我们需要银行之类的权威机构验证交易。加密货币的一个巨大优势在于，我们再也不需要这可信任的第三方了，验证过程可以在云端的分布式网络上完成。照Nick的说法，这是“可信任计算的黎明”，我觉得说的很好，这里引用一下。

在此之前，计算机是不受信任的，哪怕我用计算机转账给你，实际上还是依赖银行、Visa和其他媒介。但计算机和代码，尤其那些在云端自行运作的系统，其实可以脱离线下的实体机构来保证这些操作的执行。加密货币就是计算机原生的货币系统，一切操作都在计算机上完成，不再需要受信任的第三方机构来核实。

什么是区块链？

Naval：之前那个虫珀的比喻很形象。一开始飞虫只是被很浅的一层琥珀包围，随

着时间推移越积越厚。你看到一大块琥珀的时候，就知道已过了很长的时间了。区块链就是一连串区块，每个区块都是世界各地的计算机基于密码学原理完成大量计算后打包的，很难重新拆开。
所以每个区块就
像薄薄一层琥珀，而链有多长，
琥珀层就有多厚。
所以你可以确信，任何深埋在层层区块琥珀下的信息是从数学、密码学和经济角度不可能被撤销的。好像不该用“不可能”这词，密码学里总要加个“几乎”。

金钱的定义和历史

Naval：我想从这个问题讲起：什么是金钱？我们多次提及货币，金钱，人们总谈论黄金和价值存储。Nick创造了Bit Gold，有些人认为是比特币诞生的重要基础，比特币有自己的突破，但也是站在了Bit Gold这巨人的肩膀上。Nick还创造了“智能合约”及其背后的概念和理论，在很多以太坊之类的加密货币里都可以见到。这话题很复杂，还是从什么是金钱开始吧。如果你跑上大街问十个路人，估计会得到十个答案，所以要先把这定义明确下来。

Nick：比如律师和经济学家的答复就完全不一样。律师大概会说什么国家官方发行的才是货币，像比特币，黄金什么不是国家发行的法律意义上不算。经济学家一般说是交换媒介，相比之下是个更宽泛的定义。不过这背后假设，只有人们交换什么东西时做的交易才有意义，在现代经济体系下这假设还是蛮合理的。

但是回到货币的起源，会发现这些货币的前身——我一般称为收藏品（collectibles）——在继承，伤害补偿（像现代社会里打官司，不过没有政府的法庭，大多通过战争讨回公道），陪嫁礼等各种情境下被使用，它们的功能远不止经济学里交换媒介那一条。比如犹洛克(Yurok)印第安人收集贝壳，把它们看得可重了，还在手臂上纹身记录贝壳的长度，根据稀有程度判定的价值是多少。他们会在财产继承，伤害补偿的情境下使用贝壳。

Naval：一般大家比较认可的理论里，人类使用金钱的历史不过几千年。根据Nick对金钱起源的研究来看可能有几十万年。

Nick：几十万年前达尔文式适者生存的世界里，为什么人们还有闲情雅趣弄什么贝壳项链装饰算是个未解之谜。那些却是考古遗迹里最常见的文物。

Naval：

即使没有交换其他东西，也想要留下什么来保留价值。你可能不会囤面包，石头，房子什么，因为操作起来不太实际。另外它也是种价值尺度，一个通用的衡量标准，我总不能说一辆车等于多少面包吧。金钱包含了上面所有提到的功能。

有些人不看好加密货币，给出原因是比特币不能买东西。或许现在比特币的确没有能行使交换媒介的功能，
但它可能有储值之类别的功能。
它可能是人们口袋里或脑海中的瑞士银
行，或者是类似塞浦路斯银行危机的一种防范措施。 在我的圈子里，有很多人把比特币和法币放在同等地位，接受用比特币来结算。听上去是有点虚无缥缈，像泡沫一样，仅仅因为很多人相信它是钱你就跟着说它是钱。

有个说法我很喜欢：金钱就是永不破灭的泡沫
。如果郁金香的泡沫没有破灭，那我们今天还是会继续用郁金香交易的。当然郁金香作为货币实在不方便，储存、运输、分割都是问题。加密货币则完全相反，它易于储存、运输、分割，很多方面成本更低，甚至比其他任何形式的货币、黄金和商品都强。

是什么赋予加密货币以价值？

Nick：最关键的就是稀缺性了。如果出现通胀，你手上那份的价值就要降低。其他的像储存、运输的便捷程度和安全性也有关系。比特币这些方面都有优势，你可以很轻松地和世界各地的人交易。用硬件钱包的话安全性也有保障。普通的计算机不太安全，可能会中病毒被攻击。区块链用分布式系统就比某一台计算机要安全。硬件钱包是像USB一样的，自己有芯片，比特币的密匙就存在上面，而不是电脑上。

Naval：保存比特币的方式很多，你当然可以存在电脑上，但是电脑一般有网络连接，有安全隐患。你也可以放在交易平台上，基本等于把信任交付给了的不受监管的
银行
。你可以
用硬件钱包这种专
门的设备。你可以写在一张纸上放在
银行里。
这就是这个概念
很疯狂的地方，钱、信息、数学
成了同一种东西。
在
比特

币的世界
，我写下我的密匙
和钱包地址，放在保险箱里，就是冷
储存了。
我可以用
脑袋记住这些信息
，每次跨过边界等于是身藏几亿的巨款过境。真的是很强大很神奇的概念。

比特币计算机、账本和智能合约 Naval：你可以抽象地想象比特币是在一个区块链计算机上运行的。话又说回来，像“什么是比特币”，“什么是区块链”，“什么是区块链计算机”这种根本问题，每个人给的答案都不同。这些都是新生事物，是抽象的概念和设想，很难讲清楚。比特币之于计算机，几乎像物理学界量子力学的翻版，一出来很多圈内人都凌乱了。

Tim：和量子力学一样，又有很多new age、嬉皮士，虽然是出于一片好意，完全将其曲解用在不合适的地方。我觉得加密货币可能也会面对类似的问题。

Naval：这就是理解的层次不同吧，像我不会用默克尔树写代码，给我个比特币区块我也不会分析。从某种程度上我也像那些new age、嬉皮士，在尝试着去理解。但我觉得有必要了解下什么是区块链计算机，它怎么使比特币成为可能的。

Nick：先把这问题放一下，我想提一下有个我们之前没讲到的重要概念，也就是分布在世界各个角落的完整节点和节点上的副本 。节点可以是笔记本电脑或是更大型的机器，这些世界各地成千上万的节点都可以对账本的准确性进行完全验证，所以这可以说是加密货币最安全的运作方式了。

Naval：比方说我给了Tim10刀，Tim给了Nick10刀，原先是要白纸黑字留下记录，或者远古时代用贝壳衡量计数。比特币里用的叫账本，我们可以在上面添一条“Naval转走10刀给Tim，Tim转10刀给Nick”，问题是谁来保证账本的正确性？会不会出现假账？历史上这是中央银行的职责，或者靠纸币上的序列号验证。比特币对这问题的答案特别疯狂，不过还挺管用，那就是每一个人都有一份账本。任何一个比特币网络中的节点都保存一份完整的账本，记录了自比特币诞生之初到现在所有的交易。人们可以在自己家里运行节点，这也证明了现代计算机的存储和计算能力。所有这些计算机共同运作，互相核实手上账本是否一致；如果有不同的版本，哪个才是正确的。然后就有区块链、密码学参与进来了。

Nick：除了数据本身和密码学保护的正确性被复制之外，还有代码、计算机程序。智能合约的第二个定义里，这些节点上被复制运行的代码可以完成些简单操作。比如，在比特币基础上设立智能合约，要求得到若干个签名才给出许可。

Tim：所以智能合约本质上把原本靠人完成的操作写进了程序里，这样就不用伦理、标准约束来保证可靠的行为，这样理解可以吗？

Nick：对，合约里有一部分条约通常会和经济挂钩，但不是百分之百。这些条约有明确的逻辑结构，可以转化成代码放在区块链上，这样合约的执行力就有保障了。在阿尔巴尼亚的人也可以和津巴布韦通人过数学、逻辑和代码直接缔结智能合约，不需要经过阿尔巴尼亚或者津巴布韦权威。

Tim：这就牵涉到你说的“
干代码”和“湿代码”了。
干
代码
就是基于
计算机的编码，而
湿代码是要人脑理解的，像那些像法
律条文，在阿尔巴尼亚律师和津巴布韦律师的脑袋里，有着更流动的形态。

Nick：嗯在我看来那些法律条文像是只能在律师脑袋里运行的程序，普通人运行不了。

Tim：你怎么会对合约那么感兴趣的？

Nick
：有点自
由意志主义意识形
态的影响吧，也是因为法学院最基本
的概念。
财产法和合同法是现代商业社会的两大基石，我很好奇怎么把这些移植到网络空间。

Tim：我碰到过很多有JD（法学博士）加MBA的人，或者JD加PhD的，很少看到JD和计算机科学的组合，还是自由意志主义者。不妨谈谈这两个学位的由来？

Nick：法学学位是因为，单单从计算机科学的角度做智能合约，难免和现实脱节。

Tim：原来是这样，先学了计算机科学的……

Nick：恩，要学习下湿代码。

Tim：哈哈有意思。既然会用电脑了，就顺带看看算盘怎么使吧。好，很有型。

Naval：Nick不
但提出了智能合约的概念，还发
展了背后的理论。
智能合约
就是把湿代码转换
成干代码在区块链上执行，这样就不
能篡改。
过一段时间后，我们之间的合约就像困在琥珀里的虫子。最简单的智能合约就是，我给你钱，你得到钱。这合约很容易履行，当然也做出可以很复杂的。

Tim：合约就是承诺和承诺的履行实实践，或是有更简单的解释？说起合约我总想起各种条款，终止，仲裁什么的。

Nick：
你可以把智能合约的祖上想象成自动
售卖机。
你选择要购买一罐汽水，投了25美分进来，我就要找你一个10美分硬币和一个5美分硬币，还要把你点的汽水投放下来。要是把它写进合同里大概是这么个鬼样子：如果甲方投入一枚价值25美分的硬币，且售卖机内置传感器验证已收到大于或等于所选货品价格的款项，则乙方要如何如何……自动售卖机所做的最主要的两件事就是验证行为（有没有付钱），并自动执行操作（给出找零和货物），这也是智能合约的基本功能。

大多数能通过代码写进智能合约的与付款和金融有关，像抵押、期货什么。此外，智能合约里边也有原本是湿代码的成分，没人知道如何用电脑验证，这些可以通过引入仲裁，多重签名等需要人为操作的步骤实现。比方说房产交易里的第三方托管负责确保合约里所有条目完成后再释放抵押，这里边涉及验房什么的暂时不能在线上自动验证。

Naval：还可以借助智能合约“上链”，就是所有钱，抵押物，有关数据能进电脑的都放上去。现在有很多做这种项目还蛮有意思的。

“肥协议，瘦应用”

Naval：比特币，以太坊和其他加密货币所带来的是一套新的协议。协议是计算机之间交换信息遵循的准则，比如我们之间的交流，使用英语，说话时要有停顿，要给对方发言的机会，一开始要打个招呼，这些都是协议的一部分。在网上常见的有

TCP/IP、HTTP、SMTP。每次你的电子邮件从一个服务器发到另一个服务器都是用了SMTP，即简单邮件传输协议。这些协议是互联网的基础。

在互联网初期有这样的假设：既然带宽、服务器、硬件都很便宜，就免干脆免费吧，发送和接受数据包都不用付钱。然而这些假设正在分崩离析。比如阻断服务攻击，就是你的电脑想要我电脑的资源被拒绝了，然后你觉得反正不产生费用就不断发请求，我这边就会被淹没。垃圾邮件是另一个例子，我不耗一分钱可以给你发无数封垃圾邮件，但这会消耗你的精力。所以这些协议的免费假设越来越不实际了。

这种假设在牵扯到钱的协议上更加行不通，所以我们需要一套协议来反映资源的稀缺性并分配这些资源。加密货币和区块链用“肥协议”交换稀缺资源，并把数据保留在协议层。有两个关键点：其一是由代币控制的稀缺性。在比特币协议里稀缺性指的就是比特币本身有限的数量。其二是放在区块链上的数据。比如我写了篇文章，用哈希函数加密了放在区块链上证明是我写的，然后它就像琥珀里的虫子被区块链的价值保护了起来，别人没法改动。这些新的“肥协议”和原来很不一样，可能会催生出我们没见过的新的互联网。这就是有关“肥协议”的中心内容。

Tim：这篇Joel Monegro写的有关“肥协议”的文章里还提到很有意思的一点，就是HTTP这些“瘦协议”本身必要但没有什么价值，他们被当大众当做纯粹的工具，而在此之上的应用服务，像Google、Facebook却价值几百几千亿。对比之下，比特币现在市值百亿，建立在上面的公司最大也只是几亿的，完全相反。

Naval：是的，价值大部分被留在“肥协议”里。推荐大家都读下Joel Monegro这篇，他写很得好。文章里论证了，正因为这些协议保存了有关身份和其他方面的数据，那些应用就没有那么大权限，你也不会被应用困住。价值主要是以代币的形式在协议里体现。

Tim：这是不是意味着人们会受激励不断造出更多不同种类的加密货币自己囤着？

Naval：这恰恰是正在发生的，我几年前写过篇文章叫“比特币模式下的众筹”，说应用会发行各自的“应用币”（Appcoin），而不是满大街找风投。这些应用币和代币挂钩，被用来向大众集资，这基本就是现在的ICO，首次代币发行。现在铺天盖地都是，很多泡沫，有的都不受控制了。一些应用协议的确有发币的需要，用比特币不行，但大多数开发者只是被利益驱使，想要捕捉价值。这的确是一个很有趣、前所未有的开源软件和协议的融资的方式。

泡沫是坏事吗？

Tim：很多人脑海中泡沫百害无一利，今天头一回看到反对意见，说泡沫破灭后，

人们在一地鸡毛里才更有干劲，有动力去创造新的服务和应用，把失去的再拿回来，从而保留了长期的生命力。我之前没有从这角度想过。

Nick：一定程度上，很多泡沫是不可避免的，未来总是不确定的。

Naval：尤其是在反思内省性质的，我是说那些预测可能会改变结果的产业。一个极端的例子就是预测某人死亡的市场，如果有足够的钱在上面就变成了暗杀市场。泡沫是任何涉及网络效应的系统与生俱来的一部分。金钱就是终极的网络效应。我接受美元作为钱，只因为你也认美元是钱。假如明天我们都相信郁金香有价值，就会改用郁金香交易。如果我相信你会把某样东西当成钱，我就会投资金进去；大家都这么觉得，全跑来掺一脚，泡沫就产生了。像Nick说的，未来是不确定的。有时候我们会判断错误，偶尔要退后一步，就会有能量释放。

几年前我看到这么个说法：随着股票市场越来越高效，波动只会变得越来越大，因为对信息变化的反应速率加快了。比方说现在中国有个大型的铁路项目，连带的会有政治变动，中国期货市场波动，美国股票市场下跌等一连串事件，电脑吸越来越快地收那些信息，推断可能的结果，所以市场波动也更剧烈。未来我们应该会看到泡沫来得更快，破得也快，有大有小。未来一切可以预测、顺风顺水不过是人的幻想。

人们对加密货币或比特币最常见的误解是什么？

Nick：有个技术安全参数叫区块大小，一般人怎么理解的我不太清楚。有一群人觉得这只是个人为设定的障碍，限制了比特币每秒交易的次数。它的职能是保护网络不被人们的交易量淹没，因为交易记录太多、不断累积的话，刚才说的完整节点处理不了。

Naval：如果每台电脑都要有一份完整的交易记录，就不能有无数交易一起砸过来，这要爆炸的。如果交易数量持续飞涨，能继续运行程序的计算机就会越来越少，那谁负责信息安全呢？最初有几百万台电脑，一点点缩水到几十万、几千台，最后只有五个人可以保留完整的记录，那和中央银行就没差别了。人们的争议就是，要不要抬高上限允许更多交易，因为大家都想用比特币买星巴克去，或者只允许高额交易，保证节点多样性。

Nick：这不应该是个公开争论的议题，就好像不会有人提议说来投个票吧，要不要把石墨慢化反应堆里的石墨拿掉？石墨有它的作用，要防止反应堆温度过高熔化，这类事情还是交给工程师决定比较妥当吧。不知出于什么原因，总有一群人想把石墨抽掉，让反应全速进行。

Naval：这也是比特币面临的一个问题，因为很多人持有一点点比特币，觉得什么都和切身利益相关，发表各自的意见，互相争得面红耳赤。Nick有条推文讲得好，毁掉你对比特币的投资的最好方式，就是聚集一群互联网暴民去重新设计比特币。现在还真有点这势头。

Tim：在我们开始录音前，你说你从没见过那么多科研工作者不顾形象互撕的场面。

Naval：是的，现在最闹腾的是关于川普的推文，不过谈起政治一直都比较容易激动，接下来就轮到区块链了。经常有康奈尔、马里兰州大学等高等学府里的博士互怼，言辞激烈，职责对方道德操守，说人家是“喷子”，他们各成一派，有自己的支持者。

Tim：很多人都听过这句话：“人的忠诚度取决于选择的多少”。用在这里就是：人的文明程度取决于背后利益多少。

Naval：利益就是一切，像Charlie Munger说的，“说服别人要诉诸利益而非理性”。回头看比特币的设计，它的精妙之处恰恰在于背后的博弈论激励机制。

是什么让比特币与众不同？

Nick：可以从多个方面去看这个问题。在最重要的、最基本的计算机科学层面，我们证明了要成功攻击这个系统，实现双重支付等欺诈操作需要至少51%算力/哈希率。

Naval：就是任何篡改账本的行为对吧，其实大部分是没法改动的。还记得琥珀飞虫的比喻里，一旦一笔交易完成且被记录，回过头来再改就几乎不可能了。不过在新一层琥珀覆盖上去的过程中，还是可能有人使坏的。有个常见的误解就是，如果拥有系统内51%计算机的比特币矿工们（就像金矿工挖金子，比特币矿工“挖”比特币，他们实际做的工作就是覆上一层层琥珀）串通勾结好，他们就可以回过来修改账本历史。事实上他们不能改动现有的账本，但他们可以对正在进行的交易做手脚。不好意思打岔了。

Nick：这是计算机科学方面的一个局限性。此外，软件升级可能会改动更多的规定。这两件事，尤其是软件升级，会弄得比较政治化。

Bit Gold、比特币和工作量证明

Nick：Bit

Gold是受到金钱起源系列研究的启发。以前的纸币（比如银票）和今天的钞票 一样，也算“狐假虎威”，让人相信它依然是很值钱的东西，而不是废纸一张。不过那时候去柜面换出来的是真金白银，现在就只认美联储一张纸。

Naval：都是郁金香，绿油油的、熨压平整的郁金香。最早是贝壳、金子，然后是金本位制货币，现在法定货币背后就什么也没有了。

Nick：造币本身很方便，PayPal、DigiCash什么基本都在做这种中心权威发行的、基于信任的货币 。但是我不满足于此，因为我希望最终柜面上换来的是种“信任最小化”的东西。全世界都认为金子是值钱的，回到那些原始部落里，金子、贝壳什么依然是通用的，跑去隔壁村子他们也都接受。他们不会要你什么IOU（借条），你们交情没铁道可以并肩上战场的程度，但他们会收贝壳、铜串珠、金串珠。话说最早的金制物件是串珠，这是金属早期最重要的用途，不是刀子武器等等。所以我就研究怎么把这种“信任最小化”的特性复制到网络空间。

一番研究下来，
发觉金子值钱不是因为金子有什么奇妙的属性，而是因为它不可伪造的奢侈性（unforgeable costliness），因为它自然的信任最小化的稀缺性，即你不需要相信任何人去保证这种稀缺性。我尝试通过工作量证明（PoF）、Adam Back的哈希现金（hashcash）将其再现。工作量证明就是用计算机解数学题，从计算机科学的理论我们知道一道题要花多久才能得到答案。不过问题是能通过改进硬件提高解题速度，所以有人为此设计专门的设备。

Naval：覆上琥珀需要投入真正的资源才能做到。系统的稀缺性从有实际花费的算力中产生，因而在比特币系统里贡献的算力越多，你的选票就越重要。怎么知道你的算力是提供给比特币系统，还是随意浏览网页消耗的？这通过数学函数证明。比特币网络算法给出那些谜题，如果计算机解出来了，等于证明它为了解题投入了一定财力、时间、能源、计算力，然后就有机会投票决定账本的设计发展，并得到比特币回报。这就是矿工做的，用电脑完成工作保证网络安全，然后提交证明得到发行的新币。

Nick：中本聪的创新就是把工作量证明用在了保障系统安全上，当然中本聪是何方神圣没人知道。

Naval：比特币基于Nick、Hal Finney和其他计算机科学家的成果被创造出来，中本聪完成了理论的现实呈现。Nick你有Bit
Gold的理论设计，但可能没办法真的把它造出来。

Nick：我也是正儿八经的程序员，不过的确我没有写代码造Bit

Gold，就只有一个设计。

Naval：所以比特币的创造者好像是行家里手，并且了完美地隐藏身份，用中本聪这化名进行发表。

Nick：我再补充点关于Bit Gold的内容。有个防止飞机因电脑崩溃发生事故的协议：在飞机不同的位置放置若干芯片，它们互相传递信息，如果有冲突的话就投票，得票多的被采用作正确的信息。这在数学上被证明是给定条件下（已知芯片数量等等）的最优模式，叫做“拜占庭共识”。我将它套用在复制账本和数据的过程里，结合默克尔树，交易历史等等。互联网不像飞机，数不清大家各有多少芯片，可能会有人打肿脸充胖子，明明只有一个却说自己有100个芯片。中本聪的创新又往前走了一大步，用工作量证明来保证系统安全。支持哪个选项的哈希率最高，就认定哪个，当然这有51%算力的限制，所以有51%算力攻击的说法。

Naval：基本就是算出一题有一张选一票。比特币网络是由世界各地的计算机构成的，它们一起创造出这共有的区块链计算机。选票与贡献的CPU资源成比例，他们投票选出哪个是有效的交易，然后这笔交易被封存在琥珀里。一些像你说的嬉皮士那样的人会提出这样的反对意见，你消耗了这么多电力这么多网络资源，因为那些电脑要不停的互相传送信息、发布广播，太浪费了！很多人都持类似的观点，甚至我也一度这么想过：好吧，有朝一日说不定会有人想出比工作量证明更好的机制，权益证明（PoS）或者其他什么。

社会可扩展性

Nick：如果把人类的能力在图表上画出来，它基本就是一条平着的横线。10万年前脑容量和现在也差不多，智商没出现过大变化，就一点点弗林效应。另一方面，计算机很多性能过几年就翻一倍，内存、CPU、带宽等等。你可以对未来做很多不同猜想，我觉得以后会有大量剩余资源。电脑处理一些问题的能力可能是人的一千、一百万倍，然而我们还是保留了臃肿的官僚机构用老方法办事。能不能做个交换呢？计算机科学家和工程师通常想方设法优化系统，让它越来越高效。可不可以倒过来，牺牲系统效率换取其他能力，即使这样有不小的消耗？比如让阿尔巴尼亚人不经过受信任的权威中介给津巴布韦人付款。比特币就是这样的一个例子。

Naval：再回过来点，是什么把人类和其他动物区别开来？我们是社会性的，而且这社会性跨越了基因的界限。150个尼安德特人一同上战场，因为他们基因上有关联；1500个智人一起上战场，可能只是因为抽象的基督教信仰，而且他们可以把故事传递开。比特币带动的社会可扩展性让相互不认识，不信任的人们进行安全的交易，他们可能都不知道对方的真实身份或所在地。而且不只金钱交易，还有复杂的合约，任何可以想到的只要能编入代码，就好通过这计算机完成。虽然它缓慢、效

率低，但是可以淘汰过程里一层层官僚和收“买路费”的人。

Tim：所以可以突破150人的邓巴数是吧？

Naval：对，就是用计算可扩展性来换社会可扩展性。

Tim：我想引用下Nick的一句话：“受信任的第三方是安全漏洞。”为什么做这个交换，允许低效率？区块链计算机与网络服务器相比缓慢且昂贵，据粗略估计要慢且贵一万倍。但是区块链计算机上的应用对安全性和可靠性有较高的要求，即使效率底下、有硬件运行成本，和太高的风险权衡后依然是可以接受的。

Nick：我们累积的剩余硬件资源，最近才开始利用起来。可以拿来做工作量证明这种要消耗计算资源的安全协议，也可以用来保留副本。虽然不是特别大量的剩余，但是有足够容量、空间、带宽去复制几千几万份小的交易信息放到世界各个角落，这样就创造出了琥珀昆虫的效果。

Naval：社会可扩展性在文章中的定义大概是这样，一项技术的社会可扩展性多高，一方面就看使用人数多少。美元大概是世界上流通最广的货币了，日常生活中使用的人数可能就十亿。比特币如果被普通大众接受，理论上可以任何人使用，只要有网络就行，而现在网络很普及了，所以它的可扩展性就更高。

政府或其他组织有没有可能管制比特币和其他加密货币？

Nick：因为世界各地有那么多份完整记录的副本，消灭一部分还是可以在很多其他地方找到所有历史记录，所以要管理起来还挺难。比较容易的切入点是法币和加密货币兑换的环节，这些一般在交易所进行，一把抓起来方便。交易所安全性也不太有保障，“受信任的第三方是安全漏洞”，这也是大多数偷窃，黑客攻击出现的地方。

Naval：交易所就像银行，是监管者和小偷的蜜罐。除了交易所，也有通过同城活动交易的，约好在哪里见面用现金换比特币，那种分散交易的量也增加了不少。Bram Cohen发明的bt下载，占了四分之一甚至一半的总网络流量，政府也曾尝试关停。我不认为政府能关了比特币，而且那些敞开双臂迎接加密货币的政府会从中得到很多的。我把比特币称为“钱联网（Internet of money）”，它深深根植于网络的运作。假如美国决定灭了它，禁止加密货币，这就好像说要禁了HTTP，基本就是对准自己脑门开枪的行为。现在已经有一部分项目跑去瑞士、直布罗陀做ICO，一些项目组离开美国，尤其是纽约这些监管更严的地方。这就是把创新力给逼走了。

Tim：对纽约来说，有什么动机去支持，或者至少不干涉这种新技术？

Naval：就像互联网的出现带来了Netflix、Spotify，改变了好莱坞的格局。出版业的地位被Facebook、Twitter撼动。互联网也会从本质上改变金融界，我个人认为新的金融业最终会在智能合约、加密货币相关的创新领域落脚，这当然不是什么投资建议啊。我觉得新技术可能取代很多金融基建，如果纽约要下驱逐令，那它以后可能不再会是金融中心了。每次去纽约都觉得很欢乐，看着高楼林立，西装革履的人们，我心里清楚，20年内他们90%都会被淘汰。我现在不会考虑进入投行，因为哪些工作都会自动化，商业银行也是。银行家就是上一代的矿工，他们保证货币安全得到报酬。美联储要发货币先经过银行，银行自己会拿走一部分，把剩下的分给其他人。矿工会是新的银行家，密码学家是新的美联储，所有人都可以是新机构的拥有者。

人们担心货币贬值的时候会关注黄金。在加密货币世界有类似的规律吗？ Naval：比特币的确是一种价值储值，它总量只有2100万，这在协议里定死了，一个也不会多。还有好多比特币已经被遗失了。有人为了保证安全造了一大串复杂的密码，结果自己弄丢了密匙。也有存在电脑上，不把小心电脑处理掉了，翻遍垃圾堆要把价值1万比特币的破电脑找回来。

Nick：所以最好有硬件钱包做备份，密匙就不容易被盗或遗失。

Naval：比特币是数字黄金，像我儿子那辈成长过程中会一直有黄金，也有比特币。

Tim：有没有可能比特币离我们越来越远，到你儿子那辈就见不到了吗？

Naval：比特币本身的未来可能有点艰难，因为它面临着治理问题。其他加密货币如以太坊等等，可能会取代它的地位。但是区块链计算机这概念的消失，就好像说互联网会陨落，有点难以想象。这项技术太根本了，如果有什么数学突破可以把瓦解现有的加密机制，商业互联网也会一起下水。我觉得未来区块链计算机会在流通货币、价值储存、合同法、任何金融工具、预测市场等方面占主导。我的孩子以后会选择Bit Gold演化的数字黄金，而非实物黄金。