货币、区块链和社交扩展性

Author	Nick Szabo
Translator	Taosheng Shi
WeChat Contact	data-lake
Mail Contact	tshshi@126.com
Organization	NOKIA
Document category	Distributed System
Document location	https://github.com/stone-note/articles

Version	Status	Date	Author	Description of changes
0.1	Draft	12/7/2017	Taosheng Shi	Initiate
0.2	Draft	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere
1.0	Approved	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere

Contents

1 介绍(Introduction) 3

2 货币和市场(Money and Markets) 6

3 网络安全的社交扩展性(The Social Scalability of Network Security) 8

4 区块链和加密货币(Blockchains and Cryptocurrencies) 8

5 结论(Conclusion) 16

1 介绍(Introduction)

各种区块链正在风靡流行，其中最大最古老的区块链是比特币。迄今为止，经历了八年时间，比特币的价值也经历了从 10,000 比特币买一块比萨到（在可交易之前以传统货币定价比特币）每比特币 1,000 美元以上。截至撰写本文时，比特币的市值已超过 160 亿美元（译者：文章写于 2017 年 2 月 9 日）。八年的不间断运行，比特币区块链几乎没有经济损失，现在已成为世界上最可靠、最安全的金融网络。

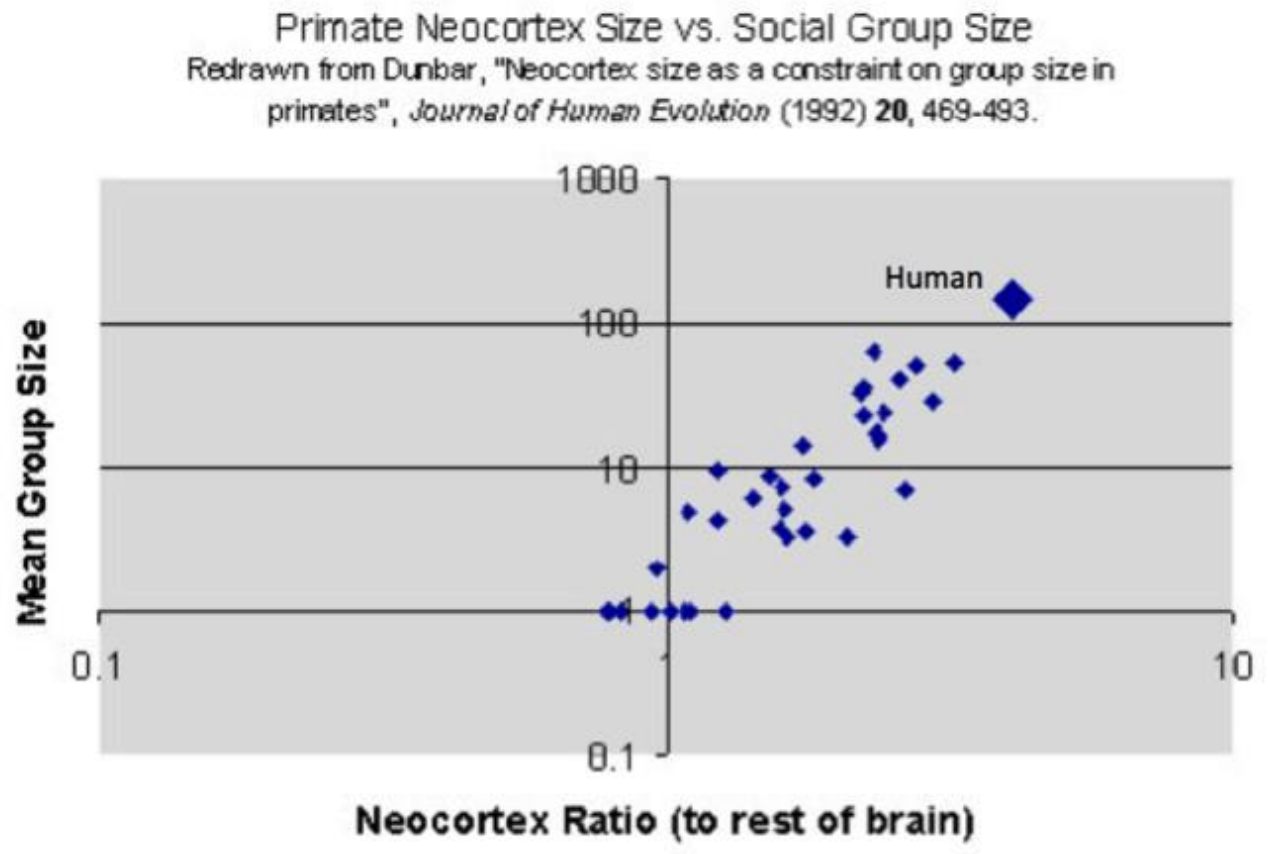
比特币成功的秘诀当然不是计算效率，或者在资源消耗方面的扩展性。 专业比特币硬件是由顶级（高薪）专家设计的，并且只完成一项特定工作——重复解决一种非常特定的，故意设计的计算难题。因为计算的唯一输出仅仅是一个“证明”（证明计算机做了代价高昂的工作量），所以这个难题求解被称为工作量证明。比特币用于难题计算的硬件可能总共消耗约 500 兆瓦以上的电力。但这不是引发工程师或商人专注于降低资源成本（至最低限度）的唯一原因。每台运行比特币的计算机并不是将协议信息减少到最少，而是使用大量冗余的“inventory vector”数据包喷射(spray)整个互联网，以确保所有消息都能够能精准打通(get accurately through to)尽可能多的比特币计算机。 因此，比特币区块链无法像传统支付网络（如 PayPal 或 Visa）那样每秒处理大量交易，但比特币激发了工程师和商人的资源感知和性能测量最大化的敏感性。

相反，比特币成功的秘诀在于：用大量的资源消耗和很差的计算扩展性“购买”更有价值的东西——社交扩展性。社交扩展性是指一个组织的能力——一种关系或 shared endeavor。这种关系或 shared endeavor 是指人们可以反复参与，并反映习俗、规则或其他（约束或激励参与者行为的）特征——以克服人类思想和组织（在激励或约束方面）的缺陷（限制谁或多少人可以参与）。社交扩展性是指随着参与者的多样性、数量及其关系的增长，参与者能够思考并响应组织和其他参与者的方式和范围。这关乎人的局限性，而不是技术的限制或物理资源的限制。那些独立的工程学科，例如计算机科学——用于评估技术本身的物理限制，包括处理更多用户所需的资源能力或更高的资源使用率——这些工程扩展性规范并不是本文的主题，但会用于和社交扩展性对比。

社交扩展性与心智的认知局限和行为倾向有关，而与机器的物理资源限制无关。尽管如此，思考和讨论技术的社交扩展性对于组织具有突出的帮助意义，而且通常是至关重要的。组织技术的社交扩展性取决于该技术如何限制或激励对该组织的参与，包括保护参与者和组织本身免受有害攻击。 考察组织技术的社交扩展性的一种方法是观察能够参与该组织而获益的人数，其次是观察制度赋予或强加给参与者的额外益处和危害（由于认知或行为原因，参与制度的预期成本和其他危害大于其收益）。（能够参与组织而获益的）人们的文化和管辖多样性往往也很重要，特别是在全球互联网环境中。组织越依赖当地的法律、习俗或语言，那么它的社会可扩展性就越差。

没有过去的组织和技术创新，参与 shared endeavor 的人数通常被限制在最多 150 人——即著名的“邓巴数”。在互联网时代，创新技术将不断扩大我们的社会能力。在本文中，我将讨论区块链（特

别是实现加密货币的公共区块链）如何提高社交扩展性，即使在计算效率和伸缩性方面出现巨大降低的情形下。



认知能力——这里以物种新大脑皮质的相对大小的形式——限制灵长类组织群体的大小。维护动物或人类群体的亲密需要大量的情感沟通和关系投资，例如灵长类动物的抚慰，闲聊，幽默，讲故事以及传统人群中的对话，唱歌和游戏等。人类的认知限制，也就是著名的 150 人左右的“邓巴数”，决定了谁可以参加一个组织或多少人参与一个组织。克服人类认知限制需要组织和技术创新。（来源）

社交扩展性的创新包括组织创新和技术创新，把认知功能从心智转移到纸上或者机器上，降低认知成本，同时增加心智之间信息流动的价值，减少脆弱性，利于寻找和发现新的互利参与者。Alfred North Whitehead 说：“这是一种极其错误的老生常谈，所有学究（copy-books）和名人在发表演讲时都会重复：我们应该培养我们做事的思考习惯。情况恰恰相反，文明的进展是通过扩大（直接执行无需思考的）重要操作的数量。” Friedrich Hayek 补充说：“我们不断地运用公式，符号和规则（而这些含义我们并不明白），并且通过利用这些公式，符号和规则，我们获得并不具备的知识的帮助。我们在（自己领域中已经证明是成功的）习惯和组织之上来发展新的实践和组织，而这又成为我们构建文明的基础。”

各种各样的创新降低了我们对参与者，中介和外部人员的脆弱性，从而降低了我们的必要性担忧：用我们有限的认知能力去担忧日益增多，日益多样化的人们会如何表现。另一类创新促进了日益增多，日益多样化的参与者之间准确收集和传输有价值的信息。还有其他的创新促使更多互利参与者能够相互发现。所有这些创新在人类史前和历史的进程中改善了社交扩展性，甚至使基于大量全球人口的现代文明成为可能。现代信息技术（IT），特别是近代以来计算机科学的发现，可以发现更多互利的匹

配，可以激励信息质量的提高，并且可以减少某些机构交易中对信任的需求（降低信任成本）。对于日益增多，日益多样化的人们来说，这些技术以非常重要的方式进一步提高了社会可扩展性。

心智之间的信息流动——我称之为主体间协议——包括口头和书面文字，习俗（传统），法律内容（规则，习俗和案例先例），各种其他符号（例如在线信誉系统的“星级”）以及市场价格等等。

信任成本最小化降低了参与者之间以及我们对中介和外部人员的潜在有害行为的脆弱性。大多数组织都经历了漫长的文化演变，比如法律（降低暴力，盗窃和欺诈的脆弱性）和安全技术，总的来说，在多个方面降低了我们的脆弱性。因此，与引入这些组织和技术演变之前的脆弱性相比，我们需要相信我们的人类同胞。在大多数情况下，一个足够值得信赖的组织（如市场）依赖于其参与者的信任——通常是隐含地，对另一个（足够值得信赖的）组织的信任（如合同法）。这些被信任的组织反过来会实施各种会计，法律，安全或其他控制措施，使其足够充分并成为惯例，至少能够促进其客户组织的功能值得信赖（通过最大限度地降低他们自己的参与者（例如会计师，律师，监管者和调查员）的脆弱性。创新只能部分消除某种脆弱性，即降低对他人的信任需求或信任风险。没有完全不需要信任的组织或技术。

即使是使用最强大的安全技术—— 加密，完全不需要信任的情况也不存在。尽管一些密码学协议以非常高的算力保证了非常高的安全可能性，确实保证了某些特定的数据关系，但考虑到参与者所有可能行为，密码学协议并不能提供百分之百的保证。例如，加密可以强力地保护电子邮件免受第三方的直接窃听，但发件人仍然相信收件人不会直接或间接地将该电子邮件的内容转发或以其他方式泄露给任何不受欢迎的第三方。再举一个例子，在我们最高强度的共识协议中，假定某些参与者或中介人的有害行为远远低于百分之百（以计算能力，股权持有量，个性化和计数），可以破坏参与者之间的交易或信息流的完整性，从而最终损害参与者。计算机科学在最近以来取得的突破可以非常显著降低脆弱性（减少漏洞），但远远没有达到消除任何可能的脆弱性（漏洞，潜在攻击者的有害行为）。

匹配是促进互利参与者之间的相互发现。匹配可能是互联网最擅长的一种社交扩展性。像 Usenet News，Facebook 和 Twitter 这样的社交网络有助于发现灵魂相近(like-minded)的人，两心相悦(mutually entertaining)的人，或者是心有灵犀(mutually informing)的人（甚至是未来的配偶！）。当人们有可能以互利的方式发现对方之后，社交网络便可以促进不同层次的个人投资关系，从不经意到频繁再到迷恋。Christopher Allen 等人对互联网游戏和相关社交网络中的群体规模和时间相互作用进行了一些有趣而详细的分析。

eBay，Uber，AirBnB 和在线金融交易所通过商业匹配活动大幅改善社交扩展性：搜索，寻找，汇集和促进互惠商业、零售交易的谈判。这些服务或相关服务还有助于支付和运输等业务，以及有助于陌生人之间的交易验证（在这些交易中承担的其他义务是否履行，以及履行质量的交流，如“星级评分”系统，Yelp 评论等等）。

鉴于互联网在社交扩展性方面的主要优势是匹配，那么区块链的在社交扩展性方面的一个直接优势是降低对信任的需要（信任成本最小化）。区块链通过锁定完整性(integrity)来降低脆弱性，例如一些重要业务（如创建和支付资金）的完整性，一些重要信息流的完整性，未来可能会有一些重要匹配功能的完整性等等。 私有计算（秘密和任意可变的活动）的信任可以由公共计算的置信度（可验证的一般不可变的行为）代替。本文将重点讨论降低脆弱性及其益处（促进标准有益行为应用于更大范围的潜在交易方），即无需信任的货币。

2 货币和市场(Money and Markets)

货币和市场通过市场匹配（广泛接受和标准化的对偿履行）将互利的买方和卖方匹配在一起，从而直接使每一个特定参与者受益。这里的市场，我使用的是亚当·斯密的术语：不是作为买卖双方聚集在一起的特定场所或服务（尽管有时可能涉及这些），而是一系列典型的成对交换，供应链凭借这些交换使产品得到协调。

货币和市场也会刺激创建更准确的价格信号，从而降低其他类似交易参与者的谈判成本和错误。因此，和以往的交换体系（对比竞争性市场，以往的交换体系更类似于双边垄断）相比，货币与市场的有效结合（竞争性市场）允许更多数量和种类的参与者协调他们的经济活动。

货币和市场涉及匹配（把买卖双方结合起来），减少信任成本（自利主义信任而不是熟人和陌生人的利他主义信任），提高扩展性（通过金钱或一种广泛接受和可反复使用的媒介实现对偿履行）和信息流质量（市场价格）。

关于货币和市场的最早思想家是亚当·斯密。 在英国工业革命爆发之初，史密斯在“国富论”中指出，即使是最微不足道的产品，也直接或间接地依赖于大量各种各样人的工作：

在一个文明发达的国家中，如果看一下最普通的工匠使用的生活用品，你会知道，为了使他们能享用它，必须贡献自己工作的一小部分(哪怕只是很小的一部分)的人多得不可胜数。例如，尽管看起来很粗糙，工人穿的毛织品上衣也是大量工人一起劳动的结果。牧羊人、选毛人、梳毛人、染工、梳理工、纺工、织工、蒸洗工、缝纫工和许许多多其他的人，必须结合他们不同的手艺才能完成这种很常见的产品。此外，把材料运输到最遥远的地方需要有多少运输从业者啊！需要多少商业和航运，需要多少造船人、航海人、制帆人、制绳人，以便把染匠所使用的不同染料带到一起——这些染料常常来自世界各个最遥远的角落！可见，为生产最普通劳动者所使用的工具需要经过多少种类繁多的劳动！且不谈如航海人的船舶、磨坊工的磨坊，或是织布匠的织机那些复杂的机器，我们只来看看牧羊人用来剪羊毛的剪刀这一非常简单的机械，它的产生就需要各种不同的劳动。采矿工、熔炉制造工、伐木工、烧炭工、造砖人、泥水匠、炉工、铁铺的设计与建筑者、锻工、铁匠……必须把他们的不同手艺结合起来，才能生产出剪刀。假如我们用同样的方式来考察剪羊毛工人的衣着和家用器具，他贴身穿的粗麻衬衫、他脚上穿的鞋、睡的床以及床的所有不同部件；他准备膳食的厨房和炉灶，烧饭用的煤炭(这或许是通过遥远的海路或者陆路运来的)，他厨房中所有的器皿，餐桌上所有的用具比如刀叉，用来盛饭菜的陶瓷和锡盘，他吃的面包喝的啤酒，抵御风雨、保持屋内温暖、照明房屋的玻璃窗户、发明玻璃所需要的知识和技艺(没有玻璃，在世界北方地区生活的人们就不可能拥有非常舒适的住所)，连同生产这些便利品中所使用的所有工具；哎呀，假如我们考察一下所有这些物品，看看每一种物品要使用多少不同的劳动，我们就会明白，没有成千上万人的互助和合作，一个文明社会中最普通的工人也不可能得到他最简易的生活用品，即使根据我们的虚假想像他们是可以得到的。同富有人家的极度奢侈相比，他的生活用品无疑极其简单而平常；然而以下说法也许是真的，即一个欧洲君主的生活用品在数量上大大超过一个勤劳节俭的农民的生活用品，但是其超过程度却也比不上这农民的生活用品超过许多非洲君主的程度——这些君主可是数以万计生命与自由的绝对主宰。（译文来自：《国富论》(英)亚当·斯密 著，孙善春，李春长 中国华侨出版社）

这是 1776 年以前的事情。自 1776 年以来，伴随着工业革命和全球化浪潮，劳动力分工已经多次重新定义、阐述和扩大。货币和市场并非相信陌生之间的利他主义，而是创造出许多互惠互利的匹配，从而激励互相漠视的巨大人类网络为共同的福祉而合作：

在文明社会中，随时有取得多数人的协作和援助的必要。别的动物，一达到壮年期，几乎全都能够独立，自然状态下，不需要其他动物的援助。但人类几乎随时随地都需要同胞的协助，要想仅仅依赖他人的恩惠，那是一定不行的。他如果能够刺激他们的利己心，使有利于他，并告诉他们，给他作事，是对他们自己有利的，他要达到目的就容易得多了。不论是谁，如果他要与旁人作买卖，他首先就要这样提议。请给我以我所要的东西吧，同时，你也可以获得你所要的东西：这句话是交易的通义。我们所需要的相互帮忙，大部分是依照这个方法取得的。我们每天所需的食料和饮料，不是出自屠户、酿酒家或烙面师的恩惠，而是出于他们自利的打算。

斯密继续描述劳动力分工和劳动生产率是如何依赖于两两交换网络的范围：“分工是由交换引起的，分工的程度，因此总要受交换能力大小的限制，也就是交换必然受市场范围限制”。随着国家和全球交换网络的发展，越来越多的生产者介入到这种交换网络，从而增加劳动分工和劳动生产率。

货币通过增加交易机会来促进社交扩展性。通过降低偶合问题（交易中的需求偶合以及单方面转移支付中需求与事件的偶合），以及作为存储和转移的形式被广泛接受，并可重复使用，货币大大降低了交易成本，从而可以进行涉及更多种类的商品和服务的更多交易，建立（更多数量和各种各样人群介入的）其他财富转移关系。

各种各样的媒体，从口头语言本身、粘土、纸张、电报、无线电到计算机网络，都已经用来传达报价，承兑以及由此产生的交易和价格，同时也传达业务监控和其他商业信息。市场和货币如何产生价格网络？这方面最为知识渊博的洞察可以从 Friedrich Haye（著名的哈耶克）的文章“知识在社会中的利用”中找到：

从根本上说，在一个关于相关事实的知识掌握在分散的许多人手中的体系中，价格能协调不同个人的单独行为，就象主观价值观念帮助个人协调其计划的各部分那样。下面，我们有必要来看一个简单而常见的例子，以弄清楚价格体系的作用。

假设在世界某地有了一种利用某种原料——例如锡——的新途径，或者有一处锡的供应源已枯竭，至于其中哪一种原因造成锡的紧缺，于我们关系不大——这一点非常重要。锡的用户需要知道的只是，他们以前一直使用的锡中的一部分，现在在另外一个地方利用起来更能盈利，因此他们必须节约用锡。

对于其中大部分用户来说，甚至不必知道这个更需要锡的地方或用途。只要其中有些人直接了解到这种新需求，并把资源转用到这种新需要上，只要了解到由此产生的新缺口的人转而寻求其他来源来填朴这个缺口，则其影响就会迅速扩及整个经济体系；而且，这不仅仅影响到所有锡的使用，它还影响到锡的替代品的使用，以及替代品的替代品的使用，还要影响所有锡制品的供应，其替代品，替代品的替代品的供应等等，而那些有助于提供替代品的绝大部分人，一点也不知道这些变化的最初原因。所有这些构成了一个市场，并非因为任一市场成员都须对市场整体全部了解，而是因为他们每个有限的视野合在一起足以覆盖整个市场。

所以，通过许多中介，有关的信息就能传递到全体成员。一个掌握所有信息的单一管理者本来可以通过下面这个事实得出解决办法，即任何商品都只有一个价格，或更确切地说，各地的价格是相互关联的，其差别取决于运输费用等等。但是事实上，没有一个人能掌握全部信息，因为它们全分散在所有有关的人手里。

。。。

令人惊奇的是，在上述一种原料短缺的情况下，没有命令发出，也没有多少人知道其原由，就使许许多多的人——他们的身份花几个月时间也无法调查清楚——更节约地利用这种原料或其产品。

。。。

价格体系正是一种人类偶然发现的，未经理解而学会利用的体系（虽然人类远非已经学会充分地利用它）。通过价格体系的作用，不但劳动分工成为可能，而且也有可能在平均分配知识的基础之上协调地利用资源。喜欢嘲弄这类主张的人，通常歪曲其论点，暗示这种论点断言，这个最适于现代文明的体系是通过某个奇迹自发形成的。

。。。

这说明，这样一种方法有根本性的错误，这种方法习惯性地忽视我们所必须应付的一个重要现象类的知识不可能是完全的，因此需要一种不断交流和获得知识的途径。

引文翻译来自: http://www.aisixiang.com/data/24310.html

3 网络安全的社交扩展性(The Social Scalability of Network Security)

很久以前，我们使用粘土交易，最近使用纸张，今天我们使用（在计算机和数据网络上运行的）程序和协议实现大部分商业交易。虽然这极大地改善了交易匹配和信息流动，但其代价是增加了对有害行为的脆弱性。

随着网络的发展，更多对彼此行为习惯和限制并不了解的人加入进来。像贝尔实验室那样狭小而亲密的办公室，同事之间彼此熟知，收入和支出通过纸质过程（而不是在办公室计算机上执行）得到很好的控制。这是基于根信任访问控制的安全性。随着组织越来越大，组织的边界开始交叉，以及更多有价值和集中的资源（如金钱）通过计算机置入或被激活，这种高效和有效的安全机制开始崩溃。接收陌生人电子邮件越多，越有可能收到网络钓鱼攻击或恶意软件附件。传统的计算机安全并不具有社交扩展性。正如我在文章“可信计算的曙光”中描述的：

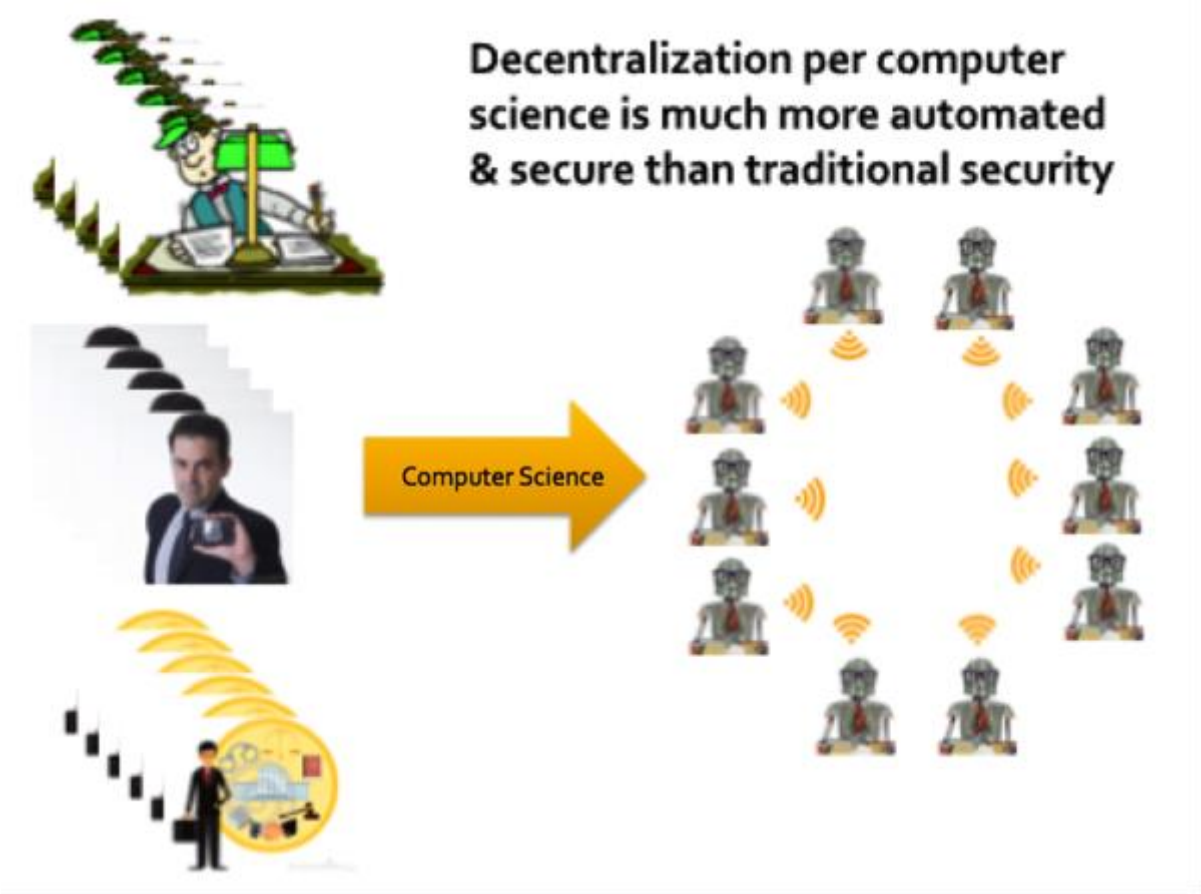
当我们使用智能手机或笔记本电脑接入小区网络或互联网时，这些交互的另一端通常运行在其他独立计算机上，例如网络服务器。实际上，所有这些服务器的体系结构都被设计为由单个人或相互了解和信任的层级人员控制。从远程 Web 或 APP 用户的角度来看，这些体系结构基于对未知“根”管理员的完全信任。这些管理员可以控制服务器上发生的一切：随意读取，更改，删除或阻止服务器上的任何数据。即使通过网络发送的数据是加密的，最终也会被解密，计算机以这种方式被完全控制。对于当前的 Web 服务，我们完全信任，换句话说，我们非常脆弱，或者更具体地说，那些有权访问服务器的人，无论是内部人员还是黑客，都可以执行我们的订单，并确保付款。另一方面，如果某个人想要忽略或伪造你对 Web 服务器的指令，那么没有强大的安全措施能够阻止它们，只有那些不可靠的且昂贵的人类组织可以阻止它们，而这些组织往往以国家为界。

许多服务器对于内部人员或外部人员来说，并不容易受到攻击。但随着越来越多有价值的资源集中到服务器上，这激发了攻击。集中的根信任安全性规模很小。随着由计算机控制的资源变得更有价值和更集中，传统的根信任安全变得更像是我们在现实世界中习惯的“拨打 100(call the cop)”。 幸运的是，通过区块链，我们可以为这些最重要的计算做得更好。

4 区块链和加密货币(Blockchains and Cryptocurrencies)

可扩展的市场和价格需要可扩展的货币，可扩展的货币需要可扩展的安全性，这样才能让大量各种各样的人使用该货币，且不会因为伪造、通货膨胀和盗窃而丧失货币的完整性。

2009 年，以“中本聪(Satoshi Nakamoto)”为通信名字的个人/小组将比特币带入互联网。中本聪在货币方面的突破是通过降低信任（信任成本最小化）来提供社交扩展性：降低交易双方和第三方的脆弱性。以“高成本计算、自动化安全”来代替“低成本计算、高成本组织的传统安全”，中本聪在社交扩展性方面获得了不错的提高。一组部分信任的中介组织取代了一个完全可信的中介组织。



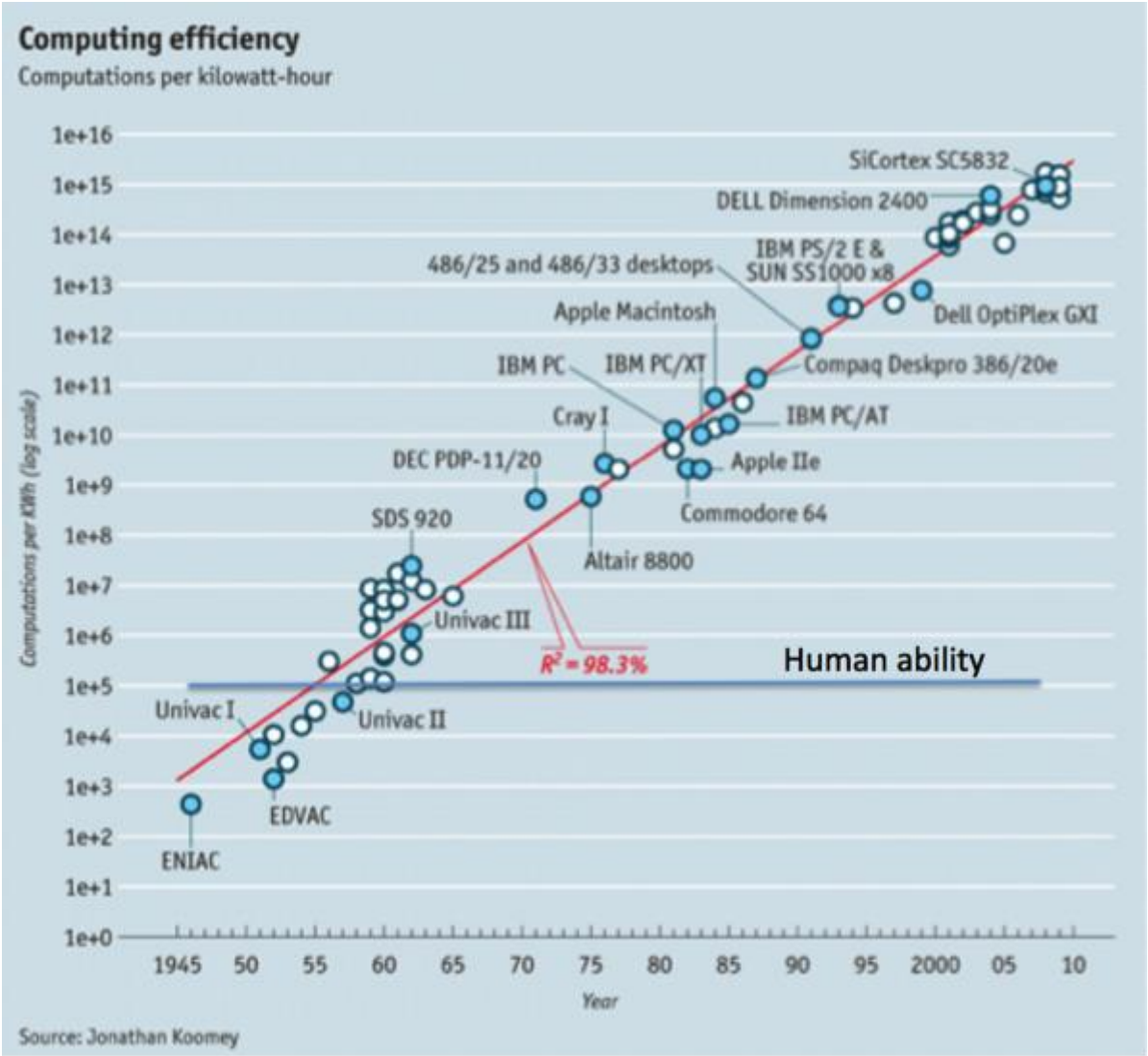
计算“类固醇”的财务控制：作为机器人大军的区块链，彼此互相检查对方的工作。

当我们通过计算机科学，而不是传统会计师，监管者，调查人员，警察和律师来保障金融网络的最重要功能时，我们从一个手动的、本地的、安全不一致的系统转向一个自动化、全球化、更安全的系统。加密货币在公共区块链上正确实现后，可以替代传统官僚银行的计算机大军。“这些区块链计算机将使我们能够把在线协议中最关键的部分放置在更加可靠和安全的基础上，并使以前不敢在全球网络上进行的信托交互成为可能。”（来源）

例如，区块链技术尤其是比特币具有以下最显著的特点：

- 独立于现有制度的基本操作
- 跨境无缝操作能力

来自于高度安全性和可靠性，区块链可以在没有人为干预的情况下自动运行。如果没有高度的安全性，这只是分布式数据库技术平白无故的浪费。分布式数据库技术，为了保持完整性，仍然维系于它必须依赖的本地官僚组织。



自 20 世纪中期以来，计算的效率提高了许多个数量级，但人类仍然在使用和过去相同的大脑。这为解决人类自身和组织的局限提供了很大的可能性。组织完全基于人类思维，计算能力及安全性做它们擅长的事情，人类思维也做他们仍然最擅长的事情。结果，人类没有更多的精力来扩大我们一直以来的组织。但是用计算机取代一些人的功能，可以提高社会可扩展性，这是极具潜力的。（需要重点注释的是——这个论断取决于人类能力线的斜率而不是绝对位置，上面显示的绝对位置是任意的，取决于我们测量的人类“计算能力”）。

一个新的中心化金融实体，一个没有“人类区块链”（传统金融所采用）的可信赖的第三方实体，极有可能成为下一个 Mt. Gox（兑换比特币的专门网站），没有这种官僚政治，它不会成为值得信赖的金融中介。

计算机和网络很便宜， 扩展计算资源需要很便宜的额外资源。扩大人类传统组织（以可靠和安全的方式）则需要越来越多的会计师、律师、监管者和警察，以及这些制度所带来的官僚政治、风险和压力的增加。律师代价高昂，管制堪比登月。计算机科学比会计师、警察和律师更能保障货币的安全。

在计算机科学中，存在安全性与性能的基本权衡。比特币的自动化完整性在性能和资源使用方面的成本很高。没有人找到有效的方法来大幅度提高比特币区块链的计算扩展性——例如交易吞吐量——并且证明这种改进不会影响比特币的安全性。

对于比特币区块链来说，既大幅度提高性能又保持完整性的改进可能是没有的，这可能是不可避免的折衷(tradeoff)之一。与现有的金融 IT 相比，中本聪在安全和性能方面做出了根本性的折衷(tradeoff)。看似浪费的挖矿过程是这些折衷中最明显的一个，但比特币也有其他方面的折衷(tradeoff)，其中之一是高度冗余的消息传递。数学上可以证明的完整性需要在所有节点之间进行全面广播。比特币无法做到这一点，但要想达到接近完美的程度，就需要非常高的冗余度。因此，一个 1 MB 区块的资源消耗要比 1 MB web 页面多得多，因为区块必须传输、处理和存储，并为比特币提供高冗余，以实现其自动化的完整性。

这些必要的折衷，为了实现必需的安全（独立性、无缝全球化和自动完整性）而牺牲性能，意味着比特币区块链本身不可能接近 Visa 的每秒交易次数，并保持自动完整性（从而创造与传统金融体系相比的独特性优势）。相反，需要一个“信任成本最小化”较弱的外围支付网络（可能是闪电网络）来承担大量低价值的比特币交易，然后使用比特币区块链定期与外围交易网络进行高价值交易的批量结算。

比特币的交易速度比 Visa 或 PayPal 更低，但由于其更强大的自动化安全性，比特币交易可能是更为重要的交易。任何体面的拥有互联网连接和智能手机的人都可以支付 0.20 美元至 2 美元的交易费用——远低于当前的汇款费用——即可在全球任何地方访问比特币。那些价值较低的交易（同时手续费也较低）可以在外围比特币网络上实施。

当讨论小 b(bitcoin)比特币（即货币功能）时，在零售业用比特币支付不会有什么不可能（就像用法币一样）。例如，比特币信用卡和债务卡——所有退款和每秒交易功能。而且还有一些巧妙的方法可以做外围比特币零售支付，其中小额支付发生在链外，然后在 Capital-B 比特币区块链上定期批量结算。随着比特币使用量的增长，区块链将逐渐演变为高价值的结算层，我们将看到外围网络被用于小型比特币零售交易。

当我设计 bit gold 时，我已经知道共识机制不能安全地扩展交易吞吐量，所以我设计了两层架构：（1）bit gold 本身，结算层，（2）Chaumian 数字现金，外围支付网络为零售支付提供更高的每秒交易量和私密性（通过 Chaumian 盲化），但希望 Visa 成为值得信赖的第三方，并因此需要会计师等的“人类区块链”以确保完整性。外围支付网络只能涉及小额交易，因此需要更很少的人力军队来避免 Mt. GOX 的命运。

Ralph Merkle：公钥密码学的先驱和层级哈希树结构（Merkle 树）的发明者。

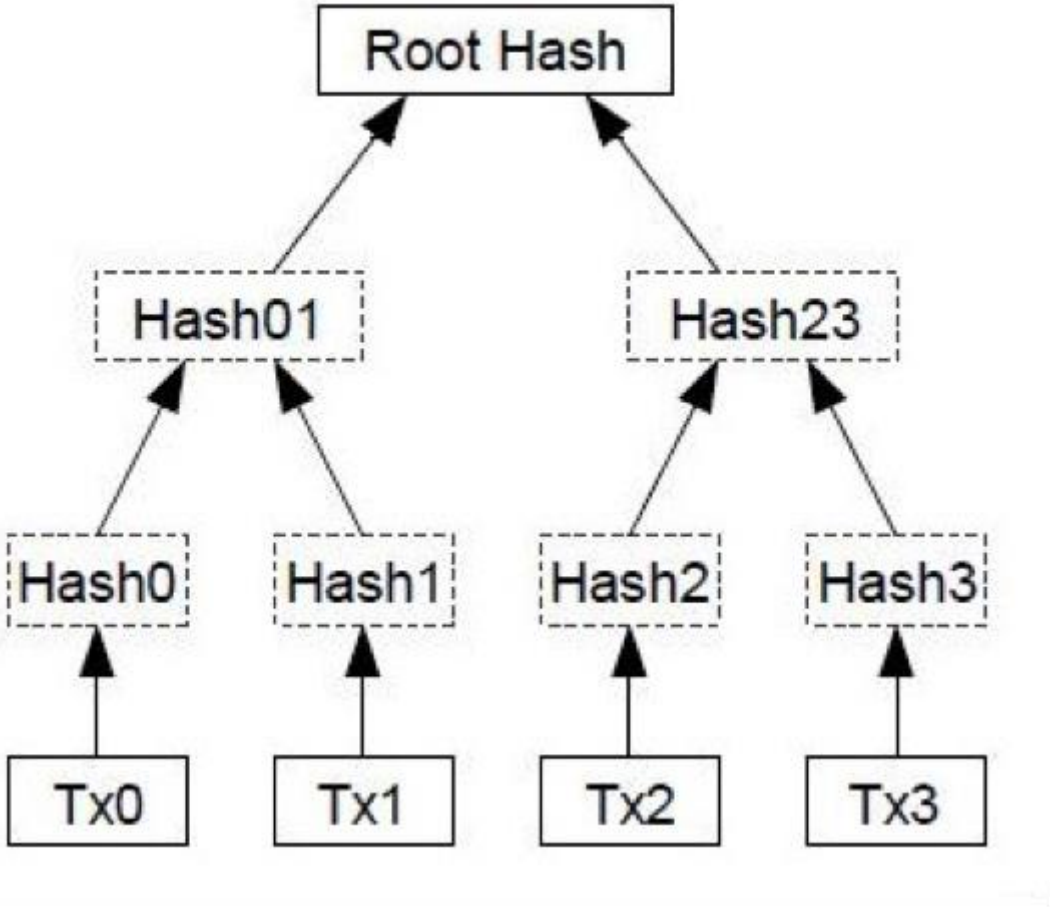
货币的设计本身需要社交扩展性，只不过通过安全性表现。例如，任何参与者或中介组织都应该很难伪造货币（稀释供给曲线，导致过度或意外的通胀）。 黄金在世界任何地方都具有价值，并且不受恶性通货膨胀的影响，因为黄金的价值不取决于中心机构(central authority)。比特币在这两方面都表现突出，并且可以在线运行。比特币可以使阿尔巴尼亚人使用比特币以最低的信任成本向津巴布韦人支付，比特币可以不向中间人支付准垄断利润，并且可以把针对第三方的脆弱性降到最小。

“区块链”有各种各样的定义，几乎所有的定义都在营销炒作的山峰间隐隐约约地挥舞着。我这里建议一个清晰的定义，可以和外行的人沟通。如果有区块，又有链，那就是一个区块链。“链”应该是Merkle 树或其他具有类似“完全不可伪造完整性”的完整性功能的密码结构 。此外，交易和任何其他数据（完整性受区块链保护）应该以客观上尽可能高的容忍最坏情况（恶意问题和行为）的方式进行复制（通常来说，系统的行为和以前的系统相比完全不同：以前规定只有 1/3 到 1/2 的恶意服务器试图破坏系统）。

比特币的社交扩展性和安全性，基于计算机科学而非警察和律师，允许非洲的客户向中国的供应商无缝跨境支付。私有区块链难以实现这一壮举，因为它需要在这些不同司法管辖地区之间共享的身份识别方案，认证授权和 PKI。（来源）

由于部分恶意节点，以及由于（希望非常罕见）需要软件更新，使得以前的区块无效——一个更危险的情况是硬分叉——区块链也需要一个对抗分叉攻击的人类治理层。最成功的区块链——比特币——通过技术专家的分散决策，以及强大的不变性约束，保持了其不可变的完整性。在此基础上，只有最重要和最罕见的错误修复和设计改进（不能用其他方法来实现），才算是一个正当的硬分叉。在这种治理审计或法律决策（例如改变帐户余额或撤销交易）的原则下，如果不能证明硬分叉是正当的，则应该由系统之外（或者系统之上）的传统治理来完成。例如，通过法院强制要求比特币用户发起一项新交易，该交易有效地取消旧交易，或没收特定密钥，从而修改特定用户的特定持有量。

我们说数据是不可伪造或不可改变的，意味着数据在提交到区块链之后，不能被无法察觉地改变。与一些炒作相反，在数据提交到区块链之前，并不能保证数据的任何来源信息，包括数据真假。这需要额外的协议，通常包括昂贵的传统控制。区块链不保证真实性，只是在最新修改中保留了真相或谎言，允许事后进行安全地分析，从而对揭露谎言更有信心。传统的计算机是计算性的蚀刻素描，而区块链是计算性的琥珀。重要的数据应该尽可能早地提交到区块链，最好是由生成数据的设备通过密码签名，最大限度地保证数据的完整性（这也是区块链的利益）。



四个交易的 Merkle 树（tx0 到 tx3）。结合适当的复制和受工作量证明保护的交易区块链，Merkle 树可以通过共识使交易数据不可伪造。在比特币中，Merkle 根哈希安全地汇总并用于验证区块中所有交易的未改变状态。

我自己 1998 年的“安全财产权”架构有 Merkle 树和复制数据，可以容忍客观部分的任意软件错误的或恶意行为，但不是区块。这个架构展示了我的理论，即可以保护全球共享的数据和事务的完整性，并使用这种能力设计一种加密货币（bit gold）。它并没有像比特币那样具有更高效、可计算的区块和账本系统。和今天的私有区块链一样，安全财产权假设并要求系统具有安全可区分和可数的节点

假设目标是 51%的 hashrate 攻击，这就设定了公共区块链（如比特币和以太坊）的一些重要的安全目标。为了回答这个问题：有人能说服并协调 51%的人吗？我们实际上关心的是最强算力矿工的身份识别问题。

区块链安全受到客观限制，区块链治理受到了潜在的 51%攻击的影响。当然，攻击并不一定要被攻击者称为“攻击”；相反，他们可能会称其为“开明治理”或“民主行动”。 实际上，修复 bug 或改进协议的一些软件更新需要一个软分叉。一些其他类型的软件更新则需要硬分叉，在比特币中，这比软分叉带来的安全和持续性风险更大。尽管区块链比其他任何网络协议都降低了信任成本，但仍远非可靠。矿工是部分受信任的受托人，而那些不是专家开发人员或计算机科学家的人，他们花了大量

时间学习区块链的设计原则和代码库。他们必须对专家开发人员社区抱有很大的信心，就像那些想要了解相关科学家的专业科学成果的非专业人士一样。

因此，公共区块链并没有完全避开“标识身份困难”的子弹，并在更高的“wet”/“social”层面关注最强算力矿工识别的其他问题。相比试图将这种固有的“wet”（基于大脑的）概念安全地映射到协议上，这可能是更合适的，因为 PKI（公共密钥基础设施）做这些是相当笨拙地。

所以我认为一些“私有区块链”有资格成为真正的区块链； 其他区块链应该在“分布式分类帐”或“共享数据库”或类似的更广泛的标题下使用。“私有区块链”与像比特币和以太坊这样的公共区块链和许可区块链完全不同，而且也不像它们那样具有社交扩展性。

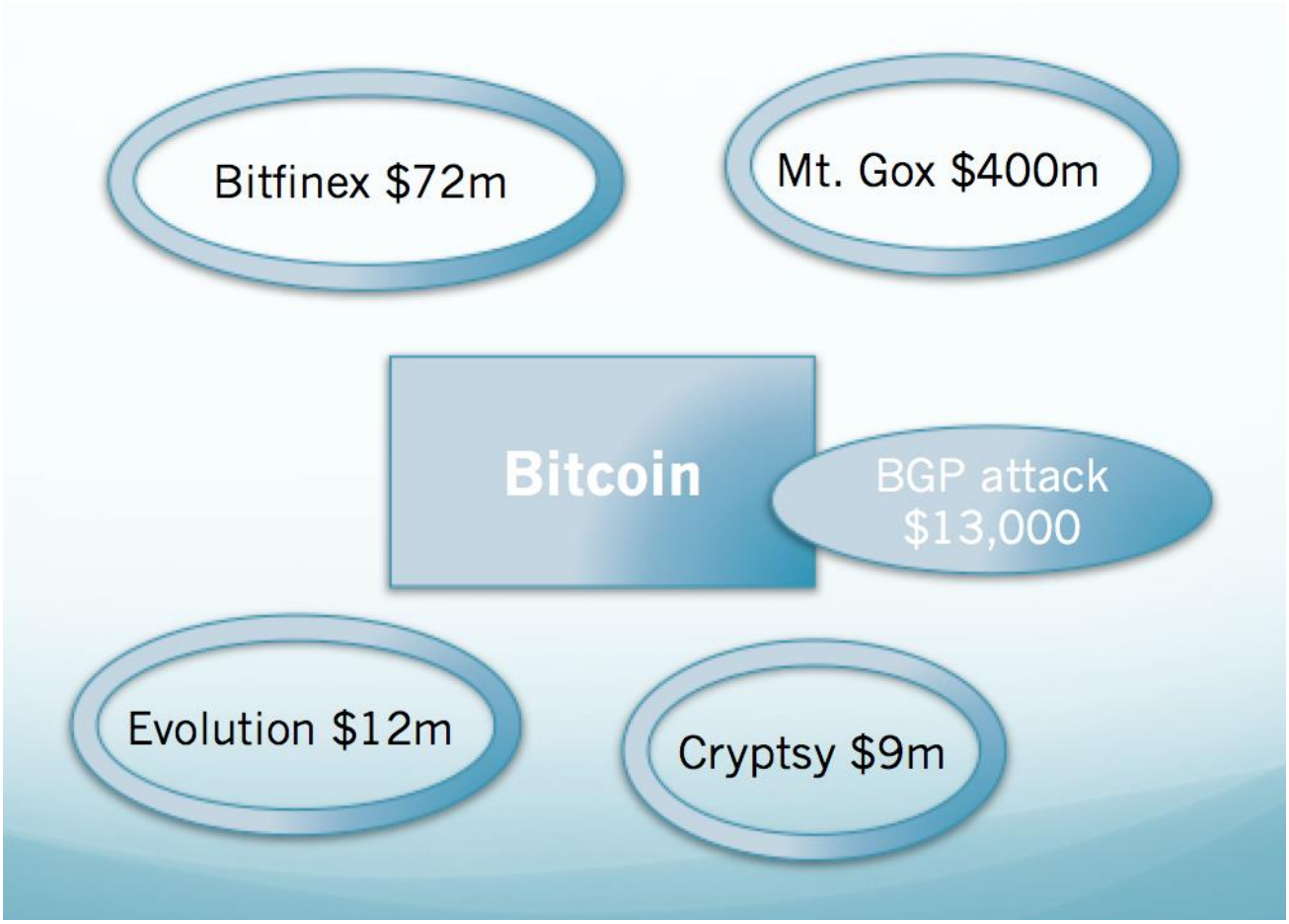
下面这些都非常类似于要求一个安全的（可区分的和可数的）服务器群，而不是公共区块链中任意的匿名矿工成员。换句话说，他们需要一些其他的，通常不具有社交扩展性的，Sybil（sockpuppet）攻击的解决方案：

- 私有区块链
- 侧链的“联盟链”模式（唉，尽管之前的希望或主张，但没有人知道如何用任何程度较低的必要信任来处理侧链）。侧链也可以是私有链，并且它非常合适，因为它们的体系结构和外部依赖性（例如在 PKI 上）是相似的。
- Multisig-based 方案，即使基于区块链的智能合约完成
- 基于阈值的“oracle”架构，将链外数据移入区块链

在识别一组服务器时，使用基于可信证书权威机构（CAs）的 PKI 是一种主要的、但通常不具有社交扩展性的方法。为了避免仅仅受信的第三方是安全漏洞的问题，可靠的 CA 本身必须是昂贵的、劳动密集型的官僚机构，他们经常做大量的背景调查，或者依赖其他人来做这些事情(e.g. Dun and Bradstreet for businesses)。（我曾经领导过一个设计和建造这样一个 CA 的团队）。CA 也充当守门人，保护这些许可的系统。CAs 可以成为政治控制和失败的单点。“公共区块链是自动化的、安全的、全球性的，但身份是劳动密集型、不安全的、本地的。”

基于 PKI 的私有区块链对银行和其他大型企业来说是件好事，因为它们已经拥有成熟的内部 PKI，涵盖所需批准重要交易的员工，合作伙伴和私人服务器。银行 PKI 相对可靠。我们也为 Web 服务器提供了半可靠的 CA，但对于 web 客户端来说通常不是这样的，尽管自从 web 的发明以来，人们一直在处理客户端证书的问题：例如，广告商希望能有一个更安全的替代电话号码和 cookie 来追踪用户身份。但它还没有发生。

PKI 对于一些重要的事情和人来说可以很好的工作，但是对于较小的实体来说，它并不是那么好或者容易。它的社会可扩展性受到传统的 wet 身份官僚机构的限制。



泛比特币生态中的一些重大盗用行为。鉴于比特币区块链本身可能是现存最安全的金融网络（并且实际上必须比传统支付网络更安全，以维持其低廉的治理成本和无缝的跨境能力），而其基于旧式集中式网络服务器的外围服务非常不安全。（来源：作者）

我们需要更多的社交扩展性的方法来安全地统计节点数量，或者用另一种方式来尽可能地统计节点数量，评估为确保区块链的完整性而做出的贡献。这就是工作量证明和复制广播的目的：为了提高社交扩展性，极大地牺牲了计算扩展性。这就是中本聪的绝妙折衷(tradeoff)。这非常绝妙，因为人类比电脑贵得多，而且这种差距每年都在扩大。这非常绝妙，因为它可以让人们跨越人类信任边界（例如国界）无缝安全地工作，相比之下，像 PayPal 和 Visa 这样的“拨打 110(call-the-cop)” 架构总是依赖于昂贵的、易出错的、有时是腐败的官僚机构，并以一定的完整性运行。

5 结论(Conclusion)

随着互联网的兴起，各种各样的网络组织的开始出现（包括社交网络，“长尾”零售商（例如亚马逊）），以及各种各样的服务开始发展（eBay，优步，AirBnB 等），让小而分散的买卖双方找到并彼此做生意。这些仅仅是利用我们新能力的最初尝试。由于近几十年来信息技术的巨大进步，能够成功地参与到网络组织的人数和种类，相比思想和制度的限制，受到计算机和网络的客观限制要少得

多，因为思想和制度的限制通常还没有经过充分的重新设计或进一步发展，以利用这些技术进步的优势。

这些互联网最初的努力已经非常集中。区块链技术是通过计算机科学实现数据完整性的，而不是通过“拨打 110(call the cops)”来实现数据完整性。到目前为止，区块链已经使一些潜在的可信赖的货币——加密货币——成为可能，并将让我们在金融领域以及其他领域取得进展。

这并不是说，我们的组织适应我们的新能力将会很容易，在某些特殊情况下，也不是没有困难或轻易而举。乌托邦计划在区块链社区非常流行，但它们不是可行的选择。对我们高度发展的传统组织进行逆向工程，甚至以新的形式恢复一些旧的组织，通常比从头开始设计更好，而不是宏大的计划和博弈理论。中本聪证明了这样做的一个重要策略——牺牲计算效率和扩展性 ——消耗更多更便宜的计算资源——以减少和更好地利用巨大人力资源开支（维护涉及现代组织下陌生人之间关系所需），例如市场，大公司和政府。