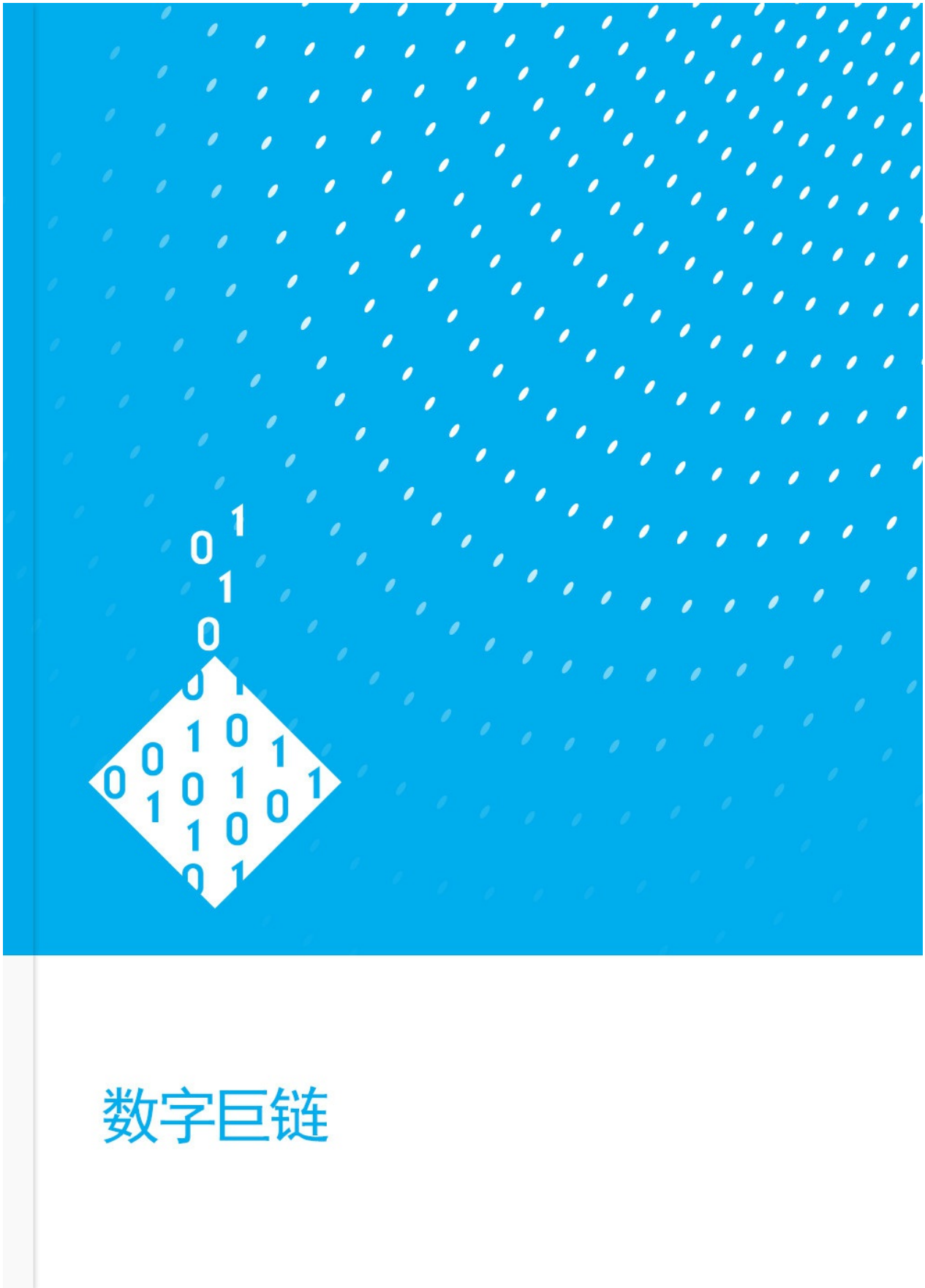
数字巨链

Table of Contents

数字巨链



作者序

在社区许多成员的帮助下，我为那些听说了比特币或加密货币，但了解不是很多而且想要进一步理解算法是如何以一种共识驱动的自发的方式行使管理职能和转移价值的初学者，企业家，冒险家写了这本薄书。

建立在一本如比特币或Ripple（它是不可篡改的）等加密总账上的无信任资产管理工具不仅可以在发达国家减少费用和冗余，而且也可以给那些发展中国家因缺乏政治资本（关系[1]）而更可能被边缘化的人以帮助。加密总账也可以帮助政府和非政府机构管理内部资产和减少金融服务的障碍，通过制定公平的竞争环境，允许来自各行各业的人以一种更安全的方式管理他们拥有的稀缺商品和价值品。

从安全地实现对部分金融业服务（如后台业务）的自动化到降低国际贸易的交易成本，加密总账这种新型的数学工具能够运用在许多新兴的细分市场，其中一些特别明显。例如，在2014年1月的采访中，唐纳德·麦金太尔问我为什么对加密货币和智能合约感兴趣， 我解释说，已经有额外的使用案例显示， 使用加密总账来追踪财产契据和合同不仅在发达国家中有效， 同样在如中国等发展中国家也是有用途的。

虽然就重要性存在一些把这些工具与一些历史上类似的事物相对照的类比--从铁路基础设施到操作系统平台--其中的核心分布式程序如比特币和它的下一代协议有潜力影响几乎任何与互联网有联系的产业。下面的一些来自专家，企业家，投资者和开发者的思考说明了加密协议的其他一些用途，而且给读者提供了一个开发和探索的基础。

但同时在各方面也可能有一些挑战和障碍，包括： 从早期接受者到普通大众的教育推广， 详尽地研究，还有必须遵守某一特定工具的所有法律和司法问题。

减少汇款方面的费用或提供更安全健壮的移动支付手段是有经济回报的事，例如，根据加特纳的说法， “从去年（2013）的2350亿美元算起，移动支付在2017年将最高达到一年7200亿美元。”寻找一种方法来建立一个在这个利基市场中提供价值的应用， 这刚好是一个去中心化的或分布式的加密总账在没有交易对手风险的情况下可以试图去实现的破坏性潜力的一部分。

最后要说的是， 这本书并不是一本加密货币经济基础或功能的注释书。在参考了经济学家的意见后， 这本书想要展示的加密货币改变交互方式和价值被转移和管理的方式的潜力， 即以一种过去十年技术上或数学上无法完成的方式。

这是一个激动人心的旅程，而且我相信加密货币将会比目前的大肆宣传还有支持者和反对者思想之争走得更远，更久。随着时间的流逝，其中一些展望和主张最终会成为雾件（指未成功实现开发目标的软件）， 然而其中不多几个有潜力影响整个商业， 就像20年前互联网和35年前的个人电脑一样。让我分享给你由我自己学习到的知识。

Tim Swanson

蒂姆·斯旺森

San Francisco, March 2013

旧金山 2014年3月（应为2014年）

---

[1] ‘关系’指亲戚关系和其他人际关系。在任何国家了解促成一件事的正确的人是有帮助的， 但是中国的‘关系’在文化和经济层面的影响是扭曲的。就算你的项目有足够的资金并且采取适当的形式，如果你和相应的政府官员或老板没有’关系’， 那么你的项目可能不会成功。

第一章：指南

本指南是为那些想要理解下列问题的人士准备的一本简短的入门读物：

1. 什么是加密总账
2. 什么是智能合约
3. 智能财产是如何起作用的
4. 无信任资产管理的破坏性影响

我通常都使用来自美国和中国的例子，若不考虑规模，这两个国家都有许多相关的商业服务和个人应用。

这并不是一本投资指南， 而且作为读者的你， 应该确保对你想要创造价值的这一特定领域进行全面细致的了解。虽然这一迅速发展的领域看似有无限的机遇，但是同样也有许多已知或未知的风险。你也应该着手研究调查，确保自己了解尼克·绍博（他开创了智能合约和智能财产这一领域）的开创性工作成果，这些都是可以在线免费找到的。

我也非常推荐， 除了向一些对加密货币应用相关商业发展熟悉的人士咨询以外，你也应该和法律顾问或一个能够帮助量化潜在法律风险的风险评估专家进行商讨。

本指南将在一般的意义上说明，即使你创建了一个表明上看似严格的能在一本加密总账上追踪和转移一份资产的智能合约， 也可能有一些传统的实体法律机构并不会承认交易进行的方式（例如，交易必须继续采用纸质的形式）。对一些加密货币社区的人士来说， 传统的机制似乎过时了。然而令人不快的事实是传统的机制（邮政邮件，传真机）仍然是商业服务所需要的， 而且也没有迹象显示近期会消失。

保持开放心态

比特币经济可能而且将会继续增长到非常大的规模，至于作为价值的虚拟体现和抽象手段的加密货币或凭证是否真正是有价值的，这取决于观察者（更准确地说，权限持有者）采取怎样的个人观点。这也是一个能够得到自我解决的困境：如果你不认为持有任何类型的加密币，元币，或“彩色币”是有意义的，那么你就不会接受它们。

就像争论所显示的，比特币和加密货币其中一个最主要的益处在于，它能减少国际贸易的成本和摩擦。下面是一张经皮埃尔·理查德授权使用的图片，它能帮助读者了解贵金属（金，银），法定货币（美元，欧元）和加密货币之间交易成本的很多差异。

交易成本	贵金属	法币	比特币	
存储	每年0.15%-1%	由FRB资助	免费且100%储备金保证	
运输	昂贵	不便利	免费且容易	
担保	自然耗损	机构保证	密码学保证	
信用媒介	不可避免	固有	不需要	
记录	手工	手工	自动	
伪造	不可能	不可避免	不可能	
发行	开采	政治	算法	
支付结算	昂贵的	中央集权的	便宜的并且分布式的	
稀缺性	高	随意的	总量2100万	
鉴定	昂贵的化验	信任方	内置机制	*

Transaction Cost	Precious Metals	Fiat Currencies	Bitcoin
Storage	0.15% to 1% per year	Subsidized by FRB*	*Free and 100% reserve*
Transportation	Expensive	Inconvenient	*Free & Easy*
Security	Physical	Institutional	*Cryptographic*
Fiduciary media	Inevitable	Inherent	*Impossible*
Recordkeeping	Manual	Manual	*Automatic*
Counterfeiting	Impossible	Inevitable	*Impossible*
Issuance	Mining	Politics	*Algorithm*
Payment clearing	Expensive	Centralized	*Cheap & Distributed*
Scarcity	High	Arbitrary	*Fixed - 21 million btc*
Authentication	Expensive assay	Trust counterparty	*Built-in*

** fractional reserve banking*

部分准备金银行制度

已经有一些经济学家和法律专家表示比特币并不是真正有价值的事物，其中有人指出在某些司法管辖区，目前加密货币还不在所有权规定范围内。他们有可能是对的，所以我作了如下注释： 加密货币仅仅是一本虚拟的账单. 然而，若不考虑这种层面的抽象，相对于法定货币来说，有人就加密货币的稀缺性发现了价值。你的邻居或你最喜欢的博客作者是否和你一样看待加密货币，长期来看这根本不重要。最根本的问题在于，凭证和协议究竟能为你或其他人提供什么样的额外的实用价值. 此外，如果价值的物质表现形式真的如此重要， 那么所有人类日常生活中的抽象活动——从签署能作为合同和金融工具的文件， 到刷一张能够电子支付的信用卡——将会是一场徒劳的脑力活动。

竞争币

如果你刚接触加密货币，包括竞争币，那么你可能是通过各种不同途径了解到的。 一种竞争币代表一种可替代的加密货币——通常它表示除比特币之外的任何一种加密货币或加密总账。 有时，一种竞争币仅仅是比特币代码的拷贝：也有一些其他种类是经过大量修改的。

域名币普遍被认为是最早出现的一种竞争币。域名币被设计来作为一个分布式的域名系统， 它能保证域名审查就算是可能做到的，也将是非常困难的。作为比特币的修改版， 它创建于2010年，而且在2011年，通过一个软件更新域名币的挖矿（第19200区块后）已经很好地和比特币相混合。（矿池必须使用一个新版本的软件）

（译者注： 混合挖矿，即当矿工挖比特币的过程中， 可以同时挖域名币）。

域名币不仅可以提供域名服务的功能， 它也可以作为一个通信系统，BT服务器， 甚至是一个公证方（其他加密货币也能实现这一功能）。任何一种竞争币或所有的竞争币还有下面章节描述的正在发展的“2.0”（下一代）项目能否成功实现它们各自的目标还是不确定的， 但像域名币所显示的，这些潜在的新创新展示了加密总账这一技术能够

这并不意味着加密货币社区都拥抱这种分裂性的变化：事实远非如此。就像所有包容性强的团体， 加密货币社区也有各种精英人士，保守派和持开放态度的人。人们是通过不同途径接触加密货币的。许多后期接受者已经了解了挖矿或者如何通过其他竞争币编码，如莱特币和狗狗币——对于新成员来说，它们是进入更大的加密生态系统的入口。由于存在能够通过法币购买或挖矿得到大量的凭证作为回报（如，十亿狗狗币相当于10美元）的心理预期——而且没有在进行比特币小数换算时被称为心理交易成本的不便，这些竞争币至少已经部分地起了这样的作用。 然而，许多比特币早期接受者经常在不同的场合对这些竞争币项目表示不认可。 因此，如果读者你选择加入加密货币社区，你应该了解到这里有各种地盘之争，而且我建议你远离这些争端，因为它们是对无信任资产管理承诺带来增值潜力和商业机会这一初衷的背离。

（注：fiat应该指fiat currency, fiat money）

本书主要关注的是加密货币生态系统相关的机遇，而不是一个特别的协议：因为很难知道， 3或5年后的市场环境如何，将面临怎样的监管问题，什么开发工具会被做出来，或者不会做出来，还有市场参与者会发现什么新的用途，等等。例如，艾丽丝可能因某些原因发现某个项目或加密货币的新用途， 而这一用途对鲍勃来说是无意义的。因此，区分自己的主观评价和别人的评价是非常重要的。 尽管类比是不准确的，但请把下面这篇关于英语的讽刺短文看作是关于比特币替代协议的先验知识

‘浪费了那么多努力在其他语言上，这对于英语来说太糟了。英语是完美的，但是有太多的精力花费在其他语言系统上，而不是一个简单而强大的字母链系统——一个字母表要是我们有一个‘法国科学院’来以一种合理的方式管理，删减，发展我们的语言多好。看看所有那些只有少部分世界人口使用的愚蠢的语言，这些人简直是浪费才智在所有这些可笑的并不促进语言生态系统发展的副产品上，因为它们完全是多余的。他们纯粹是在句法规则，语法，和风格上重新发明轮子。英语，不是唯一被使用的语言，这太糟了。而且由于英语没有100%地占有的市场，那么整个语言生态系统可能失败， 严重地失败。

为了加密协议的成功，有人主张只需要一个加密总账就可以了， 这是值得怀疑的。这就相当于说，为了因特网的成功，只需要一个网站,（如，Reddit）而且我们只需要维持这仅有的一个网站。人们喜欢其他选择，因此他们开发了替代产品. 而且毕竟还有其他可想象的空间.

据称卡尔·萨根说过 ”保持开放心态是值得的, 但是不要开放得不对一切加以怀疑”.因此, 寻找新机遇的同时也要警惕蠢人和欺骗——这些问题在所有经济领域都存在,包括加密货币这个崭新的领域. 请勤加学习, 自担风险。

第二章：智能合同

“把东西刻在石头上”是一个描述“承诺”或“义务”的常见用语，同时历史上存在众多关于审判、侵权和商业事物的神圣文本，一个可以说明持久与清晰定义的义务的例子，来自美索不达米亚——汉谟拉比的巴比伦文字，可以追溯到大约公元前1772年，其中包含282条法令。著名的“以眼还眼”（即同态复仇法）就记录在保存下来的泥板上，约有一半的文字涉及工资支付、租金和损害财产的赔偿合同，另一半则与贷款和债务有关。虽然这些义务的诠释与执行，还需要推断和历史复原，但人类努力把责任与义务编成法典，是一个永无止境的故事。

最近一个例子是，与一般看法相反，塞缪尔·戈尔德[1]温居然说：“口头合同的价值大于书面合同。”然而，无论以哪种方式陈述，戈尔德温这句经常被错误引用的名言点出了一个关键问题，如何以可靠的方式界定术语、指南和服务条款，这个问题也在不断影响物权法和竞争性资源。

2006年，加密合同思想的提出者尼克·萨博，比较了人类目前的模拟系统与数字系统的区别，即人脑解释并执行的“湿代码”，与计算机解释并执行的“干代码”的区别。与人类相反，机器语言可以看作二进制逻辑，比如合同、规则及规章，可能是由一些表面上客观的人士拟定，它们同样可能被另一类人来诠释与执行，所以结果就是，合同并不是像他们最初约定的那样执行。随着尼克·萨博介绍了计算机程序，如何（已经或将要）朝着掌握“利基”领域的湿代码前进，甚至走得更远，计算机已经触及人类困惑、浮躁、不一致、辱骂等模糊分析领域的边界，这个分歧将发生在不远的将来，也正是本书的主题。

什么是安全的？智能合同与加密账本，并不是解决人类交互关系的灵丹妙药，它们并不能超越算法本身。根据最近的一年两次的仲裁记分卡，2013年美国律师调查了165个条约仲裁和109年合同仲裁，涉及1210亿美元的纠纷。福布赖特和贾沃斯基（Fulbright & Jaworski LLP）[2]公布了年度诉讼趋势和调查报告，他们就诉讼相关事宜，调查了企业高层律师，他们发现，合同纠纷仍然是美国（占比44%）和英国（占比57%）的最大诉讼类型，其次是劳工、雇佣纠纷。除了保罗·切西亚著名的捏造合同[3]，在发达国家中，只有少数合同纠纷是因为实际合同被篡改，大多数是因为协议内容不确定，或者是它的事实与含义有争议。但如下文所述，智能合同的概念范畴更广泛：包括金融工具（合成资产）或价值的编码形式（如令牌）。

自动化电子商务每天都在增长，随着纳斯达克在1971年问世，电子证券交易所每天都在交易股票、债券及其他票据，某种情形下甚至是24小时全天候交易。尽管具有相似功能的纸质证券交易市场，至少可以追溯到1602年的荷兰东印度公司，但电子证券交易所还是应运而生了。有许多原因可以解释，为什么纳斯达克要建立电子证券交易，一个主要推动力是：电子交易通常为用户提供了更快的逻辑和组织效率，很像电子邮件（Email）相对于它的物理对手（邮政系统）所具有的优势，同时，它消除了大量的中介机构、中间人和第三方，尽管它也带来了新的第三方（中央服务器）。仍需要证券的复印件（比如股份登记书），在某些情形下，必须在文件上保存政府与企业实体，在所有现代交易市场中，现实中的这些票据仅以字节形式存在，可理解为各种约定义务、条件和现实世界服务条款的抽象形式。

> [1] 塞缪尔·戈尔德温(英语：Cecil B.DeMille，1881-1959，美国电影导演，好莱坞影业元老级人物，美国影艺学院的36 位 创始人之一。
>
> [2] Fulbright & Jaworski LLP：美国著名的律师事务所。
>
> [3] 保罗·切利亚于2010年6月30日在纽约最高法院提起诉讼，声称他应该拥有Facebook约84%的股权。

所谓智能合同是指，用来实现人类自动化交互的工具，它是一种计算机协议，一种算法，可以自我执行、自我实施、自我验证、自我约束，可用来履行一个合同。而比特币与它的直系后代统称为智能合同1.0，正如下文即将提到的，第二代智能合同--下一次密码学货币都能够自动执行协议，没有一个现实的执法部门，按法律合同的方式来仲裁。由于它们复杂的合同关系，都体现在计算机协议上，在一定条件下，它们可以转移特定的资产。

20年前，尼克·萨博把这些特殊工具统称为“合成资产”。合成资产顾名思义，用他的话说，是由多种方式结合的证券（如债券）和衍生产品（期货和期权）构成，非常复杂的付款流程（比如，什么时候付款，利息是多少）现在可以用标准化的合约来建立，由于这一过程是采用计算机分析来实现，故转账费用非常低廉。现在，律师和程序员都有建立这类工具的能力。

虽然在1971年，有人曾经质疑这一理论的先验基础论点，更不用说它的稀缺性（经济意义上的竞争性资产）与价值（不具现实事物的唯一性）都饱受争议，而且每个人都有他（她）的主观价值，在交易这些电子金融工具人群中，一些人已经看到它的潜在效用，而另一些人只看到它的投机价值。

我们信任加密账簿

去中心化加密账簿是尼克·萨博的“湿·干”系统的另一个演化。纸质账簿和电子账簿，通常由银行或结算系统这样的第三方持有，这些实体创建了一个“值得信任”的环境，同样也引来争议，它们可能被人类因素操纵或滥用（比如修改内容、销毁记录、双重支付），而且管理成本高昂。当你信任第三方，你得向第三方暴露自己的隐私。

2008年11月，中本聪——某个人或某个团队的化名--发布了一份白皮书，第一次详细阐述了，基于软件的、使用分布式加密总账的方法，解决了第三方滥用权力与脆弱性的问题，基于这份白皮书，比特币项目诞生了。

与现有方法相反，中本聪认为，在比特币协议中，分布式加密账簿可充当唯一中间人的角色，协议作为算法是无偏差的，且有审核、认证、验证、批准与传输整数值的能力，可通过分布在世界各地的、成千上万台计算机（采矿设备）来处理账簿，这些计算机运行一个开源程序以提供上述功能，挖矿所得即他们的回报（相当于向用户征收的铸币税）。通过计算得到的整数值，即该网络专用的虚拟令牌，即比特币（有时也称作密码学货币）。比特币总账还有其它潜在用途没有得到充分利用，比如管理智能合同或其它工具，资产或可被计算编码的令牌（Token）。事实上，即将发布的0.9版本，将在每笔交易（称作TX）提供额外80字节的哈希，刚好大到可以容纳一个分布式合约--该功能由于能够代表任何资产类别或财富，而不仅仅是一个数值，所以它存一年，相较于比特币能产生更多利息。

比特币加密账簿，实际是它自己的第三方存储库，因为它推翻了基于纸张的、现实世界中第三方中介机构的作用，以全网共识为基础，创造了一个非信环境。同时它也是一个分布式时间戳数据库，或者说数字公证，由于时间戳服务器[4]颁布的历史时间戳，总是被滥用和篡改，用户现在可以在加密账簿中保管时间戳，而不必担心，存储在成千上万台分布式计算机上的数据受损。更重要是，它提供了其他许多职业（如会计、审计）或机构（如数据仓库）的功能，不需要这些第三方中介就能实现双方间的交易。如爱丽丝的会计公司，可以通过区块链，来审计与协调鲍伯的精品书店一个季度的账目，一笔比特币交易，或全球比特币账簿，被称作区块链，每十分钟完成一次身份验证、交易确认、复制与审核（莱特币甚至更快，每两分半钟验证一次）。

> [4] 时间戳服务器：TSA，一款基于PKI（公钥密码基础设施）技术的时间戳权威系统，对外提供精确可信的时间戳服务。

随着近几十年来，相关数学与密码学理论的发展与成熟，比特币加密账簿（区块链）的技术内涵，已经超越了账簿本身，简而言之：比特币实际并不真实存在，它们仅仅是保管在加密账簿上的比特币交易记录，加密账簿称作区块链。一笔比特币交易（TX）由三部分组成：

> 一个输入：发送比特币的地址；
>
> 发送比特币数量；
>
> 一个输出：预期接收比特币的地址。

这些交易随后被打包进一个区块，每个区块被嵌入一个永远不断增长的链，久而久之就形成一个区块链。为了发送比特币到不同的地址，用户需要访问一个私钥，每个私钥对应一个公钥，这种特殊的加密方法被称作公钥加密，椭圆曲线数字签名算法（ECDSA），已被应用于包括金融行业的大量机构中超过十年。在实际操作中，为了将令牌从一个地址转移到另一个，用户需要输入与公钥对应的私钥。

为了验证这些交易以及账簿的变动，必须建立提供支付功能的基础网络，这个网络由分散的矿工组成。如上所述，矿机通过构建一个区块链树（称作父级）来处理比特币交易（账簿变动），铸币税（即币基产生的新币）就是他们的挖矿回报。区块链树建立在已知的验证过的树上，同时因为矿工不停添加区块而不断延长。在这个建设过程中，矿机执行的是工作量证明过程，更确切地说，是在计算一系列难度递增的墨克尔树[5]的加密哈希，以防止网络被随意添加区块。这就是说，正如电子商务网站使用验证码以防止自动垃圾邮件，为了参与比特币网络，矿机必须不断证明它不仅在运算，而且是工作（哈希计算）在验证基于共识的区块链上。在笔者写这篇文章的同时，比特币全网计算力大约为200万亿次每秒浮点运算数，是全球前500名超级计算机的计算力总和的800倍。

> [5] merkel tree：一种树状数据结构，它所构造的所有节点都是Hash值。

为了防止恶意矿工制造双重支付，这些矿工通过互联网持续保持联系，哪台机器拥有最长的树取决一个预先定义的“共识”。也就是说，所有矿机已经或将获得（通过点对点通信）最长链的副本，非最长链则被丢弃（这样的区块被称作“孤块”）并视作无效。要修改过去的区块，攻击者（流氓矿工）将不得不重做该块及它后面所有块的验证工作，直到它完成的验证工作，超过所有诚实节点的工作量（即所谓51%攻击）。每10分钟（平均）这些机器处理一个区块，账簿完成一次整数变动，处理区块的矿工获得的奖励即令牌（即：Token、比特币）。在每个块的第一笔交易，被称作“币基”交易，这些奖励的令牌将分发给矿工。

比特币软件的首次发布是在2009年，矿工每十分钟总共可获得50令牌（1令牌=1比特币）的奖励，这些令牌可以进一步细分为10^8个单元。每210000个块（大约四年），该数量减半。因此，目前矿工每十分钟仅能获得25个令牌的奖励，2017年，这个数值将降为12.5个。令牌的设计是为了鼓励个体与企业参与整个比特币生态系统中来。经过几年来业余爱好者们的实验，在比特币的市场价格的助推下，比特币渐渐发展为与法定货币相对立的一个资产类别。

虽然人们通常会说他（她）拥有10个比特币，但实际上比特币没有实体，甚至连实体的数据对象都不存在。我们谈论的只是比特币的功能，它具有在给定模式下，解锁私钥的独有功能，从而实现分布式架构的账簿上数目的变动。由于所有矿机都在明确界定的“干”规则下运行，基于共识，他们尊重账簿的登记变动。换句话说，比特币转账仅仅是：从一个地址转移一个整数值到另一个地址；所有这些变动都记录在公开账簿上。因此，用户实际上可以通过数字钱包之类的众多媒介（从笔记本电脑、平板电脑、智能手机访问），通过在线浏览器，甚至通过无线网络、冷储存技术（比如纸钱包、USB驱动）访问、传输、存储他们的令牌，不过，实际的账簿仍然是分布式保存的。

另一种看待比特币系统的方式是通过思想实验：

试着停止使用“财产”一词来指代拥有的东西（或产权），而是谈论一些事物（或资源）的拥有者。拥有者以资源的形式拥有某项产权，然后问：什么是一个比特币的所有权或产权？究竟什么是比特币？于是你就有了一个清晰的定义。当然，不存在什么比特币的产权，由于比特币可以进一步细分（最小单位称为“聪”）。经济学上并未给出“财产”这一类别的定义，因为这实际上是人类行为和稀缺资源的研究。财产是法律认可的权利，行为人之间一种关系，超越了可竞争的稀缺资源的控制权。使用公钥加密，个体可以通过区块链上的特定地址，来控制一种特定的整数值。这种“干”代码，有效的消除了中间商和无用的交易成本，同时保存账簿的完整性。从形而下的角度说，如果说协议是密码学货币的“法律”，拥有就是“所有权”，对私钥的拥有相当于一笔交易（TX）输出的设置，交易的输出指定了所有权。所有加密资产本质上都是不记名资产，拥有它就是拥有私钥。从不记名资产向登记、无纸化转变，再重回不记名资产，这一循环正如文明的演变，财产制度由占有到由今天占主导地位的发达国家登记的转变。

用法币交易比特币有几种方法。大流量的有Bitstamp、Kraken、BTC-e等公司，它们都是网络交易平台。用户在这些平台上存钱，平台则与其司法管辖区的银行进行合作，帮助用户将钱兑换成比特币。一旦用户在平台卖出比特币，银行则给平台注入法币。自2009年的创世区块以来，大约有1240万个比特币被开采，其中有很多被永久丢失了（当一个用户丢失或遗忘他/她的私钥）。在本文撰写之时，开采出的全部比特币市值约为70亿美元，万事达卡的市值则为1252.4亿美元。

非雕虫小技或昙花一现

凭借其去中心化的点对点网络，比特币可实现价值的近即时转账和非信验证，同时可作为一切财产所有权（包括命名权）的登记表，通过算法来控制稳定的货币供应量。不过，比特币相关协议还是有一定的局限性。

到目前为止，初始版本的比特币协议，尚不能跟踪和管理多个资产类别。例如，三年前，一万比特币只能买到一个披萨，令牌（Token）很容易成为披萨币。那就是说，当价值被交易，那些使用区块链的人，会尝试锚定披萨饼的价值。或更准确的说，那些使用比特币作为交易媒介的人，也可以使用披萨饼作为记账单位。（例如，设置羊驼毛袜的比特币价格时，可以参考比特币换披萨的价格）相反，比特币用户考虑比特币兑法币的价格时，则是以法币作为记账单位，因为在现实经济中法币通常被用来衡量商品的价值。从另一个角度看，用户可能是使用“彩色币”的方式来对待比特币（如下），按照惯例，一个比特币等于万分之一个披萨饼。因此，为了以去中心化的方式跟踪、交易和管理智能合同（从而实现智能合同甚至智能资产的交易），比特币留给你可施展的空间非常有限（如下）。

我们该如何在区块链上进行交易？如果是纯粹的工作量证明机制，区块链面临一些逻辑问题。一种选择是为每一种资产建立并维持一个区块链，这样就形成数以万计的竞争币。相应地，每个资产类别都需要一个哈希生成的网络来验证交易，并防止双重支付（即51%攻击）。虽然实施这些解决方案，没有任何技术难题。用盈利的方式来激励矿工，建立和维护一个挖矿网络，将会非常繁琐，在写本书的时候，存在几百种不同的山寨币（竞争币），其中大部分是比特币或莱特币的简单复制，网上甚至有自动化的工具，允许用户自行创建山寨币，如Coingen和Razorcoin。然而，尽管山寨币广泛存在，它们的创造者可以复制比特币的代码，却无法复制比特币的网络效应，正是网络效应的存在，比特币才能持续繁荣。

另一种选择是在区块链的顶部再建一个层或平台，区块链则作为参考资产的底层。所有去中心化的加密区块链都共存于该平台。最多机构参与、最多商业市场、最多社区参与（无论是软件开发者还是用户群）的是比特币，从经济学角度，这就是所谓的“网络效应”。也就是说，越多人使用网络，该网络就越有价值。类似的例子是社交媒体网站，如脸书（Facebook）：你的朋友越多使用它，它就对你越有潜在价值。又比如说信用卡，越多商家接受Visa，它就对你越有用越方便。虽然有很多其它山寨币（或竞争区块链）可能被发明，要让用户、商家、开发者们接受它，并使规模接近临界质量，将是一个长期的战争。还需要注意的是。先行者并不非得是市场的长远选择。例如大莱卡[6]是信用卡始祖，但它后来被后起之秀取代，今天已沦为小众。相似地，Friendster和MySpace是第一批获得融资的社交网络公司，但脸书成为最后的赢家。柯达（Kodak）、百事达（Blockbuster）和淘儿唱片（Tower Records）也是无法适应不同市场环境的最近例子。事实上，在充满颠覆性创新和创造性破坏的技术行业，包括最引人注目的RIM，它率先提出黑莓概念的智能手机，但因管理不善而濒临破产。

> [6] 大莱卡（Diners Card）：于1950年由创业者Frank Mamaca创办，是第一张塑料付款卡。

至少在不远的将来，比特币还是协议的重头戏

尽管在上述两种选择已经做了一些努力，像万事达币和彩色币项目都选择建立在比特币区块链之上，使用比特币区块链作为验证与传输协议，使得他们能够专注于建立资产管理工具，而不是建立一个全新的哈希网络。这两个项目都有管理资产的不同方法，万事达币发行的令牌叫万事达币（一种元币），可以在交易市场中像比特币一样买卖。2009年1月3日，比特币区块链的创始区块被公开发布，奠定了其它所有后续区块的基础。同样在2013年7月31日，万事达币的退出地址（Exodus）建立了，万事达币的框架都将架构于其上。随后的8月份只有非常有限的万事达币被创造，只有使用特殊设计的钱包的用户才能看到这些币，这种钱包可以将万事达币与比特币主链区分开来。尽管取得了一些初步发展，需要从社区众筹4700个比特币（在当时价值500万美元），这些万事达币可以嵌入短消息到区块链中，用来代表用户定义的资产，比如衍生或博彩资产，专门的数字钱包和在线工具可用来跟踪、交易和销售万事达币给世界各地的任何人。

彩色币项目与万事达币略有不同，因为一定量的比特币（如0.001比特币）被“着色”为不同的资产（如绿色代表汽车，蓝色代表房子，黄金代表黄金，粉红色代表股票），用户可使用比特币区块链交易这些“彩色”资产。例如，如果你有一个家，你可以使用0.001（或任意其它金融）来表示传输和定义它一个次级属性，颜色“蓝”或任何其他“颜色”代表资产的类别（比如一所房子），然后，你可以使用一种叫ChromeWallet的特殊数字钱包，发送和交易这些新的蓝色令牌，使用在线交易市场（甚至去中心化的交易市场），买家可以用比特币或其他彩色币购买你的“彩色”令牌。所有这些都是通过相同的账簿来管理，在这个过程中唯一的中介就是区块链，它管理“彩色”令牌正如管理其它比特币。

其他几个项目（NXT，3I公司，合约币）也有类似的功能，他们都有一个主要的目标：即，让去中心化的加密账簿（区块链），来取代以前被众多第三方充当的管理角色。虽然目前形势还不明朗，但只要有一种成功，非信资产管理的应用与全部蕴含，必将更广泛地进入大型软件开发社区。

迈克·赫恩，一个核心比特币开发者，最近刚刚从google离职，目前正全力为比特币协议工作。他们致力把智能合同功能融入协议，设计了几个代码库，以实现未来发展可能遇到的几种使用场景。我在电子邮件中问他："中本聪在使用'合同'一词时，它们是关于比特币的，而且比特币本质上是与金融有关的，所以，我认为智能合同的应用将仅限于金融领域。所以，什么样的应用才可能让密码学货币被更广泛的接受？

他说：

> "这是比特币百万个为什么之一，不是吗？我不知道。有可能并不是一个特定的杀手级应用，而是一种类型的应用，它仅仅是非常有用，可以让每个人在需要的时候随时使用它。我去年夏天尝试了小额支付这个项目，这也许是该问题的答案之一。"

由于受传统支付方式的手续费限制，小额支付一直是个金融学难题，直到比特币面世。因为它允许细分到小数点位的一百万分之一（实际上如果升级为更高版本的话，还可以细分到更高小数点位）。许多链外交易钱包和交易解决方案，可以让用户在这种额度下交易比特币，比如Coinbase和Circle。链外交易是价值的转移（比如资产）发生在公开的区块链之外，也就是说，最初的用户直接通过区块链发送比特币，这被称为链上交易。但是，现在鲍伯可以通过他的任何一种钱包发送爱丽丝比特币，后者可能使用是Coinbase（可信任的第三方）之类的区外交易服务提供商。或者说，鲍伯的令牌首先发送到Coinbase的链上钱包，并被同步到公开账簿，但随后使用一个内部数据库，这些令牌被分配给Coinbase内部链外钱包系统的特定用户。链上交易与链外交易达成一种平衡，链上交易服务商比如Blockchain.info是可靠的，不能被第三方左右，转账与交易以每10分钟一帧的速度进行（区块链的确认速度），然而读者朋友应该知道，虽然使用可信任的第三方（即时和可低于额度限制）具有一定优势，但同样也可能导致令牌的损失（如MtGox的惨剧），成千上万的客户可能倾家荡产。

同样，赫恩等人也讨论了如何在不久的将来，用移动设备（智能手机，笔记本电脑，平板电脑），通过WiFi热点接入网络，进行比特币小额支付。也就是说，目前无线网络的一个问题是，尚不存在一个自动的、安全的方式，可以让陌生人使用无线热点，而不必信任任何一方，这可能导致滥用（如信用卡诈骗）。相反，如果艾丽丝的WiFi路由，是用比特币功能启动的（比如有一个内置的钱包），那么，鲍伯就可以通过比特币支付，来使用无线网络，哪怕只有很小的费用，双方也可能达成买卖。

保证合同

假设区块链在未来得到广泛接受，在其之上是否会诞生可行的、非当前使用的技术？亚历山大·塔巴洛克[7]与我在邮件交流中，对智能合同在现实世界的应用作了初步探讨。保证合同是将针对一组目标的贡献以托管的方式持有，直到量达到一定阈值，就释放所有的贡献（如Kickstarter的众筹模式）。这种模式已被探讨作为资助公共基础设施（如一座灯塔、污水处理厂、道路、桥梁等）的替代方案，互联网的众筹模式通常是将项目放在聚光灯下，可视作智能合同的简单形式。显性保证合同则是该模式的一个变体，如果捐款达不到门槛，那些捐款者不仅将收回他们的原始资金，还会收到奖励，这将激励更多人去捐赠。

塔巴洛克写道：

> 我把智能合同与物联网视为信息不对称问题的终极解决方案，在经济学上，当交易中的一方、比另一方有更好的信息，他将不害怕被人利用，相反，信息匮乏者则倾向于不遵守合同。所以即便是交易本身是互利互惠的，但由于交易没有达成，这样对双方来说都是一种损失。智能合同和物联网，可以解决信息不对称的很多问题，它们可以让信息披露更可信，甚至可以让双方都不知情的条件下达成交易。
>
> 资本主义喜欢科技和技术，它是一个动态的系统，没有人能预知它的动向。我只是希望，用户发现显性保证合同感到惊喜。Kickstarter和其它组织的保证合同已经为人们熟知（如果有足够的人加入，你支付即可），显性保证合同做一个类Kickstarter的项目可能更具吸引力（如果有足够多的人加入，你只需支付，如果没有足够多的人加入，你得到奖励），我希望能看到类似的实验，希望会有一天在熟悉的私人领域鼓励人们参与DAC实验，来资助公共设施和政府服务，这也是我最初的动机。

---

[7] 经济学家，乔治梅森大学教授及独立研究院研究负责人，“显性保证合同”模型的创始人。

法律挑战

DAC的实施并不是没有问题，关于此点，专利律师、作家和比特币投资者斯蒂芬·金塞拉与我谈到，“既然密码学货币、加密协议和智能合同，看起来都具有潜力，按照我在法律行业的经验，法律的变革十分缓慢，如果这些领域不是所有环节都受到高度监管，并且有大量成熟的老牌运营商，并集成了银行业务，其结果就是，大多数客户与合作伙伴，还是希望继续使用传统的服务和解决方案，从而导致对创新的抵制非常强烈。同样，信用证与争议仲裁委员会，已经存在了几十年，所以这并不一定是个卖点。虽然使用独立的仲裁员或信托，有理论上的优势，但许多财产所有权与汽车所有权的合同，已经建立了一个条款系统，规定当事人哪儿可以选择仲裁员、以及如何使用信托。例如，以百分比的形式规定即使出现纠纷，当事人最终需要信托的数额也是相当小。不过，如果有足够多的买入，该条款可能在稍后作出改变。”

在他看来，这个问题实质上是密码学货币在与现有法律和商业交易的基础设施竞争。“而且，即使智能合同提出了一个非常有效并最优化的市场，培育一个用户群也将是一场长期的艰苦战争。因为，在某些方面你可能需要重新发明车轮，或重新“编码”车轮。举个例子，为了对冲违约的风险，鲍伯需要发行100万美元的债券以支付保险费。如果违约最终发生了，你可能需要与第三方合作，他来帮助你调整这桩买卖，这进一步增加了你交易的成本。有时，如果交易继续变糟，鲍伯将起诉或干脆核销损失。当然，这类交易同样可能发生在加密账簿上。此外，虽然加密协议提供了许多方法来规范管理，如命名管理。在未来数十年内，我看不到银行有什么理由要重写他们的系统，他们是典型的风险厌恶者与保守主义者。事实上，我仍然看到，法律合同的条款，已经存在了几十年，甚至长达一个世纪，因为它们经历了法律审查。虽然智能合同在理论上可以提供相似的条款，但二代币开发者与支持者应该意识到，需要许多年的持续教育，才能说服企业接受这种新型框架。

根据金塞拉与其它研究者与我的交流，智能合同可能在狭义合同上引起的问题是最少的，即那些很容易被量化的可替代的商品（如石油、金属、矿石、农业）或简单服务（如汽车修理店、美容店），也就是说，那些可被客观衡量的、机械的稳定存在的商品，低消费保障，不需要复杂的申诉与保单。虽然鲍伯和艾丽丝需要注意，不同司法管辖区，提供的不同指导政策，及有关服务的执照（如化妆品，会计），加密账簿和非信资产管理，可以开启一个以物易物的无摩擦环境，去中心化的交易，可以让本地服务提供商，以非法币的形式买卖与交易。虽然不同司法管辖区，无疑将影响税收与监管，但这种类型的“以物易物”加密系统，在一些金融系统摇摇易坠的国家，比如阿根廷和希腊，可能会变得有用并被社会采用。

阿根廷

阿根廷人文西斯·卡萨雷斯是一个比特币创业者，他为机构提供钱包服务，2014年2月，我与他有过交流。据他回忆，他在巴塔哥尼亚度过了童年，“我记得十二年前，阿根廷的通货膨胀大得惊人，我的母亲，会随身携带一个塑料袋，装她的薪水，钱一到手就得花掉。她去的那个市场，有一个雇工专门负责更换商品的价格标签，因为价格上涨太快了。”此外，卡萨雷斯指出，在国家层面，政府不希望提高税收或减少开支，所以他们只得不断印钱，这导致通货膨胀。当我和别人谈论比特币，我会根据对方的背景使用不同的比喻。然而我向阿根廷人解释比特币如何工作，他们很快就能理解它。他们意识到它不能被没收，可以用作财富保值。

1998年到2002年，按GDP测算，阿根廷的经济萎缩了28%，到了2001年底，政府拖欠了1320亿美元的债务，2002年4月创下通货膨胀率10.4%的新高，2001年12月失业率高达20%，到了2003年失业率仍维持在25%。虽然下一界政府推翻了原来的几条政策，包括外债重组，2008年阿根廷国民政府国有化私人养老基金，涉及300亿私人储蓄。

根据他的经验，卡萨雷斯说：“当我帮助阿根廷人进行面对面的交易，当你发现这些用户并非黑客或极客，他们是普通的民众，他们了解比特币作为保值手段的好处。许多人其实没有太多积蓄，但是他们能看到比特币不会通货膨胀。富人可以轻易的把资金投入到硬资产，但是生活在底层的人却做不到。比特币可以帮助穷人实现资产的保值。我想象这一情形在未来将持续发生。比特币有很多好处，不同的人可从中获得不同的好处。如果另一场类似的通胀再次上演，由于智能手机的广泛使用，比特币会呈星火燎原之势。

塞巴斯蒂安·塞拉诺，另一个阿根廷人，虚假货币支付服务提供商BitPagos创始人，基于他的亲身经验，表达了类似的观点：“2002年初，阿根廷掀起了一场以物易物的大浪潮，人们以点对点的方式交易食物、服务等任何事物。在2001年底到2002年这一期间，比索汇率呈自由落体势态，失业人口大量增加，这迫使人们回归以物易物的交易方式。事实上，这场危机中的几个月里，许多集市和“以物易物”俱乐部已经发行自己的“信用卡”，创建自己的票据作为凭证。最终形成一个联盟来发布一些便条，不过，假冒信用成为一个大问题。随着经济的复苏，对这些俱乐部的需求相应减少，人们不再去那些地方。只有少数俱乐部存活下来，大部分则关闭了。然而，我认为密码学货币和一个去中心化的资产管理系统，可以大大帮助以物易物系统度过难关。不在于价格发现，而在于防止欺诈。因为许多市场饱受便条伪造的影响，在票据发行与分发上也缺乏透明度。基于智能合同的系统，可能会被用于上述场景，我想，我们目前尚落后于智能合同系统几个世代，也许正在开发的几个新平台，有助于实现可长期运营的以物易物系统，因为合同只有在考虑时间因素时才有意义，因此，如果发生另一场金融危机，观察智能合同将如何发展，将是一件非常有趣的事情。

2013年，阿根廷比索相对于美元贬值了25%，为阻止资本外流，阿根廷决策制定了严格的资本管制政策。结果就是，缺乏政治影响的普通民众，难以保护他们的比索储蓄，由于兑换外币被严格限制。虽然一个新兴的比特币社区，在阿根廷崭露头角，但只有很少的正规店铺，接受比索购买抗通胀的比特币，或其他加密资产。非信资产管理需要让普通民众也接受它，取代当地货币（如比索），通过加密令牌来购买服务。

这种制度一旦实施，将是一个更准确的“巨无霸指数”。巨无霸指数是经济学家为测量每个国家的购买力平价（PPP），而发明的一个货币比较工具。也就是说，一个巨无霸是相对稳定的可量化的商品，不论处于何地，它以当地货币计的价格应处于同一水平上。然而，自1986年以来，由于内部货币政策影响，巨无霸的美元价格会出现明显高估或低估。商人和企业家并不非得知道全球各地的理发、加油或者飞行训练的价格，虽然这些价格指标可以提供价格发现的功能（价格发现（*Price Discovery*）是指买卖双方在给定的时间和地方对一种商品的质量和数量达成交易价格的过程。）。阿根廷人在波动非常剧烈的市场利率下交易商品与服务，他们没有使用当地货币。事实上，正如全球化以地区间的低技能岗位工资等级来套利（即在其他条件不变的情况下，使得不同地区的纺织品的生产成本趋同的过程），最终，一个去中心化的系统可以帮助企业家协调对某些地区的经济投资。

举一个投机性的例子，布宜诺斯艾利斯的机械师鲍伯，可以创造各种“彩色”令牌来代表性能调整、修理和加油，并将它们置于去中心化的交易市场，以跟踪这些特定的服务。来自阿韦亚内达郊区的爱丽丝是一个飞行员，她同样可以创造各种令牌来标记特定的飞行时间（如两小时的飞行训练），同样放在去中心化交易市场。每个交易市场可以同时列出当地服务的费率（例如供应商接受哪种法币）和各种密码学货币的汇率。通货膨胀会吞噬法币（如比索）的购买力，去中心化的交易平台可以让商品和服务提供商以去中心化的形式支付定金和交易，不需要使用一个不停贬值的法币中介。艾丽丝和鲍伯可以使用撮合服务来直接售出可赎回的服务令牌，甚至换成其它中介密码学货币。要在特定的两个加密账簿间

交易，以共识为基础的DAC可能需要智能合同来提供托管和仲裁机制，或者用户甘愿接受无保障条款的合同（即买者自负），在他们作出商业决定之前，可以由独立的行业自律机构提供一个反馈、声誉机制（如信用积分），让市场参与者来评价艾丽丝或鲍伯是否是一个冒险的商人。

但是，加密账簿是由复杂的定量机制构成的，它缺乏定性--以物易物在经济紧张时期可能奏效，但在真正的消费经济中可能不会。据斯蒂芬·金塞拉的说法，“个人、小型公司和大型机构每天都在使用数以万计的正式和非正式合约，每个合约都因本地环境的不同，而存在细微差别和微妙的相关。哪怕是雇佣一个临时助理也需要定性语言--一些正式的法律术语，这些将是难以自动化实现的。事实上，金融业以外的大部分合同，都没有完全自动化实现的条款。因此，虽然智能合同和加密账簿，创造了一个跟踪资产所有权的全防方法，但在某种情形下，你仍需要使用人类主观判断。对于已有政府补贴的公共制度，市场参与者可能会谨慎放弃使用智能合同。这样，你不仅需要提供教育推广，而且要说服消费者买入。

斯蒂芬·金塞拉和肖恩卓尔泰克还提出另一个问题：我们如何说服市场参与者，采用新系统的成本大大优于现有基础设施？例如，在一些发达国家，房主可以通过在线出售房产，而无需房产经纪人。同样，购房者可以在线购买房产并完成登记。如果你想快速卖掉它，只需轻松的使用房产经纪人。而且，虽然公寓楼、公寓和排屋通常是同义词，并不是所有房子都是可同义替换的，因为它们通常有一些需要被量化的独特属性。尽管这仅是一个小小的可被克服的技术挑战，但支持者应该知道，一些消费者（或房主）可能对通过代码合同来量化他们的资产不感兴趣。

外部视角

虽然目前大部分文献，不管是学术还是软件开发领域，都是从一个美国公民的角度写的（大部分由尼克·萨博撰写）。普雷斯顿·伯恩，一个亚当·斯密研究所研究员、伦敦证券律师，与我谈到，“尼克·萨博设想的智能合同，目前并未成为现实，它需要大量吸收传统合同的法律要素，能自动执行，在功能上自动表达，至少，当它代码写好后就应该做到这样的程度。也许，实现代码的模块化是可能的。比如，在代码里反映某些法律认可的条款（终止条款，应付特定事件的发生），并对不同类型的交易进行标准化。

伯恩认为，起草商业上可行的智能合同并非不可能，但并不容易。仅仅靠代码可能是不够的，如果一个合同是双方协商一致的，在发生争议时，法院可以强制执行。而一个智能合同是靠自身来强制执行的。合同的大部分是由以下约束：（1）商定的规则。（2）一套非常复杂的法律拟制（又称法定拟制，将原本不符合某种规定的行为也按该规定处理。），来约束这些规则如何应用于不同的情形。例如，英国的法律要求将任何已形成的合同纳入某种类型的协议，价值的实质转移本质上是创建了双方之间的法律关系。当出现违反协议、撤销协议或无效协议的事件，他们有一些补救措施：解除，例如在合同中呈现无效，具体表现为，法院命令一方做他已立约的事，并赔偿（更常见）受害方的损失。虽然有时当违约发生，双方的商业合同能够识别并理清适当的补救措施，最终的仲裁取决于（1）合同是什么（2）违约会出现什么样的后果？取决于法院或仲裁员如何裁决，法院和仲裁员拥有约束双方的能力。智能合同则是完全分布式的匿名的区块链，完全自主的DAO（分布式自治组织）不太适合这个角色。

这是草案中讨论的问题之一，如果理论是存在的，智能合同会在哪儿，忽略炒作和喝彩，主要的障碍是技术代码库和配套支持服务亟待完成，基础设施必须存在，才允许智能合同实现萨博和伯恩所描述的功能。

一些资料解释了智能合同，几乎不可能消除所有人类互动的电子商务——因此，为什么要使用一个麻烦的加密账簿？伯恩认为，或多或少存在的交易成本优势会让贷款人感兴趣。只有当加密账簿在大型组织中变得更流行，智能合同技术才能变成实用。据伯恩介绍：“企业和金融机构有较高的人员与设备费用，如果可能的话，他们的业务可以实现自动化。用分布式区块链取代复杂的服务器架构的主意，对我来说是一个相当简单且优雅的解决方案。区块链基本上是世界上最透明最精确的产品，专有区块链突然出现在金融机构、政府和企业内部只是一个时间问题。结果就是节约了资源——目前金融服务行业员工工资，可以节省下来——这些钱将重新部署到贷款业务和经济中去。

“类似的，政府对自己的财政可做同样的事，所有人都会从中受益。在英国，公共部门的工资单是1675亿英镑一年，占国家支出的25%，占GDP的12%，平摊到每个人头上约3000英镑/年。英国可以创建一个国家支持的密码学货币：加密先令，确保只有银行可以挖掘它，每个英国公民都有一个私钥，用来兑换现金或以1：1的汇率（加密英镑/英镑）存在银行，当超过6个月，可用一张包含对应公钥的芯片卡替换国家保险号码，支付工资，缴税，申请救济等等，就像扫描二维码一样简单。我们可以一夜之间消除官僚福利和数额庞大的支出。”

“这样的货币将优于任何其他形式的法币。”伯恩说，“想象一下，能够看到全球范围的每一笔实时英镑交易，还能享受加密的好处，包括安全、透明、快捷、不可逆、低成本。由于它是由节点中的大多数控制，意味着只要大多数人愿意，协议是能被修改的，所以也能从它能被修改的特性中获益，而不是那些拥有很多网络哈希能力并至少懂一些私钥知识的人获益。协议可被修改这是很有用的，例如，为了逆转欺诈行为，撤销合同或制订量化宽松政策，任何政府无可争议要做的是确保文明的持续。”

他补充说，“我知道有一些人会抵制协议的修改，并且这也不是中本聪的本意。这会导致一个国家对货币供应的绝对控制权，并有能力通过官方区块链干扰个人理财能力。我同意这个说法。但是，先进国家已经有能力这样做，我们还得为成千上万的官僚执行这些政策而买单。此外，政府背景的密码学货币阻止我们自由选择和交易密码学货币（如狗币），如果密码学货币即将腾飞，我们得开始思考这些问题。”

伯恩“用加密英镑取代英镑”的建议已经在冰岛开始实践，一个叫Auroracoin（AUC）的项目发起了，幕后团队内部预挖了1000万Auroracoin，以后将永不生产。Auroracoin的创建者计划于3月25日，分给每个冰岛公民31.8AUC，以缓解未来的银行业危机。同样，Mazacoin项目正在科美国原住民部落拉科塔国展开合作，创造另类密码学货币，宣称可以给“美国原住民社区一些财政自主权。”虽然尚不清楚如果商人接受和使用这些加密令牌，会给所在司法管辖区的监管框架带来什么变化。未来几年此类实验可能会继续发展。

伯恩还认为，违约还会引来其他发展问题，其中一个问题是整合密码学货币作为支付工具后，怎样确定还款的优先次序，用他的话说，“缺少可信任第三方的裁决，目前密码学货币支持者、主流金融机构、政府之间的对话很少，开发者和自由主义者站在与政府对立的一边，机构和公司则审慎的站在另一边，两个阵营针锋相对，似乎在准备一场战斗。”

“密码学货币技术，表面上是为了从银行和政府手上夺取商业控制权，”伯恩补充说，“这种事态并不奇怪，这是二分法的结果。但是，在实体经济中充当媒介的银行与旨在取代他们的密码学货币之间存在脱节，这是一种适得其反。技术本身是开源的，可以惠及每一个人，包括银行。但是双方的隔阂已经严重影响到密码学货币的发展。以资产抵押的点对点贷款为例，假设借款人使用密码学货币贷款，并以密码学货币作为抵押。与一个密码学货币支持者聊天，他会谈到编写一个智能合同的机会，可以消除银行等中间机构，可以避税，可以让他逾越税务机关而赚点小钱。而如果与银行打交道，他们必然谈论洗钱、恐怖主义融资和监管，其实密码学货币不必是这样。”

他认为，解决方法就是重新引入一个可信第三方（TTP），它的权限下降一个高度，但仍起着重要的监管作用。“让我们重新回到点对点贷款之资产抵押的例子，银行编写的贷款合同，通常会以某种形式协商若干谈判条款，对资产进行安全抵押，再提交给一套复杂的法律规则。”

正如萨博指出的：“经历许多个世纪的文化演变，合同与相关原则已经成为双方的共同理念，编进了普通法。重造该演变结构的代价高昂。如果我们从头开始，使用理性与经验来能重建合同法与财产权，并让现代市场行之有效，可能需要几百年。但是数字革命让我们进行机构创新的时间更为仓促。”

伯恩进一步指出：“萨博阐明了一个事实，即普通法是一个规则非常复杂的实体。他的另一个结论也是正确的，即我们起草的智能合同将让人们大大受益，密码学货币有过之而无不及，但是，这建立在与法律互动的前提之下，而不是去重写一套平行的法律系统。首先，英国普通法的一个定义或特征是它至少在历史上并不是通过立法而建立的，它是一个有机的演化过程，在现有规则上不断变化以面对的环境，在诉讼的过程中不断测试，它是直推式算法的一种形式。例如，与担保有关的法律是出了名的复杂，因为担保人出于经济利益，会通过法律工具挑战合同的合法性。这意味着在起草法律时就必须非常细致与谨慎。”

直推式算法是机器学习中使用的一种从具体经验中推理的技术。换句话说，通过教育（学习）将具体案例应用于今后类似领域的案例中去。伯恩建议，可以通过类似的过程，建立密码学货币的法律框架，但尚需时日。

“但是，即使在简单的协议里，作为银行贷款和法律实践的局外人，也会意识到，以硬规则为基础的方式距离现实还很遥远。法律是“湿代码”，这并不是一个错误，而是出于设计。让我们回到抵押贷款的例子，在现实中某一方可能会避免行使其权利，或者去寻求一个符合现实的特殊解决方案。即使贷款在默认情况下强制执行，也可能不符合任何人的利益。根据我的经验，强制执行是一个极端的解决方案，是商业合同的终级补救措施，但它也是商业合同全部信用的建立基础。智能合同可以充当可信第三方的角色，它公正执行，有足够的资源或保险，如果有人违反其义务，他们将被起诉，这是密码学货币被主流接受所必须经历的一个步骤。要实现此点，密码学货币社区要克服反政府和银行的意识形态，并与政府、银行做交易。

然而，社区对他的建议反应不一。他看到现有第三方角色的变革，“在资产抵押的例子中，假设有多个贷款人，通过这些贷款人会通过代理或可信第三方，如另一家银行或专业托管公司来进行合同管理，按他们的意愿或集体意愿来拥有或行使自己的权利。这样的合同管理行之有效是因为：（1）普通法允许贷款人与可信第三方以某种方式达成协议；（2）如果事情搞砸了，当事人知道在哪找到可信第三方。

在伯恩看来，一旦可信第三方从尼克·萨博提出的那种简单交易中移除，这样的合同将不同于以正常方式达成的合同：

（1）可信第三方与其相关费用将脱媒化（金融中介地位下降的过程），用户将变成独立的存在机构。

（2）去中心化的价格将是全额现金抵押担保，使得最基本的贷款合同在普通商业中不可行。

（3）自由裁量权将暂时搁置，以适应由算法限制的新环境。

（4）在所有可能的情形下，超出智能合同本身规定而造成损失，强制执行的可能性将有所降低，因为（a）技术上的设计不容许这样的行为（如果一方将为间接损失负责，在他的责任将会增加的情形下，他几乎可以肯定不会交出他的私钥）；（b）即使寻求法律支持的一方在法庭出示合同，要求追踪所有相关资产，引入新的合同法律制度，另一方也会故意在它之外操作，使得它不能顺利运行。

这确实是个问题，这本书的大量评论问道："数字合同的这些问题，在现实生活的执法中，是怎样解决的？毕竟，即使是由区块链来强制执行，人类仍然需要输入该合同将被执行的条件。如果发生在现实生活中，它仍将由律师和国家强制执行。但是，该问题没有明确的答案，不同司法管辖区有不同的反应方式：从接受到彻底取缔。

伯恩认为只有一个解决方法：在区块链中重新引入第三方。

正如萨博所说，"从我们目前的法律、程序与理论看，这些原则仍然适用于网络空间，我们可以保留这些根深蒂固的传统，大大缩短开发实用的数字机构的时间。"这对伯恩来说意味着，"设计智能合同对司法管辖区的具体法律原理的技术性理解是必需的，试图用算法实现复杂的普通法是不可能的。以Eurosail -UK 2007- 3BL为例，如果算法相关的法定结果是由纯机械的规定，很有可能没有人会在订立合同时提出……

伯恩认为如果它被应用，传统将很容易保持下来。方法就是要确保智能合同脚踏实地。它将仍然是以一纸合同的形式呈现，只不过它特别地被保存在区块链中，而不是自动机，后者特别适用于收集、现金扫描、掉期款项及抵押、管理或冻结账户（如果是通过区块链查询，那么账户并不是必需的），支付优先级，甚至是所有权转让（如尼克·萨博建议的用证券作抵押的汽车贷款）。

他继续说，"唯一可信第三方在个人合同中的作用需要被限制，主要通过信托当事人的私钥或根据当事人的合同条款，而不需要机械化执行，当事态恶化时，唯一的干预手段就是行使自由裁量权，比如涉及破产、弥补非预计损失时，要赋予灵活性，并参考货币属性重新更改法律。人类因素可作为保留手段，这将允许司法控制交易。但是，要推动事情向前发展，计算机程序员需要开始与律师和银行家对话。这不是说这将阻止任何人在法律体系之外使用该技术，而只是说，技术的成熟需要与法律系统保持一定联系，并提交其管辖权。"

虽然现在下定论在美国密码学货币将何去何从还为时过早，但它在未来几十年，将很可能成为学术热点。与此同时，目前有几桩涉及密码学货币的案件在进行，其中包括约翰霍普金斯大学博士通过丝绸之路（一个以非法毒品交易闻名的匿名市场）出售处方止痛药（oxydocone），以及ASIC矿业公司Alydian的破产，在破产程序中，法官提出的一些问题，是其他司法管辖区也必须熟悉的问题：什么是令牌？什么是密码学账簿？它是否存在？如果是，它在哪儿？它可以被控制或销毁吗？等等。

伯恩认为，有可能会形成一种平衡，企业与机构分别整合它们的业务，将可能是以数学、算法和加密协议的形式：一种非信平衡。如果你愿意，对大多数资本密集型（证券、企业贷款、企业并购、资产和物业购买）的大型合同来说，智能合同将确保它们在法律管辖范围，（1）可更好地评估和减轻商业和交易对手风险；（2）创建一个可被强制执行的现实资产的纽带，市场会需要它。法庭将制定一个解释框架，迫使人们转向智能资产。如果一个可信第三方知道私钥，一个中央代理可以控制他们并赋予法庭命令以效力。政府机构使用该技术同样适用，它所掌握的私钥同样受司法和宪法控制。

第三章：下一代平台

虽然比特币所代表的创新是如此的开天辟地，它仍有一些已知的技术局限。与此同时，开发团队当前着重把精力放在改善比特币协议的安全性上，来防止安全漏洞被利用，这么说并没有任何对开发者们批评的意思，不要忘了2月份的时候，交易可锻造性问题在社区引发了怎样的混乱。而对于改善这个领域中的功能性，则由社区里其他开发者挑了重担，其中一些项目建立在比特币协议之上，而另外一些项目则新建他们自己的独立账本，还有一些则是为比特币与其它账本建立沟通的桥梁。

下面我会介绍八个正在开发中的项目，他们都试图设计和实现“智能合约”或智能合约的功能，每一个项目我都采访了他们的主要开发者。

彩色币

就像之前讲的，通过加密区块链来实现并验证共识，其中的一种办法是用彩色币，概括来说，它允许用户通过对某个代币染色来使其代表某种特定的资产，例如车、房子、船、大宗商品、股份、债券（例如，带绿色的0.5 BTC代表你的房子）。这些代币可以随时随地在任何人之间交易，就像比特币一样，这样就建立了一个去中心化的无需信任的资产管理方式，在这里区块链既是账本，又是交割的手段。

Alex Mizrahi是彩色币项目旗下Chroma钱包项目的主要开发者，他说：“彩色币将给整个资产管理行业带来极大的便利，例如，房地产和投资组合管理可能会是最早采用彩色币的领域之一，事实上，对于任何形式的资产管理，通过发布它自己的颜色来代表它的资产都是很容易做到的。投资组合经理可以发行某种颜色的彩色币，来代表某个由真实资产背书的股票型投资组合，之后，这种彩色币就可以在全球范围内出售。如果他够能干，他的产品足够好，那么他的彩色币就会有市场需求。这里，所有权的转让变得非常的简单、快速和安全，就像比特币一样。在房地产领域，人们可以通过彩色币发售他们的房子，并且在区块链上流通，或者通过彩色币来管理房子的分时使用。”

Meni Rosefeld是另一名开发团队的成员，他描述了几项通过次属性（颜色）来管理资产的优势。“最大的优势是去除了准入门槛。目前，初创企业的融资需要通过笨重而低效的私下成交的方式来进行，而那些渴望上市融资的企业则必须为上市先花一大笔钱；而有了彩色币，任何人都可以很容易地发行股票来融资，这样就去除了准入门槛，鼓励了创新，而且整个社会的资源配置也会更有效。”

比特币社区里有这样一种误解--发布和跟踪次属性（颜色）需要通过中央化的服务器来实现，Rosefeld认为这是错误的。“不需要中央化的服务器来跟踪颜色，这可以通过去中心化网络里的寄主货币（例如比特币）实现，而发行某种颜色的彩色币倒确实需要一个实体来完成，但是这个募集资金的实体通常自己不运行交易所。如果没有彩色币，他们就必须依靠第三方交易所，这就回到了原来的各种弊端，例如进入壁垒、大股东锁股等等。有了彩色币，他们就可以将跟踪和交易所的功能外包给高效的去中心化网络，发行方只需关注发行和赎回彩色币，而投资者可以在没有第三方介入的情况下相互交易，这样的方式既高效又保护了隐私。”

Amos Meiri是eToro的交易主管，也是彩色币项目开发团队的成员，我问他：“难道不是在中心化交易所里私下完成所有交易更容易？这样既保障了隐私，又可以大规模实施。”他认为，“中心化交易所的确有其优势，但彩色币仍然非常有用，原因如下。首先，用户不再需要将比特币存入中心化交易所，公司也无法操控所有权记录（来实施欺诈）。最简单的道理，通常如果某人给你IOU（我欠你）承诺，你就不应该把控制权留在他和他控制的实体手里。另一个原因是，公司无法控制股份的交易，从而也没法阻止某笔交易。另外，彩色币无需维护服务器和保障安全，因为这些都集成到了区块链里。”

说说容易做起来难，已经有非常多的其它团队花了很大的努力，来实践用加密账本管理智能资产这个想法。例如今年1月发起的Counterparty.co，这个神秘的相对匿名的开发团队已经发布了相似的开源应用、文档、程序和工具，来让用户和创业者们实现智能资产功能，例如衍生品和去中心化分红。另外也在1月Jon Southurst报道了另外几个团队，其中一个叫Reality Keys，他们利用加密协议来建立预测市场，这可以用来对冲汇率波动。

万事达币

在2014年1月初，我跟Taariq Lewis有过交谈，他是BitcoinBusiness的创始人和CEO，一家比特币咨询公司，也是万事达币项目智能资产部门的负责人。万事达币是一个非营利性的众筹项目，旨在为比特币开发开源的去中心化交易所协议，这个项目获得了4700个比特币的众筹投资，当时价值500万美元，这些资金被用来支付悬赏，开发工具，撰写文档等等，所有一切到最后都会开源。

Lewis认为，“我们正处在金融和投资管理的民主化进程中，而现在看到的只是冰山一角。目前的系统包含非常狭窄的、高度中心化的组织形式，犹如P2P(点对点)发明出现之前的音乐产业一样，我们即将迎来第一波用户群体， 金融产品将在他们个体之间以P2P的形式流转。虽然这么做会引来SEC和CFTC的监管，但这里没有‘华尔街之狼’，事实上，像彩色币、合约币和万事达币这些项目将会创建应用来实现去中心化的股票和债券交易所，如此，个人和创业者们就可以发行各种分红产品，买卖资产，且无需中间商。”

我也跟Ron Gross交谈过，他是Bitblu的联合创始人和万事达币基金会的执行总监，他努力推动这个项目走向开源。“通过万事达币，我们正在开发开源软件，它最终将成为一个任何人可以在其之上构建自己应用的平台。我们仍在为核心开发团队雇佣人手，但终极目标是转为一个去中心化结构，在此结构上我们团队并不真正拥有任何东西或者人工雇佣与解雇任何人，取而代之的是由一个去中心化应用(DAA)来进行这些工作。此外，我们组织了一系列的外部悬赏，每个月给出10万美元以供组织外的开发者进行特别开发工作或只是在生态系统中进行创新。这样，新进入该领域的程序员可以通过仔细检查悬赏列表并提交相应的解决方案，或者对于系统基础进行创造性的建设来立即获取财务方面的奖励。”

Gross认为该生态系统最终会将真实世界绘制进数字空间：作为自我加强的企业行为--持续构建该生态系统将产生一个作为加密账本与真实世界之间桥梁的新金融体系。作为该前景的一部分，围绕去中心化应用、债券、资产背书币、商品、房地产、赌约、市场预测等将产生类似于智能合约代币的自然结果。他特别提到一个正在进行中的项目——万向钱包，它最终将能够处理和追踪所有的山寨币、附生币，甚至彩色币。

然而，到达目的地的道路上显然还有一些障碍。Gross认为，“开发协议并使之强健就已经是有价值的挑战了。大量更复杂的项目所需的基础结构还没有准备好，大量相关开发工作正在进行，但因其开源性，万事达币及该领域内的其他所有项目是可进入的。查看协议、参与辩论、提出你的需求、查看代码，任何开发者、任何人都可以来，并立即参与贡献。如果你贡献出了任何积极的东西，你会因其获得奖励，所以不需要有中央实体。比特天使(BitAngels)很快将会启动一个基金，该基金将通过‘黑客编程马拉松(Hackathons)’投资协议、开发去中心化应用以及其他‘2.0’初始项目，顶尖优胜者将收到50万美元的投资。通过这些努力，我们将建立一个更好的金融体系，该体系将是去中心化的，并且能创造完全的金融自由。创造这样的工具，其作用显然仍只是推测，但即使只实现一部分也将真的非常可观。”

我也跟David Johnston交谈过，他是比特天使(BitAngels)--首家致力于数字货币初创公司的天使投资网络--总经理，也是万事达币基金会的董事会成员。在他看来，“加密货币不仅仅是支付网络，也不仅仅是新的货币类型或财富贮存方式。这是一个全新的平台，现在，通过它，人们可以获得可编程货币并由此产生智能合约。我可以将这些可编程货币加到应用里去，我也可以创造其他的数字代币。这是真正使我兴奋的地方，任何人可以在这里构建任何东西。长期来讲，我们也计划将整个项目转移进一个去中心化应用(DApp)里去，以最大化资源并提高效率。”

DApp是Decentralized Application(去中心化应用)的缩写。万事达币平台，如同其他每个有争议的二代币一样，仍处在开发过程中，并且基于其社区反馈有过几轮反复改动。它也面临着来自于其他几个该领域对手--例如开放式交易(Open-transactions)、Invictus(之前名为Bitshares)的竞争。总之，这看起来是有希望产生颠覆性创新的领域。

未来币

NXT是一个完全用Java编写的新数字加密平台，于2013年11月末启动项目。该平台自带“彩色币”——这些代币的“颜色”代表了特定的资产（例如使用部分的NXT代表一辆车或一栋房子）。它也包括一个去中心化的资产交易所，这意味着你无需通过第三方就能完成资产买卖。例如，如今影响中心化交易所或在线商店的一个问题是你的法币和代币都容易失窃、被黑客攻击或者有其他麻烦。一个值得注意例子是，2013年12月33日，一家名为Sheep Marketplace的在线商家被黑客攻击，盗走了它在线钱包中的96,000个比特币，这也是迄今为止已知最大的加密货币失窃事件。因为没有可攻击的单一中心化节点，一个去中心化点对点交易所几乎不可能发生这类问题。

2014年2月，我和NXT开发团队的赞助者”Uniqueorn”交换过信息。在他看来，“基本上，最好的将NXT与其它加密货币比较的方式是不要比较。NXT完全不是山寨币。而大部分流通中的加密货币只是在克隆比特币基本代码的基础上做了一些轻微的改动，它们之中很少有为加密货币带来任何新的或实质性的东西。该平台内嵌加密信息(类似BitMessage)以及匿名支付(类似Zerocoin)功能，它们带来了额外的隐私层以保护机密信息和交易秘密。当然，无论是我们的平台还是产业的其他部分，都还有很多工作需要完成。你不能指望你的父母会坐下谈论并理解此事。对他们来说，这应该被期望是一个使他们的生活更容易而不是更难的工具。”

另一个关键区别是，跟比特币和莱特币使用工作量证明机制不同(该机制的系统难度与网络哈希算力成比例。例如，网络账本新增的哈希算力将提高区块难度水平)，NXT使用一种被称为“锻造”的机制，这基本上是NXT的流通机制（股权证明机制）。“Uniqueorn”意到，“股权证明机制可以让‘矿工’在不需要像其他加密货币一样使用大量电力的情况下产生NXT。”换句话说，进入门槛大大降低了，因为用户不需要使用第七章将要提到的那种顶尖ASIC机器。因此，用户可以在智能手机、太阳能树梅派或者笔记本电脑上“锻造”代币。实际上，算法随机选取一个节点处理所有的交易，其他节点知道该节点是单一交易“锻造者”--这样，所有的错误的交易可以被撤销。所有参与这种“锻造”努力的机器都将按照他们所拥有的NXT比例获得奖励；因此，如果你拥有1%的代币，你就有1%的机会被选来锻造下一个区块。因为交易节点是已知的，这提供了更好的安全性，想要危害网络(例如，51%攻击)，需要控制约90%的代币。

我也和“Gravition”有过通信，他是Nextcoin.org社区的创始人。据他说，核心团队决定“超越”比特币的动机之一是，“一种基于全新基础代码、抛弃消耗昂贵能源的工作量证明机制的技术先进的加密货币，肯定有需求。NXT拥有绿色环保并能抵御攻击的股权证明机制算法，加上它不仅仅是一个支付工具，而且是一个支持诸如去中心化交易和加密信息等成套服务的下一代新平台，这似乎可以填补现存守旧派加密货币所存在的明显缺陷。”

他也期盼着去中心化交易所以及彩色币功能在NXT平台上的开发，并且相信这些将“成为很多交易应用的流行标准，无论是对加密货币还是以其命名的资产。产业的其他部分将会无缝接入，所以不同加密货币品牌之间的差别将会消失。”并且，和其他几个接受采访的开发者一样，“杀手级应用将会在可能的范围内做到极简，使用单一加密货币钱包来按法币计量支付所有商家与服务，同时也通过该钱包来享有法币价格的增值，并且只要按一下按钮就能将你的钱包内容转化为另一种加密货币。对于移动设备的使用也更方便。”

以太坊

另一个引人瞩目的“2.0”项目是以太坊。该项目在2014年1月宣布启动，将带来加密账本和图灵完备的编程语言。简而言之，一个图灵完备的编程语言意味着该语言可以用来模拟任何计算机语言(不仅仅是其自身)。2009年发布的初始比特币协议与软件实现包括一个脚本语言，该语言有诸多限制（它被设计为非图灵完备的），因此远远没有得到充分利用。因而，开发者们不得不使用这个简陋的结构以在其协议上实现新功能。很多开发者，包括以太坊开发者，认识到了这些局限，认为与其构建和提供一套特定的功能组件，不如使用一个图灵完备的类似C语言的编程语言(CLL)。通过该软件，开发者就可以构建各种各样的工具，包括各种类型的智能合约、资产管理工具甚至一个去中心化自治组织(Decentralized Autonomous Organization， DAO)，这些都由以太坊账本执行、控制和审核。尽管该计划是迄今最具整体性的一个方案，但其长期成功仍有赖于大量的才智分享与网络效应。

为了获得更多以太坊的信息，我和Vitalik Buterin通了信，他是比特币杂志(Bitcoin Magazine)重要作者以及以太坊项目的首席开发者。因为“2.0”项目都具备保罗万象的能力，开发者们很难决定在哪个平台上创建他们的应用，但这不是仅有的障碍。在他看来，“我认为在2.0领域最主要的挑战将会是

(1)构建合约，

以及

(2)构建界面。

这些一直是问题，当然目前为止这两个问题没有其他一些更大的问题来得显眼，比如维护服务器架构和拓展性、保证资金的安全性、法规符合性以及与银行建立关系等。通过去中心化应用，这些问题的大部分将不会存在，所以只有这两个问题会留下来——合约设计与界面设计——现在摆在我们面前。这两个问题可以轻易地分开处理；某个人应该可以编写一个衍生的交易GUI(图形化用户界面)，并与以太坊、比特股以及任何其他人们想要在其上进行交易的不同系统自动对接。”

我交谈过的其他几个开发者和投资者也有类似观点：为终端客户创造使用简单、直观的界面将能很快使你的产品脱颖而出。尽管已经有了许多高级的、专门为商家定制的插件，但备份钱包与保障钱包安全等例行操作仍然十分笨拙，这些阻碍了对加密货币的广泛传播与接受。

Buterin之前在彩色币和万事达币项目上都工作过。尽管都是可迁移的，但这两者目前都使用比特币协议，这带来了一些局限。在Buterin看来，“比特币的关键特性之一是‘简化支付验证’(SPV)这一概念。仅仅通过下载与特定交易相关的相当小的区块链数据子集，一个比特币节点就能够验证一笔交易的有效性。由于现在一个‘完整’的比特币节点需要占据14GB空间来运行，这超出了很多用户的接受范围，该机制(子数据集验证)正成为比特币安全性必不可少的一部分。然而，那些构建在比特币区块链上的附生币协议的问题是它们不能从该协议中获益。比特币协议基础层无法获知一笔交易是否在附生币的设定里是有效的，所以比特币区块链将把有效和无效的交易都包含进去，因此附生币协议交易的有效性只能基于完整的区块链数据对整个协议进行重新计算来验证了。以太坊通过依靠一个新独立区块链取代附生协议来解决该问题。”

SPV是一种轻客户端，提供比特币用户一个轻量化方式来发送和确认交易，而不是携带整个数据库。它通过只下载所有区块头(例如默克树)而不是整个区块链自身来做到这点。由此，其灵活性可以使比特币客户端被那些可能没有足够空间或带宽来持续下载整个区块链的节点所使用。目前，正如Buterin提到的，完全确认一笔基于彩色币或比如万事达币这样的附生币的交易，只能通过重新检查整个区块链。这是对可拓展性的巨大障碍。

当描述和定义什么是一个“智能合约”以及“DAO”的时候，由于一个健壮的智能合约有时会被当作DAO使用而总是造成困惑。据Buterin说，“我想说两者之间没有清晰的界限，但其内涵意义有一些总体上的不同之处。对我而言，一个智能合约是单一目的并且短暂的，所以它为特定任务创建并且最终会消失。一份金融合约是一个好例子。DAO着眼于更长期的东西，并且包含一个内部AI(人工智能)来做决定。最后一点，去中心化自治组织是一个多人间的长期合约，其主要职责是保持资产并使用某种形式的投票系统来管理资产分布，甚至可能包括能够让人们签约或者交易他们的席位。可以有很多不同类型的DAO；比较基础的DAO完全活在区块链上；而比较高级的则可能将它们的数据储存在其他去中心化网络或是很多不同的服务器上。”

在本文的很多地方都引用了Mike Hearn的报告，包括其2013年图灵会议的报告。尽管Hearn和Vitalik Buterin使用同一个名词，DAO，但他们使用该术语时所隐含的定义却不相同。在一次电子邮件通信中，据Hearn说，“被Vitalik称作DAO的东西和我在图灵论坛上讨论的东西不太一样。我以前以为它们是相同的，但他把比特币本身叫做一个DAO，再更仔细的检查这种说法后，我认为这显然与我说的DAO不一样。假设你指的是机构，我怀疑会有很多的挑战很快随时发生。为使其运转良好，你真的需要可信计算。但在英特尔发布其支持SGX(软件防护扩展)的CPU之前，这无法良好运行，而英特尔甚至还没有为此宣布发布日期。”

在这本指导书里我对于没有任何精密内部AI组件的简单“智能合约”进行了描述。同样，对于DAO，我指的也是完全存在于区块链上的相对简单形式。随着程序员们越来越熟悉去中心化软件，以及技术发展及其实际应用的展开，每个术语的特定含义都将可能改变。

比特股

上文最后一点也被其他2.0项目的经营者看作至关重要的问题。我和Daniel Larimer进行过电子邮件通信，他是比特股的创造者，并且是第一个将比特币描述为去中心化自治公司(Decentralized Autonomous Company，DAC)的人。比特股是对加密货币的新视点，这一视点将你的钱包余额看作股份而不是货币。Larimer认为，可以把比特币看作一个DAC，其中每个比特币代表了在比特币生态系统中的一份股权。比特币交易费可以被看作是比特币系统的收入，而挖矿奖励则是比特币系统为保障其网络安全支付的费用。

Larimer决定将类比从货币改为股份，从而在设计下一代加密货币系统的时候可以考虑基础经济体系。基于这一类比，他把比特币看作一家公司，看到了很多比特币可以改进的地方。在他看来，首要原则是所有的公司都应该通过最大化产品销售收入并最小化花费来产生利润。

就比特币来说，主要的花费用于安全性，该安全性由第二章描述的昂贵的工作量证明机制(proof-of-share, PoW)保障。在他看来，一个股权证明机制(proff-of-share, PoS)(也被NXT所使用)可以被看作由股东对有效交易账本进行投票。通过这个方法，那些拥有该系统的人保障系统安全，而不是不得不花费越来越多的大量资金来做比攻击者更多的工作。Nicolas Houy最近描述了最后这点。他是法国国家科学研究院(CNRS)的研究员，他说道，“比特币矿工加入了一场算力军备竞赛。最终，大量的硬件、工程资源、能源被用于解决人为制造的极端复杂的数学计算问题。”股权证明系统有望去除这些人为的复杂性并降低资金成本进入门槛。

比特股系统做的另一件事，据Larimer说，是致力于增加进行交易的价值，由此产生额外的交易费。因为不需要向矿工支付费用，可以把交易费看作系统的利润，这些利润用于买回和回收股份。这使得仍在流通中的股份价值因此增加。从经济角度讲，这类似于获得红利。从交易费中得到的价值将按持股比例转移给股东。

他的团队正在开发的第一个比特股系统，名为比特股X。比特股X还是使用公司概念，实现银行及交易所商务模式，通过由区块链支持的一套新交易方式定义该模式。Larimer认为，比特股X的一个独有特性是系统内没有金融机构、雇员、金库或者合约。而据他说，美联储凭借抵押物发行美元，通过同样的方式(抵押发行)，比特股X可以发行比特美元。

比特股X在系统内使用股份作为抵押物以背书比特美元。可以把比特美元看作一种你能以一美元的价值按比特股X股份计价出售的资产。取决于你买卖比特美元的时间，你会得到不同份额的股份，但基于其初始模型，其购买力应大约相当于一美元。并且，他认为，就像比特币没有发行人背书其价值，比特股X的股份或者比特美元也没有发行人。整个系统的运行只不过是基于遵循一组由网络共识强制预设的规则所组成的数字链。

Larimer也相信比特股X只是众多潜在的、可被软件完全定义的商务模型之一。尽管他的团队也看到了包括保险、域名、博彩、拍卖、投票等其他商务模型，但挑战之一是寻找同时理解经济学和共识机制的开发者。投票是另一个其他该领域的创业者也已着手的问题，我们将在第八章NGO段落里详述。

我也跟Charles Evans交谈过，他是Invictus(运营比特股项目)的经济顾问。他这样看比特股：

“可以为农产品发行股份，例如咖啡、茶叶、豆蔻等等。种植某种商品的人可以持有相应的比特股，如果他发现比特股卖价可以比交付相应商品的成本价更高，那么种植者可以在交易所里提供比如100千克豆蔻换取100千克比特豆蔻，在公开市场上出售比特豆蔻，并将实物豆蔻卖给采购者。注意比特豆蔻不靠豆蔻背书。它在预测市场上交易，在市场上，来自全世界的参与者试图为一个大宗交易品发现单一的全球价格。当某人根据特殊的本地知识发现套利机会--买入比特豆蔻的同时承诺交付豆蔻，并将比特豆蔻在公开市场上卖出--市场可以发现机会。种植者可以利用全球信息市场为指导，而不是依赖自己的议价能力去和掌握更多信息的本地批发商谈判。同样地，如果比特豆蔻的价格持续上涨，世界范围内可能的种植者将会看见该价格并对价格信号作出相应的反应。”

合约币

我曾通过电子邮件和Ryan Orr交换看法，他在斯坦福大学教授全球项目融资和基础建设投资，他还是Zanbato的主席。Orr还曾近距离跟踪过合约币项目，那是第一个与比特币区块链完整集成的能够运行的协议层，支持点到点地传输合约币。一月初合约币开发团队宣布他们成功发布了一个能够运行的包括抵押资产发行、赌约、红利、可即时支取资产的协议以及世界上第一个去中心化交易所。

由于接下来的几个月里彩色币、万事达币和合约币以及其它的非区块链结构的竞争者如瑞波，OT(Open-Transactions，开放式交易)会带着各自的创新展开一场竞赛，许多外界评论员表达了对合约币与比特币的集成以及进展情况的兴趣。“我们有六个认真的竞争者这一事实说明了整个行业的巨大发展”，Orr说，“竞赛的早期集中于技术执行而后期将包含监管应对策略。‘价值网’（相对‘信息网’而言）最终就在这里。这些发展对于实际金融的未来的影响是巨大的--我们所见证的可能足以和在TCP/IP上发明http相提并论，那就是那些可能在未来支撑起价值网革命的协议。”

2014年2月我和一位首席开发者交换信息，他使用化名“PhantomPhreak”。据他所言，“合约币是一个协议，一个软件，它采用了比特币基础技术并将其扩展到简单的支付功能之外，实现了多种类金融工具。它可被用来与其它合约币用户进行安全且匿名的，完全无需中介的加密货币交易、资产创造、赌博等。它建立在比特币区块链之上，所以简单而且可靠。它的开发将非常快速，并且已经被设置了一些特性。合约币继承了比特币的安全性和可靠性。如同协议本身一样，它是开源的，它的发行是完全去中心化的。并且正如名字本身所揭示的，实现了一个完全分布式的、自动的和确定的票据交换所，所以对绝大多数交易来说，没有交易对手风险。当然，如果某些人使用合约币发行了他无法兑付的欠条，协议的匿名特性只给予了利益受损方很少的法定追索权。

最后一句尤其令人关注，因为它显示了一个目前还未用去中心化方式解决的问题，正如Preston Byrne在第二章指出的那样。随着这一领域的成熟，开发者将需要学习怎样去构造在法律上和商业上有用的智能合约。如何使这些条款在缺乏一个基于第三方履约保证的DAO,，缺乏一个独立的调解人或者缺乏一个信誉系统（例如信用积分）的前提下具有强制力，可能会很复杂，但也为相关领域的富有经验的专业人士提供了在加密货币行业展示自己的机会。一位来自合约币竞争对手的开发者告诉我，“合约币在这场游戏中已经领先，因为他们的分布式金融系统已经部署。在许多方面，这个团队都让人想到中本聪：他们是社区中那些看到以前尝试中的问题并致力解决的人。其他人在准备和观望，但真的需要发布能使我们走得更远的功能。还有，PoB（Proof-of-Burn，燃烧证明机制）是一个巨大的承诺并且提高了每个人的股份，这就是为什么有那么多和合约币同时进行的开发活动。投资者必须致力于让币工作，他们也确实在努力。他们发布了alpha版的软件，人们也在烧钱，然而他们每天都在更新代码，这意味着软件越来越好，市场也越来越活跃，这是一个令人兴奋的领域，这种层次上的竞争激励着我们每个人把产品提升一个档次。”

PoB是一种独特的分配“稀缺资源”（代币）的方式，不同于比特币、莱特币、狗币等加密货币采用工作量证明方式来分配稀缺资源（例如，代币），燃烧证明要求矿工（或者事实上任何用户）把比特币等代币发送到一个可证实无法花费的地址（一个终结者地址）以确保永远不会被任何人接触到。首次也是唯一一次燃烧在2014年1月2日开始并且持续了30天--现在所有将永存的XCP都被创造出来了。这段时间内，2130个比特币被有效率地毁灭了，市价折合约200万美元（实际的影响是其它的比特币持有者获得了0.01%的净收益）。合约币自动地将“烧掉”的代币转换成了自己的货币单位--XCP, 这一过程没有任何预挖或者创始人股份。现在创建你自己的资产需要花费5个XCP，作为一种防垃圾功能，这5个XCP被毁灭掉。虽然备受争议，PoB的确去除了公式中的人为因素。这就是说，尽管其它的“2.0”项目在典型情况下采取IPO的方式来募资，然后其资产（通常）被一个非盈利组织管理，因为仍然有值得信任的第三方介入，滥用依然可能发生。这不是说有什么滥用在发生，而是说合约币用一个不同的，但依然和中本聪在2008年用过的方法数学上类似的方法重新解决了拜占庭将军问题。

“PhantomPhreak”也看到了其它去中心化平台的潜力，“我想这里有一个非常好的机会，所谓的第二代加密货币将在大约明年起飞。比特币在许多方面都是一场革命，现在是时间对其引入的概念和范式进行一场革命了，可以说，计算机科学必须赶上来。一个安全地，分布式的区块链可以用在远较简单支付广阔的领域：高级金融工具（以合约币的方式），通信协议（如Bitmessage，Twister）等。当然，将来的金融会比今天更加去中心化，经济作为一个整体也必须相应地改变。”

Bitmessage是一个能够让用户以去中心化和无需信任的方式发送加密消息给任何人的点对点协议（即，用来发送信息的比特币协议）。Twister是一个使用比特币和BitTorrent协议的加密的去中心化点对点应用，能够让用户匿名地推文和沟通。这个领域内的其他项目有Bitcloud（去中心化云服务），Maidsafe（去中心化的dropbox和API平台）以及

SyncNet（去中心化网页浏览器）。

另外，他相信金融工具设计者可以为这一领域，尤其是合约币贡献出许多应用，“最明显的可能的贡献是简单的新特性。举例来说，目前合约币只有两种不同类型的‘赌约’，被简单地命名为‘平等/非平等’赌约或合同以示区别。然而，合约币有潜力实现几乎所有可为金融行业专业人士所用的工具。当然，通过一些例如为参考客户端编写用户友好的接口，或者算法交易引擎的方式，几乎任何一个开发者都能为合约币项目贡献良多。”

我也和开发团队的另一个成员“cityglut”交流过，谈到商业机会时他的看法是，“加密货币一般性地考虑到的、合约币特别考虑到的、可证明最有意义的是进一步的去中心化。我相信在合约币方向投资的资本将拥有他们至今不曾拥有的机会。”如上所述，这个项目整体上已经发布了正在被社区使用的代码。

他还看到了许多充满吸引力的成功机会。他说，“按照我的想法合约币现在最明显缺乏的金融工具是真正的期权功能。合约币有双重（平等/非平等）赌约和（分布式的）资产发售功能，我相信这些功能的组合会创造出充分的期权功能，但这可能在当前合约币的实现中是不可行的，即使无法由合约币的当前功能中构造出期权功能，在我看来用某种方式在合约币中实现期权功能依然是可能的和值得期

然而这里依然有挑战，“合约币的全新功能使得用户在使用的时候需要非常谨慎。因为任何人都可以创造资产，任何人都可以广播开赌约，用户必须尽己所能以确定他们正在购买的资产是合法的以及他们要参与的广播赌约是没有猫腻的。为了让前者更加易行，我们最近为每一个资产添加了一个‘描述空间’：资产的发行者可以为发行的资产加入最多42字节（UTF-8格式）的描述。至于广播，除了财务激励使得‘喂食操作者’（即，收取赌博交易费用者）必须保持诚实之外，我们设想一个（即便是非正式的）信誉系统会自然地出现，帮助用户确定哪些地址的广播是可信的而哪些是应该回避的。”

第二个属性，一种描述空间，是许多平台都致力实现以组织和管理各种不同资产的特性。信誉的问题也是被许多其它投资者、开发者和专家反复涉及的主题，一个DAO履约保证有潜力解决此问题。

开放式交易(OT)

Chris Odom是monetas的联合创始人和CTO以及OT的首席开发者。OT是使用现有技术通过“盲签”等私密特性实现无需信任的密码学金融交互的开源数字软件套装。它轻便并且无需知道账本细节，允许开发者将其应用桥接到其它加密账本上。

许多外部投资者和商业机构反复地问Odom同一个问题，在这个领域能开发出什么样的商业解决方案？然而对Odom来说“问加密货币领域有什么商业机会如同在互联网领域问同一个问题一样。这个领域极端宽广。我想我们是在讨论一种革命性的发明，可与电力，计算机或者互联网相比。它将创造出全新的领域，并且将改变所有现存的行业，虽然现在OT是与比特币集成的，因为它是一个财务加密库因而是与账本无关的，类似于OpenSSL是通信加密库。说到当下的机会，我们在CIYAM.org/open发布了一些悬赏。然而，人们绝对应该意识到风险，加密货币可以以合法和非法的方式使用，所以关键不是加密货币本身，而是如何使用它。你只需当心监管合规问题，而且如果这个问题变得非常麻烦，你必须考虑把你的公司移到另一个国家。一些国家比另外一些更不自由。对一个投资者我会指出一些关于OT的特有的方面，一个是它以低信任度运行的能力，它是联结的。以及它能够完成比特币世界里所有服务器，如MtGox服务器，Bitstamp服务器，或者任何用到服务器的比特币服务所能完成的，并且弥补它们的不足。它们中的每一个都可以被一种低信任的方式取代，至少使用OT，使用OT作为财务引擎，无需网页GUI组件。

OT优于有算法延迟的传统区块链的一个地方是，因为它使用了服务器，用户可以进行几乎即时的交易。而比特币，比特股以及其它基于区块链的工具的确认时间都以分钟计，用户只能在这样的时间间隔内进行交易，如果你能把OT置入一个分布式数据库，理论上就能拥有即时确认并且不附带中心控制的加密货币。

瑞波

由瑞波实验室商业化的瑞波是一个包含可用于包括比特币在内的任意数字货币的支付平台，去中心化货币交易所，智能合约网络的支付协议。瑞波提供了一个通过“受信任的”网关实现资产云的解决方案。瑞波和类瑞波系统可以提供即时的流动性和交易对手间的交易，可以是无需信任的第三方间的交易，并且这些第三方可以决定在网内去哪里结算他们交易的资产，例如任何一个为代理的资产提供兑付的网关。另外，不同于其它使用各种工作量证明机制的支付平台，瑞波使用了分布于全球服务器网络的共识账本。这些服务器持续地从其它网络上的服务器接收交易和建议并将其编译进一个“唯一节点表”（Unique Node List，UNL），发自不在网络中的服务器的建议被丢弃，同时其余的被服务器审查并按一定算法进行“投票”，当一个共识（定义为80%赞成交易合法）达成时，服务器确认建议，关闭账本并生成“最后关闭账目”（类似区块）。此过程周而复始，花费大约五到十五秒的时间，比所有基于工作量证明机制的系统都快。瑞波网络每月总共处理大约来自68000个用户账户的2000万美元交易。

从去年开始，瑞波实验室创造出了初始的一千亿XRP的货币供应，这被确定足够维持几百年。瑞波的设计者认识到如果一些人制造出大量的无用交易，就会形成阻塞整个网络的垃圾，为了解决这个问题网络收取三“滴”XRP的交易费用。每“滴”等同于XRP的最小可能单位，这样每笔网络交易的成本是.000003。一滴类同于比特币的“聪”--比特币的最小单位0.00000001BTC。本文写作时已有超过3500 XRP永久性地从网络中移除了。

Jon Holmquist是一个早期的比特币用户和瑞波实验室的社区联络人，按他的看法，“从15年前开始，一个商家就能在10分钟内开一个网店并且吸引来自全球用户的目光。然而，直到5年前用户都无法容易地支付给商家。随着比特币等加密货币的发展，消费者现在可以跨国界地使用货币。然而现在最大的问题之一是如何获得比特币，尤其是对哪些居住在经济欠发达地区的人们来说。瑞波让你能够交易和获取任何你想使用的货币。随着瑞波持续地发展合作伙伴关系，网络创造了一个自我维护和强化的正反馈环。作为结果，因为比特币受到了许多推动，在每个国家有一个允许用户最终从任何国家用他们自己的货币购买的法币交易所是可能的。”

基于数学的货币是一个经常被瑞波实验室的成员用来描述“可编程货币”概念的术语--即，用算法进行数学约束并且难以--如果不是不可能--伪造的虚拟代币。通过使用户能够使用XRP，一种代币，代表特定的能在全球范围即时传输和与比特币及法币交易的金融工具（例如货币），瑞波支付系统和比特币

Steve Bennet，圣何塞州立大学的金融学教授以及CrossCoin资本--一个与瑞波实验室合作的新业务孵化器--的天使投资者，指出这一项目已经“创建了一个以后会成为构建瑞波生态系统的加速器的新孵化器。目前我们致力于吸引比特币相关公司，这些公司可以为瑞波平台带来资本并为全球客户带来新的价值。” Bennet的团队（包括上面提到过的Ryan Orr）计划与新成立的及已有公司合作，为他们提供瑞波管理的访问乃至用瑞波交换一部分资产，如同一些2.0项目已经做的那样。（例如万事达币，未来币）。他的设想是为孵化器融来资源（例如网络，创业导师，法务）并帮助被孵化团队集中精力为一个更广大的并不熟悉加密货币的用户群体提供增值服务。

我还和Stefan Thomas聊过，他是WeUseCoins的联合创始人，bitcoinJS的创建者和瑞波实验室的CTO。在他看来，“现在最容易的描述瑞波的方法就是把它描述成一个移除了大多数中介并且秒级交易的外汇交易市场。并且因为减少了汇款过程的总费用，用户需要担心的汇率波动的幅度也变窄了。这就是说，过去，资金逃离可能贬值的边界的时间是以小时或天计算的。”而如上面所提到的，瑞波平台是几乎即时的并且由账本处理器（有点类似“矿工”但只需很小规模的架构）和网关构成的分布式网络支撑。

而且按Thomas的看法，“虽然处理器节点就像矿工一样选举并核实账本正确性以防止伪造和双花，这些处理器和区块链上用到的矿工不同，因为确定共识的‘轻’方法只需要非常轻的架构（例如，无需ASICs或GPUs）。账本的共识是通过互传方法达成的；类似于互联网中的互信节点的互传方法。账本本身是一束在网络中传输并经客户端（节点）选举的数字签名交易。这些节点互相投票来看哪笔交易最先到达，被确认虚假的或者不合法的交易被丢弃，其余的都会被包含在验证过的账本中并等待关闭。整个过程花费5到15秒的时间，因为欺骗而变得不可靠的节点会被其它节点忽略。时间间隔不固定因为交易束不仅大小会变化（例如消费者的消费行为并非是一致的、平滑的）--而且也表明了数据本身是如何通过目前的公共网络架构处理的。相反，VISA稍快的原因是他们使用私有中央节点，这需要高得多的管理费用和资本投入。”

“网关是资产进出瑞波网络的实际组织。从个人到大银行都可以成为网关。用户建立对可以位于世界任何地方的网关的信任路径，提供了对几乎所有本地货币的流动性。网关的一个特点是，当出现一个传统意义上的‘单点失败’时，用户依然可以获得绕过失败网关的路径。此外，网关不能占用某个特定用户的资产：无论他们拖欠每个人钱还是完全没有债务。所以例如，Bob可以借钱给被信任的网关Alice。网关靠信誉生存，所以有去尽自己义务的激励。Bob然后可以拿本地货币向Alice交换IOU(XRP)，然后把XRP发到另一个网关去交换本地货币。这个过程的时间消耗可以是秒级的，比任何基于块链的系统都快得多，而且事实上更安全（51%对80%）。”

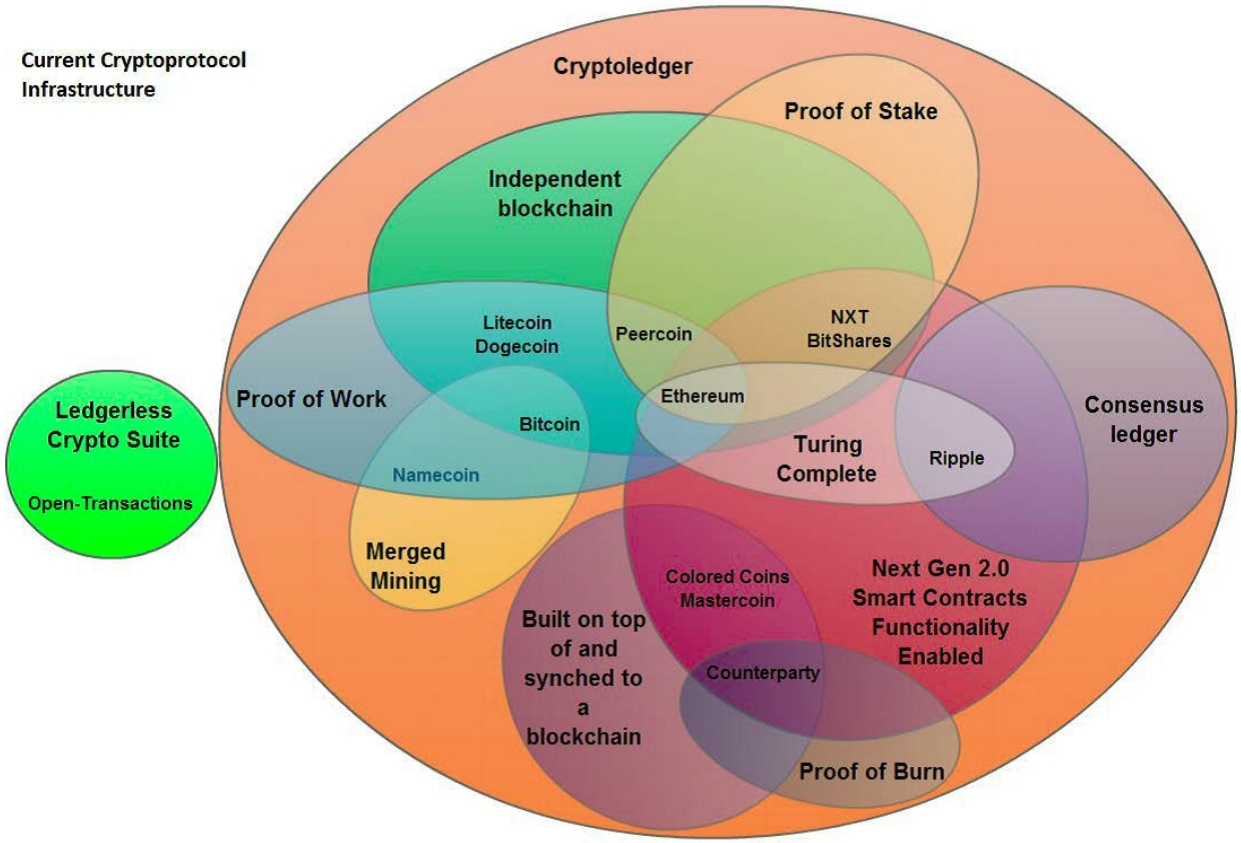
瑞波实验室把他们的技术称之为“价值网”，一个“金钱互联网”，以及“钱的http”。现存的金融机构可以在今天通过建立“信任路径”来扮演网关的角色。网关系统可以让金融机构交易数字化的资产（如商品，法币）。例如，Bob的布法罗银行可以建立网关并且与Alice的中国农业银行建立信任路径。Bob可以提供美元流动性给Alice而Alice可以提供人民币流动性给Bob，比现存的要花费数天并且收费高昂的连线服务更便宜也更快（5到15秒之间）。瑞波扮演所有参与者信任的账本的角色，然而现金余额必须在瑞波协议之外清算。XRP是网络的唯一原生货币。

Thomas继续谈到，“瑞波协议相对于本领域内其它竞争者的另一个优势是我们的代码使用了最少的可信的基础代码，提供了最安全汇编代码给对方（例如直接与焊点，与半导体金属互动的）的OP代码。这样本地客户端就更不易被高级语言层上的行为攻击。在过去的两年中我们公开了大量的包含协议的基础代码。这又带来了更多的改良和安全性修复。而且，我们继续寻找扩展协议用途的方法，使账本从根本上成为一种允许智能合约交易的数据库。因为网络比大多数其它平台略高效，使得创新可以不断发生。”这一基于合同的系统将是图灵完备的并且分为两个阶段，第一阶段是非确定的，将使合同能与现实世界的协议如DNS和HTTP交互并且允许用户包含语言解释器和参考库。

“这个领域的进化很快；例如，最初的比特币客户端比今天的笨重得多。首次使用常常需要花费24小时去下载区块链和确认交易。现在有无数的项目致力于提供增值服务并且这种竞争推动我们审视创新的新方式，例如对等辅助秘钥引导功能（peer-assisted key derivation function，PAKDF）--一种使用盲签的数学方法。这个领域内推广应用的问题之一是难以记忆长的安全密码而新用户在学习如何安全地在磁盘上存储密码又常常倍感挫折，PAKDF允许Alice使用相对弱的可以发给Bob的密码，Bob将在不知道因而也无法破解Alice密码的前提下对某样东西（例如某合同）签名，这被称为盲签，它采用了同型加密的形式，我们将其集成到了瑞波中。”

虽然用户需要记住长密码，这一关于安全对密码签名的特殊应用可以给最终用户带来便捷。简而言之，一个盲签模式“允许一个人通过另一方获取信息并不透露任何信息给另一方。”通常用来描述这一过程的而例子是，Alice把一条消息写在衬有复写纸的信封里。信被发给Bob，Bob看不到任何信息，但可以从信封的外面签名，签名会写到信封里面的复写纸上。

当前加密货币架构



这个欧拉图表示的是两个主要系统，一个是采用加密账本形式的系统，另一个不是，那里只有OT这一个例子。如前面章节所述，OT通过将其OTX协议连接至比特币等其它服务工作,因而是与账本无关的。

在加密账本部分从根本上来说有两个不同形式，使用区块链的和使用共识账本的。本文写作时仅有的使用共识账本的是瑞波协议。初创时，域名币也使用独立区块链但其挖矿过程后来与比特币合并了。另外一些独立的区块链包括莱特币，狗币，未来币，比特股和以太坊。本文写作时，以太坊团队尚未决定使用何种验证机制--可能使用一种类似点点币使用的混合机制（工作量证明机制和股权证明机制）。

工作量证明机制（PoW）最初由比特币在2009年开始采用，它包含一个矿机组成的网络。计算机们解决一系列难度逐渐提高的良性数学问题从而避免了无赖的攻击。以上的例子中，莱特币，狗币，域名币，比特币都使用工作量证明机制。以太坊也可能会。

股权证明机制（PoS）的不同在于一个区块的交易节点被随机地赋予与之直接通信的网络参与者。这种方法的一个优点是它大幅度地降低了维护网络安全所需的哈希算力。本文写作时，只有上图中的NXT使用了纯PoS机制；点点币使用了混合机制，以太坊也可能使用混合机制。

PoB 是迄今为止只有合约币使用的独特方法；一个用户发送代币（比特币）到一个被证明无法花费的地址（终结者地址）。这种方法的最大好处是无需可信任第三方或监管者去照看“IPO”资产。

里面红色的图表示本章所描述的智能合约特性，虽然比特币协议能够令人信服地使用这种合约，这种功能并未被开发团队“打开”（0.9版将允许80字节包括分布式合约哈希值的哈希值）。虽然有很多将提供这种功能的平台，一个BitPay研发的名为bitcore的基于bitcoinJS的临时解决方案将在第7章中介绍。其它提供或者很快将提供智能合约功能的平台包括彩色币，万事达币，合约币，未来币，比特股，以太坊和瑞波。

在比特币区块链上开发的项目包括彩色币、万事达币和合约币。一些其它的项目如Peercover（将在第五章讨论）已经让合约币能够和瑞波网络桥接。

虽然以太坊和瑞波被归类为上述平台中仅有的图灵完备的加密货币，需要注意的是以太坊还未发布但预期在未来六个月内发布。另外，未来币和比特股有望在未来的某个时间点包含相似的健壮性，如果不是完整的图灵完备功能的话。

一个没有在上图里划分出的大类是“山寨币”。严格地说，任何非比特币的币在早期都被称为山寨币。除了OT之外，所有图中的币都被一些人称为山寨币，然而，这种态度掺杂了个人偏好和政治，所以最好忽略。

第四章：智能财产

自从2009年比特币创世区块产生后，比特币发烧友和专业交易者们，都在进行无需信任的资产管理，但其实涉及的资产类别只有一个：比特币，且直到不久之前，比特币交易所实际上还都是不受监管的。下一个进化方向将是使用数字密码账簿来追踪、管理和交易智能合同，甚至智能资产。

根据尼克·萨博的说法，这过程中，最容易实现的部分是合同，而合同的99.9%都是“干”代码，干的意思是代码已经形式化，并且能够通过软件自动执行，而极少需要人工干预。

这部分几乎可以涵盖，现代电子化交易所交易的所有有价证券和金融工具，包括NASDAQ 和 Euronext（泛欧交易所，含NYSE纽约股票交易所）。而其中有一些颠覆性特性，会影响到金融机构中的中层管理人员，甚至全部从业人员，因为他们既不能编写代码，也不能给这样的合同提供额外的解释，由于分布式加密总账的存在，他们的审计、对账这些工作就显得很多余。

虚拟的数字化资产和金融工具，可能相对比较容易想象，因为很多读者，都有直接转账接收工资，使用第三方支付（如PayPal，支付宝等）、在线券商（如E-Trade, Scottrade）等的经验，但智能合同如何与物理资产交互并实现控制呢？

通过适当的改良就形成了智能财产？

萨博是最早给这个交互难题提供解决方案的人之一，他称其为proplet。他在论文中写到，proplet的设计目标是通过数字协议控制物理对象。在他看来，proplet的功能能够通过一个微机电系统(MEMS)实现，这是一个有着很多微型传感器的装置，能够追踪所有权、确定精确位置和提供稳健的安全策略。今天大多数智能手机、平板电脑以及部分汽车都有不同种类的MEMS（微机电系统比如加速度计）。如果是10到15年前，说服制造商给他们的产品添加proplets是几乎不可能的。而今天物联网（如家居自动化等）的发展使得含MEMS（微机电系统）产品无意中已经传播开了。2009年Kevin Ashton提出的物联网这个术语是指通过一个网络化的结构能够唯一地识别和标记任何类型的物理对象的能力。通过现有的技术如RFID（无线射频识别）、NFC（近距离无线通信）、条形码、QR码（二维码）、数字水印等手段都能够实现。因此，如冰箱、恒温器、烟雾探测器、门、吸尘器以及甚至灯泡这些设备都能够植入物联网技术。根据BI-Intelligence的预测，到2018年，大约会有90亿设备接入物联网，远远多于所有智能手机、智能电视、平板、电脑和可穿戴设备的总和。但是需要注意，仅仅因为包含了wifi功能的灯和门可以是自动的甚至是自主的，但严格意义上来说，它们也不算是智能财产，因为所有权和控制权还不能够通过智能合同自动转让给另一方。

如果一个物体不仅有物联网功能，而且有proplet功能，那么它就能通过数字协议乃至相应的智能合同来管理。事实上，萨博在谈话中表达了类似的观点“尚未注册但拥有足够转售价值而能作为抵押品的设备和电器，很适合使用新的P2P所有权注册方法及内嵌proplet或类似的方案”

萨博和其他人都会考虑的一个普遍问题是物流：如何通过合约远程控制一个物理对象。在萨博就这个问题最早发表的文章中，他用了汽车租赁和智能抵押协议的例子。汽车租赁的智能合同应该包括一个涉及时间锁（时间锁也是比特币中使用的一个术语）的扣押权条款。在这样的合同中，如果承租人不能按期偿还，智能扣押协议就会被激活，从而阻止了汽车的使用，使得债权人（和回购公司）能够拿回汽车的控制权。当然了，这类条款也应内置一定的宽限期甚至操作例外，比如当汽车正在高速公路上行驶时不激活扣押。

由Vitalik Buterin最近抛出的另外一个例子是博物馆门票。用你手机上的NFC功能结合彩色币或者比特币本身，假如你拥有一单位的币，你可以通过私钥给附加在门票上的短信签名。你买了一张博物馆门票然后你就能在门票上进行数字签名。如果你想把门票转让，你只需要将虚拟币转移给别人，那么他们就能通过他们手机中的私钥对门票进行签名，门票所有权就转让给他们了。另外再比如，假设Bob管理了一个先租后买的店铺，他就能够对电器商品使用某种“proplet”，以便于他管理所有权的借贷关系实现债权人的所有权（例如，租客没有为电视、冰箱或者游戏机支付当期租金就会导致电器自动终止服务。）

除了这一凭借药房自动化、工厂自动化、自动驾驶和语音识别技术的边际进展，在什么能做和什么法律允许做之间仍然有着一条鸿沟。

尽管药房自动化、工厂自动化、自动驾驶以及语音识别的技术一直在缓慢推进，但在什么能做和什么法律允许做之间仍然有着一条鸿沟。

然而，根据萨博所述，实现这个并没有太大的技术障碍。更主要的是学习有关技术以及对其实用性有足够信心，从而进行较大的资本投资如硬件（而非仅仅是数字货币和所有权登记等软件）。最大的障碍可能是与现有产权制度同步或者取代它。并不需要特别困难（艰深）的新技术，但是当涉及到已经登记的财产的时候（例如在美国各州登记的汽车所有权），两种注册方法之间必须同步，否则该州必须切换到使用区块链来作为注册登记的系统。呜呼！当然会涉及到大量的行动缓慢的官僚机构和政治斗争。

由于在发达国家所有权的登记已经相当成熟，所以这套系统替换现有所有权更可能先出现在发展中国家。在发达国家，区块链所有权技术最初可能主要用在金融工具和合同上。（当然，最先已经应用于存储和转移货币本身的所有权）。此外，尚未登记但拥有足够转售价值而可以抵押的设备和器具，很适合使用新的P2P所有权登记方法及内嵌proplet类似的方案。在汽车的例子中，这就意味着必须说服各州的机动车辆管理局来使用一套电脑系统，这套系统所连接的数字账簿或者数据库可以用来转移车辆所有权。

这可以通过现有的技术来令人信服地完成。然而，如果过去五年密码学货币监管的不确定性以及风险有任何启发的话（如反洗钱法，了解你的客户原则，货币转账许可证，资金服务业务等），不大可能看到，所有类似机动车辆管理局这样的机构，马上采用此方法，并允许诸如汽车（房子或者证券）这样的资产，直接交易，而没有税务或监管。

如果一个正被使用的数字账簿被矿工拒绝，智能合同会怎么样？例如，维持一个一次性的工作量证明数字账簿，在资源利用上不一定是最佳的（见第八章讨论）。如上指出，你可以使用比特币（或者山寨币）网络的共识挖矿算力，来跟踪和管理几乎所有类型的资产。就资产比哈希率而言（单位哈希的资产数而言），只跟踪一个并不是最优的。但假设Bob为机动车辆管理所，创造了一个单独的数字账簿，用来定位和追踪注册过的车辆，如果基础账簿在一两年内，失去了所有的矿工会怎么样？如果矿工放弃网络，账目不再有效，车辆的所有权可能被伪造和无法追踪。该问题的解决方案很可能是，使用数字账簿的智能合同和分布式自治组织代码库，因其开源而便于转移。因此，你可以创建或者编译智能合同的其他副本，并将其放置在多个备份账簿上。也就是说，复制一份或多份智能合同到其他账簿，花费的开发成本是最小的。主账簿或者备份账簿由州政府负责管理和挖矿，电力开支也会以税收形式转移到公众身上。

企业家还有其他的机会，制造防伪和抗干扰的集装箱，内置智能财产元器件（NFC，MEMS），使得用户能够近实时地追踪包裹。

那些工业设计顾问，也能够协助那些想将proplets嵌入产品的企业找到新机会，之后，就能够无意间实现如Richard Brown去年秋天开的玩笑：在区块链上，没有人知道你是一个冰箱。

纸张与电子化的相遇

智能合同成长在一个建立在基于纸质合同控制上的年代，通过将不同的任务委派给不同的、并不完善的代理商来防止错误、欺诈和滥用。例如审计人员可以将仓库功能中的送货、销售、收款及财务核算分给不同的部门。根据萨博的说法，这种隔离式方法中，如果想欺诈和滥用，必须在不同部门之间进行合谋。然而，在一个无纸化的数字时代，很多这些功能都显得多余，因为这些功能能够被一个分布式的数字账簿实现并可以避免被滥用（没有相应的数字密钥）。因此，这就需要更智能而不是更严格的控制。这样的控制将通过智能合同明确交易每一方的关系、职责和责任。不论公司大小，这都将改变公司内传统的层级和组织结构，使得扁平化组织成为可能。而通常情况下，越是扁平化的组织，决策者层级就会越少，信息延迟也会越小（例如能够去除一些信息不对称）。

随着CRM、ERP和其他先进的会计、审计和人力资源软件的出现，压缩了管理成本，这些层级和组织上的变化在过去的20年中一直在加速。然而，他们在信任方面提出了新挑战。例如，会计师事务所、投资公司和咨询公司的并购，使得受托责任和问责机制变得界限模糊。萨博说，随着会计师事务所利用了大量的内幕和市场信息，信任将会进一步削弱。就像精确的钟表一样，每年都必然会有大量的调查报告详细描述内幕交易、密级信息泄露和擅自执行交易这些案例。

Turdgison将军关于“R计划”（该计划意在绕过授权机制和命令层级，单方面的扔下核弹对付苏联）的名言总结了以上困局：“人的因素似乎在这里失败了，但我们不能就因为一个失误就来谴责整个项目”。闲言少叙，书归正传。即使没有内部人员的蓄意滥用，外部人员仍然会像Lulz安全黑客组织公开展示的那样，通过社会工程学获得敏感文件和信息。可能在一个以比特币和基于Ripple的数字账簿加密解决方案时代，大企业不仅能够管理关键文件的访问权限（避开Alice和Bob的窥视和刺探），还可以通过proplets轻松的管理物理工厂、校园甚至一个汽车车队。甚至可能会诞生很多加密恢复咨询的商业机会。

缓慢演进

二十多年前，汽车制造商成了现代电子数据交换(EDI)标准的前身。EDI是一个文件标准，它将纸质的商业表格变成了电子化表格后，成为多个计算机应用的公共接口，使得应用之间能够互相理解文件的含义。通过使用标准化的标记、语法和术语（例如XML），企业可以快速廉价的将结构化信息传输到其他兼容系统，使得整合更为密切。例如，制造商可以将文档无缝发送给其他供应链厂商。汽车和航空航天公司率先实施了这一项技术，他们用电脑系统将一些原本需要密集的手动操作、容易出错、时而占用系统的操作变成了自动化。

多年来，EDI已经发展到容纳了几十种形式，例如产品和价格目录、采购订单、库存状态更新、发运单、报关单及收据等。咨询公司、会计师事务所和律师事务所也已跟进这一潮流，利用ECRS和LEDES软件包将管理、账单和成本回收系统自动化为一个标准化的文档格式，这些软件包已成为任何一个规模化企业的行业标准配置。供应链业和航运业都在通过云计算服务与技术进一步融合。例如，在2013年10月，英迈收购了Shipwire这家云物流与供应链管理提供商。同月，Pacejet物流筹资450万美元试图将物流服务和UPS这样的运输公司通过云服务建立连接。

尼克·萨博做出了开创性工作，在这里我就不复述他的文字了，我建议所有对智能合同有兴趣的读者看看他的开创性作品《公共网络中关系的形成与保障》，其中有更多非常详细的论述。

虽然萨博提出了非信任系统的全局性视角，但我们应该注意，他的观点只是一个计划，一个有远见的计划而已。在未来几年内，无信任资产管理这个概念会受到很多假想的和现实世界场景的挑战，当然也会有很多著作。不得不提到的是，虽然区块链很强健，但有很多授权与之交互的系统是脆弱的，会受到黑客的攻击。假如，当Alice智能手机或者笔记本上的数字密钥，被Bob攻破，并将受智能合同控制的汽车销售给不知情的别人，她是否有追索权呢。在理想的情况下，汽车和密钥系统的安全性能够有效阻止黑客攻击，但过去五年的实践表明，密钥本身是可以被丢失、盗窃甚至敲诈走的。（如数字锁病毒和云存储的非加密钱包文件被盗等）

在所有的可能性中，如Preston Byrne与另外的法律专家对这份文稿的看法，对消费者保护的市场需求，可能不仅会阻碍、甚至可能逆转去中心化的趋势。如Byrne推测，阻力会来自一些负责认证和反欺诈的中心化机构，这些机构可能是公司、也可能是政府部门。这种情况下，Alice可以在首次合法获得所有权时，便预先指定哪个机构或法院，有权作出相关决定（通过私钥的所有权和冷存储）。在假设有竞争的市场中，她也需要付出少量的一次性费用。同样，购买者也希望，能够验证他们购买的数字资产所有权转让是合法的，并不受任何第三方支配。因此，区块链将需要与其他的所有权验证方法匹配，这种方式会比很多国家和地区现有的所有权转让系统（比如国家车辆管理局）更加经济。如果Alice不想给第三方支付这笔小额费用，她是可以使用不受管制的区块链，但这时她需要记住这句老话：。买者自负风险。

理论是灰的

就像浮士德博士所发现的，尽管某些东西在理论上看来是合理的，“理论是灰色的,生活却是绿色的。”机构所遇到的其中一个问题不是它们不遵守规则，而是没有可预见的规则可以明确涵盖所有的活动。因此减少模糊的结果，它是程序员或是商人必须要进行的研究，并在设计一个聪明合同的阶段收集所有的需求。这将是具有挑战性的一个原因，很少知道今天分权自治组织的存在他们可能会面临各种漏洞和攻击,阻止他们执行他们的职责。在2013年图灵演讲会上,迈克·赫恩(比特币的核心开发人员)指出一点:现实理论要比创建它更加困难，因此在科幻小说和电影取笑我们的想象力看似聪明的人工智能代理,创建更简单的形式的非创造机器人将是一个艰巨的任务。

时钟与记录

在过去的一个世纪当中，存在着这样一种情况，处在不同位置的雇员可能会有不同的工作方式。根据不同的信任级别，有的雇员可能只需向老板打声招呼，而其他人可能需要在特定的笔记本上进行签名才行。而有的人可能需要通过使用“卡片”烙印时间戳的方式记录一天的行程（例如，当员工上班走进办公室时，享用午餐时，午餐过后以及下班结束时都会被烙印上时间戳）。在过去十年中甚至有雇主在雇员的电脑当中安装了跟踪软件，这样他们就可以监视到雇员登录网站或者确认员工是否坐在自己的办公桌上看着显示器，有些雇主就是想知道每台机器上所发生的事情。因此，当雇员登录系统后，这种软件可以记录下所有一天当中的输入数据（如网站访问，按键，文件），有些软件程序甚至能够随机抓取屏幕快照，如此便可确认雇员是否在填写TPS报告时偷看视频。有迹象表明，在那些旧系统上是可以进行作弊的。对于在时间片甚至考勤卡的情况下，即使你没去上班也是可以让朋友或者同事帮你代签。而随着软件的出现以及基于互联网的监控，作弊将变得更加困难，如果可能的话，在滥用计算机时千万不要让公司意识到该软件已被删除或者网络已经被黑。

再次说明，智能合约和智能财产的目的不是为了刻意塑造某种极权主义的“圆形监狱”，而是使各方能够明确自己的责任，义务以及报酬。正如我在本章前面部分所述，被边缘化的个人，如中国的农民工们因户籍制度（户口）在合同纠纷中将会出现求助无门的情况，如果说他们的合同不仅能够防篡改，还能以某种方式证明他们满足了合同义务，比如说现场的时间，那么他们将会获益匪浅。

而有些要求会增大编纂成一个智能合约的难度，其中比较容易实现的是旧时钟 “按键”。使用现有的系统有几种方法可以做到这点：使用一种电子标签标记或者手机里的近场通信芯片，“时钟”只需连接到任何机械或者网络，则最终会将肯定信号发送给智能合约或者分布式自治组织，并自动支付给他们。另一个例子就是使用生物指纹识别或者瞳孔扫描技术，以验证该雇员的“时钟输入”（或输出），然后该系统将连接到之前所提到同一机械。但是这也存在着限制：举例来说，如果雇员或者承包商收到一个计件工资活，或者全天必须要频繁地切换站点，比如不同的社区，校园，甚至城市。而创造一种防篡改的手机登记设备来替代掉那种不动的时钟跟踪计件设备将会是未来新的商业机会。事实上，用户可以通过比特币的微交易能力进行小额的支付，并用数字密钥签名的方式来证明他们是在一个特定的时间量中的一个特定热点。

分布式自律组织（**DAO**）

正如我在引言中所述，一个分布式自律组织是一个虚拟的人工智能媒介，它能够执行通常由经理和管理层人员所进行的任务，操作以及功能。比如说支付账单，发放红利，甚至首次公开招股（IPO）这样的事。而且这些工作能在无需信任或者说准无需信任的环境下进行。"这种无需信任状态的平衡"是由当事方的意图和代码的功能共同决定。 分布式自律组织通过使用一个完备的图灵语言来集成一个加密总账，其本质是防篡改或者防篡改实体，并免疫实体组织中很多的弊端和漏洞（如刨切，纵火，意外暴露于专用文档）。 目前并不存在真正意义上的分布式自律组织（也称分散自律机构或者自主代理机构），它们是依附于加密总账，虽然目前也有一些整合了边缘市场的人力资源软件工具（比如说Bitpay）。

一些分析师称，比特币本身就是一个分布式自律组织，因为所有的用户在技术上必须提交一个数字密钥的形式来进行表决机制，股东（矿工）能够收到他们工作的酬劳（铸币权）- 而且其本身并不存在行政管理。然而，由于比特币协议本身的发展方向并不由“投票”直接决定，比特币更像是一个试样分布式自律组织。

但是投票机制以及独立的个性并不是一种好的方式，就像瓦努阿图人装扮成士兵并深信航空货运计划会带来战时物资，实施投票以加密协议的方式并假设会创建出一个公司，这是一个相当肤浅的认识。因为比特币如何发展的问题已经是在比特币基金会的管辖范围之内，目前比特币的生态系统是"股东"和“利益相关者”系统之间的融合。长期来说这是存在着不稳定的因素的：受托责任的界限是模糊的,部分原因是它的资助（赞助）方式以及组织如何希望被外部察觉的方式。 此外，该网络存在被用户主动放弃的可能性；一个公司的运作离不开股东的投入。这并不是说基金会就不应该存在，或者甚至这个基金会没法从外部赚钱，那么用户会选择放弃这个项目或者网络 - 更确切地说，那是因为比特币持有人没有直接参与到投票过程（就像在一个真正的公司里），决策使得协议本身的实际方向并不是朝着分布式自律组织走。

去年秋天，隐私倡导者们反对新的“硬币验证”项目（比特币的白名单），随后他们朝着这个方向开始了黑暗钱包以及Zerocoin项目的研发。而核心开发人员却有着不同的看法，比特币持有人在参与过程中并没有用数字签名的方式进行直接投票。事实上，面对基金会成员所讨论的新硬币验证路线，Roger Ver所投资的Blockchain.info（由比特币开发者Gregory Maxwell开发）促进了比特币的分享，还是潜在的白名单和黑名单的一种解决方案。这并不是任何建议的一种担保，而是分布式自律组织用于平息这些行动的例子。

分布式自律共识平台（**DACP**）

垂直机构传统地创造了等级制度，而情报以及决策都是由顶层所引导的，以及基于人力领导的自动化功能。这种现象的例子是公司任意分割遗赠以满足某些度量，因而往往它们是处在网络的边缘的。低等阶的部门在这种情况下有时会被认为可替代的，或者有些则是缺乏其他部门可能拥有的政治资本（关系），而当比特币介绍了分布式自律共识的概念后，这种情况发生了剧烈的改变，这是一种自动化在网络中心，情报在网络边缘的的概念。

与传统公司里决策权都集中在行政级别的人物手中不同的是，在分布式自律共识平台（DACP）中，其决策权是部分自动化的，如此它便具有特殊的规则从而保证不产生偏差。在这种模型中，权力和权威并非集中在一个顶点，而是通过合法私钥持有人通过他们预先批准的投票权来影响分散自律共识平台的决策权，从而达到扩展到网络边缘的目的（例如，设立公司时，投票结构通常基于个人的股权或股份拥有量）。

一个分布式自律共识平台或者分布式自律共识的法律义务和责任仍然需要追溯到那些在分布式自律共识平台上进行数字签名的密钥持有人，然后根据预先安排的投票比例计算结果。例如，Bob的时装店要求由分布式自律共识平台分配的承包商专项资金必须通过数字签名的阈值批准。如果阈值未能满足批准，那么分布式自律共识平台将不会分配资金给承办商。

基于软件的解决方案常用于计算，验证和核实股东对现有的公司和组织的投票决策力，但大部分还是依靠可信的第三方，并且很容易受到社会工程和中间人的攻击。因此，这对于电子投票的企业来说将是建立控制台和利用加密分类账的一个大好机会，允许企业的成员和各种规模的机构成员安全地签署政策决定。为了防止被内部收购以及快速溶解（例如，手动重置资产）之类的事情发生，自终止条款可被分布式自律共识平台编程设计出来，如果在特定的时间内在特定的内部地址中无法提交足够的股东签名（或语音），那么就可能触发这样的事情。

在现实世界中的一个例子：一个分布式自律共识平台可以根据预先设计的结果来创建一个保证合同的衔接，那些愿意将资金送到分布式自律平台上并遇到一个阈值时，这个分布式自律平台将实现预期的结果。在此过程中资金将会被募集起来，直到达到一个阈值之后（例如51%）才会释放出来，那些把价值摆在首位，或者那些购买了额外的股份的人需要同意上述开支，并要报销最终产品。

正如第四章所提到的，尽管这听起来可能有些未来主义，这些自动化平台在金字塔顶端并没有实现“人工智能”，亚当莱文曾说，“现在它是参与深层次结构的唯一联系点。”它有能力花费资金，但只能在广大股东的授权的情况下才能进行，比特币就是这样一个例子，分布式自律共识（DAC）和分布式自律共识平台（DACP）是共识驱动的。根据莱文所说，这种系统规则了所有人不得预挖，在这里没有特权可言，特权是效率的对立面，而这些系统结构最大的追求就是效率。

下面是莱文即将发表的一个假想的分布式自律共识平台（DACP）保证合同：

1，分布式自律共识平台（DACP）规范由Kickstarter地址参考以太坊（Ethereum）以及比特币技术提出。

2，收到的资金包括发展资金和初始分布式自律共识平台（DACP）基础资金

3，Kickstarter地址设立了资金阈值，分布式自律共识平台（DACP）赏金发放由分布式自律共识平台（DACP）协商同意后进行处理。

4，建议开发一个或多个可接受的分布式自律共识平台（DACP）。

5，完成的悬赏需要进行复核，这些悬赏是经过预设的共识所放出的，直到结果产生之前，分布式自律共识（DACs）都无法融入到悬赏解决方案。

6，一旦该平台建立并运行，分布式自律共识平台（DACP）股份持有者可以在现行市场将以太坊股份或者比特币售出，并进行固定数额的股份投机，或使用分布式自律共识平台（DACP）将（DACP）股份按如上所述地交换成分布式自律共识（DAC）。

实验案例

分布式自治组织能做的就是执行基于事先商定条件的合同。如果把一个数字签名当成一张选票，那么唯一一个能对分布式自治组织进行修改的方法，就是通过得到X倍数量的选票来批准某种执行过程。需要的具体选票数量会在之前被设置在项目硬盘上。在一定程度上，多重签名交易，即m-n交易（例如“联名银行账户”，“多重签名彩票”）已经与比特币开展合作。虽然，你又一次被限制在10,000字节内，但这不足以满足几百张“选票”i。

由于对交易进行多重签名在全球各地已经存在了数百年之久，所以它其实并不是一个新的概念。至此，正如Szabo在第三章指出的，为了承担滥用的后果，需要制定某些策略。也就是说，个人没有单独滥用某一组织的仓库（或发射导弹）ii的能力。例如，今天我们使用由脚本（一种计算机语言）的内置规则创建的比特币协议：参与交易过程的三方可以通过签署合同来发放资金。该合同经过电脑编程，只要它收到任意两个当事人发来的数字钥匙，就会发放资金。这样一来，比特币协议就变成了一个合法系统。 因为在没有签名的情况下，它不能使用此项凭证。换句话说，如果Bob正在经营一家小企业，但他想扩建仓库，那么他就需要3个签名中的2个来得到资金。对加密货币而言，把一个总账（1个比特币）转移到另一个不同的地址，此方法同样适用。一个智能合同分布式自治组织持有和控制“锁定”凭证，需要一个预订数量（临界数量）的数字签名来“解锁”iii。除分布式自治组织外，“数位证明”方法已开发出一个软件，而Bullion Bitcoin公司会对此2/3的签名过程提供协调iv。

未来，一个制造汽车车身的小型公司可以在以太坊总账（或莱特比、比特币等）上创建一个分布式自治组织。假设该公司有5位高层，每位高层都有一把可以用来利用和修改加密总账的数字钥匙。根据公司章程（智能合同或分布式自治组织制定的规章），至少需要5把钥匙中的3把才能得到凭证。公司会议结束后，高官们就资金的使用问题达成一致。3名高层主管--爱丽丝、鲍勃、卡罗尔，被要求使用他们的钥匙，来向分布式自治组织发出发放一定数额资金的指令。只要使用他们的智能手机（或任何一个能够打开总账应用程序的设备）就可以提交自己的钥匙，随后资金就会被发放。

这可以扩大公司股东们的数量。不然而幸的是，当前比特币协议存在技术限制：禁止数以百计的数字签名被转移到某一特定地址。

不过，其它项目，比如以太坊，它就有可能把成百上千的数字签名发送到分布式自治组织。这样一来，股东们就可以对公司的具体政策进行投票。举例来说，如果一家造鞋厂的董事会想要扩大新跑鞋的生产，基于预先准核的编程规则，他们需要分布式自治组织管理着的凭证来发放资金。而分布式自治组织的运行则需要股东们投票表决。基于股东投票结果的特定功能，分布式自治组织能够被预先编。比如需要多数或绝大多数（51%，67%等）投票。在这个例子中，如果公司共有1，000名股东，而分布式自治组织又被设置为需要50.1%的票数，那么除非收到501个数字签名，否则凭证是不会被发放的。

Peercover项目

Peercover 今年一月份我曾跟在Peercover[i]工作的Jared Mimms聊过，将要启动开创让任何人都成为他们自己去中心化的保险公司。经过几个月的工作，他们创建了一个使用电子账簿的智能合同，与这个合约与Ripple[ii]界面相链接。根据他的说法，“Peercover的目标是创建一个沙箱，使人们在任何地点都能在不需要代码的情况下，链接智能合同，利用计息资产（公司）来盈利。

这意味着一旦公司成立，公司就为人们提供了尽心服务，客户的加入和使用都是简单的。Peercover已经开发了一系列，他们称之为“公司类型。”这其中的每一个对于公司来说，仅只是一种“算法构架”，包括了一个“供给系统”，它允许创始人通过链接第三方服务的方式对公司注资，使他们更具有吸引力。最后，一个内置的交易体系，很快推出了简单的股票市场，市场允许创始人们出售部分资产，这样投资者就能容易的进行公平交易，自动或手动的获得股息。”Mimms声称Peercover是“在领域内第一个真正的合同代理”这可能会增加来自其他项目[iii]的竞争。

针对智能合约的推广，Mimms说道，“这些类型的仪器可以为去中心化的创新提供一个真正的机会。”尤其是，我看到了数字加密货币是如何顾及多余企业功能的自动化。

为了完成这项计划，我开始在Peercover工作，在这里我们可以为客户和企业家们提供通过网关（通过Ripple）进行贸易的能力，这并不需要构建和管理整个后台。Ripple有一个我们使用的开源API，因为当前它是真正的去中心化的商贸活动最有效和最强有力的支持，它确认时间较APIs短，每次确认只用一小时。 去年秋季，Ripple实验室开源了Ripple的协议，Ripple的网络所需的确认时间是5-15秒，而区块链的账簿[iv]确认时间是几分钟。 对于我们的第一个“智能合同”来说，我们最初专注于点对点保险公司，-合同-因为奥巴马新医改的要求。也就是说，这里有一个明显的医疗保险公司的空白，我们的平台为企业构建自己的定制解决方案提供了方便。此外，我们目前的计划之一就是在Peercover内整合社交网络功能，能够让人们（开发者、客户、商家）相互交流。

因此，所需的流程就要采取必要措施来防止欺诈，因此我们将要验证个人身份。这听起来容易，但据了解，从事各种山寨币项目的人，如果涉及到资金，一些人都将竭尽全力的为了实施欺诈而伪造、篡改“官方”照片。 DAC的声明是很大胆的，因为除了Invictus就没有其他的团队宣布在这样的环境下有任何这样的发展。当像已知的KYC（了解你的客户）公司顺带简单的提到法律合规问题，验证对于生态系统其他部分来说一直是一个障碍，尤其是交易所[v]。据几位投资者透露，维护KYC数据库很可能会外包给精通领域内法律的公司。 山寨币们，如狗币和像NXT之类山寨协定，在过去的一年，令Mimms和他的团队感到震惊，他相信这两者能引入新的营销机制，创造潜在的平台。

正是通过这些经历，“我们已经渐渐适应对数字加密货币和加密协议开明的态度。因为我们的试炼经历，我们在几天之内可以与新的山寨币或者新的山寨协议相融合，于是之后我们为用户提供非常灵活的沙箱，提供拖放功能给所有的用户。例如，如果你拥有一个自行车修理店，你可以创建一个定制合同，这个合同具有这些功能：融资选择、股票发行，分红甚至是折扣管理（例如：针对所有用户的20%的优惠券）。实际上我们也是第一家创建智能合同的公司，允许合格投资人在遵循证券交易法的情况下来进行众筹。也就是说，不必付款给像高盛或者摩根大通这样的投资银行来进行首次公开募股，只需支付200美元给kickstarter，你自己就可以在我们的平台众筹资金。你可以发行股息和允许其他人持有股票。” 这个crowdequity meme还在第七章举例讨论过，银行的未来，加入我的IPO，Bank和论坛币。如何解决在美国等国家的法律问题也应纳入一个方面的考虑，如果你的公司对这个竞争激烈的领域有兴趣的话。（例如允许非公认的投资者进行投资[vi]）。

展望未来，Mimms说Peercover也开始开发使用沃森式功能来提供全自动的客户服务。作为努力的一部分，我们已经开始实现工具，如“税”的选项，这种选项将会自动扣缴大量的税收。（如，地域内销售百分之一的消费税，可以发送到特定的加密货币的钱包地址）。而Ripple图表的用户自己创建执行了合同-我们从中构建，我们还与欧洲的一个该领域内最大的支付解决方案提供商BIPS进行合作。”[vii] 沃森是IBM开发的一个自然语言处理系统，在2011年系列危险竞争中被广泛熟知，它击败了两个冠军级别的人类对手。IBM随后改进了其能力与方案，用于医疗行业[viii]的集成系统。此外，自动化税收是另一个相对“简单”的领域，一些开发商和投资者们提到的，可以相对容易的开发和生产。

继续，“而其他平台有更崇高的目标，我们认为去中心化的第三方工具为终端用户创造了太多不必要的复杂性。因此Peercover得到的经验结论似乎是，“相比之下，我们想要赢得一个沙基平台来集资，任何人都可以创建和管理--使用高级接口--盲目地简单订立契约。例如，我们有一个顾客在两天内筹集了30000美元，只花了两百美元的kickstarter费用。

它的技术后台，它是如何操作的，没必要告知他的用户，他们没有足够的时间和足够的知识来对基础设施进行微调。最后，如果你的目标是去中心化的银行，保持简单可能开发人员和企业家们需要不断注意的首要问题”。

明细分类账项目

对中心化的平台进行开发，使其去中心化的过程，同样被另一个名叫“明细分类账（Subledger）”的项目所使用。“明细分类账”是一个真正应用会计应用程序编程接口的项目。它能整合开发者和企业的金融数据库，包括那些基于加密协议形成的实时总账分析引擎。

今年2月，我和“明细分类账”项目的联合创始人Tom Mornini有过一次谈话。据他所说：“有可能的话，应用程序的开发能使每笔交易实时进入到明细分类账中。这样一来，公司就很容易与当事人，如客户、供应商等共享账户记录。就好像区块链在加密货币中承担的角色。此项目通过减少对信任的需求来建立信任。”此外，他们还对项目进行了细化分割。这样每位客户都会有一个个人账户，而该账户中则包含了所有需要跟踪的内容；我们只在报告内容的时候进行统计。此外，为保持审计跟踪，该系统会完整记录每一笔交易，且永远不会更新旧的条目。”

他继续说道：“大多数人认为会计就是关于钱。虽然全球几乎普遍都使用这种方法来追踪钱的去处，但是我们实际上追踪的是单位账户状态发生的变化，而不是钱本身。

此外，就目前正在部署的软件而言，对“时间关闭”（例如，季度结束和任务结束之间存在滞后现象）的忽略是一个巨大的问题。“对任何企业来说，信息的可操作时间是至关重要的。不仅如此，使用“明细分类账”，审计的工作量也将大大减少。工作量的减少也意味着成本的降低、审计的可实时进行。审计人员可以检验每天、每小时、每分钟交易中的百分比。从本质上说，即能够不断验证信息的准确性。”。

此外，就目前正在部署的软件而言，对“时间关闭”（例如，季度结束和任务结束之间存在滞后现象）的忽略是一个巨大的问题。“对任何企业来说，信息的可操作时间是至关重要的。不仅如此，使用“明细分类账”，审计的工作量也将大大减少。工作量的减少也意味着成本的降低、审计的可实时进行。审计人员可以检验每天、每小时、每分钟交易中的百分比。从本质上说，即能够不断验证信息的准确性。”。

就目前来说，也许开发商可以利用像“明细分类账”这样的项目，来提供一个整合企业内网加密账户（在随后第8章会提到）的、基于“软件即服务（SaaS）”的自动化系统。今年2月，Mt. Gox’交易所的破产敲响了警钟。这个事件的发生一部分原因在于缺乏对内部账目的核对和对内部帐目核对的衡量标准。也许在今后，我们可以利用“分布式自治组织”或“明细分类账”更快地为决策者提供信息。

问题的关键：

就目前来讲，我们很难预见去中心化自治机构中的仲裁机制是否会对中国或者其他法辖区的人们有所帮助。最终该由谁或者什么来执行这个决定呢？或者说，如果你采用了去中心化自治机构，你又该采用怎样的条款来抵消引入潜在不可靠方带来的不确定性？[223]。在支付方面，有必要将防止误操作的条款写入合同，并且确切的指明资金是在什么时间通过什么渠道或者地址进行流转的。尽管在大部分地方直接存款的方式比较常见，但是一些无良雇主试图通过更改银行账户的方式来逃避债务的事情也不是没有听说过。因而基于密码学的第三方支付机构和银行业务供应者也许可以在这里寻求新的机遇[224]。可供选择的还有诸如基于原子性的交易或者从数据库角度来讲的原子事务。

中本聪协会的创始人Michael Goldstein对原子事务给出了简单的解释：双方同意交换数字加密货币，在整个交易过程中任何一方在将资金传输给对方之前都无法执行交易中己方的部分。一项交易要么被完全执行，要么根本不执行。这就意味着没有人会在交易中空手而归。在这种机制下最坏的情况就只是交易没有达成，所有人仍旧持有他们本来的东西。

我们可以用任何可以执行相同功能的形式代替“数字加密货币“这个概念，比如(美卡币，颜色币甚至是一份智能合同)。其实原子性交易的概念之前已经在诸如机票订购这样的系统中得到应用。一名乘客要么进行支付并同时选择座位要么不完成支付也不无法保留座位。预订系统只会允许上述两个事务之一发生，而不会出现其他的混合情况。

结合已有的技术加上原子性事物（译者注：也即不可再分的事物）的概念，我们可以通过多种渠道解决雇主和员工之间的支付争端。朋友,家庭或者其他相互信任的团体之间简单的业务往来涉及的正式合同程序会得到简化。举个简单的例子：Bob在家里(可以是任意的地理位置)为Alice搭建了一个网站，之后使用0.0001比特币(或者莱特币等)生成一个临时的令牌，令牌的颜色、大小、类型代表了由交易的双方事先决定并达成共识的交易数额，这就是一枚临时的“工蜂”币，Bob将这个货币通过加密账户传送给Alice。晚些时候，Alice查看并完成网站的验收，随后将一个事先商量好价值为500美金(确切数值根据事先达成的共识来决定)的令牌传送给Bob，可以使用之前的加密账户，但并不是必须的。两个令牌都有一个内建的有效期为12小时nLockTime函数，时间取值也是任意的。如果交易的两个令牌均在指定的12小时之内被成功发送和接收，那么一个原子事务便发生了，交易双方都会都会收到对方的令牌。Alice把她接收到的令牌抓取下来，因为它是Bob所提供劳务的抽象形式(她也可以根据自己的需求将令牌保存起来用于财务统计)。这时候Bob就可以把他的令牌换成任意的外汇，或者换成其他的虚拟货币（在Cryptsy，Bter等网站），甚至直接交换商品。

这个例子只是用来展示原子事务是怎样产生作用的。在这个例子中，如果交易的一方或者双方没有在指定的时间发送自己的令牌，所有的参与方都不会受到令牌，令牌会被发回到它们所属的原始钱包中。举个例子：假如Alice没有发出自己的令牌，第二天Bob就会知道他没有获得酬劳并且它的令牌被传了回来。这时候他就可以和Alice进行谈判找出问题出在哪里，毕竟他是应该获得酬劳的。在实际应用中，正如这个例子所描述的，只要有类似于能够同时处理两种令牌的网络交易机制，Bob和Alice在交易中就可以使用不同的加密账户。[226]

只要所有实际需求中使用的令牌都可以进行十进制等分，令牌传送的数额就可以成倍增长，接近于无限大或者就是无限大(假设而我们已经解决了可扩展性的问题)。即使全球70亿人同一时刻使用基于同一种令牌(比特币，莱特币等)的加密链，用户也能够给交易的各方发送小数额度的令牌(比如0.00001)。任何个人或者分权自治组织都可以通过在哈希或者代码片段中引入辅助属性用于鉴别这个令牌实际用于何种资产，是汽车、日用品、劳务、还是许可证（比如： 可以使用元数据将0.0001BTC转换成蓝色的令牌或者其他任意的属性，这些属性就可以用来作为具体资产的抽象形式）。

抽象化和十进制

因为十进制的使用，虚拟经济中的基本令牌就永远不会出现被耗尽的情况[227]。这和通货膨胀不同，并没有新的货币产生出来用于代表特定的财产。基础令牌始终和有限的原始货币资源相关联。此外，在已有的加密账户中还有内建的反垃圾功能，它限定了进行传输的最小数额，在此数额以下的传输在网络上是不被允许的，这一功能也被称为“沙粒限制”[228].同时，对于比特币来说，每隔10钟，就有25个比特币会被生成，生成相同数量的莱特币所需要的时间间隔为2.5分钟。其他的加密链也有他们自己的恒定货币生成速度，但是这并不是最重要的，更重要的本质思想是这些令牌可以被进一步细分成更细小的十进制部分，并且可以被赋予代表不同资产的属性。同理假如预先设置的原子交易没有成功，基于去中心化自治机构的银行和第三方交易服务就会发生作用。

例如，Bob是个大公司界面设计师，他来到雇主公司Adobe并在前台刷卡登记。打卡计时器向由Carol掌管的第三方独立机构运营的HR DAO发送加密签名信息，这时候的DAO会在比特币网络(或者Dogecion币等)中建立一个带时间戳的分支账户。Bob的电脑中也配备了一款软件，用来监控他存储在Adobe公司存储局域网上的上班时间(尽管这套认证机制出现了冗余，但是随后Bob可以用这些被收集的信息来证实他的确处于工作中)。当Bob完成它的工作并且再次刷卡下班的时候，就会生成另外一个加密签名来代表一天工作的完成。令牌的颜色，类型或者尺寸之间并不相关，因为他们仅仅用来表示已达成共识的完成状态。Bob的领导Alice之后就可以通过发送带有批准或者不批准状态的签名，这个签名随后就被发送到Carol的DAO中。如果是批准状态，上述的令牌随后就会被释放并发送给另一个独立的DAO，即Dan的银行，银行会存储这个由第三方机构代表Adobe公司冻结过的令牌。一旦收到两个令牌，就会触发一个基于时间的事先设定并且已达成共识的结算条款，这个条款规定在Carol掌管的契保服务商和Dan的银行之间，Carol需要向Dan的银行发送代表“劳务“的令牌(令牌可以被舍弃或者根据财务需求进行冻结)，Dan的银行需要向事先达成共识的指定电子钱包中发送令牌(价值为500美金的比特币)，这个电子钱包由Bob通过他的私钥进行控制(也就是他的银行账户)。Dan的银行也可以通过其他的DAO发送令牌，这里只是给出一个实例。

正如你所知道的一样，这种类型的系统可以使用任何时间长度的时间锁，包括时长为几年的情况，因此从长远的角度来看他还有望用于管理信托基金和执行遗嘱。比如Bob拥有1000美金，他希望在她现在1岁大的女儿21岁的时候才把这笔钱给她。Bob有很多种选择。他可以立即将1000美金换成令牌(比如比特币等)，并且将它存放在第三方机构中。也可以将1000美金存入银行并和提供基于时间定期支付服务的银行签署一份智能合同(比如20年，用1000美金购买比特币并送给Alice)。他也可以将这笔钱存入银行，用仅需要花费几美元就可以买到的一部分比特币(0.0001个)生成一份基于智能合同的金融票据，并将智能合同存到DAO银行直到某一个指定的日期。他也可以将直接用1000美金购买比特币，并使用外部状态协议将它保存在加密账户中。使用外部状态协议是因为nLockTime函数已经被内置到协议当中，这个令牌在指定的时间会被自动的转移到指定的账户(比如20年后将会被移到由Alice或者Bob掌管的账户中)[229]。然而Bob需要注意的是签署并广播了它将该项事务设定到较远的将来的消息，有可能某些节点就会从内存池中将该交易删除。如果他使用的是第三方支付机构，他同样可以创建智能合同，列出具体的条件和允许将令牌发送到事前指定地址的条款(或许Alice会有他自己的地址，或者在Bob临死之前将许可权转给她)。

通过已有的区块链来管理遗产的另一种方式被称为Oracle，这是一个自治的第三方代理机构。在它2012年面世的时候，Mike Hearn描述了一个独立可靠的oracle系统，该系统被用来监控政府机构或者新闻上的讣告内容，因而他可以依赖于加密账户中和一个协议相关的个体和信息。

换句话说，Oracle监听并使用上述数据来签署多重签名的协议，以便协议能够将资金传给它的受益者，这项协议需要oracle的签名。需要将资产传给指定受益者的受托人从oracle申请签名，并且签署协议[230]。去年Michael Goldstein展示了另一个用于体育赛事赌博的oracle。比如Bob打赌A队会赢，Alice打赌另一支队伍会赢[231]。Oracle持有该协议的决定权，假如A赢了，Bob会获得这笔资产(比特币)，如果B赢了，Alice就会获得这笔资产。双方签署的协议中并不涉及该交易在发生争议或者其他可能的问题时该如何处理。在比赛结束以后，oracle就会进行签名，移除中间人。和普通的法律纠纷需要涉及细微差别和灰色地带不同的是，体育赌博是一种客观和理想化的场景，因为其中并没有过渡地带，oracle必须具备的就是获得ESPN的数据传送权限。

减少滥用

在加密账目中采用的另外一些短期项目包括忠诚度方案、商人奖励方案以及来自Alice航空公司的“飞行常客令牌”，所谓的“飞行常客令牌”能够防止和缓和旅行黑客入侵带来的风险(比如让不乘坐航班而获得常飞里程数)232。由于网站漏洞遭到利用和用户频繁的行程变更而引起的通货膨胀，美联航的常旅客行程长度在14年的1月份显著减少。

作为替代，Alice航空公司可以减轻审计、存储和奖励的成本并且用任意数量的令牌（0.01BTC）来使用密码学账目的“合同”系统，建立一个合同定义一组里程数（本身很可能有预先设定的过期时间）。我们假设飞行员使用密码学货币的钱包，并把钱包地址提供给航空公司，用户就能在他们的钱包中收到里程数了。反过来，用户也可以通过向Alice航空公司发送特定数量的令牌来出售或者交易得到的奖励令牌。

其它的机构可以用智能合同来发型和记录它自己的用户忠诚度奖励项目。比如，赛百味在2005年终止了他的赛百味集邮俱乐部项目，在这个项目里一个消费者在某些情况下能够收到一些优惠卡（标签）。当一个消费者收集到足够数量的优惠卡，他/她就能吃免费的大餐了（薯条，饮料，三明治之类的）。然而，有许多消费者却发现了钻空子的方法，他们在eBay上买卖大量这种优惠卡，造成了优惠卡的大贬值还给上级公司带来了不明数量的损失。

因此，优惠券是可以发展的另一个成熟的领域。根据NCH 市场部的调查，“快速消费品的制造商在2012年发行了3050亿的优惠券，与上一年持平。2012年总的赎回率下跌了17%，为29亿张，为快消品公司在票面上节省了8亿美元。看起来这只是个很平凡的领域，但考虑到Juniper Reasearch预测到2016年”总的移动优惠券的赎回价值将会唱过430亿美元“，因为通过移动APP优惠券分发的数量急速上涨。我们不妨看看，美国48%的成年互联网用户在2012年兑换过数字优惠券。一个提供优惠券或折扣的公司可以建立一个DAO来管理他的兑换合同（比如某种时间锁定性的令牌），这不但能减少后勤方面的开销还能防止优惠券滥用和欺诈（例如，双花）。据美国邮务督察Roberta Williams所说，“对于每个成功的优惠券伪造按键来说，平均要使制造商损失100万美元”。这些伪造的优惠券是可以检测的，但是优惠券的通货膨胀最终迫使生厂商们赎回了更多的优惠券。优惠券信息团体估计优惠券诈骗每年会造成3-6亿美元的损失，而这些损失最终还是被强加到了消费者头上。然而，如果说支配比特币的算法被证明熟练与某件事的话，那就是防止通胀。

虽然和防止欺诈没有直接的关系，2014年2月份一个现实生活中的设计研究开始了。PointsHound，一个通过常客里程和旅馆积分提供旅行预订的网站声称他们开始在支付系统中接受比特币。如果用户选择了比特币支付这个选项，PointsHound会根据Coinbase上的市场价格进行计算，并打回到用户的钱包当中。正如联合创始人Pete Ban Dorn所说“我们的创业使得用户可以根据他们的选择来决定赎回的货币形式。也许是5000英里的里程，也许是比特币。”

“分布式自律组织”的“淘”

在发达地区，市场的参与者们对于计算机软件的使用、运行和管理都很熟悉，他们还熟谙在进行电子股票交易时运行几乎所有的商业条例检查，知道如何把各种条文写入其中以防止或者说避免对家风险。下面我们来看看普通的合同是如何被设计到一份智能合同当中来完成此种功能的，这可以是一份普通工作的合同，甚至连农民工的工作合同也可以。

它也许是这样的：雇员Bob用一枚数字密钥和他的老板Alice签署了一份智能合同，Alice也用一枚数字密钥进行了签署。在合同当中有一系列的关于付款期限的规定，和防止一方无法完成协议的措施。也许当中还会有还会有支付实际如何完成的条约：也许通过第三方代管（BTCrow），通过X银行，通过Y地址或者通过各种形式的混合方式。这个合同可以被保存在公共的去中心化密码承载形式中（例如Bitcoin，Ripple网络等）。如果存储于其中，就能免去篡改和伪造支付的风险。并且，虽然绝大多数人把比特币系统看成是一个货币追踪工具，从数学的角度上来说它更像是一个能够在特定技术条件下追踪任意数据集（例如：某个比特币）的数据库。所以过去的四年里一个特定的“令牌”就被集成了一个个整数的账目，一切就是这样发生的(也就是比特币系统)。

虽然只要得到剩下有投票权的人的信任就可以改变DAO的运作方式，最原始的合同依旧是向大众公开的，也不会被篡改。唯一可能发生的是，合同本身有个nLockTime（基于时间的锁定）条件，或者有个在未知长度时间后再生效的约束，当特定的情况没有发生的时候（比如说，完成支付），那么合同就会服从先前就定义好的终止条件。也许它会把自己发给一个先前就定好的仲裁者或者发个一个第三方DAO。虽然智能合同系统是否能在网络中解决所有问题（例如实体经济的问题）依然让人疑惑，但它确确实实能是真正的合同免于篡改的危险，并使雇员（包括雇主）免于承担第三方机构欺诈的风险。

所以简单的说来，忽略资产管理的其他方面，会发生以下场景：

Bob和Alice签订了一个智能合同，约定了各种期望以及赔偿条款等等。合同约定，付款会每个月通过各种不同的渠道进行。然而如果出现违约的情况，款项就进入了Cathy的第三方保管契约服务当中（这个服务本身也可以是一个独立的DAO）。事实上，很有可能会产生许多虚拟的第三方契约服务来维持良好诚信的声誉从而完成商务工作（就如同今天实体经济的做法）。更长远来说，很有可能出现基于独立仲裁的争议调解条款，如果其他的所有方式都失效的话（也如同今日的做法）。对于“所有其他方式都失效”，我指的是：会有一个基于时间的触发器：如果Bob和Alice都不在合同在账本中规定的特定时间内重新签署B、C或D条款，那么合同就被发给仲裁者Dan或者公共法庭的Eve了。Dan就能从众多处理过类似情况的知名仲裁者中被选出，像一个独立第三方代管机构那样，提供公正的服务（net-ARB就是一个此种类型的服务）。

这种类型的关系以及契约今天已经出现了。虽然也许刚开始把他们“代码化”有些小小的困难，这终究只是个时间问题：去年Coinsigner通过多重签名交易方法成为了第一个专注于给密码学货币提供纠纷调解的服务商。实际上，（提供此种服务）的门槛非常低，个人也可以建立一个独立的纠纷调解服务来提供中立公平的判断，而任意的三个人就可以使用此种服务，跨越国界也完全没有问题。然而，虽然本书中多次提到了这种服务，此类系统对于大企业而言是否在商业上可行，依旧是个存在各种可能答案的问题。

如果中国（或者任何其他地方）对密码学货币颁布了严格的资产管制条例，通过使用一系列的不同“着色”的货币链，Bob就能在北京从安徽给Alice发送价值X货币的虚拟资产，而不是X价值的货币本身。

这就能建立一种更高级的物物交换系统，也许使用密码学货币作为交换中介不那么搞笑，但是他能帮助那些非正式的经济系统描述和量化资产的价值并清理一些混乱的循环债和资产所有权问题。然而这些合同该如何被增强估计还得再写一本书，因为任何提供此类服务的机构都会被政策重点关照，如同今天的交易所一样。

与此同时，还有来自不同管辖者的不确定以及未知的法律风险。在中国，就很难推测各个省市自治区直辖市以及中央政府本身如何看待这种基于账目的资产管理方式。二十年前，大多数的西方评论家认为因特网会使普通的中国民众避免审查，然而GFW被证明能够阻止所有的信息。虽然要阻止去中心化的p2p行为比较困难，也许每个级别的政府需要交易的一小部分并且只认证通过政府维护的DAO，或者是有监管的第三方担保以及和实际资产及国家法律体系有合同关系的仲裁服务所完成的智能合同，这也正如Preston Byrne在第二章中建议的那样。

第六章：筹款场景

根据CB Insight公司的报告，2013年，风险投资公司投资了7400万美元给40家比特币相关公司；其中最大的两轮分别是Coinbase（2500万美元）和Circle（900万美元）。无独有偶，Garrick Hileman最近公布一些数据，发现在同一时间内，大约9750万美元的VC资金流向了36家比特币相关的初创公司。下面我们将就这一发现展开讨论。

尽管媒体对比特币的关注持续增加，即使VC今年向比特币产业投入同样数量的资金，也无助于提升部分VC基金的业绩表现。显然，即使是乐观展望，现在风投公司的实际年投资回报率大致为6.2%。在过去的十年中，他们的表现落后于罗素2000指数。为什么这么说？这并不是贬低风险投资行业，它不像其他的行业，一些风险投资人也并不像许多天使投资人一样，能够敏锐地感知和筛选出有创收能力的商业模式。

过去四十年的变化

开源软件和云计算的广泛使用，降低了软件开发成本，更重要的是也降低了新公司的创建成本。所以技术初创公司和投资门槛也有降低的趋势。而在以前，企业的资金来源，主要限于财大气粗的专业投资者，即风险投资。宏观经济的通货紧缩，使得越来越多的个人投资者、天使投资人，在投资领域中竞争。

新型的天使投资人，比昔日被动和非技术出身的高净值投资者更胜一筹。当今，越来越多的天使投资人，有着深厚的行业经验。许多投资人在他们投资的领域工作过，他们本身就是一个企业家，或者是有经验的经营者，能够感知到新业务方向和技术发展趋势。历史地看，天使投资的进入门槛是在给定承诺投资量情况下的风险量化（其次是知识和协调）。随着创业成本的降低，这个障碍也在慢慢的消失。具有深厚专业知识和运营技能的天使投资人将颠覆传统风险投资行业。这些天使投资人有更好的契合度和更友好的合同条款，这比起历史悠久的VC行规，显得没那么咄咄逼人。

这并不是说，风险投资商就不会再次蓬勃发展，然而，就好像它的发展过程一样，大部分天使投资人是企业家出身，然后学会如何产生销售和直接盈利。此外，如上文所指出的，在过去的十年，技术成本降低了。举例来说，相对便宜的云服务，如github和Computer Engine提供的服务（CaaS, SaaS 和 IaaS）,覆盖运营成本所需的资金需求更少，使得许多科技型初创公司比之前更加精简。

更胜一筹的是有组织的天使投资人，他们有一个完整的生态圈， 可以通过诸如 AngelList, 500 Startups, Plug and Play, Y Combinator, SVAngel, Bitcoin Opportunity Fund and Boost 等机构来选择投资项目。事实上，在过去的六个月中，

BitAngels.co已在全球范围内投资了700万美元给密码学相关的项目，Plug and Play提供和引导了$25,000 种子基金投入到比特币相关产业。

加密货币相关初创公司的另一个融资渠道便是IPO众筹。这其中就包括Mastercoin, 募集500万美金（在当时），由众多投资者投资4700个比特币而成。NXT 以及即将面世的 Ethereum（以太坊） IPO也包括了通过比特币转账募集资金。虽然我不是很推崇这种特殊的募集形式，但这也说明了小（或者大）的开发团队在没有VC种子基金的投资下也是能够支付运营成本的。而且，除了像Kickstarter ，Indiegogo这样的众筹网站之外，也有像BitcoinStarter 、CoinFunder类似的网站，允许个人通过他们的想法募得比特币资金。

因此，不宜过早的抹杀VC，或声称天使投资是基金池的唯一来源。事实上，在过去的两年里，比特币产业的大量资金都是来源于VC公司。例如，Andreessen Horowitz投资了近5000万美元在比特币相关的初创企业，包括了去年秋天他们主导的Coinbase 2500万美元的融资。2014年2月，Marc Andreessen，该事务所创始人之一，在接受CNBC的采访时说道，

> “【比特币】很可能是新的机遇。例如，由于世界各地有很多人不在现代支付系统中，他们无法支付费用买东西，所以很多本该有的电子商务并未发生。另外，目前的国际转帐费很高，许多商家在很多种类的商品上都不能盈利。这真是一个巨大的机会，而且每个人都可以把握它。比特币是一种开放的技术，开源、并且可以免费获得---任何人都可以参与进来。因此，任何现有生意，如果要利用比特币，比如说Western Union，都是可以参与进来的”。

虽然现在预测这些投资如何退出还为时尚早，VC投资始终是一种强大的市场力量。

风险投资的图表

除了上述CB Insights公司的调查结果，以下是四个图表（经允许转自Garrick Hileman，最初发表于2014.2.24.）：

投资总数 （单位：百万美元）

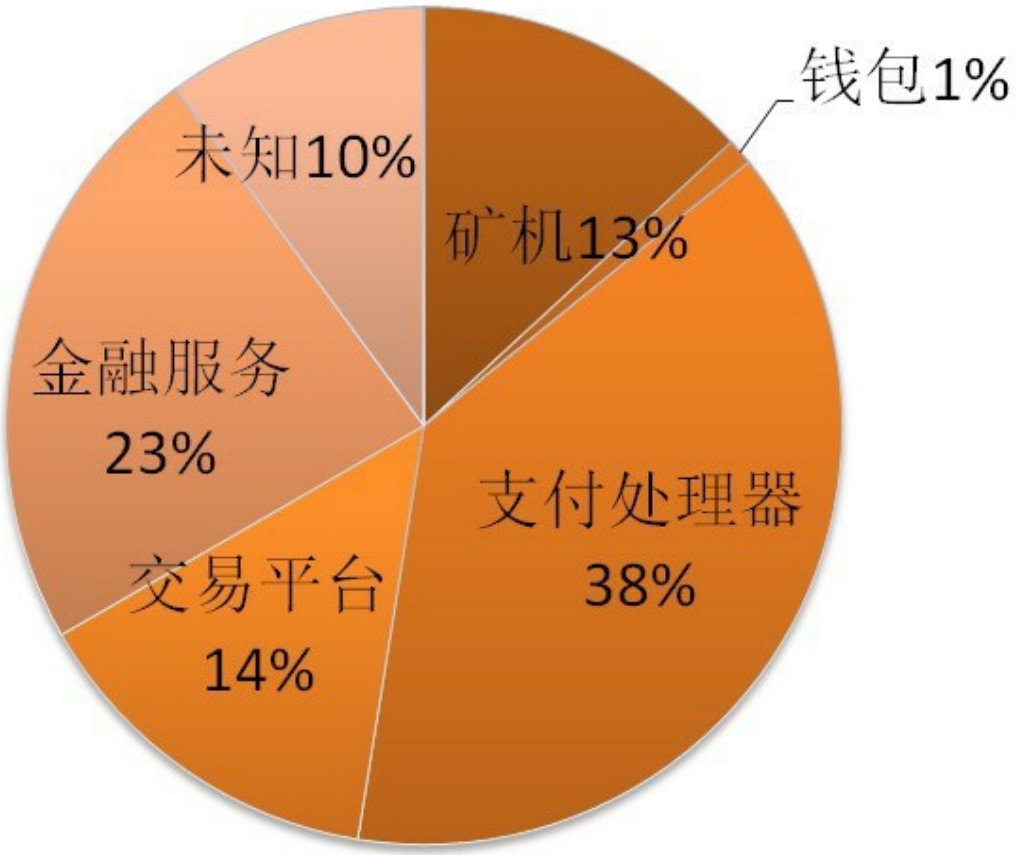
发展的阶段	2012-至今
	总数
首轮融资	72.50
其余交易	25.00
总计	97.50

交易数

发展的阶段	2012-至今
	总数
首轮融资	35
其余交易	1
总计	36

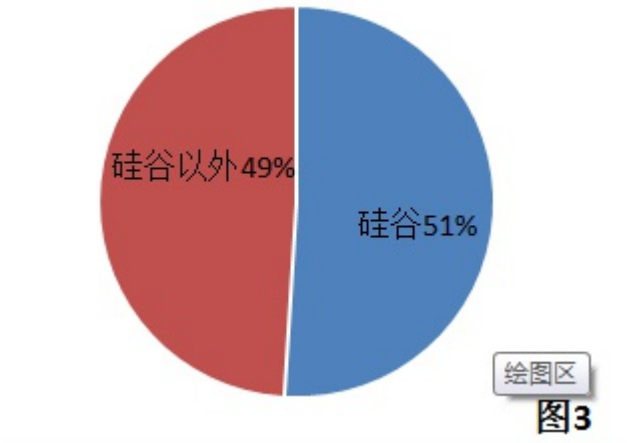
图一：VC对比特币公司的投资金额，2012-至今（右图是支付处理商，非器）

如图一（或者表一）所示，2012年至今已知的VC投资给全球范围内比特币相关公司的总数。



图二:比特币VC投资分布

图二表示，根据这些公司所属的细分行业划分的百分比结构。在Hileman的分析中，他指出，到目前为止矿机公司已经产生超过2亿美元的收入，图中未知是指收到风险投资但是未披露的项目。



图三表示了VC投资的地理分布，位于硅谷（即旧金山湾区）的公司占有大部分的份额，为51%。

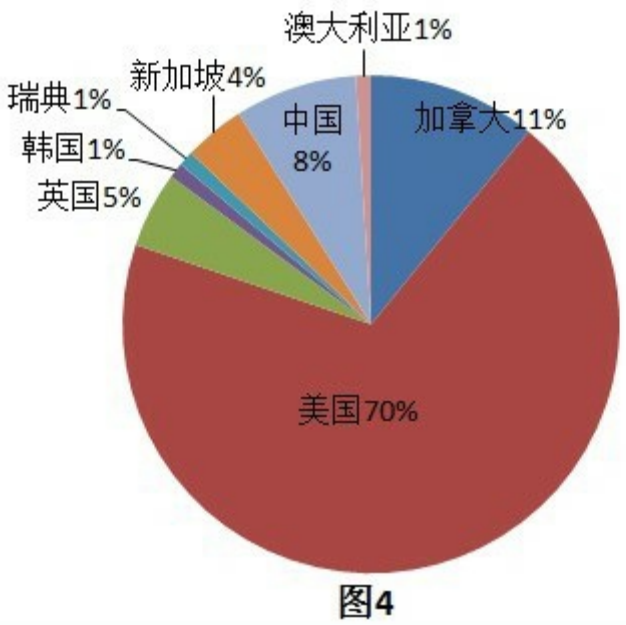


图4

为了制作表四，Hileman查阅了所有VC基金投资项目（9750万美元）总市值。表中显示了这些投资的地域分布。美国的公司占了70%。这些数字在未来一年内有可能持续增加，目前还不清楚这个地理趋势是否会持续下去。

直接来源直奔源头？

Jeremy Liew，光速创投（Lightspeed Venture Partners，LSVP）的总经理，在比特币领域内投资了多家初创公司，包括Ripple和比特币中国（BTCChina），同时，他还主持了Boost BitCoin Fund。 据他说，“我认为，有三个应用场景会导致数学货币的大规模应用。

①微支付（小额支付），因为小额支付用信用卡不太实际（可以是在线内容，也可以是游戏中的数字商品）；

②交易费非常高的跨境交易（C2C双方的汇款业务、进出口的B2B以及电子商务）；

③发展中国家跨越信用卡到电子商务和移动商务领域所需的采购？。发展中国家从固网电话跨越到移动电话技术，这也正是我预测的加密货币跨越信用卡发展的模型。如今，在俄罗斯、中国、印度常见的电子商务的支付形式是“货到付款”，这很有可能是第一个被加密货币所取代的支付方式。”

依照LSVP感兴趣的细分行业，“我们现在仍处在基础设施阶段，使得基于数学的货币更容易买（交易所），持有（钱包），花费（支付）。容易推测，该基础设施应该更加成熟，使得能够在此基础上开发更多应用，进而推动数字货币的大规模采用（被大众接受）。以上就是早期的三个主题”。当有人要求Jeremy Liew猜测一下，那个平台或者哪项技术如智能合同，将涌现出来。他回答道，“我不知道，我只知道这将是一项令人兴奋的变革。正如没有人能预测当我们还在使用POTs的时候，VoIP的应用引发了爆炸式增长。同样不可能预测加密货币的哪一部分是“可预计的”，以及是否会带来同样的增长。但肯定会很厉害？”

他针对意想不到的创新及其连锁效应提出了自己的观点；仅仅Skype一家的通话就占了全球电话流量的三分之一，它为每个人群提供了一种费用更低的新工具。同样，数码产品，如音乐、电影、游戏和和书籍---在十年前这个市场几乎不存在----到2015年将达到800亿美元的营业额，而这还仅仅是指美国。事实上，根据Ofcom,11%的美国互联网用户会为在线数字内容定期付费。在我与Mike Hearn 交流的时候，Mike对这个领域内尚未开发的商机表达了类似的观点，他指出“现在看上去似乎有大量的初创企业在这些点子上探索每一种可能的方向---最需要做的就是基础设施之类的东西，尽管它确实很枯燥。”为这些平台奠定基础可能成为未来数年的商业机会。

在第二章提到过，Ryan Orr 是斯坦福大学的教授，同时也是Zanbato的主席，Zanbato是加密货币风险投资公司CrossCoin的合伙人。他指出，“随着最近一波的监管行动，我个人对于2014年的“智能财产”项目的演进特别期待。他开始觉得智能财产对于比特币协议来说阻力更小，因为它建立了一个‘非货币’形式的应用，能满足有价值的社会需求。因此那些害怕失去货币垄断地位的监管者，不应该把它看成是直接威胁，。”

人们以非经济目的持有黄金，也会以保值目的(例如：防止通胀)持有黄金，这就是黄金的二元性/双重属性。使得政府不能完全消除黄金的货币属性(美国政府在20世纪曾经真的这么干过)。如果比特币也发展成类似的二元性，“智能合同”使得它本身合法，人们秘密持有它，并且作为一种自由手段对抗政府的失职和无能。那么事情将变得非常有趣。总之，“智能合同”会成为比特币“正式的、法定的、正规的”的一面，与比特币作为货币被监管者法规所限制的另一面无关。

天使投资在寻找什么？

Jeremy Kandah，BitAngel的执行合伙人，正领导着一个专门投资基于区块链的去中心化系统的基金。他认为：“比特币2.0协议和项目，如Mastercoin和Counterparty类似于计算机编程语言的Java和C++。当今，有成百上千的计算机语言，但只有数十种语言作为平台为数十亿美元的大型生态系统服务。如果你依赖于平台，你就是在卖空你自己，并冒着被供应商锁定的长期风险。这个领域内几乎所有项目都会开源，以方便移植到其他的区块链和去中心化平台。Open Transaction（OT）就是一个很好的例子，他们的工具包和代码库完全开源，即使有人想篡改比特币协议（我并不是说真的会有），开发者和OT应用的用户都会迅速迁移到另一条区块链上。”

Kandah 解释道，比特币本身是不是密码学货币世界的类似于TCP/IP的基础，这一点尚有争议，还需要建立大量的基础外延设施，使得去中心化的应用发挥作用，这正是“2.0”项目尝试去做的。这就意味着对开发人员和企业家有一种持续的需求，促使他们去创办公司并建立商业模式，给市场创造价值。正如他所提到的，“虽然我是个总账不可知论者，也许有更有利的方式来利用Namecoin的功能，特别是自从它以合并挖矿的方式挖比特币后，交易和确认网络已经可以正常（自我？）运行了。”

最后，他表示很看好去中心化和用户自定义的虚拟货币，以这种方式提供价值的创业者们，能提高整个比特币生态系统的整体利用率。他说，“在我们尽职调查阶段，当我们寻求那些创造价值的商业模式时，其实我们是在寻找专注于解决某一当前市场需求的团队，他们能够提供让普通用户易于交互的新解决方案。例如，很有可能以这样的方式实现‘娱乐化’--点对点网络如何运行并且与连接到区块链的手机交互，允许在所有城市的任何地方临时建设去中心化的互联网基础设施。类似地，正如Uber和Lyft建立了去中心化的出租车产业，也许还能通过区块链和无信任资产管理方法，提供行李包裹托运服务来赢利，并且能与FedEx的服务水平相当。

Kandah和David Johnston二人都提到的需要记住的另一个比喻是， 尽管有了最新版本的HTTP，但完美是“好”的最大敌人，协议背后的无保留分享和网络效应难以再现时，像BitAngels那样的基金，最终就会寻求能够理解客户的价值主张（如承诺传送和创造价值）的团队。这些客户没有必要知道区块链的工作细节，而对基于货币支付系统的稳定性、安全性、可靠性更感兴趣。

此外，我也与Ben Davenport聊过，他既是天使投资人也是Instagram中货币化小组的成员。他没有赞同某一特定的项目，在他看来，“彩色币技术使得中心化的资产能够以一种完全去中心化的方式交易。世界上的每一份权益资本都有一个中央发行人——公司本身。但想象一下它的威力吧：不通过第三方，通过比特币与陌生人来达成无信任的股票交易。通过彩色币，我可以把这种股票交易编码成单个原子交易。对我来说，这就是彩币能实现的最重要的基础功能”。

Hakim Mamoni，Seedco.in的联合创始人以及个人比特币交流平台DealCoin的创始人，持类似观点，他们认为“比特币最核心的是它是伟大的去中心化运动的一部分，这一运动说明与以前的系统相比，人类能够更好的组织自己。虽然在公元前4500年随着苏美尔的建立就意味着‘文明’的诞生，一般来说，我们在年复一年的复制同样类型，自上而下式金字塔结构。即使在美国和法国大革命后，政党还是采用的之前存在的中心化方法，因为他们没有当代的技术，只有信鸽和骏马。而现在，我们终于有了改变中心化系统、以及自我组织变革的技术能力。”（苏美尔（*Sumeria*）：今伊拉克东南部幼发拉底河和底格里斯河下游建立的古代文明，是目前已知的全世界最早产生的文明-译者注））

他认为，中央银行的角色是可以削弱和改变的。“如果你看到一个人的简历，他的过去表现不佳，你很有可能不会让他继续呆在你的团队里。我们回过头看20世纪早期，对于金融稳定性这个目标，没有一家中央银行能做得很好。因此，对于我来说，比特币是当前的杀手级应用（Killer App）--比特币钱包使得任何一个人都可以打款给世界各地任何人，这使得人们变成自己的银行。最终，有些项目就会在此基础上创造各种功能和特性，现在我们正在通过如以太坊（Ethereum）这样的项目朝着这个令人振奋的方向前进，不只是改变传统银行系统，也包括其他系统如电信网络、粮食生产乃至能源生产的去中心化。

去中心化的电子通信的方法之一是无线网状网络（Wireless Mesh Networking），它通过使网络中的节点转发数据而实现。像Commotion 和XORP等项目正致力于为终端用户提供去中心化的无线功能。

Mamoni也发现像Open-Transactions这样的项目非常激动人心，“我真的特别喜欢OT这个项目背后的思想，因为用户不需要要去信任服务器，合同会自动的以加密的方式从一台服务器传输到另一台。政府就是被设计来防止坏人的不良行为欺骗系统。然而，如果将政府管理与这些技术的新模式结合起来，传统的法规就没有必要存在了，因为这个世界里所有

的一切都是公开的，所有的一切都是通过算法和数学来完成的。因此，我认为监管机构很有可能会接受这类型技术，因为它可以防止欺诈行为。所以，Seedco.in不仅通过投资大量的初创企业从总体上来加强和巩固加密货币的生态系统，同时架设桥梁通往现有的经济结构。它不能一蹴而就，但我们相信在这个过渡期内仍是有很大价值的。”

Mamoni认为，区块链的另一个应用案例是，金融机构可以用来创建日常的LIBOR（伦敦银行间同业拆借利率）。LIBOR是一种平均利率，伦敦的主流银行相互之间进行短期资金借贷的平均利率，于每天上午11:30公布。在2012年，爆出一条丑闻，有人发现成员银行在暗中操控利率。然而，根据Mamoni所说的，如果将每一笔交易都放到区块链中，这个利率就不可能会----至少是很难---被修改或操纵，这是由于区块链是安全透明的，每个人都能看到它。

非盈利性的组织和非政府组织（NGO）也可以采用这样的区块链来实现透明的资产追踪。根据坦帕湾时报（Tampa Bay Times，美国佛罗里达州一家报社）, 在过去的十年里，大约接到了14亿美元捐赠，美国的最差的50家慈善机构在募捐方面就花费了大约9.706亿美元。区块链赋予了每一个捐献者实时审计慈善经费的权利。与去中心化自治组织（DAO）相结合，非盈利组织的管理开销（如工资单）就可以完全被人工智能所取代。

这样的透明系统在其他国家也同样适用。例如，2008年5月12日，约69,000人在中国这次三十年来最致命的地震中丧生。随后，来自中国各地和世界的援助和捐款（总额达112亿美元）汇入四川灾区。然而尘埃落定之后，几次调查发现，由于缺乏透明度和问责机制，各机构和组织侵吞了数以千万计的捐赠款。中国红十字会（RCSC）在震后四年后都没有收回这些摆放在全国各地数百个地方的捐赠箱。区块链可以用来追踪非盈利组织的捐赠款和资产，减少欺诈行为，并提供实时的透明度和审计。事实上，如第五章中所提到的，这样的组织里即使不是所有也是大部分的管理开销（如支付账单、接受捐赠）都有可能被DAO 替代。这点在第八章里有进一步的讨论。

在2014年1月，我采访了旧金山湾区某创业加速器的一个市场经理，他正在寻找在软件即服务（SaaS）的垂直领域采用比特币协议的早期初创公司，使得税收、会计、智能合同的解决方案成为可能(如基于SaaS的遗嘱、基于参数或是类似DAC的企业对企业的业务合作关系。或者，换句话说，那些专注于中小型企业和消费者的解决方案。

这次谈话的独特之处在于了解到他们对涉及到自动转账到税务申报的全流程的会计解决方案感兴趣，而这仅有一个其他类似组织提到过，这很有可能是一个被低估的商业利基市场。总之，这将涉及用加密货币（加密货币是第七章中讨论与Coinality相关的一个主题）支付项目管理人员报酬。

这位经理也特别看好去中心化自治公司（DACs）,并将其视作未来的潮流。他的团队认为，这个生态系统最终会将大部分的任务外包，分配给很多工种，尤其是：应付账款、应收账款、税务、其他会计流程、汇款（不同角色）、应急响应（基金发行）、社区投资（也就是说，当地学校的措施），房地产投资信托基金（以社区为基础的房地产投资），以及社区物业管理（租赁解释为自动服务电话）。因此，建立专注于在那些领域的公司设计DACs很可能会吸引外部投资者以及潜在客户的关注。

亚洲

我曾经与Kapronasia的创始人及常务董事Zennon Kapron用邮件交流过。Kapronasia是一家专注于亚洲金融服务行业的独立研究咨询机构，总部设在上海。Kapron 在大陆市场有很多第一手的经验。据他所说，加密货币接受度的相关应用在现在和将来都是非常重要的，尤其是在亚洲。眼下，在一些很有潜力的区域内加密货币的接受度还是很低。比起American Express来，为什么更多的人拥有Visa？很大原因就是因为接受度，Visa能在更多的地方使用。尤其是在亚洲，类似于Bitpay的POS机和商业解决方案都特别少。此外，尽管在亚洲也已经有很多的交易所，但我觉得只有一部分是考虑了用户体验的，尤其是电汇，一般的消费者可能并不觉得方便。Coinbase 是可能符合要求的一个有趣的交易平台：你可以关联你的银行账户，这就使得ACH转账（Automated Clearing House,自动清算系统，是美国金融机构间的电子清算系统,利用它可以方便地在部分美股券商和美国银行间划转资金-译者注）变得非常方便。这至少对加密货币的初期接受者来说是非常重要的一个慰藉，但是一旦越来越多的普通大众都拥有一定的加密货币余额，而且接受度变高时，需要转到法定货币的需要就会降低。所以交易所也显得不是那么重要。

随着BitPay， BitPagos和BIPS在基于比特币的商家生态系统中占据主导地位，除了YesBTC.co之外，以中国乃至亚洲为基础的同类商家还没有达到相同水平。Kapron指出一部分原因是语言和文化的差异，在亚洲大部分网站都不接受这种加密货币，尤其是在中国。事实上，在2013年12月5日中国人民银行发声明禁止第三方支付公司为加密货币（将加密货币归类为商品而不是货币）提供支付通道。电子商务巨鳄淘宝也声明不允许在其平台买卖加密货币相关的商品。尽管有这些障碍存在，但还是有可能在边缘有些机会。此外，ACH在美国是一种互联网经济产物---尽管它在2012年处理了210亿交易量总价值达36.9万亿美元----所以对于企业家来说，在保证金以及未能得到充分金融服务的人群之间还是有很大范围的竞争力的。

Kapron接着指出，“亚洲在加密货币的应用和解决方案上是落后于西方的，所以初创公司聚焦于一些比较大的解决方案，比如说交易平台、商家POS机解决方案仍然有很大的生存空间。在大陆交易平台外的这些应用市场也远远没有达到饱和。很有可能已经有一部分初创公司在秘密地筹备研发相关解决方案了，然而，除了交易平台，公开启动或投资的其他加密货币相关的初创企业就算有也很少。当然，一些较小的解决方案（如税务审计插件、Bitmessage、twister、syncnet）也将有市场。但是，像交易平台、商家接受度解决方案的市场会更大一些。

我们曾在在第三章简单的提到过Bitmessage和Twister；虽然它在技术上是可行的，但是不清楚政策制定者会对国内企业研发匿名通信工具会作出何种反应。

谈到智能合同和下一代平台的发展，“当前这些加密货币背后的技术思路和算法对智能合同和其他总账应用程序的实现是非常适合的。这些也很可能更容易实现，因为这些应用并不一定必须是全球化的，可以限定在一个较小的地理区域。例如，你可能在伦敦或者巴黎有一个专门针对不动产项目的总账，因为区域限制，涉及到政府和监管部门的批准也很少，而且政府也可以在不降低系统吸引力的同时参与到智能合同的创建和维护中来。换句话说，比特币以及其他加密货币的主要目标之一是用户可以自行操作而无需政府的干预，很多人正是由于政府的干预才给当前经济造成一些问题（美国的量化宽松政策使美元贬值，变相的支持了美国的出口）。如果是智能合同的话就没有这样的担忧，只要你相信政府会从人们最大利益点出发。”

正如第二章中Preston Byrne所提到的，包括政府部门在内的机构组织可以建立并维护这样的区块链来代替昔日冗杂的职能部门。中央银行可能利用的方式是通过第三章所提到的‘燃烧证明’(POB)。这就和在统一前东德的马克要换算或者汇兑成西德德意志马克比较类似，阿根廷中央银行将来某天有可能会宣布这是“发行的密码学货币”来防止比索贬值。阿根廷中央银行可要求比索的持有者将比索换成加密比索。根据Wences Casares 和 Sebastian Serrano在第二章中的描述，在转化过程中，原来的物理比索被回收或销毁，随后，虚拟货币在公开总账上被追踪，防止双重支付和通货膨胀。当然，这类应用的可能性仍然是有争议的。

尽管中国人民银行目前正在审查其涉及加密货币的政策，在Kapron看来，“政策调控仍将推动加密货币在整个中国区域内的整合并带来机遇。总的来说，香港和新加坡因其身为该地区支付和金融技术的创业中心而特别闻名。如果我们总结比特币的情形，两地的监管机构都对加密货币表现出积极的态度，因此，我们很可能将继续看到香港和新加坡接受加密货币并提出创新性解决方案。在许多方面，这对于地区来说是很好的，虽然这两个地区有较大的经济体量，但是无论从地理还是经济角度来看，两地的影响依然很小，这与中国的自由贸易区是相似的。香港和新加坡可能最终成为加密货币的试验床。尽管中国内陆仍然有所限制，但是通过允许香港金融业进行创新和改变，中国已经大致上实现了这一点。此外，中国和新加坡都已经有较长的全国性支付创新的历史，如EZ-link和八达通（Octopus），这两者都实现了茁壮的成

长。从多方面的原因来看，加密货币也会如此。中国和印度这样的人口和经济规模都较大的经济体很可能会追随香港和新加坡的发展轨迹，尽管经济体越大，风险也越高，特别是中印两个经济体还有严格的资本控制。较小的经济体，特别是东南亚国家，面临太多的经济和政治挑战，在亚洲的整体影响也较小，因此不太可能影响整合。”

在过去的三十年间，中国创立了15个经济特区。经济特区可以自行设定进口法规和关税，因此，比较受合资企业和外贸业务的欢迎。从去年开始，其他几个主要城市，包括上海在内，都已经开始为“自由贸易区”做筹备工作，这将为新的经济改革创造一个试验场，预期将进一步解放金融业。

2014年1月，我采访了马睿，500 Startups（美国硅谷的一家早期种子基金和创业孵化器-译者注）的一位北京的合伙人和天使投资者，500 Startups是一家创业孵化器，投资了一系列比特币初创企业如Bitdazzle和BTCJam的发展。在她看来，“加密货币是跨境小额交易的一个解决方法，因为它们能在被传统银行完全忽视的领域带来商业机会，。我认为移动支付对每个人来说都非常有趣-----特别是新兴市场-在刚刚过去的2013年里中国互联网金融进步很大，原因在于中国总体上缺乏针对消费者（也包括中小企业）金融产品。然而，由于传统支付机制的资本支出，所以这也不是一个或两个天使投资人就能使其规模化发展的。但是我依然对建立在基础设施之上的服务特别感兴趣，而比特币是最理想的选择。”

由于严格的外汇控制，中国富人想要在国外多元化发展是很难的。这个问题加上部分国内金融工具的缺乏，是由于国家仍处在发展阶段，而且大部分经济在本质上是垄断的（被大型的国有银行控制）。所以，科技公司如阿里巴巴、腾讯通过创新消费者市场带头改变格局，比如说，提供手机终端的公募基金（这里主要指其中的货币基金）、第三方支付服务。举个例子，去年支付宝与天弘基金（中国一家资产管理公司）联合推出了低成本公募基金（称为余额宝）。规模达到426亿元，拥有4900万客户，余额宝已经发展成为内地第二大公募基金。在2014年1月，中国最大的互联网公司-----腾讯公开了其与中国最大的公募基金管理者-----华夏基金的合作关系，准备推出类似的服务“理财通”。同时，腾讯将理财通与微信融合，微信是全球增长最快的社交网络服务，（超过6亿注册用户）。腾讯也是QQ 的缔造者，QQ是中国最大的社交平台，每月平均在线用户8.16亿。

马睿承认这些市场的趋势和改变以及如比特币一类的加密货币在市场扮演的角色，并指出，“全球移动终端（不仅仅是中国）的另外一个问题是支付系统的基础设施，现有的协议与快速发展扩张的设备、内容以及商品的消费不匹配。既然我们可以相对便宜的生产和配送智能设备，而且数据基础架构也在快速扩张，也是时候支付系统跟上步伐了。这也是我认为利用加密货币可以大量减少甚至移除摩擦（例如，众多机构、老化的设备、政策）的地方。加密货币更安全、更快捷、更便宜。由于这三个主要的优势，加密货币也更容易扩展。

我也采访了Jack Wang，一家名为Dearcoin的比特币初创企业的联合创始人。Dearcoin是研发比特币的消费者应用的，包括Bitpass---基于比特币的认证协议。Wang之前研发了一个比特币交易和商户工具，为General Assembly（纽约的一家创业教育机构）讲授比特币的课。他说道他喜欢“应用程序里包含的那些概念如‘彩色币’。比特币最大的创新之处在于它是一个分布式、可验证的总账系统，它作为货币只是其中的一种应用。在考虑到比特币的多个研发方向，我相信这种类型的系统会有很多潜在的颠覆性的应用，尤其时当我们进入这样的时代：

- 1)数字财产变得越来越有价值
- 2)所有财产的权利验证变为数字化。

假如比特币成为数字产权验证系统和管理的实际系统，那么它的价值就不会仅仅局限为货币的价值。”

Jack Wang通过类比无线通信行业的频谱解释了比特币的这一现象。在块链上传播和记录数字版权的能力将取决于比特币的所有权。拥有比特币的人可视作拥有这些权利。据他介绍“该应用程序可以包括任何实际权限认证-----合同、股票、房子和车子的所有权、房子和车子的钥匙的所有权、数字资料（音乐、美术等）。长远来说，我看到加密货币在很多方面的性能比如说可互换性、可转让性、无限可分性都使其在很多方面可以取代法定货币。今天，人们不再以物易物了，因为用5000个三明治去换一辆车几乎是不可能的，但你可以通过加密货币做到，加密货币它不仅仅是作为一种货币，但也是可以作为彩色币或者类似的东西。也许我们应该把这称作是：加密易物r(cryptobarte)。这也开辟了许多商业机会。因此，一旦加密货币作为除法定货币外能交换东西，传统的机构和商业模式确实会受到很大的冲击。”

当然，问题的关键在于吸引越来越多的人采用加密货币技术，使其在交易中充当一个很有用的媒介。来自香港的Eddy Travia，他是Bitcoin Institute的创始人以及世界上第一家种子期比特币初创企业虚拟孵化器Seedcoin的联合创始人。 他对如何能做到这点表达了自己的想法，他与其他Seedcoin 的天使投资人也正在寻求这样的领域：“能够使交易清晰、终端用户操作简单的任何应用，像Hive,一个内置应用程序的比特币钱包。开发团队的另一个领域是找出大众熟悉并且在他

们的日常生活中经常使用的东西，比如说CoinSimple，它使得商户在多个支付系统之间的切换变得简单，从BitPay 到 GoCoin 、BIPS 、 BitPagos 以及其他的市场参与者。.所以，这就意味着更多的商户能够接受比特币，因此更多的客户就可以使用它们的服务，也可以无缝地使用商户采用的任何比特币支付处理系统”

Travia补充道，“在某些国家，我们还在忙着帮助建设基础设施，比如墨西哥一个可靠的比特币交易平台MEXBT。 因此，一旦该部分完成（在全球各地都有交易所与支付端口可用），潜在的用户群将大幅增长。它仍需要扩大以便越来越多企业能够有足够大的市场来支撑他们对应用以及本地化定制的应用中（语言、法规等等）的投资。”

他继续说：“比特币也正处于金融和技术之间的交叉点，所以它没有像‘电子邮件’或‘安卓系统Android’那么简单，当地的法律法规必须加以考虑。当涉及到大规模应用，往往必须考虑法律因素。用户习惯了银行、移动运营商、信用卡公司，因为我们再也无须去阅读印刷精美的所有合同。但是很有可能比特币相关服务也有印刷精美的东西-----而人们不得不习惯它。有了这方面的知识和了解，Seedcoin 在某种程度上是天使投资人的一个通道，而且也能使小玩家投资这些公司并成为天使投资人。”

潜在的商业机会

随着许多用户和评论员相对集中在一个数据点，一个应用案例，即有争议的是，克里斯坦森式破坏和熊彼特式“创造性破坏”将来自于无需信任的资产管理。

企业和企业家面临的问题是，与其他地方一样，你能提供何种独特的价值机会？对需求分析有经验的商业分析师可能会找到机会为符合具体需求的智能合同设计和创建多种规格。同样，程序员将需要利用这个设计和实施计划然后按照适用的规则编写成代码。商业律师将作为顾问起草和谈判合同、审查代码，甚至是要按照Nick Szabo在十五年前归纳出的步骤做。但是要注意，如果说历史是未来的向导，长期来看很有可能这些智能合同最终会变成开源---标准化---因此，需要另谋收入来源。当我向Nick Szabo提出这个问题时，他说道“传统的合同通常由法律界以开源而不是版权的形式处理的。绝大多数的合同条款是模板，我希望智能合约的代码最后也能发展成这样。在加密货币社区（或广泛地说，块链社区），我们不该信任不开源的代码。”

事实上，已经有一个自发的叫做“算法合同类型统一标准（Algorithmic Contract Types Unified Standards）(ACTUS)”的组织正，在试图建立一个标准语言和以合同为中心的框架，来表示一个参考数据库中所有已知的金融合约。

为了听取多方观点，我也与Sean Zoltek交流过，他是纽约一家专门从事证券化和抵押的公司律师。在将一个智能合同设计和编码到计算机算法上，“我们可以轻易的制定一系列的编程规则，这种编程规则含有大量基于历史记录的各种缺省应答，而且大约有99%的把握知道如何实现。事实上，我们一直在使用标准化的形式。在过去的几十年里，无论是语法结构、还是现有的法律框架，都已经建立起来以支持这些类型的合同。例如，我可以起草一个小企业的贷款合同，包括提供默认条件的复选框。这类工具的用户界面已经存在，并且已经被简化到团体只需要做一些标准化的回答，如现有贷款的类型、资产、借贷时间。事实上，在律师事务所的许多同远比商业银行的要复杂，这是由于我们有专业、具体的案例知识。”

在他看来，现在只需要三四页的文档，或几十行代码就可以实现了，也可以完全自动的实现，不需要代理人或者律师来填一大堆的表。此外，由于它先前的案例法规是非常健壮的，法官可以审视智能合同，而且它是可以强制执行的。Zoltek认为“智能合同已经可以包含此项功能，例如，基于可能的贷款类型这样一个背景，接下来同一个银行服务产生的1000个交易（贷款）有可能是完全相同的。小额企业贷款是一个很好的例子，因为它通常涉及2000万美元的资产、商店或办公室10万美元的库存以及一些标准保单。我们甚至不用担心电子动产契据或者信用证。另外，这样的合同机制对于参与双方来说都是公平的，因为双方都需要提供输入。这与大多数银行提供给借贷方单边的服务条款且不能协商这一事实形成鲜明的对比。”

据他所说，在简化的接口和默认的条件（如信任，履约保证等）下，帮助小微企业成功是符合公司的利益的，“这完全可以用计算机代码实现，这肯定会让许多律师出一身冷汗。这反过来意味着我们的行业将会朝着复杂化和专业化的方向发展。但是偶尔也有细微的差别，并不能完全直接化或者简化。有了固定的规则，也有了它如何应用于环境，因此有些组织必须做出本能的判断。随着时间的推移和相关判例法规则的建立，最终将达到自动进行千篇一律的交易。这一情况会被加密货币如比特币放大，因为加密货币交易成本低或者没有交易成本，有明确的价值分配、价值传递、大家都信任的开源算法。你可以在此之上构建新的机制，提供超出现在比特币协议能做的更复杂的交易和金融工具。因此，一旦你搞清楚建立在新协议上的典型合同如何运行我认为这对所有参与方都是有益的。”

由于智能合同是开源的，Zoltek 提到，“在法律界有一句老话，如果你有能起作用的语言，那就用吧。除了诉讼案件（涉及一些原始创造力），合同本身几乎没有任何创造力。事实上，很多的摘要是可以重复利用之前案例的整篇文章、引用和分析，当材料承受法律挑战时这是一个常见的做法。换句话说，一旦你有了一个好论点，你可以重复利用它。此外，一旦我们制作合同，它就会变成公开的，因为它是在SEC或者其他机构备案的。事实上，没有合同里谈到了‘GE版权’--这仅仅只是一个合同。所以，如果你能通过自动化实现一些事情使生活变得更容易，我们将不得不分化进更基于创新的利基市场，这是2007年以来整个行业大体的趋势。”

然而与此同时，有经验的金融工具程序员和设计师，在这一领域还是有很大的潜在空间的。例如，Sean Percival，500 Startups的一个风投合伙人，近日解释道，“很多工程师都希望跳槽到纽约的高科技领域的初创公司，但他们的技能并不完全适合。但他们的金融编程技能与比特币相关公司非常匹配，这可能是一个绝佳的机会。

正如Szabo和其他人所指出的那样，数字货币领域内最容易摘取的果实包括金融工具和其他通过代码执行的合同，这也包括现有的以加密为基础的金融工具。例如，使用开源的Cryptotrader软件，程序员已经能够在法币-加密货币交易所如BTC-e上建立和执行套利交易。合乎逻辑的下一步就是建立一个智能合同与各种加密总账系统交互，比如说，Bitcoin 到 Ripple 、 Bitcoin 到 Counterparty（或任何其他总账）。另外，智能合同也可以是一个简单的发票-----用加密货币支付-----能够对客户提供服务并开具账单。 它也可以是担保合同，比如怎样通过众筹网站筹集资金（例如，我要交付这个产品，如果截止到Y天我能得到数量为X的认捐）

Mike Hearn在Turing 2013的演讲中曾提到，凡是能够数学量化和规范化的任何重复性工作（如填写电子表格，开立银行帐户），将会被自动化所取代。只有创造性的事物才难以被自动化。展望未来的几十年，Hearn认为其他部分也会在DAOs推动下自动化，如出租车供应商，商品交付（如水果和蔬菜），计算时间的单位（云服务），甚至是“智能道路”。

从某种意义上讲，DAO是一个自治代理，作为一个自身就是经济行为者的计算机，它把自己赚的钱都花在自己身上了，因此，它也可被称为人工生命的最初形式（尽管它还不智能）。如果一个DAO很成功切能盈利也可以成功自我复制其代码库，那么就可以创造一个“孩子”，以“与生俱来的贷款”的形式转让资产。如果它经营不善，它就会“死亡”（即从市场中被清除）。从长远的角度来看，如果你正在寻找这一领域可观的投资来说，这还是是非常重要的。

汇款、增值服务和法律方面的考虑

目前,美国多个州和联邦机构正在评估加密货币的冲击。具体的政策意向尚不清楚。然而在过去的一年里,美国参议院,证券交易委员会(SEC),商品期货交易委员会(CFTC),纽约金融服务局（NYDFS）和金融犯罪执法网络FinCEN(等)多次举行听证会收集相关信息，并不时提供监管指引。例如,在2014年1月28日和29日举行的为期两天的听证会上，纽约金融服务部就可能的监管政策与十多名证人进行面谈，证人证词覆盖领域内几乎所有话题。第二天,即2014年1月30日,金融犯罪执法网络FinCEN独立发布两个新规则,认定矿工和投资者都不是货币转账者，因此不需要执照。

2014年2月19日,加州议会发布的“AB- 129法定货币：替代货币”法案得以一致通过，该法案澄清比特币和其他虚拟货币可以作为货币持有和接受。华盛顿州最近更新其州立章程，“虚拟货币,也称为数字货币或加密货币,是一种无需经政府授权或采用的交换媒介。网络上有许多不同的数字货币被使用,最为人熟知的是比特币。在华盛顿,统一货币服务法案(UMSA)，,19.230章RCW中“货币”的定义包含了数字货币。”其他国家如中国和英国，有不同的相关法律。 2013年12月5日,中国人民银行发布了一份通知,禁止第三方支付通道(如支付宝和财付通)为加密货币交易所提供人民币充值渠道。形成对比的是,2014年3月2日,,英国的税务机关宣布放弃对比特币交易征税。

随着这些问题正得以逐步解决，其他领域中的监管不确定性可能会得到缓解。解决物流问题的一个方法是使运输条款生效，否则各种各样的交易对手规定就会生效。也就是说,如果在交易你的汽车时，你的州机动车辆管理局（DMV）无法将一个特定的智能合同或货币传输确认为正式合法的交易方式，将会怎么样?虽然你可能会找到一个合法的解决方法,但这还是以物易物的经济。举个例子，,如果法币交易所系统关闭，特定加密货币的价格发现受到影响,用户就会将其替换成其他与其价值基本相当的资产。

区块链和政策相交的另一个领域是加密货币（如比特币）的传输。由于加密货币是基于点对点传输的，所以它们可以瞬间就传输到世界的任意角落。例如，Alice有朋友或者家人在海外工作，当需要用钱的时候，若选择使用Eurogiro或者Western Union 的汇款服务，费用又高而且没有增值。此时，Alice可以发送给Bob任意数量的比特币而不需要任何手续费（也可以是其他基于密码学的令牌）。

事实上，Western Uniom在2012一年里光手续费收益就是46亿美元，净利润率达16%。世界银行最近的一个报告显示，。在2013年，2.32亿在外工作的国际移民汇款大约为5500亿美元---最大的三个汇入国为：印度710亿、中国600亿、菲律宾260亿。不同层次的中介，交易所、合规部门从中收取费用合计达740亿美元，而且没有产生任何价值。例如，平均每个非洲移民要付12.4%的汇款手续费，因此，将费用降低至5%，都可以使整个非洲大陆节省40亿美元。全球的平均汇款手续费是9%，而且很多银行还会额外收取5%的手续费用来换成当地货币。

在2014年2月份，我采访了Alan Safahi，他是ZipZapInc.的CEO。ZipZap是全球最大的现金交易网络，其用户可以用现金购买数字货币。通过这种方式，它在收集法币的支付中心与提供比特币流动性的交易平台中间充当一个机遇软件的金融中介角色。根据Safahi，ZipZap正在建设在全球范围内都可以将物理现金转化为电子货币的双向汇兑端口(both on-ramp and soon off ramp connections)，也希望将来有一天他们能够提供一个完全免费的汇款网络。“我希望汇款的手续费能降到0,现阶段我们需要收取汇款双方节点的手续费，然后随着时间的推移，我们只需要收取法币兑出费用，到最后，这将变为一个完全免费的模式，通过使用比特币类似的加密货币，一些基础服务比如说汇款是免费的。”

“作为产业，我们必须在免费汇款服务之上提供增值服务以吸引顾客” Safahi补充道，“这与在线游戏社区类似，它成功的通过采用免费模型来提供玩家们乐意付费的附加产品或功能加强。”

Safahi想颠覆现有格局。鉴于目前客户如果他或她从发展中国家汇款，需要满足一定的硬性标准，而且需要支付相当高的手续费（甚至在某些情况下会被拒绝）。Safahi想让客户转移他们的财产变得更容易。因此，“我们的使命是使客户的生活变得更简便，转变思维，在金融服务产品前客户第一而不是服务提供商。” ZipZap在2012年推出了全球现金支付网络，现已发展了700,000个支付网点。ZipZap最近在英国新增了28,000个支付网点，并将继续与更多的比特币交易所（如Bittylicious, ANX, Kraken, CoinMKT, and BIPS Market)）保持合作关系，使得客户在任意支付网点能够将当地货币兑换成比特币。

我也曾采访过Charles Hoskinson，Bitcoin Education Project的创办人以及Ethereum（以太坊）核心开发团队成员。考虑到DAOs以及无信任资产管理即将带来的冲击，他认为，“最简单的理解就是新兴市场里的35亿人面临着财产和合同的两种模式。第一是，由于机构组织和激励的不同，那些社会关系良好以及愿意去花钱贿赂政府官员的人能够保护好自

己的财产。由于受制于政府内部的变化（如政要免职）这不是一个很稳定的结构。另外一种模式是灰色系统，这是一种基于握手信任和地下灰色交易的非正式经济类型。”

因此，他认为，“对于定居海外的发达国家居民来说，因为缺乏明确的规则和财产权利，做专业的投资是冒险的，而且也很困难。当你对相关法律很了解的时候，比如说成文合同和仲裁制度，那么投资不仅会更加透明，而且更加安全和高效。像Ethereum这样利用了DAOs的项目，它们提供了很好的第三种选择：他们不需要向政府部门行贿。用户也不需要担心模糊的灰色地带。相反的，你可以很信任这样一个基于数学的账簿-并产生财务透明。所以，由于它点对点的本质，它可以超越任何司法管辖，可以被任何人用来跟踪和管理资产。这将改变发展中国家以及发达国家市场的商业行为。”

由于这是自治的系统，它也将改变银行业以及资本转移、获取、存储以及管理的方式。关联到现有司法体系的智能财产也有可能受其影响。据Hoskinson所说，“我们在五年前就开始留意法币与比特币的交易，DAO可能会同时扩大其应用及社会影响。例如，至少是1991年以后有大量的方法构建信誉系统---- 信用网络----以激励用户及时还款。通过区块链，你现在将拥有一个安全的地方放置某个金融工具或合同，然后人们可以对其进行数字签名。由于它是公开审计的，其他的用户可以看到历史记录，如果认为它是可信任的，就会建立信用评分。相应地，基于清晰界定的条款和服务的商务交易可以通过身份认证管理的形式在交易平台上进行。这将彻底改变资本流动和投资的运行方式。对第三世界来说，这也将是一个天赐良机。例如，某人有一个可信赖的DAO（或智能合同）可以创建一个货币工具（加密货币），然后在特定的条款和条件下，将其以贷款的形式借给世界上的任何人。这是可以通过外部的、防止篡改的系统（指区块链）完成，不会被可能滥用的机构所控制的区块链。因此，对于发展中国家来说，正如他们跳过铜缆而选择无线电话，有些人可能会放弃建设现存金融基础建设的复制品而选择在他们的移动设备上使用这种虚拟货币系统。”

1.当前最成功的移动支付系统是M-PESA，由Safaricom 和 Vodacom共同运营，在东非（Kenya 和Tanzania） 、中东地区以及印度服务了3000万用户。这是一个基于手机的转账以及小额金融交易平台。去年夏天，Kipochi将比特币轻钱包整合到了M-PESA中，这使得肯尼亚人民可以省掉由中间商比如MoneyGram 和Western Union收取的大量汇款费用。虽然有些人会无视移动银行的这种可能性，而喜欢桌面台式机或者亲自去银行的物理网点办理业务，肯尼亚43%的GDP是由移动手机支付完成的。事实上，根据路透社最新的报告，“M-Pesa使得67%的肯尼亚成人接触到银行，它每个月的交易量达到了10亿美元。” 在非洲大约有2.53亿单独的移动手机订阅用户（很多有两张SIM 卡），这片大陆上约70% 的人是没有得到金融服务甚至无法接触到银行。因此，建立在加密账簿上的加密货币以及无信任资产管理工具与移动手机交互，可使得一个全新的消费者群体诞生。实际上，根据Financial Access Initiative上2009年的一个报告，全世界有一半人是没有银行账户的，这对于创业者来说是一个全新的机会。

第七章：如何成为这个加密货币生态系统中的一员

对于加密货币，不论你听说过多少，或者研究了多深，现在市面上有多条途径，可以让你获得你的第一笔加密货币筹码。你可以通过挖矿来挖得，也可以在交易所买入获得，如果你是一家商户，那么还可以通过售出商品来换得。

挖矿

很不幸，现在想要通过挖矿获得比特币，并有利可图的话，需要投入一大笔资金去买入专用的ASIC矿机[10]。尽管，你可以使用的云端挖矿服务（比如Ghash.io提供的），但这样的话，你对整个比特币网络的工作原理，就不会有太多的了解。

事实上，就算是部署了ASIC矿机，大多数的挖矿系统，仅仅依靠自身，是无法完成选择、或者验证比特币交易的任务的；你仅仅是把你的矿机算力卖给了矿池。还有一种低成本的挖矿方法，那就是购买小号的USB ASIC矿机（比如说BitFury提供的）；但是，需要注意，你可能得指望挖到的币，其本身的升值，才能赚回挖矿所花销的电费（举个例子，假设你挖到了0.1个比特币，价值80美元，但你的挖矿电费是85美元，这样的话你就得等比特币升值，否则就亏了）。

在过去的几年里，在比特币挖矿业，出现了一种新的商业模式：预订。总得来说，就是客户先拿出一定数量的比特币，发给ASIC矿机制造商，该厂商使用收到的比特币，来进行投资、设计、制造、并最终把矿机发货给相应的客户。为了尽量地降低成本，厂商会分批次接受订单，每个批次的订单上，还会有一个排队列表。你在排队列表中的排位越靠后，收到矿机所需要的时间也就越久，然后才能开始挖矿，以赚回你的初始投资。尽管你可以碰碰运气，在发货之前就预订第一个批次的矿机，但风险可能会大于收益。你的资本，绑定在一种会不断贬值的资产之上，ASIC矿机不像是GPU那样[11]，还可以转卖给游戏玩家，或者3D图形设计师，它的二手转卖价格会不断降低、用途单一、可能不会按时发货、最终发货的产品的实际性能，也不能被预先确定。

或者，你可能会想，你的订单，在KnC即将推出的Neptune矿机的排队列表上，有可能比较靠前，就和那些去年冬天，才拿到阿瓦隆矿机芯片，或者今年1月份，才收到CoinTerra的新款T级矿机的人，当时所想的一样。但是，很大的可能，情况不会如此，如果你在阅读这段文字的时候，还没有下订单的话，那就更加没可能了。去年蝴蝶实验室（BFL）的ASIC订单的延期，就是一个活生生的例子。蝴蝶实验室，最早于2012年7月宣布，将推出多种型号的ASIC矿机，随后，几百名客户使用比特币进行了预订。然而，在开发和测试的过程中，他们遭遇了一系列的麻烦，发货时间被整整推迟了一年多。举个例子，在2013年3月的时候，我的一个比特币投资人朋友，花了50个比特币，在BFL那里订了4台ASIC矿机，每台的算力是25GH/s。他在去年11月末的时候，终于收到了那批机器。如果他不买矿机，而是选择持有那50个比特币，那么，在当时（2013年11月），他的那些币，可以在多家比特币交易所里，兑换成40,000-50,000美元。如果他把收到的矿机插上电源，并开始挖矿，100GH/s的算力，根据当时挖矿难度的上涨速度，一整年也挖不到1个币，更不要说挖回那50个，用于购买矿机的币了。

> 注释：
>
> [10] 专用集成电路（英语：Application-Specific Integrated Circuit，缩写：ASIC），是指依产品需求不同，而定制的特殊规格集成电路。
>
> [11] 图形处理器（英语：Graphics Processing Unit，缩写：GPU）。

购者自慎

如果说历史值得借鉴，那么，就让我们回顾一下，美国加利福利亚州的那场淘金热吧[12]，最后赚的满盆钵的，是商户以及服务公司，比如说塞缪尔·布兰南（Samuel Brannan）、菲利普·阿莫（Philip Armour）、约翰·史蒂倍克（John Studebaker）、利维·斯特劳斯（Levi Strauss）、以及韦尔斯·法戈（Wells Fargo）。制造和销售挖矿设备（镐、斧头、铲子、洗矿槽）的那些，最后的y结果是有赚有赔。而获利最少的，却是矿工们，因为他们几乎是暴露在各种各样的风险之中（前期资本成本，土地所有权的诉讼，恶劣天气，疾病，山体滑坡和塌方），并且因此，最后大部分人破了产。可是，如果你有一种参与加密货币挖矿的冲动，希望藉此更好的理解区块链验证，以及区块连网络的话，你还可以考虑，挖一挖其他的加密货币，比如说莱特币或者狗狗币，这两者都基于Scrypt算法。Scrypt是另外一种工作证明（比特币使用SHA256d算法），并需要使用更大的内存池，这反过来，使得它更不容易因为ASIC矿机的出现[13]，而导致全网算力的暴涨。这样，你就可以仍然使用那些除了挖矿，还能有其他用途，并且具有一定转手价值的GPU，来进行挖矿。

> 注释：
>
> [12] 始自1849年，贯穿19世纪50年代在美国加利福尼亚的发现大量黄金储量后的淘金浪潮。
>
> [13] Scrypt算法需要消耗大量的内存，内存的成本非常高，故相对更不容易出现ASIC矿机。

商户生态圈

我们在第二章里，简要的谈到了比特币生态圈中的，一个里程碑式的事件：2011年，有人用10,000枚比特币，换回了一份披萨。这被认为是，为公众所知的，第一次价值转移，并因此，成为了比特币和法币兑换汇率的起源。

自那之后，比特币的商户生态圈逐渐成长，已经吸引了大约50,000家线上商户加入其中。BitPay是在这一领域里，最强大的创业公司之一，它为网上商户，提供了一种接受比特币的，电子支付处理系统。2013年，它处理了总价值超过一个亿美元的比特币交易，并且，和20,000家以上的商户，签订了合作协议。Gyft，是一种接受比特币，作为其支付方式之一的，数字移动端礼品卡（Gift Card）钱包，它使得用户，可以通过使用移动设备买入、发送、接受、管理、以及兑换数字礼品卡，并且可以在超过100,000家的零售店使用。2013年11月27日，Shopify，这是一家大型的电子商务平台，宣布它旗下的75,000家商户，现在全部接受比特币支付。2014年1月9日，Overstock.com开始接受比特币支付。这一计划启动的第一天，Overstock.com就收到了价值126,000美元的比特币付款订单，并且，在接下来的两周之内，那个数字持续攀升，超过了500,000美元。随后的2014年1月23日，TigerDirect宣布，它将开始接受比特币，作为其支付方式中的一种，并且在第一周之内，就处理了价值高达500,000美元的比特币付款。2014年2月27日，Coinbase宣布，其消费者钱包的注册用户，数量超过了1,000,000，而在2013年年初的时候，这一数字不过是13,000——除此以外，更有超过25,000家的商户，已经在开始使用Coinbase平台。

同时，每天都还有其他供应商和商户，独立地加入支持比特币支付的行列。Zynga，作为社交游戏Farmville[14]的开发商，于2014年1月4日宣布，它将开始接受比特币支付（通过使用BitPay提供的服务）。在此之前的2013年5月9日，HumbleBundle宣布，它将开始支持比特币支付（通过与Coinbase合作）来购买它的游戏套装（随后，支持扩展到了整个商店）。除此之外，在CES 2014期间，Formlabs这家3D打印机的制造商，宣布它家的在线商店，现在开始支持比特币支付。还有，2014年2月4日，CheapAir.com宣布，它将开始支持使用比特币，来支付酒店费用（更早之前，该公司已经接受使用比特币，来预订机票）。

在第三章里面，我们介绍过乔恩·霍姆奎斯特（Jon Holmquist），他在担任Ripple实验室的社区联络人，同时还是比特币黑色星期五（BBF）的发起人，BBF是最大的比特币线上购物促销日，时间定在感恩节之后的第一天，所有参与活动的商户的商品，都会出现在同一个网站上。2012年秋季，他发起第一次BBF的动机之一，是“我当时正在和一家比特币商户合作，我们发起过各种形式的促销，以吸引来自比特币社区的支持，但是讽刺的是，当时找不到一个信息聚合站，来为他们做导航。我还留意到，有许多商户，他们各自独立地开展着促销活动，我当时就觉得，创造一个信息聚合站，将是一个伟大的实验，”

霍姆奎斯特架设好了网站，顾客陆陆续续开始光顾。2012年，也就是BBF的第一年，合作商家有60户，而到了2013年，这一数字上升到了600户，并且他们希望，今年能和6,000家商户达成合作。BitPay去年11月29日，处理了6,926次使用比特币的交易，而在前年的同一天，只有99比。但是，对于霍姆奎斯特而言，有一个可观的数值，常常被人们所忽略，那就是BBF的客户们，已经捐赠了价值超过100万美元的比特币，给慈善事业。这件事，如果是通过常规的信用卡交易途径，预计手续费会占到总金额的5%（也就是50,000美元）。而通过比特币来完成的话，这50,000美元，就流向了慈善事业，而不是信用卡公司。尽管这一事件，在比特币生态系统中，属于偶发事件，但在霍姆奎斯特看来，“这仅仅是一个开始，消费者从此，能够更容易的进行价值转移。同时，对于企业家和开发者们而言，他们可以持续地，通过提供（比如像网站插件这样的）一站式服务，来帮助那些想要支持加密货币支付的商户简化流程。”

或许，比特币，做为虚拟货币的特定化身，不过是一场流行风潮，商户们最终会完全放弃对它的支持。如果真是如此，切换到另外一本总账，将是相对简单的，因为，现有商户系统的前端以及后台，都可以改用其它竞争币（altcoin），或者竞争协议（altprotocol）。但是，上面所谈及的这些案例研究，充当着价值怎样可以跨国地、面向任何人地、安全地、可靠的、几近即时地进行转移，而不需要任何中间人，或者机构的介入的实证范例。

> 注释：
>
> [14] 到2010年三月为止，FarmVille的用户数已到达八千多万人，是Facebook中最受欢迎的应用程式，而加入FarmVille Fan 的的用户数也到达二千多万人[4]，FarmVille用户的总数约占 Facebook 总用户的 20%，超过世界人口的 1%。国内类似的游戏有《开心农场》

开发者，开发者，开发者！

我对话过的所有投资人，以及软件架构师都认为，这一生态系统，持续地需要有能力并且有创造力的程序员的加入。并且，因为这一领域是如此的新颖，并在不断地演化，进入门槛非常之低。因此，具有一定商业嗅觉的新手程序员，可能可以在这个不断成长的生态系统中，找到创业机会。

BTCJam

我和BTCJam的创始人，塞尔索·皮塔（Celso Pitta）聊过。BTCJam是一家创立于2013年的公司，其业务已经拓展到了全球131个国家，拥有超过12,000名的用户，这些用户之间，已经互相提供了，价值超过500万美元的，基于比特币的贷款。这一切的实现，是通过把一个全球性的点对点支付协议，与一个信用评分系统融合到一起，匹配之后，把相应的比特币借出给借币人。皮塔来自巴西，在此之前，他是在花旗银行的信用卡部门工作，与统计模型打交道。他创办这个P2P的借贷平台的动机，主要是因为巴西信用卡的利率激增，年息差不多高达200%。这与发达国家的，相对较低的信贷成本之间，形成了鲜明的对比，因为，在像巴西这样的新兴市场里，信贷选择匮乏，客户找不到什么替代品。

据皮塔所说，“除非你可以接触到FICO信用评分系统，否则，很难获得一定的信用额度。”并且，考虑到他们缺乏金融机构，以及基础设施的发展现状，大部分新兴市场，不具有一个能够准确衡量借款人的信用的信用评分系统。

相较之下，通过开放注册，用户可以在这里，提交所有他们认为合适的相关细节资料，我们已经开发了一个统计模型，这个模型，可以对他们的资料质量进行排序，并给出一个更加精准的评价。比特币网络本身，是一个完美的小额借贷平台，因为比特币可以细分到小数点后8位的特性，提供了金额拆分的灵活性，并且转账既安全，又相对快捷。

而在法币系统中，商户和贷款人面临的，不只是欺诈性扣款索偿的风险，还有与借贷金额无关的，高额固定费用（例如，借出1美元，手续费就占了10%）。使用比特币的话，某些人，就没有办法通过扣款索偿的把戏，玩弄这个系统了——比特币一旦被发出，那就是真的被发送出去了——交易不可逆转。并且，尽管在我们的系统中，也存在借款人还不起贷款的事情发生，但我们现在的履约率高达98%，对比之下，全球P2P借贷履约率，平均只有92%。

根据2013年，律商联讯（Lexis/Nexis）发布的报告，他们发现，线上商户需要为每一美元的，发生在互联网上的欺诈损失，支付3.1美元（也就是说，除了支付欺诈索偿费用、欺诈监控成本、以及银行收费，商户们还得承担商品的损失）。加密货币，可以用来应付这样的麻烦，因为它们一旦被发送出去，就不能再被收回，也不能被双重花费。皮塔认为，在银行服务不健全，甚至没有银行服务的地区，企业家们如果想要帮助当地人，获得更好的服务，那么对于他们而言，在这一领域，还有其他的机会。事实上，他发现借款人获取信用额度的动力很强，并且因此，会为了能够使用比特币和其他加密货币，而进行自我教育，以了解它们是个什么东西。但是，对于与事双方而言，挑战也摆在眼前：“于法币（比如说巴西的里亚伊R$）间的兑换不易，监管架构（在大多数国家，这仍然属于灰色区域）也不明晰，这阻碍了双方的入场。”

对比一下，像Prosper和Lending Club这样的，坐落于美国的P2P借款公司，2013年发出了24亿美元的贷款。为什么要提到这个？根据国际收支结构协会的数据，整个2010年，全球交易服务（GTS）的平均现金流利润率是38%，这给银行带来了源源不断的收入。像这样可观的利润率，使得这个领域，很适合出现技术上的突破以及创新。

众筹股票 Crowdequity

2014年2月的时候，我和乔尔·迪茨（Joel Dietz）聊过，他是Evergreen的CEO兼创始人。Evergreen是一个协议层，它可以把中心化节点提供的服务，和比特币网络连接到一起，并且它在设计之初，就把易用性摆在了很重要的位置。这一协议，使得开发者可以建设一个底层基础设施，以开发原生支持微支付的移动网络应用。

有了这一经验之后，迪茨认为，智能合同以及分布式自治组织（DAO），在未来将具有重大的影响。他说：“我认为，当下许多合同设计师（比如说律师）所做的事情，可以并且将会是成为自动化的——一行行的代码，将取代他们，完成相应的工作。合同最终只是代码，并且是这一领域的创新和应用。（Contracts are ultimately just code and are the

new innovations and apps to this space）”事实上，我认为到今年年底的时候，多种智能合同就会出现在市面上——这些合同具有易用性，并带有托管和验证功能。当然，首先得要有一个平台。但我认为，这相对而言，是比较轻松就能实现的，因为已经有了原型代码。

在他看来，分布式自治组织“从聚集资金的角度来看，具有许多好处，因为它使得组织者只需要履行核查的职责就可以了。密码货币总账的特性，以及多重签名的功能，提供了审计和逻辑判断的能力。这一手段直观且透明，同时相较于其他众筹技术，在可量化的范畴内有着更佳的表现。

举个例子，因为目前系统设计的限制，当下不存在一种途径途径，可以用来直接的回馈用户群，特别是那些贡献了内容的早期参与者。以推特（Twitter）为例，那些在网站上发布内容，并说服他的朋友和家人使用推特的用户，并没有得到奖励——只有那些股份持有人（创始人和投资人），有机会获得回报。对比之下，众筹股票，可以通过对贡献内容，和进行宣传的行为进行奖励，以此激励人们入场，创造早期的用户群。并且，最简单最透明的，资助众筹股票的方法，就是使用由分布式自治组织所管理的加密货币。”

BankToTheFuture是在这一领域，最早的众筹股票平台之一，并且已经有10家创业公司，在这个平台上面做比特币相关的项目了。

亚当·莱文（Adam Levine）曾经在一个与Kickstarter币有关的项目上工作过，这个项目提供了想类似的众筹功能，以回馈早期用户，感谢他们的支持。实际上，莱文所提出的，不只是一种使得公司和组织，可以通过一种由密码学原理控制的方式，来聚集资金（通过发行特定加密币种）。与此同时，还可以在那家公司摇摇欲坠，或者已经失败了的时候，通过利用这些加密币，来完成一次反向并购。

就算一家公司的所有潜在创意都失败了，并且放弃了这样的一个币种，但是，这个币种此时低迷的价格，可能会成为它复活的机会。另一家公司，可能会乘机买入这些廉价的、已经被废弃了的筹码。然后宣布他们将忠于企业规划，继续执行产品或服务活动的开展，通过这种诚意和行为，来重建市场对该企业的信心，这个过程类似于，捍卫所有加密货币的内在价值。

2014年2月17日，在众筹领域的一个新项目，揭开了它神秘的面纱，这个项目叫做“加入我的IPO（Join My IPO，缩写为JMI）”。该项目由阿摩司·梅里（Amos Meiri）所开发，他是染色币（Colored Coin）团队的成员，并且将在未来的几个月，发行他的第一个币种。其核心概念是，个人（支持者）可以在某个特定人开始自己的某项事业之前，向该人进行投资。举个例子，娱乐艺人、创业家、还有艺术家，可以通过发行某种币给支持者（朋友、家人、粉丝），来直接地聚集资金。

事实上，任何拥有账户的人，都能发行他们自己的、可自定义的加密货币，并把这些币发给任何拥有Chromawallet钱包（这个钱包，同样用于追踪染色币）的人。在JMI网站上，我们可以知道，项目方可以对给予支持者的回报进行定制，比如说季度性的分红，或者按收入的百分比进行分红，人们使用这些分红，就能享用项目方所创造出来的东西（比如说，书籍、CD唱片、音乐会入场券等等）。并且通过如此操作，发行这样的币种的名人们，有希望能够加强与粉丝之间的联系。与此同时，这些筹码，还能够在交易所里面进行交易，投资人和支持者们，都可以在这里实时地了解该特定项目的情况。

马克斯·凯撒（ Max Keiser）是一名电视节目主持人，吉米·多特空（Kim Dotcom）是一名互联网创业者，他们俩都发行了自己的币种——分别是MaxCoin，和Megacoin，相对于已有的竞争币（altcoin）而言，这些币并没有提供什么太多的新功能。但是，像LTBCoin和Join My IPO这样的项目，将使得用户们，不仅仅是能够使用现有的基础设施，来发行定制的币种，而且还能够使用这些币来兑换现实生活中的价值（也就是音乐会入场券、书籍、分红等）。

信用评分

说到信用评分，尼克·萨博（Nick Szabo）曾经描述过几个用户案例，这些案例与租赁，以及债权人的留置权有关。在一系列的条件被满足（或者不被满足）的情况下，控制权将回到原来的主人手中。尽管，当前的加密账本和加密协议，具有提供使用假名[15]的能力，但事实上，可能会存在某些动机，促使一些用户公开他们的地址。

那也就是说，在需要信用评分的情况下（比如说借贷），你的交易历史记录越是公开，潜在借款人就能获得越多的资料，以评估和量化借款给你的风险。因此，在实践上，鲍勃可能有一个公开的账户，他把它写在了名片上，留在了网站中。但与此同时，他可能还有几个其它的数字前包，他的所有交易、储蓄、收入都存放在这里。史查波观察到了类似的二分情况，说“在隐私性与培养声誉之间，存在着巨大的取舍。

长期使用的假名，也可以用来培养声誉，但目前的监管政策，强烈的偏好于真名实姓。”因此，为每一笔交易使用一个新的随机的地址，在今天已经成为了标准操作流程，但在长远看来，公开至少一个代表自己的账户，所能带来的激励，可能会超过人们对于隐私的关心。

简单和易于使用，是投资人和开发者们，反复提到的另外一个共同话题。尽管那些具备足够技术敏锐度，以及计算机达人们，以及成为了加密货币的早期入场者，但广大普通人群，不只是觉得虚拟筹码的工作原理晦涩难懂，并且不知道怎么去使用、保护、以及存储它们。

> 注释：
>
> [15] 通过使用暗黑钱包，或者零币（ZeroCoin），还能实现匿名。

易于使用、易于发现

肖恩·佩希瓦（Sean Percival），作为一名科技行业的前辈，现在是以投资伙伴的身份，在500 Starups这家风投公司工作。他和我说：“在为这一领域的新创业公司做评估的时候，我有一系列的评估标准，包括该公司所提供的服务的新意，以及服务对于潜在消费者的易用性。对于开发人员和我而言，下载和备份数字钱包，可能只是小事一桩，但对于绝大多数的消费者来说，他们是没有什么时间或者精力，去深入研究学习，这种新型的银行账户的使用方法的。”

值得一提，佩希瓦对于简化复杂度很有兴趣--也就是把技术流程给挪到后台，而不需要用户的关心。他实地与开发人员们一起，研究怎样为用户提供更棒的用户体验，以及更直观的交互界面，所以他发现了无数的简化流程的机会，比如说某特定服务的注册机制（举个例子：在线钱包）。或者，用他自己的话来讲，“提供一种无摩擦的渠道，使得消费者可以在不具备任何技术背景的情况下，搞定相关事物。消费者在零售店刷卡消费的时候，并不需要关注中间的具体步骤，并且，这就是加密货币所应当达成的效果。”

尽管，他和我见过的大部分投资人一样，都对法币-加密货币兑换所不感兴趣，但是，他对于像是存在证明（Proof-of-Existence，证明某份文件是否存在），或者存储证明（Proof-of-Storage，证明某台计算机，是否还有指定大小的存储空间可用）这样的概念的商业解决方案，却是愈发的感兴趣。在他看来，“组建一个合适的团队，找到合适的天才、领导者、以及市场营销人员，做出可以卖出去并盈利的产品，绝非易事，新的概念，比如像存储证明，会激励大量人才冲向独木桥，但只有少量部分人能走过独木桥，并被消费者们所接受。

因此，他们在做市场营销的时候，应当把大量精力投入在培养用户，以及教育用户之上，以此获得用户的信赖，并让用户有一种’酷’的感觉。信赖和’酷’的感觉都是不可强求的，一旦失去，就基本上再也找不回来了。”

我和丹·罗斯曼（Dan Roseman）聊过，他创办了Coinality，这是一个招聘信息发布平台，接受使用加密货币来支付薪水的潜在雇主和潜在雇员，可以在这里相遇。罗斯曼如是说，“尽管总的来说，我对加密货币还算是熟悉，但直到去年4月份的时候，我才开始探寻实际的商业发展机遇。我在2013年9月的时候，创办了这一平台，因为我看到了社区的需求（接受比特币作为酬劳），而其他招聘平台又不能满足。平台从开办到现在，已经拥有了超过1600名的注册会员，收到了来自求职者的，超过1000份的工作申请，以及大约600个的岗位招聘需求。尽管所有工作信息的上传，都会经过人工审核，但大约其中的95%，都能顺利发布，而余下的5%，通常是些垃圾信息，或者不相关的内容。我们的团队，同时还会在其他招聘平台上，寻找空闲的工作机会，并确保这些机会也会出现在Coinality上面。”

“虽说我在Coinbase的客服部门有份兼职，但我现在全职为Coinality工作，希望把它打造成这一领域的重要角色。因此，我对相关领域有着足够的了解。就目前而言，市场对C++和Python程序员的需求量是最大的。中本聪最初写第一个比特币钱包的时候，用的就是C++语言，而Python频繁地为“法币-比特币交易所”结构使用。同时，市场对于图形设计人员（设计徽标、网站布局），还有市场营销专家（带来网站流量）的需求量也很大。所以，如果你拥有这些技能，你将很有可能在这一快速演化的市场中，找到一份工作。”

罗斯曼指出了雇主们为何愿意在Coinality上招募程序员的原因。2014年2月10号，Mt.Gox公开承认它们的钱包系统中存在一个bug，该bug有可能使得攻击者能够成功双花（Double Spend）。

Mt.Gox曾经是最大的法币-比特币交易所之一，并且它的声明，为市场带来了剧烈的波动。但是，它承认的这个bug（交易可塑性），不仅早已为社区所知晓，而且Mt.Gox本身也在几年前，就发现这个bug了（它的内部资料库有一条关于此bug的条目，并且部分核心开发者也曾经指出过这个问题）。这个问题与比特币本身无关，而是与Mt.Gox自己的（容易出问题的）钱包实现方式有关。

Mt.Gox建站之初，是用来交易一款叫做《Magic: The Gathering》的游戏里面的卡牌的，随后它踏入了加密货币领域，但它的程序员们，对于保证交易所安全，所需要用到的安全套件，并不熟悉。因此，在罗斯曼看来，“那些想要招募到具备必要工作技能，以及对这种漏洞的防护意识的开发者的公司而言，他们可以在我们的招聘平台上找到合适的人，这有希望能够防止类似的，导致市场剧烈波动的事件，在未来的发生。

”背负着巨额的债务（65亿日元，约等值与6360万美元），Mt.Gox于2013年2月28日，在日本递交了破产申请（在一定程度上是因为内部财务管理的失败，以及其他技术上的问题）；与此同时，债主们的前途未卜。

BitCloud

我和凯尔·汤培（Kyle Torpey）聊过，他是CryptoCoinsNews的主编，同时还是Bitcloud开发团队的成员。

Bitcloud项目，最初于2014年一月被宣布，它是一个底层协议，适用于那些对带宽，以及存储空间有需求的去中心化应用。据汤培所说，“最开始的想法是通过’带宽证明（Proof-of-Bandwidth）’来创造‘云币（cloudcoin）’，但通过一些探索，我们发现这并不可行。

我相信亚当·莱文（Adam Levine），对于他在Let’s Talk Bitcoin这档节目中，提出的内部项目’LTBCoin’，也有相同的结论。举个例子，随着你开发出越来越多的应用，这种币将很有可能会升值，并因此，云端上的服务也会变得更贵，因为这种币的供应总量是固定的。相类似的，”平衡也很难取得，因为早期接受者可以屯币，坐等升值，而不是使用它们，这会导致‘搭便车问题’，而这一问题已经出现在了比特币和其他加密货币当中。

这也就是说，Bitcloud将是一种第三方的，用于共享存储空间的托管服务。这一服务的实现，将会通过多重签名交易来实现。多重签名交易里面，有多个参与方（鲍伯是存储空间提供方，爱丽丝是存储空间用户），同时，Bitcloud是第三方参与者，即多重签名交易的协调人。

正如我们在第四章中所谈论的那样，多重签名交易，需要两方或者更多方的参与，他们必须在一个指定的时间窗口内，提交他们的数字密钥到某个指定的地址，以触发某个指定动作（比如说释放资金）的执行。

汤培的团队，同时还在开发第一个可以利用Bitcloud的应用，“我们想要开发一个WeTube，这是一个去中心化的Youtube，它基于Bitcloud协议而存在，并且将和Bitcloud同时被推出。请注意，WeTube还只是一个开发代号。我们需要先把Bitcloud给开发出来，所以，我们称作WeTube的作品，最后可能和我们现在看到的全然不同。

新的筹资模式，将通过一个叫做Cloudshares的概念来运作，在这个概念中，通过每一笔比特币交易，用户都将获得整个Bitcloud去中心化应用（一个开放的API）中的权益份额。尽管在最开始的想法中，是准备使用Cloudshares来首先货币化整个Bitcloud网络，但我们现在已经决定，将货币化进程放置于去中心化之前。

所以，为WeTube提供存储空间的人，所接收到的权益份额，是WeTube的权益份额，而不是Bitcloud的。举个例子，如果鲍勃从爱丽丝那里购买了存储空间，他将使用比特币作为中介筹码。作为交换，他会收到一份的Cloudshare，这随即解决了早期入场者的’搭便车问题’，因为许多入场者作为投机者，并不提供或者产生新的价值。我们还可以这样想，Cloudshare就像是去中心化的应用中的一份权益份额，

在我们看来，货币化整个底层协议可不是一个好主意，因为如果你在协议层中有一份权益份额，那么你将会不得不获得分红。或者换句话说，人们不能向Bitcloud进行投资，只能向基于它而构建的去中心化应用进行投资。这样，Bitcloud就是一个免费自由的协议，并且我们不打算对它进行货币化。而现在，我们把权益份额，放在了Bitcloud这一层上面的层次，不同的应用之间的权益份额是不同的。因此，应用们本身，没有被中心化在同一个系统中，而将是和同一个协议（Bitcloud）进行互动。

CoinSimple

2014年2月份的时候，我和尼克斯·本特尼缇思（Nikos Bentenitis）见了一面。本特尼缇思是CoinSimple的联合创始人，比特币基金会教育委员会的副主席，同时还是MasterProtocolEducation.org项目的发起人。我们在本书第六章里面已经简要的提到过了CoinSimple，在这里，我们再用本特尼缇思的话来介绍一下，“CoinSimple使得电子商务的商户们，可以极其容易地接受比特币支付。通过CoinSimple，你可以使用任何现有的支付处理商（BitPay、Coinbase、BIPS、GoCoin），并且，你完全不需要找个程序员，来帮你把它们整合到你的电商商店里面去。我们已经帮你完成了开发工作，并且还添加了一个界面简明的，消费者分析的功能。”

讲到在运作在下一代平台上面的智能合同，最早会出现的使用情境，他认为可能会是“有财货作为背书的，可以用于项目资助的加密货币的发行。举个例子，一家太阳能公园，可以通过发行一种自定义的加密货币，来获得资金，而这种加密货币的购买者，可以在公园开始运营之后，获得一定量的电能作为回报。”相类似的，他认为加密货币相关应用的采用率，在不同地区的差异将很大，这在很大程度上与基础设施发展程度有关，“对于那些生活在美国，以及其他发达地区的人们而言，加密货币相关应用比较难以成为杀手级别的应用。堵车，对于世界上其他地区的人们来说，简单的支付手段（比特币协议中已经支持了），遇到现有设备（手机、银行卡）时，将成为杀手级应用。”

因此，他还认为，现在还有一些被忽视了的尚未开发领域，包括教育，“这一领域发生的事情太多，就算是最积极的投资人，也没有办法抓住所有的、每天都在不断冒出的、令人惊讶的机会。在这一领域的教育和研究机构，比如说我合作的德克萨斯州大学、尼科西亚大学、还有香港大学，可能会为投资人和创业家们提供一种，能够更快的发现商业机会的途径。”

关于在这一领域的教育方面的机会，本特尼缇思提出了一个有趣的想法。就如同编程语言和网络工程，催生了数不清的培训项目（CNA、CCNE、MCSE、A+）一般，很有可能会有类似的市场需求，培训师们可以为开发者和创业家们提供相关培训，以使得他们可以高效地利用这些新平台。也许你的公司，就能创造一个用于证明加密货币，或者智能合同设计能力的证书认定程序。相类似的，作家和写手们，可能会通过奥莱利媒体（O’Reilly Media）这样的平台，找到新的读者。除此之外，在我和本特尼缇思对话期间，他留意到，比如说像Udacity和Coursera这样的MOOC（大型开放式线上课程），可以被用来向全球用户，提供加密协议的课程和培训。截止2012年6月，全球大概有24亿的互联网用户，这些用户中的部分，可能会有兴趣并有能力，更深入的对这一领域进行研究。

BitPay

二月份的时候我还和斯蒂芬·佩尔（Stephen Pair）聊过，他是BitPay的联合创始人，兼BitGive基金会的董事会成员。如本章节之前所说，BitPay是一家大型的商户支付处理商，并且它最近放出了一个bitcoinJS的分叉，叫做bitcore。据佩尔所，“做bitcore的目的，是简化使用比特币协议，来开发应用的流程，而不需要去和C++打交道。通过使用JavaScript和node.js，开发者们可以更轻松地，在任何操作系统和平台上，运行他们所写的代码，创造一种非常灵活的、可以满足我们初始目标（开放、可以被人们马上使用）的流程。我们现在有6名员工全职为这个项目而努力工作着，我们的目标，不一定是要做出一个特定的应用程序，而是为整个社区打造一个基础库。”Node.js是一个基于Chrome的JavaScript运行时的平台，它使开发人员能够构建和扩展应用程序。

“在某种程度上而言，这与彩色币项目有些相似，因为bitcore需要和bitcoind[进程]一起工作，这意味着，不需要重新创造一条独立的区块链，同时，还能使得开发者，可以开发出更多现在实现不了的功能。Insight这个项目，就是很好的例子，它具备真实的功能，并向终端用户提供了真正的价值。”

正如人们使用网络浏览器，是为了解决真实的需求，根据佩尔的说法，“我认为总的来说，相较于现存的、可能被滥用的金融系统而言，加密货币提供了一个更棒的会计系统，安全性级别也更高。因此我认为，主流人群的接受，只是一个时间早晚的问题，并且不一定要有一个“正确的想法”来催化这个转变的发生。如果你看看密码学，和密码会计学的前进方向，你就会认同“像比特币这样的事物，在业界被广泛的接受，只是一个时间早晚的问题”这样的说法。举个例子，市面存在着对安全的国际支付系统的需求，特别是在非洲和南美地区，而比特币现在就能满足这样的需求。”

说到下一代的平台，佩尔认为，“尽管现在有好几个雄心勃勃的，正在开发中的项目，想要把当前协议中看似’丑陋’的地方给移除掉，但我觉得这种努力，有点类似于Betamax对决VHS。尽管VHS的保真度相对较低，但它最后还是赢得了那场录像带格式的战争。并且，那些所谓的’2.0项目’所提出来的创新思想，是有可能被采用，并整合进比特币协议的。过去，我在几个软件项目上工作过，当时要求一个团队同时解决10到12个难题，如果不解决的话，很多基础功能就不能实现。因此，除非这些团队在所有战线上，都获得了实质的进步，否则他们可能在同一时间，承担了过多的事情。在我们看来，’完美是优秀的敌人’，换句话说，HTTP并不像许多其他同期开发的项目那样优雅，但是，它现在正在被广泛使用，因为它已经足够好用了--同时也是因为，其他竞争对手团队苦苦地想要做出最优雅、完美的解决方案。”

Betamax是一种索尼公司提出的专利录像带标准，与它相竞争的是VHS标准，这是一种由JVC公司提出的，相近似但不需要许可证就能使用的格式。尽管从技术角度来看，Betamax在保真度参数上面更优，但它还是在‘录像带格式战争’中落败了。相类似的，HTTP协议也有许多不同的版本和分叉，有的还提供了更好的技术参数，但最后被广泛采用的是那个被认为‘足够好用’的版本。

BitPay的长期目标之一，佩尔是这样说的，“我们打算让多重签名技术的使用，变得更加便利。单这一项，就能让钱包更加的安全、易于管理，并且改善用户使用体验，因为，对于当下的普通用户而言，安全的守护住自己的钱包，几乎是不可能完成的任务。因此我认为，像苹果和微软这样的公司，最后将会把钱包，整合到它们的浏览器当中去，因为现有浏览器（比如说Chrome），已经支持nodeJS和V8这样的技术了。”V8是一个开源的Javascript引擎，由Google公司开发，并用在Chrome浏览器上。

Kraken交易所

二月份的時候，我和杰西·帕维尔（Jesse Powell）聊过，他是Payward的创始人兼CEO，而Payward又是Kraken交易所的母公司。Kraken是一家虚拟货币的交易平台，用户可以在它上面，兑换多种不同的加密货币和法币。据帕维尔所说，“像以太坊（Ethereum）这样的项目，拥有一些有趣的主张和想法，而这些是你在其他平台上面所不能实现的。我们也了解过其他的，比如说染色币和大师币，这些概念都挺有趣。但是，使用中心化的服务器，来进行交易的一大优势，是可以进行高频交易（HFT）。此外，Kraken当前支持瑞波币（XRP），和其他币种之间进行兑换的理由之一，是瑞波币用来发行财产，更加容易和健壮，因为整个网络天生就是用来做这个事的。”

尽管说，智能合同的最唾手可得的用途之一，是股票交易，但对于专业的交易员而言，似乎几乎不大可能，会直接在区块链上进行高频交易。举个例子，在绝大多数市场（特别是那些高流动性的市场）中，交易延迟是不断下降的，平均每10分钟（甚至2.5分钟）出一个块的节奏，远远不能满足需求。就目前而言，只有使用离链（off-chain）的解决方案，才能实现高频交易的特性，Kraken就是这样做的，这使得用户可以围绕一套内部的API来构建功能。

2014年二月的时候，我与萨尔瓦多·迪立·帕尔梅（Salvatore Delle Palme）进行了一次对话，他是Kraken的数字战略师，同时还是瑞波币联盟（Ripple Federation）的创始人。说到当下在这一领域的商业机会，他认为，“任何把多个不同的系统，连接到一起的想法，都是很棒的。在未来，将会有许多的机遇，这些机遇存在于改善现有的数字货币系统、传统金融系统、以及第二代加密货币协议之间的互通性之上。随着行业的发展，商户整合也将呈现出全新的意义。

此外，我曾经为Let’s Talk Bitcoin写过一篇文章，标题是《虚拟货币的原型The Archetypes of Virtual Currencies》，在文章里面，我谈到了一些关于流行文化，将如何在某些未来的数字货币的成功中，扮演重要角色。”在文章的评论里，我曾被笑话过。让我们快进六个月，然后狗狗币（Dogecoin）就出现在了我们面前。这种基于美国互联网草根文化中“柴犬笑话”而推出的加密货币，在整个生态系统中的交易量位居前三，同时总市值位居第五！狗狗币的出现，证明了流行文化的重要性，并且说明PoW币里面，不只是比特币和莱特币可以活下来。狗狗币的成功，部分可以归功于其“小费货币”的角色。它相较于比特币来说更加有趣，并且有趣是个很重要的属性。

狗狗币和莱特币是基于同样的一套代码，但是，它采取了一套不同的市场推广策略--完全围绕一种互联网“谜米（meme）”来展开--并因此，它的受欢迎程度，在多个指数（全网算力、每日交易量、Reddit关注者数量）上都已经超越了莱特币。

和我聊过的投资人、开发者、还有企业家们，都有一个共同的话题，就是“重启”金融系统，把现代科技融合到其中。根据迪立·帕尔梅所说，“把金融系统给搬到网络上来，需要花上一点时间，但是，我认为一旦这一趋势进一步确立，事物的改变将逐渐加速。加密货币这一层面，已经做得不错了，但是，社交的层面做得却是远远不够。举个例子，我们似乎距离在Facebook上面，打钱给朋友或者商户，还非常遥远，更加不用说其他的社交平台了（尽管PikaPay正在利用比特币和推特来做一些有趣的事情）。最终，我们将看到更高级别的整合。”

一些投资人还提到过另外一件事，在加密货币领域，还没有出现一家类似于e-Trade或者Scottrade那样的交易平台。迪立·帕尔梅看到了这一机会，“Kraken希望能成为数字货币届的FOREX平台。我们提供了周全的安全选项，比如说二步验证和主密码，所以，Kraken是一个很棒的，可以存放数字货币的地方。除此之外，我相信Kraken从开发之初，就免疫于像“交易延展性”这样的问题。我们的开发者很久之前，就已经意识到了这个问题。”正如之前在第三章中所提到的，今年二月中的时候，一个叫做“交易延展性”的已知漏洞，严重影响了几家交易所的运营，其中最知名的交易所是Mt.Gox。不过，Coinbase和Blockchain.info，这两个最大的网络钱包都没有被影响到。

如上所述，Kraken是一家支持多种加密货币的交易所，支持品类中包括了XRP，也就是瑞波币Ripple网络中的筹码。

迪立·帕尔梅认为，“瑞波币拥有许多的优点。于我而言，最大的优点是，他们有一个能用的完善的产品。因此，我把部分精力，放在了巩固他们的社区上。我知道，瑞波币将会在一些比特币社区不太容易涉及的重要领域，取得成功，这样的领域，比如说有分布式的交易所（瑞波币系统内置有一个分布式的交易所），还有智能合同。XRP正在为一家伟大公司的成长，增添动力，并且瑞波币提供了流动性和创新点。我觉得，他们将持续地从开源社区，以及全球的企业家们那里获得支持，并且最终做出一些让人吃惊的成就。”

帕尔梅同时也在研究着以太坊Ethereum的发展潜力，他想看看能否“把密码学财产，和原创艺术作品这两样东西联合起来，并且通过社会共识，来支撑这种财产的价值。

帕尔梅说，“总的来说，在密码学挖矿社区之内，可以拿竞争币（altcoin）来做各种试验。我认为，以太坊将成为竞争链（altchain）的试验标准，并且给出许多新的用途案例，举个例子，艺术币（artcoin）。”除了域名币、比特币、瑞波币（XRP）、莱特币、还有Ven币（XVN），Kraken最近还加入了对狗狗币的支持。

> 注释：
>
> [16] 该项目致力于向大众推广大师协议（Master Protocol）和大师币（Mastercoin）。
>
> [17] 奥莱利媒体（O'Reilly Media）是以出版电脑资讯书籍闻名于世的美国公司。

第八章：结论

尽管泡沫尚存，但数字货币更强大的功能正孕育而生。人们对此达成一个明确的共识：如果这项技术能够被精心设计并运用于金融领域，那么它将能为企业减少摩擦和管理成本。

有些平台可能会成功，有些平台可能失败，这些都是完全可能的。有些平台甚至在其未编译好时就向主流群体引进这项技术。正如约吉·贝拉所言，“预测是个苦差事，未来如何更是难以预料”

或许下面的矩阵图能够帮我们从目前无休止的分析中解脱出来。

平台矩阵

表1：

- 协议建于区块链顶层或与账簿相连：彩色币、万事达币、合约币、开放式交易
- 非区块链分布式共识网络：瑞波币
- 无智能合约功能的去中心化区块链（**SCFE**）：比特币、莱特币、狗狗币、NXT、域名币（混合挖矿）
- 内嵌智能合约功能的去中心化区块链：以太坊、Invictus（原型股，比特股）

表2：

平台	基于区块链	共识账簿	**SCFE***	图灵完备	开源	去中心化	分散式
比特币	X		**		X	X	
莱特币	X		**		X	X	
狗狗币	X		**		X	X	
域名币	X				X	X	
NXT	X		X		部分	X	
彩色币	*		X		X	X	
万事达币	*		X		X	X	
OT			X		X	X	
Invictus	X		X			X	
合约币	*		X		X	X	
以太坊	X		X	X	X	X	
瑞波币			X	X	X	X	X

> 1、SCFE 意味着“智能合约功能可用”—该协议可以使用智能合约
>
> 2、该协议拥有SCFE功能，但开发团队目前仍未启动
>
> 3、彩色币，万事达币，合约币皆寄于母链（比如比特币的区块链）来进行交易和存储

表3：

0:0	**1:0**	**2:0**	**3:0**	**4:0**	**5:0**
0:2	1:2	2:2	3:2	4:2	5:2

综述

如果你问自己这样一个问题：“哪个平台是最好的？”“哪个平台值得你的团队或企业采纳并融入？”

唯一诚实的答案是：无人可知。

写这篇指南的目的是为了给读者提供一个概览，帮助大家去了解这么一个虽然经常被炒作，但仍充满活力，并且在技术，法律，商业领域飞速发展的产业。在这篇指南中，我试图尽可能做到公正、诚实，给不同的观点、方法和平台分配均等的时间。这些行业内的创业者都非常有热情，你在开发人员，企业家，投资者和思想家身上都能够看到类似的特质。

从总体上看，我认为随着技术的发展，未来两年内将会有大量的能源投入到该行业。然而光从市场份额和坏账角度来分析，我们很难明确评判这些平台究竟孰胜孰败。

现有的数字货币协议都在追求远大的目标，但当前仍然受到显著的已知技术困扰。至少到今天为止，我们还缺乏足够的资金和人力去解决这些问题。此外，就目前看，开发一些博彩，赌博类的应用很应景，但将App开发和市场领域结合将涉及高额的法律费用，回报也会随时间递减。毕竟现在已有一些积极的参与者在推动“数字税”的进展。

如果密码协议的目的是提供无摩擦的机制，借以促进实体经济增长，那么创建应用，真正帮助终端用户提高生产率，以此取代已有的昂贵基础设施则是水到渠成。（举个例子，如果博彩业真的能够促进经济增长，那么拉斯维加斯和澳门将取代纽约和上海成为经济增长中心。）美国赌场业每年大致产生1250亿美元的收入，然而大部分人因为“数字税”不会去参与。与之类似的，美国发放了超过10亿张银行卡，其中大部分每半年都会被替换掉。

那么，在密码协议仍未在消费领域被广泛采用之际，业内公司如何能进入更广泛的消费生态系统？一些资深人士认为刚刚接触这个领域的初创企业家们没必要像交易所或汇款公司一样从支付高额合规费用的项目做起，可以尝试换个角度，去解决发展中国家那些用户们的需求，他们往往缺少银行账户，或因条件所迫难以享受主流银行服务。WordPress接受比特币的一个原因就是，并非世界上的所有人都拥有Visa卡，而实际情况是超过60个国家的用户无法使用Paypal服务。WordPress想要将触手伸到上述公司无法企及的地方。也有其他专家建议，创业家们在试图将产品增长至百万级用户的体量之前，应该先为现有的几百位客户提供优质的服务，并从中吸取经验教训。

此外，由于公众领域的洗钱法和消费者保护法的复杂性，有人则建议创业应侧重于纯粹的商业应用，比如高额融资或B2B平台。作为一个软件提供商，不持有代币或将代币兑换为法币或许能让自己处于一个安全的中间地带。其实换种思路，为商户制造一个更易使用的、带有QR二维码功能的POS机，不失为一个好办法。正如肖恩·珀西瓦尔建议的那样，重新为消费者设计接口，让使用加密货币变得更为容易。

促进现有金融基建和加密货币之间搭建桥梁的推力与日俱增。而当巨额资本（包括人力和财力）投入这个领域时，我们发现有些项目是冗余过剩的（实属重造轮子，多此一举），还有些项目是基于政治目的，而非商业动机。

任何想要涉足加密货币领域的人都应该先问自己这样一个问题：有哪些利益导向的商业应用可以建立在这些系统之上？另建一个POW机制的区块链更有效吗，还是说率领你的团队将功能同步至已有的区块链上更好？在没有一个图灵完备协议的前提下，是否可以为更大的客户基础提供新价值？你是否真的需要使用一个去中心化的处理框架，而非分布式乃至中心化（特别针对企业内部网）的框架？你的开发团队能否远程工作，以此降低管理费用，又或者他们需要被定位在一个特定的办公室或住房小区？是否需要与现有市场的参与者建立正式的合作关系，以此争取更多的资金，来更好的满足他们的需求？

今年正式初创基金规模大约有1亿美元，然而，即便创业者们可以回答上述的所有问题，一旦瓜熟落地，代码发布，有些项目或许又会和当初的设想分道扬镳。座机时代一去不复返（现在谁还用固话？），移动电话带来的去中心化趋势让我们得以随时随地拨通任何一个人的电话。智能手机和平板电脑让我们能够随时使用App解放生产力，让更多的人利用虚拟办公，直接跨过对传统方格办公室的需求。

加密货币的出现同样扰乱了我们用钱的方式，更确切的说是管理资产的方式。过去20年里，资产管理是极少没有被新的数字科技颠覆的领域之一，但这点即将改变。正如纳瓦尔·拉维康特和伊莱·多尔拉多最近所述，“大写的Bitcoin并非比特币，而是指的整张货币网络”。虽然手机上可能会出现一些银行软件，但归根结底，它本质上就是个虚拟银行的出纳，或

者ATM。而在另一方面，比特币和其后续创新使得个人金融机构成为可能。在这点上，比特币拥有像Linux平台一样的强大扩展性（相比Windows平台）。

本书的受访者，实际上是我们所有人，都是这场前所未有的、加密的、数学框架下实验的一部分，这场实验很可能会影响到各行各业。然而，去中心化并不一定是终极答案，也不一定是所有问题的灵丹妙药；它仅仅是一个工具，可以用来解决某些问题，而不是全部问题。并且不管这场试验成功与否，采用集中式管理系统的企业、组织、公司（比如IT技术支持）仍可以从这项技术中获利。

更进一步，怀疑者对于特定的未来事件，比如，哪天大家重新造了个轮子（重造区块链）的大胆猜想也是合理的。我们在这里列出的每一个项目，都可以从至少两、三个点详细调查和分析。就如卡尔·萨根所言，非凡的结论要有非凡的证据。而根据我和这些上述团队的互动，我相信即便不是全部，大部分的团队都能够达到他们所设定的里程碑和目标。

社区对于加密货币的未来众说不一；在某些国家，与全球决策者进行建设性的，技术的对话是未来更广范围接受虚拟货币的必要前提，但这个话题其他书籍同样会不可避免的提到，我这里不再赘言。去中心化应用或许会在非法市场流行开来，也可能在某些特定的市场渠道让人获利。数字货币大规模普及的关键在于这些技术是否真的解决了实际需求（例如，有什么理由说服你的母亲使用它；这项技术又如何给没有银行账户的人带来帮助？）

上文提到的所有平台，不论是一代币、还是二代币，都有潜力，为资产管理提供一个无需信任的存储和运输机制。然而，去除宣传和允诺，我们仍然有理由给大家提个醒，这项技术可能还没发展到，满足其狂热者期望的地步，要知道，流行十年至今未衰的只有P2P种子。然而，我个人认为，加密账簿依然拥有实现智能合同，智能资产和无需信任资产管理的无限潜能。

“数字工业革命”让人兴奋，你也可以成为其中一部分

关于作者

蒂姆•斯旺森：得克萨斯A&M大学的毕业生，在东亚地区工作逾六年。他也是《数字长城：中国的商业机遇与挑战》的作者。

联系邮箱：tswanson@gmail.com

最新动态（个人博客）： www.OfNumbers.com

Twitter ：@ ofnumbers

致谢

我想感谢下面这些企业家，商人，专家，投资者和愿意腾出他们时间的思想引领者， 为这本指南提供意见和反馈的所有人士：Derek Au, Steve Bennet, Nikos Bentenitis, Isaac Bergman, Vijay Boyapati, Vitalik Buterin, Preston Byrne, Zachary Caceres, Wences Casares, Raffael Danielli, Ben Davenport, Tuur Demeester, Mark DeWeaver, Joel Dietz, Charles Evans, Scott Freeman, Michael Goldstein, Ron Gross, Mike Hearn, Jon Holmquist, David Johnston, Petri Kajander, Zennon Kapron, Jeremy Kandah, Stephan Kinsella, Daniel Krawisz, Daniel Larimer, Adam Levine, Taariq Lewis, Jeremy Liew, Rui Ma, Hakim Mamoni, Robert McMillan, Amos Meiri, Jared Mimms, Alex Mizrahi, Kevin Moore, Tom Mornini, Chris Odom, Ryan Orr, Stephen Pair, Salvatore Delle Palme, Sean Percival, Jesse Powell, Chris Piaca, Celso Pitta, Mike Reid, Scott Robinson, Dan Roseman, Meni Rosenfeld, Robert Sams, Alan Safahi, Sebastian Serrano, Justin Simcock, Koen Swinkels, Nick Szabo, Alex Tabarrok, Stefan Thomas, Kyle Torpey, Eddy Travia, Stephan Tual, David Veksler, Jack Wang, Andrew White, Matthew Wilson, Yanli Xiao, Mike Youssefmir and Sean Zoltek.

还包括一些为了保护个人隐私而采用网名的人士： cityglut, Graviton,, PhantomPhreak和Uniqueorn.

在整本书中，我参考了他们的见解。这不是一份他们的意见或服务的明确的担保书，而是作为一个参考来源 允许我引用他们说过的话也不代表他们赞同这本书和我的观点。此外，为财务公开起见，这里声明 ：在所有讨论到的企业或公司中，目前我都没有参与其中。我也没有因列入这些公司或项目而得到任何报酬。