**预测市场 身份验证**

**8btc.com**

**区块链解密：构建基于信用的下一代互联网**

互联网领域最知名的“预言家”凯文·凯利在《失控》一书中指出，未来世界的趋势是去中心化的。亚当•斯密的“看不见的手”就是对市场去中心化本质的一个很好的概括。两点之间直线最短，人们之间沟通的最好方式也是直接沟通，无论从哪个角度切入，去中心化的市场本质都是无可辩驳的。

比特币的信用基础区块链技术是一种巨大的技术突破，这种以P2P为基础的去中心化的新体系，它革新了互联网与金融产业，现在的比特币行业，只想当于1994年左右的互联网，还处于基础建议阶段，但未来十年，区块链有可能取代互联网。

# 第3章 区块链应用场景

区块链技术源于比特币，它的本质是运用计算机算法和密码学等技术创造一种去中心化的数字货币系统，实现货币的发行和交易功能。下面就让我们来看看，区块链技术会给哪些领域带来变革。

## 3.1 存在性证明

### 3.1.1概述

存在性证明是指把将要存储的文件的SHA256信息摘要嵌入到区块链来证明其存在性。原理是通过两个编码过的且包含哈希的特殊地址创建一个有效的比特币转账，这个哈希被切断成两个片段，每个片段包含这些地址之一。哈希片段用来替换椭圆曲线数字签名（比特币地址生成算法）公钥的哈希，这就是为什么这些特殊的转账是不能花费的，因为这些地址是由文档的杂凑片段生成的，而不是由椭圆曲线数字签名算法的私钥生成。

地址生成且交易确认后，该文件即被永久认证。只要交易被证实，则意味着该文件存在。如果文件在交易发生时不存在，它不可能在两个地址中嵌入其SHA256消息摘要，并创建转账（由于哈希函数的抗第二原像计算性）。试图嵌入一些哈希散列，以与未来的文件哈希值相匹配，这也是不可能的（由于哈希函数的抗原像计算性），这就是为什么一旦文档所产生的转账被比特币区块确认，该文件的存在性就被证明了，而不需要一个让人信任的中央权力机构。

如果有人想在时间戳上手动确认文件的存在，他们应该遵循以下步骤：

1）计算SHA256信息摘要。

2）找到比特币区块链上的转账记录，给文档的地址发送比特币。

3）反编译base58编码的地址。

4）嵌入摘要，替换这两个地址的公钥哈希，由于摘要共有32个字节，而每个地址可容纳20个字节，剩下8个字节用零填满。

5）区块链上这两个地址间的转账可证明该文件在那个时间确实存在过。

通过简单的在区块链上登记和加入时间戳信息，POE能够让任何人匿名和安全地存放任何文件的存在性证明。文件本身并没有存放在中心化的数据库或者区块链中，因此文件数据是隐私的。在区块链上存放的仅仅是文件的密码学哈希值，以及该文件的哈希值提交至区块链中的时间信息。这样一来，人们就可以基于公开的区块链，在无需揭露数据内容或所有者身份信息的情况下公开证明某个文件或信息属于某人。

合约也可以加上时间戳和当事人的数字签名，来证明它们是何时签署这些合约的。可信的时间戳信息可以用来证明你在某个时间点持有某个文件、信息或数据，而且这些信息无法伪造。你可以给你开发的软件版本加上时间戳信息来证明在某个时间点你已经开发了某个版本的软件。你无需依赖任何机构。在以前的传统中，是由称之为TSAs（Time Stamping Authority）的可信赖的第三方来签署的可信时间戳信息的，但是容易出现数据腐败和篡改。而且在区块链中，您的时间戳信息是安全存放在全世界的，更难篡改。

存在性证明POE可以用于文件版权、专利等等。任何人都可以证明某个数据在某个时间点存在过。因为我们使用了比特币区块链来存放文件证明信息，因此任何人都可以在无需中心机构的情况下就能验证该文件证明信息。而且整个比特币网络的算力用来保护你的数据。

存在性证明POE的部分用途如下：

1、无需泄露真实的数据内容即可证明文件的所有者

2、文件时间戳

3、证明所有者和转让合同

4、确认文件完整性

如果某人存储了他的文件证明，之后重新上传该文件，系统将会识别该文件是否与之前的文件完全一致。哪怕是轻微的变化，区块链都会识别出它与之前文件是不同的。这就给用户提供了必要的安全性，即已验证的文件是不可更改的。

### 3.1.2应用案例

随着互联网技术发展，越来越多的机构，开始大力研究数字合同和数字印章技术。但是这些技术，还停留在中心化数字解决方案，许多机构更是出于本集团利益，进行研发，而不顾使用者的利益，并且成本高，方案不够透明，技术被少数人垄断和操作，容易作弊，并且各个团体机构之间，技术不公开，不透明，通用性不强，造成了公信力的缺失，也制约了这一技术快速普及与发展，在我们生活中，经常可以看到有些恶意的人故意篡改并违反原来的约定，利用手中各种关系和方法来谋取私利。让处于弱势的善良的用户，想通过当初的约定，进行司法维护公正时，发现已经无法行得通。这一切均缘于普通纸质协议，容易丢失，容易被人修改，而且存放不透明，不公开。

基于区块链技术构建的数字合同与数字印章解决方案，正是基于这种理念而产生，在区块链中，每个区块都有自己的唯一hash值，任何人都不能私自修改区块中的内容，私自修改，将会造成区块hash值的改变，而被整个网络拒绝，正是基于区块链的这种安全特性，我们将合同的验证算法，写入到区块链，使任何人都不能作弊或是破坏合同的约定内容，甚至可以将一些重要事件的环境、人、事等等内容也写入区块链中，进行永久保留。它还是开源的技术，它将和数字货币拥有相同的安全属性。在这套解决方案中，合同相关人或单位、政府部门，进行高效结合，各司职守。实现一种智能的，免维护的数字合同解决方案架构。我们畅想，未来，任何国与国之间，人与人之间或是单位与单位之间，都可以在这套框架进行协约签定，它将是未来物联网世界中，最强大的公约系统，它将作用于人类生活，维护世界秩序的方方面面，让人类受益。

将一份合同内容，经过SHA校验后，写入签名信息中，并由签约双方发起一笔交易，进而将这些数据写入区块链。合同本身具有隐私性，合同内容不会被写入区块（或是仅将加密后内容写入区块），一份合同制定完成后，会对这个合同文件，进行SHA256加密校验，防止事后，私自修改合内容，将SHA值写入区块中，以确定合同的唯一性，合法性，公示性。

在将来，用户甚至只需要发送一条短信，或是发一份邮件，或是聊天工具上发给对方一串字符，或是二维码的扫描等，就可以完成合同的签订工作。甚至还允许两个互不认识对方的人，进行匿名合同的签订。甚至包括实现人与人，硬件与人，硬件与硬件之间建立数字合同关系。



无论数字印印章还是个人数字印章，均会被写入区块中，进行身份的公示，这里公示是匿名性，但是确是可以验证的。通过钱包私匙具有唯一性，通过其加密的后数字印章同样居有唯一性。

http://www.bitnet.wang/iot0004/

http://nxtchina.org/portal.php?mod=view&aid=47

http://www.btc38.com/altcoin/vpn/8552.html

## 3.2 智能合约

### 3.2.1概述

密码学家尼克萨博（Nick Szabo）早在1994年提出的智能合约的理念，在区块链技术出现以前一直不能够应用到现实中，但是比特币出现以后，智能合约获得了重生。智能合约的理念加上区块链的技术，将会产生出什么呢？

举一个典型的活生生的例子，我们可以认为智能的原始祖先，是不起眼的自动售货机。由于箱里钱远远少于破坏者付出的代价，在潜在损失有限的评估后，根据显示的价格收取硬币，通过一个简单的机制形成了最初的计算机设计科学，有限自动，传递变化和制造。自动售货机是搬运合约：任何持有硬币的人可以与供应商交易。锁箱和其他安全机制保护储存的硬币和货物会不被破坏，足以允许自动售货机有利可图地在各种各样的区域部署。优越于自动售货机，智能合约通过数字的方法来控制有价值的、所有类型的任何资产。智能合约涉及到一个动态的、经常主动运作的财产，且提供更好的观察和核查点，其中主动措施必须分毫不差。

另一个例子，为汽车而设计出的假想数字保障系统。智能合约设计策略建议：持续完善抵押品协议以便其更充分地嵌入到处理资产的合约条款中。根据合约条款，这些协议将使加密密钥完全控制于具有操作属性的人，其人正当地拥有该财产。在最简单的实现中，为了防止偷窃，除非被合法的拥有者完成正确的“挑战-应答”过程，否则车可以呈现出不可操作状态。

如果汽车用做以确保还贷，在这种传统的方式来在实现强大的安全性同时将创造一个头痛的债权人－收款人将不再能够查收赖账的车。为了解决这一问题，我们可以创建一个智能扣押权协议：如果物主不交费，智能合同调用扣押权协议，其把车钥匙的控制权交给银行。该协议可能会比雇佣追债人更便宜、更有效。进一步的细化，如生成可证明的扣押权权注销，以及当贷款已还清、处于困境和意外情况下的账户操作。例如，当车子在75号高速路上奔跑的时候，撤销车子的操作将是粗鲁的。

在连续细化的过程中，我们从一个粗糙的抵押品体系，具体化到一个个具体化的合约：

（1）选择性地允许业主锁定和排除第三方  
（2）允许债权人接入的秘密途径  
（3A）只在违约一段时间且没有付款时秘密途径被打开; 并且  
（3b）最后的电子支付完成后将永久地关闭秘密途径。

成熟的抵押品体系将针对不同的合约执行不同的行为。继续讨论我们的例子，如果汽车的合同是一个租赁，最终付款将关闭承租人访问权; 购买了债权，那就关掉债权人的访问。通过连续的重新设计方式，抵押品体系越来越接近其合约的精髓：管理了覆盖财物，信息或被抵押的。可定性的、不同的合约条款，以及在财产在属性的技术差异，则引出不同的协议。

**智能合约是什么？**智能合约是由事件驱动的、具有状态的、运行在一个复制的、分享的账本之上的、且能够保管账本上资产的程序。从本质上讲，这些自动合约的工作原理类似于其它计算机程序的if-then语句。智能合约只是以这种方式与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。

如果你能降低抵押贷款利率，更加容易地更新遗嘱，和确保你的赌伴不会不支付赌资时，那会怎样？这些应用和其它更多的应用，是智能合约向我们许诺的未来，由于密码学货币的出现，智能合约这一技术正越来越走近现实生活。未来的某一天，这些程序可能取代处理某些特定金融交易的律师和银行。

智能合约的潜能不只是简单的转移资金。一辆汽车或者一所房屋的门锁，都能够被连接到物联网上的智能合约被打开。但是与所有的金融前沿技术类似，智能合约的主要问题是：它怎样与我们目前的法律系统向协调呢？还有，会有人真正使用智能合约吗？

比特币的出现和被广泛使用，正在改变阻碍智能合约实现的现状，从而萨博的理念有了重生的机会。智能合约技术现在正建立在比特币和其它虚拟货币–有些人将它们称为“比特币2.0”平台–之上。因为比特币本身就是一个计算机程序，智能合约能够与它进行交互，就像它能与其它程序进行交互一样。问题正逐步被解决。一个计算机程序现在可以触发支付。

### 3.2.3应用案例

#### 1用智能合约来实现保险柜

你是如何保存比特币的？当然，比特币登记在区块链上，但是你是如何保存你的私钥来保证你的资金安全的？如果你现在还没有比特币，你会如何保存你的私钥，这个小小的文件有着直接的货币价值，如何防止丢失和黑客？保持密钥的安全是大众接受密码货币的阻碍之一，每一次货币的丢失事件都给整个加密货币社区带来不好的名声，这些问题有各种不同的答案。

如果问任何一个加密货币老手，他们都会告诉你一个事实，你必须使用非常成熟的软件和真正的随机数来生成你的私钥。并且他们会告诉你使用多重签名来拆分开你的私钥，这样黑客必须破解不是一个，而是多个机器来获得你的资金。这种保护是很复杂的。经典的保存私钥安全的方法是遵循[37步操作安全准则](http://hackingdistributed.com/2014/11/30/reasonable-bitcoin-security-precautions/) ，这里涉及到物理隔离，专用笔记本和断开网络接口。但是“互联网”类的货币也需要物理隔离，专用笔记本和隐藏在使用假墓室的金塔里？所以，不足为奇的是，凡人常常选择比较大的交易所来保存他们的币。当然，这只是将安全问题外包为交易所的安全，但是面临完全相同的问题，只不过有更高的赌注。

在可用性（需要更多的备份）和安全性（更多的备份意味着更大的风险）的权衡中，一般的使用者会难以抉择。极端情况下，要么将私钥保存在多个设备上，这样就容易被盗，或者只保存一份编码私钥在物理隔离的保险库，如果用户需要访问，需要临时地重新连接网络，并且需要一段密码来还原私钥。

结果，加密货币的的历史里记载了很多起丢失货币的悲剧，要么因为自己的错误丢失货币，要么黑客偷走了私钥而盗走多部分金额。这样的事情同样发生在聪明人身上。一个计算机系毕业的大学生，是早期的比特币矿工，丢失了差不多10,000个比特币。另外一个朋友选择了一个非常非常好的密码，好的以至于在一些年后他不能回忆起这个密码，甚至使用催眠和根据他的密码选择习惯的暴力破解也无济于事。

总的来讲，我们的计算机设施在安全保存高价值的资产方面遥遥无期。比特币已经变成一种普遍的黑客的“福利”，因为他们可以侵入你的电脑盗走你的财富。我们需要一种方式去锁定我们的比特币，让黑客和小偷不为所动。

在巴巴多斯的比特币工作室里，Malte Möser 提出了[比特币私钥解决方案](http://fc16.ifca.ai/bitcoin/papers/MES16.pdf)，该方案描述了一种方式来新建保险库，它是一种特殊的帐户，一旦私钥落入攻击者手里，这些私钥达成的交易也可以被抵消。保险柜是比特币的一种去中心化的方式，让你可以申请银行丢失信用卡来撤销攻击者的交易。这里有一些有趣的地方：这样的话，保险柜在根本上是使私钥盗窃行为失去动机。攻击者知道如果他们不能拿走比特币的话，首先就会很少去攻击，对比当前情况，比特币攻击者可以保证他们的攻击行为能够获得可观的回报。

在操作上，思路也很简单。你发送你的资金到你自己创建的保险柜地址。每一个保险柜地址有一个开锁密钥和恢复密钥。当你使用开锁密钥从保险柜花费时，你必须等待预先设置的时间（非保险期），它是你创建保险柜时创建的，比如说24小时。当一切顺利的话，在不保险期之后，你保险柜里的资金是未锁定状态，你可以将它们转移到其他地址，然后像往常一样去花费它们。现在，假使Harry一个黑客掌握了你的开锁密钥，你也有24小时的时间使用恢复密钥撤销Harry发起的交易。这次偷盗行为本质上讲是失败的，资金会转移到正确的拥有者那里。它有点像现代银行依靠的“撤销”功能，但是是在比特币世界。

现在，精明的读者会问，如果Harry是非常非常聪明，他不仅偷走了开锁密钥也偷走了恢复密钥，会怎样。那样的话，他已经完全攻陷你，就网络而言，他和你已经没有区别。即便如此，保险柜依然可以保护你。恢复密钥同样有一个类似的锁定期，允许你永久性的撤销Harry所有的交易行为。不幸的是，在这种情况下，Harry也可以做同样的事，撤销你做的所有交易。为了避免反复的僵局，恢复密钥也可以烧掉资金，这样就你没有人能得到这笔钱。结局是Harry从他的偷盗行为中不能够得到任何回报。这样实际上意味者Harry首先就不会把保险柜列为目标，因为如果这样做他不会有任何收入。

在比特币契约之上构建保险柜

在比特币中实现这样的保险柜机制是遥不可及的。一种可行的方案是，为保险柜专门设计的工具，使用专门的地址为保险柜，更多的操作代码。但是我们相信架构的变更，应该是最小并且通用。因此，我们提出对比特币进行一个小的变更，称之为“比特币契约“。就像[法律契约](https://en.wikipedia.org/wiki/Covenant_(law))，比特币契约会检查交易花费的条件是否成立。本质上讲，契约是未来交易形式的一种约束。因为契约可以递归，可以保持自我永存，或者可以某段时间进行限制，它应当允许一个人实现一系列丰富的语义自定义。

扩展脚本语言的想法并不是新近提起。事实上，我们命名为契约源于一篇Greg Maxwell发表过的文章[随便说说的文章](https://bitcointalk.org/index.php?topic=278122.0)，他建议了一个不大可能的机制并且提到一些奇怪的案例。这篇文章很值得一读。

不可逆转性不会被影响

很重要的要指出，保险柜不会影响比特币交易的不可逆转性。保险柜是个人资金的保护机制：你可以将你希望安全保存的资金放到你自己创建的保险柜地址。这样做的话，你放弃了迅速消费它们的能力换来防盗。当你想使用这些币时，你可以将它们从保险柜转移到你的热钱包，你用你的钱包进行支付。只有你自己拥有的钱可以被保存到保险柜，它们也只能转回到你的所有权下。你不能欺骗某人接受一笔来自保险柜的交易，然后再将这些币收回。整个的设计关系到个人资产的保护，这将影响到他们选择哪种币来保存个人资产，保证比特币上的资产不会让人产生任何不安。

总的来讲，我们的建议是一种简单而强大的对脚本语言的扩展，这很容易推断出，它将开启更加丰富的设想的大门。

保险柜是契约的第一个用例，它解决一个自比特币系统第发布以来就一直困扰每一个比特币用户的问题。我们希望保险柜可以使人们可以安全的保存它们的线上资金，知道他们总是远离被盗，更重要的是它从根本上断除了偷窃的想法。

用智能合约来实现保险柜

如何实现安全的比特币保险柜

你是如何保存比特币的？当然，比特币登记在区块链上，但是你是如何保存你的私钥来保证你的资金安全的？如果你现在还没有比特币，你会如何保存你的私钥，这个小小的文件有着直接的货币价值，如何防止丢失和黑客？保持密钥的安全是大众接受密码货币的阻碍之一，每一次货币的丢失事件都给整个加密货币社区带来不好的名声，这些问题有各种不同的答案。

如果问任何一个加密货币老手，他们都会告诉你一个事实，你必须使用非常成熟的软件和真正的随机数来生成你的私钥。并且他们会告诉你使用多重签名来拆分开你的私钥，这样黑客必须破解不是一个，而是多个机器来获得你的资金。这种保护是很复杂的。经典的保存私钥安全的方法是遵循[37步操作安全准则](http://hackingdistributed.com/2014/11/30/reasonable-bitcoin-security-precautions/) ，这里涉及到物理隔离，专用笔记本和断开网络接口。但是“互联网”类的货币也需要物理隔离，专用笔记本和隐藏在使用假墓室的金塔里？所以，不足为奇的是，凡人常常选择比较大的交易所来保存他们的币。当然，这只是将安全问题外包为交易所的安全，但是面临完全相同的问题，只不过有更高的赌注。

在可用性（需要更多的备份）和安全性（更多的备份意味着更大的风险）的权衡中，一般的使用者会难以抉择。极端情况下，要么将私钥保存在多个设备上，这样就容易被盗，或者只保存一份编码私钥在物理隔离的保险库，如果用户需要访问，需要临时地重新连接网络，并且需要一段密码来还原私钥。

结果，加密货币的的历史里记载了很多起丢失货币的悲剧，要么因为自己的错误丢失货币，要么黑客偷走了私钥而盗走多部分金额。这样的事情同样发生在聪明人身上。一个计算机系毕业的大学生，是早期的比特币矿工，丢失了差不多10,000个比特币。另外一个朋友选择了一个非常非常好的密码，好的以至于在一些年后他不能回忆起这个密码，甚至使用催眠和根据他的密码选择习惯的暴力破解也无济于事。

总的来讲，我们的计算机设施在安全保存高价值的资产方面遥遥无期。比特币已经变成一种普遍的黑客的“福利”，因为他们可以侵入你的电脑盗走你的财富。我们需要一种方式去锁定我们的比特币，让黑客和小偷不为所动。

比特币保险柜

在巴巴多斯的比特币工作室里，Malte Möser 展示了[我们的比特币私钥解决方案](http://fc16.ifca.ai/bitcoin/papers/MES16.pdf)。特别的是，我们的论文描述了一种方式来新建“保险库“，它是一种特殊的帐户，一旦私钥落入攻击者手里，这些私钥达成的交易也可以被抵消。保险柜是比特币的一种去中心化的方式，让你可以申请银行丢失信用卡来撤销攻击者的交易。这里有一些有趣的地方：这样的话，保险柜在根本上是使私钥盗窃行为失去动机。攻击者知道如果他们不能拿走比特币的话，首先就会很少去攻击，对比当前情况，比特币攻击者可以保证他们的攻击行为能够获得可观的回报。

在操作上，思路也很简单。你发送你的资金到你自己创建的保险柜地址。每一个保险柜地址有一个开锁密钥和恢复密钥。当你使用开锁密钥从保险柜花费时，你必须等待预先设置的时间（非保险期），它是你创建保险柜时创建的，比如说24小时。当一切顺利的话，在不保险期之后，你保险柜里的资金是未锁定状态，你可以将它们转移到其他地址，然后像往常一样去花费它们。现在，假使Harry一个黑客掌握了你的开锁密钥，你也有24小时的时间使用恢复密钥撤销Harry发起的交易。这次偷盗行为本质上讲是失败的，资金会转移到正确的拥有者那里。它有点像现代银行依靠的“撤销”功能，但是是在比特币世界。

现在，精明的读者会问，如果Harry是非常非常聪明，他不仅偷走了开锁密钥也偷走了恢复密钥，会怎样。那样的话，他已经完全攻陷你，就网络而言，他和你已经没有区别。即便如此，保险柜依然可以保护你。恢复密钥同样有一个类似的锁定期，允许你永久性的撤销Harry所有的交易行为。不幸的是，在这种情况下，Harry也可以做同样的事，撤销你做的所有交易。为了避免反复的僵局，恢复密钥也可以烧掉资金，这样就你没有人能得到这笔钱。结局是Harry从他的偷盗行为中不能够得到任何回报。这样实际上意味者Harry首先就不会把保险柜列为目标，因为如果这样做他不会有任何收入。

在比特币契约之上构建保险柜

在比特币中实现这样的保险柜机制是遥不可及的。一种可行的方案是，为保险柜专门设计的工具，使用专门的地址为保险柜，更多的操作代码。但是我们相信架构的变更，应该是最小并且通用。因此，我们提出对比特币进行一个小的变更，称之为“比特币契约“。就像[法律契约](https://en.wikipedia.org/wiki/Covenant_(law))，比特币契约会检查交易花费的条件是否成立。本质上讲，契约是未来交易形式的一种约束。因为契约可以递归，可以保持自我永存，或者可以某段时间进行限制，它应当允许一个人实现一系列丰富的语义自定义。

扩展脚本语言的想法并不是新近提起。事实上，我们命名为契约源于一篇Greg Maxwell发表过的文章[随便说说的文章](https://bitcointalk.org/index.php?topic=278122.0)，他建议了一个不大可能的机制并且提到一些奇怪的案例。这篇文章很值得一读。

不可逆转性不会被影响

很重要的要指出，保险柜不会影响比特币交易的不可逆转性。保险柜是个人资金的保护机制：你可以将你希望安全保存的资金放到你自己创建的保险柜地址。这样做的话，你放弃了迅速消费它们的能力换来防盗。当你想使用这些币时，你可以将它们从保险柜转移到你的热钱包，你用你的钱包进行支付。只有你自己拥有的钱可以被保存到保险柜，它们也只能转回到你的所有权下。你不能欺骗某人接受一笔来自保险柜的交易，然后再将这些币收回。整个的设计关系到个人资产的保护，这将影响到他们选择哪种币来保存个人资产，保证比特币上的资产不会让人产生任何不安。

总的来讲，我们的建议是一种简单而强大的对脚本语言的扩展，这很容易推断出，它将开启更加丰富的设想的大门。

保险柜是契约的第一个用例，它解决一个自比特币系统第发布以来就一直困扰每一个比特币用户的问题。我们希望保险柜可以使人们可以安全的保存它们的线上资金，知道他们总是远离被盗，更重要的是它从根本上断除了偷窃的想法。

## 3.3 物联网

### 3.3.1概述

物联网，“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网。其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。传统的物联网下，由一个中心化的数据中心收集所有已联接设备的信息，会面临如下挑战：

（1）连接成本

在物联网的收入不能达到市场预期时，物联网的成本仍过分地高。许多现有的物联网解决方案成本十分高，因为除了这些服务的中间人成本以外，与中心化云和大型服务器群相关的基础设施和维护的成本十分高。

现在的物联网解决方案还存在服务供给和顾客期望的不匹配。以往信息技术行业的成本和收入一直是非常一致的。虽然大型服务器的使用寿命长达很多年，但是生产厂商与买家签订了支持合同。个人电脑和智能手机没有如此利润丰厚的支持计划，但是，它们的产品生命周期更短，这就不是一个大问题。对于物联网，设备制造企业没有足够的利润弥补多年支持和维护设备所需的成本。支持和服务于数以千亿计的智能设备所需的成本将是十分巨大的-即使是维持分发升级软件的中心化服务器的成本也十分高。

（2）失去信任的互联网

互联网原本是建立在信任的基础上的。在后斯诺登时代，很明显人们不再信任互联网了。中心化的需要信任第三方的物联网解决方案现在成了一种不切实际的幻想。现在大多数物联网解决方案为无论是政府、生产厂商或者服务提供者等中心化的机构提供了，未经用户授权，就能够通过收集和分析用户数据，接近和控制用户的设备的能力。

在物联网中，形成信任是非常困难的，而且维持信任的成本非常高，如果不是不可能的话。然而，为了物联网被人们广泛应用，隐私和匿名性必须被整合到物联网的设计中，给予用户控制自己隐私的能力。

目前的安全模型是基于封闭源代码的方法(经常被称为”不公开即安全”)已经被废弃，必须被一种新的方法-公开即安全-所取代。为了实现这一点，升级到开源软件是必需的。尽管开源系统现在可能仍然容易遭受事故和可利用性不佳，但是它们不易受到政府干涉和其它定向攻击，所以对开源系统在家庭自动化、汽车及其它设备联网化领域大有可为。

（3）设备制造商会过时

尽管许多公司迅速地进入智能连接设备市场，但是他们并没有发现在该领域生存发展非常困难。消费者每18到36个月就会更换智能手机和个人电脑，但是对于像门锁LED灯泡和其它物联网的基础设施的寿命将长达数年，甚至数十年。

举例说明，汽车的平均使用寿命是10年，美国房屋的平均使用寿命是39年，公路、铁路和航空运输系统的预期使用寿命超过50年。存在安全缺陷的门锁对仓库公司和门锁制造商的声誉而言，是一场灾难。在物联网世界，在过长的设备生命周期中，软件更新和设备维修成本将在长达数十年中增加制造商的负担，设备还在用，制造商已经倒闭了。

（4）缺少使用价值

现在许多物联网解决方案缺少有意义的价值创造。许多联网设备的价值只是它们与网络连接，但是简单地连接到网络并不能使得一个设备更加智能或者更好。联网和智能只是设备产生更好产品和服务的一种手段，而不是最终目的。

制造商认为用户会接受他们为了一些功能，例如产品质量跟踪功能，增加成本和复杂性，这纯粹是痴心妄想。一台智能、连接物联网的烤面包机是没有价值的，除非它能烤出更好吃的面包。为数不多的、成功的智能设备制造商重视简单实用的价值。他们提高设备的核心功能和用户体验，并不要求订阅服务或者应用程序。

（5）破损的商业模式

大多数物联网的商业模式也是依靠售卖用户数据或者做针对性广告。这些期望也是不切实际的。广告数据和营销数据受到信息市场特质的影响：附加容量(广告)或者增加供给(用户数据)的边际成本是零。所以，当存在竞争时，市场的价格将趋向于零，获得收益的机会将转移到整合者手中。阻碍从用户数据中获得价值的另一个更深层的原因是，普通消费者用户可能开放共享自己的数据，但是企业用户不会这样做的。

另一个问题是对从物联网智能设备应用程序获得收入的预期过于乐观。在数字时代以前，像烤面包机和门锁这样的设备不需要应用程序和服务合约，就可以发挥作用。不像个人电脑或者智能手机，它们不需要与用户进行大量的人机交互，这就使得从应用程序中获得收入的预期是不切实际的。

最后，许多智能设备制造商对创建生态系统具有不符合现实的预期。尽管实现智能电视与烤面包机之间的通信交流非常有趣，但是这样的物联网解决方案很快就会变得很繁琐，而且没有人成功地控制物联网生态系统和从中赚到钱。

区块链技术解决了闻名已久的拜占庭将军问题——它提供一种无需信任单个节点，还能创建共识网络的方法。比特币使用算法工程保证整个网络的安全，借助它，设备能在金融市场中完全独立于任何人工干预。一套算法会生成自己的比特币钱包，从而允许它与别的算法（别的钱包）进行交易。这在物联网上是一个道理，所有日常家居物件都能自发、自动地与其它物件、或外界世界进行金融活动，比如：你的智能电表可以通过调节用电量和频率，来促成更优惠的电费账单。

在去中心化的物联网中，区块链是能够促进交易处理和交互设备之间协作的基础架构。每个区块链管理自己的行为，发挥自身的作用，这样就会形成一个“去中心化的自治物联网”，从而实现数字世界的民主。

（1）用户的作用

在这一由数以千亿计的设备形成的、民主的物联网中，用户使用安全的身份确认机制与设备联系起来。用户动态地创建和维持与其它设备的交互规则。这些规则提供了一个强大的机制来确定用户与设备之间的关系，以及基于用户自己定义的准则—物质的、社会的或者暂时的—来准许设备是否可用。

当设备评测升级软件的安全或者禁止一个行为不当的参与者时，规则也可以由51%共识机制定义。用户创建并执行数字清单是基于预先定义好的一系列规则，它的目标是帮助确认自动运行设备不失效。

（2）设备的作用

另一方面，设备被授权通过搜索它们自己的软件升级，确认对方的可信度和为资源和服务交换进行支付，自动执行数字合约，例如协议、支付和与其它设备进行交易。这使得它们可以作为自我维持、自我服务的设备发挥作用。

智能设备能够自动与其它设备进行交易的能力产生了全新的商业模式，促成了新的商业机遇：物联网中的每一个设备都可以充当独立的商业主体，以很低的交易成本与其它设备分享能力和资源，例如计算周期、带宽。除了较以前更加充分地利用数以十亿计设备，形成新的商业模式以外，区块链也促进了与这些设备相关的服务和消费品的新市场的产生。

（3）制造商的作用

对物联网设备制造商和服务提供者而言，基于区块链的物联网也是非常有吸引力的。它允许他们将维护设备的责任转移给一个自我维护设备社区，这使得无论在设备生命周期还是超过生命周期，物联网不会过时，并节省大量的基础设施成本。

在这一模式中，用户控制自己的隐私，而不是被一个中心化的机构控制着，设备是主人。云的角色从一个控制者变革成了一个服务提供者。在这一新的民主中，网络中的权力从中心移向边缘。设备和云成为了平等的公民。

这种由设备驱动的民主显然能够吸引物联网生态系统中各个参与者的兴趣。但是，它的最大价值可能在于宏观层面上，不仅在于创建了一个可扩展和高效的物联网，而是创建出新的市场和塑造出新的商业模式。

（4）实现物理世界的流动

在物联网以前，只有简单的互联网(Internet)。人连网(Internet of People)已经对经济产生了巨大的影响。到目前为止，它的最大影响是创建了数字内容市场，例如音乐、[新闻](http://www.wanbizu.com/news/)、地图和其它信息。

物联网将会促成一系列相似的变革，使得物理世界像数字世界一样流动、个性化和高效。物联网潜在的五个颠覆性潜能如下:

1）释放有形资产的过剩产能

在变革数字内容市场的过程中，互联网使得三种关键的商业元素成为可能：搜素（search）、使用（usage）和支付（payment）。搜索变为即时和全面的。从音乐到百科全书，使用这些数字内容和为它们支付费用，能在网上立即实现。实现这样的变革，是因为数字内容独特的经济特性。复制数字内容的边际成本为零，所以在竞争激烈的数字市场上，数字内容的价格为零。

物联网使得我们可以非常容易地将有形资产数字化，并对它进行买卖和转移，就像今天我们处理虚拟商品一样。使用一切智能设备，从蓝牙信标到连接Wi-Fi的门锁，模拟时代的有形资产将会变成数字服务。在一个由设备驱动的民主化物联网中，会议室、酒店房间、汽车和仓库能够实时自动地报告能力、用途和可用性。通过使用空闲的资源，并非常容易地实现对这类资源的商业利用，物联网能够移除行业细分的障碍，这在以前是不可能实现的。现在由于太复杂难以监控和管理的资产，在新的数字经济时代中，将代表新的商业机遇。

2）创造流动、透明的市场

通过为有形资产和服务提供实时的供给和需求的匹配服务，物联网将创造出新的市场。这些复杂实时的数字市场将建立在由移动设备和社交网络构成的基础之上，它将迅速地扩张变革的范围。它们将促成新的点对点的经济模式和形成分享经济。设备将能够参与实时竞争，受到共识的评论和推荐，并能自动进行交易，最终形成高效的数字市场。

当大量的生产力和服务遇到强大的数字工具，实现供给与需求的匹配时，将会发生什么呢？历史上没有比Sabre公司在航空业中所起到的作用更好的例子了。Uber和Airbnb是今天的Sabres，领导着为有形资产创建具有高度流动性市场的潮流，这些有形资产包括汽车、房屋、办公室小隔间、仓库、停车位和其它应用，没有物联网这些市场都是不可能实现的。

3）对信用和风险的重新定价

在衡量个人风险和信用方面，物联网也会带来一场革命。现在信用和风险管理的规则非常粗糙，就像报纸和电视时代的广告一样粗糙。成熟的西方市场中的征信机构和税收记录在消费者信用可用性领域引起了一场革命，但是它只覆盖了世界上的一小部分人。在像美国这样的成熟市场上，不安全信贷额度经常是高质量信贷成本的8～10倍，由此可见即使在这些市场上风险定价也是多么地不被理解。

通过手机实现的仪表化和数字化与物联网结合在一起，将带来风险和信用定价的革命。将设备仪表化与结合移动支付、GPS日志和社交网络在一起，企业就可以建立更加精确的风险衡量机制，同时减少道德风险和回收成本。

消费者信用额度合理地扩张对消费者具有重大的影响，有益于现代设备的普及化。释放有形资产、创建新市场和更加精确的信用和风险评估将打开新的数字经济大门，这在物联网以前是不可思议的事情

4）提高运作效率

现在，受信息技术影响最小的经济领域是农业，信息技术支出只占农业资本支出的1%。在这一领域，物联网的潜在影响是十分巨大的。农业受资本和技术的影响非常大，但是还没有受信息技术的影响。先进的收割技术、转基因种子、药剂混用和全球存储和分配，表现了在没有利用信息技术的情况下，现代农业是如何出现的。

实现每一道农业程序的仪表化和数字化，将增加农业产出，如同农民合作机制、生物技术公司、农业设备制造商和农业资本为农业增产一样。包括可以低成本监控大片农田的遥控飞机、根据土壤和天气条件优化播种和收割的仪器和用于细节检测感应器的在内的一系列物联网技术能够应用到农业中，增加农业产出。

5）整合价值链

利用物联网的最好方式之一就是通过物联网整合价值链。到目前为止，使用数字技术整合价值链已经成为工业网络化技术的最大驱动之一。

由于实时的数据，航空公司可以在飞机降落以前安排维修，在空闲时间修理故障。如此一来，飞机可以将更多的时间用于飞行赚钱上，花更少的时间用于在地面等待维护和修理上。这种高价值服务目前只存在于非常有限和封闭的行业生态系统中。物联网将使得消费者和企业能够实现这中能够创造价值的行业和系统整合。众筹和其它开放合作平台将进一步加速共享创新和发展。

说到物联网促成工业的虚拟垂直整合，现在还没有显著的成功例子。工业互联网联盟刚刚开始踏上制定标准的漫长之路。当企业正在为标准辩论不休时，消费者却走到了企业的前头。现在，在服务和产品领域，已经有数以千计的系统对系统和系统对设备的整合方法。这些整合方法，大型企业采用的较慢，但是消费者和小企业采用的较快，他们正在引领潮流。

最后，物联网有望使得物理世界能够像虚拟世界一样容易地搜索、使用和接洽。我们把这种新兴的变革描述为物理世界的液化。就像庞大的金融市场创造了证券和货币的流动性一样，物联网能够液化所有的行业，并以人们无从想象的方式，从这些行业中挤压出更多的产能和利润。

<http://www.8btc.com/device-democracy-saving-the-future-of-the-internet-of-things>

### 3.3.2应用案例

IBM的研究团队建立了一个使用区块链技术的物联网分布式平台。IBM开发的系统名为Adept，主要基于三个原则，去中心化（设备自治、使用权限自主识别），尽可能的免维护，尽可能的通用化。

第一个原则的好处就是设备可以逐级向下失控（免控），即设备只需设置好最高权限及其更换方式就可以出厂，而不必对其进行后续的联系和控制，从而不用为这些设备建立巨型的云控制中心。购买者买回去后可以对产品最高权限的识别码（数据摘要）进行更换，并根据需要设置和向不同对象分发不同级别和内容的控制权限识别码（数字摘要）后，也可以不必对其进行后续的联系和控制，以此类推，逐级失控（免控）。最后，设备的各个使用者只要用自己的控制权限识别码接入，就可以按需按权限使用设备，对设备使用者的管理实际上基本是由设备来完成的，一般无需拥有上级权限者来参与（或第一时间参与）。

第二个原则的好处也与逐级向下失控（免控）有关，这样就省去了巨大的云控制中心的维护费用，设备就能变得更简单更稳定，更好用更不容易坏，甚至能够达到免调试免维修的程度，后期维护成本接近于零。

第三个原则的好处更是不言而喻，设备通用，使用的场景又可以随需而变，不单对于实现产品的规模化生产和降低产品成本有着巨大的好处，而且对于产品的购买方也有着产品可以大规模灵活快速部署以及低成本自由调整用途的好处，更为其妙的是这样的产品还可以在不同的使用者间流转使用，能够满足每个使用者的需求，却不用进行任何的调整。

Adept物联网技术在应用上的突破口，主要选择在某项专效功能上进行大规模部署和应用的场景中，也就是说只有某一种类的功能，但用户又特别多的，需求量特别大的产品。比如人流量特别大，但又不用派人进行管理，用户使用起来各自为政，又遵循某些统一原则的地方，如无人驾驶公路、电信和网络自动交换机、无人管理自动售货机或自助存取柜、无人超市、军队使用的自动权限认证令牌、旅游景点的自动游客导流门禁系统等。

Adept平台由三部分构成：

（1）区块链：区块链可让设备了解其他设备的功能，以及不同用户围绕这些设备的指令和权限，即追踪设备之间的关系、用户和设备之间的关系，甚至在用户同意下两个设备间的关系。这意味着智能手机可以安全地与门锁交互，或者与别人和门锁交互。这些关系将被存储在门锁和手机上，并在需要时结合到一起，确保正确的人进入家里，无需返回到云端。

（2）Telehash：设备除了使用区块链来理解交易，它们还需要沟通，所以Adept使用了Telehash，一款使用JSON来共享分布式信息的私人信息传递协议。创造者Jeremie Miller说，telehash是一款“非常简单和安全的终端到终端加密库，适合任何应用程序，终端可以是设备、浏览器或移动应用”。他补充道，“或许可以把它当作SSL和PGP的结合，专为设备和应用连接设计并创建的安全的私有网络。”

（3）BitTorrent：由于连接网络不会一直很稳定(比如使用蓝牙和Zigbee连接)，Adept会使用文件共享协议BitTorrent来移动数据，保证Adept的分散化特性。

## 3.4 身份验证

### 3.4.1概述

### 3.4.2应用案例

案例1：

基于区块链的婚姻，有效期仅有42个月

我一直觉得特技婚礼是一种有趣的悖论，一对夫妇想要取代社会中最根深蒂固的传统之一，做一些表明上的改变，并向世人展示他们的思维是多么的前瞻性。这就像是以五步抑扬格的格律，书写一本革命性的小册子一样。

但我的心脏，却因为Edurne和Mayel的婚礼而加速跳动了，12月1日，作为爱沙尼亚不断扩大的电子居住计划的一部分，这对夫妻的婚礼将不在牧师或者法官面前见证，而是通过全能的[区块链](http://8btc.com/article-44-1.html)，一种分布式的全球计算和数据存储技术。

爱沙尼亚将通过电子居住身份来扩大服务，在2014年其首次给该国的虚拟公民授予了暂居的身份。到目前为止，爱沙尼亚的电子居民可以成立公司并访问 该国的在线银行系统。明天开始，电子居住方案将提供国家认可的公证服务，包括结婚许可。为了做到这一点，他们把目光转向了BitNation，一个基于比 特币区块链提供创建管理服务工具的组织。

对于BitNation而言，它的目标更是宏伟。该组织由Susanne Tarkowski Tempelhof创立，其倡导无边界管理，并已建立起自己的虚拟国度。为了合法化这种声明，它已建立了一套工具以及服务，也许某一天它甚至可以允许人们 用区块链身份来取代他们的国民身份。当然，前提是得其他地域界定国家承认区块链作为政府记录安全和合法的存储库，那这种壮举才能成为可能。而这对夫妇的婚 礼，以及爱沙尼亚的参与，可能会是第一步。

2015年12月1日，这是Edurne和Mayel的日子。这对夫妻自称为“glomads”，他们经过不断地旅行和探索，决定不再支持任何一个 国家或者法律。他们已经写了自己的婚姻合同，有效期仅仅只有42个月，并且合同还将是保持开放的，可以随时更改。这种灵活的协议，在传统的法律框架下是无 法完成的，因此他们决定创建一个属于自己的，符合他们预期的婚姻管辖权。

案例2：

CryptID：一个基于区块链技术的开源身份识别系统

门禁系统是安全部门不可分割的一部分，它是极其重要的，几乎每一所学校、机场、公司办公室、政府办公楼、甚至是只要有人员移动的地方都会有门禁系统的限 制。甚至你口袋里的驾照都是这个行业的产物，它很有可能使用的是45年前的磁条科技，很容易被暗网上提供付费服务的人伪造。  
  
目前，很多政府部门和大公司都在使用很多安全公司提供的门禁系统。这些系统都有一个中心数据库来存储个人数据，很多还发行了某一类的身份卡。  
  
数据库越大安全要求越高，那么费用也越昂贵。其中最大的数据库需要有当地的协作数据处理中心，以及武装警卫和它们自己的门禁系统。这种中心化的案例永远受 会受制于黑客攻击、故障停机、软件许可费和升级、巨大的能源成本、硬件局限性、网络限制、技术支持、IT培训等等。今天的系统，远不够完美。  
  
CryptID是一个全新的开源身份识别系统。它是一个低成本、极其灵活的身份标识发行和验证程序，可用于任何大小的组织。该轻量级的程序使用Factom（公证通）来将加密身份数据写入区块链，并允许多种用途和很多设定，甚至允许使用身份证。  
  
因为身份记录，包括很小的照片和指纹文件，不会超过几百KB，因此CryptID的团队能够使用Factom将整个记录存入区块链，而且还会在比特币区块 链中进行时间标记。无需运行本地管理员服务器即可让其他人访问；所有的数据都是去中心化存储的，而且可以从任何地方进行访问。  
  
CryptID团队说：“我们可以将多个入口形成链条，每一个的大小为10kb，每一kb花费一定数量的进入信用，大概是0.005美元。我们使用指纹模 板（国际标准化组织标准），实际上它非常小，小于1kb。我们对图片进行裁剪并压缩，损失了一点图片质量，但仍然容易识别，大约为5~6kb。其它的信息 大约为600字节，这取决于你的名字长度。所有这些加起来大约为8~9kb，用一点点钱就可以将其很容易地存储在Factom上。”  
  
CryptID最初诞生于BitGo赞助的“无国界国际学生黑客马拉松”上创建的。这个竞赛最初的标准是创建基于无需授权、开放和去中心化账本的应用。裁 判包括Ethereum（以太坊）的创始人维塔利·博特瑞（Vitalik Buterin）和Airbitz的威尔•彭嘉敏（Will Pangman），CryptID获得了第二名。  
  
从安全角度看，使用该方案可以获得比传统解决方案更多的好处。主要的好处就是从去中心化中获得的成本节省，因为无需数据中心或专用的服务器，区块链会存储所有的信息。可以在互联网的任何地方对身份进行验证，无需管理员服务器。  
  
“数据分布在很多电脑中，可以防止腐败，而且你的身份数据几乎不可能被篡改。传统的身份识别方法依靠中心化的机构，例如州政府，来确认你的身份，这样就很容易受到攻击和篡改。”  
  
加强版的安全性，区块链系统采用了比特币多重签名地址的优势，因此没有单个参与方持有任何人的身份信息。开源意味着没有人能轻易破坏它。密码也可以和卡绑定起来，例如照片和指纹，给用户提供了额外保护。  
  
“传统的身份识别方法只需要一个验证要素，即你所持有的卡。CryptID要求使用三个。你所拥有的唯一的身份标示，你所知道的密码，以及代表你自己的指纹。”  
  
灵活性是另外一个特点。因为用户数据并非一定要存储在一个照片身份证中。这些信息可以存放在能保存几KB信息或QR扫描码的地方，只代表你的私钥和密码。甚至可以将符号隐藏在珠宝中或者你的手机APP都可以存放你的身份证件。  
  
CryptID卡的正面是CryptID.xyz发行的信息。背面显示的是指纹和二维码，如果你想要编辑卡片上的信息，则需要重新制作一张，因此，正确处置旧卡是很重要的。  
  
项目负责人史蒂文•马斯里（Steven Masley）告诉Devpost：“因为CryptID字符串可以存在存储能力为32~44字节数据的任何地方，这意味着它可以实施到目前的校对系统中，例如磁卡阅读器或智能卡阅读器。”  
  
“此外，可用智能手机来转移光学数据 ，通常，是一个可以通过扫描器或摄像头扫描的二维码。”  
  
马斯里和其合伙人达科塔•巴伯（Dakota Baber）创建CryptID以用于说明性的网页应用和独立的Windows系统程序，可以在Github上查看源代码。一个智能手机app就可以验证其它人的身份信息了。目前软件已经完成了。  
  
CryptID并非第一个基于区块链的去中心化身份解决方案。Bitnation是第一个获此殊荣的应用，它是2014年10月份发布的世界公民身份证件项目。但还没有开源，可以免费使用，并将你的身份信息永久存在区块链上。  
  
它们之间最主要的区别在于，CryptID设计用于管理员来发行身份，因此身份拥有一个具体的组织来授权使用它们。  
  
而Bitnation的身份系统则可以为用户创建一个全新且没有从属关系的身份，可以在不使用任何第三方，甚至不用Bitnation授权的情况下就能证 明你的身份。但是用户获得访问时要处于在线状态。进出真实生活中类似于门这样的物体时不太可能会使用它，尽管不是没有可能。  
  
马斯里说：“CryptID的开源性会使其获得更广泛的应用，可用于安全和独特的系统中。使用区块链的不可篡改、抗黑客攻击、身份存储都是很新奇的，在行业中是空前的。”  
  
而Bitnatiaon将来有一天会是国家发行的身份证件的取代方案。目前CryptID已经准备用于企业和高校了，会节省很大一笔安全预算。

## 3.5 预测市场

### 3.5.1概述

预测市场类似于股票市场，用户可以在预测市场中买卖股票。但是，与股票市场对一个公司的未来价值进行投机不同，预测市场的存在是为了决定未来事件结果的可能性。例如，一个预测市场可能问“川普在2016年能被选为美国总统吗？”，如果“是”股票的价格是0.43美元，这可以被理解为川普当选总统的可能性是43％。大量的经济和学术研究发现，预测市场是世界上最精确的预测工具之一，特别是当用真钱进行和具有足够的流动性和交易量（这是传统预测市场的问题所在）时。

在2007年，哥伦比亚商学院教授Michael Mauboussin让他的73位学生聚集瓶子中糖豆的数量。学生所估计的数量在250-4100之间。其实瓶子中有1116个糖豆。学生们估计值与真实值1116平均偏离700。也就是62%的错误率。然而，尽管学生的估计很不准确，但是他们估计的平均值是1151，与真实数值1116只有3%的误差。这一研究以各种形式被重复过多次，结果都与上面相同。我们正在将这种群体智慧应用到每一个学科中，从政治学到气候学，并用利益得失来强迫群体说真话。

在1968年5月，美国的一艘名为Scorpion的潜艇，在大西洋完成执勤任务返回纽波特纽斯港口的途中消失了。虽然海军知道潜艇最后的报告位置，但是不知道Scorpion发生了些什么事情，只知道自最后一次联系后，潜艇大概又前行到哪里。最后他们将搜索范围确定在方圆20英里，几千英尺深的区域。这是一个希望渺茫的搜索。人们能够想到的唯一可能的解决方案是，召集三、四位潜艇和洋流的顶级专家，问他们认为潜艇在哪里。但是，根据Sherry Sontag和Christopher Drew在《Blind Mans Bluff》的记录，一位名叫John Craven的海军军官有一个不同的计划。

首先，Craven设想一系列可以解释Scorpion可能发生的事故的情景。然后，他召集了一组具有不同背景的人，包括数学家、潜艇专家和搜寻人员。Craven让他们猜测那种情景的可能性最大，而不是让他们彼此商量得出答案。为了让猜测更加有趣，Craven采用了下注的模式，奖品是Chivas Regal酒。参与的成员就潜艇为什么出事故、下沉的速度、倾斜的角度等问题进行打赌。

没有一段信息碎片能够告诉Craven潜艇在哪里。但是，Craven相信，如果他将小组成员提出的所有答案汇集在一起，针对潜艇沉没做一个完整描述，他就能够知道潜艇在哪里。这就是Craven 所做的事情。他利用了所有的猜测，使用被称为贝叶斯理论的公式，判断潜艇的最后位置。（贝叶斯理论是计算事件的新信息如何改变你对此事件原有预期的方式。）做完这些事情，Craven获得了团队关于潜艇位置的集体估计（collective estimate）。

Craven 得出的位置并不是团队任何单个成员所猜测的位置。换句话说，团队中每个成员的猜测与Craven使用汇集起来的所有信息得出的位置一致。最后的判断是一个由团队整体做出的集体判断，而不是代表团队中最聪明人的个人判断。它也是一个绝妙的判断。

Scorpion潜艇失踪五个月以后，一艘海军船发现了它。潜艇所发现的位置与Craven团队猜测的位置相差220码（译者注：1码等于0.9144米）。

这个实例的惊人之处在于，这个团队所依靠的证据几乎没有，只是一些数据碎片。没有人知道为什么潜艇沉没，没人知道潜艇下沉的速度和倾斜角度。虽然团队中没人摘掉这些信息，但是作为一个整体的团队却知道这些信息。

### 3.5.2应用案例

Augur是一个去中心化的预测市场平台，基于以太坊区块链技术。用户可以用数字货币进行预测和下注，依靠群众的智慧来预判事件的发展结果，可以有效地消除对手方风险和服务器的中心化风险，同时采用加密货币（如比特币）创建出一个全球性的市场。



利用 Augur，任何人都可以为任何自己感兴趣的主题（比如美国大选谁会获胜）创建一个预测市场，并提供初始流动性，这是一个去中心化的过程。作为回报，该市场的创建者将从市场中获得一半的交易费用。普通用户可以根据自己的信息和判断在 Augur 上预测、买卖事件的股票，例如美国总统大选。当事件发生以后，如果你预测正确、持有正确结果的股票，每股你将获得1美元，从而你的收益是1美元减去当初的买入成本。如果你预测错误、持有错误结果的股票，你将不会获得奖励，从而你的亏损就是当初的买入成本。

许多因素使得 Augur 不同于传统的预测市场，但是最重要的区别是，Augur 是全球化和去中心化的。世界各地的任何人都可以使用 Augur ，这将为 Augur 带来空前的流动性、交易量和传统的交易所不曾有过的多种视角和话题。

信誉（REP）是 Augur 系统的代币。REP可以被看作一种与个人的公、私地址相关的“积分”，像比特币一样可分割和可交易。然而，只有这点属性类似于密码学货币。如果说比特币模拟黄金，那么可以说 REP 模拟信誉。

Augur的去中心化还体现在事件结果报告机制上。在传统的中心化预测市场，当事件发生以后，由中心化的人或者组织确定事件结果。与此不同，Augur 采用去中心化的事件结果报告机制，从而引入 REP 代币。每当事件发生以后，众多 REP 持有者对事件结果进行报告。但是，普通用户无需持有 REP 即可在 Augur 上进行预测、交易。

持有 REP 的人被期望每八周对系统中随机选择的到期事件／预测的结果进行报告。持有者只需要从三个选项：是的（事件发生了）、不是（事件没有发生）、模糊不清／不道德的（如果持有者认为结果模糊不清，可以将报告推迟到下一期，在最终没有决议就结束事件以前）报告者有两个星期的时间来做报告。我们期望这一过程能够十分快速地进行，但是当 Augur 普及以后，这一过程可能在一小时内完成。

如果信誉持有者在两周的投票期内没有报告指派给他们的事件的结果，或者进行不诚实地报告，主成分分析法（PCA）会将懒惰的、不诚实的持有者的信誉重新分配给经常报告和诚实报告的持有者。只有诚实的信誉持有者将从每一投票过程中获得交易费用。

http://www.8btc.com/augur-crowdfunding

## 3.6 资产交易

### 3.7.1概述

### 3.7.2应用案例

数字资产控股（Digital Asset Holdings），对于这家高调的区块链公司，业内似乎知道的信息，仅仅围绕于公司首席执行官Blyth Masters的一些事情，至于这家平台在做些什么，用的是什么技术，却并没有很多有用的资料。

上个月，该公司宣布将代码移交给了Linux基金会，以进行合作开发，几天之后，这家公司就宣布获得了13家金融机构的5200万美元融资。

被称为Linux基金会的开放式账本项目，获得了一些大牌公司的承诺，包括IBM，摩根大通以及富国银行。而数字资产公司在其中也是非常特殊的，除了贡献了代码，这家公司还提供了“Hyperledger”的品牌名，这是数字资产公司在2015年收购而来的。

但是，至今为止，关于数字资产公司的区块链技术，却并没有公布太多的技术细节。

这家成立于2014年的公司，此前将自己定义为一家软件提供商，利用“分布式基础设施”为客户提供“资产结算”服务，然而，在上周五公布的项目技术详细声明来看，数字资产公司已将自己描述为“企业级区块链服务和客户端 API服务”。

该公告继续表示：

“Hyperledger采用了仅追加日志（append-only log of）金融交易，它的设计需要依靠多个组织，但不会有中心控制。”

数字资产的的书面表达建议，Hyperledger将被定义为：负责协调多个客户端的服务数据和低层次的“沟通和共识层”，一个致力于提高全球金融基础设施的“数据骨干”。

“Hyperledger的目标是允许将数据骨干理念扩展到多个组织层，”它继续补充说，“我们会开源化这个项目，并相信它会作为全新金融基础设施的重要组成部分。”

Digital Asset指出“最新稳定版本”的代码，Linux基金会的Hyperledger项目和技术指导委员会对此进行审查。

该公司还承诺了一些即将进行的改进，其中包括公布一些Blockstream元素（Elements）项目的功能。

对比特币的态度

值得注意的是，Digital Asset公司承认说，他们会利用开源比特币区块链的理念，而在此前，公司首席执行官Blyth Masters 在她的公共演讲中却一直对比特币闭口不谈。

“Hyperledger利用了和比特币相同的UTXO/script 交易决策，并根据金融服务所需要的功能进行了扩展，” 该创业公司写道。

该公告继续指出，虽然该公司并不相信比特币“适用于受监管金融基础设施的多种用途”，它也为区块链应该如果保障安全，提供了宝贵的见解。

“比特币很多的设计和成熟的加密技术，一直在遭受着攻击，其市值数十亿美元的代币一直被保护着，”数字资产公司写道。

该声明提供了关于私人或许可账本公司对比特币网络的评估，而他们正在寻求构建比特币的替代型系统。

拜占庭容错

据悉，数字资产公司也证实说，它会提供一种工作量证明(POW)挖矿的替代型共识系统。比特币的共识系统，使用了去中心化的计算机网络来保障比特币区块链和交易的处理。

数字资产公司表示，Hyperledger包括一个可实现的拜占庭容错共识模块的“原型”，该模块将作为挖矿过程的替代过程。

“关于这个共识模块，我们正在和项目的其他成员合作，以保证一个可扩展、安全的拜占庭容错一致协议，可为金融机构提供结算终结性，” 声明表示。

这一概念，自原Hyperledger团队于2014年成立以来，就一直在进行开发，而且似乎仍在评估阶段。

## 3.7 电子商务

### 3.7.1概述

传统的电子商务公司，采用中心化的服务，如eBay、亚马逊、阿里巴巴等电子商务平台，对卖家实施严格监管。他们需要用户的个人信息，这些信息可能被盗取或者卖给其他人，用于精准投放广告或者危害更大的滥用。因为电子商务公司和政府审查所有的交易商品和服务，所以买家和卖家不能总是自由地进行交易。

特别是国内的电子商务平台，刷单已成潜规则，消费信任体系面临严重挑战。消费者的购买行为很大程度上依赖销售排名、购买评价等，自然也会对消费者产生误导，造成错误的选择。刷单破坏了竞争秩序，如果商家都来刷单，市场交易将会偏离公平竞争的轨道，网购生态环境将进一步恶化。刷单尽管在短期内会带来利好，但长期看会严重损害企业的品牌价值。网络交易的维系要靠商家的信用和消费者认可，一旦由于刷单引发消费信任体系崩塌，对于电商发展可能是致命的，不能够掉以轻心。

去中心化的OpenBazaar为电子商务提供了另一途径。它把权力归还到用户手中，将卖家和买家直接联系在一起，不再需要中心化的第三方来连接买卖双方。因为在交易中不存在第三方，所以不存在交易费用，没有人能够审查交易，而且公开个人信息的决定权在用户手中。

### 3.7.2应用案例

OpenBazaar是为网上点对点交易创建的去中心化网络的开源项目。OpenBazaar平台上买卖双方使用比特币进行交易，没有费用，而且不会受到政府监管机构的审查。简单的说，它就是eBay和BitTorrent结合的产物。

假如，你打算出售你的旧笔记本电脑。你需要首先下载OpenBazaar客户端，然后在你的电脑上创建一个商品目录，并标明商品的细节。当你公布这一商品目录后，该目录被发送到OpenBazaar的分布式P2P网络上。其他OpenBazaar用户搜索你设置的关键词-笔记本、电子产品等-时，他就可以发现你的商品目录。他可以接受你的报价或者不接受报价，提出新的报价。

如果你们两个人都同意价格，OpenBazaar客户端就会使用你们的数字签名在你们之间创建一个买卖合约，并将该合约发送到被称为公证人的第三方。当买卖双方产生纠纷时，公证人就介入交易。这些第三方公证人和仲裁者也是OpenBazaar网络的用户-可能是你的邻居也可能是地球另一端的陌生人-产生纠纷时，卖家和买家都信任的人。第三方为合约作证，并创建多重签名比特币账户，只有当集齐三个签名中的两个时，比特币才会被发送给卖家。

买家发送商定好的数量的比特币到多重签名地址。你会得到通知，知道买家已经发送货款，然后你就可以发货了，并告诉买家已经发货。几天以后，买家收到笔记本，他将告诉你收到笔记本，并从多重签名地址释放货款。你获得了比特币，买家获得想要的笔记本。没有交易费用，没人审查交易，买卖双方皆大欢喜。

对于一个去中心化的交易市场来说，如果产生交易纠纷该怎么办？这时候就需要第三方介入了。多重签名需要集齐三把私钥中的两把才能够从多重签名地址中取走货款。第三方公证人控制着第三把私钥，所以在买卖双方达成和解或者第三方认为卖家或者买家是正确的以前，多重签名地址中的比特币不会被移动。同时，OpenBazaar有一个信誉评分系统，允许所有的用户对其它用户进行反馈评分。如果某些人打算诈骗其他的用户，他们的信誉将会受损，第三方如果不能公正裁定交易纠纷，他们的信誉也会受损。当你在OpenBazaar平台上购物和选择第三方公证人时，你更够看到他们的信誉评分，判断其它用户是否信任他们。这样，就算是在用户信息不被公开的情况下，你依然可以凭借信誉评分系统判断是否信任别人。

资料地址：

http://www.8btc.com/openbazaar-16-3-1

## 3.8 文件存储

### 3.8.1概述

传统的中心化云服务，如亚马逊、阿里云等，其成本主要来自于数据中心建设、员工工资等，随着业务量增长，中心化的云存储架构来提供数据存取服务是昂贵和低效的，同时数据中心消耗了全球约[1.1%-1.5%的电力](http://www.koomey.com/post/8323374335)（并且以每年60%的速度增长）。用户账号和密码被盗的新闻屡见不鲜，已经证明在这种架构下，用户资料的安全性几乎是不可能的。数据中心成为了互联网的瓶颈。而采用去中心化的存储成本却只有中心化存储的1/100~1/10，一旦去中心化存储系统是完全自动化的，云存储价格最终会降至0。如同uber一样，通过基于去中心化云存储平台，你也可以出租额外的硬盘空间，并获得相应的回报。例如Storj、Enigma、Maidsafe这类的平台都已经实现了。

区块链是一种新型的去中心化协议，能安全地存储交易或其他数据，并且无需任何任何中心化机构的审核监管。一种新型的云计算平台，运行于区块链的基础设施当中，无需假设任何服务器。对于区块链，除了把它当个账本来确认交易，我们也可以认为它是由计算设备所组成的网络基础设施。但我们也不应把它理解为传统意义上的云计算，区块链的基础设施并不替代现有的云计算技术，而是将云计算基础推向了大众。相比于传统的云计算基础设施，区块链云可以认为是“瘦云”。因此它更适合运行一种叫做智能合约的程序，我们可以将智能合约理解为运行于区块链中“虚拟机”上的商业逻辑。显然虚拟机这个名字是从传统云计算中借用来的，其实它就是这些去中心化的计算机所组成的虚拟网络，这些计算机由区块链的共识机制联系在一起，这一共识就是：执行特定的计算机程序。

我们可以与传统云计算虚拟机上运行程序的开销做一个对比。在亚马逊AWS这样的云平台上运行一个应用时，收费是根据运算时间、存储、数据传输和计算速度共同决定的。而对[以太坊](https://www.ethereum.org/)这样的平台来说，你的逻辑运行于物理服务器中，但你其实无需要关心这些服务器如何运行，因为其他用户，也就是俗称的矿工正在帮你打理着服务器。这是一个类似于众包的过程，矿工们根据自己硬件的使用而获得报酬。因此，区块链云可说是有一种微型价值定价，它通过一个加密的交易确认和状态变换的记录层实现了传统云计算架构的扁平化。

在这个新的架构之上运行应用还有一项挑战：需要修改你的应用，并遵守基于区块链的Web 3.0架构。我们以太坊来为例，一个三层的Web3.0架构包括：1）先进的浏览器作为客户端；2）区块链作为共享的资源；3）由计算机组成的虚拟网络以去中心化的方式运行着商业逻辑。这一范式实际上就是加密去中心化计算发展方向的一个例子，它也是现在的网络应用架构的一个变形。

### 3.8.2应用案例

Sia是分布式文件云存储服务运营商，其发布的一款数据存储协作云服务，这项服务是基于区块链的，具有自动化点对点的特性，允许用户在可靠的安全协议下定制存储计划。类似于去中心化的存储项目Filecoin和Storj，Sia的目标是建立一个非信任的、具有容错能力的文件存储服务。

Sia平台存储有个人和用户数据，分散存储在众多节点上，可以被自动化智能合约追踪。文件由多阶段进程提供保护，并且由加密算法Twofish加密。平台的强大功能建立在RS分布式文件系统上。所有用户数据在进入Sia客户端的时候都被分割成很多小块，只留下用户恢复原始数据的少数片段。敏感用户信息块被压缩到4M，用于保护用户隐私。最后，每个压缩块又使用客户端的秘钥进行加密。安全协议用来防止黑客攻克Sia平台并窃取用户数据。主机接收到一个加密的二进制块，并且没有关于文件其它部分的信息。即便是黑客们发现了，他们也仍然需要破解众多的加密密钥用以恢复文件。

Sia平台严格而复杂的加密和去中心化分布式文件系统可被用于去中心化应用开发。它的API使得开发者可以直接在Sia客户端存储文件，允许第三方应用用户直接访问他们的客户化数据存储系统，并且不需要改变原来的客户端。  
  
这家公司也发布了与Crypti合作的消息，Crypti是灵活的后台应用开发平台。在这项合作中，Crypti的工程师可以集成Sia 的API，访问Sia的数据存储客户端。  
  
Sia团队告诉Bitcoin Magazine：“作为他们去中心化应用开发的存储层，Crypti已经集成了Sia。Sia提供了API，可以上传文件到存储网络。Crypti是一 个灵活的平台，可以集成多个后台，但是Sia是第一个去中心的尝试，允许开发人员创建实实在在的非信任Crypti应用。”  
  
第三方应用和Sia平台用户都有权发布在文件存储上的智能合约。这种特性就使得上传者和主机在存储要素上取得共识，包括存储期限、付费计划和总额，并且可以将信息嵌入到区块链中，自动建立一个不可更改的合约。  
  
Sia团队解释道:“当合约到期时，主机就会提交一个存储证明到区块链，显示它仍然是合约定义的文件。如何证明是有效的，上传人员的钱将被支付到主机，主机将返回抵押品。但是如果主机提交了无效的证明，或者没有提交证明，所有的钱都将还给上传者。”  
  
“Sia网络的超级并行性意味着上传和下载速度可以满足绝大部分连接要求。大型分布式节点整列意味着Sia是一个强大的CDN。广义网上不存在编程逻辑， 使得Sia在面对电力中断方面更灵活性，比如在电力供应中断和发生自然灾害的时候。Sia网络的具体实现上各方面都是非常先进的。”  
  
目前，Sia云存储网络售价是每T每月3美元。据网站所述，目前这个网络上已经存储有超过1T的数据。  
  
现在这个项目已经正式发布了，Sia团队的目标是让开发者和企业客户也参与进来。随着平台越来越引人注目，这个团队计划持续改进核心Sia协议，聘请高级工程师改进平台的安全协议和用户体验。

## 3.9 数据库

### 3.9.1概述

数据发展阶段分为三个阶段，最初的第一阶段，数据是无序的，并没有被充分检验过的数据，然而当大数据和大规模社交网络的兴起，进入了第二阶段，通过大数据的交叉检验和推荐，所有的数据将会根据质量进行甄别，这些数据将不再是杂乱无章，而是能够按一定人工智能算法进行质量排序。到了现在，区块链能够将让数据进入第三阶段，即有些数据将通过采用全球共识的区块链机制，这些数据可以获得基于互联网全局可信的质量，这几乎可以说人类目前获得最坚固信用基础的数据，这些数据的精度和质量都获得了前所未有的提升。这三个阶段恰好符合了互联网数据库发展需要经历的三个阶段。即从关系型数据库发展到非关系型数据库，再到区块链数据库。

在互联网诞生初期，我们所设计的系统数据库主要采用关系型数据库，这是一种采用了关系模型来组织数据的数据库。关系模型是在1970年由IBM的研究员E.F.Codd博士首先提出的，在之后的几十年中，关系模型的概念得到了充分的发展并逐渐成为主流数据库结构的主流模型。简单来说，关系模型指的就是二维表格模型，而一个关系型数据库就是由二维表及其之间的联系所组成的一个数据组织。

随着互联网web2.0网站的兴起，传统的关系数据库在应付web2.0网站，特别是超大规模和高并发的SNS类型的web2.0纯动态网站已经显得力不从心，暴露了很多难以克服的问题，而NoSQL的数据库则由于其本身的特点得到了非常迅速的发展。NoSQL一词首先是Carlo Strozzi在1998年提出来的，指的是他开发的一个没有SQL功能，轻量级的，开源的关系型数据库。这个定义跟我们现在对NoSQL的定义有很大的区别，它确确实实字如其名，指的就是“没有SQL”的数据库。但是NoSQL的发展慢慢偏离了初衷，我们要的不是“no sql”，而是“no relational”，也就是我们现在常说的非关系型数据库了。2009年初，Johan Oskarsson举办了一场关于开源分布式数据库的讨论，Eric Evans在这次讨论中再次提出了NoSQL一词，用于指代那些非关系型的，分布式的，且一般不保证遵循ACID原则的数据存储系统。Eric Evans使用NoSQL这个词，并不是因为字面上的“没有SQL”的意思，他只是觉得很多经典的关系型数据库名字都叫“\*\*SQL”，所以为了表示跟这些关系型数据库在定位上的截然不同，就是用了“NoSQL“一词。非关系型数据库的产生就是为了解决大规模数据集合多重数据种类带来的挑战，尤其是大数据应用难题。

目前大数据应用最大的难题就是很大部分是脏数据，并且不可信。因为互联网将使得全球之间的互动越来越紧密，伴随而来的就是巨大的信任鸿沟。目前现有的主流数据库技术架构都是私密且中心化的，在这个架构上是永远无法解决价值转移和互信问题。所以区块链技术将成为下一代数据库架构。通过去中心化技术，将能够在大数据的基础上完成全球互信这个巨大的进步。



区块链技术作为一种特定分布式存取数据技术，它通过网络中多个参与计算的节点开共同参与数据的计算和记录，并且互相验证其信息的有效性（防伪）。从这一点来，区块链技术也是一种特定的数据库技术。在目前互联网刚刚进入大数据时代，但是从目前来看，我们的大数据还处于非常基础的阶段。但是当进入到区块链数据库阶段，将进入到真正的强信任背书的大数据时代。这里面的所有数据都获得坚不可摧的质量，任何人都没有能力也没有必要去质疑。

<http://www.bitcoin86.com/news/8549.html>

### 3.9.2应用案例

Ascribe发布了可扩展的区块链数据库BigchainDB，试图吸收区块链的一些特征，不可更改性、无中央机构、没有资产中央控制，并通过互联网联合节点管理系统来简化设计。BigchainDB填补了去中化生态系统中一个空白，可以达到每秒百万次写入，数据存储量以P计算，次秒延迟。BigchainDB具有目前流行的去中心化数据库的特点: 随着节点数量的线性增长可平滑扩展吞吐量，完全特性的NoSQL查询语言，高效查询及权限控制。容量可扩展意味着具法律约束力的合同及证书都可储存在区块链数据库上。权限控制系统意味着私有和公有的区块链数据库都可共存。

# 第5章 走向未来之路

## 5.1社会组织开始走向去中心化

## 5.2万物互联的信息自组织

## 5.3人的生产力的再造

## 5.4建立有效的可信的基础规则下的社会效率提升

## 5.5让共享经济发挥最大的作用

## 5.6区块链带领人类走向光明的未来之路