智能合约开山之作：《智能合约》——尼克·萨博

**[狗叔UncleDoge](http://www.8btc.com/author/5770" \o "由 狗叔UncleDoge 发布) 2016-03-14 14:03 发布在 [区块链](http://www.8btc.com/blockchain" \o "查看 区块链 中的全部文章) [2](http://www.8btc.com/smart-contracts-1994" \l "comment) 1836**

译者(狗叔UncleDoge)按：“智能合约(Smart contract)”概念由计算机科学家、加密大师尼克·萨博(Nick Szabo)在1993年左右提出来，1994年他写成了《智能合约》(Smart contracts)论文，是智能合约的开山之作。尼克·萨博在数字合约和数字货币领域的研究非常出名，他创造了“智能合约(Smart contracts)”一词和相关概念。智能合约是加密货币和E编程语言的一个主要功能。早在1998年，尼克·萨博就设计出了一种叫“比特黄金”(bit gold)的去中心化的数字货币机制，由于缺少广泛支持最后失败了，但是却被公认为是比特币的最直接先驱。尼克·萨博被经常被怀疑是比特币背后的神秘发明者 — 中本聪(Satoshi Nakamoto)。



一个智能合约(Smart contract)是一个计算化交易协议，用来执行合约条款。智能合约设计的通常目的是为了满足一般的合同条件(譬如支付条款，扣押令，私密性，甚至是执法)，最大限度减少恶意和意外的状况，最大限度减少使用信任式中间媒介。相关的经济目标包括降低欺诈损失，仲裁和执法成本，还有其它的交易成本[[1]](http://www.8btc.com/smart-contracts-1994" \l "footnote-1)。

对于今天已经存在的一些技术可以被认为是粗糙的智能合约。例如，自动刷卡机(POS)和卡，电子数据交换(EDI)，公共网络带宽的供需分配。

数字现金协议(Digital cash protocols)[[2]](http://www.8btc.com/smart-contracts-1994" \l "footnote-2)是很好的智能合约例子。他们实现了网上支付，同时保留了纸币现金的特点：不可伪造性，私密性和可分性。当我们再瞟一眼数字现金协议族时，把他们放在智能合约设计的更大范围里，我们可以看到，这些协议能够被实施到种类繁多的电子无记名有价证券，而不止于数字现金。我们还可以看到将它们应用到一个完全的顾客-供应商交易体系里。我们需要的不止是数字现金协议；我们需要一个这样的协议：它能够完全保证如果付款了，商品会被发送，或者商品寄出去了，就会收到钱。现时的商业系统使用各种各样的技术来完成这个目的，如邮件确认，面对面交易，凭靠信用记录和讨债公司延长信用等。智能合约拥有可以大大减少许多商业交易欺诈和执法成本的潜力。数字现金协议使用了几个来源于密码学和计算机科学领域里新近发展的重要基础技术。大部分技术还没有被广泛地利用到促进这些合约安排，但是前景广阔。这些副协议族包括拜占庭协议(Byzantine agreement)，对称性和非对称性加密(symmetric and asymmetric encryption)，数字签名(digital signatures)，盲签名(blind signatures)，分割&选择(cut &choose)，比特承诺(bit commitment)，秘密分享(multiparty secure computations, secret sharing)，不经意传输(oblivious transfer)，和多方安全计算(multiparty secure computation)。所有这些协议除了第一个都在[[3]](http://www.8btc.com/smart-contracts-1994" \l "footnote-3)里有描述。

智能合约设计在合同法，经济学和合同起草策略上的结果很少被探索研究(反之亦然)。除此之外，我怀疑能够大大减少执行某些合约的交易成本的可能性和在智能合约上创造新商业和社会机构的机遇虽然是巨大的，但是也很少被研究过。“密码朋克”(“cypherpunks”)[[4]](http://www.8btc.com/smart-contracts-1994" \l "footnote-4)探索了一些新基石式协议的政治影响。在电子数据交换(EDI:Electronic Data Interchange)领域，传统商业交易元素(发票，收据等)的电子化交易，有时候包括加密和数字签名这些功能，可以被视为智能合约早期先行者。实际上，这些商业形式为智能合约设计者提供了很好的出发点和杀出了一条通道。

智能合约其中一个被传统电子数据交换(EDI)所忽视的重要任务是对参与方之间交易时的语义进行交流。智能合约在“智能保留条款”里有足够的机遇：软件可以对交易的一方做手脚。例如，杂货店刷卡机(POS)没有告诉顾客们他们的名字与他们的购买行为在数据库里是否是绑在一起的。职员甚至也不知道，在自己的眼皮底下他们处理了成千上万这样的交易。结果，通过隐藏的软件操作，顾客就这样把对他们有价值的和私密的资料给出去了。但是合同已经是起草好了的，交易本身也已经是设计好了的，通过这样的方法，对顾客隐藏了那些交易的重要部分。

为了使交易语义交流得更好，我们需要一些通俗的可视化比喻对合约元素作出解释。这些措施将导致隐藏了协议的细节方面，但是没有失去对合约条款的认知和执行的控制。发生在早期却是一个很好的例子是商业网 (CommerceNet，B2B非赢利性组织)开发的SecureMosiac软件所提供的功能。把文档放进信封里，往文档或信封上盖上印章进行数字签名，这样就加密了。另一方面，Mosaic服务器在没有警醒用户的情况下记录着这些联系，有时甚至是交易本身 — 典型的隐藏行为。

另一个将会考虑使用智能合约的领域是合成型资产(synthetic assets)[[5]](http://www.8btc.com/smart-contracts-1994" \l "footnote-5)。这些新型的证券由资产证券(如债券)与衍生品(期权与期货)以各种各样的方式混合而成。通过对这些复杂的期限结构进行计算化分析，非常复杂的期限结构支付(比如付款时机，利率等)现在可以建成标准化的合约和以低成本进行交易。

合成型资产允许我们对不同顾客所需求的各种期限结构进行套利，也允许我们进行合约设计时模仿其它合约，减少某些责任。在后者的例子里，合成型资产被模仿构造为德国公司股票的收益率，而不必满足境外投资者在德国股票市场上的资本收益必须给德国政府支付税收的规定。要注意很重要的一点是这些合成型资产不必像原来的所做的那样需要协商投票权。当然了，这些协议在承受来自第三方管辖权的攻击时可能必须要非常安全，这些在第三方管辖区进行交易的成本(税收)通过合成型资产被套利掉了。

最后，我们将智能合约的概念延伸到财产上。智能财产的建立可以通过将智能合约嵌入到有形的实物里。这些嵌入的协议基于合约条款将运作财产的钥匙控制权自动交到财产的合法代理人手上。例如，一部车为了防止被偷窃，除非确定拥有者完成正确的“挑战响应协议”(challenge-response protoco)，否则车是不会启动激活的。如果车是贷款买的，拥有者无法偿还贷款，智能合约将会自动调用扣押令，并将车钥匙的控制权交给银行。这个智能扣押令(smart lien)应该比回购人更便宜和更加有效。同样需要的是当贷款被还清的时候协议可证明地移除扣押令，和排除一些困难和运行中的情况。例如，当车子以75码的速度奔跑在高速路上时解除车子的操作是粗鲁的。

智能财产可能是一个很长的路，但是数字现金和合成型资产今天已经出现了，更多的智能合约机制正在被设计出来。目前为止，对来自截然不同领域如经济学和密码学的自动化合约执行来说，设计准则是很重要的，缺少交叉沟通(cross-communication)：一边是对技术缺乏意识，另一边对最好的商业用途缺乏意识。智能合约的理念是要认识到为共同目标而作出的努力，将在智能合约的概念上进行交汇。

转载自Nick Szabo的论文集  
译者：狗叔UncleDoge  
责编：萌大大

**注释**    (↵ returns to text)

1. \_The New Palgrave: Allocation, Information, and Markets\_[↵](http://www.8btc.com/smart-contracts-1994" \l "refmark-1)
2. Bruce Schneier, \_Applied Cryptography\_ (digital cash  
   objectives are on pg. 123)[↵](http://www.8btc.com/smart-contracts-1994" \l "refmark-2)
3. \_Crypto\_ and \_Eurocrypt\_ conference proceedings, 1982-1994.[↵](http://www.8btc.com/smart-contracts-1994" \l "refmark-3)
4. “Crypto Rebels”, Wired #2, also cypherpunks mailing list  
   (mail to majordomo@toad.com with body “subscribe cypherpunks”)[↵](http://www.8btc.com/smart-contracts-1994" \l "refmark-4)
5. Perry H. Beaumont, \_Fixed Income Synthetic Assets\_[↵](http://www.8btc.com/smart-contracts-1994" \l "refmark-5)