智能合约的理念
The Idea of Smart Contracts

何谓“抵押品”？ “抵押品”的目的是什么？它怎样梳理了我们的已有的关系？

我认为，尤其是合约的规范化，在我们的关系层面实现了理想化抵押品的蓝图。

多种类型的合约条款，如抵押品，债券，产权界定等等，可以嵌入在我们执行条款的硬件和软件中，通过这样的方式使那些不遵守协议者的违约成本很高，（如果需要的话，令人望而却步的）。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。在潜在的、损失有限的评估后，使钱箱里的钱远远少于破坏者付出的代价。根据显示的价格该机收取硬币，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藏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。

作为另一个例子，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，智能合约调用扣押权协议，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，如果汽车的合约是一个租赁，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。

来源于“规范和保障公众领域的关系”，由尼克·萨博

原文见 http://szabo.best.vwh.net/smart_contracts_idea.html