DAO、技术进步与合约结构

一. 引言

“智能合约” 这个概念在一开始就带有一种颠覆性的意味。Nick Szabo 在 1997 年的文章中就提到：智能合约的实质就是用数字化的方式来控制所有类型的资产 <1>，换言之就是用机器来执行（至少是部分的）产权规则。只要稍微放任我们的想象力，我们立马就会想到用这种机器代替合约和司法体系来 “改造公司制” 的可能性。

但是，**运行 “智能合约” 的前提是其环境足够安全，安全到单个群体的力量几乎无法干预和控制，进而为电子化合约赋予严格的机器属性**，所以 “智能合约” 一直没有找到合适的运行环境。直至 2009 年，比特币主网面世，甚至直到 2015 年，以太坊主网上线。

到 2014 年，去中心化自治组织的概念开始兴起 <2>，一开始这个概念其实带着蛮强的乌托邦色彩，但后来就出现了把它应用于协调人类合作、创造价值的想法。The DAO 就是一个明显的例子，其实它是为投资而设立的。

2016 年，The DAO 被黑，以太坊硬分叉，DAO 概念因此遇冷，同时遇冷的还有另一种观念：Code is Law。

2017 年 ERC-20 代币大火，许多人开始谈论一对新名词：“Token Economy（代币经济）” 以及 “自组织”。虽然似乎没有人说 Token Economy 与 DAO 有什么关联，但我可以隐约看到它对 DAO 的取法和借鉴，比如用代币来规定治理上的权限。

上述引文可以被视为一份报告，告诉了我们：内核极为相似的一组概念，在不同的时期是如何以不同的面貌出现，同时，又如何因为这些不同的面貌而改变了人们理解它的角度。在我看来，它们都是在回答同一个问题：一个数字规则的可信任执行环境，究竟能不能成为协调人类合作、创造新型组织的工具？

二. DAO，自组织与代币经济体概论

在这里我可能会先花时间做一些比较无聊的事情，是归纳一下我们现有的实践，并指出他们不够理想的地方，然后再引向我认为比较合理的方向。

（一）DAO 的定义与实践

先定义一下 DAO：

1）DAO 必须具有可辨识的边界，我们得能清楚看出来谁是、谁不是这个组织的成员，否则 DAO 就成了一个没有意义的概念。比如，整个以太坊社区算不算一个 DAO 呢？我认为不算，因为没有清晰的边界。

2）规限 DAO 成员间关系和权限的主要规则必须被表达为一套可执行的代码，运行在去中心化的系统上。这是所谓的 “去中心化”，即成员间关系主要不是靠现实中的法律来约束的。

3）DAO 必须能够根据那些可执行规则产生共同行动，包括更改自身（部分）规则，而组织外的人会被排除在正式的决策过程之外。

第三点其实是有争议的。因为历史上规模最大的 DAO，也就是 The DAO，就是在从规则到可执行代码的转化过程中出了问题，让黑客有了可乘之机，最终所有人都参与到了 The DAO 的共同行动中。当然，也可以说，这一点并不构成困扰，因为那时候的 The DAO 确实已经名存实亡了。再换句话来说，定义中到底该不该包括第三点，实际上跟你对 “Code should be Law” 的信念有关。

还有一个比较不重要的争议是，参与者可以随时拿着自己的财产退出 DAO，到底算不算是 DAO 的定义。The DAO 一开始就在支持这一点，他们认为如果不能保证这一点，财产更多的人就可以 “合法” 地拿其他参与者的钱用于他们不支持的目的。但是，如果我们放宽一点 DAO 的定义，认为 Aragon 提出的 “Private DAO” 也算是 DAO 的话，这种用多签名来实现的 DAO 是做不到可以随时退出的，你的退

出意味着合约的解除和重新订立，这也是需要共同决定来执行的。

最后，我们来看一个成功案例：MakerDAO。

MakerDAO 用 MKR 标定了成员的身份，并界定了他们对 DAO 的治理权限，让 MKR 持有者的投票结果来决定 Maker 的共同行动，这些共同行动的主要作用在于确定 MKR 对风险的承担。众所周知，Maker 发行了著名的去中心化稳定币 DAI，DAI 虽然有超额的 ETH 作为抵押品，但并不是不存在 ETH 突然暴跌、CDP 来不及清算的可能性，那这种风险谁来承担呢？就是 MKR 的持有者。在极端情形中，合约有可能增发 MKR 来补充 DAI 的抵押品，进而维持其价格。在 MakerDAO 的治理选择中，无论是增加稳定费率也好，增加抵押品种类也好，其实都是确定 MKR 的风险程度程度并要求一个合适的价格。

MakerDAO 确实可以给大家很多启发：**首先，他们做了一个可以自动化的合约（金融的、同质的），其次他们确定了一个风险因素并让某种资产来承担，最后这种资产的所有者还有治理权限，给整个系统开放新的可能性**。这个模式其实蛮值得学习的。

（二）代币与自组织

另一种我们经常听到的新型组织时间就是所谓的 “自组织”，核心的向往是说可以通过自动发放的代币来激励参与者，让这些组织成员自发地努力做事，无需明确的强制性纪律执行方，而这个过程也会自发地产生一定的成果。

虽然思路上各有侧重，但在实践上却有这么几个共同点。

1）都发行了代币，而且该代币在该项目未来的生态中会具备一定的功能。目的在于使社区成员的利益与项目的长期利益一致。

2）受激励者的工作往往并不是简单的、易于验证的工作。所以代币发放也很难完全用机器（合约）来完成。比如翻译，翻译工作不能只看数量不看质量呀。

至少就我观察到的，迄今为止，没有出现把这个模式做的特别成功的（即真的达到了发行方想要的那样”百花齐放“）。那么我们不禁要问，到底哪里出了问题？是激励机制不起作用，还是太容易被人薅羊毛了？

BES Lab 的 Jade 女士将这种代币实践的困境总结为一对悖论：如果此类行为可以被激励，那代币激励显然比不上 BTC、ETH、RMB，因此效果非常弱；如果此类行为压根不能被货币激励，那么代币又怎么会起作用呢？<3>

我非常佩服 Jade，她是这个行业里顶尖的思考者，也很有勇气戳穿幻象，指出国王其实没穿衣服。但我在此希望表达对她的小小反对，我认为代币的货币性不足不能完全解释这类实践失败的理由。

（三）为什么代币实验会失败？

（1）货币性与代币激励

为什么这些实验大多不能长久？为什么一开始大家还热火朝天，后来慢慢地就激励不动了？

最显而易见原因是这些代币在当前并没有用途，它构成一种激励纯粹是因为大家的预期或者对项目方的信任，随着这种信任的改变，激励效果也会改变。而在大多数情形中，由于这些代币在未来生态中到底能不能捕获价值还是一个问题，大家认识到了以后，激励效果也就逐渐衰减。

其次，就算他们具备用途，也不适合作为货币用于支付工资。想想看，家用化工企业的工人会接受洗衣粉作为工资吗？他们也许愿意把它当福利，但很难拿它当工资。究其原因，接受一种物，或者说判质费用比较高的物品作为支付手段，会使双方的合约变成较为原始的那种物物交换，双方都必须付出高昂费用来判断交易对手方的商品质量，这注定是一种摩擦力很大的交易形式。

这就是阿尔钦的洞见：为什么会出现货币？为了降低交易中的判质费用。钻石为什么没有成为货币？在金刚石技术出现之前，钻石在物理上也稀缺的呀。但是，钻石在市场上交易的时候，大小、色泽、瑕疵、切工，四个方面都要分别判定并定价，给你一颗钻石，你要花很多钱才能发现它真正的价格，你当然不愿意接受钻石。这就是为什么有人认为货币的用途越少越好，其实不是用途的问题，而是判质费用越低越好，只不过用途多了判质费用难免上升。

（至于那种有点像剩余索取权限的代币，就更不能用这种持续增发的形式来发放了。）

（2）企业家

另一个有趣的问题在于，如果所谓的自组织的理想，就是设计出一个可在链上自动执行的合约，自动评估各资源投入者的工作，然后给出报酬，这个过程除非引入 DAO，否则是没有企业家的角色的，因为都自动执行的合约。

但这样就很奇怪了，你能想象一个没有企业家的企业吗？企业家并不是光出钱而已，他们判断市场需求、确定要素组合、评估工作质量，最终给付报酬和获取收益。其中相当关键的一面在于评估工作质量，因为不同的成果在市场上会得到不同的价格，如果不好好评估工作质量就发工资，等于是鼓励生产低质量商品，结果就是入不敷出和资本损耗。

因此，当参与者的工作质量千差万别，难以有清晰的、可供机器执行的标准来评判其质量的话，动用合约来发放代币激励造成的结果一定都是低质量的产出，也就是我们所谓的羊毛党。这就是大多数 ” 自组织 “ 的命运。

综合上述两点，我会这样总结此类代币实践的困境：它无法成为一家企业，因为没有安排企业家，但他也无法成为一个双边市场，因为市场需要货币，而代币经济体的 Utility Token 并不能满足这种需要，只会增加摩擦力。所以，组织是有可能的，” 自组织 “ 则很难。

接下来我们要进入更为复杂的问题，什么是组织，为什么组织会有不同的形态，技术又会如何改变组织？

三. 交易费用与合约结构

我认为，组织实际上就是被合约联系起来的人类群体。虽然合约在实际上受到法律、传统风俗和道德的多重约束，使合约这一概念也多多少少有点像黑匣子，但不可否认，结成组织多多少少要基于参与者的自愿缔约。那么，所谓的组织结构，也就是合约的结构。对组织的研究，如果要有一个理论基础，我认为还是要到合约经济学或者说产权经济学中寻找，当然，解释有程度的区别，经济学的解释往往止步于合约的形态，而对更个体现象的解释就只能求助于其它学科了。

那么问题来了，为什么会有不同类型的合约呢？

首先可以确定的是，合约结构不是被双方的经济投入（数量）所决定的，不同的经济投入只是要求不同的回报，回报可以在价格中体现出来，**投入的多少无疑只决定了他们所得的市场价格是多少，而不能决定要他们要用什么样的合约来协调彼此的行为**。

因此，我们要转向交易中的一个非常重要的现象，就是在交易过程中，**交易双方往往都要付出一部分费用，这部分费用与他们准备投入多少和投入了多少资源无关，而且也没有被任何一方得到**。比如，为了做交易我们得找到交易对象，要么上淘宝，要么走路去超市。这部分费用没有被交易中的任何一方得到，却是为了达成交易所必须付出的。这部分费用就是所谓的 ” 交易费用 “。

这部分交易费用，不论如何，没有被交易双方所得到，因此，这正是双方都希望减少的费用。这就是为什么会存在不同类型的合约——因为用不同的合约达成交易时，付出的交易费用是不一样的。（有兴趣的读者可以找张五常教授的《佃农理论》的第二章来看看，教授在里面证明了如果不考虑交易费用，固定租金与分成租金在资源配置上没有差别。）

（一）交易费用分类

从概念上说，交易费用的分类方法有任意多种，也是学界吵过的话题。但在我看来，运用交易费用这个概念是为了研究合约，因此，在逻辑上只要保证没有遗漏即可，此外，应当尽可能清晰和直接。

因此我自己习惯的分类方法是这样的：

- 找寻交易对象的费用；
- 订立合约的费用；
- 在合约签订后监督对方如约执行的费用。

此种分类方法是根据时间先后顺序划分的。另有一种分类方法与上述三种费用具有不完全对应的关系，但在概念上更为清晰明了：信息费用（议价费用）、度量费用以及判质费用。因为在交易中，我们都免不了要到市场上去获取信息作为讨价还价的凭据，同时，要根据一定的指标来确定交易对手方给我们提供的商品数量，而指标的选择也会影响到交易的形式和便利性，最后，我们还要付出一定的费用来确定交易对手方给我们提供的商品的质量。

正如上文所说，给交易费用分类，无非是希望它在概念上更为清晰，在分析问题上更为便利。

（二）合约类型

生活中我们会遇到很多不同的现象和不同的合约。举个简单的例子，各位都知道工资有计件工资与计时工资的区别。那为什么有些工作（比如工厂工作）可以采用计件工资，而有些工种（办公室工作）只能采取计时工资呢？

因为办公室工作的内容往往比较多样，成果也千差万别。在这种情况下，如果采取计件工资，虽然度量的费用比较低，但相应地监督费用会变得更高（一件一件工作要看得仔细），甚至高不可攀；而且这些工作比较琐碎，难以一项一项定价，议价费用因此会变得很高。这些困难使得企业宁可采用计时工资，承担更高的度量费用，但务求节约议价费用。同理，计时工资之外，我们还会看到各种奖金和福利安排，比如全勤奖、绩效考核奖，等等，这些奖励措施无疑增加了度量的费用，但可以减少监督费用（不用上司成天盯着你工作）。

同理，在工厂的工作，由于劳动成果是标准化的，或比较容易判定出质量，工厂之外就是一个庞大的市场，不间断流动着各种标准化产品的价格，因此采用计件工资是议价费用、度量费用皆低。在香港成衣市场发达的时候，衬衫的袖子都有明确价格。

除了劳动力市场，在土地和品牌经营上，常见两种租金合约，一种是固定租金，用了资源就要付一个固定的价钱，另一种是分成租金，使用资源后对与剩余无关的经济产出收取一定比例作为租金（在佃农制度中，是对农产品产量收取分成）。连锁经营的服务业往往都是用分成合约，其实就是把品牌当成一片土地，让门店经营者去经营和使用，在这种情况下，门店经营者直接面对消费者，掌握的信息比总部多，总部为了获得这些信息作为后续租约的参考，同时约束门店经营者（他们的行为可以直接影响到品牌形象），往往会采用分成合约。

完全的分成与完全的固定租金之间是一条光谱，光谱上可能存在无数种合约，具体会采用哪种合约，端看交易费用而定。

（三）交易费用的变动与合约结构转变

正如上文所述，在合约经济学中，我们认为具体的交易费用决定了具体我们会采用怎样的合约，而交易费用的边际变动也就决定了合约会往哪个方向变动。只要我们可以独立地辨识出交易费用会如何变动，后续的经济学推论易如反掌。

举个例子，网购。各位想想网络购物与线下购物的交易费用是如何分布的？使用淘宝，只要搜索一下就有成千上万的商品陈列在你眼前，所以信息费用非常低；但缺点就在于你看不见、摸不着，而且下单之后指不定卖家会不会给你发次货，因此监督费用比较高。如果这种监督的费用太高的话，会让大家很难接受这种合约。实际上这也就是电子商务早期面临的主要问题。后来淘宝发明了一个办法，就解决了这个问题，那就是你下单之后是把钱转给支付宝，确认收货之后再让支付宝把钱打给卖家，因为卖家知道你可以拒收，你满意了他才能真的拿到钱，因此就不敢给你发残次品，这样就降低了监督费用，让网购真正流行起来。

同样的理由可以解释为什么网络购物中最早流行起来的是书和数码产品，因为这种产品都是标准化的，监督费用比较小（尤其是数码产品，线下购物的信息费用会比较高）。同理，天猫和京东后来的崛起也可以部分归为这个原因，这种自营商品的监督费用也会比较低，因为平台违约的成本相对比较高。

有了这些观念，我们就可以轻松理解第二节中讲到的经济学原理（货币和企业家），并试探性地思考技术如何改变合约、改变组织。

四. 技术与组织结构杂谈

（一）公司制与工资合约

各位有没有想过一个问题，现在我们看到的公司制，究竟有多久的历史了？

根据维基百科，股份有限公司的文献记载最早可以追溯到 1250 年的法国，就算我们说晚一点，那也是 1600 年的英国，东印度公司 <4>。而合伙制的历史更为悠久，据说可以追溯到古罗马，哪怕我们说晚一点，也是十世纪时候的意大利 <5>，那时候的 “commenda” 常被出海从事贸易的人用来搭伙凑钱（在这种合伙制中要有一个无限责任承担人（一般合伙人），TA 对企业债务的承担不以他的出资额为限，相反是以他的全部财产为限；而有限合伙人则只以出资额为限承担企业债务；有限合伙人的关系是可以买卖的）。

撇开一些极为技术性的特征，你会发现我们最熟悉的那个特征：出资人根据自己所提供的资源在公司成立时候占总资源的比重获得股息作为回报，其实很早就出现了。虽然并不完全，但这种类似于 “股权融资” 的概念，少说也出现 1000 年了。

那各位想过没有，我们现在熟悉的工资合约，又有多久的历史了？

按照我们在合约经济学中学到的东西，计件工资的合约很可能不超过 500 年，而计时工资的历史可能比这个数字更大，但不会相差太远。

为什么这么说呢？

关于计件工资。首先，在生产性机器出现以前，根本就没有很好的手段可以让人的劳动产品标准化，既然不能标准化，自然也就谈不上统一的定价。换言之，使用计件工资合约会使企业的监督费用非常高，要花很大力气才能保证劳动者产品的质量处在某个区间。但机器可以非常高效地保证产品的质量会稳定在一个区间，因此大大降低了这部分监督费用。此外，运输技术的发展也是相当关键的一个因素。因为运输技术的发达使得产业出现了地理上的集聚，然后便出现了劳动产品价格信息的集聚，这种集聚降低了计件工资的议价费用。

关于计时工资。采用计时工资的前提是时间本身很容易度量。如果连计时都是障碍重重，又谈何计时工资呢。而欧洲是在 14 世纪才出现擒纵器，钟表业是在 15 世纪才开始发展 <6>。没有这些技术，度量工作量的费用就不可能真正降下来，计件工资也就不可能出现了。

我希望在此说明的含义有些复杂：（1）技术毫无疑问会影响组织形态，因为它会影响交易费用并进一步影响合约形式；但这种关系并不像我们以为的那么简单，比如，**生产性机械的采用不仅提高了生产能力，让我们可以把工厂做的更大，同时还促成了计件工资的出现**，让愿意承担风险的和不愿意承担风险的人可以各得其所；（2）无**论这些技术怎么进步，它都没有改变 “风险承担” 的基本结构，而只是让不承担风险者的资源投入可以得到更精确的度量**，再换句话来说就是让收益的组成部分变得更加清晰、让非企业家才能的投入从企业家的实际工作中进一步剥离出去。

在 1000 年前，一位企业家想干点事情，他必须既当劳动者，又提供技术知识，还得自己干法务，他得到的收入中，到底哪一部分属于劳动报酬，哪一部分属于知识报酬，哪一部分属于企业家才能，分不清楚。但随着技术的发展，我们可以分得越来越清楚了。

（二）公正服务的市场化

最后，我在这边提供一个幻想。

回到前面的推论，判断技术进步对合约结构的影响，主要看技术对交易费用的影响。那么智能合约到底改变了什么呢？

它降低了缔约费用，你我素昧平生，但是现场发一个交易做一个 2/3 的多签名合约，这就算是缔约了，非常简单。 合约里有没钱都好说，谈妥了我们各自再打钱进去就是。但与此同时，监督费用会升高，因为是数字合约，很难对对方形成实质上的约束。

现在我们要想的是，有没有什么方式可以降低监督费用？有没有什么活动是对缔约费用比较敏感的？

我自己想到的事情是，这种缔约费用的降低会促成仲裁服务的流行并造成 “公正服务的市场化”。因为缔约极其简单，当我们无法互信的时候，可以容易地拉一个第三方仲裁机构进来，在有所分歧的时候通过第三方机构来解决争议（因此，这些第三方就是在提供 “公正” 这种服务，与我们对司法机关的期待是一样的）。有人会疑惑，那么对方与第三方仲裁机构相勾结怎么办？他们的确可以勾结，但这种没有准入的情形会造成仲裁服务方之间的相互竞争，市场会惩罚那些玩忽职守的仲裁者，迫使市场参与者提高自己的服务质量。

不是所有信任都要通过技术来建立，许多信任都是靠市场竞争来建立的。这就是我能想象到最大胆的事。

注 1：https://ethfans.org/posts/the-idea-of-smart-contract-nick-szabo

注 2：https://ethfans.org/posts/visions-of-ether-part-1

注 3：https://mp.weixin.qq.com/s?__biz=MzU0NjkwMzA1NQ==&mid=2247483689&idx=1&sn=5686610b4e2442423a5c82080e3f0078&chksm=fb57c449cc204d5f55cb0400295712bec15e21592d96d34e6211942cd3bb537aad2427676e2f&mpshare=1&scene=1&srcid=0516RfgmtaoOrX4tERDoG2cU&key=45382ee80ea507806316b6508b5bbe40b85eab48bdf91d01831eded73848ca6426e7f5e6242c4bf3862e34d93bbd04469e3b7dcb1e92e0cad2e66a43054a0ea75d97ca86293564487aa3742ce24cf164&ascene=1&uin=Mjc4MjA1NTcyNA%3D%3D&devicetype=Windows+10&version=62060739&lang=zh_CN&pass_ticket=t5crhNkJ0L1E3U3g%2BN3k%2FQbOVFuII1Af7huE%2FRLo91AYtZSYUB2SJCdSbVptZlEW

注 4：https://zh.wikipedia.org/wiki/%E8%82%A1%E4%BB%BD%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8

注 5：https://zh.wikipedia.org/wiki/%E6%9C%89%E9%99%90%E5%90%88%E4%BC%99

注 6：https://zh.wikipedia.org/wiki/%E6%99%82%E9%90%98