实现加密世界的初心：技术与机制双轮驱动与防御新体系

撰文：Brook编译：Elaine&Sissi & Leia, TEAO

加密世界的乱象与创新乏力，让人们不禁质疑：我们是否正在实质性迈向理想的未来？《协议革命与 DigiLaw 工程》前言以系统化视角探讨加密世界的本质、发展中的卡点以及未来建设的无限可能，为理解这个新星球的真实面目提供了重要思考。

如何实现加密世界的初心，维护好安全且道德的发展环境？尽管加密世界正在逐步向前迈进，但由于其仍 处于发展的初期阶段，很多秩序还在逐步建立中，新进者贸然闯入，往往很容易落得「人财两空」的下场。当现有的基础设施不能很好地支持加密世界实现去中心化的初心时，那么我们是否能够协同传统监管机构和社区大众设立一套机制，可以自发性监测并压缩作恶空 间，构筑起加密世界的「免疫系统」，全方位净化加密世界发展环境？同时，是否也可以让身陷其中的普通人获得全局视角，更好地看清加密世界发展的全貌？



## 技术与机制：双轮驱动加密世界的未来

要实现加密世界的初心，打破现有困境，尤其是瓦解「作恶」的根源，必须依赖「技术」和「机制」双轮驱动。

「We are no longer early to crypto.」Vitalik 曾表示，以太坊和 Layer2 解决方案的快速发展，尤其是在费用降低、交易速度提升和安全性增强方面的进步，标志着加密正在迈向更加成熟的阶段。确实，自比特币诞生后的十几年里，以 coding 为主的技术 Builder 们为加密世界的持续发展做出了巨大的贡献。技术无疑是加密世界开拓「无尽未来」的核心引擎。

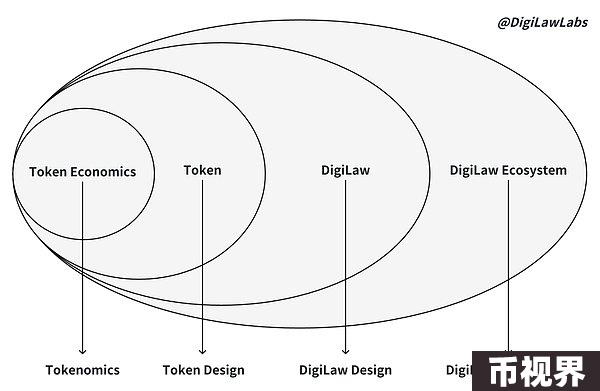
然而，「We are early to crypto being usable」。为什么加密迟迟未能实现大规模采用？除了友好性和易用性仍需改进，还有一个重要原因是，我们在「面向 DigiLaw 生态系统的机制设计与演进」的研究和应用上远远滞后于加密技术的发展。技术新开辟的广阔疆域上究竟会长出「鲜花」还是结下「恶果」，关键在于是否有足够精妙的机制来有效引导与规范。而目前加密世界的种种乱象一定程度上反映了我们的机制设计仍不够精妙完善，为作恶留下了大量的可乘之机，这无疑是加密普及和采用的一大关键障碍。

要尽快迈向下一个十亿用户，我们亟需提升 DigiLaw 生态系统的整体道德与安全水平。然而，这并非易事。

## DigiLaw 生态系统：全新「物种」

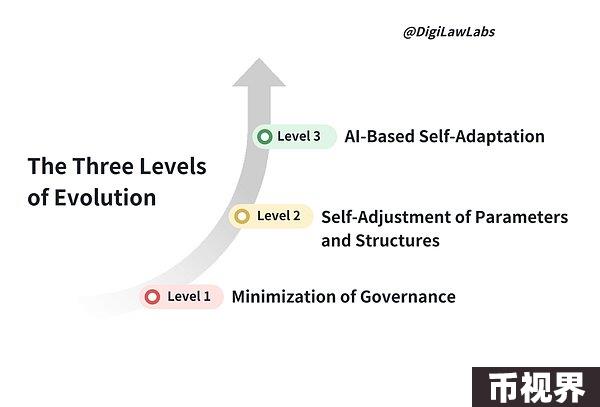
「DigiLaw 生态系统」是人类历史上前所未有的全新「物种」。 DigiLaw，作为一组完成特定目标的规则集合体，能够使参与者在这些规则的框架内协作或博弈，从而构建出一个开放且动态自演化的复杂系统 ( 本书称之为「DigiLaw 生态系统」)。与芯片、飞机、桥梁等「死」( Mechanistic ) 的复杂工程系统不同，DigiLaw 生态系统更接近于自然生态系统、全球气候、免疫系统等「活」 (Adaptive) 的复杂自适应系统，它不光包含微观层面的交互，还包含从微观到宏观的涌现。

需要说明的是，「Mechanistic」 和 「Adaptive」并非截然对立的两种状态，它们处于同一光谱的两端。整体上，加密协议生态系统更偏向「Adaptive」 状态，但目前的机制研究尚不足以支持一个 「Completely Adaptive」系统的构建与可持续运行。



这类「活系统」的设计与演进是一个全新的世界级的挑战。仅代币经济的设计就涉及逆向博弈、激励相容等诺奖级难题，更何况这类问题的解决应该上升到代币设计、DigiLaw 设计，乃至整个 DigiLaw 生态系统的设计上来 ( 关系如上图 )。从某些维度上讲，其难度不亚于先进的芯片设计、火箭和飞机设计、汽车设计、摩天大楼的设计等，所以不能只依赖诞生于这类「死」系统的 「Model-Based System Engineering(MBSE)」方法，需要进一步升级至适用于存在涌现现象的活系统的「Agent-Based System Engineering(ABSE)」方法，来对 DigiLaw 生态系统全生命周期各个层次的行为进行理解、设计与建模仿真。

此外 ，「活系统」不仅仅是设计上的难题，其演进也面临巨大挑战。如 何实现人工治理最小化？是否能构建出一套完善的自我调节体系，可以根据外部环境的变化和内部运行状况进行动态的参数和机制调整？甚至未来是否能借助强大的 AI 来实现「活」系统的自适应？

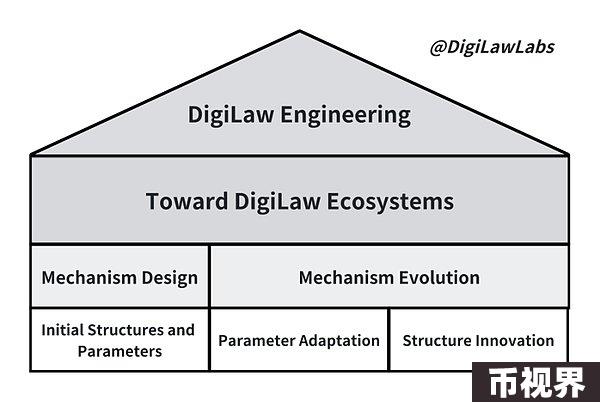


## DigiLaw 工程师：新型人才的崛起

从以太坊、AAVE、Compound 等成功穿越牛熊周期的协议中，我们不难发现，这些协议的一大共性是都在机制设计与演进上投入了大量的时间与精力。

与技术安全审计一样，如何判断一个项目是否值得信任，除了看它在技术层面是否做了合规的代码安全审计外，我们还要关注是否有 DigiLaw 工程师参与设计和不断优化其生态系统的机制结构与参数调整。如果有，这至少能证明项目方在道德和可持续性方面足够重视，尊重每一位参与者的财产安全，并从生态系统运作的规律出发，精心设计其机制。

( 注：TokenEngineering 领域常将这类人才成 为「代币工程师」，这个词确实特色、新颖且指向性明确。我也一直在「代币工程师」和「DigiLaw 工程师」之间摇摆。但是举例来讲，AAVE、Compound 等协议作为一个高度自动化的生态系统，其经济机制的参数运维（如核心借贷业务中质押率、清算比例等关键参数的调整）等高度影响着整个加密协议生态系统的安全性与效能。然而这些问题与其原生代币无关，却是今天 Compound 协议稳健高效向上发展的关键杠杆点。相较于「代币」，「DigiLaw」是更为全面的命题，我担心「代币工程师」的叫法会让人产生误解，误以为这类人才的作用仅仅聚焦在「代币」上。而「DigiLaw 工程师」则更准确地反映了他们的工作本质——设计和进化的是数字世界中的透明且不可篡改的法则。因此，我选择 「DigiLaw 工程师」这一称谓，作为「代币工程师」的 2.0 版本。）



然而，现如今加密世界对 DigiLaw 工程师的重视远远不够。尽管 TokenEngineeringCommons 等组织一直在持续推动代币工程领域的发展，且已取得显著的成果。但相对来讲，「TokenEngineering」这一理念和方法仍未大规模普及和应用。许多项目方、投资人等仍停留在「Tokenomics」层面，甚至对 「TokenEngineering」 知之甚少。这一定程度上反映出，「We are still VERY early」in DigiLaw 生态系统机制设计与演进的研究上，不光表现在理论和实践的缺失，更表现在专业人才的缺失。

加密世界想要进一步突破安全和效能上的卡点，还需进一步挖掘 DigiLaw 工程师的潜力和价值。

技术是未知领域的开拓者，机制是广袤疆土的守护者。 没有二者的协同驱动，我们很难打造出平衡、健壮且反脆弱的 DigiLaw 生态系统。终极的理想状态是，在没有任何人为干预的情况下，「技术」和「机制」的发展足以支撑起 DigiLaw 生态系统的内生性的自我安全防御与自动效能优化。

然而，技术的迭代发展和 DigiLaw 工程师人才的培养不是一蹴而就的。当双轮还不能完全支撑起加密世界的初心时，我们还需要「外源性人工防御」的协同发力，共同守卫加密世界的道德与安全。



## 防御新体系：以技术与机制共建加密世界的道德与安全

加密世界亟需建立起一套对抗风险的「防御新体系」。很大概率上，加密世界在未来的一段时间都将处于「中心化」与「去中心化」的混合状态。这里的「混合」有两层含义：一是DigiLaw 自身的「去中心化」是一个渐进的过程；二是 DigiLaw 所在的端到端全环节的「去中心化」程度也各不相同，例如尽管有些 DeFi 协议本身高度去中心化，但在实现过程中仍需依赖于中心化的基础设施服务，同时搭建在协议之上的 app 也可能是中心化的。

在这样的混合系统中，防御体系也应当是可组合的。最终的理想状态是 -- 社区大众自下而上地完成「去中心化」部分的自监管 (self-governance)，传统机构自上而下完成「中心化」部分的监管 (regulation)。目前，政府等传统机构的监管正在加速推进，这属于外部人工防御。虽然这种监管确实能压缩某些作恶空间，但有可能会限制「去中心化」的发展。而借助技术和工具，构建基于社区大众的 DigiLaw 自我监管体系，可以由内而外、自下而上地抑制「恶」与系统性风险的诞生，这一内部人工防御机制可以更柔性地解决加密世界面临的「作恶」难题，同时也与加密世界通过去中心化手段实现初心的路径是一致的。



## 结语：技术、机制与防御体系的协同驱动

所以，想要实现加密世界的初心，建立起安全且道德的数字自然环境，在现阶段看来，至少需要技术和机制的双轮协同驱动，外加可组合的防御新体系，这三者不一定是详尽的，但却是加密世界发展突破瓶颈的关键。