作者： Kokiin原文： Shuming hao123 @ QQ.com [xy 002] [xy 001] TL；DR

• Web3是用于调整和交换的新经济基础设施。 那是从根本的产权制度开始的将对复杂制度的信任从单一组织转移到分布式节点和可验证代码。
由于具有独特的经济特点，可以补充，有时还与现有机制直接竞争。

•制度经济学是经济学的子集，用经济学的方法研究制度在社会经济背景下的作用，基本理论工具是交易费用理论和产权理论。

•Token是一个产权管理工具，可以表示现有的数字或物理资产、或对他人资产的访问权限。
链上的Token可以实现密码学产权保护、竞争性产权创新和高效的产权流通。

•智能合约是一种通过代码保证自动实施的合同。 随着产权制度的细化和完善，经济活动的许多组成部分包括在生产和交易中重复机械部分、计算规则和秩序，都有可能被机器和智能合约所取代。

为什么要考虑Web3的基础逻辑

现在的Web3/Crypto充满了各种各样的新鲜名词让这个原本就模糊不清的新行业更加令人费解。 来自技术/应用的共识算法、Rollup、零知识证明、DeFi、NFT、GameFi、DAO、交叉链桥、预言机、DID、SBT、概念上的密码朋友圈、主权个人、去中心化、抗检能力、无授权、可组合性、创作者经济、分布式治理、价值互联网、永久存储、Code is Law、X to Earn，听之任之再加上各种管制禁令、意识形态、诈骗、旁门左道、效率低下、违背直觉的应用场景层出不穷，让人摸不着头脑。

爱它的人说它是未来，是不亚于互联网的基础性技术变革，恨它的人说它是概念的积累。是风险投资公司制造的资本泡沫，是自由放任主义者的自娱自乐。

集中于细节时，难以看到整体情况。 互联网刚刚被小部分极客采用，谁也不能指望未来的发展，充满了各种创新、协议和产品10年后一百不剩。 搜索引擎这样的爬虫算法、新闻门户这样的应用是浏览器外壳报纸、网络效应这样的观念如何影响社交媒体等问题可能很重要，但并不是互联网最核心的逻辑。 但只要意识到互联网“前所未有地降低了信息流通成本”的基础性逻辑，它将如何深刻改变社会，搜索引擎、社交媒体、网络购物/支付、智能手机、好的。

技术的进步更多的是堆栈而不是跳跃，所以预测未来是极其困难的，特别是政策和

技术都是极其初期的现在。 今天的Web3还非常初期，我们现在讨论的产品和服务、商业模式、令牌模式大部分都会死于泡沫的破灭。 于是，我决定，本文没有涉及ZK-Rollup的电路设计、GameFi是Tokenomics的加盖游戏还是可组合性如何影响DeFi等，只讨论最核心的问题。 Web3的创新之处在哪里？ 如何改变世界？

Web3是什么

Web3是由区块链或数字资产相关技术构建的Web体系。
定义是为了认识结构和机制，该定义十分完善，但同样令人困惑。 目前，Web3最常见的描述是“Web1对大多数用户来说是只读的，Web2允许用户读写，Web3通过区块链赋予用户读写的权限。 “

但是，能读写的是人与内容的相互关系而且，本质是社会契约关系。 前者是信息，后者是资产，两者处理的维度不同，所以将Web3仅仅看作是Web2的继续是一种视点的错位。 为什么人们不放着又便宜又快的Web2使用呢如何使用消耗能量、昂贵、缓慢且复杂的Web3？

一个创新被采用只有一个原因，既能满足人的新需求，又能更好地满足旧需求。 复杂的助记码、高额的手续费、不时出现故障的公链、日常被黑客用作提款机的协议、忍受被钓鱼网站偷钱包的风险，都是为了把可以打手机的事情放到区块链上重新做否则，很难解释为什么还买了几百万张丑陋的照片，每个人都可以右击保存。

让我们从白皮书的标题开始。
比特币、点对点电子现金系统坊新一代智能合约和去中心化APP应用平台。
本文介绍了Web3的核心创新点在于白皮书的标题。 “Token”和“智能联络”。
要从制度经济学的角度进行说明，与其说Web3是“蒸汽机”这样的技术革新类似于“资本主义”的制度创新。

制度与制度经济学

制度经济学是经济学的子集，与政治学、社会学或历史学交叉，用经济学的方法研究制度在社会经济背景中的作用。
个人满足自己愿望的能力有限，甚至没有人在地球上独自生产一支铅笔。 这有赖于智利的石墨工人、加拿大的伐木工人、台湾的粘合剂制造商、德国的生产线制造商、中国的商人，以及千百万陌生人的共同贡献。 在专业化劳动分工精妙复杂的现代社会，人需要与难以计数的陌生人和组织进行交易和合作。
人类的相互交流，特别是经济生活的相互交流，依赖于信任。 信任必须以秩序为基础，遵守该秩序将依赖于禁止不可预见行为和机会主义行为的各种规则。
这些规则称为“制度”。

为什么人类社会需要制度？ 主要原因可以归结为人的有限理性(主观智力资源不足)、客观环境的不确定性、人的机会主义倾向。 制度使人的行为具有预见性，在大规模的人际合作中减少协调活动的成本，有效利用资源。 我们之所以能把兢兢业业挣来的钱放心交给下一秒就会走神的银行出纳员，把自己的身体放心交给陌生的医生，就是因为他们受到制度的束缚。
回过神来，人类社会理所当然的事情太多了，实际上挂在了制度制造的信任网上。

制度是进化而来的，与政策不同。 当人们发现有更有效率的制度代替现有的制度时，制度变迁的可能性就会显现出来。 制度规范人与人之间的关系，而人与人之间的关系是社会关系之间进行的博弈，利益的不一致几乎出现在一切人类活动中，利益相关者的最终总目的是通过自己的选择实现对自己有利的结局。 经济学家在把经济过程当作博弈过程的同时，不仅把制度当成博弈的规则，而且把它当成博弈的结果(均衡)。 只要人们发生反复的交易和其他经济关系，通过阶段性的进化和人为的有意识的设计就会产生规则。 时间一拖再拖，历史上一切被称为革命、改革、复活、前进、后退的内容，其中最重要的实质就是制度的演化。

比较法学、政治学、伦理学、文化学及社会学，甚至人类学制度经济学对制度的关注程度和观点不同。 诺思将制度定义为社会的游戏规则。 制度是人们结成的各种经济、社会、政治等组织和体制，决定着一切社会经济活动和各种经济关系开展的框架因此，各社会学科与制度有着内在的联系，是社会科学的共有范畴。

人类社会的制度是多种多样的，从宪法到社会礼仪、信号的和谐方式，不同的制度有不同的重要性和影响。
制度经济学关注对人类经济影响最大的制度的创造和发展。
人的理性选择创造和改变产权结构、法律、契约、政府形式、规制等制度。 这些制度和组织提供激励或建立成本和收益，最终这些激励或成本与收益的关系在一定时期内支配经济活动和经济增长。

交易是人类经济活动的基本单位，也是制度经济学的基本分析单位。
制度经济学的基本理论工具是交易费用理论和产权理论。

-交易费用范式构成制度经济学的理论框架，如果没有交易费用，无论生产和交换如何安排，资源的使用都是一样的。 交易成本从根本上影响市场上生产什么，发生什么样的交换什么样的组织能够生存，什么样的游戏规则能够持续；

-交易的前提是产权，不能谈无产权交易。
交易与交换不同，不是商品的买卖，而是权利的买卖。 产权制度是经济运行的基本基础有什么样的产权制度就有什么样的组织、技术、效率；

产权方法与交易成本方法存在差异，前者需要分析个人诱因，后者将个人纳入更广阔的机构框架例如，允许将公司作为有组织的尸体进行分析。

a .产权

产权是财产所有权或产权的简称，强调财产所有者对财产拥有的最终控制权。 当今世界所有国家商业使用的法律都是从罗马法派生出来的，罗马法中财产权概念的核心是控制权。 铅笔这样最简单的商品，离不开权利和商品本身，是土地、森林、企业、知识、思想、金融产品等复杂的商品支配和享受它的权利不能通过简单的物品买卖来处理。 商品和资源的交易只有在明确界定产权的情况下才能顺利进行，市场价格机制才能发挥作用，资源得到有效配置。

私募股权、共有产权和国有产权基本涵盖产权范围。
性质不同的资源应当以不同的产权形式合作。
产权既是利益关系，也是责任关系，应对激励和约束。
适当定义的财产权限制人们使用资产的方式鼓励人们将资产的价值最大化。

财产权作为控制权派生了许多其他权利，称为权利束。 包括占有权、使用权、收益权、处置权在内的处置权分为交易权、继承权、赠与权等。 产权分割性提高了资产的有用性，使不同需求和知识的人能够投入到能够发现自己资产的最有价值的用途中。 例如，有创业才能但没有资产的人，比较容易获得他人的资产为了使双方的生产总值最大化而重要的项目和基础设施所需的巨额资本可以通过股份制筹集等。 从发展趋势看，随着生产社会化程度的提高，从产权整合到分解是社会分工发展在行使产权功能中的具体体现。

基于产权制度，产生了企业制度、市场制度、金融制度、法律制度、政治制度等其他制度。 现代社会复杂的企业结构、金融市场等创新的基础是产权制度创新。
在制度变迁和制度创新中产权都是重要的变量。
这一点，经历过市场经济改革的中国应该有深刻的理解。

b .交易费用

交易费用是经济制度的运行费用，广义上包括制度的制定成本、实施成本、维护成本、变革成本。 现实中，制度或者说交易规则有很多种，每个制度都有交易成本。例如，产权制度的成本是指衡量、定义、维护和交换产权的成本。

交易费用是制度经济学的核心可以运用交易费用理论研究人类历史和现实上的各种制度安排。 在新古典经济学的完全竞争市场中，交易费用为零，私募股权健全。
亚当史密斯的“无形之手”可以使资源配置达到帕累托最优、制度、财产权、法律

、规范等可有可无。 在存在摩擦的现实经济生活中，许多制度都是为了降低成本而建立的，或者使以前由于高交易成本而无法实现的事情成为可能。

交易费用的计量是理论的关键和难点，包括两个部分。 可通过市场衡量的成本，据一些估计，现代市场经济中的交易费用占纯国民生产总值的50%-60%，这一数字不包括建立新制度和机构的初始成本；获取信息、等待时间、贿赂、不完善的监管和实施造成的损失等难以衡量的成本。

具体来说，现实交易通过合同进行。 合同是当事人(两人以上)为了改善自己的经济状况(至少是合理的期望)在交易过程中确立的权利流动的关系。 任何交易总是在一定的合同关系中进行，现代经济学将所有市场交易无论是长期还是短期进行显性还是隐形，都是合同关系。
一位消费者购买火车票，消费者和铁路公司之间就有隐性合同。
消费者支付费用，铁路公司在规定时间内将消费者安全地送到目的地。

合同的基本功能是保持缔约国多方合作，在遵守承诺、承担责任的基础上谋求新的、更大的利益。 是合同制度的这一性质成千上万不同的、精细所有权结合为一个巨大所有权的同一所有权合理分离、分工合作，构成所有者-经营者-
使用者链上的不同环节。 在经济发展的漫长过程中，人们之间的交易行为不断扩大和发展，合同也越来越复杂。

从合同的角度看，具体交易的交易费用包括准备合同的成本(信息的收集)、达成合同的成本)、合同的监督和实施的成本。

来自产权的Token

高效的产权制度可以将产权从低效的人手转移到高效的人手里。 应用前文的交易费用理论，为了达到更有效率的产权制度，有必要降低产权的计量、定义、维护、交换的成本。

1.产权属性完善，产权属性越完善，产权制度就越有效率

2.产权界定越明确，这是市场机制有效运行的前提

3.产权有效保护、产权保护

4.产权交易成本低，这是产权顺利交易的基础

产权制度的每一步进步，都离不开这些创新。 专利、著作权所有权等无形资产的定

义使知识所有者能够从与人共享知识中获得物质利益所有权和经营权的分离导致现代股份制公司产生一个国家的法治化程度、市场化越高，市场就越有效率。
相比之下，空气所有权难以定义，有污染问题的市场失灵了。

Token是Web3的原子单位，由分散账簿共同管理。 Token起源于比特币，人类首次尝试在技术上取代货币制度，但明显宣告失败，目前比特币已成为数字黄金。
其失败是可以预见的。 因为货币制度是人类经济活动中最复杂最根本的制度。
但是，比特币为我们打开了新世界的大门。 我是Token。

在以太坊等公共基础设施上任何人都可以以非常低的成本部署Token。
截至2022年8月，CoinMarketCap列出了9000多项公开交易的Token。
这还只是Fungible Tokens的数量。 这些FT可以细分为从证券到效用、价值储藏、治理等多个类别，不同的权利对应着现实生活中的各种现有财产权。

Token的许多角色错综复杂、股票、债券、货币、礼品卡、积分、俱乐部会员、身份证、学历学位、机票等，似乎可以是任何形式的经济价值或权限(的链接版本)。
虽然新兴领域经常缺乏明确的定义但这并不意味着Token的许多作用是错误的，而是表现出了最抽象意义上表示价值的特性。 可以使用

token发布任何类型的资产和权限，包括新的资产类别。 相对于上述所有权概念，Token是一种所有权管理工具，可以表示对现有数字或物理资产或他人资产的访问权限。 如果你同意上面关于产权重要性的描述，你应该很容易就能理解这件事会产生多么大的影响。

但是产权管理为什么必须是Token呢？ 为什么必须放在区块链上呢？
支付宝(Alipay)的数字也是产权的证明，更有效率。
光发明概念是不够的，概念落地需要应用组合。 Token与链下产权比较核心优势是密码学产权保护、竞争产权创新和高效产权流通。 同时，基础性产权创新是一项复杂的经济活动，如合同创新(智能合约)、组织创新)的基础。

a .加密保护产权

只有在保护产权的背景下，人们才可能专门处理保护产权下的效率问题和操作问题。 现代社会复杂的产权机制，其基础性安排依赖于国家管理。 因为国家有相应的规则使其内部结构有序化拥有实施规则，与其他国家竞争的强制力。
这意味着，与其他组织相比，国家具有“暴力可能性”的优势。

暴力实质上也是一种资源，不仅包括军队、警察、监狱等暴力工具，还包括权威、特权、垄断权等无形资产。 这里的暴力没有任何贬义之色，制度源于个人相互制约

和演变，现行的产权保护逻辑就是如此，是因为国家承担这一职能更有效率。 国家暴力资源之所以能够更有效地使用，是因为它是针对暴力的暴力它的功能是生产和销售安全和公正这一确定性的社会产品。 如果我们处于无政府状态，所有人都必须抵制他人保护财产，国家暴力才能达到规模效应，防止“搭便车”问题。

但是，政府的保护功能是有限的。
政府的保护职能中，相当一部分是通过政府管制实现的。 政府的保护职能有偏好强调安全，倾向于牺牲竞争系统协调能力和控制能力的培养以繁荣为代价。
此外，信息和资本的全球化使得跨国交易与合作越来越频繁。 此时，单一国家的保护往往束手无策，地缘政治冲突加剧，贸易往来将进一步分裂。

区块链/Web3是与国家合作交换的新经济基础设施。 运用密码学保护产权安全，从根本产权入手，将对复杂制度的信任从单一组织转移到分布式节点和可验证代码。 由于具有独特的经济特点，可以补充，有时还与现有机制直接竞争。

b .竞争性产权创新

牵一发而动全身，历史上产权发展相当落后但是，每次进步都会产生很大的影响。 目前链条上的经济体系与实体经济关联不大，创新也很激进。 Web3通过技术手段保证了无准入、低门槛、开源和竞争性，基础性Token创新层出不穷。 “一日之币圈，一年之人”，本意是Token的下跌比传统资产要剧烈得多，表明在这种开放的竞争市场中，每天都有新的标准、协议和产品产生，并迅速被市场验证和淘汰。

例如产权定义上的将数字信息资产化的NFT，这种商品在没有被Token化之前不能自由交换。 虽然现在真正的应用只是看起来像玩具的虚拟形象和数字艺术但这是因为现有的ERC-721标准并没有真正放开数字信息产权权利捆绑，而是一味地寻求应用场景，去寻找，没有履约风险，只能沦落为见即所得的自豪经济。 但是，不断更新的新协议可分离NFT所有权和使用权的ERC-4907、不可转让的SBT一直在寻找真正的用例，很快就会在市场上优胜劣汰。
很多优秀的人才都在寻找用NFT创造更公平的创作者经济，更开放的游戏的方法。

属性定义上的DeFi协议的可组合性等。
结合后述的智能合约自动履约的特性，新的defi
APP合约可以安全地访问现有的defi APP，相当于现有的Token凭空添加了功能和权利可以从其他协议中获得流动性，提高资金使用效率。
还有令人眼花缭乱的Tokenomics设计，如

商业模式。 同一Token可以划分一系列的权利，只要拥有ETH就可以支付gas fee作为与以太坊生态相互作用的基础货币，可以享受以太坊生态繁荣带来的货币价值

上升，Merge后还可以在质押中享受红利。 Token的所有者是客户，也是所有者。将传统公司制下业务和分割的产权引入业务逻辑，以Token为纽带连接业务飞轮和金融飞轮，可以早期激励用户，加速网络效应到达临界点。
虽然有些模式被诟病为庞氏、螺旋型，但对这种商业模式的探索是有意义的。

从合约到智能合约

有了产权，下一步就是交易。 智能合同的本质是用代码保证自动实施的合同。 虽然名字是骗人的，但是智能合约其实并不聪明，很笨拙，一个bug就会导致巨额资金被攻击。 就像用自动售货机代替店员一样。用AMM取代中心化交易所，可以降低交易费用、信任成本和过程中人的风险，提高资产流通速度，加速价格发现。

算法真的能代替合同吗？ 回到交易费用理论，换句话说，算法能降低准备合同的成本(信息的收集)、达成合同的成本(协商、签订)、监督、实施的成本吗？ 理想是丰满的，通过简单的转账、超额抵押贷款、计算机/代码/机器/智能合约执行当然成本最低但是，人与人的经济活动如此复杂，目前的智能合约甚至连最基础的信用贷款合同、雇佣合同(Sadao的基础)都不能很好地实现。

智能协议的计算属性，适合处理完整的合同。 但在现实生活中由于涉及人力资本的合同对物质资本面临更高的测度成本，所以大多数合同都是不完全合同。 在完全合同理论中，合同条款规定在与合同行为相应的未来不可预测时间出现时、各合同当事人在不同情况下的权利和义务、风险分担情况、合同强制履行的方式以及合同能够达成的最终结果。 不完全契约理论下，个人有限理性、外在环境复杂性、不确定性、信息不对称与不完全性，合同当事人和仲裁者各方都知道合同条款不完善，同时需要调整不同的激励约束机制来弥补合同中的差距，纠正扭曲的合同条款，有效地适应意外干扰。

随着产权计量、定义、维护、交换成本的降低，合同不完全性在一定程度上可以得到缓解。 经济活动和合同有很多“可计算性”的组成部分，我们过去通过人力模拟实现计算。 但是随着技术的进步，当今计算机，特别是区块链智能合约的发展，更接近计算的本质。 储户和银行的访问协议要求通过银行店员协助检查复杂的支票。随着银行系统和银行卡继续降低监控合同的成本，取款机取代了银行店员。 同样，在雇主与员工的雇佣合同中，员工的生产成果需要雇主的主观评价，随着标准流水线的演变，工资取代了雇主的评价。

机器/电线合同优于人的地方在于准确高效。 当产权制度足够先进时无论是技术进步还是制度进步，计算系统都可以大大降低交易成本，提高精度，代替人成为合同的主导者。 从复杂的美团外卖配送系统可以看出趋势，巨大的系统连接骑手、商家和顾客，其中涉及多个复杂的合同的签订和履行。

-准备合同的成本：商家将商品信息呈现给平台供顾客选择

-达成合同的成本：顾客通过在线支付签订合同，骑手通过系统分配的、商家下单备货

-监督实施合同的成本：骑手/商家评估系统，系统自动计算骑手和商家收入并结算

合同由当事人自由选择，无需干预或胁迫包括是否签约的自由、选择签订合同一方的自由、决定合同内容的自由、选择合同方式的自由。
任何第三方都包括作为立法者和司法者的国家，必须尊重当事人的自由协议。 Web3的一大主张是打击Web2巨头，因为它们表面上提供了上述自由，但实质上合同解除成本极大。 区块链和智能契约的创造者是规则的创建者和维护者，本身不一定是参与者，参与者是世界上互不相识的人。 当越来越多的产权变得明确，被放在链条上的时候，请考虑一下在Web3上奔跑的、没有美团参与的外卖调度算法，或者更广义的合同系统。 将规则的制定和维持公开化、竞争化，将创造更公平、更有效率的规则减少平台权力野蛮生长“外卖员被困体系”的悲剧。

随着产权制度的细化和完善，包括经济活动中的许多组成部分，生产和交易中的机械部分，计算规则和秩序机器和智能合约可能会被取代。 金融系统产权发达，可计算性规则清晰，交易成本高，改造难度大，创造的经济效益大，这就不难解释为什么DeFi是Web3最初的爆炸性应用方向。

Web3的未来

逻辑链条顺理成章，将来我们可能会在链条下打交道、生产，但经济活动合同的制定、履行和监督都在链条上，大大降低交易摩擦，提高资源配置效率。 虽然听起来像网络朋友圈，但是思考未来总是很开心但是，很明显，现在的Web3并不是上述理想的Web3，而只是混沌的状态。 与网络的信息属性不同，由于天生的经济属性，赌徒骗子蜂拥而至，又由于其深刻的革命意义，说大话的空想家不惜传教。进步需要讲理想的现实主义者和讲现实的理想主义者，而不是只讲现实的现实主义者。Vitalik是最后一个人，不如意的现象我们都知道，但重点是解决问题我们有很多工作要做。 这还意味着蕴藏着大量的商业机会。

-加密创新，包括更好的共识算法、隐私保护、虚拟机、编程语言、分片、零知识证明和集中化存储

-用户体验、更好的开发者工具、使用方便的钱包、低廉的交易手续费、严格的资产安全保障等

-更准确、中心的预言机、更简单的法币Token变换等，与现实连接、更多实物资产所有权、现实契约链条运行、DID、SBT等

-监管干预，即使能长期与现有制度竞争，短期融合也是必由之路； [xy 002] [xy 001]-- . [xy 002] [xy 001]应用上的用Token表示的权利是什么？
应该设计什么样的交易规则来降低Token的交易成本？
没有编程背景的普通用户如何轻松地创建自己的智能合约？
建立在产权和合同之上的组织应该如何演变？ 路很远有很多值得探索的创新。

尾巴

在经济发展问题上，“技术决定论”和“制度决定论”是两个代表观点，新古典主义理论认为经济增长主要受要素投入和技术进步的影响，制度只是被动或延迟调整； 制度经济学家认为最根本的因素是制度的进步，高效的经济组织和恰当的激励制度安排，导致了西方世界的兴起和工业革命的爆发。 很难把

制度和技术分开那些关系实际上你中有我，我中有你。 这两者所谓的决定论最终必须与成本联系起来，对社会经济发展的绩效都可以用成本来分析。 把创新看作一个系统，技术创新和制度创新是两个不可缺少的组成部分只有组合起来才是互补和相互作用的。

互联网虽然信息技术的革新很多，但带来了更扁平、更没有边界的组织形态。
这篇文章一般是从制度的角度来考虑Web3的逻辑，但技术的进步也相当重要。 另外对于组织、合作、企业甚至国家理论等更为复杂的制度分析，由于篇幅所限，有机会稍后展开。
笔者并非制度经济学专家，只是煞费苦心，提供新的视角来思考Web3。