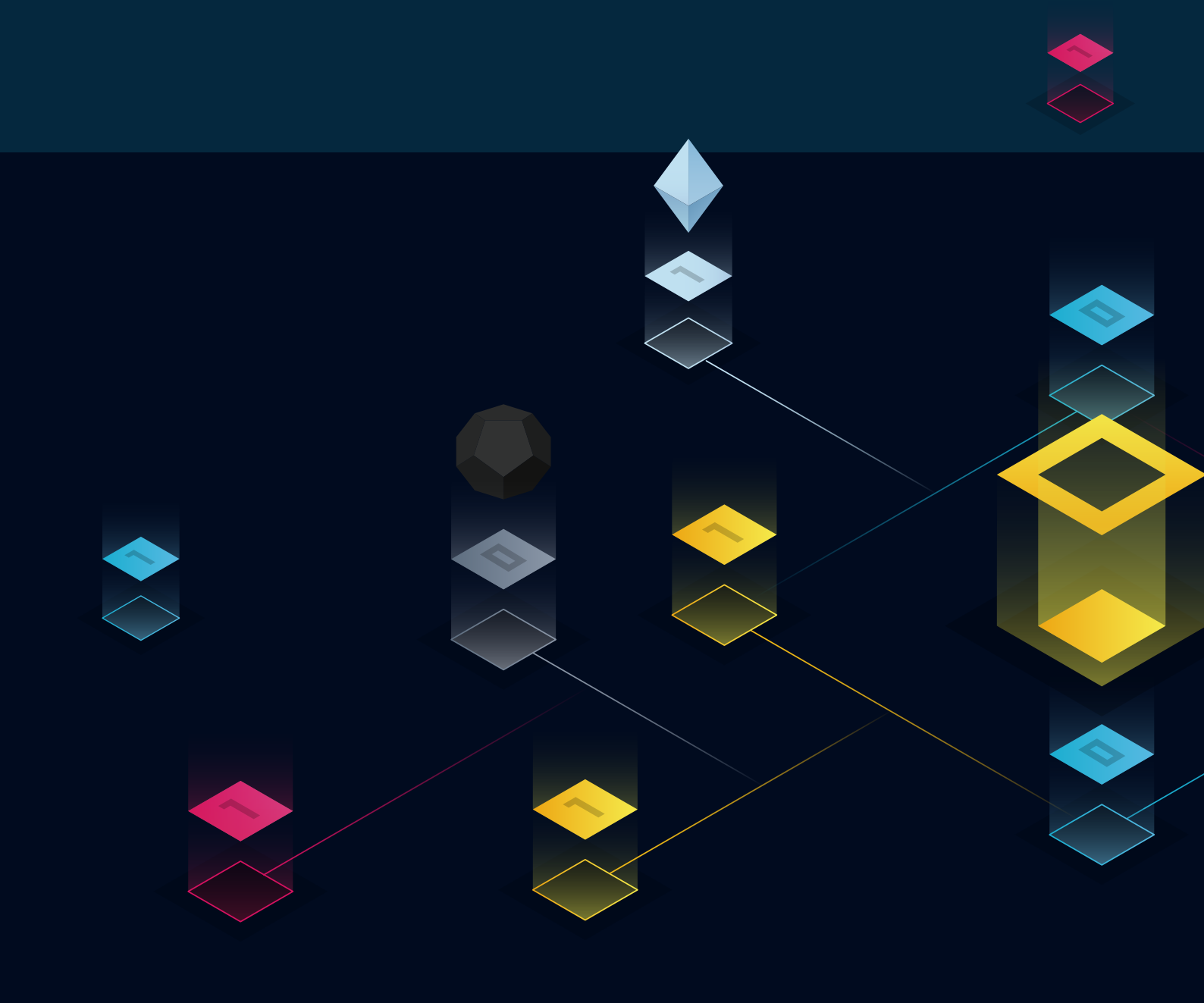
PlatON

重估一切价值

基于区块链的隐私计算和分布式经济基础设施

——PlatON.经济蓝皮书

V0.1.1



重估一切价值

Umwertung aller Werte

–尼采

PlatON 是基于区块链和密码学技术的、面向未来的隐私计算与分布式经济体基础设施。PlatON的目标是在保护数据所有权和隐私的前提下促进数据使用权的交易，并基于区块链建立数据和算力流通市场。

PlatON的定位决定了它在经济设计上有很多区别于一般公链的特点，将直接影响PlatON内置Token——LAT的价值。PlatON社区治理也有很多独特设计。

本文全面介绍了PlatON的经济设计，共分三部分。

第一部分从分布式经济体视角梳理公链的经济设计原则。第二部分介绍PlatON的经济设计，包括公链内经济活动以及公链支持的经济活动（即数据和算力流通市场）。第三部分讨论PlatON的经济设计对治理机制的影响。

目录

第一部分：公链的经济设计原则

在讨论PlatON的经济设计之前，有必要回顾现有公链的经济设计原则。

一、分布式经济体及其中基础设施付费问题

分布式经济体的核心是稀缺资源的生产和分配，并且稀缺资源配置通过市场机制而非中心化方式进行。分布式经济体由社区自治，经济活动的基础设施由社区共建、共享。区块链是分布式经济体最重要的“骨架”之一。

与公链有关的分布式经济体分为两层：

第一层在公链内，参与者主要是Token交易发起者、矿工[1]和网络节点（特别是全节点）等。经济活动主要是Token交易发起者发起交易，矿工打包交易、生产区块并运行共识算法，以及网络节点同步并存储分布式账本。TPS指标最为直接地体现了公链内的经济活动效率。本部分讨论的就是公链内的经济活动。

第二层包括基于公链的DApp、Layer 2解决方案和DeFi（开放金融）等，可以统称为公链支持的经济活动。第二层的参与者更加多元化。

不管在分布式经济体的哪一层，参与者都按照禀赋、偏好和个人选择形成了劳动分工，并根据市场交易来互通有无。

在与公链有关的分布式经济体中，最重要的基础设施是分布式账本（可以称为分布式信任基础设施）。一旦分布式账本的安全和效率没有保障，分布式经济体就会陷入低效甚至混乱的状态。矿工作为分布式经济体的核心参与者，维护分布式账本，并承担一定成本和风险。比如，PoW矿工需要投资于挖矿硬件设施并支付电费。实际上，挖矿已成为一个资本密集型行业。虽然PoS矿工需要的硬件投资和电力花销低于矿工，但是这并不意味着PoS挖矿没有成本或风险。在很多PoS型公链中，矿工需要锁定一定数量的Token。锁定Token既意味着暂时放弃Token的流动性并承担Token的价格波动风险，也意味着Token因存放在热钱包中而面临更高安全性风险。

要激励矿工维护分布式账本，就必须补偿它们承担的成本和风险。矿工激励问题本质上就是如何为基础设施付费。

[1] 在一些公链中（特别是PoS型公链），矿工也被称为验证者。第二部分介绍PlatON共识算法时，使用“验证节点”叫法，但本部分统一用“矿工”叫法。

常见做法是“**谁使用谁付费**”。比如，在比特币和以太坊中，单位时间内可被打包进公链的交易数量非常有限，交易发起者需要提供较高手续费以激励矿工优先处理自己的交易。这相当于交易发起者用手续费来竞拍公链内有限的系统资源，是保障矿工利益的重要措施，但在一定程度上牺牲了可拓展性。EOS系统资源的可拓展性更好。在EOS中，矿工处理交易发起者对智能合约的调用时，需要创造一个运行环境RAM并消耗一定的CPU算力，在将交易打包进区块并通过网络同步给其它节点时需要消耗一定的网络带宽NET。EOS不对CPU、RAM和NET这些系统资源设置上限，交易发起者可以通过它们持有的EOS获取，而非经过类似比特币和以太坊的竞拍过程。其中，CPU和NET通过抵押EOS获得或者从其它用户处租赁，RAM通过用EOS从一个特殊的智能合约处购买。

“谁使用谁付费”能否持续有效激励矿工，是一个没有明确答案的问题。

第一，这类收入取决于公链内交易活跃程度，这对矿工而言是不稳定且难以准确预测的。

第二，这类收入在数量上是否足以覆盖矿工承担的成本和风险？这一点困扰比特币社区已有相当长的时间。

第三，公平性问题。很多长期持有Token的人很少发起公链内交易，因此也很少向矿工付手续费。但它们持有Token的价值仍然依赖于矿工提供的分布式账本安全性。它们是否在“搭便车”？

出块奖励有助于缓解“谁使用谁付费”面临的这三个问题，特别在公链发展前期。

二、Token价值、出块奖励和通胀税

出块奖励与“谁使用谁付费”存在一个关键不同。“谁使用谁付费”是指已发行的Token在交易发起者和矿工之间的再分配，而出块奖励是矿工获得的新发行Token。在很多区块链文献中，出块奖励被称为“通货膨胀”，但是这个叫法实际上并不准确。

对法定货币，通货膨胀不是指货币发行，而是指物价指数（一篮子商品和服务用法定货币衡量的价格）持续上涨，但通货膨胀与货币发行之间有着紧密的联系。著名经济学家米尔顿•弗里德曼曾指出，通货膨胀在任何地方都是一种货币现象，是过多货币追逐有限商品和服务的产物。对与Token有关的分布式经济活动，目前还很难定义Token计价的物价指数和通货膨胀。

出块奖励在经济学上的核心问题是Token增发与Token价值之间的关系。

在一般公链中，Token具有双重经济属性[2]。

第一，支付属性。Token可以用于清偿区块链有关经济活动中形成的债权债务关系。

[2] 需要指出的是，稳定币、代表区块链外资产的 Token 以及加密货币交易所的平台币（有定期回购机制）不适用于这一节的分析。

第二，Token相当于分布式经济体的“入场券”或使用权。在一些PoS型公链中，Token还赋予持有者参与社区投票的权利，具有一定的治理权。但总的来说，Token不像股票和债券等金融证券那样有明确的收益权。特别是，Token没有任何所有权含义，因为分布式经济体不为任何人或机构所有。

另外，Token发行一般遵循以下做法：

1.Token发行没有信用背书或以现实资产作为支撑；

2.Token发行完全取决于供给侧，与需求侧无关；

3.Token供给由算法事先确定，是关于时间的确定性函数，与挖矿活跃程度或能源消耗无关。其中，Token发行总量可以有上限也可以无上限。在Token发行总量有上限时，往往引入新发行Token随时间递减的设计。

对具有上述特征的Token，还不存在公认有效的估值方法：

1.因为Token发行没有信用背书或以现实资产作为支撑，因此其价值不与任何信用主体或现实资产挂钩；

2.Token不像金融证券那样有未来的现金流，因此不适用现金的流折现法、套利定价等资产定价方法；

3.Token供给与挖矿的能源消耗无关，因此也很难适用成本定价法[3]。实际上，对PoW型公链，Token价格通过矿工的利益最大化行为决定了有多少算力投入挖矿，是Token价格影响挖矿成本，而非相反（本部分第三节会讨论这一点）。

尽管如此，我们的研究表明，Token价值受基本面和流动性因素影响。 **从长期看，Token价值主要由基本面决定。在短期，流动性因素对Token价值有很强的驱动作用。**

一方面，Token不代表分布式经济体的所有权，仅代表使用权。通过类似购买力平价的方法可以证明，Token价值与分布式经济体发展挂钩。在其它条件不变的情况下，分布式经济体规模越大，Token价值也越高。直观理解就是，随着分布式经济体发展，其使用权将变得更珍贵。前文已指出，与区块链有关的分布式经济活动分为公链内经济活动和公链支持的经济活动两层。Token价值除了与这两层经济活动的总量有关以外，也与它们之间的耦合关系有关（第三部分将详细讨论这一点）。

[3] 在给定时点上，PoW 型公链内 Token 的供给由算法事先确定，与有多少算力或能源投入挖矿没有关系。如果 Token 价格上升，会吸引更多算力投入挖矿，但新发行 Token 的数量并不因此增加，Token 价格不会受到供给侧的平抑。因为更多算力竞争给定数量的新发行 Token，单位 Token 的生产成本增加了。如果 Token 价格下跌，投入挖矿的算力会减少，但新发行 Token 的数量并不因此减少，Token 价格不会受到供给侧的支撑。此时，较少算力竞争给定数量的新发行 Token，单位 Token 的生产成本减少了。因此，很难用成本定价法为 PoW 型公链内 Token 定价。PoS 型公链内 Token 因为挖矿消耗的能源很少，就更不适用成本定价法。

另一方面，当有更多法定货币或其它类型的资金追逐同样数量的Token时，Token价格就有上涨趋势，反之则Token价格就有下跌趋势。资金驱动的Token价格涨跌幅度还与Token二级市场的深度有关。如果有部分Token退出流通（比如Token被锁定或用作抵押品），Token的有效供给会减少，也会支撑Token价格。

在Token增发的瞬间，可以假设基本面和流动性因素都没有显著变化，那么新发行的Token就会稀释原有Token的价值。这个效应类似于在法定货币领域，如果经济基本面不变，货币发行引发通货膨胀，存量货币的购买力被稀释。类似地，可以称Token的增发对原有Token价值的稀释为**通胀税**。一方面，通胀税的高低与Token增发速度挂钩，并由原有Token持有者按它们持有Token的数量来分担。另一方面，通胀税通过转移支付，以出块奖励的方式由矿工享有。值得注意的是，这个机制在没有中央协调的情况下运行。

与“谁使用谁付费”相比，通胀税对矿工是更稳定的收入来源。长期持有Token的人通过分担通胀税也向矿工付费，从而“搭便车”问题得以缓解。如果将矿工群体视为新的Token持有者，那么Token增发本质上是将财富从原有Token持有者转移给新的Token持有者。因此，在短期，Token增发主要是财富再分配；在长期，新老Token持有者的利益都绑定在Token价值上升上。

三、信任基础、共识算法和共识成本

公链的核心是共识算法，共识算法有两个关键点：

一是Token增发；

二是分布式账本的记账权分配。

如果说Token增发主要是为了奖励矿工对维护分布式账本所做的贡献，那么记账权分配主要为防范作恶矿工对分布式账本的破坏。接下来，我们从信任基础角度给出共识算法的一个经济学分析框架。

1. PoW——基于技术的信任

在PoW型公链中，矿工不需要持有Token，只需要配备硬件设施并消耗电能。理论上，矿工在挖出Token后可以很快将其出售。矿工对PoW型公链的风险敞口主要来自Token价格下跌对其拥有的矿机价值的影响。但如果矿机是通用型的（比如GPU），即使Token价格下跌，矿工仍可以将矿机转作其它用途（比如游戏），因此矿工对PoW型公链的风险敞口不大。只有在矿机是专用型时（比如ASIC），矿工才与PoW型公链有深度利益绑定关系。

PoW挖矿是寻找满足SHA256哈希加密问题的随机数Nonce。对这个问题，目前除了穷举法以外，没有更好的解决方法。挖矿过程与矿工的链外身份或信用无关，完全取决于它控制的算力。矿工控制的算力越大，在同样时间内完成的计算越多，就越能领先于其它矿工找到随机数Nonce并获得记账权。挖矿是完全随机性的或无记忆的：对同样的算力，其未来挖矿表现与过往业绩几乎没有任何关系。

在PoW型公链中，矿工之间是竞争关系，不存在交互式沟通协作。谁先找到随机数Nonce，谁就获得记账权和出块奖励，而其它矿工从上一个区块截至此时的工作就基本作废。为了平滑挖矿过程中的不确定性并激励矿工共担风险、共享收益，多个矿工可以形成矿池这样一种特殊的合作关系。但矿池与矿池之间仍是严格竞争关系。

只要配备硬件设施并消耗电能，任何人都可以参与PoW挖矿。PoW挖矿的开放性以及矿工之间的竞争关系，使得在Token价格上涨时，挖矿成本攀升。一方面，只要Token价格高到使得挖矿收益大于成本，就不断会有新算力投入挖矿，使得单位算力的挖矿成功概率下降，直到挖矿收益趋近于成本。另一方面，一旦有矿工投资于算力，不管是扩大算力规模，还是购买更先进挖矿设备，都会增加自己挖矿成功概率，同时降低其它矿工的挖矿成功概率。因此，一个矿工或矿池对算力的投资对其它矿工构成负外部性。其它矿工面临竞争压力，可能不得不扩大算力投资。从而，矿工面临着“囚徒困境”局面，不得不投入算力“军备竞赛”。

总的来说，PoW体现了基于技术的信任，主要靠技术为挖矿创造了一个不依赖于矿工链外身份或信用的环境，矿工之间是竞争关系，但难以内生地抑制算力“军备竞赛”对挖矿成本的抬升。

2. PoS——基于制度的信任

在PoS型公链中，矿工参与共识算法需要持有Token，对PoS型公链存在风险敞口，但面临的硬件设施要求比PoW低得多。矿工风险敞口的大小取决于矿工是否需要锁定Token。

根据本部分第一节的分析，锁定Token是暂时放弃根据市场情况出售Token的权利，也就是暂时放弃Token流动性。放弃Token流动性的成本与锁定Token的数量和时间正相关，更与持有Token的策略有关。对长期持有Token的人而言，因为本就没有出售Token的计划，锁定Token的成本很低。但对一个普通投资者而言，在Token价格波动性高的时候锁定Token，意味着很高成本。比较锁定Token的成本与参与共识算法的回报，只有倾向于长期持有Token的人才有动力锁定Token以参与共识算法，而这些人往往也是对PoS型公链有强烈认同感的人。

如果矿工不需要锁定Token就可以参与共识算法，尽管共识算法的开放性更好，但矿工与公链之间的利益绑定关系较弱。

PoS型公链为提高共识算法效率，一般会引入矿工选举机制。选举前，会赋予Token持有者一定数量的选票。选票数与Token持有量之间既可以是线性关系（比如1个Token对应着1张选票），也可以是非线性关系（比如二次方投票，quadratic voting）。Token持有者的选票可以只投给它自己，也可以全部或者部分投给其它人。Token持有者被选为矿工的机会与其得票数正相关。比如，在EOS中，1个被锁定的EOS兑换30票，可以分别向最多30个超级节点候选人投票。得票最高的21个候选人成为超级节点。而在Algorand中，用VRF（可验证随机函数，verifiable random function）抽选矿工，每个Token持有者被选中的概率与其Token持有量成正比。可以看出，矿工选举与现实世界的选举很像，不同选举程序背后有不同的设计考虑，并将对社区治理产生不同的影响。

PoS矿工有三个显著特点。第一，在DPoS型公链中，矿工需要向其支持者“拉票”，矿工的链外身份和信用很重要。矿工与其支持者之间有重复博弈。矿工的过往表现，比如出块率以及与其支持者分享出块奖励的慷慨程度，会直接影响其信用和未来“得票” 。作恶的矿工可能在接下来的选举中被选下去。第二，不同矿工之间存在一定合作关系。矿工在区块生产上不存在类似PoW挖矿的竞争关系。矿工可以像EOS那样按某一顺序轮流生产区块，也可以像Algorand那样用VRF从中再选出一个区块生产者。但接下来一般矿工会针对候选区块运行拜占庭协议直到达成共识。第三，矿工升级硬件设施不会获得更多出块奖励，从而不会形成类似PoW挖矿的算力“军备竞赛”。

PoS型公链如果允许委托投票，会形成矿池（一般被称为 staking pool ）。其经济逻辑是，普通Token持有者不一定能满足参与共识算法对硬件设施的要求或拥有相关专业知识。它们通过汇聚力量支持某一矿工并分享出块奖励，可以获得更高收益。

总的来说，PoS体现了对制度的信任。制度是为提高分布式经济体中群体合作效率而针对群体成员引入的行为规则。矿工的链外身份和信用、矿工选举程序以及矿工在区块生产和达成共识上的合作关系，都是制度的体现。

3. 共识成本

不管是PoW，还是PoS，共识算法的目标都是在存在各种差错、恶意攻击以及异步的分布式网络中，并且在没有中央协调的情况下，确保分布式账本在不同网络节点上副本的“最终一致性”。达成这种一致状态毫无疑问需要成本，我们称之为“**共识成本**”。

在PoW中，共识成本主要体现为挖矿成本，即在挖矿硬件设施上的投资以及运行这些硬件设施消耗的能源，可以称之为“**技术成本**”。PoW对矿工的链外身份和信用以及它们之间的合作没有任何要求，但在Token价格上涨时，难以内生地抑制算力“军备竞赛”对技术成本的抬升。

PoS的共识成本要复杂得多。PoS可以视为一系列制度的组合。这些制度旨在提高群体合作效率，但制度的持续、有效和稳健运行却非易事。首先，群体成员要根据制度内嵌的激励和约束调整自己的行为，以符合制度设计者的预期。这就隐含了对个体理性的要求——个体行为遵循理性准则，而不是非理性或具有机会主义的。但现实中，人性复杂多变。针对这种情况，制度往往基于参与者的身份和信用机制，并配以能加强信用机制的奖惩措施。其次，为提高群体互动的可预见性和效率，制度中往往包含针对群体互动的程序性安排，比如投票、选举和区块生产顺序等。程序性安排一般有博弈论方面的考虑。

PoS对Token持有者、矿工之间的合作要求越高，就越依赖链外身份和信用机制以及程序性安排。这一点对PoS的共识成本有很复杂的影响。

第一，在重复博弈中建立链外身份和信用机制，本身就需要成本。比如，EOS社区在超级节点选举中的贿赂行为，实际上显示了建立链外身份和信用机制的“影子成本”。

第二，链外信用机制有自我加强趋势。信用好的矿工越有可能因其支持者的投票而继续当选。它们通过参与共识算法获得出块奖励后，就越有资源维护好链外信用。这样，矿工就会走向“常任制”，矿工名单趋向固定，实质上把共识算法的参与者局限在一个小范围内。但共识算法的去中心化程度一旦减弱，就更易被攻击。

第三，矿工选举、区块生产以及达成共识等环节的程序性安排，使得共谋更易筹划和实施。而这会直接影响制度的公平性、有效性和可信性。此外，如果信息不对称非常普遍，Token持有者和矿工可以有隐含信息和动机。这会使程序性安排偏离预期效果，使其中的博弈设计不再有效。

以上这些方面，就构成了PoS的共识成本，可以称为“**制度成本**”。

此外，基于技术的信任与基于制度的信任有两个关键不同点。

首先，与技术成本相比，制度成本要隐蔽得多，也更难被准确测量。制度成本往往只有在制度失效时，或者同样制度被移植到不同环境时，才能被人们认识到。

其次，技术能产生一定条件下的确定性。比如，在现有技术条件下，区块链技术常用的SHA256哈希算法和基于椭圆曲线的数字签名算法不能被有效破解。在技术没有大幅进步的情况下，这种确定性是有保障的。而与技术带来的确定性相比，有多少制度能长期经受人性的考验？可以断言，不管是在现实世界，还是在区块链领域，都不存在完美的制度设计。

综上所述，每种共识算法都在不同程度上依赖基于技术的信任以及基于制度的信任，并由此分别产生技术成本和制度成本，**共识成本则是技术成本和制度成本之和**。对基于技术的信任的依赖程度越高，技术成本越高，反之则相反。这一关系对基于制度的信任和制度成本亦然。完全依赖基于技术的信任，或完全依赖基于制度的信任，都会造成比较高的共识成本。我们认为，存在两种信任基础之间的最佳配比，使得共识成本最小（图1）。

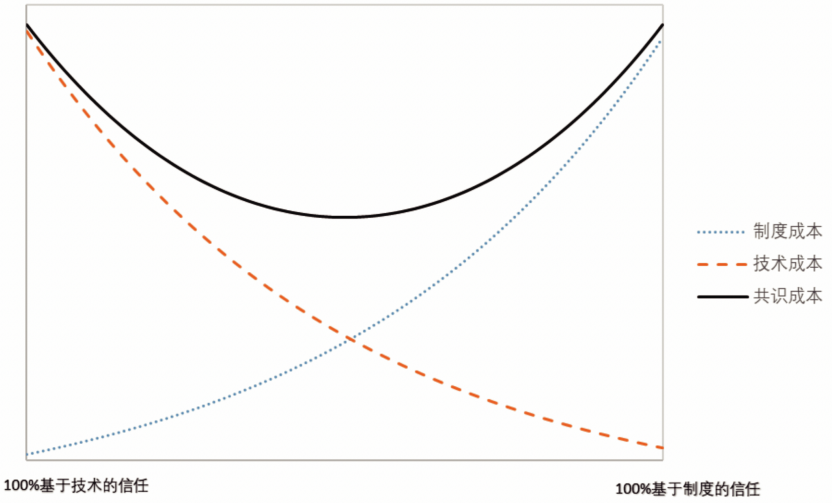


图1：共识成本

第二部分：PlatON的经济设计

一、PlatON的经济设计目标

基于前文的分析，PlatON的经济设计主要有以下目标：

第一，尽可能降低共识成本。鉴于PoW的能源消耗及其在现实世界面临的限制，我们认为PoW的在区块链领域的份额不可能无限增长。PlatON公链属于PoS类型，其共识算法被称为PPoS（PlatON PoS）。PPoS使用链外身份和信用机制以及程序化安排，但通过VRF引入的随机性来降低对它们的依赖程度。这样能有效抑制贿赂、共谋等行为。

第二，加强公链内经济活动与公链支持的经济活动（即数据和算力流通市场）之间的耦合关系，为PlatON内置Token——LAT的价值提供支撑。

第三，内生地抑制围绕PlatON公链的矿池的规模扩张，以保证PlatON公链的去中心性和安全性。

根据第一部分对分布式经济体的分层，接下来先讨论PlatON公链内的经济设计，再讨论PlatON数据和算力流通市场（即公链支持的经济活动）的经济设计。

二、PlatON公链内的经济设计

1. LAT初始发行和增发

LAT不设硬顶，分为初始发行和增发。LAT初始发行按一定比例分配给创始团队、PlatON基金会、学术基金、生态基金和私募发行方，并引入相应的锁定期安排。

随着PPoS的每轮运行，LAT将持续增发。LAT增发将按照事先确定的比例分配。大部分Energon增发用作给验证节点的区块奖励。小部分LAT增发用作给没有被选为验证节点的备选节点的Staking奖励。余下的LAT增发存入一个信托基金，用于奖励PlatON开发者社区，该信托基金由PlatON基金会管理。

每年LAT增发数量，相对上年底LAT总发行量，都是一个事先确定的比例。在PlatON主网上线后的若干年内，PlatON基金会将从自己获得的初始发行中，拿出一部分补贴验证节点、没有被选为验证节点的备选节点以及信托基金。这个补贴将逐年递减以至于0。因此，在补贴期间，验证节点以及没有被选为验证节点的备选节点将获得较高收入。

2. PPoS的3个阶段

PPoS每轮运行都分3个阶段：1. 备选节点选举；2. 用VRF从备选节点中选出验证节点；3. 验证节点轮流出块并运行拜占庭协议CBFT。需要声明的是，与PPoS有关的技术细节将在《PlatON共识黄皮书》中专门阐述，此处仅涉及PPoS中与经济设计有关的内容。

第1阶段：备选节点选举

每个LAT持有者都能参与PPoS。

如果一个LAT持有者想成为验证节点，必须锁定超过一个事先确定的最低数量LAT，成为备选节点候选人。每锁定1个LAT相当于自投了1张选票。备选节点的候选人之间不得相互投票。

其他想参与备选节点选举的LAT持有者也必须锁定LAT，但对它们锁定的LAT数量没有任何限制，每锁定1个LAT兑换1张选票，它们可以将自己的选票投给任何它们支持的备选节点候选人。

所有投票完成后，备选节点候选人按照它们的得票排序。得票最高的前若干位候选人成为备选节点，备选节点数量也是事先确定的。备选节点及其支持者锁定的LAT将继续保持锁定状态，直到一个事先确定的锁定周期结束。没有入选备选节点的候选人及其支持者锁定的LAT，在选举后可以解锁。它们不再参与这一轮PPoS，也不会获得任何补偿。

第2阶段：用VRF选出验证节点

VRF将从全部备选节点中，选出一定数量的验证节点，验证节点数量是事先确定的。VRF的过程非常复杂，但与以下实验等价。

首先，将每个备选节点的每张得票设想为一个球，用不同的颜色区分不同备选节点，并将所有球混在一起。其次，从所有球中随机抽取一个，记录其颜色，并将其放回。重复“抽取并放回”步骤若干次。最后，统计被抽中的球的颜色分布。出现次数最高的那些颜色对应的备选节点即为验证节点。

数学上可以证明，得票数越高的备选节点，经VRF被选为验证节点的概率越高。但因为VRF引入的随机性，最终选出的验证节点不一定正好是得票最高的那些备选节点。

第3阶段：验证节点运行CBFT

在CBFT中，每个验证节点均被分配一个时间窗口，在这个时间窗口内连续生产区块。每个验证节点在其时间窗口内生产的区块数量是事先确定的。此后，全部验证节点对候选区块运行CBFT直到达成共识。

在获得区块奖励和Staking奖励后，验证节点、没有被选为验证节点的备选节点与其支持者按照事先约定分享收入。此外，验证节点的收入还包括交易手续费。

3. 对PlatON公链内的经济设计的分析

第一，合理搭配基于制度的信任与基于技术的信任。与以EOS为代表的DPoS类似，PPoS中备选节点的选举，依赖于备选节点的链外身份和信用。备选节点的链外信用越好，越有可能获得高的得票数，在VRF阶段能以更高概率被选为验证节点。但VRF为从备选节点到验证节点这一环节引入了随机性，降低了对链外身份和信用的依赖程度。当然，如果有验证节点在CBFT阶段作恶，信用机制仍将发挥作用。作恶节点在未来备选节点选举中的得票将受到影响，甚至可能被选出去。另外，备选节点在选举阶段不得相互投票，也有助于抑制串谋。

第二，共识参与的公平性和开放性。在很多PoS型公链中，事先可以估算出，备选节点在得票数超过一定门槛时，能以多大概率成为超级节点。这样，就存在能以较高概率帮助备选节点成为验证节点的策略，从而验证节点选举在一定程度上可以被操纵。那么，PPoS是否面临类似问题？我们认为不存在。可以证明，在PPoS中，一个备选节点成为验证节点的概率，不仅与其得票数有关，也取决于其它备选节点的得票数，而其它备选节点的得票数在其控制以外。VRF对从备选节点到验证节点的环节引入了很多不可控因素，使得验证节点选举难以被操纵。

下文还将指出，LAT持有者对任何备选节点候选人的支持都将是有限度的，候选人不存在无限拉票的可能性。因此，相对很多PoS型公链，PPoS中的验证节点名单将呈现出更大的可变性和开放性，从而在避免“多数人暴政”的同时，也尽力避免形成“寡头统治”。

第三，内生地抑制矿池规模扩张。与其它PoS型公链一样，围绕PlatON公链也会出现矿池。作为一个缓解措施，在PPoS的每轮运行中，每个区块的出块奖励是固定的，与验证节点及其支持者锁定多少LAT无关。这在一定意义上可以视为规模不经济。这样，LAT持有者在选举备选节点时就面临如下问题：是否帮助某一候选人先成为备选节点再以较高概率成为验证节点，但之后需要与较多LAT持有者分享同样的收益？

在这个博弈中，收益最高的LAT持有者是那些投票给得票不多的备选节点而备选节点正好被选为验证节点的。但因为VRF引入的随机性，哪些备选节点能成为这样的“幸运儿”，是不可预知的。因此，一方面，LAT持有者在备选节点选举阶段有动力避免投票集中、“垒大户”等情况；另一方面，专业的验证节点运营者受制于VRF带来的不确定性，创造“超级矿池”的动力也会下降。

第四，降低共识成本。前文已比较PlatON和EOS。接下来，比较PlatON与同样使用VRF的Algorand。根据我们的理解，PlatON和Algorand存在两个关键不同。

首先，在Algorand中，VRF选出参与拜占庭协议（Algorand称之为BA★）的Token持有者。Token持有者不需要锁定自己的Token，也不接受其它人的投票。每个Token持有者被选中的概率只与自己持有的Token数量成正比。在这个安排下，参与BA★的Token持有者与Algorand公链的利益绑定关系偏弱。那些有良好链外信用但仅持有少数Token的人几乎没有被VRF选中的可能性。如果将参与BA★视为一种权力，那么这种权力主要属于Algorand中那些Token持有“大户”。而在PlatON中，参与选举的人需要锁定LAT，这样就加强了它们与PlatON公链之间的利益绑定关系。任何LAT持有者，即使自己持有的LAT不多，但如果链外信用足够好，能吸引足够多的支持者，也有希望被选为备选节点乃至验证节点。换言之，PlatON中的权力不属于“富人”，而属于“信用好的人”。

其次，在BA★的每次循环的每一个子步骤中，Algorand会通过VRF在全体Token持有者中重新、独立随机选出参与BA★的人。在这种情况下，BA★仍能正确、有效地达成共识。这就是Algorand中BA★参与者的可更换性（player-replaceable），是Algorand的一个很有吸引力的安全特征。但需要看到其对共识成本的影响：针对全体Token持有者，在BA★的每次循环的每一个子步骤都运行VRF，成本是非常高的。而在PlatON中，验证节点一经VRF选出，就能完整地参加一轮CBFT。鉴于验证节点的链外信用，我们认为不一定要在CBFT运行途中把它们替换掉。这就体现了利用链外身份和信用机制来降低共识成本的考虑。

三、PlatON数据和算力流通市场的经济设计

1. PlatON数据和算力流通市场概况

PlatON致力于建设一个高性能的计算网络，以促进数据和算力的流通。其中，PlatON在数据流通中使用同态加密和安全多方计算等密码学技术，能很好地保护数据隐私。

PlatON公链与其数据和算力流通市场之间有密不可分的联系。PlatON公链起到计算任务分发、计算任务与算力匹配以及交易记录等功能。PlatON公链设计遵循了链上共识与链下计算解耦的原则：核心计算工作都发生在公链外；通过可验证计算，公链节点不需要重复计算就能验证交易。这样就使计算免受区块链性能的限制。PlatON公链内的LAT用于结算数据和算力交易形成的债权债务关系。

从经济学角度，PlatON数据和算力流通市场主要参与者包括计算协调方、数据提供方和算力提供方等，它们本身也是PlatON公链的节点。

数据提供方根据算法定义的输入数据格式，提供相应数据用于计算，但数据仍保存在数据提供方的本地数据库中。参与PPoS的节点作为链内数据的提供者，是一种特殊的数据提供方。

计算协调方一般也是数据提供方。计算协调方获取输入数据后，先在计算网络上查找符合算力需求的算力提供方，再将输入数据、可验证计算的算法参数整合成多个子任务并分发给算力提供方。计算协调方通过分发计算任务，实现了计算的协同和去中心化。为提高容错性，计算协调方在分发计算任务时会引入一定的冗余。

算力提供方接收并执行计算任务。算力提供方加入计算网络时，会自动评估自己的计算能力并发布服务能力参数。算力提供方收到计算协调方分来的子任务后，在完成计算的同时，利用可验证计算生成正确执行的证明，并返还给计算协调方。

2. 算力交易定价

与数据交易相比，算力交易的标准化（或“大宗商品化”）、可验证和可度量等程度要高得多，交易效率和透明度更高。**可验证计算**的引入使得算力提供方的作恶或怠工等行为更易被发现。这些都使得对算力提供方的业绩评估和奖励可以客观进行。

在PlatON计算网络中，算力交易定价相对简单，算力交易定价取决于其能源消耗，因此对算力提供方的激励采取成本定价方式。另外，验证正确的计算工作量还将累计成为算力提供方的计算贡献值，相当于它在PlatON计算网络中的信用。

3. 数据交易定价

数据交易的标准化程度比较低，主要有以下三方面原因：

第一，不管在种类上，还是在来源上，数据都趋于多样化。比如，PlatON 计算网络中交易的数据可涵盖身份、健康和信用等维度。数据可来自社交网络、物联网和工业互联网等，并且很多数据是非结构化的。

第二，随着人工智能兴起，数据分析手段趋于多样化。PlatON 将支持多种数据分析算法。

第三，数据作为商品的特殊性。很多数据的所有权不明晰，难以被有效保护。数据容易在未经合理授权的情况下被收集、存储、复制、传播和使用。数据的使用是非竞争性的（non-rivalry）——数据可以被重复使用，并且重复使用不会降低数据的质量或使其数量减少。数据的使用是非排它性的（non-exclusive）——对同一份数据，不同的人可以同时使用。数据的这些特殊属性使得传统数据交易市场容易面临市场失灵问题。

PlatON 使用的同态加密和安全多方计算等密码学技术支持了数据确权，使得在不影响数据所有权的前提下交易数据使用权成为可能，这是数据交易的产权基础。PlatON 数据交易坚持数据主权原则，在隐私保护的同时有序交易数据使用权（即有序交易原则），并且数据使用者要向数据所有者付费（即有偿使用原则）。这些都有助于解决传统数据交易市场面临的市场失败问题。

数据定价有两种方法。第一种是绝对定价。数据对使用者的价值体现为数据对它们的认知能力、决策和福利等方面的提升。提升程度决定了数据使用者愿意为获得数据而付出的对价。第二种是相对定价，也就是给定一个数据集合和一个共同的任务，评估数据集合的成员对完成该任务的贡献。相对定价可以成为绝对定价的基础。Shapley 值是数据相对定价中的一个重要工具。这是著名经济学家 Lloyd Shapley（2012 年诺贝尔经济学奖得主）在 1953 年研究合作博弈时引入的一个重要概念。

第三部分：PlatON的经济设计对治理机制的影响

在本文第一部分中已提出，与 Token 有关的分布式经济活动包括公链内经济活动以及公链支持的经济活动。Token 价值既与这两层经济活动的总量有关，也与这两层经济活动之间的耦合关系有关。

经济耦合是一个重要但尚未得到充分重视的问题。比如，在很多为 DApp 搭建的公链中，DApp 中运行的是自己的 Token。在多数时候，DApp 用户对公链内 Token 和交易的需求不高。这样容易造成两方面问题。一方面，DApp 用户对公链发展不是很关心，尽管它们持有的 DApp 中 Token 的价值在很大程度上取决于公链分布式账本的安全。另一方面，公链内矿工通过维护分布式账本为 DApp 发展提供了基础，但很难直接从 DApp 发展中受益。如果经济耦合不紧密，公链内 Token 就很难从公链支持的经济活动中捕获价值。这两层经济活动的参与者之间容易出现利益不一致情况。

我们认为，可以从两个维度衡量公链内经济活动与公链支持的经济活动之间的耦合关系。

第一，公链支持的经济活动能在多大程度上提升对公链内 Token 的需求。比如，如果 DApp 和 Layer 2 解决方案使用自己的 Token，并且其用户不太需要涉足公链内 Token 交易（比如，用户可以用 DApp 和 Layer 2 的 Token 向公链矿工付手续费），提升效应会很弱。但如果 DApp 和 Layer 2 的用户需要持有甚至锁定公链内 Token，提升效应就会强一些。

第二，公链支持的经济活动的参与者与公链内经济活动的参与者在多大程度上是交叉的。对多数 PoW 型公链，挖矿是一项有鲜明特点的、资本密集型工作，矿工很少参加公链支持的经济活动，公链支持的经济活动的参与者也很少兼营挖矿，两个群体之间的交叉程度很低。一些 PoS 型公链出现了专业的矿池运营者。它们在 Token 托管、社区运行和管理支持者关系等方面有专长。它们一般不太参与 DApp 层面的活动，但在 DeFi 层面可能很积极。

与一般公链相比，PlatON 有更强的经济耦合设计。

第一，PlatON 公链内的 LAT 用于结算数据和算力交易形成的债权债务关系。数据和算力流通市场的发展将提高对 LAT 的需求，构成 LAT 的价值支撑。

第二，PlatON 计算网络的参与者通过对外提供数据、算法和算力等服务而获得 LAT。作为 LAT 持有者，它们可以参与 PPoS。它们在计算网络中经营得越好，积累的 LAT 越多，在 PPoS 中的影响力越大。换言之，对 PlatON 计算网络承诺更深、风险敞口更大的参与者，在 PPoS 中扮演的角色也更重要。这体现了一种深度利益绑定关系，也体现了以链外身份和信用为代表的链外资源向链内的传导。

我们认为，上述安排体现了 PoS 中“stake”一词的真正含义。我们倾向于将 PoS 翻译为“利益相关证明”，而非“权益证明”。公链不像公司那样，存在所有者权益（owner’s equity）的概念。Token 代表分布式经济体的使用权，没有任何所有权含义。所有的 Token 持有者都是利益相关者（stakeholder）而非股东，其核心特征就是对公链有风险敞口。任何影响公链或两层分布式经济活动的事情，都对它们的利益有影响。最重要的利益相关者就是矿工或验证节点。在 PoS 中，验证节点参与共识算法的“凭证”就是它们“利益相关”。

第三，与一般公链类似，PlatON 支持 DApp 和 DeFi 等的发展，并会引入针对 DApp 和 DeFi 的经济耦合设计。比如，PlatON 公链中的 DApp 可以发行自己的 Token。但 DApp 的 Token 必须以 LAT 作为准备金。DApp 子社区决定 DApp 的 Token 与 LAT 准备金之间的耦合关系强度。一旦 DApp 子社区通过耦合关系设定，它就具备约束力，并且通过智能合约来执行。如果 DApp 子社区希望发行更多 Token，它们必须将更多的 LAT 准备金转入智能合约。反之，如果 DApp 子社区赎回部分 Token，智能合约会将相应的 LAT 准备金退给它们。在这个安排下，随着 DApp 的发展，用户需要获取更多 LAT 作为准备金。这能帮助 LAT 更好地从 DApp 的发展中捕获价值，从而支撑 LAT 价值。为加强 DApp 与 PlatON 公链之间的经济耦合关系，PlatON 基金会将向 DApp 子社区捐赠部分初始 LAT 准备金，作为它们的“启动资金”。DApp 子社区选择的经济耦合关系越强，PlatON 基金会的捐赠力度越大。

PlatON 也将支持以 LAT 为抵押的稳定币。在数据和算力流通市场中，某些参与者可能倾向于用稳定币而非 LAT 来结算。PlatON 将提供相应的灵活度。用稳定币结算的交易越多，意味着对稳定币的更高需求，而这将促使更多 LAT 被用作抵押品。这是另一个帮助 LAT 从数据和算力流通市场中捕获价值的机制。

到此为止，本文简单讨论了 PlatON 的经济设计对治理机制的影响。PlatON 治理机制具有“社区共建、共享、共治”的特点。对 PlatON 治理机制，我们将在《PlatON 治理红皮书》中予以详细介绍。

PlatON

platon.network