Αν οι αρχαίοι Έλληνες γνώριζαν αυτόν τον νόμο
σίγουρα θα θεωρούνταν θεοί. Καθοδηγεί τον κόσμο.
Σε μια ήσυχη χειρονομία σε ένα από τα πιο άγρια χάος.
Όσο υφηλιστεύει τον υπέρτατο Κανόνα τα αντιπαθ αλογισμού
Όταν μια σειρά επιφανειακών παραγόντων συγκεντρώ-
νονται. μια απροσδόκητη και εξαιρετικά όμορφη
κανονικότητα αποδεικνύεται ότι είναι σιωπηρή.

En-Tan-Mo SCIENCE

Interpretation

AGREED VALUE SHARED BENEFIT

En-Tan-Mo

En-Tan-Mo

AGREED VALUE SHARED BENEFIT

En-Tan-Mo is an exciting new project which aims to build a decentralized world with blockchain technology.

Until the advent of blockchain technology. human society had, for thousands of years, been underpinned by a rigid hierarchy Adopting this new technology heralds a brand new world characterized by decentralization, equality and creativity. a place where the corporate pyramid has collapsed and traditional hierarchical structures have been obliterated. Resource allocation will be optimized by decentralized pricing and dynamic equilibrium processes without external intervention or manipulation.

A world where value transfers freely with better services in digital finance, energy distribution, property rights and people's lives.

http://www.entanmo.com

Foreword

前言

“

AGREED VALUE SHARED BENEFIT

”

前言

被低估的中本聪

2008 年 10 月 31 日，一篇名为《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，让“中本聪”这个名字第一次进入公众的视线。文中，中本聪介绍了电子货币比特币，同时，也首次提出了区块链的概念。

在留下 575 封邮件和 364 次在线活跃的记录后，中本聪就再也没有出现过。

十年如白驹过隙，比特币创始人中本聪真迹难寻，但他身上的光环从未褪去，有人称他为比特币之父，有人尊他为区块链创世之神，甚至还有人认为他是诺贝尔经济学奖的隐形获奖者。

但在笔者看来，即使是有这些光环傍身，中本聪仍然被人们大大低估了。

为什么这么说？

中本聪的被低估，是科技改变生活之力量的被低估。

19 世纪以来，人类进入技术大爆炸时期，也由此进入到了生活世界变革最快的时期。梳理其中那些最具创新性和影响力的技术，它们的共同特点，便是有能力通过创新的途径来扩展人类活动空间、扩大交互影响。那些改变世界的发明——如纸张、印刷术和互联网，都为自由表达、相互交流、信息与价值沟通和转换等诉求开辟了新的道路。

区块链是一种去中心化的分布式存储技术，如果我们把所有的价值物交易都当做账目，它的记账人便是全网中的所有授权者，它的账本也保管在全网所有的节点中，任意参与者都可以查看所有交易数据。在这样一个系统里，没有某一个人或者某一个操作者可以篡改数据，它是匿名的，个体的隐私也能得到有效保护，能让世界上许多地区实现安全、匿名的新通信形式与价值流通方式，它是 21 世纪创造出的独特信任机器，也是新的沟通与流转渠道。

可以想象，区块链技术对人们生活世界的改变也将是极为巨大的。

然而，也许很多人心中会存有这样的疑问：为什么我感受不到我的生活被区块链改变？

因为区块链是协议层的改革，对于普通个人而言，“看得见”的改变往往在应用层。当我们用 App 进行支付的时候，我们可能根本不知道协议层是中心化还是去中心化的，我们能看到的只是账户上数字的变化。区块链改革的层面相对更底层，这就导致了我们很难“看见”它对我们生活的改变。加之，人们对待新鲜事物的出现总是持观望或怀疑态度的，就像蒸汽机时代人们总是心怀疑虑，电话发明后不少人嗤之以鼻，这也是区块链技术至今也还没有获得与其匹配的重视程度的原因之一。

中本聪的被低估，是去中心化的被低估。

在区块链诞生之初，中本聪就告诉我们，区块链的核心是去中心化，这是区块链技术本身最激动人心的特质。

高度中心化的社会，使我们生活的各个领域都受到第三方组织机构与经济机构的宰制。它们本是“人造物”，但由于其高度组织化、精英化，能处理很多个人无法处理的事务，导致个体越来越依赖它，第三方逐步向本属于生活世界的领域扩张，形成对“生活世界的殖民化”，即原本属于私人领域和公共空间的非市场和非商品化的活动，被市场机制（金钱）和科层化的权力侵蚀了。

区块链的分布式、免信任、时间戳、非对称加密、智能合约等技术优势，天然地决定了它能让个体摆脱第三方来从事经济文化乃至各个社会领域的活动。我们可以充分想象今天的金融业、零售业、人力资源、广告传播、公共事业、知识产权保护乃至司法、科技、政治、社会等各个领域中，不依赖第三方进行的理想图景。这是社会生态的巨大变化，也是科技革命的意义所在。

然而，短短十余年过去，去中心化越来越成为一块遮羞布，越来越多的区块链项目单纯追求效率，对去中心化避而不谈或避重就轻。这正是中本聪最被低估的地方。没有了去中心化追求的区块链，只能是伪区块链。

中本聪的被低估，是我们试图改变世界的决心被低估。

在过去 3 万年或更长的时间里，人类为了各种各样的目的驯化了许多动物，但极为讽刺的是，被驯化得最成功的，

竟然是我们自己。

1977 年，福柯出版《规训与惩罚》，书中详细描述了人类历史上权力的性质及其演变历史，从封建社会的“酷刑”到启蒙时期的“温和方式”，进入现代，则以全面的规训取而代之。这种借用“层级监视”、“检查”等手段的规训技术，无处不在，并深刻体现在边沁提出的“全景敞视监狱”之上。这种建筑的构造是：四周是一个环形建筑，中心是一座四周都是窗户的瞭望塔；环形建筑被分成很多囚室，囚室的一端窗户与瞭望塔相对，而另一端窗户透入微光；通过逆光效果，囚室之中的疯人、病人或犯人的活动，则可以直观地呈现于监视者眼前，而被囚者却无法得知自己是否正在被监视。这体现了边沁的一个原则：“权力应该是可见的但又是无法确知的。”在福柯看来，现代社会图景，正是一个遍布这样“全景敞视监狱”形象的规训机制的社会，在这样的机制中，个体从身体、行为到主体均被驯化和塑造。

然而，人类的历史同样是一部反抗权力的历史，就像贵族阶级与酷刑终究在全世界的绝大多数地方成为过去，被驯化也总是伴随着反抗。

在今天，随着移动互联、大数据、虚拟现实、人工智能、人机交互等新兴技术的介入，个体被定义、被驯化的程度似乎更深了，但这并不意味着没有反抗的可能。人类不仅在生产力上改变着世界，也必将在生产关系上改变世界。

区块链就是最好的明证，它将突破层级性权力对个体的侵扰，突破“检查”对隐私的侵犯，并最终突破传统世界“层层嵌套的金字塔”，使人类成为全新的“游牧民族”，根据需要自由行动。类似的意图，中本聪早已在白皮书中进行说明。

这样的区块链，这样的中本聪，又怎能被低估呢？

> major effect of the Panopticon:to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power."
>
> (Michel Foucault)

Science Interpretation

科学解读

EN-TAN-MO

“

AGREED VALUE SHARED BENEFIT

”

信息，熵与均衡：一种区块链的数学物理观点（I）

在以下的几篇文章中，我们将从统计力学、概率论和数据分析、信息论、最优化和理性预期经济学等角度出发，对作为去中心化系统的区块链进行一系列的分析和解读。之所以称我们采用的是数学物理观点，是因为我们的核心模型中的概念包括熵、均衡、最优化，其中的论证也利用了一系列的数学工具。我们将分析一些经典的区块链体系（以比特币为主），并提出建立在科学分析基础上的新方案。

区块链是由两个看似相互矛盾的概念作为基础的：去中心化与共识机制。具体则需要在工程学层次以博弈论机制设计的方式来实现。本文我们将讨论如何以权益概率分布对应的玻尔兹曼熵作为去中心化和安全性的度量和研究工具。

1. 作为去中心化度量的熵

在玻尔兹曼统计力学中，用 $f(t,x,v)$ 表示微观粒子在 t 时刻对应位置和速度 x ，v 的概率密度函数，利用公式 $S=K\log W$ 及排列组合方法，玻尔兹曼得出了 H 泛函：

$$S(f)=-H(f):=-\int_{\Omega_x\times\mathbb{R}^3_v} f(x,v)\log f(x,v)dvdx$$

在粒子概率分布满足 $f(t,x,v)$ 的稀薄气体模型中，$S(f)$ 表示系统对应的熵。熵被用来在物理学上描述系统的无序程度。玻尔兹曼提出并证明了著名的 H 定理，即随着粒子的相互碰撞（由玻尔兹曼方程描述），系统的熵会随时间不断增加直到一个均衡状态，即

$$\frac{d(S(f))}{dt}\geq 0$$

这一结论对应于热力学第二定律（无序程度必然增加，或时间不可逆定律）。

（奥地利物理学家）Ludwig Von Boltzmann

在 Claude Shannon① 提出的信息论中，熵被用来作为信息，或者说不确定性的度量，在概率密度函数存在的情形下

$$S=-\int f\log f$$

如果随机变量的概率分布在一些离散的点 $(x_1,x_2,...,x_n)$，$P(X=x_i)=p_i$，则

$$S=-\sum_{i=1}^{n} p_i\log p_i$$

在离散分布的前提下，如果概率集中在一个点，即存在 i 使得 $P(X=x_i)=1$（或者称分布律为 $\delta(x_i)$），则 $S=0$。可以证明，熵最大的分布对应的是均匀分布，即对任意 i，$P(X=x_i)=\frac{1}{n}$。由此可以看到，熵可以被视作不确定性或者概率分布均衡性的一种度量。

例如，在没有热源的条件下，考虑一个区域内分子的扩散，用 $f(t,x)$ 表示分子的概率分布，在分子运动服从布朗运动 ② 的前提假设下，$f(t,x)$ 应当满足热传导方程

$$\partial_t f-\Delta f=0, f(0,x)=f_0(x)$$

分子的分布（对应于热量分布）区域均衡状态可以给出一个简单的证明，玻尔兹曼熵对时间的导数就是统计学中著名的 Fisher 信息：

$$\frac{dS(t)}{dt}=-\int\frac{d(f\log f)}{df}\partial_t f dx=-\int(\log f)\Delta f dx=\int\nabla(\log f)\cdot\nabla f dx=$$

$$\int\frac{|\nabla f|^2}{f}dx>0$$

关于信息论的起源，Shannon 说：我本来想把这一概念称为“信息 (information)”，但是这个名字已经被滥用了，之后我又想称它为“不确定性 (uncertainty)”。

---

① 克劳德·艾尔伍德·香农（Claude Elwood Shannon，1916.4.30—2001.2.24）美国数学家、信息论的创始人，提出了信息熵的概念，为信息论和数字通信奠定了基础。

② 指微小粒子或者颗粒在流体中做的无规则运动。公元 1827 年，英国植物学家罗伯特·布朗利用一般的显微镜观察悬浮于水中由花粉所迸裂出之微粒时，发现微粒会呈现不规则状的运动，因而称它布朗运动。

当我与 Von Neumann① 讨论时，他建议我称其为“熵”，因为：

1. 这种不确定性已经在统计物理学中被考虑过，因此已经有一个名字；

2. 更重要的是，没有人确切地知道熵到底是什么，所以你总能在辩论中占有优势。

在热力学中，在动量守恒和能量守恒的前提下，熵最大的分布成为 Boltzmann-Gibbs② 分布，它对应的是热力学中的均衡状态。热力学均衡状态即对应这样一种概率分布 μ，使得系统的熵不再增加：

$$\frac{d(S(\mu))}{dt}=0$$

熵作为不确定性度量的思想在当代的数学工作中被用于证明概率论中经典的中心极限定理：

设 $X_1, X_2, ..., X_n, ...$ 为一系列独立分布的随机变量，且数学期望和方差满足 $\mathbb{E}[X_n]=0, \mathbb{D}[X_n]<\infty$，则 $\frac{\sum_{n=1}^{N} X_n}{\sqrt{N}}$ 当 $N\to\infty$ 时依分布收敛于一个高斯分布随机变量。

（信息论之父）Claude Shannon

英国统计学家 Galton 如此评价中心极限定理的哲学意义（或许我们也可以这样描述加密货币的数学原理）：

The law would have been personified by the Greeks and deified, if they had known of it. It reigns with serenity and in complete self-effacement, amidst the wildest confusion. The huger the mob, and the greater the apparent anarchy, the more perfect is its sway. It is the supreme law of Unreason. Whenever a large sample of chaotic elements are taken in hand and marshalled in the order of their magnitude, an unsuspected and most beautiful form of regularity proves to have been latent all along.

“如果古希腊人知道这一定律，则一定会将其奉为神明。它在一个最为狂野的混乱中以沉静的姿态统治着世界。无秩序程度越高越明显，这一法则的统治就越完美。它代表了非理性的最高法则。当一系列表面混沌的因素被聚集在一起时，一种令人意想不到而极为优美的规则性却被证明被暗含其中。”

Artstein-Ball-Barthe-Naor 在 2004 年证明 ③：随着随机变量的增加伴随着信息的衰减（不确定性的增加），即 $Ent\left(\frac{\sum_{n=1}^{N} X_n}{\sqrt{N}}\right)$ 随着 N 的增加而增加。同时可以容易地证明，在数学期望和方差的约束条件下，熵最大的分布对应的是高斯分布。

SOLUTION OF SHANNON'S PROBLEM ON THE MONOTONICITY OF ENTROPY

SHIRI ARTSTEIN, KEITH M.BALL, FRANCK BARTHE, AND ASSAF NAOR

1. INTRODUCTION

The entropy of a real valued random variable X with density $f:\mathrm{R}\to[0,\infty)$ is defined as

$$\mathrm{Ent}(X)=-\int_{\mathrm{R}} f\log f$$

provided that the integral makes sense. Among random variables with variance 1, the standard Gaussian G has the largest entropy. If X_i are independent copies of a random variable X with variance 1, then the normalized sums

$$Y_n=\frac{1}{\sqrt{n}}\sum_{1}^{n} X_i$$

approach the standard Gaussian as n tends to infinity, in a variety of senses.

In the 1940's Shannon (see [6]) proved that $\mathrm{Ent}(Y_2)\geq\mathrm{Ent}(Y_1)$: that is, the entropy of the normalized sum of two

和二十世纪早期利用傅立叶变换 ④ 的证明不同，这一类新的利用信息论思想的证明是完全直观的，并

---

① 约翰·冯·诺伊曼（John von Neumann，1903.12.28 – 1957.2.8），出生于匈牙利的美国籍犹太人数学家，现代电子计算机与博弈论的重要创始人，在泛函分析、遍历理论、几何学、拓扑学和数值分析等众多数学领域及计算机学、量子力学和经济学中都有重大贡献。

② 玻尔兹曼分布，也称为吉布斯分布，是系统中的粒子在各种可能微观量子态的概率分布、概率测度，或频度分布。

③ 参见 *AMS*（美国数学学会）电子期刊 J. Amer. Math. Soc. 17 (2004), 975–982, Shiri Artstein, Keith M. Ball, Franck Barthe and Assaf Naor 发表于 2004 年的论文《*Solution of Shannon's problem on the monotonicity of entropy*》。

④ 傅里叶变换 Fourier transform）是一种线性积分变换，用于信号在时域（或空域）和频域之间的变换，在物理学和工程学中有许多应用。因其基本思想首先由法国学者约瑟夫·傅里叶系统地提出，所以以其名字来命名以示纪念。

充分说明了中心极限定理为何在热力学及信息论等领域占据核心的地位，以及高斯分布与热力学均衡状态之间的关系。

在经济物理学及 Pierre Degond 等人提出的 Kinetic mean field games 理论中，热力学中的均衡及 Gibbs 分布可以被用来描述某些特定的金融模型中的 Nash 均衡状态。

由前述可知，熵可以作为大范围网络系统中去中心化程度的度量。假设有一系列节点 $(x_1, x_2, ..., x_n)$，用 $P(X = x_i) = p_i$ 表示每个节点 i 所分布的算力或权益，则 $S = -\sum_{i=1}^{n} p_i \log p_i$ 越大就表示去中心化程度越高，同时系统的下一个出块节点具有更大的不可预测性。由此 S 可以描述系统的均衡性及安全性。同时，当节点数目 n 增大时 S 也很可能有增加的趋势，这对应着节点的增加可以自动地提高系统的稳定性和安全性而无需更新昂贵且易受攻击的中心化安全体系。

事实上，在中本聪的论文中，其数学模型的理论基础是算力基本呈均匀分布，这样才对应着下个出块节点的不可预测（最先得到 Hash 结果的节点的最大不可预测性）。同时，只有相对的算力分布稳定性才能确保中本聪关于区块序列为同质 Poisson 分布①（Homogeneous Poisson Distribution）的假设成立。关于出块节点身份和顺序的可预测性越低，系统则越安全。因此，比特币系统的安全性建立在算力分布熵原理的基础上，而与算力的大小没有直接关系。在最大熵的前提假设下，比特币可以实现去中心化（公平）和安全性的统一，这也是中本聪的比特币设计思想的天才之处。

在合理的机制设计中，随着节点数量的增多和权益的扩散及流动，信息的公开和共享，系统的算力和权益及他们的运动速度会趋近于一种均衡稳定的状态，对应于热力学中的 Gibbs 分布。以此来实现去中心化和安全性的统一。

在 Shannon 信息论中与熵相关的另一个概念是相对熵（relative entropy), 或称为 Kullback-Leibler 距离。设 μ 和 ν 为概率空间的两个不同测度（概率分布），f 表示两者之间的 Radon-Nikodym 导数，即 $f = \frac{d\mu}{dt}$，则

$$H(\mu|\nu) = \int \log \frac{d\mu}{d\nu} d\mu$$

可以证明，$H(\mu|\nu) \geq 0$，$H(\mu|\nu) = 0$ 当且仅当 $\mu = \nu$ 但 $H(\mu|\nu) \neq H(\nu|\mu)$ 即不具有对称性。由此可见，Kullback-Leibler 距离可以用来作为两种概率分布之间差别的度量，因此在数据分析和机器学习中有着极为广泛的应用。例如，统计学中经典的极大似然估计可以等价于计算使得目标概率分布与对样本随机试验得到的经验概率分布之间的 Kullback-Leibler 距离最小的参数设置。

从区块链的角度看，算力及权益的分布离均衡状态越远，可以从数学上理解为其概率分布于 Gibbs 均衡分布之间的 Kullback-Leibler 距离，这将导致系统稳定性的降低，分叉出现的可能性加大，因此，在熵和 Kullback-Leibler 距离的基础上建立的数学分析工具将有助于我们回答两个问题：

1. 加密货币（特别是比特币及其他基于算力证明 PoW 的系统）价格下跌是否会损坏其安全性?

2. 算力的集中，特别是个别 51% 算力在个别寡头集团的集中是否会导致加密货币不再安全?

在比特币白皮书中，中本聪未曾也不可能证明比特币的绝对安全，因为绝对安全本身就是不存在的。中本聪所做的是用一系列经典的概率和随机分析方法建立模型证明在一系列假设的前提之下，一系列恶意节点联合作弊成功的概率非常之小，小到几乎可以忽略不计的程度。而所谓的 51% 算力假设是这个模型的基本假设之一。

即使 51% 的假设失效，也只能认为中本聪的数学模型不再能够与现实相符合，恶意节点作弊成功的可能性增加，而不是系统就一定会被立即击溃。

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8];

p = probability an honest node finds the next block

q = probability the attacker finds the next block

q = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & if\ p \leq q \\ (q/p)^z & if\ p > q \end{cases}$$

《比特币：一种点对点式的电子现金系统》中本聪

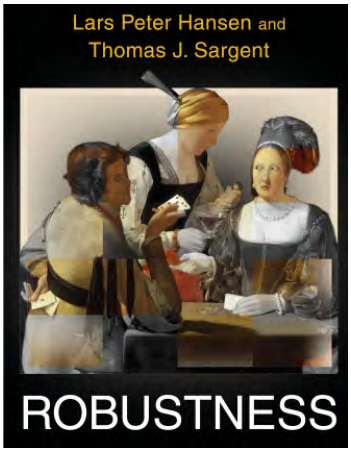
“Bitcoin: A Peer-to-Peer Electronic Cash System”：51% 算力安全性假说的起源，$p > q$ 即诚实节点的算力总和超过恶意攻击节点。

因此，对区块链系统安全的精细刻画，不应当执着于 51% 诚实算力假设，而应当以算力和权益实际分布（经验概率测度）与均衡状态分布的 Kullback-Leibler 距离的计算基础上建立全新的数学定量分析方法。

---

① Poisson 分布（Poisson Distribution) 是一种统计与概率学里常见到的离散概率分布，由法国数学家西莫恩·德尼·泊松（Siméon-Denis Poisson）在 1838 年时发表。Poisson 分布适合于描述单位时间内随机事件发生的次数的概率分布。

Kullback-Leibler 距离在金融中的应用主要来自于以诺贝尔经济学奖获得者 Thomas Sargent 和 Lars Hanson 为代表的理性预期经济学派，特别是他们合著的《Robustness》一书。在这本书中作者从熵和 Kullback-Leibler 距离的概念出发，将控制理论的观点和方法应用在经济学和金融模型分析中，提出了“模型误差分析”(model misspecification) 体系。



Sargent 与 Hanson 合著（Robustness）

理性预期经济学的几个核心观点包括：

1. 经济模型就是概率分布模型加随机过程；

2. 个体的经济行为不仅受现实客观因素的影响（如市场变化过程和实时价格），还在很大程度上取决于对未来的预期（如未来价格的变化趋势）；

3. 这种预期是可以用概率和随机的方法被代入模型作为参数被分析和使用的。

在 2008 年金融危机爆发后，数理经济学（计量经济学）受到了大量的质疑和批评，许多学者认为复杂的金融衍生品模型是造成危机的罪魁祸首。另一些人指出，在表面复杂的数学推演背后，数理经济学的一系列基本假设并不具有物理学那样的严密性且很难被检验。《科学》杂志发表了一系列文章，其主题为“经济学需要一场科学革命”：直接批评经济学和金融数学工具在现实面前的失败。在面对这些批评时，Sargent 一方面坚持数理经济学的核心思路，认为数学模型可以从根本上帮助人们理解经济运行的基本规律，同时提出了一系列新的观点。他曾对我们说：

“现代金融数学模型的核心问题是：他们都假设人是完全理性的，总是作对自己有利的选择。这明显不对。金融数学的进步需要能够模拟人的非理性行为和误判。这种模型的构建需要在一个严密的数学基础上进行，因此我利用 Kullback-Leibler 距离去模拟这种非理性。”

Sargent 与 Hanson 在《Robustness》一书中引用法国作家纪德的话：

“相信那些追求真理的人。怀疑那些自称找到了真理的人。”

“Croyez ceux qui cherchent la vérité, doutez de ceux qui la trouvent.”

最早关于 “model misspecification” 的讨论，可见于古希腊哲学家柏拉图的著作《理想国》，其中有一段苏格拉底与色拉叙马霍斯的对话 ①：

苏：我想，你不是说了吗，服从统治者是正义的？

色：是的。

苏：各国统治者一贯正确呢，还是难免也犯点错误？

色：他们当然也免不了犯错误。

苏：那么，他们立法的时候，会不会有些法立对了，有些法立错了？

色：我想会的。

苏：所谓立对了的法是对他们自己有利的，所谓立错了的法是对他们不利的，你说是不是？

色：是的。

如果“服从统治者是正义的”，那么所谓的正义就是强者的意志，但是强者往往并不知道自己真正的利益所在，他们的行为可能是非理性的，他们会误判形势，违背自己的真正利益。

2. 熵与黑天鹅

在金融体系中，我们有时需要将注意力集中在小概率事件（偶发事件）上。例如，保险公司在建立数学模型时，关注的重点是大宗理赔发生的概率。即使保险公司在大概率情况下保持很高的利润率，一旦大宗理赔突然发生就有可能将其推入破产的境地（例如 2008 年金融危机导致 AIG 保险公司濒临破产，同时期雷曼兄弟公司倒闭）。

同样，在区块链体系中，同一个节点（或一小部分作弊节点的集合）能够连续获得上传区块的权力的概率是非常之小的，但是这样的事件一旦发生就会造成极其严重的后果（账本被篡改的可能性提高），对一个区块链体系的安全性和声誉造成毁灭性的打击。

① 参见柏拉图《理想国》P3-42。

这类偶发事件又被称为“黑天鹅事件”。

由此产生了一个重要的数学分支：大偏差理论（Large deviation theory)。这一理论起源于瑞典数学家Harald Cramer在保险公司破产问题及精算方面的研究。

大偏差理论的核心定理出现在 1957 年，被称为 Sanov 定理。我们可以对 Sanov 定理作一个直观的描述。

令 $X_1, X_2, ..., X_n$ 为一系列独立分布的随机变量，概率测度记为 μ，而 $x_1, x_2, ..., x_n$ 表示经验随机变量的取值，因此经验分布

$$\hat{\mu}^N := \frac{1}{N}\sum_{i=1}^{N}\delta_{x_i}$$

则概率

$$P[\hat{\mu}^N \simeq v] \sim e^{-NS(v|\mu)}$$

根据大数定律和中心极限定理，当 N 增加时，经验分布将收敛到 μ，如果我们将 v 视为一种与作弊成功相关的其他概率分布，则可以理解为 v 对应的事件发生的概率（如作弊成功的概率）将决定于 $S(v|\mu)$，即 v 与 μ 之间的 Kullback-Leibler 距离。这一结果显然符合这样的直觉：一个概率分布与均衡状态的概率分布（极限分布）相差越大，则其所对应的随机事件发生的可能性越小。

О вероятности больших отклонений случайных величин

И. Н. Санов (Москва)

Проблема определения вероятности больших отклонений случайных величин привлекает к себе постоянное внимание. Имеется целый ряд важных исследований, посвященных этому вопросу. Из этих работ прежде всего следует назвать работы Н. В. Смирнова [1], Г. Крамера [4], В. В. Петрова [5] и ряд других. Тесную связь с этой задачей, как оказывается, имеют задача вероятностной оценки больших отклонений эмпирической кривой распределения случайной величины $ после N независимых наблюдений от теоретической кривой распределения,

Sanov 从大偏差理论出发得出熵的纯粹概率论定义

关于苏联数学家 Sanov 的生平我们知之甚少。在他 1969 年去世时的纪念文章中仅对其数学工作作了简要回顾。从俄罗斯一些卫国战争纪念资料库里我们得知，Sanov 1940 年在莫斯科取得博士学位后，很快作为工程师参加了第二次世界大战，利用其在概率领域的知识参与并解决了炮兵弹道校准问题，曾参加莫斯科保卫战，布达佩斯围攻，解放巴尔干半岛和柏林之战，获得了红星勋章和解放柏林勋章等重要荣誉。在朝鲜战争期间他又作为苏联顾问领导了金日成大学的数学系筹备组建工作。回到莫斯科后，他开始专注于概率论中大偏差理论这一方向，同时与苏联国家安全机关合作进行了多项军事背景相关研究。

Определение 5. Энтропией функции распределения Φ(л:) случайной величины на интервале [0,1] назовем двойной предел

$$E(\Phi) = -\lim_{\substack{\varepsilon\to 0\\ \varepsilon>0}}\lim_{N\to\infty}\frac{\ln P(\sup|F_N - \Phi| \le \varepsilon)}{N}$$

Из теоремы 13 следует, что

$$E(\Phi) = \int_0^1 \ln\frac{d\Phi}{dx}d\Phi$$

В случае, когда $\Phi(x)$ имеет непрерывную производную $\Phi'(x) = p(x)$,

$$E(\Phi) = \int_0^1 p(x)\ln p(x)dx$$

Нетрудно проверить, что энтропия, если она существует, будет неотрицательной. $E(\Phi) = 0$ тогда и только тогда, когда $\Phi(x) = x$, $p(x) = 1$.

Определение энтропии, даваемое обычно для других интервалов, не имеет, по-видимому, такого простого вероятностного смысла.

(Поступило в редакцию 24/11 1956 г.)

Sanov 从大偏差理论出发得出熵的纯粹概率论定义

作为苏联概率论学派的成员，Sanov 本身研究的目的在于对中心极限定理进行推广，而并未提及玻尔兹曼统计力学或任何物理背景。但他得出了熵和相对熵（relative entropy, 或 Kullback-Leibler 距离）的另一种定义方式。通过对小概率事件的描述，这个体系所得出的系列结论和玻尔兹曼统计力学及 Shannon 的信息论完全符合，并被广泛应用到物理和金融理论中。Sanov 作为一名苏联数学家，他的研究成果却在现代金融体系和华尔街的金融建模中得到了广泛应用。这正类似于康托罗维奇最优输运的工作。

在作家索尔仁尼琴的小说《第一圈》(В круге первом) 中，他曾写过这样的故事：一个叛变的苏联外交官向莫斯科的美国大使馆打去匿名电话通告苏联间谍获取美国核机密的信息，斯大林亲自下令彻查，苏联 KGB 首脑 Abakumov 集合其一些被逮捕接受改造的数学家，利用傅立叶分析和信息论的方法分析声音的来源。

在信息论诞生的同一时期，一门新的科学发展起来了：博弈论 (game theory)，同时 Nash 均衡的概念兴起。什么是博弈论，Nash 均衡和热力学均衡是否有某种联系，这些概念又将如何帮助我们理解去中心化的网络系统和构建全新的区块链结构，请看：信息，熵与均衡：一种区块链的数学物理观点（II，III）。

信息，熵与均衡：一种区块链的数学物理观点（II）

By definition, there is nothing to be changed in a model,
It works to perfection while as we can see very well,
It is reality where nothing works and all goes to pieces.
Italo Calvino: “modello dei modelli.”

区块链是由两个看似相互矛盾的概念作为基础的：去中心化与共识机制。具体则需要在工程学层次以博弈论机制设计的方式来实现。在上一篇中，我们讨论了如何以权益概率分布对应的玻尔兹曼熵作为去中心化和安全性的度量和研究工具。在这一篇中，我们重点讨论作为均衡的共识机制，稳态结构在去中心化系统中产生的原因和方式。

1. 平均场与 Mckean-Vlasov 模型

当我们把区块链看作大量节点所形成的去中心化系统时，需要解决这样的理论问题：这个系统中的信息是如何传播的，节点之间如何进行互动和形成一致，如何避免分叉结构和如何进行机制设计以避免恶意节点的攻击等。为了解决这些问题，我们需要回到物理学和数学，进行模型的重新构造。

混沌散播 (propagation of chaos) 的概念首先由美国统计物理学家 Kac 提出，在法国数学家 Alain-Sol Sznitman 的工作中建立了完整的理论体系并从此被广泛应用在物理、数学和经济学等领域。这一理论的最早动机在于构建一个严密的描述粒子运动的方程体系，建立不同的动能方程组 (kinetic equations) 之间的统一性理论。一方面当时已经有 Liouville 方程：

$$\partial_t u + \sum_1^N v_i \partial_{x_i} u + \sum_{j\neq i} -\nabla V_N(x_i - x_j)\partial_{v_j} u = 0$$

其中 $u(t, x_1, v_1, ..., x_N, v_N)$ 表示在 t 时刻，N 个对称粒子的联合概率密度函数，其中第 i 个粒子具有位置 x_i 和速度 v_i 。$V_N(\cdot)$ 表示粒子相互之间的势能作用。

另一方面对于稀薄气体的玻尔兹曼方程：

$$\partial_t u + v\cdot\nabla_x u = \int_{\mathbb{R}^3\times S_2} (u(x,\bar{v})(u(x,\bar{v}'-u(x,v)u(x,v'))\,|\,(v'-v)\cdot n\,|\,dv'dn$$

其中 n 表示方向，速度 $\bar{v}$ $\bar{v}'$ 与 v v' 满足如下条件（表示粒子之间碰撞所导致的速度变化与动量守恒）：

$$\bar{v} = v + (v'-v)\cdot n$$
$$\bar{v}' = v' + (v-v')\cdot n$$

$u(t,x,v)$ 表示在 t 时刻，位置 x 和速度 v 所对应的概率密度函数。

混沌散播是指，当粒子之间具有对称性，且 $N\to\infty$ 时，可以将其中任意的 k 个粒子看作是相互独立的。

Sznitman 在 1991 年提出了著名的定理，我们略去技术型的前提条件，其结论可以简述为：

$$\lim_{N\to\infty} \mathbb{P}(\bar{X}_1^N(\tau) = i_1, ..., \bar{X}_k^N(\tau) = i_k) = \mu_{i_1}(\tau)...\mu_{i_k}(\tau),$$
$$P(X_1^N(t) = i_1, ..., X_k^N(t) = i_k) \approx \mu_{i_1}(\frac{t}{N})...\mu_{i_k}(\frac{t}{N}),$$

通俗地说，不同粒子的随机运动之间显然是不相互独立的（粒子的碰撞和势能作用），但是当它们具有相互对称性且数量足够多时，这些粒子的整体概率分布将形成一个平均场，我们可以忽略任意有限个粒子之间的相互作用，而直接研究这一整体概率分布对单一粒子的作用。我们可以通过著名的 McKean-Vlasov 模型来说明。如果用 W_t 表示维纳测度，$X_t^{i,N}$ 表示在 t 时刻，N 个对称粒子第 i 个的位置，b 表示粒子间的相互作用，则这个粒子系统的动力学行为可以用一个建立在牛顿力学基础上的常微分方程组来表达：

$$dX_t^{i,N} = dW_t^i + \frac{1}{N}\sum_{j=1}^N b(X_t^{i,N}, X_t^{j,N})dt, i = 1, ..., N$$
$$X_0^{i,N} = X_0^i.$$

在这个方程组里，粒子之间的相互作用 $\sum_{j=1}^N b(X_t^{i,N}, X_t^{j,N})$ 显然是非常复杂的。因为要考虑到所有其他的粒子对第 i 个粒子的作用。而利用混沌散播定理可以建立一个平均场模型，由于粒子的对称性，我们可以任意选取一个并描述它的动力学行为：

$$dX_t = dW_t + \int b(X_t, y)u_t(dy)dt\ ,$$

$u_t(dy)$ ，$X_{t=0} = X_0$ 表示 X_t 所对应的概率分布测度。

u 可以用如下的 Fokker-Planck 方程描述：

$$\partial_t u = \tfrac{1}{2}\Delta u - \nabla\cdot(\int b(\cdot, y)u_t(dy)u)$$

每一个粒子所受的作用可以看作来自一个总体的“场”，决定于系统的概率分布随时间的演化。而描述这一演化过程的 Fokker-Planck① 方程模型，又可以从单个粒子的动力学行为得到。因此，混沌扩散是解释

① 福克 - 普朗克方程 (Fokker – Planck equation) 描述粒子在势能场中受到随机力后，随时间演化的位置或是速度的分布函数。此方程以荷兰物理学家阿德历安 · 福克与马克斯 · 普朗克的姓氏来命名。

微观和宏观规律之间关系的关键一步。由此可以从单个粒子的牛顿力学模型推导出宏观的玻尔兹曼方程，流体力学中的 Navier-Stokes 方程等等。 在平均场对策论中，通过 Mckean-Vlasov Fokker-Planck 方程所求得的分布对应于经济学中的帕累托最优。

系统整体的演化规律蕴含在个体的动力学行为中这一方法，可以用已故著名物理学家张首晟教授最喜欢的一首诗来解释：

一花一世界，一沙一天国

君掌盛无边，刹那含永劫

To see a world in a grain of sand, And a heaven in a wild flower, Hold infinity in the palm of your hand, And eternity in an hour.

————William Blake - Auguries of Innocence

而中国古代的佛教经典中，也恰好有“一花一世界，一叶一菩提”的表达。

2. 平均场对策论与理性预期经济学

物理学中的一个核心问题，就是大量粒子随机运动，相互作用，如何自发地形成规律性的宏观结构。经济学中对应的问题就是，大量的经济个体（理性人）之间复杂的相互作用如何形成价格体系。在平均场模型和混沌散播的理论基础上，法国数学家和经济学家提出了平均场对策论，对于这一问题给出了数学解释。

我们可以用一个简化的区块链挖矿模型来说明平均场对策论的基本原理和应用。假设一个纯工作量证明（PoW）的区块链，里面有 N 个行为模式完全相似（具有理性预期行为）的矿工。矿工通过投入算力进行哈希计算获得上传区块的权利，从而获得代币奖励。将第 i 个矿工所投入的算力记为 c_i ，算力投入需要满足限制条件 $c_i \in A$ 。这一矿工的目标是将挖矿收益最大化，而他的收益取决于他使用的算力成本和其他矿工的算力成本，因此他所采用的理性策略是：

$$\hat{c}_i := \arg\max_{c_i \in A} J(c_1, \cdots, c_N) = J(c_j; \frac{1}{N-1} \sum_{1 \le j \ne i \le N} \delta_{c_j}).$$

单个矿工收益函数显然随着他自身算力投入的增加而增加；同时，又决定于其他矿工的算力投入，因为区块链底层算法决定了当总的算力增加时，单个矿工将更难获得挖矿收益。这里的收益需要考虑成本因素，即算力所消耗的资源。

假定每一个矿工都会进行收益和成本核算，动态地调整自身的算力投入，则系统将稳定在一种“纳什均衡”（Nash equilibrium）状态。这种均衡状态对应的是一个策略（算力投入）组合：对于任意的 $i \in \{1, \cdots, N\}$ ，

$$J^i(\hat{c}_1, ..., \hat{c}_i, ..., \hat{c}_N) \le J^i(\hat{c}_1, ..., \hat{c}_{i-1}, c_i, \hat{c}_{i+1} ..., \hat{c}_N),$$

或利用对策论中的常用方式，用 c_{-i} 表示除了第 i 个参与者之外，其他所有参与者的策略集合：

$$J^i(\hat{c}_i, \hat{c}_{-i}) = J^i(\hat{c}_1, ..., \hat{c}_i, ..., \hat{c}_N) \le J^i(c_i, \hat{c}_{-i}).$$

我们给出一个简化模型的例子说明目标收益函数 J^i 。在中本聪的比特币白皮书中论证了，由于单个参与者挖到下一个区块的概率具有马科夫性（在一个区块产生之后挖到下一个区块所需的时间和之前的历史无关），仅仅决定于在上一个区块已经产生后这个参与者 i 的算力投入和其他参与者的算力投入，因此在时间 $[0,T]$ 之间挖到 N 个区块的概率满足 Poisson 分布：

$$P(N(0,T] = n) = \frac{[\Lambda(0,T)]^n}{n!} e^{-\Lambda(0,T)}$$

这个 Poisson 随机过程的强度：

$$\Lambda(0,T) = \int_0^T f(c_i(t), c_{-1}(t))dt$$

其中 $c_i(t)$ 表示矿工 i 在 t 时刻的算力投入， $c_{-1}(t)$ 表示所有其他矿工在 t 时刻的算力投入所构成的组合。根据 Poisson 过程的性质，在这个时间段内矿工 i 预计能挖到的区块总数的数学期望为：

$$E[N(0,T]] = \sum_{n=0}^{\infty} nP(N(0,T] = n) = \Lambda(0,T)$$

我们也可以建立一个更复杂的模型，用一个跳跃扩散过程的随机微分方程模拟权证价值的变化，并拟合进上面的模型中。

即使在这样一个简化的模型中，纳什均衡策略仍然是复杂和难以计算的。其复杂性来自于对于每一个单独的参与者 i ，要在他的目标函数 J^i 中考虑到其他参与者的策略概率分布 ： $\Lambda(0,T)$ 依赖于 $\sum_{1 \le j \ne i \le N} \delta_{c_j}$ 。我们可以采用上一节所介绍的平均场均衡和混沌散播的方法。对于每一个参与者 i 而言，任意另外一个单独的参与者 j 所付出的算力成本（策略）对 J^i 的改变是可以忽略不计的。其他参与者作为一个总体，通过概率分布的形式影响挖矿难度和个体收益。因此，可以把任意有限个个体的策略概率分布看作是相互独立的，在这一独立性的基础上根据大数定律，当 $N \to +\infty$ 经验概率分布 $\sum_{1 \le j \ne i \le N} \delta_{c_j}$ 将会依概率收敛（弱收敛）到一个概率测度 μ 。以上的纳什均衡问题可以被转化为：

$$\hat{c} := \underset{c \in A}{argsup}\, J(c, \mu).$$

当 $N \to +\infty$ 时，纳什均衡可以不再被看作一个离散的策略组合，而变成一个策略集合的概率分布 $\hat{\mu}$ ，满足：

$$Supp(\hat{\mu}) \subset \underset{c \in A}{argsup}\, J(c, \hat{\mu}),$$

其中 $supp(\hat{\mu})$ 表示测度 $\hat{\mu}$ 的支撑集。纳什均衡可以同时表述为：

$$\int_A J(c, \hat{\mu})\hat{\mu}(dc) = \sup_{\mu \in \rho(A)} \int_A J(c, \hat{\mu})\mu(dc),$$

其中 $\rho(A)$ 表示在集合 A 上所定义的概率测度空间。

因此，对策论中的纳什均衡问题被转化为了一个概率测度空间中的不动点问题：首先给定策略（挖矿算力投入）的概率分布 μ ，研究最优化问题 $\underset{c \in A}{sup}\, J(c, \mu)$ 得到 $\hat{c}$ 的概率分布 μ' ，由此建立映射：

$$\mu' = \Phi(\mu),$$

当这一映射存在不动点 $\hat{\mu} = \Phi(\hat{\mu})$ 时，即得到了纳什均衡 $\hat{\mu}$ 。由此我们可以推断在追求自身收益最大化时，参与者所投入的算力成本收益分布，并进一步预测区块链权证的参考价值和成本。

自其诞生以来，平均场对策论受到了主流经济学界，特别是理性预期经济学派的关注。平均场对策论被认为能够革命性地发展这一学科方向，主要基于两个原因：

1. 经济学中存在两种不同的均衡概念之间的鸿沟：均衡与一般均衡 (general equilibrium)。均衡的概念，如 Nash 均衡，更多地存在于数理经济学之中，可以在简单的模型中进行严格的数学分析和计算。而一般均衡理论，更偏向于政治经济学，表示在经济体系和市场中的供求平衡关系。一般均衡理论长久以来被许多人视为一种自由市场经济意识形态，例如，这一理论的前提是价格机制可以调节市场，但是却无法给出较为严谨的价格形成（price formation) 数学模型。

2. 经济计算的复杂性问题。理论预期经济学的一个基本假设是，人们会将模型（概率分布）的信息代入决策过程中，而个体的决策过程的积累又可以反过来改变模型。由于经济个体的庞大数量和行为复杂性，这一类模型的相关计算会变得极为复杂。而在平均场对策模型中，个体不再是与其他个体之间进行博弈，而是与其他个体所形成的“平均场”之间博弈。这样可以极大地简化计算和分析。

3. 什么是好的共识机制

诺贝尔经济学奖 Lars Hansen 曾在其演讲“经济学与统计推断”中对于经济学模型做了这样的表达：

“人们都认为复杂的问题一定要有复杂的答案，其实恰恰相反，复杂的问题可以用非常简洁的模型来解答。”

一个“简单解答”的例子，就是中本聪和比特币。2008 年，正是金融衍生品理论发展的一个高峰时期，当各国的银行执着于发展复杂的金融安全和交易体系时，中本聪却用简单的概率模型设计了颠覆性的去中心化系统。

一个好的区块链机制设计应当是简单和复杂性的统一。从微观层面，每个节点的收益模式，动力学行为应当尽可能简单，具有牛顿力学三大定律一样的严格性。而在宏观层面，这个体系应当形成一种复杂、规律性和稳健性（robustness）的结构。这种稳定性应当符合大数定律，随着节点数量的增多而自然地加强。复杂的随机性（如区块产生节点的不可预测性）应当起到加强稳定的作用。

区块链的特点决定了其与平均场对策论和理性预期经济学的结合将极大地改变金融和能源市场等众多领域。区块链作为去中心化账本，本身具有公开性和可验证的特点。这意味着：

1. 在这一体系的每个参与者都可以接触到同样的信息，来用于自身的决策。这有助于解决目前金融市场信息不对称性问题，从而建立一个更为公平的体系。区块链可以实现信息公开和隐私保护的统一，交易个体的真实身份可以通过零知识证明等技术得到隐藏，但是交易本身的规模和流动性是公开的，可以被所有参与者验证和使用。

2. 参与者得到的信息是真实且接近实时的，因此在投资决策中可以不再依赖于各种中介机构，而使用新的数据分析算法得出合理的策略。平均场对策论对模型的简化将带来计算量的极大降低，再加上计算速度的更新和分布式计算方法的应用，经济个体分布式数据处理将成为可能。这将使得经济体系更为高效，同时减少交易和咨询费用，降低中介服务成本。

此外，区块链技术可以帮助解决贫困与可持续发展的问题。目前，分布式能源体系已经得到越来越多的重视，在偏远地区利用太阳能和风力发电并供应本地的能源需求，可以有效解决环境污染和能源短缺问题。分布式能源目前所面对的主要困难并非设备技术上的，而是经济学意义上的，如何有效连接大量分散的生产供应者与需求方。区块链技术可以构建一个有效的去中心化能源账本，由大量分布广泛的参与者根据价格波动及时地调整生产与需求，在供应者与购买者的身份中灵活转换。参与者可以利用体系中的权证进行期货交易，对冲市场需求和价格波动风险。

目前大银行和企业对金融服务的控制，不再是简单粗暴的垄断（monopoly），而是升级发展为了“宰制”（Hegemony）。“宰制”这一概念最早由意大利哲学家葛兰西提出，表示统治阶级对底层的压制不仅仅存在于生产关系上，而且是知识生产，思想观念和文化上的绝对优势和压制。华尔街的少数大银行和财团，不仅仅是垄断金融服务、利润和数据，还将金融数学变成了一门玄学，一门类似于中世纪修道院中的天文学的学科，以得到普通民众的信任和顺从。华尔街金融界占据了金字塔顶尖的资源，而普通民众犹如置身在柏拉图所描述的洞穴中，无法看到金融体系运行的真正规律和逻辑，只能看到受到操控的媒体所描绘的幻象的蒙蔽。大数据科学和人工智能，如果掌握在少数大公司、银行和财团手里，只会加剧这种控制和欺骗，而目前世界各国贫富差距的迅速增加正部分地源自于这种技术和数据的垄断。区块链与大数据的结合，可以称为对这种“宰制”的一种反抗和颠覆，它将带来一场金融和经济学的文艺复兴，真正实现数据和信息的“民主化”与“公开化”。这将是一场经济体系和经济科学的双重哥白尼式的革命。

以上我们讨论了作为区块链技术理论基础的去中心化与共识机制，在最后一篇中，我们将讨论如何运用我们所发展的理论工具在工程学层面改进区块链的机制设计。

信息，熵与均衡：一种区块链的数学物理观点（III）

在之前的两篇（上，中）里，我们分别阐述了区块链的去中心化逻辑和共识机制，并从数学物理的角度设计了新的分析方法。在最后一篇中，我们将解释我们如何在 ETM 项目的共识机制设计中引入数学物理方法，将均衡的观点落实在算法和工程学层面。

1. 基于纳什均衡的选举策略机制

我们的算法设计基于博弈论机制设计（mechanism design）和纳什均衡（Nash Equilibrium）的思想。我们假设每个参与者都是理性的，系统机制的设计将使得每个人采用使得自身利益最大化的策略，这也正是实现共识机制的策略。因此，节点受到激励服从共识机制。具体实现方法如下：

系统中假设有 N 个节点，分别记为 $x_1,...,x_i,...,x_N$，在任意时间 t 处，节点 x_i 被选中的概率为：

$$P(X=x_i)=\frac{(k_i+\epsilon)S(T_i\circ x_i(t))}{\sum_i^N(k_i+\epsilon)S(T_i\circ x_i(t))}$$

其中，$S(x_i(t))$ 表示节点 x_i 在 t 时刻的权益；

$T_i\circ x_i(t)$ 表示节点 x_i 在 t 时刻的权益依据时间系数所作的单调递增（随时间）映射，由代币锁仓时间决定；

k_i 表示在 t 时刻为止成功出块次数 n_i^* 与 n_i 的比值 $\frac{n_i^*}{n_i}$，实数 $\epsilon\in(0,1)$。

我们证明，对于每个节点，在获得上传区块权力时，其最优策略（Dominant strategy）将是按时出块并在其上传的区块中不包含任何虚假信息。其策略结合 $Y=\{0,1\}$，$\alpha_i=1$ 表示节点按时上传一个包含真实信息的区块，反之记为 $\alpha_i=0,$。

因为包含虚假信息的区块会被随后的节点否认，因此不计入成功上传记录。

设时间 t_k^i 表示节点 x_i 第 k 次获得上传区块的机会，$k>1$，设在之前的 $k-1$ 次机会中成功上传真实信息区块的次数为 $n_{i,k-1}^*$。

节点的收益函数应该考虑到采取策略时获得代币奖励的收益及成功上传记录的后续影响（理性预期）。

设：

$$u_i(t_k^i+)=\alpha_i\cdot r+crP(X=x_i(t_k^i+))$$

其中 r 表示上传区块获得的代币奖励，$r>0$，c 表示一个常数用来度量未来代币奖励的预期变化情况。我们需要分析节点 x_i 在 t_k^i 时刻的策略，由于此时根据共识机制上传区块的机会仅属于节点 x_i，因此可以认为当时间 t 从 t_k^i 变成 t_k^i+ 时，$\sum_{j\neq i}^N(k_j+\epsilon)S(T_j\circ x_j(t))$ 保持不变，要求得策略 α_i 使得：

$$u_i(t_k^i+;\hat{\alpha}_i,\hat{\alpha}_i^{-1})\geq u_i(t_k^i+;\alpha_i,\hat{\alpha}_i^{-1})$$

当 $\alpha_i=0$ 时：

$$u_i(t_k^i+;0,\alpha_i^{-1})=0+cr\frac{(\frac{n_{i,k-1}^*}{k}+\epsilon)S(T_i\circ x_i(t_k^i))}{\sum_i^N(\frac{n_{i,k-1}^*}{k}+\epsilon)S(T_i\circ x_i(t_k^i))}$$

当 $\alpha_i=1$ 时：

$$u_i(t_k^i+;1_i,\alpha_i^{-1})=$$

$$r+cr\frac{(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(T_i\circ S(x_i(t_k^i))+r)}{\sum_{j\neq i}^N(\frac{n_{j,k-1}^*+1}{k}+\epsilon)S(T_j\circ x_j(t_k^i))+(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(S(T_i\circ x_i(t_k^i))+r)}$$

我们作如下补充解释，如果节点 x_i 在时刻 t_k^i 采用策略 $\alpha_i=1$，则其权益增加到 $S(T_i\circ x_i(t_k^i))+r$，而其他任意节点 x_j，$j\neq i$ 的权益保持不变。此时节点 x_i 共获得 k 次上传区块的机会，成功上传的次数增加为 $n_{i,k-1}^*+1$。

设：

$$c_1=\sum_{j\neq i}^N(\frac{n_{j,k-1}^*+1}{k}+\epsilon)S(T_j\circ x_j(t_k^i))$$

则：

$$u_i(t_k^i+;0,\alpha_i^{-1})=0+cr\frac{1}{1+\frac{c_1}{(\frac{n_{i,k-1}^*}{k}+\epsilon)S(T_i\circ x_i(t_k^i))}}\cdot$$

$$\frac{(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(S(T_i\circ x_i(t_k^i))+r)}{\sum_{j\neq i}^N(\frac{n_{j,k-1}^*+1}{k}+\epsilon)S(T_j\circ x_j(t_k^i))+(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(S(T_i\circ x_i(t_k^i))+r)}$$

$$=\frac{1}{1+\frac{c_1}{(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(S(T_i\circ x_i(t_k^i))+r)}}$$

显然：

$$(\frac{n_{i,k-1}^*+1}{k}+\epsilon)(S(T_i\circ x_i(t_k^i))+r)>(\frac{n_{i,k-1}^*}{k}+\epsilon)(S(T_i\circ x_i(t_k^i)))\,,$$

且由前提条件 $r>0$ 可得：

$$u_i(t_k^i+;1,\alpha_i^{-1})>u_i(t_k^i+;0,\alpha_i^{-1})$$

因此 t_k^i 时刻节点 x_i 的最优策略为 $\hat{\alpha}_i=1$。

同时，由于时间系数映射“$T_i\circ$”设计为单调递增的函数，选举参与者可以通过增加锁仓时间来增大其选票所占的比重，或者其自有矿机被选中的概率。这种机制设计可以避免恶意参与者通过在短时间内获取大量权益在选举中取得较大优势的情况。

2. 基于大偏差理论的安全机制分析

现在我们转入每一周期选举产生矿工团队后安全性问题的数学分析。依照网络安全和可靠性分析的最差性原则，我们假设极端的情况，有接近 49% 的矿工有联合作弊的企图。

根据概率方法可计算出，在这一周期的 101 个矿工中实际能够被选中的矿工数量约等于：

$$101-101\times(1-\frac{100}{101})^{101}=66$$

这意味着部分矿工出块数量超过一次，事实上，每个矿工被选中的次数符合参数 $\lambda=1$ 的泊松分布（泊松定理，二项分布逼近于泊松分布），这个随机变量的数学期望等于 1。

假设作弊矿工会相互配合，只在内部团队成员的区块后面继续增加而忽略其他诚实矿工的区块，也就是说，这一团队希望通过分叉的方法，利用最长链原理在某一时刻取代诚实矿工的区块链，迷惑新加入的节点。我们可以通过大数定律和大偏差原理方法证明作弊者成功的可能性变得非常小。

$P(X_i=1)=0.49, P(X_i=0)=0.51$ ，

$E[\frac{1}{N}\sum_{i=1}^{N}X_i]=0.49$ ，

根据强大数定律，当 $N\to\infty$ 时，$\frac{1}{N}\sum_{i=1}^{N}X_i$ 收敛到其数学期望，现在考虑经过 101 次区块上传，作弊者占有的区块数量超过一半的概率（即其控制的链的长度得到优势地位）：

$$P(\sum_{i=1}^{N}X_i\geq 51)$$

根据 Cramer 定理可以计算，近似地

$$\frac{1}{101}\log(P(\sum_{i=1}^{101}X_i\geq 51))=-\Lambda^*(\frac{51}{101})$$

勒让德变换

$\Lambda^*(x)=\sup_t(tx-\Lambda(t))$ ，

$\Lambda(t)=\log E[e^{tX_i}]$.

3. 总结

ETM 项目提出的统一权益证明法（Unified Proof of Stake, UPoS），最大限度地试图结合算力证明和权益证明的优点，回归比特币的原始精神内核。我们在这里暂时回到对比特币的分析，我们认为比特币的精神在于利用去中心化，随机性（不可预测性）来实现安全性。所有节点都可以参与交易验证和区块的上传，而下一个上传区块的节点身份是不可预测的（取决于计算速度），这种随机性带来了安全性。同时，节点的算力投入成本将有助于激励其维护系统的声誉和稳定性。与此相类似的，ETM 的统一权益证明法具有如下的特点：

1. 节点通过选举进入矿工团队（包含 101 个节点），通过 Hash 计算上传区块，每一轮上传区块后要进行重新选举，上传区块的顺序随着上一个矿工的计算结果随机产生。因此，在这个体系中 Hash 计算将不再用于进行算力竞争，而是用于产生（下一个出块节点）的不可预测性，这将有助于保障节点无法协调作弊或攻击系统。

2. 由于 Hash 计算的用途改变，算力需求可以大大降低，避免消耗大量资源，但仍然可以动态调整以用于设置节点的参与成本，激励节点维护系统的稳定性以及预防女巫攻击。此外，交易处理速度极大地增加，从而提升系统的整体效率。同时，系统具有了极大的可扩容性，拥有了更多应用场景的可能性。

3. 在 ETM 的体系里，系统的扩容不仅成为可能，而且还可以被利用来进一步加强系统的安全性和稳健性。随着参与节点的增加，选举结果的不可预测性会进一步增大，增加攻击者的成本。

4. 权益通过上凸函数映射进行计算，可以使得权益的分布更接近于均匀分布（具有熵极大值的分布形式），从而在选举过程中加强去中心化，避免权证向少数参与者集中，以激励更多的参与者。

5. 将权证锁定时间和历史出块效率记录加入计算，而不仅仅是计算在某一时刻点权益的分布情况，这有助于更客观地将节点的贡献纳入选举时的评价标准，进一步激励节点按照共识规则采取行动。同时，这也有助于解决被选中节点不出块的问题，本质上是一种达尔文优胜劣汰的演化方法，使得系统具有更强的稳健性。同时，对节点历史行为的记录和分析将有助于防范女巫攻击。

6. ETM 特有的侧链技术和魔方协议，将解决目前区块链侧链技术面对的挑战：侧链独立性与同步性之间的矛盾。一方面侧链存在的主要目的之一是减轻主链的压力，因此应当具有较强的独立性；另一方面作为一个系统整体的组成部分，侧链和主链的账本信息需要保持同步。我们所开发的传输协议将在对主链保持较低压力的前提下解决同步问题。侧链技术的突破具有多重意义：整个 ETM 体系的效率得到极大提高；侧链可以被运用于开发各种去中心化应用场景（DAPP）；我们下一步尝试开发的新算法可以首先应用在侧链上，实现系统的自演进和更新。

我们所采用的共识机制，在保障安全性的基础上，极大地提高了效率与去中心化程度，有效地解决了这三者之间存在的“不可能三角问题”，构造了一个继承了比特币的精神内核，但比原始比特币算法机制更符合当前经济金融结构需求的区块链技术体系。同时我们也意识到，区块链技术决不能仅仅停留在理论研究的范围内，需要在实践中得到验证。因此，我们的项目团队已经对代码进行了多次内测和公测，针对出现的问题对共识算法和代码进行了相应的改进。主网的上线正式运行，将代表 ETM 的重要阶段性成功和一个新的开始。

附录

比特币精神与区块链技术革命

中本聪创造出比特币体系已过去十年，区块链技术经历了从单一的比特币到以太坊，EOS 等众多项目共存的过程。区块链的应用也从单一的去中心化账本过渡到了多样化的区块链应用。从 2017 到 2018 年，加密货币市场经历了一轮过山车式的震荡，公众对区块链技术的态度也从无知到热情又到怀疑。在当前的形势下，又出现了“回到比特币”和“回到中本聪”的思潮。我们首先要分析，什么是比特币的精神内核。

我们认为比特币的核心思想是：去中心化，稳健性 (Robustness，又称鲁棒性) 和建立在数学算法基础上的共识和信任体系。这三点之间又是紧密联系的。去中心化，意味着在算力分布基本均衡的前提下，账本的安全性是通过所有参与节点的算力充分竞争实现的。每个参与的节点都参与账本的验证并有相对公平的收益。去中心化可以保证稳健性，这意味着对系统不依赖于中心化的服务器，对外界的攻击具有很强的抵抗能力。而这种去中心化和稳健性都是在数学算法的基础上实现的，因此可以在账本体系中尽可能不依赖于人的因素建立起信任关系。在比特币中采用的算法是算力证明法 (Proof of Work), 节点通过算力消耗争取上传区块的权益并相互竞争。这种算力证明法 (PoW) 是实现去中心化和稳健性的手段而不是目的本身。

我们必须看到并承认：比特币与区块链技术正面临着严重的危机。大规模矿池的出现导致算力集中，比特币的算力战和分叉，中本聪圆桌会议讨论修改比特币总量等等问题，都在使得比特币偏离原有的宗旨。算力和收益的集中化与去中心化的思想背道而驰，而社区的各种论战和领袖人物主导的分叉决策表明比特币体系越来越建立在利益分配体系，个人偏好而非数学算法逻辑的基础上。正如同欧洲国家不断通过全民公决来进行重大决策，是一种民主失效的表现，比特币目前的发展越来越多依靠社区讨论也显示其原始的制度设计开始出现矛盾和危机。

在加密货币市场和区块链技术的发展出现危机时，不断地有人提出“回到比特币”，希望通过在比特币原始算法的基础上进行修改补充，加入零知识证明等，创造出新的改进的比特币方案。“回到比特币”思想的合理性基于两点：比特币在过去的成功经验和其数学算法的严格性。我们对这些合理性加以分析：

1. 比特币 PoW 算法在过去的成功不代表未来也能成功，特别是在其制度设计已经显现出危机的情况下。古希腊哲学家赫拉克利特曾说“人不能两次踏进同一条河流”，中国古代也有“刻舟求剑”的反面例子。现在的计算机硬件技术、矿机技术、公众和资本对区块链和加密货币的态度与过去十年不可同日而语。例如资本的大量涌入和矿池的结合对去中心化造成的冲击是中本聪创立区块链所不存在的假设，而算力需求的不断增加造成的巨大资源浪费也是中本聪所没有考虑过的。

2. 比特币的成功主要是在安全性方面，在去中心化与效率 (交易处理速度) 方面并不尽如人意，而且资源消耗问题越来越严重。比特币不断向大型的矿池集中，导致市场出现不稳定性和受操纵的可能。

3. 比特币的模型并不是纯粹的数学模型，其中包含了许多经济学论断，特别是在“Bitcoin: A Peer-to-Peer Electronic Cash System”的第 6 节“激励 (Incentive) ”中。中本聪强调当比特币的限定数量已经全部通过挖矿进入流通之后，交易费用将可以提供足够的流动性，从而可以避免整个体系的通货膨胀。这一模型的可行性是值得怀疑的，这也正是最近比特币增量辩论的起源之一。当一个矿池具有垄断性的算力和部分社区支持时，进行硬分叉会成为理性和有利可图的选择。

4. 数学算法的可靠性要基于其前提条件。数学的精确性是有条件的，每一个定理都有确定的前提条件和假设，而这些前提条件是不能通过数学本身证明的，而是需要通过对现实世界的分析来建立和验证的。在不断变化的现实世界中，这些前提条件也会受到考验。这一点从 LTCM(Long Term Capital Management, 长期资本管理公司) 团队的故事中可以看到。这个团队的交易策略是由 Robert Merton 和 Myron Scholes 亲自制定的，而以他们命名的 Merton-Black –Scholes 模型是量化金融中的经典模型。这个团队组建于 1994 年，在初期获得了丰厚的收益，却在第 5 年遭遇了投资策略失败和资产暴跌，濒临倒闭，其崩盘影响了整个美国金融市场。这一失败并非等价于 Merton-Black –Scholes 模型的数学错误。Merton-Black –Scholes 模型中的数学推导已经被数学家普遍认可为正确且严格的。但模型的数学严格性并不等价于模型本身的正确性。这一模型的问题在于它的一些前提条件与实际市场的运行方式产生了矛盾。与此相类比，在比特币出现分叉的现状下有可能出现巨型矿池拥有的算力超过 49% 的状态，这意味着中本聪算法的最重要假设也不能成立了。矿池的算力集中现象与比特币的分叉叠加，再考虑到新的算力证明区块链项目

不断出现，意味着在整个区块链体系里算力不断被分散，在某个单个的项目或分叉中完全可能出现单个节点垄断算力甚至超过 51% 的情形，这将导致安全性的完全失效。

因此，区块链技术的革命不能通过回到中本聪比特币的原始算法进行修补，而需要新的思维实现去中心化的金融生态系统。正如马克思在“路易 · 波拿巴的雾月十八日”中所说的：“黑格尔在某个地方说过，一切伟大的世界历史事变和人物，可以说都出现两次。他忘记补充一点：第一次是作为悲剧出现，第二次是作为笑剧出现。”“人们自己创造自己的历史，但是他们并不是随心所欲地创造，并不是在他们自己选定的条件下创造，而是在直接碰到的、既定的、从过去承继下来的条件下创造。一切已死的先辈们的传统，像梦魇一样纠缠着活人的头脑。当人们好像只是在忙于改造自己和周围的事物并创造前所未闻的事物时，恰好在这种革命危机时代，他们战战兢兢地请出亡灵来给他们以帮助，借用它们的名字、战斗口号和衣服，以便穿着这种久受崇敬的服装，用这种借来的语言，演出世界历史的新场面。”

面对比特币的缺陷和问题，人们提出了权益证明法（Proof of Stake）来作为算力证明（PoW）的替代。权益证明法的核心是，上传区块的权利不再通过算力投入而决定，而是由参与的节点在系统中所占的权益比例来决定。这种算法的优点在于不需要再进行消耗大量资源的计算，并可以提高效率（交易速度）。问题在于，如何选择代表节点？这里出现了几种极端，一方面是采用以 EOS 为代表的超级节点方案，把处理交易和上传区块的权力限制在少数的超级节点。这当然可以提高效率，但是明显违背了去中心化的本质，整个系统的安全性建立在了对超级节点信任的基础上。另一方面是以 Cardano, Algorand 为代表的普选方案，所有节点都可以参加，被选中的概率通过节点权益在整个系统中所占的比例决定。这一种方案的问题在于难以保证被选中的节点按时上传区块。同时，由于参与节点完全不需要投入算力成本，将导致作弊可能性增加。基于这些考虑，ETM 项目提出了统一权益证明法（Unified Proof of Stake, UPoS），最大限度地试图结合算力证明和权益证明的优点，回归比特币的原始精神内核。因此我们的共识设计与比特币相比较，应当看做继承和颠覆的统一：继承比特币精神，实现技术和算法上的革命。

References:

[1] S. Artstein, K. Ball, F. Barthe, and A. Naor. Solution of shannon’s problem on the mono- tonicity of entropy. Journal of the American Mathematical Society, 17(4):975–982, 2004.

[2] M. Benaim and J.-Y. Le Boudec. A class of mean field interaction models for computer and communication systems. Performance evaluation, 65(11-12):823–838, 2008.

[3] J.-P. Bouchaud. Economics needs a scientific revolution. Nature, 455(7217):1181, 2008.

[4] C. Cercignani. The boltzmann equation. In The Boltzmann equation and its applications, pages 40–103. Springer, 1988.

[5] R. L. Dobrushin. Vlasov equations. Functional Analysis and Its Applications, 13(2):115–123, 1979.

[6] R. S. Ellis. Entropy, large deviations, and statistical mechanics. Springer, 2007.

[7] L. P. Hansen and T. J. Sargent. Robustness. Princeton university press, 2008.

[8] A. Gramsci. Prison notebooks, volume 2. Columbia University Press, 1992.

[9] J. Monod. On chance and necessity. In Studies in the Philosophy of Biology, pages 357–375. Springer, 1974.

[10] S. Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[11] J. Nash. Non-cooperative games. Annals of mathematics, pages 286–295, 1951.

[12] C. E. Shannon. A mathematical theory of communication. Bell system technical journal, 27(3):379–423, 1948.

[13] A.-S. Sznitman. Topics in propagation of chaos. In Ecole d’´et´e de probabilit´es de Saint-Flour XIX—1989, pages 165–251. Springer, 1991.

[14] N. N. Taleb. The black swan: The impact of the highly improbable, volume 2. Random house, 2007.

Technical interpretation

技术解读

EN-TAN-MO

“

AGREED VALUE SHARED BENEFIT

”

En-Tan-Mo 技术解读

选择 ETM 轻松开发 DApp

1. Get your apps ready for the new world

对于开发者来说，区块链不仅仅是一种技术，它更是一种全新的思维方式，是一个公平的应用平台。

目前市场上的 App 乱象丛生，大企业垄断、应用不透明、肆意获取用户权限、滥用用户隐私。而通过继承了区块链优势的 DApp，用户可以以更安全透明有效的进行交易，而且还有可能发展为一种全新的互联网使用方式：完全掌控自己的隐私数据，而不是被那些垄断巨头所控制。这样具备了公开透明、可信可靠、去中心化的诸多特性的 DApp，弥补了传统 App 的众多缺陷，必将形成全新的生态模式。

伟大的技术不应只是少数人的玩具，而应让所有人都受益，这一切都离不开开发者们的努力。ETM 不仅致力于为开发者打造一个优质的高性能应用平台，一个开放的开发者社区和自演进区块链应用组件承载平台，一个打通金融、能源、商业、生活等生态环境和价值传递的新一代互联网平台。

2. ETM 让开发者能够轻松地构建和部署 DApp

主链 – 侧链机制

每一个 DApp 单独拥有一个完整的侧链，享有整个区块链的性能，而不受其他 DApp 影响。开发者不但可以继承和复用主链强大的区块链技术，还可以根据 DApp 需求高度定制化侧链的参数：Token、交易类型、共识机制、区块参数等等。这使得开发更为灵活，为 DApp 带来更多的可能性。

Node.js

使用世界上最常用的编程语言 JavaScript 作为原生语言，拥有数量最多的开发人员，最广泛的社区和开发者，可使用海量的第三方组件，极大地减轻了开发者的工作量，让小团队甚至个人开发者也能够轻松上手。

高性能

在保障安全性与功能的基础上，ETM 采用 UPoS 共识机制，大幅提高了主链性能，实现了 3s 出块，同时 TPS 达到了 1000笔/s，而且由于侧链之间相互独立，使得整体生态应用得以无限延展，实现 N*1000/s 的高性能 。因此对用户体验有较高要求的游戏 DApp 在区块链上真正运行起来，性能瓶颈也不再是开发者想象力的枷锁。

模块化

主链 – 侧链机制以及 Node.js 的使用，使得在 ETM 上开发 DApp 轻松灵活；而得益于完善的 SDK 与 API，进一步降低了开发成本。模块化的构架让开发者专注于 DApp 业务的实现，同时能够直接享受到主链以及侧链升级带来的种种便利，而不用对 DApp 作出任何修改。

开发零成本

愈加高企的开发运营成本让开发者开始抛弃 ETH 与 EOS 等平台，整个生态也因此陷入了恶性循环。ETM 从设计伊始就极力避免这种情况的发生，我们深知繁荣的应用生态与开发者社群才是 ETM 最宝贵的财富和持续发展的最根本因素。合作共赢的理念植入了 ETM 每一个环节，ETM 侧链机制让开发者能够根据需求动态调度资源，而系统仅出于安全的考虑，按交易收取低廉的手续费，并会通过活动与社区返还给开发者。

安全可靠

ETM 创造了纳什均衡的 UPoS 共识算法，PoW + DPoS 相结合的对偶共识，比起完全依赖算力的 PoW 共识，UPoS 无疑更加安全与高效。同时创造性地在 DPoS 中引入了混沌排序，抵抗女巫攻击和联合作弊，进一步提升了整个系统的安全性。而且侧链的开发也不会破坏主链或任何其他侧链。

可扩展性

优秀的可扩展性是所有分布式系统的必要条件。在 ETM 平台上，开发者能够轻松进行部署并扩充应用节点规模，甚至根据 DApp 的需求进行动态分配，而所有这一切都能够在 ETM 开发者平台上轻松完成。

开源

ETM 遵循 MIT 协议（The MIT License）开源，所有用户以及开发者可以在 GitHub 上查看所有代码，保证了系统的透明与安全。同时得益于开源，也让更多

的开发者加入 ETM 的建设中来，为社区繁荣作出贡献。

3. 让你的想法变为现实

借助功能强大的ETM 平台、简单易用的 JavaScript，以及区块链前沿技术的革命性功能，开发者可以自由发挥，打造前所未有的新颖 DApp，让你的想法变为现实。

UPoS 共识机制详解

1. ETM 科学家用 UPoS 找到效率、安全与去中心化的均衡点

共识算法是每一个区块链系统的核心所在，也是区别于其他不同区块链系统的关键。ETM 科学家创造性地将 DPoS 与 PoW 算法改进并结合在一起，形成双稳态 UPoS 共识机制，在效率、安全与去中心化三者之间，寻找到一个平衡点，完成了这个不可能的任务。对于开发者来说，深入了解系统的共识机制，有助于掌握由算法带来的相关特性，为开发 DApp 提供指引。

SHD 完备性

在一个分布式系统中，一致性（Consistency）、可用性（Availability）、分区容错性（Partition tolerance）三者不可兼得，称之为 CAP 定理。区块链体系中，类似于 CAP 定理，存在安全性（Security，缩写为“S”）、高性能（High-performance，缩写为“H”）、去中心化（Decentralization，缩写为“D”）三者兼容的 SHD 完备性问题。而这一问题，已成为区块链发展的重要掣肘之一。

PoW：从共识到分裂

PoW 即 Proof of Work，工作量证明。是一种以比特币为代表的共识机制，矿工通过尝试解决一些复杂的难题来获取出块资格。为了赢取出块奖励，矿工们消耗了大量电力，同时损耗挖矿硬件。由于获胜的概率与算力成正比，矿工也因此陷入了一条唯算力至上的不归路。

这是一场非合作的博弈，谁出块速度最快，谁就拿走所有的出块奖励与交易费用，却让其余人消耗了大量能源而无所得。由于共识算法和区块容量的设计，比特币与以太坊基本与高性能 (H) 绝缘，而 51% 算力的制约，似乎也在一次次的分裂中瓦解无存，让人们开始质疑去中心化 (D) 的实际状况。

至此，单纯的 PoW 机制已无 SHD 完备性。

DPoS：绕不过的中心化

DPoS 即 Delegated Proof of Stake，授权股权证明。DPoS 给出一种思路，将成千上万个节点，通过某种机制（例如持有代币的数量）选举出若干（奇数个）节点，在这几个节点之间进行投票选举出每次的出块节点，而不用在网络中全部节点之间进行选择。

这种机制能够大幅度提升选举效率。在几十个最多上百节点之间进行一致性投票，一般来说可以在秒级完成并达成共识。EOS 的超级节点概念 ，以及以太坊规划的 2.0，都是这一机制的实践者。DPoS 大幅提高了系统性能 (H)，却忽视了去中心化 (D) 的根本意义，**由少数权益拥有者掌握系统的发展方向，本质上和现有的中心化系统并没有太大区别。**

2. UPoS：PoW 和 DPoS 双稳态结构打破垄断和中心化趋势，实现 SHD 完备性

PoW 带来的公平会被超性能算力打破，就像每一次的技术革命带来的高性能必然会打破原有的公平。农业的世界如此，工业的世界亦如此，互联网的世界、区块链的世界中，金字塔也在周而复始地形成和坍塌。而 DPoS 带来的高效使得公平被更快地打破，因为没有了算力的公平支撑，金字塔会更快地形成，这就像现实中的各种权证，“超发”和“集中”会更快地形成。

DPoS 的优点是，不同于 PoW，它资源浪费少、更环保、出块速度快。PoW 平均每十分钟产生一个新区块，而大多 PoS 系统只需不到十秒。根据我们的设计，ETM 测试网 3s 以内就可出块，意味着交易确认速度得到极大提升。PoW 的优点在于它理论上安全性更高，因为迄今为止没有任何一个节点拥有全网 51% 算力的假设依然成立。

基于以上考虑，我们设计了 UPoS 共识以实现 SHD 完备性。简单来说，它的工作原理如下：首先，通过上凸函数映射将所有投票人的权益转化为相应的票数；第二步，结合优选机制，在每个出块周期选举出 101 个节点出块；第三步，被选中的矿工参与改进后的挖矿博弈（ETM 挖矿比比特币挖矿更经济、去中心化程度更高）；最后一步，混沌排序算法随机选中下一位出块矿工，让安全性进一步提升。

UPoS 算法具体流程如图 1 所示。

矿工 Miners

矿工是一种能够记录交易的账户类型。这些账户在整个生态中至关重要，由他们完成并验证交易。任何账户都能够成为矿工，但是只有入选的 101 个账户才能够生成区块。

图 1 UPoS 算法流程示意图

出块周期 Round

每个周期出块的数量是 101 个，即与每轮矿工数量相同。每一轮中，每名矿工快速混沌排序决定出块顺序，每人有 3s 的出块时间。如果未按时出块或者区块未通过验证，则继续快速混沌排序寻找下一个出块矿工。每个区块的生产都需要至少其他 68 名矿工签名确认并广播。

区块奖励 Block Rewards

ETM 系统中，矿工是区块的生成者。矿工成功生成区块会获得固定的 Token 奖励。区块奖励占 Token 总量的 48%，共 2.4 亿枚，在 6 年内分配完毕，逐年递减。

6 年内的比例分别为：12.13%、10.11%、8.09%、8.09%、6.07%、3.51%

出块奖励的变更时间表如表 1 所示：

每轮交易费用 Round Fees

另一个激励措施是每轮的全部交易手续费用，由当前轮所有活跃参与者按比例均分（具体奖励与分红机制详情）。

表 1　出块奖励变更时间图

奖励	里程碑
6 ETM	初始奖励，直到区块高度 10,112,000
5 ETM	阶段1，直到区块高度 20,224,000
4 ETM	阶段2，直到区块高度 30,336,000
4 ETM	阶段3，直到区块高度 40,448,000
3 ETM	阶段4，直到区块高度 50,560,000
2 ETM	阶段5，直到区块高度 59,328,000

源于大众，归于大众，ETM 投票、优选与分红机制详解

比特币的问世，至今不过 11 年，彼时的愿景依然在目，世界却变得完全不同。

天下熙熙，皆为利来；天下攘攘，皆为利往。从未有一种技术，像区块链这样备受瞩目，由于与金融与生俱来的契合，人们逐利而至，让众多项目脱离了既有的发展轨迹，造成了一种短视的现象：发展远离技

术，大众远离核心。诸如 ETH、EOS，已成为了少数人的游戏，去中心化荡然无存。矿场、矿池、超级节点才是其中的玩家，大众已无法从中获得设定的收益。这无疑是一种畸形不健全的生态，而其中的应用无不佐证了这一点。甚至众多项目一直标榜的安全，也越来越得不到保证。

继承了中本聪精神的 ETM 科学家们，认为算力的堆砌并不能提升系统的安全性，算力的去中心化程度，也就是算力概率分布，才是比特币乃至所有数字货币安全性的核心所在。而事实也证明了这一点，当资本涌入，矿场盛行，话语权垄断在少数人手中，比特币的安全性反而每况愈下。

ETM 系统的优势

ETM 始终认为，去中心化是一种新的机制与思维模式，而不单单是一种技术构架。它更是贯穿 ETM 哲学脉络的理念，是通过「分布式系统」（构架）、「源于大众而归于大众的投票、优选与分红机制」（政治）、「UPoS 共识机制」（逻辑）所共同完成的。

相较于传统的系统与机制，去中心化带来了三大优势：

1. 容错：去中心化系统不会因为某个局部故障而导致整个系统崩溃，由于它依赖于分布式独立工作的设备，整个系统的稳健性得到保障。

2. 阻止攻击：想要攻击或者操纵去中心化系统的成本更高。去中心化的系统没有一个「中心弱点」，不但因为分布式硬件很难被集体监测与攻击，其分散于世界各地的团队与用户构建的生态同样增大了攻击的难度。

3. 抵制合谋：去中心化系统的参与者们很难合谋勾结在一起。合谋本身其实很难界定，在传统系统中，利益驱使寡头们相互勾结，最终受损的是大众。反托拉斯法为此而生，而 ETM 运用纳什均衡也是为了改善整个生态体系的平衡。

「源于大众而归于大众」的投票、优选与分红机制

对于革命性的区块链而言，同样是在旧机制内部已形成了新机制的因素，而新机制在自身的发展进程中要同传统的观念实行最彻底的决裂。不幸的是，没有去中心化思维的区块链系统已不能够作为新机制的代表，这些项目在区块链技术外表下仍然是传统中心化的脉络。

传统中心化的弊端让人诟病，ETM 意识到需要构建一个能够抵抗它的协议，其中的重要一环，就是「源于大众而归于大众」的投票、优选与分红机制。

ETM 投票机制详解

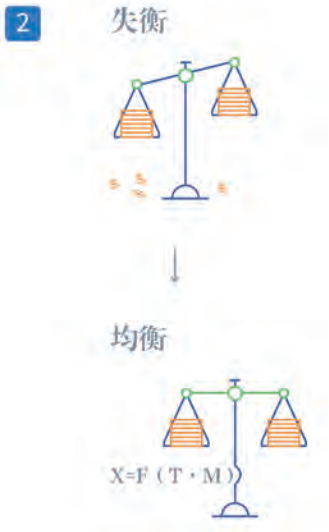
ETM 科学家们，运用数学与哲学上的诸多理论，设计了一套革命性的投票机制，为的就是改变现有格局，还数字货币以本来面目。

当用户锁仓一定金额 ETM 后，即获得投票资格，锁仓金额并不等于最终投票权益（票数），它要经过一系列的转换 $X = u \cdot t \cdot T$（其中 T 为锁仓金额，t 为时间增益系数，u 为抑制权益系数），得到最终投票权益 x（票数）。为了让整个系统不被寡头垄断，保证系统的稳定与安全，ETM 在这一系统转换中做了以下几件事：

1. 时间增益——增加散户机会

散户或者投资新人，在一个稳定的系统中很难获得突出的收益。ETM 为小额投票人设定了时间系数 t 的概念，小额权益（票数）在时间的帮助下，成倍增长，尾部用户也能够突出重围，获得成功。这个时间增益系数每 24 小时自增一次，成功的概率随着时间而增加，而在被投票人成功出块后折半，不影响大的生态平衡。

2. 抑制权益——降低寡头权



寡头在聚集大量财富后形成垄断地位，失衡的权重严重打击了大众的积极性。ETM 用上凸函数代替线性增长，甚至指数级增长的权益，让整个生态更为均衡，这个上凸函数就是「抑制权益」系数 u。通过上凸函数，抑制了资本获得超额收益的几率，进一步提高了系统的去中心化程度。

3. 不确定化（概率化）——0 到 1 的质变

一成不变的榜单是社区失去活力的罪魁祸首，ETM 将矿机入选的形式由按排名选取固定的前 101 名，变为由得票占总票数的比例概率抽选，让排名 101 名以后的矿工也有机会入选，$P = X / \Sigma Xn$。不确定化带来的是由 0 至 1 的质变，给之前永远无法入选的矿工以希望。

如此一来，整个系统的将根据概率确定矿工，算力也分散到了所有用户手中，使得垄断再无可能。大众只要有占总额 50% 的权益（票数），就必然有 50% 的席位，去中心化得以保证，安全性也得到了极大地提高。

锁仓

不同于证券交易，「锁仓」在 ETM 系统中，仅取其字面意思。对于一个稳定的内部系统而言，既要有一定的流通性，也要预防冲击而保持稳定，为了保护 ETM 生态体系的健康发展与小额用户的权益，用户需要锁定一定额度的 ETM，换取一定额度的投票权益（票数），用以投票选举出矿工。锁仓是投票的前提，用户通过锁仓获取投票资格，这部分金额仍存在于个人账户中，但无法用于任何交易。

投票人

所有 ETM 参与者都是投票人，自动拥有投票的权利。他们与矿工关系密切，决定了矿工节点的入选。

投票

在投票页面，根据矿工的得票与过往业绩，对矿工进行投票，选举出块矿工。

投票权益

投票权益（票数）是每名矿工能否入选出块节点的唯一凭证，它由该投票人锁仓金额通过权益调整函数换算而来。

入选规则

每轮区块生产，根据矿工所获得投票权益（票数）占总权益的比例，概率抽选。ETM 投票权益（票数）计算流程示意图详见图 2。

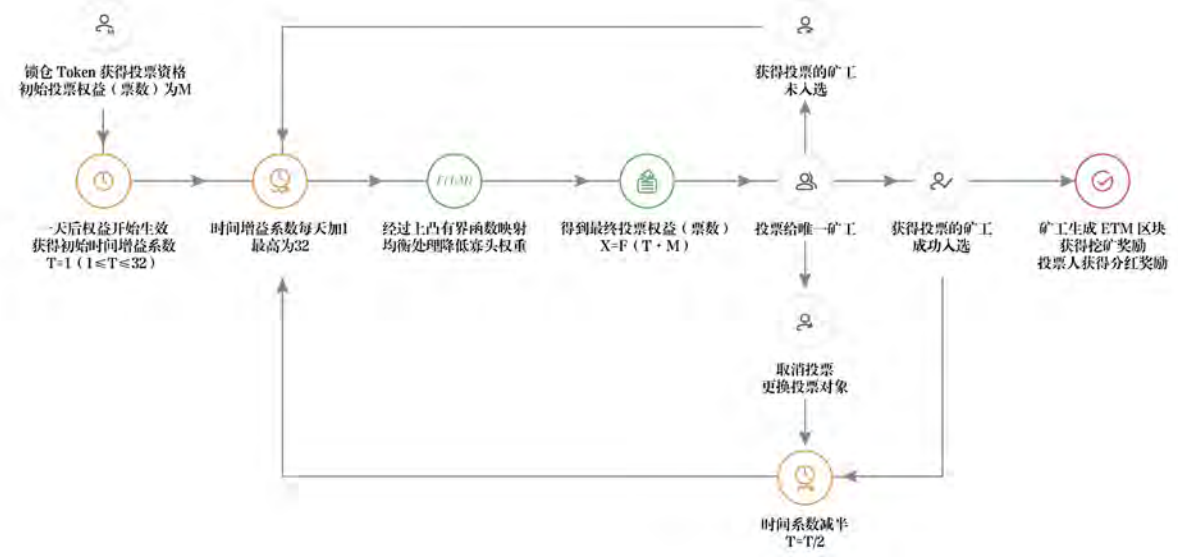


图 2 ETM 投票权益（票数）计算流程示意图

ETM 优选机制详解

如果说革命性的投票机制，带来了安全性与去中心化的提升，那么优选机制的加入，则保证了系统的稳定与高效。

在以往的 DPoS 系统中，投票通常被默认为公平民主而有效的，但这恰恰是最不合理的地方。相对的自由才能保证生态的良好发展，ETM 的优选机制是针对矿工而言的，这个机制会抑制乃至于淘汰那些差的矿工。该矿工的过往表现，赋予矿工一个优选系数 v，$v = m/n$，其中 m 为成功出块数量，n 为随机次数。一个矿工的最终入选概率 $P = v \cdot X / \sum Xn$。

1. $m \neq 0, n \neq 0\ v = m/n$
2. $m = 0, n = 0\ v =$ 上轮平均值
3. $m = 0, n \neq 0, v = 1/10 * n^2$

ETM 分红机制详解

在 ETM 系统中，矿工与投票人密不可分，每产出一个区块，投票人可以获得一定的投票分红。投票分红奖励占 Token 总量的 5%，共 2500 万枚。在 6 年内分配完毕，逐年递减。

6 年内的比例分别为：2.0224%、1.0112%、0.5056%、0.5056%、0.5056%、0.4496%。

每个区块投票分红奖励总额的变更时间如表 2：

表 2　投票分红奖励变更时间图

奖励	里程碑
1 ETM	初始奖励，直到区块高度 10,112,000
0.5 ETM	阶段1，直到区块高度 20,224,000
0.25 ETM	阶段2，直到区块高度 30,336,000
0.25 ETM	阶段3，直到区块高度 40,448,000
0.25 ETM	阶段4，直到区块高度 50,560,000
0.26 ETM	阶段5，直到区块高度 59,328,000

其中，奖励总额中有

1/2：给投中入选矿工的投票人，依入选矿工数量分成 101 份后，每名矿工的投票人按票数比例分配

1/2：累积一轮后随机选入一名入选矿工，该矿工的投票人按票数比例分配

源于大众，归于大众

不忘初心，方得始终；而初心易得，始终难求。ETM 希望做一个真正产生价值的区块链系统，解决实际的问题；让大众参与进来，而不是成为少数人的游戏；实现一个真正去中心化的自治社区，让区块链的价值传递成为现实。而 ETM 在投票与分红方面的种种设计，都是为了实现这一最初愿景的，用制度来抵抗寡头与垄断的产生，做到源于大众，归于大众。

随机源打造新世界的基石，ETM 混沌排序与时间塔算法详解

人的一生充满了不确定性，如同世上没有两片完全相同的叶子，而生活就像一盒巧克力，你永远不知道你会得到什么。面对这样的不确定性，它带来了不安与惶恐，但是也带来了光和希望。正是因为有了不确定性，也就有了无穷多的可能性，这是一个人甚至整个人类发展的动力之一，未来有了变数也就有了希望，没有人会想要那个一成不变按部就班的世界。

世界的历史进程是由一个个不确定性的意外事件推动的。如果说量子力学的不确定性原理是一切因果论的终结者，那么随机源，就是代码世界一切公平的基础。对于 ETM 的每一个参与者而言，不存在某个全知全能的上帝来决定你的未来，所有的决定都由混沌排序机制来完成。这个机制或者说理念贯穿于整个 ETM 项目，在涉及公平与安全的众多环节都有它的影子。

随机之源

我们需要随机数，用来加密信息、处理纸牌游戏的发牌、处理天气预报的未知参数、航班调度等等。计算机想要生成真随机数，就需要依赖外部世界的随机性，使用额外的硬件设备测量某些随机的物理现象：如盖氏计量器将短时间内背景辐射列出，序列的随机性源于辐射的随机性。但是这一类随机数生成器存在依赖外部设备、生成缓慢、搜集耗时、无法重现等缺陷。

计算机是确定性的，意思是它的行为取决于预先编

写的指令，所以程序中的随机数通常被称作伪随机数。但是伪随机数并不是假随机数，这里的「伪」是有规律的意思，就是计算机生成的伪随机数即是随机的又是有规律的。这些随机数通常是由随机种子根据一定的方法计算而得，即只要方法一定，随机种子一定，那么生产出来的随机数就是确定的，而区块链中使用的随机数必须能够复现，以达成共识。

混沌之源

「天地未形，笼罩一切，充满寰宇者，实为一相，今名之曰混沌。」这是古罗马诗人欧威德（Ovid）代表作《变形记》对混沌的描写，而中国古代边韶所著的《老子铭》中，也有「世之好道者触类而长之，以老子离合于混沌之气，与三光为始终」的描述。可见，「混沌」的概念在欧洲与中国古来有之，尽管含义不尽相同，哲理却非常相近。但是，在现代科学里，「混沌」即 Chaos，却是一个很不一样的概念。

在现代科学史中，真正的数学和物理学意义下的混沌理论，公认的是由麻省理工学院的气象学家洛伦兹（Lorenz）提出的。该理论是在一次气象模拟试验中，将一个小数点后六位的初始值做了四舍五入处理，仅输入了小数点后前三位数，与精确值不到千分之一的误差，最后的结果却大相径庭。而后提出了最为大众所熟知的「蝴蝶效应」比喻：亚马逊热带雨林的一只蝴蝶扇动一下翅膀，可能会在得克萨斯州掀起一场龙卷风。

失之毫厘，谬以千里，初始条件微小的差别或改变，可能引发巨大无比的后期效应，这是混沌理论最根本的特征。

自从洛伦兹在气象预报研究中发现混沌现象以来，人们陆续发现在众多自然和社会变化中均存在该现象，而科学意义下的「混沌理论」，也在生物医学、信息隐藏、流体混合等方面找到了成功的应用。

混沌排序

计算机是确定性的。但确定性往往被拿来作为攻击目标之一，在区块链系统中，出块顺序必须是确定的，一旦掌握了排序，或许就能锁定并攻击正式矿工，篡改区块信息。

在传统的区块链系统中，一旦选出了这一轮出块的正式矿工，他们的出块顺序也是固定的了。排序与名单暴露于全网，任何人都可以查看，能够被轻易锁定和攻击。

newList = F(height, list)

ETM 使用快速混沌排序解决这一问题。混沌动力系统中动力学行为对初值的极度敏感性。通俗地说，混沌就是指对初值极小的扰动可以导致映射结果极大的变化，因此在预测过程中会导致一种不确定性。这种不确定性正是我们需要的。混沌排序指正式矿工上传的顺序并非一开始就确定，而是共识层的设计规定一种算法，提取每一次成功上传区块中的某些信息作映射并进行多次迭代计算出下一名正式矿工的编号。因此只有在最后一刻才知道应该上传区块的正式矿工的身份。虽然这一信息任何人仍能查看，但是混沌排序让外界无法锁定和攻击正式矿工。同时混沌映射是确定性的，因此所有矿工都通过自己的计算得到完全一致的排序结果。系统的稳定性和安全性在去中心化的前提下得到了实现。如图 3 所示。

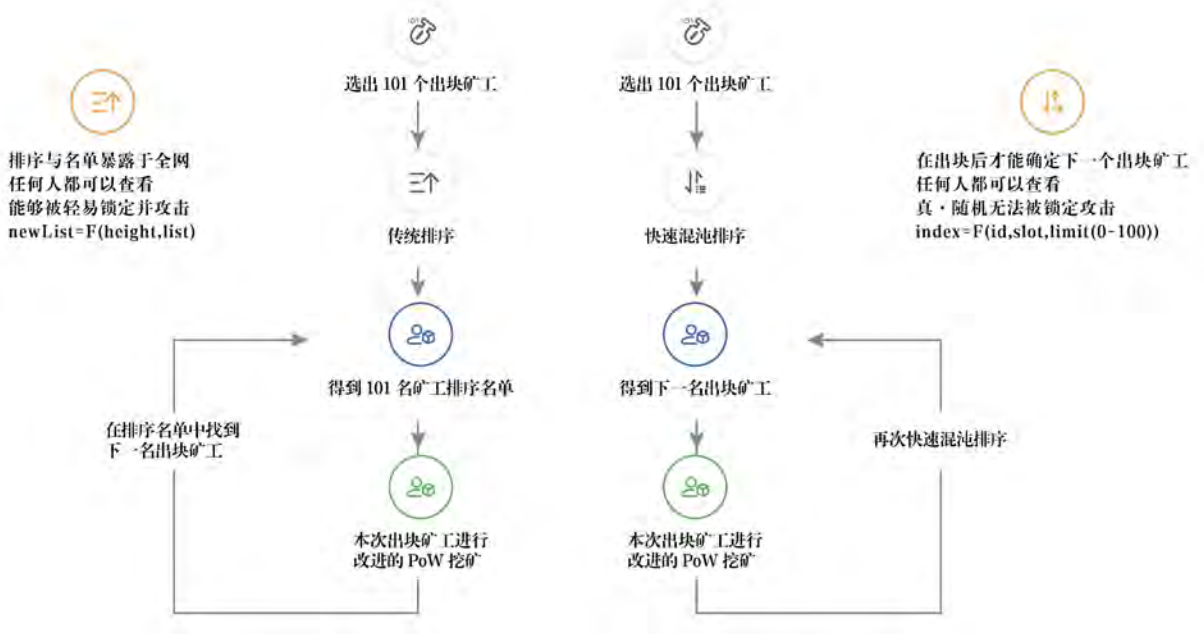


图 3 混沌排序示意图

index = F(id, slot, limit (0~100))

基于混沌算法的随机源——时间塔

在生成随机数这件事情上，一个复杂系统中，独立个体的行为是可控的，而个体集合为一个群体后却变得无法控制。因此利用区块链特性，让公众参与到随机数的生成，由每一个参与者提供随机种子，由算法共识保证随机数的可靠与公平。

根据这个思路，我们设计了时间塔算法，依赖 ETM 的纳什均衡体系，通过一系列设计，使得单个输入参数的改变，无法保证最终输出结果向其期望的方向倾斜，从而得到一个去中心化的、可靠的随机源。

时间塔算法：

算法输入：N 个 Hash 值、迭代次数 M、SHA 计算次数 X

参数说明：

1. N、M 和 X 是算法参数，通过调整 N、M 和 X 可以调节算法的时间复杂度；
2. X 是 SHA256 计算次数，为待定常量

算法步骤：

1. 记 N 个区块中第一个区块的 Hash 值为 H0
2. 计算 H0' = SHA256(H0)，重复计算，迭代 X 次，得到 Q0

```
for(i=0; i<X; i++){
H0 = SHA256(H0);
}
Q0 = H0;
```

3. 将 Q0 代入混沌算法，得到下一个被选出的区块的 index，K1 = Chaos(Q0, H, N)
4. 查找第 K1 个区块的 Hash 值，记为 H1
5. H1 = H0 + H1
6. 对 H1 进行 SHA256 计算，重复步骤 2 ~ 5，得到 Q1 ，并迭代 M 次
7. 对 Q1 到 QM 求和，输出最后的随机值

核心特点：

1. 利用迭代算法的特性，抑制并行计算的影响

2. 利用混沌算法的特性，并通过充分迭代，随机选择，降低后部区块由于时间推进而具备的信息优势

3. 能够通过对参数的调整，增减算法的时间复杂度，灵活适应不同频率的随机数需求

公平秩序

混沌排序不仅是混沌理论在 ETM 系统中最为基础的应用，它更赋予了整个系统一个基础种子，在此之上，将混沌理论运用到系统的各个环节。我们知道，在一个区块链系统中，算力的概率分布决定了系统的安全性，而这就需要以公平与秩序为基础，混沌排序解决了出块顺序这一难题，保证了内部公平。而在外部，混沌排序也将作为随机种子之一，提供给所有的 DApp 开发者，保障生态体系的公平，从根源上杜绝了作弊行为的发生。

同时，一个区块链系统如果没有一个可靠的随机源体系，那么 DApp 用户对应用没有绝对的控制权，开发者或者运营商仍能够通过各种手段，控制 DApp 内部资产（如游戏装备产出概率）、影响链上公平（如胜负判断）。ETM 基于混沌理论设计的时间塔算法，正是运用理论中的不确定性，打造了一个可靠的随机源体系，保证了系统内部的公平秩序。

ETM 侧链机制打破资源壁垒

开发者是技术的使用者和推动者，一个可持续的 Token 生态离不开开发者的建设与付出。愈加高企的开发运营成本让开发者开始抛弃 ETH 与 EOS 等平台，整个生态也因此陷入了恶性循环。ETM 从设计伊始就极力避免这种情况的发生，让开发者零成本在 ETM 进行开发。合作共赢的理念植入了 ETM 每一个环节，ETM 侧链机制让开发者能够根据需求动态调度资源，而系统仅出于安全的考虑，按交易量收取低廉的手续费，并会通过社区活动返还给开发者。

区块链的扩展之路

区块链为了保证数据的可靠性，要求所有节点都必须保存全部区块数据，导致整个系统的吞吐量较低。糟糕的性能表现严重制约着开发者的创造力，也让 DApp 迟迟无法落地，扩展已成为任何一个区块链项目的必经之路。

传统的 BTC、ETH 都采用全网节点共享一条区块链的单链方案，网络上的每个节点需要处理、存储全网的所有交易和全部数据，整个区块链系统的处理能力实际上受限于单个计算节点的处理能力。另外，受到共识算法的影响，随着节点数的增加，系统整体处理能力不但未随之提升，甚至还会降低。因此，为了让区块链系统具有更大的吞吐量，解决思路是让非关键的交易数据只在部分节点中验证和存储，从而提高交易处理速度，降低节点处理压力，从而提高整个区块链系统的性能。为了达到这一目标，ETH 提出了分片

的解决方案，将整个区块链划分为 100 个分片，每个分片内独立处理交易；而 ETM 系统则采用侧链的方案，为每个特定应用程序开发一条侧链，该应用程序的数据只保存在侧链上。这些方案使得全网由原来的单链扩展到了多链，在多链上可同时并发地处理多笔交易，突破全网处理能力受限于单个节点的限制，从而提升系统整体性能。

分片方案和侧链方案从提升系统吞吐量的角度来说，都能通过分片数或侧链数来线性增加系统吞吐量，但是前者分片数是固定的，后者可以动态调整，因此更为灵活。从安全性角度来说，分片方案需要增加验证节点，在管理上显得更为复杂；侧链方案中侧链的验证机制与主链相同，不需要专门的验证节点来验证，安全性也可以保证。从易用性角度来说，分片方案仍然继承了 ETH 的智能合约体系，开发成本较高；侧链方案则充分从开发者角度考虑，专门设置了应用部署服务器，简化侧链应用的运行、调试和维护流程，降低了开发成本。

ETH、EOS 的开发瓶颈是有限资源与无限应用的对立

那么性能真的是应用落地的唯一瓶颈吗?

对于 ETH 用户来说，想要 DApp 有好的体验就要付出较高的 Gas 费用；对于 ETH 开发者而言，ETH Stack（变量）的数量直接制约了应用的复杂度，开发者无法在 ETH 上开发稍微复杂的 DApp。在不改变其核心理念的前提下，单纯的扩容并不能改善 ETH 上的开发与使用瓶颈，近期过渡阶段的种种不明朗，也进一步加重了 DApp 用户与开发者的顾虑。

EOS 系统为了提高吞吐量，抛弃了传统的 PoW 共识机制，交易只用等待选举出来的代理节点确认和打包，不需要等待其他非信任节点的确认，大大节约了交易确认时间的消耗。EOS 系统的吞吐量号称达到百万级，在上线运行中实测也能达到数千 TPS。因此，在目前的应用环境下，TPS 并不是 EOS 系统上应用开发的瓶颈，真正阻碍 EOS 系统上应用开发的是 RAM 分配机制。

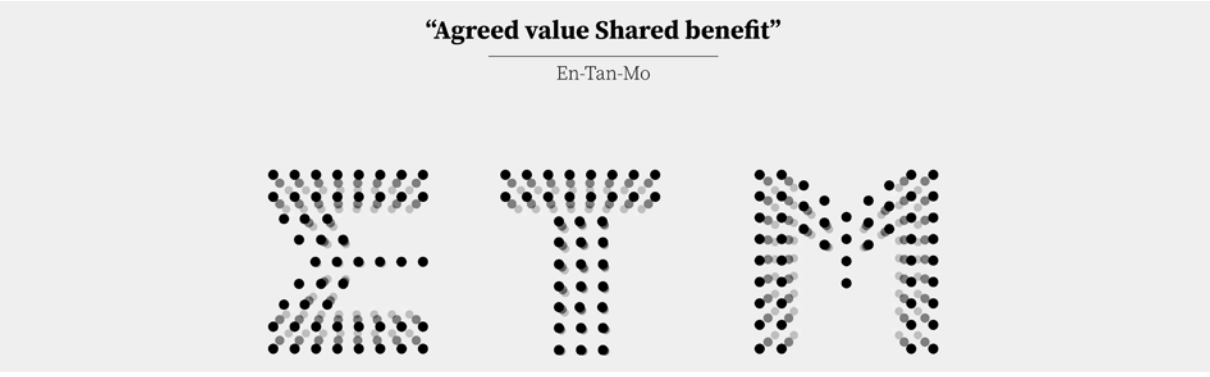
在 EOS 的系统合约内，实现了一个内存市场，EOS 合约开发者可以将一些记录写在区块的存储中，在合约中的一些操作需要消耗一定量的 RAM 才能执行。在 EOS 链上创建账户，竞拍账户名等操作都需要消耗 RAM，而 RAM 需要通过交易来获得。EOS 系统设计的算法使得 RAM 的价格会随着 RAM 使用率的增长而变化，而且用得越多，价格波动越大，这样就保证到最后 RAM 价格会特别高，永远也不会被卖完。由于 RAM 价格波动大，炒作的空间也大，使得现有的 RAM 交易基本上都是在投机炒作，真正需要 RAM 的应用开发者反而拿不到 RAM，或者说即使拿到，也要付出非常高的经济成本。正是由于投机者持续炒作 RAM，这让开发者们面对的是一个无法确定的开发成本。如果没有有效的机制改变这种局面的话，很多开发者们将会选择更加友好的基础设施平台，这势必影响 EOS 系统内应用的生态繁荣，最终影响 EOS 整个生态的价值。

随着 EOS 的演进，在实际使用与开发过程中，你会发现，瓶颈远不止 RAM 限制。在其上的任何一个操作，都需要 EOS、RAM、CPU、NET 四种资源，而这对用户与开发者来说，无疑是一场灾难。

当所有的 DApp 使用者与开发者都在竞争 ETH、EOS 及其稀有的资源时，DApp 已毫无落地的可能。

侧链机制变恶性竞争为合作共赢

对于现有区块链项目而言，机制与算法造成了内部资源过于稀缺，不同应用、开发者之间相互竞争制约了整个生态的发展与繁荣，这也是目前没有一个区块链 DApp 应用得到大众认可的根本原因。基于主链 - 侧链机制的 ETM 应用平台，打破了资源壁垒，每一个 DApp 单独拥有一个完整的侧链，享有整个区块链的性能，而不受其他 DApp 影响。创造性地用 UPoS 共识机制实现了 3s 出块，同时单链 TPS 达到了 500/s，而且由于侧链之间相互独立，使得整体生态应用得以无限延展，实现 N*5000/s 的高性能。因此对用户体验有较高要求的游戏 DApp 在区块链上真正运行起来，性能瓶颈也不再是开发者想象力的枷锁。技术的创新是一切变革的前提与基础，ETM 的技术构架也为新一代互联网应用平台的价值传递夯实了根基。



后记一
困境与超越，用户赋权可期

赋权是传播学中的一个概念，在区块链中，赋权意味着用户获得去中心化状态下的权利与自由。在本文中，将从赋权角度讨论区块链所遭遇的赋权困境，以及如何超越困境为用户赋权。

“大部分人认定数字货币一定会失败，因为自从 20 世纪 90 年代以来所有公司都失败了，我觉得正是因为中央集权，使得这些失败必然发生。我想比特币是我们第一次尝试一个去中心化、不基于信任的系统。”①

扯开过往数字货币失败的遮羞布，2009 年的中本聪曾如是说。

与在社会景观中依稀可见的“中央集权”相对，他踯躅尝试的去中心化，也可以说是一种赋权。

未来是湿的：技术助推权力下放

赋权，指某人或群体获得掌控自己本身相关事务的力量。② 在稀缺资源掌握在少数中心角色手中的历史阶段，赋权是被压制的大多数劳动者可望而不可即的伟大梦想。

历来学者对于权力这一话题的探讨变动不居。马克思以及韦伯为统治者思考权力的根源暂且不论，后现代的福柯对权力的观察已经转移到单纯对一种支配控制力量的分析。③ 他看到的权力是一种关系网络，其中的个人是流动的，统治者与被统治者之间的二元对立关系就此被解构。而他诠释的权力观念视角的下放，似乎隐喻着在技术驱动下人类隐隐走上的赋权之路。

随着区块链、人工智能、地下交通系统、5G 无线网络、比特币、增强现实、无人驾驶汽车、新太阳能技术、激光互联网、物联网、AR 头戴设备等新技术不断出现，筑造我们全新的社会图景，个体不断解放物理性的肌体活动，将盈余的时间及精力应用于更大的价值创造中去。

就像维基百科中所有的知识盈余贡献者，在透明化信息环境以及形成新规则的场域中，分散于世界各个角落，又聚合成具有更强大生产能力的群体，不断对冲那些排他性占有生产资料的权力拥有者，成为原有生产资料垄断者不可忽视的一脉力量。

从中可以窥见的的是，新兴技术不断涌现的当下，正隐喻着权力的下放——赋权的实现似乎近在眼前。正如克莱 · 舍基在《未来是湿的》中指出，“多种社会性工具现在提供另一个选择，具有松散结构的群体，可以出于非营利性目的、不受管理层指挥而运行”。④ 与福柯的观点相对应，涌现的新技术正在成为权力下放的助推器。

未来是湿的，流动性的社会款款前行，权力不再束之于高阁，新技术不断磨拭着伟大梦想。

叩问赋权：难能放权的未竟之梦

2018 年，区块链成为新技术竞赛场中的夺目新星。2019 年 2 月 4 日，Facebook 收购了区块链创业公司 Chainspace，这是 Facebook 收购的首家区块链公司。

对于新兴的“分布式账本”——区块链，扎克伯格曾在 2018 年将年度目标定为探索区块链技术在脸书中的应用，通过“去中心化”的方式向人们赋权。

---

① 《中本聪语录：除了 " 比特币之父 " 你还知道他什么？》链人 ,2018-10-20。

② 王锡苓 , 孙莉 , 祖昊《发展传播学研究的“赋权”理论探析》, 今传媒 ,2012 年第 4 期

③ 曲广娣《马克思主义权力观和韦伯、福柯权力观比较》, 清江论坛 , 2016 年 01 期

④ [美] 克莱 · 舍基《未来是湿的》, 中国人民大学出版社 2009-5 版

在区块链世界，参与者无需任何第三方机构的担保，每一个节点、每一个组织，机器和算法都有机会自由地进行。区块链中每个人有相应的经济行为，区块链技术可以通过结合经济行为和随机的数学算法使网络达到共识，并通过算法对共识进行投票从而建立一个新共识的机制。一旦有了这种共识，信任随之而生，人和人之间就会有了新的合作机会。

在这种情况下，以往掌握生产资料、意味着高效的中心化平台，就不再是充分必要条件，用户可以用透明的算法定义所在社区里面的游戏规则。由权力所有者决定的游戏规则被不断解构，基于共识的用户正在重新建立崭新的场域。

但技术所带来的结果，并不一定如乐观者预期的那样真正服务于大多数人。它的使用离不开背后的资本、信息和权力，往往那些强大的资本拥有定义价值与事实的可能性，权力极易在新的资本面前重新趋向单极。

就像是曾被寄望于实现去中心化的 PoW 共识机制——算力证明机制，任何人都可以购买矿机加入竞争挖矿，由于只有资金门槛，所以用户可以使用技术优势、组织能力来增加竞争优势。于是人们认为 PoS 使非中心化节点也可以通过自由的竞争，变成中心化节点，从而实现真正的去中心化。但事与愿违，暴力而激烈的算力竞争使算力不断趋于集中，资本摩肩接踵涌入收割富矿，挖矿规模化、企业化，单独个体无法实现的 51% 攻击成为聚集算力的矿池的惯用手法。算力高企的大型矿池俨然成为游戏主角，人们以 PoW 推翻中心节点的希冀被无情击碎。

当关于“算力集中”的问题引申到 PoS 机制——股权权益证明，同样可能面临“Stake”集中的问题——PoS 依据持币量和持币币龄来衡量谁能生产区块，任何人都可以购买币加入挖矿，而持有币量是唯一的竞争优势。这意味着在 PoS 机制里，拥有币越多、币龄越长的节点拥有越高产生新区块的权力，且时间越长越容易产生马太效应，持有币越多的人会获得更多的币奖励，从而加大贫富差距，最终产生超过 50% 的中心化节点，被动演化为非预期的中心化的结果，赋权再次成为追随者的未竟之梦。

DPoS 在 PoS 机制上加一个限制，区块生产者并不完全的依靠持币量和币龄多少诞生，而是附加了一个“选举”机制，持币用户可以通过投票来选举区块生产者，也可以通过取消投票来罢免特定的区块生产者。设计者希望通过选举来保证一定有区块生产者诞生，但弊端在于，人们不能保证有足额的真实的区块生产者，因为一个人或一个实体可能就控制着多个节点。比如 LBTC 就一度出现半数节点被鱼池一家控制的事件，而 EOS 在启动过程中，也疑似出现一个人虚拟出 7 个节点的魔幻情节。①

对于区块链的未来，人们仍不惮以美好的期待为它背书。有学者预言，到 2025 年，区块链技术将得到广泛的应用，打破传统金融机构在市场上的垄断，为产业赋能。②

但中本聪及其继承者所壮志在怀的去中心化尚未实现，依旧难能放权的算力与权益证明等新机制不得不经历迭代与更替，再次迁徙。

为用户赋权：ETM 呼唤群体性自由

在 ETM 世界中，人们共识之基在于所有社区公民皆能被赋权。

在这里，赋权意味着用户共同参与、公平收益，打造去中心化平台，它不再是想得而不可得的空想世界。

研究者窥见以往算力与权益证明的暗病——中心化枷锁。为了打破不局限于大矿池或大股东独家坐庄的中心化局面，让所有参与者都能成为 En-Tan-Mo 场域内的受益者，ETM 科学院在底层共识机制提出基础性变革，创造性地提出基于纳什均衡的 UPoS 共识机制——统一权益证明法。

在以往世界中，联盟内部更趋向于更强有力的合作者，越强的合作者的收益超越更弱小的合作者，这种超线性的收益模型最终伤害的是屈居较低算力的弱者，长此以往，强者的收益也将因为生态的坍塌而受损。而 ETM 世界里 PoW 和 DPoS 交织的双稳态 UPoS 机制，使 PoW 和 DPoS 的集中化和中心化被最大程度地限制，为所有参与者赋权。

具体来说，在比特币系统中，矿工取得区块记账权的影响因素是算力。类似解小学数学题的过程，解题最快者举手获得老师的奖赏，比特币系统中也是计算最快的矿机获得一笔不菲的比特币奖励。而对于 En-Tan-Mo 而言，矿工作为出块节点，算力只是衡量标准之一，过往表现亦被作为投票人的衡量坐标，而算力高者、过往表现优者挖矿，

---

① 《POW、POS 和 DPOS 的多中心化程度分析》, 金色财经 ,2018 年 6 月 27 日

② 何平《区块链应用实例与前沿研讨》,2018 年 3 月 16 日

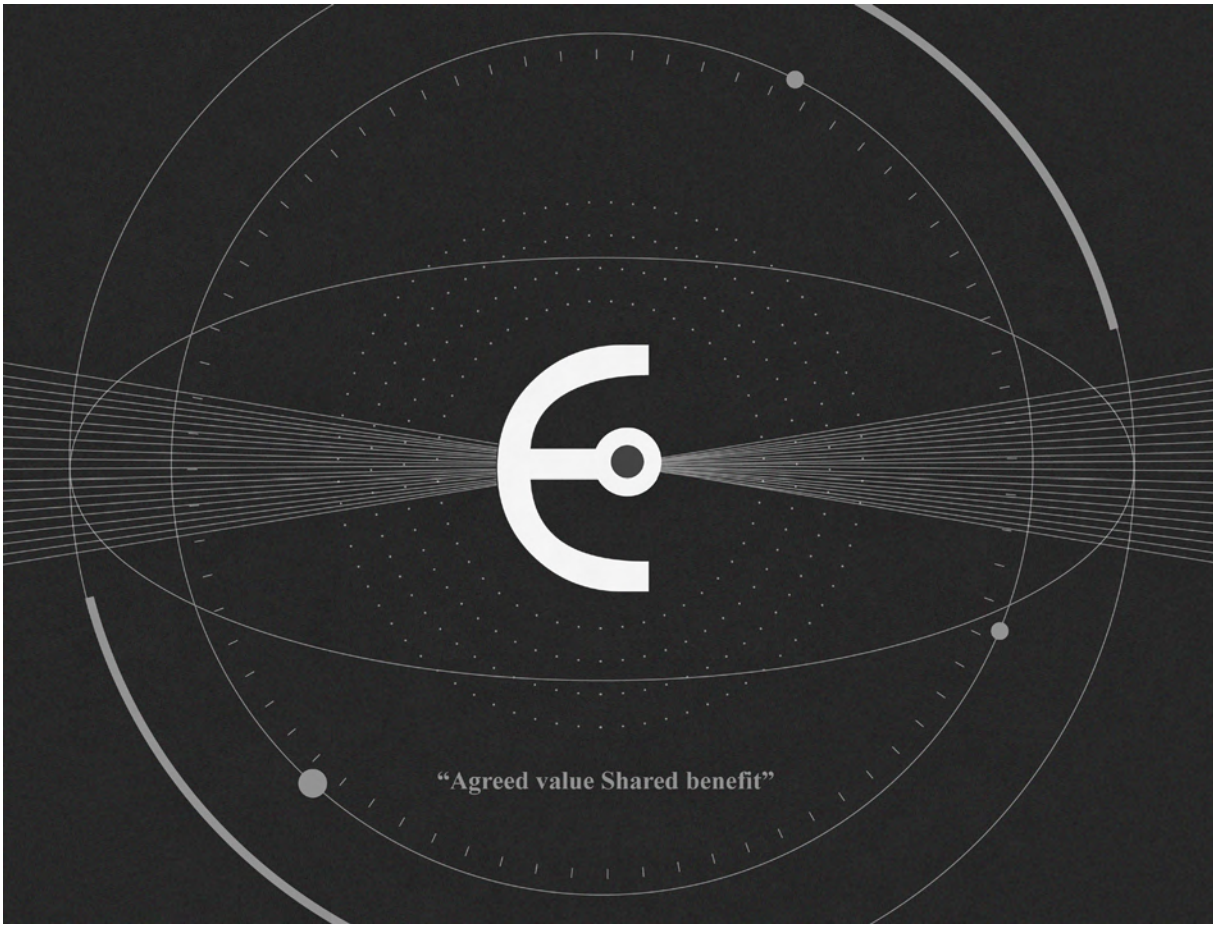
仅仅是大概率事件而非绝对化事件。再加之受到抑制函数的影响，超线性收益被 ETM 科学院采用的上凸函数取代，算力不再是竞争中的目的，仅仅是一种技术性的手段。失去了唯算力目的的支撑，不再受拥有强大算力的巨头的挤压，每个区块生产者都有权在生态圈中通过哈希计算出块获益。

ETM 创造的 UPoS 共识机制中，每个节点验证区块链交易的能力并不基于他们所使用的算力，而是基于他们获得了多少投票。而其革命性的创举又在于：作为均衡场上的大多数的持币投票人虽未直接参与到哈希计算的出块过程中，但根据拥有的 Token 数量可以获得投票选举权，此时将矿工算力及过往表现作为投票的主要依据投票给某位矿工，依据矿工表现获取相应 ETM Token 奖励。大多数人不再是旁观者，更是创造者，置身于理想中创造一个均衡普惠的世界。

所以，En-Tan-Mo 是一个非自上而下的，完全由供需市场驱动的世界，价值在信息透明化与参与平权化的世界里，完成开放式流转，ETM 给大众提供的是一个均衡的价值传递体系。参与者们在 UPoS 共识机制下相互支撑、相互激励，包容各种区块链与非区块链的应用和社区，它帮助所有渴望公平、民主、自由等价值的人们，均衡地获得属于每个个体的最高权益，从而实现权力和自由的平衡。

在张扬权力下放的时代，可以消耗自由的选择有很多，但可以填充自由的选择终究很少，如何真正被赋权达及彼方？中本聪的向往在资本的凝视中仍是一个未知数。

好在时代也有缝隙与边角，在 ETM 筑造的权力下放的群体世界里，那些如今看起来似乎寡小的自由选择仍然具有实现的可能性。



后记二
十年磨一剑，ETM 重燃中本聪精神

区块链技术无疑是当今世界一场悄无声息的革命，宁静中的这股力量，正在让世界发生着超乎我们想象的逆变。

En-Tan-Mo，简称 ETM，灵感来源于 Entente（联盟）、Transaction（交易）和 Mobius（莫比乌斯），是基于纳什均衡和价值传递理论的新一代区块链项目，是十年磨一剑后对中本聪精神的重燃与高扬。

还原去中心化：En-Tan-Mo 不是少数人的游戏

2008 年 11 月，中本聪发表题为《比特币: 一种点对点式的电子现金系统》的论文，比特币所依托的底层技术——区块链，由此进入大众视野。

这是一个激动人心的概念，它描绘了一个相当“前卫”的世界。在这个世界中，区块链通过公开透明的方式，终结了中心化机构扮演的信用“资本家”的角色， 转而将信息存储、传递的权利交由全体参与者进行民主的维护。换言之，“去中心化”从一开始就是区块链直截了当的“宣言”。这般宣言让区块链技术不再意味着对现有社会运转方式的改良或优化，而是将成型的中心化帝国和支撑其强势的逻辑直接“打翻在地”。

为了保障这一点，中本聪以效率为代价，在比特币中创造性地引入了 PoW 共识机制。

共识机制是区块链的灵魂，它回答的是，区块链在去中心化的情况下，系统如何避免成为一盘散沙，如何实现有序运转，如何成功取代中心化机构的“记账”功能的问题。

PoW 的解决方案是算力竞争。在全网节点中，谁能率先解出比特币系统给出的工作量证明谜题，谁就能成为新的区块记账者，并获得一定奖励。

然而，随着高性能矿机的出现，普通 CPU 算力获得收益的概率几乎为零，专业级矿机轻易就能获得超线性收益，而后期矿场和矿池的出现，更是彻底打破了比特币去中心化的愿景。

那些抛弃了 PoW 共识，转向 PoS 或 DPoS 共识的区块链项目，纷纷将重心转移到对效率的追求上。然而由少数权益拥有者掌握系统发展方向的项目，最终成为了大玩家的游戏，沦为“伪区块链”。名存实亡的“去中心化”，早已背离了中本聪精神的初衷。

这正是 ETM 问世的目的，也是 ETM 试图攻克的首要难题。为此，ETM 科学院巧妙地将 PoW 和 DPoS 融合在一起，创造性地设计了 UPoS（Unified Proof of Stake，统一权益证明）共识机制。

ETM 认为，真正的去中心化世界是对集权和垄断的敏感与隔绝，是一个拥抱创造力和公平性的不确定世界。

为了避免算力的垄断，ETM 采用了 PoW+，在保障安全的基础上，大幅降低算力需求，让大众能够参与进来。ETM 不会像现在的 BTC 与 ETH 被矿场把持，独立显卡高性能个人计算机、视频工作室闲置服务器、实验室高性能服务器、带 GPU 算力的云服务器等等，都将是 ETM 代理矿工候选者。

为了避免权益集中形成的垄断，在 UPoS 机制中，每个 Token 持有者都可以成为投票人，投票人手上的 Token 通过上凸权益映射转化为可投票数，选出矿工并获得奖励。

值得注意的是，在这里，投票人的票数与其拥有的 Token 数量呈上凸函数关系，Token 越多者兑换率越低，反之 Token 越少者兑换率越高——这使 En-Tan-Mo 成为一种最为公平公正的区块链网络。

不仅如此，考虑到散户或投资新人在一个稳定的系统中很难获得突出的收益。ETM 为小额投票人设定了时间系数 t 的概念，小额权益（票数）在时间的帮助下，成倍增涨，尾部用户也能够突出重围，获得更高收益。

这正是 ETM 的目的，通过全新的投票与分红机制，让每个参与者都可以以矿工或投票人的身份，平等地参与到区块链的建设中，并获得均衡的奖励，以确保整个体系不会被寡头把持，避免成为少数人的游戏，确保还原区块链去中心化的本来价值，开启更为公平、公正的区块链公链系统。我们认为，这才是中本聪精神的内核所在。

解决 SHD 完备性，ETM 不是纸上愿景

伴随比特币的价值逐步攀升，全世界大量似真若假的“项目”蜂拥而入，响应着人们对区块链的想象。散户的澎湃决心与技术常识的不对称，让众多脑洞大开的“区块链”项目有机可乘——非法集资和诈骗甚至只要披上一件“白皮书”的外衣，就能营造趋之若鹜、座无隙地的繁荣景象。即使面对无法流通、没有刚需的现状，一些虚拟货币的炒作者依旧抱着“要不百倍、要不归零”的粗暴手段涌入“区块链”。

直到监管层层收紧，不断给狂热的发币、炒币划线，一些从业者才意识到，区块链应该从盲目发币的时期进入到发展技术的时期。

ETM 早已专注于此。

区块链成于技术，它的诞生，正是由于中本聪对分布式数据存储、点对点传输、共识机制、加密算法等技术的天才结合。

区块链的发展也受限于技术。区块链是一个分布式存储系统，而在分布式系统中，一致性（Consistency）、可用性（Availability）、分区容错性（Partition tolerance）三者不可兼得，称之为 CAP 定理。区块链体系中，类似于 CAP 定理，也存在安全性（Security）、高性能（High-performance）、去中心化（Decentralization）三者兼容的 SHD 完备性问题。十年来，区块链技术深陷跛足困境中，总是不得不在三者中牺牲其一。比如比特币为了去中心化与安全性，牺牲了高效率；EOS 为了获得高效率，牺牲了去中心化等等，可以说，区块链技术的核心，便是 SHD 完备性。我们甚至可以毫不犹疑地断言，谁实现了 SHD 完备性，谁就掌握了区块链的未来。

ETM 在机制设计和技术实现上，始终瞄准于此。其凝聚了各领域众多专家学者的技术团队所设计的 UPoS 机制，当然也不会仅仅止步于解决去中心化的问题，在这个机制中，去中心化、安全与效率是不可分割的整体。

如果说前文介绍的上凸映射、时间增益、抑制权益等策略偏重的是保障去中心化，实现权证拥有者和区块矿机的分离和各自权益，那么混沌排序、不确定化（概率化）及优选机制等则是安全与效率的最佳保障。

一方面，节点通过选举进入矿工团队，通过 Hash 计算上传区块，每一轮上传区块后要进行重新选举，上传区块的顺序随着上一个矿工的计算结果随机产生。在这个体系中，Hash 计算将不再用于进行算力竞争，而是用于产生（下一个出块节点的）不可预测性，这将有助于保障节点无法协调作弊和攻击系统。

另一方面，由于 Hash 计算的用途改变，算力需求可以大大降低，避免消耗大量资源，但仍然可以动态调整以用于设置节点的参与成本，激励节点维护系统的稳定性和预防女巫攻击。交易处理速度可以极大地增加，从而提升系统的整体效率。同时，系统具有了极大的可扩容性，具有了更多应用场景的可能性。

此外，ETM 采用了一条中心链加多条衍生链的设计。中心链负责网络安全及价值交换，每一个衍生链作为独立、隔离的系统对应一个 DApp，通过继承和复用主链技术，所有应用都拥有个性化的账本、代币、共识机制、交易类型。与此同时，ETM 以自演进组件库为核心，为其它区块链提供适配平台完成资产和应用的转移，也为非区块链的应用和数据配置双向调用通道，这都使得 ETM 具有极大友好性与无限的延展性。

始于技术，成于应用，每一项新技术的发明，只有当其进入实际应用领域时才能显现其真正意义，区块链也是如此。解决了 SHD 完备性，区块链才能真正落地，稳稳当当地进入应用时代，进入一个更能召唤自由与想象力的时代。这正是中本聪的初心，也是我们对中本聪精神的高扬。

依托科学院背景，ETM 志存高远

作为区块链的创始者，多年来，中本聪的身份一直成谜。有人认为他是一位科学家，因为其几乎熟悉当时所有的前沿计算机技术，有人认为他是经济学家，因为其对经济规律的洞察与金融科技的开创性，甚至有人提议他获得诺贝尔经济学奖，也有人认为，他不是一个人，而是一个团队。

正如戴伟事后评价说：“要想开发出比特币，必须得：1、对货币有非常深入的思考 ;2、要了解密码学 ;3、认为比特币这样的系统从理论上是可行的 ;4、要有足够的动力去将这个理念开发成实际产品 ;5、编程能力出色，能保证产品安全 ;6、有足够的社交技巧，才能围绕这个产品建立一个成功的社区。密码学圈子能符合前三个条件的人已是凤毛麟角。”

为此，我们组建了具有强大科学背景的 ETM 科学院，来继续追随中本聪的脚步。

ETM 科学院成员包含：诺贝尔经济学奖得主、理性预期学派领袖 Thomas J. Sargent 教授，诺贝尔奖物理得主、大一统模型奠基人 Sheldon Lee Glashow 教授，美国马里兰大学博士、分布式系统专家 Aaron Yuan，美国加州理工大

学博士后、P2P 通信协议专家 Daniel Wang，西班牙圣地亚哥大学博士、博弈论专家 Thomas Tang 等专业学者。

ETM 所有共识机制、网络协议均由 ETM 科学院设计完成，两位诺贝尔奖得主领衔的国际化科学家团队保证了技术上的领先性。 ETM 共识机制和均衡经济结构设计建立在博弈论和分布式系统的基础上，并深刻地应用了 Thomas J. Sargent 教授提出的理性预期理论和基于时间序列分析的动态宏观经济理论。同时，ETM 均衡共识运用了 Sheldon Lee Glashow 教授复杂系统多粒子共存和相变的物理学原理，巧妙地设计了矿工、Token 持有者和普通参与者的均衡价值传递体系。

ETM 目前的工作成果归功于理论与实验、软件与硬件、技术与商业等各个不同团队和负责人之间密切地配合和共同劳动。Kantorovich 共识机制由来自数学、通讯、计算机领域的专家共同设计完成；以太坊项目参与者和区块链社区大 V 等一起设计了“En-Tan-Mo”的框架体系和权益分配机制；前谷歌、迅雷、百度等顶尖互联网公司具有丰富经验的软件工程师参与了项目纯自主代码设计。而依托 ETM 科学院的 En-Tan-Mo，使其还具有一个特别之处，即 ETM 的所有理论设计都采取双重验证的流程：先由数学家完成共识建模和数值模拟仿真实验；再由计算机和通信专家以严苛的标准对 En-Tan-Mo 项目的理论设计做实际验证。

当前的区块链乱象中，一个最有意思的现象是：作为一个世界前沿性课题，绝大多数的区块链项目都没有科学家的参与。

互联网世界中的每一座里程碑都有科学家的身影，我们熟知的，如人工智能 AI 的领导者谷歌研究院、大数据领域的王者阿里研究院等等，更不用提，万维网本身就是由欧洲物理研究所的科学家设计的。因此，我们认为，真正的区块链项目必须要有自己的科研人员和团队，这也正是 ETM 科学院成立的意义所在。

1925 年，贝尔电话公司成立了一个贝尔电话实验室公司，随后改名为贝尔实验室，这个实验室，总共诞生了 11 个诺贝尔奖、16 个最高科技奖、技术奖项、4 个图灵奖以及其他许许多多的奖项，还有 3000 多项专利，为世界科技作出了巨大贡献。

ETM 科学院也聚合了这样一群来自全世界各地一流高校的顶尖学者，他们有科研实力、有社会情怀以及远大理想。由于学科背景的不同，团队开放度高，今后还有更多的扩充可能性和学术脉络，由于从业背景的不同，团队具备更广阔的视野以及更具创新性的碰撞。ETM 科学院的未来，也具有无限可能。

结语

回溯工业革命和互联网的兴起，从没有人会将一次次迭代的伟大意义定格在蒸汽机、汽车、计算机的发明上——世界铭记的是，这些别开生面的突破为改变社会发展方式带来的剧变。所以，如果区块链是一场划破时代的技术革命，那么它一定和电气、计算机、互联网等技术文明相似，在面对不同时期的挑战时，最终成为沿革人类进步史的路径，而绝非单纯的目的。

诚如 Haseeb Qureshi 在其文章《区块链：一场始料未及的革命（Blockchain: The Revolution We're Not Ready for）》中指出的，“区块链将颠覆整个社会，它将使得仅存在于乌托邦和哲学家白日梦中的治理体系得以实现。”

这条路一定不会是坦途，但它所能释放的想象空间，让人充满向往。

韦伯曾经说过：“知识之树所结出的果会打破所有人的愉悦，但无可回避的果实并非其他，就是这样一种见识：既然我们对这些价值的冲突不可能置若罔闻，那么我们就必须要明白，那一个个的重要的行动，更不要说是作为整体的人生，如果不应像一个自然事件一样消逝，而是应被我们有意识地引导，那么它便意味着一连串的根本的决定，而通过这些决定，灵魂也像在柏拉图那里一样选择了自己的命运，也就是说，它的行动和存在的意义。”

区块链的诞生，释放了我们关于这个世界的想象空间。它带给我们的，不仅是经济资本、社会资本、文化资本重新分配的想象，更是新的本尼迪克特安德森所言的“想象的共同体”的凝聚。在这种凝聚下，我们想象新的公共空间下可能改变的人的社会存在状态、价值和意义，可能实现的人的回归，可能充满的新的情感、期许、感召，以及新的社会伦理的建构等。从这个层面来说，区块链的意义是经济学的、社会学的，更是哲学的、人类学的。

正是如此，尽管比特币已不完美，但“中本聪”仍是值得我们敬仰的一种存在。中本聪的最大贡献，不是比特币，而是让区块链这一新兴技术进入大众视野。中本聪的最大魅力，不在于他可能是世界上最富有的人之一，而在于其为我们呈现的美好蓝图：它以大众福祉为旨归，不断对去中心化进行尝试；保护个体利益，给予个人安全、隐私、参与权以尊重；它根基于经济学与数学等现代科学，为人类走向更好未来而不懈努力。这，就是让 ETM 坚定追随与发扬的“中本聪精神”。

在比特币跌宕起伏的精彩历史中，在真真假假中本聪的闹剧中，中本聪彻底消失了。他在邮件里只留下了一句话：“我们每个人都是中本聪”。确实，我们每个人都是中本聪，因为我们每个人都是区块链技术的践行者和参与者。

“

AGREED VALUE SHARED BENEFIT

”