

```

// Private fields
let library;
let self;
const __private = {};
__private.lastBlock = {};
__private.lastReceipt = null;

__private.isReady = false;
__private.cleanup = false;
__private.isActive = false;

/** 
 * Main blocks methods. Initializes submodules with
scope content.
 * Calls submodules.chain.saveGenesisBlock.
*
* @class
* @memberof modules
* @see Parent: {@link modules}
* @requires helpers/constants
* @requires modules/blocks/api
* @requires modules/blocks/verify
* @requires modules/blocks/process
* @requires modules/blocks/utils
* @requires modules/blocks/chain
* @param {function} cb - Callback function
* @param {scope} scope - App instance
* @returns {setImmediateCallback} cb, err, self
*/
// Constructor
class Blocks {
constructor(cb, scope) {
library = {
logger: scope.logger,
};

// Initialize submodules with library content
this.submodules = {
api: new blocksAPI(
scope.logger,
scope.db,
scope.logic.block,
scope.schema
process: new blocksProcess(
scope.logger,
scope.logic.block,
scope.logic.peers,
scope.logic.transaction,
scope.schema,
scope.db,
scope.sequence,
scope.genesisblock
utils: new blocksUtils(
scope.logger,
scope.logic.account,
scope.logic.block,

```

# EN-TAN-MO SCIENCE

```

scope.genesisblock
),
chain: new blocksChain(
scope.logger,
scope.logic.block,
scope.logic.transaction,
scope.db,
scope.genesisblock,
scope.bus,
scope.balancesSequence
),
};

// Expose submodules
this.shared = this.submodules.api;
this.verify = this.submodules.verify;
this.process = this.submodules.process;
this.utils = this.submodules.utils;
this.chain = this.submodules.chain;

self = this;

this.submodules.chain.saveGenesisBlock(err =>
setImmediate(cb, err, self));
}

}

/** 
* PUBLIC METHODS
*/
/** 
* Last block functions, getter, setter and isFresh.
*
* @property {function} get - Returns lastBlock
* @property {function} set - Sets lastBlock
* @property {function} isFresh - Returns status of last
block - if it fresh or not
*/
Blocks.prototype.lastBlock = {
if (!__private.isActive) {
// Module ready for shutdown
return setImmediate(cb);
}
// Module is not ready, repeat
setImmediate(function nextWatch() {
if (__private.isActive) {
library.logger.info('Waiting for block processing to
finish...');
setTimeout(nextWatch, 10000); // 10 sec
} else {
return setImmediate(cb);
}
});
};

/** 
* Get module loading status
*/

```

简体中文

EN-TAN-MO

# 引言

En-Tan-Mo，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。2011 年诺贝尔经济学奖得主、理性预期学派领袖托马斯·萨金特教授以及来自于美国加州理工大学、美国马里兰大学、法国庞加莱研究所的各领域学者们，将博弈论的研究成果革命性融入区块链中，共同创造了具有 SHD 完备性的 En-Tan-Mo。在 En-Tan-Mo 世界中，SCV 矿工和 Pareto 矿池，在 Kantorovich 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，帮助所有渴望公平、民主、自由的人们，在区块链带来的去中心化思潮中，均衡的获得属于每个个体的最高权益。En-Tan-Mo，不仅仅是一个纳什均衡的区块链底层平台，还包含了最丰富的应用和最广泛的社区，甚至包含了严谨的数学论证和丰富的经济学内涵，从而形成了完整的哲学思想和系统。因此，“技术白皮书”的形式难以体现出 En-Tan-Mo 的真正优势，研发团队以资料汇编的形式从世界、哲学、数学、经济、计算、生态等多维度向每一个关注 En-Tan-Mo 的人进行阐述。

## 名词解释：

**纳什均衡：**美国数学家，诺贝尔经济学奖得主约翰·纳什提出：在一个多人参加的博弈过程中，所有参与者各自选择的策略所组成的一个集合，任何人都不能通过单方面改变自己的策略（作弊）获得更大的利益。En-Tan-Mo 的数学家通过巧妙的设计双共识机制，从而保证理性的参与者集合达到纳什均衡状态。纳什均衡是 En-Tan-Mo 的最核心问题之一，在“En-Tan-Mo 数学”和“En-Tan-Mo 经济学”部分均有更详细阐述。

**SHD 完备性：**指区块链的三个最重要指标同时具备：安全性（Safe）、高性能（High-performance）、去中心化（Decentralization）。现有区块链系统均存在三者不可兼得的问题，如何解决 SHD 完备性是区块链 3.0 面临的主要问题。SHD 完备性在“什么是 En-Tan-Mo”章节里有更详细阐述。

**Kantorovich 共识：**Kantorovich 共识是一种革命性的 UPOS 权益证明算法，是 En-Tan-Mo 基础架构的重要组成部分。Kantorovich 共识将工作量和股份授权巧妙的融合并形成归一化权益，得到全新的统一权益证明协议（Unified Proof of Stake, UPOS），从而保证 En-Tan-Mo 的纳什均衡。Kantorovich 共识是第一个通过科学验证均衡性和安全性的 UPOS 权益证明协议，在“En-Tan-Mo 经济学”部分有更详细阐述。

**SCV 矿工：**En-Tan-Mo 中通过基础算力测试并由选举制度推选的合作竞争矿工，被称为 Smart Ledger Scrivener，智能账本记录员，简称为 Scrivener 或 SCV 矿工。候选矿工根据得票高低当选 SCV 矿工和候补矿工，获得上传区块权利，验证区块义务和区块奖励。SCV 矿工在“En-Tan-Mo 经济学”部分有更详细阐述。

**监察官：**ETM Token 的持有者在投票选举 SCV 矿工团队时的身份，被称为“监察官”。监察官将手上的 Token 在“En-Tan-Mo”中通过上凸权益映射转化为可投票数，每投票周期给予相应奖励。监察官来自拉丁语 tribunus，表示古罗马时代对行政官员或军事实行监督的官职或委员会，代表规范化、专业化和职业化。监察官在“En-Tan-Mo 经济学”部分有更详细阐述。

**Pareto 矿池：**在 En-Tan-Mo 中，所有矿机节点组成一个合作竞争型的矿池，每个出块周期选择若干 SCV 矿工有序出块，“En-Tan-Mo”将该周期中未被选中的所有矿机组建成 Pareto 矿池，运用特有的侧链技术和联盟策略，根据即时收益算法分析，参与外部区块链的生产出块，按照矿机提供算力分配矿池收入，从而保证所有矿机的正收益。帕累托最优（Pareto Optimality）是指资源分配的一种理想状态，Pareto 矿池最优是公平与效率的“理想王国”。Pareto 矿池在“En-Tan-Mo 经济学”部分有更详细阐述。

**中心链和衍生链：**En-Tan-Mo 的链状结构为一条中心链和多条衍生链，衍生链可

以通过中心链的“平行链交互层”实现其与中心链、其他衍生链及外部区块链链之间的双向资产传递，这使得用户能用已有的资产来使用“En-Tan-Mo”系统。中心链是主链，负责 En-Tan-Mo 网络安全及价值交换。衍生链是一种特殊的区块链，每一个衍生链对应一个 DAPP，是一个独立的、隔离的系统，继承和复用主链强大的区块链技术，每个应用都拥有一套个性化的账本，拥有个性化的 Token。中心链和衍生链在“En-Tan-Mo 生态”部分有更详细阐述。

**米尔商城：**“En-Tan-Mo”系统通过方便而又高效的米尔商城，帮助企业或开发者更快更经济的实现区块链应用，使得用户能够享受到去中心化带来安全和便利。“钻石之城”米尔矿是目前世界最昂贵的钻石矿，米尔商城面向开发者和用户，是 En-Tan-Mo 的价值所在。米尔商城在“En-Tan-Mo 生态”部分有更详细阐述。

**POW：**工作量证明，Proof of Work，简称 POW，是一种应对拒绝服务攻击和其他服务滥用的经济对策，它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间。比特币网络中任何一个节点，如果想生成一个新的区块并写入区块链，必须解出比特币网络的工作量证明的谜题。这道题关键的三个要素是工作量证明函数、区块及难度值。工作量证明函数是这道题的计算方法，区块决定了这道题的输入数据，难度值决定了这道题所需要的计算量。

**POS：**股权证明，Proof of Stake，简称 POS。POS 提出了币龄的概念，币龄等于参与者持有 Token 的量和时间的乘积。与 POW 消耗算力解题不同，POS 消耗的是虚拟的币龄，币龄作为记录股权的证明，持有量对应投票权和收益权，即根据币龄的多少分配相应的权利和利息。

**DPOS：**委托股权证明，Delegated Proof of Stake，简称 DPOS。DPOS 通过不同的策略，不定时的选中一小群节点，这一小群节点做新区块的创建、验证、签名和相互监督，这样就大幅度的减少了区块创建和确认所需要消耗的时间和算力成本。常规 POW 和 POS 于任何一个新加入的区块，都需要被整个网络所有节点做确认，这是 DPOS 与以上两种方法的不同点。

**UPOS：**统一权益证明，Unify Proof of Work，简称 UPOS。En-Tan-Mo 的数学家巧妙的将 POW 和 DPOS 融合在一起，颠覆性地提出了双共识机制，让每个参与者都可以以矿工或投票人的身份平等参与区块链的建设并获得均衡的奖励，矿工之间，投票人之间，矿工和投票人之间均通过简洁有效的 UPOS 共识进行调节，从而保证理性的参与者策略集合达到一种完美的纳什均衡状态。

# 0.0 En-Tan-Mo 是什么

## 区块链回顾

简要的回顾区块链历史，将有助于理解 En-Tan-Mo 的革命性。

2008 年，中本聪发表了著名的论文《比特币：点对点的电子现金系统》，2009 年 1 月创世区块被挖掘出来，“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.” 像魔咒一样开启了比特币区块链的时代。2013 年比特币发布了其历史上最重要的版本，该版本完善了比特币节点本身的内部管理、网络通讯的优化，比特币电子现金开始产生全球影响力。比特币作为第一个加密数字货币大获成功，但是比特币糟糕的扩展性严重制约区块链的后续发展。我们称比特币为区块链的 1.0 时代。

为了解决比特币扩展性的问题，Vitalik Buterin 创立了以太坊。以太坊有着明确清晰的设计思路和框架体系，从 EVM 论文到 ICO、从不同版本的 POC 到 2015 年的 Frontier 阶段，从 POW 的 Metropolis 阶段到 POS 的 Serenity 阶段，以太坊的图灵完备性，智能合约，抵抗 ASIC 设计和区块链应用构成区块链 2.0 时代的主要标志。以太坊提供了平台接口和编程语言，使开发人员能够建立和发布下一代分布式应用。

后面的故事开始被人熟知，2018 年 2 月比特币算力达到 20EH/S，Github 上超过了 9 万个区块链的开源项目，中国、美国、英国、新加坡、俄罗斯、日本、韩国等 90 多个国家都已加入区块链技术的研究。2008 年到 2018 年，区块链的思想和理念被大众消化、摸索、实践，这一切仅仅用了十年时间。对比互联网的发展，一眼就能看出区块链的成功：1974 是互联网元年，美国国防部国防高等研究计划署（ARPA）开发公布了 TCP/IP 协议，20 年后也就是 1994 年中国正式接入国际互联网。

## 0.1 为什么要建设 En-Tan-Mo

En-Tan-Mo 旨在创造一个成熟、均衡、效率的价值传递世界。因此，En-Tan-Mo 从创立初始就明确了需要解决的两条主线问题。

### 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。中本聪提出区块链依靠概率强一致性（Probabilistic Strong Consistency）实现一致性共识，并称为 Nakamoto 共识。

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。

中本聪在低效 CPU 的前提假设下，保证了安全性 S 和去中心化 D 并存，却几乎忽略了高性能 H，由于共识算法和区块容量的设计，比特币平均十分钟产生一个区块，1 秒钟只能处理 7 笔交易。不仅如此，随着高性能“ASIC 矿机”的出现，普通的 CPU 算力获得收益的概率降为 0，矿机轻易的获得了超线性收益，后期矿场和矿池的出现更是彻底打破了去中心化 D，现在比特币显然不是一个平等参与的社区。更糟糕的是，矿场和矿池不断垄断算力，必然会有少数参与者超过 51% 的算力（决定权），安全性 S 也会无法保证。因此，我们说比特币的区块链已经失去了 SHD 的平衡。

以太坊为了避免 ASIC 矿机带来的破坏性影响，采取了“反复读缓存”的 ASIC 抵抗算法，在短时间内维系了安全性 S 和去中心化 D，但其最引以为豪的智能合约的第一个大规模应用“CryptoKitties”，就令以太坊系统完全崩溃，高性能 H 显得尤为低下。而抛弃了 POW 共识，转向 POS 或 DPOS 共识的区块链系统，大幅提高了系统性能，却忽视了去中心化的根本意义，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。

En-Tan-Mo 通过设计基于 UPOS 的 Kantorovich 共识机制，采用矿工团队选举制度，保证权证拥有者和区块矿机的分离和各自权益，在保障安全性的前提下提高效率，又保持了去中心化的基本属性，从而满足 SHD 完备性。

### 均衡价值传递

互联网时代改变了信息传递的方式和理念，人们通过互联网技术便捷、低成本的传递信息，指数级的提高效率和控制成本，并且获得了全新的产品或服务。然而，信息传递和价值传递的概念不同，互联网不具有点对点的价值传递功能，价值传递依赖于中心机构承担记账功能，因为价值传递需要保证权属的唯一性，这不同于信息传递的可复制性。

比特币通过分布式共享记账技术，建立去中心化的信任，不再依赖中心化机构，从而支持点对点的价值传递，改变了价值传递和定价规则。由于矿池的出现，

比特币的价值传递发生了倾斜，普通参与者和矿机拥有者的价值获取不再对等，价值迅速向矿池集中。

以太坊通过 ASIC 抵抗算法，并消耗“Gas”以抑制链上资源，从而在一定程度上减慢了矿机的价值积累速度，我们认为是一种消极和短期的作法，对区块链的长远发展非常不利。POS 或 DPOS 共识，尝试通过打破 POW 算力垄断实现均衡，但是实力雄厚的 Token 拥有者仍然掌握了价值导向，中心化程度比 POW 更加集中。

根据目前区块链及加密货币的发展现状，价值以一种近似 80/20 定律的方式集中在少数人手里。En-Tan-Mo 希望改变现有价值传递的方式，让价值完成开放式流转，给用户提供一个均衡的价值传递体系。En-Tan-Mo 认为每个个体同时是服务的提供者和购买者，即是买家也是卖家，去中心化的市场核心是价格调节机制，而价格将以一种动态均衡的方式自组织地形成。En-Tan-Mo 使用平均场博弈论的思想研究价格动态波动，算力或投票权与权益之间应当是正相关，但并非线性的关系，从而抑制权力的过度集中，开创新一代的均衡价值互联体系 IoV ( Internet of Value )，对商业模式和经济社会产生重大变革。

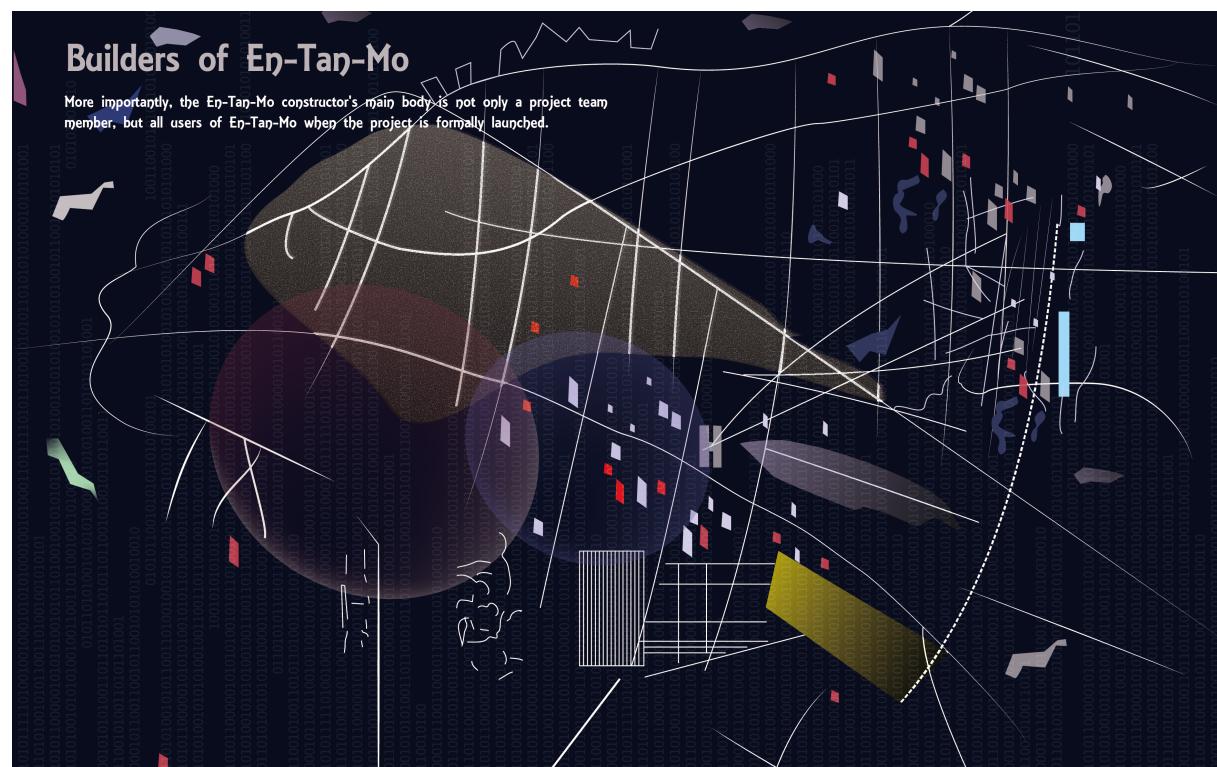
## 0.2 En-Tan-Mo 的建设者

En-Tan-Mo 的设计师和建设者来自于全球顶尖大学和研究所。最初团队由法国的数学家们组成，他们将博弈论的成果融入区块链中，并将 Entente 和

Transaction, Mobius 三个单词的精髓抽提出来，命名为 En-Tan-Mo。随后通信专家、计算机专家、经济学专家和哲学家迅速加入了 En-Tan-Mo 的团队，包括美国加州理工大学、美国马里兰大学、法国庞加莱研究所的各领域学者们。非常荣幸的，2011 年诺贝尔经济学奖得主、理性预期学派领袖托马斯·萨金特教授也欣然加入团队并担任高级顾问。从此，En-Tan-Mo 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。

En-Tan-Mo 目前的工作成果要归功于理论与实验，软件与硬件，技术与商业各个不同团队和负责人之间密切的配合和共同劳动。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 科学”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。

更重要的是，当项目正式上线后，En-Tan-Mo 的建设者主体就不仅仅是项目团队成员，而是 En-Tan-Mo 的所有用户。En-Tan-Mo 倡导自演进和共同参与，欢迎所有用户按照自己的需要，积极上传组件和发展衍生链。En-Tan-Mo 项目组将把自己的角色定义为奠基人和基础设施建设维护者，继续尽最大的努力为这个体系提供安全，稳定，高效的技术服务。同时，项目组也欢迎科学家，工程师和一切认同 En-Tan-Mo 理念的研发者加入我们的团队或以各种灵活的方式合作。



## 0.3 En-Tan-Mo 科学

En-Tan-Mo 并非一个简单的区块链项目，而是有着丰富内涵的科学体系，包含了完整的哲学思想，数学论证，经济学印证和广泛的应用生态，研究团队以资料汇编的形式尽可能详尽的向每一个关注 En-Tan-Mo 的人进行解释。

---

第一章是 En-Tan-Mo 世界。En-Tan-Mo 以服务提升与价值创新塑造区块链 3.0 的世界，En-Tan-Mo 的世界将专注于持续优化、重构、创造市场，也是均衡商业体制本质的回归和重塑。

第二章是 En-Tan-Mo 哲学。En-Tan-Mo 是一个全新的价值传递体系，链接一切有价值的事物，因此，复杂系统与多元结构，共识与价值，动态均衡与分权，自演进与开放性泛化为 En-Tan-Mo 的去中心化特征。

第三章是 En-Tan-Mo 数学。从数学的角度分析去中心化的 En-Tan-Mo，包括已经完成的数学论证和项目的发展规划，以及研究主要应用的数学工具。

第四章是 En-Tan-Mo 经济学。SCV 矿工和 Pareto 矿池，在基于 UPOS 机制的 Kantorovich 共识机制下相互支撑、相互激励，形成统一的 UPOS 算法。En-Tan-Mo 不单是技术的创新，更是商业逻辑的改革。

第五章是 En-Tan-Mo 计算。软件工程师编写了 En-Tan-Mo 的数据结构、流程图、API 接口和全部代码，用程序的形式体现了 Kantorovich 共识机制的精美和巧妙。

第六章是 En-Tan-Mo 生态。En-Tan-Mo 的跨链技术包括中心链、衍生链，将区块链从分散的孤岛中拯救出来，是区块链向外拓展和连接的桥梁，从而构建了一个可以包含千万级应用的区块链生态系统。

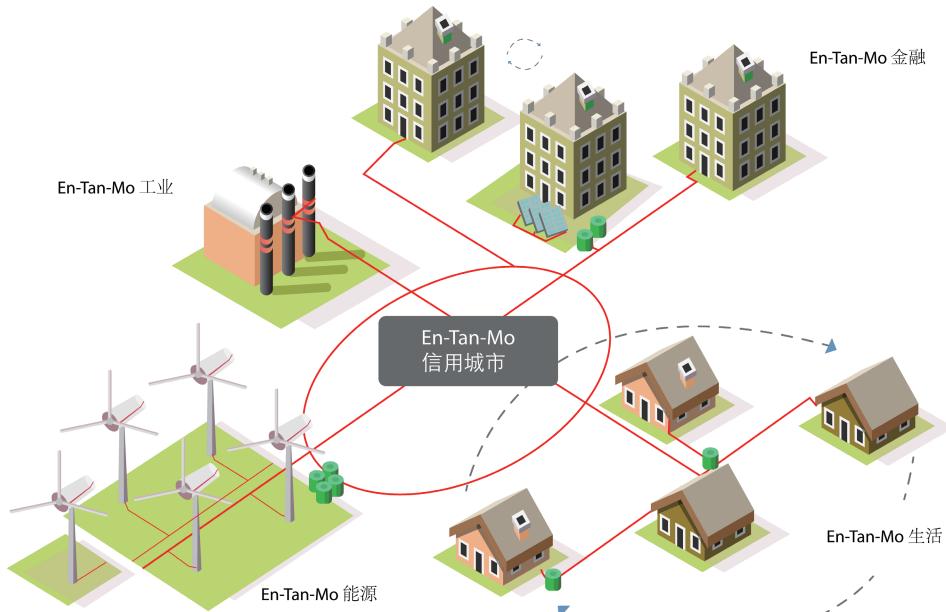
第七章是 En-Tan-Mo 组织结构。En-Tan-Mo 社区由 En-Tan-Mo 基金会，ETM FinTech 和 ETM BD 三个组织构成。基金会对用户社区提供全方位的支持，保证 En-Tan-Mo 项目的顺利运营；ETM FinTech 是隐私安全研究和系统开发的组织实体；ETM BD 是协助商业企业的合作伙伴组织。

---

### 参考文献：

- 【01】S. Nakamoto. A Peer-to-Peer Electronic Cash System. [www.bitcoin.org/bitcoin.pdf](http://www.bitcoin.org/bitcoin.pdf), 2009.
- 【02】M. E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4):401-406, 1980.
- 【03】V. Buterin. Long-range attacks: The serious problem with adaptive proof of Work. <https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-withadaptive-proof-of-work/>, 2014.
- 【04】V. Buterin. Proof of stake. <https://github.com/ethereum/wiki/wiki/Proof-of-StakeFAQ>, 2016.
- 【05】G. Wood. Ethereum: A secure decentralised generalised transaction ledger. <http://gavwood.com/Paper.pdf>.
- 【06】M. Mainelli, C. von Gunten. Chain of a lifetime: How blockchain technology might transform personal insurance. Dec 2014. Z/Yen Group, Long Finance.
- 【07】J.-P. Delahaye. Les blockchains. "Les big data à découvert". Editions du CNRS, Chapitre 15, 118, 2017.
- 【08】J.-P. Delahaye. Le Bitcoin: première cryptomonnaie. "1024" Bulletin de la Société Informatique de France, n° 4, pp. 67-104, octobre 2014.
- 【09】J.-P. Delahaye. Le Bitcoin: une monnaie révolutionnaire. Laboratoire d'Informatique Fondamentale de Lille, janvier 2014.
- 【10】M. Perrin. Distributed Systems: Concurrency and Consistency. ISTE Press, Elsevier, 2017.
- 【11】R. Perez-Marco. Bitcoin and Decentralized Trust Protocols. Newsletter of the European Math. Soc., 100 p.32, 2016.
- 【12】W. Feller. An introduction of probability theory and its applications. Vol.1, 3rd ed. John Wiley & Sons, 1957.
- 【13】Л.В. Канторович, Математические методы организации планирования производства. Издание Ленинградского государственного университета, 1939.
- 【14】С. М. Меньшиков. Актуальность экономической модели Л. В. Канторовича в наше время. Зап. научн. сем. ПОМИ, 2004, том 312, 30–46.
- 【15】M. Doob, Kantorovich. On Optimal Planning and Prices. *Science & Society*, Vol. 31, No. 2 (Spring, 1967), pp. 186-202.
- 【16】C. Grunspan, R. Pérez-Marco. Double spend races. arXiv:1702.02867v2 [cs.CR].
- 【17】R. Perez-Marco. A simple dynamical model leading to Pareto wealth distribution and stability. arXiv:1409.4857, 2014.
- 【18】J. P. Aubin. I. Ekeland. Applied Nonlinear Analysis. Wiley-Interscience, 1984.
- 【19】J. P. Aubin. Optima and Equilibria. Springer-Verlag, 1998.
- 【20】Notes on Mean Field Games, from Pierre-Louis Lions' lectures at Collège de France.
- 【21】J.-M. Lasry, P.-L.Lions. Mean field games. *Jpn. J. Math.*, 2 (2007), No. 1, 229-260.
- 【22】M. Kamgarpour, H. Tembine. A Bayesian Mean Field Game Approach to Supply Demand Analysis of the Smart Grid. 2013 First International Black Sea Conference on Communications and Networking.
- 【23】T. J. Sargent, Lars Ljungqvist. Recursive Macroeconomic Theory. MIT Press, 2000.

# 1.0 En-Tan-Mo 世界



## 1.1 En-Tan-Mo 世界蓝图

“En-Tan-Mo”是一次打破国界的科学革新，其内涵涉及哲学、数学、经济学、计算科学，相互交织、相互印证。“En-Tan-Mo”同时也在诠释一个颠覆性的全新世界。

“En-Tan-Mo”的世界蓝图：一根根纬线代表一条条供求，每个参与个体就是一根自由的经线，他可以与任意纬线发生关系，还可以自己增加纬线。而这一经纬交织的网络通过混沌排序机制，不断自主学习和自主完善。在“En-Tan-Mo”世界里，每个个体的行为都在塑造世界。这种职业自由使人们更理性、更积极、更自主、更长远。

金字塔的崩解，真正的去中心化意味着不再有集权和垄断，En-Tan-Mo创造的是一个自由平等，富有创造性，同时高效均衡的世界。这是一个非自上而下的，完全由供需市场驱动的世界，让价值完成开放式流转，给大众提供一个均衡的价值传递体系。在En-Tan-Mo世界里，每个人不再被动的每月领取固定薪水，而是自发参与不同项目得到直接奖励，同时，自己也可以创造项目发放奖励。每个人同时站在价值传递的两端，而交易价格将以动态均衡的方式自发调节以保证公平。

更为重要的一点：下一代区块链技术消除了职业的地缘限制，人类将成为全新的游牧民族，根据需要，在En-Tan-Mo世界中自由的行动。

## 1.2 数字货币世界史

仰望互联网的星空，“区块链”更像是一颗特别的

新星在这片天空中闪耀，在它的面前，任何中心化的应用都将成为历史。区块链中的“数字权证”就像人类文明长河中的货币，将会极大地提升网络交易的速度和容量，使网络不再仅仅是信息共享的通道，更是价值传递的桥梁。2009年，比特币率先带来了一个“数字黄金”系统，淘金的热潮一次又一次地席卷着整个互联网络。到2018年伊始，大约30000PH/s算力每小时产生仅仅6个区块75枚比特币。根据Digiconomist的比特币能源消费指数显示，当前比特币“挖矿”所产生的年用电量估计为39.45TWh，等价于20亿美元。如此庞大在算力进入到“数字黄金”的淘金热潮中，正如1848-1851年美国淘金热期间，人口急剧增长，衣食住行变得陡然紧张，尤其是服务业的发展无法满足社会的需要，美国批发商品的价格指数847提高到1025，这些情况与2017年的比特币世界非常接近。但难以想象的是，历史长河中几百年形成的“金本位”货币体系，在比特币世界中仅仅用了9年。

2013年，Vitalik Buterin首次提出以太坊的概念，“下一代加密货币与去中心化应用平台”，这一次的革新制造出具有图灵完备性的智能合约体系，也把以太币推向了“数字汽油”的宝座。以太坊提供各种模块让用户来搭建应用，使建立应用的成本和速度都大大改善。具体来说，以太坊通过一套图灵完备的脚本语言（Ethereum Virtual Machine code，简称EVM语言）来建立应用，所建立的应用被称为智能合约（简称合约），这是以太坊的核心。智能合约相当于一个以太坊系统里的自动代理人，当用户向合约的地址里发送一笔交易后，该合约就被激活，然后根据交易中的额外信息，合约会运行自身的代码，最后返回一个结果，这个结果可能是从合约的地址发出另外一笔交易。需要指出的是，以太

坊中的交易可以是一次交易也可以执行一段指令，这样的优势是使以太币被大量使用起来，但是，这又会过于消耗以太坊的资源，导致了以太坊随时可能被合约拖垮。这些特点使以太坊就像一条无法拓展的高速公路，所有的应用就像公路上的汽车，以太币成为汽车消耗的汽油。目前，以太坊上虽然已经有超过 9 万种合约，但是，这些合约几乎全部是同质化的 Token 应用，这就像一条狭窄拥堵而又收费过高的公路上难以承载大型汽车一样。

简而言之，比特币代表的是金本位经济，以太坊代表的是能源经济，在这两种经济生态中，可以理性地预测出未来的发展走向。

金字塔化的世界：“黄金和石油”能够成为世界经济的柱石，第一因素是稀缺性。而能源经济能够取代金本位经济是因为能源具有核心使用价值，成为人类生存最重要的不可再生的消耗品。这种资源型的属性使得世界变成一个超级金字塔，某些国家成为金字塔的顶端，更多的国家成为以提供廉价劳力的第三世界国家。国家中形成社会，社会又是一个金字塔，强有力的企业成为金字塔的顶端，大量的微小企业或组织在为这些顶端的企业提供廉价的服务。企业和组织的内部又形成一个个小的金字塔，绝大多数的普通劳动者为企业提供劳力服务，获得微不足道的工资报酬。企业和组织之间也形成金字塔的结构，顶端企业和组织获得资源的成本越来越低，底端却承受了越来越大的压力。整个世界就像层层嵌套的金字塔，金字塔的顶端对底端施加的压力越来越大。随着时间的推移，终有一天，金字塔会坍塌下来，经济危机被引发了。然而，这不是结束，金字塔又会逐渐自发的建立起来，最后坍塌，一次次的往复。

## 1.3En-Tan-Mo 大迁徙

1) POW 和 DPOS 双稳态结构打破垄断和中心化趋势

POW 创世说：在现实世界中，人类最大的共识是“劳力”，通过凝结最等量的劳力而形成的商品演变成一般等价物，即是货币。在区块链的世界中，最广泛的共识是“算力”，通过凝结最等量最公平的算力而形成的数字权证必然会演变成一般等价权证。因此，引入公平等量的算力构建起一个初始稳定的平衡，是未来权证价值稳定的基础。比特币、以太坊的创立伊始，也正是基于公平稳定的算力而逐步形成的普遍共识。

POW 和 DPOS 双稳态：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的形成和坍塌。而 DPOS 带来的高效使得公平被更快的打破，因为没有了算力的公平支撑，金字塔会更快的形成，这就像现实中的各种权证，“超发”和“集中”会更快的形成。POW 和 DPOS 交织的双稳态 UPOS 结构，使 POW 和 DPOS 的集中化和中心化被最大程度的限制，这种去中心的机制在保证高效的

同时又保证了安全性，持币人与矿工均可以参与到 En-Tan-Mo 中，共同参与社区的重大决定，决定未来的更新和发展，这是 En-Tan-Mo 世界的一项创举。

2) 矿工合作竞争关系是一种完美的公平联盟法则

POW 机制下需要矿工经过大量尝试计算，计算时间取决于机器的哈希运算速度，矿工之间是单纯的竞争关系，导致收益过低和资源极大浪费。因此，矿工们组成矿池的方式结盟，但又导致了中心化趋势加剧。合作竞争理论认为矿工活动是一种特殊的博弈，是一种可以实现双赢的非零和博弈，En-Tan-Mo 世界通过博弈思想分析矿工的互动关系，为所有参与者建立起公平合理的合作竞争关系。

只有合作竞争关系才能创造参与者价值链的新观念，利用价值链来描述所有参与者合作竞争的互动关系。价值链的思想强调了 En-Tan-Mo 世界中同时竞争与合作两种行为，两者的结合意味着一种动态的关系，而不是“竞争”和“合作”所表达出的单独的意思。矿工之间全新的关系可以用三个词定义：贡献 (Impact)、亲密 (Intimacy) 和远景 (Vision)。这涵盖了矿工建立合作竞争关系后能够创造的具体有效的成果，即能够增加的实际生产力和价值，成果主要来源于三个方面：一是减少重复与浪费，最高程度节约算力和电能；二是借助彼此的核心能力，加快整个 En-Tan-Mo 的出块速度；三是创造新机会，参与外部区块链的建设。

3) 动态供需和理性选择带来纳什均衡

加入 En-Tan-Mo 即是选择了数字化世界中的最佳联盟。而在以往的矿池联盟中，往往采取的是最优控制理论，在某一时刻所选择的最优，随着时间的推移，所有参与者的收益会锐减，这是因为最优的选择必然是会引起最大的外部竞争，从而最终使所有竞争者的收益下降。在托马斯·萨金特教授的指导下，En-Tan-Mo 的科学家运用理性经济预测理论，为合作者选择处于上升通道的动态供需选择，这是因为只有动态供需才能满足参与者的理性选择要求，实时形成纳什均衡。选择性合作即是供需关系的体现，价值正是成本与需求的有机结合。En-Tan-Mo 世界中的 POW 体现的成本因素，与 DPOS 体现的供需关系，相互纠缠，才能形成最大价值体现的统一权益法则 UPOS，并得到相对稳定的价值曲线。

4) 上凸函数机制保证参与人均衡权益

在以往的世界中，联盟内部更趋向于更强有力的合作者，越强的合作者所获得的收益比例会超越更弱小的合作者，这种超线性的收益模型最终会伤害到相对弱小的合作者，正是这个过程促使了金字塔的形成与坍塌，到最后，即使是强大的合作者也会因为金字塔的坍塌而受损。只有注重长尾效应的 En-Tan-Mo，使更广泛的合作者亦得到相对可观的收益，成为一种具有永续特性联盟机制，那么即使是强大的合作者在初始让出了部分的利益，也会随着时间的推移获得比以往更大的收益。

En-Tan-Mo 世界的基础正是一种摒除了“独角兽矿池”的贡献等量算法，甚至将这种“完全等量”（线性化算力函数）转变为一种“上凸函数”，这使得公正的天平还稍微向更广大的参与者去倾斜，通过理性的经

济学预测，这会促使更大的受众产生更广泛的共识，从而使 En-Tan-Mo 成为一种最为公平公正的区块链网络。

### 5 ) 混沌排序抵抗女巫攻击和联合作弊

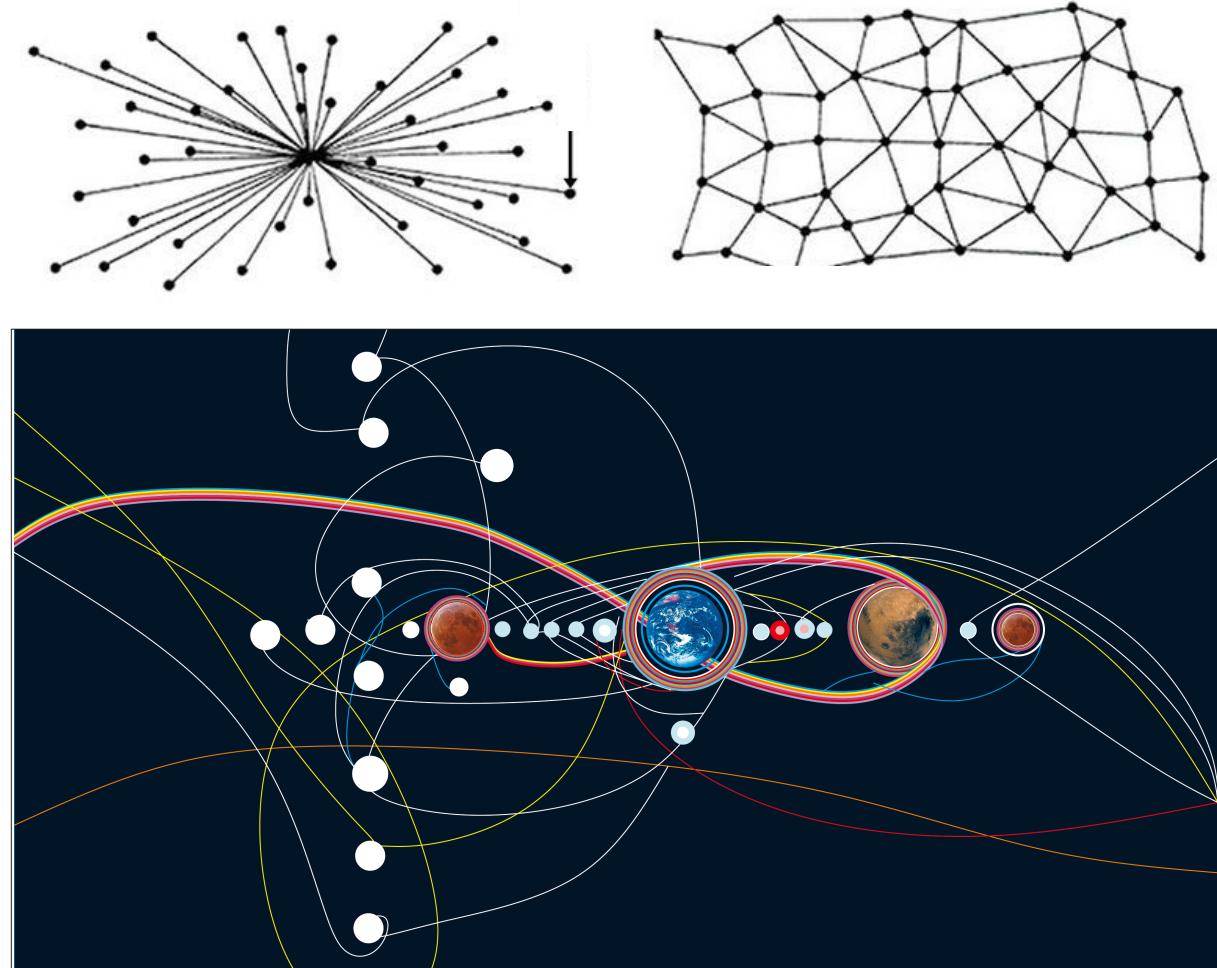
区块链的 SHD 理论中，去中心化和安全性之间存在一个无法回避的问题：女巫攻击（Sybil Attack）。女巫攻击是指利用社交网络中的少数节点控制多个虚假身份，从而利用这些身份控制或影响网络的大量正常节点的攻击方式。由于区块链节点的对等性，单一节点具有多个身份标识，可以通过控制系统的大部分节点来削弱冗余备份的作用。联合作弊也会出现相同的问题。

En-Tan-Mo 的数学家运用现代动力系统、拓扑几何理论，研究复杂不变集的结构与分岔，得出系统稳定性与复杂行为控制方法，从而基于混沌理论的遍历性和对初始条件的敏感依赖性提出了强大的混沌排序方法，为区块上传顺序打造了高度的伪随机性机制，同时又具有可以抵抗量子攻击的最高级的安全性。

### 6 ) 开放的组件库和友好的开发者大厅定义了自演进和共同参与的发展方向

En-Tan-Mo 以 BaaS (Blockchain as a Service, 区块链即服务) 为理念，以微服务为基准，以自演进组件库为核心，以开发者社区为生态原动力，为其他区块链提供适配平台完成资产和应用的自由转移，为非区块链的应用和数据提供软通道完成双向调用，为开发者提供共享大厅完成组件上传、评价和奖励的功能，为普通用户提供 BaaS 网关实现无障碍服务调用。倡导自演进和共同参与的 En-Tan-Mo，欢迎所有用户按照自己的需要，积极上传组件和发展衍生链。

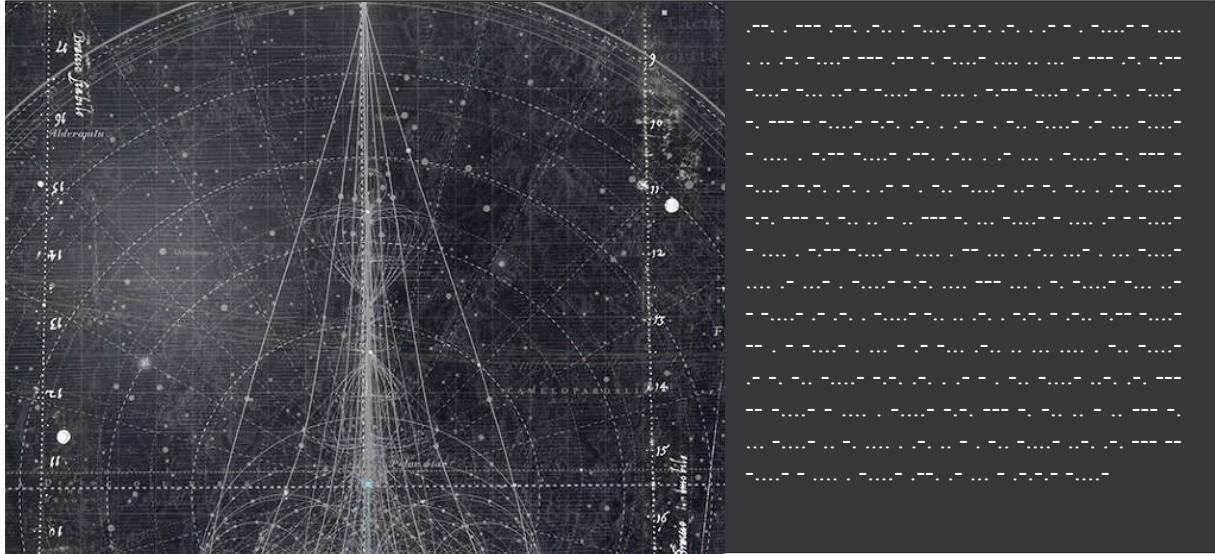
En-Tan-Mo 世界打通链与链之间，区块链和非区块链之间的信息孤岛，应用侧链独立于主链，甚至每个供需关系都成为一条独立链存在于网络当中，这是一个无限延展的平行网络，供需双方立于价值传递的两端。每个人在供需两端随意切换，在不同服务链间自由切换，提供服务和接受服务，高效且没有附加费用的消耗，价值在链与链之间任意流转。



“Hello ! En-Tan-Mo World ! ” 所有加入的矿工会进入到一个资源网格联盟，是一种具有长期最佳收益的算力、存储、带宽承载分布式云；所有的节点根据供需关系，自由平等的选择交易，获得均衡的受益。En-Tan-Mo 本身就是一个能够承载高频次、高流量的大型去中心化数字权证交易所、联盟矿池，混沌排序机制还天然形成一个博弈场。En-Tan-Mo还是一个最好的开发者社区、区块链DAPP应用平台。你好！欢迎来到一个处处体现均衡、平等的全新世界。

## 2.0 En-Tan-Mo 哲学

En-Tan-Mo 是在一种抽象空间中对现实物理世界中的价值生产及交换关系通过拓扑同构映射实现的重建，蕴含着深厚的哲学思想。在其庞大架构之下，渗透的是去中心化之精髓，将 En-Tan-Mo 层层剥离，可抽提出“泛我”的概念。溯源于古希腊时期普罗泰格拉的“人是万物的尺度”，去中心化自此由“梵我”至“同我”至“泛我”之进化。复杂系统与多元结构，共识与价值，动态均衡与分权，自演进与开放性泛化为 En-Tan-Mo 的去中心化特征。



### 2.1 复杂系统与多元结构：“符号价值与象征交换”

多元结构是受符号代码支配的描述，再度被释放于 En-Tan-Mo 复杂系统之中，多元结构将运作于不同领域之间的通路，转化为一张复杂的系统网络。符号逐步脱离所涉对象的过程，以及这种符号对人的控制。多元结构所取用的，En-Tan-Mo 复杂系统会将其还回，但却多了一重差异，将周流的象征解放出来以营造一种差异，遵循 En-Tan-Mo 自身的相互包含律。

En-Tan-Mo 的多元结构，有力地溢出了自身的界定，以潜在的方式居间、聚焦，外在于复杂系统的限制条件，界定抽离于 En-Tan-Mo 的过程之外。除了通过界定而拥有的结构之外，还带有一种意义的过剩，复杂系统与 En-Tan-Mo 的述行力融为一体，从而产生关联的共变。众多韵律，众多主体，共变着的滑移，形成了空间形式化的符号价值与象征交换。

### 2.2 共识与价值：“千座高原”

“千座高原”盘踞于传统思想模式中的种种层、编码、超越性平面、纹理化空间等，一座座流播强度的“高原”，En-Tan-Mo “高原”平等与对等的形态从中抽提。多元性、异质性的连接则成为链节点之间彼此沟通的横贯线，共识在连接中凸显，而价值传递成为了可能。“千

座高原”是影响一个链段走向的元素，它不限于时间上，还意味着重现思想与人生开端的溯源能力。这也就是说，它能让我们重回起头处，体验到最初的、边缘上的取向如何发生，并由此而生出某种边际处的敏感。

节点的平等被分布于一条 En-Tan-Mo 演变曲面之上，被分配于一个轮回语段结构之中。目的就是描绘一种对等事实状态，维持 En-Tan-Mo 主体间关联的平衡，或探索一种已经存在的无意识。链段抽提的平等旨在模仿某种完全完美之均衡，作为既成之物而被给予的事物，而此种对均衡的模仿是基于 En-Tan-Mo 化结构或支撑性的对等轴面。

### 2.3 动态均衡与分权：“波斯人信札”

通过 En-Tan-Mo 世界同时性发展所形成的均衡，这些具有相似的速度，共有阶段的序列。主体不再关涉部分性的客体，而是关涉差异性的速度，En-Tan-Mo 的动态均衡将脱离预先存在或被导向存在的主体。不具有客体，也不具有主体，一种自然实在和一种客体之中，统一性不断遭到阻碍，但在泛主体化的 En-Tan-Mo 之中，新的统一性却获得分权与开放之间的互补，而主体也不再能够形成二元分化。

中心化的权力，自由结构体制的问题，永远纠缠于最有权力的因素。而 En-Tan-Mo 的分权，换取的是去中心化的自治，自治并不等同于非完全的自由，仅是一种较中心化更自由的形态。“人生而自由却无往不在枷锁之中”，这种二律背反已经证明了形而上学的不可能。

## 2.4 自演进与开放性：“作者之死”

在主体的解构和渐进缺席下，结构本身成为了总体，个体在和总体的相互关系中定义自身的意义和存在方式。因此，结构本身作为独立于个体的存在和对现实进行的同构映射将作为历史记录和真实性的依据。显然，一种静态的结构将与历史结构的演进和现实世界结构的复杂性将不断产生矛盾。Levi-Strauss 在其名著“原始社会”的后记中已经提出了结构和演进之间

关系的复杂性问题及其在人类社会政治经济学分析中的重要性。En-Tan-Mo 中解决这一问题的方式是在设计中内嵌入自演进的逻辑，使得这一体系能够在去中心化和结构保持稳定的前提下保障与现实之间的共时性和映射的合理性。

作者之死指作者作为创作的主体对作品不再具有垄断的地位，在现代写作中主体的身份已经被消解。因此，时间，空间和起源的概念都必须重新被理解。En-Tan-Mo 的建设过程本身就是一种写作，这种写作的目的是在一个新的空间维度内实现自由意志和秩序结构的统一。这种创作在制定一种自身体系内的元历史或书写历史的规则，而真实性将通过对历史结构的共识得到定义。对任何一个主体而言，任意地制定规则乃至改变历史将带来一种难以克制的权力诱惑。因此，En-Tan-Mo 不仅意识到创作主体被解构的可能性，而且主动地实现这一解构过程，以创造一个真正去中心化的，公平的体系。

En-Tan-Mo 系统要创造的是一种新的历史结构和在历史结构中精神性的展开过程。这种创造绝非随意的，而是基于严格的数学论证和对现实世界经济结构的研究。En-Tan-Mo 将在以集中的形式和速度对人类社会经济结构的发展史进行重现，正如同单个胚胎的发育能够在某种程度上重演生物的进化阶段。因此 En-Tan-Mo 不仅仅是一种新的交易方式，而是一场宏大的人类学实验，它将重新构建我们对包括财产的本质，所有制的起源和权力的分配方式等基本问题的认识。

“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，从过去继承下来的条件下创造。”

每一个 En-Tan-Mo 的参与者都会是一种新的历史结构的建设者和见证者。

### LA MORT DE L'AUTEUR

l'énonciation même qui le définit, suffit à faire « tenir » le langage, c'est-à-dire à l'épuiser.

L'éloignement de l'Auteur (avec Brecht, on pourrait parler ici d'un véritable « distancement », l'Auteur diminuant comme une figurine tout au bout de la scène littéraire) n'est pas seulement un fait historique ou un acte d'écriture : il transforme de fond en comble le texte moderne (ou — ce qui est la même chose — le texte est désormais fait et lu de telle sorte qu'en lui, à tous ses niveaux, l'auteur s'absente). Le temps, d'abord, n'est plus le même. L'Auteur, lorsqu'on y croit, est toujours conçu comme le passé de son propre livre : le livre et l'auteur se placent d'eux-mêmes sur une même ligne, distribuée comme un *avant* et un *après* : l'Auteur est censé *nourrir* le livre, c'est-à-dire qu'il existe avant lui, pense, souffre, vit pour lui ; il est avec son œuvre dans le même rapport d'antécédence qu'un père entretient avec son enfant. Tout au contraire, le scripteur moderne naît en même temps que son texte ; il n'est d'aucune façon pourvu d'un être qui précéderait ou excéderait son écriture, il n'est en rien le sujet dont son livre serait le prédicat ; il n'y a d'autre temps que celui de l'énonciation, et tout texte est écrit éternellement *ici et maintenant*. C'est que (ou il s'ensuit que) écrire ne peut plus désigner une opération d'enregistrement, de constatation, de représentation, de « peinture » (comme disaient les Classiques), mais bien ce que les linguistes, à la suite de la philosophie oxfordienne, appellent un *performatif*, forme verbale rare (exclusivement donnée à la première personne et au présent), dans laquelle l'énonciation n'a d'autre contenu (d'autre énoncé) que l'acte par lequel elle se profère : quelque chose comme le *Je déclare* des rois ou le *Je chante* des très anciens poètes ; le scripteur moderne, ayant enterré l'Auteur, ne peut donc plus croire, selon la vue pathétique de ses prédécesseurs, que sa main est trop lente pour sa pensée ou sa passion, et qu'en conséquence, faisant une loi de la nécessité, il doit accentuer ce retard et « travailler » indefiniment sa forme ; pour lui, au contraire, sa main, détachée de toute voix, portée par un pur geste d'inscription (et non d'expression), trace un champ sans origine — ou qui, du moins, n'a d'autre origine que le langage lui-même,

### LA MORT DE L'AUTEUR

c'est-à-dire cela même qui sans cesse remet en cause toute origine.

Nous savons maintenant qu'un texte n'est pas fait d'une ligne de mots, dégageant un sens unique, en quelque sorte théologique (qui serait le « message » de l'Auteur-Dieu), mais un espace à dimensions multiples, où se marient et se contestent des écritures variées, dont aucune n'est originelle : le texte est un tissu de citations, issues des mille foyers de la culture. Pareil à Bouvard et Péuchet, ces éternels copistes, à la fois sublimes et comiques, et dont le profond ridicule désigne précisément la vérité de l'écriture, l'écrivain ne peut qu'imiter un geste toujours antérieur ; jamais originel ; son seul pouvoir est de mêler les écritures, de les contrarier les unes par les autres, de façon à ne jamais prendre appui sur l'une d'elles ; voudrait-il s'exprimer, du moins devrait-il savoir que la « chose » intérieure qu'il a à la présenter de « traduire », n'est elle-même qu'un dictionnaire tout composé, dont les mots ne peuvent s'expliquer qu'à travers d'autres mots, et ceci indéfiniment : aventure qui advint exemplairement au jeune Thomas de Quincey, si fort en grec que pour traduire dans cette langue morte des idées et des images absolument modernes, nous dit Baudelaire, « il avait créé pour lui un dictionnaire toujours prêt, bien autrement complexe et étendu que celui qui résulte de la vulgaire patience des thèmes purement littéraires » (*les Paradis artificiels*) ; succédant à l'Auteur, le scripteur n'a plus en lui passions, humeurs, sentiments, impressions, mais cet immense dictionnaire où il puise une écriture qui ne peut connaître aucun arrêt : la vie ne fait jamais qu'imiter le livre, et ce livre lui-même n'est qu'un tissu de signes, imitation perdue, infiniment reculée.

L'Auteur une fois éloigné, la prétention de « déchiffrer » un texte devient tout à fait inutile. Donner un Auteur à un texte, c'est imposer à ce texte un cran d'arrêt, c'est le pourvoir d'un signifié définitif, c'est fermer l'écriture. Cette conception convient très bien à la critique, qui veut alors se donner pour tâche importante de découvrir l'Auteur (ou ses hypothèses : la société, l'histoire, la

# 3.0 En-Tan-Mo 数学

本节将从数学角度研究去中心化的区块链系统，包括我们完成的工作和项目的发展规划和方向，以及通俗地介绍项目开发应用到的数学工具。同时从这一角度给出我们发展En-Tan-Mo项目的理由。

## 3.1 去中心化的安全性问题

2009年，中本聪发表了题为“*A Peer-to-Peer Electronic Cash system*”的论文，给出了比特币区块链思想的核心数学模型和理论证明，利用泊松分布证明该区块链的作弊（我们称之为对系统安全性的攻击）可能性很低，从而解决了分布式记账体系的信任困难问题，即拜占庭将军问题。时至今日，中本聪理论中的一些重要假设发生了变化，导致比特币区块链相关结论不再正确。

中本聪关于在区块链中作弊可能性的概率定量估计的基本思想：

当一个交易完成后，一组可具有合作性的攻击者立即开始上传包含虚假信息的区块并以此为基础建造假链。如果在诚实的矿工已经延伸了 $z$ 个区块的时刻，攻击者所挖的区块数量满足泊松分布。则在此前提下，中本聪利用全概率公式计算出了假链能够在某一时刻取代真链的定量估计，但随着ASIC矿机和矿池的出现，上述前提假设不再成立。依靠算力得到新的区块，本质上是Binomial随机游走问题，其中：

$p$  = probability an honest node finds the next block;  $p$ 表示某一个诚实者找到下一个区块的概率

$q$  == probability the attacker finds the next block;  $q$ 表示作弊者找到下一个区块的概率， $p+q=1$

当交易后诚实矿工已经挖出了 $n$ 个区块时，我们将攻击者所挖的区块数量记为随机变量 $X_n$ 。该问题可以转化为赌博积分问题 (Problem of points)，即把作弊者每次建造一个区块记为成功，概率为 $q$ ；将诚实者建造一个区块记为失败，概率为 $p=1-q$ 。则 $P\{X_n=k\}$ 表示这个随机试验在 $n$ 次失败前恰有 $k$ 次成功的概率，满足负二项分布 (Negative Binomial distribution):

$$P\{X_n=k\} = C_{k+n-1}^k p^n q^k$$

如果满足以下条件：

1. 诚实矿工所挖的区块数量 $n$ 较大；
2. 存在一个有限的常数 $\lambda$ ， $n \frac{q}{p} \rightarrow \lambda$ 。记， $I_n = n \frac{q}{p}$  则根据以下计算

$$P\{X_n=k\} = \frac{n^k}{(n+I_n)^n} \frac{I_n^k}{(n+I_n)^k} \frac{(k+n-1)!}{(n-1)! k!} = \frac{I_n^k}{k!} \frac{1}{(1+\frac{I_n}{n})^n} \frac{n(n+1)...(n+k-1)}{(n+I_n)^k}$$

$$(1 + \frac{I_n}{n})^n \rightarrow e^\lambda$$

可得随机变量 $X_n$ 的分布律趋近于参数为 $\lambda$ 的泊松

分布 (Poisson distribution):

$$P\{X_n=k\} \rightarrow \frac{\lambda^k}{k!} e^{-\lambda}$$

在矿机和矿池存在的条件下，上述假设条件 (2) 难以满足，因此中本聪的定量估计是不正确的，该数学模型已经不能对比特币金融风险进行精确控制。不仅如此，当作弊者具有一定强度的算力资源，并且通过非光滑控制的方法调节自己的算力（例如在作弊开始时突然增大算力），则作弊成功的概率远非如中本聪所估计的那样小。

因此，通过不依赖于算力的权益计算方法，控制 $q$ 的大小，同时加快区块产生的速度，可以更有效地控制作弊者成功的概率，并得到关于这一概率的更准确的定量估计。

当诚实矿工已经挖出 $z$ 个区块时，诚实矿工与攻击矿工所挖的区块数量差距可以用随机变量 $z - X_n$ 来表达。利用赌徒破产问题 (Gambler's Ruin problem) 的方法可以得到，当真链和假链之间的差距为 $z - k$ 个区块时，假链长度最终在某一时刻能超过真链的概率是：

$$\begin{cases} (q/p)^{z-k}, & \text{if } z > k \\ 1, & \text{if } z \leq k \end{cases}$$

此时，作弊者成功的概率估计 $P(z)$ 可用全概率公式计算如下：

$$P(z) = P\{X_z \geq z\} + \sum_{k=0}^{z-1} P\{X_z = k\} \left(\frac{q}{p}\right)^{z-k} = 1 - \sum_{k=0}^{z-1} C_{k+z-1}^k (p^z q^k - q^z p^k)$$

根据C. Grunspan 和 R.-P. Marco的工作，作弊者在掌握远小于51%的算力时，就有很大成功的可能性。这说明单纯的算力证明法 (POW) 的安全性并不如预计的强，我们提出POW加DPOS相结合的对偶共识，用矿工的选举制度来进行监督和制约，可以有效地加强安全性。

## 3.2 Nash 均衡与共识算法

“En-Tan-Mo”在设计共识算法时，利用了Nash均衡的思想，我们先介绍Nash均衡的基本定义，然后简要说明如何利用在我们的共识设计中。

设 $S_1, S_2, \dots, S_N$ 为紧致的距离空间， $J_1, \dots, J_N$ 为定义在 $\prod_{i=1}^N S_i$ 上的连续函数。我们记 $P(S_i)$ 为定义 $S_i$ 的所有Borel概率测度所构成的紧致距离空间

定义：在混合策略博弈中的Nash均衡表示这样的策略组合 $(\pi_1, \dots, \pi_N) \in \prod_{i=1}^N P(S_i)$ ，使得对于任意的 $i=1, 2, \dots, n$ ,

$$J_i(\bar{\pi}_1, \dots, \bar{\pi}_N) \leq J_i((\bar{\pi}_j)_{i \neq j}, \pi_i) \quad \forall \pi_i \in P(S_i)$$

$$\text{其中 } J_i(\pi_1, \dots, \pi_N) = \int_{S_1 \times \dots \times S_N} J_i(s_1, \dots, s_N) d\pi_1(s_1) \dots d\pi_N(s_N) .$$

定理：((J. Nash, 1950), (Glicksberg, 1952)) 在以上假设条件下，对于混合策略存在至少一个不动点。目前已有大量文献讨论例如比特币等区块链系统的博弈

论分析且文献数量在不断增加。Nash 均衡指一种策略状态的集合，任何人不能通过单方面地改变策略来获得更大利益。这对于去中心化系统是至关重要的，因为在这类系统中没有一个中心化的控制者可以通过“惩罚”偏离行为来维持秩序。

问题在于：Nash 均衡的策略并非一定是高效的。在比特币系统中甚至可以说 Nash 均衡对应的策略是非常低效浪费的。这是因为对于比特币而言唯一的安全机制来源是算力证明，矿工可以随意加入或离开系统。这种挖矿一个纯粹非合作游戏，获胜的唯一决定因素是算力。这种算力证明机制在令参与者服从共识方面是非常成功的，例如诚实挖矿和服从“最长链法则”。但同时，每个矿工都有驱动依靠升级挖矿装备来获得更大利润。这种“军备竞赛”导致了巨大的资源浪费和实质性的垄断者出现。这种浪费和损耗现象在经济学中被称为“公地悲剧”，在算法博弈论中则被称为“无秩序的代价”。

这一问题的唯一解决方式是通过机制设计，“经济学的工程层面”。机制设计又被称为经济学中的逆问题：不是在已有机制设计下研究结果，而是寻找能够实现所需要结果的机制。区块链系统是应用机制设计理论的完美领域，因为在这里设计者在制定规则方面有极大的自由。在这里，机制可以被视为将策略和结果相连接的过程。Nash 均衡的重要性在于，如果博弈参与者都是理性的且能很好地预测结果，则他们一定会预测到 Nash 均衡策略。否则，一定会有参与者有驱动采用其他策略。在区块链体系下这一问题更为迫切：因为没有中心化权力的限制，一旦参与者感受到更大利益的驱动就会实施新的策略而不再服从共识。在 ETM 系统中使用了 POW 与 DPOS 双共识机制设计以实现去中心化前提下 Nash 均衡状态的高效性。在未来计划的工作中将在机制设计中引入康托洛维奇价格机制和 Vickery 拍卖模型。

### 3.3 投票制度中的权益调节模型

目前在许多区块链系统中采用了代表权益证明(DPOS)，相对于单纯的算力证明(POW)有节省资源和区块产生速度较快的优势。这一理论的预设是在一个区块链体系中占有较多权益(Token)的人更可以被信赖。“En-Tan-Mo”认为，根据目前区块链及加密货币的发展现状，权益以一种近似 Pareto 分布的方式集中在少数人手里。为了避免选举权力的过度集中，所以我们需要对他们的投票权与权益之间应当是正相关，但并非线性的关系。在这里对我们的方案作出一些简要说明。

设系统中有 N 个节点，某个节点 i 在投票开始时占有的权益占总权益的比例为  $\alpha_i$ ,  $\sum_{i=1}^N \alpha_i = 1$ 。我们定义一个严格上凸函数映射  $f$ ,  $\frac{\partial f(\alpha_i)}{\partial \alpha_i} > 0$ ,  $\frac{\partial^2 f(\alpha_i)}{\partial \alpha_i^2} < 0$ ，我们规定这一节点所拥有的选票数量在总选票中的比例为  $B_i = \frac{f(\alpha_i)}{\sum_{i=1}^N f(\alpha_i)}$ ，显然  $\sum_{i=1}^N B_i = 1$ 。

根据严格上凸函数的简单性质  $f(\sum \alpha_i) < \sum f(\alpha_i)$ ，可得对于两个相对权益分别为  $\alpha_i$ ,  $\alpha_j$  的节点（不失一般性，设  $\alpha_i > \alpha_j$ ）：

$$\frac{B_i}{B_j} = \frac{f(\alpha_i)}{f(\alpha_j)} = \frac{f\left(\frac{\alpha_i}{\alpha_j}\alpha_j\right)}{f(\alpha_j)} < \frac{\frac{\alpha_i}{\alpha_j} f(\alpha_j)}{f(\alpha_j)} = \frac{\alpha_i}{\alpha_j}$$

问题在于，在这一机制下，大股东有可能尝试通过将自己的股权分散到多个不同账户以在投票中获得优势。这一类行为在网络安全中被称为女巫攻击。

从博弈论的角度，我们认为这将不是一种理性策略。论证如下：

大股东在已有的 stake 基础上分散化到多个节点确实可以增加自己的投票权；

参与者行为的最终动机是获得更大的利益，在 En-Tan-Mo 中即是获得更多的 Token 奖励。投票权只是手段而不是目的；

在 ETM 的交易机制中，每次投票是伴随着一段交易发生的。而交易会产生交易费用。这样对于攻击者（女巫攻击）而言，分散化投票是有成本的。因为攻击者必须产生大量的毫无意义的交易以获得更多投票机会，随之带来交易费用的损耗。

En-Tan-Mo 建立在博弈论和 Thomas Sargent 的理性预期 (rational expectation) 经济理论之上。我们的数学理论认为，大股东 stake 分散化的理性预期收益将无法覆盖其所付出的交易费用损耗。因此，这种分散化将不是参与者的合理选择。

### 3.4 混沌排序

En-Tan-Mo 项目的共识设计将安全性作为核心目标之一，并设定了极高的标准。针对 DPOS 体系中可能出现的多位 SCV 矿工协调进行作弊的问题，共识层将采用混沌排序的方式加以解决。

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。在上传区块的过程中，如果某几个矿工希望联合起来作弊，则他们需要连续地确认一个包含虚假信息的区块。为此目的，他们需要尽早地知道不同矿工上传区块的排列次序并有足够的空间加以协调。混沌重排指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  $\Psi$  并进行多次迭代计算出下一名矿工的编号。因此直到矿工只有在最后一刻才知道应该上传区块的矿工身份。

1. 一个类 Hénon 多维映射，其动力学方程如下：

$$x(n+1) = ay(n) + by(n)^2$$

$$y(n+1) = cx(n) + dy(n) + dx(n)z(n)$$

$$z(n+1) = x(n)^2 + ey(n)x(n)$$

2. 令 256bit 的二进制和其对应的十进制数分别为 I 和 D，其映射关系可描述如下：

(1) 利用 Matlab 中均匀分布生成函数 randi 生成一个随机迭代数  $N_1 (3 \leq N_1 \leq 13)$ 。

(2) 利用时刻的系统输出，随机产生初值的选取维度 ( $idxo$ )  $s = x(N_1) + y(N_1) + z(N_1)$

$$idxo = \text{mod}(s, 3) + 1$$

(3) 利用其它 2 个维度的信号产生 2 个随机数

$$(seg1, seg2)$$

例如：

$idxo = 2$ , (即从 x 维选取 i 作为初值), 那么

$$seg1 = \text{mod}(x(N_1), 12)$$

$$seg2 = \text{mod}(z(N_1), 12)$$

(4) 将 I 看作 32 个 8bit 块构成，利用 seg1 和 seg2 将 I 切分为 3 个区块

$$I1 = \text{slit}(I, seg1), I2 = \text{slit}(I, seg2), I3 = \text{slit}(I, seg3)$$

其中  $seg3 = 256 - seg1 - seg2$ , slit 函数所对应的切分规则如下图：



(5) 利用 I1,I2,I3 分别生成“系统参数缩放值” (var-par), “系统迭代次数” (val-N), “系统初值缩放值” (val-init)

(6) 利用 val-par, val-N, val-init 初始化超混沌系统，并进行计算，选取第  $idxo$  维的信号作为输出，并通过换取运算产生 1-101 之间的一个整数，即 D

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。

### 3.5 Kantorovich 对偶，与去中心化

“En-Tan-Mo” 区块链的共识称为康托洛维奇共识，来自于苏联数学家康托洛维奇在最优运输领域的工 作，尤其是其在 1939 年的著作中提出的康托洛维奇对偶定理。这一定理是线性规划和最优运输中早期的开创性结果之一。我们简要介绍这一理论及其在去中心化的区块链系统中应用的可能性。

设  $X, Y$  为两个集合（或对应现实中的区域），我们要将  $X$  处的物质运送到  $Y$  处。设  $c(x, y)$  为将每个对应的点  $X$  到  $Y$  的运输成本（或密度函数）。设  $\gamma$  表示在区域  $X \times Y$  上物质的概率分布， $\mu$  和  $\nu$  分别表示其在  $X$  和  $Y$  上的边缘分布。可用  $\int_{X \times Y} c(x, y) d\gamma(x, y)$

表示从  $X$  到  $Y$  的整体运输成本。康托洛维奇对偶定理指出：

$$\inf_{\gamma \in \Pi(\mu, \nu)} \int_{X \times Y} c(x, y) d\gamma(x, y) = \sup \left\{ \int_Y \psi(y) d\nu(y) - \int_X \varphi(x) d\mu(x) : \psi(y) - \varphi(x) \leq c(x, y) \right\}$$

其中  $\inf$  和  $\sup$  分别表示下确界和上确界。在此略去严格的数学细节，仅给出一个通俗的解释：如果“En-Tan-Mo”有一个去中心化的交易体系， $\psi(y)$  表示在  $y$

处卖出的价格； $\varphi(x)$  表示在  $x$  处买入的价格，那么

$$\int_Y \psi(y) d\nu(y) - \int_X \varphi(x) d\mu(x)$$

表示这个交易体系的最终利润。对偶定理的结果表示，在限制条件  $\psi(y) - \varphi(x) \leq c(x, y)$  下，整体运输成本最小化的策略恰好对应利润最大化的策略。

这一定理指出了建立一个合理价格体系对于优化资源运输和配置的重要性。由于这一理论在经济学层面的可能解释，康托洛维奇的这一理论在苏联学术界曾长期遭到批判，他本人也被逮捕入狱。

在区块链的技术层面，最优运输对应的就是价值传递的最佳策略和组合方式。“En-Tan-Mo”认为合理的方式应当是采用去中心化的体系建立完善的信任机制，让每一个节点根据自身掌握的交易信息作出决策，形成一个透明的、信息公开化的市场，利用市场自身的调节机制形成一个动态均衡的价格体系。这也就是“En-Tan-Mo”希望实现价值传递的方式。

### 3.6 去中心化体系中的动态价格形成

在“En-Tan-Mo”系统中，每一个个体同时是服务的提供者和购买者，即是买家也是卖家。去中心化的市场核心是价格调节机制，而价格将以一种动态均衡的方式自组织地形成。“En-Tan-Mo”使用平均场博弈论的思想研究去中心化交易体系中的价格动态形成问题。这一模型又被称为 Lasry-Lions 价格形成模型。假设价格偏好具有一定的随机性。用密度函数  $f_B$ ,  $f_V$  分别描述买家和卖家的数量。 $t$  表示时间， $x$  表示价格。例如  $f_B(x, t)$  表示时刻  $t$  而价格为  $x$  时的买家数量。用  $p(t)$  表述动态均衡过程所产生的价格。 $a$  表示交易费用。得到如下平均场方程组：

$$\begin{aligned} \frac{\partial f_B}{\partial t} - \frac{\sigma^2}{2} \frac{\partial^2 f_B}{\partial x^2} &= \lambda \delta(x - p(t) + a), & \text{if } x < p(t), t > 0 \\ f_B \geq 0, \quad f_B(x, t) &= 0 \quad \text{if } x \geq p(t), \quad t \geq 0 \\ \frac{\partial f_V}{\partial t} - \frac{\sigma^2}{2} \frac{\partial^2 f_V}{\partial x^2} &= -\lambda \delta(x - p(t) - a), & \text{if } x > p(t), t > 0 \\ f_V \geq 0, \quad f_V(x, t) &= 0 \quad \text{if } x \leq p(t), \quad t \geq 0 \\ \lambda &= -\frac{\sigma^2}{2} \frac{\partial f_B}{\partial x}(p(t), t) = +\frac{\sigma^2}{2} \frac{\partial f_V}{\partial x}(p(t), t) \end{aligned}$$

其中乘子  $\lambda$  用于刻画时刻  $t$  的交易数量。 $\sigma$  用于描述随机性， $\delta$  表示一个 delta 函数。给定初始条件：

$$f_B(x, 0) = f_B^0, \quad f_V(x, 0) = f_V^0$$

这一方程组类似于一维热传导方程，但它的难度在于其中出现的自由边值问题。自由边值问题是现代偏微分方程理论中的核心问题，起源于物理学中的相变问题，在目前在许多领域中有广泛的应用。

在去中心化的区块链体系中，由于采取了分布式记账，每个节点可以通过它所掌握交易信息动态地调节自身的行为，因此这实质上是一种贝叶斯型反馈控制问题，即参与者可以通过后验概率实时地调整策略以尽可能增加自己的收益。“En-Tan-Mo”将在后续工作中引入带贝叶斯控制系统的动态价格方程模型，将区块链技术与人工智能，深度学习技术紧密结合。

# 4.0 En-Tan-Mo 经济学

区块链与其相关技术的变化将会对当代经济状况产生巨大的颠覆作用。工业革命出现在一个商业模式以等级制度和金融资本主义为根据的世界里。区块链革命将会见证一个由人力资本主义和高度自治为主导的经济体制。

这一切最终将如何呈现，目前尚不清晰。企业家和创新者将会一如既往地通过不断试错去解决这个不确定性。毋庸置疑的是，在我们确切知道这种颠覆将如何呈现之前，大量的财富将被创造和毁灭。

而 En-Tan-Mo 的贡献在于，当这场颠覆出现时，En-Tan-Mo 提供一个均衡的价值传递模型，让人们清晰地认识到这场颠覆的含义。

## 4.1 En-Tan-Mo 加密货币经济学

信任关系广泛存在于商业活动尤其是金融系统中，交易中每一组信任关系背后，都代表着相应不确定性的存在，与相应交易费用的节省。En-Tan-Mo 让可绝对信任的交易信息流成为现实，这使许多交易环节中人与人的信任关系能够转为人与技术的信任，将不确定性降至 0，以及整个交易过程中的信任关系重新组织，让交易费用整体下降成为可能。

现有的区块链技术除了整体效率较低，还带来了显著的负面影响。目前区块链的应用在交易速度（比特币 7 笔 / 秒）、隐私性、资产可追回性（Mt.Gox 被黑）等存在一些不够理想的地方。En-Tan-Mo 不仅需要提高整体效率，还将在商业组织中提供一种业务稳定运作，其相关业态将随之配套，利益分配机制也相应确定，En-Tan-Mo 在应用时采用技术保证决策者利益没有明显的负面影响。

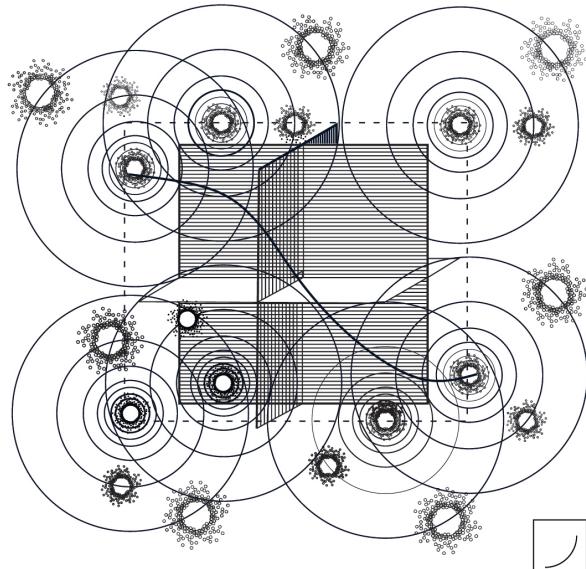
En-Tan-Mo 加密经济学的研究对象是：在密码安全且无需信任的账本中，制度的重要性。古典主义和新古典主义经济学家将稀有资源的生产和分配，以及支撑生产和分配的要素作为研究对象。这是一门把规则作为研究对象的经济学。规则（如法律、语言、产权、规定、社会准则和意识形态）使得分散的和投机的人们之间的活动得以相互协作。规则可以促进交换——不仅是经济交换，还有社会和政治交换。

En-Tan-Mo 加密经济学正是聚焦在支撑区块链及其衍生应用上的经济学原理和理论。它着眼于区块链机制设计中主要使用到的博弈论和激励设计。经济和作为其分支的制度经济学一样，都是一个协调交换的系统。但制度经济学并非着眼于规则，而是聚焦在账本上：由规则构成的数据。

En-Tan-Mo 经济学对如下内容感兴趣：传递价值的治理规则；服务于这些价值的社会、政治和经济机构的发展；以及 En-Tan-Mo 是如何在全世界范围内改变价值传递模式的。

## 4.2 纳什均衡

En-Tan-Mo 系统的一个重要优势是在设计的过



程中积极与深刻地应用博弈论作为机制设计的工具。在已有区块链系统如比特币系统中效率低下的问题可被称为“无秩序的代价”。在 En-Tan-Mo 中，En-Tan-Mo 的数学家通过巧妙的设计双共识机制，让每个参与者都可以以矿工或投票人的身份平等参与区块链的建设并获得均衡的奖励，矿工之间、投票人之间、矿工和投票人之间均通过简洁有效的共识协议进行调节，从而保证理性的参与者策略集合达到一种完美的纳什均衡状态。共识机制及其算法是 En-Tan-Mo 实现去中心化的核心和基础，其本质是要实现“没有统治者的统治”或者说“去中心化的自适应控制”。En-Tan-Mo 共识机制算法的最重要基础是纳什均衡。这一概念由美国数学家，诺贝尔经济学家得主 John F. Nash 提出，其定义是：

在一个多人参加的博弈过程中，所有参与者各自选

择的策略所组成的一个集合，任何人都不能通过单方面改变自己的策略（作弊）获得更大的利益。

En-Tan-Mo 研究中的另一个重要创新是将理性预期理论和博弈论相结合。ETM 项目的资深顾问托马斯·萨金特教授是理性预期理论领域的领军人物。在区块链系统的博弈论分析中需要注意到如下事实：参与者会受到驱动进行预测，而他们对未来的预测将直接影响到他们当下的决定。这对于 ETM 的机制设计是至关重要的。因为设计者本身需要“预测”参与者在不同处境下所可能采取的决定和策略。这一类设计对应于现代控制理论中的预测控制问题。系统的安全性依赖于对纳什均衡的正确预测，而这一预测本身又依赖于机制设计者对于参与者信念和决策的预测。ETM 科学顾问委员会将在这一方向进行更具有数学严格性的研究。

En-Tan-Mo 认为，单纯的 POW 和 DPoS 共识无法保证所有区块链参与者的纳什均衡状态。以比特币为例，矿工在最先算出哈希值之后，如果上传虚假的区块最终不会被系统采用，这样会导致损失算力挖矿所消耗的成本，从而保证所有参与者的均衡收益。具体地说：1. 如果所有区块链参与者都可以参加挖矿，那么计算的难度要足够大才可以使得作弊成功（即包含虚假信息的分叉在某一时刻超过主链长度）的概率足够小；2. 每个矿工付出的成本要足够大才能阻止他冒险采用作弊的策略。随着 ASIC 矿机的出现，普通参与者在比特币区块链中几乎不可能得到任何收益，算力的大幅提升同时会导致挖矿难度的增加，从而增加了作弊者相互协调采取合作策略的可能性，纳什均衡状态被完全打破。以太坊的完全节点也都是经过加强的专用 GPU 矿机，普通大众根本承受不起，几乎所有的轻客户端根本不需要操心挖矿的问题。与 POW 同理，POS 或 DPoS 共识机制，以 Token 拥有数量作为唯一标准，大股东在投票权上是处于垄断地位的，这必然将导致决策是由少数人制定的，没有大众参与，财富迅速向少数人手中集中，均衡同样被打破。

En-Tan-Mo 的纳什均衡是让所有的参与者都能成为 En-Tan-Mo 世界的直接受益者，利益不能被大矿池或大股东垄断，必须在底层共识机制提出基础性变革。En-Tan-Mo 中的博弈参与者即所有用户，参与者在 En-Tan-Mo 中有三种身份状态：SCV 矿工、监察官和 Pareto 矿池，获得的利益指其通过投票选举或上传区块的方式得到 ETM Token 及非 ETM Token 奖励。通过选举制度遴选 SCV 矿工，每个出块周期由若干 SCV 矿工合作有序出块，每个矿工作弊损失的挖矿成本虽然变小了，但是随之增加的是作弊被开除出矿工团队的预期损失；为了提高 En-Tan-Mo 出块效率，监察官有义务选择出最佳 SCV 矿工，并根据选择成功率获得相应 ETM Token 奖励，票数和 Token 数量的关系被上凸函数抑制，保证了全体股东的利益。SCV 矿工和监察官之间独立性和关联性并存，权利和利益分配清晰平衡。Pareto 矿池中的矿机虽然在本周期内不能获得 ETM Token 奖励，但是以联盟的形式参与外部区块

链的生产出块，获得其他区块链的 Token 奖励，从而保证所有矿机的正收益。因此，通过 DPOS 和 POW 统一权益证明共识，En-Tan-Mo 中 SCV 矿工、监察官和 Pareto 矿池三者内部和三者之间达到了纳什均衡。

为了说明共识机制的经济学设计如何影响参与者的决策（策略选择包括两种：诚实挖矿或作弊），我们重复强调如下假设和规则：

假设：至少一半的参与者是诚实的；

规则：1. 只有最长的链会被最终认可；2. 选举制度中，上传包含虚假信息的区块或效率低的参与者将被排除 SCV 矿工。

### 4.3 Kantorovich 共识

采用 POW 算力证明的第一代和第二代区块链被人批评的地方包括：1. 交易处理的速度过慢，如比特币目前的交易速度完全不能与传统的金融体系如银行信用卡相比；2. 区块上传的速度过慢导致拖累交易最终确认的速度；3. 容量问题，目前的效率使得这些区块链难以扩大规模；4. 算力挖矿导致的资源浪费和环境污染。

为此，En-Tan-Mo 提出基于纳什均衡的 Kantorovich 共识机制。监察官作为 En-Tan-Mo 股东，不直接参与 En-Tan-Mo 出块，而是根据拥有 Token 获得投票选举权利从而获取投票 ETM Token 奖励，监察官将矿工算力和过往表现作为投票的主要依据选择出最佳 SCV 矿工，使得 En-Tan-Mo 保持高效率和安全性；SCV 矿工作为 En-Tan-Mo 出块节点，被监察官选出合作竞争的挖矿，从而获得出块的 ETM Token 奖励，SCV 矿工在每个出块周期有序出块，在不降低安全性的前提下减小哈希值的计算难度，从而增加每个区块的产生速度，提高效率；未被选中的矿机进入 Pareto 矿池组成联盟，运用特有的衍生链技术参与外部区块链的生产出块，按照矿机提供算力分配非 ETM Token 奖励，从而保证所有矿机的正收益。所以，Kantorovich 机制可以在保障安全性的同时提高效率，增加系统的可扩展性。

目前中心化的体系在效率方面仍具有较强的优势。但是如果采用更加巧妙的数学结构设计，通过去中心化和适当的合作竞争制（比如 En-Tan-Mo 的 Kantorovich 共识）之间的平衡，完全可以得到安全性、稳定性和效率兼备的区块链系统，这也是我们的主要工作目标。

Kantorovich 共识是一种革命性权益证明算法，它决定了各个矿工节点如何达成网络的一致性，该算法是 En-Tan-Mo 基础架构的重要组成部分，是区块链技术的重大创新。Kantorovich 共识重新设计了需要能量消耗的工作量证明（POW）协议，该问题是区块链

长久以来无法扩大应用的障碍。算法由科学顾问委员会领导的博弈论团队设计而成，并通过同行评审，这是第一个具有科学凭证其安全性的 UPOS 统一权益证明共识。

Kantorovich 共识的思想受到了苏联数学家，1975 年诺贝尔经济学奖得主 Leonid Kantorovich（列昂尼德·康托洛维奇）工作的启发。他在 1930 年代提出严格的最优运输数学模型和 Kantorovich 对偶定理，这一理论证明了可以利用价格非集中化的方法达到资源配置的最优。康托洛维奇由于去中心化经济学观点长期受到苏联主流学术界批评和抨击，庆幸的是，他本人因为参与苏联原子弹计划免于更严厉的迫害。同时，康托洛维奇的经济理论在西方学术界得到了认可并被广泛应用。Kantorovich 最优运输理论是近 20 年数学最重要研究方向之一，菲尔兹奖得主 Cedric Villani 和 Pierre Louis Lions 的工作都建立在这一基础上。因此 En-Tan-Mo 将共识机制命名为 Kantorovich 共识以致敬他的数学成就和特殊时代表现出的超凡勇气。

## 4.4 SCV 矿工和监察官

En-Tan-Mo 中经过矿工团队选举制度被选中并通过基础算力测试的矿工被称为 SCV；Token 的持有者在投票选举 SCV 矿工团队时的身份，被称为“监察官”。监察官将手上的 Token 在 En-Tan-Mo 中通过上凸权益映射转化为可投票数，每投票周期给予相应奖励；候选矿机根据得票高低当选 SCV 矿机和候补矿机，获得上传区块权利，验证区块义务和区块奖励。

假设一个 SCV 矿工作弊，试图上传包含虚假信息的区块，Double Spend 等，面对的结果是：1. 由于大多数 SCV 矿工是诚实的，可以利用概率论方法证明，作弊矿工上传的虚假区块将会最终成为分叉并消失，因此将损失掉算力挖矿过程中所耗费的成本；2. 由于 Kantorovich 共识机制中的轮换选举制度，作弊矿工将确定地在下一次选举中被开除出矿工团队，从此失去挖矿获取 Token 的机会和之前投入的保证金。因此，任何一个 SCV 矿工一旦被投票选入矿工团队中，理性选择必然是高效地完成任务并上传真实的区块信息。

由此可见，虽然整个 En-Tan-Mo 体系中并没有一个中心化的监督者强制规范 SCV 矿工和监察官的行为，但是其中包含的经济学设计将作为“看不见的手”利用 SCV 矿工和监察官对自身最大利益的追求引导所有参与者服从共识，这样就解决了 En-Tan-Mo 参与人相互之间的信任问题和效率问题。

## 4.5 Pareto 矿池

En-Tan-Mo 系统的奖励方式采用经济学理论作为设计基础，其优点体现在三个方面：

1. 公平性：在外部 POW 区块链体系中，个体之

间分配不均，例如比特币和以太币的权益严重向若干中心矿池或矿场集中；在 En-Tan-Mo 体系中，所有个体在共识机制面前是平等的。

2. 去中心化：在外部 DPOS 区块链体系中，实力雄厚的 Token 持有者掌握系统的决定权，重新回到中心化轨道或出现多个寡头垄断；在 En-Tan-Mo 体系中，Token 持有者和区块生产者职、权、利分离，所有个体均享有去中心化带来的资源和优势。

3. 最优性：在外部区块链体系中，个人收益单一，链与链之间像一座座孤岛，未能打通；在 En-Tan-Mo 体系中，Token 持有者获得投票激励，矿机节点在 SCV 矿工和 Pareto 矿池间的切换从而获得最佳收益。

在 Kantorovich 共识机制中，所有矿机节点组成一个合作竞争型的矿池，每个出块周期选择若干 SCV 矿工有序出块，En-Tan-Mo 将该周期中未被选中的所有矿机组建成 Pareto 矿池，运用特有的侧链技术和联盟策略，根据即时收益算法分析，参与外部区块链的生产出块，按照矿机提供算力分配矿池收入，从而保证所有矿机的正收益。

Pareto 矿池的经济学原理核心在于：订立联盟策略；选择合适区块链；建立联盟结构与管理制度；矿机在 SCV 矿工和 Pareto 矿池间的切换。

Pareto 矿池具有如下特点：

1. 组织的去中心化：Pareto 矿池以共同分享市场、合作挖矿为基本目标，矿池间的成员关系由外部区块链收益策略决定，并非一成不变。Pareto 矿池本身是一个动态的、开放的系统。

2. 行为的战略性：Pareto 矿池的方式与结果是对外部区块链竞争环境的长期谋划。联合行为也注重从战略的高度改善矿池联盟共有的经营环境和经营条件，其最大的着眼点是在经营活动中积极地获取外部经济资源。

3. 合作的平等性：Pareto 矿池不同于以往的战术性合作，它是联盟各方在资源共享、优势互补、相互信任、相互独立的基础上，通过事先达成共识结成的一种平等关系，按照算力分配收益，从根本上改变了矿机之间不平等关系的局面。

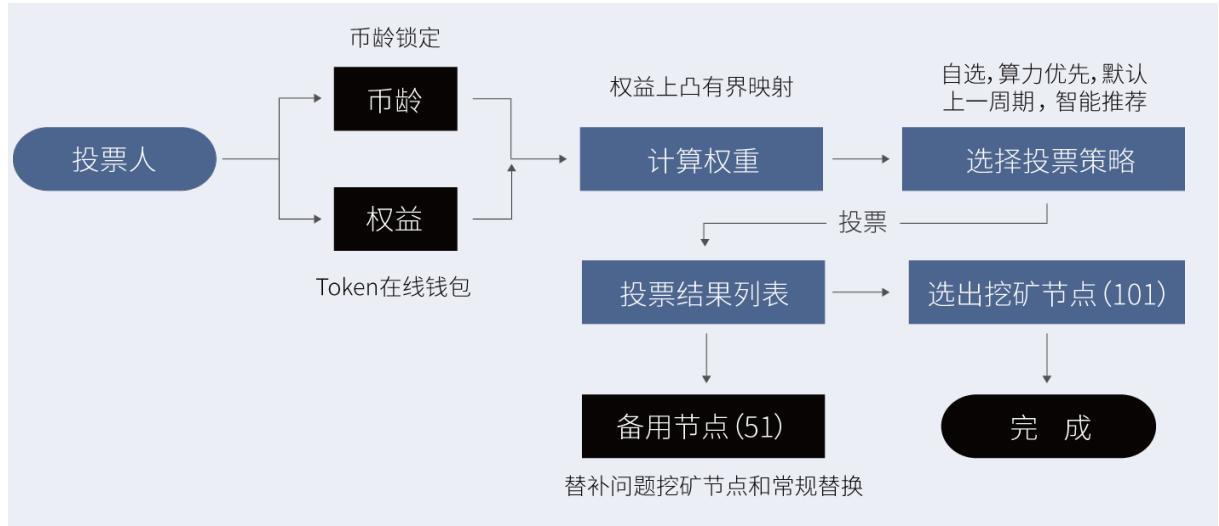
4. 管理的复杂性：在 Kantorovich 共识机制中，第一次出现了真正意义的“双挖”，矿机需要在 SCV 矿工策略和 Pareto 矿池策略间切换，最大的收益建立在严谨的共识机制和巧妙的管理制度上。

帕累托最优（Pareto Optimality），也称为帕累托效率（Pareto efficiency），是指资源分配的一种理想状态，假定固有的一群人和可分配的资源，从一种分配状态到另一种状态的变化中，在没有使任何人境况变坏的前提下，因此，帕累托矿池最优是公平与效率的“理想王国”。

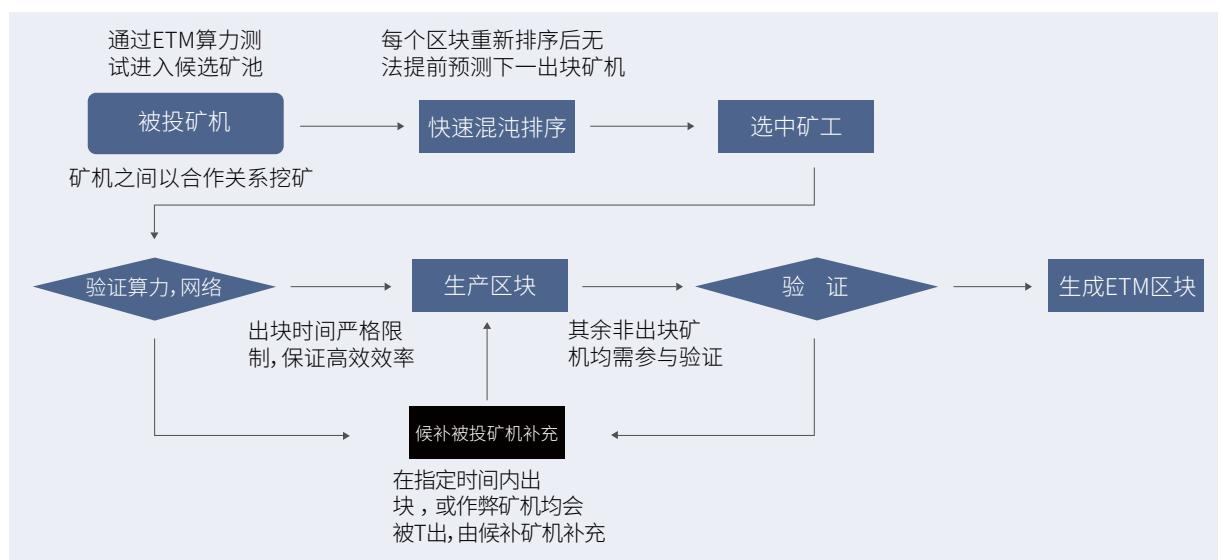
# 5.0 En-Tan-Mo 计算

## 5.1 En-Tan-Mo 算法与流程

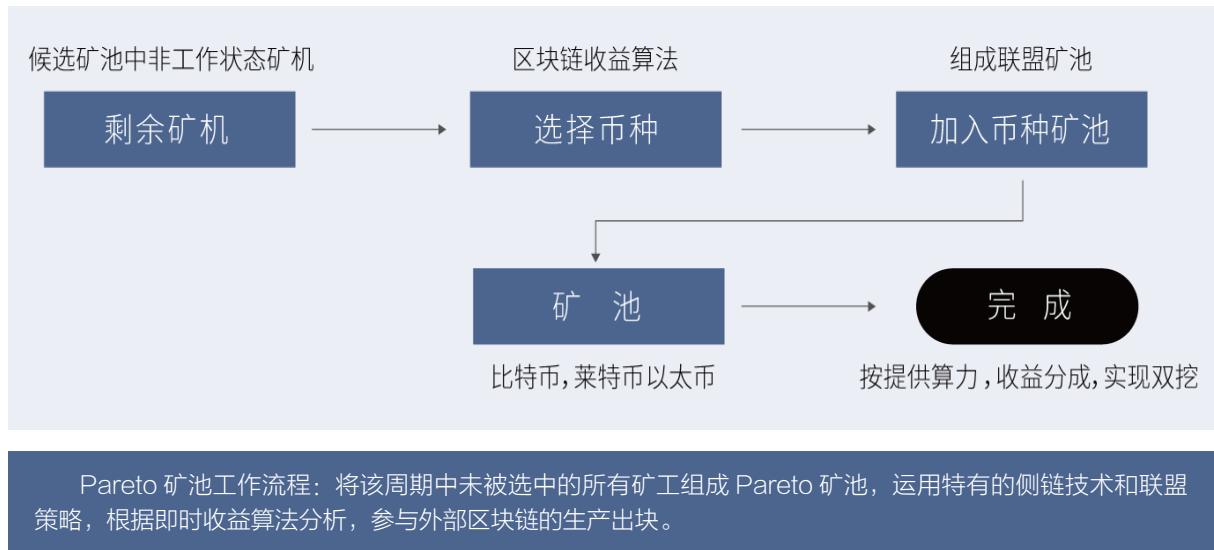
Kantorovich 共识流程图：基于 Nash 均衡思想的 Kantorovich 共识机制采取了矿工团队选举制度，每个出块周期选择若干 SCV 矿工有序出块，在不降低安全性的前提下减小哈希值的计算难度，从而增加每个区块的产生速度，提高效率。



监察官投票流程：监察官将手上的 Token 在 En-Tan-Mo 中通过上凸权益映射转化为可投票数，每投票周期给予相应奖励。



SCV 矿工工作流程：候选矿工根据得票高低当选 SCV 矿工和候补矿工，获得上传区块权利，验证区块义务和区块奖励。



## 核心代码

### 1. 监察官 Token 权益均衡算法

SCV 矿工由监察官通过投票选举产生，获得上传区块的权利。监察官的票数与其拥有的 Token 数量呈上凸函数关系，从而保证了 En-Tan-Mo 生态的均衡性。“权利”是表明 SCV 矿工上传区块的顺利性和合法性。“上凸”表示监察官的 Token 兑换率，为了权益均衡，Token 越多者兑换率越低，反之 Token 越少者兑换率越高。

```

F(balance) = weights
// 阈值映射关系 注：为了权益均衡 Token 越多者兑换率越低，反之 Token 越少者兑换率越高
thresholdMap = Map(range,rate)
// 根据币值区间得到计算率
rate = thresholdMap.get(range)
// 根据兑换率得到委托人 Token 权重
weights = balance * rate

```

### 2. 监察官 投票激励机制

En-Tan-Mo 的 UPOS 机制通过对监察官的 Token 奖励提高其投票的积极性，增强平台参与度，遴选最佳 SCV 矿工，保证 En-Tan-Mo 高效安全运行。En-Tan-Mo 的投票激励机制包含投票奖励和出块奖励两种，监察官可以自由选择百分比获取这两种奖励。投票奖励根据监察官拥有票数固定获得，参与投票即获得奖励，该奖励为恒定值；出块奖励必须当监察官正确选择了 SCV 矿工才可以获得，该奖励为浮动对冲值。

```

F1(tickets) = token
// 投放比例
tickets1 = fixed assignment // 分配给固定 tickets
tickets2 = dynamic assignment // 分配给动态

```

```

tickets // 固定收益 + 动态收益 (根据投票选中节点占总节点数比例)
token = fixed(tickets1) + dynamic(tickets2)

```

### 3. SCV 矿工 出块顺序算法

为了确保 En-Tan-Mo 的安全性，选择 SCV 矿工来生成区块的排序方法必须是确定性系统，同时又具有伪随机。由此，En-Tan-Mo 运用了是绝对安全的、具有混沌性的非线性动力学理论来达成这点。

```

// 锁定委托人投票权益
lock(balance)
// 计算可用投票的权重
tickets = F(balance) * F(time)
// 投票得到受托人列表
delegations = votes(tickets)
// 打乱改变顺序
shuffle(delegations)

```

### 4. SCV 矿工 出块哈希算法

En-Tan-Mo 不仅需要安全性和去中心化，还需要达到高效率，SCV 矿工之间不是竞争关系，而是采用合作竞争的方式出块，通过快速混沌排序为每一个区块指定一个 SCV 矿工，该矿工需要尽快完成 Sha256 计算，上传区块。

```

// 双 hash 计算
blockhash = sha256(sha256(block))
// 检查计算时间，如果没在指定时间内计算出结果表示矿机不达标
checkNodePerformance(useTime)
// 检查计算量是否达到指定要求
checkResult(blockhash,difficulty)
// 如果不符合则改变 nonce
block.nonce = block.nonce + 1

```

## 5.2 En-Tan-Mo 数据

### 块头数据结构

块头包含有关该块的所有信息。由下列字段组成块

- 一个标识块的版本的 32 位整数
- 块创建时的 32 位时间戳
- 前一个块的 64 位 ID
- 与事务数相对应的 32 位整数
- 一个 64 位整数，对应于传送的总量
- 一个 64 位整数，对应与该块关联的总费用
- 与代表的奖励相对应的 64 位整数
- 一个 32 位整数，对应于有效负载的长度
- 有效载荷的 256 位散列
- 生成该块的代理的 256 位公钥

Version	Timestamp
Previous block Id	
Number of transactions	Length of payload
	Amount of ETM transferred
	Amount of fee
	Reward of the delegate
	Payload hash
	Delegate's public key

### 块头数据样例

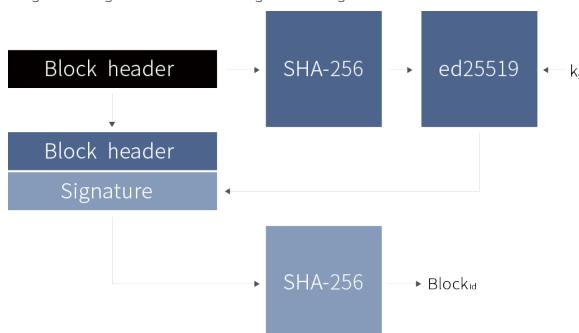
```
"id": "15787022670460703397",
"version": 0,
"timestamp": 23039010,
"height": 1574052,
"previousBlock": "4576781903037947065",
"numberOfTransactions": 0,
"totalAmount": 0,
"totalFee": 0,
"reward": 500000000,
"payloadLength": 0,
"payloadHash": "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
"generatorPublicKey": "c0ab189f5a4746725415b17f8092edd3c266d1e758e840f02a3c99547b3a527f",
"blockSignature": "c6b2bcc960066be078efbffffed625f61553a7bc18ebde3892636c2f36850de234a9c
70ba3e33b606db2eff724398026984e4d391c1fbe70c94dd9d07ff0060b",
"totalForged": "500000000"
}
```

## 区块 ID 生成流程

生成块头的 SHA-256 哈希，并使用委托的密钥进行 (ed25519 算法) 签名。

一旦块头已经被签名，系统就会使用 SHA-256 对完成的块头进行散列生成 Block Id。

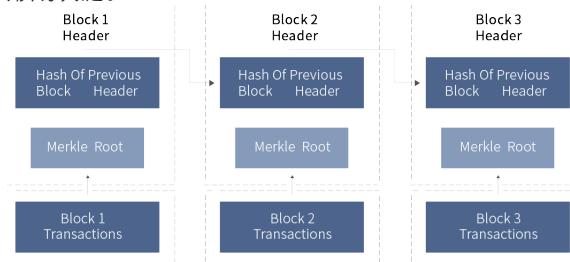
A signed block generates its block using the following flow:



## 区块链结构

可以看出区块主要由区块头和区块体两部分组成。区块头包含版本号、前一区块地址、时间戳、Merkle 树的根植等信息。区块体主要包含交易的计数和交易账单详情。

区块链是由一串使用密码学方法产生的数据块组成的，每一个区块都包含了上一个区块的哈希值( Hash )，从创始区块 ( Genesis Block ) 开始连接到当前区块，形成块链。



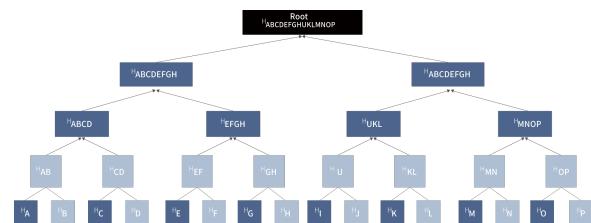
## 数据存储默克尔树结构

Merkle Tree，通常也被称作 Hash Tree 运用树状数据结构存储哈希值。

Merkle 树的叶子是数据块 ( 例如，文件或者数据 )

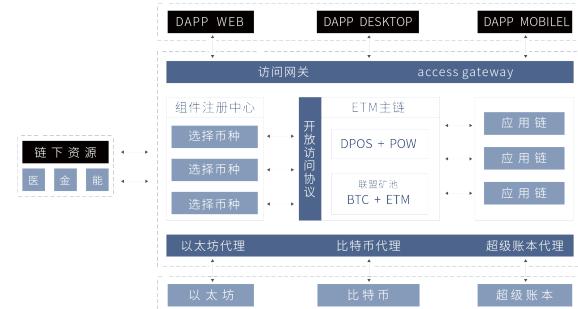
的哈希值。

非叶节点是其对应子节点串联字符串的哈希值。



## 5.3 En-Tan-Mo 接口

En-Tan-Mo 以 BaaS ( Blockchain as a Service, 区块链即服务 ) 为理念，以微服务为基准，以自演进组件库为核心，以开发者社区为生态原动力，为其他区块链提供适配平台完成资产和应用的自由转移，为非区块链的应用和数据提供软通道完成双向调用，为开发者提供共享大厅完成组件上传、评价和奖励的功能，为普通用户提供 BaaS 网关实现无障碍服务调用。从而打通链与链之间，区块链和非区块链之间的信息孤岛，帮助技术开发者和普通用户从互联网转向区块链。系统架构图如下：



系统架构图描述：

- . 应用层 ( Web, 桌面, 移动 ) 通过统一访问网关进行数据访问
- . 通过应用组件与链下资源 ( 现有系统 ) 进行数据交互
- . 应用组件通过开放访问协议进行链上数据交互
- . 应用组件内部对链上链下数据进行整合
- . 主链与应用链通过内部协议数据交互和价值传递
- . 通过代理层与第三方进行跨链交互

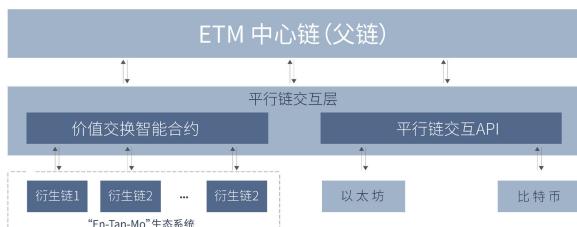
## 参考文献：

- [24] D. Fudenberg, J. Tirole. Game Theory. Boston: MIT Press, 1991.
- [25] N. Nisan, A. Ronen. Algorithmic mechanism design. Proceedings of the 31st ACM Symposium on Theory of Computing (STOC '99), pp. 129–140, 1999.
- [26] C. Papadimitriou. Algorithms, games, and the Internet. Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC '01), 749-753, 2001.
- [27] N. Houy. The Bitcoin mining games. Ledger, vol. 2016.
- [28] A. Kiayias, E. Koutsoupias, M. Kyropoulou, Y. Tselekounis. Blockchain Mining Games. arXiv:1607.02420v1 [cs.GT] 8 Jul 2016.
- [29] A. Sapirshtein, Y. Sompolinsky, A. Zohar. Optimal selfish mining strategies in bitcoin. CoRR, abs/1507.06183, 2015.
- [30] J. P. Aubin, A. Desilles. Traffic Networks as Information Systems: A Viability Approach. Mathematical Engineering 8445, Springer, 2017.
- [31] J. F. Nash. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, 36(1):48-49, 1950.
- [32] I. Bentov, A. Gabizon, A. Mizrahi. Cryptocurrencies without proof of work. In 3rd Workshop on Bitcoin and Blockchain Research - Financial Cryptography, 2016.
- [33] S. Micali. Computationally sound proofs. SIAM J. Comput., 30(4):1253–1298, 2000.
- [34] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld. Proof of activity: Extending bitcoin’s proof of work via proof of stake. SIGMETRICS Performance Evaluation Review, 42(3):34-37, 2014.
- [35] C. Dwork, N. A. Lynch, L. J. Stockmeyer. Consensus in the presence of partial synchrony. J. ACM, 35(2):288-323, 1988.
- [36] S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak. Proofs of space. In CRYPTO 2015.

# 6.0 En-Tan-Mo 生态

## 6.1 中心链和衍生链

在区块链所面临的诸多问题中，区块链之间互通性极大程度地限制了区块链的应用空间。不论对于公有链还是私有链来看，跨链技术就是实现价值传递的关键，将区块链从分散的孤岛中拯救出来，是区块链向外拓展和连接的桥梁。现有的跨链技术主要以侧链为主，但其实际上实现的仅仅只是价值锁定，而不是价值传递。为此，En-Tan-Mo 经过对现有跨链技术的研究，提出了一种平行链交互协议，很好的实现了链与链之间的价值传递，从而构建了一个可以包含千万级应用的区块链生态系统。



为了解决区块链快速膨胀和区块链即服务 (BaaS) 的问题，En-Tan-Mo 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。衍生链是一种特殊的区块链，每一个衍生链对应一个 DApp，是一个独立的、隔离的系统，继承和复用主链强大的区块链技术，每个应用都拥有一套个性化的账本和 Token，其共识机制、区块参数、交易类型都是可以被定制的。各衍生链之间具有平行关系，即衍生链与衍生链之间互为平行链。它们可以通过中心链的“平行链交互层”实现其与中心链、其他衍生链及外部区块链之间的双向资产传递，这使得用户能用已有的资产来使用 En-Tan-Mo 系统。

## 6.2 平行链交互协议

En-Tan-Mo 的平行链交互协议使得支持多种不同的区块链的价值交换成为可能，主要包含链 - 适配模块和价值交换智能合约两部分。设计链适配器主要目的是为价值交换智能合约提供 En-Tan-Mo 与不同链的交互接口，以便验证不同链上的交易。同时，链适配器也可以由社区建设者自己开发和不断改进并获得 Token 奖励，以适用于更多的功能，例如应用可以借助于链适配器在不同协议的底层区块链之间切换。价值交换智能合约是平行交互协议的核心，它可以让用户在 En-Tan-Mo 中心链与衍生链、衍生链与衍生链、



及 En-Tan-Mo 与外部区块链( 包括但不限于比特币、以太坊等 ) 系统等实现资产交换，从而构建成一个链 - 链价值互联网络。

### 链适配器

链适配器就如同计算机的设备驱动程序，它把下层区块链协议转换为 En-Tan-Mo 中心链更容易使用调用的程序，从而运行 En-Tan-Mo 中心链上的价值交换智能合约。其涉及的技术包含但不仅限于 Hash Time Lock Contracts ( HTLC ) 、 SPV 证明、API 开发等。

En-Tan-Mo 首先会提供比特币区块链、以太坊 ( Ethereum ) 等几种最常用的区块链系统的适配器实现，并在运行稳定后进行开源。任何人都可以贡献、改进开放链访问协议，或实现新的适配器。En-Tan-Mo 计划支持更多的区块链协议，并给予相应的 Token 奖励。

### 价值交换智能合约

虽然区块链这一创新技术早已成为全球焦点，但始终存在着一个问题：不同区块链系统之间的价值交易仍然需要像交易所等这样的第三方中间商，而这正是这些去中心化技术所想要取代的东西。En-Tan-Mo 用最小化信任的智能合约与链适配器取代了这种第三方，来承担起不同链之间的桥梁。这种方式加深了区块链领域中最主要的两个元素之间的互连，使 En-Tan-Mo 离统一的全球性价值传递网络更近一步。

价值交换智能合约依赖于 En-Tan-Mo 的图灵完备虚拟机而运行，给用户提供了足够的安全性保障。一个衍生链与中心链的价值交换智能合约就像一个去中心化的交易所一样，它拥有一个 ETM 钱包地址和对应链钱包地址的控制权。当用户在衍生链上发起转账，并且被中心链通过适配器确认后，价值交换智能合约就会自动在中心链上发起对用户的 ETM 钱包地址等额的转账，以此来完成价值的交换。同时，为了防备用户交换价值时面临的风险，En-Tan-Mo 融入了比特币系统的 Hash Time Lock Contracts 技术。

对于具体交换过程，以比特币与 ETM 的互换为例，步骤如下：

比特币区块链用户 A 首先必须在 En-Tan-Mo 注册，以便绑定用户 A 的 ETM 钱包地址与 BTC 钱包地址的映射关系；

用户 A 生成一个随机秘密数 a，求得其哈希值 H(a)。然后，在比特币区块链上向价值交换智能合约的比特币地址发起一笔特殊交易，该交易基于 Hash Time Lock Contracts 技术锁定 12 小时。En-Tan-Mo 价值交换智能合约为了获得该笔 Token 必须出示一个哈希值 H(a) 的原像，否则 12 小时后，该交易的 BTC 自动返回到用户 A 的比特币钱包地址中。

En-Tan-Mo 智能合约通过比特币链适配器监控着比特币区块链中这些特殊交易的确认情况，并对其进行 SPV 验证。一旦 SPV 验证通过，En-Tan-Mo 价值交换智能合约会在中心链中向用户 A 的 ETM 钱包地址发起一笔特殊交易，该交易锁定 6 小时。若用户 A 想要获取该交易中的 ETM Token，必须出示哈希值 H(a) 的原像 a，否则 6 小时后，该笔交易中的 ETM Token 自动退回智能合约的 ETM 钱包地址中。一旦用户 A 出示秘密数 a 领取了该笔交易中的 ETM Token，智能合约就会知晓秘密数 a，因此智能合约就可以通过适配器访问比特币区块链网络，并作为一个用户领取用户 A 在比特币区块链中所发起的那笔交易中的比特币。

至此，交易完成。

需要强调的是，中心链仅仅只是作为一个去中心化的价值交换场所，并不是依靠锁定用户 A 的比特币来实现的价值转移。用户 A 转账给智能合约比特币钱包地址的比特币，智能合约服务于需要将 ETM Token 交换成比特币的用户。同时，用户 A 将比特币交换成 ETM Token 之后，中心链并不限制其仅能转移回比特币区块链，也可以选择通过同样的过程转换成其他外部区块链的 Token。因此，En-Tan-Mo 实现的是价值交换，而不是资产锁定。另外，初始的价值交换智能合约的所有钱包地址 Token 数量都为零，它需要相应区块链用户的投资。作为回报，智能合约将价值交换过程中用户所花费的交易费按投资比例分红给相应的投资者。在投资过程中，用户可以随时向智能合约取回投资款。

总之，基于价值交换智能合约，En-Tan-Mo 所构建的是一个链 - 链价值互联网络。同时，En-Tan-Mo 不凭空创造价值，仅作为价值互联中一个价值传递者。

## 应用生态系统

En-Tan-Mo 是新一代的区块链平台，它把不同应用加到独立运行的不同衍生链上，有效地解决了外部区块链系统的区块快速膨胀，区块体积庞大，同步时间超长等关键问题。En-Tan-Mo 的多衍生链模式为处理高交易量下如何解决网络拥堵的问题提供了一

种理想的解决方法，用户只有用到相关的应用时才需要下载对应的衍生链，大大减小了无效的同步数据，保持了整个 En-Tan-Mo 网络的高效运行。而且，得益于价值交换智能合约实现的链 - 链价值互联网络与网络编码技术、闪电支付网络等技术有效结合，En-Tan-Mo 将可以支持千万级应用和打通整个区块链生态系统。

## 6.3 米尔商城

En-Tan-Mo 系统通过方便而又高效的米尔商城，帮助企业或开发者更快更经济的实现区块链应用，使得用户能够享受到去中心化带来安全和便利。类似于现在中心化的 App 应用，我们将衍生链上去中心化的应用称为 DApp 应用。

米尔商城有如下优势：

(1) 提供容纳千万级应用的区块链生态系统。  
(2) 衍生链上的资产也可以通过 En-Tan-Mo 的平行链交换协议完成和其他币种 (ETM/BTC/ETH 等) 的兑换，使得基于“En-Tan-Mo”开发的应用将具有更大的用户群体。

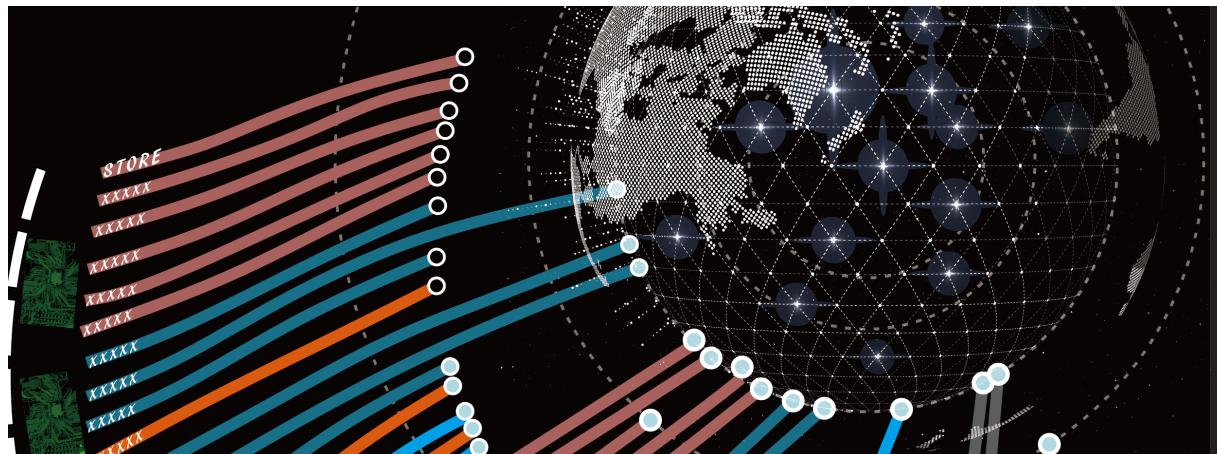
(3) 基于“En-Tan-Mo”的平行链交换协议，DApp 可以访问多个底层区块链的数据，从而使得 DApp 可以基于多个底层区块链而运行。

(4) 利用“En-Tan-Mo”的衍生链技术及其提供的一系列 SDK、API 和模板，开发者只需要关心业务逻辑，就能够很容易的构建、测试和发布自己的个性化 DApp，这将极大的降低了新型应用的落地的研发成本，有助于开发者更好更快的拥有米尔商城的 DApp。并且，这些 DApp 可以被所有 En-Tan-Mo 的节点下载并执行，并对所有的区块链用户提供服务。

(5) 基于“En-Tan-Mo”的衍生链技术，熟练的开发者可以自行定制米尔商城 DApp 个性化的数据库、共识机制、交易类型以及账户体系。

(6) “En-Tan-Mo”将内建一套完善的奖励制度，对于优秀的 DApp，米尔商城将给予 Token 奖励。

西伯利亚东部发现了一处全球最大钻石矿——“钻石之城”米尔矿，这处矿藏的估值过 1000 亿人民币，是目前世界最昂贵的钻石矿。这里用米尔商城表达 En-Tan-Mo 的 DApp Store 资源丰富，潜力巨大。



# 7.0 En-Tan-Mo 组织结构

En-Tan-Mo 社区由 En-Tan-Mo 基金会，ETM FinTech 和 ETM BD 三个组织所构成。En-Tan-Mo 基金会是三个组织的核心，该基金会是在新加坡成立的非营利性机构，保证 En-Tan-Mo 项目的顺利运营，为 En-Tan-Mo 用户社区提供全方位的支持。此外，En-Tan-Mo 还有一家领导区块链技术研究和开发的组织实体 ETM FinTech 技术开发公司、一家协助商业企业投资和应用开发的 ETM BD 商务拓展公司。

## 7.1 En-Tan-Mo 基金会

En-Tan-Mo 基金会是在新加坡成立的非营利性机构，其核心任务是规范，保护和推广自主研发的 En-Tan-Mo 底层架构和区块链协议。同时，还起到研究和提议区块链与加密货币的法规的作用；保护、加强和进化 En-Tan-Mo 生态系统；聚集、教育和培养 En-Tan-Mo 社区。

与此同时，在整个 En-Tan-Mo 社区的有效监督下，以独立的第三方身份，为社区的长期发展提出总体规划。除此之外，En-Tan-Mo 基金会还将作为公益机构，关注世界范围内的公共事业与慈善事业，促进全球公信体系的发展。

En-Tan-Mo 基金理事会，通过民主决策来确定基金会的大政方针，理事会领导下的秘书长负责，执行决策制。监事会，监督理事会的运作，监事会中一般都包括一些知名公众人物和专业的财务人员。

### En-Tan-Mo 基金会理事会

En-Tan-Mo 基金会理事会直接管理慈善项目。基金会分为产品研发、财务管理、市场推广，人力资源、及法务事项等部门，共同维护基金会的日常维护与管理。

### En-Tan-Mo 基金会慈善项目部

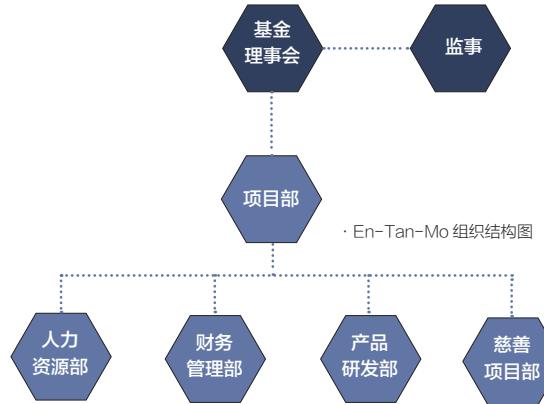
En-Tan-Mo 基金会慈善项目部，是基金会的核心业务部门，负责运作和管理基金会的公益项目，实现基金会的公益目标，用以执行理事会的整体决策。En-Tan-Mo 基金理事会将通过规划和筹资，帮助基金会实现预期目标。在基金会的早期发展过程，负责起草 En-Tan-Mo 基金会章程，由理事会通过作为理事会的运营规则。

En-Tan-Mo 基金会项目部，还负责紧急事件的应急机制，需要由 En-Tan-Mo 理事会商讨公关处理，共同讨论并一致决策后，方可对外披露。基金发展的整体方向，由理事会将对新增推广渠道进行调研，包括渠道的方向、可延伸性和推广力度。

### En-Tan-Mo 财务管理部

En-Tan-Mo 拥有一套独立、公开、透明的财务管理机制。

En-Tan-Mo



· En-Tan-Mo 组织结构图

(a) En-Tan-Mo 基金会所有的交易将为专业财务人员核准，并记录在区块链的区块中，实现公开、透明、不可回溯的财务监管。此外，基金会的所有支出，亦会通过专业财务人员审核，并在区块中进行财务的相关登记。

(b) En-Tan-Mo 基金会通过财务报告制度对资金进行对帐，财务报告将由基金委派的专家财务人员，和 En-Tan-Mo 社区人事管理委员授权人员进行审核。

(c) En-Tan-Mo 基金会的资金募集，重大事项，发展情况，都定期会向社区汇报。重大事项与职能变更，都将提前以公告的形式向社区汇报。

### En-Tan-Mo 人力资源部

En-Tan-Mo 拥有向全社区公开的人力资源体系，有别于传统的公司结构，En-Tan-Mo 的人事从招聘到录用，都是公平公正公开，并全程区块链记录的。

(a) 对于任何新增人员的招聘，都由专业的人员对其进行两轮以上面试，形成独立评价报告并写入招聘记录。所有的记录将具有不可篡改，永久回溯的特性。

(b) 对于满足招聘要求的人员，需要最终向相关委员会进行审批。核心开发人员，以及核心管理人员需要经过尽职调查流程。最终由 En-Tan-Mo 的基金会核心团队审核。

(c) 对于可能外包的业务，将拟定外包协议，确定工资薪酬，并签订相关的外包协议，对全社区进行公开，外包的合同将写入智能合约中。

### En-Tan-Mo 基金监事会

En-Tan-Mo 基金会监事会将对所有 En-Tan-Mo 参与者负责。对基金会理事、项目人员履行职责的合法性进行监督，维护公司及股东的合法权益。监事需要对基金会的财务状况和经营管理情况进行有效的监督、检查和评价。基金理事会应当根据监事会的要求，向监事会报告基金项目的签订、执行情况、资金运用情况和盈亏情况。

## 7.2 ETM FinTech 技术开发公司

ETM FinTech 技术开发公司的角色主要是开发，维护这一全新生态系统，En-Tan-Mo 的开发主要分为四个阶段：

“彼特拉克”：实现完全由网络基础协议和严格的加密技术保护和支持的、全新的、均衡的、高效的、去中心化的 En-Tan-Mo 区块链，形成了一套全新的 Token 规则和体系，同时开放技术社区和开发者大厅，培育和形成 En-Tan-Mo 的文化。

“马萨乔”：开发零知识证明技术以更好的保护用户隐私，结合闪电网络及网络编码技术以提升交易速度、降低区块链的负担，提高可扩展性。通过智能合约、平行链交互协议和链配适器形成 En-Tan-Mo 的生态系统，各类资产在中心链和衍生链上进行数字登记，得到资产安全和数据完整性保证。

“达·芬奇”：共识机制完全实现动态纳什均衡：算力单元会进入到一个混币计算联盟，是一种具有长期最佳收益的算力承载组件；所有的节点根据供需关系，自由平等的选择交易，获得均衡的受益。En-Tan-Mo 成为一个能够承载高频次、高流量的大型数字权证交易所、联盟矿池、DApp 应用平台，混沌排序机制还天然形成一个博弈场。En-Tan-Mo 还是一个最好的开发者社区、区块链应用组件承载平台。

“乔尔乔内”：在这一时期中，En-Tan-Mo 将进一步超越经济领域，迎来区块链 3.0 时代的辉煌和盛况。En-Tan-Mo 可用于实现全球范围内日趋自动化的物理资源和人力资产的分配，促进科学、健康、教育等领域的大规模协作，主要在自动化采购，智能化物联网应用，供应链自动化管理，虚拟资产兑换、转移，产权登记等场景中都将得以实现。

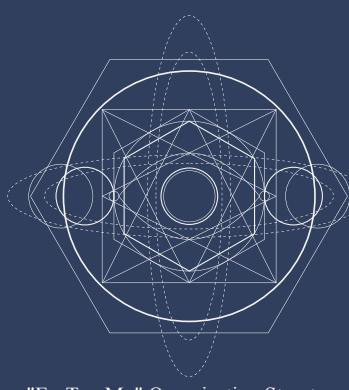
系统一旦发布，ETM FinTech 将不再掌控系统的走向，只有系统的权益人、Token 的拥有者和有兴趣的研究人员一起决定系统将来的发展。

## 7.3 ETM BD 商业拓展公司

ETM BD 商业拓展公司的角色是开发、支援和孕育商业企业，并且协助将这些业务整合至 En-Tan-Mo 的衍生链生态系统中。En-Tan-Mo 通过提供自由衍生链、智能合约、应用托管等一体化的行业解决方案，致力于打造一个易于使用、功能完备、即插即用的系统。利用 En-Tan-Mo 生态系统，开发者可以快速迭代他们的 En-Tan-Mo 应用，并发布到系统内置的去中心化应用商店中，这些应用可以被平台中的分布式节点下载并执行，并服务于普通用户，整个过程都由诚实安全的 En-Tan-Mo 衍生链网络提供安全保证。

任何对 En-Tan-Mo 区块链技术感兴趣，希望通过该技术改革产业的个人或企业，ETM BD 都将通过直接投资、协助开发、提供解决方案等多种灵活的方法，帮助他们实现 En-Tan-Mo 的链上应用。

The role of ETM BD is to develop, support, and nurture business enterprises, and to help integrate these businesses into the En-Tan-Mo's derivative chain ecosystem. En-Tan-Mo is committed to creating an easy-to-use, full-featured, plug-and-play system by providing integrated industry solutions such as free derivative chaining, smart contracts, and application hosting. With the En-Tan-Mo ecosystem, developers can quickly iterate their En-Tan-Mo applications and publish them into the system's built-in decentralized application store. These applications can be downloaded and executed by distributed nodes in the platform. And serve ordinary users, the entire process is provided by the honest and secure En-Tan-Mo derived chain network security.



"En-Tan-Mo" Organization Structure

## 后注：

### 1、政策性风险

目前各国家对于区块链项目以及互换方式融资的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性；市场风险中，若数字资产市场整体价值被高估，那么投资风险将加大，参与者可能会期望互换项目的增长过高，但这些高期望可能无法实现。

### 2、监管风险

包括 En-Tan-Mo 在内的数字资产交易具有极高不确定性，由于数字资产交易领域目前尚缺乏强有力的监管，故而电子 Token 存在暴涨暴跌、受到庄家操控等情况的风险，个人参与者入市后若缺乏经验，可能难以抵御市场不稳定所带来的资产冲击与心理压力。虽然学界专家、官方媒体等均给出谨慎参与的建议，但尚无成文的监管方法与条文出台，故而目前此种风险难以有效规避。

不可否认，可预见的未来，会有监管条例出台以约束规范区块链与电子 Token 领域。如果监管主体对该领域进行规范管理，互换时期所购买的 Token 可能会受到影响，包括但不限于价格与易售性方面的波动或受限。

### 3、团队风险

当前区块链技术领域团队、项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。En-Tan-Mo 项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等方面挂钩，也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。En-Tan-Mo 基于创始人多年行业积累的人脉，汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链领域的资深从业者、具有丰富经验的技术开发人员等。团队内部的稳定性、凝聚力对于 En-Tan-Mo 的整体发展至关重要。在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致 En-Tan-Mo 整体受到负面影响的可能性。

## 免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在 En-Tan-Mo 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

本文档内容不得被解释为强迫参与互换。任何与本文档相关的行为均不得视为参与互换，包括要求获取本文档的副本或向他人分享本文档。参与互换则代表参与者已达到年龄标准，具备完整的民事行为能力，与 En-Tan-Mo 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对 En-Tan-Mo 进行了清晰必要的了解。

En-Tan-Mo 团队将不断进行合理尝试，确保本文档中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、Token 及其机制、Token 分配情况。文档的部分内容可能随着项目的进展在新版中进行相应调整，团队将通过在网站上发布公告或新版文档等方式，将更新内容公布于众。请参与者务必及时获取最新版文档，并根据更新内容及时调整自己的决策。

En-Tan-Mo 明确表示，概不承担参与者因：依赖本文档内容本文信息不准确之处，以及本文导致的任何行为而造成的损失。团队将不遗余力实现文档中所提及的目标，然而基于不可抗力的存在，团队不能完全做出完成承诺。

En-Tan-Mo 是平台发生效能的重要工具，并不是一种投资品。拥有 En-Tan-Mo 不代表授予其拥有者对 En-Tan-Mo 平台的所有权、控制权、决策权。En-Tan-Mo 作为一种数字加密货币不属于以下类别：

- (a) 任何种类的货币；
- (b) 证券；
- (c) 法律实体的股权；
- (d) 股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

En-Tan-Mo 的增值与否取决于市场规律以及应用落地后的需求数，其可能不具备任何价值，团队不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。在适用法律允许的最大范围内，对因参与互换所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，本团队不承担责任。

En-Tan-Mo 平台遵守任何有利于互换行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。

En-Tan-Mo 平台明确向参与者传达了可能的风险，参与者一旦参与互换，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。

### **备注：**

本文档是对英文版技术白皮书的中文翻译，尽管我们尽量保证精确性但仍可能与英文版本存在微小偏差，如果本文内容和解释出现和英文版的区别则以英文版本为基准。