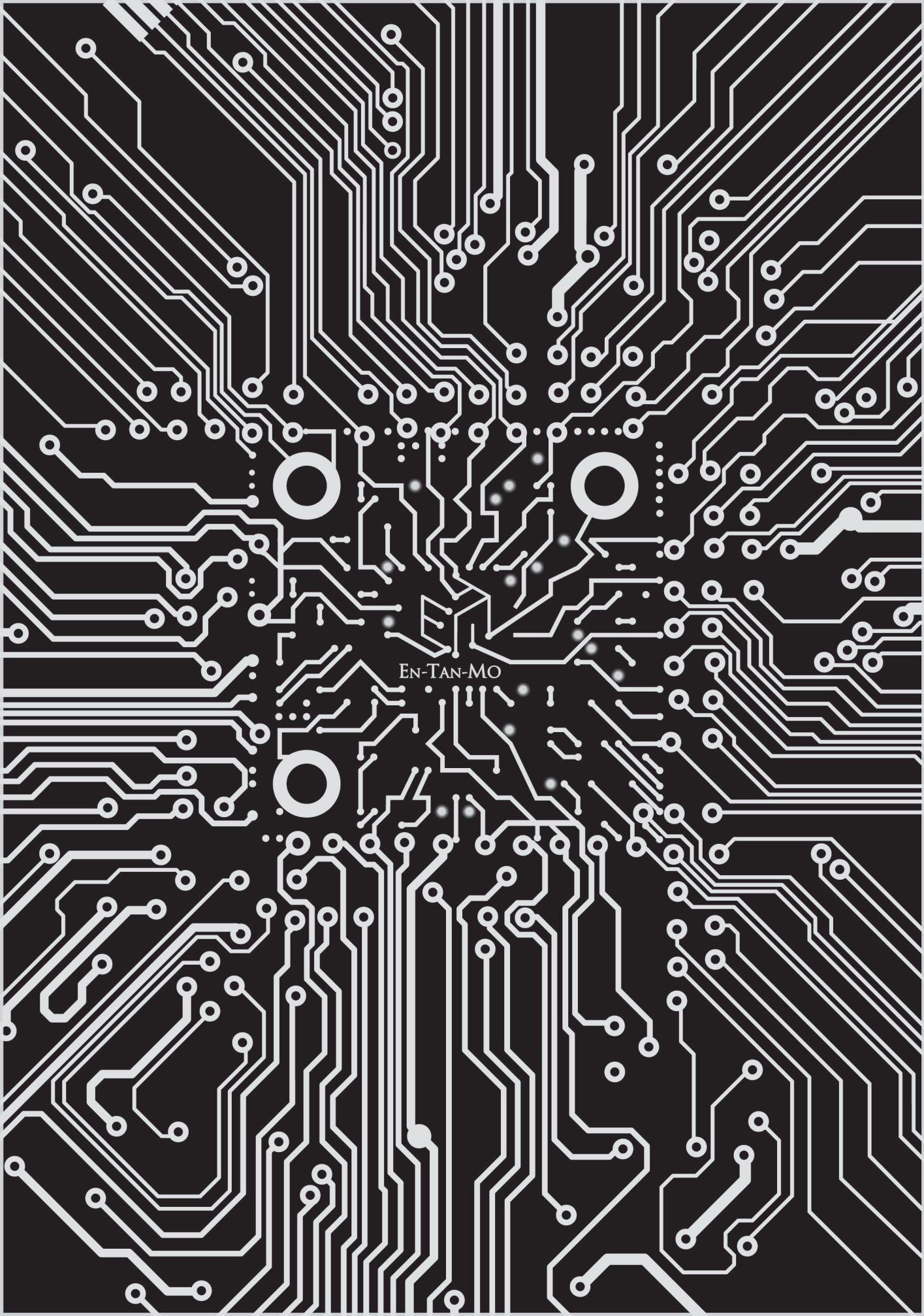
# EN-TAN-MO SCIENCE

EN-TAN-MO

AGREED VALUE SHARED BENEFIT


En-Tan-Mo

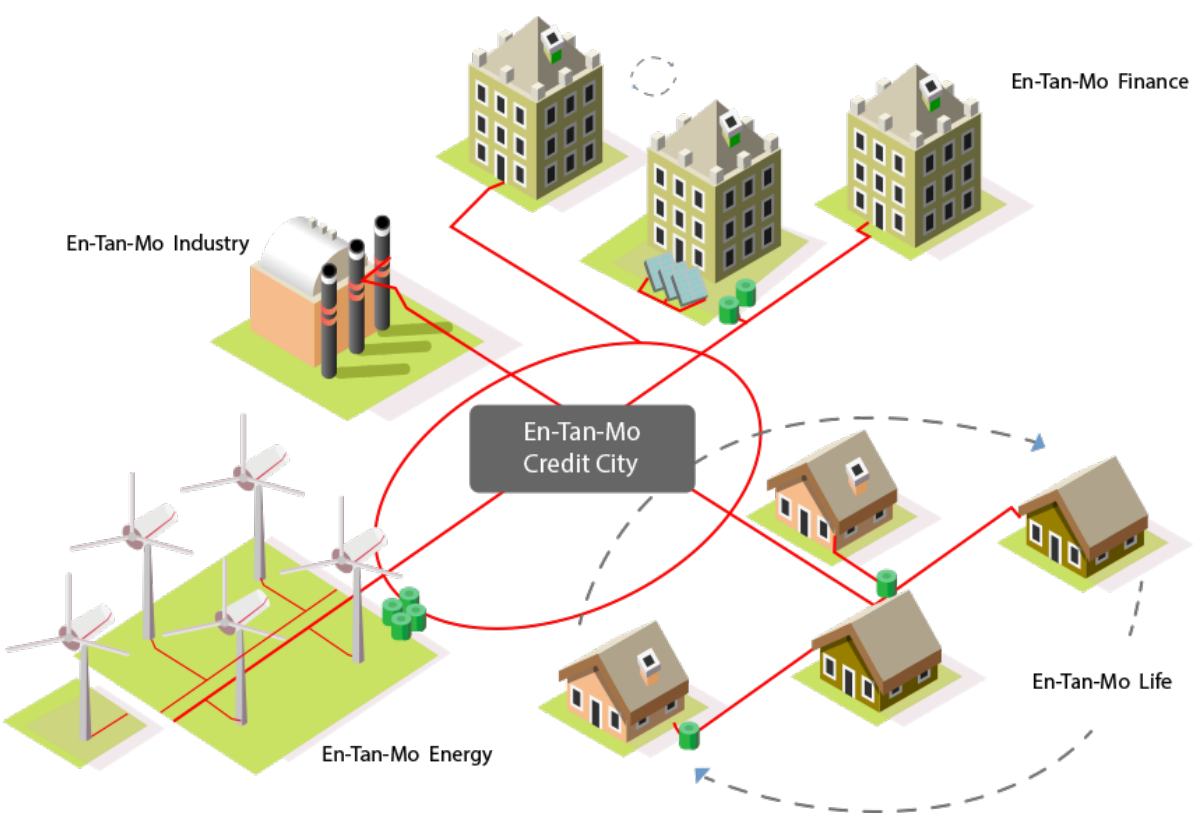
# PROJECT DESCRIPTION

ETM

# Introduction

En-Tan-Mo is a new generation blockchain project based on game theory and the idea of value transfer. En-Tan-Mo is constructed using advanced methods from game theory and has achieved SHD completeness. The members include: 2011 winner of the Nobel Prize for economics, Thomas Sargent; researchers from California Institute of Technology, the University of Maryland and the institut Henri Poincare. It is designed in such a way that all participants are entitled to their fair share of stakes in the wave of decentralization brought by blockchain technology. In the world of En-Tan-Mo, SCV miners and the Pareto mining pools are supporting and motivating each other, so autonomous communities will emerge with equality and fairness being essential principles. En-Tan-Mo is also an open and inclusive system in the way that it incorporates the applications and communities of various other blockchain and non-blockchain systems. En-Tan-Mo is not only of cutting-edge design with respect to its mathematical construction, but also contains the largest number of applications and the widest community of users of any blockchain system. En-Tan-Mo has also initiated serious studies of its implications in terms of philosophical systems and economic theory. Hence the simple form of "technical white book" is not sufficient to account for the significance and complexity of En-Tan-Mo. The development team will explain its application and potential in the language of philosophy, mathematics and economics, and in relation to ecosystems token systems and others. The target audience is everyone who cares about En-Tan-Mo. Contact details in the form of the UNI-ID and electronic wallet of all responsible personnel will also be published.

---



# 0.0 What is En-Tan-Mo

## Blockchain Review

The revolutionary nature of En-Tan-Mo can be glimpsed from the history of blockchain development.

In 2008, Satoshi Nakamoto published "Bitcoin: a peer to peer electronic cash system". In January 2009, the genesis block was created and the age of Bitcoin began. In 2013, a new version of Bitcoin was published, which is the most important to date. This version improved the inner management and network optimization system. From then on Bitcoin began to have global influence. Bitcoin has been very successful as the first cryptocurrency but its development has been seriously hindered by its poor performance in terms of scalability. We call this the age of Bitcoin blockchain 1.0.

Vitalik Buterin created Ethereum to solve the scalability problem. Ethereum is very clear in terms of design and structure. This development consists of important transformations: from EVM paper to ICO; from different versions of POC to Frontier in 2015; from POW Metropolis to POS serenity. The hallmarks of blockchain 2.0 are Turing completeness, smart contract, ASIC resisting algorithms and blockchain Apps. Ethereum provided platform nodes and programming languages such that developers could build and publish their next generation distributed type Apps.

In February 2018 Bitcoin computing POWer reached 20EH/s. More than 90,000 open sourced projects appeared on Github. Blockchain developers come from more than 90 countries including China, the USA, the UK, Singapore, Russia, Japan and South Korea. From 2008 to 2018, it took only 10 years for the idea of blockchains to be explored and popularized. The success of blockchain can be seen clearly by comparing it with the development of the Internet. 1974 marks the genesis of the Internet when Defense Advanced Research Projects Agency (ARPA) published TCP/IP; it was not until 1994 that China was officially part of the World Wide Web system.

---

## 0.1 Why En-Tan-Mo

En-Tan-Mo aims to create an organized, balanced and efficient world that transmits value. Thus, from its inception En-Tan-Mo has been clear about its two main embedding problems.

### SHD completeness

In distributed systems, the CAP theorem states that there exists incompatibility between Consistency, Availability and Partition tolerance. Satoshi Nakamoto proPOSed that a type of uniform consensus can be reached in blockchains via strong probabilistic consistency. This is called Nakamoto consensus.

In blockchain systems, the SHD problem is that, just as in the CAP theorem, there is no compatibility between security, high-performance and decentralization.

On the hypothesis of low-efficient CPU, Satoshi Nakamoto's theory ensured the coexistence of safety and decentralization but at the price of totally sacrificing high-performance. Due to the consensus algorithm and scalability design of Bitcoin, one block is produced every 10 minutes and only 7 transactions can be processed every second. Moreover, with the emergence of ASIC mining systems, the probability of mining a block using only ordinary CPUs falls to almost 0. The ad hoc mining systems easily obtained a super-linear rewards ratio. However, the emergence of mining pools completely destroyed the promises of decentralization. Because of this, Bitcoin obviously ceased to be a community of equal participants. What was worse, there was the danger that the monopoly of over 51% of computing POWer in the hands of mining pools would lead to the concentration of POWer and thus undermine the security of the whole system. We concluded that the Bitcoin system was no longer SHD balanced.

To counter the destructive influence of ASIC systems, Ethereum adopted the ASIC resisting algorithm which for a while ensured security and decentralization. However, the first mass application of smart contract-Cryotokitties, which etheruem was especially proud of, brought down the system completely and highlighted its lack of high performance. The blockchain systems which turned away from POW consensus and adopted POS or DPOS, even though they significantly upgraded system performance, were not essentially different from the established centralized systems in other categories.

By using duality type Kantorovich consensus, En-Tan-Mo will make a fair selection from the community of miners, guarantee the separation of stake-holders and miners and their respective interests, and hence improve efficiency without centralization or loss of security. Thus SHD completeness will be attained in the En-Tan-Mo system.

### Balanced transmission of value

The age of the Internet has changed the ways we transmit information. People transmit information via the Internet at higher speed and lower cost, enabling them to improve their efficiency exponentially and to control cost. They can also obtain completely new products or services. However, the concept of information transmission is different from that of value transmission. Value transmission via the Internet is not point-to-point, but rather depends on central organizations doing the ledgering. The reason for this is that value transmission needs to ensure uniqueness of ownership ("jus in re propria"), and is different from the

reproductive nature of information transmission.

By using distributed ledgering technology, Bitcoin has established a decentralized trust system which no longer depends on centralized agencies such that value transmission can be completely peer to peer. This has changed the rules of value transmission and pricing. With the emergence of mining pools, the value transmission system of Bitcoin has been compromised with the result that value has become concentrated in mining pools. Owners of mining machines and ordinary participants no longer exercise equal rights in the pursuit of value.

Ethereum uses the ASIC resisting algorithm and introduces "Gas" to limit resources on blockchains. This has to a certain extent slowed down the value accumulation process in the hands of mining pools. We consider these measures unconstructive and myopic as they will have negative effects in the long term. The systems that use DPOS consensus have tried to break the POW monopoly of computing POWers to maintain balance. But large stake holders still control the flow of value distribution and this has made them even more centralized.

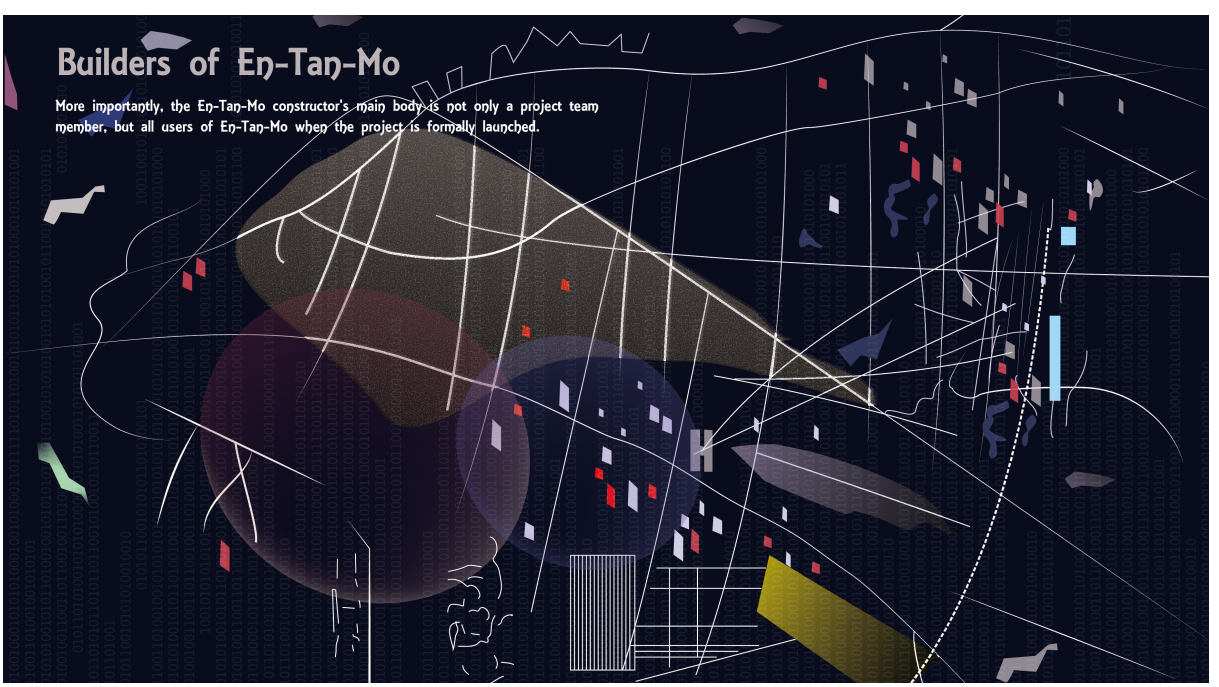
Judging from the current status of blockchains and crypotocurrencies, value is distributed close to Pareto distribution with high concentration. En-Tan-Mo hopes to further develop information transmission via the Internet, change the way value is transmitted towards open circulation, and provide a balanced value transmission system for users. En-Tan-Mo considers each entity as both a buyer and provider (seller) of services. The core of a decentralized market is price formation, and price will emerge through dynamic equilibrium in a self-organized way. En-Tan-Mo uses mean field game theory to study price formation. In terms of election, voting rights should correlate POSitively with stakes or mining capacity but dependence should be nonlinear. This will prevent high concentration of POWer and create a new type of Internet of value, and reform business modes and socio-economic relations.

## 0.2 En-Tan-Mo builders

En-Tan-Mo's designers and builders come from the world's top universities and research institutes. Originally the team was comPOSed of mathematicians who applied game theory in the development of blockchain systems. Experts in the fields of telecommunication, computer science and economics have joined the En-Tan-Mo team. Since then, all the theoretical designs of En-Tan-Mo have adopted a double process. Firstly, the mathematicians complete the consensus design. Secondly, researchers in computer science or telecommunications rigorously verify the theoretical results by numerical simulation and hardware experiments.

The results of the En-Tan-Mo project are due to close cooperation between interdisciplinary teams. The Kantorovich consensus mechanism has been designed by experts in the fields of mathematics, telecommunications and computer science. Also former software engineers from Google, Thunder, Baidu and other top Internet companies with rich experience are contributing to the original code development of the project.

More importantly, once the project is released online, the En-Tan-Mo builders will no longer be confined to members of the development team but include every user of En-Tan-Mo. As a self-evolutionary and participative system, En-Tan-Mo welcomes all users to actively upload compartments and develop derivative chains according to their needs. The En-Tan-Mo development team considers itself the initiator and infrastructure builder of this project. The team will do everything within its POWer to provide secure, stable and efficient technical service for future development. Moreover, it looks forward to collaborations with scientists, engineers and everyone who identifies with the ideas of En-Tan-Mo.



## 0.3 En-Tan-Mo science

En-Tan-Mo is not only a blockchain project. It is a research project with investigations in philosophy, mathematics and economics. The development team provides information in the form of collections of essays which are available to all who are interested in En-Tan-Mo.

---

Chapter 1 The En-Tan-Mo world. En-Tan-Mo builds a world of blockchain 3.0 with improved services and an innovative value system. The world of En-Tan-Mo will focus on the improvement, restructuring and creation of markets. It will bring regeneration and transformation of the concept of equilibrium as essential business value.

Chapter 2 En-Tan-Mo philosophy. En-Tan-Mo is a completely new value transmission system that connects everything with value via blockchains. Thus, the decentralized nature of En-Tan-Mo epitomizes its essential principles: polycentric POWer; openness; equality; participation; interaction and evolution.

Chapter 3 En-Tan-Mo mathematics. The En-Tan-Mo system will be investigated from a mathematical point of view. This chapter will provide up to date conclusions, future research plans and an introduction to the mathematical tools that can be used.

Chapter 4 En-Tan-Mo economics. In the framework of the Kantorovich consensus, SCV miner and Pareto mining pools will be provided with mutual supports and incentives. En-Tan-Mo brings not only technological innovation but also the reformation of business logic.

Chapter 5. En-Tan-Mo computation. En-Tan-Mo data structure, API node and codes written by software engineers will be demonstrated to illustrate the advantages of the Kantorovich consensus system.

Chapter 6. En-Tan-Mo ecology. With its multi-chain technology, En-Tan-Mo includes two different categories of chains: central chains and derived chains. This structure will enable blockchains to break out of isolation, to be connected with the outside system and be capable of further expansion. In this way, a blockchain system can be built that incorporates Apps with over 10 Mirion users.

Chapter 7. En-Tan-Mo organizations. En-Tan-Mo community consists of En-Tan-Mo Foundation, ETM Fintech, and ETM BD. En-Tan-Mo Foundation provides all-round support to user community and ensures the smooth operation of ETM project. ETM Fintech is an entity on privacy security and system development. ETM BD serves as an organization that promotes business development.

---

**References:**


【01】S. Nakamoto. A Peer-to-Peer Electronic Cash System. 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-Stake FAQ, 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. Labaratoire 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.

# 1.0 The En-Tan-Mo World

## 1.1 The Blueprint of the En-Tan-Mo World

"En-Tan-Mo", the interpretation of a subversive new world, is an interdisciplinary scientific project covering areas including philosophy, mathematics, economics and computer science.

In the En-Tan-Mo world, supply and demand as well as participating individuals are seen as latitude and longitude lines respectively. The former intersects and add to the latter as it sees fit. Together they weave a web that is in constant self-learning and self-improvement through the chaotic shuffling mechanism. Each player has the POWer to reshape the world of "En-Tan-Mo" with individual action and the freedom to choose profession makes people more rational, active, autonomous and far-sighted.

The collapse of pyramid:the real decentralization entails the absence of dictatorship and monopoly. "En-Tan-Mo" will go further down the path towards equality and freedom by creating a world that is full of uncertainty, highly innovative and in general equilibrium. Each individual only follows the dynamics of free market and responds rationally to incentives. In the world of En-Tan-Mo, people receive and distribute utilities through active participation in different projects or the creation of new projects rather than wait passively for their monthly salaries. Each individual is both the creator and recipient of the value transferred and transaction fee will be determined by the process of dynamic equilibrium to ensure fairness.

It should also be noted that in the En-Tan-Mo world, the elimination of professional boundaries enables mankind to become a new itinerary nomadic tribe.

## 1.2 The History of Digital Currencies:

Ever since its birth, block chain has been standing out as an emerging technology in the history of the internet, making all centralized applications obsolete. "Token" is to block chain what currency is to business. It has greatly improved the speed and scalability of internet transactions. Consequently, the internet now serves not only as the channel for information sharing but also as the bridge for value transfer. In 2009, the creation of Bitcoin ushered in a new era of "electronic gold'. Since then, waves of gold rush has been sweeping the internet with ever-increasing intensity. It is estimated that, up to the early 2018, only 6 blocks (with 75 bitcoins as rewards) are mined every hour with the hashing rate of approximately 30000PH/s. Bitcoin Energy Consumption Index, issued by Digiconomist, shows that the electricity consumed by bitcoin mining amounts to 39.45TWh per year, an equivalent to 2 billion USD. With massive amount of computational resources pouring into the mining of digital gold, the Bitcoin world in 2017 has a lot in common with the United States during the 1848-1851 Gold Rush. Back then, America suffered from an acute shortage of food and clothing as a result of population explosion. The growth of service sector failed to keep pace with the surge in social demand with U.S. wholesale commodity price index soaring from 847 to 1025. What amazes us, however, is that it only took the Bitcoin world 9 years to establish its own "Gold Standard Monetary System", an endeavor that took the real world hundreds of years to accomplish.

In 2013, Vitalki Buterin first came up with the idea of Ethereum meaning "the next generation of cryptocurrency and decentralized application platforms". This revolutionary innovation gave birth to the smart contract system with Turing completeness, pushing ETH to the height of "digital gasoline". Ethereum allows users to build applications at low cost and great speed on a variety of modules. To be more specific, it uses the Ethereum Virtual Machine Code (EVM language) to establish a kind of application called smart contract which is the core of the whole system. These contracts can be seen as the automatic agent in the Ethereum system. After being activated upon receipt of a transaction sent to the contract address by the user, they run their own code according to the additional information embedded in the transaction and send back the result which could be another transaction from the address of the contract. It should be pointed out that an Ethereum trade can be either a transaction or a segment of instructions and this very feature allows Ether to be used in large quantities. However, it strains resources so that Ethereum is likely to be weighed down with contracts at any time. If we compare Ethereum to a nonscalable highway, then applications are automobiles fueled by ETH gasoline. Currently, there are over 900,000 contracts in Etheruem, most of which are homogeneous token applications, like huge cars cramming a narrow, congested and over-charging highway.

In short, Bitcoin represents the gold standard economy and Ethereum the energy economy. In these two economic ecosystems, rational predictions can be made on the trend of future development.

In the pyramid world, scarcity makes gold and oil the cornerstones of the world economy. The non-renewable feature and pivotal use-value of energy are the very reason why it has replaced gold as the core products driving the world economy. Unfortunately, its resource-driven nature turns the world into a pyramid with few countries at the top and many countries, those belongs to the third world in particular, at the bottom as providers of cheap labor. Within countries, societies are moulded by another pyramid. POWerful enterprises standing at the top enjoy cheap services offered by numerous small and micro companies and organizations who are pyramids themselves. Most of the ordinary workers sweat and toil in those places in exchange for pitiful salaries. The pyramid also exists between different enterprises and organizations. Those at the top are able to acquire resources at diminishing cost while those at the bottom are left to bear the pressure. Eventually, the outbreak of economic crisis will bring about the collapse of pyramids. However, a new pyramid will be erected on the ruins and

the same process will go over and over again.

## 1.3 En-Tan-Mo Mass Emigration

1) POW and DPOS Dual Structure: Breaking Monopoly and Centralization

POW genesis: the most widely accepted consensus in the real world is "labor". Commodity that embodies equal amount of labor is called universal equivalent which usually takes the form of currency. However, things are different in the world of block chain. As consensus has been reached on "computation cost", digital tokens invested with equal and fair computation POWer evolve into the universal equivalent in the block chain system. Therefore, it is imperative to introduce equal and fair computational POWer to achieve initial equilibrium for it helps to ensure future stability in token value. Both Bitcoin and Ethereum have based their mechanisms on fair and equal computational POWer ever since their inception.

POW and DPOS dual structure: the invention of mining machines derailed the level playing field created by the POW systems, just as reinforced productivity generated by every technical revolution broke the old state of fairness. Pyramids are built and demolished repeatedly in different fields, be it agriculture, industry, the internet and block chain. DPOS expedites the process with its high efficiency. Without fairness in computing resources, pyramid would come into existence at accelerating rate. The same is true of tokens in real world. The dual structure of POW and DPOS, by exercising maximum constraints over centralization of pure POW or DPOS mechanism, ensures both efficiency and security as stake holders and miners are allowed to jointly make decisions on issues concerning the community as well as future updates and development. This is, to our view, the major achievement of En-Tan-Mo.

2) Cooperation among Competing Miners: Fair Coalition Rules

POW system requires competing miners to do a large quantity of hashing computation, leading to low utility and waste of energy. To solve this problem, miners seek to form coalitions such as mining pools, only to exacerbate centralization. According to the Cooperation-Competition Theory, mining, as a unique form of game, is a win-win situation instead of a zero-sum game. By using the game theory in the analysis of interaction among miners, En-Tan-Mo encourages players to forge fair and equitable cooperation.

En-Tan-Mo puts forward the new idea that only with cooperation can the value chain for all competing players be created. Such a value chain is used to describe the cooperation-competition relationship among different miners. It emphasizes the co-existence of competition and cooperation in the En-Tan-Mo world. Acting together, the two form a dynamic relationship with richer implications than any of them alone. This brand new relationship among miners is defined by three words: Impact, Intimacy, and Vision. They refer to the concrete and effective outcome generated by such a relationship, i.e. the increase in productivity and value, which manifests itself in the following three aspects: First, the reduction in duplication and waste and better conservation of computation resources and electricity; second, accelerated formation of new blocks as miners draw upon each other's competitive edge; third, the creation of new opportunities that allow players to participate in the construction of external block chains.

3) Dynamic supply-demand, Rational Choice and Nash equilibrium

Joining En-Tan-Mo is to side with the best coalition in the digitalized world. Previous mining pools often follow the rules of the optimal control theory. Consequently, the tenser competitions get, the smaller utility dwindles. Led by Professor Thomas Sargent, scientists of the En-Tan-Mo project employ the rational prediction theory to put in place the dynamic supply-demand mechanism that leads to a real time formation of Nash equilibrium based on participants' rational choice strategies. Selective cooperation is the manifestation of supply and demand. Value is the organic combination of cost and demand. In En-Tan-Mo, the cost factor of POW entwines with DPOS supply-demand relationship, jointly formulating coalition rules that create maximum value and reduce volatility.

4) Concave Function Mechanism and Equilibrium Stakes

Traditionally, coalitions tend to favor the most POWerful collaborators. The stronger the collaborators, the greater proportion of income they receive. This super-linear income model will eventually hurt relatively weak collaborators, and it is this process that has led to the formation and collapse of the pyramid. In the end, even a strong collaborator will suffer from the fall of the pyramid. En-Tan-Mo, by paying attention to the long-tail effect, enables relatively all partners to obtain relatively considerable benefits. This will make the coalition structure more sustainable. POWerful collaborators who have given-up some benefits at the initial stage will also gain greater profits on the long run.

The foundation of the En-Tan-Mo world is exactly the contribution algorithm that eliminates the "unicorn pool". It even turns this "completely equal" (linearized arithmetic function) into concave functions, which allows fair scales to be slightly tilted towards the wider range of players. Through rational expectation mechanism, it would contribute to more extensive consensus, making En-Tan-Mo the fairest blockchain network.

5) Chaotic Shuffling, Resistance to Sybil Attack and Coalition attack

In SHD theory, the inevitable problem between decentralization and security is Sybil attack. The Sybil attack, in computer security, is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. The attacker subverts the blockchain system (which is considered a peer-to-peer network system) by creating a number of pseudonymous identities, using them to gain a disproportionately large influence. The

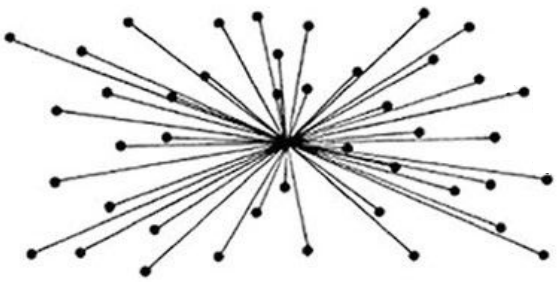
same issue will arise with regard to coalition attacks.

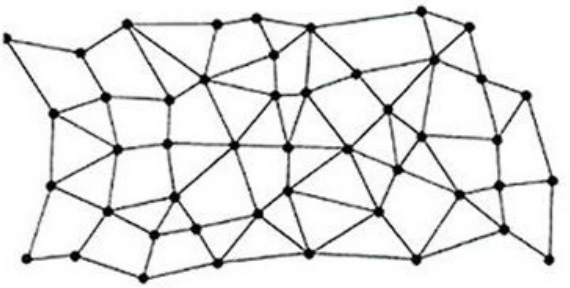
Mathematicians of the En-Tan-Mo project used modern theory of dynamical systems, topology as well as structural and bifurcation theory of complex invariant sets to study systems stability and control methods. They proPOSed a POWerful method of chaotic shuffling based on ergodic theory and sensitive dependence on initial conditions. In such a way, an efficient pseudo-random mechanism with the highest resistance to quantum attack is devised for shuffling mining sequences.

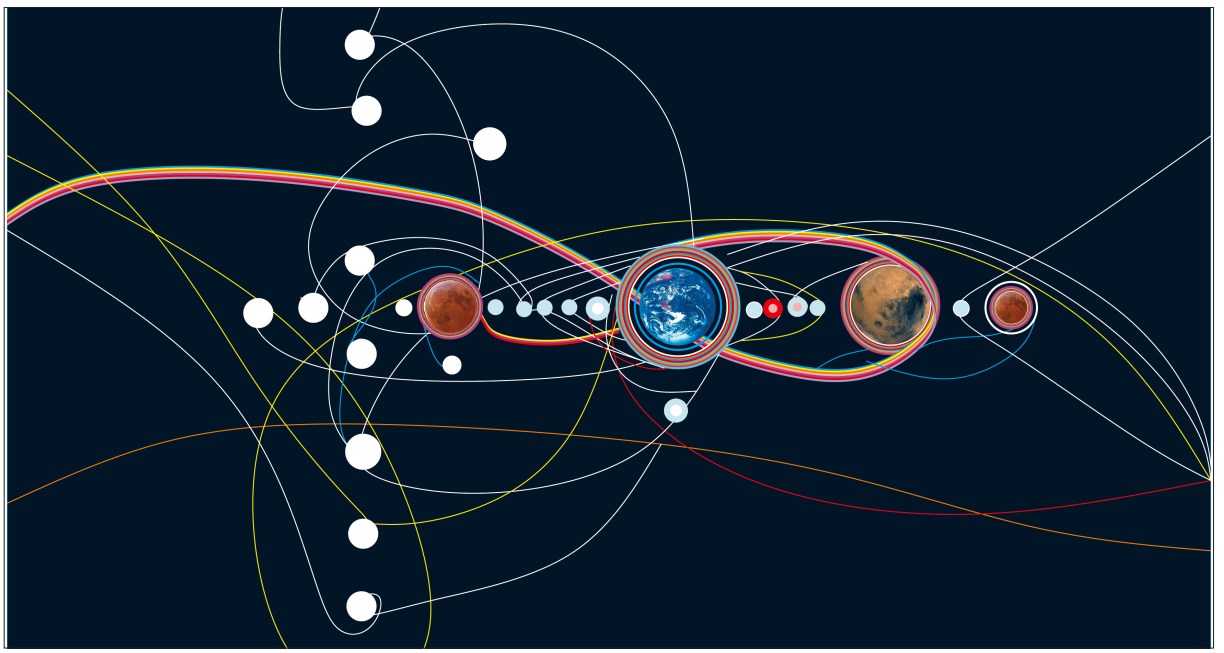
6) Open Component Library and Friendly Developer Lobby Point the Way for Self-Evolution and Common Participation

En-Tan-Mo is based on the idea of BaaS (Blockchain as Service) and the standard of micro-service. Taking the self-evolving component library as its core and the developer community as its driving force, it provides an adaptation platform for other blockchains to complete the free transfer of assets and applications. En-Tan-Mo provides two-way soft channels for non-blockchain applications and data. It also provides developers with the ability to complete component uploads, reviews, and rewards in the shared lobby. For ordinary users, En-Tan-Mo provides BaaS gateways with access to barrier-free service. As a platform advocating self-evolution and common participation, En-Tan-Mo welcomes users to actively upload components and develop derived chains.

In the En-Tan-Mo world, interconnection is built among different chains and between block chains and non-block chains. Side chains are independent of the main chain. Even each relationship between supply and demand constitutes an independent chain in the parallel network that extends infinitely. Individuals are be both sellers and buyers in an efficient system without additional cost. Value flows freely between different block chains.



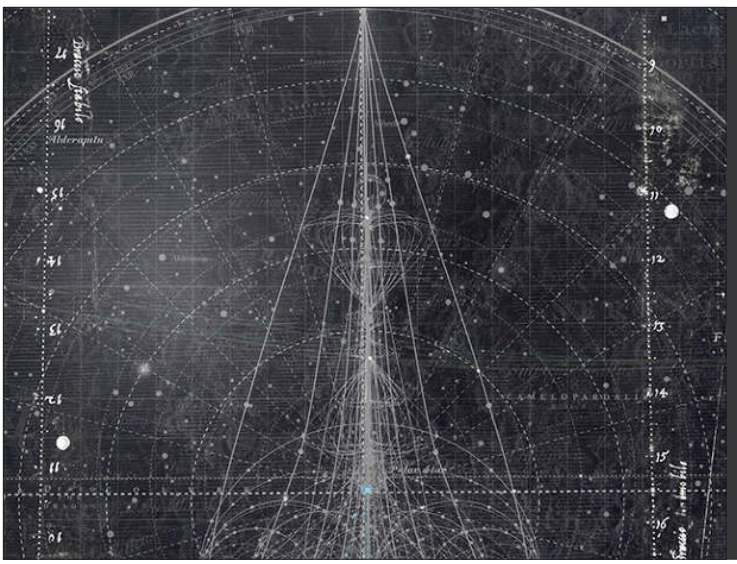


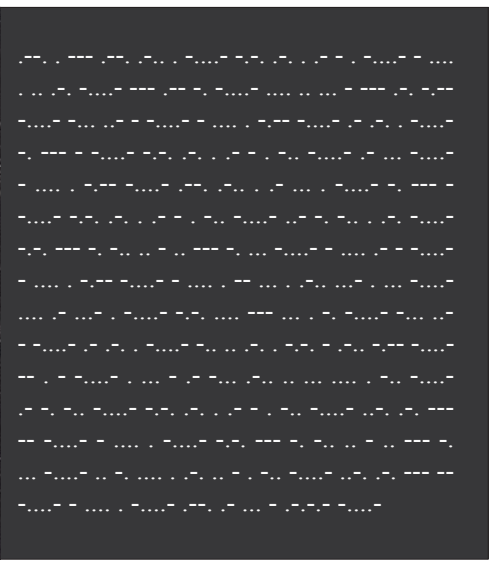


The "Hello! En-Tan-Mo World!" computing node will join a hybrid computation coalition. This is a computation carrier component with the best POSsible long-time utility. Each node chooses transactions according to supply and demand and gets a fair share of utility in return. En-Tan-Mo itself is a large-scale high-frequency exchange for digital tokens, a coalition mining pool, and a DAPP application platform with a natural gaming field formed by chaotic shuffling. It is also the best developers' community and the carrier for block chain application components. Hello! Welcome to a whole new world of equilibrium and equality!

# 2.0 En-Tan-Mo philosophy

En-Tan-Mo is the reconstruction of production and exchange relations in the real world through topological isomorphism mapping in an abstract space, and contains profound philosophical thoughts. Within its huge structure, the essence of decentralization is to infiltrate En-Tan-Mo layers, and the concept of "ubiquitous self" can be extracted. En-Tan-Mo's philosophy can be traced back to ancient Greece and to Protagoras's famous observation that "Man is the measure of all things". Decentralization has evolved from a world in which Man worships a God or gods, to one in which he worships himself, to one in which nobody worships anybody and everybody is equal. . Complex systems and multivariate structures, consensus and value, dynamic equilibrium and devolution, self-evolution and openness are the decentralized features of En-Tan-Mo.





## 2.1 Complex Systems and Multivariate Structure: "Signal value and symbol exchange"

Multivariate structure is described by a symbolic code and is repeatedly released in the En-Tan-Mo complex system. The multivariate structure transforms the pathways operating in different domains into a complex network system. The symbolic code gradually signs off from the object in question, and from its control over people. The En-Tan-Mo complex system takes the symbolic code and returns it to the multivariate structure but it creates a lot of differences. Liberating the symbol of the current flow to create a difference, the symbolic code follows the law of mutualinclusion. The multi-structure of En-Tan-Mo effectively overflows, intervenes in the complex system which can no longer constrain it and defines the process outside of En-Tan-Mo. In addition to the structures owned by the definition, there is also a surplus of meaning. The complex system is integrated with the performance of En-Tan-Mo, which leads to the co-variation of the association. Numerous rhythms, numerous subjects, and co-moving slips form a formal symbolic value and symbolic exchange of space.

## 2.2 Consensus and Value: "A Thousand Plateaus"

"A Thousand Plateaus" is entangled in various layers, codes, transcendental planes, textured spaces, etc. in the traditional ideological model, all streaming intensity, equal and reciprocal with the "plateau" of En-Tan-Mo. The connection of diversity and heterogeneity becomes the cross-over of communication between chain nodes. The consensus is highlighted in the connection, and value transmission becomes POSsible. The "A Thousand Plateaus" is an element that influences the direction of a segment. It is not only limited to time, but also means the ability to trace the origin of ideas and life. This means that it allows us to return to the very beginning and experience how the initial, marginal orientation took place, which in turn leads to some kind of marginal sensitivity. The equality of nodes is distributed over the evolving surface of En-Tan-Mo and is distributed in a structure of recurrent passages. The purPOSe is to depict a state of reciprocal facts, maintain the balance between En-Tan-Mo subjects, or explore an existing unconscious. The equality of segment extraction is designed to imitate aabsolutely perfect equilibrium and is given as a fait accompli, and this equilibrium imitation is based on the En-Tan-Mo structure or the supporting equiaxial surface.

## 2.3 Dynamic Equilibrium and Decentralization: "Persian Letters"

The equilibrium formed by the simultaneous development of the En-Tan-Mo world, has a similar speed to that world and proceeds by similar stages. The host is no longer concerned with the guest, but with the

difference of speed. En-Tan-Mo's dynamic equilibrium will be separated from the pre-existing guest. There is no host and no guest, just a natural reality and an object, and the unity of host and guest is constantly hampered. However, in the generalized En-Tan-Mo, the new unity develops complementarity, and the subject can no longer form a dualistic differentiation.

Centralized POWer, which is the problem of free structural systems, is always entangled in the most POWerful elements. The decentralization of En-Tan-Mo is autonomous decentralization. Autonomy is not the same as incomplete freedom. It is only a more centralized form. "Man is born free but is everywhere in chains" This contradiction has proved a metaphysical imPOSsibility.

## 2.4 Internal evolution and Open: "Death of the Author".

In the deconstruction and gradual absence of the subject, the structure itself becomes the whole, and the individual defines its own meaning and existence in its mutual relationship with the whole. Therefore, the structure itself has existence as an independent entity and an isomorphic mapping to reality will serve as a basis for historical records and authenticity. Obviously, a static structure will continue to conflict with the evolution of historical structures and the complexity of the structure of the real world structure. In the POStscript of his famous book The Primitive Society, Levi-Strauss has drawn attention to the complexity of the relationship between structure and evolution and its importance in the socio-political analysis of human society. The way to solve this problem in En-Tan-Mo is to embed self-evolving logic in the design, so that this system can guarantee the synchronism between reality and decentralization and the structure remains stable.

The author's death refers to the author's role as the subject of creation. He no longer has a monopoly of work. The author's identity has been destroyed in modern writing. Therefore, the concepts of time, space and origin must all be addressed again. The construction process of En-Tan-Mo itself is a kind of writing. The purPOSe of this writing is to realize the unity of free will and an ordered structure within a new dimension of space. This kind of creation is in the process of formulating a meta-historical rule or of writing history within its own system, and its authenticity will be determined by general consensus. For any one subject, arbitrarily setting rules and even changing history will bring about an unbridled temptation to POWer. Therefore, En-Tan-Mo not only recognizes the POSsibility that the creative subject can be deconstructed, but also actively implements this deconstruction process in order to create a truly decentralized, fair system.

---



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 » indéfiniment 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,





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 Pécuchet, 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 la prétention 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 dernier, 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 hypostases : la société, l'histoire, la

# 3.0 En-Tan-Mo Mathematics

This part will discuss blockchain systems from a mathematical point of view including our current work and future plans. We will also give a brief and intuitive introduction to mathematical theories used. Moreover, we will explain why we are building En-Tan-Mo.

## 3.1 Security problem in decentralized system

In 2009, Satoshi Nakamoto published "Bitcoin: peer to peer electronic cash system" in which he illustrated the mathematical foundations of Bitcoin and proved that the probability of successful attack on bitcoin system security (double spending) is extremely low given certain Poisson distribution assumptions. In this way he gave a solution to the trust problem in distributed ledgering system, alias Byzantine general problem.

We summarize the principal ideas of Nakamoto regarding quantitative probability estimates of successful cheating in blockchain system:

At the conclusion of one transaction a group of coordinated attackers starts trying to mine block with false information and build a fork upon it. At the moment that the honest miners have extended $n$ blocks, Nakamoto calculated the probability that the fork can at some point catch up with the real chain using full probability formula. But with emergence of ASIC mining pools the original hypothesis can no longer stand as the distribution of the fork does not conform to Poisson distribution. The computational struggle to extend new blocks is essentially a Binomial random walk problem from perspective of stochastic analysis.

$p$ = probability an honest node finds the next block;

$q$ = probability the attacker finds the next block;

We denote by $X_n$ the blocks mined by the attackers at the moment that the honest miners have mined $n$ blocks. This problem can be treated as a problem of points such that $q$ denotes the probability that the cheater successfully mines a new block; $p = 1 - q$ denotes an honest miner has won in the hashing and mines a new block, this is apparently equivalent to the probability that the attackers fail. If we look from the point of view of the attackers, then $P\{X_n = k\}$ can denote the probability of the event such that exactly $k$ successes occurs before $n$ failures and it can be described using Negative Binomial distribution:

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

Under the following assumptions:

1. The number of blocks mined by honest miners n is sufficiently large;

2. There exist a finite constant $\lambda$, $n\frac{q}{p} \to \lambda$. Denote $l_n = n\frac{q}{p}$, by the following calculations

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

$$(1+\frac{l_n}{n})^n \to e^{\lambda}$$

It can be obtained that the distribution law of random variable $X_n$ is approximately Poisson distribution $P\{X_n = k\} \to \frac{\lambda^k}{k!} e^{-\lambda}$.

However, with the emergence of mining pools the assumption (2) can no longer be satisfied, therefore the quantitative estimates of Nakamoto can no longer stand as a correct risk management control model for crypto-finance. Moreover, once the group of attackers obtains sufficiently strong computation resources and adjust its computational capacity by using impulse control(suddenly increasing hashing rate at the beginning of an attacking process, for example), then the probability of his success is significantly larger than what Nakamoto has estimated.

Therefore, by using proof of stake algorithms and control $q$, while increasing the creation rate of blocks can more effectively undermine the chance of successful attacks and obtain more precious estimates on that probability.

When the chain of honest miners has been extended by $z$ blocks, the difference in number of blocks between this chain and the one being mined by attackers can be denoted as $z - X_n$. Using methods from the gambler's ruin problem it can be derived that as the difference in number of blocks is $z - k$, the probability such that the chain of attacking group can at some point in the future catch up with the chain of honest miners is:

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

The probability of success of the attackers can be estimated as follows using full probability formula:

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

As can be seen in the works of C. Grunspun and R.-P. Marco, this probability is quite large even when the proportional computational recourses under control of the attackers is significantly less than 51%. For these arguments we will in En-Tan-Mo use a duality type consensus protocol as to monitor and constrain behaviors of miners by an election processes.

## 3.2 Nash equilibrium and consensus algorithms

The concept of Nash equilibrium is frequently used in the designing of En-Tan-Mo consensus algorithms. We first introduce its definition then briefly explains how it plays a central role in En-Tan-Mo consensus protocols.

SupPOSe $S_1, S_2, ..., S_N$ denote compact metric spaces and $J_1, ..., J_N$ define continuous functions on product space $\Pi_{i=1}^{N} S_i$. We denote by $P(S_i)$ the compact metric space of all Borelian probability measures defined on $S_i$.

Definition: In a game of mixed strategies Nash equilibrium means the tuple $(\bar{\pi}_1, ..., \bar{\pi}_N) \in \Pi_{i=1}^{N} P(S_i)$ such that, for any $i = 1, 2, ..., n$,

$$J_i(\bar{\pi}_1, ..., \bar{\pi}_N) \le J_i((\bar{\pi}_j)_{i \ne j}, \pi_i) \quad \forall \pi_i \in P(S_i)$$

where $J_i(\pi_i,..\pi_N) = \int_{S_1\times\cdots\times S_N} J_i(s_1,...,s_N)d\pi_1(s_1)...d\pi_N(s_N)$.

Theorem(Nash1950)(Glicksberg1952) Under the above assumptions, there exists at least one equilibrium point in mixed strategies.

There is a vast and expanding literature on game theory analysis of blockchain systems such as Bitcoin. Nash equilibrium is a state of strategies (for all nodes) which no participant can gain by unilateral deviation. This is essential to ensure the stability and security of a decentralized system as there cannot be a centralized controller maintaining order by "punishing" deviations.

The problem is that strategies at Nash equilibrium are not always efficient. In Bitcoin one can even say that the Nash equilibrium is highly wasteful. This is due to the fact that the only security mechanism is proof of work, with miners enter and exit freely. This is a purely non-cooperative game and the only deciding factor for wining is hashing rate. This POW mechanism design has been very successful in making miners follow the consensus in the sense of honest mining and following "the longest chain rule". In the mean time, miners always have incentives to upgrade their mining machines to maximize their profits. Eventually the computational arms race leads to wasteful mining pools and de facto blockchain oligarchs. In economics this is often referred to as "tragedy of commons" and in algorithmic game theory "price of anarchy".

This problem can only be remedied at the level of mechanism design, "the engineering side of economics". Mechanism design is also called inverse problem in game theory: not studying the outcomes based on mechanisms but rather seeking suitable mechanism which can lead to desired outcomes. Blockchain systems are the perfect domain for using mechanism design theory as designers have a lot of freedom at designing protocols or even laying down constitutions. Here mechanism can be seen as a procedure which assigns outcomes to strategies. The reason that Nash equilibrium is so important for mechanism design is that: if players are rational and can predict well what will happen, then they will predict a Nash equilibrium. Otherwise, someone will have incentive to deviate and not follow the consensus. In blockchain systems this problem become more acute: as there is no central POWer to put constraints, participants will deviate as soon as they feel the incentives. In ETM we used dual POW and DPOS mechanism design to achieve high efficiency of Nash equilibrium while maintaining strong decentralization. In our future work we plan to study the applications of Kantorovich type price mechanism and Vickery auction in ETM mechanism design.

## 3.3 Stake redistribution model in electoral system

Currently many blockchain systems adopted delegated proof of stake consensus(DPOS). DPOS consensus has the advantages of economizing resource expenditure and higher rate of blocks mining. The underlying theoretical proPOSition is that the nodes which own higher stakes within the given system can be more trustworthy. According to studies in the En-Tan-Mo system, based on analysis of current state of blockchains and crypto-currencies, the stake is usually highly concentrated in hands of minorities with Pareto type distributions. In order to prevent the concentration of voting POWer we need to designate the dependence of voting POWer on stakes as POSitively correlated but nonlinear. Here we only gave a brief review of our plan.

SupPOSe there exist $n$ nodes within the system and at the time of voting the proportion of stake owned by a given node $i$ is $\alpha_i$, $\sum_{i=1}^{N}\alpha_i = 1$. We define a strictly concave function $f$, $\frac{\partial f(\alpha_i)}{\partial \alpha_i} > 0$, $\frac{\partial^2 f(\alpha_i)}{\partial \alpha_i^2} < 0$. The proportion of voting POWer of this given node will be given by $\mathrm{B}_i = \frac{f(\alpha_i)}{\sum_{i=1}^{N} f(\alpha_i)}$, apparently $\sum_{i=1}^{N}\mathrm{B}_i = 1$.

By well-known property of concave functions $f(\sum_i \alpha_i) < \sum_i f(\alpha_i)$, it can be concluded two nodes with relative stake proportion given by $\alpha_i$, $\alpha_j$, with $\alpha_i > \alpha_j$ without loss of generality:

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

## 3.4 Chaotic shuffling

The consensus design of the En-Tan-Mo project has made security one of the most essential objectives and set a very high standard. In response to problem o coordinated attacks from multiple SCV miners in the DPOS system, the consensus layer will use chaotic shuffling algorithms.

Chaos: The extreme sensitivity of the dynamic behavior of the dynamic system to the initial value.

To put it simply, chaos refers to the fact that minimal perturbation to the initial value can result in a very large change in the mapping result, which can lead to an uncertainty in the prediction process. This uncertainty is exactly what we need. In the process of uploading blocks, if several miners want to join together to cheat, they need to continuously identify a block containing false information. For this purPOSe, they need to know the order of the uploading blocks of different miners as soon as POSsible and have enough time to coordinate. The chaotic shuffling refers to the fact that the order of miners' uploads is not determined at the outset, but that the consensus layer design specifies an algorithm that extracts certain information from each successful upload block for

mapping and performs multiple iterations to calculate the next miner. The number, therefore, is not known until the last minute.

1. We define a Hénon-type muti-dimensional mapping with the following dynamic:

$$x(n+1) = ay(n) + by(n)^2$$
$$y(n+1) = cx(n) + dy(n) + dx(n)z(n)$$
$$z(n+1) = x(n)^2 + ey(n)x(n)$$

2. Let 256bit binary and its corresponding decimal numbers be I and D, respectively, and the mapping relationship can be described as follows:

(1) Generate a random number of iterations $N_1 (3 \le N_1 \le 13)$ by using uniform distriution generating function randi in Matlab.

(2) Randomly generate the idxo of initial value by using system output at time mome

$$s = x(N_1) + y(N_1) + z(N_1)$$
$$idxo = \mathrm{mod}(s,3) + 1$$

(3) Generate two random numbers $(seg1, seg2)$ using the other two dimensions of the signal

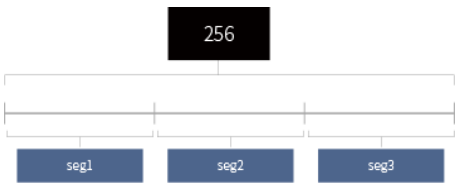
E.g:

$idxo = 2$, (i.e. select i from the x dimension as the initial value), then $seg1 = \mathrm{mod}(x(N_1),12)$

(4) Treat I as 32 8-bit blocks, divide I into 3 blocks using $seg1$ and $seg2$

$$I1 = slit(I, seg1), \quad I2 = slit(I, seg2), \quad I3 = slit(I, seg3)$$

$seg3 = 256 - seg1 - seg2$, the splitting rules corresponding to the slit function are as follows:




(5) Generate "system parameter scaling value" (var-par), "system iteration number" (val-N), and "system initial value scaling value" (val-ini) using I1, I2, and I3, respectively.

(6) Use val-par, val-N, val-ini to initialize the hyperchaotic system and perform calculations. Select the idxo-dimensional signal as the output, and generate an integer $D$ between 1-101 by exchange operation.

The chaotic mappings are deterministic, therefore at each step all miners obtain exactly the same result by calculating independently. The system can achieve stability and security while maintaining strong decentralization.

## 3.5 Kantorovich duality, optimal transport and decentralization

The consensus protocol in "En-Tan-Mo" is given the name Kantorovich consensus in homage to Soviet Mathematician Leonid Kantorovich for his work in the field of optimal transport, especially the duality theorem given in his work in 1937. This is one of the ground breaking results in linear programming and optimal transport. Here we given a brief review of the theory and how it might be related to construction of decentralized blockchain systems.

$X$, $Y$ are two sets that correspond to two given domains in the physical world and certain amount of material has to be transported from $X$ to $Y$. $c(x,y)$ denotes the transport cost from each point $x$ to $y$. $\gamma$ denotes the joint probability distribution on domain $X \times Y$ while $\mu$ and $v$ denote respective marginal distributions on $X$ and $Y$.

Then $\int_{X\times Y} c(x,y)d\gamma(x,y)$ can be used to denote the overall transport cost.

Kantorovich duality theorem states that:

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

here $inf$ and $sup$ denote infimum and supremum respectively. Overlooking strictness in mathematical details, we give an intuitive explanation of how it can be used: in a decentralized system as "En-Tan-Mo", if $\psi(y)$ designate the price of selling at point $y$ while $\varphi(x)$ designate the price of buying at $x$, then $\int_Y \psi(y)d\nu(y) - \int_X \varphi(x)d\mu(x)$ can be used to designate final cost of transactions. Duality theorem shows that under given condition $\psi(y) - \varphi(x) \le c(x,y)$, the strategy to minimize transportation cost is in dual relation with the strategy that maximize profit.

This theorem pointed out the importance of construction of a rational pricing system to the optimization of resource transport and allocation. Due to its implications in terms of economics this mathematical theory was for a long time rejected and criticized in Soviet Union by orthodox academics.

From the perspective of blockchain technology, optimal transport corresponds to the best strategy for transmitting value. It is reasonable to construct a trusting mechanism based on decentralized systems, to enable each participant making its autonomous decision with available transaction information such that a transparent market can emerge. A fair pricing system will emerge via dynamical equilibrium process that is based on the self-adaptive mechanism of the market itself. This is exactly how value-transfer can be achieved.

## 3.6 Dynamical price formation in decentralized system

In "En-Tan-Mo", each participant is at the same type provider(seller) and buyer of services. The core of decentralized system is the price mechanism and price formation can be achieved through self organization via dynamical equilibrium processes. "En-Tan-Mo" will use mean field game theory to study the price formation mechanism in decentralized trading system. This model is also called Lasry-Lions Price formation model. SupPOSe that price preference has some randomness. The density functions $f_B$, $f_V$ designate respectively the numbers of buyers and sellers(venders). $t$ denotes time of certain transaction and $x$ the price. For example $f_B(x,t)$ means the

number of buyers at a moment $t$ such that the price is $x$. $a$ denotes the transaction cost. The following mean field game systems will be used:

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

given initial conditions:

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

Here the multiplier $\lambda$ is used to describe the number of transactions at moment t. $\sigma$ describes randomness and $\delta$ is just a delta function.

Equations in this system are in some way similar to the simple model of one dimensional heat equations, however, the difficult part is the free boundary conditions. Free boundary value problem is one of the essential problems in modern theory of partial differential equations which naturally arises in many concrete physical problems such as phase transitions and it has wide applications in many fields.

In a decentralized blockchain system, due to the use of distributed ledgering, each nodes can adjust its own strategy dynamically in response to available transaction information. Therefore there exist essentially Bayes type adaptive control problems such that each participant uses a POSteriori probability distribution to change strategy so as to maximize its own potential profit. In further work, "En-Tan-Mo" plans to consider dynamical price formation model with Bayasian controls and connect blockchain technology with artificial intelligence and deep learning.

---

**References:**


【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. Japn. 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.

# 4. En-Tan-Mo Economics

Blockchain and related technologies will bring about a revolutionary transformation in modern economics. While industrial revolutions took place in a world underpinned by hierarchical business models and financial capitalism, the blockchain revolution will witness the birth of an economic system featuring humane capitalism and individual autonomy.

It is still unclear how it will unfold. Entrepreneurs and innovators will as usual explore the uncertainty by trial and error. However, there is no doubt that a staggering amount of wealth will be created and destroyed before a clear vision of this revolutionary transformation emerges.

The contribution of En-Tan-Mo is that it provides a balanced value transfer model at the start of this revolution so that people can have a better grasp of its meaning and significance.

---

## 4.1 En-Tan-Mo Crypto-Economics

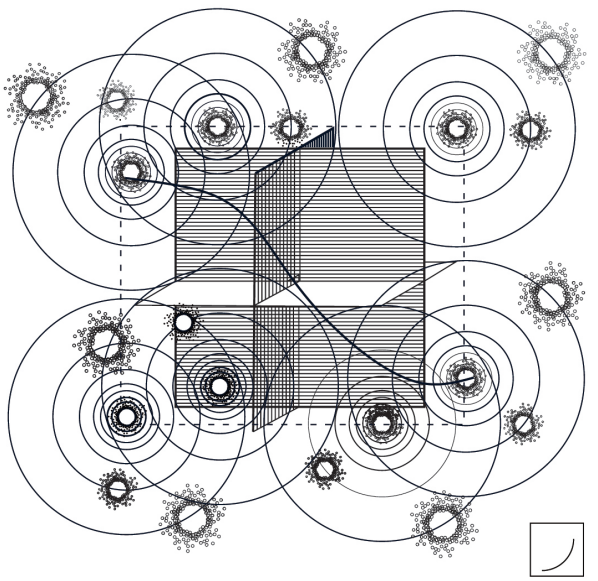
Trust-based relationship is common in business, especially in finance. Underlying each such relationship is the desire to eliminate uncertainty and minimize transaction costs. En-Tan-Mo makes possible for transactional information flows to be absolutely secure. This significantly enhances trust between people with technological guarantees and so obliterates uncertainty. Moreover, this enhancement of traditional relationships of trust bring with it a reduction of overall transaction costs.

Current blockchain technologies have other negative aspects besides overall low efficiencies. The blockchains application fall short on problems including trading speed (7 per sec for Bitcoin), privacy and retrievability (Mt.Gox being hacked). En-Tan-Mo will not only enhance overall efficiency but also ensure stable business operation. Relevant business models and value distribution system will be set up accordingly.

The object of En-Tan-Mo crypto-economics is to provide the role previously undertaken by institutions in a ledgering system with secure cipher and automatic trust. Classical and neo-classical economics studies the production and distribution of rare resources as well as the factors driving these processes. En-Tan-Mo crypto-economics studies protocols, protocols (such as laws, languages, property rights, social codes and ideologies) that enable collaboration between dispersed groups of people engaging in speculation and facilitate transactions in economy as well as social and political sectors.

En-Tan-Mo crypto-economics focus on the economic principles and theories bracing blockchains and their derived applications. Economics and its branch institutional economics work with communication and exchange systems. But institutional economics concentrate not only on protocols but on ledgers, i.e. data based on protocols.

En-Tan-Mo economics is interested in the following topics: protocol governing value transfer; social, political and economic institutional development with regard to this protocol; and how En-Tan-Mo change the value transaction mechanism at a social level.



## 4.2 Nash equilibrium

The reason why ETM excels in existing blockchain systems is that it proactively applies the game theory to mechanism design, which offers a solution to ingrained problems or "the price of anarchy" in blockchain systems, such as the low efficiency of bitcoin mechanism. With intricately designed dual-consensus mechanism, the En-Tan-Mo mathematician allows all players to contribute, be it as miners or voters, in the building of blockchain and get a fair share of reward. A brief but effective consensus agreement will be put in place to adjust the relationship within miners and voters and between miners and voters. Hence the strategy set of all rational players will converge to Nash equilibrium.

Consensus mechanism and algorithms form the foundations of En-Tan-Mo decentralizations, with the

essential purpose of achieving "rules without rulers" and "decentralized self-adaptive control". The most important concept in En-Tan-Mo consensus is Nash equilibrium which was introduced by the American mathematician and Nobel Prize winner, John F. Nash. It can be defined as a stable state system involving the interaction of different participants, in which no participant can gain by a unilateral change of strategy if the strategies of the others remain unchanged.

An important innovation in ETM consensus mechanism design is the extensive application of "rational expectation theory" in game theoretic analysis. Professor Thomas J. Sargent, senior advisor of ETM project, is world-renowned for his academic achievement in rational expectation theory. There are several things that need to be taken into account: participants have incentives to forecast and their beliefs about the future affect their present decisions. This is essential for ETM consensus mechanism design as the designer needs to "forecast" the decisions and strategies of the participants in various given situations. This corresponds to predictive model control in modern control theory. The security of the system depends on correct prediction of Nash equilibrium which in turn depends on the prediction of people's beliefs and response strategies. This has already been done in an informal way in our analysis. In the future ETM technology team will conduct more rigorous study in this direction.

En-Tan-Mo reckons that pure POW or DPoS is not enough to ensure that the strategies of blockchain users converge to Nash equilibrium. Take Bitcoin as an example, the miner who wins the hashing race and attempts to upload a block with false information would suffer a loss of computational power if the system denied extension. This is how the bitcoin system ensure fair utility for all miners. To be more specific: 1. if all blockchain users are allowed to participate in mining, then the hashing has to be difficult enough to sufficiently control the probability of successful cheating. Successful cheating occurs when a group of dishonest miners is able to construct a chain with blocks with false information that will eventually catch up with the chain of honest miners. 2. The cost of mining has to be sufficiently large so as to prevent the miner from risking using a dishonest strategy. With the appearance of ASIC miner, it is practically impossible for an ordinary miner to win a hashing race. The rise in computational power in the systems also causes it to be more difficult to engage in hashing. This overturns the Nash equilibrium. In Ethereum the full nodes are also ad hoc GPU miners which ordinary users cannot afford. Light users no longer care about mining. Likewise, in DPoS consensus systems represented by Steemit, the stake has become the standard such that large shareholders have assumed dominant positions in terms of voting. This leads to the reasonable conclusion that decisions are made by PoWerful minorities without mass participation. Wealth becomes centralized in the hands of a few and thus equilibrium is broken.

En-Tan-Mo and its consensus mechanism aim to provide a system in which all participants are direct recipients of benefits. Benefits cannot be monopolized by large mining pools or big shareholders, and fundamental reforms have to start from consensus mechanisms. Players in the En-Tan-Mo game are all users and they can be categorized into three kinds of identities: SCV miner, tribunal, and Pareto miner (a members of a Pareto mining pool). They obtain ETM tokens or other rewards by either voting or extending blocks. SCV miners are elected and they cooperate in extending blockchain in an orderly way within a given period. Even though a dishonest miner has less to lose because of the decreased cost of mining, he will suffer greater loss if he is expelled from the SCV mining group due to his dishonest behavior having been detected. In order to increase the efficiency of En-Tan-Mo blocks construction process, tribunals have the duty to select the best SCV miner and will be rewarded with ETM tokens for so doing. The proportional voting stake is related to proportional token stake by a concave function so as to ensure fairness for the majority of stake holders. SCV miners and tribunals are independent and interconnected at the same time in different respects so that the distribution of POW and stakes is clear and in equilibrium. Miners in Pareto mining pools at their current status cannot obtain ETM token rewards but they can participate in the mining of other blockchain systems as part of an entente effort. This arrangement ensures the interests of all miners at all times. Therefore, by dual consensus protocols in which DPoS and POW are coupled, the strategies of all players in En-Tan-Mo will evolve during interactions between different types of identities and eventually converge to Nash Equilibrium.

In order to explain how consensus design affects the decisions of players (with different kinds of strategies, and with honest or dishonest mining), we repeat the following rules and hypothesis:

Hypothesis: At least half of the miners are honest;

Rules: 1. Eventually only the longest chain will be accepted; 2. Dishonest or low efficiency miners will be voted out in the election processes.

## 4.3 Kantorovich Consensus

Widely recognized drawbacks of first and second generation blockchain systems using POW are: 1. The low processing rate of transactions. For example, the current transaction rate of Bitcoin is in no way comparable to traditional institutions such as credit card systems of banks. 2. Low speed in block construction, leading to delays in transaction confirmations. 3. Scalability. The current level of efficiency constrains the scaling of blockchains. 4. Waste of resources and environmental pollution due to POW mining.

For these reasons, En-Tan-Mo proposes Kantorovich consensus mechanisms based on the concept of Nash equilibrium. Tribunals are shareholders in En-Tan-Mo. They do not participate in block construction but rather obtain ETM token rewards by voting based on their previous or current proportional stakes in the system. Tribunals select SCV miners based on previous performance in hashing tests and mining. This ensures the high-performance and

security of En-Tan-Mo. SCV miners obtain ETM tokens by engaging in orderly mining. The hashing rate can be reduced without loss of security so that blocks can be constructed and uploaded at higher speed. The miners not elected will enter Pareto mining pools to form a coalition and mine blocks on other chains using specially designed derived chain technologies. They will receive payoff with other tokens according to their computational resources. In this way all miners are receiving positive payoff. Therefore, Kantorovich consensus can improve efficiency and scalability without loss of security.

Centralized systems still enjoy certain advantages in terms of efficiency. But by using better mathematical design of mechanism structures it is possible to balance decentralization with some centrally coordinated cooperation, and this can ensure the compatibility of security, stability and efficiency in a blockchain system. This is our main objective.

Kantorovich consensus protocol is a revolutionary kind of proof of stake protocol. It provides the rules by which all mining nodes will eventually reach consensus in networks. The algorithm is the key part in the En-Tan-Mo infrastructure and represents a great leap forward in blockchain technology. The Kantorovich consensus design has improved on energy consuming PoW protocols to overcome long-standing obstacles to the extension of blockchain applications. The algorithm is designed by our leading scientist and game theory team, and is to our knowledge the first POW and DPoS coupling consensus.

The reason we use the name Kantorovich consensus is because we are inspired by the work of Leonid Kantorovich, the Soviet mathematician who won the Nobel prize in economics in 1975. He proposed a strict mathematical model for studying optimal transport and Kantorovich duality theorem. This theory showed that optimal allocation can be achieved by decentralized price system. The economic theory of Kantorovich was for a long time rejected and criticized by "orthodox" academics in Soviet Union. He was saved from further persecution due to his involvement in the Soviet atomic project. The economic theory of Kantorovich was widely recognized and put into application in the west. Optimal transport is one of the most important and dynamic directions in mathematical research for the past 20 years. Many important mathematical discoveries of Cedric Villani and Pierre Louis Lions (both winners of the Fields medal) are closely related to the Kantorovich duality theory.

## 4.4 SCV miner and tribunal

Miners who were chosen during the election processes and passed the hashing test are called SCV miners, or SCV. Stake holders voting to select SCV miners are called tribunals. The proportional token stake of each tribunal is mapped into a number of voting tickets by a concave function. During each period voting will be rewarded. Eligible miners can become SCVs by winning sufficient votes and will then be able to upload verified blocks in order to obtain tokens as rewards.

Let's suppose a miner tries to behave in dishonest way for example, double spend or upload blocks with false information. The results will be as follows: 1. Since most SCVs are mining in an honest way, it can be argued using probability theory that the block mined by the dishonest miner will be a fork which eventually vanishes; therefore this miner will lose his mining cost. 2 Due to the periodical election system in the Kantorovich consensus mechanism, the dishonest miner will be expelled from the mining group at the next election and therefore lose the chance of getting further tokens as well as his previous deposit. We conclude that the rational behavior of any SCV will be to mine blocks honestly and efficiently.

Even though there does not exist a centralized monitor enforcing the behavior of SCVs and tribunals, the mechanism design will be the "invisible hand" in term of economics that guides them to obey the consensus simply by pursuing their own interests. This solves the trust and efficiency problems in En-Tan-Mo.

## 4.5 Pareto mining pools

The incentive mechanism of En-Tan-Mo is based on economic theory and has three advantages.

1. Fairness.In most blockchain systems such as Bitcoin and Ethereum, stakes are unfairly distributed with a bias towards several central mining pools. In En-Tan-Mo all individuals have fair chances because of the consensus mechanism.

2. Decentralization. In other DPoS blockchain systems, large stake holders control decision processes. This leads back to centralized control or monopoly by oligarchy. In the En-Tan-Mo system, stake holders and miners are separated in their responsibility, rights and interests. All participants can benefit from the resources and advantages of decentralization.

3. Optimality. In other blockchain systems, users have non-diversified value; different chains are like isolated islands without connections. In the En-Tan-Mo system, stake holders obtain reward tokens by voting and miners optimize their interests by switching between identities as SCVs and Pareto miners.

Under the Kantorovich consensus mechanism, all miners form a cooperative mining pool. In each period, selected SCVs extend the chain in an orderly way. En-Tan-Mo organizes all unselected miners to form a Pareto mining pool. By using specially designed side-chain technologies, coalition strategies and analytical algorithms of potential real-time income, these miners participate in the mining of other blockchain systems. The rewards are distributed according to their computational resources and ensure positive outcomes for all miners.

The core economic principles of Pareto mining pools are: design of coalition strategies; choosing appropriate

blockchains; building coalition structure and management systems; switching miners' mechanisms between SCV and Pareto miner status. A Pareto mining pool has the following characteristics:

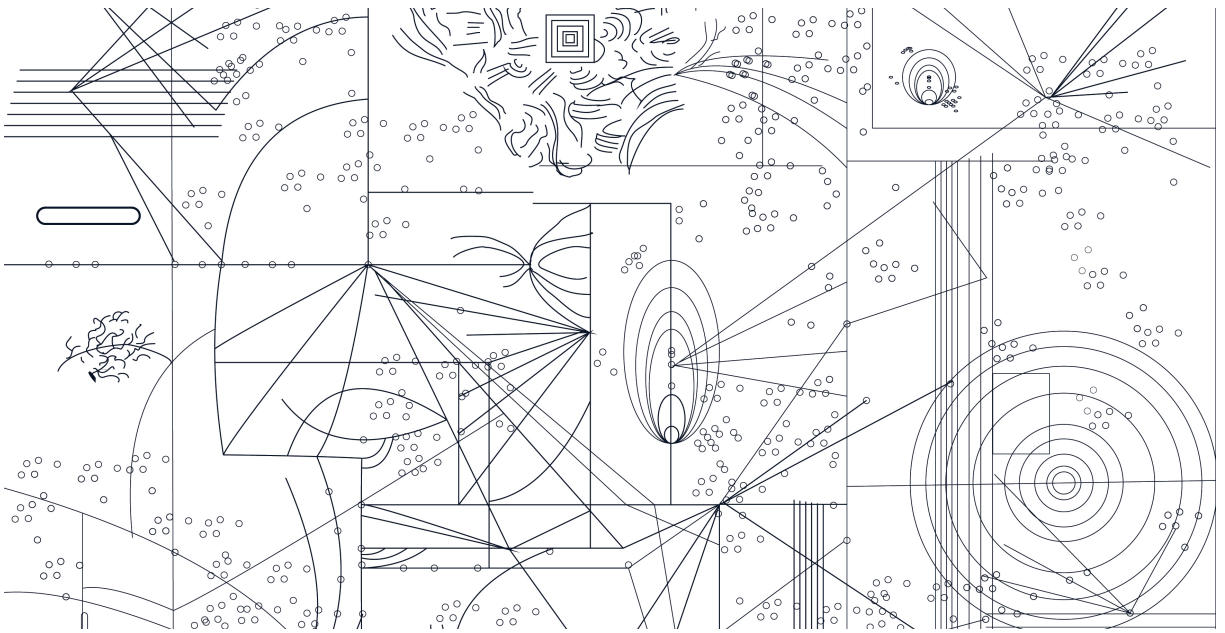
1. Decentralized organization. The main objectives of Pareto mining pools are sharing the market and cooperative mining. The relation between their members is not fixed but depends on the utility strategies of blockchains. The Pareto mining pool itself is a dynamic and open system.

2. Strategic actions. The design of Pareto mining pools results from far-sighted planning. The coalition will also place emphasis on strategically improving the business environment. The focus is on the active acquisition of economic resources.

3. Equal opportunity in cooperation. Pareto pool collaboration is more strategic than tactical. It is based on sharing resources, joint advantages, mutual trust and mutual independence. By reaching mutual agreement in advance and fair division of rewards based on computational resources, this mechanism has fundamentally closed the gap between miners.

4. Managerial complexity. The Kantorovich consensus mechanism defined for the first time genuine "multiple mining". Miners need to switch between SCV and Pareto pool strategies to maximize their profits.

Pareto efficiency or Pareto optimality is a state of allocation of resources from which it is impossible to reallocate so as to make any one individual or preference criterion better off without making at least one individual or preference criterion worse off. An allocation is Pareto optimal if no further Pareto improvement can be made. In other words, Pareto improvement is the way to obtain Pareto optimality. The Pareto mining pool corresponds to the ideal state of fairness and efficiency.



**References:**


【23】 T. J. Sargent, Lars Ljungqvist. Recursive Macroeconomic Theory. MIT Press, 2000.

【24】 T. J. Sargent. Dynamic Macroeconomic Theory. Harvard University Press, 1987.

【25】 J. V. Neumann, O. Morgenstern. (1944) Theory of Games and Economic Behavior. Princeton University Press. 2nd edition, 1947, 3nd edition, 1953.

【26】 J. Harsanyi. Games with incomplete information played by 'Bayesian' players. Management Science 14:159-182, 320-334, 486-502, 1967.

【27】 D. Fudenberg, J. Tirole. Game Theory. Boston: MIT Press, 1991.

【28】 N. Nisan, A. Ronen. Algorithmic mechanism design. Proceedings of the 31st ACM Symposium on Theory of Computing (STOC '99), pp. 129–140, 1999.

【29】 C. Papadimitriou. Algorithms, games, and the Internet. Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC '01), 749-753, 2001.

【30】 N. Houy. The Bitcoin mining games. Ledger, vol, 2016.

【31】 A. Kiayias, E. Koutsoupias, M. Kyropoulou, Y. Tselekounis. Blockchain Mining Games. arXiv:1607.02420v1 [cs.GT] 8 Jul 2016.

【32】 A. Sapirshtein, Y. Sompolinsky, A. Zohar. Optimal selfish mining strategies in bitcoin. CoRR, abs/1507.06183, 2015.

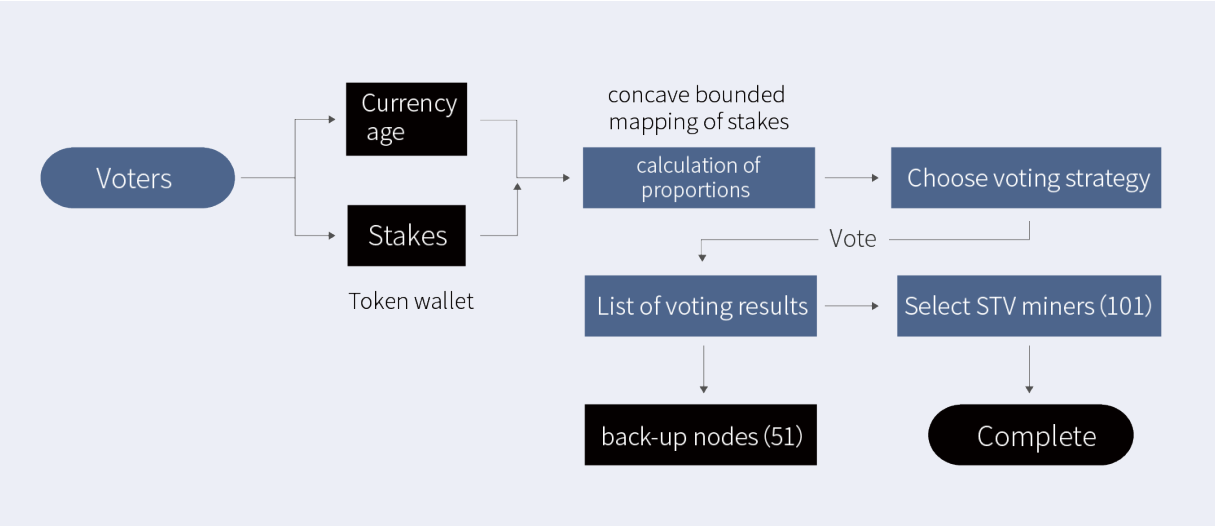
【33】 J. P. Aubin, A. Desilles. Traffic Networks as Information Systems: A Viability Approach. Mathematical Engineering 8445, Springer, 2017.

【34】 J. F. Nash. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, 36(1):48-49, 1950.

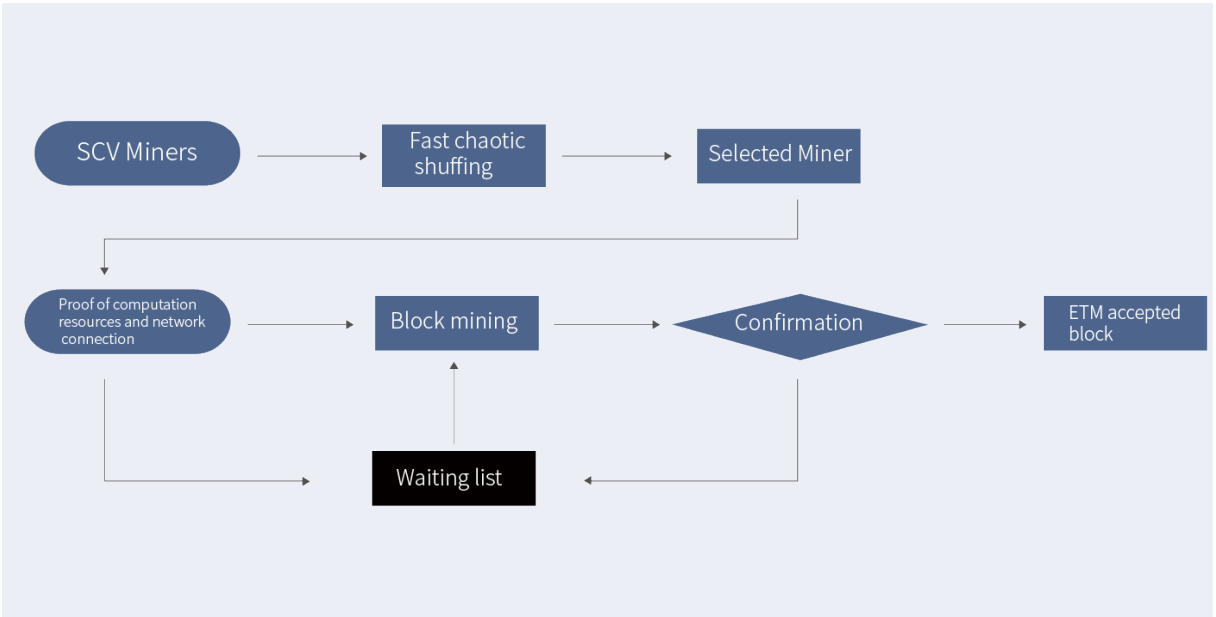
# 5. En-Tan-Mo computation

## 5.1 En-Tan-Mo flowchart

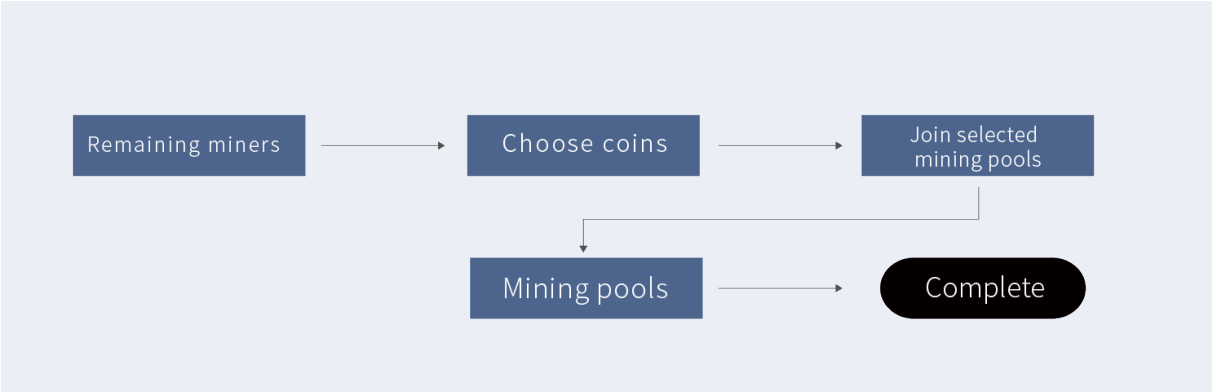
Kantorovich consensus protocol flowchart: Based on the idea of Nash equilibrium, Kantorovich consensus used the miners' team election system such that SCV miners mine blocks in given order. Without loss of security, Hashing difficulty can be reduced so that mining can be faster and more efficient.




Tribunal voting procedure: Votes of each tribunal can be calculated using a concave function of proportional token stakes. Rewards will be given within each period.




SCV miner working procedure: eligible miners which obtained more votes become SCV miner. They are responsible for mining and verifying blocks with due rewards.




Pareto mining pool procedure: Remaining unelected miners form Pareto mining pool, using specialized side-chain technology, coalition strategy and real-time utility algorithmic analysis, participate in the mining of blocks in other blockchain systems.

## En-Tan-Mo core codes

1.Tribunal Token stake equilibrium algorithm

SCV miners are elected by voting of tribunals and they have the rights to mine blocks. The function which maps token stake into number of votes is increasing and concave to ensure the equilibrium of En-Tan-Mo ecosystem. All blocks mined by SCV miners are legitimate. "Concavity" means that the stake to votes translation rate is in inverse relation with regard to the token stakes.

```
F(balance) = weights
//threshold mapping stake to votes translation rate is in inverse relation with regard to the token stakes to ensure equilibrium
threshold Map = Map(range,rate)
rate obtained from the token value interval
rate = threshold Map.get(range)
Token weights obtained from translation rate
weights = balance * rate
```

2.Tribunals Voting incentive mechanism

En-Tan-Mo is different from POW system, it provides rewards to tribunals as well to motivate participation in the platform. SCV miners can be selected and the systems will run efficiently and securely. En-Tan-Mo's voting incentive mechanism includes two kinds of rewards: voting rewards and out-of-block rewards. The tribunals are free to choose the percentage to obtain these two kinds of rewards. Voting rewards are obtained on the basis of the number of votes held by the tribunals. This reward is constant when participating in a vote. The mining bonus can only be obtained when the tribunals select the right SCV miners. The reward is a floating hedging value.

```
F1(tickets) = token
//Delivery ratio
tickets1 = fixed assignment //deliver to fixed tickets
tickets2 = dynamic assignment //deliver to fluctuating tickets //fixed rewards + fluctuating rewards(According to the proportion of selected nodes in the total number of nodes)
token = fixed(tickets1) + dynamic(tickets2)
```

3. SCV miners mining sequence algorithm

The sequence of SCV mining must be deterministic and pseudorandom to ensure the security of En-Tan-Mo. This absolute security is achieved by using chaos theory and nonlinear dynamics.

```
//Lock the voting rights of the client lock(balance)
//Calculate to get voting weights
tickets = F(balance) * F(time)
//Voters obtain list of delegates
delegations = votes(tickets)
//Shuffling
shuffle(delegations)
```

4. SCV miners Hashing algorithm

En-Tan-Mo needs to achieved high-performance besides security and decentralization. SCV miners do not compete in mining but cooperate in sequential mining. By fast chaotic shuffling each block is designated to one SCVminer. This miner has to finish SHA256 hashing as soon as possible and propagate the block.

Multiple hashing

```
blockhash = sha256(sha256(block))
//check time cost, miners that did not obtain results in designated time are considered unqualified
checkNodePerformance(useTime)
//Check whether the amount of calculation meets the specified requirements checkResult(blockhash,difficulty)
//If not, then change nonce
block.nonce = block.nonce + 1
```

## 5.2 En-Tan-Mo Data

### Blockheader data structure

Blockheader contain all information of the block. It is composed of the following fields:

- a 32-bit integer that identifies the version of the block
- 32-bit timestamp when the block was created
- 64-bit ID of previous block
- 32-bit integer corresponding to the number of transactions processed in the block
- A 64-bit integer that corresponds to the total number of transfers
- A 64-bit integer that corresponds to the total cost associated with the block
- 64-bit integers that correspond to the rewards represented
- A 32-bit integer corresponding to the length of the payload
- 256-bit hash of the payload
- Generate the 256-bit public key of the agent of the block

| 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 | |

--- -- -... ..- -.. ... -- .- -. -....- . --.- ..- .. - -.-- -....- -... .- .-.. .- -. -.-. .. -. --. -....- .- .-.. --. --- .-. .. - .... -- -....- ..-. --- .-. -....- -.-. ..- .-. .-. . -. -.-. -.-- -....- .... --- .-.. -.. . .-. ... -....- ... - ...- -....- -- .. -. . .-. ... -....- .- .-. . -....- ...- --- - . -.. -....- -... -.-- -....- - .... . -....- --- -- -... ..- -.. ... -- .- -. -....- - --- -....- --- -... - .- .. -. -....- - .... . -....- .-. .. --. .... - ... -....- - --- -....- ..- .--. .-.. --- .- -. -....- -... .-.. --- -.-. .-. ... .-.-.- -....- - .... . -....- -. ..- -- -... . .-. -....- --- ..-.

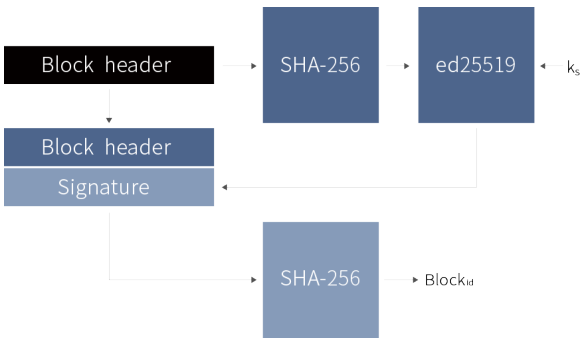
```
    "id": "15787022670460703397",
    "version": 0,
    "timestamp": 23039010,
    "height": 1574052,
    "previousBlock": "4576781903037947065",
    "numberOfTransactions": 0,
    "totalAmount": 0,
    "totalFee": 0,
    "reward": 500000000,
    "payloadLength": 0,
    "payloadHash":
"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
    "generatorPublicKey":
"c0ab189f5a4746725415b17f8092edd3c266d1e758e840f02a3c99547b3a527f",
    "blockSignature":
"c6b2bcc960066be078efbfffed625f61553a7bc18ebde3892636c2f36850de234a9c
70ba3e33b606db2eff724398026984e4d391c1fbbe70c94dd9d07ff0060b",
    "totalForged": "500000000"
  }
```

### Block ID generating procedure

Generate hash SHA-256 of blockheader and use the trusted key to perform (ed25519 algorithm) signature.

Once the block header has been signed, the system uses SHA-256 to hash the completed block header to generate the Block Id.

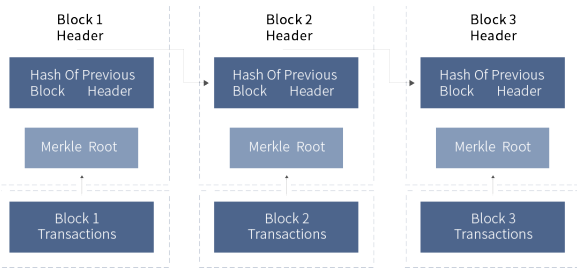
A signed block generates its block using the following flower




### Blockchain structure

It can be seen that the block mainly consists of a block header and a block body. The block header contains the version number, the address of the previous block, the timestamp, and the root of the merkle number. The block body mainly contains the transaction count and transaction bill details.

The blockchain consists of a series of data blocks generated using cryptographic methods. Each block contains the hash of the previous block, starting from the genesis block and connecting to the current area. Blocks form block chains.

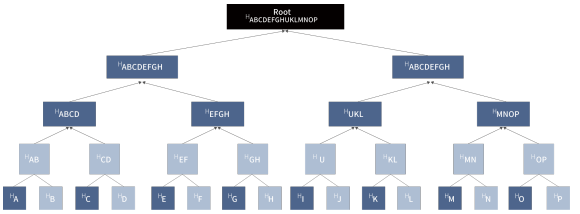



### Data storage Merkel tree structure

Merkle Tree, also commonly referred to as Hash Tree, is a tree that stores hash values.

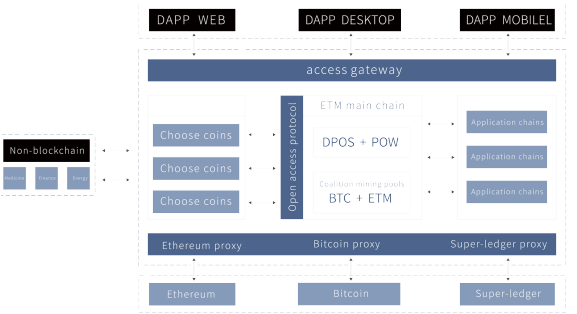
The leaves of a Merkle tree are hash values of data blocks (eg, files or data).

Non-leaf nodes are hashed with their corresponding sub-node concatenation strings




### 5.3 En-Tan-Mo interface

En-Tan-Mo is based on the idea of BaaS (Blockchain as Service) and the standard of micro-service. Taking the self-evolving component library as the core and the developer community as the driving force, it provides an adaptation platform for other blockchains to complete the free transfer of assets and applications. En-Tan-Mo provide two-way invocation of soft channels for non-blockchain applications and data, it provides developers with the ability to complete component uploads, reviews, and rewards in the shared lobby. For ordinary users , En-Tan-Mo provides BaaS gateways to implement accessibility service calls. In this way, each blockchain is connected to other chains as well as non blockchain systems and this helps technology developers and ordinary users move from the Internet to the blockchain.




System Structural Diagram Description:

Application layer (web, desktop, mobile) data access through unified access gateway

.Data interaction through application components and offline resources (existing systems)

. Application components interact with data via the open access protocol

. The application component internally integrates the data on and off the chain

. The main chain and the application chain communicate through the internal protocol data and value transmission

. Cross-chain interaction with third parties through the proxy layer

**References:**


【35】 I. Bentov, A. Gabizon, A. Mizrahi. Cryptocurrencies without proof of work. In 3rd Workshop on Bitcoin and Blockchain Research - Financial Cryptography, 2016.

【36】 S. Micali. Computationally sound proofs. SIAM J. Comput., 30(4):1253–1298, 2000.

【37】 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.

【38】 C. Dwork, N. A. Lynch, L. J. Stockmeyer. Consensus in the presence of partial synchrony. J. ACM, 35(2):288-323, 1988.

【39】 S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak. Proofs of space. In CRYPTO 2015,

【40】 Slasher: A punitive proof-of-stake algorithm. https://blog:ethereum:org/2014/01/15/ slasher-a-punitive-proof-of-stakealgorithm.

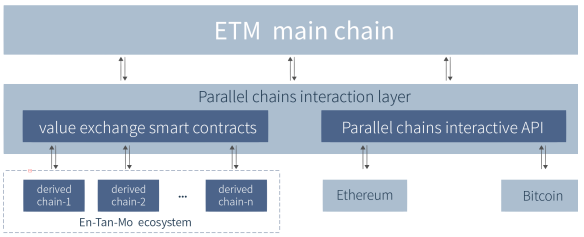
【41】 S. Park, K. Pietrzak, A. Kwon, J. Alwen, G. Fuchsbauer, P. Gazi. Spacemint: A cryptocurrency based on proofs of space. IACR Cryptology ePrint Archive, 2015: 528, 2015.

【42】 M. Rosenfield. Analysis of hashrate-based double spending. arXiv:1402.2009v1, 2014.

# 6 En-Tan-Mo Ecosystem

## 6.1 Central chain and derivative chains

Among the many problems faced by blockchain systems, the lack of interoperability between blockchains greatly limits the application potential. For both public and private chains the key to achieving value transfer is through inter-chain technologies. These technologies can build bridges to connect and expand previously isolated blockchain systems. What they can achieve is more value lock-in rather than more value transfer. Based on investigations of current interchain technologies, En-Tan-Mo proposes a new parallel chain interactive protocol to facilitate value transfer and build a blockchain ecosystem that can include apps each with over ten Mirions users.

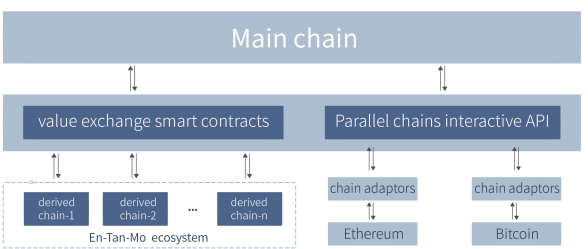



In order to solve the problem of rapid expansion and BaaS, En-Tan-Mo has designed a system of one central chain with multiple derivative chains. The central chain is responsible for network security and value transfer. A derivative chain is a special kind of blockchain targeted at specific DAPP. It is an independent and isolated system. By inheriting and replicating technologies from the central chain, each DAPP has its own ledger and token system. Its consensus mechanism, block parameter and transaction types can be customized. Derivative chains are parallel to each other.

They can achieve bidirectional transfer of assets between the central chain, other derivative chains, and external blockchain systems through the "parallel chain interaction layer". This enables users to utilize their existing assets to use the En-Tan-Mosystem.

## 6.2 Parallel chain interaction protocol

En-Tan-Mo's parallel chain interaction protocol makes it possible to support value transfer between different blockchains. It mainly consists of two parts: a chain-adaptation module and a value exchange smart contract. The main purpose of designing a chain adapter is to provide En-Tan-Mo interaction interfaces with different chains for value exchange smart contracts in order to verify transactions on different chains. Simultaneously, builders in the community can themselves develop and improve on chain adaptors for diversified functions and obtain tokens as rewards. For example, applications can switch between underlying blockchains with different protocols using chain adaptors. Value exchange protocol is the core of parallel interaction protocols. It enables users to exchange capital on and between all kinds of blockchains, including central, derivative and external chains. An internet system of interchain value connection will be thus constructed.




### Chain adaptors

The chain adapter is like a device driver for a computer. It converts the underlying blockchain protocol into an easier-to-use way for the En-Tan-Mo central chain, allowing it to run value exchange smart contracts over the En-Tan-Mo central chain. The technologies involved include but are not limited to Hash Time Lock Constructs(HTLC), SPV proof, and API development.

En-Tan-Mo will first provide adapters for some of the most commonly used blockchain systems such Bitcoin and Ethereum, and will become an open source system after stable operation. Anyone can contribute to improving open-chain access protocolsor and implement their own code. En-Tan-Mo plans to support more blockchain protocols and give corresponding rewards in the form of tokens.

### Value exchange smart contract

Although the innovative technology of blockchain has long been a global focus, there has always been a problem: value transactions between different blockchain systems still require third-party middlemen such as exchanges, and it is these that need to be replaced by decentralization technology. En-Tan-Mo uses minimum trust smart contract and chain adapters to replace these middlemen and function as bridge between different chains. This method has deepened the connection between the two most important elements in blockchains and brought En-Tan-Mo closer to becoming a global value transfer network.

Value exchange smart contracts rely on En-Tan-Mo's Turing complete virtual machine to operate and provide users with adequate security. A value exchange smart contract between central and derivative chains is like a decentralized exchange. It has an ETM wallet address and control over it on corresponding chains. Once a user initiates a transfer on a derivative chain which is recognized by the central chain adapter, the value exchange smart contract will automatically transfer an equivalent amount to the user's ETM wallet address on the central chain to complete the exchange of value. Simultaneously, En-Tan-Mo has incorporated Hash Time Lock Constructs in order to eliminate risk for users during

exchanges.

For the specific exchange process, let us take the exchange of Bitcoin and ETM as an example. The steps are as follows:

Bitcoin blockchain User A must first register with En-Tan-Mo to bind the mapping relationship between User A's ETM wallet address and the BTC wallet address;

User A generates a random secret number (a) and finds its hash value H(a). Then, a special transaction is initiated on the bitcoin blockchain to the Bitcoin address of the value exchange smart contract, which is locked for 12 hours based on Hash Time Lock Controls technology. The En-Tan-Mo value exchange smart contract must produce a hash image H(a) of the original image in order to obtain the token,. Otherwise, 12 hours later, the BTC of the transaction automatically returns to user A's Bitcoin wallet address.

The En-Tan-Mo smart contract monitors the confirmation of these special transactions in the Bitcoin blockchain through the bitcoin chain adapter and performs SPV verification. Once the SPV verification is passed, the En-Tan-Mo Value Exchange Smart Contract initiates a special transaction in the central chain to User A's ETM wallet address, which is locked for 6 hours.If User A wants to obtain the ETM token in the transaction, the original image (a) of the hash value H(a) must be presented. Otherwise, the ETM token in the transaction is automatically returned to the ETM wallet address of the smart contract after 6 hours. Once User A presents the secret number (a) to retrieve the ETM token in the transaction, the smart contract will know the secret number (a), so the smart contract can access the Bitcoin blockchain network through the adapter and accept User A as a user. So in the transaction Bitcoin has been transferred from one user to another. The transaction is then complete.

What needs to be emphasized is that the central chain is only used as a decentralized value exchange, and it does not rely on locking in User A's Bitcoin to achieve value transfer. User A transfers Bitcoin to the smart contract Bitcoin wallet address, and smart contracts can be used for those users who want to exchange ETM tokens for Bitcoin. At the same time, after User A exchanges bitcoins for ETM tokens, these tokens can be transferred back to not only the bitcoin blockchain but also to other external blockchain tokens through the same process. Therefore, what En-Tan-Mo achieves is value exchange, not asset locking. In addition, all value exchange smart contract addresses initially have zero tokens. They need investment from corresponding blockchain users. In return, the smart contract distributes the transaction fees spent by the user during the value exchange process to the appropriate investors in proportion to their investment. During the investment process, users can retrieve investment funds from smart contracts at any time.

In sum, based on value exchange smart contract, what En-Tan-Mo will construct is an inter-chain value network. En-Tan-Mo does not create value out of thin air but serves as an agent of value transfer.

Application Ecosystem

En-Tan-Mo is a new generation blockchain platform. By running APPs on independent derivative chains, it effectively solves problems that have been troubling other blockchain systems such as block size expansion and delayed synchronization. The multi derivative chain mode has provided an ideal solution to the network congestion problem under high frequency trading conditions. Users only need to download a derivative chain when the corresponding APP is needed. This can greatly reduce useless synchronization data and keep the entire En-Tan-Mo network in state of high performance. Moreover, thanks to the value exchange smart contract, inter-chain network can be effectively integrated with technologies such as high-performance graphene technology, lightening payment network. As a result, En-Tan-Mo can support APPs with over ten Mirion users and interconnect withentire blockchain ecosystems.

## 6.3 Mir Mall

En-Tan-Mo's Mir Mall can conveniently and effectively help companies or developers put blockchain into application more quickly and economically so that users can enjoy secure use of the facility. In view of the centralized nature of current APPs, we call decentralized applications on derivative chains DAPPs. Mir Mall has the following advantage:

(1) It provides the blockchain ecosystem with APPs of over ten Mirion users;

(2) Assets from derivative chains can be traded with other tokens(such as ETM/BTC/ETH) through En-Tan-Mo parallel chain exchange protocols. As a result, applications based on En-Tan-Mo will have a larger number of users.

(3) Based on the En-Tan-Mo parallel chain exchange protocol, DAPPs can access data from multiple underlying blockchains, allowing DAPP to operate based on multiple underlying blockchains.

(4)With the use of En-Tan-Mo's derived chain technology and a series of SDKs, APIs, and templates provided by developers, developers only need care about business logic and can easily build, test and publish their own personalized DAPP. The reduction of the R&D costs of developing new types of applications will help developers to better and more quickly own DAPPs at Mir Mall. Moreover, these DAPPs can be downloaded and executed by all ETM nodes and serve all blockchain users.

(5) Based on En-Tan-Mo's derived chain technology, skilled developers can customize the mall DAPP's personalized database, consensus mechanism, transaction types, and account system.

(6) En-Tan-Mo will build a comprehensive reward system. Developers of excellent DAPP will receive tokens as rewards.

# 7 "En-Tan-Mo" Organization Structure

En-Tan-Mo community consists of En-Tan-Mo Foundation, ETM FinTech and ETM BD with the Foundation as its core. En-Tan-Mo Foundation is a Singapore-registered non-profit organization which aims to ensure the smooth operation of ETM project and provide all-round support to ETM user community. In addition, En-Tan-Mo project is supported by Fintech, a technology development company with a focus on blockchain technology research and development, and ETM BD Business Promotion Company.

## 7.1 En-Tan-Mo Foundation

The En-Tan-Mo Foundation is a non-profit organization established overseas and is mainly responsible for the ecological construction and technical support of the En-Tan-Mo community. The core task of the En-Tan-Mo Foundation is to regulate, protect and promote the self-developed En-Tan-Mo infrastructure and block-chain protocols. At the same time, it also plays a role in investigating and proposing regulations on block-chains and cryptocurrencies, protecting, enhancing, and advancing the En-Tan-Mo ecosystem, and aggregating, educating, and nurturing the En-Tan-Mo communities.

Under the effective supervision of the entire En-Tan-Mo community, we propose that the foundation, as an independent third party, would plan for long-term developments.

In addition, the En-Tan-Mo Foundation will also act as a public interest organization, pay attention to public affairs and philanthropy around the world, and promote the development of a global public trust system.

The En-Tan-Mo Foundation Council has adopted a democratic decision-making process to determine the constitutional policies of the Foundation and the Secretary-General's responsibilities, under the leadership of the Council. The board of tribunals oversees the operations of the council. The board of tribunals generally includes some well-known public figures and professional financial personnel.

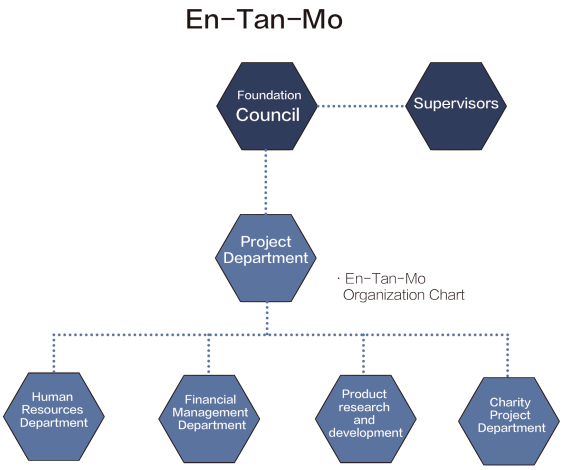
### En-Tan-Mo Foundation Council

The En-Tan-Mo Foundation Council's main focus is charity work. The Foundation is divided into product research, financial management, marketing promotion, human resources, legal affairs, etc.; all these divisions will jointly run the foundation's day-to-day operations.

### En-Tan-Mo Foundation Charity Project

The En-Tan-Mo Foundation's Charity Project Department is the core business unit of the Foundation. It is responsible for the operations and management of the foundation's public welfare projects and fulfills the foundation's public welfare goals to implement the Council's overall decisions. The En-Tan-Mo Foundation Board will help with selecting, planning and financing ideas based on their excellence, and the team will turn them into reality. In the early development process of the foundation, the Foundation Charity Project was responsible for the drafting of the En-Tan-Mo Foundation constitution, which was approved by the council as its own operating rules.

The project department of the En-Tan-Mo Foundation is also responsible for the emergency response mechanism. Under the control of the En-Tan-Mo Council, the Foundation discusses public relations; after reaching



· En-Tan-Mo Organization Chart

a consensus decision, it will disclose it to the public. The overall direction of the development of the Fund will be drafted by the Council; it will include new promotion channels, extensibility, and implementation of the channels.

### En-Tan-Mo Financial Management Department

En-Tan-Mo has an independent, open and transparent financial management mechanism.

(a) All transactions of the En-Tan-Mo Foundation will be approved by professional financial officers and recorded in the block to achieve open, transparent and non-retroactive financial supervision. In addition, all expenditures of the foundation will also be audited by professional financial officers and relevant financial registrations will be made in the block.

(b) The En-Tan-Mo Foundation will publish a monthly financial report to reconcile the funds. The financial report will be audited by the expert finance officers appointed by the Fund and authorized personnel by the En-Tan-Mo Community Personnel Management Committee.

(c) The fundraising, major events and development of the En-Tan-Mo Foundation will be reported to the community on a regular basis. Changes in major issues and functions will be reported to the community in advance in the form of announcements.

### En-Tan-Mo Human Resources Department

En-Tan-Mo has a human resources system that is open to the entire community. It is different from the traditional corporate structure. En-Tan-Mo's personnel recruitment practices are fair and open, and they are recorded in blockchain.

(a) For any recruitment of junior personnel, professional staff will perform two rounds of the aforementioned tests to form an independent evaluation report and write it into the recruitment record. All records will have features that cannot be tampered with and

permanently backtracked.

(b) Candidates meeting the recruitment requirements, will need final approval by the relevant committee. The core developers, as well as the core managers, need to go through the duty-dividing process, as reviewed and approved by the foundation core team of En-Tan-Mo.

(c) For businesses that may be outsourced, an outsourcing agreement will be drafted, discussed and signed, and wages and salaries will be determined. The entire community will be notified, and outsourced contracts will be written into smart contracts.

### En-Tan-Mo Fund Board of Tribunals

The En-Tan-Mo Foundation Board of Tribunals is responsible for all En-Tan-Mo participants. In order to oversee the legitimacy and performances of the directors and of project personnel and to safeguard the legitimate rights and interests of the company and its shareholders, tribunals need to effectively inspect and evaluate the financial status and management of the Foundation. The Fund's Council shall, according to the requirements of the Board of tribunals, report to the Board of tribunals itself on the signing and implementation of the Fund project, the use of funds, profits and losses.

## 7.2 ETM FinTech Technology Development Corporation

The role of ETM FinTech is mainly to develop and maintain this new ecosystem. The development of En-Tan-Mo is mainly divided into four phases:

"Petrarch": ETM FinTech will develop a brand-new, decentralized En-Tan-Mo blockchain that is completely protected and supported by network-based protocols and strict encryption technologies, forming a whole new set of currency rules and systems, and can be traded or exchanged with legal currency.

"Masaccio": ETM FinTech will digitally register all kinds of assets on the block-chain to ensure asset security and data integrity, develop En-Tan-Mo smart contracts, use zero-knowledge related technologies, and develop Lightning Network technologies network and coding technology to increase transaction speeds, reduce the burden on the blockchain, and increase scalability.

"Da Vinci": ETM FinTech will use En-Tan-Mo to evolve the ecosystem in broader application scenarios. The development of smart contract standards is the key. Financial transactions can be transformed into use on En-Tan-Mo, including stocks, private equity, crowdfunding, bonds, hedge funds and all types of financial derivatives: futures, options, etc.

"Giorgione ": In this period, En-Tan-Mo will further evolve in the economic field. It can be used to achieve the increasingly global distribution of physical resources and human assets, and to promote large-scale collaboration in science, health, education and other fields mainly in automated procurement, intelligent networking applications, supply chain automation management, virtual asset exchange, property registration and other scenarios.

Once the system is released, ETM FinTech will no longer control the direction of the system. Only the system's stakeholders, the owners of tokens, and interested researchers will decide the future developments of the system.

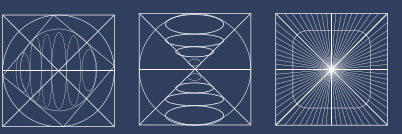
## 7.3 ETM BD Business Cooperation Company

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, fully-featured, plug-and-play system by providing integrated industry solutions such as free derivative chaining, smart contracts, and application hosting. Within 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 assurance.

Any individual or company that is interested in the En-Tan-Mo blockchain technology and wants to change the industry through this technology, will receive help and support by the ETM BD through a variety of flexible methods such as direct investment, assisting development, providing solutions and realizing En-Tan-Mo's blockchain application.

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

"En-Tan-Mo" Organization Structure



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 assurance.

### Notes:

1. Policy Risks

Regulatory policies for block-chain projects and swap-financing are not yet clear in all countries; there are market risks for participants deriving from unclear policies. If the overall value of the digital asset market is overestimated, then investment risks will increase and participants may expect the growth of swap projects to be excessive, but these high expectations may not be realized.

2. Regulatory Risks

The transaction of digital assets including En-Tan-Mo has extremely high uncertainty. Due to the lack of strong supervision in the field of digital asset trading, there is a risk that electronic tokens will surge or plunge and be controlled by the dealer. If people lack experience after entering the market, it may be difficult to resist the asset shocks and psychological pressure brought about by market instability. Although experts from the academic circles, official media, etc., agree in often suggesting careful participation, there are no written regulatory methods or provisions. Therefore, it is difficult for such risks to be effectively avoided.

It is undeniable that in the foreseeable future, regulatory regulations will be introduced to restrict the blockchain and electronic token fields. If/When the sector management will be more tightly regulated, tokens purchased during the swap period may be affected by fluctuations or restrictions on prices, easiness of sale, and other market related shocks.

3.Team Risk

Currently, there are many teams and projects in the field of blockchain technology. The market competition is fierce and there is high project operating pressure. Whether the En-Tan-Mo project will be able to break through a field crowded with many outstanding projects and will be widely recognized is not only linked to its own team ability and planning, but also affected by the presence of many competitors and even oligarchs; and there is the possibility of vicious competition between them. En-Tan-Mo is based on the founder's many years of industrial networking, bringing together a team of talents with both vitality and strength, attracting senior players in the block-chain field and experienced technical developers. The stability and cohesion within the team are crucial to the overall development of En-Tan-Mo. We cannot rule out the eventuality of the departure of core personnel and the internal conflicts in the team, which would negatively affect the performance of En-Tan-Mo.

---

## Disclaimer

This document is for informational purposes only. The content of the document is for reference only and does not constitute any investment advice, offer or invitation to sell shares or securities in En-Tan-Mo or its related companies. Such solicitation must be conducted in the form of a confidential memorandum and must comply with the applicable laws. The contents of this document are not to be understood as encouraging participation in the interchange. Nothing related to this document should be construed as participation in the interchange, including requesting a copy of this document or sharing this document with others. Legal age and full civil capacity are required for participation in any transaction. The contract signed with En-Tan-Mo is real and effective. All participants voluntarily signed the contract and declared to have clearly and fully understood of the structure and functions of En-Tan-Mo before signing the contract.

The En-Tan-Mo team will continue to make reasonable attempts at ensuring that the information in this document is true and accurate. During the development process, the platform may be updated, including but not limited to platform mechanisms, tokens and their mechanisms, and the distribution of tokens. Some of the contents of the document may be adjusted accordingly in the new version as the project progresses. The team will publish the updated content by posting an announcement or a new version of the document on the website. Participants are expected to obtain the latest version of the document in a timely manner and make timely adjustments based on the updated content.

En-Tan-Mo expressly states that it does not assume any liability for the participant's inaccurately relying the contents of this document and any actions resulting from this document. The team will spare no effort to achieve the goals mentioned in the document. However, based on the existence of outside intervening factors, the team may not always be able to completely fulfill the commitment.

Whether or not the value-added of En-Tan-Mo depends on the market law and the needs after the application

is put into place. It may not have any value, the team does not make any commitment to its value-added, and is not responsible for the consequences of its value increase or decrease. To the fullest extent permitted by applicable law, the team shall not be liable for damages and risks arising from participation in the interchange, including but not limited to direct or indirect personal damages, loss of commercial profits, loss of business information, or any other economic loss. Our team decline any responsibility.

The En-Tan-Mo platform complies with any industry self-discipline statements that are conducive to the healthy development of the exchange industry. Participation means that the representative will fully accept and comply with such norms. At the same time, all information disclosed by the participants to complete such inspections must be complete and accurate.

The En-Tan-Mo platform clearly disclosed possible risks to the participants. Once participating in the exchange, they have confirmed their understanding and acknowledged the terms and conditions in the detailed rules, and accept the potential risks of the platform at their own risk.

“ AGREED VALUE SHARED BENEFIT ”