Αν οι αρχαίοι Έλληνες γνώριζαν αυτόν τον νόμο
σίγουρα θα θεωρούνταν Θεοί. Καθοδηγεί τον κόσμο.
θε για ήσυχη χειρονομία σε ένα από τα πιο σύγκλιτα.
Όσο υψηλοτερώσει τον υπέρτατο Κανόνα τον ανηφθ αν σχεδιού
Όταν μια σειρά επιφανειακών παραγόντων συγκεντρώ-
νονται. μια απροσδόκητη και εξαιρετικά όμορφη
κανονικότητα αποδεικνύεται ότι είναι σωστή.

EN-TAN-MO SCIENCE

Interpretation

AGREED VALUE SHARED BENEFIT

EN-TAN-MO

EN-TAN-MO

AGREED VALUE SHARED BENEFIT

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

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

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

http://www.entanmo.com

Foreword

“

AGREED VALUE SHARED BENEFIT

”

Preamble

Satoshi Nakamoto: an Underestimated Name

On 31 October 2008, a paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System brought its writer "Satoshi Nakamoto" in the limelight for the first time ever in which Bitcoin, a digital currency was briefed on and blockchain, a concept never heard of before, ushered in.

Following Satoshi's 575 emails and 364 live records online is his disappearance ever since.

A decade on, the initiator of Bitcoin remains hard to be tracked down. Meanwhile, however, his halo above head has never ever faded away. Some call him the father of Bitcoin, some revere him as the Deity of blockchain, and others even assume him the invisible Nobel economics prize winner.

In the writer's opinion though, surrounded by the halo as such, he cannot have been underestimated enough.

Reasons behind?

Underestimating Satoshi Nakamoto is synonymous with that of the power science and technology has transformed our lives.

At the threshold of the 19th century, human beings have been embracing a technological booming era during which the world has been witnessing its fastest evolution. A closer look into the technologies, the most innovative and influential, reveals that they are commonly featured by expanding people's space and interaction via innovation. Creations altering this world, such as paper, printing and the Internet, have all blazed a new trail for needs of free expression, mutual communication and the transfer of information as well as values.

Blockchain is deemed as a distributed ledger. Provided that all transactions are entries, then their bookkeepers are each and every authorizer within the network whose own ledger is stored in multiple copies by other nodes for anyone to search into. System as such allows no one or not a single operator to tamper with the data. Thanks to its anonymity, individual privacy can be well protected and new means of communications together with values transfer, safe and anonymous, achieved across the globe. A unique trust machine created in the 21st century, it is a brand new channel for communications and transfer also.

Imaginably, the blockchain technology would be substantially changing people's lives.

Meanwhile, however, many may ask: Why haven't I felt my life being changed by blockchain?

Given the fact that the blockchain is a revolution at the protocol level and that for ordinary people, visible changes are at the application level, when we make our payments via Apps, probably, we may have no idea at all whether the protocol is centralized or decentralized as what we see is the change of figures on our accounts only. Moreover, since the revolution is basically at a lower level, it can be rather difficult for us to "see" those ameliorations in our lives. Furthermore, onlookers or skeptics about new things, invariably, people are very much concerned, as evidenced by their skepticism of steam engine and condescendence to telephone upon creation per se, one of the factors why the blockchain technology has yet gained its due public attention up until now.

Underestimating Satoshi Nakamoto means the underestimation of decentralization.

Fast forward to the birth of blockchain, Satoshi Nakamoto made it explicit that the core of blockchain is

decentralization, a most thrilling feature of its technology.

Highly centralized society makes us fall victim to third parties and major economic institutions on all fronts. They are by nature artificial, but due to their highly organized and elite characteristics and the fact that they can deal with an array of things beyond human capacity, individuals are increasingly reliant on them. Gradually, the third party sprawls onto the domain to which lives belong. "Colonisation of lives", therefore, has come into being, meaning that non-market and non-commercial activities within the range of private domain and public space have been eroded by market mechanism (money) and stratification.

Technical strengths of blockchain such as decentralization, trustless nature, timestamp, asymmetrical encryption and smart contract simply enable individuals to engage in activities of economy, culture and all social sectors even free from any third party's interference. We can fully envision a future where every social sector is not reliant on any third party, for instance, financing, retailing, HR, advertising, public service, IPR protection, science and technology, politics and society. Not only is it a drastic social transformation, but what matters for scientific and technological revolution.

Short as a decade or so, under the guise of decentralization comes a growing number of blockchain projects, either bypassing it or riding off on side issues, in pursuit of efficiency merely. It is on this point that Satoshi Nakamoto has been underestimated. The blockchain without pursuit of decentralization is nothing but a fake one.

Underestimating Satoshi Nakamoto is about undermining our resolve to change the world.

Over the past 30 thousand years or beyond, human beings have tamed a great deal of animals for various purposes, but ironically, only to find that it is ourselves who have been tamed the most.

In 1997, Michel Foucault published his book entitled Discipline and Punish, which gave a detailed description of the nature of power throughout human history and its evolution from "torture" in the feudal society to "wild manners" in the Enlightenment. It has been replaced by comprehensive discipline when entering into the Modern society. Ubiquitous is this disciplinary technology taking advantage of "layered oversight" and "inspection" and deeply embodied in "Panopticon prison", an idea invoked by Jeremy Bentham. The architecture consists of a circular structure with an inspection house at its center, windows equipped; its perimeter is divided into cells of equal size with a window on one side opposite to the inspection house and a window on the other letting light through; because of backlighting, the watchman can follow closely to the activities of psychiatrics, patients and criminals in the cells while they themselves cannot tell if they are been observed or not. Here is an embodiment of Jeremy Bentham's principle: "Power should be visible but in the meantime, untouchable." From Foucault's perspective, the modern society is a disciplinary one scattered around by "Panopticon prison" as such. Of this mechanism, individuals are tamed and taught from body, behavior to subjectivity.

Meanwhile, however, human history itself is also against power. In the end, aristocracy and torture have been rendered history in the majority of regions the world over. Likewise, taming is always accompanied by uprising.

Nowadays has witnessed the emergence of new technologies, such as mobile Internet, big data, virtual reality, artificial intelligence and ergonomics. It therefore seems that individuals have been tamed and defined to a greater extent. True as is it, that doesn't necessarily mean there is no probability of resistance. In fact, human beings have been changing this world not only on its productivity, but shall on its relation of production.

The blockchain, best evidence of the afore-mentioned statement, would be making a breakthrough in addressing the interference of hierarchical power with individuals and evasion of privacy by "inspection", which shall ultimately surmount the "ever so hierarchical pyramid" of traditional world. Human beings, in return, become brand new "nomads" and take actions based on their needs. Similar ideas have long been elaborated on in the white paper by Satoshi Nakamoto.

So blockchain as such, Satoshi Nakamoto as such, how on earth can they be underestimated?

Science Interpretation

En-Tan-Mo

“

AGREED VALUE SHARED BENEFIT

”

Information, Entropy and Equilibrium: a mathematical physics perspective of blockchain (Section I)

This paper contains a series of analysis and interpretations on blockchain-based distributed system, given from the perspective of statistical mechanics, probability theory and data analysis, information theory and optimization and rational expectation. We say this paper adopts a perspective of mathematical physics, for the reason that our core model is constructed based on ideas such as entropy, equilibrium and optimization and that multiple mathematical tools are used to support our arguments. Our purpose is to provide a solution through the analysis on traditional blockchains (notebly Bitcoin).

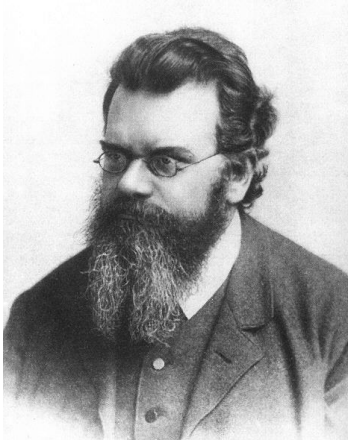
Blockchain is founded on two seemingly contradicting ideas---decentralization and consensus. To bring them to life, we need to make mechanism designs using the idea of game theory. Therefore, the first section of this paper will mainly focus on how entropy can serve as a gauge for decentralization and security and how we can use it as a tool to study them.

1. Entropy: measure of decentralization

In statistical mechanics, entropy is defined as: $S = K \log W$,from which Boltzmann obtains H-functional,

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

where $f(t,x,v)$ represents the probability density function of a microscopic particle. x and v are the position and velocity of the particle at time t respectively. For a rarefied gas with particle probability distribution $f(t,x,v)$, $S(f)$ is the entropy.



Ludwig Von Boltzmann (Austrian Physicist)

Entropy is a physical quantity that measures disorder in the system. Based on the formula above, Boltzmann derived the famous H-theorem, in which he proved that the continued collision between particles causes the system's entropy to increase over time until it reaches an equilibrium. The theorem can be expressed as follows:

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

Boltzmann's conclusion corresponds to the second law of thermodynamics (the total entropy of a system increases as time elapses and the process is irrreverisble).

When Claude Shannon ①proposed information theory, he used entropy as a gauge of how much information is produced, or of the amount of uncertainty.

Suppose there is a probability distribution function,

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

If the probability distribution of random variables $(x_1, x_2, ..., x_n)$ is discrete and $P(X = x_i) = p_i$,then we have

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

① Claude Elwood Shannon (April 30, 1916 – February 24, 2001) was an American mathematician, electrical engineer, and cryptographer known as "the father of information theory". Shannon is noted for having founded information theory with a landmark paper, A Mathematical Theory of Communication, that he published in 1948.

If there is a i that makes $P(X=x_i)=1$, then $S=0$ .Thus, we can infer that uniform distribution produces the maximal entropy, i.e. for any i, $P(X=x_i)=\frac{1}{n}$.

Let's consider, for instance, the diffusion of molecules without heat source in a given region. $f(t,x,v)$ represents the probability distribution of molecules. Assuming that molecule movements subject to Brownian motion①, then $f(t,x,v)$ should satisfy heat function,

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

We can give a simple proof for the equilibrium state of molecule distribution (corresponds to heat distribution). Taking derivative of Boltzmann entropy with respect to time, we can obtain the famous Fisher information,

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

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

It is said that Shannon asked Von Neumann what he should call his measure of information or uncertainty and Von Neumann② suggested entropy, saying "You should call it entropy for two reasons: first because that is what the formula is in statistical mechanics but second and more important, as nobody knows what entropy is, whenever you use the term you will always be at an advantage."

In thermodynamics, Boltzmann-Gibbs③ distribution is the distribution that maximizes the entropy, provided that momentum and energy are conserved. It corresponds to systems in thermal equilibrium. For such systems, there exists a probability distribution, in which case the entropy ceases to increase.

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

As a measure of uncertainty, entropy is also applied to modern mathematics to prove the classic central limit theorem in probability theory

Suppose $X_1,X_2,...,X_n,...$ is a sequence of independent and identically distributed random variables, whose mean and variance satisfy $\mathbb{E}[X_n]=0,\mathbb{D}[X_n]<\infty$, then as $N\to\infty$, $\frac{\sum_{n=1}^{N}X_n}{\sqrt{N}}$ converges to a random variable that follows Gaussian distribution.

Claude Shannon (the Father of Information Theory)

Sir Francis Galton, an English statistician, lauded the central limit theorem in this way (perhaps the same description can also be applied to the mathematical thoughts underpinning cryptocurrency),

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

---

① Brownian motion is the random motion of particles suspended in a fluid (a liquid or a gas) resulting from their collision with the fast-moving molecules in the fluid. This motion is named after the botanist Robert Brown, who was the most eminent microscopist of his time. In 1827, while looking through a microscope at pollen of the plant Clarkia pulchella immersed in water, the triangular shaped pollen burst at the corners, emitting particles which he noted jiggled around in the water in random fashion.

② John Von Neumann (December 28, 1903 – February 8, 1957) was a Hungarian-American mathematician, physicist, computer scientist, and polymath. Von Neumann was generally regarded as the foremost mathematician of his time[2] and said to be "the last representative of the great mathematicians He made major contributions to a number of fields, including mathematics, physics, economics, computing and statistics.

③ Boltzmann distribution (also called Gibbs distribution) is a probability distribution or probability measure that gives the probability that a system will be in a certain state as a function of that state's energy and the temperature of the system. It is also a frequency distribution of particles in a system.

most beautiful form of regularity proves to have been latent all along."

In 2004, Artstein-Ball-Barthe-Naor proved that information decreases (or uncertainty rises) as the number of random variables increases. That is, $Ent\left(\frac{\sum_{n=1}^{N} X_n}{\sqrt{N}}\right)$ is an increasing function of N. Plus, a proof can be given easily on Gaussian distribution being the distribution with the largest entropy under variance and mean restrictions.

SOLUTION OF SHANNON'S PROBLEM ON THE MONOTONICITY OF ENTROPY

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

1. INTRODUCTION

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

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

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

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

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

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

Unlike the early cumbersome works that make use of Fourier transform in the 20th century, these new implementations of information theory give a completely intuitive proof of central limit theorem. Not only do they fully demonstrate why central limit theorem is at the heart of thermal dynamics and information theory, but they explain the relation between Gaussian distribution and thermal equilibrium.

In his theory kinetic mean field games, Pierre Degond, an econophysicist, uses the equilibrium of thermal dynamics and Gibbs distribution to describe the Nash equilibrium in certain financial models.

From the above, we know that entropy can be seen as a gauge of how decentralized is a large-scale network system. Suppose $(x_1, x_2, ..., x_n)$ are a sequence of nodes and their respective computing power or stake is denoted by $P(X = x_i) = p_i$, then the larger $S = -\sum_{i=1}^{n} p_i \log p_i$ gets, the more decentralized the system and the less predictable the next producer. As such, we can use S to measure equilibrium and security of a system. Besides, S increases with n. It follows that when nodes increase a decentralized system will automatically become safer and more stable, as opposed to a centralized one that requires expensive maintenance and is vulnerable to attacks.

As a matter of fact, the theoretical foundation of Satoshi Nakamoto's mathematical model lies in the idea that computing power is, by and large, evenly distributed within the network. This is how Satoshi ensures that the next block producer (i.e. the node who first computes the hash result) are the least predictable. Plus, his assumption that block sequence subjects to homogeneous Poisson distribution holds true only when there is a relatively stable distribution of computing power. We know that the more unpredictable the block producer gets, the more secure the Bitcoin network becomes. Thus, Bitcoin's security is not depends on how much computing effort a node invests, but on the entropy of computing power distribution. A stroke of genius, truly. With this design, Satoshi is able to bring about decentralization and security simultaneously for Bitcoin, provided that the network has the maximal entropy.

As nodes grow, stakes flow and information disclosed and shared, the system's computing power and stakes would tend toward equilibrium and stability in terms of distribution and speed of motion. That is, they come to follow Gibbs distribution. This is how wise mechanism design ensures decentralization and security.

Relative entropy (also called Kullback-Leibler divergence) is another important concept concerning entropy in Shannon's information theory. Assume μ and ν are two probability distribution defined on the same probability space and f is the Radon-Nikodym derivative of μ with respect to ν, i.e. $f = \frac{d\mu}{dt}$, then

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

We can prove that $H(\mu|\nu) \geq 0$. If and only if $\mu = \nu$, $H(\mu|\nu) = 0$ .However, $H(\mu|\nu) \neq H(\nu|\mu)$,meaning they are asymmetric. Kullback-Leibler divergence is a measure of divergence from one probability distribution to another, with extensive applications such as data analysis and machine learning.

To put this in the context of blockchain, we can infer that the network is more likely to fork and that stability erodes when the distribution of computing power and stakes deviates from equilibrium, or in mathematical terms, when the Kullback-Leibler divergence of true distribution with respect to Gibbs distribution increases. Using entropy and Kullback-Leibler divergence as our mathematical tools for analysis, we may be able to answer the following questions,

First, will a price drop hurt the stability of cryptocurrencies (in particular, Bitcoin and other PoW-based systems)?

Second, is Bitcoin no longer safe because of the concentration of computing power (or will that be the case when more than 51% of the network's computing power is controlled by a few oligarchies?)

Satoshi Nakamoto never attempted to prove Bitcoin's absolute security, nor can he do so. Because absolute security is, in itself, something that does not exist. What he tries to do is to prove that the probability of a group of malicious actors catching up with the honest chain is so small that it is almost negligible. Thus he builds a model based on classic probability and random analysis methods with 51% attack being one of its basic assumptions.

Even if the 51% assumption falls through, it doesn't necessarily entail a breach of network security. It only means that Satoshi's mathematical model no longer fits the reality and that attackers get a better chance at outpacing the honest nodes.

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

p = probability an honest node finds the next block

q = probability the attacker finds the next block

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

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

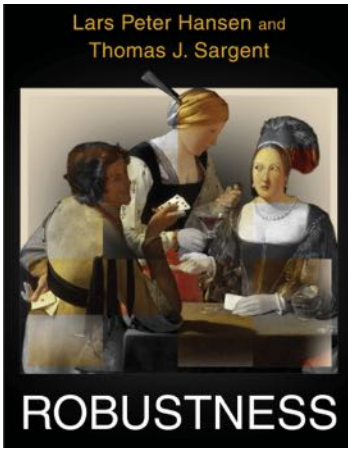
("Bitcoin: A Peer-to-Peer Electronic Cash System ")

an excerpt from *Bitcoin: A Peer-to-Peer Electronic Cash System* by Satoshi Nakamoto

The origin of the 51% assumption, where $p > q$ implies the honest nodes control more computing power than the group of attackers.

Therefore, efforts to defend blockchain security have to shift focus from warding off the 51% attack. More thoughts should to be given to the construction of a new set of mathematical methods for quantitative analysis featuring the Kullback-Leibler divergence from the true distribution of computing power and stakes to the equilibrium distribution.

Kullback-Leibler divergence was also applied to problems of the financial sector, mostly by Lars Peter Hansen and Thomas J. Sargent, Nobel-Prize winning economists and leaders of the rational expections school. Together the two scholars wrote a book entitled *Robustness*, in which they introduced "model misspecification" by incorporating the ideas of entropy, Kullback-Leibler divergence and control theory in the analysis for economic and financial model.



Robustness
by Lars Peter Hansen and Thomas J. Sargent

The core ideas of rational expectation theory include,

1. Economic model is the combination of probability distribution model and stochastic process.

2. Individual economic behavior is affected not only by objective factors (such as market change and real-time price), but, to a large extent, by their forcasts of the future (say, future trend of price change).

3. Through probability and stochastic methods,

we can use and analyze this expectations as parameters for the model.

After the outbreak of the financial crisis in 2008, mathematical economics, also known as econometrics, came under fire. Some critics believed that it was the sophisticated financial derivative model it developed that eventually led to the crash, while others pointed out that in addition to its seemingly complex mathematical deduction, econometrics was based on a set of assumptions that neither easy to verify nor as rigorous as those of physics. Against this backdrop, the Science magazine published a series of articles, in which pointed criticism were made against economics and financial mathematical instruments for their failure in the real world, calling for a scientific revolution on economics. Despite rising skepticism, Professor Thomas Sargent remains true to his faith in mathematical economics and at the same time, presents fresh ideas. In his view, mathematical models hold the key to the basic laws behind economic activities. He once observed, The fundamental problem with the mathematical model of modern finance lies in its assumption that people are completely rational and always make choices that best serve their interest. That is not true, obviously. An advanced mathematical model of finance should be able to simulate people's irrational behaviors and misjudgments in real-world circumstances. This requires the model to be grounded in a rigorous mathematical basis. Therefore, I use Kullback-Leibler divergence to measure such irrationalities.

Robustness, co-authored by Thomas Sargent and Lars Hanson, cites the following remark from Andre Gide, a French author,

"Croyez ceux qui cherchent la vérité, doutez de ceux qui la trouvent.

The earliest discussion on model misspecification can be traced back to the debate between Socrates and Thrasymachus,

"But are rulers of states absolutely infallible, or are they sometimes liable to err ?

To be sure, they are liable to err.

Then in making laws they sometimes make them rightly and sometimes not ?

True.

When they make them rightly, they make them agreeable to their interest ; when they are mistaken, contrary to their interest ; you admit that ?

Yes. "

2. Entropy and Black Swan Theory

Events of small possibilities (also known as accidental events) have a massive role to play in the financial market. Take insurance companies as an example. The probability of occurrence of large-loss claims is a big focus when insurers build mathematical model for their business. Because even though in most cases they remain highly profitable, an unpredicted major claim would immediately drive them to the brink of bankruptcy, as evidenced by the bailout of AIG and the collapse of Lehman Brothers during the 2008 financial crisis.

Similarly, although it is highly unlikely for the same node (or a small group of collaborating attackers) to add consecutive blocks to the chain, such extreme outliers, if take place, would cause devastating consequences (a tampered ledger, for instance), ruining blockchain's security and its reputation.

This kind of rare events with major effect is called the black swan events.

The black swan theory brings us to another important work of mathematics in this aspect—large deviation theory, stemmed from the studies on the ruin and actuarial mathematics of insurers by Harald Cramer, a Swedish mathematician.

The core idea of large deviation theory, known as Sanov theorem, was first developed in 1957. In the following paragraphs, we will give an intuitive description of Sanov theorem.

Let $X_1, X_2, ..., X_n$ be a set of independent and identically distributed random variables. μ denotes probability measure. $x_1, x_2, ..., x_n$ represent the values of empirical random variables. Thus, empirical distribution is given as

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

Then, probability

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

From the law of large numbers and central limit theorem, we know that empirical distribution will converge to μ with the increase of N. If v denote the probability distribution of an event such as a

successful cheat, then the probability of occurrence of such event will depend on $S(\nu|\mu)$, namely the Kullback-Leibler divergence from ν to μ. For a random event, the larger the discrepancy between probability distribution and equilibrium distribution, the less likely the occurence.

О вероятности больших отклонений случайных величин

И. Н. Санов (Москва)

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

The Probabilistic Definition of Entropy
by Sanov based on the large deviation theory

So far, little is known about the personal life of Sanov. When Sanov died in 1969, an article was published in his honor, but it only included a brief review of his mathematical achievements. Thanks to the database in memory of the Great Patriotic War, we manage to get a glimpse of the life of the Soviet mathematician. It was not long after Sanov got his doctoral degree in Moscow in 1940 that he joined the second world war. As an engineer, he helped artillerymen with the calibration of ballistic trajectory by taking advantage of his expertise in the realm of probability. He had fought in the Battle of Moscow, the Siege of Budapest, the Balkan's liberation from Nazi Germany and the Battle of Berlin and was thus awarded the Order of Red Star and the Order of Berlin Liberation for his service. During the Korean War, he served as one of the Soviet advisors in North Korea where he led the organization and founding of the department of mathematical science of Kim Il-sung University. The large deviation theory became a major theme in Sanov's studies after he returned back to Moscow. At the same time, he conducted several military researches with the Soviet national security organs.

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

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

Из теоремы 13 следует, что

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

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

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

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

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

(Поступило в редакцию 24/11 1956 г.)

The Probabilistic Definition of Entropy
by Sanov based on the large deviation theory

As a member of the school of probability theory in Soviet Union, Sanov concentrated his studies mainly on promoting the central limit theorem and Boltzmann's work in statistical mechanics was never mentioned. Interestingly enough, his definition of relative entropy or Kullback-Leibler divergence, derived from the description of events with small probabilities, completely coincides with those of Boltzmann and Shannon. Moreover, Sanov's work enjoys wide-range application in modern finance, such as the construction of Wall street's financial models, just like another Soviet mathematician Kantorovich who proposed the optimal transport problem.

In his book *In the First Circle*, Russian novelist Aleksandr Solzhenitsyn wrote a story about a rogue Soviet diplomat who made an anonymous call to the US embassy in Moscow, warning them of a nuclear espionage. To investigate this affair, Stalin ordered Abakumov, head of KGB, to assemble a group of arrested mathematicians to trace the source of this phone call by using the methods of Fourier analysis and information theory.

When information theory was introduced in the 1940s, a new theory gained traction. That is, the game theory and Nash equilibrium. What is the game theory? In what way does Nash equilibrium link with thermal equilibrium? How will these theories and ideas contribute to our understanding of distributed systems and more importantly, to our effort to build a new and better structure for blockchain? Now, let's move on to section 2.

Information, Entropy and Equilibrium: a mathematical physics perspective of blockchain (Section II)

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

Blockchain is founded on two seemingly contradicting ideas---decentralization and consensus. To bring them to life, we need to make mechanism designs using the idea of game theory. In the previous section, we discuss how to use Boltzmann entropy as a measure of decentralization and security of blockchain system. The focus of this section is the how does equilibrium come into existence in distributed systems and why.

1. Mean Field and Mckean-Vlasov Model

When we consider blockchain as a distributed network formed by a lot of nodes, here comes the following questions: how does information disseminate across the network? In what ways do nodes interact and synchronize with one another? How do we guarantee that all nodes would keep working on the longest chain? And in terms of mechanism design, what can we do to make the network robust against attacks? To answer them, we need to revamp the blockchain model with the help of physical and mathematical tools.

The concept of propagation of chaos, first conceived by Kac, an American statistician, was later expanded a full-fledged theory, with extensive applications in the fields of physics, mathematics and economics, thanks to the work of the French mathematician Alain-Sol Sznitman. The early drive behind their efforts was to put in place a unified theory that covered different kinetic equations by developing a set of rigorous formulas for particle motion. On the one hand, there was Liouville's equation,

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

where $u(t, x_1, v_1, ..., x_N, v_N)$ represents the joint probability density function of N symmetric particles.

On the other, Boltzmann's equation for rarified gas was given as,

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

where n denotes direction. Velocity $\bar{v}$ $\bar{v}'$ and v v' satisfy the following conditions,

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

$u(t, x, v)$ is the probability density function at position x and velocity v in time t.

Propagation of chaos implies when particles are symmetric and $N \to \infty$, we can regard any k particles as being independent from each other.

In 1991, Sznitman proposed a famous theorem, the conclusion of which can be simplified as

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

In layman's terms, the theorem shows although the random motion of individual particle is obviously not independent from each other (as a result of particle collisions and momenta), the global probability distribution of these particles combined can be regarded as a mean field when they are symmetric and in large numbers. In this case, we can directly study the impact of the global probability distribution on a single particle without considering the interactions between any limited number of particles. This can be illustrated with the McKean-Vlasov model. The kinetic behaviors of the particle system can be described by a system of ordinary differential equations

based on Newtonian mechanics as,

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

where W_t represents Weiner measure, $X_t^{i,N}$ is the position of i from N symmetric particles in time t and b denotes interactions between particles.

In the above system of equations, the interactions between particles $\sum_{j=1}^{N} b(X_t^{i,N}, X_t^{j,N})$ is obviously very complicated, given that all the forces from other particles on i need to be taken into account. But with propagation of chaos, a model of mean field can be built. Due to the symmetry of particles, we can choose an arbitrary particle and describe its kinetic behavior as,

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

where $u_t(dy)$ is the probability measure of X_t and the initial value of X_t is given by $X_{t=0} = X_0$.

u follows the Fokker-Planck equation,

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

The force acted on each individual particle can be seen as a "field". It depends on the probability distribution of the system and evolves over time. And the Fokker-Planck equation describing the evolution can be derived from the kinetic behaviors of a single particle. Therefore, propagation of chaos represents an important tool to explain the relations between the laws of the microscopic world and thoses of the macroscopic world. From the mechanical model of a individual particle, we are able to deduce equations including the Boltzmann equation① at macroscopic level and the Navier-Stokes equation of fluid mechanics. In mean field game theory, the distribution derived from Mckean-Vlasov Fokker-Planck② equation corresponds to Pareto optimality③ in economics.

From the above we know that the individual's kinetic behaviors imply the laws governing the evolution of the system as a whole, as expressed in the favorite poem of the late physicist Professor Zhang Shoucheng,

To see a world in a grain of sand,

And a heaven in a wild flower,

Hold infinity in the palm of your hand,

And eternity in an hour.

—William Blake - Auguries of Innocence

Similar thoughts are also embodied in the Buddhist classics,

To see the world in a grain of sand,

And a leaf in a bodhi.

2. Mean Field Game Theory and Rational Expectation

One of the key questions in physics is how do the stochastic motion and interaction of a large number of microscopic particles come to spontaneously follow macroscopic laws. This corresponds to another question in economics. How do complex interactions between agents (rational men) shape the price mechanism? To give a mathematical answer to these questions, some

---

① The Boltzmann equation or Boltzmann transport equation (BTE) describes the statistical behaviour of a thermodynamic system not in a state of equilibrium, devised by Ludwig Boltzmann in 1872.[2] The classic example of such a system is a fluid with temperature gradients in space causing heat to flow from hotter regions to colder ones, by the random but biased transport of the particles making up that fluid. In the modern literature the term Boltzmann equation is often used in a more general sense, referring to any kinetic equation that describes the change of a macroscopic quantity in a thermodynamic system, such as energy, charge or particle number.

② In statistical mechanics, the Fokker–Planck equation is a partial differential equation that describes the time evolution of the probability density function of the velocity of a particle under the influence of drag forces and random forces, as in Brownian motion. The equation can be generalized to other observables as well. It is named after the two Netherlands physicists, Adriaan Fokker and Max Planck.

③ 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 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. It is an economic concept with extensive application in game theory, engineering and social science. Closely related to it is Pareto improvement , which is a change to a different allocation that makes at least one individual or preference criterion better off without making any other individual or preference criterion worse off, given a certain initial allocation of goods among a set of individuals. An allocation is defined as "Pareto efficient" or "Pareto optimal" when no further Pareto improvements can be made, in which case we are assumed to have reached Pareto optimality.

French mathematicians and economists introduced the mean field game theory.

The basic principles and applications of mean field game theory can be illustrated by a simplified blockchain mining model. Suppose there are N miners with identical behavior pattern working on a pure PoW blockchain. These miners vie to find the next block by performing hash computation and whoever wins receives a coin (token) as reward. Let the hash power invested by the miner i be c_i and $c_i \in A$. i strives to maximize his payoff from the mining effort and his payoff depends on the mining cost of both he himself and other players as well. Therefore, the rational strategy is described as,

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

As we know, the payoff function of an individual miner is an increasing function of his computing power. At the same time, the function depends on how much hash power other miners invest also. Because blockchain's underlying algorithm makes it harder for individual miner to get payoff when there is increasing amount of computing power within the network. Thus, a miner's payoff is closely related to his payout, namely how much resource that mining consumes.

Assume each miner does his own payoff and payout calculations and adjusts his investment of computing power accordingly, then the network is in Nash equilibrium. Such equilibrium corresponds to a strategy combination that for any $i \in \{1, \cdots, N\}$

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

Or

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

where c_{-i} is the strategy combination of all players in the game other than i.

Payoff function J^i can also be given by a simplified model. In the Bitcoin whitepaper, Satoshi proved that given the probability of an individual miner finding the next block follows Markov property (as the time needed to generate the next block depends on the investment of the hash power of miner i himself and other miners in the network, not on the preceding blocks), the probability of mining N blocks within time $[0,T]$ is subject to Poisson distribution,

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

Intensity

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

where $c_i(t)$ denotes the computing power devoted by i in time t. $c_{-1}(t)$ is the computing power of all miners except i in time t.According to Poisson process, the mean of the expected blocks mined by i in this time slot is expressed as,

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

If we assume p and κ are constant, then the expected payoff of i can be written as,

$$E[J^i(0,T]] = p\kappa\Lambda(0,T) - \int_0^T c_i(t)dt$$

where p is the value of a coin (token) and κ is the number of coins (tokens) given to the miner for generating a new block.

We can also build a more complex model based on the one above, using the stochastic differential equation of a jump-diffusion process to simulate the change of coin (token) value.

However, the Nash equilibrium strategy remains sophisticated and computationally intractable, even for the simplified model. The complexity arises from the fact that the objective function J^i of any player i has to take the probability distribution of other players' strategy into account, i.e. $\Lambda(0,T)$ depends on $\sum_{1 \le j \ne i \le N} \delta_{c_j}$ As such, we might as well consider this Nash equilibrium problem from the perspective of the aforementioned mean field equilibrium and propagation of chaos. For every player i,the hash power devoted by any another player j (or strategy) has negligible effect on J^i. Players, except for i,affect the difficulty of mining and individual payoff as a whole in the form of probability distribution. Therefore, for any limited number of players, their respective probability distribution of strategy can be regarded as independent from one another. In this case, we know from the law of large numbers that when $N \to +\infty$, probability distribution $\sum_{1 \le j \ne i \le N} \delta_{c_j}$ converges in probability (or weakly converge) to a probability measure μ.The Nash equilibrium strategy in question converts to,

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

When $N \to +\infty$, Nash equilibrium is no longer a discrete strategy combination, but the probability distribution of strategy combination μ that satisfies,

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

where $supp(\hat{\mu})$ is the support set of measure $\hat{\mu}$ .Nash

equilibrium can also be expressed as,

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

where $\rho(A)$ is the probability measure space defined on set A.

Thus, the problem of Nash equilibrium in game theory is transformed to the problem of fix point in probability measure space: given μ is the probability distribution of strategy (the input of mining effort) and from $\sup_{c\in A} J(c,\mu)$ we derive the probability distribution of $\hat{c}$ as μ', then we have the mapping

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

If fixed point $\hat{\mu} = \Phi(\hat{\mu})$ exists in the above mapping, then we obtain Nash equilibrium $\hat{\mu}$. Based on this, we can infer the cost-payoff distribution of a player in pursuit of his maximal interests and then predict the a token's reference value and cost.

Ever since its introduction, mean field game theory has attracted attentions from mainstream economics, in particular rational expectation. It is believed that this theory will facilitate the development of economics in a disruptive fashion, for the following two reasons,

First, there is two kind of economic equilibrium, namely equilibrium and general equilibrium. Equilibrium, for example Nash equilibrium, belongs to the realm of econometrics. It can be mathematically analyzed and calculated in a rigorous manner through a simple model. In contrast, general equilibrium is more of an idea of political economy that describes the relationship between market supply and demand as well as a state of economy. It has long been seen as one of the main ideas championed by free market economy, as evidenced by one of its basic assumption that the market is adjusted by price mechanism. However, it has yet to produce a rigorous mathematical model for price formation.

Second, economic computation is tricky. One of the fundamental assumption of rational expectation is when people make decisions, they use the information from economic model (probability distribution). And the model, in turn, is refined by the collection of individual decision-making. Given the sheer size of economic agents and the complex nature of their behaviors, calculation for such model is fairly difficult. However, we can make things much easier by using the mean field game model, in which the game is between one player and the "mean field" of other players, not between individual players.

3. What makes a Good Consensus

When asked about economic models, the Nobel Prize-winning economist Lars Hansen replied,

" People would say, 'Well, this is a very complicated problem, therefore it requires a complicated solution.' And at that step, I would say, 'Well, wait a minute. Just because it's a complicated problem doesn't mean the best course of action immediately is one that's complicated."

Bitcoin is one of the examples of a simple solution to a complicated problem. 2008 witnessed a boom in financial derivatives and related theories. While banks worldwide were preoccupied with developing ever more sophisticated system for safe transactions and trading, Satoshi Nakamoto, using a tool as simple as a probability model, ushered in a disruptive innovation—Bitcoin blockchain.

A good blockchain mechanism design should be the combination of simplicity and complicity. At the microscopic level, each node's payoff model and kinetic behaviors should be as simple and rigorous as Newton's laws of motion. While at the macroscopic level, the system should a reflection of sophistication, discipline and robustness. On the one hand, it ought to function in keeping with the law of large numbers, becoming more robust with the increase of nodes within. On the other hand, randomness (or the unpredictability of block producer) should serve to boost its stability.

As a distributed, open and verifiable ledger, blockchain, coupled with mean field game theory and rational expectation theory, holds vast promise in the financial market and the energy sector. To be more specific,

1. Blockchain helps to put in place a more equitable system by tackling the problem of asymmetric information in the financial market. On-chain information is equally accessible to all. This means no one in the network possesses more information for decision-making than the other. Besides, blockchain is able to deliver information transparency and individual privacy simultaneously. For every transaction, the parties involved are anonymous because of zero-knowledge proof

while the information of its size and liquidity are shared, verified and used across the network.

2. Blockchain provides participants with real-time and tamper-proof information so that middlemen are excluded from their decision-making. This helps to reduce the cost of transactions and makes economic system more efficient. The implementation of mean field game theory in the analysis of Nash equilibrium strategy will significantly reduce the difficulty in calculation and thus give rise to a new set of data analysis algorithms. An era for distributed, agent-based data processing is also on the horizon, enabled by faster data processing speed and the application of distributed computation methods.

3. Blockchain technology alleviates poverty and contributes to sustainable development. An increasing number of countries and regions are adopting distributed energy systems as they have shown potential in solving problems including energy shortage and environmental pollution. For example, in some remote areas where power facilities are underdeveloped, wind power and solar energy are harnessed by the distributed energy system to generate electricity. Currently, the major challenge confronting distributed energy is not a lack of know-how and equipment, but the absence of an effective system that links distributed service providers with their buyers. With blockchain technology, we can build a distributed energy ledger system in which participants are both buyers and sellers who timely adjust supply and demand based on price changes. In addition, participants can trade coins (tokens) as futures in order to offset risks posed by fluctuation in price and demand.

In today's world, the control of large banks and corporate giants over financial service is more than a monopoly, but a hegemony. The term "hegemony", first conceived by Italian philosopher Antonio Francesco Gramsci, refers to the fact that the ruling class enjoys supremacy over the underclass both in terms of the sheer amount of wealth and knowledge, thoughts and culture. A handful of banks on Wall Street dominate the supply of service and data, control industrial profits and turn financial mathematics into a metaphysics, something that needs to be worshiped and obeyed like the astronomy in Medieval monasteries. While elites from Wall Street possess the best resources in the world, the ordinary people are lost in the Plato's cave, unable to fathom the true laws and logics behind financial operations. What they are left with is a false fantasy created for them by the press under manipulation. And the situation will only go worse if nascent technologies, big data and artificial intelligence, among others, fall to the hands of the entitled, as the monopoly on technologies has already been held accountable for the widening gap between the rich and the poor in many countries. Blockchain, combined with big data, is a rebellion against the hegemony. By embracing openness and democracy of data and information, it will usher in a double Copernican revolution on economic system and economic science and a renaissance of finance and economics.

In this section, the focus of our discussion is decentralization and consensus. The last section will show how we intend to improve the mechanism design of blockchain with our theoretical tools.

References:

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

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

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

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

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

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

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

Information, Entropy and Equilibrium: a mathematical physics perspective of blockchain (Section III)

In the previous two sections, we elaborate on the logic behind blockchain's decentralization and its consensus mechanism, and present new methods for analysis from the mathematical physics angle. In this section, we are going to explain how do we embed the idea of equilibrium in the underlying algorithm by implementing mathematical physics in the mechanism design of En-Tan-Mo's consensus.

1. Election Strategy Based on Nash Equilibrium

The cornerstones of our algorithm design are game theory mechanism design and the idea of Nash equilibrium. Assume all players are rational, and the goal of mechanism design is to guarantee that the strategy that maximizes player's payoff is the one that leads to consensus so that players (nodes) are incentivized to follow consensus. To be more specific, assume the network has N nodes $x_1,...,x_i,...,x_N$, For node x_i , the probability of being elected in any time t is given as

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

where $S(x_i(t))$ denotes the stake of x_i in time t. $T_i\circ x_i(t)$ represents the stake monetone increasing fuction of t, which is determined by token lock-up period. k_i is the sucessful block generation ratio $\frac{n_i^*}{n_i}$ in time t. Real number $\epsilon\in(0,1)$.

We prove that for the node who wins the right to forge the next block, the dominant strategy is to produce a block within its time slot and make sure the block doesn't include fake transactions. We denote the node's strategy set by $Y=\{0,1\}$, where $\alpha_i=1$ represents the node producing a block that only contains true transactions. Otherwise $\alpha_i=0$, because a block with false information will be later rejected by other nodes in the network and deleted from the record of successful block generation.

Suppose t_k^i represents the κ th time x_i wins the right to sign a block, $k>1$ and in the previous $k-1$ th times x_i sucessfully chained $n_{i,k-1}^*$ valid block(s).

The node's payoff function should consider how many token(s) it can get from following a certain strategy and the impact of a successful block generation (rational expectation). Suppose

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

where r represents the reward for a successful block generation and $r>0$. c is a constant that measures the expected changes of token reward in the future. We need to analyze the strategy of x_i in time t_k^i .Based on consensus mechanism, we know that at time t_k^i, x_i is the only one with the right to forge a block. Therefore, when t_k^i becomes t_k^i+, $\sum_{j\neq i}^N(k_j+\epsilon)S(T_j\circ x_j(t))$ remains constant.

We are trying to obtain strategy α_i that satisfies

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

When $\alpha_i=0$,

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

When $\alpha_i=1$,

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

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

With respect to the equations above, we make the following explanation. If the strategy of x_i at time t_k^i is $\alpha_i=1$, then its stake increases to $S(T_i\circ x_i(t_k^i))+r$ while the stake of an arbitrary node x_j , $j\neq i$, remains constant. At this point, x_i has κ chance(s) in total to produce a block and he suceeds $n_{i,k-1}^*+1$ time(s).

Assume

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

then

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

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

$$=\frac{1}{1+\frac{c_1}{(\frac{n^*_{i,k-1}+1}{k}+\epsilon)(S(T_i\circ x_i(t^i_k))+r)}}$$

Obviously

$$(\frac{n^*_{i,k-1}+1}{k}+\epsilon)(S(T_i\circ x_i(t^i_k))+r)>(\frac{n^*_{i,k-1}+1}{k}+\epsilon)(S(T_i\circ x_i(t^i_k)))$$

and from $r>0$,we have

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

Thus, the dominant strategy of x_i in time is t^i_k , $\hat{\alpha}_i=1$.

As $T_i\circ$ is a monotone increasing function of time, electors can increase their vote proportion by extending lock-up period. Through this mechanism design, we prevent malicious actors from gaining an unfair advantage in the election by aquiring a large proportion of stake in a short span of time.

2. Analysis on the Security Mechanism Based on Large Deviation Theory

This part will focus on the mathematic analysis of network security after each round of election. From the principle of network security and reliability analysis, we assume the extreme worst-case scenario. That is, 49% of candidates for block generator have the intention to launch a coordinated attack.

Based on probability calculation, we obtain that in this round the number of candidates chosen as block producers roughly equals to

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

This means some block producers will generate more than one block. In fact, for each block producer, the number of times of being chosen follows Poisson distribution, (because according to Poisson theorem, binomial distribution approaches Poisson distribution.) with a mean that equals to 1 .

Assume attackers collaborate. They only add blocks following one of them and neglect the blocks produced by honest generators. This means the attackers want to mine a fork to overtake the honest chain at some point as the longest chain and deceive newly joined nodes into believing their chain as the valid chain. We can use the law of large numbers and large deviation theory to prove the possibility of a successful attack is negligible.

$$P(X_i=1)=0.49, P(X_i=0)=0.51$$

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

From the strong law of large numbers, we know when $N\to\infty$, $\frac{1}{N}\sum_{i=1}^{N}X_i$ converges to its mean. Now we consider the possibility of attackers mining over a half of the 101 newly chained blocks (i.e. the attacker chain grows longer than the honest chain).

According to Cramer's Rule, we can obtain the following equation approximately

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

Legendre transformation

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

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

3. Summary

En-Tan-Mo's Unified-Proof-of-Stake (UPoS) algorithm is a hybrid model that draws upon the respective merits of Proof-of-Work and Proof-of-Stake and strives to keep and cherish Bitcoin's founding ideas. To better understand it, we'd first like to make a brief analysis on Bitcoin. It is our view that Bitcoin's security is based on the inherent randomness of a distributed network. Here randomness refers to the unpredictability with respect to the next block generator. (All nodes are involved in the solving of the mathematical puzzle, whoever gets the result first becomes the miner to sign the next block.) Besides, nodes have skin in the game because doing the proof-of-work consumes a lot of hash power which gives them all the more reason to defend the network's reputation and stability. As opposed to Bitcoin's Proof-of-Work, En-Tan-Mo's Unified-Proof-of-Stake has the following characteristics:

1. 101 nodes will be elected as producer candidates. The candidates produce blocks via hash computation and will be replaced through a re-election after each block is mined. The sequence of the block producer is randomly generated using the hash result calculated by the creator of the previous block. Under Unified-Proof-of-Stake (UPoS) algorithm, hash computation is no longer a competition between nodes, but a procedure to generate the necessary unpredictability for the mining sequence. This to a large extent eliminates the possibility of coordinated cheat and attacks.

2. Under Unified-Proof-of-Stake, mining is no longer a resource-intensive task, because hash

computation is modified for a new purpose. But the difficulty of the hash computation is tweaked on a dynamic basis as a way to adjust the mining cost. As such, nodes are motivated to defend the system and guard against Sybil attack. Plus, a UPoS-based system enjoys higher efficiency, with much faster TPS. Thus, it is in a good position to scale to diverse real-world applications.

3. In En-Tan-Mo, scaling means not only more potential but also stronger security and robustness. The more nodes participate, the less predictable the block generator and the more economically impractical the attack.

4. Stake is calculated via a convex function so that the distribution of stake will tend towards uniform distribution (the distribution with maximal entropy). In this way, we make sure that decentralization is embedded throughout the election process, prevent stake from centralizing in the hands of the powerful and encourage more extensive participation.

5. In the selection of the following producer, we will consider not only the size of stake held by each candidate, but also the duration of lock-up period and the record of successful block production. As such a more objective candidacy evaluation system is put in place by taking the candidates' contribution to the network into account, which tackles the problem of non-producing block generator and inspires nodes to follow the rules and reach consensus. Besides, keeping a record of nodes' past behaviors serves as a good countermeasure against Sybil attack. In a nutshell, we pursue an the-survival-of-the-fittest approach in order to inject robustness into the network.

6. With unique side-chain technology and magic cube protocol, En-Tan-Mo strives to address an importance challenge to side chain: the contradiction between independence and synchronization. On the one hand, side chain should be independent from the main chain because it is designed to divert traffic from the main chain. On the other hand, side chain should synchronize ledger with the main chain. As such, we devise a new transmission protocol under which ledger is synchronized without imposing too much pressure on the main chain. The benefits of this innovation in side chain technology are plenty: the efficiency of En-Tan-Mo network is greatly enhanced; side chain is capable of hosting a variety of Dapps. Efforts to develop a new algorithm is already under way and we intend to first implement it in side chain. With this new algorithm, we hope to achieve self-evolution and upgrading for En-Tan-Mo.

Unified-Proof-of-Stake (UPoS) is a consensus mechanism that delivers enhanced efficiency, stronger decentralization and better security simultaneously, thus putting an end to the trade-off between the three attributes. On top of it, we build En-Tan-Mo, a blockchain that is borne out of the core ideas of Bitcoin but better fits into the current economic and financial infrastructure. At the same time, we are aware that our endeavor to promote blockchain technology should not be restricted to theoretical research only. The full potential of the technology cannot be unlocked unless we put it into real-world test. Therefore, our team has run several beta and public test to debug our consensus algorithm and code. The En-Tan-Mo main net is going live, which will be a testament to our past success and mark a new beginning.

References:

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

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

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

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

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

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

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

Appendix:

Bitcoin's Ideas and Blockchain Revolution

This year marks the 10th anniversary of Bitcoin, the first cryptocurrency. Over the course of a decade, the crypto-market has witnessed a remarkable boom, as evidenced by the emergence of a myriad of blockchain projects, notably Ethereum and EOS, and by the increasing number of Dapps running on them. However, the previous year 2018 was a roller coaster ride for the market with price as well as reputation taking a nose-dive from the 2017 peak. Amid rising calls for a "back to Bitcoin" and "back to Satoshi", we want to first figure out what is Bitcoin really about.

Bitcoin, in our opinion, is underpinned by three tightly interrelated ideas: decentralization, robustness and a mathematical algorithm-based trust or consensus mechanism. Decentralization means the security of Bitcoin is made possible by all the participants through a computationally intensive mining process, given that hash power is generally even distributed across the network. Everyone has the right to verify the ledger and is rewarded on a fair basis. Decentralization also contributes to robustness, because a distributed network doesn't rely on a central server to deliver security, thus it is highly attack-resistant. As decentralization and robustness are achieved via mathematical algorithm, trust is established without men. Under Bitcoin's Proof-of-Work algorithm, nodes vie for the right to mint the next block. Proof-of-Work is a means to an end, not an end in itself.

But we can't afford to overlook the hard fact that Bitcoin and blockchain technology alike are buffeted by a serious crisis. The rise of big mining pools has led to a harmful concentration of hashing power, fueling an "arms race" between Bitcoin miners and adding to the possibility of fork. Heated discussions took place at the Satoshi Roundtable over the supply cap of Bitcoin. All of which are telling examples of Bitcoin gradually deviating from its founding principles. They indicate that Bitcoin is shifting away from mathematic algorithm to individual preference and interest distribution. When democracy and establishment fail people, they use referendums to make important decisions. The same is true of Bitcoin, as evidenced by its increasing reliance on community discussions.

In response to the crisis arisen from the development of cryptocurrency and blockchain technology, there has been increasing calls for a " back to Bitcoin", where advocates hope to present new solutions by making adjustment or supplement, such as zero-knowledge proof, to the original algorithm. The idea of " back to Bitcoin" is plausible based on two things, Bitcoin's decade-long success and a mathematically rigorous algorithm.

1. Bitcoin's algorithm has been working well for years but this doesn't mean it will remain so in the future, especially at a time when the vulnerabilities in its mechanism design are beginning to show. As the Greek philosopher Heraclitus once said, "no man ever steps in the same river twice." Today's Bitcoin is too faced with a new circumstances where computer hardware, mining technology and the public's attitude toward cryptocurrency are nothing like what they were 10 years ago. For instance, when Satoshi Nakamoto invented Bitcoin blockchain, he neither expect the massive influx of capital nor the rise of mining pools, the very things that are detrimental to Bitcoin's decentralization. Another thing Satoshi didn't anticipate is the huge electricity waste resulted from Bitcoin's increasingly insatiable demand for hash power.

2. Bitcoin is successful in terms of network security, while its performance in decentralization and efficiency (TPS) is much less satisfying, with ever more intensive energy consumption. Since large mining pools mint most of the new bitcoins nowadays, market volatility and manipulation become more likely.

3. Bitcoin is essentially founded on a mathematical model supported by economic judgements. One of the most prominent examples can be found in Section 6 "Incentive" of ***Bitcoin: A Peer-to-Peer Electronic Cash System***, in which Nakamoto wrote, "Once the predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free." However, the feasibility of such a model is under doubt and that's partly why there has been an increasing number of debates over a rise in Bitcoin's supply limit. Hard fork would be a rational and profitable choice when a mining pool gains the monopoly on the network's hash power as well as enough support from the crypto-community.

4. The reliability of a mathematical algorithm

depends on its foundations. Mathematics is a science of conditional accuracy, in which each theorem is established upon a specific set of preconditions and assumptions. These preconditions are not the product of mathematical deductions, but are borne out of scientific analysis and need to be constantly tested and verified by ever-changing real-life situations.

The collapse of LTCM (Long Term Capital Management) may be the best case to illustrate the point. Merton-Black-Scholes model, named after its developers Robert Merton and Myron Scholes, is a classical model of quantitative finance. Although the model helped LTCM team to make a handsome fortune in the first 4 years of its implementation, it failed miserably in the fifth, creating a vicious, bankrupting spiral of bad investment decisions and a sharp decline in assets. The fall of the fund giant caused an financial earthquake in the US. However, this didn't mean that Merton-Black-Scholes model was invalid. On the contrary, it was widely recognized as mathematically correct and rigorous.

But being rigorous in mathematical terms didn't make it a correct model in its own right. The problem with the Merton-Black-Scholes model was that the ways how market worked had changed over time so that some of its premises were no longer in consistent with the real-world situations. The forked Bitcoin has arrived at a similar point where the most fundamental assumption of Nakamoto's algorithm may be shattered by the emergence of giant mining pool that controls more than 49% of the network's hash power. As hash power centralizes, forks of Bitcoin increase and new blockchain projects emerge in large numbers, the odds of a 51% attack against a single blockchain network or fork increase drastically. This would render a complete failure of blockchain's security mechanism.

Therefore, the revolution in blockchain technology is not about tinkering with the Nakamoto's original algorithm, but about putting in place a distributed financial ecosystem using a new way of thinking. To quote the great philosopher, Karl Marx, in his famous book The Eighteenth Brumaire of Louis Napoleon, "Hegel remarks somewhere that all great world-historic facts and personages appear, so to speak, twice. He forgot to add: the first time as tragedy, the second time as farce," and "men make their own history, but they do not make it as they please; they do not make it under self-selected circumstances, but under circumstances existing already, given and transmitted from the past. The tradition of all dead generations weighs like a nightmare on the brains of the living. And just as they seem to be occupied with revolutionizing themselves and things, creating something that did not exist before, precisely in such epochs of revolutionary crisis they anxiously conjure up the spirits of the past to their service, borrowing from them names, battle slogans, and costumes in order to present this new scene in world history in time-honored disguise and borrowed language."

With a view to address the vulnerabilities of Bitcoin, Proof-of-Stake (PoS) was invented as an alternative consensus to Proof-of-Work (PoW). In PoS-based cryptocurrencies, the next block producer is chosen on a stake basis rather than on a hash power basis. The good thing is this algorithm does not involve the solving of a computationally intensive puzzle and enjoys greater efficiency (TPS). But the difficulty lies in how to select the nodes that can be trusted for the block validation. With respect to this, several different solutions have been conceived. One blockchain EOS entrusts a limited number of supernodes to handle transactions and sign blocks. This, of course, is more efficient, but clearly runs counter with the goal of decentralization. In this case the security of the whole network hinges on the trustworthiness of the supernodes entirely.

Another solution is the universal election adopted by blockchains such as Cardano and Algoran, among others. In these blockchains, the next generator is elected from stakeholders. Those who have more stakes have a greater chance of being elected. However, this solution is not free of problems either. One is that it's hard to guarantee the producer will forge a block within his time slot. Plus, as there is no requirement for hash power input in the election, cheat becomes more likely. Based on the analysis of the pros and cons of different algorithms, we En-Tan-Mo launch the Unified-Proof-of-Stake (UPoS), a new protocol that stems from the founding ideas of Bitcoin and maximizes the advantages of both Proof-of-Work and Proof-of-Stake. It is a combination of Bitcoin's heritage and disruptive innovation---a technical and algorithm revolution in the spirit of Bitcoin.

Technical interpretation

En-Tan-MO

“

AGREED VALUE SHARED BENEFIT

”

En-Tan-Mo Technology Interpretation Development

En-Tan-Mo is the choice for convenient DApp development

1. Get your apps ready for the new world

For app builders, the value of blockchain goes beyond the benefits of deploying a novel technology. It brings a change of mindset and an equitable platform for app development.

Today's app market is riddled with bad business practices. Technology behemoths monopolize profits. App transparency is lacking. Abuse of user permission runs rampant while personal data is sold and leveraged. However, things could change with blockchain-powered DApp, which enables users to make transactions in a safer, transparent and efficient manner, and opens up possibilities for new way of life in the internet age : taking your privacy back from the internet giants. Being transparent, open, reliable and decentralized, DApp addresses the major deficiencies of traditional apps, and is bound to give rise to a brand new business ecosystem.

A great technology should benefit all rather than some. However, this would be impossible without the hard work of developers. For this reason, En-Tan-Mo is committed to putting in place a sound and high-performance platform for app development; a platform that runs an open, thriving developer's community and self-evolving blockchain application components; and a platform that shatters the walls between finance, energy, business and people's daily lives and encourages free flows of value.

2. En-Tan-Mo enables developers to write and deploy Dapp easily.

Main Chain-Side Chain Mechanism

Each DApp runs on an exclusive side chain with full functionality so that it is independent from one another. DApp builders can take technologies from main chain and directly implement them on side chain, and customize token, transaction type, consensus, block parameter and other side chain parameters according to their needs. This helps to inject flexibility and diversity into DApp development.

Node.js

JavaScript is enabled in En-Tan-Mo. As one of the most commonly used scripting language, JavaScript support a great variety of third-party components and thus holds appeal to extensive developers and communities. As such En-Tan-Mo makes it prossible for developers, both as individuals and as aggregates, to get started right away and substantially reduces their workload.

High-performance

While ensuring security and decentralization, En-Tan-Mo's Unified-Proof-of-Stake (UPoS) algorithm greatly enhances the performance of main chain with TPS reaching 1000/s and the time needed to produce a new block being shortened to 3 seconds. Since side chains are independent from each other, En-Tan-Mo enjoys infinite potential to scale. With the increase of DApps, the network will be able to allow N*1000 transactions per second. Therefore, it is capable of running DApps that demand better user experience, such as game. In short, under Unified-Proof-of-Stake (UPoS), developers can give free rein to their imagination without worrying about scalability.

Modular Framework

The adoption of the main chain-side chain mechanism and Node.js makes DApp building on En-Tan-Mo easier and more flexible. Moreover, the well-developed SKD and API further lower the cost of development. Such a modular framework allows developers to focus only on their products and directly benefit from main chain and side chain upgrades without making adjustment accordingly.

Zero Development Cost

Mainstream currencies such as ETH and EOS

recently suffered from a loss of DApp builders as a result of unaffordable development and operation cost, and this has pushed their entire app ecosystem into a vicious cycle. En-Tan-Mo is aware that a prosperous app ecosystem and active development community are the most valuable assets and the very force driving the platform's sustainable development. Therefore, the idea of win-win cooperation is embedded in its mechanism design from the very beginning so as to prevent such situation from happening. En-Tan-Mo's side chain enables developers to allocate and mobilize on-chain resources on a dynamic basis while the network only charges a small amount of transaction fees for security concerns. And these fees will be re-distributed back to developers through community activities.

Secure and Reliable

En-Tan-Mo's Unified-Proof-of-Stake (UPoS) algorithm is a Nash equilibrium-based consensus mechanism that combines the merits of both Proof-of-Work and Delegated-Proof-of-Stake. Thus it delivers better security and efficiency as opposed to the computationally-intensive Proof-of-Work algorithm. En-Tan-Mo also introduces the chaotic shuffling mechanism as an effective way to guard against Sybil attack and coordinated attack, further improving the network's security. Moreover, development on any side chain won't undermine main chain and other side chains.

Scalability

A sound distributed system should enjoy good ability to scale. On En-Tan-Mo, developers can easily deploy applications, increase the size of nodes and allocate them according to the need of DApp.

Open-source

En-Tan-Mo is an open-source, transparent and secure network under the MIT license and our code can be checked on GitHub. In this way we encourage everyone to be part of the En-Tan-Mo community and contribute to its development.

3. A Platform where Your Ideas Become Reality

Empowered by En-Tan-Mo, JavaScript and frontier blockchain functionalities, developers are able to build first-of-a-kind DApps, turning their most creative ideas into reality.

Interpretations on Unified-Proof-of-Stake (UPoS)

1. Under UPoS scientists from En-Tan-Mo strike a balance between performance, security anddecentralization.

Consensus algorithm is at the heart of a blockchain-based network. And it is the very feature blockchains use to distinguish themselves from each other. Combining the Proof-of-Work and Delegated-Proof-of-Stake in an innovative fashion, En-Tan-Mo scientists launch Unified-Proof-of-Stake (UPoS), a consensus mechanism that delivers high-performance, security and decentralization simultaneously. A deeper understanding of the network's consensus algorithm empowers DApp builders to take full advantage of related features and provides good guidance for their development.

2. SHD Completeness

CAP theorem states that it is impossible for distributed systems to provide consistency, availability and partition tolerance simultaneously. Similarly, there exists in blockchain-based platforms a problem called SHD Completeness which implies that a trade-off has to be made among security, high-performance and decentralization. The failure to deliver SHD completeness has already become a serious impediment to blockchain development.

3. PoW: from consensus to division

Proof-of-Work (PoW) is a consensus algorithm implemented by a large number of blockchain system, notably Bitcoin. Under such algorithm, computers compete for the right to forge the next block through the solving of a computationally tractable puzzle and the process is called mining, Whoever wins will be incentivized with a newly minted coin(or token). However, mining consumes a massive amount of electricity and wears down hardware. And the chance of winning is proportional to how much hash power a computer controls, thus inevitably leading to a hash power build-up within the network.

PoW-based mining is a non-cooperative

game. Incentive and transaction fee go to the winner only while other computers who too put in a large amount of resources get nothing in return. Moreover, the design of traditional PoW algorithm and block size limit have always been a drag on the scalability for Bitcoin and Ethereum. As forks multiply, 51% becomes more like a imminent crisis rather than a distant threat. All of these make people start to wonder whether PoW-based blockchains are still as decentralized as intended.

From the above, it is fair to say that PoW is not a SHD-complete mechanism.

4. DPoS: decentralized in appearance, centralized in essence

DPoS, otherwise known as Delegated Proof of Stake, offers a new solution to network security. It works as follows: a panel of delegates will be elected based on certain mechanism, say the holding of stakes. And an odd number of block producers will be chosen from the elected delegatesvia a vote instead of all nodes across the network.

This protocol, by holding a vote among dozens to hundreds of delegatesat at most, allows the network to reach consensus in seconds. Consequently, it boosts efficiency and is implemented by EOS (which uses a few supernodes to create blocks) and Ethereum 2.0. However it falls short of decentralization, despite improvement on network performance, as larger stake holders are given overriding power over the network. It follows that DPoS systems are not essentially different from existing centralized ones.

5. UPoS: a hybrid PoW and DPoS model that breaks monopoly, ends decentralization and achieves SHD completeness

There is a long-standing pattern in human history that a new technological revolution will invariably bring about unfair advantage and hence disrupt the level playing field, as witnessed in areas as varied as agriculture, industrial sector and the internet. Blockchain is no exception. It is known that fairness brought by PoW has been severely undercut by the invention of super-efficient mining machines. DPoS only seems to expedite the process. Because under the consensus, in which a few larger stake holders are charged with enormous power, centralization or pyramid structure will come into existence at accelerating rate.

DPoS is more environmentally-friendly and efficient, compared with the resource-intensive PoW algorithm. It adds a new block within 10 seconds, as opposed to PoW's ten minutes. While PoW is often criticized for being too wasteful, it excels in security, for the reason that so far there hasn't been once 51% attack. According to our design, En-Tan-Mo only needs less than 3 seconds to find the next block. This means a transaction is confirmed much more swiftly.

Through weighing the two traditional consensus algorithms' advantages against their disadvantages, we devise a protocol called Unified-Proof-of-Stake as a way to achieve SHD completeness. To put it simply, it works as follows: first, we map the stakes of voters into votes via a concave function. Second, in each "round" we select the best 101 miners to be block producers. Third, block producers participate in a mining game (which is more economically practical and decentralized than that of Bitcoin). Last but not least, the next producer is securely chosen via chaotic shuffling.

UPoS algorithm is shown in flow chart 1..

6. Miners

Miners refer to a specific type of account that records history of transactions. They play a key role in En-Tan-Mo ecosystem through the initiation and verification of transactions. Though everyone can become miners, only 101 of whom will be elected as block producers.

7. Round

We call every 101 blocks a "round". In each round, there are 101 block producers, each has 3 seconds to find the next block and their sequence is determined by the chaotic reshuffling mechanism. If a block producer fails to generate a new block in the allotted time period, or creates a block that contains false transaction information, then the system would automatically enable the chaotic shuffling to find the next producer. Plus, every newly minted block requires the signatures of at least 68 miners and is broadcasted across the network.

8. Block Reward

In En-Tan-Mo, block producers are chosen from miners. If a block producer generate a valid block, then he will be rewarded for his work in the form of token.

Block reward amounts to 240 million tokens, accounting for 48% of En-Tan-Mo's total supply. These tokens will be distributed in six years with the each year's share declining steadily.

The shares of token distributed in the first six years are 12.13%, 10.11%, 8.09%, 8.09%, 6.07%, 3.51% respectively.

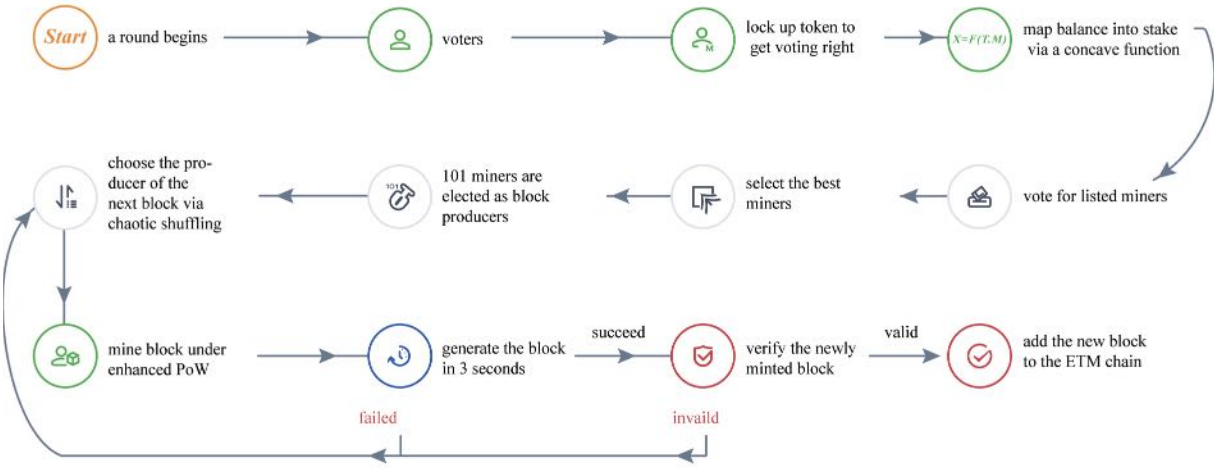
The timetable of block reward is shown in table 1.

9. Transaction Fees for Each Round

Apart from block reward, En-Tan-Mo incentivizes participants with transaction fees. The active participants of each round will be given a proportional share of transaction fees. (see more details in reward and bonus system)

Table 1 Timetable of Block Reward

Reward	Stage
6 ETM	Preliminary Stage, before 10，112，000 blocks
5 ETM	Stage 1，before 20，224，000 blocks
4 ETM	Stage 2，before 30，336，000 blocks
4 ETM	Stage 3，before 40，448，000 blocks
3 ETM	Stage 4，before 50，560，000 blocks
2 ETM	Stage 5，before 59，328，000 blocks



Flow Chart 1 UPoS Algorithm chart 1

From the Mass, For the Mass: interpretations of En-Tan-Mo voting, election and bonus system

Invented in 2008, Bitcoin has witnessed a sea change in the world over the course of a little more than a decade.

Never has a technology attracted so much attention like blockchain. Born with a close affinity with finance, it has been, unfortunately, exploited most for profit rather than for progress. The emergence of a large number of short-sighted blockchain projects represents a shift away from the technology focus. They derail the industry, and marginalize ordinary users. Mainstream currencies such as Ethereum and EOS become a game for the

few where the powerful acquire an unfair leverage and the ordinary are excluded from sharing the benefits. This not only leads to an unhealthy ecosystem, but also puts network security at risk.

Upholding the same visions as Satoshi Nakamoto's, En-Tan-Mo scientists believe that the build-up of hash power will not make blockchain network safer. It is the level of decentralization, i.e. hash power probability distribution, that plays a decisive role in the security of Bitcoin and other cryptocurrencies. This is evidenced by the fact that Bitcoin's security deteriorates with capital influx and the rise of mining monopolies.

1. The Strength of En-Tan-Mo Blockchain

In the view of En-Tan-Mo scientists, decentralization is not only a technical framework but more importantly, a new mechanism, a change in mindset and the common thread running throughout En-Tan-Mo's philosophical thoughts. In En-Tan-Mo, decentralization is brought to life by distributed system (framework), the people-centered voting, election and bonus system (politics) and the Unified-Proof-of-Stake consensus protocol (underlying logics).

Compared with traditional system, distributed system has three major strengths.

1. Fault Tolerance: In distributed systems, a partial glitch does not lead to a systematic breakdown, because the system is dependent upon many decentralized, independent components, all of which have a role to play in keeping it running. Therefore, such systems are more robust than others.

2. Robustness against Attack: It is prohibitively expensive to manipulate or attack distributed systems, because they don't have a central authority. Besides, due to their decentralized nature, distributed hardware and ecosystem are hard to be monitored and attacked simultaneously.

3. Resistance against Collusion: Collusion is somewhat hard to define. Traditionally, oligarchies collude to prey on the ordinary people. To end this practice, anti-trust law is adopted throughout the world. For distributed systems, the possibility of such collusion between malicious actors is significantly lowered. With a view to better address this problem, En-Tan-Mo implements the idea of Nash equilibrium to foster a more equitable ecosystem.

2. A People-centered Voting, Election and Bonus System

Blockchain is a new generation of technology borne out of the traditional infrasturacture. Yet a clear furrow needs to be ploughed between the old and the new if we are to pursue truly revolutionary progress. Clearly, a blockchain system that fails to deliver decentralization is inadequate and nothing more than a centralized system in disguise.

Alarmed by the harms of centralization, En-Tan-Mo realizes it is time to put in place a new infrastructure that redresses them. One of the key component of the effort is the people-centered voting, election and bonus system.

En-Tan-Mo Voting System

By implementing mathematical and philosophical theories into mechanism design, scientists from En-Tan-Mo devise a voting system in a bid to change traditional structure and to steer cryptocurrency back on track.

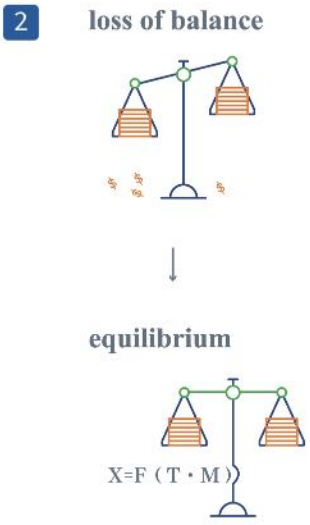
Users obtain voting right after the lock-up of a certain portion of ETM. Note that token balance doesn't equal voting stake (the number of votes). The coversion from balance to stake is governed by the function $X = u t \cdot T$ (where T is the balance locked up. t is time gain coefficient and u is the coefficient of stake constraints). To eliminate monopolies and guarantee network stability and security, En-Tan-Mo makes the following changes.

1. Time Gain Coefficient----increasing opportunities for private investors

More too often private investors get an unfair

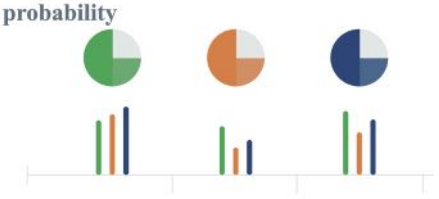
share of market profits. That's why En-Tan-Mo introduces the concept of time gain coefficient in a bid to deliver equality for small stake holders. Under such mechanism, stakes (votes) increase over time so that even users with small holdings are rewarded with considerable payoffs. Every 24 hours the time gain coefficient increases automatically. Therefore for small holders the probability of getting a bonus also improves over time and is halved when the block producer whom they vote for successfully adds a block to the chain.

2. Stake Constraints----lowering the weight of oligarchs



Oligarchs amass massive wealth, monopolize resources and create imbalances. All of these have severely dampened the enthusiasm of the ordinary users to participate and contribute. To prevent large stake holders from acquiring too much weight of the system, En-Tan-Mo maps balance to stake through a concave function rather than a linear function. This concave function is u, a coefficient used to restrict the stake of big holders. Through this design, large holders are unable to get superlinear reward, our ecosystem becomes more equitable and decentralization is further enhanced.

3. Uncertainty (probability)---making the impossible



The lack of mobility is the culprit of an anemia community. Hence En-Tan-Mo's makes sure that block producers are selected on a dynamic basis. To be more specific, block producers are chosen via a probabilistic draw among miners based on their share of votes, rather than from the top 101 high-performers. This otherwise can be written as $P = X / \sum Xn$. The result is that miners who rank below the 101th place may make it to producers also. Through this mechanism design, En-Tan-Mo introduces uncertainty into the election outcome so that miners who used to stand no chance now have a possibility of being elected.

As such hash power is in general evenly distributed among users and monopoly is kept in check. As long as the ordinary majority controls 50% of stakes(votes), they would have 50% say in the system. Thus, decentralization is secured and security is boosted.

Lock-up

Unlike bond market, En-Tan-Mo only use "lock up" in a literal sense. For every system, it is essential to have liquidity. However, a degree of stationarity is also needed in case of unexpected shocks. Thus En-Tan-Mo requires users to lock up a certain amount of ETM tokens in exchange for stakes (votes) and they can use these votes to decide who will be the block producer. The lock-up is the prerequisite of becoming a voter. The sum being locked is still kept in users' personal accounts but it can't be used for transactions. Through the lock-up mechanism, En-Tan-Mo protects the rights and interests of small holders and sets the system on a sustainable course.

Voters

Voters refer to every En-Tan-Mo participants. They are closely associated with miners and have a say in the election of miners.

Voting

The voting page will list out each miner's votes

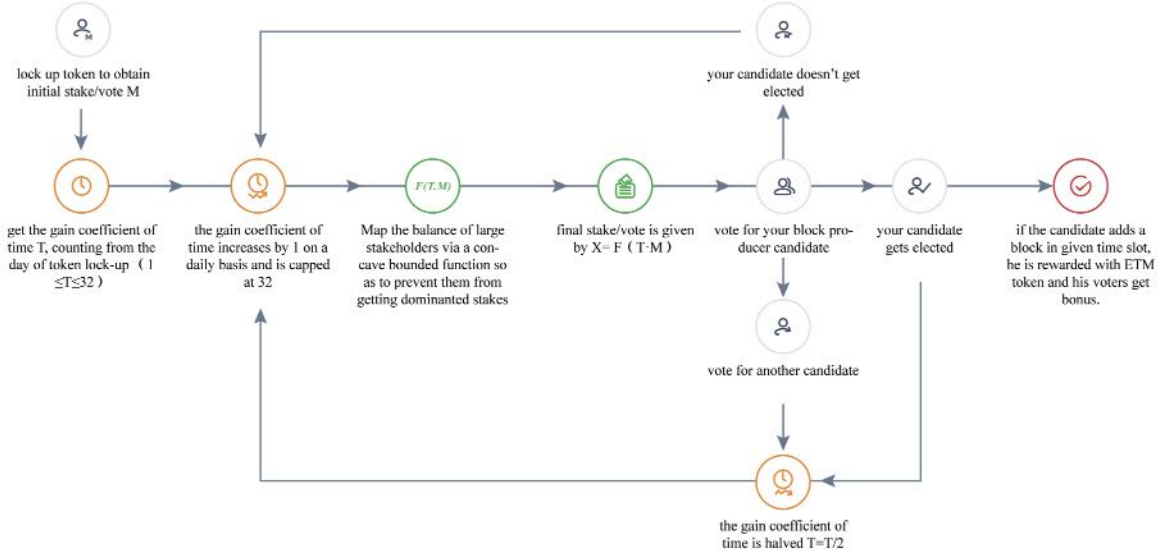
and performance record. Voters can choose whoever they want to become block producers.

Vote/Stake

Vote/Stake is the only measure of the qualification of block producer. It is obtained via a concave function based on the amount of token locked up.

Election Rules

In each round, a probabilistic selection will be made among miners based on their share of stake (votes). En-Tan-Mo voting stake (vote) calculation is shown in flow chart 2.



Flow Chart 2 En-Tan-Mo Voting Stake (Vote) Calculation

En-Tan-Mo Optimal Election System

If we see revolutionary voting system as a boost to security and decentralization, then optimal election system is the guarantee of stability and efficiency.

The voting mechanism of traditional DPoS-based systems are usually regarded as fair, democratic and effective. Yet En-Tan-Mo believes that only relative freedom can ensure the healthy development of the ecosystem. As such, we introduce an optimal election system with a view to phase out non-performing miners. Based on past performance, each miner will be assigned an optimal coefficient $v = m/n$, where m is the number of blocks a miner has successfully produced and n is the number of times he gets selected. For a miner, the probability of being elected is represented by $P = v \cdot X / \sum Xn$.

1. $m \neq 0, n \neq 0$ $v = m/n$
2. $m = 0, n = 0$ $v =$ the average value of previous round
3. $m = 0, n \neq 0, v = 1/10 * n^2$

En-Tan-Mo Bonus System

In En-Tan-Mo system, miners and voters are closely related. When a block producer mines a new block, his voters can obtain bonus. Such bonus totals 25 million ETM tokens, taking up 5% of the total supply. It will be distributed over the course of 6 years and the amount given decreases steadily year-by-year.

The share is 2.0224%, 1.0112%, 0.5056%, 0.5056%, 0.5056%, 0.4496% respectively

The timetable of block voting bonus is shown in table 2.

We plan to distribute voting bonus as follows,

1/2 will be first evenly divided into 101 shares and then given to the voters of elected block producers. The bonus a voter receives is proportional to the votes he/she casts.

1/2 will be given to the voters of a random

elected block producers after the round is over. The bonus a voter receives is proportional to the votes he/she casts.

3. From the People, For the People

As a traditional Chinese saying goes, "never forget why you started and your mission can be accomplished." When it comes to En-Tan-Mo, its founding vision is to create true value and remove the impediment of blockchain's development; to embrace extensive participation instead of being the game restricted to the elite; to become a truly decentralized autonomous community, makes the unobstructed value transfer a reality and put an end to monopoly once and for all. As such, En-Tan-Mo's entire infrastructure, be it voting system or bonus system, are designed to realize these goals and be true to its promise----from the people, for the people.

Table 2 Timetable of Block Voting Bonus

Reward ▾	Stage ▾
1 ETM	Preliminary Stage, before 10，112，000 blocks
0.5 ETM	Stage 1，before 20，224，000 blocks
0.25 ETM	Stage 2，before 30，336，000 blocks
0.25 ETM	Stage 3，before 40，448，000 blocks
0.25 ETM	Stage 4，before 50，560，000 blocks
0.26 ETM	Stage 5，before 59，328，000 blocks

Source of Randomness: En-Tan-Mo chaotic shuffling and tower of time algorithm, the foundation of a brand new world

Life is like a box of chocolate, you never know what you are going to get. In a world full of uncertainty, one never knows what the future has in store. Though uncertainty always comes along with anxiety and fear, it also gives birth to new hope and endless possibilities, driving individual and human progress. A world of stationarity is a world that doesn't worth living in.

The wheel of world history is pushed forward by a collection of unexpected events. If we say the uncertainty principle of quantum physics is the end of the relation between cause and effect, then randomness holds the key to the equality in the crypto-community. In En-Tan-Mo, order is built via an algorithm instead of an omniscient god. This algorithm is called chaotic shuffling. It is embedded throughout the entire En-Tan-Mo infrastructure and features prominently in mechanisms to keep the network safe and equitable.

Source of Randomness

Randomness is indispensable for a variety of things including encryption, the shuffling of cards, the handling of unknown parameters in weather forecast and flight dispatch. If a computers want to generate random numbers, it cannot do without real-world randomness. To be more specific, it has to measure random physical phenomenon using a particular hardware or equipment. Some random number generators obtain randomness from background radiation detected by Geiger counter over short timescales. But such method requires extra devices, takes time to collect data and produce result that can't be reproduced.

Computers are deterministic, that is, they act under pre-programmed instructions. Therefore, computationally generated random numbers are often called pseudo-random numbers. Here "pseudo" doesn't mean these numbers are fake. It only means they are apparently random numbers with a underlying pattern. These numbers are usually generated from random seeds. In other word, if a pseudo-random number generator is reinitiated with the same seed, it will produce the

same set of random numbers. This reproducibility is harnessed by blockchain to reach consensus.

Source of Chaos

The idea of chaos is a time-honored concept for Europe and China alike. Though it may mean differently, the philosophical implications is very much the same. In the Metamorphoses, Ovid described chaos in the famous line, "Ere land and sea and the all-covering sky were made, in the whole world the countenance of nature was the same, all one, well named Chaos, a raw and undivided mass, naught but a lifeless bulk, with warring seeds of ill-joined elements compressed together." Similar descriptions of a shapeless mass can also be found in Chinese classic literature. However in modern science, chaos is discussed in a wholly different way.

Chao theory, in mathematical and physical sense, is first conceived by Edward Lorenz, a meteorologist from MIT. When Lorenz was running a numerical computer model of weather prediction, he entered a rounded initial value instead of the full precision value. However, the minute variation in initial data which was seemingly inconsequential later yielded grossly divergent results. This finding eventually led to his famous theory known as the "butterfly effect". The most cited analogy for it is that the flapping of butterfly's wings in Brazil would set off a tornado in Texas.

As a Chinese saying goes, "a miss is as good as a mile." A small change in initial condition would result in vast discrepancy. That is the most fundamental idea of chaos theory.

Ever since Lorenz discovered the dynamic system's sensibility to initial value, similar patterns have also been found in other natural and social phenomenon. And chaos theory has been applied extensively in a variety of disciplines, including biomedicine, computer science and fluid mechanics.

Chaotic Shuffling

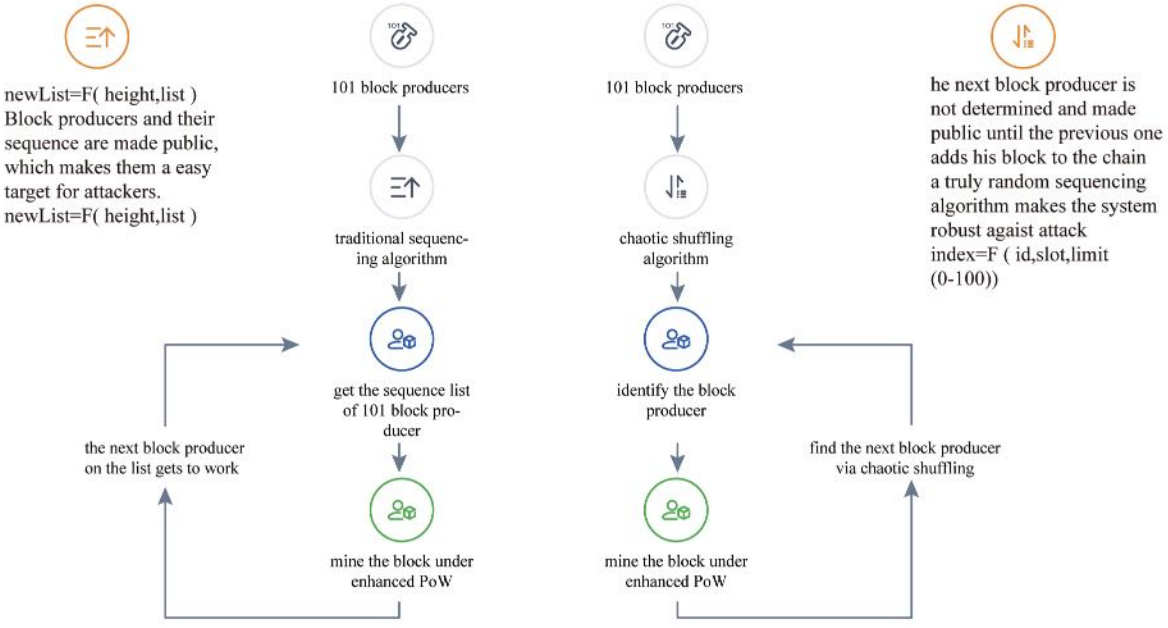
Computer is deterministic, yet this very feature is often exploited by attackers. For a blockchain system, the sequence of miners has to be deterministic. However this also increases miners' risk of being targeted and attacked should the sequence is known to malicious actors who want to temper with transactions.

newList = F(height, list)

In traditional blockchain systems, the sequence of miners is determined and made public as soon as they are chosen, making them susceptible to attacks. as shown in flow chart 3.

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

To address this problem, En-Tan-Mo implements the chaotic shuffling algorithm which takes advantage of the dynamic system's extreme sensitivity to initial data. As we know from chaotic theory, a minor change to the initial value would lead to grossly different outcomes. In other word, it would add a degree of uncertainty to the prediction process. Yet such uncertainty can be very helpful when it comes to enhance network security. Through chaotic shuffling algorithm, the sequence of block producers is not determined



Flow Chart 3 Chaotic Shuffling

from the very beginning. The method to obtain the number of the next producer is take a fraction of data from the earlier block, map it and do iterative calculation. So the identity of the next block producer is not made known until the last minute. By then it would be too late for malicious actors to plot and initiate an attack against him. Plus, chaotic shuffling is deterministic. Every miner can get the same result with the same initial value. In this way, En-Tan-Mo realizes stability and security while preserving decentralization.

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

The Random Source of Chaotic Shuffling---- Tower of Time

For every intricate system, individual behaviors may be controllable, but the collective behaviors are not. Thus we can use the blockchain characteristics to ensure the reliability and equality of random number generation by allowing every participants to be the provider of random seeds.

With this in mind, we devise the Nash equilibrium-based tower of time algorithm. Under this algorithm, anyone who makes a deliberate change to a single parameter will get the result in his favor. Hence the algorithm can serve as a genuinely distributed and reliable source of randomness.

Tower of Time Algorithm

Algorithm input: N hash value, M iterations, X SHA computation

Description of Parameters

1. N, M and X are algorithm parameters. By changing N, M and X, we can adjust the time complexity.
2. X is a constant that denotes the times of SHA256 computation.

Procedures:

1. Denotes the hash value of the first block of N blocks by H0.
2. Iterating H0' = SHA256(H0) X times, we get Q0

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

3. SubstituteQ0 into chaotic shuffling algorithm and get the index of the next block. K1 = Chaos(Q0, H, N).
4. Find the hash value of K1 block and denote it by H1.
5. H1 = H0 + H1
6. Do SHA256 computation on H1. Repeat step 2 to 5 and then obtain Q1 and iterate it M times.
7. Sum Q1 to QM and output the final result.

Characteristics:

1. We use the characteristics of iterative algorithm as a way to mitigate the influence of parallel computing.

2. By using the characteristics of chaos algorithm and through iteration and random selection, we prevent subsequent block producers from gaining more information over time.

3. The time complexity can be adjusted via changes to the parameters so that the algorithm can meet the need of random number of varied frequency.

Order and Equality

Chaotic shuffling is the most important implementation of chaos theory in En-Tan-Mo blockchain. It spreads random seed across the network so as to maintain equality and establish order within the network. Plus, it will be provided to all DApp developers as a way to eradicate cheat and make the application ecosystem fairer.

Without a reliable source of randomness, DApp users are not in control of their own fates as developers and operators still hold sway over the DApp's assets (the production rate of in-game items) and equality (the wining rate). En-Tan-Mo's tower of time algorithm, derived from chaos theory, uses the very "chaos" to build a reliable source of randomness so as to establish order and equality in the network.

En-Tan-Mo Side Chain: removing barriers to resource

Developers are the beneficiaries and facilitator of blockchain technology. A sustainable token ecosystem cannot be built without the effort of dedicated developers. However, we have recently seen the bleeding of DApp builders from mainstream currencies such as ETH and EOS as

a result of increasingly costly development and operation, and this has pushed their entire app ecosystem into a vicious cycle. To prevent such situation from happening, En-Tan-Mo embeds the idea of win-win cooperation throughout its mechanism design from the very beginning. En-Tan-Mo's side chain enables developers to allocate and mobilize on-chain resources on a dynamic basis while the network only charges a small amount of transaction fees for security concerns. And these fees will be re-distributed back to developers through community activities.

Blockchain Scalability

Scalability is a major bottleneck to development that no blockchain project can afford to ignore. Traditional blockchains, such as Bitcoin, lacks the ability to scale for they demand miners' full knowledge of the whole blockchain in a bid to ensure the network's security. The scalability issue limits developer's creativity and hinders DApp from becoming mainstream application.

Traditionally, Bitcoin and Ethereum rely on a single chain to process and store the data and transactions of the whole network and require every node to keep a copy of the entire history. As such, the processing capacity of the blockchain as a whole is in fact limited by that of a individual node. Plus, due to their consensus algorithm, the system's overall processing speed tends to decrease rather than increase with the increase of nodes. With a view to improve scalability, several solutions have come forward. The key idea is to let insignificant data and transactions be verified and stored only by partial nodes. Sharding, the proposal of Ethereum, divides the network into 100 different shards and allows them to process transactions independently. En-Tan-Mo, however, approaches it differently. For every DApp there will be an exclusive side chain on which it runs and stores data. This multichain structure lifts the cap on network's processing capacity, enabling it to handle concurrent transactions in an efficient manner.

Scalability can be enhanced either by shards or by side chains. Yet the former is fixed while the latter enjoys more flexibility. Besides sharding adds to the difficulty of management, because it needs more validators to keep the network safe. Side chain, in contrast, shares the same validation mechanism with the main chain and doesn't require additional nodes to do the job. When it comes to affordability, sharding is more expensive than side chain protocol. The former uses the costly smart contract. The latter is much more developer-friendly as it streamlines operation, debugging and maintenance procedures via the building of application-specific server.

Bottleneck to the Development of Ethereum and EOS: limited resource vs. unlimited applications

Is scalability really the only bottleneck to blockchain adoption?

For DApp builders on Ethereum, better user experience means more gas. But cost is not the only problem they are worrying about. The complexity of DApp hinges on the number of Ethereum stacks. That is, building a slightly sophisticated DApp is basically out of the question. As such, simply boosting scalability will do very little to improve Ethereum's ability to attract developers and encourage extensive adoption, given that the network's core ideas remain the same. In addition, Ethereum is heading towards an uncertain future, as it plans to migrate from PoW to PoS, which even raises mores concern among DApp users and developers.

To shorten the time of confirmation, EOS shifts away from Proof-of-Work and charges a handful of supernodes with the responsibility to verify and pack transactions for the whole network. Claiming to be able to scale to millions transactions per second, EOS does considerably well, achieving thousands under real test conditions. Therefore, the true impediment to EOS development is not scalability but something else. In our view, it is RAM.

There exists a memory market on EOS where contract developers write information into a block and perform operations by consuming RAM. RAM is an tradable resource that is used in many operations, say creating an account and biding for an account name. According to EOS's algorithm, RAM price fluctuates based on demand. The more RAM one uses, the higher the price goes until it reaches a point where RAM becomes so expensive that no one can afford and that's how EOS makes sure the platform will never run out of it. The volatility in RAM price breeds speculation. Most of the RAM is held by speculators while DApp developers are starved of this very resources they need to launch their product. Even if they do get it, the cost would be too expensive. Should there be a proper mechanism to keep RAM market in order, developers would turn to other platform with developer-friendly environment before long. This is bound to undermine EOS, both in terms of its DApp ecosystem and its value as an application platform.

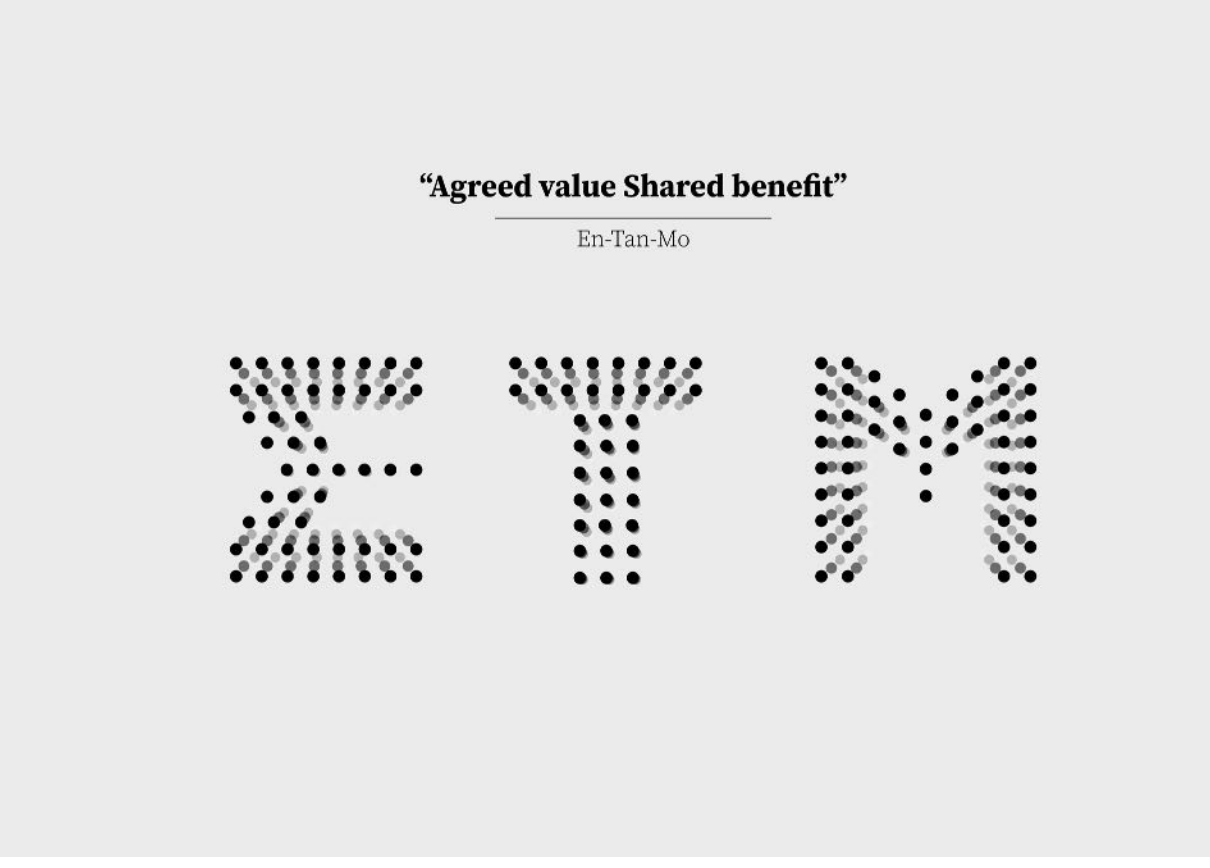
Taking a closer look at the way EOS works, we will find that RAM is far from being the only impediment to the platform's development and adoption. For every task performed, four resources, namely EOS, RAM, CPU and NET, are required. This is beyond doubt a catastrophe for users and developers.

The question we should ask is, when necessity becomes rarity, is there any possibility of

mainstream adoption for blockchain?

Side Chain: No more cut-throat competition. It's time for win-win cooperation.

A brief review of current blockchain projects shows that the development of the whole blockchain ecosystem is seriously hindered by the scarcity of resources and the vicious competition between DApps and developers. That's also the reason why there has not so far been any blockchain-based DApp that gains mainstream adoption. En-Tan-Mo, powered by the main chain-side chain structure, removes barriers to resources, with each DApp running independently on an exclusive side chain with full functionality. En-Tan-Mo's Unified-Proof-of-Stake (UPoS) algorithm is able to manage 500 transactions per second and reduces the average block intervals to 3 seconds. With independent side chains, En-Tan-Mo enjoys infinite potential to scale. As side chain increases, the network will be able to do N*1000 transactions per second, carrying DApps with better user experience, such as game. In short, on En-Tan-Mo, scalability will not stand in the way of developers' imagination becoming reality. Backed by powerful technical infrastructure, En-Tan-Mo lays the foundation for the new generation of internet application platform and paves the way for future technical innovation and reform.



Epilogue (I)

Rising above Challenges: User Empowerment is on the Horizon

Abstract: As a concept of communication science, empowerment in blockchain means power and freedom for all users under decentralization. This paper will elaborate on the current challenges confronting blockchain empowerment and explore ways to overcome them.

"A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system", ① said Satoshi Nakamoto in 2009, facing up to digital currency's disappointing record in going mainstream.

Satoshi's attempts to decentralization, as opposed to centralization, represent another form of empowerment in social context.

Here Comes Everybody: Technology-enabled Power Delegation

Empowerment refers to the process of enabling an individual or a group of individuals to act on his/their own authority. ② Yet empowerment seemed nothing more than a distant dream for the working class, those oppressed and exploited, when scarce social resource was controlled by the few protagonists or central authorities.

Power has always offered rich food for thought. Apart from the observations on its origin by Marx and Weber, studies of power shifted focus away from the analysis of seeing it purely as an instrument of coercion, due to the work of the French postmodernist Foucault.③ Foucault deconstructed the relationship between rulers and the ruled by seeing power as a network of relations, where individuals are in constant flux. And his interpretation on power also seems to indicate that mankind, backed by technologies, is about to embark on a path towards empowerment.

A brand new social landscape is taking shape with human physical limit extended and more value created, thanks to the advent of such nascent technologies as blockchain, Bitcoin, artificial intelligence, underground transportation network, enhanced reality, 5G WiFi, driverless cars, new solar technology, laser-delivered internet, IoT and AR head-mounted devices,Just like Wikipedia editors. Individuals, dispersed across the globe, join together following new rules in a transparent, information-enabled environment and emerge as a powerful force against the monopolies with exclusive ownership of means of production.

Hence behind today's emerging technologies boom, a future of power delegation begins to brew----individual empowerment seems imminent. Just as pointed out by Clay Shirky in Here comes everybody, the variety of social tools that are in place today enable a community of loose structure to run in a not-for-profit manner and without organization at the administrative level.④ This corresponds perfectly to Foucault's

---

① *What do you know about Satoshi Nakamoto, other than the "father of Bitcoin"?* ChainHR, ,2018-10-20.

② *Probe into "empowerment"of communication science.* Wang Xiling, Sunli, Zuhao. Today's Massmedia. Vol.4, 2012.

③ *The comparison between Foucault's theory of power and Marx's theory of power.* Qu Guangdi. Qingjiangluntan. Vol.1, 2016.

④ *Here comes everybody: the power of organizing without organizations.* Clay Shirky. China Renmin University Press. Edition 5, 2009.

observations, both indicating that emerging technologies are becoming bolsters for power delegation.

The future is for everybody and in constant flux. With the advent of new technologies, power is no longer untouchable and great dreams are within reach.

What is the path towards empowerment?

Power Delegation Remains an Unfulfilled Dream

The year 2018 saw blockchain featuring prominently in the technology arena. In February 4th 2019, Chainspace, a blockchain startup, was acquired by Facebook, becoming the first-of-its-kind in the tech giant's business empire.

In 2008, Mark Zuckerberg, Facebook's founder, made the adoption of blockchain technology, a distributed ledger, in Facebook its 2018 goal as part of his efforts to empower users via decentralization.

In the blockchain world, participants, be it nodes or organizations, interacts freely without a third party in between, and reach consensus via a random algorithm. A vote is held on an algorithmic basis in order to put in place a new consensus if the old one should fail. Thus trust is built across the network, unlocking new possibilities for peer-to-peer cooperation.

This renders centralized platforms unnecessary. New rules are laid by algorithms rather than by the ones in power. A consensus-based model is opening up new horizons for all users within.

Nevertheless the benefits of technology do not always serve the common good as optimists would have expected. Capitals are never out of the picture, and with the ability to shape facts and values as they wish, once again drive power towards centralization.

Proof-of-Work algorithm used to be placed high hopes for achieving decentralization. Yet the fact that anyone with the mining gears can be miners allows them to amplify advantages by leveraging their technical strengths and organization capacity. As such an alternative approach called Proof-of-Stake came along, believing decentralization can be obtain through a couple of very centralized supernodes. None of them, unfortunately, managed to rein in centralization and worse still, they gave rise to a hash power "arms race"that only tends to get ever more intensive and fierce with each passing day. Under these mechanisms, mining becomes an enterprise characterized by economy of scale and corporatization as capitals flood in in large numbers. The 51% attack, though impossible for individual nodes, may be rendered possible by large mining pools with massive hash power. That magnates come back at the center of the mining arena shattered the hopes for decentralization via Proof-of-Work.

Similar problems are also confronting Proof-of-Stake algorithm. As coin age and holding are the decisive factors in the selection of block producers, the ones with older coins and larger holdings are more competitive and of course more likely to be elected. This gives rise to the Matthew effect, where the more holdings one has, the more reward he gets. As a result, the gap between large stakeholders and small ones are widened, adding to the possibility of 51% attack. Though unintentionally, Proof-of-Stake is centralized indeed. The pursuit of empowerment once again comes to a halt.

To address the shortfalls of the abovementioned consensus mechanisms, Delegated-Proof-of-Stake adds a constraint to Proof-of-Stake, i.e an election mechanism, so that block producers are not chosen merely on the ground of holdings and coin age, but are elected and removed by voters through the casting and withdrawal of votes. In this way, the mechanism designer enables block producers to be chosen on a fairer basis. However the bad thing is it can't ensure there will be enough real producers, because it is possible that several nodes are controlled by the same person or organization. For example F2Pool once controlled more than half of LBTC's nodes. And rumor has it that there was a person who controlled 7 nodes on EOS.

Despite setbacks, people are optimistic about blockchains future. A scholar once predicted that by 2015, blockchain technology will be extensively adopted in breaking monopolies in financial markets and

empowering industries.

Yet so far decentralization remains an unfulfilled ambition for Satoshi and his predecessors. Iterations and improvements have to be made on consensus mechanisms.

Empowerment for the Users: En-Tan-Mo calls for Public Freedom

For En-Tan-Mo, individual empowerment is something that is embedded in its consensus.

On its distributed platform, empowerment indicates joint participation and fair rewards, which are not fantasies but realities.

Scientists from En-Tan-Mo reckon the failure of traditional consensus mechanisms is resulted from the inability to eradicate centralization. Determined to plough a clear furrow between itself and the blockchains dominated by big mining pools and large stakeholders, En-Tan-Mo is committed to delivering benefits to all via the Unified-Proof-of-Stake algorithm, a underlying, fundamental renovation at the protocol level.

The scale is traditionally tipped in favor of the strong over the weak. Mining collisions function likewise, in which the more hash power one controls, the more rewards he reaps. Yet such a super-linear rewards model will lead to an anemia ecosystem in the long run that in turn hurts everyone, the strong and the weak alike. To address this issue and to empower all participants regardless, En-Tan-Mo implements a hybrid model of Proof-of-Work and Delegated-Proof-of-Stake, which limits the tendency towards centralization to the largest extent.

In Bitcoin, hash power determines who gets to write the next block and it works very much the same as a rudimentary math class. The larger the hash power, the greater the possibility of outpacing others in solving the crypto-puzzle and being rewarded handsomely in the form of Bitcoin. However, in En-Tan-Mo, hash power is not the only but one of the criteria for candidacy. Performance record will be taken into account also. Besides, top-performing candidates with high hash power are not necessarily block producers though it is true that they have a better chance of being selected. When it comes to large stakeholders, their payoffs are subject to a concave function so as to put a check on super-linear rewards. As such in En-Tan-Mo, there will be neither hash power "arms race"nor hash power monopolies, and everyone will benefit from a thriving ecosystem, because it makes sure that hash power is merely a means to an end, not an end in itself.

Under En-Tan-Mo's Unified-Proof-of-Stake, a vote-based mechanism is deployed to select block producers, in place of the traditional hash power-based one. It is innovative in a way that it put in place an equitable and ideal world where the majority of participants are no longer bystanders but creators and contributors. Though voters do not directly involved in block generation, they have a strong say in who gets to do that. By mapping token holdings into votes, voters pick their favored candidates on the basis of past performance and hash power and get ETM token rewards if their picks succeed.

En-Tan-Mo is a bottom-up, market-driven platform with an equilibrium-based value transfer infrastructure that allows value to flow around freely in an equal and transparent manner. Participants motivate and support each other under Unified-Proof-of-Stake consensus, and run a variety of applications, blockchain-based and non-blockchain-based. In this way, En-Tan-Mo enable all the people who long for fairness, democracy and freedom to pursue their maximal stake and interest on an equal footing and secure an equilibrium between power and freedom.

In an age of power delegation, there are plenty of ways to give freedom away, yet those to get it back are few. How can we create a future where people are truly empowered, as Satoshi envisaged? The answer remains elusive, especially at a time when the majority of blockchains are hijacked by large capitals.

However, there is a silver lining. In the En-Tan-Mo world, choices for freedom, no matter how small it seems, are still allowed.

Epilogue (II)

A Decade on, Satoshi's Spirit Back Strong Thanks to En-Tan-Mo

Undoubtedly, the Blockchain technology is deemed as a serene revolution across the world nowadays. However tranquil, the power within is now changing our world beyond our imagination.

En-Tan-Mo, or ETM for short, is inspired by Entente, Transaction and Mobius. It is a blockchain project of new generation based on Nash Equilibrium and Value Transfer theory, a saber forged ten years on in a bid to once again shed light on the spirit of Satoshi Nakamoto.

Decentralization Overview: En-Tan-Mo Is Not an Elite Game

Fast forward to 2008, Satoshi Nakamoto published his dissertation entitled Bitcoin: A Peer-to-Peer Electronic Cash System, drawing public attention to the cyptocurrency and its underlying technology blockchain for the first time.

A thrilling concept, it describes a world more than avant-garde in which blockchain terminates such role centralization has been playing as a credit "capitalist" and in return hands over the right of information storage and conveyance to participants as a whole in a democratic manner . In other words, "decentralization" is a "declaration" per se from the very beginning for Blockchain, the one that makes the technology no longer synonymous with reform or optimization on current social operations, but "overturning" the established empire of centralization and its logic behind.

To this end, at the expense of efficiency, Satoshi ushered a consensus mechanism called Proof of Work (PoW) in Bitcoin.

Soul of Blockchain, consensus mechanism answers how would the system operate systemically and replace successfully the function of "bookkeeping" of centralized institutions under decentralized circumstances.

Computing power consumption is the solution of PoW. Of all the nodes across the network, whoever finds the answer to a mathematical puzzle first becomes the bookkeeper for the new block and receives certain reward hereof.

Nevertheless, highly efficient mining machines have outperformed ordinary CPU-mining in terms of computing power and reaped super- linear payoffs thereafter. Worse still, the emergence of large mining pools later on has dashed the hope of decentralization for Bitcoin in every sense of the term. d hereof.d hereof.

Such projects as turning down PoW and turning to PoS or DPoS have shifted their emphasis onto the pursuit of efficiency. In the end, unfortunately, they render a game played by major players where the growth direction is mastered by a minority of large stakeholders, thus turning to "pseudo-Blockchain". "Decentralization" in its nominal sense only has far too early deviated from the original idea of its initiator's spirit.

It is for this reason that ETM is given birth to and remains the thorny problem of prime importance. To this end, ETM Academy of Sciences has designed a hybrid consensus model called UPOS (Unified Proof of Work) with PoW and DPoS combined.

ETM deems that true decentralized world is an uncertain one embracing creativity and fairness and

featured by sensitivity and seclusion to a central authority and monopoly.

ETM adopts PoW+ in order to avoid monopoly on computing power. At no expense of security, it cuts computing needs in a dramatic fashion in an attempt to get the public involved. Highly-efficient PCs with independent CPU, idle servers in video workshops, servers with excellent performance in laboratories and cloud servers with GPU, to name just a few, would all be candidates for ETM block producers.

To ward off monopoly caused by centralized stakes, within the UPoS mechanism, each and every token holder is a voter who transfers their token into votes through a convex mapping and uses his votes to select miners and get rewarded thereby.

Here is worth mentioning that the relationship between the votes voters enjoy and the number of token they have is govern by a convex function. Namely, the more token there is, the lower conversion rate is and vice versa, which renders En-Tan-Mo the fairest and most just system in blockchain world.

In addition, having considered the fact it can be very difficult for individual investors to gain a fair share of profits in a certain stable system, ETM sets up a coefficient t for small stakeholders. Under the auspices of time, votes increase by leaps and bounds, which enables private investors stand out from the crowd.

This is exactly what ETM is for. Thanks to its brand new voting and bonus mechanism, all participants can be part of blockchain construction in the name of miners or voters and get rewarded equally, ensuring that the entire system fails to be manipulated by oligarchy and rendered an elite game. That decentralization, the original values of blockchain is ensured to be restored and a more equitable and just public chain system is what we believe the core of Satoshi's spirit.

On SHD Completeness, ETM Has a Say.

Following the incremental rise of Bitcoin's value is a great deal of so-called "projects" mushrooming, catering to people's imagination on blockchain. The mismatch between individual investors' enthusiasm and technique know-how provides an opening for impractical "blockchain" projects to exploit. Worse still, simply covered by a "White Paper", the illicit fundraising and fraud can appeal to numerous attractors. Even faced with the current situation where there is no circulation or rigid need for virtual currency, some speculators swarm into "blockchain" still with the mindset: Either Multiplied by One double O, Either divided to zero.

Not until supervision tightens and red lines drawn for feverish coin issuance and speculation are related insiders aware that blockchain should be transferring from issuance craze to technical growth.

ETM has long been focusing on it.

Blockchain, given credit to its technology, its birth is a prime example of perfect combination of distributed data storage, peer-to-peer transmission, consensus mechanism and encrypted algorithm done by Satoshi.

The development of Blockchain is restrained by technology also. Given the fact that of the distributed storage system, consistency, availability and partition tolerance cannot be compatible with each other, also known as CAP theorem, Blockchain is no exception. The compatibility of SHD (Security, High-performance and Decentralization) within blockchain renders a pending issue. Over the past decade and beyond, invariably, has born witness to the stilted development of blockchain technology in which trade-off has to be made among the three features. As evidenced by the fact that Bitcoin sacrifices high-performance in exchange for the rest two and EOS's sacrifice of decentralization for high-efficiency, it is fair to say that the compatibility of SHD consists of the core of blockchain technology. We can assume even without any hesitation that whoever achieves their compatibility can hold the reins of blockchain.

ETM has been focusing on it throughout mechanism design and technology achievement process. UPoS mechanism, pooling wit and wisdom of experts and scholars in technical teams across all sectors, would definitely not be stopping on finding out solution to decentralization. Of this mechanism, decentralization, security and high-performance are an inseparable entity.

In the event that such afore-mentioned strategies as convex mapping, time gain and stake constraints put their emphasis on safeguarding decentralization to separate token owners from blockchain miners and redeem stakes respectively, then mechanisms like chaotic algorithm, uncertainty (probability) and premium render the prime guarantee for security and high-performance.

On the one hand, nodes become miners by election before forging block via hash computation. A re-election is required after each round of block production. The sequence of miners is generated in a random manner depending on the result calculated by the previous miner. Of this system, hash algorithm is no longer used to do the proof of work, but to create unpredictability (with respect to the next block generator). This ensures there is no room for cheat and coordinated attack.

On the other, the change of hash computation slashes computing power consumption, reducing resource waste by a large margin. Yet the difficulty of the hash computation can be tweaked still to adjust the cost for nodes in a dynamic manner, which in turn incentivizes nodes to safeguard network stability and ward off Sybil attack. More transactions, therefore, can be handled per second and the system's overall efficiency enhanced accordingly. In the meantime, with the boost in scalability, more extensive adoption is made possible.

Furthermore, ETM adopts the design of one main chain with side chains attached. Within the design, the main chain is in charge of the network security and value transfer, and its side chains, each running a single DApp, function as independent and isolated systems. Through inheriting and implementing the main chain technology, all applications owns a distributed ledger with customized token, consensus and transaction. Meanwhile, however, with self-evolving components as its core, ETM not only provides other blockchain with adaptive platforms for their assets and applications transfer, but configures two-way transfer channels for non-blockchain applications and their data, which makes ETM a user-friendly platform with immense potential to scale.

Initiated by technology and established in application, each technology cannot be proven meaningful until once implemented into practice, and blockchain is no exception. Only when SHD completeness issue is sort out can blockchain be done justice to before its application in a new era featured by freedom and imagination. Being exactly the original idea of Satoshi's, it renders our reiteration on his spirit as well.

ETM Aims High with its Scientific Background Shines.

Over the years, Satoshi, the initiator of Blockchain, remains a mystery. Some assume him a scientist as he was familiar with almost all the state-of-the-art computing technologies up to date; some honor him as an economist for his insight into economic rules and groundbreaking contribution to financial technology; and others even indicate him the Nobel economics prize winner. In the meantime, however, it is said that Satoshi is a team rather than an single man.

Just as Mr. Wei DAI, the cryptologist remarked: "In order to develop Bitcoin, requirements shall be met as follows: 1. Profound thinking on currency; 2. Knowledge of cryptology; 3. Believing in distributed systems like Bitcoin can work; 4. Highly-motivated to make that happen; 5. Outstanding programming skills to ensure network security; 6. Social skills if necessary to establish a successful community based on Bitcoin. Within the cryptology circle, unfortunately, candidates meeting the first three conditions are very rare indeed."

To this end, we have established ETM Academy of Sciences specifically to track him down.

Its members include: Prof. Thomas J. Sargent, Nobel Prize winner in economics and leader of rational expectations school, Prof. Sheldon Lee Glashow, Nobel Prize winner in physics and founder of Grand Unified theory model, Dr. Aaron Yuan, distributed system expert at the University of Maryland, Post-doc Daniel Wang, P2P Protocol expert at the California Institute of Technology and Dr. Thomas Tang, Game theory expert at University of San Diego, to name just a few.

All consensus mechanisms and protocols are designed by ETM Academy of Sciences. Led by two Nobel Prize winners, the interdisciplinary team is here to stay, ensuring the technical advancement. ETM

consensus mechanism and its equilibrium economic design, based on the game theory and distributed system respectively, implement Prof. Sargent's rational expectations theory and dynamic macroeconomic theory on the basis of time sequence analysis. Meanwhile, ETM equilibrium consensus designs equilibrium value transfer system in which miners, token holders and ordinary participants coexist after applying Prof. Glashow's thoughts related to particles coexistence and phase transition in complicated system.

The fruitful result yielded by ETM currently shall be giving credit to the close cooperation and concerted efforts jointly conducted amongst teams in theory and practice, software and hardware, technology and business operation. For instance, Kantorovich consensus mechanism is jointly designed by experts from mathematics, communications and IT sectors; the infrastructure of "En-Tan-Mo Science" and stake distribution mechanism are brought to life by Ethereum participants together with VIPs in crypto-community; experienced software engineers previously working for top Internet companies such as Google, Thunder and Baidu have been involved with project coding design independently. Under the auspices of ETM Academy of Sciences, there is another special asset, namely, all the theoretical designs have been through dual verification process, meaning they would be verified by mathematicians via consensus modeling and simulated experiments for their numerical value before being verified again in accordance with strict standards by IT and communications experts for En-Tan-Mo project under real circumstances.

Of interest a phenomenon in the crypto-fever nowadays is: A state-of-the-art subject as such, the majority of which involves no scientists.

Every milestone throughout the Internet development phase is accompanied by scientists, as evidenced by Google Institute, leader in artificial intelligence, and Ali Research, giant of big data, not to mention World Wide Web, a product designed by a scientist from the European Physical Society per se with which we are familiar. As a result, we deem that true blockchain projects shall have their own research crew, the reason behind the establishment of ETM Academy of Sciences.

In 1925, Bell Telephone Company set up an experiment subsidiary named Bell Laboratory afterwards. This laboratory has born witness to 11 Nobel Prize, 16 top Science and Technology Awards, 4 Turing Awards and 3000 patents altogether, a huge contribution to science and technology all over the world.

Similarly, ETM Academy of Sciences has a consortium of first-rate scholars across the globe. They are competent enough to conduct related research with affection for society and aspiration for themselves. The interdisciplinary background is synonymous with open-mindedness in the team and more probability in the foreseeable future for team extension and academic connections building. Different backdrop means wider views and more creative ideas clashing with each other. So it is fair to say that nothing is impossible for ETM Academy of Sciences.

Conclusion

Dating back to the Industrial Revolution and the Emergence of the Internet, in retrospect, one would never ever define each revolution on the invention of steam engine, vehicles or PCs, instead, engraved in the world history are drastic changes in society brought by those breakthroughs. Therefore, provided that blockchain is an epoch-making revolution in technology, then it must be similar with electrics, PCs and the Internet, a roadmap passing on human history to generations to come but not an end in itself at all.

As pointed out by Haseeb Qureshi in his essay entitled Blockchain: the revolution we're not ready for, "Blockchain is going to upend entire societies. It's going to enable new kinds of governance systems that were before only the daydreams of utopians and philosophers."

This path is meant to be uneven, but the space of imagination it unleashes is ever so longing.

Max Weber, the German philosopher once said, "Inevitably, the tree of knowledge yields nothing but a perspective which may break the jubilance of all: Since we cannot turn a deaf ear to conflicts amongst those values, we shall be keenly aware that actions of importance as such, let alone life as a whole, should they not eclipse one by one like a natural incident but are consciously guided by us, then they mean a

series of fundamental decisions taken. Through those decisions, our souls have chosen their fates as of Pluto's, so to speak, the relationship between actions and meaning of existence."

The birth of blockchain unleashes the space of our imagination for this world. Not only does it enable us to imagine the relocation of economic, social and cultural capital, but reflects upon "Imagined Communities", an idea raised by Mr. Benedict Anderson as well. Thanks to that, we can imagine a brand new public space under which our existing status, values and meaning may be human-oriented and filled with new affection, expectations, inspiration and social ethic construction. To this extent, blockchain is concerned with economics, sociology and even further anthropology and philosophy.

Therefore it is in this regard that imperfect as Bitcoin though, Satoshi deserves our reverence still. His greatest contribution is not about Bitcoin, but making blockchain technology a household name; nor is he the most charming person for his wealth the world over, but for the bright blueprint he presents to us: a world where decentralization is pursued for the common good and individual security, privacy and rights of participation are well respected; and a brighter future for mankind, guided by modern sciences as economics and mathematics. This is "Satoshi's spirit" per se, followed closely and publicized by ETM.

Following the ups and downs of Bitcoin and numerous dramas, true or false, is Satoshi's complete disappearance. His legacy is nothing but one sentence in email box: "Satoshi Nakamoto is each and every one of us." Yes, indeed. He lies in the heart and soul of ours since we are practitioners and participants of blockchain technology per se.

EN-TAN-MO