

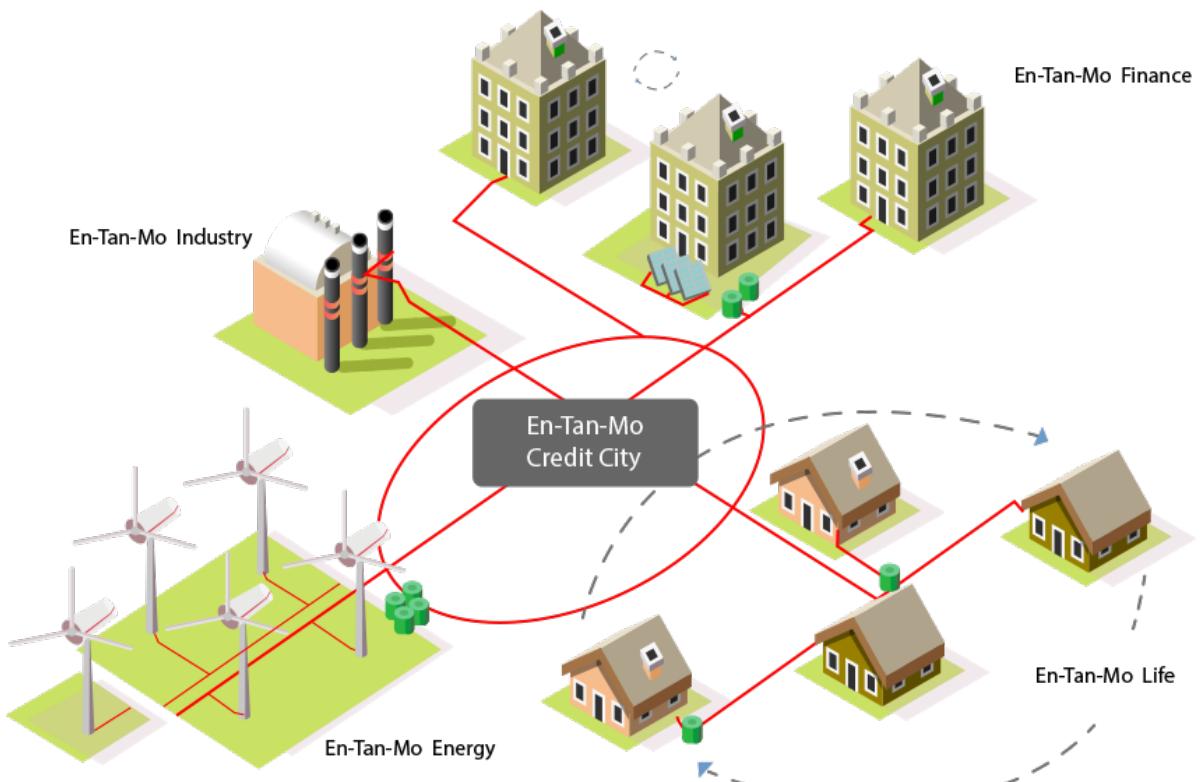
EN-TAN-MO

EN-TAN-MO SCIENCE

日本語

Annotation

En-Tan-Mo はナッシュ均衡と価値伝達理論に基づき新たなブロックチェーンである。2011 年のノーベル経済学賞の受賞者トマス・サーデント教及びアメリカのカリフォルニア工科大学、メリーランド大学、フランスのポアンカレ研究所の各領域の学者たちは共同研究を通じ、ゲーム理論の研究結果をブロックチェーンに取り入れ、完備な SHD を有する En-Tan-Mo を作り上げた。En-Tan-Mo の世界では、Kantorovich コンセンサスの指導を受け、Stakhnov マイナーと Pareto マイニングプールは相互協力と励ましを通して、各ブロックチェーンと非ブロックチェーンのシステムを包括し、分散型ブロックチェーンの影響を受け、すべての参加者に均衡の各自体の最高権益を獲得させる。En-Tan-Mo は最先端の数理モデリングだけでなく、多数のアプリケーションと幅広いブロックチェーンシステムのユーザーを有し、数学理論と経済学原理の厳密検証から成り立ったシステムである。したがって、「技術白書」の形式で En-Tan-Mo の意義と複雑性を説明することは不十分である。ここで、開発チームは哲学、数学、経済、並びにエコシステムなどの多方面から En-Tan-Mo を解釈した上、各部分の責任者に Uni-ID と電子ウォレットを提供する。



0.0 En-Tan-Mo とは

ブロックチェーンの発展

ブロックチェーンの開発発展の歴史を回顧することは En-Tan-Mo の革新性を理解されやすくなる。

2008 年にサイト・ナカモトという人物が『ビットコイン：ピア・ツーピア電子キャッシュシステム』という論文を投稿してきた。後に 2009 年 1 月 genesis ブロックが作成し、ビットコインの時代が始まると言われた。2013 年に今まで最も重要な新バージョンのビットコインが開発し、ビットコインの内部管理の改善とネットワーク最適化能力を向上させ、世界中にビットコインの影響力を拡大させた。しかし、最初の暗号通貨として大きな成功を収めたビットコインの拡張性が低いため、ブロックチェーンの持続的な発展の妨げとなった。その拡張性の低いビットコインに使用された初期のブロックチェーン技術をブロックチェーン 1.0 と呼ばれた。

ビットコインの拡張性問題を解決するため、ヴィタリック・ブテリン (VitalikButerin) がイーサリアムを考案した。イーサリアムには明確な設計と構造システムがあり、EVM から ICO、そして異なるバージョンの POC から 2015 年の frontier 階段、更に、POW の Metropolis 階段から POS の Serenity 階段において、イースリアムのチューリング完全、スマートコントラクト、ASIC 耐性及びブロックチェーンアプリの性能はブロックチェーン 2.0 到来を証明した。イースリアムは開発者にプラントフォームノードとプログラミング言語を提供し、次のアプリの開発と発表させる基礎を築いた。

2018 年 2 月、ビットコインのコンピューティング・パワーが 20EH/S に達し、Github では現れたオープンソースプロジェクトは 9 万を超え、中国、アメリカ、イギリス、シンガポール、日本、韓国などを含み 90 個以上の国々はブロックチェーン技術研究に参入した。2008 年から 2018 年までのわずか十年間、ブロックチェーンの思想と理念は大衆に受け入れ、実現した。それに対して、インターネットがアメリカの国防部の国防高等研究計画局が TCP/IP プロトコル・スイートを開発するの 1974 年から発足し、中国では国際インターネットとの接続したのは 20 年後の 1994 年であった。インターネットの発展と比べ、ブロックチェーンの発展が飛躍的であることは明らかにした。

0.1 En-Tan-Mo の建設理由

En-Tan-Mo は組織的、均衡的、効率的な価値観を作り世界に伝わることを目指している。したがって、En-Tan-Mo が創立から解決すべき問題は二つある。

SHD の完備性

分散システムにおいて一貫性 (Consistency)、可用性 (availability)、分断耐性 (Partitiontolerance) の三つの保証を提供することは不可能である。そのことはいわゆる CAP 定理とされた。サイト・ナカモトはナカモトコンセンサスを提出し、ブロックチェーンは確率的強一貫性を依頼し、一様合意問題 (Uniform consensus) を実現することができると明示した。

ブロックチェーンシステムには、CAP 定理との同じように、安全性 (Security)、高性能 (High-performance)、分散型 (Decentralization) という三つの要素のうち二つしか同時に満たすことができないの SHD 完備性の問題が存在している。

サイト・ナカモトの仮設では低性能の CPU を前提とし、安全性と分散型の共存を保ったが、完全に高性能を無視した。分散型コンセンサスとブロックチェーンの拡張性により、ビットコインは十分ごとに一つのブロックを作成し、1 秒ごとにわずか 7 つの取引しか処理できない。また、高性能の「ASIC マイニング」の開発に伴い、普通の CPU のコンピューティング・パワーの収益の確率はゼロに落ちる可能性がある。更に、その特別なマイニングは簡単に超線形な収益を収める一方、後に出現したマイニングプールは完全的に分散型を破壊した。したがって、参加者に対して今のビットコイン明らかに非平等なコミュニティとなった。

それにもかかわらず、マーリングプールは次第にコンピューティング・パワーを独占し、少数の参加者は 51% 以上のコンピューティング・パワー（決定権）を握る恐れがあり、安全性も確保することができない。ということは、ビットコインのブロックチェーンは SHD の均衡を失った。

ASIC マイニングの破壊的な影響を避けるため、イーサリアムは ASIC 耐性アリゴリズムを採用し、短時間内に安全性と分散型を維持した。しかし、はじめてのスマートコントラップ Cryptokities はイーサリアムシステムを完全に崩壊させ、その高性能の欠如を明らかにさせた。一方、POW コンセンサスを捨て POS あるいは DPOS コンセンサスのブロックチェーンシステム採用し、EOS のようにシステムの性能を大幅向上したが、分散型の根本的な意義を無視し、結局少数権益者がシステムの発展方向をコントロールした。それは本質的に既存の集権型システムとほぼ同じことである。

En-Tan-Mo は双対型の Kantorovich コンセンサスを採用し、マイナーコミュニティで選挙制度を取り、ステークホルダーとマイナーを分離し、それぞれの権益を保証する。安全性を保つと同時に効率を向上し、更に分散型の基本属性も維持することから SHD の完備性を満足する。

均衡価値伝達

インターネット時代は情報伝達の方式と理念が変わってくる。人々は簡便で低コストのインターネット技術を利用して情報を伝達し、効率が改善でき、コストがコントロールできる。それに新しい製品やサービスも手に入る。しかし、情報伝達と価値伝達の概念は違う。インターネッ

トにはペアツーペアのような価値伝達の機能がない。価値伝達は中央管理システムに依頼してレッジャーの機能を担う。それは情報伝達の複製性と区別し、価値伝達が所有権の唯一性を保証する必要があるからである。

ビットコインは分散型シェアレッジャー技術で分散型ブロックチェーンの依頼システムを建て、中央管理システムを依頼しないことになる。そうすると、ペアツーペアの価値伝達をサポートし、価値伝達と定価のルールを変える。マイニングプールが出現するため、ビットコインの価値伝達は傾き、一般参加者とマイニングマシンの所有者の取得する価値は対等ではなくなり、価値が急速にマイニングプールに集中していく。

イーサリアムは ASIC 抵抗的計算方法を通じ、「ガス」を消耗してブロックチェーンの資源を抑えるため、ある程度にマイニングマシンの価値累計のスピードを緩める可能である。これは消極的で短期的なやり方であり、ブロックチェーンの長期的な発展に悪い影響を与えるかもしれないと考えられる。バランスが取れるために、EOS を代表とする DPOS コンセンサスメカニズムはコンピューティング・パワーに独占していた POW を打ち破ってみたが、価値が大規模なステークホルダーによって導かれるため、中心化の程度は POW よりさらに高い。

ブロックチェーンとクリプトクロスの現在の発展状況により、価値は Pareto に似ている分散型の方式で少人数の手に集中している。En-Tan-Mo は現存する価値伝達の方式を変えてほしく、価値を開放式な回転を完成させ、ユーザーに均衡な価値伝達システムを提供する。En-Tan-Mo は個人がサービスの提供者であるとともに、購買者でもあると考えている。すなわち、買い手であると同時に売り手でもある。分散型ブロックチェーンの市場の核心は価格の調整メカニズムであり、それに価格が動態的均衡という方式で自発的に形成する。「En-Tan-Mo」は平均場ゲーム理論を利用し、価格の動態的な変動を研究する。コンピューティング・パワーまたは投票権は権益との関係は正比例の関係であるべきが、線形関係ではない。しかがって、権力の過度集中を抑え、最新世代のバランスの取れた価値インターネットを切り開き、ビジネスモデルと経済社会に大きな変革を生み出す。

0.2 En-Tan-Mo の建設者

En-Tan-Mo のデザイナーと建設者は世界一流の大学と



研究所からくる。最初にこのチームはフランスの数学者たちに組み立てられる。彼らはゲーム理論の成果をブロックチェーンに入れ、Entente、Transaction と Mole という三つの単語のエッセンスを抽出し、En-Tan-Mo と名付ける。その後、通信専門家、計算機専門家、経済学専門家と哲学学者

も直ちに En-Tan-Mo のチームに入る。アメリカのカリフォルニア工科大学、メリーランド大学、フランスのボアンカレ研究所の各領域の学者たちが含まれる。2011 年のノーベル経済学賞の受賞者トマス・サーボント教授、2015 年ノーベル物理学賞を受賞したアーサー・マクドナルド教授も前後このチームに入る。これから、En-Tan-Mo にある全ての理論デザインは二重の検証のような流れを採用する。まず、数学者はコンセンサスモデリングと数値シミュレーション実験を完成する。そして、計算機専門家と通信専門家によって厳しい標準で En-Tan-Mo プロジェクトの理論デザインに実際的な検証を行う。

En-Tan-Mo の目前の仕事の成果は理論と実験、ソフトとハンド、技術とビジネスなどのそれぞれのチームと担当者の間に密接な協力の賜物である。

Kantorovich コンセンサスメカニズムは数学、通信と計算機領域の専門家によって共にデザインして完成する。元のゴールドマンデータの科学者、およびブロックチェーン項目研究レポートのライターなどは「En-Tan-Mo 科学」のフレームシステムと ICO 方案をデザインした：元のグーグル、迅雷、百度などの一流のインターネット会社から来た豊富な経験があるソフトエンジニアがそのプロジェクトの生コードのデザインに力を入れる。

さらに重要なところ、このプロジェクトが正式的に公開されると、En-Tan-Mo の建設者主体はプロジェクトのチームメンバーのみならず、En-Tan-Mo の全てのユーザーになる。En-Tan-Mo は自発的な進化と全員参加を提唱し、全てのユーザーは自らのニーズに基づき、積極的に組み立て部品をアップロードし、デリバティブチェーンを発展する。En-Tan-Mo プロジェクトチームは自分自身のキャラクターを創始者と基礎施設建設の保護者だと定める。最大の努力を尽くし、このシステムに安全、安定、高効率的な技術サービスを提供する。その同時に、プロジェクトチームも科学者、エンジニアと En-Tan-Mo の理念を認めてくれる開発者をチームに入ってほしい、または各種の柔軟な方式で協力してほしい。

0.3 En-Tan-Mo 科学

En-Tan-Mo は簡単なブロックチェーンのプロジェクトではなく、豊富な内包がある科学的なシステムである。その中に完全な哲学思想、数学論証、経済学証明と広汎性の応用生態が含まれる。研究チームは資料のアセンブリーという形式で En-Tan-Mo に注意を払う人々にできる限り詳しく説明する。

第一章は En-Tan-Mo 世界である。En-Tan-Mo はサービス改善と価値革新でブロックチェーン 3.0 の世界を作り出す。En-Tan-Mo の世界は持続的改良、再構、市場創造に注目し、ビジネス体制を均衡させる本質の復帰と改造である。

第二章は En-Tan-Mo 哲学である。En-Tan-Mo は新しい価値伝達システムであり、価値がある物事を全てリンクしている。したがって、一般的に En-Tan-Mo の分散型ブロックチェーンの特徴には分権、開放、平等、参与、インタラクティブと進化などがある。

第三章は En-Tan-Mo 数学である。数学の角度から分散型ブロックチェーンの En-Tan-Mo を分析する。すでに完成された数学論証、プロジェクトの発展企画および研究に主に応用された数学工具などが含まれる。

第四章は En-Tan-Mo 経済学である。Stakhnov マイナーと Pareto マイニングプールは Kantorovich コンセンサスメカニズムで互いにサポートし、互いに励ます。En-Tan-Mo は技術の革新のみならず、ビジネスロジックの改革もある。

第五章は En-Tan-Mo 計算である。ソフトエンジニアは En-Tan-Mo のデータ構造、フローチャート、API インタフェースと全てのコードをプログラミングする。プログラムの形式で Kantorovich コンセンサスメカニズムの精緻と巧みをあらわす。

第六章は En-Tan-Mo 生態である。En-Tan-Mo のクロスチェーン技術には中心チェーン、デリバティブチェーンなどがある。それはブロックチェーンを分散した孤島から救ってきて、ブロックチェーンが外へ拡張と繋がりの架け橋になり、おびただしいアプリケーションが含まれるブロックチェーンの生態システムを構造する。

第七章は En-Tan-Mo 組織構造である。En-Tan-Mo コミュニティは En-Tan-Mo 基金会、IOEM と Emgo という三つの組織で構成される。基金会はユーザーコミュニティに全方位的な支持を提供し、En-Tan-Mo プロジェクトが順調に運営することを保証する；Emgo はプライバシーの安全研究とシステム開発の実体組織である；IOEM はビジネス企業を協力するパートナー組織である。

References:

- 【01】 S. Nakamoto. A Peer-to-Peer Electronic Cash System. www.bitcoin.org/bitcoin.pdf, 2009.
- 【02】 M. E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4):401-406, 1980.
- 【03】 V. Buterin. Long-range attacks: The serious problem with adaptive proof of Work.
<https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-withadaptive-proof-of-work/>, 2014.
- 【04】 V. Buterin. Proof of stake. <https://github.com/ethereum/wiki/wiki/Proof-of-StakeFAQ>, 2016.
- 【05】 G. Wood. Ethereum: A secure decentralised generalised transaction ledger. <http://gawood.com/Paper.pdf>.
- 【06】 M. Mainelli, C. von Gunten. Chain of a lifetime: How blockchain technology might transform personal insurance. Dec 2014. Z/Yen Group, Long Finance.
- 【07】 J.-P. Delahaye. Les blockchains. "Les big data à découvert". Editions du CNRS, Chapitre 15, 118, 2017.
- 【08】 J.-P. Delahaye. Le Bitcoin: première cryptomonnaie. "1024" Bulletin de la Société Informatique de France, n° 4, pp. 67-104, octobre 2014.
- 【09】 J.-P. Delahaye. Le Bitcoin: une monnaie révolutionnaire. Laboratoire d'Informatique Fondamentale de Lille, janvier 2014.
- 【10】 M. Perrin. Distributed Systems: Concurrency and Consistency. ISTE Press, Elsevier, 2017.

1.0 En-Tan-Mo 世界

1.1 En-Tan-Mo 世界の設計図

En-Tan-Mo は、哲学、数学、経済学、コンピューター・サイエンスなど、さまざまな分野間の連携による科学技術革新の国際化なプロジェクトである。

「En-Tan-Mo」世界の設計図：系統内のそれぞれの経糸は、それぞれの供給と需要を表すことである。各参加者は一つの自由の縛糸として、任意の経糸とかかわることができ、しかも自分で経糸を増やすこともできる。この経糸と縛糸の絡み合ったネットワークは、カオティク・シャフリング・メカニズムを通じ、自己適応と改善する。「En-Tan-Mo」の世界に各参加者の行動がこの世界を変えられるという職業の自由性は人々をより合理的、能動的、自律的にすることができる。

本物の分散型は集権と独占がないことを意味する。「En-Tan-Mo」は、平等と自由を目指し、不確実性とイノベーションを満ちり、しかも一般均衡の世界を創り出そうとしている。各参加者は自由市場のダイナミックスにのみ従い、インセンティブに理性的な反応をする。En-Tan-Mo 世界では、受動的に毎月の給与をうけることではなく、さまざまなプロジェクトに積極的に参加することから、直接に給与をもらえる。同時に、独自のプロジェクトを作成し供与を受け取ることもできる。各参加者は、価値移転の授与または受領することができ、そして取引価格は、公平性を確保するための動的均衡のプロセスによって決定される。

1.2 電子通貨の世界史

インターネットの技術の進展において、ブロックチェーン技術により、すべての集中化されたアプリケーションが時代遅れになる可能性がある。「トークン」はネット上の取引の速度とスケーラビリティを大幅に向かせることから、インターネットは情報共有だけでなく、価値移転のチャンネルにもなる。2009年、ビットコインは「電子黄金」のシステムを作り、ネット上でのグールドラッシュを起させた。2018年のはじめのところから、およそ30000PH/S計算力では一時間に6つのブロックを生成し、75枚のビットコインしかマイニングできなかった。Digiconomistというビットコインのエネルギー消費指標によると、現在ビットコインは年間39.45TWhのペースでエネルギーを利用し、20億ドルに相当する。1848～1851年アメリカのカリフォルニアで起きたゴールドラッシュによって、人口の急増で引き起こした食料不足、社会サービスの不足などの問題と同じように、2017年のビットコインゴールドラッシュも類似の問題をもたらした。数百年に渡って確立した金本位の貨幣制度は、わずか九年でビットコイン世界に確立した。

2013年ヴィタリック・ブテリンがイーサリアムと次世代の暗号化通貨と分散型アプリケーションプラットフォームを開発した。これにより、チーリング完全性を備えたスマートコンタクトシステムが作り出し、ETHは「電子ガソリン」の地位に達した。イーサリアムは、ユーザーにさまざ

まなモジュールを提供し、ユーザーがアプリケーションを開発するのコストを削減させると同時に、開発のスピードも向上させる。イーサリアムはEVM言語(Ethereum Virtual Machinecode)を通じ、アプリケーションを開発する。開発されたアプリケーションは、イーサリアムの核心であり、スマートコンタクトと呼ばれる。スマートコンタクトは、イーサリアムシステムの自動エージェントと同等である。ユーザーが契約のアドレスに取引を送信すると、契約が有効となる。次に、取引内の追加情報を従い、契約は独自なコードを実行し、最終的に結果を返す。この結果が契約のアドレス内で起きた別の取引である可能性もある。イーサリアム内の交易は、取引または命令のセグメントである。これによってイーサリアムが大量に使用することができるが、契約の莫大な費用により、イーサリアムの崩壊につながる可能性がある。目前イーサリアムで9万件を超える契約があり、しかも同様トークンアプリケーションであるゆえ、イーサリアムがスケーラブルでないハイウェイ、すべてのアプリケーションが自動車、ETHがガソリンにすれば、現在のイーサリアムは非常に混雑しかも高価なハイウェイのように、大規模のアプリケーションを載せることができない。

要するに、ビットコインは金本位経済を代表し、イーサリアムはエネルギー経済を代表する。これら異なる経済生態系から将来の発展の傾向を合理的に予測することができる。

ピラミッドの世界：「黄金と石油」が世界経済の礎石となるのは彼らの希少性によって決められることである。金本位経済の代わりにエネルギー経済が主導となるのは、エネルギーが人類にとって再生できない必要な消耗品からである。このエネルギー経済は世界をスーパー・ピラミッドとさせた。この世界ではエネルギー資源を有する少数の国がピラミッドのトップを占め、多くの資源のない国が安価な労働力を提供する第三世界の国となった。それと同様に、それぞれの国でもピラミッドも存在している。少数の大企業がピラミッドのトップを占め、中小企業または組織がこれらの大企業に安価なサービスを提供するピラミッドの底となった。さらに、企業と組織の内部でも小型のピラミッドがあり、労働者がピラミッドの底として低供与の労働力を提供する。世界はフランタル・ピラミッド構造のように、ピラミッドの底に行けば行くほど圧力が次第に増加する。最終的にピラミッドが崩壊により、経済危機が勃発した。しかし、新たなピラミッドが自発的に構築し、周期的の悪循環となった。

1.3 En-Tan-Mo の マス・イミグレーション

1) POW と DPOS の二重構造：独占と集中化を破る

POWの起源：現実世界では、合意は「労働費用」に依存し、労働力を凝らした商品は一般的な等価物となり、すなわち貨幣である。ブロックチェーンの世界では、合意は「計算力」に依存している。電子トークンは一定量の計算資源を費やすことによって得られる。したがって、POWシステムの導入は、初期の安定した均衡を維持することができ、トークン価値の

安定に基礎を築いた。ビットコインとイーサリアムも最初からPOWの安定な計算力に依頼し、一般的なコンセンサスを達したことである。

POWとDPOSの二重構造：POWシステムの公平性はマイニングツールによって壊された。技術の革新による公平性が失うことが何回も繰り返して起こった。そして、DPOSの高性能の計算力はその公平性をより一層ぶち壊した。公平的な計算力が失い、「過量トーカン供給」と「集中化」という問題もより早く浮かび上がる。POWとDPOSの二重構造は、単一のPOWまたはDPOSシステムの集中化の傾向を制限する可能性がある。この分散型のメカニズムは高性能を保つと同時に、安全性も保障することができる。ステークホルダーとマイナーもEn-Tan-Moに参加することができ、未来の発展の方向を決めることができる。

2)マイナーの間における協力と競争の関係は完璧な公正連盟法則である。

POWシステムでは、マイナーは多数の計算を行う必要があり、計算時間はマシンのハッシュ速度に依存する。互いに純粋な競争関係にある。これは、収益が低く、リソースの無駄に関わる。したがって、マイナーはマイニングプールとして構成する方法で連盟を形成したが、集中化の傾向も高まった。En-Tan-Moのコンセンサスでは、公正かつ合理的なインセンティブシステムが構築されるように、マイナー間の相互関係がゲーム理論によって分析される。

参加者のバリューチーンの新しいコンセプトを作り出すことができるには、協力的な競争関係だけであり、バリューチーンを使用して、すべての参加者の競争と協力の双方向関係を記述することができます。バリューチーンのアイディアは、En-Tan-Mo世界における競争と協力が同時に働くことを強調する。2つの組み合わせは、「競争」と「協力」という言葉の別個の意味ではなく、ダイナミックな関係を意味する。マイナー間の新しい関係は、インパクト、インテイマー、ビジョンという3つの言葉で定義される。これは、協力的で競争関係を確立した後にマイナーが生み出す具体的かつ効果的な結果、すなわち増加できる実際の生産性と価値をカバーしている。その成果は次の三つの方面から出てくる。まず、重複と廃棄を削減し、できる限り計算資源と電力を節約する：次は、互いの核心能力を利用し、ブロックチェーン拡張を加速する。最後に、外部ブロックチェーンの建設に参加する新たな機会を作り出す。

3)ダイナミックな需給と理性的な選択によるナッシュ均衡

En-Tan-Moに参加することは、デジタル世界で最高の同盟を選ぶことである。過去のマイニングプールでは、最適な制御理論が採用されることが多い。ある時に決められた最適性には、時間のたつと共にすべての参加者の収益が急激に削減される。それは最適の選択は必然的に最大の外部競争を引き起こし、最終的にはすべての競争相手の収益を低下させるであろう。トマス・サージェント教授の指導のもとで、トマス・サージェント教授の指導の下、En-Tan-Moは参加者の理性的な選択戦略に基づいてナッシュ平衡をリアルタイムで形成する動的な需給メカニズムを提供する合理予測理論理論を適用した。選択的な協力は、需給関係の実施形態である。価値は、コストと需要の有機的な組み合わせである。

En-Tan-Mo世界におけるPOWのコストの要素はPOSの需給関係と繋がることで、こういう最大な価値がある連盟法則が形成でき、相対的に低いボラティリティが得られる。

4)上に凸関数メカニズムは参加者の平等な権利を保証する

過去の世界では、同盟はより強力な協力者に向かう傾向があった。協力者が強ければ強いほど、弱い協力者よりも所得の割合が高くなる。結局のところ、強力な協力者でさえ、ピラミッドの崩壊に悩まされます。この超線形収入モデルは、最終的に比較的弱い協力者を傷つけ、ピラミッドの形成と崩壊につながったのはこのプロセスである。結局のところ、強力な協力者でさえピラミッドの崩壊に悩まされる。ロングテール効果に注意を払うEn-Tan-Moだけが比較的広範なパートナーに比較的大きな利益をもたらし、永続的な特性を持つ同盟メカニズムになり、強力な協力者でさえ初期の段階でいくつかの利点を放棄し、時間のたつとともにこれまで以上に大きな利益を得ることができるだろう。

En-Tan-Mo世界の基盤は、まさに"ユニコーンプール"を排除する貢献アルゴリズムの一種である。これは、この「完全等量」(線形化された計算能力関数)を凹型関数に変え、公正なスケールをより広い範囲のプレーヤーに向かってわずかに傾斜させることもできます。可能にする「機能」は、合理的な経済予測を通じて、より多くの観客に幅広いコンセンサスをもたらし、En-Tan-Moをもっとも公平かつ公正なブロックチェーンネットワークにさせる。

5)混沌としたシャフリング、シビル攻撃への抵抗と連合攻撃

ブロックチェーンのSHD理論では、分散型ブロックチェーンとセキュリティの間に避けられない問題がある：シビル攻撃(Sybil Attack)。シビル攻撃とは、複数の偽のアイデンティティを制御するために、ソーシャルネットワーク内の少数のノードの使用を指し、それによってこれらのアイデンティティを利用して、ネットワーク内の多数のノーマルノードを制御または影響を及ぼす。ブロックチェインノードの等価性により、単一のノードは複数のアイデンティティを持ち、システム内のほとんどのノードを制御することで冗長バックアップの効果を低減できます。コラボレーションでも同じ問題が生じるだろう。

En-Tan-Moの数学者は、複雑な不变集合の構造と分岐を研究するために、現代の力学系と位相幾何学理論を使用し、システム安定性と複雑な挙動制御法を導き出すことで、カオス理論に基づくエルゴード性と初期条件機密性の高い依存関係は、強力なカオスソート方法であり、ブロックアップロードシーケンスのための高度な擬似ランダムメカニズムを作成すると同時に、量子攻撃に対する最高レベルのセキュリティを備えている。

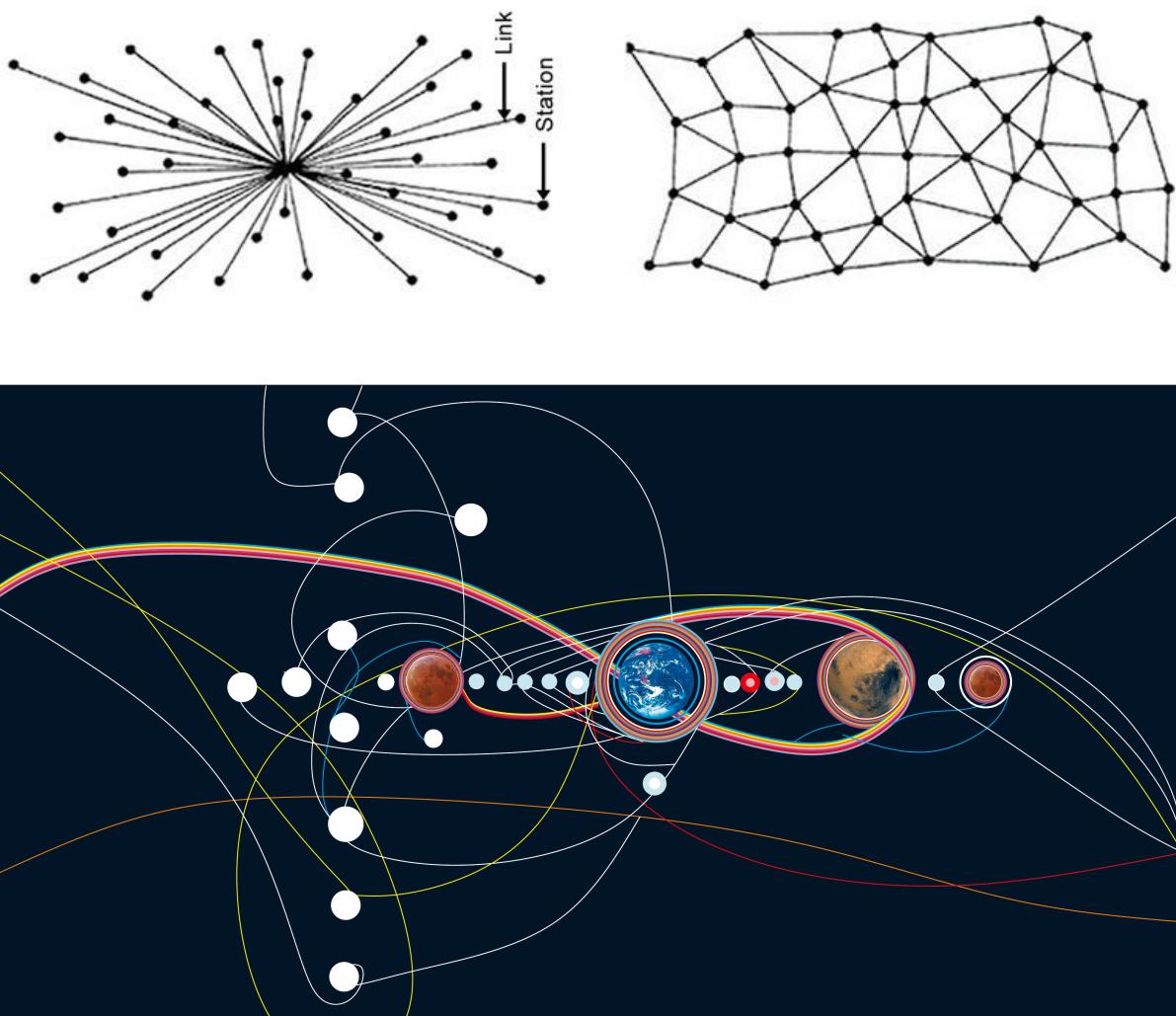
6)オープンコンポーネントライブラリとフレンドリーな開発者ロビーは自発的な進化と参加の方向性を決める

En-Tan-Moは、BaaS(サービスとしてのブロックチェーン)をコンセプトとし、マイクロサービスをベンチマークとして、自己進化するコンポーネントライブラリをコアとし、開発者コミュニティをエコロジー原動力として、資産とアプリケーションの無料転送を完了するための適応プラット

フォームを提供し、非ブロックチェーンのアプリケーションとデータチャネルに双方向の呼び出しを提供し、開発者にコンポーネントのアップロード、評価、報酬を提供し、一般ユーザー向けのアクセシビリティサービスコールのためのBaaS ゲートウェイを提供する。自発的な進化と参加を提倡するEn-Tan-Moは、すべてのユーザーが積極的にコンポーネントをアップロードし、それぞれのニーズに応じてデリバリーチェーンを開発することを歓迎する。

En-Tan-Moの世界では、チェーンやブロックチェーン、

非ブロックチェーンの間に情報島が形成されている。アプリケーションのサイドチェーンはメインチェーンとは独立しており、各需要と供給関係もネットワークに存在する独立したチェーンになる。これは無限に拡張してきたネットワークであり、価値の両側に供給と需要の両立を図っている。誰もが供給と需要の両面を自由に切り替えて、異なるサービスチェーン間で切り替える。サービスの提供とサービスの受け取り、効率的で消費の追加コストなしで、チェーン間のチェーン転送の価値を自由に使用できる。

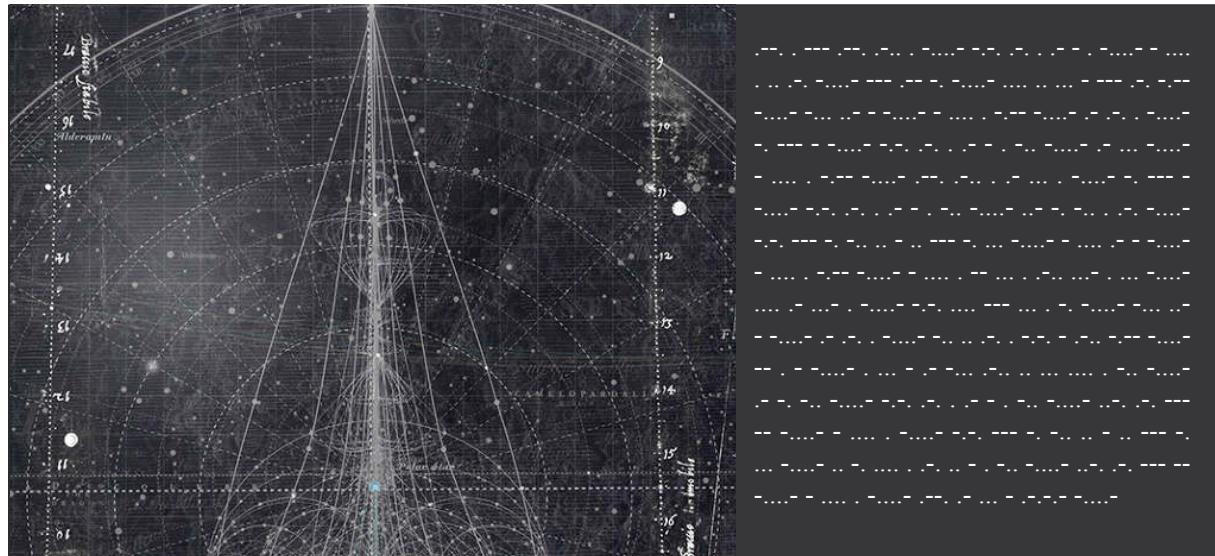


“Hello ! En-Tan-Mo World !” 加盟部隊は長期的な最善の利益をもたらす計算能力ベアリング・コンポーネントの一種である混在通貨コンピューティング・アライアンスに参加し、すべてのノードが需給関係に応じて自由かつ均等に取引を選択する。バランスのとれた利益を得る。

En-Tan-Mo自体は、高頻度を耐え、高トラフィックを運ぶトーカン取引所であり、同盟マイニングプールであり、DAPP アプリケーションプラットフォームでもある。カオスソートメカニズムは自然にゲームフィールドを形成する。En-Tan-Moは、最高の開発者コミュニティであり、ブロックチェーンアプリケーションコンポーネントホスティングプラットフォームでもある。ここにちは！ バランスと平等があらわれた新しい世界へようこそ。

2.0 En-Tan-Mo 哲学

En-Tan-Mo は現実世界の中の価値生産及び交換関係をトポロジカル同型写像を通して抽象空間において再建し、深い哲学思想を反映していた。分散型の思想が骨として En-Tan-Mo を構築し、古代ギリシャのプロタゴラスの「人は万物の尺度である」から抽出した「ユビキタス」概念はその中核である。というのは、分散型 En-Tan-Mo ブロックチェーンが平等な世界であり、複雑系統と多変量構造、コンセンサスと価値、動的平衡と分権、自己進化と開放性はその特徴である。



2.1 複雑系と多変量構造：記号価値と象徴交換

多変量構造は記号コードから解釈された後、再び En-Tan-Mo 複雑系統にリリースし、各領域の経路を複雑なネットワークシステムと転換させる。記号コードは次第に相関の目標と人へのコントロールから離脱した。En-Tan-Mo 複雑系統が使用した記号コードを多変量構造に返還したが、返還した記号コードは電流フロー (current flow) の象徴を解放し、元記号コードと差別を生じられ、En-Tan-Mo 相互インクルージョン法則に従っている。En-Tan-Mo の多変量構造は効率的オーバーフローし、制約を受けない複雑系統に介入し、En-Tan-Mo 以外のプロセスを定義した。定義によって構造を所有するほか、意義的な過剰も存在している。複雑系統は En-Tan-Mo のパフォーマンスと統合され、協調の共変に繋がる。数多くのリズムと主題、共に動くことから、空間形式化の記号価値と象徴交換を生成した。

2.2 コンセンサスと価値：“千の台地”

“千の台地”は伝統的なイデオロギーモードの中の各種の層、コード、超越的な面、テクスチャ区間などと絡み合っている。En-Tan-Mo 「台地」の平等互恵の関係において、多様性と異質性の連結は各チェーンノード間の通信のクロスオーバーになり、コンセンサスが浮上し、価値伝達が可能となった。「千の台地」はセグメントの方向に直接に影響を与える要素であり、時間に限らず、思想と人生の

根源を辿る能力の再現を意味している。つまり、「千の台地」は我々を最初の状態に戻り、初期の限界的な方向性がどのように起こったかを経験することが可能となり、それによっていくらかの限界感度が生じる。

ノードの平等は、En-Tan-Mo の進化する表面に分布し、反復性の通路の構造に分配している。その目的は対等な事実状態を描写し、En-Tan-Mo の主体間のバランスを維持し、あるいは既存な無意識状態を探索することである。セグメント抽出の平等はある完全な平衡を模倣するように設計し、完全な実例として与えられ、この平衡模倣は En-Tan-Mo 構造またはサポート性の等軸に基づいた。

2.3 動的平衡と分権：“ペルシア人の手紙”

En-Tan-Mo 世界の同時性の発達で形成した平衡は類似なスピードと共有段階の序列がある。主体は部分性の客体に関連しなく、差異性のスピードに関連する。En-Tan-Mo の動的平衡は予めに存在する主体またはガイドされて存在する主体を離れる。客体がなく、主体もなく、ある自然な現実とある客体の中にあり、統一性が絶えず障害にあうが、一般化された En-Tan-Mo の中に、新しい統一性は分権と開放の間にある補足を取得し、主体が二重化にならない。

中心化のパワーは自由構造システムの問題であり、常に一番大切な要素に付き纏う。En-Tan-Mo の分権は自律的な分

散型ブロックチェーンである。自律は非完全の自由に等しいわけではなく、ただ中心化より更に自由な形態だけである。「人間はフリーで生まれたが、どこでもチェーンに囲まれる」。このような矛盾は形而上学の不可能を証明した。

2.4 自発的な進化と開放性：“作者の死”

主体の脱構築と次第に欠席する背景に、構造自体は総体になり、個体が総体との相互関係に自体の意義と在り方を定義する。したがって、構造自体は個体と独立した存在として、現実に行われた同形写像を歴史記録と真正性の証拠とする。明らかなところ、静態的な構造は歴史構造の進化および現実世界の構造の複雑さとの間に絶えずに矛盾を生み出す。Levi-Strauss は自分の著書『原始社会』のあとがきに構造と進化の関係の複雑さ、およびその複雑さが人類社会政治経済学の分析における重要性をはっきりと述べる。En-Tan-Mo の中にこの問題を解決する方法はデザインに自発的な進化のロジックをはめ込むことである。そうすると、

分散型ブロックチェーンと安定な構造を前提にし、このシステムは現実との共時性とマッピングの合理性を保障する

作者の死は作者が創作の主体として作品に独占に支配できなく、現代の創作に主体の身分がもう消えてなくなる。したがって、時間、空間と起源の概念を改めて理解しなければならない。En-Tan-Mo の建設過程のそれ自体は創作であり、その創作の目的は新しい空間ディメンションの中に自由意志と秩序構造の統合を実現するためである。この創作は自体のシステムの中に最初の歴史を書き、または歴史の規則を書く。それに、真正性は歴史構造についてのコンセンサスで定義される。任意のある主体にとって、恣意的に規則を制定するまたは歴史を変えることはパワーにある抑えられない誘惑をもたらす。そのため、En-Tan-Mo は創作主体が脱構築される可能性を意識するのみならず、本的な分散型ブロックチェーンで公平な体系を作り出すために、この脱構築のプロセスを積極的に実現する。

LA MORT DE L'AUTEUR

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

*

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

LA MORT DE L'AUTEUR

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

*

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

*

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

3.0 En-Tan-Mo 数学

本節は数学の角度から切り出し、分散型化のブロックチェーンシステムをめぐって研究を展開し、今までの研究結果と項目発展の方向と計画を紹介する一方、項目開発中で使った数学理論も説明する。そして En-Tan-Mo を開発する理由を述べる。

3.1 分散型化の安全性問題

2009年、サイト・ナカモトが『ピア・ツーピア電子通貨システム』という論文を投稿した。その論文ではサイト・ナカモトはビットコインブロックチェーン思想の中核数学モデリングと理論を説明し、ポアソン分布という理論を用いてP2Pネットワークには攻撃者による偽造は計算論的にほとんど不可能であると証明し、分散型台帳技術への信頼問題いわゆるビザンチン将軍問題を解決した。しかし、今日に至って、状況の変化と伴いサイト・ナカモト理論の一部の重要な仮設も変化し、ビットコインブロックチェーンに関する結論が今の状況とふさわしいことが明らかにした。

| 信頼問題（コンセンサス アルゴリズム）

サイト・ナカモトはブロックチェーンに詐欺行為の発生の確率について次のように述べた。

一つの取引が完成した後、攻撃者は直ちに捏造のチェーンをアップロードし、そしてそ \pm 時、攻撃者のチェーンの長さはポアソン分布に満足することができる。それを前提とし、サイト・ナカモトは「ギャンブルー破産問題」の理論を使って攻撃者のチェーンが、より善良なチェーンに追いつく確率を計算した。だが ASIC マイニングとマイニングプールの出現は以上の仮設を不成立とさせ、攻撃者のチェーンの長さもポアソン分布に満足できなくなる。計算能力を活かして新たなブロックを得ることは、本質的に Binomial ランダムウォーク問題と言えよう。

p = Probability an honest node finds the next block; p = 善良なノードが先にブロックを生成する確率

q = probability the attacker finds the next block; q = 攻撃者が先にブロックを生成する確率 $p+q=1$

取引後、善良のチェーンは N 個のブロックを生成する時、攻撃者の生成するブロックが X_n とする。その問題をギャンブルー・ポイント (Problem of Points) 問題として扱い、つまり攻撃者のブロックを生成する成功率は q 、善良者のブロックを生成する失敗率は $p=1-q$ とし、 $P\{X_n=k\}$ は n 回の失敗前に k 回の成功の確率であり、負の二項分布に満足する：

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

以下の条件を満足すれば、

1. 善良者が生成したブロックの数量 n のほうが多い。

2. 一つの有限常数 λ が存在し λ , $n \frac{q}{p} \rightarrow \lambda$ $l_n = n \frac{q}{p}$

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

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

以上の式で計算すると、確率変数 X_n は λ のポアソン分

布に接近していることが明らかにした：

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

しかしマイニングプールが存在すると、上述の条件 (2) に満足できなくなるため、サイト・ナカモトの確率推計は間違ったことが明示された。したがって、サイト・ナカモトの数学モデリングは精確にビットコインのリスクマネジメントをコントロールすることができなくなった。その上、攻撃者は大量の計算資源を有すれば、ノンスムースコントロール (nonsmooth control) の方法を用いて、計算能力を調節し、（例えは攻撃する時突然計算能力を向上する）、攻撃者の成功の確率はサイト・ナカモトの推測より遥かに超えた。

それに、ブルーフ・オブ・ステークを利用し、 q の数値をコントロールすると同時に、ブロックの生成スピードを促進することは、攻撃者の成功率を抑えることができ、その確率より精確に推計できる。

善良のチェーンに Z 個のブロックが増加すると、善良のチェーンと攻撃者のチェーンの差は $Z-X_n$ であり、ギャンブルー破産問題の方法を用いて、その差は $Z-K$ になると、攻撃者のチェーンの長さはある時点善良のチェーンの長さを超える確率は以下のように：

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

ここで、攻撃者の成功の確率はおよそ $P(z)$ であり、以下の式で計算する：

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

C. Grunspun と R.-P. Marco によると、攻撃者が計算資源は 51% 以下を把握すれば、成功する可能性が大きいことであった。要するに、単純な POW の安全性は予想通り低かった。そのため、弊社は POW と DPOS の結合の双対型プロトコルを提出し、マイナー選挙制度を通して制約と監視を実現し、安全性を向上する。

3.2 ナッシュ均衡とコンセンサスアルゴリズム

“En-Tan-Mo” はコンセンサスアルゴリズムをデザインする際、ナッシュ均衡の思想を利用した。ここでは、まずナッシュ均衡の基本的な定義を紹介し、そしていかにそれをコンセンサスデザインの中に利用するのかを簡単に説明する。

仮に S_1, S_2, \dots, S_N は緊密な距離空間で、 J_1, \dots, J_N は $\prod_{i=1}^N S_i$ 定義された連続関数だとすれば $P(S_i)$ は、 S_i の上に定義された全ての Borel 確率測度によって構成された緊密な距離空間になる。

定義：混合戦略のゲームにあるナッシュ均衡はこの

戦略グループ $(\pi_1, \dots, \pi_N) \in \Pi_{i=1}^N P(S_i)$ を現し、それで恣意的な $i = 1, 2, \dots, n$,

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

$$\text{その中に } J_i(\pi_1, \dots, \pi_N) = \int_{S_1 \times \dots \times S_N} J_i(s_1, \dots, s_N) d\pi_1(s_1) \dots d\pi_N(s_N)。$$

定理： ((J. Nash, 1950), (Glicksberg, 1952)) は以上の仮な条件のもとで、混合戦略に対して少なくとも一つの不動点がある。

目前、ビットコインなどのブロックチェーンシステムへの理論分析の文献が次第に増えている。ナッシュ均衡は、参加者が一方的に策略を変え最大利益を得ることができない戦略の集合である。それを確保するため、分散型システムが不可欠で S_1, S_2, \dots, S_N システムの中に、「罰」 J_1, \dots, J_N とを通して順序を維持するコントローラは存在しない。

問題となるのは、ナッシュ均衡の戦略が必ずしも効率的ではないということである。ビットコインシステムでは、ナッシュ均衡が非常に無駄であると言えるのであろう。これは、ビットコインに対して唯一のセキュリティメカニズムは計算力である。マイナーは自由にシステムを出入りすることができる。これは純粋に非協力的なゲームであり、勝利を決める唯一の要因はハッシュレートである。この POW メカニズムの設計は、マイナーに誠実にマイニングする「最長のチェーンルール」のようなコンセンサスに従わせることに成功した。一方、マイナーは常に利益を最大化するため、マイニングツールをアップグレードする。そして、計算力の競争が次第に激しくなることにより、資源の独占や資源の浪費が生じる可能性がある。経済学では、これを「コモンズの悲劇」と呼ばれ、そしてアルゴリズムゲーム理論では、「無秩序の代償」と呼ばれた。

この問題は、メカニズムを通して設計した「経済学のエンジニアリング面」でしか解決できない。メカニズムの設計は、ゲーム理論の逆問題とも呼ばれる。メカニズムに基づいた結果を研究するのではなく、望ましい結果につながる適切なメカニズムを模索することである。ブロックチェーンシステムは、メカニズム設計理論を使用するための完璧な領域である。設計者はプロトコルの設計し、さらに規則の設定にも自由がある。このメカニズムは、戦略と結果をつながる過程と視ることができる。ナッシュ均衡がメカニズム設計にとって非常に重要である理由は、プレーヤーが理性的かつ結果を予測することができれば、ナッシュ均衡戦略を予測することもできるということである。そうでなければ、一部の参加者はほかの戦略を採用し、コンセンサスに従わない可能性がある。ブロックチェーンシステムでは、この問題が次第に深刻になっている。制約をおく中心的な権限がないため、参加者はインセンティブを感じると新たな戦略を選択しコンセンサスを従わなくなる。ETM システムでは、POW と DPOS を結合する二重メカニズムを利用し、分散型を前提にナッシュ均衡の効率性を実現する。将来の計画では、ETM メカニズムは Kantorovich タイプと Vickery オークションのアプリケーションを導入する予定がある。

3.3 投票制度にある権益調整モデル

目前多くのブロックシステムに権益所有量証明 (DPOS)

が採用され、単純的な計算能力証明 (POW) と比べ、資源を節約することとブロックを生み出すスピードが早いという優位がある。この理論の仮説はあるブロックシステムに割と多いトークンを占有する人が信頼されるということである。

「En-Tan-Mo」の考えでは、目前のブロックと暗号通貨の発展現状に基づき、権益は Pareto 分布に似ているある方式で少数人の手に集中する。選挙権の過度集中を避けるために、投票権と権益との間に正比例な関係であるべき、線形関係ではない。ここではこちらの方案について簡単に説明しておく。

仮にシステムに n 個のノードがあり、あるノード i が投票を始める時占有した権益は総権益の比率は α_i , $\sum_{i=1}^N \alpha_i = 1$, だとすれば、厳しく上に凸な関数写像 f , $\frac{\partial f(\alpha_i)}{\partial \alpha_i} > 0$, $\frac{\partial^2 f(\alpha_i)}{\partial \alpha_i^2} < 0$, を定義し、このノードにある票数が総票数での比列を $B_i = \frac{f(\alpha_i)}{\sum_{i=1}^N f(\alpha_i)}$ と規定すると、明らかに $\sum_{i=1}^N B_i = 1$ 。

上に凸な関数の簡単な性質 $f(\sum \alpha_i) < \sum f(\alpha_i)$ により、二つの相対的な権益は別々に α_i , α_j のノードになる（一般性あり、仮に $\alpha_i > \alpha_j$:

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

この新しいコンセンサスの仕組みの下で、大株主が複数の口座を管理することによって投票に利点を得ようとする可能性がある。これは、サイバーセキュリティにおけるシビル攻撃と呼ばれている。

ゲーム理論の角度からみれば、これは理性的な行為ではなく、その論証が以下に挙げられる。

参加者の最終の動機付けは最大利益を獲得することである。すなわち、En-Tan-Mo システムの中からもより多くのトークンを得ることである。投票権は手段であり、目的ではない。

ETM トランザクションメカニズムでは、各投票は取引後に行われる。そしてこの取引は一定の手数料がかかる。したがって、(シビル攻撃) の攻撃者にとって、これは余分なコストを意味する。攻撃者は、より多くの票を得るために大量の無意味な取引をしなければならないので、取引の手数料も次第に増える。

En-Tan-Mo は、ゲーム理論とトマス・サージェントの合理的期待 (Rational Expectation) 理論に基づいている。本団体の数学的な研究は、シビル攻撃によって得られた効用は、余分な取引手数料の費用をカバーすることができないことを示している。したがって、シルビの攻撃は合理的な選択ではない。

3.4 クアティック シャフリン (chaotic shuffling)

En-Tan-Mo プロジェクトのコンセンサス設計はセキュリティを最も重要な目的にし、非常に高い標準を設定した。DPOS システムの複数の SCV マイナーが協力しカンニング

する問題に対し、コンセンサス層はクアティックシャフリルを採用しこれを解決する。

カオス：力学系中の力学行為は初期値に対する極端に感度する。

簡単に言えば、カオスとは、初期値に対する最小の変動がマッピング結果に非常に大きな変化をもたらし、予測プロセスにおいて不確実性を招く可能性があるということを指す。しかし、この不確実性は我々にとって必要とするものである。ブロックをアップロードする過程において複数のマイナーが強力し不正行為をしたい場合、偽の情報を含むブロックを持続的に確認する必要がある。この目的を達するために、彼らはできるだけ早く異なるマイナーのアップロードしたブロックの順序を知り、調整するのに十分な時間が必要である。カオス的シャフリンとは、最初にマイナーのアップロードの順番が決められないということであるが、コンセンサス層設計では、アップロードに成功した各ブロックから特定な情報を抽出し、複数の計算を通して次のマイナーの番号を得る。したがって、ブロックをアップロードしたマイナーの身分最後までわからない。

Hénon 型の多次元写像を定義するには、次の動的関数を使用する。

$$\begin{aligned}x(n+1) &= ay(n) + by(n)^2 \\y(n+1) &= cx(n) + dy(n) + dx(n)z(n) \\z(n+1) &= x(n)^2 + ey(n)x(n)\end{aligned}$$

256 ビットバイナリとそれに対応する 10 進数はそれぞれ I と D とし、マッピング関係を次のように記述することができる。

(1) Matlab の中の一様分布関数 Randi を使用し、反復の乱数を生成する。 $N_i (3 \leq N_i \leq 13)$

(2) N 1 時刻のシステム出力を利用し、初期値 X0 のランダムを生成する (idxo)

$$\begin{aligned}s &= x(N_1) + y(N_1) + z(N_1) \\idxo &= \text{mod}(s, 3) + 1\end{aligned}$$

(3) 他の二つの次元を使用し二つの乱数 (seg1, seg2) を生成する。

たとえば：

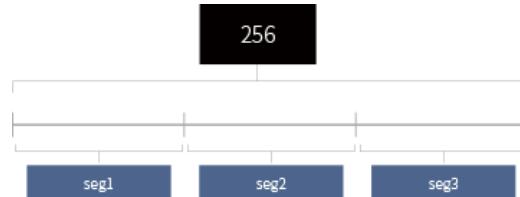
$idxo = 2$ (すなわち、X 次元から i を初期値として選択する)、次に、

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

(4) i を 32 個の 8 ビットブロックとして扱い、seg1 と seg2 を使って i を三つのブロックに分割する。

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

そして、 $seg3 = 256 - seg1 - seg2$,slit 関数に対応する分割ルール以下の通りである。



(5) I1, I2, I3 をそれぞれ使用し、「システムパラメータスケーリング値」(var-par)、「システム反復番号」(Val-N)、

及び「システム初期値スケーリング値」(Val-init) を生成する。

(6) Hyperchaotic システムを初期化して計算を実行するには、val-par, val-N, val-init を使用する。idxo 次元の信号を出力として選択し、交換操作によって 1 – 101 の整数を生成し、すなわち D である。

クアティックマッピングは決定的なものであるため、各ステップですべてのマイナーが独立な計算を通して一致な結果を得た。分散型を維持しながら、システムは安定性とセキュリティを達成することができる。

3.5 Kantorovich 双対、最適な運輸と分散型ブロックチェーン

“En-Tan-Mo” ブロックのコンセンサスは Kantorovich コンセンサスだと呼ばれ、ソ連の数学者 Kantorovich が最適な運輸領域での仕事、特に 1937 年に出した Kantorovich 双対定理から出てきた。この定理は線形規則と最適運輸に早期的な創始的結果の一つである。これから、この理論およびそれを分散型ブロックチェーンのブロックチェーンシステムに応用される可能性を紹介する。

仮に X, Y を二つの集合とし（または現実の区域に対応する）、 X 所にある物質を Y 所に運ぶ。仮に $c(x, y)$ は全ての対応する点 X から Y までの運輸コスト（または密度関数）で、 γ は区域 $X \times Y$ に物質の確率分布で、 μ と ν は別に区域 X, Y の周辺分布だとすれば、 $\int_{X \times Y} c(x, y) d\gamma(x, y)$

のような形式でからまでの整体運輸コストが表せる。Kantorovich 双対定理が指摘した：

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

その中に \inf と \sup はそれぞれ上限と下限を表す。ここで複雑な詳細な計算を略し、ただ大体な解釈を出す：「En-Tan-Mo」には分散型ブロックチェーンの取引システムがあり、 $\psi(y)$ は y 所に売り出された値段を表す； $\varphi(x)$ は x 所で購入した値段を表す。それで、

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

はこの取引システムの最終的な利益を表す。双対定理の結果の表示のように、制約条件 $\psi(y) - \varphi(x) \leq c(x, y)$ で、整体の運輸コストを最小化する策略は具合に利益最大化の策略に応対する。

この定理は資源運輸と配置の改良について、合理的な価格体系を打ち立てることの重要性を指摘する。この理論が経済学から説明できる可能性がある

ため、Kantorovich によって出したこの理論がソ連学術界に長期的に批判を受けていた。ご本人も逮捕されたことがある。

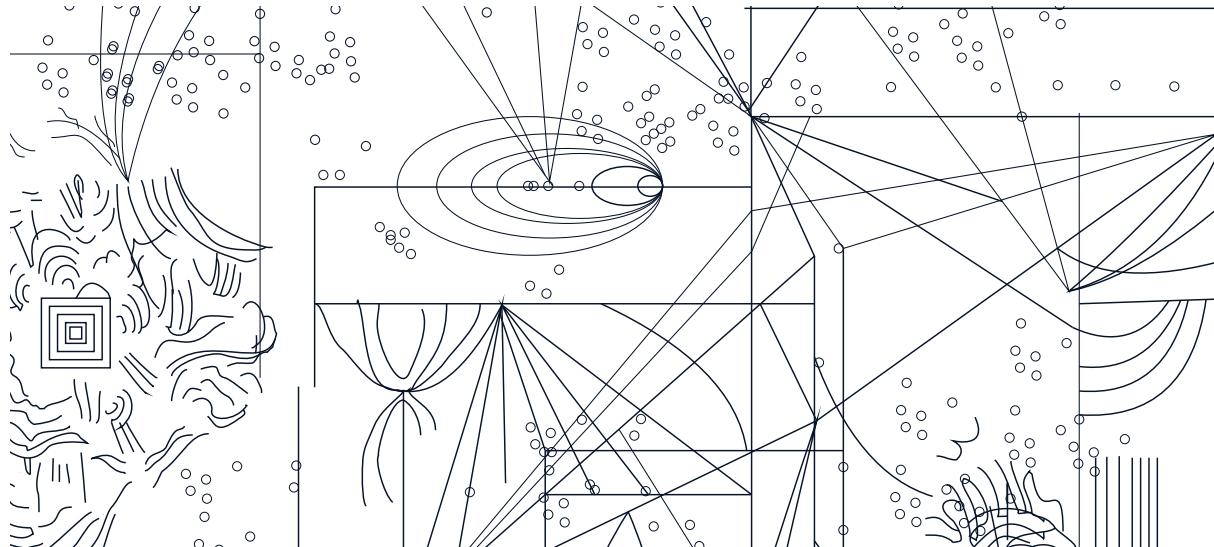
ブロックの技術のレベルから見ると、最適な運輸が対応したのは価値伝達の最適な策略と組み合わせる方式である “En-Tan-Mo” の考えでは、合理的な方式は分散型ブロックチェーンのシステムを採用し、整っている信用機制を打ち立てる。全てのノードは自分自身がマスターした取引の情報によって策略を作り出し、透明的で公開された市場を形成する。その上で、市場自身の調整の仕組みで動態均衡の価格システムを形成する。これこそ「En-Tan-Mo」が価値伝達を実現してほしい方式である。

3.6 分散型ブロックチェーンのシステムに

“En-Tan-Mo” のシステムの中に、全ての個体はサービスの提供者である同時に購入者でもある。即ち、買い手である同時に売り手でもある。分散型ブロックチェーンの市場核心は価格調節の仕組みにあり、価格はある動態均衡のような方式で自発的に形成する。「En-Tan-Mo」は平均場ゲーム理論の思想を利用して分散型ブロックチェーンのシステムの中における動態価格の形成問題を研究する。このモデルは Lasry-Lions 価格形成モデルとも呼ばれる。

仮に価格の選好には一定のランダム性がある。密度関数 f_B , f_V でそれぞれ買い手と売り手の数量を表す。 t が時間を表し、 x が価格を表す。例えば $f_B(x,t)$ は時間が t であり、価格が x である時の買い手の数量。 $p(t)$ を動態均衡のプロセスに出てきた価格を表す。 a は取引の費用を表す。以下の平均場方程式が出てくる：

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



References:

- 【11】 R. Perez-Marco. Bitcoin and Decentralized Trust Protocols. Newsletter of the European Math. Soc., 100 p.32, 2016.
- 【12】 W. Feller. An introduction of probability theory and its applications. Vol.1, 3rd ed. John Wiley& Sons, 1957.
- 【13】 Л.В. Канторович, Математические методы организации планирования производства. Издание Ленинградского государственного университета, 1939.
- 【14】 С.М. Меньшиков. Актуальность экономической модели Л. В. Канторовича в наше время. Зап. научн. сем. ПОМИ, 2004, том 312, 30–46.
- 【15】 M. Doob, Kantorovich. On Optimal Planning and Prices. Science & Society, Vol. 31, No. 2 (Spring, 1967), pp. 186-202.
- 【16】 C. Grunspan, R. Pérez-Marco. Double spend races. arXiv:1702.02867v2 [cs.CR].
- 【17】 R. Perez-Marco. A simple dynamical model leading to Pareto wealth distribution and stability. arXiv:1409.4857, 2014.
- 【18】 J. P. Aubin, I. Ekeland. Applied Nonlinear Analysis. Wiley-Interscience, 1984.
- 【19】 J. P. Aubin. Optima and Equilibria. Springer-Verlag, 1998.
- 【20】 Notes on Mean Field Games, from Pierre-Louis Lions' lectures at Collège de France.
- 【21】 J.-M. Lasry, P.-L.Lions. Mean field games. Jpn. J. Math., 2 (2007), No. 1, 229-260.
- 【22】 M. Kamgarpour, H. Tembine. A Bayesian Mean Field Game Approach to Supply Demand Analysis of the Smart Grid. 2013 First International Black Sea Conference on Communications and Networking.
- 【23】 T. J. Sargent, Lars Ljungqvist. Recursive Macroeconomic Theory. MIT Press, 2000.

その中に、乗法の因子 λ を用いて時間 t の取引の数量を表す。 σ はランダム性を描き、 δ はある delta 関数を表す。最初の条件を以下のように示す：

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

この方程式が一次元熱伝導方程式と似ているが、その難しさは自由境界問題にある。自由境界問題は現代偏微分方程式の理論における核心な問題であり、物理学の相変化問題から起源し、今多くの領域に応用されている。

分散型ブロックチェーンのシステムにおいて、レジャーを採用するため、ノードがマスターした取引の情報を通して動態的に自身の行為を調節する。したがって、実際はあるベイズ型フィードバックコントロール問題だと見える。即ち参与者は事後確率でリアルタイムで策略を調整することで、できる限り自分の収益を増やす。「En-Tan-Mo」はフォローの仕事にベイズコントロールシステムをつけた動態価格の方程モデルを引用し、ブロックチェーン技術、人工知能と深い学習技術をしっかりと結びつく。

4.0 En-Tan-Mo 経済学

ブロックチェーンと相關技術の変化は近代経済に革命的な変革をもたらす。産業革命はビジネスモードが階層制と金融資本主義によって支配されていた世界でおこった。ブロックチェーンの革命は、人間資本主義と個人の自主性によって主導される経済システムを目撃するであろう。

それがどのように展開するかはまだ不明であるが、起業家とイノベーターはいつものように試行錯誤を通して不確実性を探求する。しかし、この革命的な変化が起こる前に、膨大な富が創造され破壊されることが確実な事実である。

En-Tan-Mo の貢献は、この革命が起こる時に、バランスの取れた価値伝達モデルを提供し、人々にその革命の意義をより明確に了解することができるということである。

4.1 En-Tan-Mo 暗号経済学

信用関係はビジネスにおいて特に金融システムにおいて一般的である。このような関係の根底にあるのは、不確実性を排除し、取引コストを最小限に抑えることである。En-Tan-Mo は、トランザクション情報フローを完全に安全することを可能にする。人と人の信頼関係を人と技術への信頼関係と転換することにより、不確実性がなくなった。その伝統的な信頼関係の強化によって、取引コストを全体的に削減される。

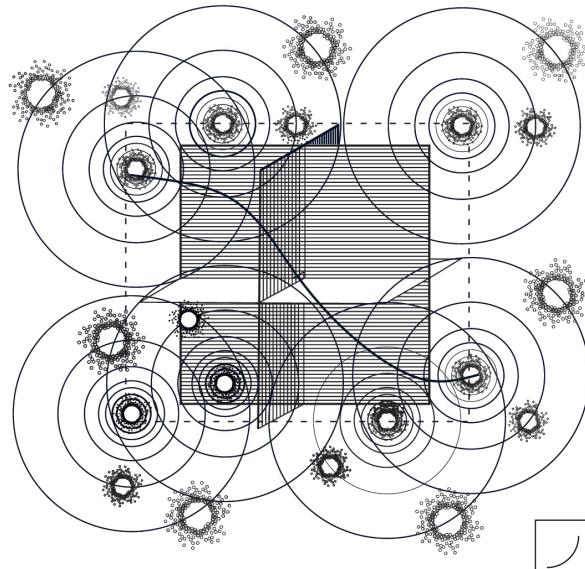
現在のブロックチェーン技術は全体的に効率が低いことに加え、ほかのマイナス影響をもたらした。ブロックチェーンのアプリは取引速度（ビットコインでは7つ／秒間）、プライバシー、財産の可逆性（Mt. Gox はバックキングされる）などの問題によって制約を受ける。

En-Tan-Mo は全体的な効率性を向上させる一方、安定な運用システムを提供し、相関の仕組みを安定させ、利益分配メカニズムも確定させる。En-Tan-Mo を利用する時、決定者の利益にマイナス影響をもたらすことがない。

En-Tan-Mo 暗号経済学の研究対象は安全な暗号と自動信頼を備えた台帳には制度の重要性である。古典派と新古典派経済学者は、希少資源の生産と分配及びこれらのプロセスの基礎となる要素を研究している。En-Tan-Mo 暗号経済学は、プロトコルを対象とした経済学である。プロトコル（法律、言語、財産権、社会規範、イデオロギーなど）は分散したグループと投機的な人との協力を可能にする。経済だけでなく、社会的及び政治的な取引においても有用である。

En-Tan-Mo 暗号経済学は、ブロックチェーンとその派生したアプリが組み込まれている経済原理と理論を研究している。経済学とその一派の制度派経済学は同じコミュニケーションと交換システムである。しかし、制度派経済学はプロトコルに着目することではなく、台帳、すなわちプロトコルに基づいたデータに重点をおいている。

En-Tan-Mo 経済学は次の内容に関心を寄せている。それは価値伝達へのプロトコルの規制、この価値に関わる社会的、政治的及び経済的な制度の発展。En-Tan-Mo が社交面で価値伝達の仕組みをどのように変えることができるのかのことである。



4.2 ナッシュ均衡

ETM システムの一つの重要な優位は設計の過程においてゲーム理論をメカリズム設計のツールとして積極的に応用している。既に存在するブロックチェーンシステム、たとえばビットコインシステムの中に存在した効率低下の問題を「無秩序の代償」と呼ばれた。En-Tan-Mo の中に、En-Tan-Mo の数学家は二重メカリズムを設計し、すべての参加者はマイナーまたは投票者としてブロックチェーンの建設に参加することができ、そしてバランスの取れた報酬を得ることができる。さらにすべてのユーザーは簡単しかも非常に有効なコンセンサスプロトコルに規制され、それによって理性のユーザー戦略集合がナッシュ均衡に達することができる。

コンセンサスメカニズム及びそのアルゴリズムは En-Tan-Mo が分散型を形成する基盤である。その本質的な目

的は「中央管理者がいない管理体制」と「分散型の自己適応コントロール」を達成することである。En-Tan-Mo コンセンサスメカニズムのアルゴリズムにおける最も重要な基礎はノーベル経済学賞の受賞者ジョン・ナッシュが提出したナッシュ均衡である。それは、プレイヤー全員がお互いに最適な戦略を選択し、これ以上自らの戦略を変更する動機がない安定な状態になるような戦略の組み合わせのことをいう。

En-Tan-Mo 研究のもう一つ重要なオリジナルは合理的期待理論とゲーム理論を結合することである。ETM プロジェクトのシニアコンサルタント Thomas J. Sargent 教授の合理的期待理論にたいしての研究は世界中で最高の水準に達している。ブロックチェーンシステムのゲーム理論への分析は次のような事実を注意する必要がある。参加者はインセンティブによって予測を行い、この未来への予測がこれらの参加者の目前の決定に影響を与えること。この点は ETM のメカニズム設計にとって非常に重要なことである。それは、設計者はそれぞれの参加者の情報を「予測」してから戦略を定めることである。この設計は現代制御論中の予測制御問題である。系統の安全性の保障はナッシュ均衡への正確な予測に依頼している。そしてこの予測はメカニズムの設計者が参加者の信念と策略の予測に依頼している。後の分析には非数学化の方式でこの問題を解決した。ETM プロジェクト団体は今後ともこの方向に向けて厳密的な研究を進んでいくと計画した。

En-Tan-Mo は、POW または DPOS コンセンサスがブロックチェーンのすべての参加者がナッシュ均衡に収束することを保証できないと指摘した。ビットコインを例にし、マイナーがハッシュ計算で勝てた後、虚偽の情報を含むブロックをアップロードしたが、システムに採用されないため、マイニングに費やされる費用を失い、すべての参加者の均衡収益を保った。具体的にいえば、1. すべてのブロックチェーン参加者がマイニングに参加できる場合、不正行為の成功率を完全に制御するには、ハッシュ計算は十分に難しくする必要がある。すなわち虚偽の情報を含むチェーンはある時期善良のチェーンに追いつく確率は最小限にする。2. 不正な戦略の使用を防ぐため、マイナーのコストは大きくする必要がある。ASIC マイニングツールの登場により、普通の参加者がビットコインのブロックチェーンから収益を得ることは事实上不可能である。計算資源の増加はマイニングをより困難にさせる。したがって、不正者間の協力を促進し、ナッシュ均衡を完全に覆す。イーサリアムでは、フルノードは通常のユーザーには余裕のない特別な CPU マイナーである。ライト・ユーザーはもはやマイニングを気にかけない。同様に、Steemit を代表とする DPOS コンセンサス・システムでは、大株主が投票権において支配的な立場に立ち、大衆に参加しないため、富が少数の人に集中し、均衡も崩れていた。

En-Tan-Mo とそのコンセンサスの仕組みは、すべての参加者が給付を直接受領する制度を提供することを目指している。大規模なマイニングプールや大株主が利益を独占することを防ぐため、コンセンサスメカニズムから基本的な改革をする必要がある。En-Tan-Mo ゲームのすべてのプレイヤーはユーザーであり、そして参加者は En-Tan-Mo に Stakhanov マイナー、監督者と Pareto マイニングプールと分類することができる。彼らは投票または新たなブロックをアップロードを通して ETM トーケンやほかの報酬を得る。Stakhnov マイナーは選挙制度で選出され、一定の時間内ブ

ロックの生成に協力する。不正なマイナーのマイニングコストが削減したが、不正な行動が検出されたため Stakhnov マイニンググループから追放されれば大きな損失を被るのである。En-Tan-Mo ブロックを生成する効率を高めるため、監督者は最良の Stakhnov マイナーを選定する義務があり、成功率によって ETM トーケンが報われる。そして投票数とトーケンは凹型関数による規制され、全体の株主の利益を保証する。Stakhnov マイナーと監督者は独立性を保っていたが、お互い関連性も持ち、そして相互の権力と権益の分配が明確かつ平衡的である。Paeto マイニングプールの中のマイナーはこの週間に ETM トーケン報酬を得ることができないが、連盟の形で外部のブロックチェーンのマーニングに参加すると、トーケン報酬が得られる。

その取り決めにより、すべてのマイナーの利益が保証される。したがって、DPOS と POW が結合された二重コンセンサスプロトコルによって、Stakhnov マイナー、監督者と Pareto マイニングプールはナッシュ均衡に収束した。

コンセンサスメカニズムの経済学設計が参加者の決定（戦略選択は不正と正直なマイニングである）にどのように影響を施すのかを説明するために、以下のルールと仮設を強調する。

仮設：少なくとも半分のマイナーは正直ことである。

ルール：1. 最長のチェーンのみが採取的に受け入れる。
2. 選挙制度では、虚偽な情報を含むブロックをアップロードするマイナーあるいは効率が低いマイナーは Stakhnov マイナーから排除される。

4.3 Knatorvich コンセンサス

POW を使用した第一世代と第二世代のブロックチェーンの欠点は次のとおりである。1. 取引の処理率が低い。たとえば、ビットコインの現在の取引レートは、銀行のクレジットカードシステムなどのユーライの金融機関には匹敵しない。2. ブロックをアップロードする速度が遅く、取引確認も遅延する。3. スケーラビリティ。現在の効率のレベルは、ブロックチェーンのスケーリングを制限する。4. 計算能力による資源の浪費と環境汚染。

そのため、En-Tan-Mo はナッシュ均衡に基づいてカントロービッチコンセンサスを出す。監察員は En-Tan-Mo の株主として、直接に En-Tan-Mo のブロックチェーンに参与せず、所有のトーケンに基づいて投票選挙権を得ることで、投票 ETM トーケンの奨励を取得する。監察員はマイナーの計算能力と今までの実績を主な根拠とし、最高のスタッカノフマイナーを選び、En-Tan-Mo を高効率と安全性を維持させる；スタッカノフマイナーは En-Tan-Mo のブロックのノードとして、監察員によって選ばれて非競争にマイニングすることで、ブロックの ETM トーケンを取得する。スタッカノフマイナーはブロックサイクルごとに序列にブロックし、安全性を減らさない前提にハッシュ値を計算する難しさを減らす。それでブロックのハッシュレートを速め、効率を高める；選ばれなかったマイナーはパレートマイニングプール連合に入り、特有のデリバティブチェーン技術を利用して外部

のブロックの产出に参与し、マイニングマシンに提供された計算能力に基づいて非 ETM トーケンを配分し、それで全てのマイニングマシンのポジティブな収入を保証する。そのため、カントロビッチコンセンサスは安全性が保障できる同時に効率を高め、システムの可拡張性も増やす。

目前、中心化のシステムは効率の面にわりと強い利点がある。しかし、もっと巧妙な数学の構造デザインを採用すれば、分散型ブロックチェーンと適当な協力集中（例えば En-Tan-Mo のカントロビッチコンセンサス）とのバランスを取ることで、安全性・安定性・高効率を兼備するブロックシステムが立てられる。これこそ我々の主な目標である。

カントロビッチコンセンサスはステークプロトコルへの新しい計算方法であり、各ノードがいかにインターネットの一致性を達成するのかを決定する。この計算方法は En-Tan-Mo インフラの重要な一部であり、ブロックチェーン技術の重大なイノベーションである。カントロビッチコンセンサスは、ブロックチェーンが今までアプリケーションの拡張を障害する問題、すなわちエネルギー需要の消費に関するワーカロード証明（pow）契約を改めてデザインした。計算方法は IOEM チーフ・サイエンティストがリーダーしているゲーム理論チームによってデザインしたものである。それに学術コミュニティのピアレビューを合格する。これは初めて科学的にその安全性を証明した DPOS と POW カップリング権益証明契約である。

カントロビッチコンセンサスはソ連の数学学者、1975 年経済学のノーベル賞受賞者レオニード・カントロビッチが最適輸送という数学領域においての仕事からヒントを得る。カントロビッチは厳しい最適輸送の数学モデルを提唱する。それはカントロビッチ双対と呼ばれ、核心は分散型ブロックチェーンの方法を利用してリソース構成の最適化が達成できると証明する。カントロビッチはその数学理論に導かれた分散型ブロックチェーンの見方で大統領スターリンに刑務所に拘留されたことがある。その後ソ連の原爆プログラムに参画したので釈放された。フランスの数学家ヴィラニはこの方法を利用して行われた研究はフィールドアワードを受賞した。そのため、カントロビッチが数学においての実績及び特殊な時代に現れる勇気に敬意を差し上げるために、En-Tan-Mo はコンセンサスメカニズムをカントロビッチコンセンサスと名付ける。

Kantorovich コンセンサスはソ連の数学学者、1975 年経済学のノーベル賞受賞者レオニード・カントロビッチが最適輸送という数学領域においての仕事からヒントを得た。カントロビッチは厳しい最適輸送の数学モデルを提唱する。それはカントロビッチ双対と呼ばれ、核心は分散型ブロックチェーンの方法を利用してリソース構成の最適化が達成できると証明する。カントロビッチの数学理論に導かれた分散型ブロックチェーンの見方が主流の学術界から批判されたが、ソ連の原爆プログラムに参画したので大きな迫害を受けなかった。同時に、カントロビッチの経済理論は西方の学術界で広く受け入れ、しかも応用された。Kantorovich 最適輸送理論が近 20 年来最も重要な研究方向の一つである。フランスの数学家ヴィラニはこの方法を利用して行われた研究はフィールドアワードを受賞した。そのため、カントロビッチが数学においての実績及び特殊な時代に現れる勇気に敬意を差し上げるために、En-Tan-

Mo はコンセンサスメカニズムをカントロビッチコンセンサスと名付ける。

4.4 スタッカノフマイナーと監察員

En-Tan-Mo において、マイナーチームの選挙制度に選ばれ、基礎の計算能力テストに合格したマイナーがスタッカノフと呼ばれ、略称 SCV。スタッカノフマイナーに投票するトーケンの持ち主は「監察員」と呼ばれる。監察員は手に入れたポロポーションナルトーケン・ステークをマッピングで投票数に転化できる。投票サイクルごとにあるふさわしい奨励を与える。候補者としてのマイナーは票数によって SCV マイナーと候補のマイナーになる。それでブロックをアップロードする権力をもたらし、ブロックの義務と奨励を検証する。

仮にある SCV マイナーがカンニングすることで偽情報と二重支出が含まれるブロックをアップロードしてみれば、その結果は二つがある。1. 大多数の SCV マイナーは誠実なので、確率論の方法を利用して証明できる。カンニングするマイナーはアップロードした偽のブロックが最終に消える。そのため、計算能力のマイニングしている過程に消耗したコストを損失する。2. カントロビッチコンセンサスメカニズムの交代選挙制度により、カンニングしているマイナーは間違いなく今度の選挙にマイナーチームから除名されるに違いない。それからでマイニングでトーケンを取得するチャーンスと今まで投入した保証金を失う。したがって、任意のある SCV マイナーは一旦投票されマイナーチームに入るなら、合理的な選択は高効率的にタスクを完成し、それに実際のブロック情報をアップロードするに違いない。

そのため、En-Tan-Mo システムの全体には SCV マイナーと監察員の行為を厳しく規制する中心化の監督者がいなくても、SCV マイナーと監察員が自分自身の最大な利益への求めという「見えない手」を利用し、全ての参与者の従順コンセンサスを導く。これで En-Tan-Mo の参与者の間ににおける信頼問題と効率問題が解決できる。

スタッカノフはソ連の三十年代のあるマイナーであり、効率が高いので宣伝のモデルになる。そのあとソ連では、高効率で過負荷ワーカロードを完成するマイナーは Stakhanovites だと呼ばれる。En-Tan-Mo においてカントロビッチコンセンサスメカニズムによって選ばれたマイナーは効率と信頼できるモデルである。監察員はラテン語の Tribunus から来て、旧ローマ時代にエグゼクティブまたは軍事を監督する官職と委員会である。

4.5 パレートマイニングプール

En-Tan-Mo システムの奨励方式は経済学理論をデザインの基礎とし、その利点は三つの点で現れる：

1. 公平性：外部の POW ブロックチェーンの体系において、個体の間に不均一な分布がある。例えば、ビットコインとエテリアムの権益が若干の中央マイナーまたはマイニングプールへ集中する傾向が強い；En-Tan-Mo システムの中に、全ての個体がコンセンサスメカニズムの前で平等である。

2. 分散型ブロックチェーン：外部のDPOS ブロックチェーンの体系において、ビッグトークンの持ち主はシステムの決定権をマスターし、改めて中心化の軌道に戻るまたは多くの寡頭に独占される；En-Tan-Mo システムの中に、トークンの持ち主とブロック生産者は職位、権力、利益などの点で分離し、全ての個体は分散型ブロックチェーンによる資源と優位をお楽しみする。

3. 最適性：外部のブロックチェーンの体系において、個人の収益が単一で、チェーンとチェーンの間に1つずつの島のようであり、通じられない；En-Tan-Mo システムの中に、トークンの持ち主は投票のインセンティブをもらえ、マイニングマシンのノードがSCVマイナーとパレートプールの間に転換し、最適な収益を取得する。

カントロビッチコンセンサスメカニズムにおいて、全てのマイニングマシンのノードが団結と協力なマイニングプールを組み合わせる。ブロックサイクル毎に若干のSCVマイナーを選んで序列的にブロックする。En-Tan-Moはその

周期に選ばれなかった全てのマイニングマシンをパレートマイニングプールに構成させる。特有のサイドチェーン技術とアライアンス戦略を運用し、リアルタイムの収入アルゴリズムによって分析し、外部のブロックチェーンのブロック生産に参与し、マイニングマシンの計算能力に基づくマイニングプールの収入を配分し、それで全てのマイニングマシンのプラス収入を保障する。

パレートマイニングプールの経済学原理の核心は同盟の策略を巡らす；適切なブロックを選択する；同盟の構造と管理制度を立てる；マイニングマシンはSCVマイナーとパレートマイニングプールの間における転換などにある。

パレートマイニングプールの特徴が以下のように示す：

1. 組織の分散型ブロックチェーン：パレートマイニングプールは共にしじょうを共有することと協力にマイニングすることを基本的な目標とする。マイニングプールの間におけるメンバー関係が外部のブロックチェーンの収益策略に決定され、永遠に不变なわけではない。パレートマイニングプールそのものはそもそも動的で開放的なシステムである。

2. 行為の戦略性：パレートマイニングプールの方式と結果は外部のブロックチェーンの競争環境への長期な計画である。共同作業は、戦略の視点からマイニングプールの同盟に共有される業務環境と業務条件の改善にも重点を置いており、最大の焦点は、事業活動における外部経済資源を積極的に獲得することである。

3. 協力の平等性：パレートマイニングプールは過去の戦術協力とは異なり、資源の共有、互いの補完、互いの信頼及び相互独立に基づき、事前に達成された合意によって形成された平等な関係である。計算能力による収入の分配に従い、マイニングマシンの間における不平等の状況が根本的に変わった。

4. 管理の複雑さ：カントロビッチコンセンサスメカニズムの中で、初めて真の「二重的なマイニング」が起こる。マイニングマシンは、SCVマイナー戦略とパレート炭マイニングプール戦略の間に切り替える必要があり、最大の利益は厳密なコンセンサスメカニズムとスマートな管理システムに基づいている。

パレート効率（Pareto efficiency）とも呼ばれるパレート最適性（Pareto Optimality）は、理想的なリソース割り当ての状態であり。固有のグループおよび配分可能なリソースを仮定し、分配のある状態から別の分配状態に至る状態の変化において、誰かの状況を悪くすることなく、少なくとも1人をより良くなります。パレートの最適状態は、パレートを改善する余地がないようなものである；言い換えれば、パレート改善はパレート最適性への最適な道と方法である。したがって、パレートマイニングプールの最適化は公平性と効率性の「理想的な王国」である。

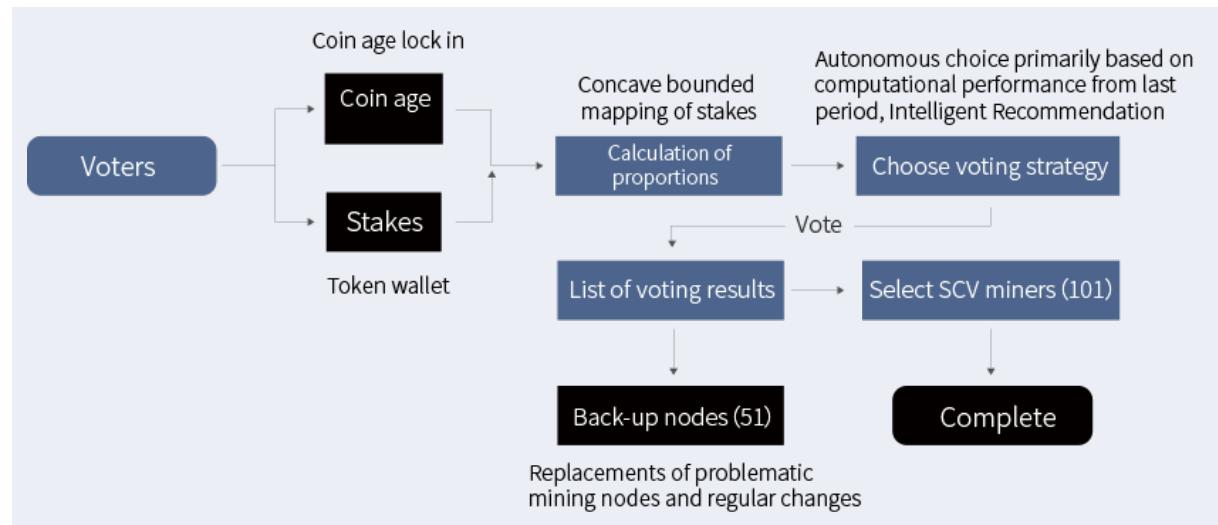
References:

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

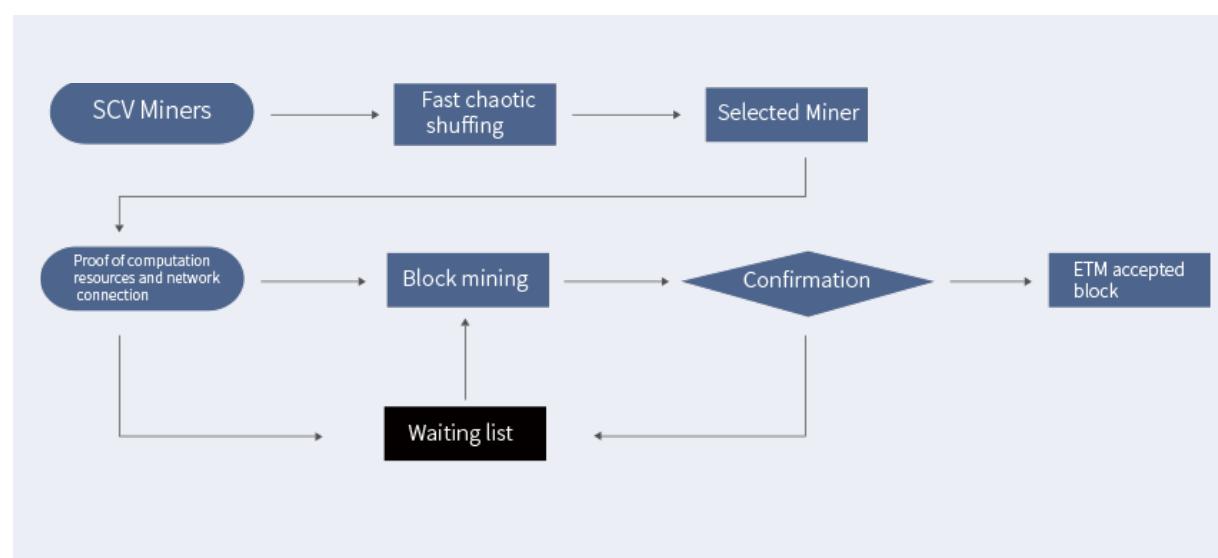
5.0 En-Tan-Mo 計算

5.1 En-Tan-Mo フローチャート

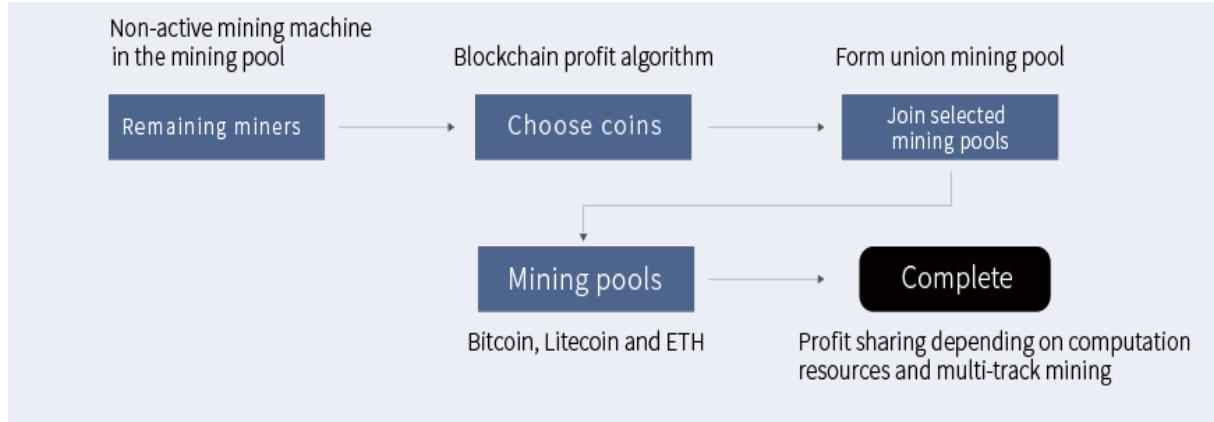
Kantorovich コンセンサス流れ図：ナッシュ均衡の思想に基づき Kantorovich コンセンサスはマイナーグループの選挙制度を通じ、ブロック生成する周期において若干の SCV マイナーが所定の順序でブロックを生成する。安全性を保証することを前提としてハッシュ計算の難易度を下げることで、ブロック生成の速度を向上し、効率を高める。



監察官の投票手順：各監察官が持っていたトークステークは En-Tan-Mo に凹関数で計算され投票数となる。投票すると対応の報酬をもらうことができる。



SCVマイリングの作業手順：最高の得票数を得た候補マイリングは SCVマイリングとなり、ブロックをアップロードする権利を持ち、ブロックのマイリングの奨励を検証する責任を負っている。



Pareto マイリングプールの作業手順：ブロック生成周期において落選なマイリングを集中し、Pareto マイリングプールを形成する。特別なサイドチェーン技術と連合戦略を用いて、リアルタイムユーティリティアルゴリズムによって分析し、他のブロックチェーンシステムのマイリングに参加する。

En-Tan-Mo のコアコード

1. 監察官のトーケン均衡アルゴリズム

SCVマイナーは監察官から投票で選出され、ブロックをアップロードする権利を持っている。監察官が持った投票数と所有したトーケンの数量は上に凸関数の関係となり、En-Tan-Moの生態系の平衡を保障した。SCVマイナーはブロックをアップロードすることは正当なものであり、「凸面」は監察官が所有したトーケンの引換率を表す。所有したトーケンが多ければ、引換率が低い。逆に所有したトーケンが少ないと、引換率が高い。

$F(\text{balance}) = \text{weights}$

// 閾値関数 権益均衡のため、所有したトーケンが多ければ、引換率が低く、逆に高い。

ThresholdMap = Map(range,rate)

// トーケン値間隔から計算率を得る

Rate = thresholdMap.get(range)

weights = balance * rate

// 引換率によって依頼人の所有のトーケン重みを得る

2. 監察官 投票インセンティブ・メカニズム

En-Tan-MoはDPOSとは違い、監察官の監察官にもトーケンを与え、プラットフォームに参加する意欲を高める。そして最優秀のSCVマイナーを選び出し、En-Tan-Moを効率的かつ安全に運営することを保障する。En-Tan-Moの投票インセンティブ・メカニズムには投票者への報酬とブロックをアップロードすることへの報酬という二つ種類がある。監察官はこの二種類の報酬を得る割合を自由に選ぶことができる。監察官への報酬は所有した投票数から決められ、投票すれば固定の報酬を得られる。ブロックをアップロードすることへの報酬は、監察官が優秀なSCVマイナーを選出した場合のみ得ることができる。その報酬は変動ヘッジ価値である。

$F_1(\text{tickets}) = \text{token}$

// 供給比

$\text{tickets1} = \text{fixed assignment}$ // 固定チケットに供給する

$\text{tickets2} = \text{dynamic assignment}$ // 変動するチケッ

トに供給する

// 固定収益 + 変動収益 (選出されたノードが総ノード数に占める割合により)
 $\text{token} = \text{fixed}(\text{tickets1}) + \text{dynamic}(\text{tickets2})$

3. SCVマイナーのマイリング・シーケンス・アルゴリズム

En-Tan-Moの安全性を確保するため、SCVマイナーはブロックを生成することが確定的かつ擬似ランダムのシステムを使用する必要がある。したがって、En-Tan-Moはカオス理論と非線形動力学を用いて絶対的な安全を達成する。

// クライアントの投票権を固着させる

$\text{Lock}(\text{balance})$

// 投票過重を計算する

$\text{tickets} = F(\text{balance}) * F(\text{time})$

// 投票者は代表者のリストを取得する

$\text{delegations} = \text{votes}(\text{tickets})$

// シャッピング

4. SCVマイナー ハッシュアルゴリズム

En-Tan-Moは安全性と分散型を保障するほか、高性能を達成する必要がある。SCVマイナーの間は競争関係ではなく、お互い協力しブロックをアップロードする。各ブロックにマイナーを指定し、SHA256をできるだけ早く完成し、ブロックをアップロードする。

// 双ハッシュ計算

$\text{blockhash} = \text{sha256}(\text{sha256}(\text{block}))$

// 計算時間を検査し、特定の時間内で計算結果を得ていないマイナーは不合格である

$\text{CheckNodePerformance} (\text{useTime})$

// 計算量が指定された要件に満たすのかをチェックする
 $\text{checkResult}(\text{blockhash}, \text{difficulty})$

// 不合格ならノースを変える

$\text{block.nonce} = \text{block.nonce} + 1$

5.2 En-Tan-Mo データ

ブロックヘッダのデータ構造

ブロックヘッダにはブロックに相関するすべての情報を含んでいる。次のフィールドで構成されている。

- ブロックヘッダにはブロックにに関するすべての情報を含んでいる。次のフィールドで構成されている。

 - ・ ブロックバージョンを識別する 32 ビット整数
 - ・ ブロックが生成された時の 32 ビットのタイムスタンプ
 - ・ 前のブロックの 64 ビット ID
 - ・ ブロックで処理されたトランザクションに対応する 32 ビット整数
 - ・ 転送回数に対応する 64 ビット整数
 - ・ ブロックに関連する総費用に対応する 64 ビット整数
 - ・ ペイロードの長さに対応する 32 ビット整数
 - ・ ペイロードの 256 ビットハッシュ
 - ・ ブロックを生成した 256 ビットの公開鍵

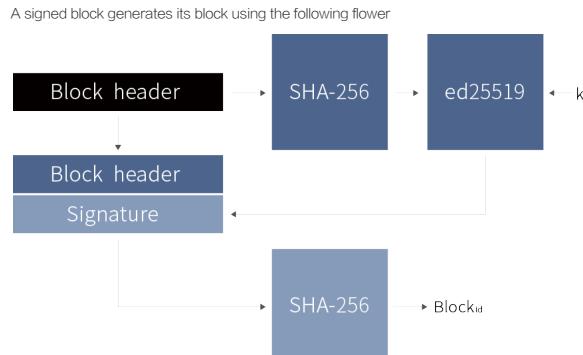
Version	Timestamp
	Previous block Id
Number of transactions	Length of payload
	Amount of ETM transferred
	Amount of fee
	Reward of the delegate
	Payload hash
	Delegate's public key

块头数据样例

ブロック ID の生成手順

ブロックヘッダのハッシュ SHA-256 を生成し、とラステッド・キーを使用し (ed25519 アルゴリズム) 署名を実行する。

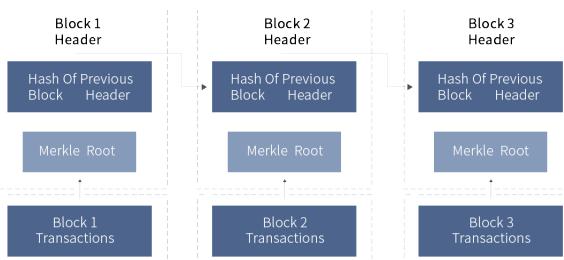
ブロックヘッダーが署名されると、システムは SHA-256 を利用し、完成したブロックヘッダをハッシュしてブロック ID を生成する。



ブロックチェーン構造

ブロックはブロックヘッダとブロックボディからなっている。ブロックヘッダには、バージョン番号、前のブロックアドレス、タイムスタンプ及びマークル番号のルートが含まれている。ブロックボディーには主に取引件数と取引明細が含まれている。

ブロックチェーンは暗号学を使用し生成された一連のデータブロックで構成されたものである。各ブロックには、前のブロックのハッシュ値が含まれる。起点のブロックからはじまり、現在のブロックと接続しブロックチェーンを形成する。

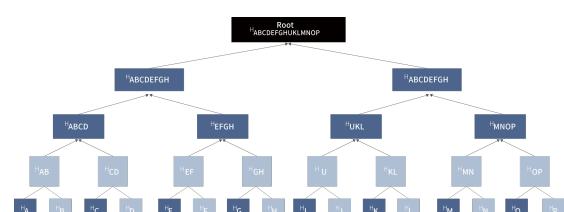


データ保存のマークル木構造

マークル木はハッシュ木と呼ばれ、ハッシュ値を保存する木である。

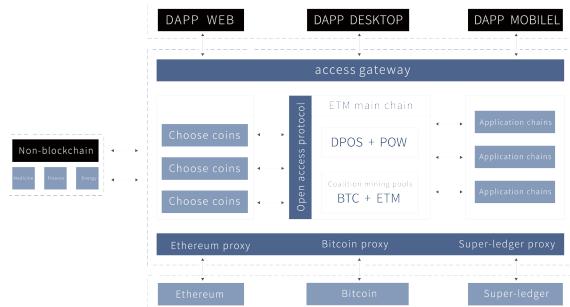
マークル木の葉はデータブロック（たとえば、ファイルまたはデータ）のハッシュ値である。

非リーフノードは、対応するサブノードの連結する文字列のハッシュである。



5.3 En-Tan-Mo インターフェース

En-Tan-Mo は BaaS (Blockchain as a Service ブロックチェーンはサービスである) を理念とし、マイクロサービスを提供することを基準にする。その核心は自己進化するコンポーネントライブラリであり、開発者コミュニティを原動力とすることで、他のブロックチェーンに資産とアプリケーションの自由移転に適用のプラットフォームを提供する。非ブロックチェーンのアプリケーションとデータ用の双方向起動のソフトチャネルを提供し、開発者が共有ロビーでコンポーネントのアップロード、レビュー、及び奨励することができる。通常のユーザーの場合、En-Tan-Mo は BaaS のゲートウェイを提供し、アクセシビリティサービスを実装する。このように、各ブロックチェーンは他ブロックチェーンと非ブロックチェーンと接続し、技術開発者と一般ユーザーのネットからブロックチェーンへの移動に役割を果たした。そのシステムの構造は以下の図のように：



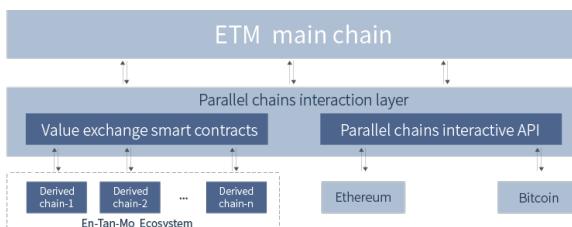
システム構造図の説明：

- ・アプリケーション層（ウェブ、デスクトップ、モバイル）は統一なアクセスゲートウェイを通してデータアクセスをする。
- ・アプリケーションコンポーネントとオフラインリソースによってデータを相互交換する。
- ・アプリケーションコンポーネントは、オープンアクセスプロトコルを通してブロックチェーンでのデータの相互交換を実現する。
- ・アプリケーションコンポーネントの内部は、チェーンでのデータを統合する。
- ・メインチェーンとアプリケーションチェーンは内部プロトコルを通してデータ交換と価値伝達する。
- ・プロキシレイヤーを通して第三者との相互連携する。

6.0 En-Tan-Mo エコシステム

6.1 中央チェーンとデリバティブチェーン

ブロックチェーンが直面する多くの問題の中に、ブロックチェーン間の相互運用性はブロックチェーンのアプリケーションスペースを大きく制限する。パブリックチェーンやプライベートチェーンに関しては、クロスチェーン技術が価値伝達を実現するキーである。分散した島々からブロックチェーンを回収することは、ブロックチェーンの拡張と接続の架け橋である。既存のクロスチェーン技術は主にサイドチェーンを中心に、実際に価値伝達ではなくバリューロックのみを実現している。そのため、En-Tan-Moは、既存のクロスチェーン技術を研究した後、チェーンとチェーンの間の価値伝達を実現するパラレルチェーンの相互作用プロトコルを提案し、チェーンとチェーンとの間における価値伝達を完璧に実現し、それによって千万以上のユーザーがあるブロックチェーンエコシステムを構築する。

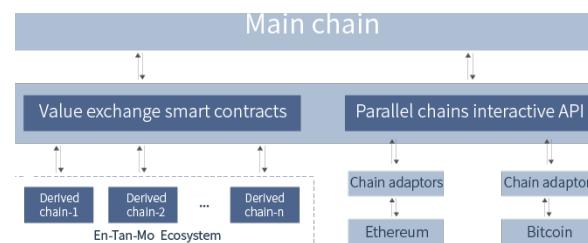


ブロックチェーンの急速な拡大とサービス (BaaS) としてのブロックチェーンの問題を解決するために、En-Tan-Mo は中央チェーンに加えて複数の派生チェーンの設計を採用し、中央チェーンがネットワークセキュリティと価値交換を担当する。デリバティブチェーンは特殊なブロックチェーンの一一種で、各デリバティブチェーンは一つの DAPP に対応している。DAPP は独立したシステムであり、メインチェーンの強力なブロックテクノロジを継承して再利用することによって、各アプリケーションには個人化の帳簿があり、個人のトークンがあり、そのコンセンサスメカニズム、ブロックパラメータ、およびトランザクションタイプの全てがカスタマイズができる。各デリバティブチェーンには平行な関係がある。すなわち、一つのデリバティブチェーンともう一つのデリバティブチェーンは互いに平行している。それらは中央チェーンの「パラレルチェーンインタラクションレイヤー」を介して、それと中央チェーン、他のデリバティブチェーン、および外部ブロックチェーンとの間に資産を双方向に転送することができる。そこで、ユーザーが既存の資産を使って En-Tan-Mo システムを利用することができる。

6.2 パラレルチェーンの相互作用プロトコル

En-Tan-Mo のパラレルチェーンの相互作用プロトコルは、異なるブロックチェーンの価値交換をサポートすることを可能にし、主にチェーンアダプターモジュールと価値交換のスマート契約から構成される。チェーン・アダプターを設

計する主な目的は、異なるチェーン上の取引を検証するためには、価値交換スマートコントラクトに En-Tan-Mo が異なるチェーンとのインターフェースを提供することである。同時に、チェーン・アダプターはコミュニティ・ビルダーによって開発され、次第に改良され、より多くのコインが得られる。例えば、アプリケーションはチェーン・アダプターを借りて異なるプロトコルの下位ブロックチェーンの間に切り替えることができる。価値交換のスマート契約は、パラレルチェーンの相互作用プロトコルの中核であり、ユーザーを En-Tan-Mo 中央チェーンとデリバティブチェーン、デリバティブチェーンとデリバティブチェーン、En-Tan-Mo と外部ブロックチェーン（ビットコインとエテリアムなどが含まれるが、限られない）のシステムの中に、資産交換を実施させる。それによってインターチェーンのバリューネットワークを構築する。



チェーン・アダプター

チェーン・アダプターは、コンピュータのデバイスドライバのようなもので、下位ブロックチェーンプロトコル En-Tan-Mo 中央チェーンのさらに使いやすい方法に変換させ、En-Tan-Mo 中央チェーンの価値交換のスマート契約を実行させる。その中に含まれる技術には、ハッシュ・タイム・ロック・コントロール (HTLC)、SPV 認証、および API 開発などが含まれるが、これに限定されない。

En-Tan-Mo は、ビットコインのブロックチェーンやエテリアムなどの一般的に使用されているブロックチェーンシステムのチェーン・アダプターを最初に提供する。運行が安定してから普及される。オープンチェーンのアクセスプロトコルを改善したり、個人のコードを実装したりすることが誰でもできる。En-Tan-Mo は、より多くのブロックチェーンのプロトコルをサポートし、それに相応しいコインを報酬として提供する予定である。

価値交換のスマート契約

ブロックチェーンという革新的な技術はすでにグローバルに注目されてきたが、常に一つの問題がある。それは異なるブロックチェーンシステムの間における価値の取引には、依然として取引所のような仲介者が必要である。それこそ分散型ブロックチェーン技術が置き換えたいものである。En-Tan-Mo は、このような仲介者を、最小化信頼のスマート契約とチェーン・アダプター

に置き換え、異なるチェーンの架け橋の機能を担う。

このアプローチは、ブロックチェーン領域における最も重要な2つの要素の相互的な接続を深め、統合されたグローバルな価値の配信ネットワークに近づける。

価値交換のスマート契約はEn-Tan-Moのチューリング完全仮想マシンに依存しており、ユーザーに適切なセキュリティを提供する。デリバティブチェーンと中央チェーン間の価値交換のスマート契約は、分散型ブロックチェーンの取引所と同じように、ETMウォレットアドレスとそれに対応するチェーンウォレットアドレスを管理する。ユーザーがデリバティブチェーンの上で転送を開始し、中央チェーンを介してアダプターによって確認されると、価値交換のスマート契約は、価値交換を完了するために、中央チェーンにユーザーのETMウォレットアドレスの転送を自動的に開始する。同時に、ユーザー交換の過程に直面するリスクを避けるために、En-Tan-Moにビットコインシステムのハッシュ・タイム・ロック・コントロール(HTLC)技術が組み込まれる。

具体的な交換プロセスについては、ビットコインとETMの交換を例にとる。手順は次のとおりである。

ビットコインブロックチェーンのユーザーAは、ユーザーAのETMウォレットアドレスとBTCウォレットアドレスの間のマッピング関係をバインドするために、最初にEn-Tan-Moに登録する必要がある。

ユーザーAは、任意の秘密番号aを生成し、そのハッシュ値H(a)を計算する。そして、特別な取引は、ハッシュ・タイム・ロック・コントロール技術に基づき、12時間ロックされた価値交換のスマート契約のビットコインアドレスに対し、ビットコインブロックチェーンで開始される。En-Tan-Mo価値交換のスマート契約は、コインを取得するために元のイメージのハッシュイメージH(a)を生成しなければならず、12時間後に取引しているBTCが自動的にユーザーAのビットコインウォレットアドレスに戻る。

En-Tan-Moスマートコンタクトはビットコインチェーンアダプターを通じ、ブロックチェーン内の特別な取引の確認状況を監視し、SPV検証を実行する。SPV検証に合格すると、En-Tan-Mo価値交換スマートコンタクトは中央チェーン内でユーザーAのETMウォレットアドレスに向かって特別な取引を発起する。そして取引の固定時間が6時間である。ユーザーAは取引内のETMトーカンを取得したい場合、ハッシュ値H(a)の原画像を提示する必要がある。そうでなければ、取引のETMトーカンは、6時間後に自動的にスマートコンタクトのETMウォレットアドレスに返還される。ユーザーAが秘密の番号Aを提示し取引内のETMトーカンを取得した後、スマートコンタクトはその秘密の番号aを記憶し、それにアダプターを通じビットコインブロックチェーンネットワークにアクセスし、ユーザーAがビットコインブロックチェーン内で始また取引のビットコインを別のユーザーに転送する。ここで、取引が完了した。

ここで強調したいのは、中央チェーンは分散型の価値交換の場所としてのみ使用され、ユーザーAのビットコインをロックし価値移転を達成する場所ではない。スマートコンタクトは、ユーザーAがスマートコンタクトのビットコインウォレットアドレスに転送しビットコインを、ETMトーカンをビットコインに交換したいユーザーに使用できる。同時に、ユーザーAがビットコインをETMトーカン

を交換したと、中央チェーンはそれらトーカンの移転を制限することがない。しかも他のブロックチェーンのトーカンと転換することができる。したがって、En-Tan-Moが実現するのは資産交換ではなく、価値交換である。さらに、すべての価値交換スマートコンタクトのウォレットアドレスには、最初のトーカンがない、相関のブロックチェーンの投資が必要である。スマートコンタクトは価値交換の間に発生した手数料を投資の比例によって相関投資者に分配する。投資過程において、ユーザーはいつでもスマートコンタクトから投資資金を回収することができる。

要するに、価値交換のスマートコンタクトに基づき、En-Tan-Moが構築するものは、鎖間価値のネットワークである。それにEn-Tan-Moは価値を創造することではなく、価値移転の代理人として運営している。

En-Tan-Mo アプリケーションエコシステム

En-Tan-Moは新しい世代のブロックチェーンプラットフォームである。各種のアプリケーションを独立したデリバティブチェーンに運営することで、外部ブロックチェーンシステムのブロックのサイズ膨大、同期の遅延などの問題を効果的に解決した。En-Tan-Moの多デリバティブチェーンモードは、高頻度の取引場合においてネットワークの輻輳問題に対する理想的な解決策を提供した。ユーザーは相関のアプリケーションを利用することのみ、デリバティブチェーンをダウンロードする必要がある。これによって、無用な同期データを大幅に削減し、En-Tan-Moネットワーク全体の高性能な状態を保った。また、価値交換スマートコンタクトを通して、インターチェーンネットワークと高性能グラフエン技術、迅速ペイメントネットワークなどの技術を統合され、一千万人以上のユーザーを持つアプリケーションを支持することができる一方、各ブロックチェーンエコシステムを相互連結させる。

6.3 ミル・モール (mir mall)

En-Tan-Moシステムは便利かつ高効率なミル・モールを通し、企業や開発者がより経済的にブロックチェーンのアプリケーションを運営することを支援し、ユーザーに安全と便利を感じさせる。デリバティブチェーンに分散型のアプリケーションをDAPPと呼ばれた。そしてのミル・モールは次の利点がある。

(1) 一千万人以上以上のユーザーを持つアプリケーションにブロックチェーンエコシステムを提供する。

(2) デリバティブチェーンでの資産はEn-Tan-Moのパラレルチェーン交換プロトコルを通じ他のトーカン(ETM/BTC/ETHなど)と交換することができる。したがって、En-Tan-Moに基づく開発したアプリケーションはより多くのユーザーを獲得することができる。

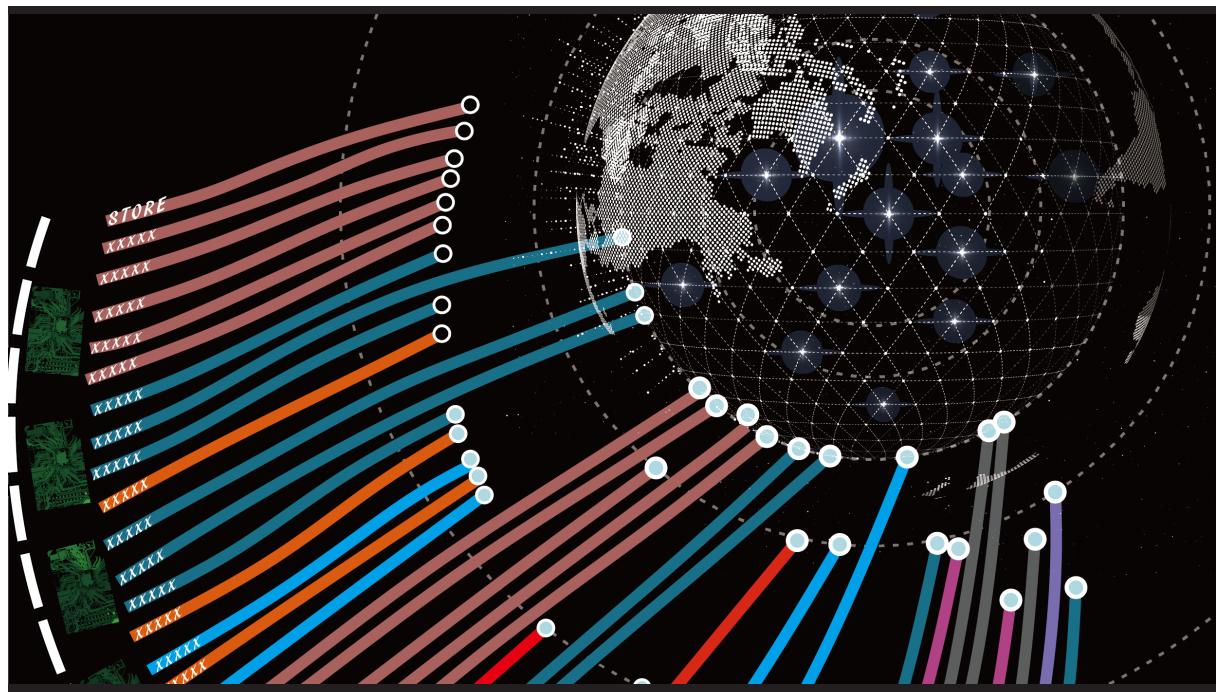
(3) En-Tan-Moパラレルチェーン交換プロトコルに基

づき、DAPP は複数の下位ブロックチェーンデータにアクセスすることができる。それに DAPP は複数の下位ブロックチェーンに基づき運営することができる。

(4) En-Tan-Mo のパラレルチェーン技術と一連の SDK、API 及びテンプレートを利用し、開発者はビジネスロジックを関心することだけで、パーソナライズな DPAA を簡単に開発、テスト、公開することができる。それに新たなアプリケーションを開発するコストの削減は、開発者がミル・モールで DAPP をより良くかつ迅速的に開発することに役立つ。それらの DAPP はすべての ETM ノードによってダウンロードされ、運行されることができ、そしてすべてのブロックチェーンユーザーに提供する。

(5) En-Tan-Mo のパラレルチェーン技術に基づき、熟練した開発者はミル・モールの DAPP のパーソナライズデータベース、コンセンサスメカニズム、取引の種類及びアカウントシステムをカスタマイズすることができる。

(6) En-Tan-Mo は完善な報酬制度を構築する。優秀な DAPP 開発者に、ミル・モールは報酬としてトークンを与える。東シベリアには、一千億元の価値を持つダミルダイヤモンド鉱山を発見し、世界で最も高価なダイヤモンド鉱山である。ここで En-Tan-Mo は DAPP アプリケーションストアにミル・モールと名づけることは、DAPP ストアが豊かな資源を持ち、強大な潜在力を持っていること表すことである。



7.0 En-Tan-Mo の組織の構造

En-Tan-Mo のコミュニティは En-Tan-Mo 基金会、IOEM と Emgo などの三つの組織で構成される。En-Tan-Mo 基金会はその中の核心であり、海外に設立された非営利団体であり、En-Tan-Mo ユーザコミュニティを全方位的にサポートし、En-Tan-Mo プロジェクトの円滑な発展を保証する。さらに、En-Tan-Mo には、プライバシーセキュリティの研究と開発をリードする組織 Emgo と、ビジネスを支援する投資会社およびパートナーである IOEM がある。

7.1 En-Tan-Mo 基金会

En-Tan-Mo 基金会は海外に設立された非営利団体であり、主に En-Tan-Mo コミュニティの生態建設と技術支援を担当している。En-Tan-Mo 基金会の中心的な任務は、自発的な En-Tan-Mo インフラストラクチャとブロックチェーンプロトコルを規制、保護と推進することである。同時に、ブロックチェーンとクリプトクロスの規制を研究する機能を担い、En-Tan-Mo エコシステムの保護、強化、進化の役割も担っている：En-Tan-Mo コミュニティを収集し、教育し、トレーニングする。

同時に、En-Tan-Mo コミュニティ全体の有効的な監督で、独立した第三者として、コミュニティの長期的な発展のための全体的な計画が提案される。また、En-Tan-Mo 基金会は公益団体としての役割も果たし、世界の公的福祉

・チャリティーという事業に注目し、世界の公的信用制度の発展を促進する

En-Tan-Mo 基金会の評議会は、理事会の指導のもとで、主な方針と事務総長の責任を決定するため、民主的な意思決定という方式を採用する。監査役会は理事会の運営を監督する。監査役会には、一般的によく知られている公的な人物や専門的な財務担当者が含まれている。

En-Tan-Mo 基金会の理事会

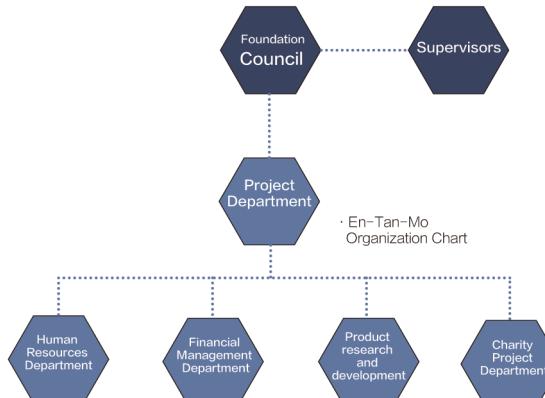
En-Tan-Mo 基金会の理事会は、主な機能はチャリティーの団体である。基金会は、製品の開発、財務管理、マーケティング、人事、および法務などに分かれ、基金会の日常的な管理をともに維持しています。

En-Tan-Mo 基金会慈善项目部

En-Tan-Mo 基金会のチャリティープロジェクトは基金会の中核事業部であり、基金会の公的福祉のプロジェクトの運営および管理を担当し、基金会の公的福祉の目標を実現し、理事会の全体的な意思決定を実施する。En-Tan-Mo 基金会の理事会は計画と資金調達を通じ、チームが基金会の背後にあるアイデアを現実に変える。基金会の早期的な開発過程において、En-Tan-Mo 基金会の法案の審議を担当し、理事会によって評議会の運営規則を設定して認める。

En-Tan-Mo 基金会のプロジェクト部門は緊急対応の仕組みを担当する。En-Tan-Mo 理事会によって広報を議論する必要があり、合意してから公衆に公開することができる。ファンの発展の全体的な方向性は、理事会によってチャネルの方向性、拡張性、および普及などを含む新しいプロモーション・チャネルについて調査される。

En-Tan-Mo



En-Tan-Mo 財務管理部

En-Tan-Mo は独立、公開、透明な財務管理システムを有している。

(a) En-Tan-Mo 基金会は、その事業予算を一年前に発表する。その基金会は非営利組織であり、その主要収入はプライベート・エクイティとトークン割引である。すべての取引は専門の財務役員から審査し、そしてブロックに記録することを通して、公開、透明、かつ非遡及的な財務管理を実現する。そのほか、基金会のすべての支出も専門の財務役員によって審査され、関連するブロックに登録する。

(b) En-Tan-Mo 基金会は資金を照合するために毎月の財務報告を公表する予定である。そして財務報告書は、基金会によって任命された専門家財務官および En-Tan-Mo コミュニティの専任人事管理委員によって審査される。

(c) En-Tan-Mo 基金会の資金調達、主要イベントおよび発展状況について定期的にコミュニティに報告される。重要な問題や機能の変更は、公告の形でコミュニティに事前に報告される。

En-Tan-Mo 人事部

En-Tan-Mo は全コミュニティに向けて公開された人事システムを有している。伝統的な会社の結構と区別し、En-Tan-Mo の人材採用は透明と公平であり、ブロックチェーンには記録を残している。

(a) 人材の採用は公正な選考を行い、二回以上の面接を通じ、採用記録に独立な評価報告を記入する。すべての記録は改ざんできず、永久にバックトラックされる

(b) 採用条件に満足する志望者は、関連委員会の最終審査を受ける必要がある。またコア開発者及びコア管理者は業務分割プロセスを経り、そして En-Tan-Mo の基金会のコアチームの審査を受ける。

(c) アウトソーシング業務に対して、契約を作成され、給料と賃金を決定する。契約したアウトソーシング契約をコミュニティ全体に公開され、スマートコンタクトに書き込む。

En-Tan-Mo 基金監査役会

En-Tan-Mo 監査役会はすべての En-Tan-Mo 参加者に対して責任があり、基金会の取締役およびプロジェクト要員の合法的な職責実行を監査し、会社と株主の正当な権益を保護する。また監査役会は基金会の財務状況と経営管理状況を審査と評価する。その上、基金理事会も監査役会の要求に応じて基金プロジェクトの締結と実施及び資金の使途と損益状況を報告する。

7.2 ETM FinTech 技術開発会社

ETM FinTech の主要任務は開発と新たなエコシステムを維持することである。En-Tan-Mo の開発は次の4つの段階に分けられている。

「ペトラルカ」：ETM FinTech は完全に保護されたネットワークプロトコルと厳密な暗号化技術によってサポートされ、真新しい分散型の En-Tan-Mo ブロックチェーンを開発する。そのブロックチェーンには新たな貨幣規則とシステムを生成し、法定通貨と交易あるいは交換することができる。

「マサッヂオ」：ETM FinTech は、資産のセキュリティとデータの完全性を確保するため、En-Tan-Mo のスマートコンタクトを開発し、ゼロ知識に関連する技術でライトニングネットワークを開発し、取引速度を向上するとともにブロックチェーンの負担を軽減し、そのスケーラビリティを高める。

「ダ・ヴィンチ」：ETM FinTech は En-Tan-Mo を使用し、幅広いアプリケーションシナリオでエコシステムを進化させる。そしてスマートコンタクトの契約基準の開発はその基盤である。株式、プライベートエクイティ、クラウドファンディング、債券、ヘッジファンドなどのあらゆるタイプの金融デリバティブ（先物、オプションなど）を含む金融取引は En-Tan-Mo での使用が可能になる。

「ジョルジョーネ」：この期間内において、En-Tan-Mo は更に経済領域を超えて、全世界における物理的リソースと人的資産の分配に参与し、自動配達、インテリジェントネットワーキングアプリ、サプライチェーン自動化管理、仮想資産交換、資産登録なども含め科学、健康、教育などの分野での大規模な共同作業を促進する。

そのシステムが開放すると、ETM FinTech はシステムを制御しなくなった。システムの利害関係者、トークンの所有者、また関心を寄せた研究者だけがシステムの将来の展開を決定する。

7.3 ETM BD ビジネス会社

ETM BD の役割は企業を開発、支援し、そして En-Tan-Mo の派生チェーンエコシステムにこれらのビジネスを統合することである。En-Tan-Mo は、自由派生連鎖、スマートコンタクトおよびアプリケーションホスティングなどを統合する方案を提供し、使い安く、十分な機能を有し、プラグアンドプレイのシステムを作成することに取り込んでいる。En-Tan-Mo エコシステムを利用し、開発者は En-Tan-Mo のアプリを迅速的に開発し、そして分散型のアプリストアに公開することができる。これらのアプリは、プラットフォーム中の分散ノードによってダウンロードおよび実行され、通常のユーザーに提供される。この過程の安全は正直かつ安全な En-Tan-Mo 派生チェーンネットワークによって保証される。

ETM BD は直接投資、共同 ICO、開発支援、解決方案の提供などの柔軟な方法を通して、En-Tan-Mo ブロックチェーン技術に关心を寄せ、この技術を通して産業を改革したい個人や企業を支援し、En-Tan-Mo ブロックチェーンの運用を実現する。

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



"En-Tan-Mo" Organization Structure

后注:

1、政策リスク

現在ブロックチェーンプロジェクト及びスワップ・ファイナンスに対しての規制政策は、各国ではまだ明確ではない。したがって、その不透明な政策のゆえ参加者に損失をもたらす可能性がある。また、デジタル資産市場の価値が過大に評価されれば、投資リスクも増加する。参加者はスワップ・プロジェクトの成長が過度になると予想し、この高期待に応じない可能性もある。

2、規制リスク

En-Tan-Mo を含むデジタル資産の取引の不確実性が極めて高い。デジタル資産取引における強力な規制が欠如するため、電子トーケンが暴騰または暴落し、更にディーラーによって制御されるリスクもある。個人参加者は市場に参入してから経験が不足のため、市場の不安定さからもたらした資産ショックや心理的な圧力に抵抗するのが難しい。学界の専門家や公式的なメディアは、慎重な参加することを提案したが、書面による規制や規定がないため、このようなリスクを効果的に回避することは困難である。

将来ブロックチェーンと電子トーケンフィールドを制限する規制条例が導入されることはあることである。この領域を規範的に管理すれば、スワップ期間中に購入されたトーケンの価格の変動または販売の容易さに影響を与えるのであろう。

3、チームリスク

現在、ブロックチェーン技術の分野には多くのチームとプロジェクトが存在している。市場競争が激しく、プロジェクトを運営する圧力も高い。En-Tan-Mo は多くの優秀なプロジェクトからはみだして広く認識されるかどうかは、チームの能力と計画と関係がある。その一方、市場において多くの競合相手または寡頭の存在によって影響をされ、悪質な競争に巻き込む可能性がある。En-Tan-Mo の創業者の人脈が広い上、ブロックチェーン分野のベテランや経験豊富な技術開発者を招聘され、活力ありかつ才能を備えたチームを集めた。チーム内の安定性と結束は、En-Tan-Mo の発展にとって不可欠なものである。しかし、今後の発展において、コア要員の退職やチーム内部紛争が起こることにより、En-Tan-Mo にマイナスな影響をもたらす可能性もある。

免責条項

本文書は情報提供のみを目的とし、内容は参考用であり、En-Tan-Mo またはその関連会社の株式あるいは有価証券を売却するための投資勧誘することがない。以上のような勧説は、極秘な備忘録の形で行われる必要がある一方、証券の適用法とほかの法律を守るべきである。本文書の内容もインターチェンジへの参加を勧説するものとして理解されるべきではない。本文書の副本を要求するかまたは本文書を他人と共有することを含め、本文書と関連する行為は、インターチェンジへの参加と解釈されるべきではない。取引に参加するには法定年齢となる行為能力者である。En-Tan-Mo と締結した契約は真実かつ有効であり、そしてすべての参加者は契約する前に十分に En-Tan-Mo の内容を理解し、本人の意識に基づき締結したものである。

En-Tan-Mo チームは、本文書の情報が真実かつ正確であることを確保するため、引き続き合理的な試みを行う。開発過程において、プラットフォームメカニズム、トーケン及びそのメカニズム、トーケンの配布などを含みプラットフォームが更新される可能性がある。そして、プロジェクトの進捗に合わせ本文書の内容の一部を調整することもあるが、本チームは更新された文書をウェブサイトで公開し、参加者に提供する。参加者は更新された文書に基づき方策を調整する。本書の内容に依頼し不正確な行為により損失をもたらすことに対して En-Tan-Mo は一切の責任を負わない。本チームは本書で言及された目標を達成するために努力を惜しまないが、外部介入の要素が存在するゆえ、本チームは完全に目標を実現することができない可能性もある。

En-Tan-Mo は投資商品ではなく、プラットフォームの運営にとって重要なツールである。En-Tan-Mo の所有者は、En-Tan-Mo プラットフォームの所有権、管理または決定権を持つとはいえない。En-Tan-Mo はデジタル暗号化トーケンとして以下のカテゴリに属しない。

- (a) あらゆる通貨。
- (b) 有価証券
- (c) 法人の持分
- (d) 株式、債券、手形、ワント、証明書または権利を付与する文書。

En-Tan-Mo の付加価値が、市場法則と需要によって決められる。本チームはその付加価値が必ず上昇することを保証せず、そしてその価値の上昇と低下によりもたらした結果にも責任を負わない。適用法で許可されている最大限の範囲内で、本チームは直接的または間接的な個人損害、商業的利益の損失、ビジネス情報の損失、またはほかの経済的な損失を含み、インターチェンジへの参加によりもたらした損失に一切の責任を負わない。

En-Tan-Mo プラットフォームは、あらゆるインターチェンジ業界の健全な発展を促進する規制条例と業界の自己規律に関する声明を遵守する。そして En-Tan-Mo の参加者もその規範を完全に受け入れ、遵守する。同時に、参加者は検査されたすべての情報が正確であること保証する。

En-Tan-Mo プラットフォームは参加者に起こりうるリスクを明らかにした。インターチェンジの参加者は、En-Tan-Mo の各条項を認め、プラットフォームの潜在的なリスクも自己責任で受け入れることを確認していた。

備考：

この文書は英語の技術白書を日本語で翻訳したものですが、正確性を保証しようとしていますが、英語版との差異は軽微ですが、この文書の内容と解釈が英語版と異なる場合は英語版をベンチマークとして使用します。