

# **EN-TAN-MO**

---

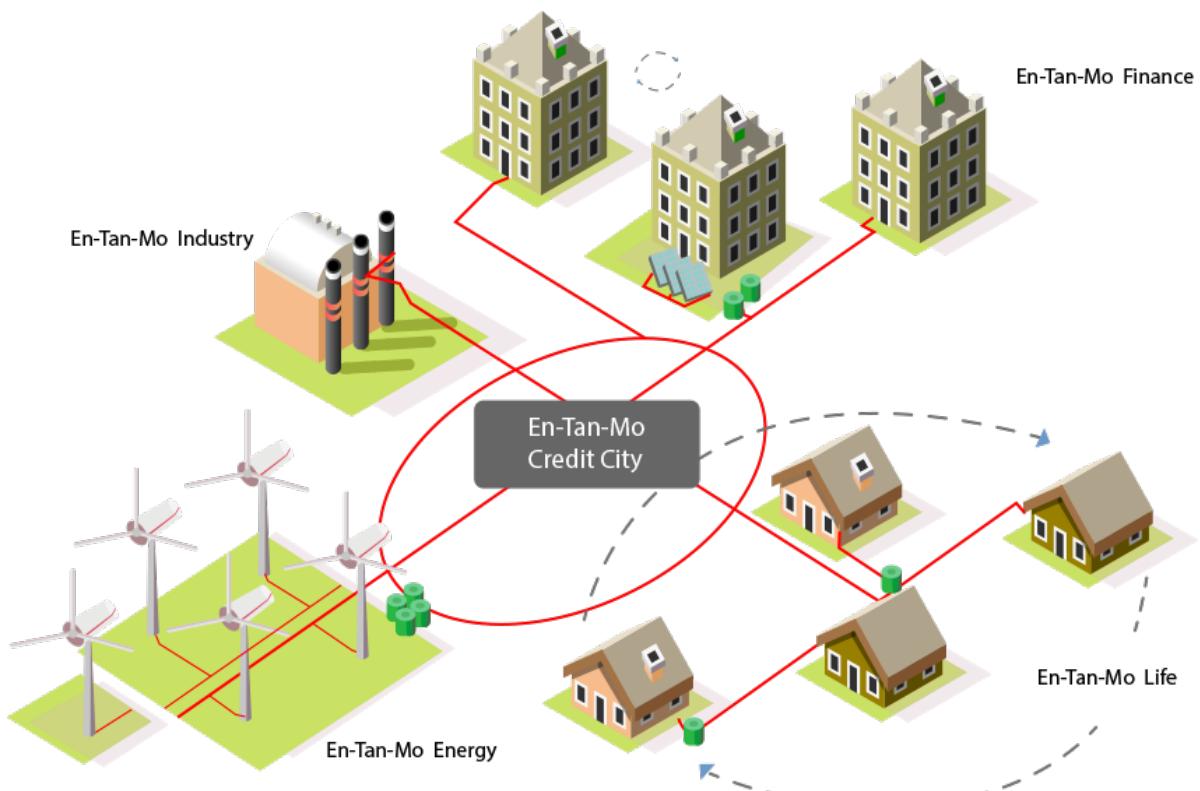
# **SCIENCE**

---

Français

# Introduction

Le nom En-Tan-Mo est une abréviation des mots Entente, Transaction et Mole. En-Tan-Mo, est un projet de blockchain de nouvelle génération, basé sur la théorie des jeux et le transfert de valeurs. En-Tan-Mo a été conçu selon des méthodes de théorie des jeux avancées, et a atteint la complétude SHD. Parmi les membres du projet, on compte Thomas Sargent, prix Nobel d'économie 2011 ; des chercheurs de l'Université de technologie de Californie, de l'Université de Maryland, et de l'Institut Henri Poincaré. En-Tan-Mo. Dans le monde d'En-Tan-Mo, les mineurs Stakhnov et les pools de minage Pareto se soutiennent et s'encouragent, créent des communautés autonomes fondées sur les principes d'équité et d'impartialité. En-Tan-Mo est un système ouvert et inclusif, en ce sens qu'il incorpore les applications et communautés de nombreux autres systèmes (blockchains ou non-blockchains). En plus d'être à l'avant-garde de la technologie en termes de conception mathématique, En-Tan-Mo offre le plus grand nombre d'applications et une communauté d'utilisateurs plus large que celle de n'importe quelle autre système de blockchain. En-Tan-Mo est aussi le fruit d'une réflexion de fond quant à ses implications philosophiques et économiques. De fait, nous ne saurions nous contenter ici d'un simple livre blanc « technique » : il est indispensable d'évoquer l'importance et la complexité d'En-Tan-Mo. Notre équipe de développeurs expliquera donc au lecteur le potentiel et les applications d'En-Tan-Mo en termes philosophique, mathématiques et économiques, et mettra le système en relation aux écosystèmes, aux systèmes de tokens et plus encore. Ce document s'adresse à toute personne qui s'intéresse à En-Tan-Mo. Vous y trouverez le contact de chaque membre de notre équipe sous la forme d'une UNI-ID et d'un portefeuille électronique.



## 0.0 Qu'est-ce qu'En-Tan-Mo ?

Pour prendre la mesure de la révolution représentée par En-Tan-Mo, il peut être intéressant de retracer brièvement l'histoire des blockchains.

En 2008, Satoshi Nakamoto publie Bitcoin : a peer-to-peer electronic cash system. En janvier 2009, le bloc originel est créé et l'ère du Bitcoin s'ouvre. En 2013, une nouvelle version de Bitcoin, la plus importante à ce jour, est mise en service. Cette version améliore Le système de gestion interne et d'optimisation du réseau. À partir de là, Bitcoin devient un phénomène mondial. En dépit du succès que lui garantit son statut de cryptomonnaie originelle, le développement de Bitcoin est entravé par sa faible capacité à évoluer. Cette étape est appelée « ère de la blockchain Bitcoin 1.0 ».

Vitalik Buterin crée Ethereum afin de résoudre ce problème d'évolutivité. Ethereum possède une structure de design clairs. Ces développements constituent une transformation importante : d'EVM à ICO, de différentes versions de POC à Frontier en 2015, de POW Metropolis à POS Serenity. Les marques de fabrique de « Blockchain 2.0 » sont le Turing-complet, les contrats intelligents, les algorithmes résistants à ASIC et les Apps de blockchains. Ethereum offre des nœuds de plate-formes et des langages de programmation tels que les développeurs sont en mesure de créer et mettre en service une nouvelle génération d'Apps de types répartis.

En février 2018, la puissance informatique de bitcoin atteint 20EH/s. Github compte plus de 90 000 projets en open source. On trouve des développeurs dans plus de 90 pays, y compris la Chine, les États-Unis, la Grande-Bretagne, Singapour, la Russie, le Japon et la Corée du Sud. De 2008 à 2018, il n'aura fallu qu'une décennie pour que le concept de blockchain soit accepté et connu du grand public. Ce succès soudain est évident si on le compare avec le développement d'Internet. Internet apparaît en 1974, lorsque l'ARPA inaugure le TCP/IP, mais ce n'est qu'en 1994, soit vingt ans plus tard, que la Chine est officiellement connectée au réseau.

### 0.1 Pourquoi En-Tan-Mo ?

En-Tan-Mo a pour but de créer un monde organisé, équilibré et efficace, qui génère de la valeur et embrasse l'ère de blockchain 3.0. Pour cette raison, et ce depuis sa création, En-Tan-Mo fait preuve de clarté en ce qui concerne ses deux problèmes d'intégration principaux.

#### La complétude SHD

Dans les systèmes distribués le théorème CAP établit qu'il existe une incompatibilité entre la cohérence, la disponibilité et la tolérance au partitionnement. L'hypothèse de Satoshi Nakamoto est qu'un type de consensus uniforme peut être atteint dans les blockchains, par le biais d'une forte cohérence des probabilités. C'est ce qu'on appelle le consensus de Nakamoto.

Dans les systèmes de blockchains, le problème SHD est, de même que dans le théorème CAP, qu'il n'existe nulle compatibilité entre sécurité, haute performance et décentralisation.

Dans l'hypothèse d'un processeur peu performant, la théorie de Satoshi Nakamoto permet la coexistence de la sécurité et de la décentralisation, mais au sacrifice de la haute performance.

En raison de l'algorithme de consensus et de la conception évolutive de Bitcoin, un bloc est produit toutes les dix minutes et il ne peut y avoir que sept transactions par minute. De plus, avec l'émergence des systèmes de minage ASIC, la probabilité de parvenir à miner un bloc avec un processeur normal tombe presque à zéro. Les systèmes de minage obtenaient jadis un ratio de récompenses extrêmement linéaire. Toutefois, l'émergence des pools de minage a totalement anéanti cette promesse de décentralisation. De fait, Bitcoin a cessé d'être une communauté égalitaire. Pire encore, il n'est pas exclu que plus de 51 % de la puissance computationnelle ne tombe

aux mains des pools de minage. Un tel monopole conduirait à une concentration des pouvoirs qui menacerait la sécurité du système tout entier. Nous concluons que le système Bitcoin ne répond plus aux critères d'équilibre SHD.

Pour contrer l'impact destructif des systèmes ASIC, Ethereum a adopté l'algorithme de résistance à ASIC afin de maintenir – pour un temps du moins – la sécurité et la décentralisation. Toutefois, la première application à grande échelle du contrat intelligent CryptoKitties, dont Ethereum est si fier, a provoqué l'effondrement complet du système et mis en évidence ses lacunes en termes de hautes performances. Les systèmes de blockchain qui ont tourné le dos aux consensus POW au profit des POS ou des DPOS, dont EOS est le parfait représentant, ont considérablement augmenté la performance du système. Ceci étant, il s'agit essentiellement de systèmes centralisés.

Grâce à un consensus Kantorovich de type dual, En-Tan-Mo engendre une sélection juste entre mineurs, garantissant la séparation entre actionnaires et mineurs, ainsi qu'entre leurs intérêts respectifs. Il en découle une efficacité améliorée, sans centralisation ni perte de sécurité. Ainsi, En-Tan-Mo atteint la complétude SHD.

#### Des transferts de valeur équilibrés

Internet a modifié notre façon de transmettre l'information. Nous pouvons désormais transmettre une information beaucoup plus rapidement, quoi que pour un coût moindre, et il en découle une amélioration exponentielle de l'efficacité et à une maîtrise des coûts. Nous créons également des produits et services entièrement nouveaux. Néanmoins, un flux d'information est différent d'un transfert de valeurs. Ces derniers, sur internet, ne se font pas de point à point mais par le biais d'organisations centralisées, qui se chargent de maintenir la comptabilité. Il y a une raison à cela : le transfert de valeurs se doit d'assurer la propriété exclusive d'un bien (« jus in re », ou « droit réel

»), tandis que l'information est reproductive à l'infini.

Avec sa technologie de comptabilité distribuée, Bitcoin a établi un système de confiance décentralisé, indépendant de toute agence centralisée, de sorte à ce que le transfert de valeurs soit entièrement en peer to peer. Les règles de transfert de valeur et de tarification s'en sont trouvées bouleversées. Avec l'émergence des pools de minages, le système de transfert de valeur de Bitcoin a été compromis, du fait que la valeur s'est trouvée concentrée entre les mains des pools. Les détenteurs de machines de minage et les utilisateurs ordinaires ne sont plus égaux dans leur recherche de profits.

Ethereum se sert de l'algorithme résistant à ASIC et a proPOSé « Gas » afin de limiter les ressources sur les blockchains. Dans une certaine mesure, cela a ralenti l'accumulation de valeurs entreprise par les pools de minage. Nous considérons néanmoins que ces mesures sont inefficaces, et même contre-productives à long terme. Les systèmes utilisant le consensus DPOS, dont EOS est le parfait représentant, ont tenté de briser le monopole de puissance de calcul du POW afin de maintenir un équilibre. Mais les grands actionnaires ont gardé la main sur le flux de distribution de valeurs, ce qui n'a fait que centraliser encore un peu plus le système.

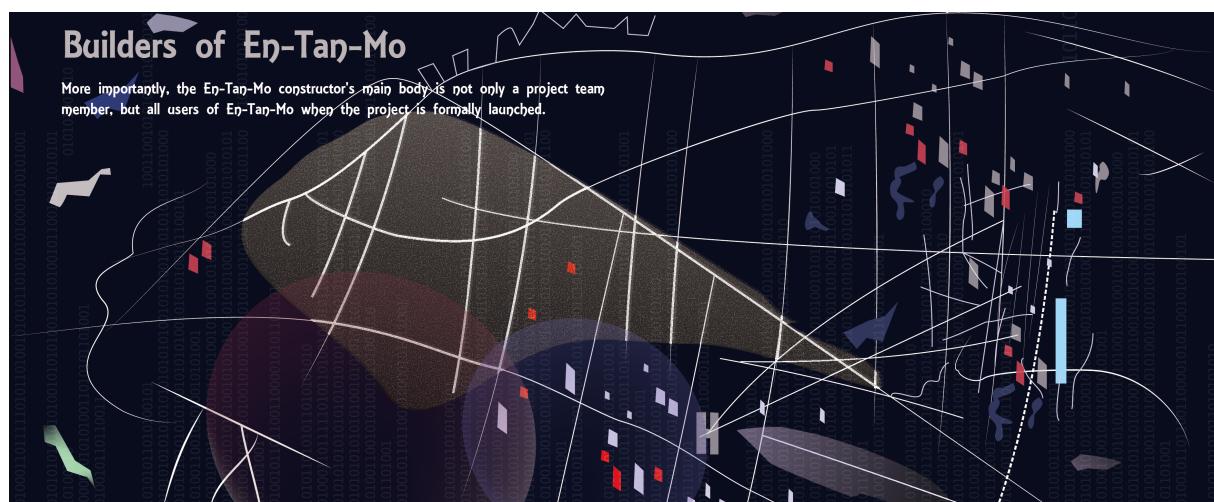
Si l'on se base sur la situation actuelle des blockchains et des cryptomonnaies, la distribution de valeurs est proche d'une distribution Pareto en haute concentration. En-Tan-Mo compte développer la transmission d'informations par le biais d'internet, modifier la manière dont les valeurs sont transmises vers une circulation ouverte, et fournir un système de transfert de valeurs équilibré à ses utilisateurs. En-Tan-Mo considère que chaque usager est à la fois acheteur et fournisseur (vendeur) de services. Au cœur d'un marché décentralisé, on trouve la formation des prix, prix qui émergeront spontanément d'un équilibre dynamique. En-Tan-mo étudie la formation des prix sous l'angle de la théorie des Jeux à champs moyen. En termes d'élections, le droit de vote doit être corrélé POSitivement aux enjeux ou aux capacités de minage, mais la dépendance doit être non-linéaire. Un tel système empêche la haute concentration de pouvoirs, créé un nouveau genre « d'internet des valeurs », modifie notre manière de faire du business et nos relations socio-économiques.

## 0.2 Les concepteurs d'En-Tan-Mo

Les concepteurs d'En-Tan-Mo proviennent des meilleures universités et instituts de recherche du monde. À l'origine, il s'agissait d'un groupe de mathématiciens, qui ont appliqué la théorie des jeux au développement des systèmes de blockchains. Par la suite, des experts issus des champs de la télécommunication, de l'informatique et de l'économie ont rejoint l'équipe. Depuis, En-Tan-Mo a adopté un système de validation rigoureux : dans un premier temps, les mathématiciens proPOSSent un modèle de consensus ; dans un second temps, les informaticiens et les experts en télécommunications mettent ces modèles théoriques à l'épreuve des faits, à travers une série de simulations numériques et d'expériences hardware.

Ce projet a pu aboutir grâce à un processus de coopération renforcée entre des équipes interdisciplinaires. Le mécanisme de consensus Kantorovich a été conçu par nos experts en mathématiques, télécommunications et informatique. On compte également, pour le développement du codage, des ingénieurs informatiques issus de Google, Thunder et Baidu, entre autres entreprises leaders dans le domaine cybernétique.

Mais ce qui est plus important encore, c'est qu'après le lancement du projet, la communauté des concepteurs d'En-Tan-mo ne se limitera plus aux membres de cette équipe de développement, du fait qu'elle comprendra tous les utilisateurs du système. En tant que système participatif et auto-évolutif, En-Tan-Mo permet à tous ses utilisateurs d'uploader activement des compartiments et de développer des chaînes dérivées, selon leurs besoins. Les développeurs d'En-Tan-Mo se voient comme les initiateurs et bâtisseurs d'une infrastructure. Cette équipe fera tout ce qui est en son pouvoir afin de fournir un service technique sûr, stable et efficace qui servira de base aux évolutions qui s'ensuivront. De surcroît, l'équipe En-Tan-Mo est impatiente de collaborer avec les chercheurs, les ingénieurs et quiconque se sent proche de la philosophie En-Tan-Mo.



### **0.3 la science d'En-Tan-Mo**

En-Tan-Mo est davantage qu'un projet de blockchain. C'est un projet de recherche aux implications philosophiques, mathématiques et économiques, et aux applications infinies. Les développeurs invitent tous ceux qui s'intéressent à ce projet à se plonger dans une série d'essai, dont voici le sommaire.

---

Chapitre 1 : L'univers En-Tan-Mo. En-Tan-Mo offre un univers de blockchain 3.0, constitué de services améliorés et de valeurs innovantes. L'univers En-Tan-Mo se concentre sur l'amélioration, la restructuration et la création de marchés. Cela conduira à une génération et une transformation du concept d'équilibre en tant que valeur essentielle en business.

Chapitre 2 : la philosophie En-Tan-Mo. En-Tan-Mo est un système de transmission de valeur entièrement nouveau, qui connecte tout ce qui a de la valeur via blockchains. Ainsi, la nature décentralisée d'En-Tan-Mo incarne ses principes essentiels : pouvoirs décentralisés, ouverture, égalité des chances, participation, interaction et évolution.

Chapitre 3 : Les mathématiques d'En-Tan-Mo. Nous aborderons En-Tan-Mo sous l'angle des mathématiques. Nous évoquerons nos conclusions provisoires, les plans de recherche à venir et une présentation rapide des outils mathématiques à la base d'En-Tan-Mo.

Chapitre 4 : L'économie d'En-Tan-Mo. Dans le cadre du consensus Kantorovich, mineurs Stakhanov et mineurs Pareto se soutiendront mutuellement et partageront les fruits de leur travail. En plus de l'innovation technologique, En-Tan-Mo porte en lui une logique de business réformée.

Chapitre 5 : La science informatique En-Tan-Mo. Nous expliciterons la structure de donnée d'En-Tan-Mo, le nœud API et les codes de nos ingénieurs informatiques, de sorte à démontrer les avantages du système de consensus Kantorovich.

Chapitre 6 : l'écosystème d'En-Tan-Mo. Avec sa technologie multi-chaînes, En-Tan-Mo comprend deux catégories de chaînes : les chaînes centrales et dérivées. Cette structure permettra aux blockchains de sortir de l'isolement, de se connecter à des systèmes externes et de s'étendre. Ainsi, il est possible de concevoir un système de blockchains qui incorpore, par le biais des Apps, plus de dix millions d'utilisateurs.

Chapitre 7 : le fonctionnement d'En-Tan-Mo.. La communauté En-Tan-Mo se compose de trois organisations. La Fondation En-Tan-Mo, Emgo et OEM. La Fondation apportera son assistance aux utilisateurs, et garantira la stabilité opérationnelle du système. Emgo se chargera de la recherche, en termes de confidentialité, de sécurité et de développement du système. OEM encadrera les partenariats commerciaux.

---

#### **References:**

- [01] S. Nakamoto. A Peer-to-Peer Electronic Cash System. [www.bitcoin.org/bitcoin.pdf](http://www.bitcoin.org/bitcoin.pdf), 2009.
- [02] M. E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory*, 26(4):401-406, 1980.
- [03] V. Buterin. Long-range attacks: The serious problem with adaptive proof of Work. <https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-withadaptive-proof-of-work/>, 2014.
- [04] V. Buterin. Proof of stake. [https://github.com/ethereum/wiki/wiki/Proof-of-Stake\\_FAQ](https://github.com/ethereum/wiki/wiki/Proof-of-Stake_FAQ), 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.
- [11] R. Perez-Marco. Bitcoin and Decentralized Trust Protocols. Newsletter of the European Math. Soc., 100 p.32, 2016.

# 1.0 L'univers En-Tan-Mo

## 1.1 L'architecture d'En-Tan-Mo

"En-Tan-Mo" est un projet international d'innovation scientifique au croisement de disciplines telles que la philosophie, les mathématiques, l'économie et l'informatique. En-Tan-Mo est l'émanation d'un monde nouveau et subversif.

L'architecture de l'univers En-Tan-Mo : une trame dont chaque fil représente une offre ou une demande. Chaque participant est un électron libre. Il lui appartient d'entretenir une relation avec n'importe quel fil de son choix, ou d'ajouter ses propres fils. Ce réseau, dont la latitude et la longitude s'entremêlent du fait d'un mécanisme aléatoire et chaotique, persiste à s'améliorer grâce à un processus d'apprentissage automatique auto-adaptatif. Dans l'univers En-Tan-Mo, chacun contribue à refaçonner le monde à travers ses actes. Cette liberté de mouvement est susceptible de façonnner des hommes plus rationnels, plus actifs, plus autonomes et plus prévoyants.

L'effondrement de la pyramide et une véritable décentralisation libèrent du totalitarisme et du monopole. En-Tan-Mo persévétera sur le chemin de l'égalité et de la liberté. Ce projet s'efforce de créer un monde d'incertitude, d'innovation et d'équilibre généralisé. Chacun suit exclusivement la dynamique du libre-échange et réagit rationnellement aux opportunités qui se présentent à lui. Dans l'univers En-Tan-Mo, on ne se contente plus de rester passif et d'attendre son salaire mensuel : on se crée un revenu en s'engageant dans des projets existants, ou en créant son propre projet. La valeur des transactions sera déterminée par un processus d'équilibre dynamique afin de garantir l'équité.

## 1.2 Histoire mondiale des cryptomonnaies :

Au fur et à mesure que se développera internet, les technologies de blockchains rendront obsolète la centralisation des applications. Les Tokens, comme les monnaies qui les ont précédés, peuvent amplifier la vitesse et l'évolutivité des transactions online. Internet ne se limitera pas à l'échange de données mais deviendra une plate-forme essentielle à l'échange de valeurs. En 2009, Bitcoin a créé un système « d'or électronique » et internet a connu plusieurs vagues de ruées vers l'or. Depuis le début de l'année 2018, avec un taux de hachage d'environ 30000PH/s, il n'est possible de miner que six blocs par jour (pour 75 Bitcoins de récompense). Selon l'index de consommation d'énergie Bitcoin de Digiconomist, la consommation électrique annuelle de Bitcoin est aujourd'hui de 39,45TWh (coût approximatif : 200 Millions de dollars). Lors de la ruée vers l'or américaine de 1848-1851, il y eut une augmentation soudaine de la population, une pénurie de nourriture, de vêtements et de services sociaux. L'index des biens de consommation courante passa de 847 à 1025.

Aujourd'hui, la ruée vers le Bitcoin est d'une ampleur comparable. S'il fallut des siècles à l'or pour s'imposer en tant que standard monétaire, il n'aura fallu que neuf ans à Bitcoin pour y parvenir.

En 2013, Vitalik Buterin lance Ethereum et, dans la foulée, une nouvelle génération de cryptomonnaies et de plate-formes d'applications décentralisées. Cette innovation crée un système Turing-complet de contrats intelligents, et ETH devient rapidement « le carburant électronique ». Ethereum offre un grand nombre de modules à ses utilisateurs, afin de créer des applications plus vite mais pour plus cher. Pour être précis, Ethereum crée une application grâce à l'Ethereum Virtual Machine Code (Langage EVM). L'application qui en découle, le cœur d'Ethereum, est dénommée contrat intelligent. Le contrat intelligent équivaut à un agent automatisé dans le système Ethereum. Lorsqu'un usager envoie une transaction à l'adresse du contrat, celui-ci est activé. Ensuite, selon les informations additionnelles de la transaction, le contrat se sert de son propre code et délivre un résultat. Ce résultat peut initier une autre transaction à partir de l'adresse du contrat. L'échange Ethereum peut être une transaction ou un segment d'instructions. L'avantage de ce système est qu'Ethereum peut être utilisé en de larges quantités. Le désavantage est que ces contrats sont coûteux, ce qui risque de conduire à la chute d'Ethereum. Si on comparait Ethereum à une autoroute non-évolutive, les applications seraient des véhicules et ETH le carburant. Aujourd'hui, la plupart des 900,000 contrats présents sur Ethereum sont des applications de tokens similaires. On pourrait parler d'une autoroute très encombrée, et très coûteuse.

En somme, Bitcoin représente une économie fondée sur l'or et Ethereum une économie fondée sur l'énergie. Dans ces deux types d'écosystèmes économiques, on peut raisonnablement prédire la tendance des développements à venir.

Le Monde-Pyramide : La valeur de l'or et du pétrole est relative à leur rareté. Une économie-or peut se substituer à une économie-énergie si l'énergie devient un bien non-renouvelable indispensable à la survie de l'humanité. Cette structure énergétique fait du monde une super-pyramide, avec certains pays au sommet et d'autres qui fournissent une main d'œuvre bon marché. En son sein, chaque pays forme lui-même une pyramide, avec des entreprises puissantes à son sommet et d'autres pour leur fournir des services à bas-prix. Et au sein même de chaque entreprise ou organisation, on trouve une autre pyramide, dans laquelle les salariés de base travaillent contre une maigre rémunération. Le monde est une pyramide fractale, qui subit une pression croissante de la part de son sommet. Tôt ou tard, la pyramide s'effondrera et une crise économique adviendra. Ensuite, une autre pyramide émergera des ruines de la précédente, et le phénomène se poursuivra de manière cyclique.

## 1.3 Émigration de masse En-Tan-Mo

1) Structure duale POW/DPOS : briser le monopole et la centralisation

Genèse des POW : Dans le monde réel, le consensus dépend du « coût du travail » et la valeur de l'argent est définie en fonction d'une certaine quantité de « travail ». Dans le monde des blockchains, le consensus dépend du « coût informatique » : les tokens électroniques sont obtenus en fonction des ressources computationnelles investies. L'introduction des systèmes de POW a permis d'établir un équilibre stable, qui a servi de base à la stabilité à venir de la valeur du token. Depuis l'avènement de Bitcoin et Ethereum, la POW fait consensus.

La structure duale POW/DPOS : L'équité des systèmes de POW a été réduite à néant par les machines de minage. Cette mise à mort de l'équité par le biais d'innovations technologiques s'est produite à de nombreuses reprises au cours de l'Histoire. DPOS a accéléré ce processus du fait d'une absence totale de coûts informatiques intégrés. Ce phénomène est comparable à l'émergence de l'inflation et de la concentration dans n'importe quel autre système de tokens. La structure duale POW/DPOS peut limiter les tendances centralistes des mécanismes de POW ou de DPOS pris séparément. Ainsi, un mécanisme décentralisé garantit haute performance et sécurité. Les actionnaires et les mineurs sont tous à même de participer aux processus décisionnels d'En-Tan-Mo.

2) La coopération compétitive des mineurs : des règles de coalition justes

Dans les systèmes POW, les mineurs doivent hacher et sont en compétition les uns avec les autres. C'est un système insatisfaisant, coûteux sur le plan énergétique. En conséquence, les mineurs forment des coalitions au sein des pools de minage, mais il en découle une intensification de la centralisation. La théorie de la compétition coopérative considère que le minage est un jeu à somme nulle. Dans le consensus En-Tan-Mo, les relations interactives entre mineurs sont analysées par la théorie du jeu, de sorte à être justes et à mettre en œuvre un système incitatif raisonnable.

La compétition coopérative est le seul système qui soit en mesure de renouveler le concept de chaîne de valeur auprès des usagers, et pour transmuer cette chaîne de valeur en expression des connexions interactives qui les lient. Le concept de chaîne de valeur met en avant le comportement de compétition et de coopération simultané qui se met en place au sein de l'univers En-Tan-Mo. La combinaison des deux engendre une relation dynamique. Les mineurs se lient d'une façon nouvelle, que l'on peut définir en trois mots : Impact, Intimité et Vision. Ce concept comprend les résultats effectifs et concrets obtenus par les mineurs après avoir établi une relation compétitive et coopérative, à savoir une valeur et une productivité augmentées. Cet état de fait découle essentiellement de trois facteurs : la réduction des doublons du gaspillage, des ressources computationnelles

et de la consommation électrique ; une accélération de la croissance de la blockchain ; la création d'opportunités nouvelles du fait de la création de nouvelles blockchains.

3) Offre et demande dynamique, rationalité et Équilibre de Nash

Rejoindre En-Tan-Mo, c'est se joindre à la meilleure coalition qui soit dans le monde électronique. Au sein des pools de minage habituels, l'intensification de la compétition mène peu à peu à un système insatisfaisant. Sous la direction de Thomas Sargent, prix Nobel d'économie 2011, En-Tan-Mo applique la théorie de la prédition rationnelle afin de fournir un mécanisme d'offre et de demande dynamique qui conduit à une formation en temps réel de l'Équilibre de Nash, fondée sur les stratégies rationnelles des participants. La coopération sélective incarne l'offre et la demande. La valeur est la combinaison organique du coût et de la demande. Au sein d'En-Tan-Mo, l'élément « coût du POW » et l'élément « offre-demande DPOS » s'allient pour former des règles de coalition à valeur maximale et conduisent à une instabilité réduite.

4) Mécanisme de fonction concave et enjeux de l'équilibre

Traditionnellement, les alliances tendent à favoriser les collaborateurs les plus puissants. Plus ils sont forts, plus ils sont récompensés. Ce modèle de revenu super-linéaire finira par nuire aux collaborateurs les plus faibles, et c'est ce qui conduit à la formation et à l'effondrement de la pyramide. En-Tan-Mo, en prêtant une attention particulière à l'effet de longue traîne, permet à la quasi-totalité des partenaires de faire des bénéfices conséquents. Il en découle une structure de coalition plus viable. Les collaborateurs puissants, qui ont renoncé à certains bénéfices au départ, font des profits plus importants à l'arrivée.

Les fondations de l'univers En-Tan-Mo sont précisément le type d'algorithme de contribution qui éliminent l'effet « licorne » des pools. Elles transforment la fonction arithmétique linéarisée « totalement égalitaire » en fonctions concaves, qui permettent une répartition des revenus plus juste et plus large. Du fait d'un mécanisme d'anticipation rationnelle, un public plus large fera consensus, et En-Tan-Mo s'affirmera comme le réseau de blockchain le plus juste.

5) Mélange chaotique, résistance aux attaques Sybil et aux attaques en coalition

En théorie SHD, le problème inévitable entre décentralisation et sécurité est celui de l'attaque Sybil. L'attaque Sybil, en sécurité informatique, est une attaque au sein d'un système de réputation qui est renversé par la création de fausses identités dans un réseau informatique peer to peer. Grâce à ce grand nombre de fausses identités, l'attaquant acquiert une influence disproportionnée. Les attaques de coalition conduisent à des situations similaires.

Les mathématiciens se sont servis de théories de systèmes dynamiques similaires, de la topologie, ainsi

que d'une théorie des bifurcations structurelle d'ensembles invariables afin d'étudier la stabilité des systèmes et les méthodes de contrôle. Ils ont proPOSé une méthode puissante de mélange chaotique, fondée sur la théorie ergodique et une dépendance sensible aux conditions initiales. Ainsi, un mécanisme pseudo-aléatoire puissant permet l'élaboration de séquences de minage aléatoires, qui ont le potentiel de parvenir à une sécurité POST-quantique.

6) La bibliothèque de comPOSants libre d'accès et le forum amical des développeurs définissent la direction de l'évolution et de la participation

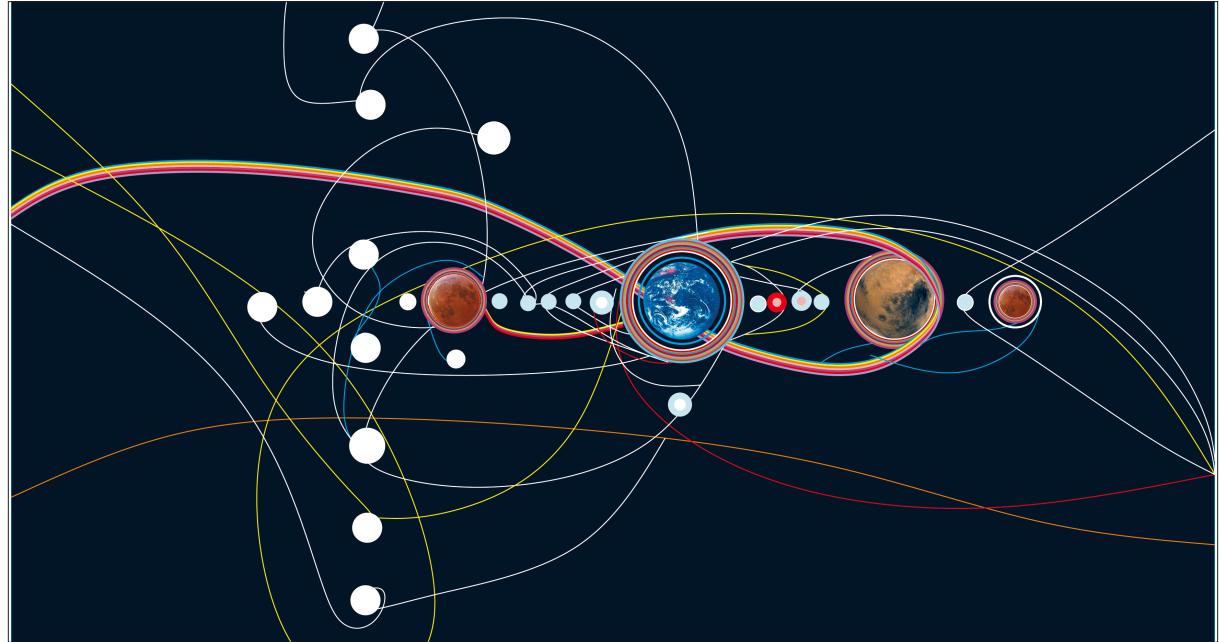
En-Tan-Mo est basé sur le concept de BaaS (Blockchain as Service) et le standard du micro-service. Avec la bibliothèque de comPOSants auto-évolutifs libre d'accès en son cœur et la communauté des développeurs comme moteur, En-Tan-Mo proPOSe une invocation synchrone des soft channels pour les applications et données qui existent en-dehors de la blockchain. En-Tan-Mo donne aussi aux développeurs la POSSibilité d'uploader des comPOSants, de publier des critiques et de distribuer des récompenses dans le forum. Pour les usagers ordinaires, En-Tan-Mo fournit des portes d'entrée BaaS afin de mettre en œuvre une accessibilité du service après-vente.

POW : La Proof of Work (POW) est une contre-mesure économique visant à prévenir le déni ou le

mésusage de service. L'initiateur doit se livrer à un certain nombre de calculs, qui prennent un certain temps. Lorsqu'un nœud dans le réseau Bitcoin souhaite générer un nouveau bloc et l'intégrer à la blockchain, il doit résoudre une énigme. Les trois éléments clé de ce processus sont la POW, les blocs et le degré de difficulté. La POW et le travail qu'elle demande équivalent à sa méthode de calcul. Le bloc détermine la saisie des données et le degré de difficulté détermine la quantité de calcul requise.

POS : La Proof of Stake (POS). La POS introduit le concept de « temporalité de la monnaie », à savoir la durée de POSsession d'une certaine somme par tel ou tel participant. Indépendamment des énigmes relatives aux POW, la POS est calculée en fonction de la temporalité virtuelle de la monnaie. La durée de détention de celle-ci, ainsi que la quantité de monnaie détenue, accordent certains droits relatifs au vote et au revenu.

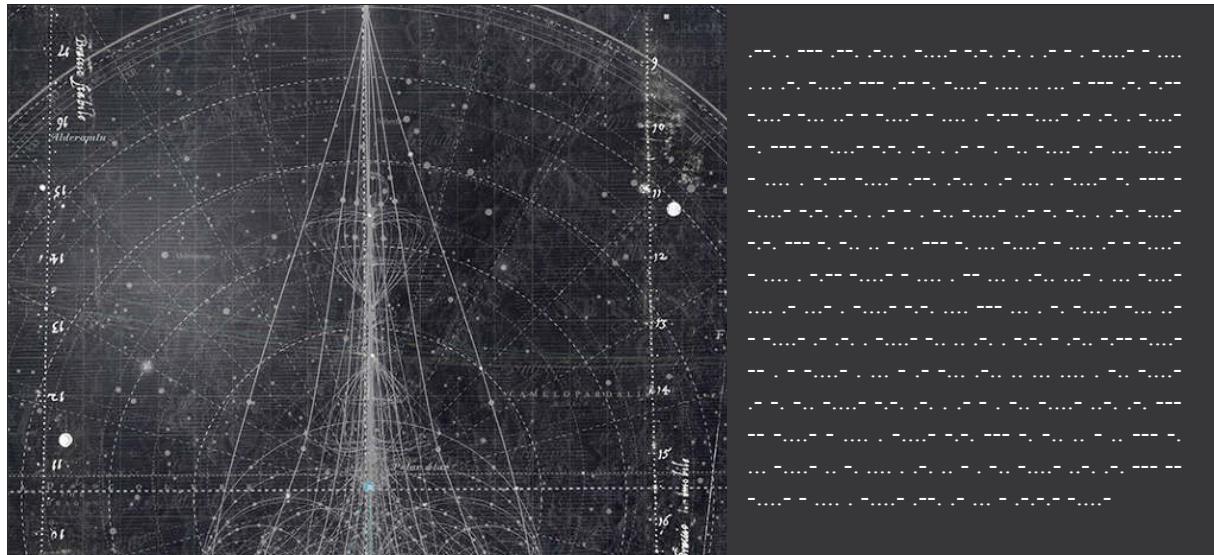
DPOS : Delegated Proof of Stake (DPOS) : La DPOS sélectionne un petit nombre de nœuds, de temps à autre et selon des stratégies variables. Ce petit groupe de nœuds créée, vérifie, certifie et supervise de nouveaux blocs. Cela réduit considérablement le temps nécessaire à la création et à la validation de blocs, ainsi que les coûts computationnels. Les POW et POS conventionnels doivent être confirmés par chaque nœud du réseau, pour tout nouveau bloc. C'est ce qui différencie la DPOS des deux méthodes suscitées.



Le nœud informatique « Hello! En-Tan-MoWorld » se joindra à une coalition informatique hybride. Il s'agit d'un comPOSant informatique de très longue durée. Chaque nœud opère des transactions en fonction de l'offre et de la demande, et est récompensé en conséquence. En-Tan-Mo est un échange de mandats digitaux à haute fréquence et à grande échelle, un pool de minage en coalition, et une plate-forme d'application DAPP. En-Tan-Mo est également la meilleure communauté de développeurs et la meilleure plate-forme de comPOSants d'applications de blockchains. Hello! Bienvenue dans un monde équilibré et égalitaire !

## 2.0 La philosophie En-Tan-Mo

En-Tan-Mo est une récréation des interconnexions de production et d'échanges du monde réel à travers l'homéomorphisme d'un espace abstrait, qui se réfère à une pensée philosophique. Dans l'immensité de sa structure, l'essence de la décentralisation est d'infiltrer En-Tan-Mo couche par couche, jusqu'à en extraire le concept du « moi omniprésent ». La philosophie d'En-Tan-Mo remonte aux sources de la philosophie grecque et à la célèbre remarque de Platon dans Protagoras : « L'homme est la mesure de toute chose ». La décentralisation a évolué à partir d'un monde où l'homme vénérait le divin, puis lui-même, puis plus rien du tout, de sorte que tous sont égaux. Les systèmes complexes et les structures multivariées, le consensus et la valeur, l'équilibre dynamique, l'auto-évolution et l'ouverture forment les caractéristiques décentralisées d'En-Tan-Mo.



### 2.1 Systèmes complexes et structure multivariée : "valeur du signal et échange de valeur"

La structure multivariée est décrite par un code symbolique et constamment libérée à l'intérieur du système complexe En-Tan-Mo. La structure multivariée modifie les chemins qui se dessinent à l'intérieur d'un système de réseau complexe. Le code symbolique se détache progressivement de l'objet en question, et de son contrôle de l'humain. Le système complexe En-Tan-Mo s'empare du code symbolique et le renvoie, modifié, à sa structure multivariée. Libérant le symbole du courant afin de changer le cours des choses, le code symbolique se plie au principe d'inclusion mutuelle. La multi-structure d'En-Tan-Mo déborde d'un système qui ne peut la contenir, s'interpose en son sein propre et définit le processus en dehors d'En-Tan-Mo. En sus des structures POSSédées par leur propre définition, il existe un surplus de signification. Le système complexe est intégré à la performance d'En-Tan-Mo, ce qui conduit à la co-variation de l'association. De nombreux rythmes, de nombreux sujets et de nombreuses combinaisons forment un système de valeur symbolique formel et un échange symbolique d'espace.

### 2.2 Consensus et Valeur: "Mire Plateaux"

Mire Plateaux (Gilles Deleuze + Félix Guattari, 1980) est emmêlé dans divers codes, couches, plans transcendantaux, espaces nuancés, etc. dans le modèle

idéologique traditionnel, tout cela avec une intensité de flux égale et réciproque à celle du « plateau » d'En-Tan-Mo. La connexion de diversité et d'hétérogénéité est au croisement de la communication entre les nœuds de chaînes. Le consensus est mis en lumière par la connexion, et la transmission de valeur devient POSSible. Le « Mire plateaux » est un élément qui influe la direction d'un segment. Il n'est pas seulement limité dans le temps, mais capable de retracer l'origine des idées et de la vie même. Cela signifie que nous pouvons retourner aux origines et revivre l'expérience initiale, le parcours d'intégration originel, ce qui nous conduira à éprouver une sorte de sensibilité marginale. L'égalité des nœuds est distribuée sur la surface évolutive d'En-Tan-Mo et distribuée dans une structure de passages récurrents. Le but est de décrire un état de faits réciproques, de maintenir l'équilibre entre sujets d'En-Tan-Mo, ou d'explorer un subconscient préexistant. L'équité de l'extraction de segments est conçue pour imiter un équilibre absolument parfait, tenu pour acquis, et cette imitation de l'équilibre est fondée sur la structure d'En-Tan-Mo, ou sur la surface équiaxiale qui la soutient.

### 2.3 Equilibre dynamique et décentralisation: "Les lettres persanes (Montesquieu, 1721)"

L'équilibre qui découle du développement de

l'univers En-Tan-Mo POSSède une vitesse similaire à celui-ci et passe par des étapes comparables. L'hôte ne se soucie plus de son invité, mais de la différence de rythme. L'équilibre dynamique d'En-Tan-Mo sera séparé de son invité préalable. Il n'y a pas d'hôte et d'invité, juste une réalité naturelle et un objet. L'unité de l'hôte et de l'invité est constamment réfrénée. Toutefois, dans le cadre de l'En-Tan-Mo généralisé, la nouvelle unité développe la complémentarité, et le sujet ne peut plus se livrer au dualisme.

Le Pouvoir Centralisé, qui est le problème des systèmes structurels libres, est toujours empêtré dans les éléments les plus puissants. La décentralisation d'En-Tan-Mo est autonome. L'autonomie n'est pas comparable à une liberté incomplète. Ce n'est qu'une forme plus centralisée et plus libre. « L'homme est né libre et partout il est dans les fers » (Rousseau, 1762). Il a été démontré que cette contradiction est une impossibilité métaphysique.

## 2.4 Évolution interne et ouverture: "La mort de l'auteur (Roland Barthes, 1967)"

Avec la déconstruction et la dissolution progressive du sujet, la structure elle-même devient le tout. L'individu définit les termes de sa propre signification et de sa propre existence dans son interrelation au tout. De fait, la structure elle-même a une existence propre en tant qu'entité, ainsi qu'une cartographie isomorphisme

de la réalité qui servira de base au récit historique et à son authenticité. De toute évidence, une structure statique continuera d'entrer en conflit avec l'évolution des structures historiques et la complexité structurelle du monde réel. Dans son célèbre livre Anthropologie structurale, Levi-Strauss a insisté sur la complexité des relations entre structure et évolution, sur leur importance dans le cadre d'une analyse socio-politique des sociétés humaines. Dans le contexte d'En-Tan-Mo, ce problème est résolu par l'intégration d'une logique auto-évolutive intégrée, de sorte que le système puisse garantir un synchronisme entre réalité et synchronisation qui préserve l'intégrité de la structure.

La mort de l'auteur fait référence au rôle de l'auteur en tant que sujet de sa création. Il n'a plus le monopole de son propre travail. L'identité de l'auteur a été anéantie par l'écriture contemporaine. De fait, les notions de temps, d'espace et d'origine doivent être reconSIDérées. Le procédé génératif d'En-Tan-Mo lui-même est une forme d'écriture. Son but est de parachever l'unité du libre-arbitre et une structure organisée dans une nouvelle conception de l'espace. Ce genre de création découle du procédé qui consiste à formuler une règle méta-historique ou à écrire l'histoire dans son propre système, et son authenticité sera déterminée par le consensus général. Pour quelque sujet que ce soit, les règles arbitraires et la réécriture de l'histoire conduiront à la tentation du Pouvoir. De fait, En-Tan-Mo ne se contente pas d'admettre la POSSibilité qu'un sujet créatif puisse être déconstruit, mais met ce processus de déconstruction en pratique afin de créer un système qui soit réellement décentralisé, réellement juste.

### 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 : ce 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'antécéderance qu'un père entretient avec son enfant. Tout au contraire, le scripteur moderne naît en même temps que son texte ; il n'est d'aucune façon pourvu d'un être qui précéderait ou excéderait son écriture, il n'est en rien le sujet dont son livre serait le prédicat ; il n'y a d'autre temps que celui de l'énonciation, et tout texte est écrit éternellement *ici et maintenant*. C'est que (ou il s'ensuit que) écrire ne peut plus désigner une opération d'enregistrement, de constatation, de représentation, de « peinture » (comme disaient les Classiques), mais bien ce que les linguistes, à la suite de la philosophie oxfordienne, appellent un *performatif*, forme verbale rare (exclusivement donné 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 Péchuchet, 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 hypothèses : la société, l'histoire, la

## 3.0 En-Tan-Mo : une perspective mathématique

Ici, nous aborderons les blockchains du point de vue mathématique. Cette démonstration vaudra pour nos travaux actuels autant que pour nos projets à venir. Nous présenterons, de manière intuitive et brève, les théories mathématiques employées. Nous expliquerons également les raisons pour lesquelles nous avons développé En-Tan-Mo.

### 3.1 Problèmes de sécurité dans les systèmes décentralisés

En 2009, Satoshi Nakamoto publie Bitcoin: peer to peer electronic cash system. Dans ce texte, il POSe les fondations mathématiques du Bitcoin et démontre que la probabilité de tricherie, dans le minage de Bitcoins, est extrêmement faible si l'on se réfère à certains aspects de la Loi de Poisson. Ainsi, Nakamoto résout la question de la confiance en ce qui concerne la comptabilité. Cet aspect est explicité par le Problème des Généraux Byzantins.

Voici un résumé des idées essentielles de Nakamoto, en ce qui concerne les probabilités de triche réussie dans les blockchains :

Lorsqu'une transaction est conclue, un tricheur tente de hacher et d'uploader un block rempli d'informations fausses et d'en faire une fourchette. Dans l'hypothèse où la taille de la fourchette est fidèle à la loi de Poisson lorsque la chaîne originale se voit ajouter un bloc, Nakamoto calcule la probabilité qu'une fourchette puisse se raccrocher à la chaîne à l'aide d'une formule de probabilité pleine. Avec l'émergence des groupes de mineurs ASIC, l'hypothèse originale ne tient plus pour peu que la fourchette ne se conforme plus à la loi de Poisson. La lutte computationnelle pour le droit d'uploader de nouveaux blocs est essentiellement un problème de marche aléatoire binomial du point de vue de l'analyse stochastique.

$p$  = probabilité qu'un node honnête trouve le bloc suivant ;

$q$  = probabilité qu'un attaquant trouve le bloc suivant

Nous désignons par  $X_n$  les blocs extraits par le tricheur au moment où la chaîne originale a été étendue par des blocs  $n$ . Ce problème peut être traité comme un problème de points tel que  $q$  indique la probabilité que le tricheur mine avec succès un nouveau bloc;  $p = 1 - q$  indique qu'un mineur honnête a gagné dans le hachage et mine un nouveau bloc, ce qui équivaut apparemment à la probabilité que le tricheur échoue. Si nous regardons du point de vue du tricheur, alors peut indiquer la probabilité de l'événement  $P\{X_n = k\}$  tel que les succès de  $k$  exactement se produisent avant les échecs de  $n$  et il peut être décrit en utilisant la distribution binomiale négative:

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

Selon les hypothèses suivantes :

1. Le nombre de blocs minés par des mineurs honnêtes est suffisamment grand.

2. Il existe une constante  $\lambda$ ,  $n \frac{q}{p} \rightarrow \lambda$  dénote  $l_n = n \frac{q}{p}$  fini, par les calculs suivants

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

Il peut être conclu que la loi de distribution des variables aléatoires  $X_n$  est approximativement conforme à

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

Toutefois, avec l'émergence des groupes de minage, l'hypothèse (2) ne peut plus être considérée comme valide, donc les estimations quantitatives de Nakamoto ne tiennent plus la route en tant que modèle de gestion du risque pour la crypto-finance. De surcroît, pour peu que le tricheur obtienne des ressources computationnelles fortes et ajuste sa puissance computationnelle, sa probabilité de réussite est très largement supérieure aux estimations de Nakamoto.

Ainsi, en se servant des algorithmes et du contrôle des proof of stake tout en accélérant la vitesse de création des blocs, on peut réduire les probabilités de triche réussie et obtenir des estimations plus fiables d'une telle probabilité.

Lorsqu'une chaîne de mineurs honnêtes a été rallongée de blocs, la différence, en terme de nombre de blocs, entre cette chaîne et la chaîne minée par le tricheur peut être dénotée :  $z - X_n$ . En se servant de méthodes empruntées au problème de la "Gambler's ruin", on peut extrapoler un différence en nombre de blocs de  $z - k$ , et la probabilité que la chaîne du attaquant ratrappé un jour celle des mineurs honnêtes est :

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

Les probabilités de succès d'un tricheur peut être évaluée tel que suit en se servant d'une formule de probabilité complète

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

Ainsi qu'on peut le voir dans les travaux de C. Crunspun et R-P. Marco, cette probabilité est assez élevée même lorsque les ressources computationnelles proportionnelles du tricheur sont significativement inférieures à 51 %. Pour y remédier, En-Tan-Mo emploie un protocole de consensus de type duel, de sorte à surveiller et contenir le comportement des mineurs par le processus électoral.

### 3.2 L'équilibre de Nash et les algorithmes de consensus

Le concept de l'Equilibre de Nash est fréquemment utilisé dans le design des algorithmes de consensus En-Tan-Mo. Après l'avoir brièvement défini, nous expliquerons de quelle manière il joue un rôle central dans les protocoles de consensus d'En-Tan-Mo.

SupPOSons que  $S_1, S_2, \dots, S_N$  dénote les espaces métriques compacts et que  $J_1, \dots, J_N$  définit la continuité des espaces de produits  $\prod_{i=1}^N S_i$ . On dénote par  $P(S_i)$  l'espace métrique compact de toutes les mesures de probabilité boréales définies sur  $S_i$ .

Définition : Dans un jeu à stratégies mixtes, l'Équilibre de Nash équivaut au n-uplet  $(\pi_1, \dots, \pi_N) \in \prod_{i=1}^N P(S_i)$  de sorte à ce que, pour chaque  $i = 1, 2, \dots, n$ ,

$$J_i(\pi_1, \dots, \pi_N) \leq J_i((\pi_j)_{j \neq i}, \pi_i) \quad \forall \pi_i \in P(S_i)$$

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

Théorème (Nash, 1950) (Glicksberg, 1952) Selon l'hypothèse ci-dessus, il existe au moins un point d'équilibre dans les stratégies mixtes.

Il existe une littérature vaste et en expansion sur l'analyse de la théorie des jeux de systèmes de blockchain tels que Bitcoin. L'équilibre de Nash est un état de stratégies (pour tous les nœuds) qu'aucun participant ne peut gagner par déviation unilatérale. Ceci est essentiel pour assurer la stabilité et la sécurité d'un système décentralisé car il ne peut y avoir de contrôleur centralisé qui maintient l'ordre en «punissant» les écarts.

Le problème est que les stratégies à l'équilibre de Nash ne sont pas toujours efficaces. En Bitcoin on peut même dire que l'équilibre de Nash est très gaspilleur. Cela est dû au fait que le seul mécanisme de sécurité est une preuve de travail, les mineurs entrant et sortant librement. Ceci est un jeu purement non-coopératif et le seul facteur décisif pour gagner est le taux de hachage. Cette conception du mécanisme POW a très bien réussi à faire en sorte que les mineurs suivent le consensus dans le sens d'une exploitation minière honnête et suivent «la règle de la chaîne la plus longue». Dans le même temps, les mineurs ont toujours des incitations à améliorer leurs machines minières pour maximiser leurs profits. Finalement, la course aux armes computationnelle conduit à des gisements miniers inutiles et à des oligarques de facto de blockchain. En économie, on parle souvent de "tragédie des communs" et de théorie des jeux algorithmiques "prix de l'anarchie".

Ce problème ne peut être résolu qu'au niveau de la conception des mécanismes, «le côté ingénierie de l'économie». La conception de mécanismes est aussi appelée problème inverse dans la théorie des jeux: elle n'étudie pas les résultats basés sur des mécanismes mais cherche plutôt un mécanisme approprié qui peut mener aux résultats désirés. Les systèmes de blockchain sont le domaine parfait pour utiliser la théorie de conception de mécanisme car les concepteurs ont beaucoup de liberté pour concevoir des protocoles ou même établir des constitutions. Ici, le mécanisme peut être vu comme une procédure qui attribue des résultats aux stratégies. La

raison pour laquelle l'équilibre de Nash est si important pour la conception des mécanismes est que: si les joueurs sont rationnels et peuvent prédire bien ce qui va se passer, alors ils prédisent un équilibre de Nash. Sinon, quelqu'un sera incité à dévier et à ne pas suivre le consensus. Dans les systèmes blockchain, ce problème devient plus aigu: comme il n'y a pas de pouvoir central pour imPOSer des contraintes, les participants vont dévier dès qu'ils ressentent les incitations. Dans ETM, nous avons utilisé la conception de deux mécanismes POW et DPOS pour atteindre une haute efficacité de l'équilibre de Nash tout en maintenant une forte décentralisation. Dans notre travail futur, nous prévoyons d'étudier les applications du mécanisme de prix de type Kantorovich et la vente aux enchères de Vickery dans la conception de mécanisme ETM.

### 3.3 Modèle de redistribution des enjeux dans le système électoral

À ce jour, de nombreux systèmes de Blockchains ont adopté un système de proof of stake par consensus, ce qui a l'avantage d'économiser les frais de recours et de créer des blocs plus rapidement. La proPOSITION théorique sous-jacente est que celui qui POSSède des enjeux plus importants dans le système est davantage digne de confiance. Selon les études dans le système En-Tan-Mo, basées sur l'analyse de l'état actuel des blockchains et des crypto-monnaies, l'enjeu est habituellement concentré entre les mains du minorités disPOSant d'un type de distribution Pareto. De façon à éviter la concentration de la force de vote, il nous faut définir une dépendance du droit de vote aux enjeux qui soit POSitivement corrélée mais non-linéaire.

Dans le cadre de ce nouveau mécanisme de consensus, il se peut qu'un grand nombre de parties prenantes essaient d'obtenir des avantages en votant en contrôlant plusieurs comptes. C'est ce qu'on appelle l'attaque Sybil dans la cyber-sécurité.

Nous pensons que cela ne peut pas être une stratégie rationnelle du point de vue de la théorie des jeux pour les arguments suivants:

Nous commençons avec la proPOSITION que les participants sont motivés par la poursuite de l'utilité supérieure, dans le système ETM cela signifie plus de récompenses symboliques. Voter est un moyen pour une fin, pas une fin en soi.

Dans le mécanisme de transaction ETM, chaque vote intervient après une transaction. Cela entraînera un certain montant de frais de transaction. Ainsi, pour les attaquants (d'attaque Sybil) cela signifie un coût supplémentaire. Comme les attaquants doivent initier une quantité énorme de transactions sans signification pour gagner plus de voix, cela entraînera des frais de transaction.

En-Tan-Mo est basé sur la théorie des jeux et la théorie économique de l'attente rationnelle de Thomas

Sargent. Notre étude mathématique montre que l'attente rationnelle de l'utilité acquise par l'attaque Sybil ne sera pas en mesure de couvrir le coût des frais de transaction supplémentaires. Par conséquent, l'attaque Sybil ne sera pas le choix rationnel.

De plus, le mécanisme de consensus de l'ETM fournit plus de mesures de sécurité telles que le brassage chaotique des mineurs, qui sera le sujet de la section suivante.

Pour les détails techniques, veuillez vous référer à la version anglaise de notre document.

### 3.4 Mélange chaotique

La conception consensuelle du projet En-Tan-Mo a fait de la sécurité l'un des objectifs les plus essentiels et a établi un très haut niveau. En réponse au problème des attaques coordonnées de plusieurs mineurs SCV dans le système DPOS, la couche de consensus utilisera des algorithmes de réarrangement chaotique.

**Chaos:** L'extrême sensibilité du comportement dynamique du système dynamique à la valeur initiale.

Pour le dire simplement, le chaos fait référence au fait qu'une perturbation minimale de la valeur initiale peut entraîner un très grand changement dans le résultat de la cartographie, ce qui peut conduire à une incertitude dans le processus de prédiction. Cette incertitude est exactement ce dont nous avons besoin. Dans le processus de téléchargement de blocs, si plusieurs mineurs veulent s'unir pour tricher, ils doivent continuellement identifier un bloc contenant de fausses informations. À cette fin, ils doivent connaître l'ordre des blocs de chargement des différents mineurs dès que POSSible et avoir suffisamment de temps pour coordonner. Le remaniement chaotique fait référence au fait que l'ordre des téléchargements des mineurs n'est pas déterminé au départ, mais que la conception de couche consensus spécifie un algorithme qui extrait certaines informations de chaque bloc de téléchargement réussi pour le mappage et effectue plusieurs itérations pour calculer le mineur suivant. Le nombre, par conséquent, n'est pas connu jusqu'à la dernière minute.

Les mappages chaotiques sont déterministes, donc à chaque étape tous les mineurs obtiennent exactement le même résultat en calculant indépendamment. Le système peut atteindre la stabilité et la sécurité tout en maintenant une forte décentralisation.

Pour les détails techniques, veuillez vous référer à la version anglaise de notre document.

### 3.5 Dualisme de Kantorovich, transport optimal et décentralisation

Le protocole de consensus d'En-Tan-Mo a reçu le nom de Kantorovich en hommage au mathématicien soviétique Leonid Kantorovich, en raison de son travail dans le champ de l'optimisation des transports, tout particulièrement le théorème de la Formation duale qu'il énonça en 1937. Il s'agit d'une découverte révolutionnaire

en programmation linéaire et en optimisation des transports. Ici, nous évoquerons brièvement la théorie et la manière dont elle peut être utile dans la construction de systèmes de blockchains décentralisés.

$X$  et  $Y$  correspondent à deux emplacements donné dans le monde physique, et une certaine quantité de matériel doit être transportée de  $X$  à  $Y$ .  $c(x,y)$  dénote le coût de transport d'un point  $y$  à  $y$ .  $y$  dénote distribution de probabilité conjointe sur le domaine  $X \times Y$  tandis que  $\mu$  et  $\nu$  dénote la loi de probabilité marginale, respectivement.

Alors,  $\int_{X \times Y} c(x,y) d\gamma(x,y)$  peut être employé pour désigner le coût de transport global. Le théorème de la Formation duale de Kantorovich proPOSE que :

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

Ici,  $\psi$  et  $\varphi$  désignent respectivement la Borne supérieure et la Borne inférieure. Sans se préoccuper de faire des mathématiques dans le détail, nous donnerons une explication intuitive de la manière comment cela peut être mis à profit dans un système décentralisé du type d'En-Tan-Mo, si  $\psi(y)$  désigne le prix de vente au point  $y$  tandis que  $\varphi(x)$  désigne le prix d'achat à  $x$ , alors

$\int_Y \psi(y) d\nu(y) - \int_X \varphi(x) d\mu(x)$  peut être employé pour désigner le coût final de la transaction. La Formation duale démontre que sous certaines conditions  $\psi(y) - \varphi(x) \leq c(x,y)$ , la stratégie nécessaire à la réduction des frais de transport est en relation dueille avec la stratégie de maximisation des profits.

Ce théorème a mis en évidence l'importance d'un système de tarification rationnel dans l'optimisation des transports et allocations de ressources. Du fait de ses implications économiques, cette théorie mathématique fut longtemps critiquée et rejetée en URSS.

Du point de vue de la technologie blockchain, le transport optimal correspond à la meilleure stratégie de transmission de valeurs. En-Tan-Mo considère qu'il est raisonnable de bâtir un mécanisme de confiance basé sur les systèmes décentralisés, de sorte à permettre à chaque participant de faire de ses décisions autonomes une information transactionnelle disponible, de sorte à permettre l'émergence d'un marché transparent. Un système de tarification juste émergera via le procédé d'Équilibre dynamique, lui-même basé sur le mécanisme auto-adaptatif du marché. C'est de cette manière, précisément, que la transmission de valeurs s'effectue sur En-Tan-Mo.

### 3.6 Formation dynamique du prix dans un système décentralisé

Avec En-Tan-Mo, chaque participant est en même temps fournisseur (vendeur) et acheteur de services. Le cœur du système décentralisé est le mécanisme du prix et la génération du prix peut être accomplie par le biais d'une organisation autonome, via différents procédés d'équilibre dynamique. En-Tan-Mo utilise une théorie du jeu de terrain pour étudier les mécanismes de formation du prix dans les systèmes d'échange décentralisés. Ce

modèle est également appelé Modèle de formation du prix Lasry-Lions. Imaginons que la préférence du prix comporte des éléments aléatoires. Les densités de probabilité  $f_B$ ,  $f_V$  désignent respectivement le nombre d'acheteurs et de vendeurs.  $t$  désigne l'heure de certaine transaction et  $x$  leur montant. Par exemple,  $f_B(x,t)$  exprime le nombre d'acheteurs à un moment  $t$ , de sorte que le prix est  $x$ .  $\lambda$  désigne le coût de transaction. Ce qui suit fait usage d'un Jeu à champ moyen :

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

Compte-tenu des conditions initiales :

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

Ici, le multiplicateur  $\lambda$  est employé pour décrire le nombre de transactions au moment  $t$ .  $\lambda$  décrit l'aspect aléatoire et  $\lambda$  est une simple fonction de Dirac.

Les équations, dans ce système, sont d'une certaine façon similaire à l'Équation de la chaleur à une dimension. Toutefois, la difficulté réside dans les conditions de bords libres. Le problème de la valeur des bords libres est un des problèmes essentiels de la théorie moderne des Équations aux dérivées partielles, qui se pose naturellement dans bien des cas de problèmes physiques concrets, par exemple la transition de phase, et qui a de nombreuses applications dans de nombreux domaines.

Dans un système de blockchain décentralisé, du fait de la comptabilité distribuée, chaque node peut ajuster sa propre stratégie de façon dynamique, en réponse aux informations disponibles quant aux transactions. Ainsi, il existe surtout des problèmes de contrôle adaptatif de type Bayes, de sorte que chaque participant se sert d'une probabilité de distribution a posteriori pour adapter sa stratégie et maximiser ses profits personnels. À l'avenir, En-Tan-mo prévoit d'adopter un modèle de formation dynamique du prix pourvu de contrôles Bayasiens et de connecter la technologie blockchain avec l'intelligence artificielle et le deep learning.

## References:

- [12] W. Feller. An introduction of probability theory and its applications. Vol.1, 3rd ed. John Wiley& Sons, 1957.
- [13] Л.В. Канторович, Математические методы организации планирования производства. Издание Ленинградского государственного университета, 1939.
- [14] С. М. Меньшиков. Актуальность экономической модели Л. В. Канторовича в наше время. Зап. научн. сем. ПОМИ, 2004, том 312, 30–46.
- [15] M. Doob, Kantorovich. On Optimal Planning and Prices. Science & Society, Vol. 31, No. 2 (Spring, 1967), pp. 186-202.
- [16] C. Grunspan, R. Pérez-Marco. Double spend races. arXiv:1702.02867v2 [cs.CR].
- [17] R. Perez-Marco. A simple dynamical model leading to Pareto wealth distribution and stability. arXiv:1409.4857, 2014.
- [18] J. P. Aubin, I. Ekeland. Applied Nonlinear Analysis. Wiley-Interscience, 1984.
- [19] J. P. Aubin. Optima and Equilibria. Springer-Verlag, 1998.
- [20] Notes on Mean Field Games, from Pierre-Louis Lions' lectures at Collège de France.
- [21] J.-M. Lasry, P.-L. Lions. Mean field games. 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.

## 4. Règles économiques des blockchains

Les blockchains et les technologies associées sont sur le point de révolutionner l'économie. La Révolution Industrielle s'est mise en place dans un contexte dominé par la hiérarchie et l'accumulation du capital. De la « Révolution blockchain » découle un capitalisme à dimension humaine, fondé sur l'autonomie individuelle.

Le déroulement de cette révolution demeure incertain. Les entrepreneurs et les investisseurs devront, comme toujours, mettre ces incertitudes à l'épreuve des faits, à travers des tentatives plus ou moins fructueuses. Il est toutefois certain qu'une quantité extravagante de richesses sera produite et détruite en chemin, jusqu'à ce qu'émerge une vision claire de cette nouvelle économie.

Ce qu'offre En-Tan-Mo, en ce début de révolution, est un modèle équilibré de transfert de valeurs, qui met en lumière le sens et l'importance des bouleversements en cours.

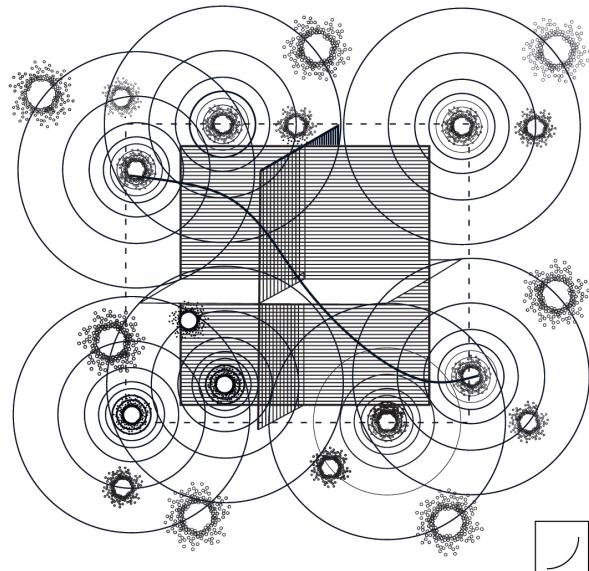
### 4.1 Crypto-économie d'En-Tan-Mo

Il est courant, dans le monde des affaires, d'établir des relations de confiance afin d'éliminer les incertitudes et de limiter les frais de transactions. En-Tan-Mo garantit la sûreté des flux d'informations relatifs aux transactions. De telles garanties technologiques éliminent les incertitudes et consolident la confiance entre acteurs. Ce renforcement de confiance conduit, par essence, à une réduction générale des frais de transaction.

En sus d'une efficacité discutable, les technologies de blockchain actuelles comportent d'autres aspects négatifs. Les blockchains sont limitées par la vitesse de transaction (sept transactions par seconde pour le Bitcoin), ainsi que par un manque de confidentialité et de sécurité (cf., par exemple, le hacking de Mt. Gox), etc. En-Tan-Mo ne se contente pas d'améliorer l'efficacité du processus : En-Tan-Mo procure un système stable, pourvu d'un mécanisme de distribution de valeurs clairement défini. En-Tan-Mo ne peut que servir les intérêts des décideurs qui en adopteront l'usage.

La crypto-économie d'En-Tan-Mo se substitue aux institutions pour ce qui est d'établir un système de comptabilité fiable, au chiffrement sécurisé et automatisé. L'économie classique et néo-classique étudie la production et la distribution de ressources rares, ainsi que les éléments qui sous-tendent ces processus. La crypto-économie En-Tan-Mo est une économie dont le protocole constitue l'objet. Les protocoles (tels que les lois, langues, droits de propriété, codes sociaux et idéologies) permettent à différents groupes d'individus, dispersés et engagés dans un processus spéculatif, de s'entendre. Les protocoles s'avèrent utiles non seulement dans le cadre de transactions économiques, mais également de transactions sociales et politiques.

La crypto-économie d'En-Tan-Mo étudie les principes et théories économiques des blockchains. Leurs applications dérivées sont pleinement intégrées. L'économie et ses émanations institutionnelles fonctionnent grâce à des systèmes de communication et d'échange. Toutefois, l'économie institutionnelle ne se concentre pas uniquement sur les protocoles mais



également sur la comptabilité, c'est-à-dire de la donnée fondée sur des protocoles.

L'économie d'En-Tan-Mo recoupe les sujets suivants : les protocoles de régulation des transferts de valeurs, le développement social, politique et institutionnel au regard de ces protocoles ; et la manière dont En-Tan-Mo peut modifier les mécanismes de transaction de valeurs sur le plan social.

### 4.2 L'équilibre de Nash

Pour En-Tan-Mo, l'Équilibre de Nash est un concept issu tout à la fois de l'économie et des mathématiques. Du fait du mécanisme de consensus duel d'En-Tan-Mo, chaque utilisateur peut assumer le rôle de mineur ou d'électeur lors de sa contribution à l'élaboration de

la blockchain, et obtenir une récompense adéquate en fonction de principes équilibrés. Les interactions entre utilisateurs sont régulées par des protocoles de consensus simples et efficaces, grâce auxquels l'ensemble du système est certain d'atteindre l'Équilibre de Nash.

Les mécanismes et algorithmes de consensus sont à la base de la décentralisation d'En-Tan-Mo. Leur objectif premier est d'obtenir des « règles sans régulateurs » et un « contrôle décentralisé auto-adaptatif ». L'Équilibre de Nash, tel que défini par le mathématicien et prix Nobel américain John Nash, est au cœur d'En-Tan-Mo. Il s'agit d'un système simple, impliquant des interactions entre différents participants, au sein duquel il est impossible pour un seul individu de profiter d'un changement de stratégie unilatéral si les stratégies des autres participant demeurent inchangées.

Du point de vue d'En-Tan-Mo, le seul usage des POW et des DPOS est insuffisant à garantir que la stratégie du blockchain aboutisse à l'Équilibre de Nash. Par exemple, avec le Bitcoin, lorsqu'un mineur gagne la course de hachage, s'il uploadé un bloc contenant des informations fausses, le bloc ne sera pas intégré à la chaîne et, par conséquent, le mineur perdra ce qui a été investi lors du minage. Plus concrètement :

1. Si tous les utilisateurs de la blockchain contribuent au minage, le hachage doit être suffisamment difficile pour contenir efficacement la probabilité d'une escroquerie. Une escroquerie efficace ne peut se produire que lorsqu'un pool de mineurs malhonnête est capable de construire une chaîne de faux blocs susceptible de rivaliser avec une chaîne de mineurs honnêtes.

2. Le coût du minage doit demeurer suffisamment élevé pour prévenir la rentabilité d'un acte malhonnête.

Avec l'apparition des mineurs ASIC, il est devenu presque impossible pour un mineur ordinaire de gagner une course de hachage. L'émergence de ressources computationnelles dans les systèmes rend le hachage de plus en plus difficile, ce qui va à l'encontre de l'Équilibre de Nash. Avec Ethereum, l'ensemble des nodes est composé de mineurs GPU, que les utilisateurs ordinaires ne peuvent s'offrir. Les utilisateurs de Light ont totalement renoncé au minage. De même, dans les systèmes de consensus DPOS représentés par Steemit, l'enjeu est devenu la norme, de sorte que les grands actionnaires dominent les votes. Il est raisonnable de conclure que dans de tels cas, une minorité de puissants décide pour l'ensemble du pool, sans véritable processus démocratique. Les richesses se trouvent concentrées entre quelques mains et l'Équilibre de Nash est rompu.

De par ses mécanismes de consensus, En-Tan-Mo propose un système qui profite à tous les participants. Les bénéfices ne peuvent être monopolisés par de grands pools de mineurs ou de gros actionnaires. Les réformes fondamentales ne peuvent se produire que sur la base d'un consensus. Chaque joueur du jeu En-Tan-Mo est un utilisateur susceptible d'être catalogué selon son identité : mineur Stakhanov, superviseur ou mineur Pareto (membre d'un pool de minage Pareto). Ils obtiennent leurs tokens ETM et autres récompenses en votant ou en

allongeant la blockchain. Les mineurs Stakanov sont élus et contribuent à rallonger la chaîne de façon ordonnée et sur une période déterminée. Bien qu'un mineur malhonnête ait moins à perdre du fait du coût réduit du minage, il a davantage à perdre s'il est exclu du pool Stakhanov pour fraude. Afin d'améliorer l'efficacité du processus de construction de blocs En-Tan-Mo, les superviseurs ont le devoir de sélectionner les meilleurs mineurs Stakhanov et sont, pour cela, récompensés en tokens ETM. Le nombre d'enjeux de votes alloué à chaque électeur est proportionnel à ses enjeux de tokens, de sorte à garantir l'équité entre actionnaires. Les mineurs Stakhanov et les superviseurs sont, à la fois et à bien des égards, connectés et indépendants, de sorte à garantir l'équilibre et la transparence de la répartition des pouvoirs et des enjeux. Dans l'état actuel des choses, les mineurs Pareto ne peuvent pas obtenir de tokens ETM mais peuvent collaborer au minage d'autres systèmes de blockchains dans le cadre d'un effort collectif. Cet arrangement garantit que les intérêts de chaque mineur sont préservés à tout moment. Ainsi, le couplage des DPOS et des POW en protocoles de consensus duels permet à chaque joueur En-Tan-Mo de faire évoluer sa stratégie en fonction de son identité. Cela conduit à l'Équilibre de Nash.

Afin d'expliquer la manière dont le consensus affecte les décisions des joueurs (en tenant compte de différentes stratégies, ainsi que des mineurs honnête et malhonnêtes), nous insisterons sur les règles et hypothèses suivantes :

Hypothèse :

Au moins la moitié des mineurs sont honnêtes.

Règles :

1. Seule la chaîne la plus longue sera, in fine, acceptée.
2. Les mineurs malhonnêtes ou inefficaces seront exclus au fil des élections.

### 4.3 Consensus de Kantorovich

Parmi les failles reconnues des systèmes de blockchain de première et seconde génération, on compte :

1. Un taux de traitement des transactions assez bas. Par exemple, le taux de traitement actuel du Bitcoin ne peut être comparé à celui des institutions traditionnelles, tels que les cartes bancaires.
2. La lenteur de construction des blocs, qui retarde considérablement la confirmation des transactions.
3. L'évolutivité : le niveau actuel d'efficacité limite l'évolutivité des blockchains.
4. Le gaspillage de ressources et la pollution environnementale qui découlent du minage POW.

Pour toutes ces raisons, En-Tan-Mo offre un mécanisme de consensus Kantorovich fondé sur les concepts de l'Équilibre de Nash. Les superviseurs sont actionnaires d'En-Tan-Mo. Ils ne contribuent pas à la construction de blocs mais, en lieu et place, sont éligibles à l'obtention de tokens ETM en fonction de leurs enjeux proportionnels, passés ou présents, dans le système. Les superviseurs choisissent les mineurs Stakanov selon leurs performances en termes de hachage et de minage. Ce système garantit, pour En-Tan-Mo, un niveau de performance et de sécurité élevé. Les mineurs Stakanov obtiennent leurs tokens ETM en se livrant à un minage ordonné et non-compétitif. Le taux de hachage peut être réduit sans que la sécurité ne soit affectée, de sorte que les blocs peuvent être bâties et uploadés très rapidement. Les mineurs non-élus intègrent des pools de minage Pareto, afin de miner des blocs sur d'autres chaînes, à l'aide de technologies de blockchain dérivées spécialement conçues à cet effet. Ils recevront d'autre tokens en fonction de leurs ressources computationnelles. Ainsi, tous les mineurs sont récompensés d'une manière ou d'une autre. Le consensus de Kantorovich améliore l'efficacité et l'évolutivité de l'ensemble, sans jamais compromettre la sécurité.

Les systèmes centralisés continuent de présenter certains avantages en termes d'efficacité. Mais grâce à de meilleurs designs mathématiques en termes de structures mécaniques, il est possible d'équilibrer la décentralisation avec un peu de coopération coordonnée centralisée, de sorte à garantir la compatibilité de la sécurité, de la stabilité et de l'efficacité dans un système de blockchain. C'est là notre objectif principal.

Le protocole du consensus de Kantorovich est un protocole de proof of stake révolutionnaire. Il fournit un ensemble de règles auquel l'ensemble des nodes de minages peut se référer afin de s'accorder dans les réseaux. L'algorithme est un aspect fondamental de l'infrastructure En-Tan-Mo, et représente un grand pas en avant pour les technologies de blockchain. Le consensus de Kantorovich améliore la capacité des protocoles POW, consommateurs d'énergie, à surmonter les obstacles à l'allongement des applications de blockchains. L'algorithme a été conçu par notre équipe, constituée de scientifiques et de théoriciens du jeu de haut niveau. Il s'agit du premier couplage de POW et DPOS.

Les mineurs élus et en capacité de passer le test de hachage sont dénommés mineurs Sakhanov, ou SCV. Les actionnaires qui élisent les mineurs Stakanov sont appelés les superviseurs. L'enjeu-token proportionnel de chaque superviseur est divisé en bulletins de vote par une fonction concave. Au cours de chaque période, le vote est récompensé. Les mineurs éligibles peuvent devenir SCV en suscitant un nombre suffisant de voix. Le cas échéant, ils sont autorisés à uploader des blocs vérifiés de sorte à obtenir des tokens.

Imaginons qu'un mineur tente une action malhonnête, par exemple une double-dépense ou l'upload d'un bloc fallacieux. Les conséquences seront

les suivantes :

1. La majorité des SCV minant honnêtement, on peut partir du principe que le bloc fallacieux sera une fourchette vouée à disparaître, entraînant une perte du coût de minage.

2. Du fait des élections périodiques dans le mécanisme de consensus Kantorovich, le mineur malhonnête sera exclu du pool de minage au cours de l'élection suivante. Ainsi, il perdra l'opportunité d'obtenir de nouveaux tokens, ainsi que son dépôt de garantie. On peut en conclure que, pour un mineur SCV, la seule approche rationnelle possible est de miner honnêtement et efficacement.

Malgré l'absence d'un moniteur centralisé susceptible de sanctionner le comportement des SCV et des superviseurs, le design du mécanisme est, par essence, la « main invisible » qui dicte les règles économiques auxquelles chacun se conformera dans son propre intérêt. Cette dynamique résout les problèmes d'efficacité et de confiance tout à la fois.

## 4.5 Les pools de minage Pareto

Le mécanisme incitatif d'En-Tan-Mo est fondé sur la théorie économique et comporte trois avantages :

1. Un système juste. Dans la plupart des systèmes de blockchains tels que Bitcoin ou Ethereum, les enjeux sont distribués de manière inéquitable, avec un biais en faveur des pools de minages centraux. Avec En-Tan-Mo, chaque individu a toutes ses chances, du fait du mécanisme de consensus.

2. Un système décentralisé. Dans les autres systèmes de blockchains DPOS, les gros actionnaires contrôlent les processus décisionnels. Il en résulte un contrôle centralisé, voire le monopole d'une oligarchie. Dans le système En-Tan-Mo, les actionnaires et les mineurs ont des droits, responsabilités et intérêts distincts. Chacun peut bénéficier des ressources et des avantages d'un système décentralisé.

3. Un système optimal. Dans les autres systèmes de blockchains, les utilisateurs ont des valeurs non-diversifiées, les différentes chaînes sont des îlots isolés, déconnectés les uns des autres. Avec En-Tan-Mo, les actionnaires reçoivent leurs tokens via un système de vote et les mineurs optimisent leurs bénéfices en changeant d'identité, selon qu'ils sont SCV ou Pareto.

Grâce au mécanisme de consensus Kantorovich, les mineurs se réunissent au sein d'un pool de minage coopératif. Au cours de chaque période, les SCV sélectionnés rallongent la chaîne de façon ordonnée. En-Tan-Mo permet aux autres mineurs de s'organiser en pools de minage Pareto. De par l'usage de technologies de side-chain spécialement conçues à cet effet, de stratégies de coalition et d'algorithmes analytiques de revenu potentiel en temps réel, ces mineurs participent au minage d'autres systèmes de blockchains. Les récompenses sont distribuées en fonction de leurs

ressources computationnelles et garantissent une issue favorable à chaque mineur.

Les principes économiques de base des pools de minage Pareto sont : définir des stratégies de coalition ; choisir les blockchains appropriées ; bâtir des structures collaboratives et des systèmes de management ; intervertir des mécanismes de minage entre statuts SCV et Pareto. Un pool de minage Pareto a les caractéristiques suivantes :

1. **Organisation décentralisée.** Les principaux objectifs du minage Pareto sont de se partager le marché du minage coopératif. Les relations entre membres sont fluctuantes, selon les stratégies utilitaires de la blockchain. Le pool Pareto est, en soi, un système dynamique et ouvert.

2. **Actions stratégiques.** La conception des pools Pareto a été mûrement planifiée. La coalition met l'accent sur une amélioration stratégique de l'environnement du business. Il s'agit avant tout d'acquérir des ressources économiques.

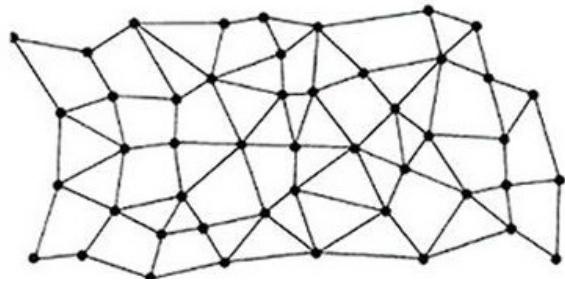
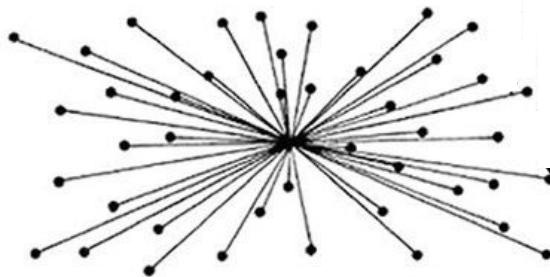
3. **L'égalité des chances à travers la coopération.** La collaboration Pareto est plus stratégique que tactique. Il s'agit d'abord de mutualiser les ressources et les atouts, à travers une confiance mutuelle et une garantie partagée d'indépendance. En s'accordant à l'avance sur

une répartition juste des récompenses en fonction des ressources computationnelles, ce mécanisme réduit intrinsèquement les écarts entre mineurs.

4. **Complexité managériale.** Le mécanisme de consensus Kantorovich a, pour la première fois, défini un « minage multiple » authentique. Les mineurs doivent alterner entre des stratégies de pool SCV et Pareto afin de maximiser leurs profits.

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

L'efficacité Pareto, ou optimisation Pareto, est un « état » d'allocation des ressources qui décourage l'accaparation d'une ressource à des fins égoïstes. Un tel acte nuirait automatiquement à au moins un autre membre du pool, et ce de manière visible. Une allocation de ressources est optimale, du point de vue de Pareto, lorsqu'elle ne peut être améliorée dans le cadre du pool. En d'autres termes, l'amélioration Pareto conduit à la perfection Pareto. Le pool Pareto incarne cet



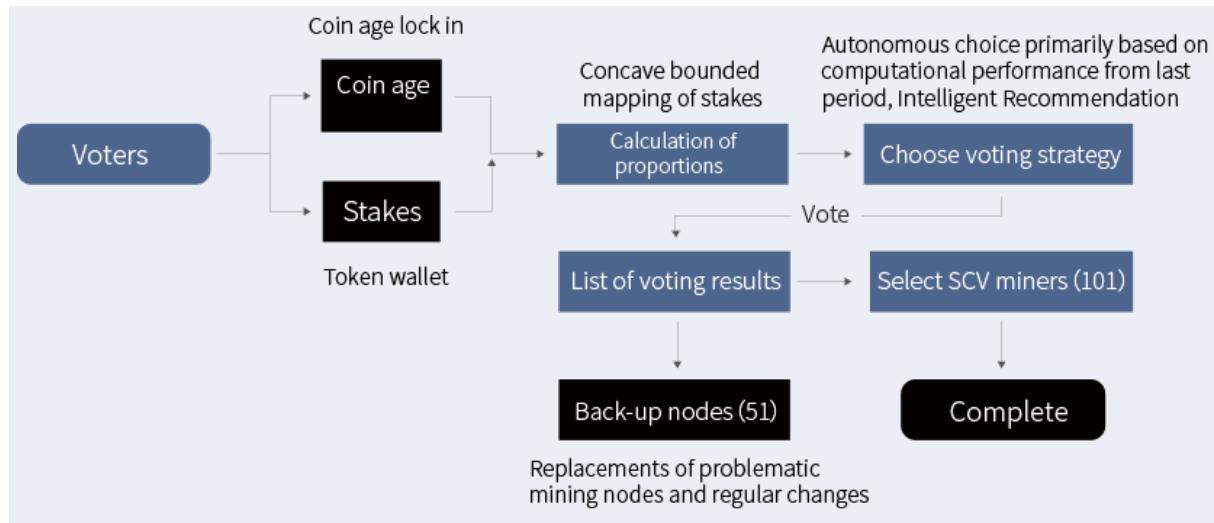
## References:

- [23] T. J. Sargent, Lars Ljungqvist. Recursive Macroeconomic Theory. MIT Press, 2000.
- [24] T. J. Sargent. Dynamic Macroeconomic Theory. Harvard University Press, 1987.
- [25] J. V. Neumann, O. Morgenstern. (1944) Theory of Games and Economic Behavior. Princeton University Press. 2nd edition, 1947, 3rd edition, 1953.
- [26] J. Harsanyi. Games with incomplete information played by 'Bayesian' players. Management Science 14:159-182, 320-334, 486-502, 1967.
- [27] D. Fudenberg, J. Tirole. Game Theory. Boston: MIT Press, 1991.
- [28] N. Nisan, A. Ronen. Algorithmic mechanism design. Proceedings of the 31st ACM Symposium on Theory of Computing (STOC '99), pp. 129–140, 1999.
- [29] C. Papadimitriou. Algorithms, games, and the Internet. Proceedings of the 33rd ACM Symposium on Theory of Computing (STOC '01), 749-753, 2001.
- [30] N. Houy. The Bitcoin mining games. Ledger, vol, 2016.
- [31] A. Kiayias, E. Koutsoupias, M. Kyropoulou, Y. Tselekounis. Blockchain Mining Games. arXiv:1607.02420v1 [cs.GT] 8 Jul 2016.
- [32] A. Sapirshtein, Y. Sompolinsky, A. Zohar. Optimal selfish mining strategies in bitcoin. CoRR, abs/1507.06183, 2015.
- [33] J. P. Aubin, A. Desilles. Traffic Networks as Information Systems: A Viability Approach. Mathematical Engineering 8445, Springer, 2017.
- [34] J. F. Nash. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, 36(1):48-49, 1950.

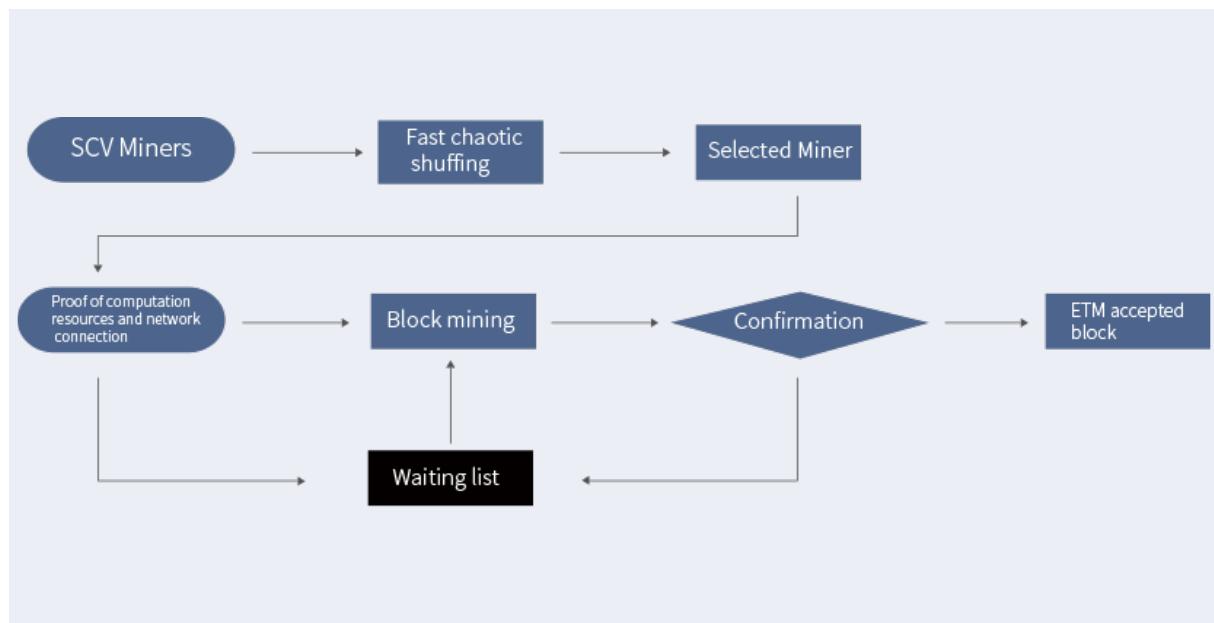
## 5. La science informatique d'En-Tan-Mo

### 5.1 Diagramme de flux En-Tan-Mo

Le protocole de diagramme de flux selon le consensus de Kantovich : Basé sur l'Équilibre de Nash, le consensus de Kantorovich utilisait le processus électoral de sorte à ce que les mineurs SCV minent les blocs dans un ordre donné. Sans perte de sécurité, la difficulté de hachage peut être réduite de sorte à ce que le minage soit plus rapide et plus efficace.

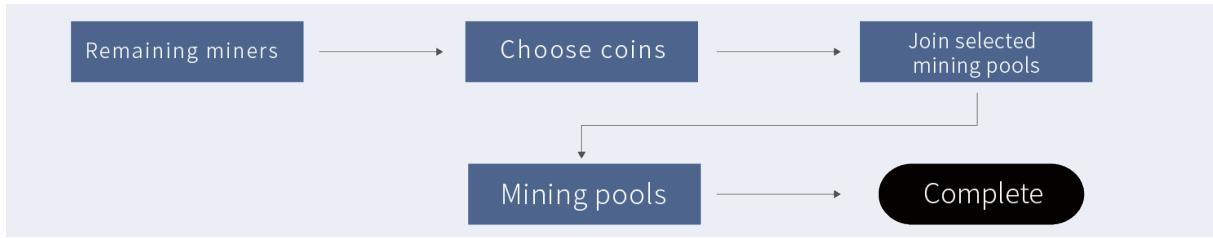


Procédure de vote du Tribunal : les voix de chaque tribunal peuvent être calculées en fonction d'une fonction concave d'enjeux-tokens proportionnels. Les récompenses seront distribuées pour chaque période.



Procédure des mineurs SCV ; les mineurs éligibles qui ont obtenu le plus de voix deviennent des mineurs SCV. Ils sont responsables du minage et de la vérification des blocs et récompensés en conséquence.

Procédure des pools de mineurs Pareto : le résidu de mineurs non-élus, grâce à une technologie de side-chain définie, une stratégie de coalition et une analyse algorithmique en temps réel, participent au minage des blocs dans d'autres systèmes de blockchains.



## Codes de base En-Tan-Mo

### 1. Algorithme d'équilibre de pieu de Tribunal

Les mineurs de SCV sont élus par le vote des tribunaux et ils ont le droit d'exploiter des blocs. La fonction qui cartographie le pion jeton en nombre de voix est croissante et concave pour assurer l'équilibre de l'écosystème En-Tan-Mo. Tous les blocs exploités par les mineurs SCV sont légitimes. "Concavité" signifie que la mise au taux de traduction des votes est en relation inverse par rapport aux enjeux symboliques.

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

//threshold mapping stake to votes translation rate is in inverse relation with regard to the token stakes to ensure equilibrium

```

thresholdMap = Map(range,rate)
rate obtained from the token value interval
rate = thresholdMap.get(range)
Token weights obtained from translation rate
weights = balance * rate
  
```

### 2. Mécanismes incitatifs des votes de tribunaux

En-Tan-Mo est différent du système POW, car il récompense les tribunaux et encourage la participation à la plate-forme. Les mineurs SCV peuvent être sélectionnés et les systèmes fonctionneront de façon efficace et sûre. Le mécanisme d'incitation au vote d'En-Tan-Mo comporte deux types de récompenses : les récompenses pour le vote et les récompenses hors-bloc. Les tribunaux sont libres de déterminer le pourcentage nécessaire à l'obtention de ces deux types de récompenses. Les récompenses de vote sont obtenues sur la base du nombre de votes détenus par les tribunaux. Cette récompense est constante lorsque la participation aux élections est effective. Le bonus de minage peut seulement être obtenu lorsque les tribunaux choisissent les bons mineurs SCV. La récompense est une couverture de risques flottante.

$F1(\text{tickets}) = \text{token}$

```

//Delivery ratio
tickets1 = fixed assignment //deliver to fixed
tickets
  
```

```

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

$\text{token} = \text{fixed}(\text{tickets1}) + \text{dynamic}(\text{tickets2})$

### 3. Séquence de l'algorithme de minage des mineurs

La séquence du minage SCV doit être déterministe et pseudo-aléatoire afin d'assurer la sécurité d'En-Tan-Mo. Cette sécurité absolue est obtenue grâce à la théorie du chaos et aux dynamiques non-linéaires.

```

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

### 4. Algorithme de hachage des mineurs SCV

En sus de la sécurité et de la décentralisation, En-Tan-Mo doit atteindre de hautes performances. Les mineurs SCV ne sont pas en compétition mais en coopération dans le cadre du minage séquentiel. Chaque bloc est attribué à un mineur SCV par un processus de fast chaotic shuffling. Ce mineur doit terminer SHA256 aussi vite que possible et propager le bloc.

Multiple hashing

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

```

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

```

## 5.2 Les données En-Tan-Mo

### Structure de données Blockheader

Le Blockheader contient toutes les informations du bloc, il est composé des champs suivants :

- Un entier 32-bit pour identifier la version du bloc
- Un entier 32-bit (timestamp) pour la date de création du bloc
- Un entier 64-bit ID du bloc précédent
- Un entier 32-bit correspondant au nombre de transactions contenu dans le bloc
- Un entier 64-bit correspondant au nombre total de transfers
- Un entier 64-bit correspondant au coût total associé au bloc
- Un entier 64-bit correspondant aux récompenses représentées
- Un entier 32-bit correspondant à la quantité de charge utile
- un hachage 256-bit de la charge utile
- Génération de la clé publique de 256-bit de l'agent du bloc

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

---

### References:

- 【35】 I. Bentov, A. Gabizon, A. Mizrahi. Cryptocurrencies without proof of work. In 3rd Workshop on Bitcoin and Blockchain Research - Financial Cryptography, 2016.
- 【36】 S. Micali. Computationally sound proofs. SIAM J. Comput., 30(4):1253–1298, 2000.
- 【37】 I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld. Proof of activity: Extending bitcoin’s proof of work via proof of stake. SIGMETRICS Performance Evaluation Review, 42(3):34–37, 2014.
- 【38】 C. Dwork, N. A. Lynch, L. J. Stockmeyer. Consensus in the presence of partial synchrony. J. ACM, 35(2):288–323, 1988.
- 【39】 S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak. Proofs of space. In CRYPTO 2015,
- 【40】 Slasher: A punitive proof-of-stake algorithm. <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stakealgorithm>.
- 【41】 S. Park, K. Pietrzak, A. Kwon, J. Alwen, G. Fuchsbauer, P. Gazi. Spacemint: A cryptocurrency based on proofs of space. IACR Cryptology ePrint Archive, 2015: 528, 2015.
- 【42】 M. Rosenfeld. Analysis of hashrate-based double spending. arXiv:1402.2009v1, 2014.

## Procédure de génération de la blockID

Génération hachage SHA-256 du blockheader et utilisation de la clé sécurisée pour signature (algorithme ed25519).

Une fois que le blockheader a été signé, le système utilise SHA-256 pour hacher le blockheader terminé afin de générer la BlockID

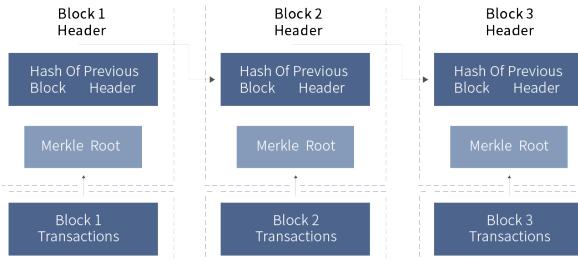
A signed block generates its block using the following flow:



## Blockchain structure

On observe que le bloc est essentiellement constitué du blockheader et du corps de bloc. Le blockheader contient le numéro de version, l'adresse du bloc précédent, le timestamp, et la racine du numéro merkle. Le corps du bloc est surtout constitué d'un décompte des transactions et du détails des factures.

La blockchain consiste en une série de blocs de données générés par méthodes cryptographiques. Chaque bloc contient le hachage du bloc précédent, et ce depuis le bloc de genèse. Les blocs forment des blockchains.

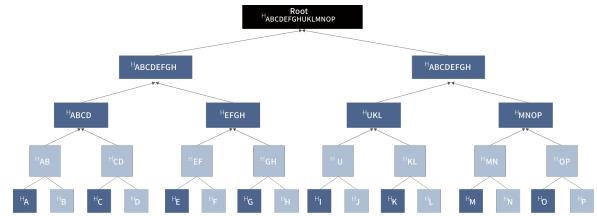


## Structure de stockage des données de l'arbre de Merkle

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

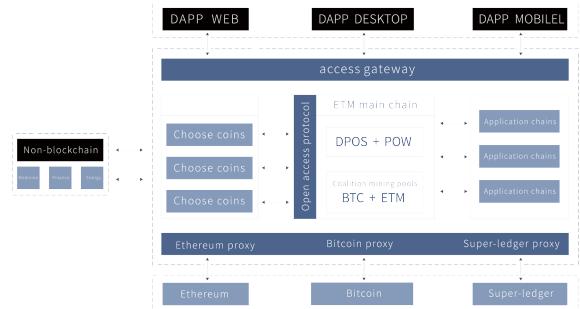
The leaves of a Merkle tree are hash values of data blocks (eg, files or data).

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



## 5.3 En-Tan-Mo interface

En-Tan-Mo est basé sur l'idée du BaaS (Blockchain as Service) et le standard du micro-service. Prenant la bibliothèque de composants auto-évolutive pour noyau la communauté de développeurs comme moteur. En-Tan-Mo offre aux autres blockchains une plate-forme pour compléter le transfert libre d'actifs et d'applications. En-Tan-mo offre une two-way invocation de soft channels pour les applications et données n'appartenant pas aux blockchains, et offre aux développeurs la capacité de compléter les uploads d'éléments, des critiques et des récompenses dans le shared lobby. Pour les usagers ordinaires, En-Tan6mo procure des portes d'entrée vers la mise en place d'appels de service d'accès. Ainsi, chaque chaîne est connectée à d'autres chaînes et à des systèmes extérieurs aux chaînes, ce qui aide les développeurs et les usagers ordinaires à passer d'internet aux blockchains.



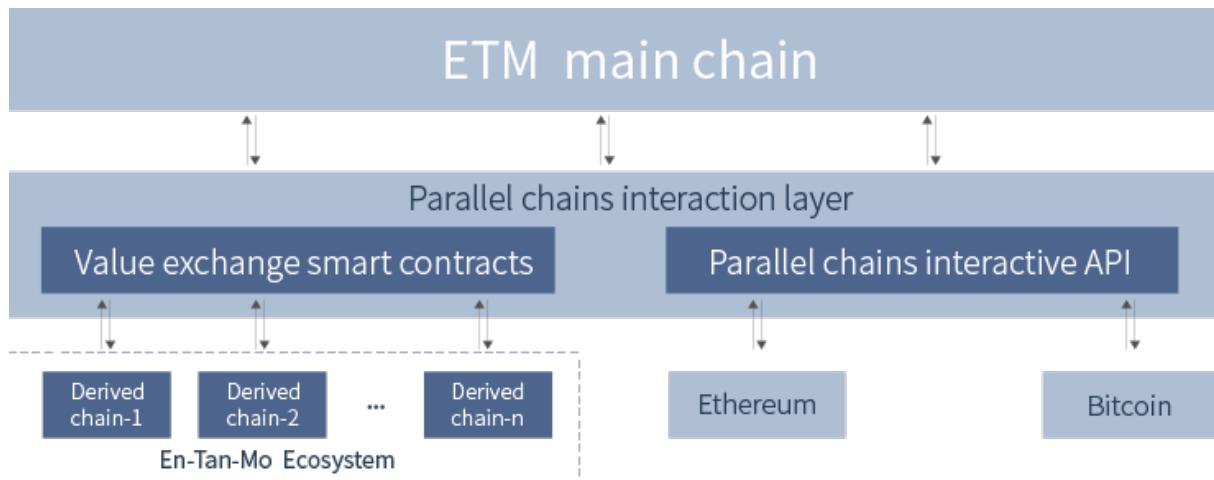
## Description du diagramme structurel du système:

Couche d'application (web, desktop, mobile) accès aux données via une passerelle d'accès unifiée. Interaction de données via des composants d'application et des ressources hors ligne (systèmes existants). Les composants de l'application interagissent avec les données via le protocole d'accès ouvert. Le composant d'application intègre en interne les données sur et hors de la chaîne. La chaîne principale et la chaîne d'application communiquent via les données de protocole internes et la transmission de valeur. Interaction croisée avec des tiers via la couche proxy.

# 6 L'écosystème En-Tan-Mo

## 6.1 Chaîne centrale et chaînes dérivées

Parmi les nombreux problèmes auxquels sont confrontés les systèmes de blockchains, l'absence d'interopérabilité entre blockchains limite considérablement le potentiel d'application. Qu'il s'agisse de chaînes publiques ou privées, la clé d'un transfert de valeurs réussi est d'employer une technologie inter-chaînes. De telles technologies connectent et augmentent des blockchains jusque-là isolées, plus propices à l'enfermement propriétaire qu'à un transfert de valeurs fluide. Après avoir étudié les technologies inter-chaînes existantes, En-Tan-Mo est en mesure de proposer un nouveau protocole interactif de chaînes parallèles, qui facilite de transfert de valeurs et met en place un écosystème de blockchains qui peut, via les apps, atteindre plus de dix Mirions d'utilisateurs.

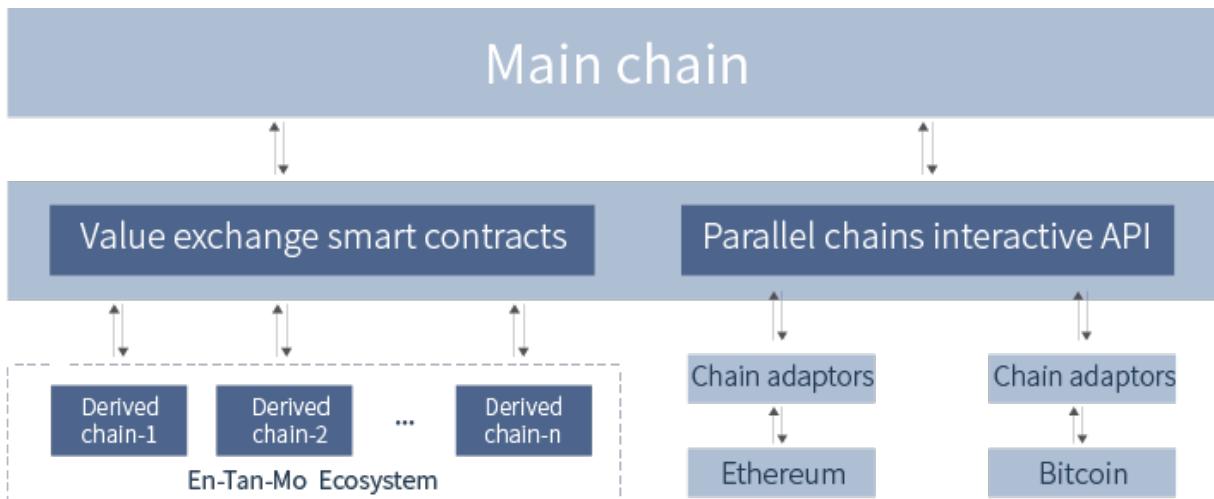


Afin de résoudre le problème de l'expansion rapide et du BaaS, le système En-Tan-Mo comporte une chaîne centrale et de multiples chaînes dérivées. La chaîne centrale est responsable de la sécurité du réseau et des transferts de valeurs. Une chaîne dérivée est une blockchain de type DAPP, indépendante et isolée. En héritant des, et en répliquant les technologies de la chaîne centrale, chaque DAPP possède son propre livre de compte et son propre système de tokens. Son mécanisme de consensus, ses paramètres de blocs et les types de transactions peuvent être personnalisés. Les chaînes dérivatives sont parallèles les unes des autres.

Elles permettent le transfert bidirectionnel d'actifs entre la chaîne centrale, les autres chaînes dérivées et des systèmes de blockchains extérieurs grâce au « parallel chain interaction layer », qui permet aux utilisateurs d'intégrer des actifs existants à En-Tan-Mo.

## 6.2 Protocole d'interaction des chaînes parallèles

Le protocole d'interaction des chaînes parallèles En-Tan-mo rend possible le transfert de valeurs entre des



blockchains différentes. Il est essentiellement constitué de deux éléments : un module de chain-adaptation et un contrat intelligent d'échange de valeurs. L'objectif principal de l'adaptateur de chaînes est de pourvoir En-Tan-mo d'interfaces lui permettant d'interagir avec différentes chaînes dans le contexte de contrats intelligents et de transferts de valeurs, de sorte à pouvoir vérifier plusieurs transactions sur plusieurs chaînes. Simultanément, les membres de la communauté peuvent développer et améliorer la diversification des fonctions des adaptateurs de chaînes, et obtenir des tokens en récompense. Par exemple, des applications peuvent passer d'une blockchain à une autre à l'aide de différents protocoles d'adaptateurs de chaînes. Le protocole d'échange de valeurs est au cœur d'un ensemble de protocoles d'interaction parallèles. Il permet aux utilisateurs d'échanger et de transférer des capitaux sur un large ensemble de blockchains, y compris la chaîne centrale, les chaînes dérivées et les chaînes extérieures. Un système internet de connexion de valeurs par interchaînes sera donc mis en place.

### Adaptateurs de chaînes

L'adaptateur de chaîne est comparable à un pilote d'installation. Il convertit le protocole de blockchain de sorte à ce qu'il soit plus facile à mettre en relation avec la chaîne centrale En-Tan-Mo, afin qu'il puisse y effectuer des contrats intelligents de transferts de valeurs. Parmi les technologies employées à cet effet, on compte Hash Time Lock Constructs (HTLC), SPV proof, et API development.

En-Tan-Mo proposera, dans un premier temps, des adaptateurs pour les systèmes de blockchains les plus courants, tels que Bitcoin et Ethereum, et sera disponible en open source à terme. Chacun sera en mesure d'améliorer les protocoles d'open-chain access et d'y planter ses propres codes. En-Tan-Mo encouragera la création de nouveaux protocoles de blockchain, et des tokens seront attribués en récompense.

### Contrats intelligents et échanges de valeurs

Quoique la technologie innovante des blockchain attire l'attention des investisseurs du monde entier, un problème se pose depuis longtemps : les transactions entre systèmes de blockchains nécessite l'assistance d'un tiers tel que les exchanges, et c'est ce qui doit être remplacé par la technologie de décentralisation. En-Tan-Mo emploie des contrats intelligents de confiance minimum et des adaptateurs de chaîne, qui remplace ces intermédiaires et connectent les chaînes. En approfondissant la connexion entre les deux plus importants éléments des blockchains, cette approche conduira En-Tan-mo à devenir un réseau de transfert de valeurs mondial.

Les contrats intelligents d'échange de valeurs dépendent de la Turing complete virtual machine d'En-Tan-Mo, qui en assure le fonctionnement et la sécurité. Un contrat intelligent d'échange de valeurs entre des chaînes dérivées et la chaîne centrale est comparable à un échange décentralisé. Il dispose d'une adresse de portefeuille ETM et le contrôle sur les chaînes correspondantes. Une fois qu'un utilisateur initie un transfert vers une chaîne dérivée qui est reconnu par l'adaptateur de chaînes, le contrat intelligent d'échange de valeurs transférera automatiquement le montant équivalent vers l'adresse de portefeuille ETM de la chaîne centrale afin de conclure l'échange. Simultanément, ETM a incorporé Hash Time Lock Constructs, de sorte à éliminer les risques pour les utilisateurs durant les échanges.

Pour prendre un exemple, imaginons une transaction Bitcoin/ETM. Il se passerait ceci :

L'Utilisateur A, qui se trouve sur la blockchain Bitcoin, s'enregistre avec En-Tan-Mo afin d'attacher le connexion entre l'adresse du portefeuille ETM de l'Utilisateur A et l'adresse du portefeuille BTC.

L'Utilisateur A génère un numéro secret aléatoire (a) et trouve sa valeur de hachage H(a). Alors, une transaction spéciale est initiée de la blockchain Bitcoin vers l'adresse Bitcoin du contrat intelligent d'échange de valeurs, qui est vérrouillé pour douze heures par la technologie Hash Time Lock Controls. Le contrat intelligent d'échange de valeurs En-Tan-Mo doit produire une image de hachage H(a) conforme à l'image originale afin d'obtenir le token. Sans cela, au bout de douze heures, le BTC de la transaction est automatiquement renvoyé à l'adresse de portefeuille Bitcoin de l'Utilisateur A.

Le contrat intelligent En-Tan-Mo surveille la confirmation de ces transactions spéciales dans la blockchain Bitcoin grâce à l'adaptateur de chaîne Bitcoin et effectue une vérification SPV. Une fois la vérification SPV effectuée, le contrat intelligent de valeur d'échange En-Tan-Mo initie une transaction spéciale dans la chaîne centrale, à destination de l'adresse de portefeuille ETM de l'Utilisateur A, qui sera vérifiée six heures durant. Si l'Utilisateur A désire obtenir le token ETM durant la transaction, l'image originale (a) de la valeur de hachage H(a) doit être soumise. Sans cela, le token ETM de la transaction est automatiquement renvoyé à l'adresse du portefeuille ETM au bout de six heures. Une fois que l'Utilisateur A présente le numéro secret (a) afin d'obtenir son token ETM, le contrat intelligent connaîtra le

numéro (a) et sera donc en mesure d'accéder au réseau de blockchain Bitcoin via l'adaptateur et d'accepter l'Utilisateur A. Ainsi, du Bitcoin a été transféré d'un utilisateur à un autre et la transaction est complète.

Il est important de préciser que la chaîne centrale n'est utilisée que comme échange de valeurs décentralisé, et qu'elle n'a pas besoin de verrouiller l'Utilisateur A pour achever le transfert de valeurs. L'Utilisateur A transfère du Bitcoin à l'adresse de portefeuille du contrat intelligent, les contrats intelligents pouvant être employés par quiconque souhaite échanger des tokens ETM contre du Bitcoin. En même temps, une fois les Bitcoins échangés contre des tokens, ces tokens peuvent être renvoyés non seulement à la blockchain Bitcoin, mais également vers n'importe quelle autre blockchain, selon le même procédé. De fait, ce qu'En-Tan-Mo accomplit est un échange de valeurs plutôt qu'un verrouillage d'actifs. De plus, les contrats intelligents d'échanges de valeurs n'ont, au départ, aucun token. Il leur faut pour cela que des utilisateurs de blockchain investissent. En retour, le contrat intelligent distribue les frais de transaction de l'utilisateur durant le procédé d'échange de valeurs aux investisseurs appropriés en fonction de leur investissement initial. Durant le processus d'investissement, les utilisateurs sont en mesure de retirer les fonds d'investissement des contrats intelligents à tout moment.

En somme, en se basant sur les contrats intelligents d'échange de valeur, En-Tan-mo bâtit un réseau de valeurs interchaînes. En-Tan-Mo ne crée pas de valeur à partir de rien, mais sert d'agent de transfert.

### Écosystème des applications

En-Tan-Mo est une plateforme de blockchain de nouvelle génération. En gérant les APPs sur des chaînes dérivées indépendantes, on résout les problèmes qui perturbaient jusque-là les autres chaînes, par exemple l'augmentation de la taille des blocs et les délais de synchronisation. Le mode de chaînes multi-dérivatif est une solution idéale aux problèmes d'encombrement des réseaux, en cas de transactions nombreuses. Les utilisateurs ont juste besoin de télécharger une chaîne dérivée lorsqu'ils ont besoin de l'APP correspondante. Cela réduit grandement les données de synchronisation inutiles et garantit les hautes performances constantes du réseau En-Tan-Mo. De plus, grâce aux contrats intelligents d'échanges de valeurs, les réseaux interchaînes peuvent être efficacement intégrés avec des technologies telles que les graphènes de haute-performance, ce qui allège les réseaux de paiement. Ainsi, En-Tan-Mo est capable de supporter les APPs de plus de dix Mirions d'utilisateurs, et de s'interconnecter avec des systèmes de blockchains entiers.

## 6.3 Mir Mall

Le Mir Mall d'En-Tan-Mo peut, sans effort et de manière efficace, aider les entreprises et les particuliers à intégrer des blockchains à des applications plus rapidement et économiquement, de sorte à ce que l'utilisateur se sente en sécurité. Au vu de la nature centralisée des APP actuelles, nous appelons les applications décentralisées sur chaînes dérivatives des DAPP. Mir Mall possède les avantages suivants :

- (1) Donner accès à un écosystème d'APP de plus de dix Mirions d'utilisateurs.
- (2) Les actifs des chaînes dérivées peuvent être échangés contre d'autres tokens (tels que ETM/BTC/ETH) à travers les protocoles d'échange des chaînes parallèles d'En-Tan-Mo. En résultat, les applications basées sur En-Tan-Mo auront davantage d'utilisateurs.
- (3) À partir des protocoles d'échange des chaînes parallèles En -Tan-Mo, les DAPP peuvent accéder aux données de multiples blockchains, ce qui leur permet d'opérer sur chacune de ces chaînes.
- (4) Grâce à la technologie de chaînes dérivées d'En-Tan-Mo et une série de SDK, d'API et de modèles fournis par les développeurs, ces derniers peuvent se concentrer sur leur stratégie de business et fabriquer, tester et publier facilement leurs DAPP personnelles. La réduction de coûts en recherche et développement qui s'ensuit aidera les développeurs à posséder rapidement leurs propres DAPP sur Mir Mall. De surcroît, ces DAPP pourront être téléchargées et exécutées par n'importe quel nœud ETM, et être mises à disposition de n'importe quel utilisateur de blockchain.
- (5) À partir de la technologie de chaînes dérivées En-Tan-Mo, les développeurs peuvent customiser les bases de données personnalisées, les mécanismes de consensus, les types de transactions et le système de comptabilité des DAPP du Mir Mall.
- (6) En-Tan-Mo mettra en place un système de récompenses complet. Les développeurs de DAPP d'excellence seront récompensés en tokens.

## 7 Le fonctionnement d'En-Tan-Mo

La communauté En-Tan-Mo se compose de trois organisations : la Fondation En-Tan-Mo, IOEM et Emgo. La Fondation En-Tan-Mo est la fondation sur laquelle reposent les deux autres groupes. La Fondation est une organisation à buts non-lucratifs établie à l'étranger. Elle offre un soutien exhaustif aux utilisateurs En-Tan-Mo, et s'assure du bon développement du projet En-Tan-Mo. Emgo est une organisation leader dans le domaine de la recherche en ce qui concerne la sécurité et le développement. Quant à IOEM, il s'agit d'une société de soutien à l'investissement pour les entreprises du monde entier.

### 7.1 La Fondation En-Tan-Mo

La Fondation En-Tan-Mo est une organisation à buts non-lucratifs établie à l'étranger, principalement en charge de la construction de l'écosystème et d'apporter un soutien technique à la communauté En-Tan-Mo. Ses tâches principales sont la régulation, la protection et la promotion de l'infrastructure autonome En-Tan-Mo et des protocoles de blockchains. Par ailleurs, elle contribue également à étudier et proposer des systèmes de régulation sur les blockchains et les cryptomonnaies. Elle se voulait à protéger et améliorer l'écosystème En-Tan-Mo, ainsi qu'à souder, éduquer et nourrir les communautés En-Tan-Mo.

Sous la supervision active de la communauté En-Tan-Mo dans son ensemble, nous proposons que la Fondation se charge de planifier le développement à long terme d'En-Tan-Mo. En sus, la Fondation agira en organisme d'intérêt public, s'intéressera aux affaires du monde et à la philanthropie dans le monde entier, de sorte à promouvoir un système de confiance mondial et public.

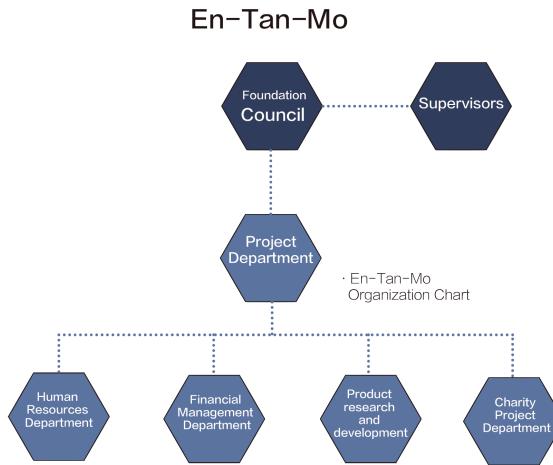
Le Conseil de la Fondation En-Tan-Mo a adopté un fonctionnement démocratique en ce qui concerne la prise de décisions, ses politiques constitutionnelles et les responsabilités de son secrétaire général, qui agira sous la tutelle du Conseil. Le directoire chapeaute les opérations du Conseil. Ce comité comprend des personnalités publiques reconnues, ainsi que des professionnels de la finance.

#### Le Conseil de la Fondation En-Tan-Mo

Les opérations caritatives sont au cœur des préoccupations du Conseil de la Fondation En-Tan-Mo. La Fondation se divise en différents pôles : recherche de produits, promotion et marketing, ressources humaines, aspects juridiques, etc. Chaque pôle contribuera à la gestion quotidienne des affaires de la Fondation.

#### Les Opérations Caritatives de la Fondation En-Tan-Mo

Le Département des Opérations Caritatives de la Fondation En-Tan-Mo est au cœur de la « business unit » de celle-ci. Il est responsable des opérations et du management des projets d'aide publique de la Fondation, du respect des décisions du Conseil et de la réalisation des objectifs. Le Directoire de la Fondation contribuera



à sélectionner, planifier et financer des idées en fonction de leur excellence, et l'équipe se chargera d'en faire une réalité. Aux premières heures du projet, le département des Opérations Caritatives a été chargé d'établir la constitution de la Fondation En-Tan-Mo, qui fut ensuite adopté par le Conseil.

Le département caritatif d'En-Tan-Mo est également responsable des mécanismes de réactivité. Sous le contrôle du Conseil En-Tan-Mo, la Fondation définit sa politique de relations publiques et, après consensus, la dévoile au grand public. Les grandes lignes de développement du Fond seront ébauchées par le Conseil, et incluront de nouveaux canaux promotionnels, qui seront mis en place puis développés.

#### Le Département des Finances En-Tan-Mo

En-Tan-Mo dispose d'un mécanisme de finances indépendant et transparent.

(a) La Fondation En-Tan-Mo dévoilera son budget un an à l'avance. La Fondation est une association à buts non-lucratifs. Ses sources de financement principales sont le capital-investissement et le token discounting. Chaque transaction sera validée par un directeur administratif et financier professionnel et inscrite dans le bloc afin de garantir une supervision financière transparente et non-rétroactive. Par ailleurs, toutes les dépenses de la Fondation seront soumises à l'audit de directeurs administratifs et financiers professionnels, et les registres seront inscrits dans le bloc.

(b) La Fondation En-Tan-Mo publiera un rapport financier mensuel, qui garantira le rapprochement des

fonds. Ce rapport sera soumis à l'audit des directeurs administratifs et financiers désignés par le Fond et des employés désignés par le Comité des Ressources Humaines d'En-Tan-Mo.

(c) La communauté En-Tan-Mo sera régulièrement informée des levées de fonds, des événements importants et du développement de la Fondation. Les changements ou événements importants seront annoncés à l'avance.

### Le Département des Ressources Humaines d'En-Tan-Mo

En-Tan-Mo dispose d'un système de ressources humaines ouvert à la communauté tout entière, ce qui diffère d'une structure d'entreprise classique. Les pratiques d'embauche d'En-Tan-Mo sont justes, transparentes et inscrites dans la blockchain.

(a) Le recrutement des employés de base se fera selon deux séries de test effectués par l'équipe, de sorte à générer un rapport d'évaluation qui sera inscrit dans les archives. Ces rapports seront inéltérables.

(b) Les candidats sélectionnés seront soumis à l'approbation financière d'un comité. Les développeurs et les managers d'importance devront se soumettre à un processus de division des tâches approuvé par la hiérarchie de la Fondation En-Tan-Mo.

(c) Les tâches qui relèveront de la sous-traitance seront soumises à un accord de sous-traitance rigoureux, dont tous les aspects seront précisés à l'avance (y compris les aspects financiers). La communauté tout-entière sera informée, et les contrats de sous-traitance seront mués en contrats intelligents.

### Le Directoire En-Tan-Mo

Le Directoire En-Tan-Mo est en charge de l'ensemble des contributeurs d'En-Tan-Mo. Afin d'être en mesure de chapeauter et légitimer tout ce qui est effectué par le personnel et de préserver les intérêts de l'entreprise et de ses actionnaires, le Directoire a le devoir d'inspecter et d'avaluer scrupuleusement la situation financière et la gestion de la Fondation. Le Conseil rendra des comptes au Directoire, selon ses exigences, pour tout ce qui concerne les projets, les dépenses, les pertes et profits.

## 7.2 La Corporation de Développement Technologique ETM FinTech

Le rôle d'ETM FinTech est principalement de développer et d'entretenir ce nouvel écosystème. Le développement d'En-Tan-Mo est essentiellement planifié en quatre phases :

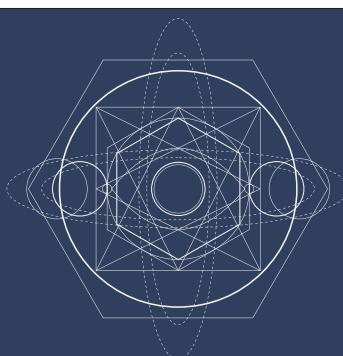
Petrarch : ETM FinTech développe une nouvelle blockchain En-Tan-Mo décentralisée, totalement protégée par, et fondée sur des protocoles « network-based » et des technologies de cryptage strictes, qui donne naissance à une nouvelle monnaie qui peut être échangée contre des monnaies légalement reconnues..

Masaccio : ETM FinTech enregistre toute sortes d'actifs sur la blockchain, de sorte à s'assurer de leur sécurité et de l'intégrité des données. Emgo développe les contrats intelligents, se sert de technologies de preuve à divulgation nulle de connaissance et développe des technologies Lightning Network afin d'améliorer la vitesse de transaction, de réduire la charge de la blockchain et d'en améliorer l'évolutivité.

Da Vinci : ETM FinTech se sert d'En-Tan-Mo pour conduire le système à épouser des scénarios d'application plus vastes. Le développement du standard des contrats intelligents est la clé. Les transactions financières peuvent être converties de sorte à être compatibles avec En-Tan-Mo, y compris les actions, le capital-investissement, le crowdfunding, les obligations, la gestion alternative et tout type de produits dérivés financiers.

Giorgione : A ce stade, En-Tan-Mo prend pleinement part au champ économique. On peut l'employer à améliorer la distribution mondiale de ressources matérielles et d'acrits humains, à promouvoir une collaboration de grande échelle dans le domaine des sciences, de la santé, de l'éducation. En-Tan-Mo se verra employé dans des champs aussi variés

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

que l'approvisionnement et acquisition automatisés, les réseaux intelligents, l'automatisation des chaînes logistiques, l'échange d'actifs virtuels, l'enregistrement de titres de propriété et bien d'autres.

Une fois le système lâché dans la nature, ETM FinTech n'en contrôlera plus la direction. Seuls les actionnaires du système, les possesseurs de tokens et les chercheurs intéressés auront le pouvoir de décider du développement du système.

## 7.3 L'ETM BD Business Cooperation Company

Le rôle d'ETM BD est de développer, maintenir et encourager les initiatives de business, et de contribuer à les intégrer dans le système de chaînes dérivées d'En-Tan-Mo. En-Tan-Mo vise à créer un système simple à l'usage, complet, plug-and-play et user-friendly. Pour ce faire, En-Tan-Mo proposera des solutions intégrées telles que le chaînage dérivé gratuit, les contrats intelligents et l'hébergement d'applications. À l'intérieur de l'écosystème En-Tan-Mo, les développeurs peuvent aisément itérer leurs applications En-Tan-Mo et les mettre à disposition dans la boutique d'apps décentralisée du système. Ces applications peuvent être téléchargées et exécutées par des nœuds distribués sur la plate-forme, et être mis au service des usagers ordinaires. Le processus entier a lieu dans l'environnement honnête et sécurisé des chaînes dérivées d'En-Tan-Mo.

Tout individu ou entreprise intéressé par la technologie de blockchain En-Tan-Mo, et désireux de l'employer pour modifier le paysage économique, recevra le soutien d'ETM BD sous des formes diverses, tels que l'investissement, le « joint-ICO », l'assistance au développement, des solutions et des applications En-Tan-Mo.

---

### Notes :

#### 1. Politique de risques

La réglementation des blockchains et projets associés est loin d'être claire sur tous les territoires. Ce flou juridique entraîne des risques inhérents. Si la valeur globale du marché des actifs numériques est surévaluée, les risques liés à l'investissement augmentent et les participants peuvent s'attendre à une croissance excessive. Toutefois, il est toujours possible que rien ne se passe.

#### 2. Risques régulatoires

Les transactions d'actifs numériques, y compris En-Tan-Mo, comportent un taux d'incertitude élevé. Du fait de l'absence de toute supervision des échanges d'actifs numériques, il demeure toujours possible que les tokens explosent ou plongent, ou qu'ils soient contrôlés par le fournisseur. Si l'on manque d'expérience, il peut être éprouvant de se soumettre à la pression psychologique liée aux fluctuations du marché. Bien que les experts et les chercheurs s'accordent à recommander la prudence, aucun système préventif n'a été mis en place. De fait, il est difficile d'éviter ce genre de risques.

Il est certain que dans un avenir plus ou moins proche, des régulations seront établies afin d'encadrer ou de restreindre le champ des tokens électroniques. Si/when ces régulations sont mises en place, les tokens obtenus au préalable sont susceptibles de subir des fluctuations, des restrictions quant à leur valeur, leur revente et autres chocs liés aux marchés financiers.

#### 3. Risque collectif

Aujourd'hui, de nombreuses équipes travaillent sur les technologies de blockchain. La compétition est féroce et fait pression sur les projets en cours. La capacité d'En-Tan-Mo à percer et à être reconnu dans ce contexte de saturation ne dépendra pas que du travail de ceux qui défendent ce projets, mais aussi de la concurrence - potentiellement sauvage - de ses rivaux, parmi lesquels on compte des oligarches. En-Tan-Mo repose sur la riche expérience, la vitalité et la détermination de son fondateur, qui a su réunir une équipe de talent autour de lui, composée de développeurs de haut niveau et de professionnels de la blockchain. La stabilité et la cohésion de cette équipe est fondamentale pour le bon développement d'En-Tan-Mo. Il n'est toutefois pas impossible d'exclure le départ de certains membres clés de l'équipe, ou la possibilité de conflits internes, qui seraient susceptibles d'affecter négativement la performance d'En-Tan-Mo.

### Clause de non-responsabilité

Ce document est purement informatif. Le contenu de ce document ne constitue pas une publicité pour de

l'investissement, une offre ou une invitation à vendre des actions ou à s'investir de quelque manière que ce soit dans En-Tan-Mo ou toute autre entreprise. Ce type de sollicitations doit se faire dans un contexte confidentiel et en conformité à la loi. Le contenu de ce document ne doit pas être interprété comme une incitation à participer à En-Tan-Mo. Nul démarque associée à ce document, y compris la demande ou le partage d'une copie de ce document, ne saurait être interprété comme une participation effective au projet. L'âge légal et la pleine capacité des droits civiques est requise pour toute participation à une transaction. Tout contrat signé avec En-Tan-Mo est réel et effectif. Tous les participants ont signé leur contrat volontairement, après avoir déclaré comprendre pleinement et clairement la structure et les fonctions d'En-Tan-Mo au préalable.

L'équipe d'En-Tan-Mo s'efforcera de faire en sorte que les informations présentes dans ce document demeurent véritables et exactes. Au cours du processus de développement, la plate-forme est susceptible d'être mise à jour, ce qui incluse les mécanismes de la plate-forme, les tokens et leurs mécanismes, et la distribution de tokens entre autres choses. Certains éléments décrits dans ce document sont susceptibles d'être ajustés au fur et à mesure que le projet progresse. Certains éléments de ce documents sont donc susceptibles d'être ajustés en conséquence. L'équipe annoncera et publiera toute nouvelle version de ce document sur le site internet. Les participants sont tenus de se procurer toute mise à jour de ce document dès sa parution, et de tenir compte des changements qu'une telle mise à jour pourra contenir.

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

En-Tan-Mo ne saurait être responsable du fait qu'un participant agisse inconsidérément sur la seule foi de ce document, ou de son incompréhension de ce document. L'équipe fera tout ce qui est humainement possible pour atteindre les objectifs décrits dans ce document. Toutefois, du fait de facteurs extérieurs, l'équipe ne saurait garantir le bon déroulement des opérations décrites dans ce document.

En-Tan-Mo est un outil important en termes de performance de plate-forme mais il ne s'agit pas d'un produit d'investissement. Le fait de s'équiper d'En-Tan-Mo ne donne pas droit à la possession, au contrôle ou à un pouvoir de décision concernant la plate-forme. En-Tan-Mo, en tant que cryptomonnaie digitale, ne correspond à aucune des catégories suivantes :

- (a) quelque type de monnaie que ce soit ;
- (b) caution de garantie
- (c) parts de l'entreprise
- (d) actions, obligations, billet, mandat, certificat ou quoi que ce soit qui garantisse quelque droit que ce soit

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

La valeur ajoutée d'En-Tan-Mo est susceptible de dépendre des lois du marché, ou pas. En-Tan-Mo peut n'avoir aucune valeur que ce soit. L'équipe ne s'engage pas à ce qu'En-Tan-Mo ait quelque valeur que ce soit et ne saurait être responsable des fluctuations de la valeur d'En-Tan-Mo. Dans la limite de ce qui est autorisé par la loi, l'équipe ne saurait être responsable des risques et pertes engendrées par une participation au projet, y compris la perte de profits, d'informations ou toute autre forme de perte économique. Notre équipe ne saurait être tenue responsable de quoi que ce soit.

La plate-forme En-Tan-Mo se conforme aux règles d'auto-discipline indispensables au sain développement des entreprises et de l'industrie. La participation au projet signifie que le participant accepte de se conformer à de telles normes. De même, toute information donnée aux participants afin de s'y conformer devra être complète et avérée.

La plate-forme En-Tan-Mo a informé tout participant des risques. Une fois impliqués, les participants ont signifié leur compréhension et leur connaissance des termes et conditions qui leurs ont été donnés, et accepté de se joindre à la plate-forme.