everiToken

WHITEPAPER TECHNIQUE

Version 3.1

Zug, Suisse

everiToken

Dernières Modifications: 26 mars 2019

DISCLAIMER

- Le whitepaper technique d'everiToken est destiné à un usage purement informatif.

- Ce whitepaper ne représente en aucun cas l'expression ou l'évocation de quelconques garanties, preuves, attentes, etc…

- Les spécifications techniques ainsi que les procédés technologiques de réalisation décrits dans ce whitepaper sont susceptibles d'évoluer avec le temps.

- L'équipe technique est susceptible d'être remodelée ou réorganisée à tout moment, sans quoi la perte d'un élément-clé de l'équipe technique pourrait mener à l'échec ou à l'aboutissement seulement partiel du projet.

- Ce whitepaper est fourni « en tant que tel ». L'équipe en charge du projet ainsi que chacun de ses membres ne pourraient en aucun cas être considérés responsables de son contenu ainsi que des conséquences résultant de l'usage de ce contenu.

- Le token décrit et mentionné dans ce whitepaper ne possède aucune valeur pratique. Son usage est restreint au le monde virtuel et dans le seul but de confirmer les droits de chaque utilisateur vis-à-vis de ce token.

- Tout événement se produisant au sein de la blockchain ou de ses sous-jacents tels qu'ils sont décrits dans ce whitepaper technique est le fruit d'un processus automatique dicté par un programme, et nous ne pourrons aucunement être tenus responsables de ses conséquences. Les individus ou organisations sont responsables des conséquences de leur propre usage de la blockchain everiToken.

- L'intégralité du contenu de ce whitepaper technique peut être utilisée à des fins non-commerciales. En revanche, ce whitepaper technique ne saurait d'aucune sorte être modifié ou altéré. Nous ne pourrons aucunement être tenus responsable des conséquences de l'utilisation du contenu de ce document.

everiToken

Sommaire

everiToken

Partie I. Origine et Vision

Avènement de l'Économie Tokenisée

La technologie « blockchain » a fêté son 10ème anniversaire en février 2019. En dépit de son évolution à travers le temps, une interrogation majeure reste en suspens : la blockchain révolutionne-t-elle les moyens de production au point de créer de la valeur pour l'économie mondiale ?
Si l'on s'en tient aux données actuelles, les actifs gérés au sein des différentes blockchains (décrits comme « actifs on-chain ») consistent pour la plupart de cryptomonnaies de toutes sortes, représentant une valeur de marché totale d'environ 150 million de dollars. Les actifs représentés sur ces différentes blockchains sont généralement caractérisés par une forte volatilité ainsi qu'une intense spéculation, et ils ne parviennent pas à créer une quelconque valeur pour l'économie mondiale. Depuis l'ère de Satoshi Nakamoto, le monde entend faire de ces cryptomonnaies un moyen de paiement. Pourtant, les cryptomonnaies ne remplissent pas ce rôle, qui reste confiné aux monnaies traditionnelles. En réalité, le terme « cryptomonnaie » ne fait pas référence à une véritable monnaie en état de circuler.

D'un côté, le droit d'émettre une monnaie est le fruit d'un processus politique et le pouvoir monétaire doit appartenir à l'État. Il est donc très difficile pour une cryptomonnaie de remplacer les monnaies traditionnelles (appelées « monnaies-fiat »). Sans autorisation et sans soutien de la part de l'État, les « monnaies virtuelles » ne demeurent qu'un idéal sans réel espoir de succès.

D'un autre côté, la plupart des actifs courants mondiaux (qu'ils soient matériels ou immatériels) ne sont pas sur des blockchains (ils sont donc « off-chain ») et les interactions entre les blockchains et les actifs « off-chain » sont grandement limitées.

Un token n'est-il donc qu'une « monnaie virtuelle » de plus ? Pas du tout. Selon la définition de base du terme « token », il s'agit d'un « symbole ou d'un signe », mais il faudrait davantage le considérer comme un certificat plutôt que comme une « monnaie virtuelle ». De tels certificats peuvent représenter toutes sortes de droits et de permissions, comme par exemple des points de fidélité, coupons, certificats

d'identité, diplômes, titres de propriété, clés d'accès, billets pour événements en tous genres, ainsi que tout objet destiné à certifier des droits et permissions.
Si l'on se penche sur le passé, le fait de certifier des droits et permissions à travers une preuve a constitué un élément majeur des civilisations humaines au cours de l'Histoire. Les comptes, propriétés, qualifications et autres preuves ont toujours été représentatifs de certains droits et permissions pour ceux qui les détenaient. Comme l'écrit Yuval Noah Harari dans « Une brève histoire de l'Humanité », ces « réalités fictives » constituent les raisons majeures pour lesquelles les individus les plus sages se sont décidés à construire la civilisation humaine. Si ces preuves de droits et de permissions étaient toutes digitales, électroniques et protégées par cryptographie afin de déterminer leur authenticité et leur intégrité, la civilisation humaine entrerait dans une nouvelle révolution. Ce phénomène porte le nom d'« **économie tokenisée ».**

Maintenir des certificats sur la blockchain permet d'établir de solides fondations en termes de confiance et de traçabilité, impossible à atteindre dans le cadre de l'infrastructure centralisée traditionnelle. Par conséquent, si un certificat apparait comme la face émergente de l'économie tokenisée, alors la blockchain constitue la partie immergée de cette économie tokenisée. Chacune est intimement reliée à l'autre et lui est dépendante.

Analyse Concurrentielle

En tant que **blockchain publique** créée pour les besoins de l'économie tokenisée, everiToken possède actuellement deux concurrents principaux : Ethereum et EOS. Notre avantage competitif apparait comme évident lorsque l'on analyse les forces, faiblesses, opportunités et menaces au sein de notre marché.

Forces et Faiblesses（Strength and Weakness):

Le projet everiToken part du principe selon lequel la blockchain doit être utilisée en tant qu'outil pour l'économie tokenisée afin de maintenir et gérer de façon efficace les différentes preuves de droits et de permissions selon les trois caractéristiques suivantes :

1. **Preuve de Droits Digitaux et de Permissions** : Ce certificat doit être une forme digitale crédible de preuve de droits et permissions, qui doit être adossée à quelque chose possédant une valeur inhérente et intrinsèque (que celle-ci soit

tangible ou intangible).

2. **Sécurité, Encryption et Gestion des Autorisations**: Ce certificat doit être vérifiable, immuable, privé, supervisé, protégé par cryptographie et uniquement utilisable par ceux qui y sont autorisés.
3. **Négociabilité:** Ce certificat peut être facilement vendu et échangé.

Au vu des différents critères mentionnés ci-dessus, nous proposons un ensemble de solutions permettant la mise en œuvre de l'économie tokenisée, afin de promouvoir la gestion et la mise en circulation de tokens et d'établir les fondations de cette économie tokenisée. Plus spécifiquement, nous nous sommes assurés que notre solution comportait les trois caractéristiques suivantes, en vertu des critères mentionnés ci-dessus :

- **Rapidité et Simplicité d'Émission des Tokens :** les utilisateurs n'ont pas besoin d'écrire en langage informatique et peuvent facilement émettre leurs propres tokens à travers notre API (pour les applications, sites internet et autres applications tierces)

- **Efficacité de Transfert des Tokens :** garantit les transferts en tokens en l'espace de quelques secondes, pour des volumes de l'ordre de la centaine de million de tokens, et cela simultanément.
- **Gestion Flexible des Autorisations :** un modèle simple, élégant et unifié permettant d'atteindre la gestion des autorisations, supportant la multipropriété, le recouvrement des clés privés, l'autorité à plusieurs niveaux, la légalité, la supervision par les autorités gouvernementales ainsi que d'autres besoins complexes sans nécessiter d'efforts supplémentaires en termes de programmation

Examinons Ethereum et EOS:

Ethereum: ERC20/ERC721

Le moyen principal employé pour mettre en place l'économie tokenisée au sein d'Ethereum est de développer des smart-contracts basés sur les protocoles dits ERC20 et ERC721. Parmi ces-derniers, ERC20 supporte les tokens dits « fongibles » (FT) et ERC721 supporte les tokens dits « non-fongibles » (NFT). Cependant, de sérieux problèmes demeurent :

- **TPS (Transactions Par Seconde)**: A l'heure actuelle, Ethereum ne peux supporter qu'un maximum de 20 transactions par seconde et est donc incapable de satisfaire les besoins nécessaires à l'utilisation et à la circulation d'un token.
- **Coût**: L'implémentation des smart-contracts sur la blockchain Ethereum nécessite le paiement de frais (appelés « gas ») pour chaque étape. Pour des fonctions impliquant une logique commerciale complexe (comme par exemple le fait de partager les droits de détention des tokens entre plusieurs utilisateurs, la supervision, la conformité vis à vis de la loi, etc…), le prix peut très vite se révéler trop élevé et incontrôlable.
- **Popularité:** la mise en œuvre de l'économie tokenisée à travers Ethereum est basée sur les smart-contracts, qui ne sont pas accessible aux individus ne disposant pas d'un bagage de développeur informatique à moins de faire appel à des applications tierces du fait de leur nature complexe. Cela donne lieu à des inquiétudes concernant la sécurité et le respect des régulations, tout en faisant obstacle à l'adoption par le grand public.
- **Non-Standardisation :** Puisque différent smart-contracts suivent des méthodes de développement complètement différentes les unes des autres, les données traitées au sein de ces tokens virtuels ne peuvent être mutuellement échangés et sont donc isolées entre eux. Ceci n'est pas un facteur favorable à la mise en place de l'économie tokenisée. De plus, les utilisateurs ne peuvent pas utiliser une méthode standardisée pour identifier avec précision l'ensemble des cryptoactifs qu'ils possèdent.

EOS

EOS a lancé son « mainnet » en juin 2018 avec pour principal objectif de remédier aux problèmes rencontrés par Ethereum en créant de Nouvelles solutions. Pourtant, cela a engendré une nouvelle vague de problèmes :

- **Sécurité** : Les transactions sous forme de tokens peuvent être adossées à des entités extrêmement précieuses et non-renouvelables/impossibles à recréer. Pourtant, le développement continue à être tributaire des développeurs dont les connaissances et l'expertise sont parfois limitées, ce qui apporte peu de garanties quant à la maitrise des risques et des enjeux sécuritaires de ces derniers.

Les smart-contracts EOS sont basés sur **WebAssembly,** qui est un langage relativement nouveau et est encore en phase beta de son développement. Par ailleurs, les smart-contracts EOS sont « Turing-complets » , ce qui signifient qu'ils sont vulnérables à certaines failles de sécurités parfois provoquées de manière non intentionnelle.

La plupart des gens sont incapables d'écrire des smart-contracts de façon sûre. Afin d'émettre et de transférer des tokens, les utilisateurs doivent s'en remettre à des applications tierces et doivent faire confiance au code rédigé par ces tiers. Ainsi, le contrôle des actifs n'est plus entre les mains des utilisateurs mais est délégué à un tiers.

- **Non-Standardisation** : Tout comme Ethereum, les données traitées au sein de différents smart-contracts ne peuvent ni interagir ni coopérer.
- **Régulation, Confiance et Conformité :** En raison de l'expertise technique requise par l'absence de standardisation et par les besoins de lecture du code, il est difficile pour le gouvernement de mettre en place une régulation. De la même manière, les non-développeurs peuvent éprouver des difficultés à décider s'ils peuvent faire confiance à certains programmes, ce qui rend l'utilisation des blockchains difficile pour les personnes ordinaires et les gouvernements.
- **Efficacité d'Exécution** : Dans le but de répondre à divers besoins, les smart-contracts EOS possèdent des fonctions complexes. Le système inclue de nombreux modules et le fait de planifier et de mobiliser certaines ressources se révèle très difficile. Cela ajoute considérablement au niveau de difficulté général du système et réduit la vitesse à laquelle certaines opérations sont réalisées. Du fait des conflits potentiels existant entre différentes données et fonctionnalités, il est parfois difficile d'avoir recours au multithreading pour accélérer ces opérations, et les coûts de planification sont élevés. Pourtant, pour l'économie tokenisée, ces fonctionnalités complexes sont cruciales et doivent être implémentées.
- **Popularité** : Les besoins de l'économie mondiale en matière commerciale sont complexes, variables et inconstants. Cependant, les smart-contracts requièrent beaucoup de temps pour être développés et testés, ce qui rend difficile le fait de

répondre aux besoins de différents secteurs en un temps limité. Cela constitue un obstacle au développement de l'économie tokenisée.

La différence majeure entre everiToken et les autres est qu'everiToken a recourt à des *safe contracts* alors que les autres utilisent des *smart-contracts*. Cela signifie qu'EveriToken n'est pas « Turing-Complet » et certaines applications ne peuvent être réalisées au sein d'everiToken. Cependant, everiToken peut réaliser 99% des scenarios d'applications requis par l'économie tokenisée et everiToken est la blockchain publique la plus sûre, la plus économique et la plus facile d'utilisation pour les individus à travers le monde.

OM（Opportunités et Menaces）

Afin d'exploiter au mieux les atouts d'everiToken, nous avons créé le standard EvtLink qui permet de connecter « payeurs » et « payés » au sein de différents canaux de données incluant notamment NFC, Bluetooth et QR code. everiPay est un protocole de paiement base sur EvtLink et spécialement conçu pour effectuer des micropaiements en tokens en face-à-face en utilisant la blockchain publique everiToken comme infrastructure de base et everiPass comme protocole de validation des droits de propriété des tokens.
everiPay/everiPass inclue un standard de génération de **QR code** ainsi qu'une définition de protocole de communication. Nous avons réussi à mettre en œuvre une liste impressionnante de fonctionnalités incluant nos innovations :

- **Traitement Instantané :** Une transaction est automatiquement réglée.
- **Décentralisation** : Paiement P2P (peer to peer), pas de plateforme centralisée, personne ne peut modifier les données inscrites sur la blockchain et tout le monde peut accéder à cette plateforme.
- **Haute Sécurité :** Les données et le contenu inscrits dans la blockchain ne peuvent être modifiés, afin de garantir la protection et la sécurité des propriétés des utilisateurs

- **Compatibilité :** everiPay/everiPass supporte tous les tokens supportés par everiToken, ainsi que les monnaies, points de fidélité et même des clés électroniques pour ouvrir des portes. Il suffit d'un téléphone pour l'utiliser n'importe où.

- **Pratique d'Utilisation :** Même si vous ne pouvez pas vous connecter à Internet, vous pouvez effectuer une transaction.

Basé sur les cinq critères mentionnés ci-dessus, everiPay/everiPass peut se révéler comme le service le plus sûr, pratique et facile d'utilisation pour les paiements en face à face et pour la gestion des droits de propriétés des tokens.

Résumé

Certaines menaces demeurent. Comme mentionné précédemment, Ethereum et EOS peuvent être de formidables blockchains pour répondre à certains besoins au sein de l'économie tokenisée. Cependant, leur plus grand problème est la grande barrière à l'entrée pour les nouveaux utilisateurs constituée par les smart-contracts et leur nature. Nous avons résolu ce problème en développant les *safe contracts* et everiToken est désormais prêt à supporter l'économie tokenisée pour tout le monde, à l'échelle mondiale.

Basé sur l'analyse ci-dessus, nous avons mis au point un nouveau concept qui correspond parfaitement et est favorisé par la plupart des applications blockchains et propose une nouvelle blockchain publique ainsi qu'un écosystème, **everiToken,** afin de développer au mieux l'économie tokenisée. Les actifs, certificats et coupons du monde réel peuvent être **digitalisés** à travers l'émission de tokens et peuvent être utilisés avec des standards sans précédents en termes de sécurité, rapidité et de compatibilité du réseau

Partie II. La Technologie everiToken

Safe Contracts

Les smart-contracts sont, en théorie, un moyen efficace de faciliter l'échange décentralisé de biens et de services sans recourir à un intermédiaire. Pourtant, ils souffrent en pratique de multiples failles de sécurité qui résultent d'erreurs d'implémentation et de logique, menant à des conséquences telles que des « lock-outs » , fuites de moyens d'accès et d'invalidation non-contrôlée. Ainsi, les smart-contracts échouent souvent à fournir un niveau suffisant de confiance et peuvent être vus comme moins fiables que les contrats traditionnels et autres moyens d'échanges.

everiToken introduit l'idée nouvelle de *safe contracts* à travers son API. Plutôt que de programmer directement, les utilisateurs s'en remettent à des safe contracts pour faciliter les processus tels que l'émission et le transfert de tokens. En simplifiant les fonctions et en les réduisant aux besoins de base, les safe contracts permettent d'assurer que toutes les transactions effectuées sur la blockchain le sont de façon sûre et sans failles, puisque les fonctionnalités offertes par l'API sont entièrement revues et vérifiées. Bien que les safe contracts ne soient pas Turing-complets, ils peuvent atteindre la majorité des fonctionnalités voulues à travers les APIs, et fournissent une véritable flexibilité aux émetteurs de tokens dans le cadre de la réalisation de services « hors-blockchain » .
De plus, les safe contracts ont l'avantage d'augmenter l'accessibilité et le nombre de transactions par seconde. L'utilisation des APIs facilite l'intégration au sein de workflows déjà existant, sans avoir besoin de programmer de nouveaux codes d'intégration d'autres blockchains à partir de zéro. L'utilisation des APIs permet de distinguer plusieurs types de traductions et des transactions indépendantes en token peuvent être prises en charge en parallèle à des vitesses sans précédent (10 000 TPS atteint sur le mainnet en décembre 2018).

Base de Données

EOS utilise une base de données basée sur Boost.MultiIndex (liste chainée) qui supporte les opérations de rollback (annulation des requêtes). Les instances de tous les contrats en vigueur sont inscrites dans la mémoire de la base de données. Afin de

supporter le rollback lors de la configuration et le retour à la normale lorsque le code du contrat test anormal, il est nécessaire d'enregistrer des données supplémentaires pour le rollback à chaque opération. De plus, toutes les données sont stockées et traitées dans la base de données en mémoire. Avec l'augmentation du nombre d'utilisateurs et de transactions avec le temps, il est probable que la demande de mémoire s'accroitra de façon sensible. Cela se traduira par une demande accrue de capacité de mémoire pour les producteurs de blocks. De plus, si le programme se heurte à un crash ou à un redémarrage, les données mises en mémoire seront perdues. Pour restaurer les données, il faudrait répéter toutes les opérations au sein des blocks, ce qui nécessiterait un temps de redémarrage long et inenvisageable en pratique. Tout en préservant la base de données en mémoire d'EOS, nous avons développé une base de données de tokens basée sur RocksDB et comportant plusieurs atouts.

- RocksDB est une base de données très mature, utilisée à échelle industrielle et possédant une caractéristique de clé-valeur qui a été vérifiée et est utilisée pour les opérations principales de Facebook.

- RocksDB est basée sur LevelDB, mais offre de meilleures performances et davantage de fonctionnalités que LevelDB. Par ailleurs, elle permet d'optimiser les situations de stockage en low-latency, comme Flash et SSD.

- Si nécessaire, RocksDB peut être utilisée comme base de données en mémoire.

- L'architecture fondamentale de RocksDB supporte naturellement le rollback vers différentes versions ainsi que la persistance, et leur influence sur la performance générale et extrêmement basse.

Notre base de données de tokens possède RocksDB comme moteur de stockage sous-jacent. Grâce à cette technologie, nous pouvons garantir un rollback à moindre coût. De plus, la base de données de tokens supporte également des fonctions optionnelles telles que la persistance des données, la sauvegarde quantitative ainsi que la sauvegarde incrémentale pour résoudre des problèmes tels que le démarrage à froid.

Du fait de la nature abstraite des opérations effectuées sur everiToken, le code est fixé, et l'information nécessaire pour chaque opération est minimale. Ainsi, la redondance des données est très basse en comparaison d'autres systèmes tels qu'EOS, ce qui permet également une diminution de la taille des blocks.

Modalités du Token

Généralités

Créé pour l'économie tokenisée, everiToken est unique de par ses méthodes basées sur les tokens eux-mêmes et sur la gestion de ces derniers. Les tokens sont à distinguer des monnaies virtuelles issues par les banques centrales et des cryptomonnaies telles que BTC et ETH.
Nous définissons un token comme une preuve de droits ou de parts dans un actif, une période de temps, un lieu particulier, ou encore un service fourni par une entité particulière à un instant précis. Les tokens sont divisés en deux catégories : fongibles (FT) et non-fongibles (NFT). Il existe des différences au sein des différents scenarios d'applications et des différentes structures. D'après notre analyse, les tokens non-fongibles pourraient jouer un rôle encore plus important au sein de l'économie tokenisée. Ainsi, nous commenceront notre analyse par les tokens non-fongibles.

Tokens Non-Fongibles

Avant de comprendre les tokens non-fongibles, considérons le nombre élevé de pierres sur une plage. Dans le monde réel, chaque pierre possède un poids, une forme un type de roche différents. Il n'existe aucune pierre tout à fait identique. De plus, les pierres ne peuvent être facilement combinées ensembles, ce qui nous mène à dire que chaque pierre est « indivisible » et « ne peut être combinée » .

Un exemple au sein de la blockchain est celui de CryptoKitties, qui fut un temps un jeu très populaire au sein du monde de la blockchain. Chaque chat possède certains attributs qui lui sont uniques. Un token non-fongible (NFT) est similaire à un individu, une pierre ou un chat sur la blockchain. Il est naturellement différent et unique au sein du monde réel, comme le sont les NFT dans notre système.

D'une façon générale, les NFT sont divisés en différentes catégories selon leurs différents types de valeurs. Nous pouvons regrouper les NFT similaires pour former différents domaines.

En se concentrant sur les tokens, everiToken réussit à atteindre un haut niveau de standardisation. Tous les tokens émis sur mesure selon les désirs des utilisateurs

possèdent la même structure. En particulier, chaque token contient un **nom de domaine** qui correspond à un domaine spécifique (qui est la classe à laquelle le token appartient). L'émetteur définit également un **nom de token** qui doit être unique parmi le domaine. Un nom de token porte généralement une signification particulière. Par exemple, le code barre d'un produit peut être utilisé comme une règle de nomination, qui inclue certaines informations sur le pays d'origine et le fabricant du produit. Le caractère unique de chaque token est déterminé par le nom de domaine ainsi que le nom du token. Par ailleurs, l'information quant à la propriété est incluse, et chaque token possède au moins un **propriétaire**.

Comme mentionné ci-dessus, l'**identifiant** d'un token est uniquement déterminé par le nom de domaine et le nom du token. La structure de base d'un token est expliquée au sein du schéma 1. En plus de l'identifiant du token, la structure montre également le propriétaire du token et d'autres informations nécessaires.

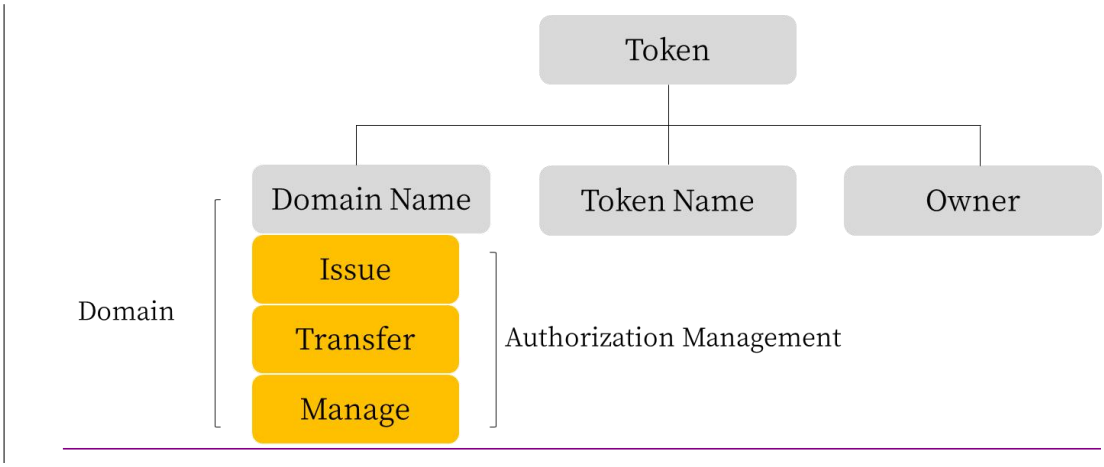


Figure 1. The token structure of everiToken

Les détails du domaine peuvent faire l'objet d'une requête par nom de domaine. Chaque domaine montre également les informations relatives à la gestion des permissions.

Chacun a le droit d'émettre son propre token. Le token lui-même n'a aucune valeur, et son utilité est adossée à la crédibilité effective de son émetteur. Lorsqu'un nouveau token est émis, il peut être transféré aux autres grâce à des transactions.

Pour les NFTs, le transfert de tokens signifie également qu'un changement de propriétaire du token se produit. Chaque token possède un **groupe propriétaire** (il peut y avoir un ou plusieurs propriétaires). Lorsqu'un changement dans le groupe propriétaire est requis, un membre du réseau peut confirmer l'opération en signant une signature digitale, et le groupe propriétaire change après que les nœuds everiToken ont confirmé que la transaction est conforme aux standards de permission et se synchronisent avec les autres nœuds.

Gestion des Permissions

Le système everiToken contient trois types de permissions concernant la gestion des permissions : Émission, Transfert et Gestion.
(1) **Émission** correspond au droit d'émettre des tokens au sein de ce domaine.
(2) **Transfert** correspond au droit de transférer le droit de transférer des tokens au sein de ce domaine.
(3) **Gestion** correspond au droit de modifier le domaine, incluant la gestion des permissions et d'autres paramètres.

Chaque permission spécifique suit une structure en forme d'arbre et est par conséquent appelée un **arbre de permissions.** En tant que racine, chaque permission possède un seuil et est connectée à un ou plusieurs acteurs.

Acteurs

Les acteurs peuvent être catégorisés en trois groupes : comptes, groupes réguliers, et groupes propriétaires. Les comptes sont des utilisateurs individuels, les groupes sont des comptes regroupés et un groupe de propriétaires est une forme particulière de groupe régulier.
Un groupe peut être un club, une entreprise, un département gouvernemental, une fondation, ou même un simple individu. Un groupe détient la clé publique du groupe, et les clés publiques et le poids de chaque individu. Les opérations sont approuvées lorsque la somme des poids de chaque membre autorisé au sein d'un groupe approuvant une opération remplis les critères préalablement établis par le groupe.

En parallèle, le membre qui détient la clé publique du groupe peut autoriser les modifications au sein des membres du groupes ainsi que leur poids. Ce mécanisme est appelé **« autonomie de groupe » .**

Lorsqu'un groupe est créé, le système génère automatiquement un identifiant. Lorsque l'émetteur désigne les propriétés de gestions des permissions pour un domaine, il peut directement faire référence aux identifiants de groupes déjà existant et reproduire leurs systèmes de permission. Du fait de l'autonomie de groupe, chaque groupe peut être réutilisé de façon pratique.

Le propriétaire du token possède un nom spécial au sein du groupe, finissant par « .owner » , ce qui donne naissance à un ensemble de propriétaires d'un token. Cet ensemble est spécial et dynamique car il fait référence aux propriétaires réels de chaque token, et les conditions d'autorisation du groupe stipulent que chaque personne accepte la propriété des autres au sein du groupe (ce qui signifie que le poids de chaque personne est 1, et le seuil du groupe est égal au nombre de membres au sein du groupe).

Gestion

Les permissions sont fixées par les émetteurs des tokens, et chaque permission est gérée par au moins un groupe. Lorsque le token est émis, l'émetteur spécifie les informations et le poids relative de chaque groupe sous chacune des autorisations et fixe également un seuil pour le token. Avant d'exécuter une opération au sein d'un domaine particulier, le système vérifie d'abord si le groupe opérant possède assez de poids, et l'opération sera uniquement approuvée si le poids dépasse le seuil minimal fixé. Ce design par groupes est adapté à de nombreuses situations au sein du monde réel, et l'instauration flexible de poids et de seuils répond à tous types de besoins complexes. Un exemple est fourni à travers le schéma 2.

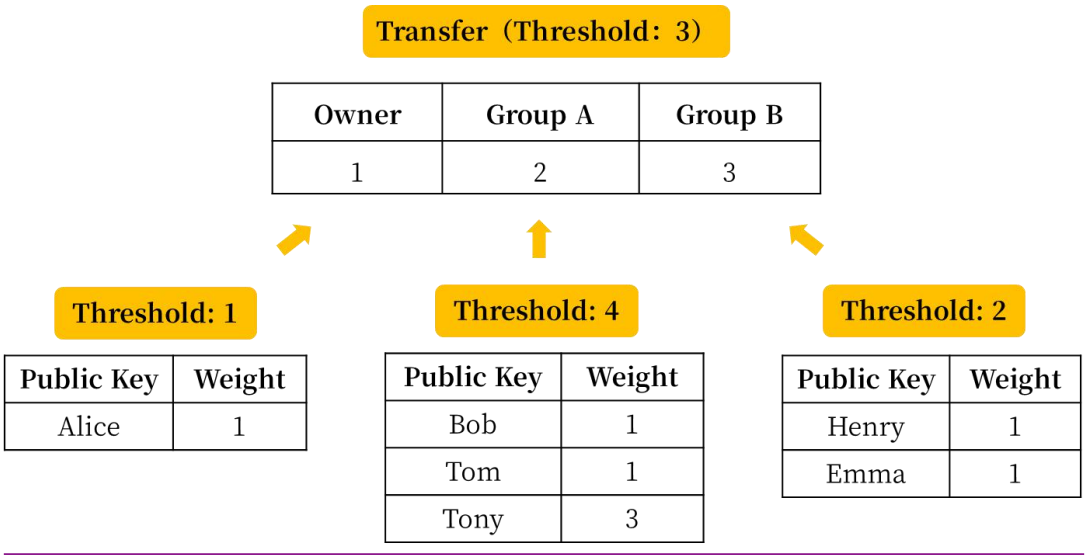


Figure 2. Transfert des Permissions

Le schéma 2 décrit les autorisations de transfert d'un domaine. La valeur du seuil est 3, et il y a 3 groupes impliqués, à savoir le Propriétaire, le Groupe A et le Groupe B. Basé sur l'état actuel des poids de chaque groupe (respectivement 1, 2 et 3), le Propriétaire et le Groupe A doivent fournir la permission en même temps, alors que le groupe B est autorisé à remplir unilatéralement les critères d'autorisation de transfert. Pour chaque groupe, le propriétaire est autorisé par Alice uniquement.; le groupe A peut satisfaire son seuil (4) d'autorisation en autorisant au moins Bob/Tony ou Tom/Tony; le Groupe B doit être autorisé par Henry et Emma pour atteindre le seuil (2).

N'importe quel utilisateur a le droit d'émettre des tokens, mais l'objectif est différent pour chaque domaine en termes de nombre de tokens. Par exemple, le transfert de propriété doit être approuvé par les agences gouvernementales avec une stricte supervision; les cartes de membres et coupons requièrent le sceau de la marque de l'entreprise pour être validées; Un ticket de concert est inutile après le concert, mais une place de parking peut voir son propriétaire changer à travers le temps.

Lorsque les tokens sont émis, l'émetteur du token peut implémenter des règles de gestion des permissions au sein du domaine. Le scenario suivant démontre la praticité de la gestion des permissions.

Le schéma 3 montre à quel point des problèmes complexes peuvent être résolus en

utilisant le mécanisme de gestion des permissions d'everiToken.

Une entreprise a construit un nouveau bâtiment de bureau et espère émettre 1000 tokens représentant les droits de propriété du bâtiment. L'entreprise met en place un FCC (Fonds Commun de Créances) pour émettre et maintenir ces tokens. Dans la vie réelle, l'émission des tokens et le transfert de propriété doivent être examines et approuvés par les bureaux locaux de propriété. Ils doivent être issus en conformité avec les standards locaux et les détails du token (total, émetteur, structure de gestion des autorisation, etc…) peuvent être affichés sur sa plateforme officielle. En plus de cela, le département central des propriétés possède l'autorité la plus haute pour limiter et gérer le bureau local des propriétés et des propriétaires.

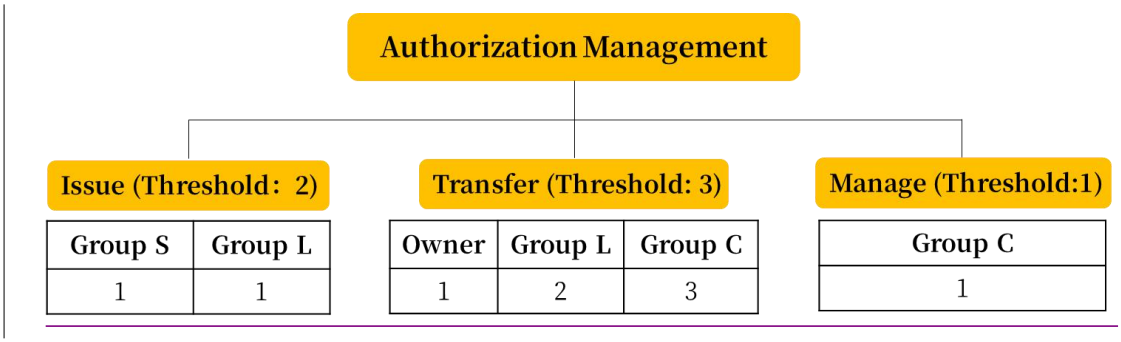


Schéma 3. Structure de Gestion des Permissions

Le Groupe S représente le FCC, l'émetteur, et le propriétaire initial du token au sein du domaine. Le **Groupe L** représente le bureau local de propriété et le **Groupe C** représente le département central de propriété.

Dans la plupart des cas, le transfert d'un token ne requiert que l'autorisation du propriétaire et celle du bureau local de propriété (poids combine de 3, satisfaisant le seuil minimal). Dans ce processus, l'opération de transfert est auditée par le bureau local de propriété. En cas d'accident, comme par exemple le décès d'un propriétaire de token ou bien la perte de la clé privée par celui-ci, le département central de propriété peut transférer la propriété du token à son propriétaire légitime après un recours pénal auprès des institutions concernées.

Si une partie de l'identifiant d'un token est perdue (ce qui peut arriver avec une probabilité non-négligeable) ou si le FCC et les propriétaires de tokens s'entendent

pour ajouter de nouveaux tokens, ils peuvent le faire en s'assurant que l'autorité émettrice réponde à leurs besoins. Par exemple, si le département central de propriété requiert un gel temporaire de la circulation de ce type de token, il peut changer le seuil de permission de transfert à travers les permissions qu'il détient, empêchant tous les tokens de circuler au sein du domaine.

Tokens Fongibles

Émission

Tout le monde peut émettre des tokens fongibles après s'être inscrit avec un symbole unique tel qu'EVT. Les utilisateurs peuvent décider du nombre total de tokens en circulation grâce à ce symbole. Par la suite, ils peuvent également décider du nombre de token émis dans l'immédiat.

Transfert

Toute personne possédant ses propres clés privées peut transférer ses tokens à autrui.

Autres Détails

Chaque compte enregistre le nombre de tokens détenus pour chaque symbole associé. Un registre indépendant en « clé unique » sera mis à disposition pour stocker les informations de base concernant les tokens pour chaque symbole différent. Les utilisateurs peuvent également autoriser les détenteurs d'autres clés privées à transférer un certain nombre de tokens portant un symbole spécifique. Cette fonctionnalité est appelée « **allocation de tokens** » et peut être utilisée lors d'un échange de tokens.

Mode de Transaction Basé sur le Token

Généralités

everiToken utilise un **mode de transaction basé sur le token** concernant tous les tokens du système.

Pour chaque token au sein du registre des tokens, nous créons un espace de données

indépendant pour stocker l'historique complet de propriété de chaque token. Ainsi, il est très facile de procéder à la compartimentation et à la parallélisation car l'espace occupé par les données d'un token en particulier n'a aucune corrélation avec celui occupé par d'autres tokens. En conséquence, les opérations menées sur divers tokens peuvent être aisément prises en compte en parallèle et sans conflit. Cela permet d'atteindre un haut niveau de performance et d'améliorer constamment le nombre de transaction par seconde en appliquant la compartimentation (sharding) ou la parallélisation (ajout de processeurs).

Le mode de transaction basé sur le token fut inventé par un groupe de membres clés de l'équipe d'everiToken et a fait ses preuves de façon remarquable au sein des tokens non-fongibles d'everiToken.

Une blockchain adoptant le modèle de transaction basé sur le token telle qu'everiToken peut diviser une base de données en deux parties, l'une étant Token DB et l'autre étant Block DB. La première est celle au sein de laquelle le modèle basé sur le token opère, en stockant et gérant les espaces de données de l'intégralité des tokens non-fongibles. Block DB, le second, stocke les blocks originaux.

Token DB et Block DB sont toutes deux des bases de données en plusieurs versions capables de procéder à un « rollback » rapide lorsqu'un block doit être inversé. Par exemple, everiToken utilise Rocks DB comme système de base de données sous-jacent de Token DB.

Token DB et Block DB sont toutes deux des bases de données suivant le modèle « ajout-seul » (append-only). Ainsi, lorsque quelqu'un actualise un registre, la nouvelle valeur issue de la version mise à jour sera ajoutée à la base de données. Cependant, le registre contenant l'ancienne version ne sera pas retiré.

Token DB

Token DB est une base de données indexée pour rapidement chercher et changer le statut le plus récent de la blockchain tel que la propriété des tokens et le solde des comptes en tokens au sein de la chaine.

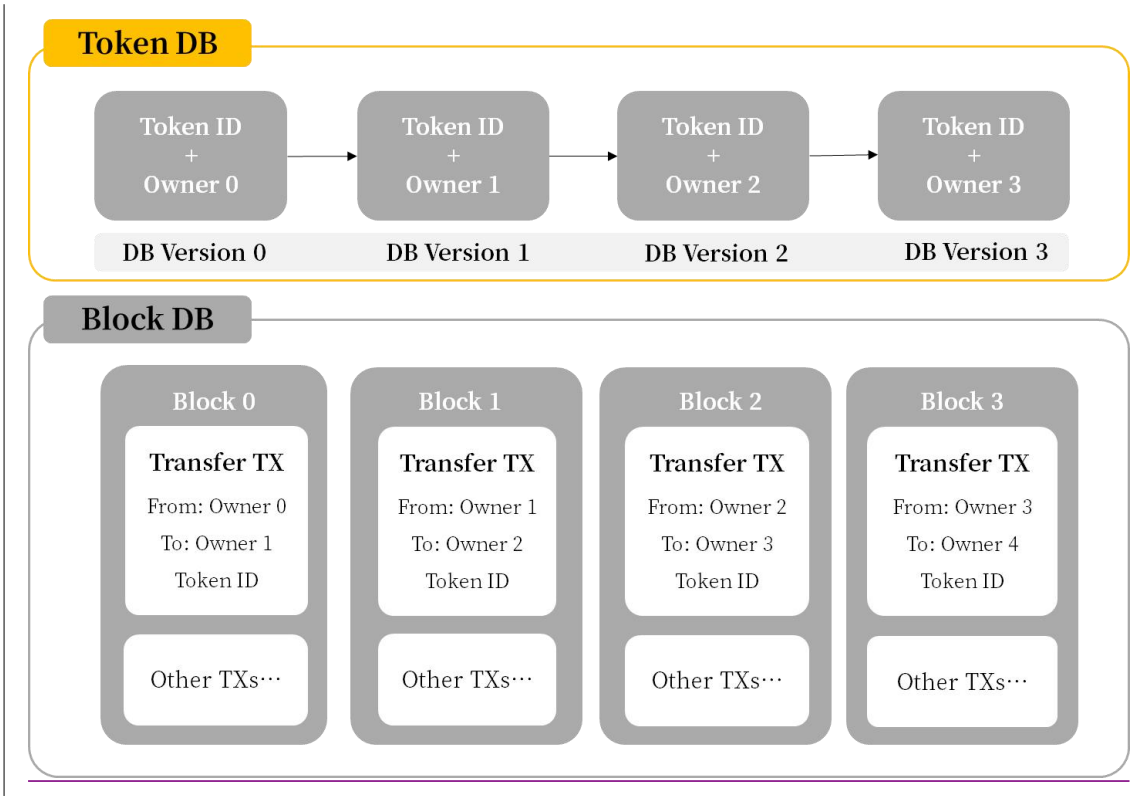
Token DB peut être considérée comme une base de données « clé-unique » . La clé indique l'identifiant des tokens et la valeur représente les droits de propriétés actuels des tokens. Puisque la base de données est en mode « ajout-seul » , chaque clé prendra un nombre de valeurs élevé, mais seule la dernière valeur représente le statut actuel de propriété du token, alors que les autres valeurs sont uniquement là pour fournir une référence historique et éventuellement un « rollback » . Pour chaque token, un espace de stockage de données indépendant inclue tout l'historique de propriété, comme une chaine séparée.

La valeur principale de la chaine réside dans la propriété initiale. Par exemple, lorsque quelqu'un exécute une transaction, les nouvelles données de propriété seront ajoutées dans la base de données. Les anciennes versions pourraient être utilisées pour effectuer un « rollback » si la valeur du block a besoin d'être renversée et celle-ci sera alors envoyée à la corbeille.
Puisque chaque token possède un espace de stockage de données indépendant, la compartimentation est très aisée à mettre en place. Par exemple, si l'on a 2 ordinateurs pour un nœud, on peut laisser chaque ordinateur gérer la moitié des tokens. Si l'on a 100 tokens, le premier ordinateur gèrera les tokens 1 à 50, le second gèrera les tokens 51 à 100. Parce que changer de propriétaire d'un token n'aura aucun impact sur les autres tokens, les deux ordinateurs peuvent gérer le système de façon parallèle.

Block DB

Block DB est responsable du stockage des blocks originaux de la chaine, et ce de façon irréversible. Chaque block stocke toutes les informations, y compris les noms, paramètres des actions exécutées, signatures du block et plus encore.

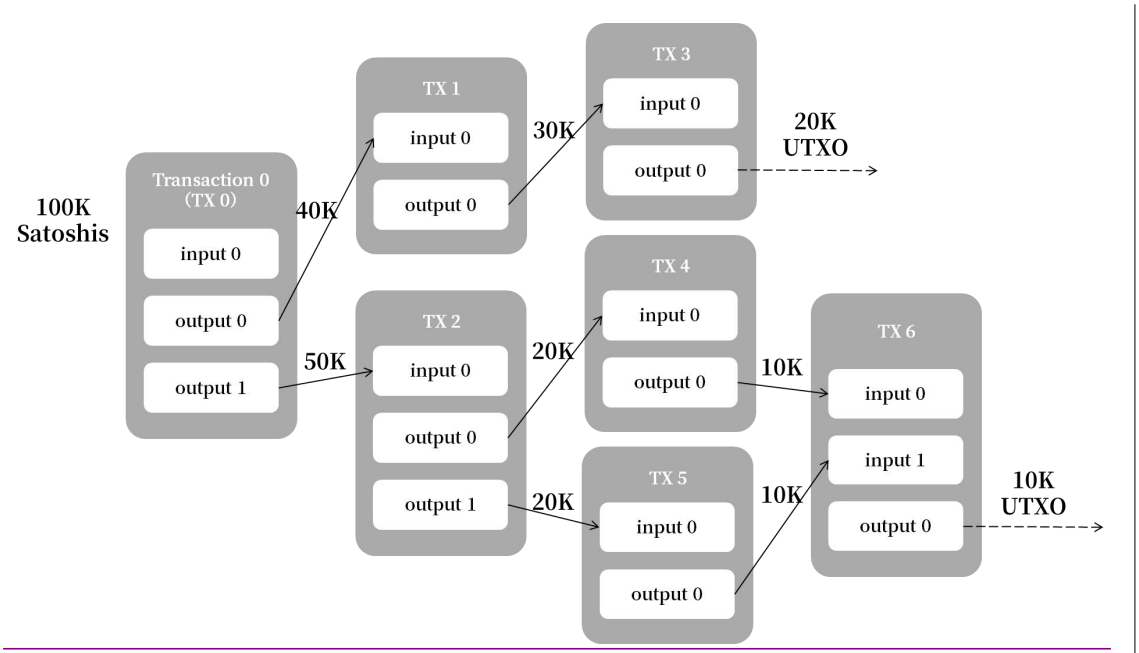
Le graphe suivant montre comment les deux types de bases de données collaborent dans le cadre des tokens non-fongibles.



Comparaison des Modèles de Transaction

a) UTXO

Dans le modèle UTXO, chaque propriétaire de token transfère un token qu'il possède à une autre personne en signant digitalement le hash de la transaction précédente ainsi que la clé publique (adresse) du prochain propriétaire, ajoutant ceux-ci à la fin du token. Ce mécanisme est essentiellement une retranscription continue des inputs et outputs où le propriétaire des tokens ne possède pas directement ceux-ci, mais plutôt possède l'output lié à un nombre spécifique de tokens qui peut être signé en tant qu'input pour un nouveau propriétaire qui contrôlera à son tour le nouvel output.



(Source: bitcoin.org)

Comme vous pouvez le voir, UTXO est un excellent moyen d'éviter les « doubles-dépenses » car il est évident qu'un input ne peut être utilisé qu'une fois, mais ce système comporte aussi des inconvénients:

- BTC n'est pas un token non-fongible, il s'agit d'un token fongible. Il est inutile de garder un identifiant unique pour chaque UTXO (everiToken supporte à la fois les tokens non-fongibles et fongibles).

- Les UTXO périment et constituent un gâchis de ressources de calcul et de stockage pour le nombre élevé d'UTXO.

b) A base de compte

Le modèle de transaction à base de compte est similaire à celui des banques. On crée un compte à la banque et économise de l'argent sur ce compte, ce qui a un impact sur le solde. Cela est complètement différent de la façon dont UTXO fonctionne. Cela est plus efficace que UTXO car il suffit de mettre à jour le solde dans la base de données, sans créer de nouveau UTXO. Ainsi, le modèle UTXO n'est pas adapté aux tokens non-fongibles. De plus, le modèle à base de compte n'est pas adapté à la compartimentation car lorsque l'on transfère quelque chose à quelqu'un d'autre, il

nécessite d'accomplir 2 étapes: la première consiste à modifier le compte de l'ancien détenteur, la seconde à modifier le compte du nouveau détenteur. Pour des raisons de sécurité, les 2 étapes doivent être complétées en une seule opération, mais dans le cadre d'un environnement compartimenté, cela est très difficile et le niveau de performance est faible. En revanche, le modèle à base de token ne nécessite qu'une seule étape dans ce cas précis, qui consiste à ajouter les nouvelles données de propriété du token.

Sécurité

En se concentrant sur les fonctions liées aux tokens, everiToken élimine les abstractions inutiles, ce qui a pour effet non seulement d'augmenter l'efficacité du système mais également de garantir un niveau de sécurité remarquable. Bien que le type de tokens sur everiToken puisse être très élevé et théoriquement illimité, la structure unifiée de tokens permet au système ou à n'importe quel tiers-parti de les auditer en suivant les mêmes principes. Cela peut être vu comme un système qui ne reconnait qu'une unique forme de smart-contract, ce qui évite de compliquer le processus d'audit et protège des failles de sécurité.

Éléments Clés du Code everiToken

Au printemps 2019, everiToken a introduit quatre organisations charges de réviser l'intégralité du code de la blockchain, incluant Hacken Proof, Chaitin ainsi que d'autres. Des analyses statiques et dynamiques ont également été réalisées.

Puisqu'everiToken utilise le terme de *safe contract,* une fois qu'il a été prouvé que notre code est sûr, alors tous les contrats basés sur everiToken sont également reconnus comme sûrs.

Script (everiSigner)

everiSigner est un plugin de signature hors-ligne pour explorateurs. Le processus de signature complet est effectué au sein de ce plugin afin que les clés privées ne soient jamais exposées. Le site interagit avec everiSigner en créant un nouveau canal pour assurer la sécurité; le site fait passer le contenu à signer à travers le canal et everiSigner envoie les données signées en retour.

Clé privée perdue

En vertu de la gestion des permissions, les tiers partis peuvent fournir de nombreux services. Par exemple, l'Entreprise C est spécialisée dans les services de protection des mots de passe et Alice craint d'avoir oublié ou perdu la clé privée de son propre token. Alice peut gérer: l'autorisation de transfert du domaine au propriétaire (1), Groupe C (1) et fixer le seuil à 1. Dans ce cas, si Alice a oublié sa clé privée et ne peut recevoir la permission par elle-même, elle peut tout de même recevoir la permission par le Groupe C si elle prouve qu'elle est bien Alice (en montrant sa carte d'identité o uses empreintes digitales). Ainsi, Alice peut restaurer ses tokens en les transférant vers un nouveau compte après vérification.

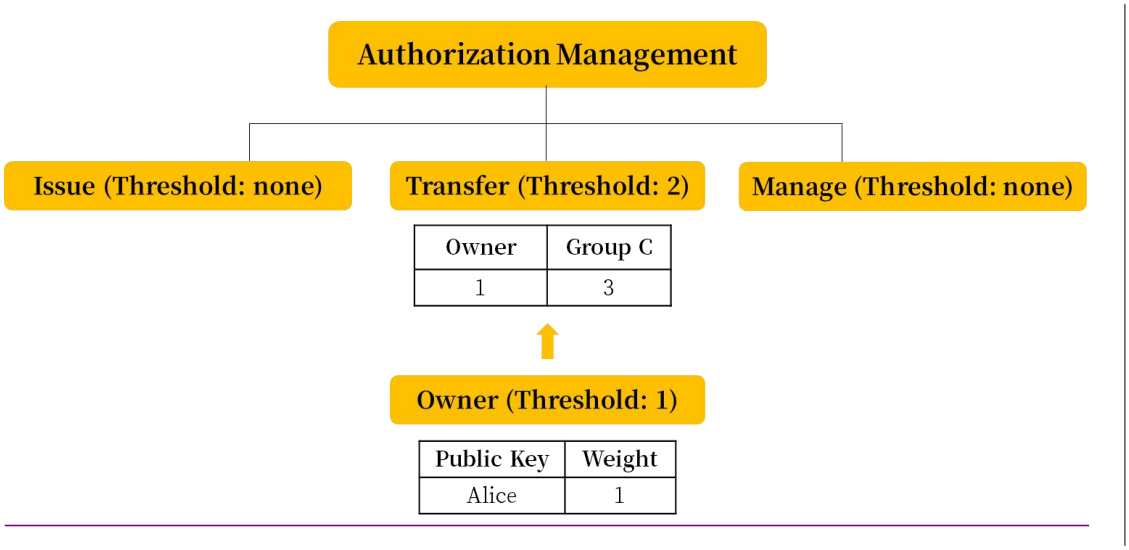


Figure 4. L'Entreprise C fournit un service de recouvrement des clés

Bien sûr, le Groupe C pourrait voler le token d'Alice, mais toutes les opérations seraient enregistrées sur la blockchain, ce qui porterait atteinte à la crédibilité du Groupe C.

Algorithme de Consensus

everiToken utilise l'algorithme de consensus BFT-DPOS. DPOS a fait ses preuves comme algorithme capable d'atteindre les niveaux de performances requis pour les applications sur la blockchain. Avec cet algorithme, ceux qui détiennent des tokens EVT peuvent sélectionner les producteurs de blocks à travers un système de vote en continu. Chacun peut choisir de participer au processus de production de blocks et

recevra une opportunité d'en produire, du moment qu'il ou elle arrive à convaincre les autres détenteurs de tokens de voter en sa faveur.

everiToken permet aux blocks d'être produits toutes les 0,5 secondes, et exactement un producteur est autorisé à produire un block à un instant donné dans le temps. Si le block n'est pas produit au moment prévu, alors le block de ce créneau passe son tour. Lorsqu'un ou plusieurs blocks passent leur tour, un trou de 0,5 seconde apparait dans la blockchain.
Le nombre de producteurs de blocks pour la blockchain everiToken est dynamique. Pour la première année, 15 producteurs sont fixés. Par la suite, le nombre sera décidé par un comité de gouvernance sur la blockchain. Pour plus de praticité, nous utiliserons le chiffre 15 pour ce whitepaper.

Au sein d'everiToken, les blocks sont produits en 180 manches (12 blocks pour chacun des 15 producteurs). Au début de chaque manche, 15 producteurs uniques sont choisis d'après les préférences de votes émises par les détenteurs de EVT. Les producteurs sélectionnés sont programmés dans un ordre approuvé par 11 producteurs ou plus.

Si un producteur rate un block et n'a pas produit un seul block au cours des dernières 24 heures, il est alors retiré de la liste des producteurs jusqu'à ce qu'il notifie la blockchain de son intention de recommencer à produire des blocks. Cela permet de garantir le fait que le réseau opère de façon paisible, en minimisant le nombre de blocks manqués par l'absence de programmation de certains producteurs qui apparaissent comme peu fiables.

L'algorithme des généraux byzantins (BFT) est utilisé pour fournir une couche supplémentaire de sécurité aux utilisateurs en demandant à ce que toutes les confirmations soient signées par tous les producteurs. Aucun producteur ne peut signer 2 blocks avec le même marqueur de temps ou avec le même numéro de block. Lorsque 11 producteurs ont signé un block, il est considéré irréversible. N'importe quel producteur mal intentionné devrait générer une preuve cryptographique de sa trahison en signant deux blocks avec le même marqueur de temps ou le même numéro. Selon ce modèle, un consensus irréversible devrait être atteint en 1 seconde.

Système de Bonus

Les bonus ont été ajouté lors de la mise en ligne d'everiToken 3.0 en février 2019. Il s'agit d'un élément puissant, flexible et pratique à combiner avec d'autres fonctionnalités existantes. Les bonus sont principalement destinés à distribuer des profits aux participants et actionnaires d'après un ensemble de règles. Il y a deux types de bonus supportés pour le moment, correspondant à deux différents moyens de collecter les profits: bonus passifs et actifs.

Dans le cas des bonus passifs, le profit est collecté lors de chaque transaction au sein d'un token fongible. Ainsi, si les gérants d'un token fongible décident de lui attacher un bonus passif, alors chaque transaction (non seulement celles en EVT) fera l'objet d'un prélèvement en tant que « carburant » , mais une taxe additionnelle s'appliquera pour le token fongible.

Il existe plusieurs manières de contrôler les frais réels d'une transaction. La principale est celle du taux de transaction. Le montant des frais de transactions est égal au taux multiplié par la valeur de la transaction. Il y a un seuil minimum et un maximum pour contrôler les bornes inférieurs et supérieurs des frais finaux. Cela permet d'éviter d'avoir à prélever des frais exagérément élevés pour les transactions importantes.

Le manager d'un token fongible peut décider comment les frais seront prélevés, comme par exemple en précisant quelle partie est responsable des frais et de la méthode employée pour le prélèvement. La première méthode est similaire à une carte de crédit. Le payeur paie un montant *n* mais le payé reçoit moins de *n* car les frais sont soustraits du montant initial. La seconde méthode ressemble plus à celle d'une banque traditionnelle. Si l'on veut transférer un montant *n* à quelqu'un d'autre, on doit payer un frais supplémentaire pour cette transaction en sus du montant original.

En ce qui concerne le bonus actif, celui-ci est enclenché de façon manuelle, un peu comme les dividendes d'une entreprise. Le montant est décidé par le gestionnaire du token fongible.

Que le bonus soit actif ou passif, il doit comporter un ensemble de règles de

distribution. Trois types de règles sont actuellement valides: fixe, par pourcentage et pourcentage restant. « Fixe » est le montant fixe garanti pour le receveur, alors que la règle du pourcentage est calculée par la valeur en pourcents multipliée par le montant total du bonus. Le « pourcentage restant » est différent des autres règles et est constitué du montant restant multiplié par la valeur en pourcent.

Pour chaque règle, il est également nécessaire d'assigner un receveur. Celui-ci n'est pas limité à une seule adresse, mais peut également être le détenteur d'un token fongible, et chaque détenteur peut recevoir le montant correspondant à son solde en fonction de la quantité totale de tokens fongibles en circulation. De plus, les participants à un système de tokens fongibles ne sont pas limités à ce token fongible utilisé à des fins de profit, mais chaque token fongible enregistré sur everiToken est acceptable. Ainsi, il est possible d'émettre un « token bonus » seulement pour la distribution de profits, et il bénéficiera de la transparence, l'intégrité et la liquidité garanties par everiToken.

Lors de l'implémentation, il est nécessaire de faire l'inventaire de toutes les adresses des participants ainsi que du solde de leurs comptes lorsqu'ils possèdent plus d'une adresse. Cela est susceptible de demander une plus grande capacité de stockage car chaque adresse de participant requiert 34 bytes. Nous avons grandement optimisé cette situation, et dans la plupart des cas, chaque adresse ne requiert que 4 bytes pour être stockée. Avec 1 million de participants ou plus, le « coût » sera seulement de 4Mb au lieu de 34Mb. Grâce à l'optimisation poussée de notre base de données de tokens, le système peut lire et mettre à jour les soldes des participants en mobilisant une faible quantité de ressources.

Fonctions de Verrouillage

Des fonctions de verrouillage sont incluses dans le système d'everiToken. Les tokens peuvent être verrouillés pour une certaine période, qu'ils soient fongibles ou non-fongibles. Cela dépend des conditions fixées lors de la proposition de verrouillage. Que les conditions soient satisfaites ou non pendant la période de verrouillage, les tokens déverrouillés seront transférés vers différentes adresses enregistrées à la fin de la période initialement fixée. Actuellement, les conditions de verrouillages peuvent seulement être ajustées à l'aide des clés publiques, ce qui

signifie que Durant la période de verrouillage, seules les clés approuvées peuvent autoriser l'accès.

Autres Détails Techniques

Blockchain Principale

Nous ne voulons pas réinventer la roue. Ainsi, nous avons intégré les meilleurs aspects des blockchains publiques déjà existantes et nous avons corrigé certains de leurs défauts. Nous avons adopté le Graphene (DPOS+PBFT) comme algorithme de consensus. Le code de l'algorithme de consensus est issu de la version 3.0 du DPOS d'EOS, amélioré par nos soins. Tout en admettant que la structure du code d'EOS est excellente et en reprenant certains de ses éléments, nous avons mis au point une blockchain publique complètement nouvelle.

Au cours du développement, nous nous sommes avant tout consacrés à la mise au point des Safe Contracts (en lieu et place des Smart Contracts), un nouveau modèle de base de données (basé sur RocksDB pour de meilleures performances) ainsi que le protocole de paiement en tokens everiPay.

Cette pratique comporte de nombreux avantages:

- Le Graphène est une technologie qui a fait ses preuves. Le « DPOS » ainsi que les autres mécanismes de base ont été entièrement testés par des projets tels que Bitshare et EOS.
- Réutiliser l'algorithme de consensus peut en partie réduire la charge de travail, en nous permettant de nous focaliser davantage sur l'optimisation des opérations liées à everiToken.

Opérations d'Autorisation

Les opérations d'autorisation d'everiToken incluent principalement les multisignatures, le calcul des pondérations, la définition des seuils, etc… Puisque le transfert de chaque token est indépendant de celui des autres, les opérations de transfert de différents tokens peuvent être exécutées en parallèle. De plus, puisque le statut des autorisations de chaque groupe est indépendant de celui des autres, les

opérations d'émission et de gestion peuvent également être exécutées en parallèle entre différents groupes.

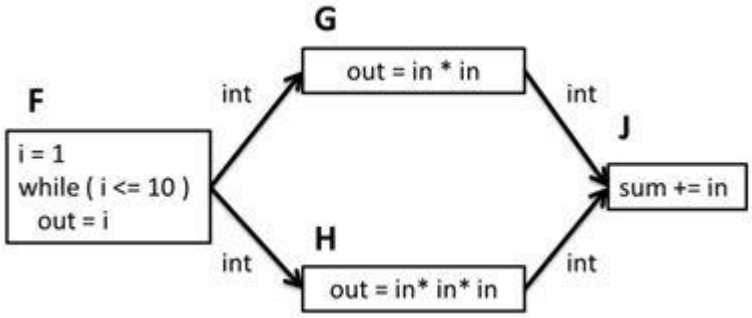
Chaque transaction est constituée d'un paquet de données ainsi que d'une liste de signatures. Dans le cas de la vérification des permissions, chaque signature doit être vérifiée. Il n'y a aucune corrélation entre les différentes signatures, donc les opérations d'autorisation peuvent être exécutées en parallèle.

Moteur d'Exécution

Au sein du système everiToken, puisque chaque opération liée au token est complètement indépendante des autres, les processus concomitants ne requièrent pas de compartimentation et de charges additionnelles créées par ceux-ci. De plus, puisque les opérations liées aux tokens sont limitées, le code est également intégré à la plateforme. Tant que chaque type d'opération est testé de façon répétitive, le système est complètement stable.

L'exécution d'une transaction peut être découpée en plusieurs phases telles que le recouvrement des signatures, la vérification des permissions, le calcul, l'écriture dans la base de données, etc… Chacune des phases est exécutée dans un ordre séquentiel, mais certaines d'entre elles sont indépendantes des autres à travers plusieurs transactions différentes. L'une de ces phases est appelée le *recouvrement des signatures*. Il n'y a pas de dépendance logique vis à vis des signatures de chaque transaction, et chaque signature de transaction est également indépendante des autres. Le recouvrement des signatures est donc possible en simultané pour des transactions différentes. Une autre de ces phases est intitulée *vérification des permissions*. Elle peut sembler similaire à celle du recouvrement des signatures, mais imaginez vérifier les permissions liées à deux transactions de transfert de tokens: même si tous les tokens n'ont pas un rôle dans la fonction des autres, s'il y a deux transactions ordonnant le transfert du même token, le système rencontrera alors une situation inattendue s'il tente de vérifier les permissions en parallèle. Parce que les propriétaires du token participant à la vérification, cela ferait l'objet d'un changement lors de la première transaction. Ainsi, il n'y a aucun moyen d'exécuter certaines

phases en parallèle, mais ces situations peuvent être planifiées de façon méticuleuse. Ce que nous avons implémenté peut-être observable ci-dessous à travers le *graphe de dépendance*. Notre système met en parallèle le flux de données en utilisant ce graphe. Les processus de calculs sont représentés par des nœuds et les canaux de communication entre ces calculs sont représentés par des bords.



Ci-dessus apparait un exemple de calcul de la somme des séquences des carrés et des cubes de 1 à 10. Dans notre modèle, chaque nœud représente une phase d'une transaction, et il existe un planificateur qui recevra les transactions et les décomposera afin de construire le graphe entier.

Transactions Suspendues

Une transaction suspendue est une transaction qui a été effectuée après de multiples retards. Les transactions ordinaires non-suspendues sont effectuées d'un seul trait, et toutes les conditions doivent être remplies lorsque la transaction est soumise. Pourtant, et en réalité, beaucoup de transactions sont effectuées selon un processus particulier. Les participants impliqués dans une transaction peuvent être dans l'incapacité de compléter leurs signatures au même moment. La suspension de la transaction permet à ces signatures d'être fournies petit à petit jusqu'à ce que la transaction soit un succès.

everiPay / everiPass / EvtLink

everiPay / everiPass

everiPay/everiPass est un moyen de paiement conçu pour les micropaiements en face à face utilisant la blockchain everiToken

EvtLink fait référence aux standards de génération de QR codes et à la définition du protocole de communication.

Voici certains des aspects majeurs concernant everiPay/everiPass/EvtLink:

- **Traitement instantané:** Une transaction constitue un règlement.
- **Décentralisation**: paiement Peer to Peer, pas de plateforme centralisée, personne ne peut modifier les données inscrites sur la blockchain et tout le monde peut participer à la fixation du prix
- **Sécurité:** Les données et le contenu de la blockchain sont immuables afin de maximiser la fiabilité et la protection de la propriété des utilisateurs
- **Facilité d'utilisation:** Même sans être connecté à Internet
- **Compatibilité**: everiPay/everiPass supporte tous les tokens émis sur everiToken. Par ailleurs, les opérations fonctionnelles quotidiennes telles qu'utiliser une clé pour ouvrir une porte sont supportées. L'atout majeur réside dans la possibilité d'utiliser ce système partout ou presque, juste avec son téléphone.
- **Extrême rapidité:** everiToken a rapidement atteint un niveau très élevé de Transactions par Seconde (TPS) et les transactions peuvent être effectuées en 1 à 3 secondes, selon la qualité de l'équipement ou du réseau.
- **Standardisation:** Doté d'une technologie unique parmi les portefeuilles électroniques, EvtLink est un standard d'échanges entre portefeuilles, blockchains et applications directement conçu pour l'écosystème entier. On peut utiliser n'importe quelle application pour le décrypter.

En vertu des caractéristiques exposées ci-dessus, everiPay/everiPass garantit un service sûr, pratique ainsi qu'une bonne expérience d'utilisation dans le cadre des paiements en face à face.

Pour accéder à everiPay/everiPass, le récepteur du paiement doit utiliser une application qui décrypte EvtLink et pousse les transactions vers la blockchain everiToken. Cela est très simple, car nous fournissons des API faciles d'utilisation ainsi que des templates de code pour les développeurs. Cela est aussi facile que d'utiliser Lydia pour recevoir des paiements.

QR Code du récepteur

Le QR code du récepteur ne supporte pas toutes les fonctionnalités offertes par everiPay. Par exemple, les émetteurs de paiements doivent se connecter à internet pour effectuer une transaction, et le récepteur ainsi que l'émetteur doivent tous les deux entrer manuellement le montant de la transaction. De plus, ils ne reçoivent pas de notification automatique lorsque le paiement est effectué.

Cependant, les récepteurs de paiements n'ont pas à utiliser d'application supportant cette méthode de paiement. Ils doivent simplement utiliser un portefeuille supporté par everiToken sur leur téléphone pour vérifier qu'ils ont bien reçu l'argent de l'émetteur. Cela est adapté à tous types et toutes tailles de vendeurs, ainsi qu'aux échanges simples entre individus.

Utiliser everiPay plutôt qu'un QR code de récepteur est recommandé car il s'agit de la solution la plus transparente, sûre et facile d'utilisation.

Comment EvtLink fonctionne-t-il ?

EvtLink est le standard en format binaire qui représente everiPay/everiPass. La blockchain publique everiToken utilise des actions réalisées à travers everiPay et everiPass pour exécuter des transactions sur evtLink

Ci-dessous se trouve le processus détaillé des paiements réalisés par everiPay/everiPass d'un point de vue technique:

1. Le payeur sélectionne un type de token à utiliser, puis le portefeuille du payeur montre une série de QR codes dynamiques comprenant un identifiant unique LinkId en 128-bit, une signature (celle du payeur) ainsi que le symbole du token utilise pour le paiement. Notons que le LinkId ne doit pas être changé au cours du déroulement, sauf si la transaction est déjà exécutée. Cela permet d'éviter qu'un paiement ait lieu en double parce que la blockchain n'autorise

pas deux actions avec le même LinkId sur EvtLink.

2. L'application du portefeuille du payeur émet donc en continu des requêtes concernant la transaction liée au LinkId en invoquant l'API nommée 'get_trx_id_for_link_id' jusqu'à ce que celle-ci renvoie un identifiant de transaction valide. Le portefeuille changera alors le LinkId lorsqu'il affichera un QR code la fois suivante. De plus, le portefeuille affichera le résultat de la transaction en faisant une requête par identifiant de transaction. Les portefeuilles de payeurs n'ont pas besoin d'envoyer les transactions directement.

3. En parallèle, le récepteur du paiement scanne le QR code à l'aide de son téléphone/scanner/appareil intelligent. Après le scan et le décryptage de l'EvtLink, celui-ci est envoyé vers la blockchain. Par la suite, tous les nœuds de la chaîne se synchroniseront, et le « get_trx_id_for_link_id » retournera l'identifiant de la transaction.

Encodage Base42

Base42 est un algorithme d'encodage pour les conversions « binaire vers texte » . Il est similaire à l'encodage hexadécimal, mais utilise 42 comme base ainsi qu'une unique séquence alphabétique. Les caractères de l'alphabet sont les mêmes que les caractères de l'encodage du mode alphanumérique d'un QR code. Il est donc facile de stocker des textes encodés en base42 au sein d'un QR code. Cela permet l'utilisation d'un QR code plus facile à scanner.

Part III. Modèle Économique

Fuel/Carburant (EVT)

Afin d'éviter des attaques du type DDoS contre le système, de prouver son « intérêt » (staking) dans le cadre du vote du système DPOS et afin de fournir une récompense raisonnable aux producteurs de blocs, nous émettrons l'EVT et l'utiliserons comme carburant. Toute opération sur la blockchain demandera des frais de services prélevés sous forme d'EVT, pour un montant variable qui sera une récompense pour le producteur du bloc. Le nombre d'EVT prélevés comme frais de services sera complètement « flottant » et variable, et les frais collectés seront prioritairement destinés à éviter les attaques malveillantes, et n'auront pas d'impact sur l'usage régulier pour la plupart des utilisateurs.

La méthode employée pour la création et le transfert d'EVT est identique à celle en vigueur au sein des blockchains les plus courantes. L'EVT est utilisé pour récompenser les producteurs de blocs qui mettent leurs ressources à contribution, et pour éviter tout comportement malveillant.

150 millions d'EVT (15% de la circulation totale) seront distribués à l'équipe de base du projet (14% pour les 5 cofondateurs d'everiToken et 1% pour les contributeurs clés).
400 millions d'EVT (40% de la circulation totale) seront distribués aux membres de la communauté qui construisent des applications sur l'infrastructure d'everiToken et contribuent massivement à l'écosystème à travers le savoir-faire technologique, les ressources, la promotion, le financement, etc…
450 millions EVT (45% de la circulation totale) seront distribués aux investisseurs à travers plusieurs tours de financement.

Tous les services délivrés sur everiToken impliqueront des frais sous forme de fuel:

$$ServiceFuelCost = FuelUsed \times R$$

Dans cette formule, $FuelUsed$ est le prix correspondant à une action spécifique.

L'unité de prix est l'EVT. *R* représente le **taux d'ajustement**. Les producteurs de blocs peuvent indépendamment décider à tout moment de procéder à une **augmentation du taux** lorsque la chaine est trop encombrée ou sous attaque. Ils peuvent également procéder à une **diminution du taux** si le prix de l'EVT est trop élevé. Le taux réel *R* est calculé comme la médiane des taux pratiqués par les 15 producteurs de blocs. Les utilisateurs de la blockchain peuvent supposer que R est égal à 1 lorsqu'ils font appel une API pour la première fois. Si R n'est pas changé par le producteur de bloc, l'invocation de l'API sera bel et bien effectuée. Si R a été change, l'invocation échouera et l'utilisateur devra essayer une nouvelle fois d'effectuer la tâche voulue.

Par exemple, si le prix de la commande *créerUnCompte* est de 2 EVT.
Habituellement, un utilisateur peut invoquer la commande *créerUnCompte* avec 2 EVT.
Si les producteurs de blocs procèdent à une hausse du taux et le fixent à R=1,1 , alors le prix passera à 2,2 EVT.

Nous utiliserons la médiane des différents taux de R parmi les producteurs de blocs. Si 3; 5; 2; 2; 1; 1 producteurs suggèrent respectivement un taux R de 1,15; 1,2; 1,1; 1,3; 1,4; 1,45, alors la valeur finale de R sera de 1,2.

EVT « épinglé »

Un EVT épinglé est similaire aux autres EVT mais ne peut être transféré. Il peut être utilisé comme fuel uniquement. Convertir un EVT en EVT épinglé est autorisé. Le taux de change de l'EVT par rapport à celui de l'EVT épinglé est toujours égal à 1. **Puisque l'EVT épinglé n'est pas une monnaie**, il n'est pas risqué de procéder à un airdrop d'EVT épinglés pour les donner à quelqu'un d'autre.

D'une façon générale, il ne faut pas convertir les EVT en EVT épinglés, car les EVT permettent de payer les frais de service (fuel). Si quelqu'un décide de convertir un EVT en EVT épinglé, l'EVT épinglé sera automatiquement lié au récepteur, d'où le terme d'**EVT épinglé**.

L'EVT épinglé appartient à un compte et ne peut être transféré à d'autres. Il est donc

pratique et sans risque de procéder à un airdrop d'EVT épinglés vers d'autres utilisateurs. Les entreprises et autres organisations peuvent convertir les EVT en EVT épinglés puis les affecter à certains comptes spécifiques. Les EVTs épinglés ne peuvent être transférés entre différentes adresses.

Un **payeur** est représenté par un compte qui paie pour effectuer une transaction donnée. everiToken permet aux utilisateurs de spécifier les payeurs dans le cadre d'une transaction. Cela est utile pour créer des comptes. Pour des raisons de sécurité, les payeurs doivent apposer des signatures supplémentaires pour la transaction.

Chaque domaine possède un nombre spécifique d'EVT épinglés.
La blockchain préfère consommer en priorité les EVT épinglés issus du domaine (si le solde n'est pas égal à 0) lorsqu'il s'agit de transférer ou de détruire des tokens au sein d'un domaine.
Les utilisateurs peuvent prépayer les EVT épinglés d'un domaine à l'aide de leurs EVT.

Émission Supplémentaire d'EVT

La quantité initiale d'EVT est d'1 milliard. La chaine peut émettre un nombre supplémentaire d'EVT selon une base annuelle. Le taux réel d'émission sera décidé par le comité de gouvernance de la blockchain everiToken. Nous n'émettrons aucun EVT supplémentaire avant le 1er Janvier 2020.

Producteurs de Blocs (PdB)

- Nombre de PdB: Fluctuant

Nous offrons peu de libertés aux PdB et il est donc difficile pour eux d'agir de façon malveillante. Le seul mal qu'ils peuvent commettre consisterait en une attaque de « Déni de Service » (DoS). Afin d'équilibrer les revenus des PdBs et d'assurer un certain niveau de décentralisation, nous utilisons un nombre fluctuant de PdB qui est supérieur ou égal à 15. En 2019, nous en aurons 15. Pour les années à venir, ce

nombre sera décidé par un vote du comité de gouvernance de la blockchain.

Part IV. Écosystème

Outils

everiWallet

Comme son nom l'indique, everiWallet est un portefeuille pour everiToken, qui supporte à la fois les navigateurs web et les smartphones. Visitez cette page pour plus d'informations: https://www.everiwallet.com/

EVTJS

EVTJS est la librairie de liaison de l'API d'everiToken pour JavaScript et elle supporte à la fois NodeJS ainsi que les différents navigateurs. Elle est également supportée par everiSigner, et il est donc possible d'utiliser cette librairie pour construire des applications web sur everiToken. Plus d'informations à cette adresse: https://www.github.com/everitoken/evtjs

evtScan

evtScan est l'explorateur de la blockchain everiToken. Tout le monde peut chercher une information spécifique sur les blocs créés par les nœuds du réseau everiToken. Cela inclut les détails des transactions, comptes, groupes et domaines présents sur la blockchain, ainsi que des statistiques et des analyses. Pour les développeurs, evtScan est un outil efficace afin de confirmer si l'information est convenablement reliée à la chaine. Pour les utilisateurs, cet outil offre une méthode pour vérifier l'authenticité des transactions. Plus d'informations à cette adresse: https://evtscan.io/

Comité de Gouvernance Décentralisée sur la Blockchain

La blockchain publique everiToken possèdera un comité de gouvernance décentralisée sur la blockchain afin de prendre des décisions importantes, comme choisir le nombre de PdB ou ordonner l'émission d'EVT supplémentaires. Le comité devrait voir le jour avant le 1er janvier 2020.

Entreprise Fiduciaire

everiToken n'est impliqué dans l'identifiant des tokens particuliers. La valeur d'un token est garantie par des **entreprises fiduciaires**. Ces entreprises peuvent apposer une signature supplémentaire lors de l'émission des tokens afin que toute personne reconnaisse sa confiance en ce token si elle fait confiance à l'entreprise apposant la signature. Ce procédé est similaire au protocole TLS.

Part V. Conclusion

L'économie tokenisée est bel et bien en passe de toucher chaque coin du monde. Ethereum et EOS ont fourni de très bonnes bases au travers des smart-contracts, mais ces systèmes ne sont pas adaptés au développement de l'économie tokenisée tel que le monde entier peut les utiliser.

everiToken est né du désir de ses fondateurs de créer une blockchain avec un modèle basé sur le token, capable de bénéficier à chacun, n'importe où. Nous avons bâti un système révolutionnaire qui permet aux développeurs, entreprises et utilisateurs d'émettre, transférer et vérifier l'utilisation de tokens de façon simple et peu coûteuse. Nos safe contracts se sont débarrassé de l'aspect Turing-complet, afin de grandement réduire le nombre potentiel de complications ainsi que leur impact au sein du système. Au lieu de créer sans arrêt de nouveaux modèles, nous avons créé un modèle qui s'adapte à tous, devenant la solution de préférence pour plus de 99% des individus. Nous avons amélioré la vitesse, la sécurité, l'opérabilité, la stabilité et la supervision nécessaire pour créer une économie tokenisée efficace et prospère tout en offrant une plateforme décentralisée pour chaque personne dans le monde désireuse d'apprendre, créer, interagir et véritablement échanger de la valeur digitalement parlant. Rejoignez la révolution de l'économie tokenisée et visitez notre site à l'adresse suivante www.everitoken.io

Fondateurs

Hengjin Cai，Directeur de Recherche Scientifique

Le Dr. Hengjin Cai est professeur et maître de recherche au sein de l'Institut d'Informatique à l'Université de Wuhan depuis 2005. Il est un expert titulaire au sein de Laboratoire Mondial de FinTech, chercheur visiteur à l'Institut de Haute Technologie de l'Académie Chinoise de Science de Shenzhen et membre du Comité Chinois d'Intelligence Artificielle et de Big Data. Il possède une solide expertise des sciences de service, de l'Intelligence Artificielle et de la blockchain. Il a récemment publié un livre intitulé *Un Système Blockchain Avec Une Intelligence Mécanique et Humaine Intégrée.* En 2017, il a gagné le Prix WU Wenjun d'Intelligence Artificielle. Il a également reçu le Prix du Président de l'Université de Wuhan en 2012 récompensant son extraordinaire contribution à l'enseignement. En tant que conseillé très impliqué, il a conduit les élèves à la Victoire de 80 prix et récompenses à travers différentes compétitions majeures en Chine et dans le monde, parmi lesquelles la Coupe Microsoft Imagine, la Coupe Morgan Stanley de Finance Informatique à Haute-Performance, le concours National Intel d'Innovation ainsi que la compétition d'Entrepreneuriat des Étudiants Universitaires de Chine.

Brady Luo, CEO Brady-everiToken

Brady est un fervent supporter de l'économie tokenisée à l'échelle mondiale grâce à la technologie blockchain. Il possède une licence en ingénierie électrique de l'Université d'Aéronautique et d'Astronautique de Pékin ainsi qu'un master en finance de la Brandeis University (États-Unis), et il a participé au cursus de stratégie blockchain de la Said Business School de l'université d'Oxford. Brady est naturellement porté vers l'entrepreneuriat et a été élu pour figurer au sein de la 3ème vague du programme « 1000 talents » de Shanghai, en ayant vendu deux de ses startups précédentes. Il a

travaillé pendant 4 ans en tant qu'analyste chez Oppenheimer, l'un des dix plus gros gestionnaires d'actifs américains ainsi que pour le plus grand groupe financier japonais, Mitsubishi UFJ.

Bozhen Chen, Directeur des Opérations

Bozhen possède une riche expérience en gestion des opérations dans le cadre de projets gouvernementaux. Il est spécialisé dans la communication et les relations publiques. Il est diplômé de l'université d'Aston où il a obtenu une licence d'administration des entreprises. Il a travaillé pour le compte d'entreprises des secteurs du e-commerce, de la logistique, des services B2B ainsi que des organismes gouvernementaux. C'est à travers ces expériences qu'il a su construire un solide savoir-faire en termes d'exécution, de communication et de relations publiques à travers de multiples secteurs. Il est l'hôte permanent de la Grande Conférence de l'Internet en Chine, dirige le Centre du Service Publique de l'e-Commerce de Tongxiang et est directeur du Centre d'Entrepreneuriat du Web pour la Jeunesse. Il a obtenu de nombreuses récompenses en tant que leader de la jeunesse chinoise.

Ceeji Cheng, Chef de Produit

Ceeji est un développeur full-stack, expérimenté dans l'architecture de systèmes avec plus de 10 années de développement logiciel, entrepreneuriat et management à son actif. Il a notamment gagné le premier prix des Olympiades nationales d'informatique et a créé sa propre entreprise où il officiait comme cofondateur et directeur technique.

Harry Wang, Directeur Technique

Harry est un ingénieur architecte système expérimenté avec plus de 10 ans d'expertise dans les milieux de la finance et d'Internet. Il travaillait chez Tianfeng Securities à Shanghai avant de participer à la création d'un hedge fund de trading quantitatif en tant que partenaire technique. Il a développé un système très performant de trading quantitative qui est actuellement utilisé au sein de plusieurs marchés et dans le cadre

de plusieurs produits à travers le monde.