Achain Blockchain Whitepaper

Build to be boundless

Table des matières

Résumé

Le Blockchain Achain (dénommé Achain) est engagé à construire monde de blockchain sans bornes, fondé en 2015. La blockchain est maintenant considérée comme une des innovations technologiques ayant le plus grand potentiel ainsi que créativité dans le monde. Il y a eu trois points tournants dans l'histoire de l'homme : la première révolution industrielle, qui fut marquée par des machines remplaçant le travail manuel, la seconde révolution industrielle, qui introduisit le moteur à combustion interne ainsi que d'autres techniques de production massive, et la troisième révolution industrielle, qui est guidée par l'informatique, l'énergie nucléaire, la technologie spatiale et la bio-ingénierie. Cependant, les fondements de notre relation avec la production sont restés les mêmes : elle reste confinée à une structure centralisée et pyramidale. Plus la structure est complexe et plus elle génère de niveaux, plus il est difficile d'assurer son efficacité. La blockchain, aussi connue comme « le réseau à haute valeur ajoutée », est un réseau décentralisé et sûr qui permet des échanges de valeur de pair à pair (peer-to-peer). Achain croit que la technologie de la blockchain est l'innovation qui permettra de changer nos relations de production et qui ouvrira la voie vers la prochaine grande révolution de l'histoire de l'humanité. Avec l'aide d'Achain, nous pouvons créer un monde dans lequel les gens sont directement connectés, un monde fiable, collaboratif, échangé en pair à pair et soutenu par des valeurs orbitant autour du consensus social.

Achain accomplira ce but en trois phases. Premièrement, nous construirons un réseau blockchain stable et sécuritaire avec un design modulaire qui permettra la création de contrats intelligents ainsi que la transmission d'actifs numériques. Des sandbox intelligents seront utilisés pour créer un environnement où il est possible de tester et de surveiller l'exécution de contrats. Les sandbox assurent que les contrats soient assez sécuritaires pour éviter des accidents de DAO similaires[1] avant d'être officiellement téléchargés sur la chaîne. Deuxièmement, nous utilisons le « forking » pour répondre aux besoins de certaines entreprises tels les assurances, la préservation de document, les cryptomonnaies, le tracing, le crédit personnel, et plusieurs autres. Cette phase mènera à la création d'un réseau de blockchain évolutif, facile d'utilisation, à faible coût et bien adapté. Finalement, grâce au Value Exchange Protocol (VEP), nous connecterons ensemble ces forks et autres réseaux actifs, et ouvrirons même l'échange de données avec d'autres réseaux (possiblement non blockchain) pour créer un monde de données internet connectées et multidimensionnel. En utilisant des données multidimensionnelles tels les crédits personnels, les actifs, la production et la consommation de données, le consensus communautaire et le comportement individuel, le tout permettra des échanges intégrés plus organiquement. Le token, nommé ACT par Achain, détient la valeur de son écosystème. Posséder des ACT vous donnes accès à tous les services blockchain de base tels la création de contrats intelligents, le « forking » de réseaux, et beaucoup plus.

Achain a été conçu pour mettre en première place la sécurité, la stabilité et l'évolutivité pour ainsi créer l'écosystème mentionné ci-dessus. Achain, en tant que chaîne publique, choisie le mécanisme de consensus DPoS (Delegated Proof of Stake), qui occupe moins de ressources, et crée à partir ce celui-ci un mécanisme de consensus nommé Result-Delegated Proof of Stake (ci-après dénommé RDPoS). Sous une même situation de sécurité, RDPoS améliore la performance des transactions de tout le réseau ainsi que d'autres paramètres du réseau dans son ensemble. Théoriquement il a atteint un niveau qui excède les 1,000TPS (Transactions Par Seconde).

[1] https://en.wikipedia.org/wiki/The_DAO_(organization)

1 Historique et engagements

1.1 L'histoire du développement du réseau

Le 29 octobre 1969, deux points séparés, ARPANET Université de Californie à Los Angeles (UCLA) et l'Institut de Recherche de Stanford (IRS), ont été connecté avec succès grâce à un câble, signifiant l'arrivée de l'ère d'Internet. Dans les 50 dernières années, avec l'émergence de compagnies basées sur Internet tels Amazon, Google, Facebook, Alibaba, etc., les technologies de l'information ont prouvé comment elles pouvaient changer le monde.

Le 31 octobre 2008, Satoshi Nakamoto présenta son idée du Bitcoin dans un essai, Bitcoin : A Peer-to-Peer Electronic Cash System, déclarant l'arrivée du réseau de transfert de valeurs. Bitcoin a impressionné le monde par ses caractéristiques d'antifraude, de registre distribué, d'anonymité et de fiabilité. Cependant, sa performance et son consensus de PoW (Proof-of-Work) restent encore à être améliorés. Ces dernières années, groupes et individus se sont attardés à l'innovation technique de la performance des échanges, de l'algorithme de consensus et de l'anonymité sécuritaire de la blockchain. Par exemple, la technologie Graphene et le Lightning Network ont amélioré ses performances; le Proof of Stake (POS), le Delegated Proof of Stake (DPoS) et le Practical Byzantine Fault Tolerance (PBFT) furent proposé pour raffiner l'algorithme de consensus; le Zero-knowledge Proof (ZKP) et la technologie de monnaie mixe vont augmenter la sécurité.

1.2 Pourquoi avons-nous besoin de la blockchain?

Avons-nous vraiment besoin de la blockchain? En étant un des premier participant et témoin, Achain croit que cette innovation aura un impact irréversible et qu'elle n'aura pas une durée de vie éphémère.

Ceci est basé sur deux raisons. En premier temps, nous avons besoin d'information réelle, valable, et qui peut réduire le coût de confiance. Les ordinateurs et l'Internet rendent le partage d'information moins cher et plus facile. Avec les technologies de l'information, nous pouvons optimiser la chaîne de valeur et améliorer l'efficacité de nos collaborations. Cependant, nous sommes conscients de la transmission plus rapide d'information fausse et hasardeuse, donc dans ce sens nous prioriserons la sécurité avant le coût de l'établissement d'un réseau de confiance.

En deuxième temps, nous avons besoin d'un réseau pour connecter le consensus social, notre comportement, et nos incitatifs de valeur. Nous avons seulement été témoins de petits changements dans nos relations avec la production : elle demeure une structure pyramidale centralisée et hiérarchique. Plus cette structure devient complexe et plus elle génère de niveaux, plus il devient difficile d'assurer son efficacité.

La blockchain intègre le stockage distribué, la technologie de cryptage, le réseau P2P et d'autres technologies. Il possède l'avantage technologique de la décentralisation et de la fiabilité, ce qui est connu sous le nom de réseau de valeur. La blockchain va non seulement résoudre plus efficacement les problèmes de confiance entre les gens, mais il créera aussi un nouveau réseau de production – un échange de valeurs pair-à-pair.

1.3 Les problèmes non résolus

Depuis son invention en 2008, le Bitcoin a dérivé la technologie de la blockchain, et de nombreux enthousiastes des technologies ont contribué au développement du blockchain. Il y a eu l'Ethereum, qui sert comme plateforme décentralisée, le Bitcoin et le Lite Coin, qui se concentrent sur le développement de cryptomonnaies, Factom, qui permet le dépôt de notarisation, Zcash et Dash, qui protègent l'intimité des utilisateurs, Bitshare, qui fonctionne comme un échange décentralisé de cryptomonnaies, et même Corda, la plateforme populaire de comptabilité distribuée par R3CEV.

Malgré le développement rapide de la technologie de la blockchain, il y a encore des changements à venir.

(1) Des risques de sécurité des contrats intelligents. Les utilisateurs pourraient perdre leurs actifs digitaux lors d'une attaque de pirates informatiques.

(2) Des difficultés de coopération et d'interconnexion de différentes plateformes de blockchain dans différents champs d'utilisation. Bien que des échanges d'information de ce genre aient été tentés, ils restent insuffisants pour supporter le développement complet d'un écosystème de la blockchain.

(3) Des difficultés de liaison entre l'univers de la blockchain et la réalité non basée sur la blockchain. Les idées ne peuvent être facilement mises en application, tel le suivi de l'authentification de produits.

(4) Présentement, l'industrie de la blockchain requiert de hautes qualifications techniques, ce qui résulte à un coût élevé des entreprises à grande échelle.

(5) Une faible performance des transactions comparée aux systèmes centralisés.

1.4 Pourquoi avons-nous besoin d'Achain?

Achain priorise la sécurité, la stabilité et l'extensibilité. En introduisant un design de pointe des machines virtuelles, du sandbox intelligent, du Value Exchange Protocol, et du mécanisme de forking, Achain crée un réseau de blockchain évolutif, facile d'utilisation, à faible coût et personnalisable. L'optimisation de l'intervalle des blocs, du volume des blocs et de l'algorithme de consensus aide aussi Achain avoir une performance atteignant les 1000TPS. Achain croit qu'en même temps que les innovations technologiques permettront de créer un nouveau réseau de relation avec la production, cela permettra aussi de résoudre le problème de confiance dans les communications interpersonnelles, et de plus intégrera organiquement le consensus sociétal, le comportement individuel, ainsi que l'échange de valeurs dans un ensemble inséparable.

2 Principes

2.1 Stabilité

La stabilité du réseau est essentielle pour le fonctionnement d'une solution blockchain. Cependant, ce fait est de plus en plus contesté par de potentielles incertitudes à cause de la nature décentralisée de la plateforme et de son nombre d'utilisations toujours en expansion. Achain, avec sa philosophie de design modulaire et de simplification, a développé LVM (Lua Virtual Machine). Le nouveau VM, exclusivement désigné aux contrats intelligents, offre deux avantages. Il possède un taux de performance amélioré alimenté par le langage Lua, protégeant efficacement contre un potentiel couplage de système. Il adopte aussi une structure exécutée séparément et construite indépendamment pour prévenir que l'entièreté du réseau soit affectée par des risques locaux.

2.2 Sécurité

PoW a été utilisé pour maintenir la sécurité du réseau Bitcoin, mais due à une augmentation de la demande en minage et en authentification, une quantité significative d'énergie se retrouvèrent dans les mains des mineurs et des pools de minage, résultant à la centralisation non voulue du « serveur central ». Si une entité contrôle 51 pour cent de la puissance de calcul, théoriquement, il est possible de contrôler la majorité des transactions de Bitcoin, ce qui est connu comme une attaque DOS (denial-of-service). En outre, une haute consommation d'énergie génère un énorme coût.

Comparé au modèle PoW, le modèle PoS (Proof-of-Stake) vise à un niveau plus élevé de sécurité ainsi qu'une gamme plus large d'applications. Le modèle PoS contribue à la sécurité du réseau seulement quand il attire assez de détenteurs pour le minage PoS.

Basé sur le PoS, le DPoW a été créé plus tard en tant que version améliorée, mais Achain est allé jusqu'à inventer une version plus commerciale et acceptée universellement, le mécanisme de consensus RDPoS. En fonctionnant aussi sécuritairement que le DPoS, le RDPoS peut augmenter la réponse du bloc, et améliorer la stabilité et la sécurité du réseau.

De plus, Achain a proposé un mécanisme de sandbox intelligent. Chaque contrat créé doit en premier temps passer un test dans le sandbox intelligent pour être testé automatiquement contre une détérioration ou des loopholes (échappatoire). Le réseau détermine lui-même si un nouveau contrat écrit se qualifie pour être téléchargé sur l'écosystème d'Achain.

2.3 Évolutivité

L'évolutivité est proposée pour résoudre le problème d'incompatibilité des blocs dans la blockchain. Premièrement, nous croyons que la mise à niveau et que le forking sont des évolutions efficaces du réseau. Après des forks, cela générera une chaîne principale ainsi qu'un nombre de sous-chaînes. Toutes les chaînes sont totalement équivalentes en structure, mais chacune reçoit un logo différent basé sur différents consensus de la communauté. Chaque sous-

chaîne peut être personnalisée en accord à différentes utilisations en construisant le VEP (Value Exchange Protocol), qui comme une passerelle, permet le partage d'information et de valeurs parmi les chaînes. Ce genre de collaboration forme un réseau d'applications multiples. Non seulement cela, mais les données en ligne de cas non basé sur la blockchain seront aussi incorporées dans l'écosystème d'Achain. Le tout est complété par les contrats intelligents pour répondre à des cas dans le monde réel.

2.4 Facilité d'utilisation

Achain fournit une facilité d'utilisation de deux façons. La première est de fournir le Blockchain comme Service (Blockchain as a Service, ou BaaS) pour réduire le seuil technique des entreprises et des particuliers. Les utilisations de la blockchain deviennent faciles d'utilisation grâce au forking de chaînes, à la personnalisation d'information, à la création et à la mise à niveau de contrats intelligents, aux suivis de transaction d'actif, et complète le tout avec une visualisation. La seconde est d'offrir le support de multiples langages de programmation, de Lua ou C++ jusqu'à Java, ce qui encourage la plupart des développeurs et enthousiastes à s'impliquer facilement.

3 Implémentation

3.1 Contrat intelligent et LVM

Le principe conventionnel du contrat intelligent est de permettre l'accès à l'information à l'intérieur du réseau du blockchain. Cependant, Achain a reconstruit cette technologie en une qui permet l'interaction d'information entre le système de blockchain et à l'extérieur du réseau. Ceci peut aussi réaliser une synchronisation des activités journalières, tels les processus d'affaires ou les applications légales, et l'échange d'état des données.

Les applications des business sont en réalité très complexes dût à la nature de leur structure de données et des règles d'entreprise. En réponse, Achain produit deux aspects de la préparation pour surmonter cette complexité. La première est de séparer les idées abstraites et les besoins généraux derrière une potentielle utilisation pour ainsi conceptualiser à l'avance l'interface API et la structure de donnée. La seconde est de sélectionner un langage complet de Turing pour estimer le plus près possible les règles du monde physique réel.

Lua, le premier choix d'Achain, est une machine virtuelle avec un compilateur optimisé et un bytecode. Étant adapté à l'application du blockchain, Lua permet la compilation statique et l'exécution sur demande.

Dans le réseau de la blockchain, il y a 5 niveaux dans le cycle de vie des contrats intelligents :

Création du code source dans Lua.

Compilation vers le GPC bytecode.

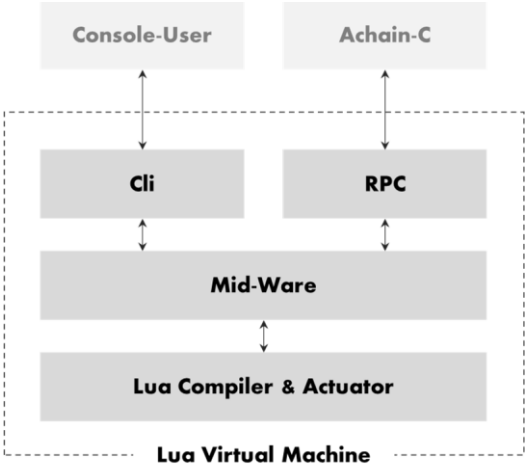
Enregistrement du contrat et du dépôt d'acompte.

Appel de l'API du contrat.

Mise à niveau ou destruction du contrat.

Pour des considérations économiques, les tokens seront seulement utilisé lors des enregistrements, des appels et des mises à niveau. D'un côté, l'exécution de contrats occupe des ressources informatiques, la capacité de la blockchain et le trafic du réseau. De l'autre, des moyens économiques augmentent le seuil potentiel de cyberattaques.

Les modules séparés pour l'exécution de contrats, Lua virtual machine (LVM), fonctionne comme-ci :



Architecture du LVM

Le LVM inclut 4 parties : le CLI (Command Line Interface), RPC (Remote Procedure Call), Mid-ware et LCA (Lua Compiler & Actuator).

Comment est-ce que le LVM fonctionne? Premièrement, les contrats sont entrés à partir de la console en tant qu'une ligne de commande Lua. Ensuite, le CLI reçoit la commande et la transfère au Mid-ware. Si le RPC reçoit en même temps la requête Lua de la blockchain, le Mid-ware transférera les deux commandes et requêtes au LCA de manière synchrone. Finalement, le LCA opère l'environnement d'exécution, reçoit les scripts Lua, exécute les programmes, et retourne les résultats au Mid-ware. Le CLI et le PRC retournent les résultats du Mid-ware vers la console et la blockchain séparément.

Il y a une demande fréquente d'exécuter des contrats au travers d'un réseau de blockchain actif. Pour assurer une haute efficacité, Achain suit deux principes. Le premier est de minimiser le temps de démarrage et de fermeture du processus LVM. Le second est d'assurer que les outputs d'exécutions sont cohérents à différents nœuds et temps avec des inputs similaires.

LVM supporte des langages de programmation avancés, tels C#, Java, Solidity (le langage de programmation d'Ethereum). Cela permet à la majorité des développeurs et enthousiastes de s'impliquer.

3.2 Accord consensuel

Le réseau de blockchain ne peut fonctionner sans consensus. Présentement, les solutions de consensus les plus courantes sont : PoW, PoS, PBFT et DPoS. Achain a sélectionné le DPoS et l'a amélioré en un nouveau mécanisme nommé RDPoS (Resulted-Delegated Proof of Stake).

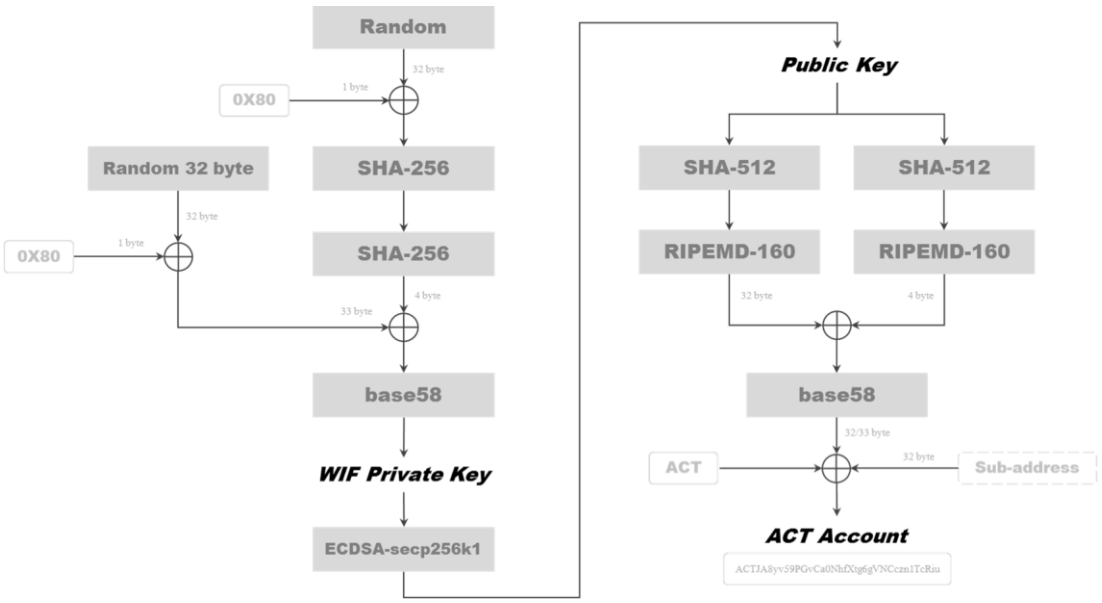
Le RDPoS hérite de tous les avantages du DPoS. Non seulement il est nécessaire pour consommer la puissance de calcul redondante pour recevoir un nouveau bloc, mais aussi les résultats d'exécution d'un contrat peuvent alternativement être vérifiés par des nœuds agents ou tous les nœuds dépendant de l'état du réseau.

Il est incapable d'établir un consensus communautaire sans raison, qui se nomme habituellement un token dans le monde de la blockchain. Achain est ainsi une blockchain publique grâce à leur propre token, ACT. Les possesseurs d'ACT ont le droit de participer à des événements de la communauté, tels que créer ou émettre des contrats intelligents, accéder aux services du réseau, aux agents de vote, ou profiter en tant qu'agent. Dans la communauté d'Achain, les candidats sont votés par tous les détenteurs d'ACT. Le top 99 des candidats ayant le plus grand nombre de votes pourra être promu comme agent et recevra le droit de vérifier les transactions tour par tour. Personne ne peut modifier la séquence de vérification elle-même. Les récompenses sont données en échange du travail; aucun travail ne sera pénalisé.

Théoriquement, RDPoS améliore mieux les capacités du réseau que le DPoS. Spécialement dans le cas d'une exécution à long terme ou d'une haute utilisation du stockage, tous les nœuds, non seulement les nœuds agents, prennent part à la vérification. Le RDPoS peut ainsi réduire le niveau de congestion du réseau en entier. De plus, en optimisant le mécanisme de consensus, les membres des groupes d'agent changent continuellement. C'est important pour le réseau de rester décentralisé.

3.3 Compte

Le compte est spécifiquement conçu pour des transactions sécuritaires dans le réseau de la blockchain. Il y a 3 éléments qui doivent être mentionnés lorsque nous parlons de la théorie de la blockchain : le compte, la clé publique et la clé privée (clé privée, clé publique et compte dans cet ordre spécifique). Grâce à la méthode SHA (Secure Hash Algorithm), la blockchain est un réseau sécuritaire, car les clés privées sont trop difficilement déchiffrables. Le hash value est le raffinement d'un objet, comme un programme, un email, une page web, etc. Normalement son output a une capacité fixe et est plus petit que son input. Le détail du procédé de génération est ainsi :



Procédé de génération d'une clé privée, d'une clé publique et d'un compte ACT

Nous divisons les comptes en deux catégories en accord avec la longueur en byte : le compte principal et le sous-compte.

Le compte principal contient de 35 à 36 bytes, mais le sous-compte contient de 67 à 68 bytes. Évidemment, le sous-compte a plus de bytes que le principal, car le sous-compte contient le compte principal ainsi qu'un autre 32 bytes de caractères aléatoires. Pour cette raison, le compte principal peut s'associer à plusieurs sous-comptes, tant et aussi longtemps qu'ils ont tous les mêmes 32 ou 33 premiers bytes. Il est ainsi plus facile d'améliorer la performance des transactions grâce à ce design. Des transactions parallèles parmi différents sous-comptes sont permises si ces sous-comptes appartiennent au principal. Le design principal/sous est principalement utilisé dans les échanges de cryptomonnaies pour réduire la consommation de compte.

Achain a sélectionné le modèle de compte au lieu du modèle UTXO (Unspent Transaction Output) qui est appliqué au Bitcoin. UTXO est un excellent design avec des particularités telles les transactions parallèles et une meilleure autonomie. En revanche, il est très difficile de réaliser un contrat intelligent sous un design orienté vers les transactions. Il est plus facile d'initier des transactions au travers de déclencheurs causés par un changement d'état ou de condition.

3.4 Le réseau de forking

« Les « hard fork » rendront le réseau plus durable », comme affirmait le cofondateur de la fondation Ethereum, Taylor Gerring.

Achain préconise un réseau de fork adéquat pour deux raisons : premièrement, le hard forking maintient la vigueur du réseau; deuxièmement, le hard fork satisfait différents scénarios d'utilisation. Le réseau de blockchain est un genre de consensus social supporté par les membres de la communauté. Lorsque le consensus social change, le hard forking devient inévitable. Certains forking blockchain survivront tandis que d'autres disparaîtront à cause d'un manque de support. Le forking est le processus d'évolution de chaque organisation autonome, et éventuellement chaque forking blockchain qui aura survécu sera la preuve d'une meilleure solution pour résoudre les problèmes du monde réel. En second lieu, la blockchain est encore à un stade précoce de son développement. Outre les cryptomonnaies, d'autres cas d'utilisation restent encore à être vérifiés. Plusieurs technologies tels le lightning network, la preuve à divulgation nulle de connaissance, les chaînes secondaires, et les réseaux séparés, ont tous émergé récemment du domaine du blockchain. Ces innovations démontrent que différents taux de transaction, différents algorithmes de consensus, et différentes caractéristiques des technologies pourraient être combinés ensemble pour satisfaire les divers prérequis. Idéalement, différents réseaux de forking rempliront leurs besoins correspondants. Cependant, le réseau de fork peut aussi générer des problèmes qui seront discutés dans la section qui suit.

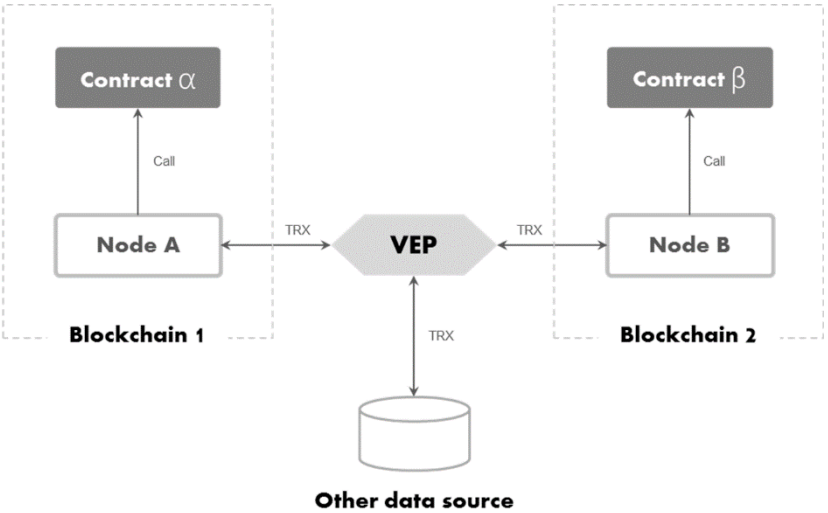
Achain est désigné comme le blockchain initial. Pour Achain, les utilisateurs peuvent facilement créer de multiples nouvelles blockchains à partir des forks, et ils peuvent même le faire continuellement à partir de blockchains nouvellement créées. Toutes les blockchains résultant d'un fork sont égales, ce qui signifie qu'ils ne sont pas hiérarchiques d'une perspective technique ou économique. Le VEP (Value Exchange Protocol) enregistrera et diffusera le message suite à la création d'une nouvelle blockchain résultant d'un fork, ce qui inclut les blocs de genèse, l'identification de blockchain, les nœuds sources, les cryptomonnaies, le service d'identification, etc. Chaque forking déclenchera la diffusion d'un nouveau message VEP. Quand les blockchains ont besoin de communiquer entre eux, le nœud d'une blockchain cherchera pour un autre nœud dans un autre blockchain à partir du message VEP diffusé, et échangera des informations et des valeurs sous la structure du VEP. Le VEP fonctionne comme le service DNS qui fournit les enregistrements, mises à jour et services d'accès.

En fonction d'atteindre ces buts, Achain a installé son propre BaaS (Blockchain as a Service), et utilise une multitude de langages de programmation ainsi qu'un développement visualisé pour réduire les difficultés d'adoption. N'importe qui pourrait utiliser le réseau de forking pour développer sa propre application, ce qui encourage les innovations de la communauté. Quand la communauté d'Achain deviendra plus active, la valeur d'Achain augmentera, et de plus en plus de développeurs rejoindrons le réseau de forking d'Achain. Cette stimulation mutuelle permettra à l'écosystème d'Achain de prospérer.

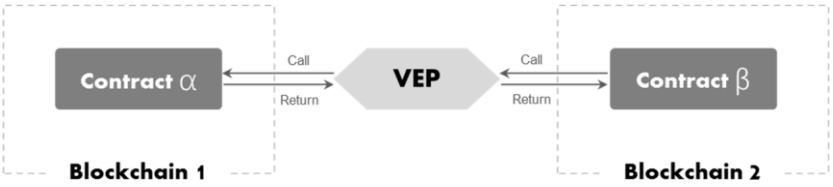
3.5 Value Exchange Protocol

Le VEP est un protocole de communication inter-chaîne. Une seule blockchain a ses limitations pour supporter de nombreuses différentes applications, mais un réseau de blockchains connectés pourrait produire une valeur superposée. Plus les blockchains résultant d'un fork seront connectées, plus il y aura de valeur créée. Avant de discuter comment le VEP fonctionne, regardons comment chaque nœud se font confiance l'un l'autre dans un réseau de blockchains. La blockchain entrepose les informations inchangeables et fiables, ce qui dépend d'un registre ainsi que d'un algorithme de consensus distribués. La blockchain est aussi une communauté basée sur un consensus convenu, la confiance entre les nœuds des blockchains se base sur un tel consensus ainsi qu'aspiration économique. De la même façon, la blockchain en entier pourrait être vue comme un « nœud », et quand plusieurs « nœuds » sont connectés, les « nœuds » ont besoin d'un nouveau consensus parmi le réseau de forking blockchains. Cela devient encore plus difficile puisque le réseau de forking blockchains a aussi besoin d'égalité, de confiance, et de balance entre les différents intérêts, sans mentionner les mauvais nœuds dans le réseau. Il est donc important de mettre en place des règles à l'avance, tout comme les humains ont besoin de coopérer au travers d'organisations sous différentes lois, contrats et morales.

Le VEP définit les règles de connexion et de communication. Le VEP enregistre chaque forking blockchain, et fournit les demandes et les services d'accès pour chaque forking blockchains autorisés. Le VEP supporte deux majeurs scénarios d'utilisation : la communication inter-chaîne et l'invocation de contrats intelligents inter-chaîne. La communication inter-chaîne signifie que les contrats intelligents se communiquent et s'invoquent entre eux, avec la possibilité de la création de nouvelles informations, ce qui est indirectement déclenché par le changement du registre ou des informations hors-ligne. Par exemple, des prêts impayés, qui sont définis dans les contrats intelligents, impacteront le crédit personnel. Les archives des prêts sont stockées dans le blockchain A, les informations de crédits dans le blockchain B, et les identifications personnelles dans une base de données publique hors-ligne. Un simple exemple de l'invocation du contrat intelligent inter-chaîne est l'échange inter-chaîne de tokens, ce qui garantit une valeur totale inchangée.



La communication inter-chaîne



L'invocation de contrats inter-chaîne

Le VEP inclu les informations qui suivent :

(1) Les informations d'enregistrement de la blockchain, l'identité du réseau, l'identité du service, les nœuds sources, etc.
(2) Le protocole de vérification inter-chaîne.
(3) Le protocole de communication.
(4) Le protocole d'échange d'actifs.
(5) Le mécanisme de récompenses et de punitions.

3.6 Axé sur les événements

Basé sur le VEP, le réseau de forking d'Achain peut communiquer et échanger des valeurs. Au travers de l'IOT (Internet of Things) et de l'IA (Intelligence Artificielle), le réseau de forking Achain peut même soutenir les données hors-ligne, telles les banques de données publiques ou d'entreprises, et finalement atteindre des événements à temps réel poussés par le monde réel.

Il y a 5 étapes au mécanisme axé sur les événements :

(1) Reconnaître les différentes scènes, les catégoriser et mettre en place les standards de réponse.
(2) Service d'écoute ouvert et la capture d'information.
(3) Calculer et vérifier les réponses.
(4) Exécuter les contrats intelligents à partir du VEP.
(5) Retourner les résultats exécutés.

4 Utilisations

4.1 Financement de la chaîne d'approvisionnement

Le financement de la chaîne d'approvisionnement, aussi connût sous financement des fournisseurs ou affacturage inversé, est une solution mise en place pour optimiser le cash-flow. Il permet aux entreprises d'étendre leurs termes de paiement aux fournisseurs tout en permettant à leurs larges fournisseurs ou fournisseurs SME d'être payés plus tôt. C'est une des industries ayant le taux de croissance le plus haut de ces dernières années. Cependant, il y a trop de partis impliqués, ce qui mène à un stockage éparpillé des données. L'information de l'inventaire des fournisseurs est listée dans leur système de gestion d'entrepôt; l'information des livrables se retrouve dans le CRM des compagnies de logistique; les informations de financement se retrouvent à la banque; et les données d'opération sont dans les mains de l'entreprise elle-même. Il est très difficile d'établir un système de crédit puisque toutes les données sont non-transparentes et incomplètes. Par conséquent, les institutions financières seront très prudentes et éventuellement passeront à côté de projets prometteurs à cause du coût élevé de l'évaluation du crédit.

Achain peut aider les entreprises et les institutions financières à reconstruire un système de crédit qui est optimisé sur l'efficacité du financement de la chaîne d'approvisionnement. La solution est de construire une entreprise de système de crédit basé sur Achain et qui s'occupe de l'entreposage, de la logistique et du financement des fournisseurs de services. Le système basé sur la blockchain permet à toutes les compagnies de la chaîne d'approvisionnement d'avoir accès aux données collectées durant la production, la logistique et la vérification des comptes. Les E-reçus seront utilisés et leurs émission, confirmation, circulation, scission et acceptation sont déclenchées au travers de contrats intelligents par les différents partis de la chaîne d'approvisionnement. Aussi, le tout ne sera déclenché et enregistré seulement quand les données seront mises à jour dans l'un des systèmes de l'entreprise qui a été mutuellement convenu entre tous les partis. Toutes les actions faites dans le système seront enregistrées et stockées dans la blockchain et ne pourront être modifiées ou effacées.

Achain utilise des technologies tels le BaaS et les sandbox intelligents pour permettre un déploiement à suivi rapide sur la blockchain. Cela permet aux utilisateurs de rapidement construire un réseau de blockchain à faible coût. De plus, Achain accepte l'utilisation du VEP pour établir un protocole de connexion et activer le mécanisme axé sur les événements par l'intégration de données. Dans ce cas, tous les participants sont capables de vérifier les données pour ainsi assurer un transfert de fonds plus efficace dans la chaîne d'approvisionnement.

4.2 Authentification

L'industrie du détail est naturellement catégorisée par la fragmentation des données de transactions, la diversification des nœuds d'échange et la complexité du réseau d'échange. L'emballage d'un item comprend habituellement sa date de production, son lieu d'origine et son fabricant, peu importe ses canaux de vente. Par contre, il est difficile de vérifier les informations

listées. Une grande marge de profits crée un excellent incitatif à la fraude, spécialement pour les denrées à haute valeur, tels les diamants, les sacs de luxes, les produits de soin de la peau, etc.

L'existence de fraude endommage l'intérêt du consommateur et cause des dommages à la crédibilité et à l'image d'une entreprise authentique. Il y a trois majeures difficultés de l'industrie envers l'authentification des produits. En premier, il doit retracer non seulement jusqu'au procédé de production, mais aussi au procédé de logistique, ce qui implique une haute complexité dans la coopération inter organisation. Deuxièmement, l'information est isolée dans différents systèmes centralisés utilisés par des centaines de partis. Dernièrement, un système centralisé est risqué puisque l'information peut être changée ou effacée par un seul parti.

Achain propose la solution à l'industrie du détail : Blockchain + IoT

Avec IoT, les données de production et de logistique peuvent être collectées en temps réel au travers de dispositifs intelligents et ensuite être entreposées dans le réseau retraçable d'Achain grâce au VEP. La structure d'entreposage de donnée unique à la blockchain et au registre distribué assure que les données dans la chaîne ne puissent être effacées ou altérées. Pendant ce temps, des cryptages asymétriques et des mécanismes anonymes assurent la sécurité de l'information. Les clients peuvent facilement accéder au profil complet d'un produit en y entrant son numéro de produit et numéro de lot.

La blockchain peut résoudre la difficulté de l'authentification tout en prévenant la divulgation d'information corporative. L'information est transparente à tous les partis relatifs : manufacturiers, fournisseurs de logistique et consommateurs. L'information d'achat et les détails de logistiques fournissent un support instructif aux manufacturiers pour analyser leur stratégie de production. De tels mécanismes bénéficient aussi aux fournisseurs de logistiques en leur permettant de fournir des données de support. La technologie de la blockchain crée une société transparente et efficace.

5 Plan de développement

5.1 Plan

Étape 1. Singularité （2014~2016）

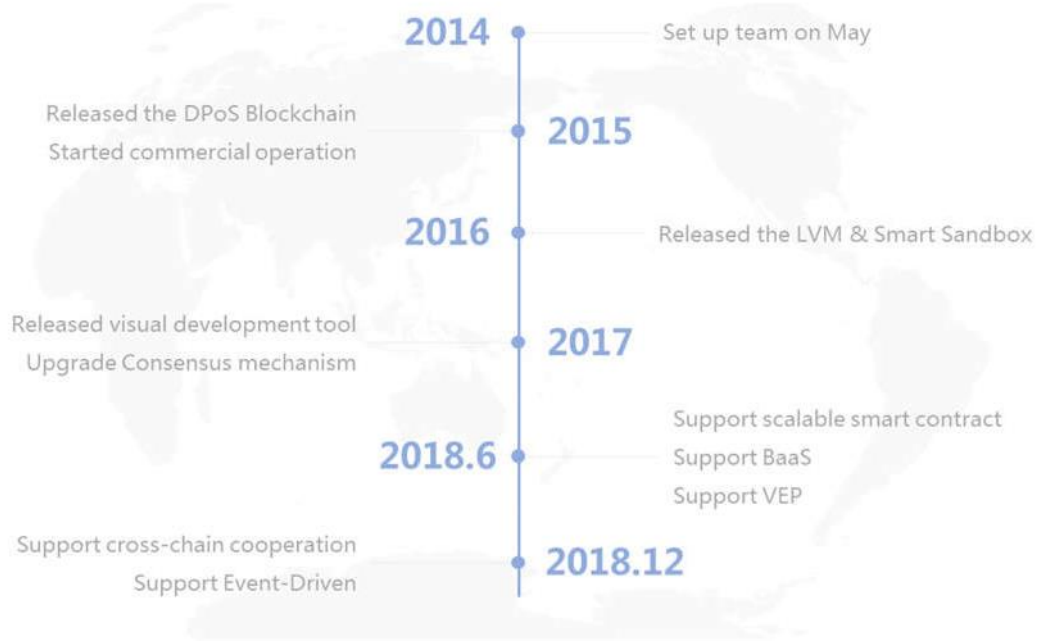
La première étape consiste à améliorer la sécurité et la stabilité du réseau d'Achain. Les contrats intelligents, les actifs digitaux, et la simulation sandbox sont mis à disponibilité au travers de la méthodologie du design modulaire. Le sandbox peut automatiquement tester et surveiller l'environnement dans lequel les contrats intelligents nouvellement créés opèrent. Ainsi, les tests assurent que ces contrats fonctionnent de façon stable et sécuritaire dans le réseau d'Achain.

Étape 2. Galaxie （2016~2017）

Achain se divise en plusieurs sous-chaînes pour rencontrer les besoins de différentes utilisations réelles, incluant les assurances, e-documentations, cryptomonnaies, enquêtes de registre, cotes de crédit, et plusieurs autres qui peuvent être remplis par les sous-chaînes au travers d'un réseau blockchain interconnecté, facile d'utilisation et personnalisé.

Étape 3. Cosmos （2017~2018）

Le concept et la technologie de BaaS et de VEP (Value Exchange Protocol) peuvent non seulement unifier la chaîne principale et les sous-chaînes, mais aussi connecter les réalités non blockchain à l'écosystème de la blockchain. Ceci pousse l'interconnectivité du monde vers une plus grande et englobante dimension.



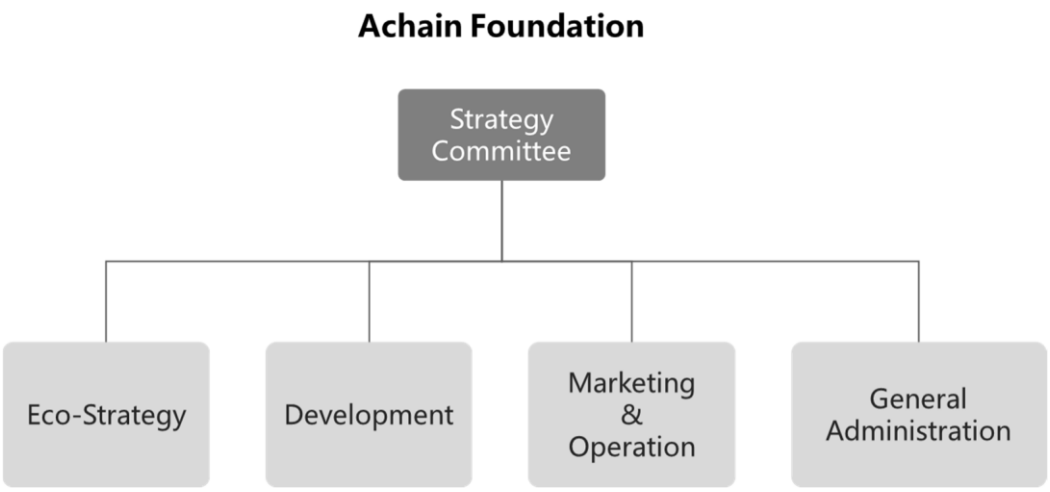
Plan de développement d'Achain

6 Gouvernance du programme

6.1 À propos de la fondation Achain

La fondation Achain est responsable du développement d'Achain, de sa transparence dans l'administration et des communications à l'intérieur de son réseau de communautés. La fondation crée une structure d'administration efficace et soutenable pour faciliter la gestion des affaires de la communauté. Elle s'occupe aussi de sécuriser les fonds qu'Achain obtient. Elle consiste d'un centre de stratégie, d'un centre de développement technologique, d'un centre de marketing et d'un centre d'administration.

6.2 Gouvernance de la fondation



Structure de gouvernance de la fondation

Ci-dessous est une introduction détaillée de tous les secteurs :

Le comité de stratégie est responsable de la gestion et de la prise de décision pour tout événement majeur. Ceci peut inclure l'embauche ou le renvoi du personnel exécutif, et plusieurs autres. L'adhésion au comité de stratégie dure 3 ans avec possibilité de rallonge. Le président du comité est élu par les fondateurs d'Achain et les actionnaires dans le premier cycle et par tous les membres du comité dans les cycles suivants.

Le centre d'éco-stratégie est responsable de la coopération interindustrielle d'Achain, se concentrant spécialement sur la formation d'ententes stratégiques avec des compagnies provenant des secteurs du financement Internet, des ICO, du commerce transfrontalier, du Big Data et de l'AI. Ceci prépare Achain pour une utilisation commerciale plus large.

Le centre de développement est responsable de l'avancement, du testage, de l'annonce et de l'inspection des technologies de base. Les membres du centre maintiennent une communication sainte entre les bénéficiaires et les contributeurs concernant le progrès des projets. Ceci peut inclure tenir en place des conférences ou des rencontres régulières par rapport aux technologies.

Le centre de marketing et d'opération est responsable de la promotion et de la communication de nouvelles technologies, produits, communautés et projets.

Le centre d'administration générale sert aux finances, aux affaires légales, aux ressources humaines et aux autres fonctions administratives. Les finances impliquent le planning, l'exercice et la revue du budget pour tous les projets. Les affaires légales impliquent l'écriture et la revue de document de tout type pour éliminer tout risque de pratiques illégitimes. L'administration générale est responsable des affaires humaines tels l'assignation de nouveaux postes et la distribution des salaires.

6.3 Nous contacter

Site officiel:https://www.achain.com/

E-mail: Hi@achain.com

Forum: https://newforum.achain.com/

Telegram FR: https://t.me/Achain_FR

Telegram EN: https://t.me/AchainOfficial

Twitter: https://twitter.com/AchainOfficial

Facebook: https://www.facebook.com/Achain-124056884987435/

Slack: https://slack.achain.com/

WeChat: Achain_secretary

QQ: 626348505

6.4 Open source

Github: https://github.com/Achain-Dev/Achain

7 Équipe technique

Fondé en 2015, Achain possède sa propre équipe technique composée de 17 membres cœur qui sont pleinement expérimentés dans la blockchain et la technologie des cryptomonnaies.

Founder					
Tony Cui					
Core Developers					
Aqua Zhao	Eric Wong	Li gong Liu	Jack Lee	Owen Yeung	Will Xiao
Arthur Qiang	Ray Kwok	Mical Chine	Araon Zhang	Tim Fish	Norman Fan
Hiroshi Shu	Ting Tong	Beck Chu	Sunny Gao		