Ælf – Un Cadre de Blockchain du Parallélisme de Multi-Chaînes

V 1.2

Le 25 Novembre, 2017

Abstrait

La communauté de Blockchain a connu un développement rapide au cours des dernières années. D'abord apparu comme un mécanisme décentralisé et sécurisé de transmission P2P, Bitcoin de Satoshi a prouvé le concept de crypto-monnaie décentralisée. Ethereum a ensuite contribué à la mise en œuvre avec succès de «Contrats Intelligents» polyvalents pour la communauté. Il a déchaîné un grand potentiel de Blockchain dans diverses applications et industries. En conséquence, de nombreux crypto-actifs alternatifs ont été construits sur Blockchains. Ce n'est que l'aube de Blockchain, car les barrières entre la communauté de Blockchain et le monde des affaires doivent encore être brisées. Nous sommes à un tournant que la prochaine phase de Blockchain mènera l'intégration entre Blockchain et le monde des affaires entités, et apportera inévitablement des actifs numériques beaucoup plus solides.

Afin d'entrer dans le nouveau paradigme de Blockchain, il doit y avoir un système polyvalent d'exploitation conçu pour répondre aux besoins commerciaux. Cette chaîne doit répondre à trois défis principaux:

1. Blockchains actuelles ne sont pas évolutives, car les performances d'un seul nœud / machine minière déterminent celles de l'ensemble du système.
2. Blockchains actuelles ne séparent pas les ressources pour différents Contrats Intelligents, ce qui entraîne des interférences entre les exécutions de Contrats Intelligents.
3. Blockchains actuelles n'ont pas de Protocole de Consensus prédéfini pour l’adoption des mises à jour ou de nouvelles technologies.

Ce livre blanc présente une architecture très efficace de Blockchain qui intègre des principes et des technologies de Pointe dans la conception de l’informatique pour l'amener au niveau commercial. Nous imaginons qu'il crée un "écosystème Linux" pour Blockchain. Nous nous concentrons sur la définition et la fourniture des composants les plus basiques, essentiels et chronophages du système et les améliorations significatives en fonction des chaînes existantes sur le marché. Le système permet de personnalisation aux développeurs pour répondre à leurs propres besoins, en particulier les exigences commerciales pour diverses industries. Il contiendra les caractéristiques principales ci-dessous:

1. Présente le concept de Chaîne Principale et de Chaînes Latérales multicouches pour gérer divers scénarios commerciaux. Une chaîne est conçue pour un cas d'utilisation, distribuant différentes tâches sur plusieurs chaînes et améliore l'efficacité du traitement
2. Permet ÆIf de communiquer avec les systèmes de Blockchain externes via la messagerie, par exemple. Bitcoin, Ethereum
3. Autorise le traitement en parallèle pour les transactions non concurrentes et le service en nuage
4. Définit les composants de base du bloc minimum viable et de la Collection de Genesis Contrat Intelligent pour chaque Chaîne afin de réduire la complexité des données et d'obtenir une personnalisation élevée
5. Permettre aux parties prenantes d'approuver les amendements au protocole, y compris la redéfinition du Protocole de Consensus; permet aux Chaînes

Latérales de rejoindre ou de quitter dynamiquement la Chaîne Principale sur la base du Protocole de Consensus, introduisant ainsi la concurrence et l'incitation à améliorer chaque Chaîne Latérale.

Contenu

1. Systèmes Actuels de Blockchain

À présent, la technologie de Blockchain et son application se développent exponentiellement. De nombreuses industries expérimentent comment migrer de l'architecture du réseau traditionnelle à celle du réseau basé sur Blockchain. Cependant, les systèmes actuels de Blockchain ne sont pas encore capables et efficaces de fonctionner comme un système polyvalent d'exploitation et d'appuyer diverses applications. Bitcoin comme la conception pionnière de Blockchain est plus similaire à une application. Ethereum a démontré certaines caractéristiques d'un Système d'Exploitation - les développeurs peuvent programmer des applications comme Contrats Intelligents sur Ethereum, la Chaîne fournit le langage de programmation et un Adaptateur sous forme de Solidité, etc. Cependant, du point de vue du Système d'Exploitation moderne, il y a encore plusieurs inconvénients sur Ethereum, comme le manque de découplage entre les composants du système, le manque de personnalisation de la plupart des modules et les interfaces insuffisantes du système, etc.

Cette approche manque de la conception holistique du système et n'est pas encore commercialement viable pour des scénarios d'application intersectoriels. Cela limite grandement l'application commerciale de la technologie de Blockchain.

1.1. Blockchain Général vs. les Scénarios Complexes d'affaires

Le défi actuel qui entrave l'adoption commerciale à grande échelle de la technologie de Blockchain est son incapacité à répondre aux exigences de divers scénarios complexes d'affaires. Ces scénarios ont souvent des caractéristiques différentes en termes de processus et de logique d'exécution, nécessitant des solutions distinctes. Par conséquent, Blockchain «toute faite» fait face à un dilemme difficile pour équilibrer les besoins de différents scénarios d'affaires. Par exemple, l'émission d'un ticket est de haute fréquence, ce qui signifie qu'un TPS élevé dans le système est souhaitable; d'un autre côté, le contrat juridique numérique met l'accent sur la haute sécurité et la fiabilité.

Il existe deux solutions générales pour répondre à ces exigences:

i. Utilisez Blockchain comme base de données uniquement et ne traitez pas de logique commerciale. Cette approche vise à gérer tout scénario d'affaires et à maintenir la compatibilité. De nombreuses chaînes similaires à Bitcoin utilisent cette approche. Ils enregistrent les données et le hachage, dans une sortie de transaction "OP_RETURN", stockée à Blockchain.

ii. Enregistrer divers Contrats Intelligents complexes sur une seule Blockchain. Ces Contrats Intelligents doivent servir des modèles commerciaux prédéfinis de divers scénarios. Ethereum représente ce type de Chaînes. Du fait que tous les Contrats Intelligents sont écrits sur une seule chaîne, Blockchain devient complexe, nécessite des coûts de maintenance élevés et manque de structure efficace pour exécuter les Contrats Intelligents.

1.2. Limitation des Performances du Traitement Séquentiel

Comme Blockchain est de plus en plus largement utilisée, en particulier dans la

gestion de transactions à grande échelle, sa capacité de traitement des transactions subit une pression énorme en utilisant un traitement séquentiel, ce qui engendre des goulets d'étranglement dans les performances du réseau. Les systèmes actuels de Blockchain sont confrontés à de multiples défis pour améliorer leur capacité, parfois au détriment de l'efficacité des transactions. Par exemple, les frais de transaction de Bitcoin deviennent plus chers à mesure que le volume des transactions augmente et qu'un important carnet de commandes attend une confirmation depuis longtemps. Ethereum fait face à un nombre croissant de congestions lors des ventes de Token. Cependant, dans l'architecture traditionnelle de l'IT, les techniques modernes telles que le partitionnement, le sharding et l'architecture décentralisée se sont révélées très efficaces pour améliorer les performances du système.

D'un autre côté, le concept de traitement parallèle des tâches n'a pas été adopté pour accroître l'efficacité. Lorsqu'un bloc contient une grande quantité de données de transaction et des Contrats Intelligents complexes, la transaction séquentielle a atteint sa limite d'efficacité de la formation et de la vérification du bloc.

1.3. Complexité et Redondance des Données

Comme décrit dans la section 1.1, Blockchain universelle est utilisée pour répondre aux besoins de différents scénarios d'affaires. L'inconvénient du système universel de Blockchain est la complexité excessive des Contrats Intelligents et du Protocole de Consensus, le manque de solution sur mesure, adaptée à des scénarios d'affaires spécifiques et des données redondantes.

1.4. Dilemme de la Mise à jour du Protocole

Malgré l'adoption croissante de Blockchain, il est encore au stade naissant. L'amélioration et l'innovation significative sont encore à venir dans le futur. Ces mises à jour sont essentielles pour faire évoluer Blockchain et suivre l'intérêt de l'environnement et des parties prenantes en perpétuelle évolution. La grande variété de parties prenantes au sein de l'écosystème est généralement difficile à parvenir à un Consensus sans un mécanisme efficace de gouvernance, conduisant à la plupart des mises à jour actuelles du Protocole dans l'impasse ou les différends. Bitcoin en est un exemple vivants car la communauté a trouvé difficile d'obtenir un accord pour l'introduction de nombreuses nouvelles fonctionnalités dans les dernières années.

1.5. Inflation du bloc

Plus un système de Blockchain est performant, plus son coût de maintenance est élevé. L'exécution d'un Nœud Complet de Bitcoin Actuel nécessite plus de 130 G d'espace et plus de 180 G pour Ethereum. Cette situation ne sera pas améliorée à l'avenir. Au fur et à mesure que de plus en plus d'utilisateurs adoptent Blockchain et mènent plus d'activités de transaction, l'inflation du Bloc va s'accélérer et les coûts de maintenance augmenteront encore plus. Des mesures doivent être prises pour atténuer le cercle vicieux.

1.6. Support de communication inefficace Pair-à- Pair

Les Blockchain existantes sont principalement communiquées en fonction du réseau de diffusion. Et le support pour la communication P2P est inefficace et non sécurisé. Un exemple est que si certaines données ne sont concernées que par un groupe d'utilisateurs, ces données devraient être communiquées entre des nœuds finis, au

lieu d'être diffusées à tous les nœuds.

1.7. Percée en attente pour la communication de l'inter-chaîne

Les systèmes de Blockchain existantes ont expérimenté la communication de l'inter-chaîne pour traiter les logiques commerciales associées. Cependant, les résultats sont encore insatisfaisants. La communication actuelle de l'inter-chaîne comprend un mécanisme centralisé et un mécanisme HTLC. Le mécanisme centralisé s'écarte de l'idée de Blockchain, ce qui entraîne un manque de confiance, une défaillance de nœud unique, un goulot d'étranglement de nœud unique et n'est applicable qu'à certains scénarios. Le mécanisme HTLC ne peut traiter que des scénarios spécifiques tels que l'échange d'actifs, et imposer des exigences strictes sur les protocoles et Protocoles de Consensus des chaînes communicantes. Et la mise en œuvre d'un tel mécanisme est généralement complexe. Par conséquent, il est impératif de résoudre les deux problèmes critiques, c'est-à-dire. La compatibilité du Protocole et la compatibilité de format d'échange de données

2. Principaux objectifs de Ælf

2.1. Un système d'exploitation hautement personnalisable pour une utilisation commerciale

Nous envisageons Ælf comme un système d'exploitation hautement efficace et personnalisable et deviendra le "système Linux" dans la communauté de Blockchain. Prenez Linux à titre d'exemple, Le Linux Noyau et diverses versions de Linux constituent la grande famille de Linux. Le Linux Noyau résout les parties les plus fondamentales, critiques et chronophages, permettant à d'autres développeurs de créer des systèmes personnalisés en fonction du scénario de l'application et des besoins du client. Cela fait le système d'exploitation serveur de Linux le plus populaire, prenant en charge toutes sortes d'industries.

La même idée a été incorporée dans le design de Ælf. Premièrement, nous définissons et implémentons Ælf Noyau qui inclut les fonctions fondamentales d'un système de Blockchain, C'est à dire le système minimum viable de Blockchain. Deuxièmement, nous développons un «shell» en tant qu'interface interactive de base avec le Cœur. Les utilisateurs peuvent soit utiliser le système d'exploitation de Blockchain complet, soit développer rapidement un système d'exploitation personnalisé basé sur le Cœur en redéfinissant le Cœur via les interfaces.

2.2. Interaction de l’inter-Chaîne

Ælf interagira avec Bitcoin, Ethereum et d'autres systèmes de Blockchain. L'interaction de l’inter-chaîne avec les chaînes principales sera réalisée via la messagerie. Et il formera également une multi-niveaux structure endogène de l’inter-chaîne basée sur l'interaction de l’inter-chaîne, afin de partager les actifs numériques, les utilisateurs et les informations.

2.3. Amélioration des performances

Dans l'architecture traditionnelle de l’informatique, la structure distribuée est la solution populaire pour limiter les capacités de désengorgement. Le système de Blockchain doit également prendre en charge le traitement parallèle distribué, par exemple. traitement parallèle de plusieurs transactions avec des données non concurrentes pour améliorer l'efficacité des transactions. En outre, lorsqu'une chaîne est devenue trop complexe pour être traitée efficacement, elle doit être divisée en chaînes parallèles pour décharger le trafic.

La conception initiale de Blockchain efficace devrait se concentrer sur la résolution de scénarios spécifiques d’affaires plutôt que sur la combinaison de tous les Contract Intelligent sur une seule chaîne. Afin de fournir une performance optimale en fonction des besoins de l'entreprise, la chaîne doit fournir une structure efficace et personnalisée de données, une logique de Contrat Intelligent et un protocole de consensus spécifiquement pour l'objectif ciblé. En faisant cela, les composants et les données de la Chaîne seront beaucoup plus simples et faciles à gérer.

De plus, Ælf peut définir le mécanisme de déclenchement de l'instantané dans le système. Après un cycle défini, il prend un instantané des données actuelles et ajuste les données détaillées de transaction. Un nouveau bloc Genèse comprendra toutes les transactions subséquentes. Cette idée a été adoptée dans l'architecture de base de données informatique traditionnelle pour alléger l'inflation du système.

2.4. Mise à jour du Protocole

Selon la Genèse de Blockchain, le mécanisme de vote et celui de mise à jour doivent être clairement définis. Avec l'introduction du Protocole de Consensus pour inclure de nouvelles fonctionnalités à l'avenir, il évite l'impasse et le différend sur la mise à jour du Protocole.

2.5. Module de Chaîne Privée

Un nombre considérable d'entreprises est intéressé à la Chaîne Privée pour tirer parti de l'avantage de la technologie de Blockchain. Ces Chaînes privées existent généralement isolément sans aucun lien avec un écosystème externe ou d'autres entreprises. Nous fournissons un modèle similaire au service de cloud en Amazon "AMI", dans lequel les utilisateurs peuvent créer rapidement une Chaîne indépendante en utilisant le module de Chaîne Privée et en obtenir la pleine propriété.

3. Approches de base pour réaliser le système de Ælf

3.1. Améliorations de performance

Le principe de base de Ælf est de résoudre des problèmes techniques pratiques en utilisant des solutions qui ont déjà été testées. Au lieu d ' "optimiser" les concepts de Blockchain, plus attention est accordée à fournir une configuration mature pour l'exécution stable des applications métier.

Quelques idées d'amélioration de la performance explorées aujourd'hui:

La plupart des solutions de fragmentation de Blockchain sont mises en œuvre en divisant un consensus unique en plusieurs sous-consensus. Donc, fondamentalement, le consensus dans son ensemble est divisé, laissant plusieurs groupes sous-consensus plus faciles à attaquer qu'un seul. Les personnes peuvent augmenter le caractère aléatoire pour compliquer le chemin de routage, mais cela affectera la spécialisation du nœud minier.

Le nœud d'extraction de PoW a considérablement diminué à mesure que de plus en plus de bassins miniers les ont remplacés par un système de registre spécialisé. Ces bassins sont capables d'assurer l'efficacité de l'exploitation minière et la diffusion en temps opportun, ce qui ralentit la vitesse de formation du bloc et le maintient stable. En tirant parti des expériences de l'industrie informatique, les pools miniers ont abandonné l'utilisation de strandard du logiciel officiel de nœud, mais en agrégeant la puissance de calcul via l'équilibrage de charge et en exécutant des contrats intelligents de manière parallèle asynchrone, place globalement ses propres nœuds pour améliorer l'efficacité de la diffusion.. Cependant, la performance des bassins miniers est encore limitée par les différences techniques utilisées dans le bassin, et par le fait que les nœuds sont tous conçus de manière égale, et également limités par le procotol lui-même. Ainsi, la mise à niveau d'un seul nœud ne conduit pas à l'amélioration de l'ensemble du réseau

Voici les nœuds de la logique de Ælf: dans Ælf sont catégorisés en fonction de leurs rôles; ceux qui fournissent des services standard sur les clusters sont open-sourced et travaillentà travers le DPoS pour parvenir à un consensus de la chaîne principale. Les nœuds d'extraction délégués sont en mesure de protéger les Chaînes Latérales au maximum et de partager le fort consensus de la Chaîne Principale. Cette méthode augmente la pression pour chaque délégué, mais améliorera l'efficacité au fur et à mesure de l'ajout de Chaînes Latérales, car les nœuds déléguée d'exploration peuvent fonctionner en clusters. Les Chaînes Latérales sont indépendantes les unes des autres, ainsi une Chaîne Latérale supplémentaire augmentera l'efficacité de l'ensemble du système. De plus, l'efficacité de chaque Chaîne Latérale bénéficiera également du traitement parallèle.

3.2. Séparation des ressources

Pour protéger Contrats Intelligents des interférences mutuelles inutiles et maintenir leur fonctionnement stable sur Blockchain, Ælf abandonne une solution à one-chain-fits-all chaîne unique et conçoit une Blockchain publique qui est capable d'assurer le bon fonctionnement de chaque contrat.

Ælf envisage une plate-forme de l’informatique en nuage similaire à AWS. Aucune entreprise ne voudrait être dérangée par d'autres entreprises. Par exemple, les transactions sur le marché futur ne seront pas perturbées par le trafic généré par le Vendredi Noir. Cependant, cette interférence apparemment impossible est

généralement vue dans le domaine de Blockchain. Le principal obstacle prévenant donc l'application de la technologie de Blockchain dans les cas réels réside dans sa conception initiale.

3.3. Structure de la Gouvernance

En raison de limitations historiques, la structure de gouvernance actuelle de Blockchain est souvent mal définie lors de sa création. Ce problème devient plus proéminent lorsqu'il y a une majeure mise à niveau fonctionnelle ou une stagnation causée par des bogues. Par exemple, Bitcoin, est coincé dans les problèmes de mise à l'échelle pour plus de deux ans et finalement fourchu; les différences sur l'incidence DAO entre la communauté Etheruem et la fondation ont conduit à la naissance de l'ETC. Par conséquent, nous clarifions la méthode d'orientation de Ælf avant que les utilisateurs entrent dans le monde de Ælf:

Nous reconnaissons le fait que les détenteurs de Tokens d'authentification à Ælf ont le plus grand droit dans l'avenir de Ælf, et les intérêts des détenteurs de Tokens d'authentification sont liés au destin de Ælf, en particulier ceux avec des Tokens immobilisés à long terme.

3.3.1. Ressemblance de la Démocratie Représentative

L'un des principes clés de Ælf est de désigner des nœuds spécialisés pour effectuer des tâches spécialisées. En Ælf, les décisions vitales seront prises à travers un mécanisme qui ressemble à la démocratie représentative. Les nœuds délégués doivent avoir suffisamment de votes d'autres parties prenantes pour participer à la gouvernance de Ælf. Les nœuds miniers constituent dans une certaine mesure la santé du système de Ælf, de sorte que ces nœuds sont responsables d'être un registre, de distribuer des bonus et des valeurs de feedback aux parties prenantes qui les ont confiées via des Contrats Intelligents.

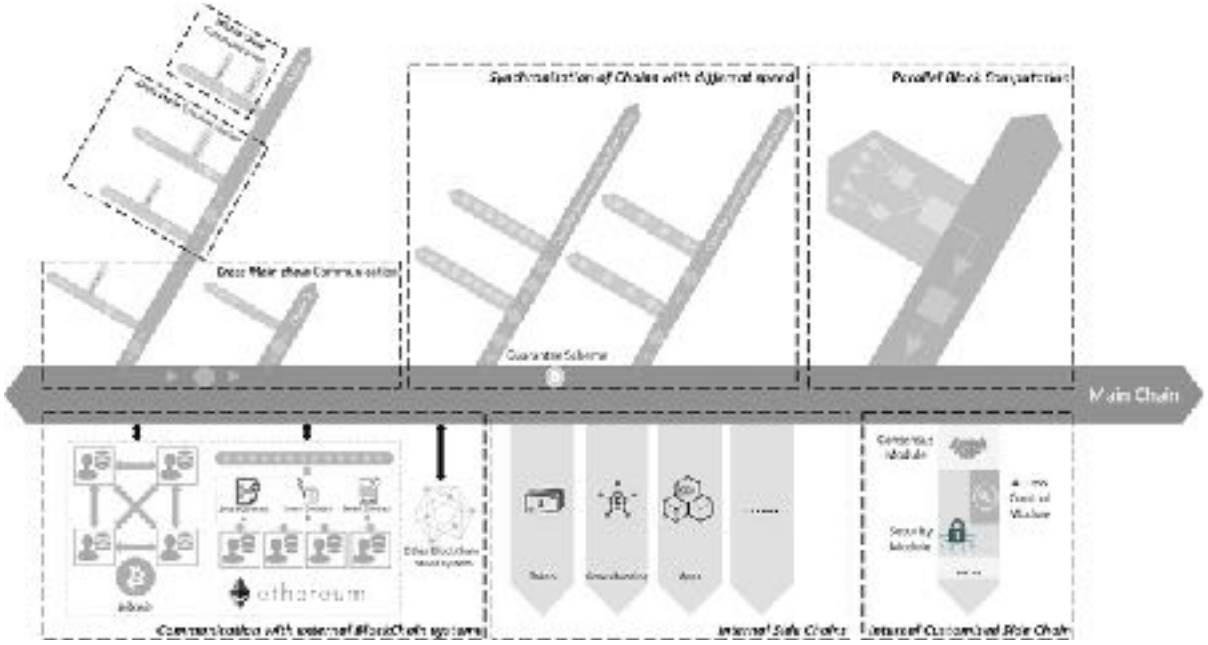
3.3.2. Exercice du Pouvoir par les Délégués

Foundation réalise sa gouvernance en soumettant le code source et en déléguant les nœuds miniers à réviser et à voter. Le processus se déroule comme suit: Les membres de la fondation fournissent un code source ouvert et soumettent de nouvelles fonctionnalités. Ensuite, les délégués choisissent des caractéristiques spécifiques à incorporer en fonction de leurs besoins. Si une caractéristique est adoptée par suffisamment de délégués, elle obtient l'approbation de l'ensemble du système.

4. Système de Ælf

4.1. Architecture de Ælf

Nous présentons le Ælf composé d'une Chaîne Principale et de plusieurs Chaînes Latérales attachées à la Chaîne Principale (Figure 4.1). La différence par rapport au système traditionnel à Chaîne Unique est que Ælf est un «écosystème ramifié» où la Chaîne Principale fonctionne comme l'épine dorsale du système et se connecte à plusieurs Chaînes Latérales (peut être même plusieurs couches).



Within chain communication	**la communication de l'intérieur de la chaîne**
Cross chain communication	**Communication de l'interchaîne**
Chain 1	**Chaîne 1**
Cross main chain	**L'inter-chaîne principale**
Chain 2	**Chaîne 2**
Smart contract	**Contrat Intelligent**
Communication with external Blockchain systems	**Communication avec les systèmesexternes de Blockchain**
Other Blockchain based system	**Autre système basé sur Blockchain**

Synchronisation of chains with different speed	**Synchronisation de chaînes à différentes vitesses**
Main chain	**Chaîne principale**
Ganrantee scheme	**Système de garantie**
Token	**Token**
Crownedfunding	**Crownedfunding**
Apps	**Apps**
Internal side chains	**Internes Chaînes latérales**
Parallel block communication	**Communication de blocs parallèles**

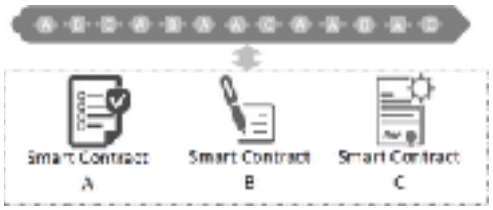
Consensus module	**Module de consensus**
Security module	**Module de sécurité**
Access control module	**Module de contrôle d'accès**
Internal customised side chain	**interne Chaîne latérale personnalisée**

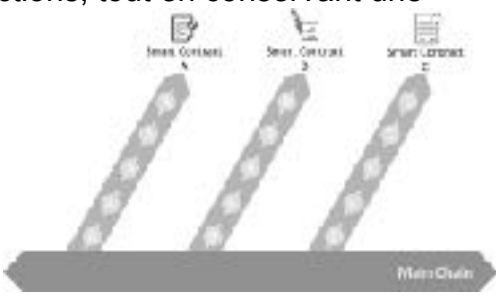
Figure 4.1: Vue d'ensemble de la structure de Ælf

Ælf se connecte à Bitcoin, Ethereum et à d'autres systèmes Blockchain via un adaptateur, afin d'être compatible avec les éco-systèmes populaires existants. Les chaînes latérales incluent le système intégrées au Ælf et d'autres chaînes générées en fonction du système d'exploitation de Ælf ou du Ælf Noyau. La Chaîne Principale interagit avec les chaînes latérales par l'indexation dynamique de Chaîne Latérale.

4.1.1. Une Chaîne Un Contrat

Par rapport à la structure traditionnelle d'«une chaîne à tous les types de contrats», Ælf impose «une chaîne à un type de contrat». Comme l'illustre dans la figure 4.2 (b), chaque Chaîne se consacre à la transaction d'un type et résout le problème d'entreprise d'un type. Cela rend toute la structure et les données plus simples et bien plus adaptées aux besoins commerciaux. En ajoutant de nouvelles Chaînes Latérales à Ælf, Ælf sera doté de nouvelles fonctions, tout en conservant une structure «facile à gérer».





(a) une chaîne à tout type de contrat **(b) en Ælf, une chaîne à un type de contrat**

Smart contract	**Contrat intelligent**
Main chain	**Chaîne principale**

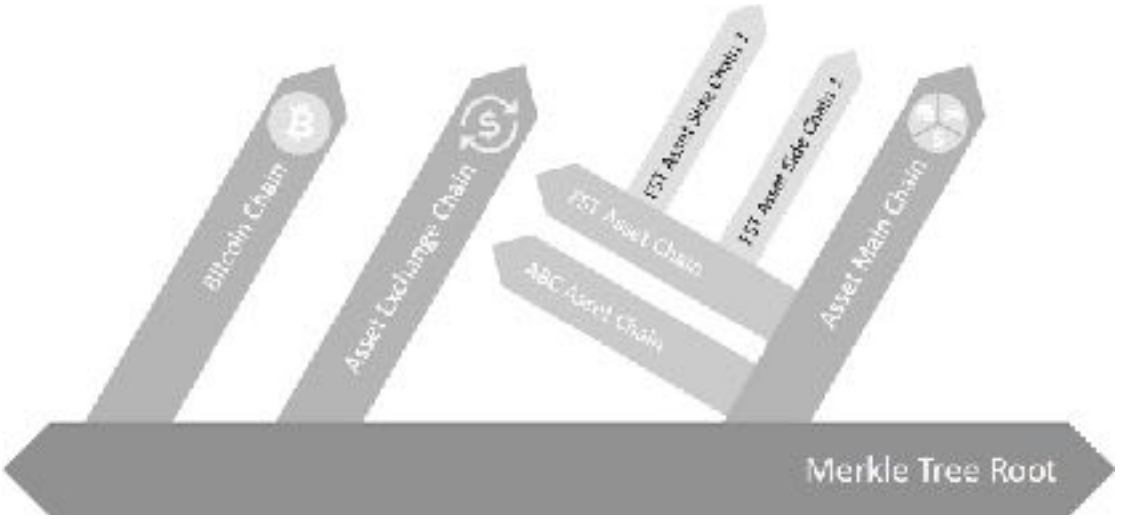
Figure 4.2: Une Chaînes avec une structure complexe de données

4.1.2. Indexation Dynamique de la Chaîne Latérale

Ælf est un système dynamique, où toutes les Chaînes Latérales sont attachées à la Chaîne Principale. La Chaîne Principale contient l'index des limites du système (l'enregistrement de ce que les chaînes latérales sont attachées). Ils interagissent les uns des autres via la Chaîne Principale sous la forme d'arbre de Merkle et la vérification par une entrée d'information externe. Ainsi, les Chaînes Latérales n'interagissent pas directement, ce qui permet les Chaînes Latérales d'ajouter ou d'exclure dans système de Ælf.

4.1.3. "Branche d'arbre" Extension de la Chaîne Latérale

Comme l'illustre dans la Figure 4.3, Ælf définit une «structure de Chaîne Principale et de Chaîne Latérale». Théoriquement, toute Chaîne Latérale peut également être connectée avec quelques sub Chains--- ?sous-chaînes ? en dessous, agissant comme une «Chaîne Principale» dans une partie du système. Cela crée la structure des branches dans le système qui permet à Ælf de s'étendre horizontalement et verticalement. Cette idée est similaire au partitionnement et au sharding dans l'architecture de base de données. Il permet à chaque fragment d'exécuter des fonctions spécifiques et lorsqu'un fragment est trop volumineux pour gérer, il peut être



décomposé en plusieurs parties. En Ælf, cela correspond aux Chaînes Latérales.

Bitcoin chain	Chaîne de Bitcoin
Asset exchange chain	Chaîne d'échange d'actifs
Asset chain	Chaîne d'actifs
Asset side chain	Chaîne latérale d'actifs
Asset main chain	Chaîne principale d'actifs
Racine d’Arbre de Merkle	Racine d'arbre de Merkle

Figure 4.3: Structure de la Chaîne Latérale multicouche

2. Ælf Chaîne Principale

La Chaîne Principale est Blockchain exécutée par Ælf OS, agissant comme l'épine dorsale de tout le système. La Chaîne Principale se compose d'un système

d’indexation de la Chaîne Latérale, un système de Token et d'un Protocole de consensus DPoS.

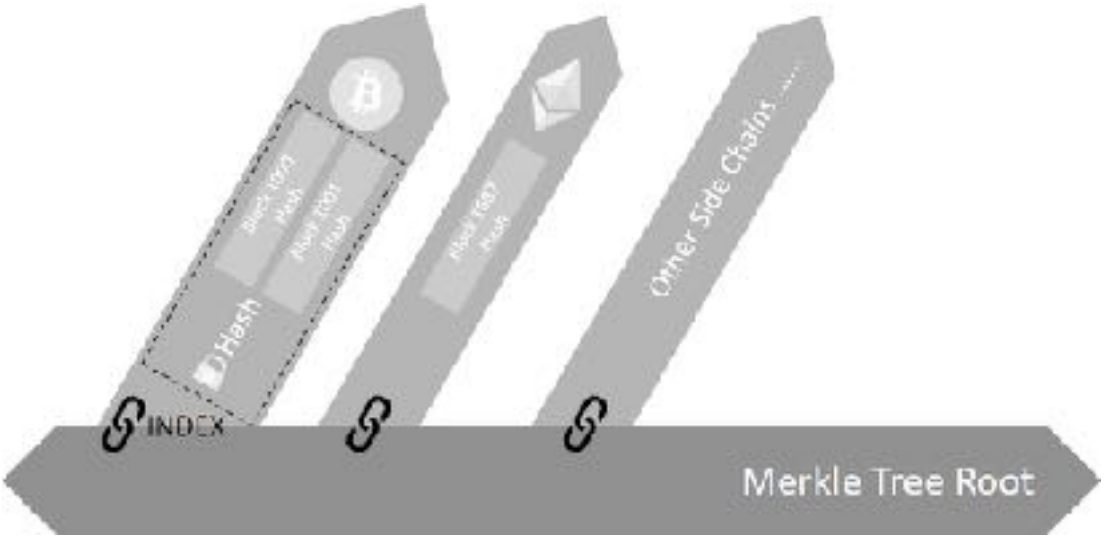
2.1. Système d'indexation de la Chaîne Latérale

Le système d'indexation de la Chaîne Latérale relie toutes les Chaînes au sein de l'éco-système de Ælf. Ælf indexe deux types de chaînes:

- Chaînes externes de haute importance, peuvent être utilisées pour étendre la limite de Ælf, par exemple, Bitcoin, Ethereum
- Chaînes Latérales internes fonctionnant sous le système d'exploitation de Ælf, ce qui contribue à l'économie du système de Ælf en utilisant Ælf Token

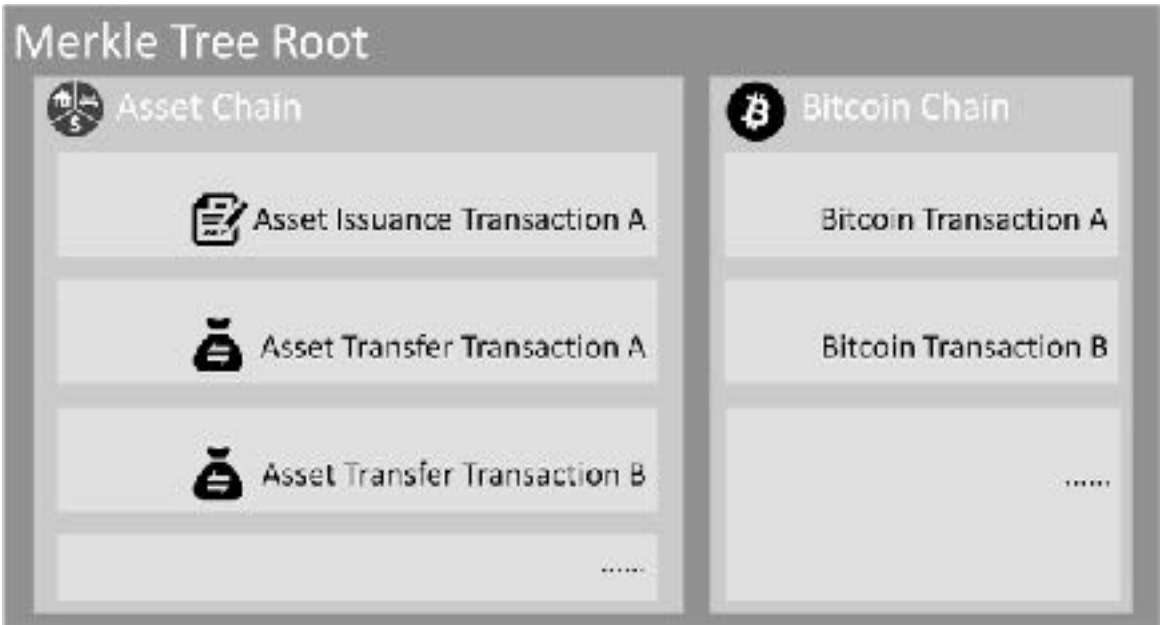
L'indexation de la Chaîne Latérale fonctionne selon les étapes suivantes:

- Les nœuds de la Chaîne Principale lisent les informations des Chaînes Latérales et forment un Arbre de Merkle
- La tête du nouveau Bloc enregistre la Racine d’Arbre de Merkle. Comme illustré dans la figure 4.4, si nous voulons confirmer la transaction TX1 sur le 1000e bloc de BTC, nous avons seulement besoin de prouver l'existence de l'Arbre de Merkle du 1000e bloc de BTC tel qu'il est stocké sur la Racine d’Arbre de Merkle de la Chaîne Principale, et Merkle preuve de TX1 sur le 1000e bloc de BTC via la messagerie. Cette approche fonctionne également pour d'autres chaînes telles que Ethereum tant qu'une Racine d’Arbre de Merkle est formée.



Blick 1000 Hash	Blick 1000 hachage
Hash	hachage
Index	Index
Other side chains	Autres chaînes latérales
Racine d’Arbre de Merkle	Racine d'arbre de Merkle

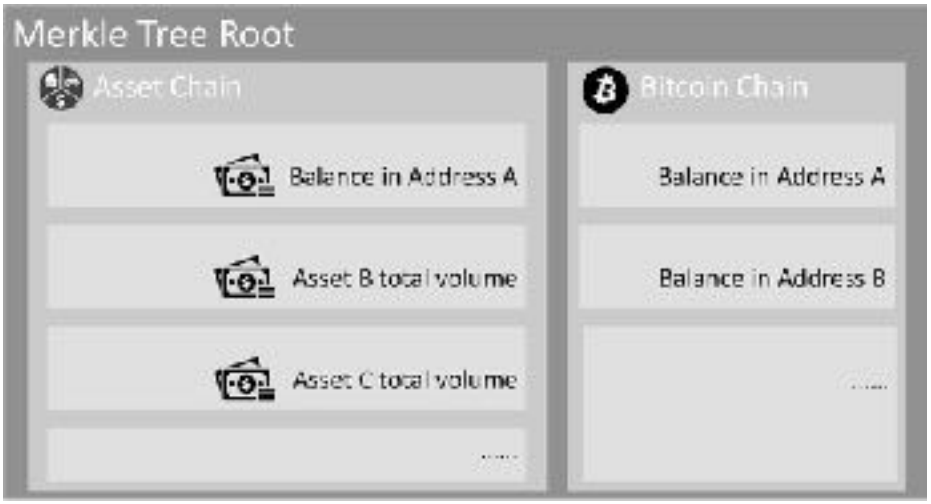
Figure 4.4: Indexation de la Chaîne Latérale



Afin d'améliorer l'efficacité de la vérification, nous suggérons d'étendre la structure d'un Arbre de Merkle, y compris non seulement les hachages de Bloc, mais aussi la Racine d’Arbre de Merkle de transactions dans la Figure 4.5 et les états de la figure 4.6.

Racine d’Arbre de Merkle	Racine d'arbre de Merkle
Asset chain	Chaîne d'actifs
Asset issuance transaction A	Transaction d'assurance d'actifs A
Asset transfer transaction A	transaction de transfert d'actifs A
Bitcoin chain	Chaîne de Bitcoin
Bitcoin transaction A	Bitcoin transaction A
Bitcoin transaction A	Bitcoin transaction A

Figure 4.5: Indexation des Transactions



Racine d'Arbre de Merkle	Racine d'Arbre de Merkle
Asset chain	Chaîne d'actifs
Balance in address a	Solde de l'adresse a
Asset b total volume	Volume total de l'actif b
Asset c total volume	Volume total de l'actif c
Bitcoin chain	Chaîne de Bitcoin
Balance in address a	Solde de l'adresse a
Balance in address b	Solde de l'adresse b

Figure 4.6: Indexation d'état

Une question clé à discuter est le calendrier de l'indexation de la Chaîne Principale à la Chaîne Latérale. Si la Chaîne Principale indexe fréquemment une Chaîne Latérale avec une probabilité élevée de fourche, elle gaspille des efforts pour indexer les blocs orphelins. Par conséquent, nous suggérons une stratégie différente d'indexation pour chaque Chaîne Latérale en fonction de ses caractéristiques et cela peut être défini dans le système. Stratégie d'indexation pour Blockchain similaire à Bitcoin peut être après une minute d'un bloc est formé. Cela a été prouvé statistiquement comme un bloc peut être confirmé pas un orphelin après une minute de formation. Au sein de Ælf, si une Chaîne Latérale et la Chaîne Principale adoptent la fusion de l'exploitation minière, l'indexation en temps réel peut être effectuée en raison des mêmes mineurs.

Main chain	Chaîne principale
Index	Index
Side chain	Chaîne latérale
Different block generation speed	Vitesse de génération de blocs différente
Index a&b due to different speed	Index a & b en raison de la vitesse différente
Forked side chain	Chaîne latérale fourchue
Fork	Fourchette
Orphaned block	Bloc orphelin

Index d&e due to different speed	Index d & e en raison de la vitesse différente

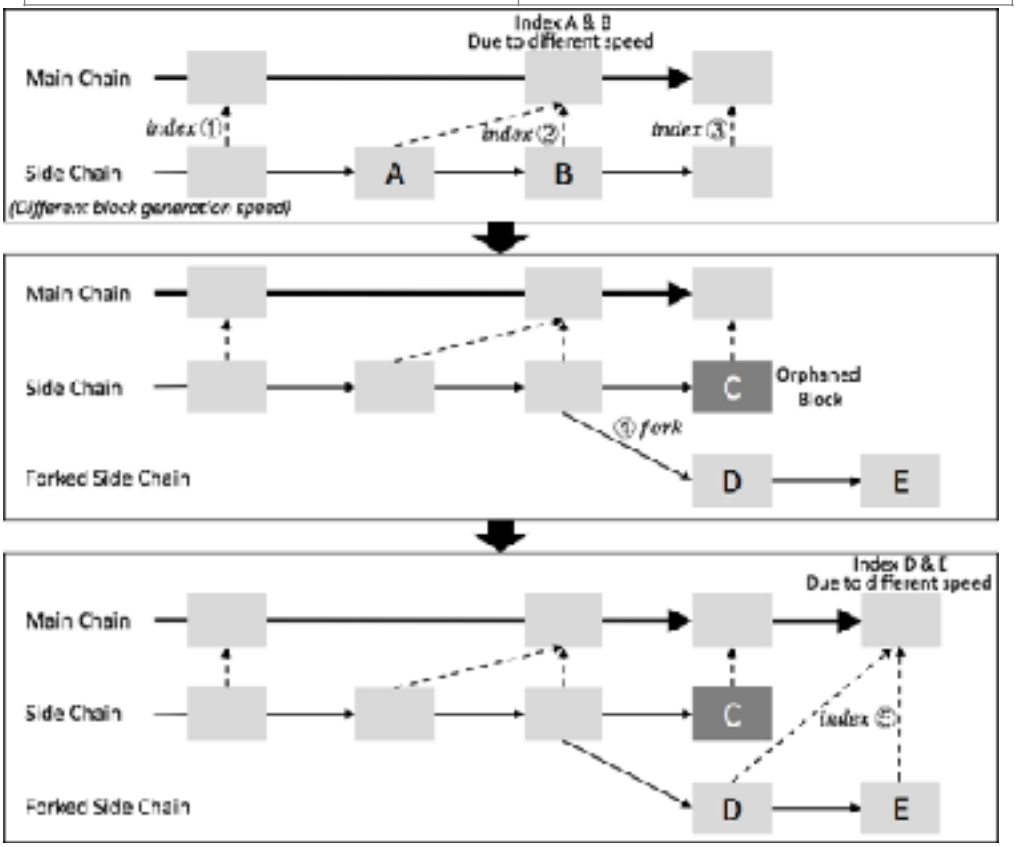


Figure 4.7 Chronométrage de l'indexation

2.2. Système de ÆIf Token

ÆIf Token incite un comportement honnête dans le système. Toutes les Chaînes Latérales acceptent les ÆIf Token comme stockage de valeur et moyens de transfert de valeur. Il peut être transféré à travers des Chaînes qui acceptent ÆIf Token.

Quand une Chaîne Latérale s'applique à être indexée par la Chaîne Principale, elle reçoit des Tokens bloqués de la Chaîne Principale. Lorsque la Chaîne Latérale reçoit des frais de transaction, elle partage partiellement avec les mineurs de la chaîne principale. Lorsque la Chaîne Principale constate que l'indexation d'une Chaîne Latérale est économiquement défavorable à son profit, la Chaîne Principale a le droit de mettre fin à l'indexation, ou de permettre la concurrence de deux Chaînes Latérales offrant les mêmes services.

2.3. Protocole de Consensus

Un mécanisme stable et efficace de formation de blocs est la base du système de ÆIf. Le fonctionnement et la maintenance de ÆIf est plus compliqué que Bitcoin et Ethereum. Cela est dû au fait que la formation de Blocs ÆIf nécessite que la Chaîne Principale enregistre les informations provenant des Chaînes Latérales, et que ÆIf est conçu pour fournir des services d'entreprise basés sur le nuage dans une structure plus complexe. De plus, les mineurs doivent mettre à jour les informations de plusieurs chaînes en parallèle. La Chaîne Principale adoptera le DPoS pour assurer la haute fréquence et la prévisibilité de la formation de Bloc, afin d'améliorer l'expérience de l'utilisateur.

2.4. DPoS

ÆIf délègue 2N+1 nœuds miniers. N commence par 8, et augmente 1 chaque année. Ces nœuds du système de ÆIf appliquent toutes les règles de consensus de ÆIf.

Le but de ces nœuds miniers délégués est de permettre le relais de transaction, la confirmation de transaction, les blocs d'empaquetage et le transfert de données. Comme ÆIf adopte une architecture de multi- Chaînes Latérales, les nœuds miniers doivent fonctionner en tant que mineurs pour certaines Chaînes Latérales.

2N + 2 nœuds feront l'objet d'un calcul aléatoire d'ordre chaque semaine. Le processus de Randomisation est illustré comme suit:

ÆIf se déroule sur le long de la ligne de temps avec des unités de traitement que nous appelons « tour » (flèche horizontale dans la Figure 4.8 et la Figure 4.9). Dans chaque tour, un nœud minier produira un bloc chaque fois, tandis qu'un nœud aura une transaction supplémentaire à la fin de chaque tour (flèche verticale dans la figure 4.9).

Chaque nœud minier $node$) possède trois propriétés principales dans un tour spécifique t): (1) Clé privée, $in_{node(i)}$, qui est une valeur entrée du nœud minier et qui est gardée en privé par le nœud minier lui-même en tour t. Il sera publié au public après que toutes les générations de blocs en tour t auront été complétée; (2) Clé publique, $out_{node(i)}$, qui est la valeur de $in_{node(i)}$. Chaque nœud du réseau de ÆIf peut rechercher cette valeur à tout moment; (3) Signature, $sig_{node(i)}$, qui est une valeur générée par le nœud minier lui-même au premier tour. Après le premier tour, il

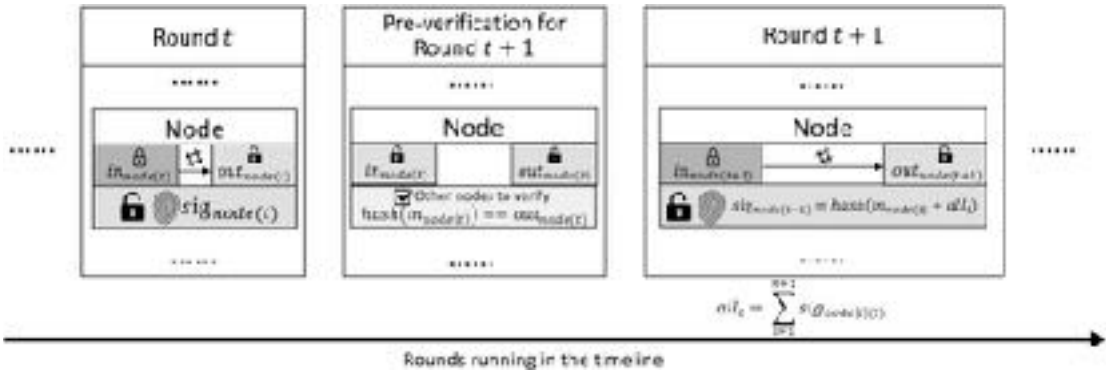
ne peut être calculé qu'après la fin du tour précédent. Il est utilisé comme signature de ce nœud minier dans ce tour et il est également ouvert au public à tout moment comme le $out_{node(i)}$. Voir la Figure 2.1 pour plus de détails.

node	nœud
In node	Le nœud d'entrée
Out node	Le nœud de sortie
sig node	Le sig nœud

.

Il y a deux processus principaux dans le DPoS: (1) Pré-vérification; et (2) calcul de l'ordre à chaque tour.

Pré-vérification (Fig 4.8): avant qu'un nœud commence sa génération de bloc en rond $t+1$), il faut vérifier son état en rond t). En rond $t+1$, $in_{node(i)}$ est déjà publié au public, et $out_{node(i)}$ peut être interrogé à tout moment. Donc, pour vérifier le statut de $node$ in rond t, les autres nœuds peuvent vérifier $hash(in_{node(i)}) == out_{node(i)}$.



Round	Tour
Pre-verification for round	Pré-vérification pour tour
Node	Nœud
In node	Le nœud d'entrée
Out node	Le nœud de sortie
Sig node	Sig nœud
Other nodes to verify hash	Autres nœuds pour vérifier le hachage

Figure 4.8 Pré-vérification.

Calcul de l'ordre (Fig 4.9): Dans la Fig 4.9, nous avons utilisé 4 nœuds miniers comme exemple pour expliquer notre stratégie de calcul d'ordre. Dans chaque tour N les nœuds miniers ont $N+1$ génération de bloc. Au premier tour (Tour 1 dans la Fig 4.9), l'ordre des générations de blocs ainsi que la signaturesig) pour chaque nœud sont totalement arbitraires. Au second tour (Tour 2 dans la Fig 4.9), les générations de blocs sont de nouveau arbitrairement ordonnées. Cependant, à partir $sig_{node(i+1)} - hash(in_{node(i)} + all_t)$
du deuxième tour, la signature sera calculée par

où

$$all_t = \sum_{i=1}^{n-1} sig_{node[i](t)}$$

ici, $node[i](t)$ signifie le nœud traitant la i^{th} transaction en tour t.

$$sig_{node(i)} mod(N) = \begin{cases} 0, & first\ place \\ 1, & second\ place \\ 2, & third\ place \\ \cdots & \\ n-1, & n^{th}\ place \end{cases}$$

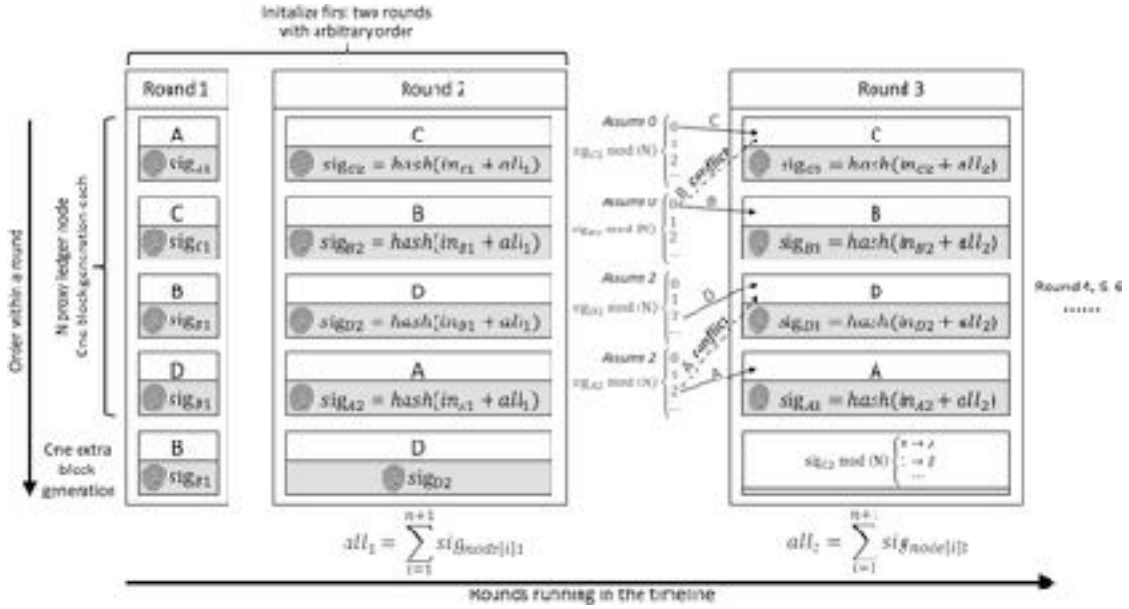
Dans tour 3, la commande dans un tour est générée à partir de la commande et de la signature du nœud du tour précédent. En tour^{t+1}, nous traversons la signature des nœuds au tour ^{t} à l'ordre. L'ordre d'un nœud $^{t+1}$ est calculé par

Pour les cas de conflit, c'est-à-dire les résultats pointant vers des endroits qui ne sont pas vides, nous orientons le nœud vers l'emplacement disponible suivant. Si le nœud est en conflit àl'endroit ^{ta}, nous allons commencer à trouver l'endroit disponible à partir de la première place.

Sig node	**Sig nœud**
Mod	mod
First place	première place
Second place	deuxième place
Third place	troisième place
Nth place	n^{ème} place

Le nœud pour traiter la transaction supplémentaire est calculé à partir de la signature du nœud à la première place du tour précédent.

$$sig_{node[0]t}mod(N) = \begin{cases} 0, & A \\ 1, & B \\ 2, & C \\ \cdots \end{cases}$$



Initialize first two round with arbitrary order	**Initialiser les premiers deux tours avec un ordre arbitraire**
Round	**Tour**
Order within a round	**ordre dans un tour**
N proxy ledger node	**n proxy nœud de registre**
One block generation each	**Une génération de blocs chacun**
One extra block generation	**Une génération de bloc supplémentaire**
Sig	**Sig**
Has	
Sig node	**Sig nœud**
assume	**assume**
Rounds running in the timeline	**Tours en cours d'exécution dans la chronologie**

Figure 4.9 Détails du calcul de l'ordre pour les Premiers Trois Tours

est décidé par: (1) toutes les signatures du tour précédent $t-1$; (1) la valeur de lui-même en tour $t-1$; (3) quel nœud génère le bloc supplémentaire. Donc, il ne peut être calculé après tour précédent $t-1$ complété. De plus, comme il a besoin de toutes les signatures du tour précédent et que la valeur in est entrée indépendamment par chaque nœud, il n'y a aucun moyen de contrôler la commande. La génération d'un bloc supplémentaire est utilisée pour augmenter le caractère aléatoire. En général, nous créons un système aléatoire en s'appuyant sur des entrées supplémentaires de l'extérieur. Baser sur l'hypothèse qu'aucun nœud ne peut connaître tous les autres entrées des nœuds dans un tour spécifique, aucun nœud ne

pourrait contrôler l'ordre.

Si un nœud ne peut pas générer un bloc en tour t, il ne peut pas non plus entrer son in pour ce tour. Dans ce cas, le précédent in sera utilisé. Puisque tous les nœuds miniers sont considérés comme des nœuds fiables, une telle situation ne devrait pas arriver trop. Même cette situation s'est produite, la stratégie mentionnée est suffisante pour y faire face de manière équitable.

Chaque nœud n'a qu'un certain T en second pour traiter les transactions. Dans la condition de réseau actuelle, T = 4 est une considération raisonnable, ce qui signifie que chaque nœud n'a que 4 secondes pour traiter les transactions et soumettre le résultat au réseau. Tout délégué qui ne parvient pas à soumettre dans les 4 secondes est considéré abandonner ce bloc. Si un délégué a échoué deux fois de suite, il y aura une période de fenêtre calculée comme W heures ($W = 2^N$, N représente le nombre d'échec) pour ce nœud.

Dans la conception systématique, ÆIf définit qu'un seul nœud génère des blocs dans une certaine période. Par conséquent, il est peu probable qu'un fork se produise dans un environnement où les nœuds miniers travaillent sous une bonne connectivité. Si plusieurs groupes de nœuds orphelins se produisent en raison de problèmes de réseau, le système adoptera la chaîne la plus longue en raison du fait

que provient probablement du groupe de nœuds orphelins avec le plus grand nombre de nœuds minier. Si un nœud vicieux exploite dans deux fourchus de Blockchain simultanément pour attaquer le réseau, ce nœud devrait être exclu de l'ensemble du réseau.

Les nœuds minier de DPoS sont élus d'une manière qui ressemble à la démocratie représentative. Les nœuds élus décident comment distribuer le bonus aux autres nœuds miniers et aux parties prenantes. Ce mécanisme sera discuté plus en détail dans le chapitre suivant.

2.5. Confirmation des Transactions

Comparé au système actuel de Blockchain, Ælf a une confirmation plus rapide et plus prévisible. Contrairement à PoW, DPoS ne doit pas empaqueter les hachages à plusieurs reprises. Ainsi, le temps nécessaire à un nœud d'extraction pour l'empaquetage d'un bloc est stable et peut être contrôlé dans T (4 secondes).

Ælf recommande: une confirmation rapide que acceptée par 5 blocs est utilisée pour les transactions générales; celle acceptée par 15 blocs est utilisée pour des transactions substantielles. Ainsi, une transaction générale sera confirmée dans 20 secondes, une transaction substantielle, dans 60 secondes.

Notez, c'est une recommandation conservatrice. Bitcoin recommande une confirmation de 6 blocs, mais de nombreux utilisateurs utilisent seulement un ou deux blocs pour confirmer. Les utilisateurs expérimentés sont autorisés à observer et à collecter des données de leur propre Blockchain et à adapter un temps de confirmation pour eux-mêmes en fonction du temps de traitement moyen par leurs propres nœuds miniers, et celui par l'ensemble du réseau.

3. Chaîne Latérale de Ælf

Les chaînes indexées par la Chaîne Principale de Ælf sont considérées comme des Chaînes Latérales. Comme mentionné précédemment, il est recommandé que chaque Chaîne Latérale soit conçue pour gérer un type spécifique de transaction (Figure 4.8).

Lorsqu'une nouvelle Chaîne Latérale est créée via Ælf OS, il est recommandé de la fusion de l'exploitation minière avec la Chaîne Principale et d'établir ses propres Protocoles de Consensus. Pour contribuer à l'éco-système de Ælf, Chaînes Latérales doivent réserver une certaine quantité de Ælf Token et partager des frais de transaction partiels avec la Chaîne Principale.

Lorsqu'une Chaîne Latérale doit vérifier les informations d'une autre Chaîne Latérale, elle doit inclure les informations d'en-tête de bloc de la Chaîne Principale de Ælf. Les Chaînes Latérales n'interagissent pas directement les unes avec les autres. La vérification est effectuée à l'aide de la Racine d'Arbre de Merkle fournie par la Chaîne Principale.

Chain 1	**Chaîne1**
Contains	**Contient**
Merkle tree root of main block 998,999 and 1000	**Racine d’Arbre de Merkle du bloc principal 998,999 et 1000**
Transaction verification from block 900	**Vérification de transaction du bloc 900**
Side chain transaction verification	**Vérification de transaction de chaîne latérale**
Chain 2	**Chaîne2**

Figure 4.8: Interaction de Messagerie entre deux ChaînesLatérales

Il est très compliqué d'obtenir des informations d'état à partir de systèmes UTXO tels que Bitcoin, par exemple le solde disponible à partir d'une adresse. La communication entre Chaînes peut être adressée via un adaptateur de Blockchain, où il crée un en-tête de bloc compatible incluant l'Arbre de Merkle avec Bitcoin. Ælf adopte un tel adaptateur et envisage d'établir une Chaîne Latérale entièrement compatible de Bitcoin en utilisant Ælf OS pour coopérer avec Bitcoin largement utilisé et interagir avec ses actifs.

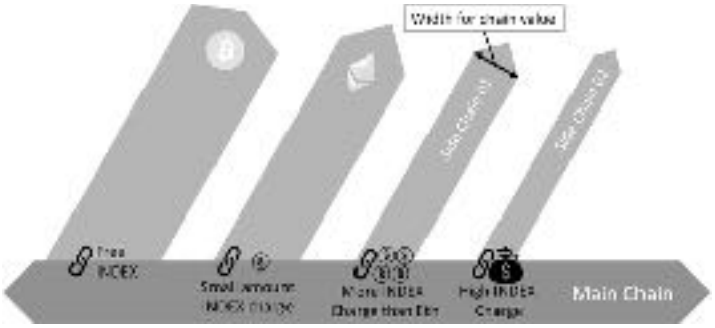
1.4. L'économie de Ælf

Une économie vertueuse jette les bases d'un éco-système durable de Ælf.

Pour le PoS et le DPoS, tout acteur peut vendre ses Tokens et quitter l'écosystème en un minimum de temps (le PoS a une certaine période de lock-up). L'un des défis auxquels sont confrontés les PoS et les DPoS est le fait que les échanges contiennent un grand nombre de Token dans le système, ce qui leur rapporte des intérêts à un coût quasiment nul.

Pour PoW, les mineurs font face à des considérations plus complexes avant de quitter. La sortie est limitée par des facteurs externes tels que le coût de l'électricité, la dépréciation des machines minières, le bail et les ressources humaines.

Ælf utilisera DPoS sur la Chaîne Principale pour inciter les grandes parties prenantes à maintenir un système stable et déploiera le PoW pour la Chaîne Latérale où l'extraction crée Ælf Token. Dans le système de Ælf, le Protocole de Consensus sur chaque Chaîne peut être personnalisé pour atteindre des objectifs spécifiques.

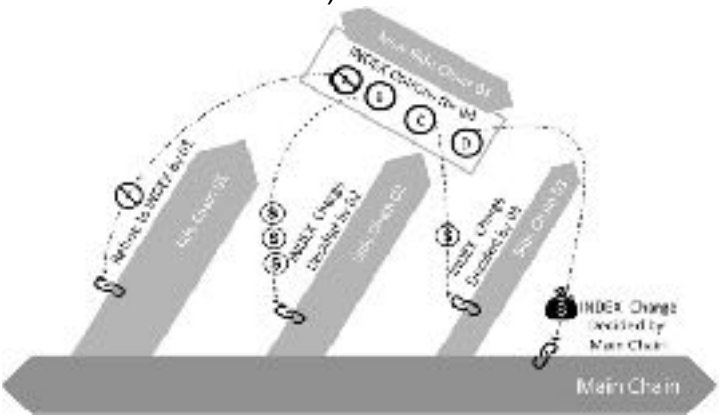


Width for chain value	**Largeur pour la valeur de chaîne**
Free index	**Index gratuit**
Small amount index charge	**Charge d'indexation de faible montant**
More index charge than eth	**Plus Charge d'indexation que d'Eth**
High index charge	**Charge élevée d'indexation**
Side chain	**Chaîne latérale**
Main chain	**Chaîne principale**

Figure 4.9: Mécanisme de tarification de l'indexation des Chaînes Latréales de Ælf

Après qu'une Chaîne Latérale est incluse par l'éco-système de Ælf, elle paiera un certain montant de frais de transaction à la chaîne principale pour l'indexation. L'IFL adopte une stratégie de frais de transaction dynamique pour refléter le niveau de contribution différent de chaque chaîne latérale à l'éco-système. Par exemple, Ælf

facturera moins de frais de transaction pour une chaîne secondaire avec une contribution élevée (par exemple, aucun frais sur l'indexation de Bitcoin pour son adoption large et les actifs associés.) D'autre part, une chaîne latérale avec peu de valeur pour l'éco-système et consommant les ressources des autres chaînes seront facturées des frais de transaction élevés).



New side chain 04	Nouvelle chaîne latérale 04
Index options for04	Options d'index pour04
Refuse to index by 01	Refus d'indexer par 01
Side chain	Chaîne latérale
Index charge decided by 02	Charge d'indexation décidés par 02
Index charge decided by 03	Charge d'indexation décidés par 03
Index charge decided by main chain	Charge d'indexation décidés par la chaîne principale
Main chain	Chaîne principale

Figure 4.10.: Indexation de la Sous-Chaîne

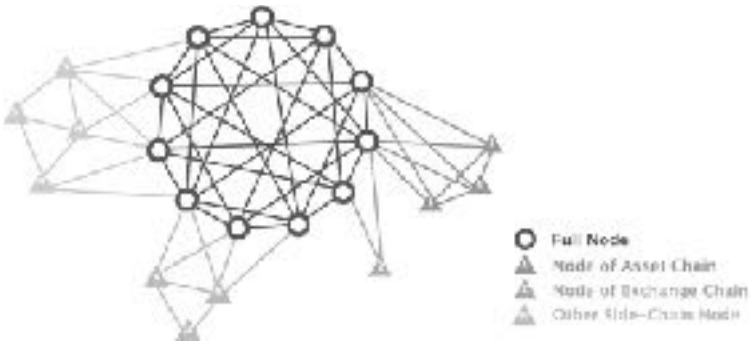
L'écosystème de chaque Chaîne Latérale vote pour déterminer sa stratégie d'indexation pour les Sous-Chaînes indépendantes de la Chaîne Principale. Sa propre stratégie inclut, mais sans s'y limiter, la portée de l'entreprise (par exemple, une chaîne d'assurance inclura seulement les Sous-Chaînes qui sont également dans le secteur de l'assurance de l'entreprise) et le système de frais des Sous-Chaînes. Toute chaîne peut également décider de ne pas inclure de Sous-Chaîne ou d'inviter activement une Chaîne à devenir une Sous-Chaîne, comme un moyen pour enrichir son écosystème. Au sein de l'écosystème de Ælf, toute chaîne peut s'appliquer pour devenir une Sous-Chaîne d'une autre Chaîne ou même plusieurs Chaînes.

1.5. Chaîne Latérale du Système Intégré à Ælf

La Topologie de Nœud de Ælf consiste en un réseau P2P interconnecté entre les Nœuds Complets de la Chaîne Principale, les nœuds légers et les nœuds de Chaînes Latérales. Les nœuds non miniers sont généralement des nœuds légers. Les nœuds de ledger sont aussi des Nœuds Complets. Les Nœuds des Chaînes Latérales sont distribués dans la Topologie de Nœud de Ælf en fonction de sa relation d'indexation avec la Chaîne Principale. Les Chaînes Latérales seront développées sous la direction de la Fondation. Nous croyons qu'il est nécessaire de construire un système comme celui-ci. Ælf ne vise pas à construire une Chaîne

Latérale en soi, mais fournira un modèle et une infrastructure de développement pour une Chaîne Latérale, et facilitera les communications entre les chaînes latérales.

Par exemple, il existe un réseau basé sur le contenu, où les utilisateurs peuvent acheter du contenu avec le Token de ce réseau. Lorsqu'un "twitter" décentralisé rejoint Ælf, Ælf aidera les utilisateurs à partager des contenus via ce réseau, à distribuer des ressources de réseau et à échanger ce Token "twitter" avec des Tokens de réseau de distribution de contenu sur un échange décentralisé.



Full node	**Nœud complet**
Node of asset chain	**Nœud de la chaîne d'actifs**
Node of exchange chain	**Nœud de la chaîne d'échange**
Other side-chain node	**Autre Nœud de chaîne latérale**

Figure 4.11: Illustration de la Topologie de Nœud de Ælf

1.5.1. Chaîne Latérale de l'Enregistrement d'informations et l'Authentification

Inscription et Authentification de l'information Chaîne Latérales crée une grande valeur pour les industries en ligne et hors ligne. Actuellement, il a été largement adopté en O2O businesses, tels que le commerce électronique, l'appellation et la livraison de l'automobile. D'énormes opportunités doivent encore être dégagées dans des entreprises telles que la chaîne d'approvisionnement, la logistique, la notation de crédit, etc., où leurs grands actifs informationnels peuvent être migrés vers cette Chaîne Latérale à l'avenir.

1.5.2. Chaîne Latérale de Propriété des Actifs Numériques

La fonction principale de cette Chaîne Latérale est de stocker les informations d'actifs numériques et de propriété du portefeuille numérique.

1.5.3. Chaîne Latérale de Distribution Initiale d'Actifs

La fonction principale de cette Chaîne Latérale est de faciliter l'initiation des actifs (First Coin Sales). Une fois la distribution terminée, les actifs seront déplacés vers la Chaîne Latérale de propriété des actifs Numériques. L'avantage est que les transactions normales ne seront pas interrompues lors d'une vente à grande échelle de pièces de monnaie.

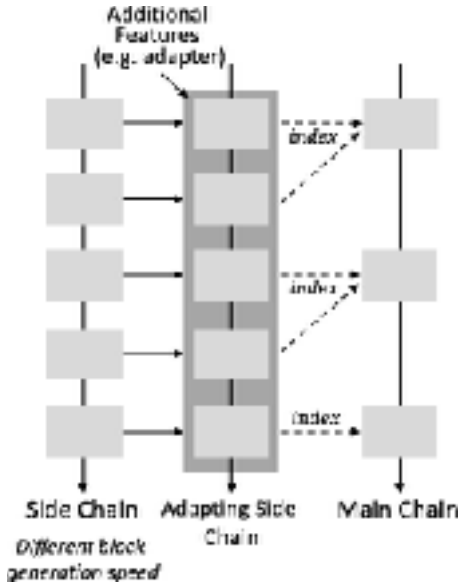
1.5.4. Chaîne Latérale d'échange Décentralisée

Une transaction décentralisée de Chaîne Latérale fonctionne comme un échange. Il permet le KYC, le transfert d'actifs, le placement / retrait et l'exécution de commande.

1.6. Optimisation de l'inter-Chaîne de Ælf

Pour les transactions transversales à différents niveaux, la chaîne principale fournit une garantie pour la chaîne la plus lente. C'est seulement un mécanisme optionnel si nécessaire. Ces deux mécanismes peuvent être une solution efficace pour améliorer la vitesse de transaction de l'inter-Chaîne de Ælf.

Les transactions de l'inter-Chaîne doivent être optimisées pour correspondre à la vitesse de formation de blocs entre les chaînes différentes. Nous concevons deux mécanismes pour résoudre ce problème. Premièrement, le mécanisme de la chaîne latérale hiérarchique. Nous classons les chaînes en différents niveaux en fonction de la vitesse de formation de blocs de la chaîne, et fournissons un module d'adaptation ou une chaîne latérale d'adaptation dédiée pour effectuer le même niveau de transactions croisées pour chaque niveau de la chaîne. Deuxièmement, le mécanisme de garantie de niveaux de croisement. Pour les transactions de l'inter-Chaîne à différents niveaux, la chaîne principale fournit une garantie pour la chaîne la plus lente. Ceci est seulement un mécanisme optionnel si nécessaire. Ces deux mécanismes peuvent être une solution efficace pour améliorer la vitesse de transaction de l'inter-Chaîne de Ælf.



Additional feathers e.g. adapter	**feathers supplémentaires, par ex. adaptateur**
Index	**Indexation**
Side chain	**Chaîne latérale**
different block generation speed	**vitesse différente de génération de bloc**
Adapting side chain	**Adaptation de la chaîne latérale**
Main chain	**Chaîne principale**

Figure 4.12: Illustration de la Topologie de Nœud de Ælf

5. Système d'exploitation de Ælf

5.1. Définition du Système de Blockchain Viable Minimum

Le système de Ælf crée une structure de Chaîne hautement spécialisée et efficace pour gérer tous les types de scénarios d'affaires. Cela permet également de «la division de la chaîne» pour résoudre le problème de capacité lorsque la demande augmente. Afin d'améliorer davantage son potentiel commercial, il est essentiel d'exposer le bloc et l'infrastructure les plus fondamentaux du système pour les développeurs et la communauté. Les chapitres suivants discutent le système de Blockchain viable minimum et le Système d'Exploitation de Ælf en tant que base pour réaliser une personnalisation et une efficacité élevées.

Bloc: Un bloc est utilisé pour enregistrer un état dans le système. La transition du dernier Bloc au Bloc actuel est définie par les transactions incluses dans le Bloc actuel.:Un Bloc oc est utilisé pour enregistrer un état dans le système. La transition du dernier Bloc au Bloc actuel est définie par les transactions incluses dans le Bloc actuel.

Transaction: la logique de transaction est définie en tant que Contrat Intelligent. Contrat Intelligent est essentiellement un Protocole. Il donne toujours la même sortie avec la même entrée.

Compte: Un compte est utilisé pour distinguer les limites du stockage de données. Il se compose de systèmes de clé publique et celui de clé privée.

Communication du réseau P2P: La transmission des données entre les nœuds s'effectue via le réseau P2P sous-jacent.

Protocole de Consensus: Un Protocole de Consensus définit les règles et l'autorité pour mettre à jour un état dans Blockchain.

5.2. Ælf Noyau

5.2.1. Système de Blockchain minimum viable intégré

Ce sont les composants fondamentaux du système de Blockchain fonctionnant dans Ælf Noyau. Ils sont liés aux interfaces pertinentes pour définir les parties personnalisables du Contrat Intelligent, du Consensus de Protocol et de la zone personnalisable de l'en-tête Blockchain.

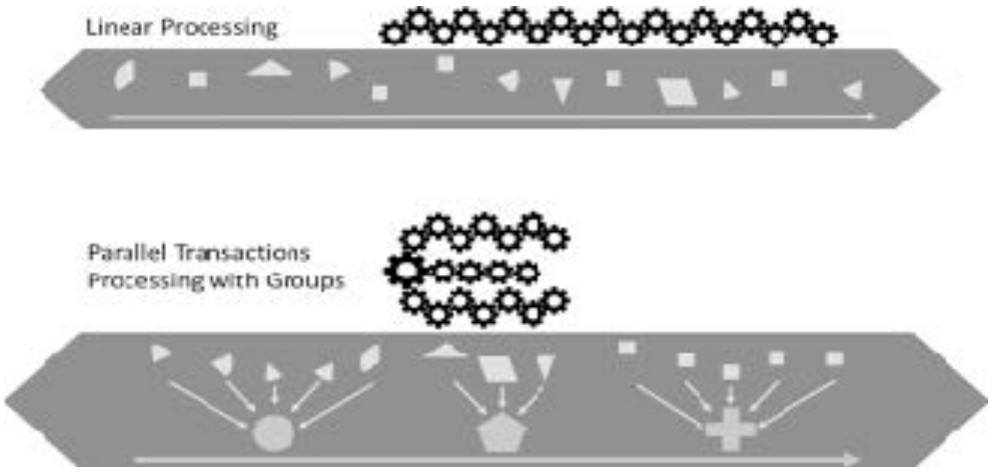
5.2.2. Système de Compte Unifié

Le système de Bitcoin introduit des clés publiques et privées dans le concept de compte. Le Pay to Script Hash donne l'autorité de transaction à un Contrat Intelligent. Ethereum définit le compte possédant extérieurement et le compte de contrat. Ælf Noyau définit les deux types de comptes comme des Contrats Intelligents.

5.2.3. Traitement Parallèle des Transactions dans un Bloc

Ælf analyse l'état statique des transactions et évalue la plage de données impactée de chaque transaction. Comme l'illustre dans la Figure 5.1 Plusieurs transactions sans conflits de lecture / écriture peuvent être traitées en parallèle, sans affecter la sortie de chaque transaction. Au cours du processus de la formation de blocs, les nœuds affectent des transactions à différents groupes en fonction du mutex des

transactions. Les transactions au sein d'un groupe seront traitées en séquence, alors que tous les groupes seront traités simultanément.



Linear processing	**Traitement linéaire**
Parallel transactions processing with groups	**Traitement parallèle des transactions avec des groupes**

Figure 5.1: Traitement parallèles des transactions dans un bloc

Il existe des transactions spéciales qui ne peuvent pas être traitées en parallèle en raison du fait que la plage de données impactée change pendant le traitement d'autres transactions. Dans telles circonstances, les nœuds donneront la priorité aux transactions qui peuvent être traitées en parallèle. Avec des frais de transaction, ces transactions spéciales dans un groupe non parallèle seront traitées en séquence. Sinon, les nœuds peuvent rejeter le traitement de ces transactions. Il est à noter que lorsqu'un nœud malveillant accepte une transaction qui ne peut pas être traitée en parallèle et pris du temps, la probabilité que d'autres nœuds rejettent ce bloc augmente.

La loi d'Amdahl est une règle empirique en architecture informatique. Elle porte le nom de l'informaticien Gene Amdahl. Il donne l'accélération théorique dans l'efficacité lors de l'utilisation du traitement parallèle.

Pensez à un programme qui fonctionne sur un seul processeur. en termes de temps d'exécution, "f" est la proportion du temps d'exécution que la partie bénéficiant des ressources améliorées occupait à l'origine, donc (1-f) est la proportion de temps d'exécution qui est fixée pour le traitement séquentiel. S'il y a des processeurs "m" (nombres) qui fonctionnent en parallèle, alors l'accélération théorique de ce programme sera calculée comme suit:

$$SpeedUp_{\&'()*+} = \frac{1}{(1-f) + \frac{f}{m}}$$

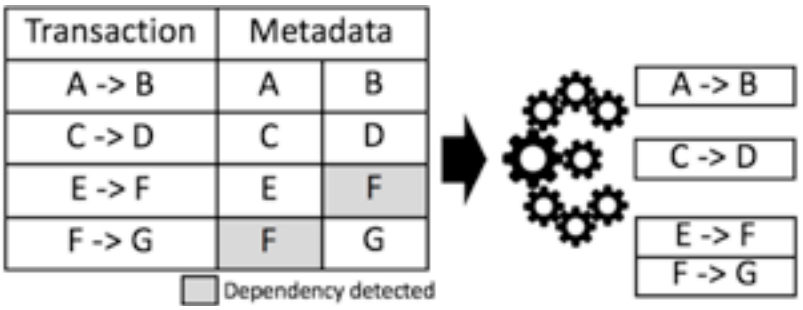
Speed up	Accélération

Deux conclusions majeures sont menées:

- (1)L'accélération ne s'améliore guère lorsque f est au minimum.
- (2) Lorsque m augmente au maximum, l'accélération est limitée de 1/(1-f). •

La loi d'Amdahl est un mode de taille fixe, ce qui signifie qu'il va résoudre des problèmes de taille fixe avec une proportion fixe d'exécution en parallèle.

La plupart des transactions de Blockchain ne sont pas corrélées. Du point de vue de la loi d'Amdahl, l'exécution des données peut être grandement accélérée. cependant, la majeure partie du système actuel de Blockchain s'exécute en séquence, et tous les nœuds exécutent le même ensemble de calcul. Cela gaspille des ressources et empêche la vitesse de transaction. EVM, par exemple, ne traite pas seulement les transactions de manière séquentielle, mais exige également des frais de gaz, ce qui se traduit par une efficacité extrêmement faible.



Transaction	Métadonnée		A->B
A->B	A	B	C->D
C->D	C	D	E->F
E->F	E	F	F->G
F->G	F	G	

Dépendance détectée

Figure 5.2

Pour résoudre les problèmes de Blockchain, une transaction à faible vitesse n'est pas une option. Ælf vise à construire un système de Blockchain avec un haut TPS sur chaîne par le traitement parallèle. La clé de la solution consiste à séparer les données de transaction et la dépendance de calcul afin de résoudre le data hazard de données. Nous pourrions nous référer à l'architecture du microprocesseur de l'Intel, où une station de réservation sépare la dépendance aux circuits électriques avec d'autres techniques telles que le renommage de registres pour traiter les grands data hazard de données rencontrés fréquemment dans RAW, WAW et WAR et exécuter des ALU en parallèle.

Ælf Parallel Execution Scheduler (GPES) adopte une approche similaire. Dans le test interne régulier, Ælf sépare la dépendance de calcul, la dépendance de données dans Blockchain du pool de mémoire. GPES a également un ensemble de prétraitement, c'est-à-dire une prédiction sur le temps de calcul, une pré-indexation du segment de code qui peut être traité en parallèle, initier le pipeline, et exécuter un traitement parallèle en plusieurs dimensions.

Cet ensemble de langage d'indexation peut être utilisé pour résoudre des problèmes plus complexes de logique parallèle.

Le pipeline de Ælf est également une méthode importante pour augmenter la vitesse. Il est largement adopté, tel que traitement de CPU, méta fonction (carte, agrégat premier, et contient). Cet ensemble de Turning langage incomplet est parfait pour le traitement des flux de données (ou des flux de transactions simples). Les fonctions de traitement parallèle et le calcul sans contexte / immuable utiliseront complètement les cœurs et les nœuds

En général, le traitement parallèle est une stratégie globale.

5.2.4. Transactions marquées par des Blocs

Une transaction valide dans la période entre la diffusion et la confirmation est considérée dans un état "en attente". Habituellement, les transactions seront rapidement emballées et confirmées. Cependant, il y a aussi des cas où les

transactions sont laissées non confirmées sur une période relativement longue, par exemple, au moment de la congestion du réseau de Bitcoin ou quand une majorité de mineurs sont insatisfaits des frais de gaz. Lorsqu'une transaction n’est confirmée ou non plus capable d’être retirée pour une période relativement longue, elle sera considérée dans un état de "chaos".

Ælf exige que la diffusion pour chaque transaction soit étiquetée avec une "marque", qui est l'en-tête de hachage du dernier bloc lorsque la transaction se produit. Ensuite, le nœud minier ne traitera que l'en-tête de hachage des 64 blocs récents. Si une transaction n'est pas confirmée après la génération de 64 blocs, ces transactions sont considérées comme ayant expiré. En d'autres termes, une transaction qui n'est pas confirmée dans les 5 minutes, les détenteurs de Tokens peuvent reconstruire cette transaction.

Une autre fonction du marquage des transactions est d'obsolète Blockchain de fourcher efficacement. Un nœud marque avec succès une transaction lorsque les hachages de cette transaction

sont inclus les 64 derniers blocs. Si un nœud reçoit une grande quantité de hachages de marquage invalides provenant de la chaîne la plus élevée, et n'est capable pas d'empaqueter ces transactions, puis il fonctionne probablement sur une chaîne fourchue. Si les nœuds reçoivent une grande quantité de transactions avec un marquage invalide, il y a une forte probabilité que cette Blockchain soit fourchue. À ce moment, les nœuds peuvent suspendre la transaction pour éviter les risques.

5.2.5. Collection du Contrat Intelligent

Le contrat de la Chaîne de Ælf a une collection de Contrats Intelligents qui sont définis pendant la Genèse. Cette collection est nommée comme Collection de Genesis Contrat Intelligent, en homage de Satoshi. L'essence de la Collection du Contrat Intelligent est une classe qui définit les principales fonctions, le Protocole de Consensus de la chaîne et le mécanisme de mise à jour de la collection.

5.2.6. Mise à jour du Contrat Intelligent

Les fonctions de Ælf sont définies par la Collection du Contrat Intelligent. Par conséquent, la mise à jour de la Collection aura un impact sur les fonctions de la Chaîne entière. Le mécanisme de mise à jour de la collection est défini par la collection précédente. Par exemple, nous définissons que si 80% des votes pour une nouvelle Collection de Contrat Intelligent dans le 100e bloc le plus récent sont confirmés par les blocs 2000, la nouvelle collection remplacera la collection originale. Les nœuds qui ne mettent la collection pas à jour seront terminés pour le travail.

5.2.7. Protocole de Consensus Personnalisable

Pour un scénario spécifique d'affaires, le Protocole de Consensus a un impact majeur sur la décision des participants. Pour une chaîne privée avec un niveau de confiance élevé, PBFT est un Protocole de Consensus populaire. Il crée de hautes performances avec un petit nombre de mineurs pré-assignés. Dans un environnement de faible confiance, la stabilité de Blockchain est maintenue via des Protocoles de Consensus tels que PoW, PoS et DPoS.

Ælf définit les Protocoles de Consensus comme une partie de la Collection du Contrat Intelligents et peut mettre en œuvre tout type de Protocole de Consensus basé sur un scénario d'affaires. Nous utilisons Bitcoin et Peercoin comme un exemple pour illustrer les considérations du choix du Protocole de Consensus.

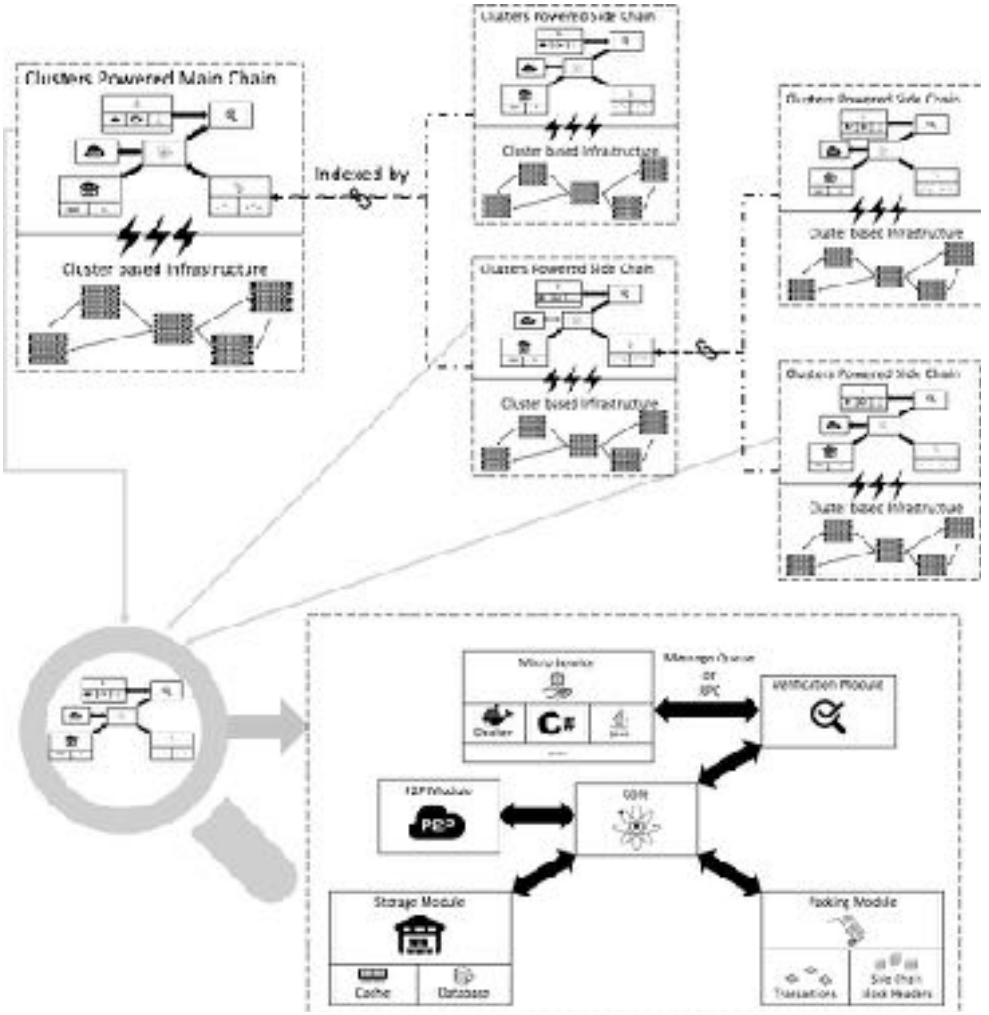
PoW utilisé par Bitcoin authentifie Blockchain uniquement basée sur des informations de l'en-tête de Bloc sans aucune forme d'entrée. D'autre part, le PoS utilisé par Peercoin nécessite des données de stake transaction au sein du Bloc, sa propre authentification de la transaction en plus de l'en-tête Block. Nous recommandons aux futurs utilisateurs de suivre le Protocole de Consensus qui nécessite uniquement des informations d'en-tête de bloc, afin d'obtenir une authentification en temps opportun. En outre, pour des scénarios spécifiques, un Protocole de Consensus personnalisé doit être mis en œuvre.

5.2.8. En-tête de Bloc Personnalisable

Pour faciliter la recommandation que le Protocole de Consensus n'utilise que des informations d'en-tête de bloc, nous introduisons l'en-tête de bloc personnalisable. L'en-tête de Bloc de Peercoin ne contient pas d'information qui vérifie la légitimité du Bloc, donc un Bloc de stake Block ne peut pas vérifier la légitimité de Bloc par lui-même. Ælf Noyau permet de personnaliser la structure de l'en-tête de bloc lors de la

création d'une Chaîne. Auto-preuve basée sur l'en-tête de bloc peut être fait en vérifiant transactions non dépensées Merkle Tree avec Hash (TxID + N + Value), calculer la racine stockée, pour obtenir TxID, N et Value et verification de l’Arbre de Merkle.

3. Interface utilisateur du système d'exploitation de Ælf



Cluster powered main chain	**Chaîne principale alimentée par le cluster**
Cluster powered side chain	**Chaîne latérale alimentée par le cluster**
Cluster powered side chain	**Chaîne latérale alimentée par le cluster**
Cluster based infrastructure	**Infrastructure basée sur un cluster**
Indexed by	**Indexé par**
Micro service	**Micro service**
Docker	**Docker**
P2p module	**Module P2p**
Storage module	**Module de stockage**
Cache	**Cache**
Database	**Base de données**
Message queue or rpc	**File d'attente de messages ou RPC**
Verification module	**Module de vérification**
Packing module	**Module d'emballage**
Transactions	**Transactions**

Side chain block headers	**En-têtes de bloc de chaîne latérale**

Figure 5.3: Interface du système d'exploitation de Ælf

1.3.1. Exécution du Contrat Intelligent

Le Système d'exploitation de Ælf définit les Contrats Intelligents comme des Protocoles. Il peut être exécuté dans toutes les formes de réalisation de service.

Le Système d'exploitation de Ælf préfère Docker et prend également en charge les langages natifs de programmation tels que Java, C #, Go, Javascript, LUA.

Pour Docker, Ælf fournit des services RPC internes pour accorder l'accès aux variables de lecture et comptes utilisateur lors de la réalisation de Contrat Intelligent. Pour le langage natif de programmation, Ælf fournit des SDK respectifs aux fonctions d'exécution.

1.3.2. Micro-service

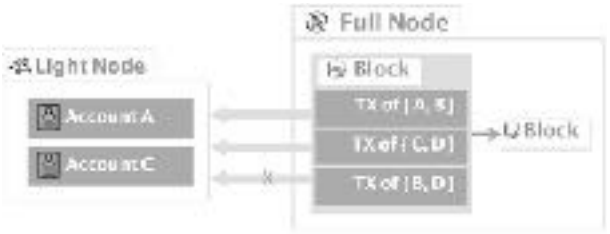
Les Contrats Intelligents sont définis comme micro-service en Ælf. Cela rend les contrats Intelligents indépendants du langage spécifique de programmation. Le Protocole de Consensus devient essentiellement un service tel qu'il est défini dans Contrat Intelligent.

1.3.3. Cloud Base

Grâce à l'approche du micro-service, Ælf Noyau étend le traitement parallèle à un nuage, permettant ainsi l'exécution de contrats basés sur le cloud.

Ælf Noyau a défini la structure et les normes de données, les données chaudes donc peuvent être stockées dans la RAM. En utilisant un service de base de données décentralisé mature, il peut effectivement améliorer les performances du système IO.

1.3.4. Nœud léger



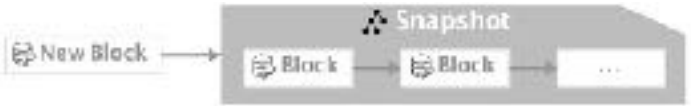
Light Node	**Nœud léger**
Account A	**Compte A**
Account C	**Compte C**
Full Node	**Nœud Complet**
Block	**Bloc**
TX of(A,B)	**TX de(A,B)**
TX of(C,D)	**TX de(C,D)**
TX of(B,D)	**TX de(B,D)**
Block	**Bloc**

Figure 5.4: Illustration de la structure de données du nœud léger

Grâce à la personnalisation et au mécanisme interne de vérification de l'Arbre de Merkle, chaque nœud de Ælf ne gère que les informations pertinentes dans le système. Cela permet aux nœuds d'être plus légers et d'augmenter considérablement la compatibilité avec les terminaux de bureau mobiles et légers.

1.3.5. Modules optionnels

1.3.5.1. Mécanisme de nettoyage des données



New Block	**Nouveau bloc**
Block	**Bloc**
Block	**Bloc**
Snapshot	**Instantané**

Figure 5.5: Illustration du mécanisme de nettoyage des données

Le système de Ælf adopte un mécanisme d'instantané et réinitialise la formation du bloc, en ajoutant les données d'origine au nouveau Bloc Genesis. Mais le système de Ælf ne s'appuiera pas sur les données historiques mais seulement sur les

nouvelles données à traiter. L'histoire humaine a perdu beaucoup de détails, mais cela n'affecte pas la décision des gens envers la situation actuelle. De même, si les données sont trop volumineuses pour être enregistrées, le système doit pouvoir abandonner certaines données historiques.

1.3.5.2. Tunnel de données

Le Tunnel de Données est un mécanisme permettant d'exécuter un transfert P2P. Ces données ne seront pas enregistrées dans le Bloc. La tunnellisation de données s'applique uniquement au transfert de données P2P crypté. Par exemple, si A achète des données de B, B transfère des données à A tandis que A transfère des l'actif à B, tous les deux via le tunnel de données. La conception vise à permettre le transfert de données entre deux nœuds directement. Dans le système actuel de Blockchain, la seule stratégie consiste à diffuser des transactions et tous les nœuds doivent traiter cette transaction. C'est un gaspillage de ressources et cela limitera aussi le volume des transactions traitées.

Le tunnel de données peut être réalisé via un protocole de plug-in. Mais cela nécessitera l'approbation de tous les nœuds. Si cela ne s'est pas produit, les choses deviendront insolubles. (par exemple, les développeurs rencontrent souvent des problèmes lorsque IE ne prend pas en charge certaines fonctionnalités en chrome) Avec ce protocole, Ælf prendra en charge plus d'applications, par exemple un contrat d'achat de données (voir ci-dessous).

1.3.5.3. Modèle de Confirmation Rapide

ÆIf permet une confirmation rapide de la transaction si le destinataire a été autorisé par l'expéditeur. L'autorisation n'est valable que pour un certain type de transaction pendant une certaine période et entre des adresses attribuées. Par exemple, A veut lancer un modèle de confirmation rapide avec B lors d'un transfert d'actif. A doit initier une transaction avec une certaine quantité d'actifs réservés pour cette transaction, et spécifier B comme la contrepartie. Au cours du processus de transaction réel, A enverra la transaction signée à B via le Tunnel de Données. B confirme instantanément la transaction lors de la réception de la transaction. Les actifs affectés seront ensuite transférés à B après que B signe la transaction avec son adresse. A recevra les actifs restants. le Tunnel de Données est terminé après la transaction.

1.3.5.4. Module de Token

Le module Token définit toutes les logiques et algorithmes pour le porteur de valeur (Token). Il sert spécifiquement des scénarios tels que le paiement pour l'allocation des ressources, ou la récompense pour maintenir la stabilité de ÆIf.

Dans la plupart des chaînes publiques, le mécanisme des Tokens est indispensable. Il est utilisé pour inciter le développement sain de l'ensemble du réseau et régler la contribution des différents rôles. Donc ÆIf conçoit un module de Token, où chaque Chaîne Latérale reconnue par le système d'exploitation de ÆIf est autorisée à accepter ÆIf Token.

1.3.5.5. Personnalisation

ÆIf permet aux développeurs de personnaliser rapidement le système en redéfinissant les paramètres dans chaque module, et d'implémenter les Chaînes Latérales par le système d'exploitation de ÆIf. ÆIf suit le principe que «une chaîne dessert un scénario spécifique d’affaires», et établit une architecture hautement abstraite et modulaire. Pour les utilisateurs d'entreprise et les entrepreneurs, cela a accéléré le processus de mise en œuvre de leurs idées commerciales. Pour les utilisateurs sophistiqués, il permet une personnalisation élevée pour leurs propres Chaînes, et libère le fonctionnement complet de Blockchain.

6. Développement d'un écosystème de Ælf

Toute nouvelle technologie ne réussit pas sans adoption commerciale et un écosystème durable. Ælf a proposé un plan technique avec application commerciale instillé tout au long de la conception. Il est essentiel d'établir un écosystème de Ælf, y compris des ressources internes et externes. Nous poursuivrons l'objectif en luttant simultanément dans trois dimensions: la technologie, les affaires et le capital.

6.1. Technologie

Les chapitres ci-dessus ont présenté les principales caractéristiques techniques de Ælf. L'équipe de Ælf possède plusieurs années d'expérience dans le développement de Blockchain, a notamment participér à quelques projets d'entreprise axés sur le commerce. La solution technique proposée par Ælf vise à résoudre les obstacles les plus urgents pour l'adoption commerciale de Blockchain, tels que l'évolutivité, la sécurité, la personnalisation et l'interopérabilité. Il fournit une infrastructure très efficace pour adopter de nouveaux protocoles et soutenir toutes sortes de scénarios commerciaux à l'avenir

6.2. Applications commerciales

Ælf est destiné à devenir finalement la nouvelle «infrastructure Internet» pour soutenir la prochaine génération de «commerces numériques». L'équipe et ses conseillers ont conseillé de nombreux projets de Blockchain dans le passé et nous voyons que certaines industries seront les « pionniers » et les « stars de Blockchain » sur Ælf:

Financial services	**Services financiers**
Internet of things	**Internet des objets**
Smart city	**Ville intelligente**
insurance	**Assurance**
Digital identity and IPs	**Identité numérique et IPs**

Figure 6.1: Illustration des Applications d'affaires d Ælf

1) Services financiers

Blockchain a attiré beaucoup d'attention dans le secteur des services

financiers, car il réduit considérablement les intermédiaires et assure des transactions sécurisées. Il est très probable que de multiples chaînes sur ÆIf seront développées spécifiquement pour les services financiers, tels que le paiement transfrontalier, le financement du commerce, la chaîne d'approvisionnement, etc. La fonction du traitement parallèle est capable de gérer les transactions commerciales à l'échelle international, et la fonction de communication en chaîne permet une coordination sans heurt de l'enregistrement des actifs, de la gestion des comptes et des transactions en temps réel.

2) Assurance

L'assurance est un autre domaine très attrayant qui sera perturbé par Blockchain. Une chaîne latérale de Ælf dédiée à l'assurance intégrera divers DAPPs pour l'assurance, transformant ainsi toute la chaîne de valeur de l'industrie, de l'identité de l'utilisateur à l'exécution du contrat d'assurance, en passant par la gestion des réclamations.

3) Identité numérique et IPs

   La structure multi-chaîne de Ælf a une chaîne intégrée pour l'identité numérique. Ceci assure la performance d'une telle chaîne latérale si une autre chaîne latérale est occupée, par exemple. un nouveau Token est émis de l'autre côté de la chaîne.

   Au sein de Ælf, l'identité numérique peut être utilisée par d'autres chaînes latérales via la "messagerie". À l'aide de l'adaptateur, Ælf est également capable de récupérer des informations et des données provenant d'autres chaînes établies, telles que Bitcoin et Ethereum.

4) Ville Intelligente

   Les gouvernements seront également intéressés à Ælf car il leur permet d'exécuter en toute sécurité et commodément certaines tâches administratives sur Ælf. Le gouvernement ou l'organisation peut personnaliser le protocole de consensus pour répondre aux exigences de sécurité nationale. Les activités, telles que l'enregistrement des services publics, les identités des citoyens, la divulgation d'informations par les agences gouvernementales et les sondages peuvent être réalisées sur Ælf avec une grande transparence et efficacité. Quelques pays expérimentent dans ce domaine, notamment l'Estonie, Singapour, la Chine, etc.

5) Internet des objets

   Ælf prend en charge le service de nœud léger et de cloud, ce qui réduit les besoins en calcul pour les appareils qui y sont connectés, tout en conservant des performances élevées. C'est essentiel pour gérer des milliards d'appareils et permettre le micro-paiement entre eux pour relier Internet des objets.

Ælf a jeté des bases solides pour les industries ci-dessus et plus de s'y efforcer, nous identifierons activement de nouvelles opportunités d'affaires et DAPPS comme une partie de l'écosystème de Ælf.

1) Interopérabilité avec les DAPPs existants sur les chaînes existantes

   Il existe déjà des DAAPs éprouvés sur des chaînes existantes, comme sur Bitcoin et Ethereum. Ælf tirera parti de sa fonctionnalité d'interopérabilité pour se connecter aux DAPPs afin de permettre l'échange de actifs et également de saisir les données de transaction provenant des DAPPs

2) Nourrir nouvelles idées de startups

   L'équipe de développement et ses conseillers sont fortement impliqués dans la formation et la commercialisation de nouvelles idées dans la communauté globale de Blockchain. De nouvelles idées de start-up nous ont approchés pour des conseils techniques et commerciaux. Nous tirerons parti de cette connection forte pour nourrir nouvelles idées de start-ups et les inclure dans l'écosystème de Ælf. Avec les VCs, nous sommes confiants d'identifier et de lancer les projets les plus prometteurs sur Ælf.

3) Transformer les entreprises établies en «Blockchain savvy»

Les entreprises établies offrent une autre opportunité de faire partie de l'écosystème de ÆIf. Ils possèdent déjà une vaste clientèle et une valeur prouvée pour leurs affaires actuelles. ÆIf peut les transformer en modèles encore plus puissants avec de fortes incitations et récompenses pour les clients, en résolvant certains points essentiels dans

l'industrie comme décrit ci-dessus. L'équipe de Ælf a été en discussion avec quelques sociétés Internet et entreprises traditionnelles sur le modèle d'affaires perturbateur sur Ælf. Nous prévoyons que quelques annonces passionnantes seront faites dans un proche avenir. En outre, l'équipe a l'intention de collaborer avec des sociétés de conseil en stratégie globale pour repousser les limites des modèles économiques de la prochaine génération sur l'éco-système de Ælf.

6.3. Capitaux

La construction d'un écosystème nécessite sans aucune doute une grande quantité de capitaux. En plus de tirer parti du fonds collectés lors de la vente de Token, l'équipe et ses conseillers ont établi une solide alliance avec les principaux fonds crypto au niveau mondial. L'équipe et ses conseillers recommandent de nombreux projets de vente de Token à l'international pour collecter des fonds et développer leurs solutions avec succès. Le réseau international de capitaux et la réputation assurent une solide capacité de financement pour soutenir le futur pipeline avec une vision à long terme.

Les références

1. Satoshi Nakamoto. Bitcoin: Un système de paiement électronique pair-à-pair. 2008.

2. Vitalik Buterin. Livre blanc Ethereum: Un Contrat Intelligent de Nouvelle Génération et une Plate-Forme d'Application Décentralisée. 2013.

3. Melanie Swan. Blockchain: Blueprint for a new economy. ” O’Reilly Media, Inc.”,2015.

4. Frederick P. Brooks. The Design of Design: Essays from a Computer Scientist. “Addison-Wesley”, 2010.

5. Andrew S. Tanenbaum. Systèmes modernes d'exploitation “Pearson”, 2007.

6. Joseph Poon et Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016.

7. Gavin Wood. Ethereum: Asecure decentralized generalized transaction ledger. 2014.

8. Hyperledger Whitepaper. 2016.

9. Muhammad Saqib Niaz and Gunter Saake. Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data. 2015.

10. Robert McMillan. The inside story of mt. gox, Bitcoin’s 460 dollar million disaster. 2014.

11. Sunny King, Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012.

12. David Schwartz, Noah Youngs, et Arthur Britto. The ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 5, 2014.

13. Leslie Lamport. le Parlement à Temps Partiel. *ACM Transactions on Computer Systems*, 21(2):133–169, mai 1998.

14. Leslie Lamport, Robert Shostak, et Marshall Pease. Le problème des généraux byzantins *ACM Transactions sur les Langages et Systèmes de Programmation (TOPLAS)*, 4(3):382–401, 1982.

15. Leslie Lamport. Heure, horloges et l'Ordre des Événements dans un Système Distribué. *Communications de l'ACM*, 21(7):558–565, juillet 1978.

16. Paul Tak Shing Liu. Système de dossier médical de Blockchain, grosses données et tokenization. *Sécurité de l'Information et des Communications*, pages 254–261. Springer, 2016.

17. Robert Love. Développement du Noyau Linux. "Addison-Wesley", 2010.

18. Shawn Wilkinson and Tome Boshevski, Storj: Un Pair à Pair Réseaux de Stockage sur un Nuage . 2016.

19. Contrat. URL *https://en.Bitcoin.it/wiki/Contract,* 2014.

20. Activation obligatoire du déploiement de segwit, UASF, BIP 0148. URL *https://github.com/Bitcoin/bips/blob/master/bip-0148.mediawiki,* 2017.

21. Propriété Intelligente. URL *https://en.Bitcoin.it/wiki/Smart_Property*, 2016.