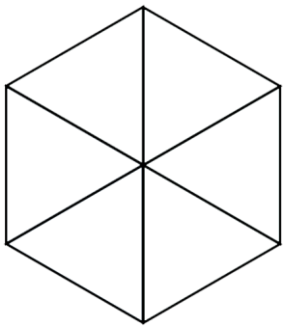

ASURE: PREMIER RÉSEAU BLOCKCHAIN ÉVOLUTIF POUR LES SYSTÈMES DE SÉCURITÉ SOCIALE DÉCENTRALISÉS

Paul Mizel, Fabian Raetz et Gamal Schmuck
Fondation Asure

1 octobre 2019

https://asure.network

Abstrat

La sécurité sociale est un élément essentiel du développement économique et politique des sociétés. Cependant, plus de 4,1 milliards de personnes dans le monde n'ont pas accès aux systèmes de sécurité sociale[1] Et d'autre part, les systèmes sociaux existants ont d'autres défis à relever pour des raisons démographiques (par exemple, taux de natalité de 1,5 contre 2,5 en moyenne mondiale) ou financières (coûts administratifs de plus de 50%, voire plus de 100%). Blockchain Ethereum ne peut actuellement effectuer qu'un maximum de 1,3 million de transactions par jour[2] Les systèmes de sécurité sociale reposent en partie sur plusieurs centaines de millions de transactions par mois et ne peuvent donc pas être mis en œuvre de manière durable en utilisant Blockchain dès à présent.

Les systèmes de sécurité sociale basés sur Blockchain présentent plusieurs avantages par rapport aux systèmes de sécurité sociale conventionnels. Ils assurent une qualité constante et beaucoup plus élevée des données utilisées et stockées grâce à l'intégrité des processus, l'immuabilité et la pérennité du système, permettant une analyse précise en temps réel de celles-ci. La transparence et l'immuabilité des transactions assurent la sécurité du système contre la manipulation et la corruption. En utilisant Blockchain pour éliminer le travail manuel lourd et sujet aux erreurs, il est possible d'atteindre un haut degré d'automatisation, de rentabilité et de facilité de suivi des processus métier.

Les développements passés de la technologie Blockchain et leurs résultats montrent que les transactions financières exécutées par leur intermédiaire peuvent être effectuées de manière sûre, automatique et sans intermédiaires. Cela donne à penser que les systèmes de sécurité sociale, en tant que systèmes au service du public et utilisant des transactions financières fondées sur des règles, constituent un cas d'utilisation raisonnable des blockchains publiques.

Les solutions correspondantes d'Ethereum Blockchain telles que Casper, et Sharding dans le pipeline qui résoudront à terme le problème de scalabilité de la couche 1. Même en ce qui concerne les personnes qui n'ont accès à aucun système de sécurité sociale, le nombre de transactions requises pour les versements et les paiements s'élève au moins au nombre de personnes concernées, soit des milliards de transactions mensuelles pour le seul système de retraite.

L'objectif de cet article est d'examiner une solution de niveau 2 pour une extensibilité optimale tout en conservant tous les avantages de la technologie de blockchain pour les systèmes de sécurité sociale décentralisés.

Note: asure.network est un travail en cours. Des recherches actives sont en cours et de nouvelles versions de ce document seront publiées sur http://asure.network Pour tout commentaire ou suggestion, contactez-nous sur research@asure.network.

Glossaire

EVM Ethereum Virtual Machine est conçu pour servir d'environnement d'exécution pour les contrats intelligents basés sur Ethereum.

Blockchain Un système dans lequel un enregistrement des transactions est conservé sur plusieurs ordinateurs reliés en réseau peer-to-peer.

Ethereum Une plate-forme logicielle décentralisée qui permet les ContratsIntelligents et les applications distribuées (DApps).

ETH C'est le symbole natif de Ethereum blockchain.

BTC C'est le symbole natif de Bitcoin blockchain..

ERC20 Une norme technique utilisée pour les contrats intelligents sur blockchain Ethereum pour la mise en œuvre des jetons.

ContratsIntelligents Un contrat intelligent est un protocole informatique destiné à faciliter, à vérifier ou à faire respecter numériquement la négociation ou l'exécution d'un contrat. Les contrats intelligents permettent l'exécution d'actions transfrontalières crédibles sans l'intervention de tiers. Ces transactions sont traçables et irréversibles.

Compte Un hachage d'une clé publique qui peut contenir des valeurs. Les valeurs de maintien ne sont accessibles qu'en connaissant la clé privée correspondante.

GDPR Le Règlement Général sur la Protection des Données (UE) 2016/679 (" GDPR ") est un règlement du droit communautaire sur la protection des données et de la vie privée pour tous les individus dans l'Union européenne (UE).

PAYG un mode de financement des assurances sociales, en particulier de la prévoyance vieillesse, mais aussi de l'assurance maladie et de l'assurance chômage. Les cotisations versées servent directement à financer les bénéficiaires, c'est-à-dire qu'elles leur sont remboursées.

Contenu

1 Introduction

L'écosystème Asure se compose du réseau Asure, de Blockchain Asure, de la plate-forme Asure et d'applications tierces.

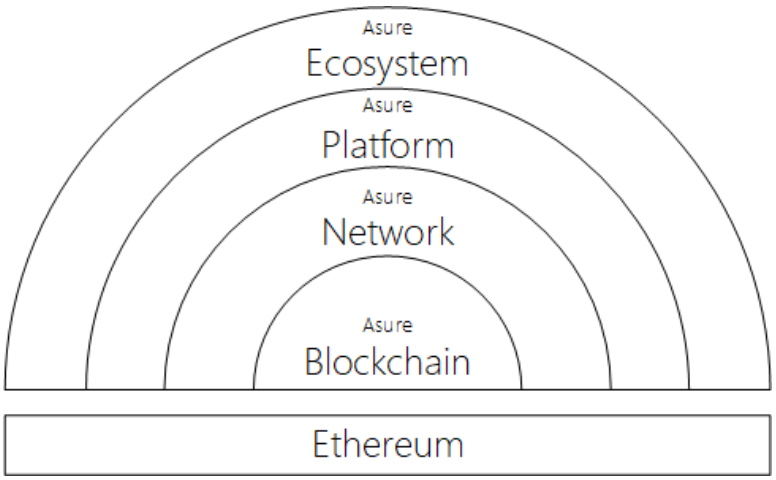

Figure 1: Asure écosystème

Le réseau Asure est un réseau modulaire évolutif pour les systèmes de sécurité sociale décentralisés. Elle jette les bases de l'accès de 10 milliards de personnes aux systèmes de sécurité sociale et a un impact social considérable là où il est le plus nécessaire. [3]

En tant que base technologique qui assure une performance optimale en ce qui concerne le débit des transactions tout en maintenant le caractère décentralisé du réseau, elle garantit le niveau requis de transparence et de rentabilité au sein du système. Il est mis en œuvre autant de chaînes latérales Plasma connectées à Asure Blockchain qu'à Ethereum Blockchain ou à toute autre chaîne compatible EVM. Chaque chaîne latérale est exploitée par plusieurs fournisseurs de nœuds indépendants qui doivent mettre en jeu des jetons ASR pour parvenir à un consensus entre eux et donc au sein du réseau. En jalonnant des jetons ASR, les fournisseurs de nœuds peuvent gagner des jetons supplémentaires en offrant leur puissance de calcul. Il y aura une chaîne latérale pour chaque système de sécurité sociale au sein du réseau Asure.

Asure Blockchain contient la chaîne racine Asure et les chaînes latérales connectées. La chaîne racine offre des avantages dans le domaine de la sécurité et de la communication en chaîne. Tous les nœuds Asure Blockchain en cours d'exécution représentent le réseau Asure. La plate-forme Asure connecte l'infrastructure dorsale à des applications qui peuvent être utilisées par les utilisateurs finaux ou des interfaces de programmation pour les développeurs afin de construire des applications sur la plate-forme Asure.

1.1 Systèmes de sécurité sociale

La sécurité sociale est un système d'assurance dans lequel les risques assurés (tels que la maladie, la maternité, le besoin de soins de longue durée, les accidents du travail, les maladies professionnelles, le chômage, la réduction de la capacité de gain, la vieillesse et le décès) sont couverts conjointement par tous les assurés. Les systèmes de sécurité sociale absorbent de nombreux risques de la vie, préviennent les difficultés extrêmes et créent ainsi un équilibre social.

Les personnes qui n'ont pas accès aux systèmes de sécurité sociale risquent de tomber dans la pauvreté si elles sont frappées par un coup du sort comme une maladie, une mauvaise récolte ou un handicap. Ils peuvent alors devoir liquider leurs économies, vendre du bétail et d'autres moyens de production et envoyer leurs enfants travailler à la place de l'école afin de financer leurs dépenses quotidiennes. [20]

Les bénéficiaires de la sécurité sociale de base sont plus disposés à investir dans l'éducation et le capital physique, ce qui comporte des risques supplémentaires, mais aussi la perspective d'une amélioration des revenus. Des études empiriques suggèrent que l'existence de systèmes de sécurité sociale, en particulier dans le secteur informel, renforce la propension à investir et favorise ainsi la croissance économique précisément là où cela contribue le mieux à réduire la pauvreté. [21]

Il existe un large éventail de systèmes de sécurité sociale et leur mise en œuvre concrète varie d'un pays à l'autre. Aux fins du présent document, nous définissons comme suit le fonctionnement des systèmes de sécurité sociale les plus courants :

Pension de retraite

Un système de retraite se compose d'un certain nombre de cotisants et de retraités. Les cotisants paient des primes mensuelles qui sont redistribuées aux retraités actuels. En contrepartie, les cotisants ont le droit de recevoir leur pension après une certaine période de temps, en fonction du temps et du montant des primes payées. Dans certains systèmes, les primes sont payées par l'entreprise sur la moitié du cotisant, ce qui signifie une réduction massive des transactions nécessaires. Les versements de rente ont habituellement lieu à une date fixe et tous les retraités sont payés en même temps. Cela en fait un cas d'utilisation idéal pour les opérations de paiement de masse.

Soins de santé

Les parties concernées par les soins de santé sont diverses - il y a des assurés qui paient une prime, il y a des médecins, des hôpitaux, des pharmacies et d'autres prestataires de services qui émettent des factures. Celles-ci peuvent être compensées par le système ou par la personne assurée qui soumet les factures au système et se fait rembourser les frais. Ici il y a différentes

possibilités comment vous pouvez réaliser le traitement par lots, l'assuré peut soumettre les factures accumulées à la fin de l'année où les médecins, hôpitaux, pharmacies et autres prestataires de services peuvent également soumettre leurs factures collectives par lots.

Chômage

L'assurance-chômage est la protection contre la perte d'emploi. Les participants ayant un emploi paient une prime lorsqu'en cas de perte d'emploi, le temps est compensé par les cotisants pour retrouver un emploi.

L'assurance sociale

L'assurance sociale, l'assurance soins de longue durée ou l'assurance soins infirmiers est une assurance obligatoire pour couvrir le risque de devenir dépendant des soins de longue durée. Les prestations de l'assurance sociale sont accordées en fonction du "niveau des besoins en matière de soins de longue durée". Dans le cas des soins ambulatoires professionnels ou (partiellement) hospitaliers, les coûts sont couverts jusqu'à concurrence d'un certain montant maximum (y compris les aides aux soins, les mesures visant à améliorer le cadre de vie ainsi que les prestations volontaires de soins infirmiers). L'assurance sociale obligatoire n'est donc pas une assurance complète. Pour obtenir une couverture complète, il est nécessaire de souscrire une assurance complémentaire privée de soins infirmiers. En cas de besoin, la personne assurée a droit à une assistance en matière de soins infirmiers en tant que prestation sociale complémentaire adaptée à ses besoins.

Soutien aux enfants et aux jeunes

En Allemagne, l'aide à l'enfance et à la jeunesse couvre tous les services et toutes les tâches des institutions publiques et indépendantes au profit des jeunes et de leurs familles. La protection de l'enfance et de la jeunesse n'est pas un pilier direct de l'assurance sociale, mais est principalement assurée par des institutions indépendantes, qui travaillent en étroite collaboration avec les autorités. Il est principalement financé par l'argent des contribuables.

Assurance invalidité / Assurance accidents

L'assurance accidents obligatoire a pour but de prévenir les accidents du travail, les maladies professionnelles et les risques sanitaires liés au travail et de rétablir la santé et la performance professionnelle des assurés "par tous les moyens appropriés" après la survenance de ces événements assurés.

1.2 Blockchain

Un Blockchain est une base de données décentralisée qui contient une liste sans cesse croissante d'enregistrements de transactions. La base de données est étendue chronologiquement linéaire,

semblable à une chaîne à laquelle de nouveaux éléments sont constamment ajoutés en bas (d'où le terme "blockchain"). Si un bloc est complet, le suivant est créé. Chaque bloc contient la somme de contrôle du bloc précédent. Le développement de Bitcoin par Satoshi Nakamoto en 2009 est l'une des implémentations de blockchain qui démontre le potentiel de la technologie pour les transactions financières. Le potentiel perturbateur de Blockchain devient de plus en plus évident. Après l'invention de Ethereum blockchain et Ethereum Virtual Machine (EVM), le monde a reçu les outils nécessaires pour construire des organisations autonomes décentralisées (DAO) qui fonctionnent. Dans un tel système, de multiples autorités contrôlent différents composants et aucune autorité unique n'a la confiance totale de toutes les autres. La technologie Blockchain est parfaitement adaptée à un fonctionnement autonome et décentralisé de la sécurité sociale.

2 Réseau Asure

Le réseau Asure se compose des clients de nœuds dans lesquels le blockchain Asure est utilisé et synchronisé entre les nœuds individuels à l'aide du consensus. Pour obtenir le nombre d'opérations requises, la charge doit être répartie sur plusieurs blockchains. Une ou plusieurs blockchains peuvent être spécifiques à un seul système de sécurité sociale. Afin de bénéficier de l'écosystème de blockchain, et la grande valeur ajoutée pour l'évolutivité n'apparaît que lorsque les actifs peuvent être transférés entre les différentes blockchains. De plus, les chaînes latérales spécialisées peuvent bénéficier de la sécurité de la chaîne racine et ainsi les actifs sont mieux protégés. [6]

2.1 Exigences

Dans un scénario évolutif, les besoins de base en matière de sécurité sociale et de blockchain sont les suivants :

Débit des transactions

Le réseau Asure doit être en mesure d'augmenter le débit des transactions à travers les chaînes latérales de manière à ce que les pays et les résidents puissent effectuer leurs transactions financières à l'intérieur de la chaîne hors ligne.

Vie privée

Afin de protéger la vie privée des utilisateurs, aucune donnée privée ne peut être stockée sur Blockchain. Si possible, les transactions ne doivent pas être affectées à un utilisateur. Les données personnelles sont cryptées et stockées en dehors de Blockchain. En utilisant la méthode Zero-Knowledge-Proof, le stockage des données personnelles peut être complètement évité.

Pour qu'une sécurité sociale fondée sur blockchain puisse être mise en place, elle doit respecter les lignes directrices en matière de protection des données et de respect de la vie privée des réglementations nationales et internationales telles que le règlement général sur la protection des données (GDPR) de l'Union européenne. [7]

Transparence

La transparence au sein du réseau Asure est un facteur important pour protéger les systèmes de sécurité sociale contre la corruption et la manipulation. Tout en respectant la vie privée des utilisateurs, il est important d'assurer la transparence du système en général, afin de permettre par exemple des statistiques en temps réel sur l'ensemble des flux monétaires.

Règles métier du système

La sécurité sociale a de nombreux facteurs d'influence et les règles, ceux-ci doivent être remplies, adaptées et exécutées, c'est pourquoi il est notre exigence d'être en mesure d'exécuter des règles commerciales personnalisées dans la chaîne latérale avec EVM ou EWASM.

Sécurité

Un système qui organise et stocke les transactions financières des systèmes de sécurité sociale doit satisfaire à de multiples exigences de sécurité. Il faut s'assurer que les données ne peuvent pas être manipulées ou volées et que le système résiste aux attaques, aux pannes et autres pannes.

2.2 Autres technologies

Poon et Buterin ont présenté le cadre Plasma en 2017 pour résoudre le problème de mise à l'échelle en disposant plusieurs blockchains indépendants en une hiérarchie arborescente. Des propositions consécutives de plasma ont décrit des sites hors chaîne pour des transferts simples de jetons fongibles et non fongibles. Ces propositions comprennent Plasma MVP, Plasma Cash et Plasma Debit. Le cadre Plasma fait l'objet de recherches actives et, selon l'application et les exigences, la mise en œuvre du plasma varie[8] Loom et OmiseGO sont parmi les premiers à mettre en œuvre le plasma et continuent leurs recherches dans ce domaine.

Le plasma a été introduit très récemment et est l'une des solutions les plus prometteuses proposées pour le calcul scalable sur blockchain. Le livre blanc sur le plasma est très large et ne contient pas toutes les informations techniques nécessaires pour une mise en œuvre immédiate. Le plasma peut fournir une évolutivité pour les applications Ethereum. Il s'agit d'un protocole de chaîne latérale spécifique à l'application.

Polkadot, d'autre part, a été présenté par Gavin Wood en 2017. L'objectif du concept est de créer une solution hétérogène multi-chaînes permettant de relier des chaînes latérales adaptées individuellement aux blockchains publiques. Polkadot permet à différentes blockchains d'échanger des messages d'une manière sécurisée et fiable.

Le réseau Raiden est une solution de mise à l'échelle hors chaîne avec une technologie de canal de paiement et de canal d'état, permettant des paiements quasi instantanés, à faible coût et évolutifs. Il est complémentaire de Ethereum blockchain et fonctionne avec tous les jetons compatibles ERC20.

2.3 Plasma

Le réseau Asure utilisera le cadre Plasma pour créer un réseau en blockchain modulaire évolutif pour les besoins des systèmes de sécurité sociale.

Pour repousser encore plus loin les limites de la couche 1 afin d'exploiter efficacement le système de sécurité sociale, la mise à l'échelle de la couche 2 est considérée comme la solution la plus efficace. Il facilite la mise en œuvre de la sécurité dans le système car il repose sur la couche 1. La solution sera conçue comme une combinaison de la chaîne racine d'Asure et des chaînes latérales correspondantes pour répondre aux besoins des systèmes de sécurité sociale.

Les chaînes latérales Asure peuvent être connectées à des contrats intelligents d'Ethereum ou à d'autres technologies de blockchains qui fonctionnent avec des modèles de conception Plasma.

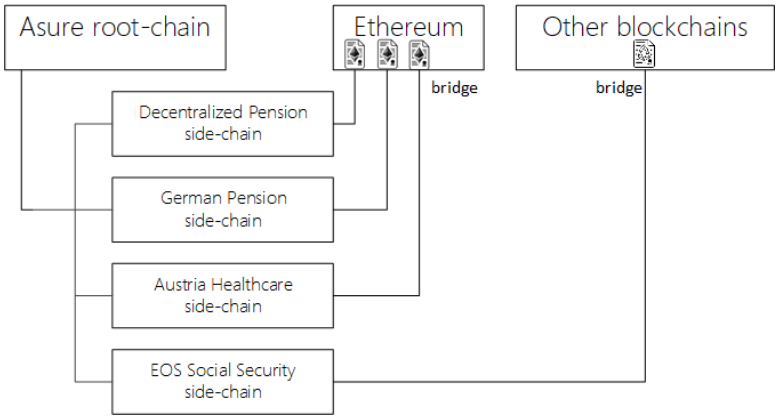

Figure 2: Chaînes latérales d'Asure

3 Asure Blockchain

D'un point de vue technique, les systèmes de sécurité sociale peuvent être décrits comme un certain nombre de transactions (financières) fondées sur des règles qui sont exécutées entre un total (généralement) légèrement changeant de différentes parties à condition de maintenir un équilibre entre la valeur déposée et la valeur retirée sur une période donnée. Un tel système peut être mis en œuvre numériquement en créant un système de blockchain, qui supporte les contrats intelligents et les monnaies crypto.

Les systèmes de sécurité sociale conventionnels génèrent actuellement jusqu'à des centaines de millions de transactions par mois, en fonction du nombre de parties concernées et du cas d'utilisation spécifique de la sécurité sociale.

Primes mensuelles de retraite = 54.445 Mio
Pensions mensuelles = 25.646 Mio
Transactions mensuelles sur les pensions = 80.091 Mio

Table 1: Par exemple, le système de retraite légal allemand: [12]

Afin de mettre au point un système de blockchain capable de traiter ces transactions, il est nécessaire d'augmenter le débit de transactions réalisable du système et le traitement automatique par lots au sein d'une transaction pour réduire au minimum le nombre total de transactions.

Ces deux exigences peuvent être satisfaites par l'utilisation de chaînes latérales, comme spécifié dans le Cadre Plasma. L'Asure Blockchain fonctionne comme la chaîne latérale évolutive de l'implémentation Asure Plasma. C'est la chaîne de base du réseau Asure et jette les bases d'une évolutivité optimale des systèmes de sécurité sociale basés sur blockchain.

Les actifs transférés de la chaîne Ethereum Blockchain à l'une des chaînes latérales d'Asure sont bloqués dans le Contrat Plasma d'Asure sur Ethereum Blockchain jusqu'à ce qu'une transaction de sortie sur Ethereum Blockchain soit réalisée. Selon les spécifications Plasma MVP, un équivalent de cette valeur est créé par l'utilisation du modèle de conception de l'opérateur (Proof-Of-of-Authority) sur l'Asure Blockchain et attribué à l'utilisateur.

Les ressources disponibles sur Asure Blockchain peuvent alors être utilisées pour des actions de transfert dans le système. Le consensus entre tous les fournisseurs de nœuds de Asure Blockchain est atteint grâce à un algorithme de consensus de preuve d'intérêt en utilisant une version adaptée du moteur de consensus Tendermint. Monnaie d'appel d'offres peut traiter jusqu'à 10 000 transactions par seconde. A l'aide de zones et de concepts de sharding, cette taille peut être multipliée par 1000. Cela garantirait le fonctionnement durable de la sécurité sociale sur blockchain . [15]

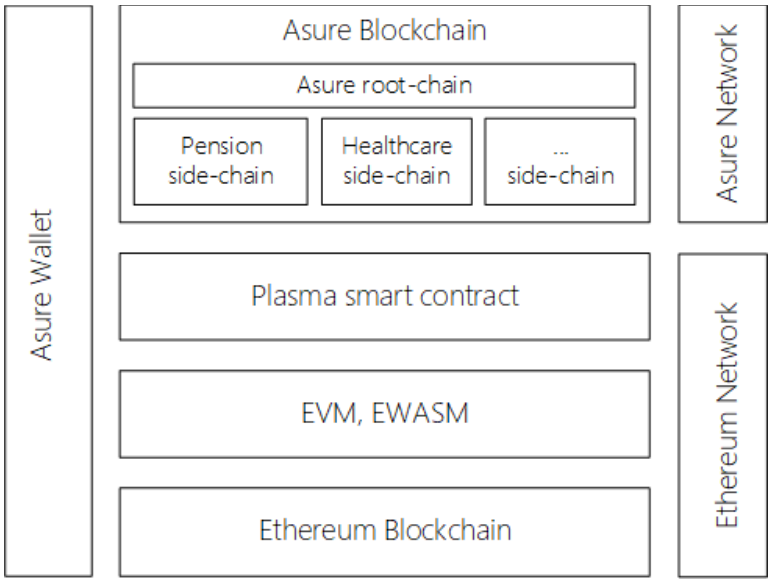

Figure 3: Architecture d'Asure

L'Asure Blockchain a plusieurs principes fondamentaux.

3.1 Sécurité

L'Asure Blockchain comprend plusieurs fonctionnalités qui le protègent contre des attaques telles que les dépenses non autorisées, les dépenses doubles, la falsification d'actifs, et la falsification de blockchain.

Chaque bloc ajouté à blockchain, en commençant par le bloc contenant une transaction particulière, est considéré comme une confirmation de cette transaction. Idéalement, les destinataires et les expéditeurs recevant des paiements devraient attendre qu'au moins une confirmation ait été distribuée sur le réseau avant de supposer que le paiement a été effectué. Plus le destinataire attend de confirmations, plus il est difficile pour un attaquant d'inverser avec succès la transaction dans blockchain à moins que l'attaquant ne contrôle plus de la moitié de la performance totale du réseau, auquel cas il s'agit d'une attaque à 51%. Cette construction n'est pas conçue pour prévenir 51% des attaques, mais plutôt pour encourager la propagation des blocs.

3.2 Algorithme de consensus

Il existe différentes versions pour les algorithmes de preuve. 13] L'acceptation à long terme et le mouvement de la communauté s'oriente vers la preuve d'intérêt où les validateurs créent les blocages et sont récompensés pour avoir fait le bon travail. Asure Blockchain utilisera un algorithme consensuel de preuve d'enjeu (PoS). Il utilisera dans la première mise en œuvre du MVP le moteur de consensus Tendermint[14].

3.3 Confidentialité avec (ZK-SNARKS et ZK-STARK)

L'Asure Blockchain tient compte, entre autres, des aspects relatifs à la protection de la vie privée qui revêtent une grande importance pour la sécurité sociale.

ZK-SNARKS (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) offre la possibilité d'effectuer des transactions anonymes. Les ZK-SNARKS ne résistent pas à l'informatique quantique. ZK-STARK (Zero-Knowledge Scalable Scalable Transparent Argument of Knowledge) est la dernière innovation visant à atteindre la confidentialité sur le blockchain avec l'utilisation de calculs rapides et évolutifs et est résistant au Quantum Computing. [16]

Comme Ethereum effectue également des recherches dans ce domaine dans la couche 1, il sera possible pour les assurés de garder l'anonymat sur les transactions de sécurité sociale. [17]

L'état des technologies du savoir zéro n'est pas encore tout à fait réalisable, mais cela va changer à l'avenir.

3.4 EVM, WASM, eWASM, *WASM

EVM fournit un calcul turing-complet pour qu'Ethereum puisse exécuter un programme général, également connu sous le nom de contrat intelligent. Plasma EVM est une nouvelle version de Plasma qui peut exécuter l'EVM dans la chaîne plasma, et ses clients peuvent être basés sur les clients actuels d'Ethereum (go-ethereum, py-evm, parité). Nous proposons une construction Plasma applicable à l'état pour garantir uniquement l'état valide soumis à la chaîne racine, fournissant un moyen d'entrer et de sortir du stockage de compte entre deux chaînes car chaque chaîne a une architecture identique. Un autre avantage est que les outils de développement d'Ethereum peuvent également être utilisés dans la chaîne plasma. eWASM n'est qu'un sous-ensemble "aromatisé" d'Ethereum de Web Assembly, qui est un format d'instruction binaire. eWASM repose sur des instructions qui sont très proches du CPU du monde réel. Les améliorations de performance sont significatives et semblent plus sûres. WebAssembly est soutenu par Mozilla, Google, Apple, et Microsoft, la communauté est également active, il va être un standard web largement utilisé. La chaîne Ethereum Blockchain traite environ 15 transactions par seconde (TPS), ce qui n'est pas suffisant pour la mise en place d'un système de sécurité sociale. Les améliorations apportées à Ethereum (également appelé couche 1), qui sont actuellement en cours, devraient permettre d'augmenter sensiblement le nombre de TPS. Parmi les améliorations, mentionnons un algorithme consensuel basé sur la preuve d'enjeu (PoS), et par l'introduction de eWASM - une machine virtuelle basée sur WebAssembly.

3.5 Autres technologies

Parity Substrate est un cadre de haut niveau pour la création de monnaies cryptographiques et d'autres systèmes décentralisés utilisant les dernières recherches en matière de technologie blockchain.

Cosmos-SDK est un framework de blockchain qui permet aux développeurs de créer facilement des applications de blockchain interopérables personnalisées au sein du réseau Cosmos sans avoir à recréer une fonctionnalité de blockchain commune, éliminant ainsi la complexité de construire une application ABCI Tendermint. Nous envisageons le SDK comme le framework de type npm pour construire des applications sécurisées de type blockchain sur Tendermint.

LotionJS vise à rendre l'écriture de nouvelles blockchains plus rapide. Il s'appuie sur Tendermint en utilisant le protocole ABCI. Lotion vous permet d'écrire des applications sécurisées et évolutives qui peuvent facilement s'interopérer avec d'autres blockchains sur le réseau Cosmos.

4 Plate-forme Asure

La plate-forme Asure se compose de composants qui fournissent le réseau et le protocole pour l'utilisation et la construction des systèmes de sécurité sociale, y compris le client, les SDK, les outils et les applications frontend. L'objectif de la plateforme est de créer un écosystème dans lequel les systèmes de sécurité sociale peuvent être développés, testés, simulés, gérés et utilisés de manière productive aussi rapidement que possible.

4.1 Client

Le client principal est le point d'entrée dans le réseau Asure, capable de faire fonctionner un nœud. Les nœuds sont connectés les uns aux autres dans un réseau peer-to-peer et relaient les nouvelles informations par le protocole Gossip. Chaque nœud conserve une copie complète d'une séquence d'événements totalement ordonnée dans Asure blockchain. Les nœuds sont utilisés pour former et exploiter le réseau Asure et s'assurer que les transactions sont incluses dans Asure blockchain.

4.2 Kits de développement logiciel (SDKs)

Le SDK fournit des fonctionnalités standardisées sur lesquelles les applications peuvent être construites. Notre objectif premier est de simplifier le développement de nouvelles solutions écosystémiques afin qu'elles ne nécessitent que peu ou pas de soutien de la part des développeurs.

4.3 Outils

Les outils supportent la création, le test et la simulation des solutions créées sur le réseau Asure et blockchain et permettent d'accélérer le processus de développement.

4.4 Applications frontales

Afin d'obtenir l'acceptation des utilisateurs, les applications standard de blockchain sont fournies, telles que blockchain-explorer, pool, applications mobiles (Android, iOS,) avec un portefeuille pour rendre possible l'expérience des paiements mobiles à une échelle globale, ainsi que de libérer le plein potentiel du commerce mobile.

5 Travail Antérieur

Dans le domaine de la sécurité sociale, Asure se concentre principalement sur l'assurance pension. Dans le cadre de la recherche en cours, nous avons porté les aspects spécifiques du système de retraite allemand sur Ethereum Blockchain. En nous basant à la fois sur notre expérience pratique et sur notre expertise de plusieurs années de travail dans le domaine de l'assurance, nous avons développé l'ossature théorique du fonctionnement d'un système de retraite décentralisé ainsi que la mise en œuvre d'un tel système de preuve de concept.

5.1 Recherche sur la technologie et l'automatisation de blockchain

Fabian Raetz, directeur technique d'Asure, a réalisé un projet de recherche à l'Université des sciences appliquées et de l'art de Dortmund en 2013 où il a analysé les technologies émergentes de blockchain et leurs éventuelles applications. [18]

En 2014, une petite équipe dirigée par Paul Mizel et Fabian Raetz a développé sa propre monnaie basée sur blockchain comme preuve de concept et a testé différents types de problèmes de blockchain et de systèmes économiques (NRJ Coin). [19]

Paul Mizel a constitué une équipe à Kiev fin 2015 pour les projets d'innovation basés sur l'IA "Insure Chat", "Insure Assistant" et "Insure Advisor". Les applications qui en ont résulté étaient des chatbots entièrement automatisés pour le support, la gestion des réclamations et d'autres tâches avec un mécanisme d'apprentissage unique et une connexion aux plateformes sociales comme Facebook, Telegram, Skype et autres.

Pile technologique : IBM Watson, Microsoft Bot Framework, MS Luis,.NET. Algorithmes utilisés : Text Mining, analyse de régression, SVMs, réseaux de neurones.

5.2 Système de retraite allemand

Afin de démontrer le potentiel de la sécurité sociale basée sur blockchain, Asure a créé un prototype basé sur le modèle du système légal allemand de retraite par répartition.

L'Asure dApp deviendra l'implémentation de référence pour les dApps utilisant blockchain et la plate-forme Asure.

Il comprendra

- une étude de faisabilité technique du système de retraite légal allemand mis en place sur Blockchain Ethereum et sur le protocole / plate-forme Asure.
- une implémentation complète de portefeuille.
- une vue d'ensemble et la gestion de vos polices d'assurance.
- un magasin d'assurance pour trouver et acheter des polices d'assurance.

Veuillez essayer l'Asure dApp qui fonctionne actuellement sur le testnet Ethereum Rinkiby : https://dapp.asure.io

5.3 Système décentralisé des pensions

Pour démontrer que Blockchain peut résoudre les problèmes à l'échelle mondiale, Asure a également mis au point un prototype de système mondial de retraite entièrement décentralisé, qui n'est donc entre les mains ni des gouvernements ni d'aucune compagnie d'assurance.
Il s'agit d'une expérience en phase alpha conçue pour montrer comment les systèmes de sécurité sociale peuvent être améliorés à l'avenir à l'aide de la technologie blockchain. L'idée est de mettre en place un système de retraite par répartition sur Ethereum Blockchain. Les membres versent leurs cotisations à l'ETH et reçoivent en échange des jetons ERC20. Aucune cotisation n'est investie sur le marché des capitaux et, par conséquent, aucun intérêt n'est gagné. Au lieu de cela, les EPF versées sont utilisées directement pour le paiement des créances de prévoyance en suspens. Le montant de la pension à verser dépend du nombre de jetons de pension dont dispose le retraité, c'est-à-dire combien de cotisations il a versé dans le système.

En règle générale, les systèmes par répartition ne fonctionnent que parce que les États introduisent des systèmes de sécurité sociale obligatoires et peuvent donc garantir un nombre stable de membres et de cotisations. Dans un système de pension décentralisé, personne ne peut être contraint de devenir membre. L'adhésion d'Asure crée plusieurs incitations qui sont destinées à conduire à une acceptation de masse.

Dans le système de pension décentralisé comme dans un système classique, celui qui cotise le plus perçoit une pension plus élevée. La longévité de l'épargne joue également un rôle. Plus les versements réguliers sont longs, plus la rente sera versée longtemps.

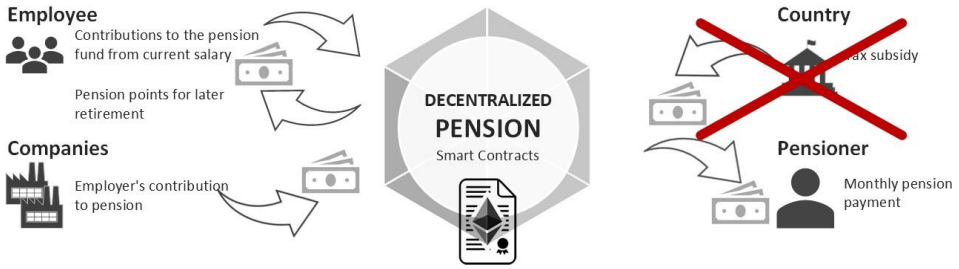

Figure 4: Modèle PAYG

Le dApp de pension décentralisée Asure fonctionne actuellement sur le testnet d'Ethereum Rinkeby. Il a été développé dans le cadre du hackathon ETHBerlin et peut être consulté via le lien suivant : `https://ethberlin.asure.io`

La pension est un pari que la valeur que je verse est au moins aussi grande, sinon plus grande, que le paiement. La pension décentralisée est basée sur le système de pension allemand et a mis en place un "contrat de génération". La jeune génération paie la génération plus âgée en fonction de ses possibilités et, en retour, les droits à pension sont symbolisés, sous la forme de jetons de droits à pension (PET).

Des modèles incitatifs ont été élaborés dans le cadre du projet

Le système exclut l'administration de l'âge, évitant ainsi la fraude et les preuves. Le temps est divisé en périodes où une période est un mois. Au cours de chaque période, des dépôts peuvent être effectués. Pour chaque période, un prix indicatif est fixé, qui peut changer si la médiane des dépôts de la période précédente présente une grande différence par rapport au prix indicatif.

Si le nombre maximum de périodes a été payé, le nombre maximum de versements de pension est également possible. Supposons que le maximum le nombre de périodes est de 480, soit 40 ans. Pour des versements mensuels de 40 ans, il y a droit à une rente de 40 ans. Si quelqu'un n'utilise le système que depuis 2 ans, l'application est pour 1 mois seulement. L'incitation à utiliser le système au maximum récompense les participants en leur accordant une période d'admissibilité à la pension plus longue.

$$MoisIntitulés = \frac{MoisPayés^{2}}{12 \cdot 40ans} \quad (1)$$

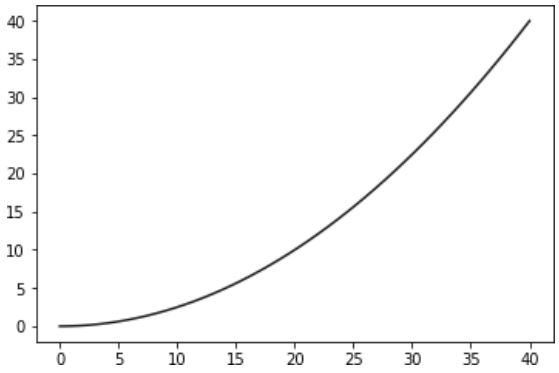

Figure 5: Rentes décentralisées versées par rapport aux années perçues

Étant donné que tout le monde peut payer des montants différents dans le système, le payeur maximum a droit à une double pension au maximum. Tous ceux qui paient plus que le prix cible de la période recevront plus de PET jusqu'à un maximum de 2 PET par période. Maximum possible de 960 PET, ce qui permet de redistribuer deux fois plus de PET qu'une personne qui active 480 PET par la suite.

$$DPT = \begin{cases} 1 + \frac{montant - montant_{max}}{prixCible - montant_{max}} * DTP & montant \ \ prixCible \\ \frac{montant - montant_{min}}{prixCible - montant_{min}} * DTP_{bonus} & sinon \end{cases} \quad (2)$$

$$prixCible - montant_{max} \neq 0 \quad and \quad prixCible - montant_{min} \neq 0 \quad (3)$$

Comme autre incitatif pour les adopteurs précoces, un bonus a été fourni dans le système qui a un multiplicateur de 1,5 et avec le temps logarithmique approchant logarithmiquement 1,0, il est prévu d'approcher annuellement.

$$DTP_{bonus} = f(an) = 1.5 - 0.12 * log(an) \quad (4)$$

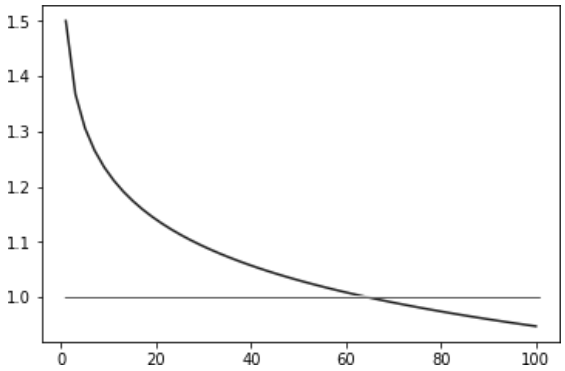

Figure 6: Prime de retraite décentralisée par année

Si tout le monde quitte le système, les derniers participants sont récompensés davantage, ainsi nous garantissons que le système reste lucratif, avec zéro participant dans le système, le système est remis à son état initial.

Par la limitation sur 2 PET au maximum ou avec le facteur 1,5 initialement 3 PET par période dans les premières années une possibilité d'utilisation résulte avec plusieurs comptes dans le système à payer dans lequel le système empêche que les PET ne soient pas transférables.

A l'aide de ces incitations et d'une conception transparente et d'une approche DAO transparente, cela commencera comme une expérience sociale après les simulations nécessaires et les ajustements de paramètres sur Ethereum mainnet.

Avantages

La pension indépendante Crypto présente de nombreux avantages, le contrat intergénérationnel permet la sécurité de l'inflation. Il est autonome et décentralisé selon l'idée du DAO. Il n'y a pas d'intermédiaire. La confidentialité est assurée car aucune donnée personnelle n'est nécessaire pour participer au système. Il est totalement transparent car toutes les transactions sont sur le blockchain et il est également de source ouverte.

En savoir plus...

Nous avons résumé nos idées sur la façon dont un système de retraite de pair à pair fondé sur la redistribution pourrait se présenter et partager nos résultats avec l'ensemble de la collectivité.

Papier de dépôt: `https://www.asure.network/asure.depot.en.pdf`

6 Futur Travail

Ce travail présente un chemin cohérent vers la construction du réseau Asure ; cependant, nous considérons également ce travail comme un point de départ pour de futures recherches sur les systèmes décentralisés de sécurité sociale. Dans cette section, nous identifions et remplissons deux catégories de travaux futurs. Cela comprend les travaux qui ont été achevés et qui attendent simplement une description et une publication, ainsi que des questions en suspens pour améliorer les protocoles actuels.

6.1 Travaux en cours

Les sujets suivants représentent les travaux en cours.

- Implémentation Plasma MVP.
- Application mobile (Android, iOS)
- Recherche décentralisée sur les systèmes de sécurité sociale.
- Contrats et protocoles de l'interface Asure-in-Ethereum.
- Une spécification de protocole Asure entièrement implémentable.

6.2 Questions ouvertes

Il y a encore des points à améliorer qui peuvent avoir une incidence positive sur le rendement du réseau. Elles peuvent être abordées plus tard après avoir recueilli suffisamment de statistiques sur lesquelles on peut se baser pour décider de l'importance et de la nécessité d'apporter des changements :

- Une meilleure solution pour les stratégies d'entrée et de sortie de masse.
- Une solution sécurisée pour le problème de non-disponibilité des données.
- Une application plus pratique de SNARK/STARK.
- De meilleures stratégies pour accélérer la mise en œuvre des systèmes de sécurité sociale et des nouveaux modèles économiques.
- Une meilleure primitive pour la fonction Proof-of-Stake Prove, qui est publiquement variable et transparente.

Comme la sécurité sociale n'est qu'une forme d'assurance spécialisée, il est évident qu'il faut également soutenir les assurances décentralisées sur la plate-forme et qu'il s'agit d'un bon complément pour étendre cette plate-forme au marché. L'écosystème Asure est constitué du réseau Asure, du protocole Asure, de la plate-forme Asure et des applications tierces potentielles dans le domaine de la sécurité sociale et de l'assurance. L'acceptation de l'écosystème augmentera régulièrement en raison des effets de réseau et des effets de synergie qui en résulteront.

7 Organisation

La Fondation Asure est une organisation à but non lucratif qui repose sur trois piliers principaux : l'innovation, la collaboration et la recherche avec une communauté de membres engagés dans la recherche et le développement de solutions nouvellement développées créées sur le réseau Asure, Blockchain, et la plate-forme pour concevoir des solutions de Blockchain avec les systèmes de sécurité sociale et d'assurance dans un mode DAO.

La fondation comprend des chercheurs en technologie ainsi que des experts en assurance. La Fondation Asure fait partie intégrante de notre travail, ce qui nous permet de coordonner les interactions dans les différentes parties de l'écosystème.

8 Remerciements

Ce travail est l'effort cumulé de plusieurs personnes au sein de l'équipe de la Fondation Asure, et n'aurait pas été possible sans l'aide, les commentaires et la révision des collaborateurs et conseillers de la Fondation Asure. Nous remercions également tous nos collaborateurs et conseillers pour leurs entretiens utiles, en particulier Andrey Kuchaev, Alexander Bohner, Dirk Mattern, Dennis Rittinghof, Michael Lurz, Emanuel Kuceradis et le professeur Dr Hirsch.

Conclusion

Bien que la recherche de solutions de mise à l'échelle fonctionnelles concernant les systèmes en blockchain soit un vaste sujet et nécessite beaucoup plus de recherche en général, les évaluations dans ce document indiquent que des solutions efficaces pour améliorer ou même remplacer les

systèmes existants peuvent être élaborées en utilisant blockchain tout en maintenant les avantages financiers et socio-culturels. Le plasma a un grand potentiel en tant que base technologique de mise à l'échelle spécifiquement pour les systèmes de sécurité sociale basés sur blockchain. Compte tenu de plusieurs difficultés comme l'indisponibilité des données, d'autres problèmes et de la grande communauté qui travaille sur ces questions, il s'agit d'un chemin caillouteux, mais aussi d'un chemin faisable.

Chez Asure, nous pensons que l'avenir de la sécurité sociale et de l'assurance sociale sera défini par des technologies de blockchain de manière décentralisée, ce qui crée une toute nouvelle expérience orientée vers le monde numérique. Elle ne peut être réalisée qu'en utilisant une plate-forme de blockchain décentralisée comme base pour créer un réseau, blockchain, une plate-forme et un protocole pour toutes sortes de risques dans le monde.

Le concept de mise en œuvre de la sécurité sociale par le biais de blockchain est unique et offre un énorme potentiel pour améliorer la vie humaine dans le monde entier. La motion en faveur de la sécurité sociale sur Blockchain apporterait plus de confiance, de satisfaction, de liberté et de paix mondiale. Asure est conceptuellement ouvert, et nous pensons qu'il est très bien adapté pour servir de plate-forme fondamentale à un très grand nombre de solutions de sécurité sociale dans les années à venir.

Avec notre vente symbolique, nous voulons qu'un large éventail de personnes participent à ce voyage à long terme et créent une histoire à succès en changeant le fonctionnement de la sécurité sociale dans notre nouvelle ère numérique. Participez à ce voyage et participez à notre Token Generation Event - nous nous réjouissons de vous accueillir à bord !

Site Web	`https://asure.network`
Medium:	`https://medium.com/AsureNetwork`
Twitter:	`https://twitter.com/AsureNetwork`
Chaîne Telegram:	`https://t.me/AsureNetwork`
Facebook:	`https://fb.me/AsureNetwork`

Liste des tableaux

Liste des figures

Références

[1] World social protection report 2017-2019, *Universal social protection to achieve the sustainable development goals*, International Labour Office, Geneva, 2nd edition, 2017.

[2] Etherscan, *Ethereum Transaction Chart*, https://etherscan.io/chart/tx, 2017.

[3] Worldometers, *World Population Forecast (2020-2050)*, http://www.worldometers.info/world-population/, 2017.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf, 2009.

[5] Carmela Troncoso, Marios Isaakidis,George Danezis, Harry Halpin, *Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments, In Proceedings on Privacy Enhancing Technologies*, De Gruyter Open, volume 2017, 2017.

[6] David Knott, *Construction of a Plasma Chain 0x1*, https://blog.omisego.network/construction-of-a-plasma-chain-0x1-614f6ebd1612, 2017.

[7] GDPR Info, *General Data Protection Regulation*, https://gdpr-info.eu/, 2018.

[8] Joseph Poon and Vitalik Buterin, *Plasma: Scalable Autonomous Smart Contracts*, https://plasma.io/, 2017.

[9] Minimal Viable Plasma, https://ethresear.ch/t/minimal-viable-plasma/426, 2017.

[10] Plasma Cash, https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298, 2017.

[11] Ethereum, https://ethereum.org, 2014.

[12]Deutsche Rentenversicherung, *Wichtige Eckzahlen*, https://www.deutsche-rentenversicherung.de/Allgemein/de/Navigation/6_Wir_ueber_uns/02_Fakten_und_Zahlen/03_statistiken/wichtige_eckzahlen_node.html, 2016.

[13] Andrew Tayo, *Proof of work, or proof of waste?*, https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025, 2017.

[14] Jae Kwon, *Tendermint: Consensus without Mining*, https://tendermint.com/static/docs/tendermint.pdf, 2014.

[15] Zach, *Tendermint: Benchmarks*, https://github.com/tendermint/tendermint/wiki/Benchmarks, 2018.

[16] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev, *Scalable, transparent, and post-quantum secure computational integrity*, https://eprint.iacr.org/2018/046.pdf, 2018.

[17] Christian Reitwiessner, *zkSNARKs in a nutshell*, http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf, 2016.

[18] Fabian Raetz, *Aufbau und Funktionsweise des Bitcoin-Protokolls*, 2014.

[19] NRJ Coin Project, *NRJ Coin Project*, https://github.com/nrjcoin-project, 2014.

[20] European Report on Development (ERD): Deutsches Institut für Entwicklungspolitik, https://www.die-gdi.de/erd/, 2018.

[21] Health as Human Capital: Theory and Implications A New Management Paradigm, HCMS Group, http://www.hcmsgroup.com/wp-content/uploads/2012/05/WP01-HHC-Theory-and-Implications-2012-01-161.pdf, 2012.

[22] etherscan.io: gaslimit chart, https://etherscan.io/chart/gaslimit, 2012.

Fait avec ♥ en Allemagne