Hydro Raindrop

Authentification publique sur la Blockchain

Janvier 2018

TABLE DES MATIÈRES

Sommaire

HYDRO: Étymologie – du grec ancien ὕδρο (*hydro*), qui vient du mot ὑδωρ (eau).

Hydro permet aux systèmes privés nouveaux et préexistants d'intégrer et d'exploiter impeccablement la dynamique immuable et transparente d'une blockchain pour améliorer la sécurité des applications et des documents, la gestion des identités, les transactions et l'intelligence artificielle.

Dans ce document, une référence sera faite aux systèmes privés, tels que les API, qui utiliseront la blockchain publique d'Hydro pour améliorer la sécurité de l'authentification publique..

La technologie proposée s'appelle «Raindrop» - une transaction qui s'effectue via un smart contract qui valide publiquement l'accès privé au système et peut compléter les méthodes de certification privées existantes. La technologie vise à fournir une sécurité supplémentaire pour les données financières sensibles qui sont de plus en plus exposées au piratage et aux violations.

La mise en œuvre initiale de Hydro Raindrop est réalisée sur la plate-forme API Hydrogen. Ce package d'API modulaire est disponible pour les entreprises et les développeurs du monde entier pour initier, construire, tester et déployer des plates-formes et des produits de technologie financière sophistiqués.

Hydro Raindrop sera disponible pour la communauté mondiale des développeurs en tant que logiciel open source afin que les développeurs puissent intégrer Hydro Raindrop à n'importe quelle API REST.

Blockchain & Ethereum

Hydro est en cours de mise en œuvre dans le réseau Ethereum. Avant de donner plus de détails sur le projet, il est important de comprendre quelques idées fondamentales pour Blockchain et Ethereum.

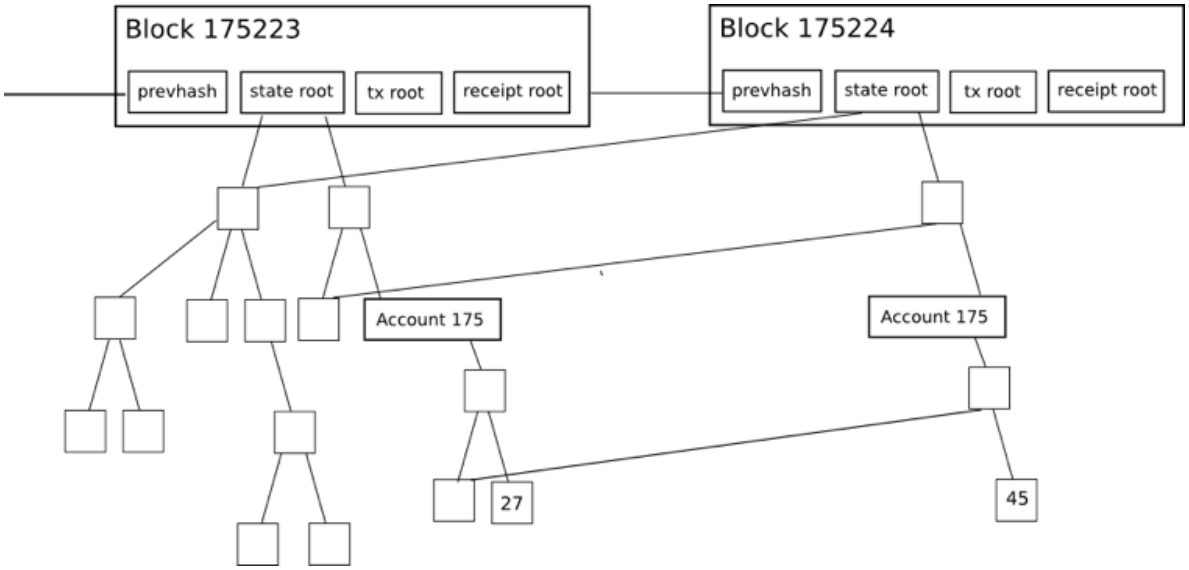
Construire sur Ethereum

Tout comme les applications comme Snapchat ont été construites avec Swift et d'autres outils offerts sur la plate-forme Apple iOS, les applications blockchain peuvent également être construites sur Ethereum. Snap Inc. n'avait pas besoin de construire iOS, il l'utilisait comme infrastructure pour lancer une application de média social qui change la donne.

Le projet Hydro est similaire. Il est basé sur des milliers de développeurs dans le monde, travaillant pour rendre la technologie blockchain sous-jacente plus rapide, plus puissante et plus efficace. Hydro utilise cette infrastructure en constante amélioration en développant des interactions centrées sur les produits autour de la technologie blockchain, ce qui peut apporter des avantages significatifs aux applications de services financiers.

Arbres de Merkle

Les arbres de Merkle sont utilisés dans les systèmes distribués pour une vérification efficace des données. Ils sont efficaces car ils utilisent des "hashes" au lieu de fichiers complets. Les hashes sont des moyens de coder des fichiers qui sont beaucoup plus petits que le fichier lui-même. Chaque en-tête de bloc dans Ethereum contient trois arbres Merkle pour les transactions, les reçus et les états:



Source: Merkling in Ethereum; Vitalik Buterin, Ιδρυτής Ethereum

Cela permet à un light client d'obtenir facilement des réponses vérifiables à des requêtes, telles que:

- Ce compte existe-t-il?
- Quel est le solde actuel?
- Cette transaction a-t-elle été incluse dans un bloc particulier?
- Un événement spécifique s'est-il produit sur cette adresse aujourd'hui?

Smart Contracts

Une caractéristique clé d'Ethereum et d'autres réseaux basés sur les blockchain est les smart contracts. Ce sont des blocs de code auto-exécutables qui peuvent interagir avec plusieurs parties, éliminant le besoin d'intermédiaires fiables. Le code d'un smart contract peut être considéré comme similaire aux clauses légales d'un contrat papier, mais il peut également obtenir davantage en raison de fonctionnalités étendues. Ces contrats peuvent comporter des règles, des conditions et des pénalités pour non-conformité ou autres procédures. Lorsqu'elles sont activées, elles sont exécutées comme indiqué à l'origine lorsqu'elles sont installées dans la public chain, offrant des données intégrées inchangées et décentralisées.

Les smart contracts sont un outil important pour construire sur l'infrastructure Ethereum. La fonctionnalité de base de la couche blockchain Hydro est obtenue grâce à des contrats personnalisés, comme indiqué plus loin dans cet article.

Machine virtuelle Ethereum

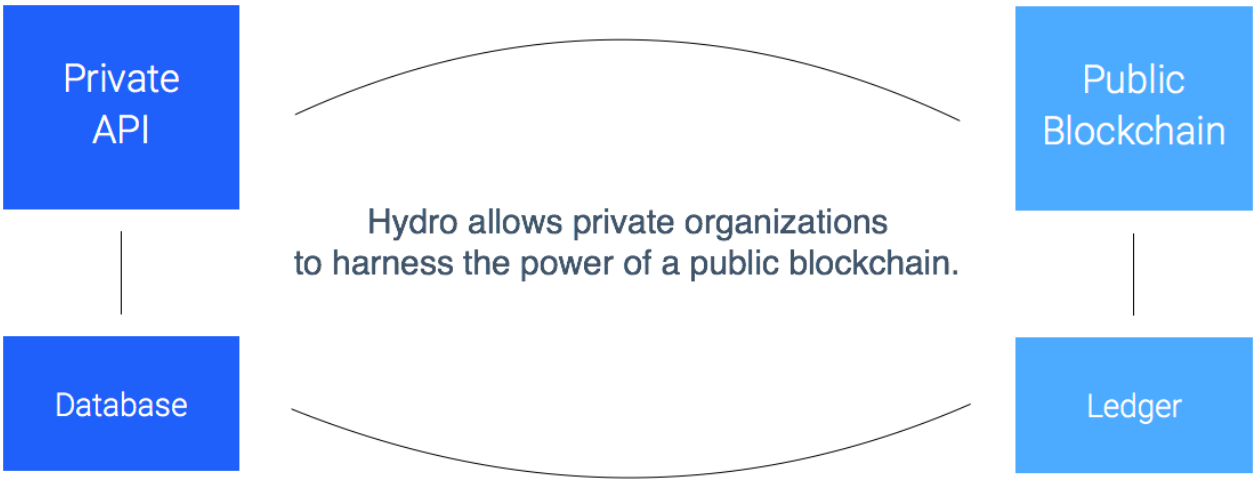
La machine virtuelle Ethereum ou bien Ethereum Virtual Machine (EVM) est l'environnement d'exécution pour les smart contracts dans Ethereum. Le EVM aide à prévenir les attaques par déni de service (DoS), assure que les programmes ne sont pas affectées et permet une communication transparente. Les actions sur le EVM ont un coût qui leur est associé, appelé le gas, qui dépend des ressources de calcul nécessaires nécessaires. Chaque transaction a une quantité maximale de gas qui peut être utilisée, appelée une limite de gas. Si le gas consommé par une transaction atteint la limite, il interrompt le processus.

Public Ledger

Public Ledger pour les systèmes privés

Les systèmes qui gèrent des plates-formes de services financiers, des sites Web et des applications peuvent souvent être décrits comme des médias en continu: ils envoient, reçoivent, stockent, mettent à jour et traitent des données pour les personnes avec lesquelles ils interagissent. En raison de la nature de ces données et des services financiers en général, ces systèmes ont souvent des fonctions complexes de manière privée et centralisée. La confiance dans les structures privées, à son tour, ouvre la porte à une variété de fusibles, de transparence, ainsi que des gains d'efficience afin d'adopter l'intégration des forces extérieures qui dépassent la portée du système interne.

Tel est le cas de la plate-forme API d'Hydrogen. Hydro cherche à exploiter les avantages mentionnés ci-dessus en permettant aux utilisateurs d'Hydro d'interagir avec une blockchain d'une manière parfaitement intégrée dans l'écosystème de base d'Hydro.

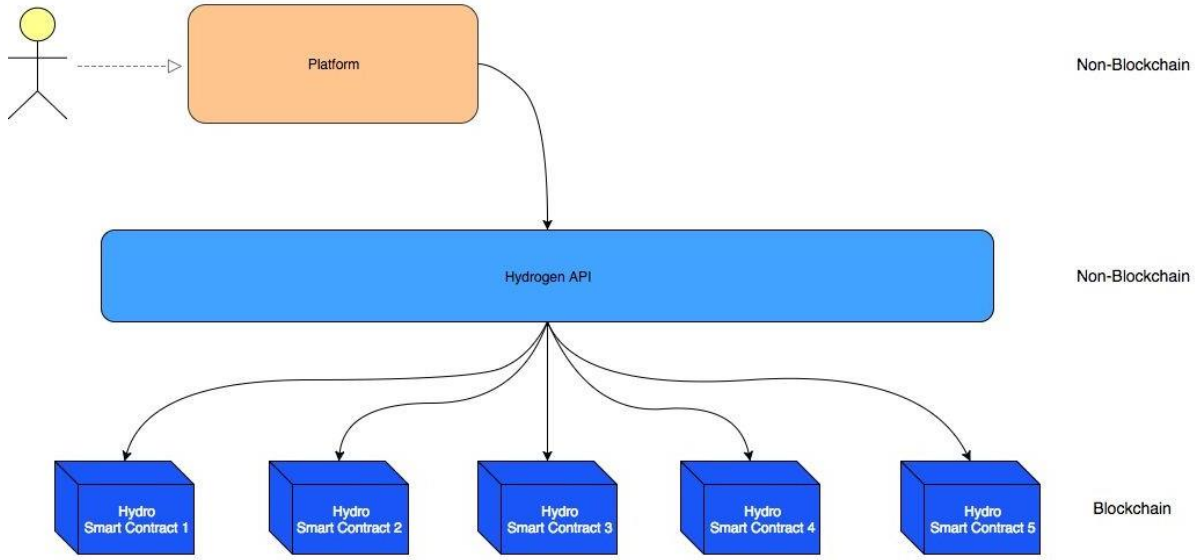


Les fonctions publiques de blockchain peuvent être exécutées avant, pendant ou après des opérations privées. L'interaction entre les données privées et publiques peut servir à valider, sceller, enregistrer ou améliorer les processus au sein d'un écosystème.

L'éthique de ce modèle rend les processus plus robustes en exploitant les avantages de la technologie blockchain, en particulier là où elle peut produire les effets les plus positifs. Bien que cette structure hybride puisse ne pas s'appliquer à toutes les plateformes, Hydro met l'accent sur la création de valeur pour les situations dans lesquelles elle est en place.

Architecting pour l'adoption

Hydro est différent de beaucoup d'initiatives de blockchain existantes car il peut être indépendant et placé autour de systèmes nouveaux ou préexistants sans nécessiter de changement systématique. Au lieu de remplacer, Hydro cherche à s'améliorer. Les plates-formes et les institutions associées à l'API Hydrogen peuvent avoir un accès automatique à la blockchain.



L'éventail des plateformes de services financiers pouvant exploiter l'Hydrogen est vaste. Ces plates-formes peuvent alimenter pratiquement n'importe quelle expérience, héberger un nombre illimité de services propriétaires, effectuer des opérations de données privées et évoluer dans n'importe quel environnement. Ceci est réalisé grâce à l'adaptation structurelle de l'Hydrogen et travaille avec Hydro, agissant comme un guide complémentaire à l'adoption.

Raindrop

Construit dans le public ledger d'Hydro, il y a une blockchain basée sur le service d'authentification "Raindrop". Cela fournit une couche de sécurité visible distincte, inchangée, à l'échelle mondiale, qui vérifie si une demande d'accès provient d'une source approuvée.

Les protocoles d'authentification privés comme OAuth 2.0 offrent différents niveaux de robustesse et d'utilité pour la gamme d'instances d'utilisation existantes. Il n'y a pas besoin de rivaliser ou d'essayer de remplacer ces protocoles. Hydro offre un moyen de les renforcer en intégrant les mécanismes de blockchain dans le cadre du processus d'authentification. Cela peut ajouter une couche de sécurité utile pour aider à prévenir les violations du système et la fuite d'informations confidentielles.

Avant d'examiner l'aspect technique de Raindrop, nous examinerons le problème qu'il tente de résoudre.

La situation de la sécurité financière

L'avènement de l'ère des données («âge des données») a apporté la vulnérabilité aux systèmes, ce qui est particulièrement important pour les services financiers. Les plates-formes financières peuvent être considérées comme des passerelles vers un grand nombre de données privées et sensibles, telles que les numéros d'identité, les enregistrements de compte et les historiques de transactions. En raison de l'importance des données d'identification, l'accès à partir de sources non désirées, vous suivez souvent des résultats catastrophiques.

Le cabinet de recherche Trend Micro publié un rapport que les articles volés trouvés de renseignements personnels identifiables (PII) sont vendus sur le Web profond pour aussi peu que 1 $, les documents numérisés comme les passeports sont disponibles pour aussi peu que 10 $, et les identifiants bancaires pour seulement 200 $, ce qui rend la distribution données volées de plus en plus fragmentées et introuvables.

Malheureusement, le système financier actuel n'a pas de résultats immédiats en matière de prévention, de diagnostic et de communication des violations de données avec ses parties prenantes.

- Selon une étude récente de Javelin Strategy & Research intitulée - *The 2017 Identity Fraud Study* - 16 milliards de dollars ont été volés à 15,4 millions de consommateurs américains en 2016 en raison de défaillances du système financier pour protéger les informations personnelles identifiables (PII).

- En avril 2017, Symantec a publié le rapport *Internet Security Threat Report*, qui estime qu'au cours de l'année 2016, 1,1 milliard de fichiers PII ont été mis à la disposition de diverses sources.

- Dans l'article *2016 Year End Data Breach Quickview* de Risk Based Security, il a été constaté qu'en 2016, il y avait 4.19 violations de données dans les entreprises du monde entier, exposant plus de 4,2 milliards d'enregistrements.

- Dans *2017 Thales Data Threat Report – Financial Services Edition*, une enquête auprès des professionnels de l'informatique dans les services professionnels, a révélé que 49% des entreprises de services financiers ont subi une faille de sécurité dans le passé, 78% dépensent plus pour se protéger, mais 73% lancent de nouvelles initiatives liées à l'IA, IoT et technologies cloud avant de préparer des solutions de sécurité appropriées.

Equifax Breach

Le 29 juillet 2017, Equifax, une agence américaine d'évaluation du crédit âgée de 118 ans, a été piratée. 143 millions de consommateurs avaient des PII exposés, y compris des numéros de sécurité sociale. 209 000 clients ont eu des données de carte de crédit compromises.

Quelle était la cause de cette violation?

Il a commencé avec l'une des technologies de backend utilisées par Equifax. Struts est un framework open source pour le développement d'applications web dans le langage de programmation Java, créé par Apache Software Foundation. Le CVE-2017-9805 est un point vulnérable dans Apache Struts sur l'utilisation du plugin Struts REST avec le gestionnaire XStream pour gérer les chargements XML. En cas d'infraction, elle permet à un attaquant distant non authentifié d'exécuter du code malveillant sur le serveur d'applications pour soit prendre le contrôle de la machine, soit lancer d'autres attaques. Cela a été patched par Apache deux mois avant la violation d'Equifax.

Apache Struts contient une faille dans le plug-in REST XStream qui est déclenché car le programme désécurise de manière non sérielle l'entrée fournie par l'utilisateur dans les requêtes XML. Plus précisément, le problème se produit dans la méthode toObject () de XStreamHandler, qui n'impose aucune restriction à la valeur entrante lors de l'utilisation de la désérialisation XStream dans un objet, ce qui entraîne des vulnérabilités d'exécution de code arbitraires.

Même si le plugin REST était exposé, cela aurait-il de l'importance? Existe-t-il un moyen d'utiliser la technologie blockchain pour sécuriser les informations financières de ces 143 millions de clients tout en s'appuyant sur l'API REST en place et les systèmes Java?

Ajouter un Blockchain Layer

Il est clair que l'intégrité des portes de données financières peut être améliorée.

Regardons comment un niveau de sécurité supplémentaire peut être atteint grâce à Hydro.

Les mécanismes de consensus fondamentaux du réseau Ethereum assurent une validité transactionnelle car les participants traitent collectivement les transactions correctement signées. Ce fait conduit à la décentralisation et à la stabilité, mais surtout, il fournit un vecteur pour atténuer l'accès non autorisé à une passerelle qui traite des données sensibles.

Avec Hydro, l'authentification peut dépendre des opérations de transaction dans la blockchain. Par exemple, une API peut choisir de valider des développeurs et des applications en leur demandant de démarrer des transactions spécifiques avec une charge de données particulière entre des adresses spécifiques dans la chaîne de blocs, tant qu'un protocole d'authentification démarre.

Le Hydro Raindrop

La Rain («pluie») contient des paquets d'eau emballés allant de 0,0001 à 0,005 cm de diamètre. Dans une tempête typique, il y a des milliards de ces paquets, chacun avec une taille, une vitesse et une forme aléatoires. Pour cette raison, on ne peut pas prédire avec précision la nature exacte de la pluie. De même, chaque transaction d'authentification Hydro est unique et pratiquement impossible à réaliser au hasard - nous l'appelons donc Raindrops.

Les plateformes de services financiers utilisent généralement la vérification du microcrédit pour valider les comptes des clients. L'idée est simple: la plateforme crée de petits dépôts de montants aléatoires dans les comptes bancaires déclarés par les utilisateurs. Afin de prouver que l'utilisateur détient effectivement ce compte, il doit transférer les montants de dépôts à la plateforme, qui sont ensuite validés. La seule façon dont l'utilisateur peut connaître les montants valides (sauf pour deviner) est l'accès à ces comptes bancaires.

La vérification basée sur Raindrop with Hydro est proportionnelle. Au lieu d'envoyer un montant à l'utilisateur et de le relayer, nous définissons une transaction et l'utilisateur doit l'exécuter à partir d'un porte-monnaie bien connu. La seule façon qu'un utilisateur peut faire une transaction valide est d'accéder à ce portefeuille.

En utilisant Raindrops, le système et l'accessor peuvent suivre les efforts d'autorisation dans un public ledger inchangé. Cette transaction basée sur blockchain est déconnectée des fonctions système de base, apparaissant sur un réseau distribué, et dépend de la propriété des clés privées. Par conséquent, il sert d'élément de validation utile.

Un regard attentif

Le processus de vérification de l'identité d'Hydro comporte quatre éléments:

1. *Accessor* - Le groupe cherche l'accès à un système. Dans le cas d'Hydrogen, l'accessor est une institution financière ou une application utilisant les API Hydrogen pour son infrastructure numérique de base.
2. *System* - Le système ou la passerelle auquel accède l'accessor. Pour Hydrogen, le système est l'API Hydrogen elle-même.
3. *Hydro* - Le module utilisé par le Système pour communiquer et s'interfacer avec la blockchain.
4. *Blockchain* – Le public ledger distribué qui traite les transactions HYDRO et contient les contrats d'Hydro smart, par lesquels les informations peuvent être importées, reçues ou exploitées.

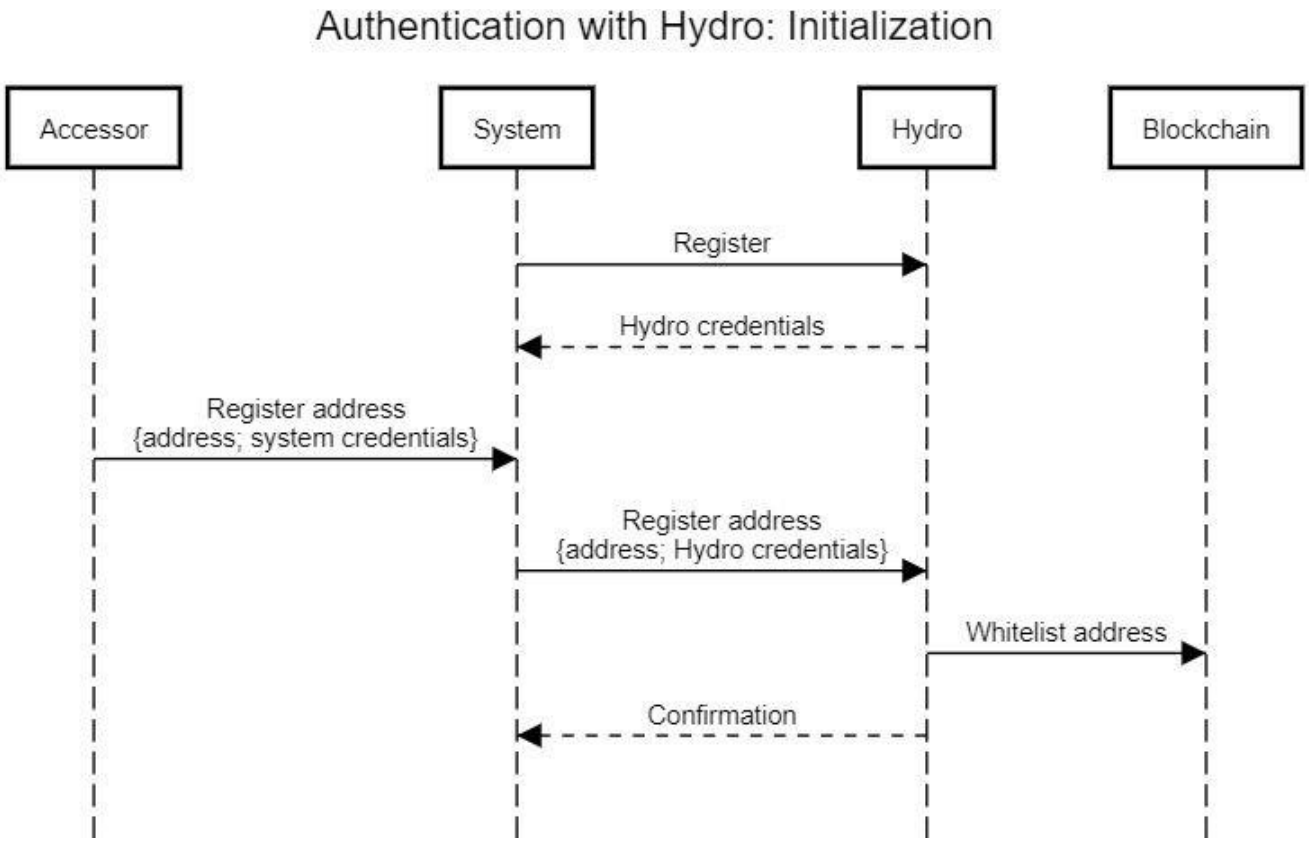
Chaque Raindrop se compose d'un ensemble de cinq paramètres de trading:

1. *Sender* - L'adresse pour commencer la transaction.
2. *Receiver* - La destination de la transaction Cela correspond à l'appel d'une méthode dans un Hydro smart contrat.
3. *ID* - Un identifiant associé au système.
4. *Quantity* - Un nombre précis d'HYDRO à envoyer.
5. *Challenge* - Une chaîne alphanumérique générée de manière aléatoire.

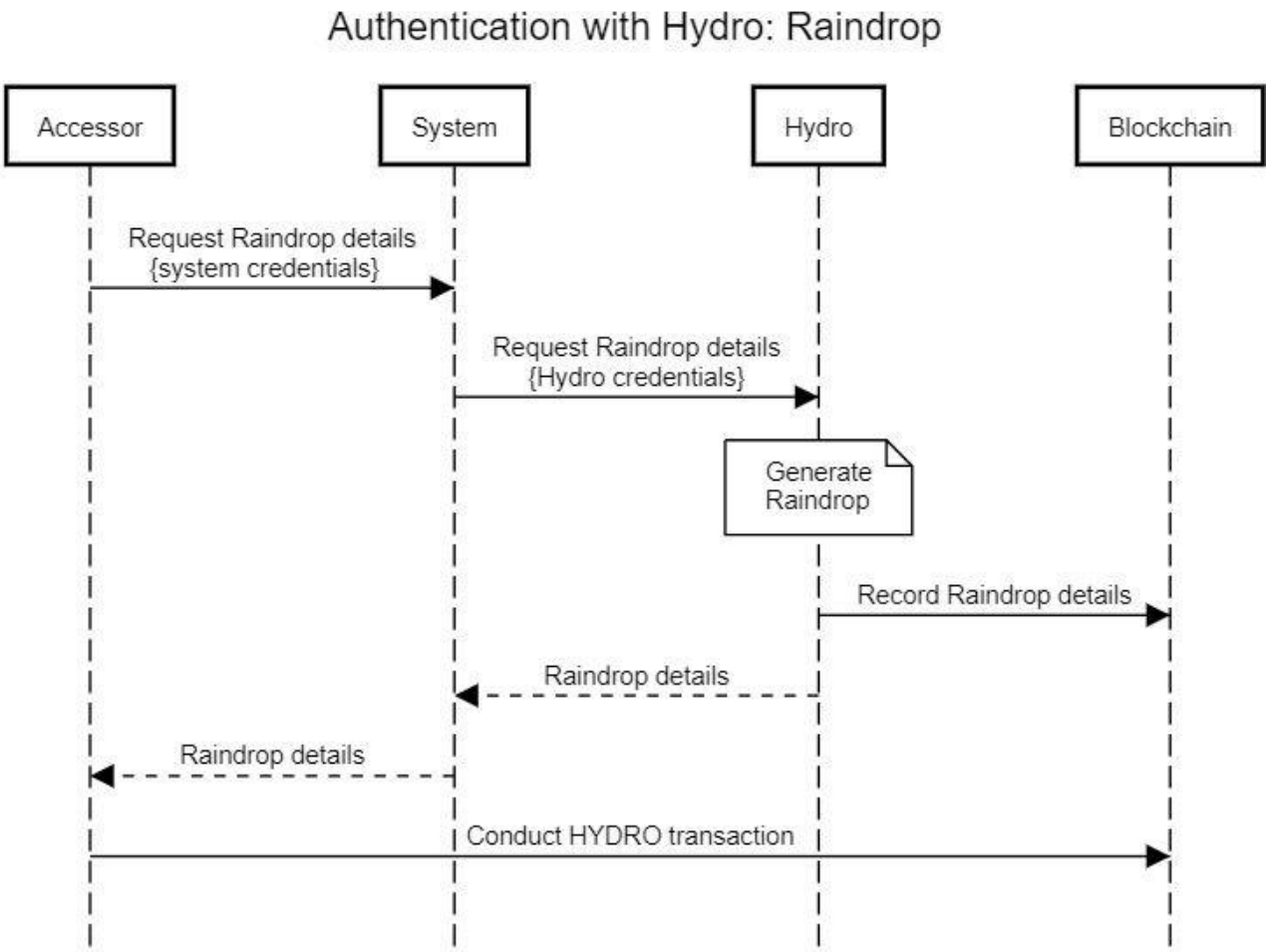
Voici un résumé du processus d'authentification, qui peut généralement être classé en trois étapes:

1. Initialization (Initialisation)
2. Raindrop
3. Validation

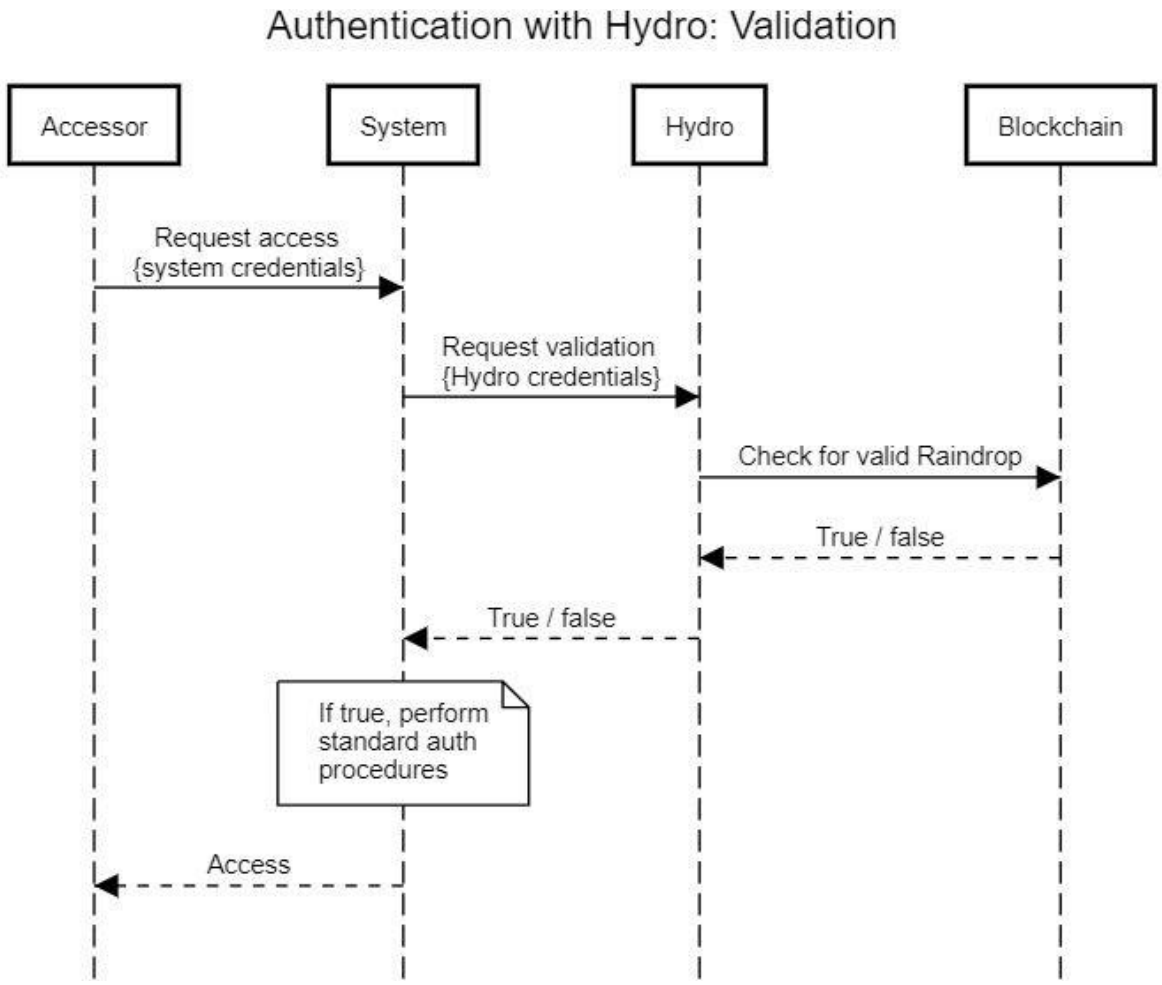
L'initialisation commence par l'enregistrement d'un système (par exemple Hydrogen) pour utiliser Hydro et obtenir des informations d'identification, permettant au système de communiquer avec la chaîne de blocs via le module Hydro. Le système embarque un accessor (par exemple une institution financière) qui enregistre une public ledger, puis transmet l'adresse enregistrée à Hydro. Cette adresse est écrite inchangée dans la blockchain, dans une whitelist stockée dans un Hydro smart contract. Le système reçoit une confirmation que l'adresse a été ajoutée à la liste blanche, qui peut également être vérifiée en tant qu'événement visible publiquement. Le système ne doit être enregistré qu'une seule fois, tandis que la whitelisting des accessor ne doit être affichée qu'une fois par accessor.



Une fois l'initialisation terminée, le noyau du processus d'authentification Hydro peut commencer. Accessor, qui doit exécuter une transaction Raindrop, initie ce processus en demandant des détails Raindrop à partir du système, et le système transfère la demande à Hydro. Hydro crée un nouveau Raindrop, stocke les détails spécifiques inchangés dans la blockchain et renvoie tous les détails à Accessor via le système. L'accesseur, avec toutes les informations requises, effectue une transaction de l'adresse enregistrée à une méthode dans le contrat Hydro smart. Si l'adresse n'est pas dans la liste blanche, l'action est rejetée. Dans le cas contraire, elle est enregistrée dans le contrat intelligent. Il est important de noter que cette transaction devrait avoir lieu en dehors du Système, directement à partir de l'Accesseur de la Blockchain, car elle doit être signée avec la clé privée de l'Accesseur (que seul l'Accesseur devrait pouvoir obtenir).



La dernière étape du processus est la validation. À ce stade, Accessor demande l'accès au système via le mécanisme du système installé. Avant d'appliquer l'un des protocoles d'authentification standard, le système demande à l'Hydro, si accessor a effectué ou non une transaction Raindrop valide. Hydro travaille avec le smart contract, vérifie la validité et répond par une détermination vrai / faux. Le système est en mesure de décider comment procéder sur la base de cette détermination - si elle est fausse (false), le système peut refuser l'accès, s'il est vrai (vrai), le système peut fournir un accès.



Si nous considérons que les informations d'identification du système de base ou le protocole de système existant en place, en tant que facteur d'authentification, il est important que Hydro fournisse un second facteur. En examinant les deux principaux vecteurs d'attaque, nous pouvons facilement confirmer son utilité:

- Vector 1 - L'attaquant vole les informations d'identification du système Accessor
    - L'attaquant tente d'accéder au système avec des informations d'identification système valides
    - Le système vérifie avec Hydro pour voir s'il existe une transaction blockchain valide
    - Hydro renvoie false, et le système refuse l'accès
- Vector 2 – L'attaquant vole la clé privée du portefeuille d'Accessor
    - L'attaquant essaie d'effectuer une transaction Hydro à partir de l'adresse enregistrée, sans avoir besoin de détails Raindrop
    - L'attaquant ne peut pas effectuer une transaction blockchain valide

- L'attaquant ne peut pas non plus demander l'accès au système sans les informations d'identification système appropriées

Il est clair que l'attaquant doit voler à la fois les informations d'identification du système de base et les clés du porte-monnaie privé de l'utilisateur pour accéder au système. À cet égard, Hydro a ajouté avec succès un facteur d'authentification supplémentaire.

Ouverture de la Raindrop au public

Bien que ce service d'authentification basé sur blockchain ait été conçu pour assurer l'écosystème de l'API Hydrogen, il est largement applicable à différentes plates-formes et systèmes. Parce que d'autres peuvent bénéficier de ce niveau de vérification et de sécurité, il est ouvert à l'utilisation.

Tout comme Hydrogen l'incorporera comme condition préalable à l'accès à l'écosystème de l'API, tout autre système peut l'ajouter aux procédures et protocoles existants. Chaque plate-forme, API, application, logiciel d'entreprise, plate-forme de jeu, etc., peut utiliser Hydro à des fins d'authentification. Le document sera disponible dans GitHub pour ceux qui veulent intégrer ce niveau de blockchain dans un cadre d'authentification ou une API REST.

Case Study - Raindrop With OAuth 2.0

Il existe des dizaines de façons dont Raindrop peut être utilisé par des organisations privées. Les API privées, les bases de données et les réseaux ont créé des systèmes élaborés de tokens, de clés, d'applications et de protocoles au cours de la dernière décennie, dans le but de sécuriser les données sensibles. Google, par exemple, est devenu l'un des fournisseurs de produits les plus populaires sur le marché avec Google Authenticator. Comme mentionné précédemment, il n'y a aucune raison de concurrencer ou de remplacer ces protocoles existants.

En tant qu'étude de cas (Case Study), nous présentons un bref aperçu de la manière dont Hydrogen implémente la certification Hydro en tant que niveau de sécurité dans le cadre de sécurité global de l'API:

1. Les partenaires de l'API Hydrogen doivent principalement avoir les adresses IP de leurs différents environnements "whitelisted".
2. Les partenaires doivent demander une "whitelisted" pour être une adresse Hydro.
3. Tous les appels aux API Hydrogen et les transferts de données sont cryptés et transmis via le protocole HTTPS.
4. Les partenaires doivent compléter une transaction Hydro Raindrop valide à partir de l'adresse Hydro enregistrée.

5. Les partenaires doivent utiliser la validation OAuth 2.0. OAuth 2.0 (Open Authorization) est un standard ouvert pour l'authentification et l'autorisation basée sur les "tokens". Hydrogen prend en charge les types de licence "Owner Password Certificates" et "Customer Certificates", et chaque utilisateur API doit fournir des informations d'identification pour une demande d'authentification.
6. Si aucun des cinq éléments ci-dessus n'est violé, le partenaire Hydrogen dispose d'un jeton unique qui doit être vérifié et vérifié avec chaque appel d'API.
7. Le "token" est valide pendant 24 heures, après 24 heures, le partenaire doit se valider à nouveau.

Si l'une de ces étapes est violée, l'utilisateur est immédiatement verrouillé par l'accès API. Un pirate ne peut pas contourner ces facteurs de sécurité en devinant au hasard, car il existe des milliards de combinaisons uniques.

L'authentification basée sur Hydro blockchain est un élément important du protocole de sécurité de l'Hydrogen. Le Groupe d'Hydrogen encourage ses partenaires à créer plusieurs portefeuilles de signatures (multi-signature wallets) et de stocker leurs clés privées dans plusieurs endroits sûrs indépendamment des autres pouvoirs, donc il n'y a pas de vulnérabilité. Un portefeuille multi-signatures correctement sécurisé est non seulement difficile à voler, mais la nature publique de la blockchain permet également une reconnaissance rapide de tout vol en rapport avec la sécurité de l'API.

Tout le monde peut voir une tentative d'authentification au Hydro smart contract, ce qui signifie que les jours où les plates-formes sont compromises pendant des mois peuvent être une chose du passé. Les hackers d'API peuvent maintenant être contrecarrés avec plus d'immédiateté en raison de la capacité de détecter des tentatives d'autorisation inattendues en temps réel, de n'importe où dans le monde.

Des risques

Tout comme les technologies naissantes, telles que les débuts des médias sociaux, des e-mails et des applications de streaming (dépendantes de la connectivité dial-up), il est important que l'équipe de développement surveille de près les nouveaux développements des volumes et des transactions d'Ethereum. Pourriez-vous imaginer YouTube essayant de lancer en 1995? Ou Instagram étant d'abord offert sur le Blackberry?

Les principaux développeurs d'Ethereum tels que Vitalik Buterin et Joseph Poon ont proposé de passer au protocole Ethereum Plasma: Scalable Autonomous Smart Contracts :

> **Le plasma est un cadre proposé pour l'exécution incitative et forcée des smart contracts qui est adaptable à un nombre significatif de mises à jour par seconde (potentiellement des milliards) permettant à la chaîne de représenter une quantité importante d'applications financières décentralisées dans le monde. Ces contrats intelligents sont encouragés à poursuivre leur fonctionnement de manière autonome via des frais de transaction de réseau, qui dépend finalement de la chaîne de blocs sous-jacente (par exemple Ethereum) pour appliquer des transitions d'état transactionnelles.**

D'autres, comme The Raiden Network, ont proposé une solution hors-chaîne (off-chain) conçue pour accélérer les transactions et réduire les frais. Actuellement, Raindrop exercera très peu de pression sur Ethereuem, donc l'évolutivité est un très faible risque de succès technologique.

Conclusion

L'immutabilité d'une blockchain publique offre de nouvelles façons d'améliorer la sécurité des systèmes privés comme les API.

Ce document a montré trois choses importantes:

1. Les public blockchains peuvent ajouter de la valeur aux services financiers.
2. Hydro Raindrop peut améliorer la sécurité des systèmes privés.
3. Il existe des applications directes de Hydro Raindrop dans la plate-forme API Hydrogen.

L'équipe de Hydro croit que le cadre mis en place pourrait constituer l'infrastructure de sécurité standard pour un nouveau modèle public-privé hybride privé, qui profitera à tous les acteurs du secteur des services financiers et au-delà.

Sources:

Ethereum; Merkling in Ethereum
Trend Micro; What Do Hackers Do With Your Stolen Identity?
Javelin Strategy & Research; *The 2017 Identity Fraud Study*
Symantec; *Internet Security Threat Report*
Risk Based Security; *2016 Data Breach Trends - Year in Review*
Thales; *2017 Thales Data Threat Report – Financial Services Edition*
Apache.org; Apache Struts 2 Documentation - S2-052
Joseph Poon and Vitalik Buterin; Plasma: Scalable Autonomous Smart Contracts