Гідро Рейндроп

Відкрита Аутентифікація На Блокчейні

Січень 2018

Зміст

Введення

HYDRO (далі, ГІДРО): Етимологія – від д.-грець. ὕδωρ – (hudro-) – вода.

Гідро дозволяє новим та існуючим приватним системам (private systems) безперешкодно інтегрувати і ще краще використовувати незмінну і прозору динаміку відкритого блокчейну (public blockchain) для підвищення безпеки додатків і документів, управління ідентифікаційної інформацією, а також для роботи з транзакціями і штучним інтелектом.

У цьому документі, буде показано, як приватні системи, такі як API, можуть використовувати відкритий блокчейн Гідро для підвищення безпеки через відкриту аутентифікацію (public authentication).

Пропонована технологія називається 'Рейндроп' - транзакція виконується через смарт контракт, який публічно перевіряє доступ до приватної системі, і може доповнити існуючі приватні методи аутентифікації. Дана технологія покликана забезпечити додаткову безпеку для важливих фінансових даних, які все частіше піддаються ризику від злому і порушень.

Первісна реалізація Рейндропа здійснена на платформі Hydrogen API. Цей модульний набір API команд доступний підприємствам і розробникам по всьому світу для створення прототипів, збірки, тестування і розгортання складних фінансових технологічних платформ і продуктів.

Рейндроп буде доступний світовій спільноті розробників як програмного забезпечення з відкритим вихідним кодом, який дозволить розробникам інтегрувати Рейндроп з будь-яким REST API.

Блокчейн і Ефіріум

Гідро реалізується на мережі Ефіріуму. Але перш, ніж представити більше деталей про проект, важливо пояснити деякі фундаментальні ідеї про блокчейн і Ефіріум.

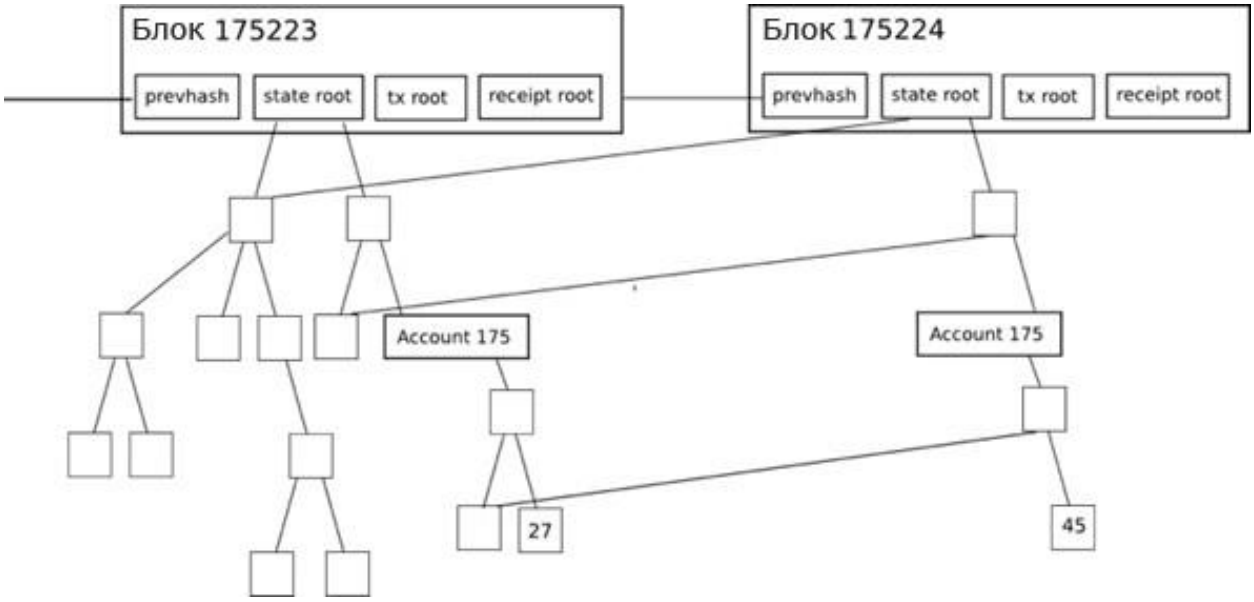
Разробка на базі Ефіріуму

Подібно до того, як і багато програм, наприклад Snapchat, були побудовані за допомогою Swift і інших інструментів пропонованих поверх платформи Apple iOS, так і блокчейн додатки можуть бути реалізовані на базі Ефіріуму. Корпорації Snap не треба було створювати iOS, замість цього, вона використовувала її як інфраструктуру для запуску соціального медіа додатку, який міняє правила гри.

Проект Гідро володіє подібними властивостями. Він спирається на тисячі розробників по всьому світу, які працюють над тим, щоб зробити базову технологію блокчейн швидше, сильніше і ефективніше. Гідро підтримує цю постійно покращуючу інфраструктуру, розробляючи орієнтовані на кінцевий продукт засоби взаємодії, що використовують технологію блокчейн, які можуть запропонувати відчутні переваги для додатків фінансових послуг.

Дерева Меркла

Дерева Меркла використовуються в розподілених системах для ефективної перевірки даних. Вони ефективні, тому що використовують хеші файлів замість самих файлів. Хеші - це способи кодування файлів, набагато менше за розміром, ніж сам файл. Кожен заголовок блоку в Ефіріумі містить три дерева Меркле для транзакцій, надходження і станів.



Джерело: [Merkling in Ethereum](), Vitalik Buterin, засновник Эфіруму.

Це полегшує клієнтові отримання перевіряються відповідей на такі запити, як:

- Чи існує даний акаунт?
- Який поточний баланс?
- Чи була ця транзакція в певний блок?
- Чи пройшли по цьому адресу певні події?

Смарт контракти

Ключовою концепцією Ефіріуму і інших мереж заснованих на блокчейн, є смарт контракти. Це самостійно виконуючі блоки коду, з якими можуть взаємодіяти декілька сторін, що усуває необхідність в довіреному посереднику. Код смарт контракту можна розглядати як аналогію правових положень в традиційному паперовому контракті, але він дозволяє отримати набагато ширші функціональні можливості. Контракти можуть мати правила, умови, штрафи за недотримання або ініціювати інші процеси. При спрацьовуванні, контракти виконуються так, як це було спочатку зазначено при розгортання публічної ланцюжка, пропонуючи вбудовані елементи незмінності і децентралізації.

Смарт контракти є життєво важливим інструментом, для розробки на основі інфраструктури Ефіріуму. Основна функціональність блокчейн шару Гідро досягається за допомогою призначених для користувача контрактів, про що буде сказано далі в цьому документі.

Віртуальна Машина Ефіріуму

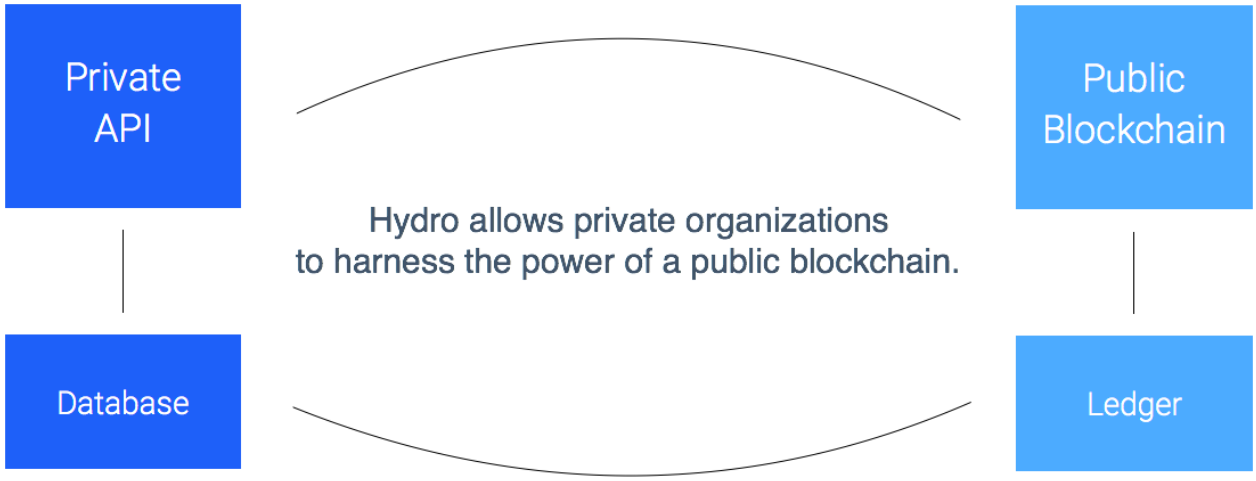
Віртуальна Машина Ефіріуму (ВМЕ) є середовищем виконання для смарт контрактів Ефіріуму. ВМЕ допомагає запобігти DoS-атаки, гарантують що програми залишаються не володіючими станом, і забезпечує зв'язок, яка не може бути перервана. Дії ВМЕ пов'язані з витратами, званими газом, кількість яких залежать від необхідних обчислювальних ресурсів. Кожна транзакція має максимальну кількість газу, відведений йому, відома як ліміт газу. Якщо газ, споживаний транзакцією досягне межі, то вона припинить своє виконання.

Відкритий журнал

Відкритий журнал для приватних систем

Системи, які забезпечують роботу платформ фінансових послуг, веб-сайтів і додатків, часто можуть бути описані як носії потоку даних - вони відправляють, отримують, зберігають, оновлюють і обробляють дані для об'єктів, з якими вони взаємодіють. Через характер цих даних і фінансових послуг в цілому, ці системи часто представляють собою складні операції на приватній і централізованій основі. Розрахунок на приватні структури, в свою чергу, дає можливість отримати різні переваги в плані безпеки, прозорості та підвищення ефективності, шляхом інтегрування зовнішніх коштів, можливості яких перевершують ті, які надає внутрішня система.

Так йде справа з платформою Hydrogen API. Гідро прагне використовувати вищезгадані переваги, дозволяючи користувачам Hydrogen взаємодіяти з блокчейном способами, які надійно інтегруються в фундаментальну приватну екосистему Hydrogen.

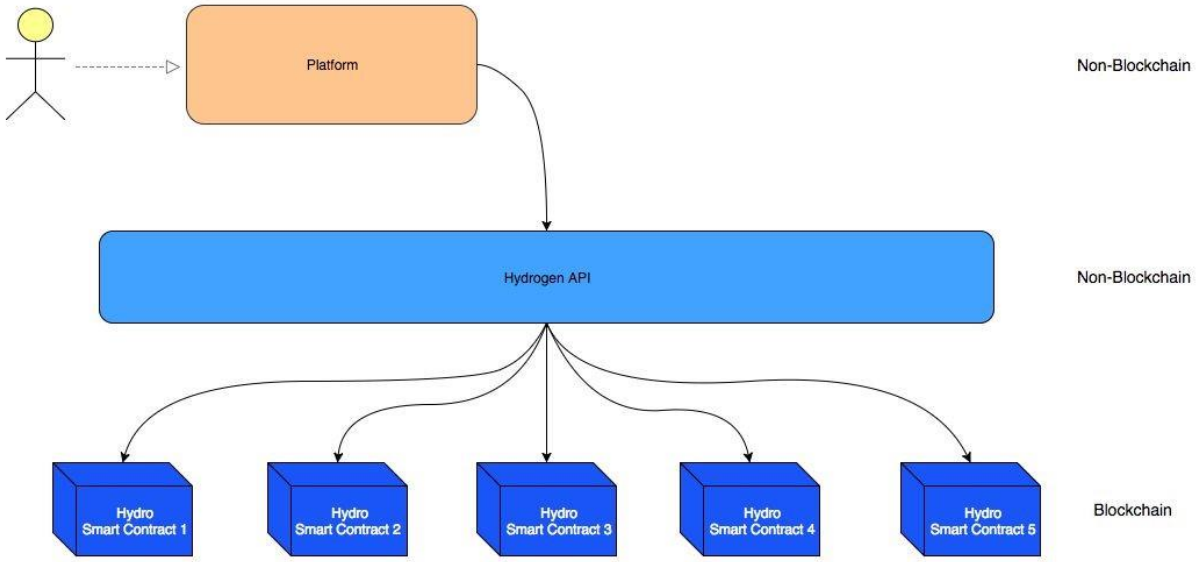


Відкриті операції на основі блокчейн, можуть виникнути до, під час або після приватних операцій. Взаємодія між приватними і відкритими елементами може використовуватися для перевірки, реєстрації, записи або поліпшення процесів в екосистемі. Ідеал цієї моделі - зробити процеси більш надійними, використовуючи переваги блокчейн технології, особливо там, де вона може надавати найбільш позитивний вплив. Хоча ця гібридна структура не може бути застосовна до всіх платформ, Гідро фокусується на тому, що б бути корисною в тих випадків, коли це можливо.

Архітектура для прийняття

Гідро відрізняється від багатьох існуючих проектів на основі блокчейн, оскільки вона може існувати незалежно і на різних рівнях, поєднуючись з новими або існуючими системами, не вимагаючи

при цьому системних змін. Гідро прагне не замінювати, а розширювати наявні функції. Платформи і організації, які використовують Hydrogen API, автоматично отримують доступ до блокчейн.



Спектр платформ фінансових сервісів, які зможуть скористатися Hydrogen, широкий. Ці платформи можуть забезпечувати практично будь-яку функціональність, надавати будь-яку кількість запатентованих сервісів, забезпечувати будь-які приватні дії з даними і розгортатися в будь-якому оточенні. Це забезпечується модулярной структурою Hydrogen, яка синергічна з Гідро і діє, як доповнює його допоміжний засіб.

Рейндроп

Служба аутентифікації на основі блокчейн, побудована на основі публічного журналу Гідро, називається 'Рейндроп'. Вона забезпечує окремий, незмінний, глобально прозорий рівень безпеки, який перевіряє, що запит на доступ виходить з авторизованого джерела.

Приватні протоколи аутентифікації, такі як OAuth 2.0 пропонують різні рівні надійності і корисності для цілого ряду різних існуючих варіантів використання. Немає необхідності конкурувати з цими протоколами або намагатися замінити їх - Гідро пропонує спосіб поліпшити їх, включивши принцип роботи блокчейн як компонент процедури аутентифікації. Це може додати корисний рівень безпеки, що допомагає усунути уразливості системи і запобігти компрометацію даних.

Перш ніж розглядати технічні аспекти Рейндропа, спочатку поглянемо на проблему, яку він намагається вирішити.

Стан фінансової безпеки

Початок цифрової ери призвів до зростання кількості вразливостей, що особливо важливо для фінансових сервісів. Фінансові платформи часто є шлюзами для великої кількості приватних і конфіденційних даних, таких як ідентифікаційні номери державних органів, облікові дані користувачів і історії транзакцій. Зважаючи на виняткову важливість цих даних, несанкціонований доступ до них призводить до катастрофічних результатів.

Фірма Trend Micro вивчаючи галузь опублікувала доповідь, в якій йдеться що вкрадена персональна ідентифікаційна інформація (ПІІ) продається в Deep Web всього за 1 $, скани документів таких як паспорта за 10 $, а банківські облікові дані всього за 200 $, що робить поширення викрадених даних все більш хаотичними і не відслідковується.

На жаль, існуюча фінансова система не має бездоганну репутацію, коли мова заходить про запобігання, діагностики та передачі даних про порушення її клієнтам.

- Згідно недавньому дослідженню "The 2017 Identity Fraud Study", проведеному компанією Javelin Strategy & Research – В 2016 році, 16 млрд доларів було викрадено у 15,4 млн жителей США через збій фінансових систем в сфері захисту ПИИ.
- У Квітні 2017 року, компанія Symantec опублікувала доповідь "Internet Security Threat Report", де зазначені оцінки, згідно котрим, за 2016 рік было викрадено 1,1 млрд різних фрагментів ПИИ.
- Звыт "2016 Year End Data Breach Quickview", опублікований компанією Risk Based Security, повідомляє, що в 2016 році у

всьому світі відбулося 4149 порушень збереження даних, вказуючи 4,2 млрд випадків.

- "2017 Thales Data Threat Report – Financial Services Edition" - міжнародний звіт, який роблять IT-фахівці з професійних послуг - вказує, що 49% організацій, які надавали фінансові послуги в минулому зазнали втрат від порушень безпеки, 78% витрачають більше ресурсів для власного захисту, але 73% запускають нові ініціативи пов'язані зі штучним інтелектом, інтернетом речей і хмарними технологіями, не забезпечивши заздалегідь відповідних рішень безпеки.

Злом компанії Equifax

29 липня 2017 року, компанія Equifax - агентство кредитних звітів працює 118 років на території США, була зламана. 143 млн. персональних даних клієнтів, включаючи номери соціального страхування, були піддані ризику. Дані, що стосуються кредитних карт 209 тис. Клієнтів, були скомпрометовані.

Яка була причина цього порушення?

Вона виходила від одного серверного додатка, використаного компанією Equifax. Struts є фреймворком з відкритим вихідним кодом для розробки веб додатків на мові Java, що належить організації Apache Software Foundation.CVE-2017-9805 є вразливістю в Apache Struts, пов'язаною з плагіном Struts REST, який використовує обробник XStream для обробки XML корисних даних. При експлуатації, вона дозволяє хакерам, які знаходяться віддалено і не пройшли перевірку автентичності, запускати шкідливий код на сервері додатків, щоб взяти машину під свій контроль, або проводити з неї подальші атаки. Ця вразливість була виправлена організацією Apache за 2 місяці до злому Equifax

Apache Struts містила недолік в плагіні REST Plugin XStream який спрацьовує, коли програма небезпечно десеріалізует XML запит. Говорячи більш конкретно, проблема полягала в методі toObject () класу XStreamHandler, яка не накладає ніяких обмежень на вхідні дані при використанні XStream десеріалізації в об'єкт, що призводить до виникнення вразливостей довільного виконання коду.

Навіть якщо цей REST плагін був скомпрометований, чи повинно це мати значення? Чи існує спосіб використовувати технологію блокчейн для захисту фінансових даних тих 143 млн. Клієнтів, в той же час покладаючись на діючі REST API і системи засновані на Java?

Додавання блокчейн шару

Очевидно, що цілісність фінансових шлюзів, що обробляють дані, може бути поліпшена. Давайте розглянемо, як додатковий рівень безпеки досягається через Гідро.

Основоположні механізми консенсунса мережі Ефіріуму забезпечують трансакціонну достовірність, оскільки учасники спільно обробляють транзакції, які належним чином підписані. Ця обставина призводить до децентралізації і незмінності, але, що більш важливо, вона забезпечує вектор для пом'якшення наслідків несанкціонованого доступу до шлюзу, який обробляє конфіденційні дані.

При використанні Гідро, аутентифікація може бути заснована на транзакційних операціях блокчейн. Наприклад, API зможе перевіряти розробників і додатки, вимагаючи від них ініціювати певні транзакції, з конкретними корисними даними, між конкретними адресами в блокчейне, як попередня умова для ініціації стандартного протоколу аутентифікації.

Гідро Рейндроп

Дощ(Рейн) складається з водяних крапель, діаметр яких знаходиться в діапазоні від 0,0001 до 0,0005 сантиметрів. При звичайному зливі, випадають мільярди таких крапель, у кожної з яких випадковий розмір, швидкість і форма. Тому не можна достовірно передбачити точну структуру дощу. Аналогічно, кожна аутентифікаційна транзакція Гідро є унікальною і практично неможливо, щоб вона відбулася випадково - ось чому ми називаємо їх краплями Дощу (Рейндропи).

Платформи фінансових послуг зазвичай використовують перевірку мікроплатежами для перевірки облікових записів клієнта. Дана концепція проста: Платформа робить невеликий платіж на випадкову суму на банківський рахунок, про який клієнт заявляє, що він належить йому. Для того, щоб довести, що користувач дійсно володіє цим рахунком, він або вона повинні повернути назад цей платіж платформі, який потім перевіряється. Єдиний спосіб, який користувач може знати дійсну суму (крім вгадування) - це мати доступ до банківського рахунку, про який йде мова.

Перевірка на основі Рейндропу з Гідро є аналогічною. Замість того, щоб відправляти користувачеві суму і повертати її назад, ми визначаємо транзакцію і користувач повинен виконати її з відомого йому гаманця. Єдиним способом, яким користувач може провести підтверджену транзакцію, є доступ до гаманця, про який йде мова.

Використовуючи Рейндропи, як система, так і користувач, який має до неї доступ, можуть відстежувати спроби авторизації в незмінному відкритому журналі. Ця заснована на блокчейне транзакція відокремлена від основних системних операцій, відбувається в розподіленій мережі і залежить від володіння закритими ключами. Тому, вона служить корисним вектором валідації.

Детальний розгляд

В процесі Гідро аутентифікації беруть участь 4 об'єкти:

1. Аксессор (Accessor) - сторона, намагається отримати доступ до системи. У разі Hydrogen, аксессор - це фінансова установа або додаток використовує Hydrogen API для своєї основної цифрової інфраструктури.
1. Система (System) - система або шлюз, до яких намагається отримати доступ аксессор. Для Hydrogen, цією системою є сам Hydrogen API.
2. Гідро (Hydro) - модуль, який використовується Системою для зв'язку і взаємодії з блокчейном.
3. Блокчейн (Blockchain) - розподілений відкритий журнал, який обробляє транзакції Гідро і містить смарт контракти Гідро, в який інформація може бути поміщена, витягнута або іншим чином оброблена.

Кожен Рейндроп, в цілому, являє собою набір з п'яти параметрів транзакції:

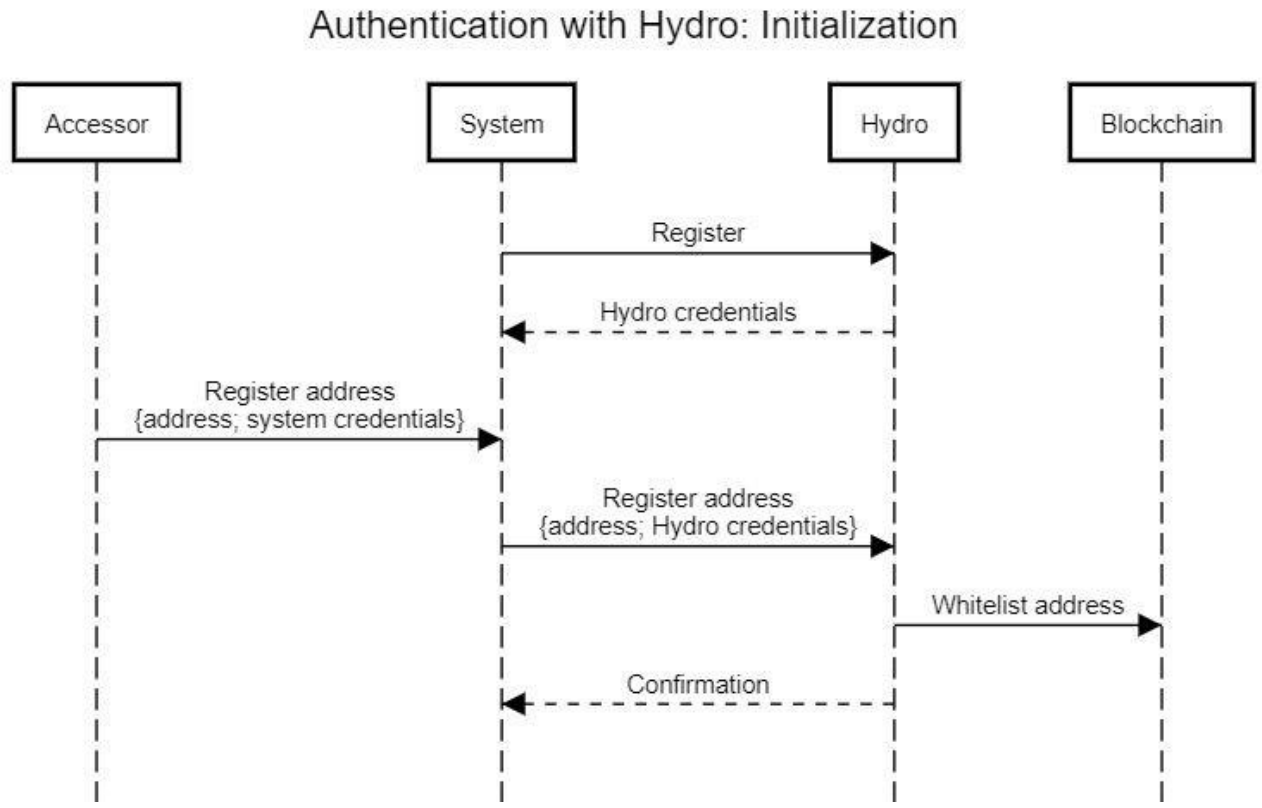
1. Відправник (Sender) - Адреса яка повинна запустити транзакцію.
2. Одержувач (Receiver) - Кінцевий пункт транзакції. Це відповідає викликом методу в смарт контракті Гідро.
3. ID - Ідентифікатор, пов'язаний з Системою.
4. Кількість (Quantity) - Точна кількість Гідро для відправки.
5. Виклик (Challenge) - буквено-цифровий рядок, згенерований випадковим чином.

Нижче наводиться схема процесу аутентифікації, яку зазвичай можна розділити на 3 етапи:

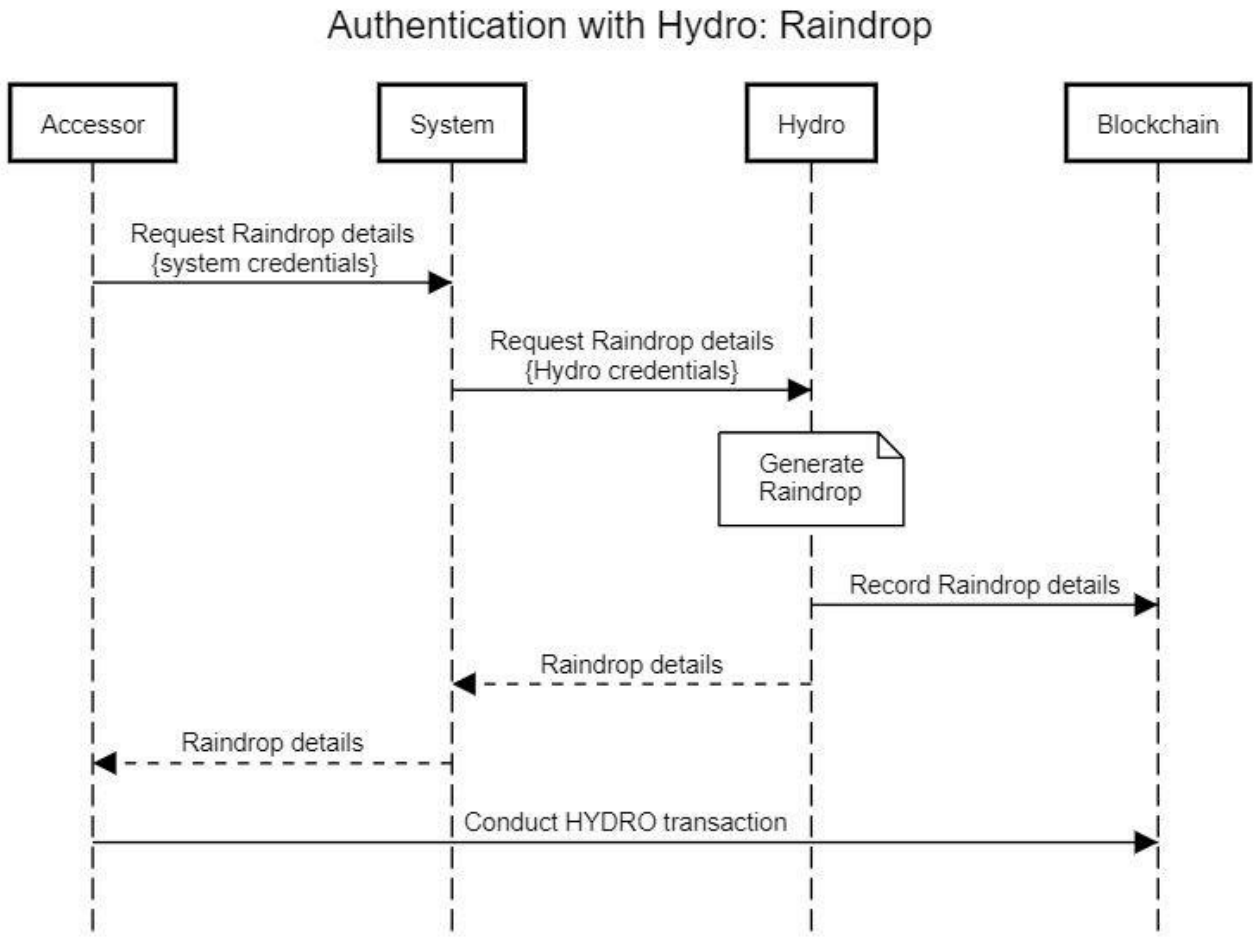
1. Ініціалізація
2. Рейндроп
3. Затвердження

Ініціалізація починається з реєстрації Системи (наприклад, Hydrogen) для використання Гідро та отримання облікових даних, що дозволяє системі зв'язуватися з блокчейном через модуль Гідро. Системою керує аксессор (наприклад, фінансова установа), який реєструє публічну адресу, а потім передає зареєстровану адресу в Гідро. Ця електронна адреса без зміни записується в блокчейні в білий список, що зберігається в смарт контракті Гідро. Система отримує

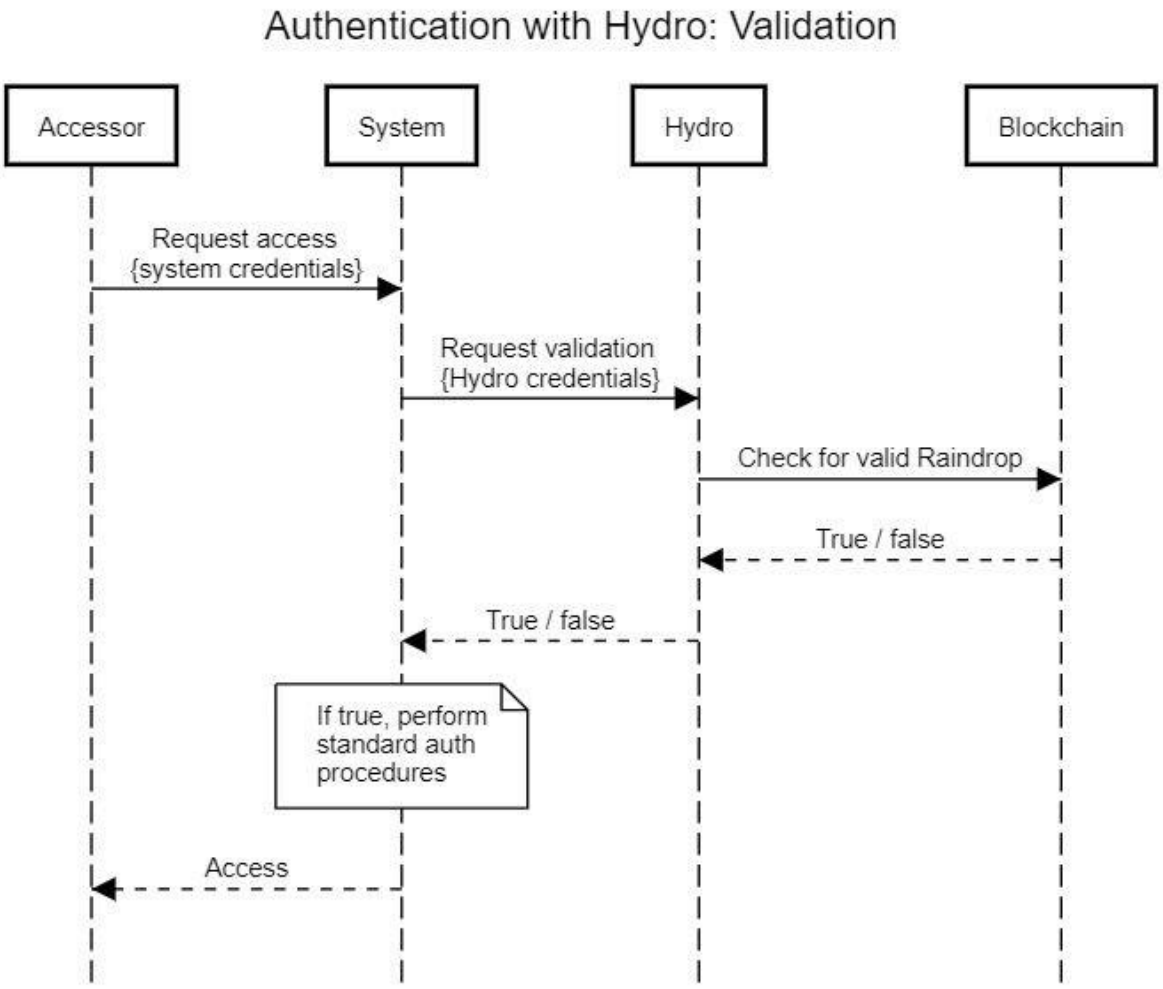
підтвердження про те, що адреса був занесена в білий список, що можна перевірити як загальнодоступну подію, яку всім видно. Реєстрація в системі потрібна один раз, а занесення в білий список - один раз для кожного аксессора.



Після того, як Ініціалізація завершена, запускається ядро аутентифікації Гідро. Аксессор, який повинен виконати Рейндроп транзакцію, запускає цей процес, запитуючи докладні дані Рейндропа з Системи, а Система перенаправляє запит на Гідро. Гідро генерує новий Рейндроп, зберігає певні відомості в блокчейн, не змінюючи їх, і повертає вже докладні дані аксессору через Систему. Аксессор, має всю необхідну інформацію, проводить транзакцію з зареєстрованої адреси, звертаючись до методу смарт контракту Гідро. Якщо адреса була внесена в білий список, то дія відхиляється, а якщо занесена, то вона записується в смарт контракт. Важливо відзначити, що ця транзакція повинна відбуватися поза Системою, безпосередньо від аксессора до Блокчейну, так як вона повинна бути підписана закритим ключем аксессора (до якого повинен мати доступ тільки аксессор).



Нарешті, заключним етапом є Валідація. Тут, аксессор офіційно запитує доступ до Системи через її встановлені механізми. Перед виконанням будь-якого стандартного протоколу аутентифікації, Система запитує у Гідро, чи виконав Акссесор валідну Рейндроп транзакцію. Гідро взаємодіє зі смарт контрактом, перевіряє на достовірність його, і відповідає позначкою - true / false. Система може вирішити, як вона повинна діяти на основі цієї позначки. Наприклад - якщо false, то заборонити доступ, якщо true, то надати доступ.



Якщо ми будемо розглядати основні облікові дані Системи - або будь-який інший існуючий протокол Системи, який є в наявності - як один з факторів аутентифікації, важливо, що рівень Гідро забезпечує корисний другий фактор. Вивчаючи два основних вектори атаки, ми можемо легко підтвердити його користь:

- Вектор 1 - Зловмисник краде основні облікові дані Системи у Аксессор
  - Зловмисник намагається отримати до Системи за допомогою валідних облікових даних.
  - Система спільно з Гідро визначає - чи було зроблено валідна транзакція на блокчейне.
  - Гідро повертає false, і Система забороняє доступ.
- Вектор 2 - Зловмисник краде закритий ключ від гаманця Аксессор
  - Зловмисник намагається провести Гідро транзакцію з зареєстрованої адреси, без необхідних параметрів Рейндропа.
  - Зловмисник не може зробити валідну блокчейн транзакцію.
  - Зловмисник також не може запросити доступ до Системи без відповідних облікових даних Системи.

Очевидно, що Зловмисник повинен заволодіти як основними системними обліковими даними, так і закритим ключем від гаманця аксессора, щоб отримати доступ до системи. У зв'язку з цим, Гідро успішно додає додатковий фактор аутентифікації

Відкриття Рейндропу суспільству

Не дивлячись на те, що блокчейн сервіс аутентифікації був спроектований щоб захистити екосистему Hydrogen API, він широко застосовується до різних платформ і систем. Відчуваючи, що інші потенційно можуть отримати вигоду з цього рівня верифікації, ми відкриваємо його для використання.

Точно також, як Hydrogen буде впроваджувати його в якості однієї з передумов доступу до своєї екосистемі API, так і будь-яка система може додати його до існуючих процедур і протоколів. Будь-яка платформа - API, додаток, корпоративний софт, ігрова платформа і т.д. - може використовувати Hydro для аутентифікації. Офіційна документація буде доступна на сайті GitHub для тих, хто хоче включити цей блокчейн шар в інфраструктуру аутентифікації або REST API.

Приклад використання – Рейндроп с OAuth 2.0

Існують десятки способів використання Рейндропу для приватних організацій. Закриті API, бази даних і мережі створили складні системи токенів, ключів, додатків і протоколів за останнє десятиліття, намагаючись захистити конфіденційні дані. Наприклад, Google, став одним з найпопулярніших постачальників на ринку, за допомогою програми Google Authenticator. Як було сказано раніше - немає необхідності замінювати існуючі протоколи.

Як приклад використання, розглянемо коротко, як Hydrogen реалізує Гідро аутентифікацію в якості рівня безпеки в своєму власному загальному API фреймворка безпеки:

1. Партнери Hydrogen API, по-перше, повинні мати білий список IP адрес власних різних оточень.
2. Партнери повинні робити запит на внесення публічної адреси Гідро в білий список.
3. Всі виклики до Hydrogen API і передача даних шифрується і передається через HTTPS протокол.
4. Партнери повинні завершити валідну Гідро Рейндроп транзакцію з зареєстрованого Гідро адреси.
5. Партнери повинні використовувати OAuth 2.0 валідацію. OAuth (Open Authorization) - це відкритий стандарт для аутентифікації і авторизації на основі токенів. Hydrogen підтримує типи доступу - 'Облікові дані власника ресурсу' і 'Облікові дані клієнта', і кожен користувач API повинен надавати облікові дані для запиту аутентифікації.

6. Якщо жоден з п'яти вищих пунктів не порушується, то партнеру Hydrogen видається унікальний токен, який перевіряється і верифицируется при кожному виклику API.
7. Токен буде діяти 24 години, після чого партнер повинен знову підтвердити себе.

Якщо який-небудь з цих пунктів порушується, то доступ користувача до API негайно блокується. Хакер не зможе обійти ці фактори безпеки, вгадуючи випадковим чином символи, тому що існують трильйони унікальних комбінацій.

Блокчейн аутентифікація Гідро є важливим компонентом протоколу безпеки Hydrogen. Команда Hydrogen закликає партнерів до установки гаманців з мульти-підписами, і зберігати закриті ключі в кількох захищених місцях незалежно від інших облікових даних, щоб не було єдиної точки уразливості. Правильно захищений гаманець з мульти-підписами не тільки важко викрасти, але в силу відкритості блокчейну також швидко розпізнати будь-яку крадіжку, тому що це пов'язано з безпекою API.

Будь-хто може відстежувати спроби аутентифікації в смарт-контракті Гідро, що означає, що час платформ які були скомпрометовані місяцями, можуть піти в минуле. Тепер, спроби злому API можуть бути перервані з великою оперативністю через здатність виявляти несподівані спроби авторизації в реальному часі, з будь-якої точки світу.

Ризики

Також, як і в будь-якій технології, яка зароджується, наприклад, як в ранні часи соціальних мереж, електронної пошти і потокових додатків (які були залежні від dial-up підключення), дуже важливо, щоб основна команда розробників ретельно відстежувала нові розробки в швидкостях транзакцій і обсягах Ефіріуму. Чи не могли б ви уявити, що YouTube намагався запуститися в 1995 році? Або щоб Instagram вперше пропонувався на Blackberry?

Основні розробники Ефіріуму, такі як Віталік Бутерін і Джозеф Пун в роботі 'Плазма: Розширюються Автономні Смарт Контракти' ("Plasma: Scalable Autonomous Smart Contracts"), пропонує покращити протокол Ефіріум:

> *Плазма є пропонованим фреймворком для більш інтенсивного і примусового виконання смарт контрактів, які можуть масштабуватися до значної кількості поновлення станів в секунду (потенційно мільярди), що дозволить блокчейну мати можливість представляти велику кількість децентралізованих фінансових додатків, по всьому світу. Стимулюється продовження автономної роботи цих смарт контрактів за рахунок платежів за мережеві транзакції, що в кінцевому підсумку залежить від базового блокчейна (Наприклад, Ефіріуа) для забезпечення переходу станами транзакцій.*

Інші проекти, такі як Raiden Network, запропонували рішення масштабування поза ланцюжка, призначене для прискорення транзакцій і низьких комісій. У той же час, Рейндроп буде мінімально навантажувати фреймворк Ефіріуму, тому масштабованість є невеликим ризиком для успіху технології.

Висновок

Незмінюваність відкритого блокчейну пропонує нові способи підвищення безпеки закритих систем, таких як API.

Цей документ висвітлює 3 важливі речі:

1. Відкритий блокчейн може внести свій вклад в фінансові послуги.
2. Гідро Рейндроп може підвищити безпеку приватних систем.
3. Існує непосредственние застосування Гідро Рейндропа в рамках платформи Hydrogen API.

Команда Гідро вважає, що нова структура може стати стандартною інфраструктурою безпеки для нових моделей змішаних приватних і публічних систем, яка принесе користь всім зацікавленим сторонам в сфері фінансових послуг і за її межами.

Джерела:

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 Contract