Hydro Raindrop

Uwierzytelnianie publiczne w Blockchain

Styczeń 2018

SPIS TREŚCI

Streszczenie

HYDRO: Etymologia – od starożytnej greki ὑδρο (*hydro*), który pochodzi od słowa ὕδωρ (woda).

Firma Hydro umożliwia nowym i istniejącym prywatnym systemom integrację i optymalne wykorzystanie niezmiennej i przejrzystej dynamiki blockchain w celu zwiększenia bezpieczeństwa aplikacji i dokumentów, zarządzania tożsamością, transakcji i sztucznej inteligencji.

W tym dokumencie odniesiemy się do systemów prywatnych, takich jak API, które będą wykorzystywać publiczny blockchain firmy Hydro w celu zwiększenia bezpieczeństwa poprzez publiczne uwierzytelnianie (public authentication).

Proponowana technologia nosi nazwę "Raindrop" - transakcję, która odbywa się za pośrednictwem smart contract, który publicznie zatwierdza prywatny dostęp do systemu i może uzupełniać istniejące prywatne metody certyfikacji. Technologia ma na celu zapewnienie dodatkowego bezpieczeństwa poufnych danych finansowych, które są w coraz większym stopniu narażone na piractwo i naruszenia.

Początkowa implementacja Hydro Raindrop jest przeprowadzana na platformie Hydrogen API. Ten modułowy pakiet API jest dostępny dla firm i deweloperów na całym świecie w celu inicjowania, konstruowania, testowania i rozwijania zaawansowanych platform i produktów technologia finansowej.

Hydro Raindrop będzie dostępny dla globalnej społeczności programistów jako oprogramowanie open source (Open source software), dzięki czemu programiści mogą zintegrować Hydro Raindrop z dowolnym interfejsem API REST.

Blockchain & Ethereum

Hydro jest wdrażane w sieci Ethereum. Zanim podamy więcej szczegółów na temat projektu, ważne jest, aby zrozumieć podstawowe idee blockchain i Ethereum.

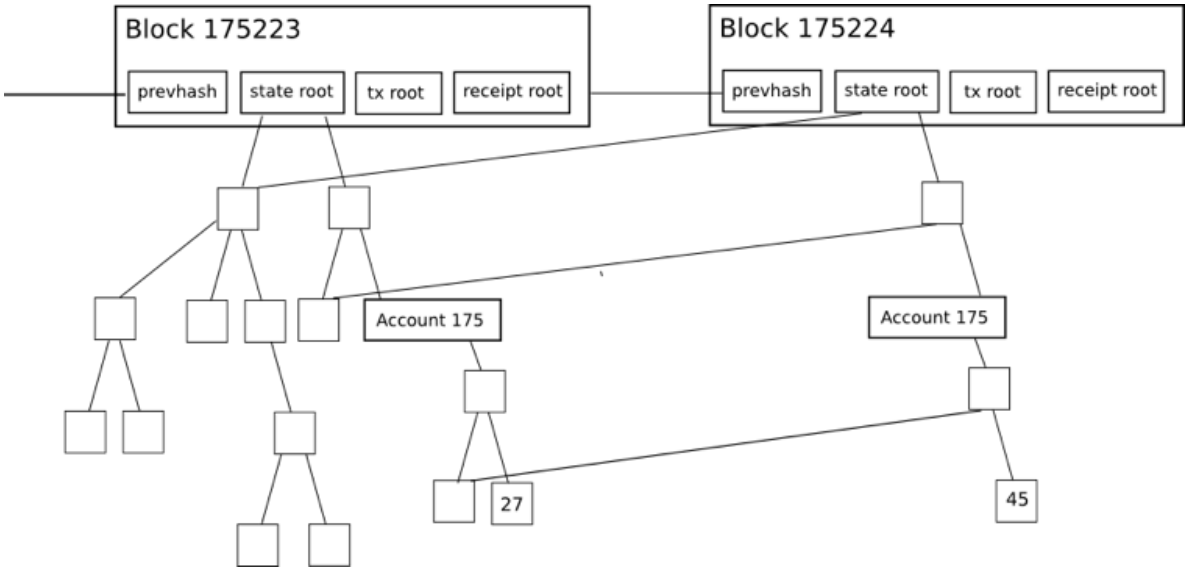
Opierając się na Ethereum

Ponieważ aplikacje takie jak Snapchat zostały zbudowane za pomocą Swift i innych narzędzi oferowanych przez platformę Apple Ios, więc aplikacje blockchain mogą być budowane na Ethereum. Snap Inc. nie musiał budować IOS, używał go jako infrastruktury do uruchomienia aplikacji mediów społecznościowych.

Projekt Hydro jest podobny. Opiera się na tysiącach programistów na całym świecie, którzy pracują nad tym, aby technologia blockchain była szybsza, silniejsza i bardziej wydajna. Firma Hydro wykorzystuje tę stale ulepszaną infrastrukturę, opracowując interakcje ukierunkowane na produkty w ramach technologii blockchain, które mogą przynieść wymierne korzyści aplikacjom usług finansowych.

Merkle Trees

Merkle Trees są używane w rozproszonych systemach sprawdzania danych. Są skuteczne, ponieważ używają tak zwanych hashes zamiast pełnych rekordów. Hashes to metody kodowania plików znacznie mniejsze niż sam plik. Każdy nagłówek bloku w Ethereum zawiera trzy drzewa Merkle dla transakcji, zarobków i statusów:



Źródło: Merkling in Ethereum; Vitalik Buterin, Założyciel Ethereum

Ułatwia to Light Client uzyskanie sprawdzalnych odpowiedzi na pytania takie jak:

- Czy to konto istnieje?
- Jaki jest obecny bilans?
- Czy ta transakcja została zawarta w konkretnym block?
- Czy zdarzyło się dzisiaj konkretne wydarzenie pod tym adresem?

Smart Contracts

Kluczową cechą Ethereum i innych sieci opartych na blockchain są "smart contracts". Są to samopowrotne bloki kodu, które mogą wchodzić w interakcje z wieloma częściami, eliminując potrzebę niezawodnych pośredników. Kodeks w smart contracts może być postrzegany jako podobny do klauzul prawnych w tradycyjnej umowie papierowej, ale może również osiągnąć znacznie bardziej ekspansywną funkcjonalność. Takie umowy mogą zawierać zasady, warunki i kary za nieprzestrzeganie przepisów lub inne procedury. Po aktywacji są wykonywane zgodnie z pierwotnym zgłoszeniem, gdy są zainstalowane w public chain, zapewniając osadzone dane, które są niezmienione i zdecentralizowane.

Smart contracts są ważnym narzędziem budowy infrastruktury Ethereum. Podstawową funkcjonalność warstwy blokowej Hydro osiąga się poprzez niestandardowe umowy, o których mowa w dalszej części tego artykułu.

Maszyna wirtualna Ethereum

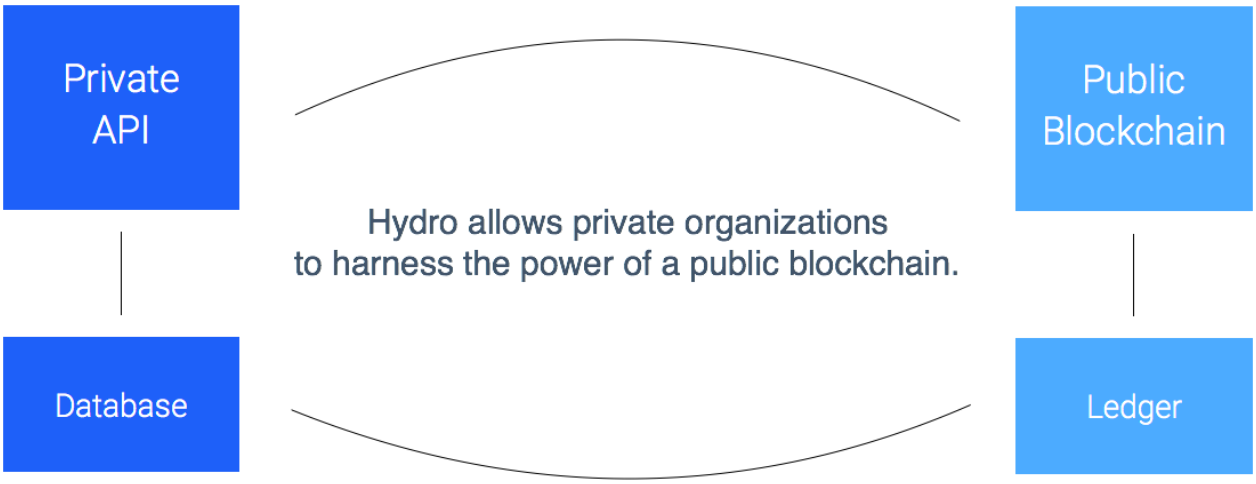
Wirtualna maszyna Ethereum (EVM) jest środowiskiem uruchomieniowym dla smart contracts w Ethereum. EVM pomaga zapobiegać atakom Denial of Service (DoS), zapewnia, że programy pozostają nienaruszone i umożliwia bezproblemową komunikację. Działania na EVM mają związane z nimi koszty, zwane gas, które zależą od wymaganych zasobów obliczeniowych. Każda transakcja ma maksymalną dopuszczalną ilość gas, zwaną gas limit. Jeśli gas zużyty przez transakcję osiągnie limit, przerywa proces.

Public Ledger

Public Ledger dla systemów prywatnych

Systemy, które zarządzają platformami, stronami internetowymi i aplikacjami usług finansowych, często mogą być określane jako media strumieniowe - wysyłają, odbierają, przechowują, aktualizują i przetwarzają dane dla osób, z którymi współpracują. Ze względu na charakter tych danych i ogólnie usługi finansowe, systemy te często mają złożone funkcje w sposób prywatny i scentralizowany. Zaufanie do prywatnych struktur z kolei otwiera drzwi do różnych zabezpieczeń, przejrzystości i rentowności, w celu ich przyjęcia poprzez włączenie sił zewnętrznych, które wykraczają poza zakres systemu wewnętrznego.

Tak jest w przypadku platformy Hydro API. Hydro stara się wykorzystać powyższe zalety, pozwalając użytkownikom Hydro na interakcję z blockchainem w sposób, który jest płynnie zintegrowany z podstawowym ekosystemem Hydro.

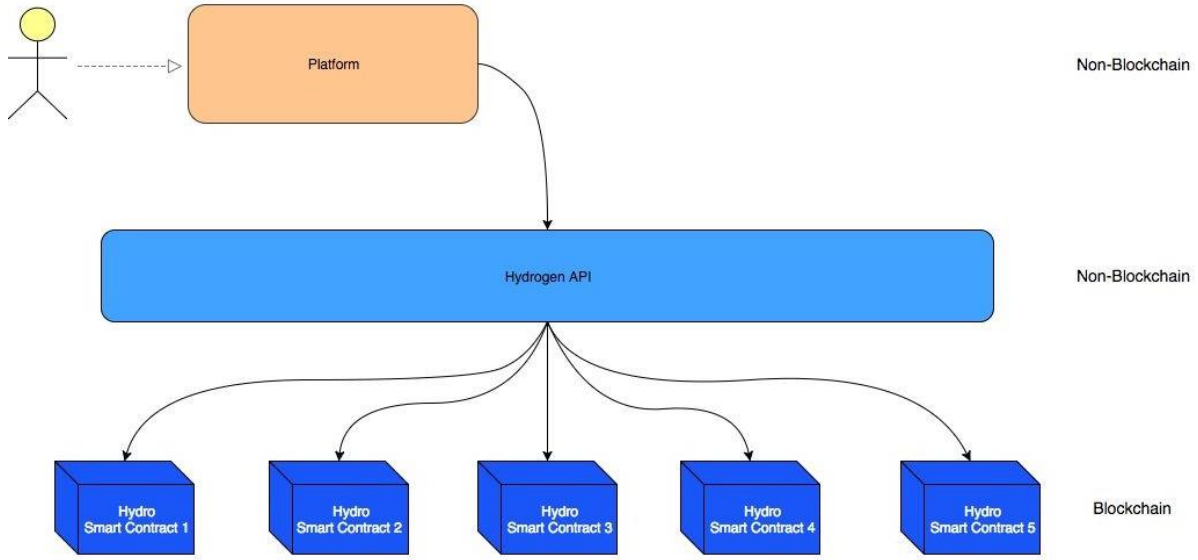


Funkcje publiczne oparte na blockchain mogą być wykonywane przed, w trakcie lub po prywatnych operacjach. Interakcja między danymi prywatnymi i publicznymi może służyć do walidacji, uszczelniania, rejestrowania lub wzmacniania procesów w ekosystemie.

Etos tego modelu sprawia, że procesy są bardziej niezawodne, wykorzystując zalety technologii blockchain, szczególnie tam, gdzie może ona przynieść najbardziej pozytywne efekty. Chociaż ta hybrydowa struktura może nie mieć zastosowania do wszystkich platform, Hydro skupia się na zapewnieniu wartości dla sytuacji, w których jest zainstalowana.

Szablon architektoniczny

Hydro różni się od wielu istniejących inicjatyw blockchain, ponieważ może być niezależny i umieszczony wokół nowych lub istniejących systemów bez konieczności dokonywania systematycznych zmian. Zamiast zastępować, Hydro dąży do poprawy. Platformy i instytucje powiązane z interfejsem Hydrogen API mogą mieć automatyczny dostęp do blockchain.



Zakres platform usług finansowych, które mogą korzystać z Hydrogen, jest szeroki. Platformy te mogą zasilać praktycznie dowolne doświadczenie, zawierać dowolną liczbę zastrzeżonych usług, wykonywać dowolne prywatne operacje danych i wdrażać je w dowolnym środowisku. Jest to możliwe dzięki strukturalnej modularności Hydrogen i jest synergiczne z Hydro, działając jako dodatkowy czynnik przyspieszający adopcję.

Raindrop

Zbudowany na szczycie tej Public ledger Hydro jest usługą uwierzytelniania opartą na blockchain, nazywaną "Raindrop". Oferuje ona odrębną, niezmienną, globalnie widoczną warstwę zabezpieczeń, która sprawdza, czy żądanie dostępu pochodzi z autoryzowanego źródła.

Prywatne protokoły uwierzytelniania, takie jak OAuth 2.0, oferują różne poziomy niezawodności i użyteczności dla szeregu istniejących przypadków użycia. Nie ma potrzeby konkurowania lub próby zastąpienia tych protokołów. Hydro oferuje sposób na ich wzmocnienie poprzez integrację mechanizmów blockchain w ramach procesu uwierzytelniania. Może to zwiększyć użyteczną warstwę zabezpieczeń, aby zapobiec naruszeniom systemu i wyciekowi poufnych informacji.

Zanim przejdziemy do technicznego aspektu Raindrop, przyjrzymy się problemowi, który próbuje rozwiązać.

Sytuacja bezpieczeństwa finansowego

Pojawienie się data age spowodowało podatność na systemy, co jest szczególnie ważne w przypadku usług finansowych. Platformy finansowe mogą być postrzegane jako bramki dla wielu prywatnych i poufnych danych, takich jak numery ID, zapisy rachunków i historie transakcji. Ze względu na ważność poświadczeń, dostęp z niechcianych źródeł, często następuje katastrofalne wyniki.

Firma Trend Micro opublikowała raport stwierdzający, że skradzione dane osobowe, nazywane Personally Identifiable Information (PII), są sprzedawane w Deep Web za jedyne 1 USD, skany dokumentów, takie jak paszporty, są dostępne za jedyne 10 USD, oraz poświadczenia logowania do banku dla za jedyne 200 USD, dzięki czemu dystrybucja skradzionych danych jest łatwo dostępna.

Jednak istniejący system finansowy nie ma krystalicznie czystej historii, jeśli chodzi o zapobieganie, diagnozowanie i komunikowanie naruszeń danych z akcjonariuszami.

- Zgodnie z niedawnym opracowaniem Javelin Strategy & Research pt - *The 2017 Identity Fraud Study* - 16 miliardów dolarów skradzionych z 15,4 miliona konsumentów w USA w 2016 r. z powodu awarii systemu finansowego w celu ochrony danych osobowych (PII).

- W kwietniu 2017 r. Firma Symantec opublikowała raport *Internet Security Threat Report*, która szacuje, że w 2016 r. 1,1 miliarda plików PII zostało udostępnionych różnym źródłom.

- W artykule *2016 Year End Data Breach Quickview* z Risk Based Security stwierdzono, że w 2016 r. w przedsiębiorstwach na całym świecie odnotowano 4,149 naruszenia danych, które wystawiając ponad 4,2 miliarda danych.

- Στο *2017 Thales Data Threat Report – Financial Services Edition*, Ankieta przeprowadzona wśród global IT professionals w sektorze usług profesjonalnych wykazała, że 49% organizacji usług finansowych doświadczyło naruszenia bezpieczeństwa w przeszłości, 78% wydaje więcej pieniędzy na ochronę, ale 73% wprowadza nowe powiązane inicjatywy. z technologiami AI, IoT i chmurowymi przed przygotowaniem odpowiednich rozwiązań bezpieczeństwa.

Equifax Breach

W dniu 29 lipca 2017 r. Equifax, 118-letnia amerykańska agencja ds. Informacji kredytowych, została zhackowana, a 143 miliony PII zostało ujawnionych, w tym numery ubezpieczenia społecznego, ponieważ naruszono dane karty kredytowej 209 000 klientów.

Jaka była przyczyna tego naruszenia?

Zaczęło się od jednej z technologii zaplecza wykorzystywanych przez Equifax. Struts to otwarte środowisko programistyczne do tworzenia aplikacji internetowych w języku programowania Java, stworzone przez Apache Software Foundation. CVE-2017-9805 to luka w Apache Struts związana z używaniem plugin REST Struts z obsługą XStream do obsługi ładunków XML. Jeśli zostanie wykorzystany, umożliwia zdalnemu nieuwierzytelnionemu atakującemu uruchomienie złośliwego kodu na serwerze aplikacji w celu przejęcia maszyny lub wykonania z niej dalszych ataków. Zostało to załatane przez Apache dwa miesiące przed naruszeniem Equifax.

Apache Struts zawiera błąd w REST XStream, który jest wyzwalany, ponieważ program niezabezpiecznie deserializuje dane wejściowe dostarczone przez użytkownika w żądaniach XML. Mówiąc dokładniej, problem występuje w metodzie toStreamHandler toObject (), która nie nakłada żadnych ograniczeń na wartość przychodzącą podczas deserializacji obiektu XStream, który generuje luki w zabezpieczeniach wykonywania dowolnego kodu.

Nawet jeśli ta wtyczka REST została naruszona, powinno to mieć znaczenie? Czy istnieje sposób na wykorzystanie technologii blockchain do zabezpieczenia informacji finansowych tych 143 milionów klientów, a jednocześnie polegają na istniejącym REST API i systemach opartych na Javie?

Dodawanie warstwy Blockchain

Oczywiste jest, że integralność bramek danych finansowych może zostać poprawiona.

Zobaczmy, jak można osiągnąć dodatkowy poziom bezpieczeństwa dzięki Hydro.

Podstawowe mechanizmy konsensusu w sieci Ethereum zapewniają ważność transakcyjną, ponieważ uczestnicy wspólnie przetwarzają transakcje, które są odpowiednio podpisane. Fakt ten prowadzi do decentralizacji i stabilności, ale przede wszystkim zapewnia wektor do ograniczania nieautoryzowanego dostępu do bramy, która obsługuje wrażliwe dane.

W przypadku Hydro uwierzytelnianie może zależeć od operacji transakcji w blockchain. Na przykład interfejs API może zatwierdzać programistów i aplikacje, wymagając od nich rozpoczęcia określonych transakcji z konkretnym ładunkiem danych między określonymi adresami w łańcuchu bloków, o ile rozpoczyna się protokół uwierzytelniania.

Hydro Raindrop

Rain ("deszcz") zawiera pakiety skondensowanej wody w zakresie od 0,0001 do 0,005 centymetra średnicy. W typowej burzy są miliardy takich pakietów, każda o losowym rozmiarze, prędkości i kształcie. Z tego powodu nie można wiarygodnie przewidzieć dokładnej natury deszczu. Podobnie, każda transakcja uwierzytelniania Hydro jest wyjątkowa i praktycznie niemożliwa do zrealizowania przez przypadek - dlatego nazywamy je Raindrops.

Platformy usług finansowych zazwyczaj używają weryfikacji mikrokredytów do sprawdzania kont klientów. Pomysł jest prosty: platforma tworzy niewielkie depozyty losowych kwot na kontach bankowych zadeklarowanych przez użytkowników. Aby udowodnić, że użytkownik faktycznie posiada to konto, musi on przenieść kwoty depozytów z powrotem na platformę, które następnie zostają zatwierdzone. Jedynym sposobem, w jaki użytkownik może poznać prawidłowe kwoty (poza domysłem), jest dostęp do tych kont bankowych.

Weryfikacja oparta na Raindrop with Hydro jest proporcjonalna. Zamiast wysyłać użytkownikowi kwotę i przekazywać ją z powrotem, definiujemy transakcję i użytkownik musi wykonać ją ze znanego portfela. Jedynym sposobem, w jaki użytkownik może dokonać ważnej transakcji, jest uzyskanie dostępu do tego portfela.

Dzięki Raindrops zarówno system, jak i użytkownik mogą śledzić wysiłki związane z autoryzacją w niezmienionej public ledger. Ta transakcja oparta na blockchain jest odłączona od podstawowych funkcji systemowych, pojawiających się w sieci rozproszonej i zależna od własności kluczy prywatnych. Dlatego służy jako przydatny element walidacji.

Uważne spojrzenie

W procesie weryfikacji tożsamości Hydro są cztery elementy:

1. *Accessor* - Grupa szuka dostępu do systemu. W przypadku Hydrogen accessor jest instytucją finansową lub aplikacją wykorzystującą interfejsy API Hydrogen do swojej podstawowej infrastruktury cyfrowej.
2. *System* - System lub brama, do których uzyskuje dostęp Accessor. W przypadku Hydrogen system jest samym API Hydrogen.
3. *Hydro* - Moduł wykorzystywany przez system do komunikacji i łączenia się z blockchain.
4. *Blockchain* – Rozproszona public ledger, która przetwarza transakcje HYDRO i zawiera Hydro smart contracts, dzięki którym można importować, odbierać lub obsługiwać informacje.

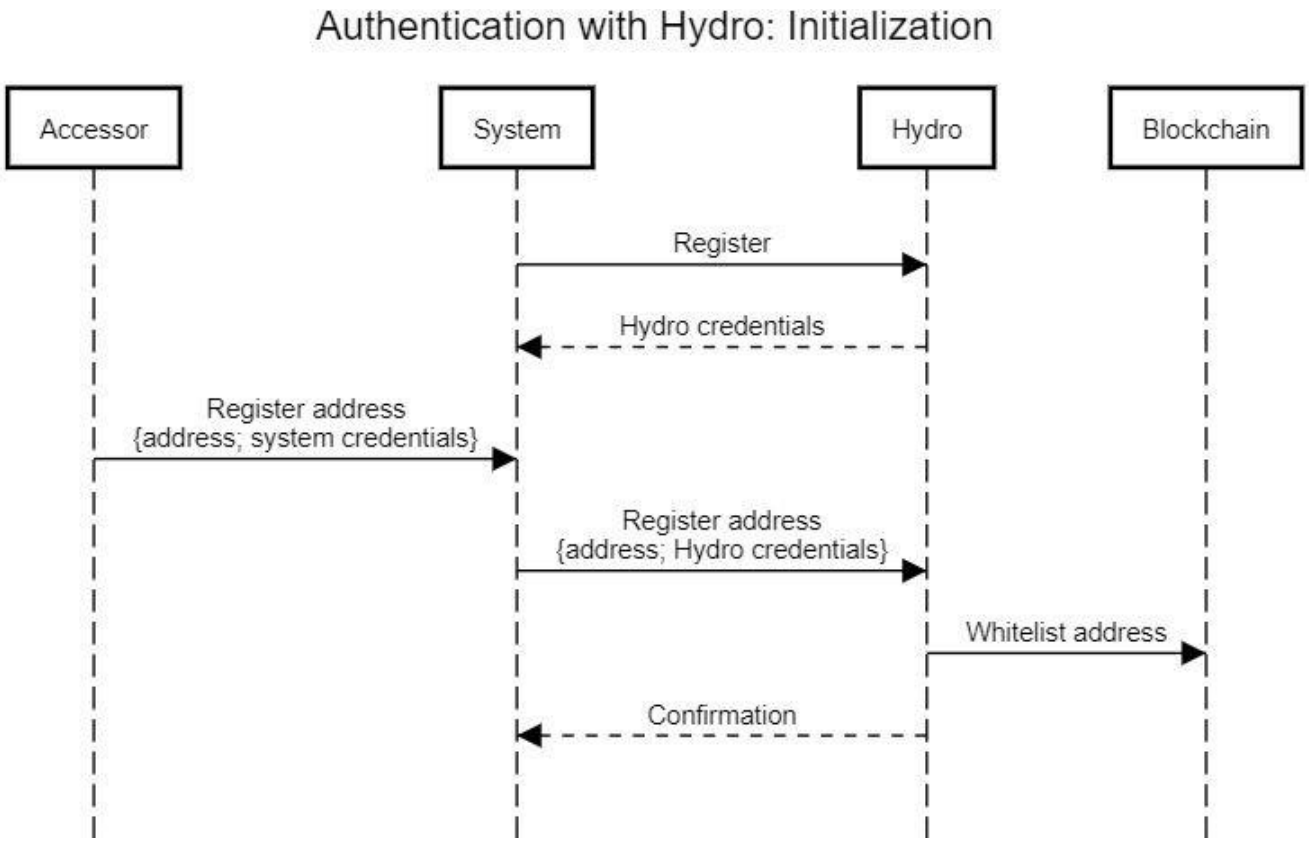
Każda Raindrop składa się z zestawu pięciu parametrów transakcyjnych:

1. *Sender* - Η διεύθυνση που πρέπει να ξεκινήσει τη συναλλαγή.
2. *Receiver* - Miejsce docelowe transakcji. Odpowiada to wywołaniu metody w Hydro smart contract.
3. *ID* - Identyfikator powiązany z systemem.
4. *Quantity* - Dokładna liczba HYDRO do wysłania.
5. *Challenge* - Losowo wyprodukowana seria alfanumeryczna.

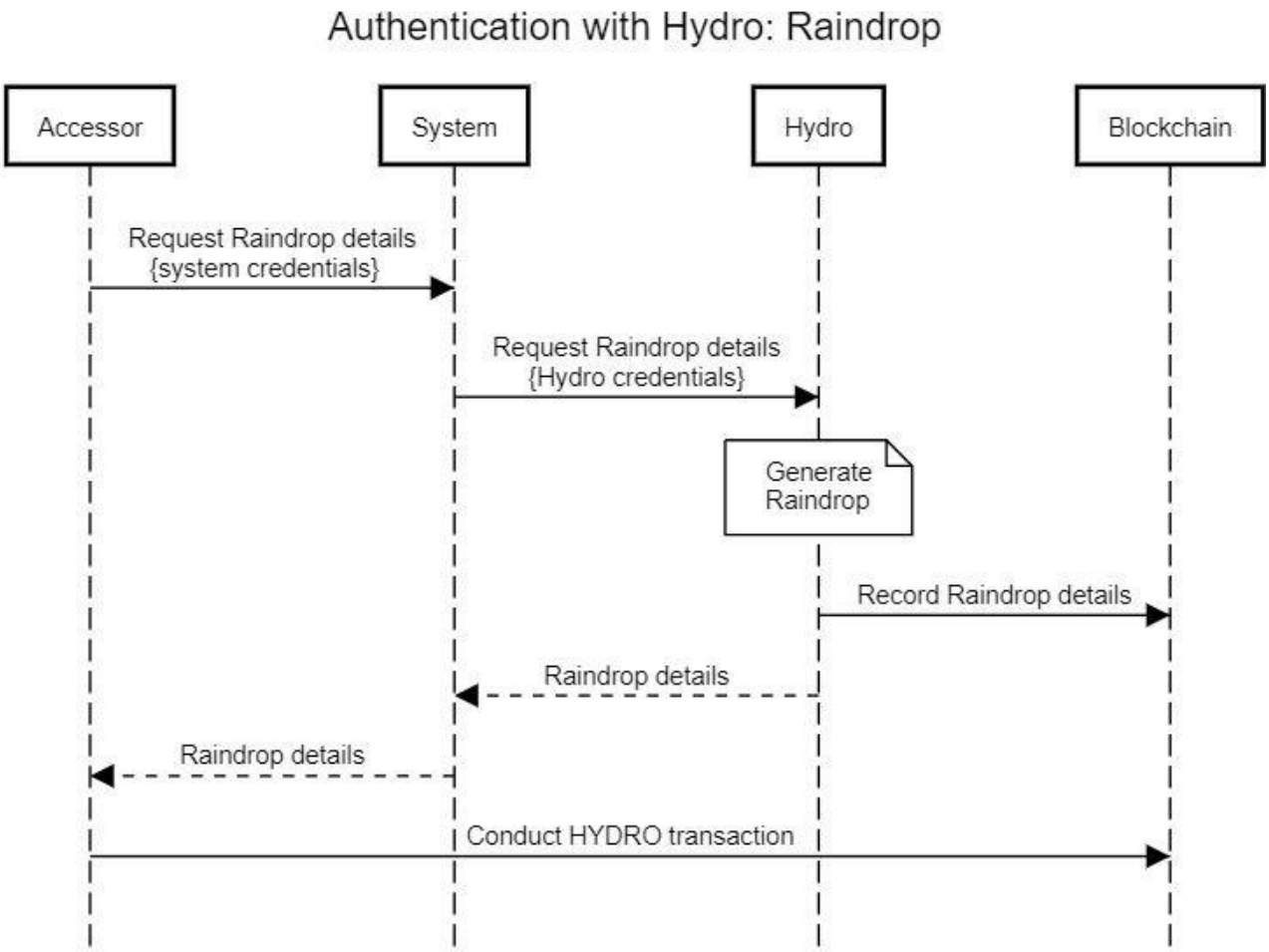
Poniżej znajduje się podsumowanie procesu uwierzytelniania, które można ogólnie podzielić na trzy etapy:

1. Initialization (Inicjalizacja)
2. Raindrop
3. Validation (Walidacja)

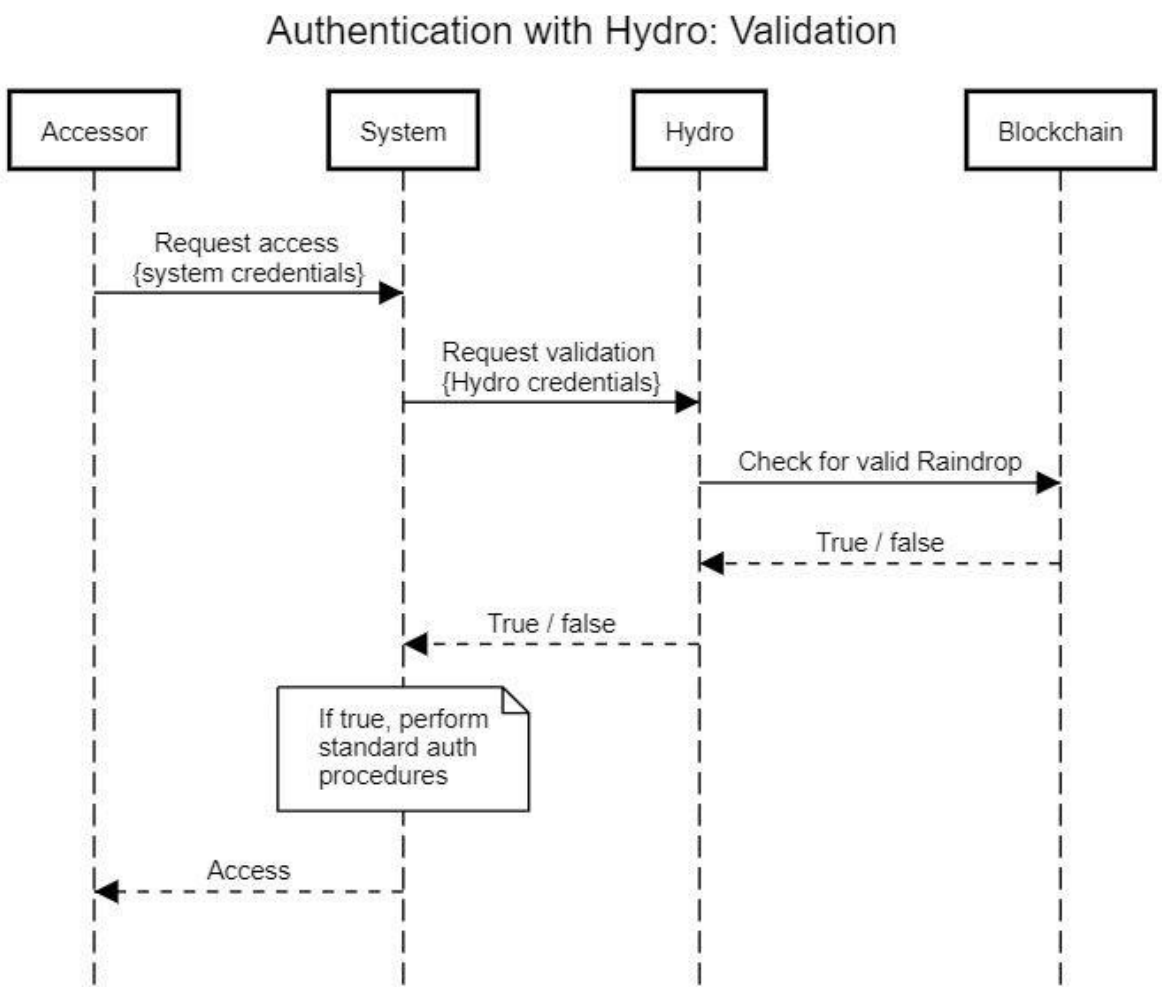
Inicjalizacja rozpoczyna się od systemu (np. Hydrogen), zarejestrowanego do używania Hydro i uzyskania certyfikatów, umożliwiając systemowi komunikację z blockchain za pośrednictwem jednostki Hydro. System monitoruje Accessor (np. instytucja finansowa) który rejestruje public ledger a następnie przesłał zarejestrowany adres do Hydro. Ten adres jest zapisany niezmieniony w blockchain, do whitelist przechowywanej w Hydro smart contract. System otrzymuje potwierdzenie, że adres został dodany do whitelist, które można również zweryfikować za pomocą publicznego wyświetlania. System musi być zarejestrowany tylko jeden raz, podczas gdy whitelist Accessor może być wyświetlana tylko raz na Accessor.



Po zakończeniu inicjowania, rdzeń procesu uwierzytelniania Hydro może się rozpocząć. Accessor, który musi wykonać transakcję Raindrop, inicjuje ten proces, prosząc o szczegóły dotyczące Raindrop z Systemu a System przesyła żądanie do Hydro. Hydro tworzy nową Kroplę Deszczu, przechowuje określone szczegóły niezmienione w blockchain i zwraca wszystkie szczegóły do Accessora za pośrednictwem systemu. Accessor, dostarczone ze wszystkimi wymaganymi informacjami, przeprowadza transakcję z zarejestrowanego adresu na metodę w Hydro smart contract. Jeśli adres nie znajduje się na whitelist, energia jest odrzucana - w przeciwnym razie jest rejestrowane w smart contract. Ważne jest, aby pamiętać, że ta transakcja powinna mieć miejsce poza Systemem, bezpośrednio z Accessora do Blockchain, ponieważ musi być podpisany kluczem prywatnym Accessor (który tylko Accessor może uzyskać).



Ostatnim krokiem w procesie jest sprawdzenie poprawności. W tym kroku Accessor żąda dostępu do systemu za pośrednictwem zainstalowanego mechanizmu systemu. Przed zastosowaniem dowolnego ze standardowych protokołów uwierzytelniania system pyta Hydro, jeśli Accessor dokonał ważnej transakcji Raindrop, czy nie. Hydro łączy się z smart contract, sprawdza ważność, i odpowiedzi z prawdziwą lub fałszywą determinacją. System jest w stanie zdecydować, jak postępować na podstawie tego ustalenia - jeśli jest fałszywe (false), System może odmówić dostępu, a jeśli to prawda (true) System może zapewnić dostęp.



Biorąc pod uwagę główne poświadczenia systemu lub istniejący istniejący protokół systemowy, jako czynnik uwierzytelniający, Hydro jest ważne do zaoferowania i jeden drugi czynnik. Badając dwie główne agencje ataku, możemy natychmiast potwierdzić jego użyteczność:

- Vector 1 - Atakujący kradnie dane uwierzytelniające Accessor
  - Osoba atakująca próbuje uzyskać dostęp do system z prawidłowymi poświadczeniami systemu
  - System sprawdza za pomocą Hydro, czy istnieje prawidłowa transakcja blockchain
  - Hydro zwraca wartość false, a system odmawia dostępu
- Vector 2 – Napastnik kradnie klucz prywatny z portfela Accessor
  - Atakujący próbuje przeprowadzić transakcję Hydro z zarejestrowanego adresu, bez szczegółów dotyczących Raindrop
  - Atakujący nie może ukończyć transakcji blockchain

- Atakujący nie może żądać dostępu do Systemu bez odpowiednich poświadczeń systemowych

Oczywiste jest, że atakujący musi wykraść główne poświadczenia system i prywatny klucz Accessora aby uzyskać dostęp do systemu. Pod tym względem Firma Hydro z powodzeniem dodała dodatkowy współczynnik uwierzytelnienia.

Otwieranie Raindrop dla publiczności

Chociaż ta usługa uwierzytelniania oparta na blockchain została zaprojektowana w celu zapewnienia ekosystemu Hydrogen API, ma on szerokie zastosowanie w różnych platformach i systemach. Ponieważ inni mogą korzystać z tego poziomu weryfikacji i bezpieczeństwa, jest on otwarty do użytku.

Podobnie jak Hydrogen włączą go jako warunek dostępu do ekosystemu API, ta sama puszka i każdy inny system, aby dodać go do istniejących procedur i protokołów. Każda platforma, czy API,aplikacja, oprogramowanie biznesowe, platforma gier itp., może używać Hydro do celów uwierzytelniania. Dokument będzie dostępny na GitHub dla tych, którzy chcą zintegrować ten poziom blockchain w ramce uwierzytelniania lub interfejsie API REST.

Case Study - Raindrop With OAuth 2.0

Istnieje wiele różnych sposobów z którymi Raindrop może być używany przez prywatne organizacje. Prywatne interfejsy API, bazy danych a sieci stworzyły przetworzone systemy z "tokens", klucze, aplikacje i protokoły w ciągu ostatniej dekady, w celu zabezpieczenia wrażliwych danych. Google na przykład stał się jednym z najpopularniejszych dostawców produktów na rynku z aplikacją Google Authenticator. Jak wspomniano wcześniej, nie ma powodu do rywalizacji lub zastąp istniejące protokoły.

Jako studium przypadku(Case Study), jest krótki przegląd tego, jak Hydrogen stosuje certyfikację Hydro jako poziom bezpieczeństwa w ogólnym systemie zabezpieczeń interfejsu API:

1. Partnerzy Hydrogen API powinieneś przede wszystkim mieć adresy IP swoich różnych środowisk na whitelist.
2. Partnerzy powinni zrobić aplikacja aby umieścić na whitelist adres Hydro.
3. Wszystkie połączenia z interfejsami API Hydrogen i transfery danych są zaszyfrowane i przesyłane za pośrednictwem protokołu HTTPS.
4. Partnerzy musi wypełnić ważną transakcję Hydro raindrop z zarejestrowanego adresu Hydro.

5. Partnerzy powinni używać Sprawdzanie poprawności OAuth 2.0. OAuth 2.0. (Open Authorization) to otwarty standard do uwierzytelnienia i autoryzacja na podstawie z tokens. Hydrogen obsługuje "Poświadczenia właściciela właściciela zasobu" i rodzaje grantów "Poświadczenia klienta", i każdego użytkownika API musi podać dane uwierzytelniające dla żądania uwierzytelnienia.
6. Jeśli żadna z powyższych pozycji nie naruszony, partner Hydrogen ma unikalny token, który musi zostać sprawdzony i być zweryfikowanym z każdym wywołaniem API.
7. Token jest ważny przez 24 godziny, po 24 godzinach partner powinien ratyfikowany znowu.

Jeśli któryś z tych kroków zostanie naruszony, użytkownik jest natychmiast zablokowany przez dostęp API. Haker nie może ominąć tych czynników bezpieczeństwa, zgadując losowo, ponieważ istnieją tryliony unikalnych kombinacji.

Ein Mehrfachsignaturen Portemonnaie ist richtig versichert ist nicht nur schwierig, gestohlen werden, aber die Öffentlichkeit der blockchain ermöglicht auch die schnelle Erkennung von Diebstahl, wie es um die Sicherheit API bezieht. Właściwie zabezpieczone portfel z wieloma podpisami jest nie tylko trudne do kradzieży, ale publiczny charakter blockchain pozwala również na szybkie rozpoznanie każdej kradzieży ponieważ dotyczy bezpieczeństwa interfejsu API.

Każdy może zobaczyć próba uwierzytelnienia dla Hydro smart contract, co oznacza że dni platform które są zagrożone przez wiele miesięcy może być przeszłość. Można teraz uniknąć hakerów API z większą bezpośredniością ze względu na możliwość wykrycia nieoczekiwanych prób autoryzacji w czasie rzeczywistym z dowolnego miejsca na świecie.

Ryzyka

Podobnie jak wszystkie powstające technologie, takie jak wczesne dni korzystania z mediów społecznościowych, poczty elektronicznej i przesyłania strumieniowego (które były zależne od łączności dial-up), ważne jest, aby główny zespół programistów dokładnie śledził nowe osiągnięcia w zakresie szybkości i ilości transakcji w Ethereum. Czy możesz sobie wyobrazić, że YouTube próbuje uruchomić w 1995 roku? Lub Instagram po raz pierwszy oferowany na telefonie Blackberry?

Twórcy Core Ethereum, tacy jak Vitalik Buterin i Joseph Poon, zaproponowali Plasma: Scalable Autonomous Smart Contracts uaktualnij do protokołu Ethereum:

> **Plazma jest proponowaną strukturą dla motywowanej i egzekwowanej realizacji smart contracts, która jest skalowalna do znacznej liczby aktualizacji stanu na sekundę (potencjalnie miliardowych), umożliwiając blockchain możliwość reprezentowania znacznej liczby zdecentralizowanych aplikacji finansowych na całym świecie. Te smart contracts są motywowane do dalszego działania autonomicznie za pośrednictwem opłat za transakcje sieciowe, które są ostatecznie uzależnione od leżącego u podstaw łańcucha blockchain (na przykład Ethereum) w celu wymuszania transactional state transition.**

Inne, takie jak The Raiden Network, zaproponowały rozwiązanie poza łańcuchem, zaprojektowane w celu przyspieszenia transakcji i obniżenia opłat. Obecnie Raindrop wywiera bardzo niewielką presję na Ethereum, więc skalowalność jest bardzo małym ryzykiem sukcesu technologicznego.

Conclusion

Niezmienność publicznego blockchain oferuje nowe sposoby zwiększenia bezpieczeństwa prywatnych systemów, takich jak API.

Ten dokument pokazał trzy ważne rzeczy:

1. Public blockchains mogą dodać wartość usługom finansowym.
2. Hydro Raindrop może zwiększyć bezpieczeństwo prywatnych systemów.
3. Istnieją bezpośrednie aplikacje Hydro Raindrop w platformie Hydrogen API.

Zespół Hydro uważa, że stworzone ramy mogą stanowić standardową infrastrukturę bezpieczeństwa dla nowego hybrydowego modelu publiczno-prywatnego, co przyniesie korzyści wszystkim podmiotom z branży usług finansowych i nie tylko.

Źródła:

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