Hydro Raindrop

Autenticazione Pubblica sulla Blockchain

Gennaio 2018

SOMMARIO

Sintesi

HYDRO: Etimologia – Dall'antico Greco ὑδρο- (*hudro-*), da ὕδωρ (*húdōr*, "acqua")

Hydro rende possibile a sistemi già esistenti, così come a nuovi, di integrare con continuità e sfruttare le immutabili e trasparenti dinamiche di una blockchain pubblica per migliorarne l'applicazione e la sicurezza di documenti, gestione d'identità, transazioni, e intelligenza artificiale.

In questo documento, si tratterà del caso di sistemi privati, ad esempio APIs, per utilizzare la blockchain pubblica Hydro per migliorare la sicurezza attraverso l'autenticazione pubblica.

La tecnologia qui presentata si chiama "Raindrop" (goccia di pioggia) - una transazione effettuata attraverso uno "smart contract" (contratto intelligente), che convalida pubblicamente l'accesso a sistemi privati, e può essere integrato in modo complementare a sistemi privati di autenticazione già esistenti. Lo scopo di questa tecnologia, è quello di fornire maggiore sicurezza per dati finanziari di origine sensibile, i quali sono soggetti a un sempre crescente rischio di brecce informatiche ed hacking.

La prima implementazione dell'Hydro Raindrop sarà effettuata sulla piattaforma Hydrogen API. Questo insieme di APIs modulare è disponibile ad aziende e sviluppatori a livello globale, per prototipare, costruire, testare, e sviluppare sofisticate piattaforme finanziare e prodotti.

L'Hydro Raindrop sarà reso disponibile come software open source all'intera comunità mondiale di sviluppatori, per permettere l'integrazione di Hydro Raindrop con qualsiasi REST API.

Blockchain & Ethereum

Hydro è sviluppato sul network Ethereum. Prima di fornire ulteriori dettagli sul progetto, è importante capire le idee fondamentali che costituiscono la blockchain, ed Ethereum.

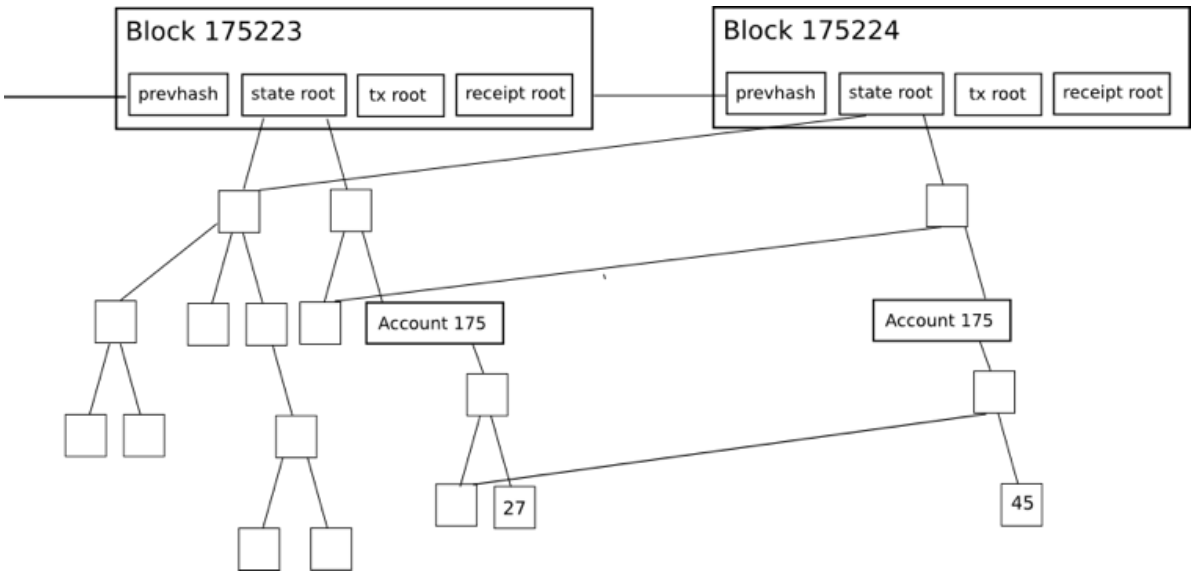
Sviluppare su Ethereum

Così come applicazioni tipo Snapchat sono state costruite utilizzando Swift, ed altri strumenti forniti dalla piattaforma iOS Apple, anche le applicazioni della blockchain possono essere costruite sulla piattaforma Ethereum. Snap Inc. non necessitava di costruire iOS, lo ha semplicemente usato come infrastruttura per lanciare un'applicazione social-media di successo.

Il progetto Hydro è simile. Si basa sulle migliaia di sviluppatori, che a livello globale stanno lavorando per rendere la tecnologia blockchain più veloce, forte e più efficiente. Hydro sfrutta questa infrastruttura che è costantemente in sviluppo ed in miglioramento, sviluppando interazioni specifiche al prodotto attorno alla tecnologia blockchain, che possono fornire tangibili benefici ad applicazioni di servizi finanziari.

Alberi di Merkle

Gli alberi di Merkle, sono utilizzati in sistemi assegnati per un'efficiente verifica dei dati. Essi sono efficienti perché usano hashes al posto di interi file. Gli Hashes sono un mezzo per codificare file, che sono molto più piccoli del file originale. Ogni intestazione di un blocco su Ethereum, contiene tre alberi di Merkle rispettivamente per transazioni, ricevute, e stati:



Fonte: Merkling in Ethereum; Vitalik Buterin, Fondatore Ethereum

Questo rende semplice, anche per un client leggero, ottenere risposte verificabili a domande tipo:

- Questo account esiste?
- Qual è il bilancio corrente?
- Questa transazione è stata inclusa in un blocco particolare?
- È successo un evento particolare in questo indirizzo oggi?

Contratti Intelligenti

Un concetto chiave abilitato da Ethereum ed altre reti basate sulla blockchain, è quello dei contratti intelligenti. Essi sono blocchi di codice auto-eseguenti coi quali diverse parti possono interagirci, togliendo la necessità di un mediatore. Il codice nei contratti intelligenti può essere visto come simile a clausole legali in un tradizionale contratto su carta, ma più raggiungere funzionalità molto più espandibili. I contratti possono avere regole, condizioni, penalità per non-conformità, o possono far partire altri processi. Quando avviati, i contratti si eseguono come originariamente dichiarato al tempo di sviluppo sulla catena pubblica, offrendo, integrati in essi, elementi di immutabilità e decentralizzazione.

I contratti intelligenti sono uno strumento vitale per costruire sull'infrastruttura Ethereum. La funzionalità principale della blockchain Hydro è ottenuto attraverso contratti personalizzati, i quali verranno discussi più avanti in questo documento.

Macchina Virtuale Ethereum

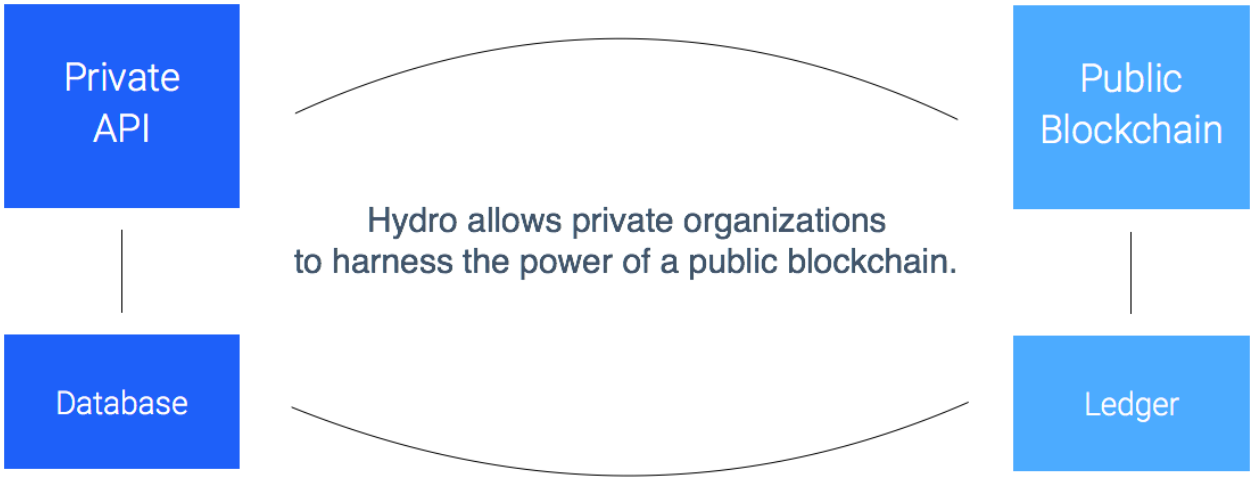
La Macchina Virtuale Ethereum (MVE) è l'ambiente d'esecuzione per i contratti intelligenti su Ethereum. L'MVE aiuta a prevenire attacchi Denial of Servie (DoS – Negazione del Servizio), si assicura che i programmi rimangano stateless (protocollo di comunicazione), e abilita comunicazioni che non possono essere interrotte. Le azioni sulla MVE hanno dei costi associati, chiamati gas, che dipende dalle risorse computazionali richieste. Ogni transazione ha un massimo di gas assegnato, conosciuto come "gas limit". Se il gas consumato da una transazione supera il limite consentito, allora il processo di essa verrà terminato.

Registro Pubblico

Un Registro Pubblico per Sistemi Privati

I sistemi che azionano piattaforme di servizi finanziari, siti, e applicazioni, possono spesso essere descritti come mezzi di scambio dati – inviano, ricevono, immagazzinano, aggiornano, e processano i dati per le entità che si interfacciano con essi. Per la natura di questi dati, e più genericamente di questi sistemi, essi spesso ospitano operazioni complesse in un modo privato e centralizzato. La dipendenza da strutture private, a sua volta, apre le porte per una varietà di sicurezza, trasparenza, ed aumenti di efficienza che possono essere ottenuti incorporando forze esterne che superano la portata del sistema interno.

Questo è il caso con la piattaforma API di Hydrogen. Hydro mira a toccare questi summenzionati guadagni, permettendo agli utenti di Hydrogen di interfacciarsi con una blockchain in un modo che risulta integrato con continuità dell'ecosistema Hydrogen, fondamentalmente privato.

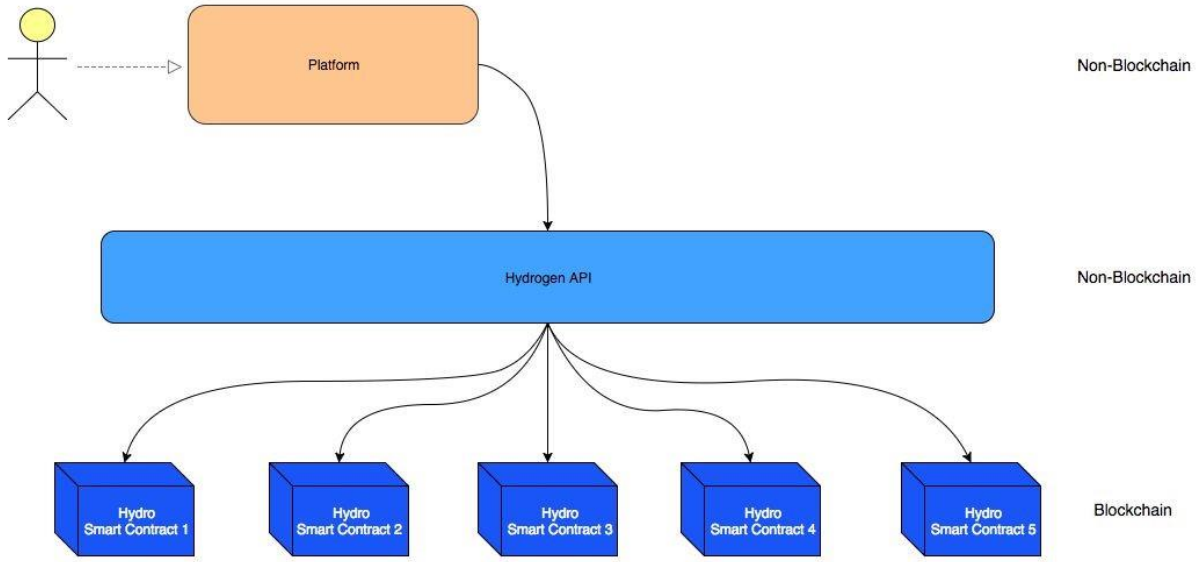


Operazioni pubbliche, basate sulla blockchain, possono avvenire prima, durante, o dopo operazioni private. L'interazione tra elementi privati e pubblici, può servire a validare, marchiare, registrare o migliorare i processi all'interno dell'ecosistema.

L'etica di questo modello e rendere i processi più robusti, toccando i benefici della tecnologia blockchain direttamente dove può produrre risultati più positivi. Mentre questa struttura ibrida potrebbe non essere applicabile a tutte le piattaforme, Hydro si concentra sull'offrire valore per i casi in cui lo è.

Architettura per L'Adozione

Hydro varia dalle esistenti iniziative basate sulla blockchain, perché può esistere indipendentemente e può essere affiancato a nuovi sistemi, oppure già esistenti, senza necessitare cambiamenti sistemici. Piuttosto di sostituire, Hydro mira a migliorare. Piattaforme ed istituzioni che si inseriscono nell'APIs di Hydrogen possono automaticamente accedere alla blockchain.



Gli ambiti in cui le piattaforme di servizi finanziari possono sfruttare Hydrogen sono vasti. Queste piattaforme possono azionare virtualmente ogni esperienza, ospitare qualsiasi numero di servizi proprietari, eseguire qualsiasi operazione di dati privati, e schierarsi in qualsiasi ambiente. Questo è dovuto alla modularità della struttura di Hydrogen, che è sinergico con Hydro, comportandosi come un catalizzatore complementare per l'adozione.

Raindrop

Costruita sul registro pubblico di Hydro, vi è un sistema di autenticazione basato sulla blockchain, chiamato "Raindrop". Esso offre un distinto, immutabile e globalmente visibile strato di sicurezza che verifica come una richiesta di accesso provenga da una fonte autorizzata.

I protocolli privati di autenticazione, ad esempio OAuth 2.0 offrono diversi livelli di robustezza ed utilità per il vario spettro di utilizzi che esiste. Non vi è la necessità di competere o tentare di sostituire questi protocolli – Hydro offre un mezzo per migliorarli, incorporando i meccanismi della blockchain come un componente della procedura di autenticazione. Questo può aggiungere utili strati di sicurezza in più, per contrastare brecce di sistema e compromissione di dati.

Prima di esaminare gli aspetti tecnici di Raindrop, si cerchi di capire il problema che vuole risolvere.

Lo Stato della Sicurezza Finanziaria

L'avvento dell'era dei dati ha comportato un aumento nella vulnerabilità di essi, e questo è particolarmente di interesse per servizi finanziari. I servizi finanziari sono spesso dei mezzi di transito di grandi quantità di dati sensibili e privati, ad esempio numeri d'ID governativi, credenziali di accounts e lo storico delle transazioni. A causa dell'elevata importanza di questi dati, un accesso indesiderato ad essi, comporta risultati catastrofici.

L'azienda Trend Micro ha pubblicato una relazione dove viene riportato come le voci contenenti Informazioni Identificative Personali (IIP) rubate, vengano vendute sul Deep Web per somme pari ad $1, scannerizzazioni di documenti, ad esempio passaporti, sono disponibili per $10, e credenziali di accesso a banche online per $200, rendendo quindi la distribuzione di dati rubati sempre più frammentata e non tracciabile.

Sfortunatamente, l'esistente sistema finanziario non ha una storia immacolata per quanto riguarda prevenire, diagnosticare e comunicare brecce nei propri dati, con i propri portatori d'interessi.

- Secondo uno studio recente di Javelin Strategy & Research - The 2017 Identity Fraud Study - $16 miliardi furono rubati da 15.4 milioni di utenti americani nel 2016 a causa del fallimento del sistema finanziario nel tutelare le Informazioni Identificative Personali (IIP).

- Nell'Aprile del 2017, Symantec ha pubblicato il suo Internet Security Threat Report, dove si è stimato che 1.1 miliardi di frammenti di IIP furono compromessi in diverse azioni nel corso del 2016.

- La 2016 Year End Data Breach Overview di Risk Based Security, scovò che 4,149 brecce di dati colpirono aziende di tutto il mondo nel 2016, esponendo più di 4.2 miliardi di documenti.

- La 2017 Thales Data Threat Report – Financial Services Edition, un'indagine globale di professionisti del settore informatico, ha scoperto che il 49% di organizzazioni di servizi finanziari ha subito brecce di sicurezza, il 78% sta spendendo di più per proteggersi, ma il 73% sta lanciando nuove iniziative legate a IA, IdC (Internet delle Cose), e tecnologie cloud, prima ancora di prepararsi adeguatamente.

La Breccia di Equifax

Il 29 luglio 2017, Equifax, un'agenzia di rapporti di crediti di 118 anni americana, è stata hackerata. Le IIP di 143 milioni di utenti furono esposte, tra cui il numero di previdenza sociale. I dati delle carte di credito di 209,000 clienti furono compromessi.

Qual è stata la causa di questa breccia?

Tutto cominciò con una delle tecnologie di backend utilizzate da Equifax. Struts è un framework open source per sviluppare applicazioni web in Java, creata da Apache Software Foundation. CVE-2017-9805 è una vulnerabilità di Apache Struts legata all'utilizzo del Struts REST plugin con XStream handler, per maneggiare carichi XML. Se sfruttata, permette ad un hacker non autenticato di eseguire codici maligni sul server di applicazione in maniera remota, per prendere controllo della macchina, o lanciare ulteriori attacchi da essa. Questo è stato patchato da Apache due mesi prima della breccia di Equifax.

Apache Struts ha una falla nel REST Plugin XStream che viene innescata quando il programma de-serializza gli input forniti dall'utente nelle richieste XML. Più in dettaglio, il problema avviene nella modalità toObject() di XStreamHandler, che non impone alcuna restrizione sul valore in input quando si utilizza la de-serializzazione XStream in un oggetto, risultando in vulnerabilità di esecuzione arbitrarie di codice.

Anche se il REST plugin fosse stato compromesso, avrebbe dovuto essere importante? C'è un modo per utilizzare la tecnologia della blockchain per rendere sicure le informazioni di questi 143 milioni di utenti che stanno ancora facendo affidamento su incombenti sistemi basati su REST API e Java?

Implementazione della Blockchain

È chiaro che l'integrità dei portali di dati finanziari può essere migliorata. Si esamini di seguito come un layer di sicurezza aggiuntiva può essere ottenuto tramite Hydro.
Il fondamentale meccanismo di consensi della rete Ethereum, assicura validità transazionale, perché i partecipanti processano collettivamente le transazioni propriamente firmate. Questa realtà porta a decentralizzazione ed immutabilità, ma, più importantemente, fornisce un mezzo per mitigare accessi non autorizzati ad un gateway che maneggia dati sensibili.

Con Hydro, l'autenticazione può essere confermata su delle operazioni transazionali sulla blockchain. Un'API ad esempio, può scegliere se validare sviluppatori ed applicazioni richiedendo che essi mandino determinate transazioni, con carichi di dati ben definiti, tra determinati indirizzi sulla blockchain, come una condizione che fa partire un protocollo standard di autenticazione.

L'Hydro Raindrop

La pioggia contiene pacchetti di acqua condensata che vanno da 0.0001 a 0.005 centimetri di diametro. In un tipico temporale vi sono miliardi di questi pacchetti, ognuno di dimensione casuale, velocità, e forma. A causa di ciò, non è possibile prevedere con certezza l'esatto comportamento della pioggia. In modo simile, ogni transazione di autenticazione Hydro è unica e virtualmente impossibile che sia stata scaturita a caso – da qui il motivo del nome *Raindrops*.

Le piattaforme di servizi finanziari utilizzano comunemente una verifica tramite *micro-depositi,* per validare gli account dai clienti. Il concetto è semplice: la piattaforma esegue piccoli depositi di somme casuali nel conto bancario del presunto utente. Per provare che l'utente possiede tale conto, lui o lei devono riallocare il deposito ricevuto nella piattaforma, venendo poi validati. L'unico modo per cui un utente possa sapere la somma versatogli (oltre ad indovinare) è quello di accedere nel conto bancario in questione.

La verifica basata su Raindrop con Hydro è analoga. Anziché mandare all'utente una determinata somma, e farsela ritornare, si definisce una transazione che deve essere eseguita dall'utente da un determinato portafoglio. L'unico modo per cui l'utente possa eseguire una transazione valida è quello di accedere al portafoglio in questione.

Usando Raindrops, sia il sistema che chi vi accede possono monitorare i tentativi di autenticazione sull'immutabile registro pubblico. Questa transazione basata sulla blockchain è disaccoppiata dalle basilari operazioni

di sistema, avviene su una rete distribuita, e dipende dalla proprietà delle chiavi private. Di conseguenza, risulta un ottimo mezzo di validazione.

Uno Sguardo in Dettaglio

Vi sono quattro entità coinvolte nel processo di autenticazione Hydro:

1. *Accessor* – La parte che tenta di accedere al sistema. Nel caso di Hydrogen, l'Accessor è l'istituzione finanziaria o l'applicazione che utilizza Hydrogen APIs come fulcro della propria infrastruttura digitale.
2. *System* – Il sistema o portale a cui accede l'Accessor. Per Hydrogen, il sistema è l'Hydrogen APIs in sé.
3. *Hydro* – Il modulo utilizzato dal System per comunicare ed interfacciarsi con la blockchain.
4. *Blockchain* – Il registro pubblico distribuito che processa le transazioni HYDRO e contiene i contratti intelligenti Hydro, attraverso i quali l'informazione può essere mandata e ricevuta, o possono essere eseguite operazioni su di essa.

Ogni Raindrop, nella sua interezza, è rappresentata da 5 parametri:

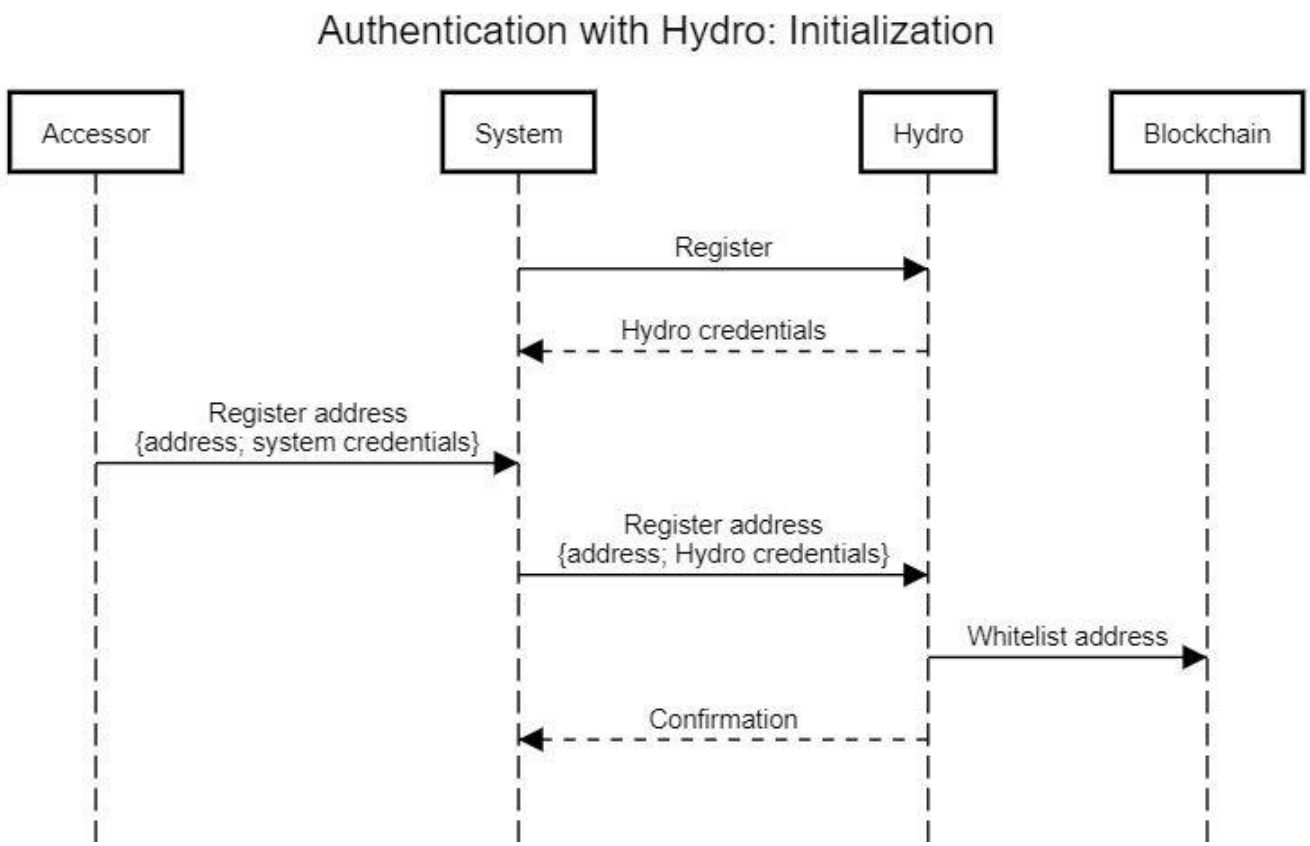
1. *Sender* – L'indirizzo che devi iniziare la transazione.
2. *Receiver* – La destinazione della transazione. Questo corrisponde a chiamare un metodo in un contratto intelligente Hydro.
3. *ID* – Un identificativo che è associato al System.
4. *Quantity* – Una precisa somma di HYDRO da inviare.
5. *Challenge* – Una stringa alfanumerica generata a random.

Qui sotto vi è lo schema del processo di autenticazione, che può essere generalmente classificato in 3 steps:

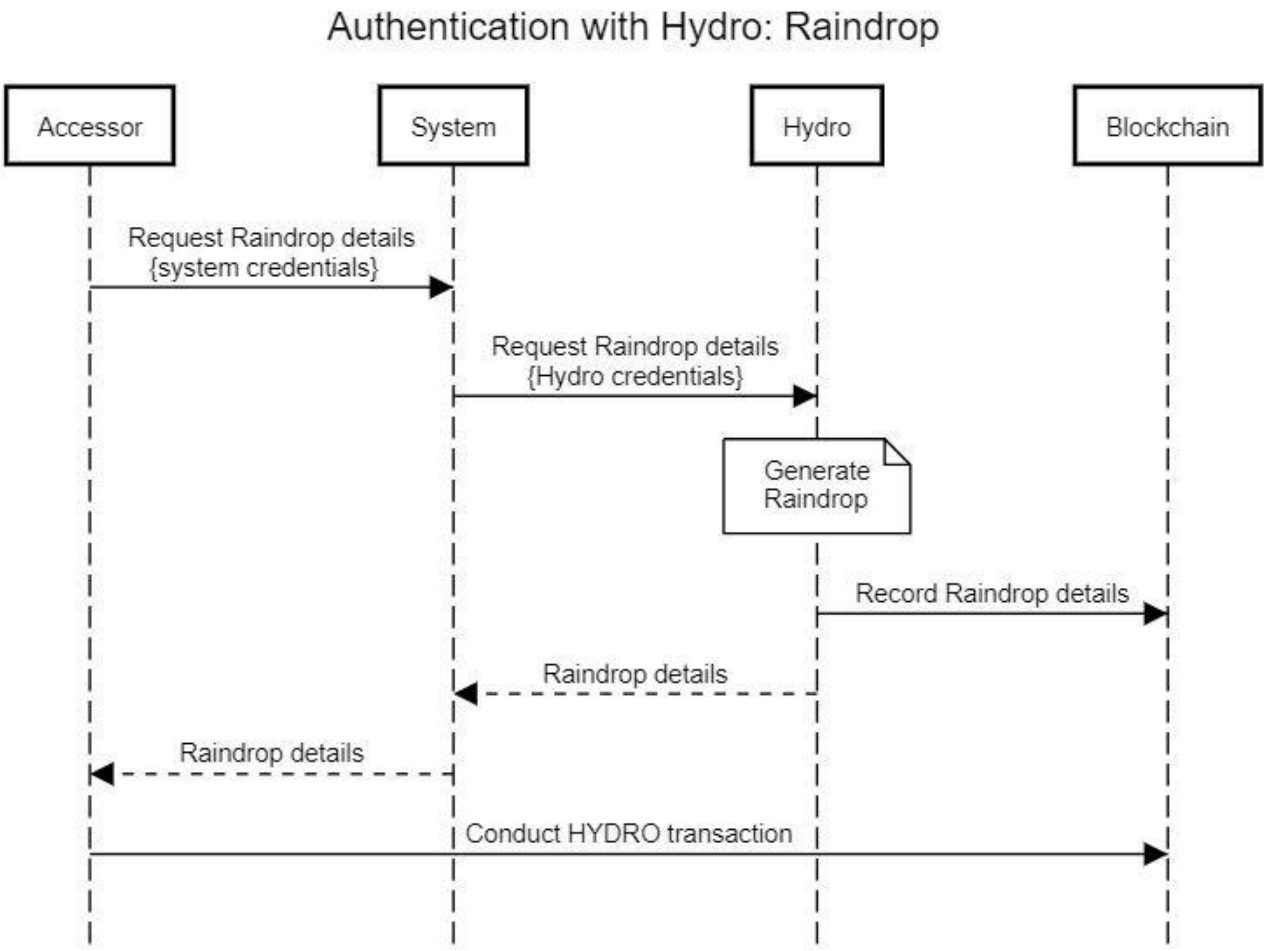
1. Inizializzazione
2. Raindrop
3. Validazione

L'inizializzazione comincia con una registrazione del System (es. Hydrogen) ad utilizzare Hydro ed ottenendo le credenziali, abilitando il System a comunicare con la blockchain tramite il modulo Hydro. Il System accoglie un Accessor (es. istituzione finanziaria) che registra un indirizzo pubblico, il quale viene passato ad Hydro. Questo indirizzo è permanentemente scritto nella blockchain in una lista bianca contenuta in un contratto intelligente Hydro. Il System riceve la conferma dell'inserimento nella lista bianca, che può inoltre essere verificata come un evento visibile pubblicamente.

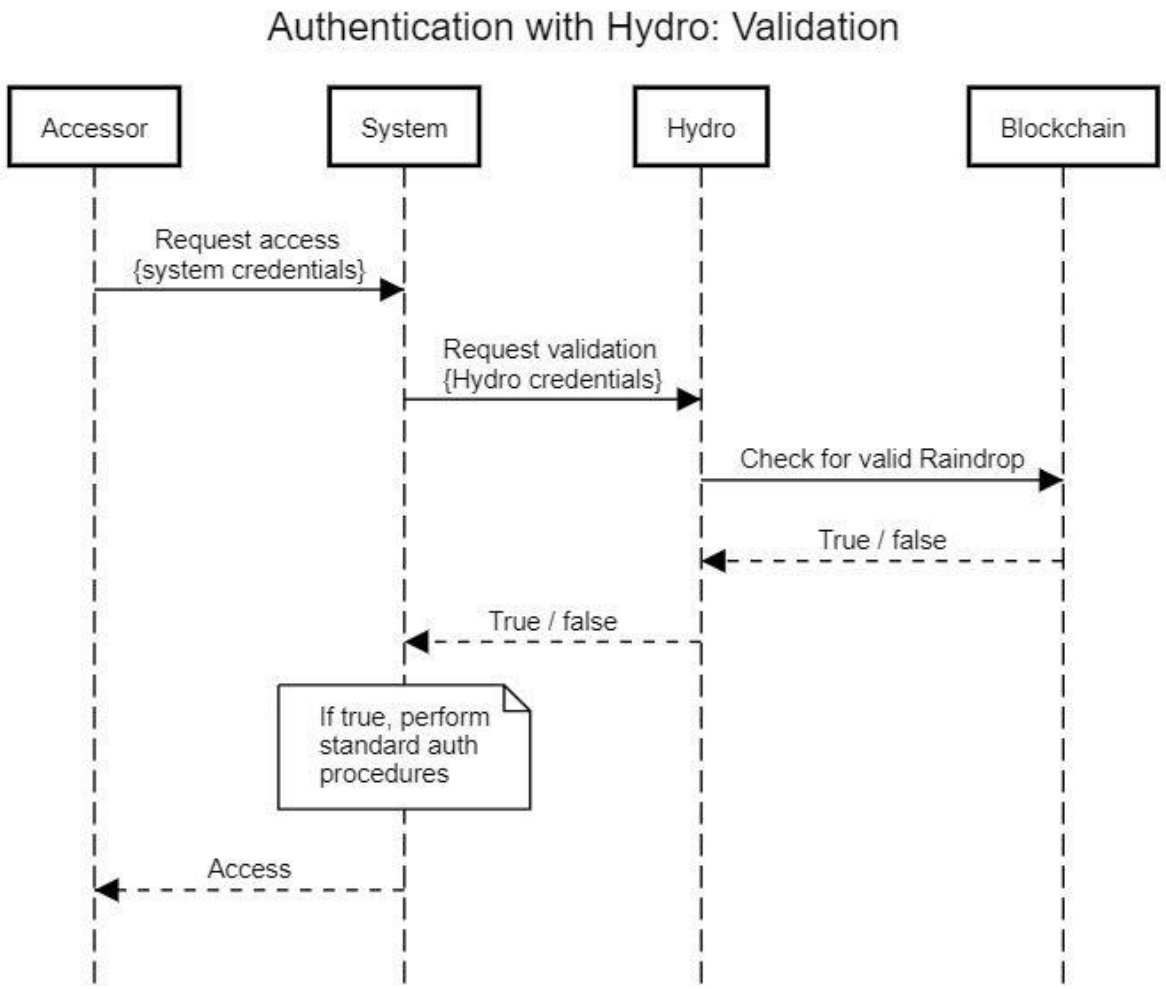
La registrazione del System deve avvenire una volta sola, invece l'inserimento nella lista bianca degli Accessors deve avvenire una volta sola per Accessor.



Quando l'inizializzazione è completa, il processo chiave dell'autenticazione Hydro può cominciare. L'Accessor, che deve eseguire una transazione Raindrop, fa partire il processo richiedendo i dettagli della Raindrop dal System, e il sistema indirizza la richiesta ad Hydro. Hydro genera una nuova Raindrop, immagazzina certi dettagli permanentemente nella blockchain, e ritorna i dettagli completi all'Accessor, tramite il System. L'Accessor, con tutte le informazioni di cui ha bisogno, esegue una transazione da un indirizzo registrato ad un metodo nel contratto intelligente Hydro. Se l'indirizzo non è nella lista bianca, l'azione è rifiutata – altrimenti, risulta registrata nel contratto intelligente. È importante notare che questa transazione dovrebbe avvenire al di fuori del System, direttamente dall'Accessor alla blockchain, dato che dev'essere firmata con la chiave privata dell'Accessor (che solo lui è in grado di ottenere).



L'ultimo passo del processo è la Validazione. In questo passo, l'Accessor richiede ufficialmente accesso al System tramite il meccanismo stabilito dal System. Prima di implementare qualsiasi dei suoi protocolli standard di autenticazione, il System chiede ad Hydro se l'Accessor ha eseguito una transazione Raindrop valida. Hydro si interfaccia con il contratto intelligente, ne controlla la validità, e risponde con una designazione vero/falso. Il System è quindi in grado di decidere come procedere basandosi sulla designazione – Se è falsa, il System nega l'accesso, se è vera il System garantisce l'accesso.



Se si considerano le credenziali basilari del System – o qualsiasi tipo di protocollo sia attivo – ad essere un fattore di autenticazione, è importante che Hydro fornisca un utile secondo fattore. Esaminando i principali vettori di attacco, se ne può prontamente confermare l'utilità:

- Vettore 1 – L'aggressore ruba le credenziali base del System dell'Accessor
    - L'aggressore tenta di ottenere l'accesso al System con delle credenziali valide
    - Il System controlla con Hydro se una transazione valida è stata eseguita sulla blockchain
    - Hydro restituisce "falso", e il System nega l'accesso
- Vettore 2 – L'aggressore ruba la chiave(i) privata del portafoglio dell'Accessor.

- L'aggressore tenta di eseguire la transazione Hydro dall'indirizzo registrato, senza conoscere i dettagli Raindrop
- L'aggressore non può eseguire una transazione valida
- L'aggressore non può richiedere accesso al System senza le adeguate credenziali

Risulta chiaro quindi che l'aggressore deve rubare sia le credenziali base del System, che la chiave(i) privata del portafoglio dell'Accessor per accedere al System. A questo proposito, Hydro ha con successo aggiunto un'ulteriore fattore di autenticazione

Aprire Raindrop al Pubblico

Mentre questo servizio di autenticazione basato sulla blockchain fu architettato per mettere in sicurezza l'ecosistema Hydrogen API, è ampliamente applicabile a diverse piattaforme e sistemi. Siccome pensiamo che altri possono potenzialmente beneficiare da questo layer di verifica, lo metteremo a disposizione per l'utilizzo.

Così come Hydrogen lo integrerà come una precondizione per accedere il proprio ecosistema di API, ogni sistema potrà aggiungerlo ai propri protocolli esistenti. Qualsiasi piattaforma – sia essa un API, applicazione, azienda di software, piattaforma di gaming, etc. – può sfruttare Hydro con scopi di autenticazione. La documentazione formale sarà disponibile su GitHub per coloro che volessero incorporare questo layer di blockchain in un framework di autenticazione o REST API.

Caso di Studio – Raindrop con OAuth 2.0

Vi sono dozzine di modi in cui la pubblicazione di Raindrop può essere utilizzata da organizzazioni private. APIs private, database, e reti hanno creato elaborai sistemi di tokens (gettoni), chiavi, applicazioni, e protocolli nell'ultimo decennio, tutto nel tentativo di mettere in sicurezza dati sensibili. Google, ad esempio, è diventato uno dei più popolari fornitori di prodotti nel mercato con l'app Google Authenticator. Come menzionato in precedenza, non vi è ragione di competere o rimpiazzare protocolli già esistenti.

Come caso di studio, ecco una breve panoramica di come Hydrogen implementi l'autenticazione Hydro come livello di sicurezza nel suo API security network:

1. I partner di Hydrogen API devono prima di tutto avere gli indirizzi IP dei propri ambienti, immessi in una lista bianca.

2. I partner devono richiedere di mettere nella lista bianca un indirizzo Hydro pubblico.
3. Tutte le chiamate all'Hydrogen API e trasferimento di dati sono criptati e trasmessi tramite protocollo HTTPS.
4. I partner devono aver completato una valida transazione Raindrop dall'indirizzo Hydro registrato.
5. I partner devono utilizzare la validazione OAuth 2.0. OAuth (Open Authorization) è uno standard per autenticazione e autorizzazione basato su un sistema token. Hydrogen supporta "Resource Owner Password Credentials" e "Client Credentials" come tipo di concessioni, e ogni utente dell'API deve fornire le credenziali per una richiesta di autenticazione.
6. Se nessuno dei 5 step precedenti è stato violato, il partner di Hydrogen sarà concesso un token unico, che va controllato e verificato con ogni chiamata API.
7. Il token sarà valido per 24 ore, dopo le quali il partner deve verificarsi di nuovo.

Se qualsiasi di questi step venga violato, l'utente è immediatamente bloccato dall'accedere all'API. Un hacker non può bypassare questi step indovinando a caso, dato che ci sono trilioni di uniche combinazioni.

L'autenticazione Hydro basata sulla blockchain è una componente importante del protocollo di sicurezza Hydrogen. Il team Hydrogen incoraggia i partner ad impostare portafogli multi-firma, e conservare le chiavi private in diverse posizioni sicure, non assieme ad altre credenziali, così da evitare qualsiasi punto debole. Un portafogli multi-firma messo in sicurezza, non solo è molto difficile da rubare, ma la nature pubblica della blockchain permette la veloce identificazione di qualsiasi ladro alla sicurezza dell'API.

Chiunque può visualizzare un tentativo di autentificazione al contratto intelligente Hydro, il che significa che l'era di piattaforme compromesse per mesi, può essere una cosa del passato. Gli hackers dell'API possono essere contrastati con repentinità per via della possibilità di identificare tentativi di autenticazione inaspettati in tempo reale, da qualsiasi parte nel mondo.

Rischi

Così come ogni tecnologia nascente, ad esempio l'inizio dei social media, email, applicazioni di streaming (che si basavano sulla connettività dial-up), è importante il team di sviluppo principale tenga traccia dei nuovi sviluppi nella velocità e volume nelle transazioni Ethereum. Ti immagineresti Youtube che tentava di partire nel 1995? O instagram inizialmente uscito per Blackberry?

Sviluppatori principali di Ethereum come Vitalik Buterin e Joseph Poon hanno proposto l'aggiornamento Plasma: contratti intelligenti autonomi scalabili al protocollo Ethereum:

> **Plasma è un framework proposto per l'incentivata e forzata esecuzione dei contratti intelligenti, che risulta scalabile fino ad un significante numero di cambi di stato al secondo (potenzialmente miliardi) abilitando la blockchain ad essere in grado di rappresentare un significante numero di applicazioni finanziare decentralizzate globalmente. Questi contratti Intelligenti sono incentivati a continuare le operazioni anonimamente tramite le tasse nelle transazioni nella rete, che è decisamente dipendente dalla sottostante blockchain (es. Ethereum) per forzare transizioni di stato transazionali.**

Altri, come il "The Raiden Network" hanno proposto una soluzione della scalabilità al di fuori della blockchain, disegnata per operare transazioni più veloci e tasse più basse. Ora come ora, il Raindrop metterà **sotto minimo sforzo** il framework Ethereum, di conseguenza la scalabilità è un rischio minore per il successo della tecnologia.

Conclusione

L'immutabilità della blockchain pubblica offre nuovi modi per migliorare la sicurezza di sistemi privati quali APIs.

Questo documento ha sottolineato tre importanti concetti:

1. La blockchain pubblica può aggiungere valore nei servizi finanziari.
2. La Raindrop Hydro può aumentare la sicurezza di sistemi privati.
3. Vi sono applicazioni immediati del Raindrop Hydro nella piattaforma Hydrogen API.

Il team Hydro crede che il framework qui presentato può essere uno standard per le infrastrutture di sicurezza, per un nuovo modello ibrido di sistema privato-pubblico, che beneficerà tutti i portatori d'interessi nell'industri dei servizi finanziari ed oltre.

Fonti:

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