

Hydro Raindrop
Autentificarea publică pe Blockchain

ianuarie 2018

CUPRINS

rezumate

[Blockchain și Ethereum](#)

[clădire pe Ethereum](#)

[Merkle Trees](#)

[Contracte inteligente](#)

[Ethereum Mașină virtuală](#)

[Cartea publică](#)

[O carte publică pentru sisteme private arhitează
pentru adoptare](#)

[Raindrop](#)

[Starea securității financiare](#)

[Equifax breșă](#)

[Adăugarea unui strat Blockchain](#)

[Cele Hydro Raindrop](#)

[O privire detaliată](#)

[Deschiderea cele raindrop publicului](#)

[studiu de caz - Raindrop With OAuth 2.0](#)

[riscuri](#)

[Concluzie](#)

rezumate

HYDRO: Etimologie - De la Ancient ὕδρο- (*h udro-*), from ὕδωρ (*h údōr*, "apă")

Hydro permite sistemelor private noi și existente să integreze și să valorifice dinamica imuabilă și transparentă a unui blockchain public pentru a spori securitatea aplicațiilor și documentelor, gestionarea identității, tranzacțiile și inteligența artificială.

În această lucrare, se va face un caz pentru sistemele private, cum ar fi API-urile, de a folosi blocul public public Hydro pentru a spori securitatea prin autentificarea publică.

Tehnologia propusă este numită "Raindrop" - o tranzacție realizată printr-un contract inteligent care validează în mod public accesul la sistemul privat și poate completa metodele de autentificare private existente. Tehnologia este menită să ofere securitate suplimentară pentru datele financiare sensibile care sunt din ce în ce mai expuse riscului de hacking și încălcări.

Implementarea inițială a Hydro Raindrop se efectuează pe platforma Hydrogen API. Acest set modular de API-uri este disponibil pentru întreprinderi și dezvoltatori la nivel global pentru a prototipa, construi, testa și a implementa platforme și produse sofisticate de tehnologie financiară.

Hydro Raindrop va fi pus la dispoziția comunității dezvoltatoare mondiale ca software open source, pentru a permite dezvoltatorilor să integreze Hydro Raindrop cu orice REST API.

Blockchain & Ethereum

Hydro este implementat pe rețeaua Ethereum. Înainte de a oferi mai multe detalii cu privire la proiect, este important să înțelegem câteva idei fundamentale despre blockchain și Ethereum.

[clădire pe Ethereum](#)

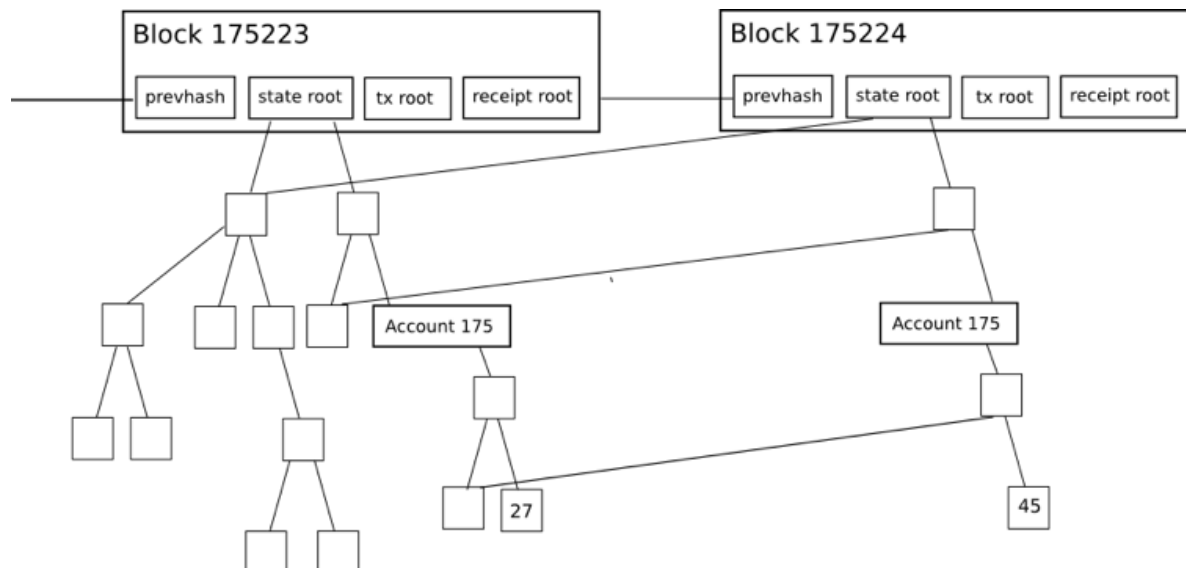
Aplicațiile precum Snapchat au fost construite cu ajutorul instrumentelor Swift și a altor instrumente oferite pe platforma Apple iOS, iar aplicațiile blocate pot fi construite pe partea de sus a Ethereum. Snap Inc. nu avea nevoie să construiască iOS, a folosit-o ca infrastructură pentru a lansa o aplicație media socială în schimbare de joc.

Proiectul Hydro este similar. Se bazează pe mii de dezvoltatori la nivel global, care depun eforturi pentru a face tehnologia de blocare mai rapidă, mai puternică și mai eficientă. Hydro folosește această infrastructură care se îmbunătățește constant, dezvoltând interacțiuni axate pe produs în jurul tehnologiei blocurilor, care pot oferi beneficii tangibile aplicațiilor de servicii financiare.

Merkle Trees

Merkle trees sunt utilizate în sisteme distribuite pentru o verificare eficientă a datelor. Ele sunt eficiente deoarece folosesc hashes în loc de fișiere complete. Hashes sunt modalități de codare a fișierelor care sunt mult mai mici decât fișierul propriu-zis.

Fiecare antet bloc din Ethereum conține trei copaci Merkle pentru tranzacții, încasări și stat:



Source: [Merkling in Ethereum](#); Vitalik Buterin, Ethereum fondator

Acest lucru face ca un client ușor să obțină răspunsuri verificabile la întrebări, cum ar fi:

- Acest cont exista?
- Care este soldul actual?
- A fost tranzacția inclusă într-un anumit bloc?
- A avut loc un eveniment special în această adresă astăzi?

Contracte inteligente

Un concept cheie, pe care îl oferă Ethereum și alte rețele bazate pe blocuri, este acela al contractelor inteligente. Acestea sunt blocuri de cod de auto-execuție pe care mai multe părți le pot interacționa, reducând nevoia de intermediari de încredere. Codul într-un contract inteligent poate fi văzut ca fiind similar cu clauzele juridice dintr-un contract tradițional de hârtie, dar poate și să obțină o funcționalitate mult mai expansivă. Contractele pot avea reguli, condiții, sancțiuni pentru neconformitate sau pot declanșa alte procese. Atunci când sunt declanșate, contractele se execută așa cum sa spus inițial la momentul desfășurării în lanțul public, oferind elemente încorporate de imutabilitate și descentralizare.

Contractul inteligent este un instrument vital pentru construirea infrastructurii Ethereum. Funcționalitatea centrală a stratului de blocare Hydro este realizată prin contracte personalizate, așa cum este discutat mai târziu în această lucrare.

Ethereum Mașină virtuală

Masina virtuala Ethereum (EVM) este mediul de rulare pentru contracte inteligente pe Ethereum. EVM ajută la prevenirea atacurilor Denial of Service (DoS), asigură menținerea apatrizilor și permite comunicarea care nu poate fi întreruptă. Acțiunile pe EVM au costuri asociate cu acestea, numite gaze, care depind de resursele de calcul necesare. Fiecare tranzacție are o cantitate maximă de gaz alocată acesteia, cunoscută ca o limită g. Dacă gazul consumat de o tranzacție atinge limita, va înceta să continue procesarea.

Cartea publică

O carte publică pentru sisteme private

Sistemele care furnizează platforme de servicii financiare, site-uri web și aplicații pot fi deseori descrise drept medii ale fluxului de date - ele trimit, prelucrează, stochează, actualizează și procesează date pentru entitățile cu care interfață. Datorită naturii acestor date și a serviciilor financiare în general, aceste sisteme adesea găzduiesc operațiuni complexe într-o manieră privată și centralizată. Reliance pe structuri private, la rândul său, deschide ușa pentru a obține o varietate de securitate, transparență și câștiguri de eficiență prin încorporarea forțelor externe care depășesc acoperirea sistemului intern.

Acesta este cazul platformei API a hidrogenului. Hydro își propune să profite de avantajele menționate mai sus, permițând utilizatorilor de hidrogen să interconecteze cu un blocaj în moduri care sunt integrate perfect în ecosistemul hidrogen fundamental privat.

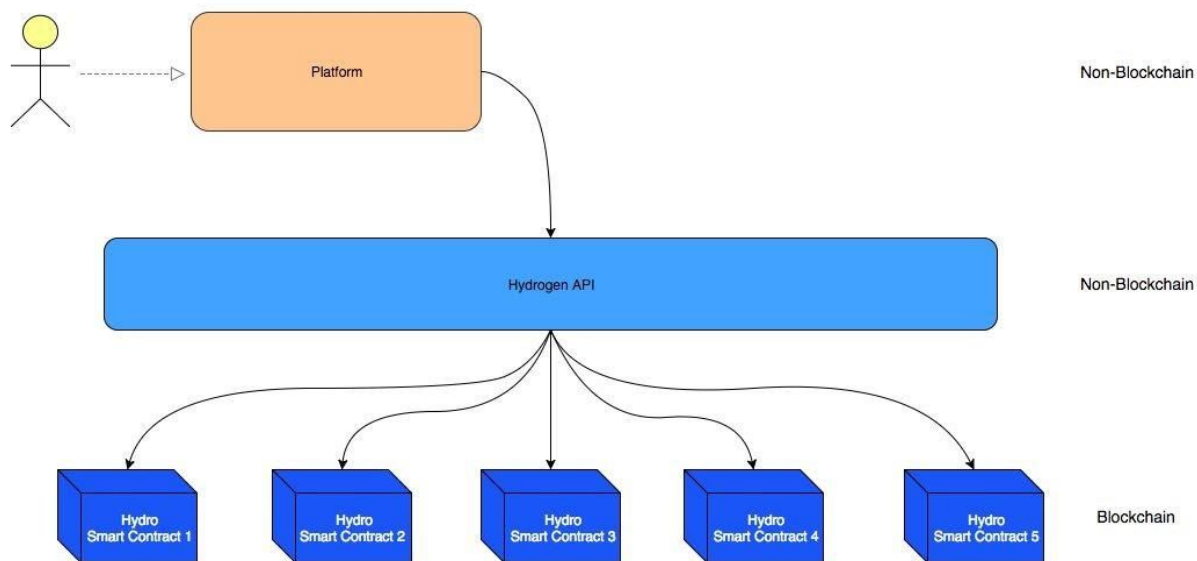


Operațiunile bazate pe blochează pot să apară înainte, în timpul sau după operațiuni private. Interacțiunea dintre elementele private și publice poate servi la validarea, ștampilarea, înregistrarea sau îmbunătățirea proceselor din cadrul unui ecosistem.

Etosul acestui model face ca procesele să devină mai robuste, beneficiind de avantajele tehnologiei blocurilor, în special în cazul în care pot produce cel mai mare impact pozitiv. Deși acest cadru hibrid nu poate fi aplicabil tuturor platformelor, Hydro se concentrează asupra furnizării de valoare pentru cazurile în care este.

Arhitez pentru adoptare

Hydro diferă de numeroasele inițiative de blockchain existente, deoarece poate exista independent și strat în jurul sistemelor noi sau existente fără a necesita schimbări sistemice. În loc să o înlocuiască, Hydro dorește să se amplifice. Platformele și instituțiile care se conectează la API-urile Hydrogen pot accesa automat blocul de blocuri.



Sfera de aplicare a platformelor de servicii financiare care pot utiliza hidrogenul este largă. Aceste platforme pot genera practic orice experiență, pot găzdui orice număr de servicii proprietare, pot efectua orice operațiune de date private și pot fi implementate în orice mediu. Acest lucru este posibil datorită modularității structurale a hidrogenului și este sinergic cu Hydro, care acționează ca un motor complementar de adopție.

Raindrop

Construit pe partea de sus a acestei cărți publice Hydro este un serviciu de autentificare bazat pe blochează, denumit "Raindrop". Acesta oferă un strat distinct, imuabil, vizibil la nivel global, care verifică faptul că o solicitare de acces provine dintr-o sursă autorizată.

Protocoalele private de autentificare, cum ar fi OAuth 2.0, oferă niveluri variate de robustețe și utilitate pentru spectrul cazurilor de utilizare care există. Nu este nevoie să concurezi sau să încerci să înlocuiști aceste protocoale - Hydro oferă o modalitate de a le îmbunătăți prin încorporarea mecanicii blockchain ca o componentă a unei proceduri de autentificare. Acest

lucru poate adăuga un nivel util de securitate pentru a ajuta la atenuarea încălcărilor sistemului și a compromisurilor de date.

Înainte de a examina aspectele tehnice ale Raindrop, să aruncăm o privire mai întâi la problema pe care încearcă să o rezolve.

Starea securității financiare

Creșterea vârstei datelor a adus cu ea o creștere a vulnerabilității și acest lucru este deosebit de important pentru serviciile financiare. Platformele financiare sunt adesea gateway-uri către cantități mari de date private și sensibile, cum ar fi numerele de identificare ale guvernului, acreditările contului și istoricul tranzacțiilor. Din cauza importanței critice a acestor date, accesul nejustificat este de obicei întâlnit cu rezultate catastrofale.

Firma de cercetare din industrie Trend Micro a publicat un raport care a constatat că articolele furate de informații cu caracter personal (PII) sunt vândute pe Web Deep pentru doar \$ 1, scanări ale documentelor precum pașapoartele sunt disponibile pentru doar 10 \$ și acreditări de conectare la bancă pentru suma de 200 de dolari, ceea ce face ca distribuirea datelor furate să devină din ce în ce mai fragmentată și mai puțin detectabilă.

Din nefericire, sistemul financiar existent nu are un istoric nemaipomenit atunci când vine vorba de prevenirea, diagnosticarea și comunicarea încălcărilor de date cu părțile interesate.

- Potrivit unui studiu recent realizat de Javelin Strategy & Research - Studiul privind fraudă de identitate din 2017 - 16 miliarde de dolari au fost furate de la 15,4 milioane de consumatori din SUA în 2016 din cauza eșecurilor sistemului financiar de a proteja Personally Identifiable Information (PII).
- În aprilie 2017, Symantec a publicat Raportul privind amenințările la Internet, care estimează că 1,1 miliarde de piese de PII au fost compromise în diferite capacități pe parcursul 2016.
- Raportul rapid privind încălcarea datelor de la sfârșitul anului 2016 privind securitatea bazată pe risc, a constatat că au avut loc 4,149 de încălcări ale datelor în întreprinderi la nivel global 2016, expunând peste 4,2 miliarde de înregistrări.

- Raportul privind amenințările la adresa datelor din 2017 Thales - Ediția serviciilor financiare, un sondaj al profesioniștilor IT la nivel global în servicii profesionale, a constatat că 49% dintre organizațiile de servicii financiare au suferit o încălcare a securității în trecut, 78% cheltuiesc mai mult pentru a se proteja, 73% lansează noi inițiative legate de tehnologiile AI, IoT și cloud înainte de a pregăti soluții de securitate adecvate.

Equifax Breach

La 29 iulie 2017, Equifax, o agenție americană de raportare a creditelor de 118 ani, a fost hacked. 143 milioane de consumatori au prezentat PII, inclusiv numerele de securitate socială. 209.000 de clienți au compromis datele de pe cardul de credit.

Care a fost cauza acestei încălcări?

Începe cu una dintre tehnologiile backend folosite de Equifax. Struts este un framework open source pentru dezvoltarea de aplicații web în limbajul de programare Java, construit de Apache Software Foundation. CVE-2017-9805 este o vulnerabilitate în Apache Struts în legătură cu utilizarea pluginului Struts REST cu un handler XStream pentru a manipula sarcini utile XML. Dacă este exploatat, permite unui atacator care nu are autentificare la distanță să execute un cod rău intenționat pe serverul de aplicații, fie pentru a prelua mașina, fie pentru a lansa alte atacuri. Acest lucru a fost patch-out de Apache cu două luni înainte de încălcarea Equifax.

Apache Struts conține un defect în XStream Plugin-ul REST care este declanșat deoarece programul insecure de-serializează intrarea furnizată de utilizator în cererile XML. Mai precis, problema apare în metoda toObject () a lui XStreamHandler, care nu impune nicio restricție asupra valorii primite când se utilizează deserializarea XStream într-un obiect, rezultând în vulnerabilități arbitrare de execuție a codului.

Chiar dacă acest plugin REST a fost compromis, ar trebui să aibă importanță? Există o modalitate de a utiliza tehnologia blockchain pentru a securiza informațiile financiare ale acestor 143 milioane de clienți, în timp ce încă se bazează pe actualul sistem REST API și Java?

Adăugarea unui strat Blockchain

Este clar că integritatea gateway-urilor cu date financiare poate fi îmbunătățită. Să examinăm modul în care se realizează un strat suplimentar de securitate prin Hydro.

Mecanismele fundamentale de consens ale rețelei Ethereum asigură valabilitatea tranzacției, deoarece participanții procesează colectiv tranzacții care sunt semnate în mod corespunzător. Această realitate duce la descentralizare și imutabilitate, dar, mai important, oferă un vector pentru atenuarea accesului neautorizat la o poartă care gestionează datele sensibile.

Cu Hydro, autentificarea poate fi bazată pe operațiunile tranzacționale pe blocul de blocuri. Un API, de exemplu, poate alege să valideze dezvoltatorii și aplicațiile solicitându-i să inițieze anumite tranzacții, cu sarcini utile de date, între anumite adrese din blocul de blocuri, ca o condiție prealabilă pentru lansarea unui protocol standard de autentificare.

Cele Hydro Raindrop

Ploaia conține pachete de apă condensată, variind de la 0,0001 până la 0,005 cm în diametru. Într-o furtună tipică, există miliarde din aceste pachete, fiecare având mărime, viteză și formă aleatoare. Din acest motiv, nu se poate prezice fiabil natura exactă a ploii. În mod similar, fiecare tranzacție de autentificare Hydro este unică și practic imposibilă să apară întâmplător - de aceea îi numim Raindrops.

Platformele de servicii financiare utilizează în mod obișnuit verificarea micro-depozitelor pentru a valida conturile clientului. Conceptul este simplu: platforma face depozite mici ale sumelor aleatoare în conturi bancare ale unui utilizator. Pentru a dovedi că utilizatorul deține propriul cont, el trebuie să retransmită sumele depuse înapoi la platformă, care apoi sunt validate.

Singurul mod în care utilizatorul poate cunoaște sumele valide (pe lângă ghicitul) este accesarea conturilor bancare în cauză.

Verificarea bazată pe Raindrop cu Hydro este similară. În loc să trimitem utilizatorului o sumă și să îl retransmitem, definim o tranzacție și utilizatorul trebuie să o execute dintr-un portofel cunoscut. Singurul mod în care utilizatorul poate efectua o tranzacție valabilă este accesarea portofelului în cauză.

Prin utilizarea Raindrops, atât sistemul, cât și accesoriul pot monitoriza încercările de autorizare pe un registru public imuabil. Această tranzacție bazată pe blochează este decuplată de la operațiile de bază ale sistemului, are loc într-o rețea distribuită și depinde de proprietatea asupra cheilor private. Prin urmare, servește ca vector de validare util.

O privire detaliată

Există patru entități implicate în procesul de autentificare Hydro:

1. Accessor - Partea care încearcă să acceseze un sistem. În cazul hidrogenului, accesoriul este o instituție sau o aplicație financiară care utilizează API-urile hidrogen pentru infrastructura sa digitală de bază.
2. Sistem - Sistemul sau gateway-ul accesat de Accessor. Pentru hidrogen, sistemul este API-ul Hydrogen.
3. Hydro - Modulul utilizat de sistem pentru a comunica și interfața cu blocul de blocuri.
4. Blockchain - registrul public distribuit care procesează tranzacțiile HYDRO și conține contractele Hydro smart, prin intermediul cărora informațiile pot fi împinse, trase sau operate altfel.

Each Raindrop, in its entirety, is a set of five transactional parameters:

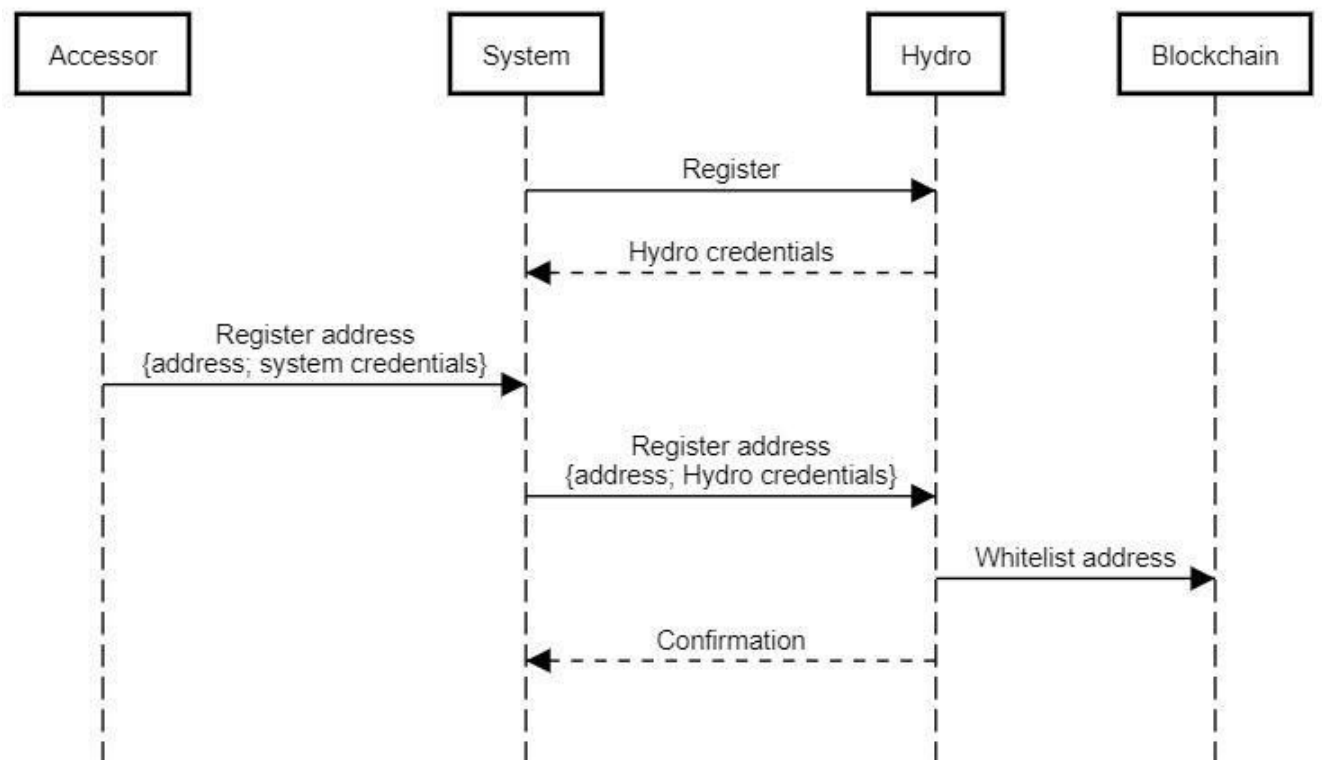
1. *Expeditor - Adresa care trebuie să inițieze tranzacția.*
2. *Receptor - destinația tranzacției. Aceasta corespunde apelării unei metode într-un contract Hydro smart.*
3. *ID - Un identificator care este asociat cu sistemul.*
4. *Cantitate - Un număr precis de HYDRO pentru a trimite.*
5. *provocare - Un șir alfanumeric generat aleator.*

Mai jos este o schiță a procesului de autentificare, care poate fi în general clasificată în trei etape:

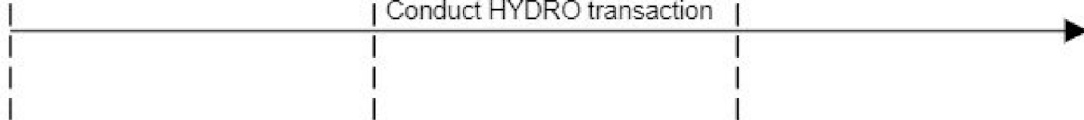
1. Inițializarea
2. Raindrop
3. Validarea

Inițializarea începe cu înregistrarea unui sistem (de exemplu, hidrogen)

Authentication with Hydro: Initialization

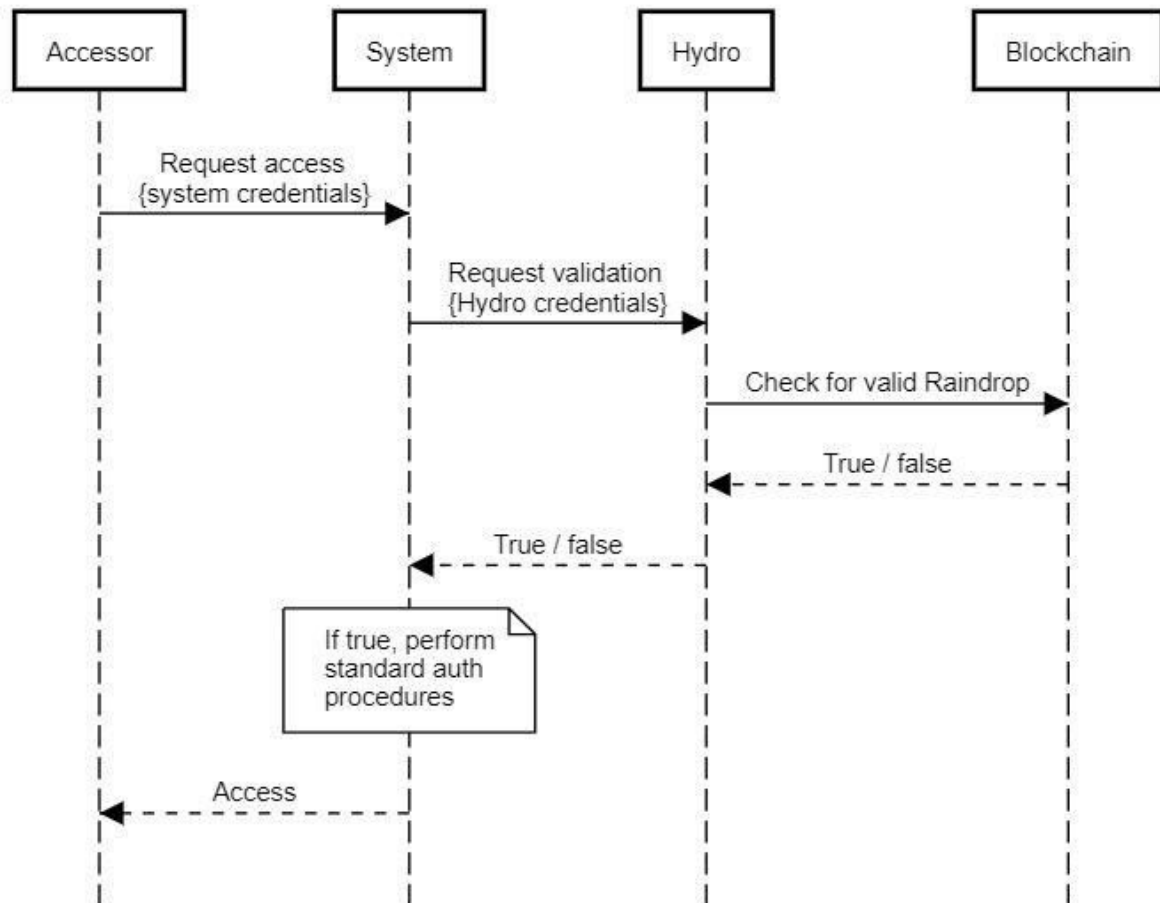


După terminarea inițializării, nucleul procesului de autentificare Hydro poate începe. Accessor, care trebuie să execute o tranzacție Raindrop, începe acest proces solicitând detalii de la Raindrop de la sistem, iar sistemul trimite cererea către Hydro. Hidrogenul generează un nou Raindrop, stochează anumite detalii imutabile pe blocul de blocuri și returnează detaliile complete Accesoriului prin Sistem. Accesoriul, dotat cu toate informațiile necesare, efectuează o tranzacție de la adresa înregistrată la o metodă din contractul Hydro smart. Dacă adresa nu este listată pe listă, acțiunea este respinsă - în caz contrar, aceasta este înregistrată în contractul inteligent. Este important să rețineți că această tranzacție ar trebui să aibă loc în afara sistemului, direct de la Accessor la blocul de blocuri, deoarece trebuie să fie semnat cu cheia privată a Accesoriului (pe care numai Accessor ar trebui să o obțină).



Ultimul pas al procesului este Validarea. În acest pas, Accessor solicită oficial accesul la sistem prin intermediul mecanismului stabilit de sistem. Înainte de a implementa oricare dintre protocoalele standard de autentificare, Sistemul solicită Hydro dacă accesul a efectuat sau nu o tranzacție valabilă Raindrop. Hydro interfețează cu contractul inteligent, verifică validitatea și răspunde cu o denumire adevărată / falsă. Sistemul este capabil să decidă cum ar trebui să procedeze pe baza acestei desemnări - dacă este falsă, sistemul poate refuza accesul și, dacă este adevărat, sistemul poate acorda acces.

Authentication with Hydro: Validation



Dacă luăm în considerare acreditările de bază ale sistemului - sau orice protocol existent în sistem - care este în general un factor de autentificare, este important ca stratul Hydro să reprezinte un al doilea factor util. Examinând cei doi vectori de atac primari, putem confirma cu ușurință utilitatea acestora:

- Vector 1 - Atacatorul fură acreditările de bază ale sistemului Accessor
 - 1 Atacatorul încearcă să obțină acces la sistem cu acreditări de sistem valide
 - Sistemul verifică cu Hydro pentru a determina dacă o tranzacție valabilă a fost făcută pe blocul de blocuri
 - Hydro returnează false și sistemul refuză accesul
- Vector 2 - Atacatorul fură cheia privată la portofelul Accessor
 - 1 Atacatorul încearcă să efectueze o tranzacție Hydro de la adresa înregistrată, fără a solicita detalii Raindrop
 - Atacatorul nu poate efectua o tranzacție blocată validă

- Atacatorul nu poate, de asemenea, solicita accesul la sistem fără acreditările de sistem corespunzătoare

Este clar că atacatorul trebuie să fure atât acreditările de bază ale sistemului, cât și cheia privată a portofelului pentru a accesa sistemul. În acest sens, Hydro a adăugat cu succes un factor suplimentar de autentificare.

[Deschiderea celei raindrop publicului](#)

În timp ce acest serviciu de autentificare bazat pe blocuri a fost conceput pentru a ajuta la protejarea ecosistemului Hydrogen API, acesta este foarte aplicabil pe diferite platforme și sisteme. Pentru că simțim că alții pot beneficia de acest nivel de verificare, îl deschidem pentru utilizare.

Așa cum Hidrogenul o va integra ca o condiție prealabilă pentru accesul la ecosistemul său API, tot așa orice sistem poate adăuga la procedurile și protocoalele existente. Orice platformă - fie un API, o aplicație, un software pentru întreprinderi, o platformă de jocuri, etc. - poate utiliza Hydro pentru scopuri de autentificare. Documentația oficială va fi disponibilă pe GitHub pentru cei care doresc să integreze acest strat de blocaj într-un cadru de autentificare sau REST API.

[studiu de caz - Raindrop With OAuth 2.0](#)

Există zeci de moduri în care lansarea Raindrop poate fi utilizată de organizații private. API-urile private, bazele de date și rețelele au creat sisteme complexe de jetoane, chei, aplicații și protocoale în ultimul deceniu, în încercarea de a asigura date sensibile. Google, de exemplu, a devenit unul dintre cei mai cunoscuți furnizori de produse de pe piață cu aplicația Google Authenticator. După cum sa menționat anterior, nu există nici un motiv pentru a concura sau a înlocui aceste protocoale existente.

Ca studiu de caz, este prezentată o scurtă trecere în revistă a modului în care Hydrogen implementează autentificarea Hydro ca nivel de securitate în cadrul general de securitate API:

1. Partenerii API ai hidrogenului trebuie să aibă în prealabil adresele IP ale diferitelor lor medii pe lista albă.
2. Partenerii trebuie să ceară să se prezinte pe lista albă o adresă hidro publică.

3. Toate apelurile către API-urile cu hidrogen și transferurile de date sunt criptate și transmise prin protocolul HTTPS.
4. Partenerii trebuie să încheie o tranzacție valabilă cu hidro-raindrop de la adresa Hydro înregistrată.

Partenerii trebuie să utilizeze validarea OAuth 2.0. OAuth (autorizație deschisă) este un standard deschis pentru autentificarea și autorizarea bazate pe token. Hidrogenul acceptă "acreditările parolei proprietarului resurselor" și "clientul"

Credite ", iar fiecare utilizator API trebuie să furnizeze acreditări pentru o solicitare de autentificare.

5. În cazul în care nici unul dintre cele cinci elemente de mai sus nu este încălcat, partenerului cu hidrogen îi este acordat un jeton unic, care trebuie verificat și verificat cu fiecare apel API.
6. Jetonul este valabil 24 de ore, după care partenerul trebuie să se valideze din nou.

Dacă oricare dintre acești pași este încălcat, utilizatorul este imediat blocat de accesul API. Un hacker nu poate ocoli acești factori de securitate ghicind întâmplător, pentru că există trilioane de combinații unice.

Autentificarea bazată pe blochează hidrogen este o componentă importantă a protocolului de securitate pentru hidrogen. Echipa Hidrogen încurajează partenerii să creeze portofele cu mai multe semnături și să stocheze cheile private în mai multe locații securizate independent de alte acreditări, astfel încât nu există un singur punct de eșec. Un portofel multi-semnătura protejat corespunzător este nu numai dificil de furat, dar natura publică a blocului permite, de asemenea, recunoașterea rapidă a oricărui furt, deoarece se referă la securitatea API-ului.

Oricine poate vedea o încercare de autentificare a contractului Hydro smart, ceea ce înseamnă că zilele când platformele sunt compromise de luni întregi pot fi un lucru din trecut. API-urile hackerilor pot fi acum compromise cu mai multă imediate datorită abilității de a detecta încercări neautorizate de autorizare în timp real, de oriunde din lume.

riscuri

La fel ca orice tehnologie în devenire, cum ar fi primele zile ale aplicațiilor sociale, e-mail și streaming (care se bazau pe conectivitatea dial-up), este important ca echipa de dezvoltare de bază să urmărească îndeaproape noile evoluții în vitezele și volumele tranzacției Ethereum. Vă puteți imagina că YouTube încearcă să lanseze în 1995? Sau Instagram fiind oferit pentru BlackBerry?

Dezvoltatorii Core Ethereum, cum ar fi Vitalik Buterin și Joseph Poon, au propus contractele Smart Plasma: Scalable Autonomous Smart to upgrade la Protocolul Ethereum:

Plasma este un cadru propus pentru executarea contractelor inteligente stimulate și executate, care este scalabil la o sumă semnificativă de actualizări de stat pe secundă (potențial miliarde), permițând blocului să reprezinte o cantitate semnificativă de aplicații financiare descentralizate la nivel mondial. Aceste contracte inteligente sunt stimulate să continue să funcționeze în mod autonom prin taxe de tranzacționare în rețea, care se bazează, în cele din urmă, pe blocul de blocare (de exemplu, Ethereum) pentru a impune tranzițiile de stat tranzacționale.

Alții, cum ar fi The Raiden Network, au propus o soluție de scalare în afara lanțului, proiectată să alimenteze tranzacții mai rapide și taxe mai mici. În acest moment, Raindrop va pune o presiune foarte minimă asupra cadrului Ethereum, astfel scalabilitatea este un risc foarte mic pentru succesul tehnologiei.

Concluzie

Imutabilitatea unui blockchain public oferă noi modalități de a spori securitatea sistemelor private, cum ar fi API-urile.

Această lucrare a arătat trei lucruri importante:

1. Blocurile publice pot aduce valoare adăugată în serviciile financiare.
2. Hydro Raindrop poate îmbunătăți securitatea sistemelor private.

3. 3. Există aplicații imediate ale Hydro Raindrop în cadrul platformei Hydrogen API.

Echipa Hydro consideră că cadrul stabilit poate fi infrastructura standard de securitate pentru un nou model de sisteme hibrid private-privat, care va aduce beneficii tuturor părților interesate din industria serviciilor financiare și dincolo de aceasta.

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](#)