Hydro Raindrop

Autentificarea publică pe Blockchain

ianuarie 2018

CUPRINS

rezumate

HYDRO: Etimologie - De la Ancient ὑδρο- (*h udro-*), from ὕδωρ (*h údōr*, “apă”)

Hydro permite sistemelor private noi şi existente să integreze şi să valorifice dinamica imuabilă şi transparentă a unui blockchain public pentru a spori securitatea aplicaţiilor şi documentelor, gestionarea identităţii, tranzacţiile şi inteligenţa 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 tranzacţie realizată printr-un contract inteligent care validează în mod public accesul la sistemul privat şi 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 şi încălcări.

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

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

Blockchain & Ethereum

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

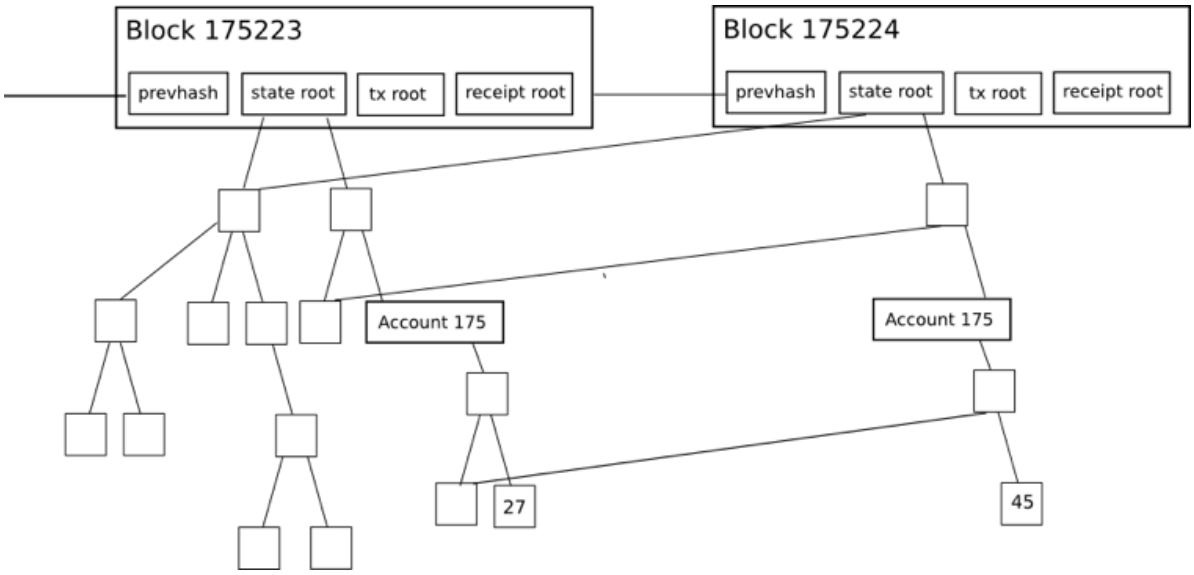
clădire pe Ethereum

Aplicaţiile precum Snapchat au fost construite cu ajutorul instrumentelor Swift şi a altor instrumente oferite pe platforma Apple iOS, iar aplicaţiile 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 aplicaţie 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 şi mai eficientă. Hydro foloseşte această infrastructură care se îmbunătăţeşte constant, dezvoltând interacţiuni axate pe produs în jurul tehnologiei blocurilor, care pot oferi beneficii tangibile aplicaţiilor 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 fişiere complete. Hashes sunt modalităţi de codare a fişierelor care sunt mult mai mici decât fişierul propriu-zis.
Fiecare antet bloc din Ethereum conţine trei copaci Merkle pentru tranzacţii, încasări şi stat:



Source: Merkling in Ethereum; Vitalik Buterin, Ethereum fondator

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

- Acest cont exista?
- Care este soldul actual?
- A fost tranzacţia 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 şi alte reţele bazate pe blocuri, este acela al contractelor inteligente. Acestea sunt blocuri de cod de auto-execuţie pe care mai multe părţi le pot interacţiona, reducând nevoia de intermediari de încredere. Codul într-un contract inteligent poate fi văzut ca fiind similar cu clauzele juridice dintr-un contract tradiţional de hârtie, dar poate şi să obţină o funcţionalitate mult mai expansivă. Contractele pot avea reguli, condiţii, sancţiuni pentru neconformitate sau pot declanşa alte procese. Atunci când sunt declanşate, contractele se execută aşa cum sa spus iniţial la momentul desfăşurării în lanţul public, oferind elemente încorporate de imutabilitate şi descentralizare.

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

Ethereum Maşină virtuală

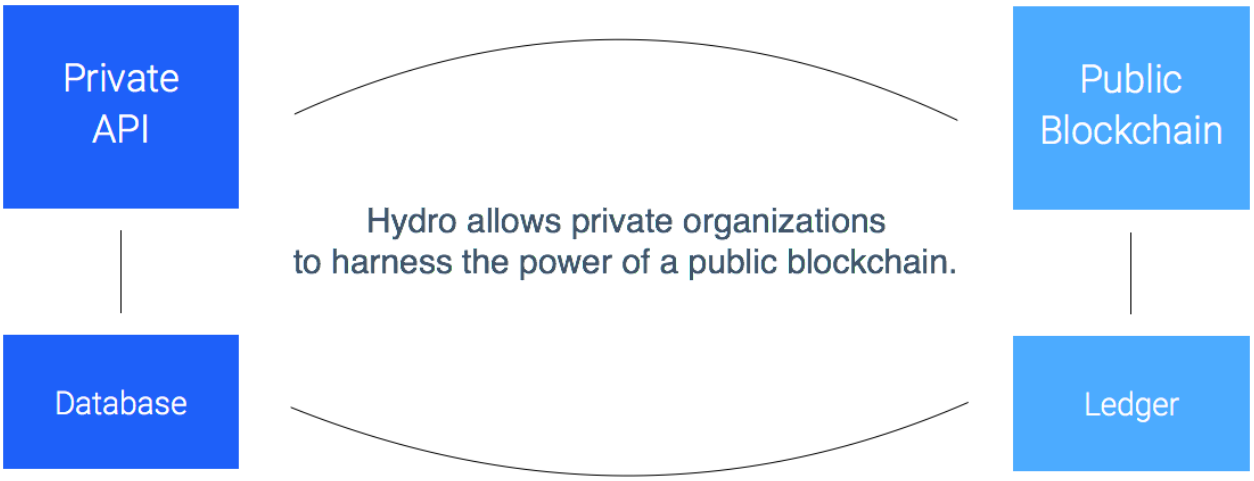
Masina virtuala Ethereum (EVM) este mediul de rulare pentru contracte inteligente pe Ethereum. EVM ajută la prevenirea atacurilor Denial of Service (DoS), asigură menţinerea apatrizilor şi permite comunicarea care nu poate fi întreruptă. Acţiunile pe EVM au costuri asociate cu acestea, numite gaze, care depind de resursele de calcul necesare. Fiecare tranzacţie are o cantitate maximă de gaz alocată acesteia, cunoscută ca o limită g. Dacă gazul consumat de o tranzacţie 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 şi aplicaţii pot fi deseori descrise drept medii ale fluxului de date - ele trimit, prelucrează, stochează, actualizează şi procesează date pentru entităţile cu care interfaţă. Datorită naturii acestor date şi a serviciilor financiare în general, aceste sisteme adesea găzduiesc operaţiuni complexe într-o manieră privată şi centralizată. Reliance pe structuri private, la rândul său, deschide uşa pentru a obţine o varietate de securitate, transparenţă şi câştiguri de eficienţă prin încorporarea forţelor externe care depăşesc acoperirea sistemului intern.

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

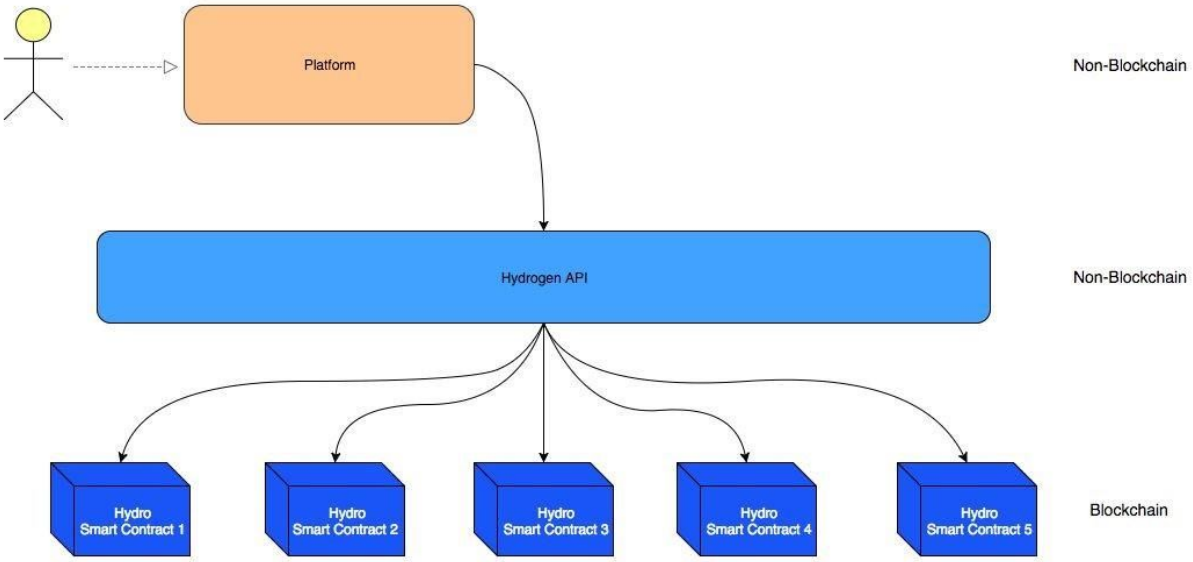


Operaţiile bazate pe blochează pot să apară înainte, în timpul sau după operaţiuni private. Interacţiunea dintre elementele private şi publice poate servi la validarea, ştampilarea, înregistrarea sau îmbunătăţirea proceselor din cadrul unui ecosistem.

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. Deşi acest cadru hibrid nu poate fi aplicabil tuturor platformelor, Hydro se concentrează asupra furnizării de valoare pentru cazurile în care este.

Arhitez pentru adoptare

Hidro diferă de numeroasele iniţiative de blockchain existente, deoarece poate exista independent şi strat în jurul sistemelor noi sau existente fără a necesita schimbări sistemice. În loc să o înlocuiască, Hydro doreşte să se amplifice. Platformele şi instituţiile 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 experienţă, pot găzdui orice număr de servicii proprietare, pot efectua orice operaţiune de date private şi pot fi implementate în orice mediu. Acest lucru este posibil datorită modularităţii structurale a hidrogenului şi este sinergic cu Hydro, care acţionează ca un motor complementar de adopţie.

Raindrop

Construit pe partea de sus a acestei cărţi publice Hyro 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 robusteţe şi utilitate pentru spectrul cazurilor de utilizare care există. Nu este nevoie să concurezi sau să încerci să înlocuişti aceste protocoale - Hydro oferă o modalitate de a le îmbunătăţi prin încorporarea mecanicii blocchain ca o componentă a unei proceduri de autentificare. Acest

lucru poate adăuga un nivel util de securitate pentru a ajuta la atenuarea încălcărilor sistemului şi 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 securităţii financiare

Creşterea vârstei datelor a adus cu ea o creştere a vulnerabilităţii şi acest lucru este deosebit de important pentru serviciile financiare. Platformele financiare sunt adesea gateway-uri către cantităţi mari de date private şi sensibile, cum ar fi numerele de identificare ale guvernului, acreditările contului şi istoricul tranzacţiilor. Din cauza importanţei 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 informaţii cu caracter personal (PII) sunt vândute pe Web Deep pentru doar $ 1, scanări ale documentelor precum paşapoartele sunt disponibile pentru doar 10 $ şi 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 şi mai puţin detectabilă.

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

- Potrivit unui studiu recent realizat de Javelin Strategy & Research - Studiul privind frauda de identitate din 2017 - 16 miliarde de dolari au fost furate de la 15,4 milioane de consumatori din SUA în 2016 din cauza eşecurilor sistemului financiar de a proteja Personally Identifiable Information (PII).

- În aprilie 2017, Symantec a publicat Raportul privind ameninţările la Internet, care estimează că 1,1 miliarde de piese de PII au fost compromise în diferite capacităţi pe parcursul 2016.

- Raportul rapid privind încălcarea datelor de la sfârşitul 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. C VE-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 importanţă? Există o modalitate de a utiliza tehnologia blocchain pentru a securiza informaţiile financiare ale acestor 143 milioane de clienţi, în timp ce încă se bazează pe actualul sistem REST API şi Java?

Adăugarea unui strat Blockchain

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

Mecanismele fundamentale de consens ale reţelei Ethereum asigură valabilitatea tranzacţiei, deoarece participanţii procesează colectiv tranzacţii care sunt semnate în mod corespunzător. Această realitate duce la descentralizare şi 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 operaţiile tranzacţionale pe blocul de blocuri. Un API, de exemplu, poate alege să valideze dezvoltatorii şi aplicaţiile solicitându-i să iniţieze anumite tranzacţii, cu sarcini utile de date, între anumite adrese din blocul de blocuri, ca o condiţie prealabilă pentru lansarea unui protocol standard de autentificare.

Cele Hydro Raindrop

Ploaia conţine 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 şi formă aleatoare. Din acest motiv, nu se poate prezice fiabil natura exactă a ploii. În mod similar, fiecare tranzacţie de autentificare Hydro este unică şi practic imposibilă să apară întâmplător - de aceea îi numim R aindrops.

Platformele de servicii financiare utilizează în mod obişnuit 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 deţine propriul cont, el trebuie să retransmită sumele depuse înapoi la platformă, care apoi sunt validate.

Singurul mod în care utilizatorul poate cunoaşte 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 şi să îl retransmitem, definim o tranzacţie şi utilizatorul trebuie să o execute dintr-un portofel cunoscut. Singurul mod în care utilizatorul poate efectua o tranzacţie valabilă este accesarea portofelului în cauză.

Prin utilizarea Raindrops, atât sistemul, cât şi accesorul pot monitoriza încercările de autorizare pe un registru public imuabil. Această tranzacţie bazată pe blochează este decuplată de la operaţiile de bază ale sistemului, are loc într-o reţea distribuită şi depinde de proprietatea asupra cheilor private. Prin urmare, serveşte ca vector de validare util.

O privire detaliată

Există patru entităţi implicate în procesul de autentificare Hydro:

1. Accessor - Partea care încearcă să acceseze un sistem. În cazul hidrogenului, accesorul este o instituţie sau o aplicaţie 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 şi interfaţa cu blocul de blocuri.
4. Blockchain - registrul public distribuit care procesează tranzacţiile HYDRO şi conţine contractele Hydro smart, prin intermediul cărora informaţiile 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 iniţieze tranzacţia.

2. Receptor - destinaţia tranzacţiei. Aceasta corespunde apelării unei metode într-un contract Hydro smart.

3. ID - Un identificator care este asociat cu sistemul.

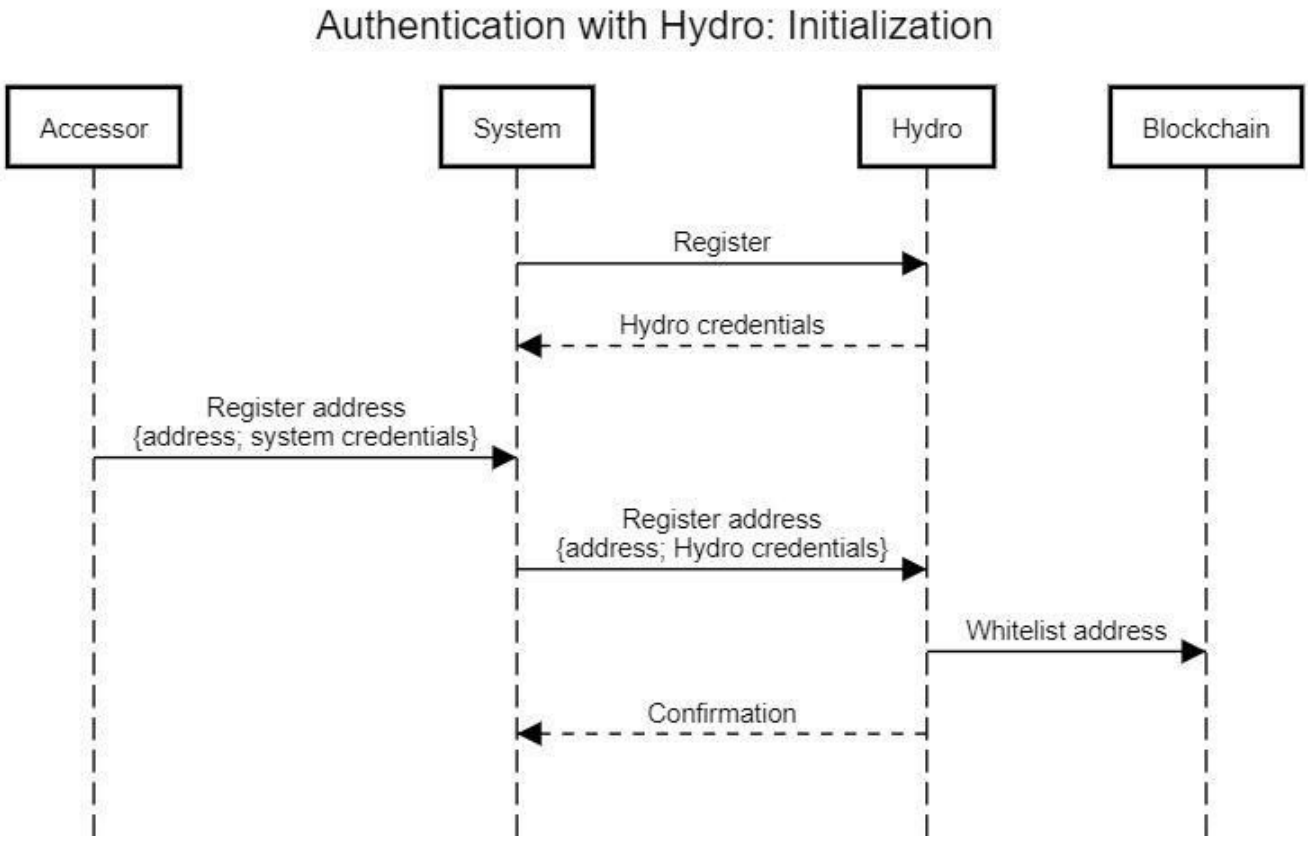
4. Cantitate - Un număr precis de HYDRO pentru a trimite.

5. provocare - Un şir alfanumeric generat aleator.

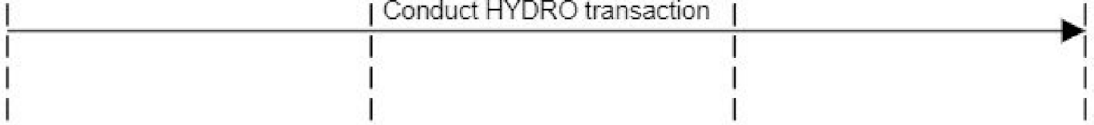
Mai jos este o schiţă a procesului de autentificare, care poate fi în general clasificată în trei etape:

1. *Iniţializarea*
2. *Raindrop*
3. *Validarea*

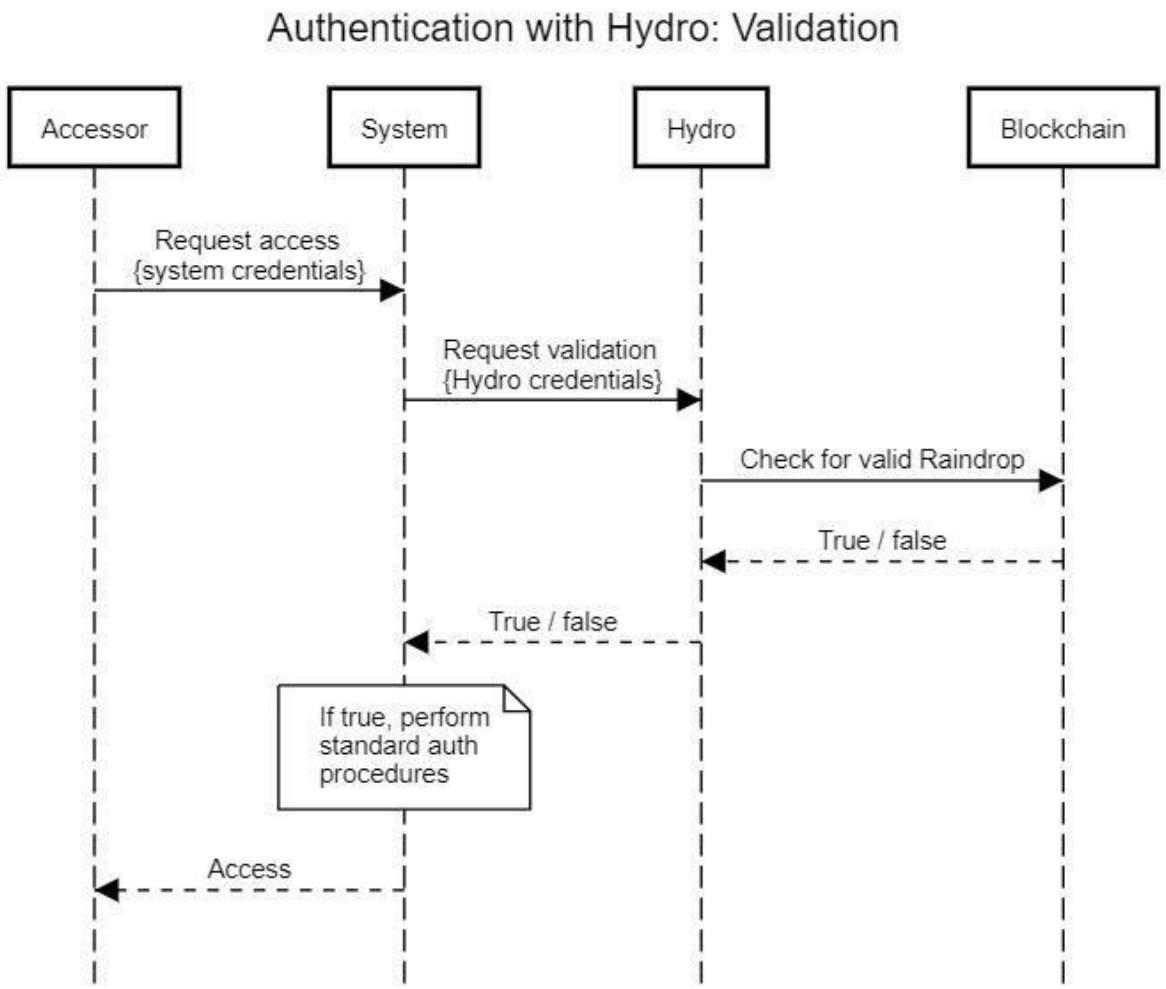
Initializarea începe cu înregistrarea unui sistem (de exemplu, hidrogen)



După terminarea iniţializării, nucleul procesului de autentificare Hydro poate începe. Accessor, care trebuie să execute o tranzacţie 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 immutabile pe blocul de blocuri şi returnează detaliile complete Accesorului prin Sistem. Accesatorul, dotat cu toate informaţiile necesare, efectuează o tranzacţie de la adresa înregistrată la o metodă din contractul Hydro smart. Dacă adresa nu este listată pe listă, acţiunea este respinsă - în caz contrar, aceasta este înregistrată în contractul inteligent. Este important să reţineţi că această tranzacţie 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 Accessorului (pe care numai Accessor ar trebui să o obţină).



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 accesorul a efectuat sau nu o tranzacţie valabilă Raindrop. Hydro interfeţează cu contractul inteligent, verifică validitatea şi 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 şi, dacă este adevărat, sistemul poate acorda acces.



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 uşurinţă utilitatea acestora:

- Vector 1 - Atacatorul fură acreditările de bază ale sistemului Accessor
    1. Atacatorul încearcă să obţină acces la sistem cu acreditări de sistem valide
    - Sistemul verifică cu Hydro pentru a determina dacă o tranzacţie valabilă a fost făcută pe blocul de blocuri
- Hydro returnează false şi sistemul refuză accesul
- Vector 2 - Atacatorul fură cheia privată la portofelul Accessor
    1. Atacatorul încearcă să efectueze o tranzacţie Hydro de la adresa înregistrată, fără a solicita detalii Raindrop
- Atacatorul nu poate efectua o tranzacţie 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 şi cheia privată a portofelului pentru a accesa sistemul. În acest sens, Hydro a adăugat cu succes un factor suplimentar de autentificare.

Deschiderea cele 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 şi sisteme. Pentru că simţim că alţii pot beneficia de acest nivel de verificare, îl deschidem pentru utilizare.

Aşa cum Hidrogenul o va integra ca o condiţie prealabilă pentru accesul la ecosistemul său API, tot aşa orice sistem poate adăuga la procedurile şi protocoalele existente. Orice platformă - fie un API, o aplicaţie, un software pentru întreprinderi, o platformă de jocuri, etc. - poate utiliza Hydro pentru scopuri de autentificare. Documentaţia 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 organizaţii private. API-urile private, bazele de date şi reţelele au creat sisteme complexe de jetoane, chei, aplicaţii şi protocoale în ultimul deceniu, în încercarea de a asigura date sensibile. Google, de exemplu, a devenit unul dintre cei mai cunoscuţi furnizori de produse de pe piaţă cu aplicaţia Google Authenticator. După cum sa menţionat 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 şi transferurile de date sunt criptate şi transmise prin protocolul HTTPS.
4. Partenerii trebuie să încheie o tranzacţie valabilă cu hidro-raindrop de la adresa Hydro înregistrată.

Partenerii trebuie să utilizeze validarea OAuth 2.0. OAuth (autorizaţie deschisă) este un standard deschis pentru autentificarea şi autorizarea bazate pe token. Hidrogenul acceptă "acreditările parolei proprietarului resurselor" şi "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 şi verificat cu fiecare apel API.
6. Jetonul este valabil 24 de ore, după care partenerul trebuie să se valideze din nou.

Dacă oricare dintre aceşti paşi este încălcat, utilizatorul este imediat blocat de accesul API. Un hacker nu poate ocoli aceşti factori de securitate ghicind întâmplător, pentru că există trilioane de combinaţii 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 şi să stocheze cheile private în mai multe locaţii securizate independent de alte acreditări, astfel încât nu există un singur punct de eşec. Un portofel multi-semnătura protejat corespunzător este nu numai dificil de furat, dar natura publică a blocului permite, de asemenea, recunoaşterea 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 abilităţii 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 aplicaţiilor sociale, e-mail şi streaming (care se bazau pe conectivitatea dial-up), este important ca echipa de dezvoltare de bază să urmărească îndeaproape noile evoluţii în vitezele şi volumele tranzacţiei Ethereum. Vă puteţi imagina că YouTube încearcă să lanseze în 1995? Sau Instagram fiind oferit pentru Blackberry?

Dezvoltatorii Core Ethereum, cum ar fi Vitalik Buterin şi 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 şi executate, care este scalabil la o sumă semnificativă de actualizări de stat pe secundă (potenţial miliarde), permiţând blocului să reprezinte o cantitate semnificativă de aplicaţii financiare descentralizate la nivel mondial. Aceste contracte inteligente sunt stimulate să continue să funcţioneze în mod autonom prin taxe de tranzacţionare în reţea, care se bazează, în cele din urmă, pe blocul de blocare (de exemplu, Ethereum) pentru a impune tranziţiile de stat tranzacţionale.**

Alţii, cum ar fi The Raiden Network, au propus o soluţie de scalare în afara lanţului, proiectată să alimenteze tranzacţii mai rapide şi taxe mai mici. În acest moment, Raindrop va pune o presiune foarte minimă asupra cadrului Ethereuem, astfel scalabilitatea este un risc foarte mic pentru succesul tehnologiei.

Concluzie

Imutabilitatea unui blockchain public oferă noi modalităţi 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 îmbunătăţi 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

