Hydro Raindrop

Javna provjera zasnovana na blockchain tehnologiji

Siječanj 2018

Sadržaj

Općenito

Blockchain i Ethereum

- Blockchain temelji
- Merkle stabla
- Pametni ugovori
- Virtualni Ethereum stroj

Poslovna knjiga

- Poslovna knjiga za javne sisteme
- Arhitektura uvajanja

Raindrop

- Stanje financijske sigurnosti
- Equifax prodor
- Dodavanje blockchain sloja
- Hydro Raindrop
- Detaljni osvrt
- Pružanje Raindrop-a javnosti
- Studija slučaja - Raindrop sa OAuth 2.0

Rizici

Zaključak

Općenito

HYDRO: Etimologija - Od starogrčke riječi ὑδρο- (*hudro-*), ὕδωρ (*húdōr*, "voda")

Hydro omogućuje novim i postojećim privatnim sustavima pesprijekornu integraciju i polugu za nepromjenjivu i transparentnu dinamiku javnog blockchaina za povećanja primjenjivostisigurnosti dokumenata, menadžmenta identiteta, prijevoda i umjetne inteligencije.

U ovom izvješću će biti napravljen slučaj za privatne sisteme, kao što su API, da koriste javni Hydro blockchain za povećanje sigurnosti putem javne potvrde.

Predložena tehnologija je nazvana "Raindrop" - transakcija preovedena putem pametnog ugovora koji će ovjeriti javni pristup javnim sustavima i koji će komplementarno postojećim privatnim metodama provjere. Tehnologija je namijenjena da pruži dodatnu sigurnost za povjerljive financijske podatke koji su pod povećanim rizikom od hakiranja i prodora.

Prvotna implementacija Hydro Raindrop-aa je provedena na Hydrogen API platformi. Ovaj modularni set API-a je dostupan globalno poduzećima i developerima za izradu prototipa, izgradnju, testiranje i razvoj sofisticirane financijske platforme i produkata.

Hydro Raindrop će biti dostupan svjetskoj zajednici developera kao open source program kako bi omogućio developerima integraciju Hydrogen Raindrop sa bilokojim ostalim API-ima.

Blockchain i Ethereum

Hydro je implementiran na Ethereum mreži. Prije pružanja više detalja o projektu, veoma je važno razumijeti osnovne ideje o blockchainu i Ethereumu.

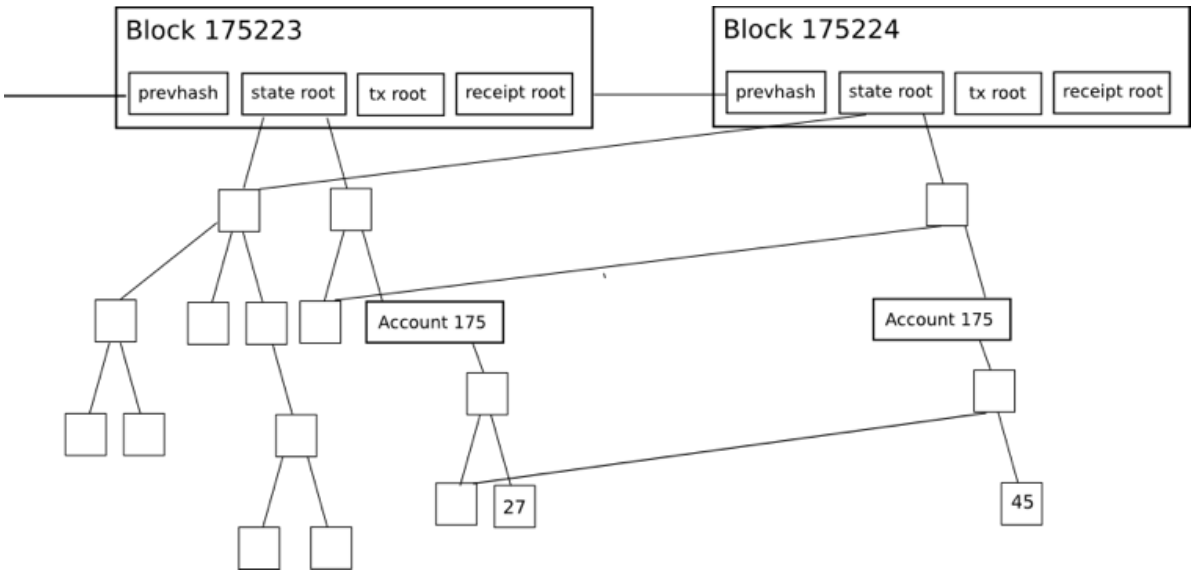
Izgradnja na Ethereumu

Koliko god su aplikacije kao Snapchat izgrađene sa Swift i ostalim ponuđenim alatima na iOS platformi, isto tako i blockchain aplikacije mogu biti izgrađene na temelju Ethereuma. Snap Inc. nije trebao izgraditi iOS negoli ga je iskoristio kao infrastrukturu za pružanje prekretnu aplikaciju za društvene mreže.

Projekt Hydro je u tome sličan. On se zasniva na tisućama developera globalno koji rade na unaprijeđenju blockchain tehnologije čineći je bržom, jačom i više učinkovitom. Hydro konstantno iskorištava to radi unaprijeđenja infrastrukture od developerovih interakcija putem njihovih produkata zasnovanih na blockchain tehnologiji koja pruža vidljive prednosti za financijski orijentiranu primjenu usluga.

Merkele stabla

Merkle stabla su korištena kao efikasna provjera podataka u distribuiranim sustavima. Ona su učinkovita zato što koriste hashove umjesto pune provjere datoteka. Hashovi su načini za enkripciju datoteka koji su mnogo manji negoli datoteka sama. Svako zaglavlje blocka u Ethereumu sadrži tri Merkele stabla za transakcije, potvrde i stanja.



Izvor: Merkling in Ethereum ; Vitalik Buterin, osnivač Ethereuma

Ovo omogućuje malom klijentu za jednostavnu potvrdu odgovora na upite, kao što su:

- Postoji li ovaj račun?
- Koje je trenutačno stanje računa.
- Je li je ova transakcija bila uključena u odeđenom blocku?
- Je li je određeni događaj nastao u ovoj adresi danas?

Pametni ugovori

Ključni koncept, omogućen od Ethereuma i ostalih mreža zasnovanih na blockchainu, su pametni ugovori. Oni su samo izvršujući blokovi koda sa kojim više stranaka može dijelovati isključujući tako potrebu posrednika. Kod u pametnom kontraktu može biti gledan slično kao pravne odredbe u tradicionalnom pisanom ugovoru, ali isto tako može postići šire funkcije. Ugovori mogu imati svoja pravila, uvjete i sankcije, u slučaju ne poštivanja, isto kao i imati ulogu pokretača drugih procesa. Ukoliko pokrenuti, ugovori se izvršavaju kao što je prvotno ugovoreno u trenutku zadavanja na javnom blockchain lancu pružajući tako ugrađene elemente mepromijenjivosti i decentralizacije.

Pametni ugovori su osnovni alat za izgradnju na Ethereum infrastrukturi. Srž funkcionalnosti sloja Hydro blockchaina je ostvarenje putem prilagođenih ugovora kao što će biti kasnije rečeno.

Virtualni ethereum stoj

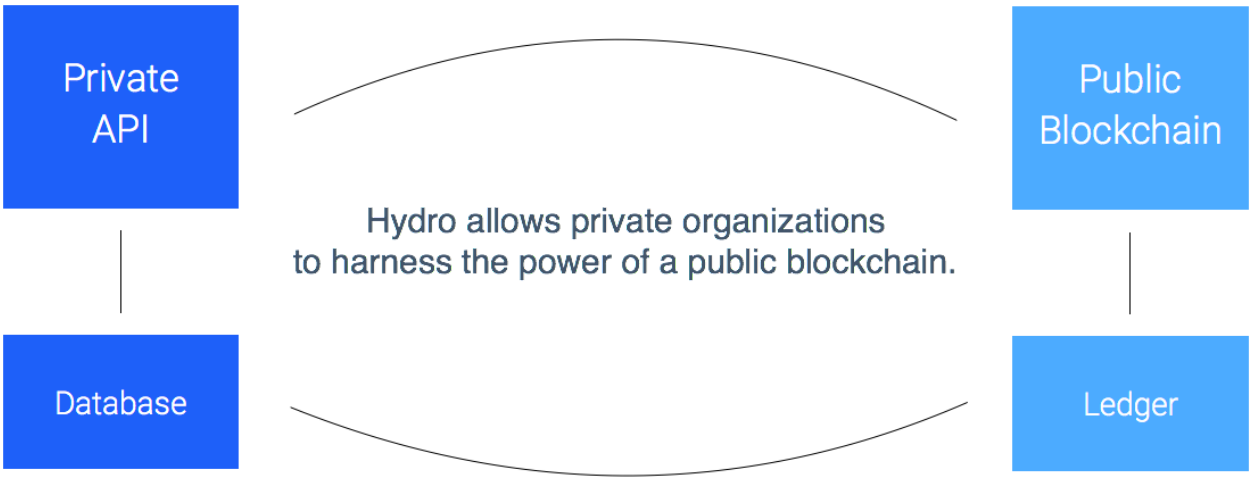
Virtualni Ethereum stroj (EVM) je trenutna okolina za pametne ugovore na Ethereumu. EVM pomaže prevenciji napada uskraćivanjem usluge (DoS), osigurava programima neovisnot od država i omogućuje komunikaciju koja ne može biti prekinuta. Radnje na EVM-u su povezani sa troškovima, nazvanima *gas*, koji ovise o potrebnim računalnim troškovima. Svaka transakcija ima maksimalnu količinu dodijeljenog gas-a zvanu *gas limit*. Ukoliko gas upotrijebljen pri tansakciji dosegne limit, on će prestati sa daljnim procesuiranjem.

Poslovna knjiga

Poslovna knjiga za javne sisteme

Sustavi koji pokreću platforme financijskih usluga, internetske stranice i aplikacije mogu često biti opisane kao sredstva prijenosa podataka - oni šalju, primaju, sahranjuju, ažuriraju i procesuiraju podatke za entitete sa kojima se razmjenjuju. Radi naravi tih podataka, i financijskih usluga općenito, ti sistemu često skladište kompleksne operacije na privatni i centralizirani način. Zavisnost na privatnim strukturama nudi na spektar sigurnosnih, transparentnih i efikasnih potencijalnih dobiti od inkorporiranja vanjskih sila koje premašuju doseg unutrašnjih sistema.

Takav je slučaj sa Hydrogenovom API platformom. Hydro namjerava dosegnuti priješnje navedene dobiti omogućujući Hydrogen korisnicima za razmjenu putem blockchaina na način koji je neprimjetno integriran u temeljni privatni Hydrogen ekosistem.

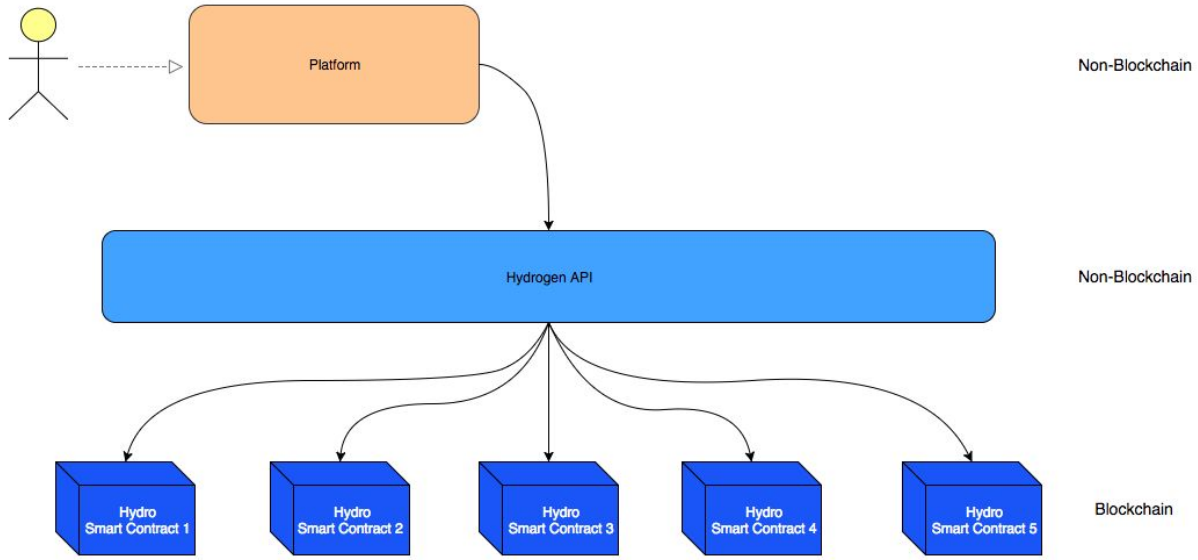


Javne radnje zasnovane na blockchainu se mogu ostvariti prije, tijekom ili nakon privatnih radnji. Uzajamno djelovanje između privatnih i javnih elemenata mogu služiti za potvrdu, obilježavanje, snimanje ili povećavanje procesa unutar ekosistema.

Etos ovoga modela je izrada čvršćih procesa dosezanjem prednosti posebno blockchain tehnologijom gdje je moguće ostvariti pozitivan utjecaj. Dok možda ovaj hibridni okvir nije namijenjen za sve platforme, Hydro se usredotočuje na pružanje trenutnih vrijednosti za slučajeve u kojima se nalazi.

Arhitektura usvajanja

Hydro se razlikuje od mnogih postojećih blockchain pothvata zato što može postojati nezavisno i zajedno djelovati sa već postojećim sustavima bez potrebe za sistemske promjene. Rađe negoli li zamjenjivati, Hydro namjerava usvojiti. Platforme i institucije koje se spoje na Hydrogen API-e mogu automatski pristupiti blockchainu.



Razmjer platforma financijskih usluga koje mogu koristiti Hydrogen je velik. Te platforme mogu pokretati virtualno bilo koje iskustvo, skladištiti bilo koji broj posjedovnih usluga, izvesti bilo koju radnju sa privatnim podacima i razviti u bilo kojem okruženju. To je omogućeno Hydrogenovom strukturnom modularnosti te je sinergično sa Hydro radeči kao komplementarni upravljač za prihvačanje.

Raindrop

Izgrađen na temelju Hydro javne knjige je usluga provjere zasnovana na blockchainu nazvanom "Raindrop". To nudi izrazit, nepromijenjiv i globalno dostupan sloj sigurnosti koji provjerava zahtjev pristupu koji dolazi od autoriziranog izvora.

Privatna provjera protokola kao što je OAuth 2.0 nudi različite stupnjeve snage i korisnosti za spektar postojećih slučajeva upotrebe. Mala je potreba za konkuriranje ili pokušaj za zamjenu tih protokola - Hydro nudi način za njihovo povećanje putem usvajanja blockchain mehanizma kao komponentu procedure provjere. Ovo može dodati korisni sloj sigurnosti kao pomoć protiv prodora u sustav i ugroženost podataka.

Stanje financijske sigurnosti

Razvitkom doba podataka je doprinjelo njihovoj ugroženosti i to je iznimno važno za financijske usluge. Financijske platforme su često prolaz za velike količine privatnih i osjetljivih podataka kao što su državni osobni podaci, uvjerenja računa i povijest transakcija. Radi razmjera važnosti tih podataka, neovlašten pristup je uobičajeno suočen sa katastrofalnim ishodima.

Istraživačka firma Trend Micro je objavila izvješće u kojem je saznato za niz ukradenih Osobno Identificirajućih Informacija (PII) koje se prodaju na crnom tržištu interneta sa najnižim cijenama od $1, preslike dokumenata kao što su pasoši su dostupni već od $10, a podaci za pristup bankovnim računima za od $200 nadalje čineči distribuciju ukradenih podataka uveće dijelomičnim i nepratljivim.

Nažalost postojeći financijski sustav nema pesprijekornu povijest u pogledu prevencije, diagnoze i kominiciranja prodora u baze podataka sa svojim klijentima.

- Prema navodima nedavnog istraživanja od Javelin Strategy & Research - *The 2017 Identity Fraud Study* - $16 milijardi je ukradeno od 15.4 milijuna građana U.S. 2016. zbog nesposobnosti financijskog sustava da zaštiti Osobno Identificirajuće Informacije (PII).

- U travnju 2017., Symantec je objavio svoje izvješće *Internet Security Threat Report*, u kojemu procjenjuje da je oko 1.1 milijardi dijelova PII ugroženo u različitim razmjerima tokom 2016.

- U godišnjem osvrtu od Risk Based Security *2016 Year End Data Breach Quickview*, je ustanovljeno da je 4,149 ugroženih podataka nastalio u poduzećima globalno 2016., izlažući preko 4.2 milijarde zapisnika.

- U izvješću globalnih IT stručnjaka u stručnim uslužnim djelatnostima *2017 Thales Data Threat Report – Financial Services Edition*, saznato je da je 49% od organizatora financijskih usluga bilo žrtva sigurnosnih prodora u prošlosti, 78% provodi više vremena radi na boljoj zaštiti sebe, ali 73% je krenulo u novu inicijativu povezanu sa AI, IoT i cloud tehnologijama prije pripreme adekvatnog sigurnosnog rješenja.

Equifax prodor

29. srpanja 2017, Equifax, 118 godina stara U.S. agencija za kreditno izvješćivanje je hakirana. 143 milijuna klijenata je bila PII izložena, uključujući brojevi socijalnog osiguranja. 209,000 klijenata je ugroženo u pogledu podataka kreditnih kartica.

Što je bio razlog ovog prodora?

Sve je počelo sa jednom prijašnjom tehnologijom korištenom od Equifaxa. Struts je open source okvir za razvijajuće web aplikacije u Java programskom jeziku napravljenog od Apache Software Foundation. CVE-2017-9805 jesigurnosni propust u Apache Struts povezano sa korištenjem Struts REST priključka sa XStream handler to handle XML nosivosti. Ukoliko iskorišten, omogućuje daljinskom neautoriziranom napadaču da pokrene maliciozni kod na aplikacijskom serveru da ili preuzme stroj ili da pokrene buduće napade sa njega. Taj sigurnosni propust je uklonjen dva mjeseca prije Equifax prodora.

Apache Struts sadrži manu u REST Plugin XStream koja je pokrenuta kada se program nesigurno deserializira unos od korisnika u XML zahtjevu. Posebno se problem pojavljuje u XStreamHandler toObject() metodi, koja ne sadrži bilo koja ograničenja od zaprimajuće vrijednosti kada se koristi XStream deserializacija kao objekt, rezultirajući arbitrarnim izvršenjem koda kod propusta.

Iako je ostatak REST priključka ugroženo, je li je to važno? Postoji li način da se koristi blockchain tehnologija da se osiguraju financijske informacije tih 143 milijuna klijenata sve dok se zaslanja na sadašnji REST API i Java baziranom sustavu?

Dodavanje blockchain sloja

Jasno je da se integritet prolaza financijskih podataka može poboljšati. Proučimo kako se može dodati dodatni sloj sigurnosti pomoću Hydro.

Temeljni suglasni mehanizam Ethereum mreže osigurava transakcijsu potvrdu zato što učesnici kolektivno procesuiraju transakcije koje su pravilno potpisane. Ta realnost dovodi do decentralizacije i nepromijenjivosti, ali najvažnije je što pridonosi vektor za smanjenje neautoriziranog pristupa prolazu koji kontrolira osjetljive podatke.

Sa hydro, autorizacija se može predvidjeti pri transakcijskom postupku na blockchainu. Na API-u se na primjer može odrediti validacija developera i aplikacija zahtjevajući od njih da pokrenu dotičnu transakciju sa pojedinim podatkovnom nosivosti između pojedinih adresa na blockchainu kao preduvjet koji pokreće standardni provjeravajući protokol.

Hydro Raindrop

Kiša sadrži pakete kondenzirane vode razmjera od 0.001 do 0.005 centimetra u promjeru. Tijekom obične kiše, tu su milijarde i milijarde tih paketa, svaki različite veličine, brzine i oblika. Zbog toga je nemoguće pouzdano predvidjeti točnu prirodu kiše. Slično, svaka Hydro provjera transakcije je jedinstvena i virtualno nemoguće da se dogodi slučajno - zato ih nazivamo Raindrops.

Platforme za financijske usluge često koriste mikro uplate kao provjere da potvrde klijentove račune. Taj je koncept jednostavan: platforma napravi malu uplatu nasumičnog iznosa na račun korisnika. Kako bi korisnik uistinu dokazao da je vlasnik dotičnog računa, korisnik mora poslati natrag uplaćeni iznos na platformu što je onda provjereno. Jedini način da korisnik zna točni iznos (osim nagađanja) je da pristupi svojemu bankovnom računu.

Raindrop bazirana provjera sa Hydro je analogna. Rađe negoli li da korisnik šalje natrag uplaćeni iznos, mi definiramo transakciju, a korisnik ju mora izvršiti iz već znanog novčanika. Jedini način da korisnik potvrdi transakciju je da pristupi novčaniku koji je u pitanju.

Pri korištenju Raindropa i sustav i pristupnik mogu pratiti autorizacijske pokušaje na nepromijenjivu javnu glavnu knjigu. Ova transakcija zasnovana na blockchainu je odvojena od osnovnih sustavnih radnji, odvija se na distribuiranoj mreži i ovisi o vlasništvu privatnih ključeva. Stoga služži kao korisni vektor potvrde.

Detaljni osvrt

Postoje četiri entiteta uključena u proces Hydro provjere:

1. *Pristupnik* - Stranka koja pokušava pristupiti sustavu. U slučaju korištenja Hydrogena, pristupnik je financijska institucija ili aplikacija koja koristi Hydrogenove API-e za svoju jezgru digitalne infrastrukture.
2. *Sustav* - Sustav ili prolaz koji je korišten od Pristupnika. Za Hydrogen je sustav sam Hydrogen API.
3. *Hydro* - Modul koji koristi sustav za komunikaciju i sučelje sa blockchainom.
4. *Blockchain* - Distribuirana javna glavna knjiga koja procesuira HYDRO transakcije i sadrži Hydro pametne ugovore putem kojih se informacije mogu slati, primati ili drugačije koristiti.

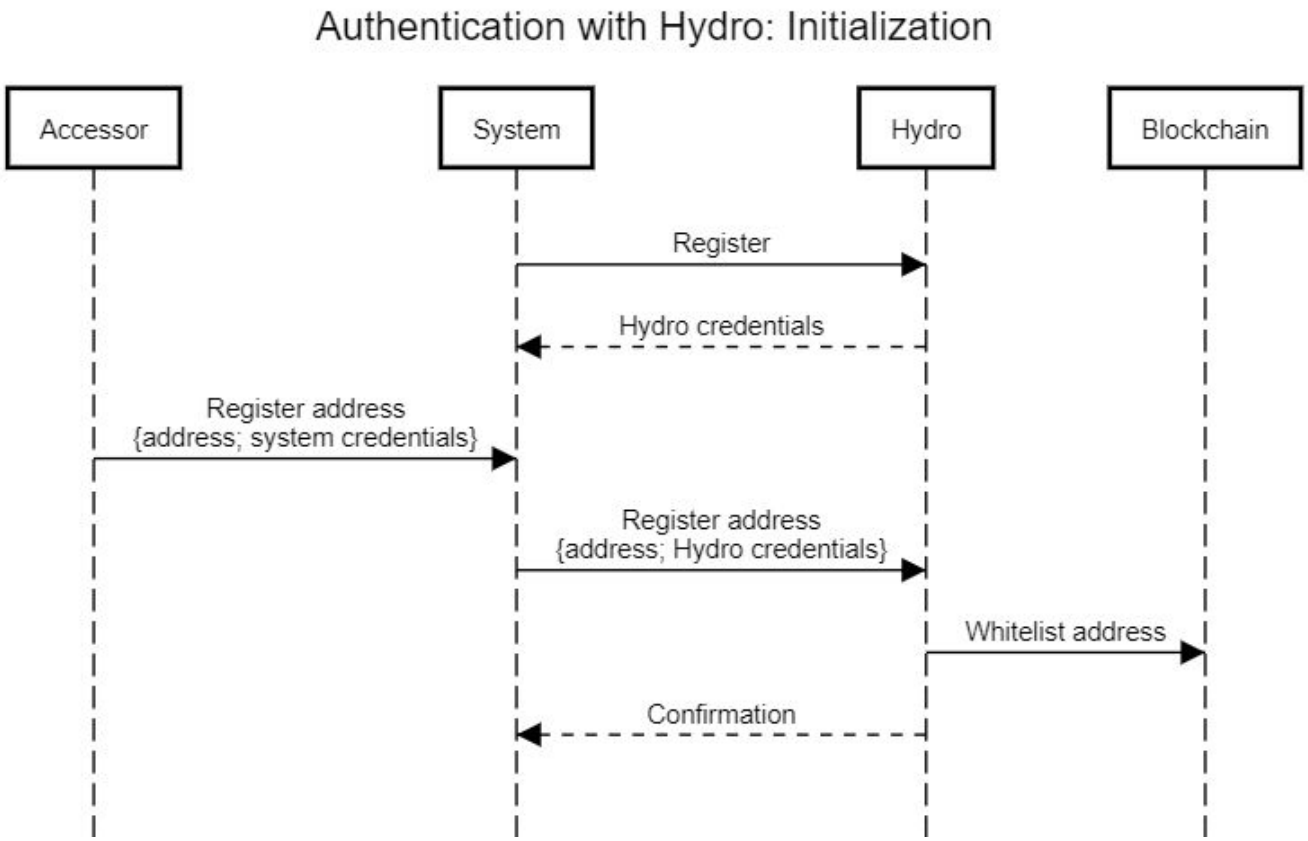
Svaki Raindrop, u svojoj cjelosti, je set od pet transakcijskih parametara:

1. *Pošiljatelj* - Adresa koja mora pokrenuti transakciju.
2. *Primatelj* - Odredište transakcije. To korenspondira sa nazivanjem metode u Hydru pametnim ugovorom.
3. *ID* - Prepoznavatelj koji je povezan sa sustavom.
4. Kvantiteta - Precizan broj HYDRO-a koji se šalje.
5. Izazov - Nasumično generiran alfanumerički niz

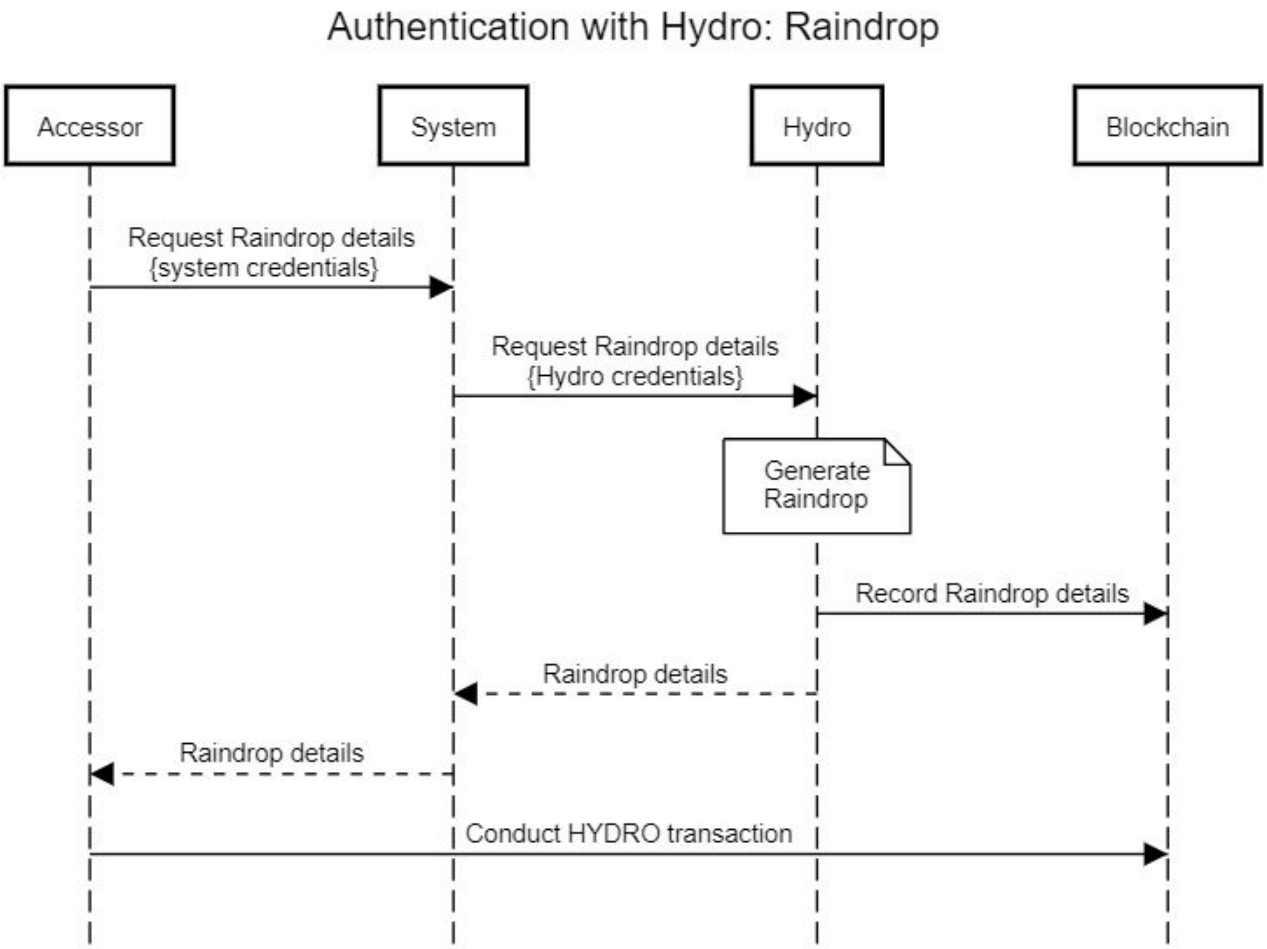
Ispod je okvir procesa provjere koji može biti općenito svrstan u tri razine:

1. Pokretanje
2. Raindrop
3. Provjera

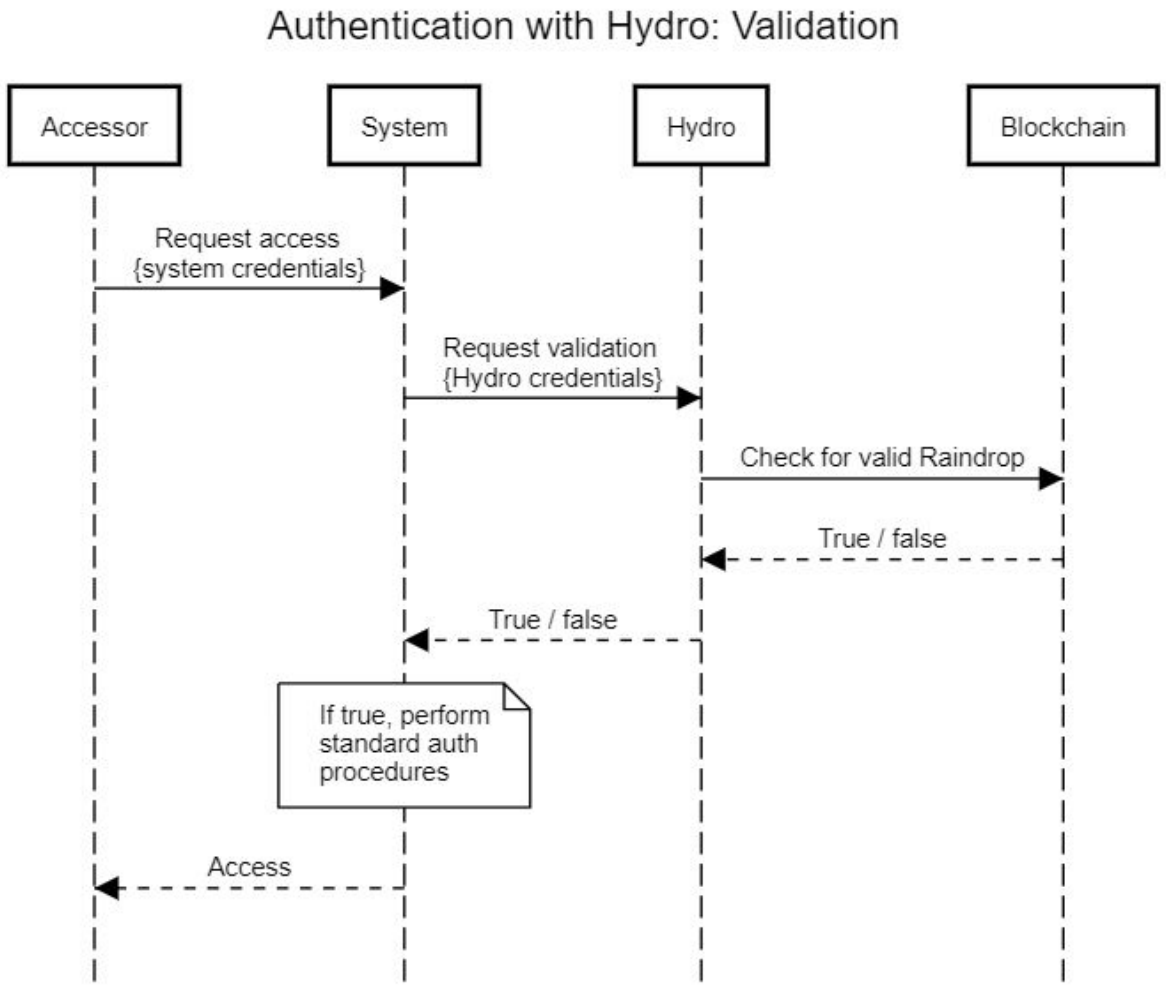
Provjera započinje sa sustavom (npr. Hydrogen) koji se registrira za uporabu Hydro-a i dobivanja akreditiva omogućujući sustavu da komunicira sa blockchainom putem Hydro modula. Sustav uključuje pristupnika (npr. financijsku instituciju) koji se registrira kao javna adresa i time prenosi registriranu adresu Hydro-u. Ta adresa je nepromijenjivo zapisana na blockchainu na popis dopuštenih koji je pohranjen u Hydro pametnom ugovoru. Sustav dobiva potvrdu da je adresa na popisu dopuštenih te se ujedno može potvrditi kao javno vidljivi događaj. Sustav registracije se mora odviti samo jednom dok se pristupnik mora staviti na popis dopuštenih jednom po svakom pristupniku.



Nakon što je pokretanje završeno, jezgra Hydro procesa provjere može započeti. Pristupnik, koji mora izvršiti Raindrop trnsakciju, započinje proces zhtjevajući Raindrop detalje od sustava, a sustav preusmjerava zahtjev Hydro-u. Hydro generira novi Raindrop, skladišti određene detalje nepromijenivo na blockchainu a vraća sve detalje pristupniku putem sustava. Pristupnik, opremljen sa svim detaljima, provodi transakciju sa registrirane adrese putem metode na hydro pametnom ugovoru. Ukoliko adresa nije na popisu dopuštenih, postupak je prekinut - u suprotnom, on je zabilježen u pametnom ugovoru. Važno je naglasiti da se ta transakcija treba odviti izvan sustava, izravno od pristupnika na blockchain zato što mora biti potpisana sa pristupnikovim privatnim ključem (koji samo pristupnik može nabaviti).



Posljednji korak procesa je provjera. U ovom koraku, pristupnik službeno zahtjeva pristup sustavu putem mehanizma uspostavljenog od sustava. Prije ugradnje bilo kojih od standardnih protokola provjere, sustav pita Hydro je li pristupnik proveo valjanu Raindrop transakciju. Hydro koristi sučelje sa pametnim ugovorom, provjerava valjanost i odgovara sa idtinito/neistinito odgovorom. Sustav je u mogućnosti odlučiti kako da nastavi na temelju toga odgovora - ukoliko nije istinito, sustav može zabraniti pristup, a ukoliko je istinito, sustav može dopustiti pristup.



Ukoliko uzmemo u obzir temelj sustavnih akreditiva - ili bilo kojih postojećih sustavnih protokola koji su u uporabi - kako bi bio jedan faktor provjere, važno je da Hydro sloj pruža korisni sekundarni faktor. Pri proučavanju dva primarna napadna vektora, mi možemo spremno potvrditi njihovu korisnost:

- Vektor 1 - Napadač ukrade pristupnikovu akreditaciju temeljnog sustava
    - Napadač pokušava dobiti pristup sustavu sa valjanum sustavnim akreditacijama
    - Sustav provjerava sa Hydro-m da odluči je li je valjana transakcija napravljena na blockchainu
    - Hydro odgovori neistinito i sustav zabrani pristup
- Vektor 2 - Napadač ukrade privatni ključ(eve) pristupnikova novčanika
    - Napadač pokušava izvršiti Hydro transakciju sa registrirane adrese bez pribavljenih Raindrop detalja
    - Napadač ne može izvršiti valjanu blockchain transakciju

- Napadač ujedno ne može zatražiti pristup sustavu bez valjane akreditacije sustava

Izvidno je da napadač mora ukrasti akreditaciju temeljnog sustava i pristupnikov privatni ključ(eve) novčanika kako bi pristupio sustavu. U ovom slučaju Hydro je uspješno dodao dodatni faktor provjere

Pružanje Raindropa javnost

Dok je ova usluga provjere zasnovana na blockchainu stvorena kako bi osigurala Hydrogenov API ekosistem, široko je dostupna različitim platformama i sustavima. Zato što smo sigurni da će drugima moguće koristiti ovaj sloj provjere, mi ga dajemo na uporabu.

Kao što će Hydrogen integrirati ga kao preduvjet za pristup njezinom API ekosistemu, tako će ga bilo koji sustav moći dodati postojećim procedurama i protokolima. Bilo koja platforma - bilo ona API, aplikacija, programsko poduzeće, platforma za igranje etc. -može koristiti Hydro za namjeru provjere, Formalna dokumentacija će biti dostupna na GitHub-u za sve one koji žele inkorporirati ovaj blockchain sloj u sučelje provjere ili REST API.

Studija slučaja - Raindrop sa OAuth 2.0

Postoji tucet načina za primjenu Raindrop-a od privatnih organizacija. Privatni API-ovi, baze podataka i mreže su stvorile složen sustav tokena, ključeva, aplikacija i protokola tokom posljednjeg desetljeća u pokušaju da zaštite osjetljive podatke. Google,kao primjer, je postao kao jedan od najpopularnijih pružatelja produkta na tržištu sa svojom Google Authenicator aplikacijom. Kao što je napomenuto prije, malo je pa skoro i nema razloga za konkurenciju ili zamjenu postojećih protokola.

Kao studija slučaja, ovdje je sažeti osvrt kako Hydrogen primjenjuje Hydro provjeru kao sloj zaštite u svojem sveukupnom API sigurnonom sučelju:

1. Hydrogen API partneri moraju prvotno imati IP adrese od svojih raznih okolina kojima je dopušten pristup.
2. Partneri moraju zatražiti zahtjev da njihova Hydro adresa bud na popisu dopuštenih.
3. Svi pozivi prema Hydrogen API-ima i prijenosu podataka su enkriptirani i poslani preko HTTPS protokola.
4. Partneri moraju izvršiti valjan Hydro Raindrop transakciju sa registrirane Hydro adrese.
5. Partneri moraju koristiti OAuth 2.0 provjeru. OAuth (Open Authorization) je otvoreni standard za provjeru i autorizaciju baziranu na tokenima. Hydrogen podržava tipove dozvola kao što su "Resource Owner Password Credentials" i "Client Credentials" i svaki API korisnik mora pružiti akreditaciju za autoriziran zahtjev.

6. Ukoliko ni jedan od pet elemenata nisu iskorištena onda je Hydrogen partnerima dodijeljen jedinstveni token koji je provjeren i potvrđen sa svakim API pozivom.
7. Token je valjan 24 sata nakon čega se partner mora iddentificirati.

Ukoliko je bilo koji od koraka iskorišten, korisniku je odmah zabranjen pristup API-u. Haker ne može zaobići te faktore sigurnosti nasumično pogađajući zato pto postoji preko bilijun jedinstvenih kombinacija.

Hydro provjera temeljena na blockchainu je važna komponenta Hydrogen sigurnosnog protokola. Hydrogenov tim podržava pratnere da uspostave višestruko potpisane novčanike te da čuvaju privatne ključave na više sigurnosnih lokacija neovisno od ostalih akreditacija tako da ne postoji jedinstvena točka prodora. Sigurno čuvan i višestruko potpisan novčanik nije samo teško za ukrasti negoli je prirodna narav blockchaina za brzo identificiranje kradljivca jer ga povezuje sa sigurnosti API-a.

Svatko može vidjeti pokušaj provjere Hydro pametnog ugovora što znači da su dani, kada su platforme bile sigurnosno ugrožene mjesecima, pri kraju. API hakeri sada mogu biti suočeni sa bržom reakcijom zato što je sposobnost za otkrivanje nedozvoljene autorizacije u pravom vremenu, od bilokud na svijetu.

Rizici

Kao i svaka početna tehnologija, kao što su to bili prvi dani društvenih mreža,emaila i aplikacija za streaming (koje su bile zavisne na dial-up povezanosti), važno je da jezgra development tima brižno prati nove razvoje u Ethereum transakcijskim brzinama i volumenu. Možete li zamisliti pokušaj osnivanja YouTube 1995.? Ili da Instagram prvi stupio na tržište negoli Blackberry?

Jezgra Ethereum developera kao što su Vitalik Buterin i Joseph Poon su predložili Plasma: Scalable Autonomous Smart Contracts nadogradnju za Ethereum protokol:

> **Plasma je predloženo sučelje ua poticajuče i prisilno izvršenje pametnih ugovora što je proporcionalno uvelikoj količini ažuriranja stanja po sekundi (potencijalno milijarde) omogučujući blockchainu da bude predstavnik velikoj količini decentraliziranih aplikacija diljem svijeta. Ti pametni ugovori potiču za nastavak autonomnih radnji putem mrežnih transakcijskih naknada, što je u konačnici zavisno o temeljnom blockchainu(npr. Ethereum) za prisilnom transakcijsskom stanju tranzicije.**

Ostali, kao što je The Raiden Network, su predložili rješenje mjerenja izvan lanca radi bržih transakcija i nižih naknada. U ovom trenutku, Raindrop će biti minimalni teren na Etherum sučelju, tako da je mjerenje veoma mali rizik za uspjeh tehnologije.

Zaključak

Nepromijenjivost javnog blockchaina pruža nove načine povećanja sigurnosti za javne sustave kao što su API.

Ovo izvješće je dokazalo tri važne stvari:

1. Javni blockchaini mogu dodati vrijednost financijskim uslugama.
2. Hydro Raindrop može povećati sigurnost u privatnim sustavima.
3. Postoje trenutne aplikacije za Hydro Raindrop unutar Hydro API platforme.

Hydro tim vjeruje da će buduće sučelje biti standard sigurnosti infrastrukture za novi model hibridnog privatno-javnog sustava koji će doprinjeti svim klijentima u industriji financijskih usluga i dalje.

Izvori:

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