(Nederlands/Dutch)

Hydro Raindrop
Public Authentication On The Blockchain

Februari 2018

Inhoudsopgave

Samenvatting

HYDRO: Afgeleid van het Griekse woord ὑδρο- (*hudro-*), ὕδωρ (*húdōr*, "water")

Hydro stelt de gelegenheid om nieuwe en bestaande privésystemen naadloos te integreren en het beïnvloeden van een onveranderlijke en transparante dynamiek van de openbare blockchain met als doel de applicatie- en documentbeveiliging, identiteitsbeheer, transacties en kunstmatige intelligentie te verbeteren.

In dit document wordt een case gemaakt met betrekking tot private systemen, zoals APIs, om de beveiliging te verbeteren met de publieke Hydro blockchain via openbare authenticatie.

De bedachte technologie wordt de "Raindrop" genoemd - een transactie uitgevoerd door een smart contract welk publieke systeemtoegang publiekelijk valideert en bestaande privé authenticatie methoden kan aanvullen.
De technologie is bedoeld als aanvullende beveiliging voor gevoelige financiële gegevens welk een verhoogd risico lopen door hacking en andere inbreuken.

Initiële implementatie van de Hydro Raindrop zal worden uitgevoerd op het Hydrogen API Platform. Deze modulaire set van API's is overal ter wereld beschikbaar voor bedrijven en ontwikkelaars, om te bouwen, testen en uit te rollen van geavanceerde financiële techologie platforms en -producten.

De Hydro Raindrop zal beschikbaar worden gesteld aan de ontwikkelaars community als een open source software, zodat ontwikkelaars de Hydro Raindrop kunnen integreren met elk andere REST API.

Blockchain & Ethereum

Hydro is geïmplementeerd op het Ethereum netwerk. Het is belangrijk om enkele fundamentele ideeën over de blockchain technologie en Ethereum te begrijpen, alvorens er meer in detail wordt getreden over het project.

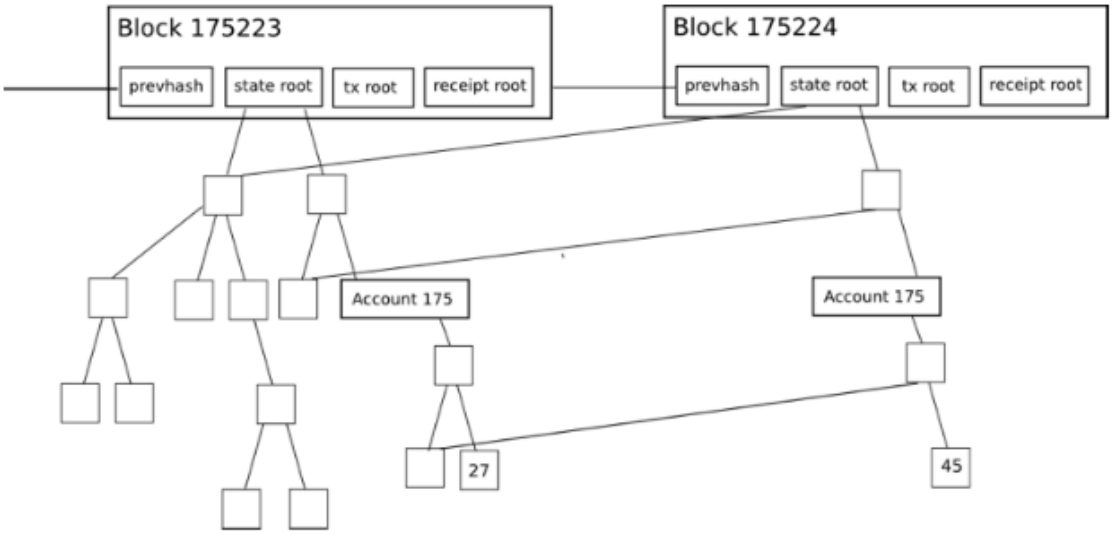
Bouwen op Ethereum

Veel apps zoals Snapchat zijn gebouwd met Swift en andere tools bovenop het Apple iOS platform, hetzelfde kan worden gebouwd met blockchain applicaties bovenop Ethereum.
Snap Inc. hoefde iOS niet te bouwen, maar het is gebruikt als infrastructuur om een game-changing social media applicatie te lancheren.

Het project Hydro is vergelijkbaar. Het is afhankelijk van duizenden projectontwikkelaars welke werken om de onderliggende blockchain technologie sneller, sterker en efficiënter te maken. Hydro maakt gebruik van deze constante verbeterende infrastructuur door het ontwikkelen van productgerichte integraties rondom de blockchain technologie welke tastbare voordelen kan bieden voor de financiële services.

Merkle Trees

Merkle trees worden gebruikt in gedistribueerde systemen voor efficiënte data verificatie.
De efficiëntie vloeit voort uit het gebruik van hashes in plaats van volledige files. Hashes zijn manieren van het coderen van bestanden en welk vele malen kleiner zijn dan het orginele bestand. Elke block header in Ethereum bestaat uit drie Merkle Trees for transacties, ontvangsten en states:



Source: Merkling in Ethereum; Vitalik Buterin, Ethereum Founder

Dit maakt het makkelijk voor een kleinere cliënt om geverifieerde antwoorden op vragen te krijgen, bijvoorbeeld:

- Bestaat dit account?
- Wat is het huidige saldo?
- Is deze transactie opgenomen in een bepaald blok?
- Heeft er een bepaalde gebeurtenis plaats gevonden op dit adres vandaag?

Smart Contracts

Een sleutelconcept mogelijk gemaakt door het Ethereum - en andere blockchain gebaseerde netwerken, genaamd smart contracts. Dit zijn zelf uitvoerbare codeblokken waar meerdere partijen interactie mee kunnen uitvoeren, waardoor er geen tussenpersonen meer nodig zijn. De code in een smart contract kunnen worden gezien als de wettelijke clausules in een traditioneel papieren contract, maar kan ook veel uitgebreider functioneren. Contracten kunnen regels, voorwaarden, boetes voor ingebrekestelling of kunnen andere processen in werking zetten. Wanneer ze worden geactiveerd, worden de contracten uitgevoerd zoals origineel staat omschreven op het moment van implementatie op de openbare keten, waarbij ingebouwde elementen zijn verwerk van onveranderlijkheid en decentralisatie.

Ethereum Virtuale Machine

De Ethereum Virtuale Machine (EVM) is de omgeving voor smart contracts op het Ethereum netwerk. De EVM helpt Denial of Service-aanvallen (DoS) te voorkomen, zorgt dat programma’s stateloos blijven, en maakt het mogelijk om communicatie niet te laten verstoren. Acties op het EVM brengen kosten met zich mee, het zogenoemde Gas, welk afhangen van de benodigde computerresourches. Elke transactie heeft een maximale hoeveelheid gas toegewezen, het zogenoemde Gas Limit. Als het verbruikte Gas tijdens de transactie de limiet bereikt, dan stopt het met de verwerking.

Public Ledger

Een Public Ledger voor Private Systemen

De systemen welk de drijfkracht verschaffen achter financiële dienstplatformen, websites en applicaties, kunnen vaak worden omschreven als mediums van informatiestromen - ze verzenden, ontvangen, opslaan, updaten en verwerken informatie voor de entiteiten waarmee ze communiceren. Vanwege de aard van deze data, en van financiële diensten in het algemeen, bevatten deze vaak complexe operaties in een private en gecentraliseerde manier. Vertrouwen op privéstructuren opent op zijn beurt deuren voor verschillende veiligheids-, transparantie - en efficiëntiewinsten door het incorporeren van externe krachten die het bereik van het interne systeem overschrijden.

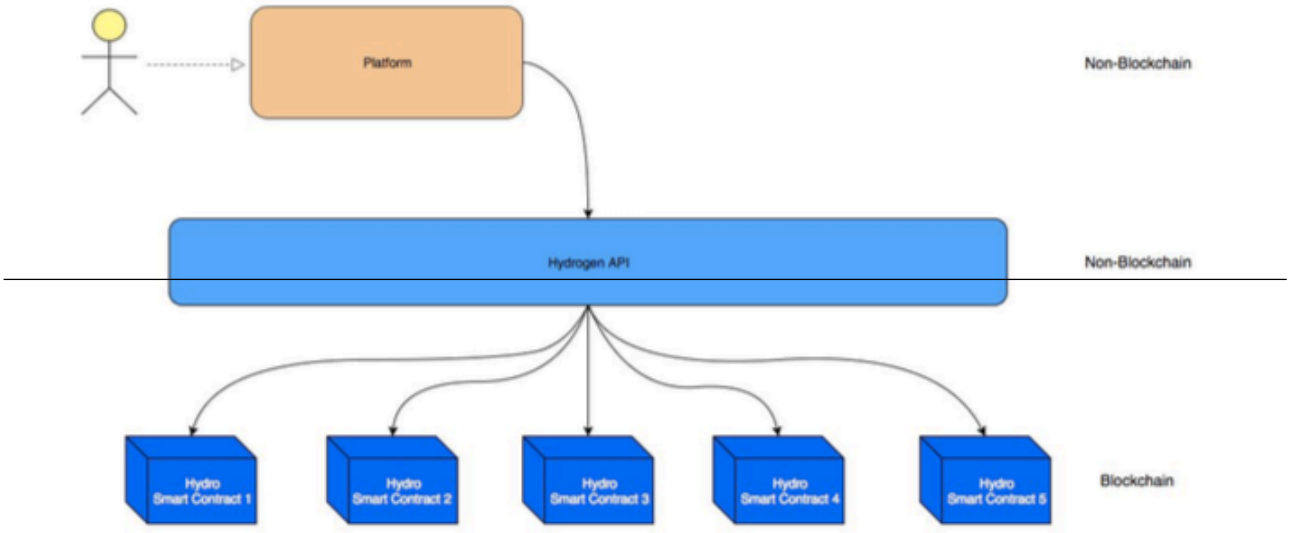
Dit is het geval met het Hydrogen's API platform. Hydro richt zich op het benutten van de bovengenoemde voordelen door Hydrogen-gebruikers te laten communiceren met een blockchain op manieren die naadloos worden geïntegreerd in het fundamentele private Hydrogen-ecosysteem.

Publiekelijke blockchain-gebaseerde operaties kunnen plaatsvinden voor, tijdens of na privé-operaties. Het samenspel tussen private en openbare elementen kunnen dienen om processen te valideren, te bestempelen, vast te leggen of te verbeteren binnen een ecosysteem.

De ethos van dit model is het robuuster maken van processen door het gebruiken van de voordelen van blockchain-technologie, en specifiek waar het de meest positieve impact kan hebben. Hoewel dit hybride framework mogelijk niet toepasbaar is op alle platforms, richt Hydro zich op het bieden van waarde voor de casus waarin dit wel het geval is.

Ontwerpen voor Adoptie

Hydro onderscheidt zich voor vele bestaande blockchain-projecten, omdat het onafhankelijk kan bestaan en er gelaagd kan worden rond nieuwe of bestaande systemen zonder dat er systematische veranderingen vereist zijn. In plaats van vervangen, streeft Hydro naar verbetering. Platforms en instellingen welk zich aansluiten op de Hydrogen API's krijgen automatisch toegang tot de blockchain.



De reikwijdte van platforms betreffende financiële diensten welk gebruik maken van Hydrogen is zeer breed. Deze platforms kunnen vrijwel een onbeperkt aantal eigen services huisvesten, het uitvoeren van elke private data operaties en in elke omgeving uitrollen. Hydrogen's structurele modulariteit maakt dit mogelijk en is synergetisch met Hydro, welk fungeert als een aanvullende stimulans ten behoeve van adoptie.

Raindrop

Bovenop de Hydro public ledger is een op blockchain gebaseerde authenticatie service gebouwd, genaamd de "Raindrop". Deze service biedt een duidelijke, onveranderlijke en een wereldwijd zichtbare beveiligingslaag welk controleert of een toegangsverzoek afkomstig is van een geautoriseerde bron.

Private authentificatieprotocollen zoals OAuth 2.0 bieden verschillende robuustheidniveaus en een bepaalde bruikbaarheid binnen het bestaande gebruikersspectrum. Er is weinig noodzaak om te concurreren met of het vervangen van deze protocollen - Hydro biedt een manier om deze te verbeteren door incorporatie van de blockchain mechanica binnen de authenticatie procedures. Dit kan een bruikbare beveiligingslaag toevoegen om systeeminbreuken en data compromissen tegen te gaan.

Voordat we dieper ingaan op de technische aspecten van Raindrop, gaan we eerst naar het probleem kijken wat we proberen op te lossen.

De Staat of Financiële zekerheid

De opkomst van het data tijdperk heeft een zekere toename van kwetsbaarheid met zich meegebracht, en dit is voornamelijk belangrijk voor financiële diensten. Financiële platforms zijn vaak toegangswegen tot grote hoeveelheden privé- en gevoelige data zoals ID-nummers, accountgegevens en transactiehistorie. Omdat deze gegevens vaak een dermate hoeveelheid gevoelige informatie bevatten, wordt er met ongerechtvaardigde toegang een mogelijk catastrofale resultaat bereikt.

Het onderzoeksbureau Trend Micro publiceerde een rapport waarins stond dat gestolen regelitems met Persoonlijk Identificeerbare Informatie (PII). Op het Deep Web worden scans van documenten verkocht voor $1,-, paspoorten voor een bedrag van slechts $10,- en inloggegevens van de bank voor slechts $200,-. Hierdoor is de distributie van gestolen data steeds meer gefragmenteerd en ontraceerbaarder.

Helaas heeft het bestaande financiële systeem geen vlekkeloze historie als het gaat om het voorkomen, diagnosticeren en communiceren van datalekken met zijn aandeelhouders.

> ➢ Volgens een recente studie door Javelin Strategy & Research - *The 2017 Identity Fraud Study* - In 2016 is er $16 miljard gestolen van 15.4 miljoen Amerikaanse klanten vanwege het falen om PPI te beveiligen binnen het financiële systeem.

➢ In April 2017, Symantec publiceerde het *Internet Security Threat Report* , waar in 2016 volgens schatting 1,1 miljard PPI in verschillende hoedanigheid is aangetast.

➢ De *2016 Year End Data Breach Quickview*,door Risk Based Security, constateerde dat er wereldwijd in het bedrijfsleven 4149 datalekken plaats vonden, met meer dan 4,2 miljard files.

➢ De *2017 Thales Data Threat Report – Financial Services Edition* , onderzocht wereldwijd IT-professionals in de dienstverlening sector, waaruit bleek dat 49% van de financiële dienstverleningsorganisaties gekampt heeft met een inbreuk op de beveiliging, waarbij 78% meer uitgeeft om zichzelf te beschermen, en 73% passende beveiligings-oplossingen lanceert omtrent passende nieuwe initiatieven gerelateerd tot AI, IoT en cloudtechnologieën.

Equifax Breach

Op 29 juli 2017, Equifax, een 118 jaar oude Amerikaans kredietbureau, maakt een groot datalek bekend. Persoonlijke informatie van 143 miljoen kredietaanvragers liggen op straat, inclusief BSN gegevens. Naast persoonsgegevens zijn er creditcard gegevens van 209.000 Amerikaanse klanten buitgemaakt door hackers.

Wat was de oorzaak van deze inbraak?

Het begon met één van de back-end technologieën welk gebruikt werd door Equifax. Struts is een open source framework voor het ontwikkelen van webapplicaties in de Java programmeertaal, gebouwd door de Apache Software Foundation. CVE-2017-9805 is een kwetsbaarheid in de Apache Struts en is gerelateerd aan het gebruik van de REST-plug-in Struts met de XStream-handler om XML-payloads te verwerken. Als het wordt misbruikt, kan een externe niet-geverifieerde aanvaller een virus op de toepassingenserver uitvoeren om de computer over te nemen of andere aanvallen te starten. Twee maanden voor de inbraak bij Equifax werd dit openbaar gemaakt door Apache.

Apache Struts bevat een fout in de REST-plug-in XStream die wordt geactiveerd terwijl het programma door de gebruiker geleverde invoer onnauwkeurig in XML-aanvragen deserialiseert. In meer detail, het probleem treedt op in de toObject()-methode van de XStreamHandler, welk geen beperking oplegt aan de inkomende waarde in een object bij het gebruik van XStream-deserserialisatie. Dit resulteert in kwetsbaarheden in de uitvoering van een willekeurige code.

Zou het hebben uitgemaakt als de REST-plugin was aangepast? Is er een manier om de blockchain-technologie te gebruiken om financiële informatie van deze 143 miljoen klanten te beveiligen, terwijl men nogsteeds gebruik maakt van REST API en Java gebaseerde systemen.

Toevoegen van een Blockchain Laag

Het is duidelijk dat er verbeteringen nodig zijn omtrent de integriteit van gateways voor financiële gegevens. Laten we eens kijken hoe een extra beveiligingslaag kunnen toevoegen met Hydro.

De fundamentele concesusmechanismen van het Ethereum netwerk zorgt voor validaties tijdens transacties, omdat deelnemers gezamenlijk transacties verwerken welk allen correct zijn gevalideerd. Dit leidt tot decentralisatie en immumiteit, maar wat nog belangrijker is, het biedt een richting voor het verminderen van ongeautoriseerde toegang tot gevoelige gegevens in de gateway.

Met Hydro kan authenticatie worden vastgesteld op transactionele operaties op de blockchain. Bijvoorbeeld een API, welk kan kiezen om ontwikkelaars en applicaties kan verplichten om validaties plaats te laten vinden door bepaalde transacties met bepaalde data, tussen bepaalde adressen op de blockchain te voegen, welk als voorwaarde zijn gesteld om een standaard authenticatieprotocol kickstarten.

De Hydro Raindrop

Regen bevat gecondenseerde pakketten water met een diameter van 0,0001 tot 0,005 centimeter. In een typische stortbui zijn er miljarden pakketten, elk van willekeurige grootte, snelheid en vorm. Daarom kan men de exacte waarde van regenbui niet op betrouwbare wijze voorspellen. Vergelijkbaar is dat elke Hydro-authenticatietransactie op een unieke en bijna op toeval gebasseerde wijze tot stand komt - dit is waarom wij ze Raindrops noemen.

De financiële dienstverlening platforms maken vaak gebruik van mirco-deposit-verificaties om klantaccounts te valideren. Het concept is eenvoudig: het platform maakt een kleine storting van willekeurige bedragen naar het bankaccount van de rekeninghouder. Om te bewijzen dat de gebruiker inderdaad de eigenaar is het betreffende account, moet hij of zij de kleine bedragen terugstorten naar de bank, welk vervolgens worden gevalideerd. De enige manier waarop de gebruiker de bedragen kan weten (anders dan raden) is de betreffende bankrekening te openen.

De Raindrop-gebaseerde verificatie met Hydro is analoog. In plaats van de gebruiker een bedrag te sturen en terug te laten sturen,

definiëren we een transactie waarbij de gebruiker deze moet uitvoeren vanuit de geregistreerde wallet. Door toegang tot de betreffende portemonnee te krijgen, is dit de enige manier hoe de gebruiker een geldige transactie kan uitvoeren.

Door het gebruik van Raindrops, kunnen beide, het systeem als de accessor, de autorisatiepogingen controleren op een resistente public ledger. De op blockchain gebaseerde transactie is ontkoppeld van de basissysteemoperaties, uitgevoerd op een gedistribueerd netwerk en afhankelijk van het eigendom van de private keys. Daarom dient het als een nuttige validator.

Een Gedetailleerde Kijk

Er zijn vier entiteiten welk betrokken zijn bij het Hydro-authenticatieproces:

1. *Accessor* - De partij welk toegang probeert te krijgen tot het systeem. In het geval van Hydrogen is de accessor een financiële instelling of app, welk voor de kern van de digitale infrastructuur de Hydrogen API's gebruikt.
2. *System* - Het systeem of gateway waar de accessor toegang tot heeft. Voor Hydrogen is het systeem de Hydrogen API zelf.
3. *Hydro* - Is de module die door het systeem wordt gebruikt voor communicatie en interface met de blockchain
4. *Blockchain* - De gedistribueerde public ledger welk Hydro-transacties verwerkt en de Hydro smart-contracten bevat, waardoor die informatie kan worden gepusht, gepullt, of op een andere wijze kan worden geopereerd.

Elke Raindrop, is in zijn geheel een verzameling van vijf transactieparameters:

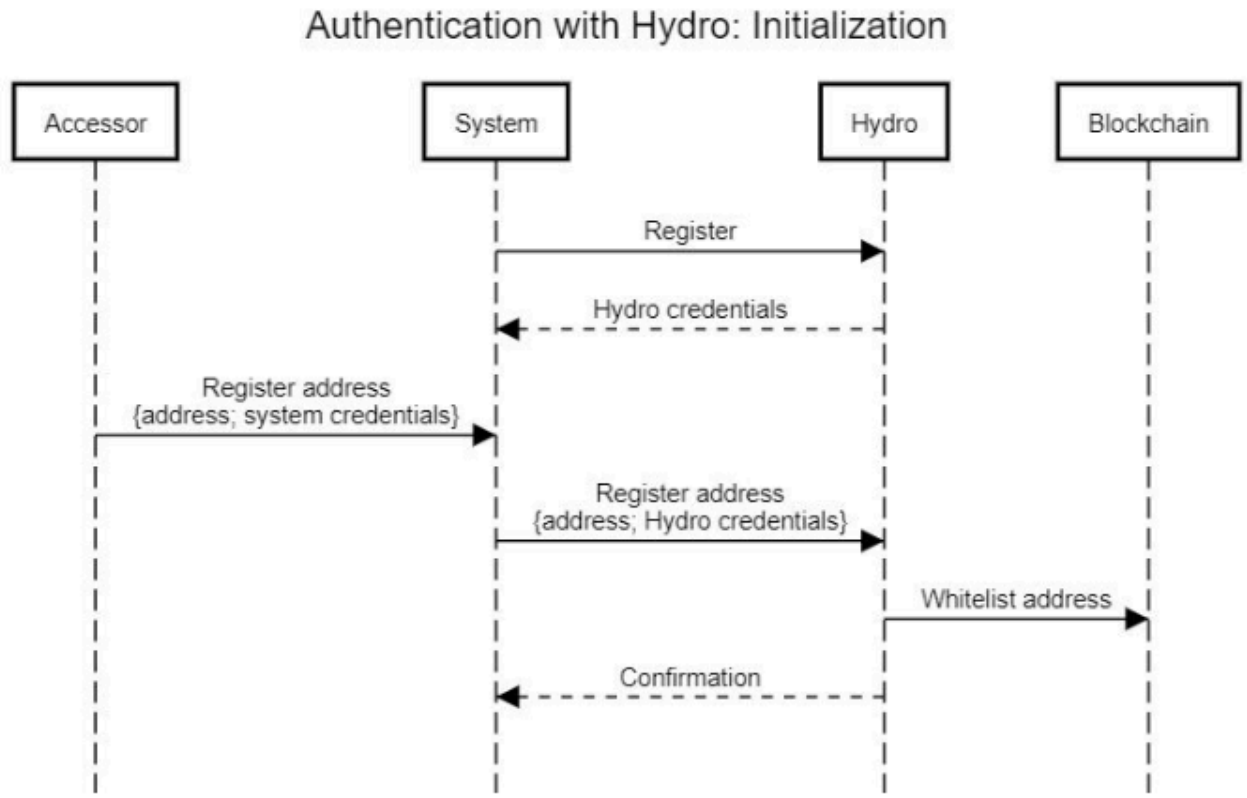
1. *Sender* - Het adres dat de transactie moet starten.
2. *Receiver* - Het ontvangende adres. Deze komt overeen met welk is gebruikt in het Hydro smart-contract.
3. *ID* - Een ID die aan het systeem is gekoppeld.
4. *Quantity* - Het exacte aantal Hydro om te versturen.
5. *Challenge* - Een willekeurig gegeneerd alfanumerieke reeks.

Hieronder vind u een overzicht van het authenticatieproces, welk verdeeld kunnen worden in drie fasen:

1. Initialization
2. Raindrop
3. Validation

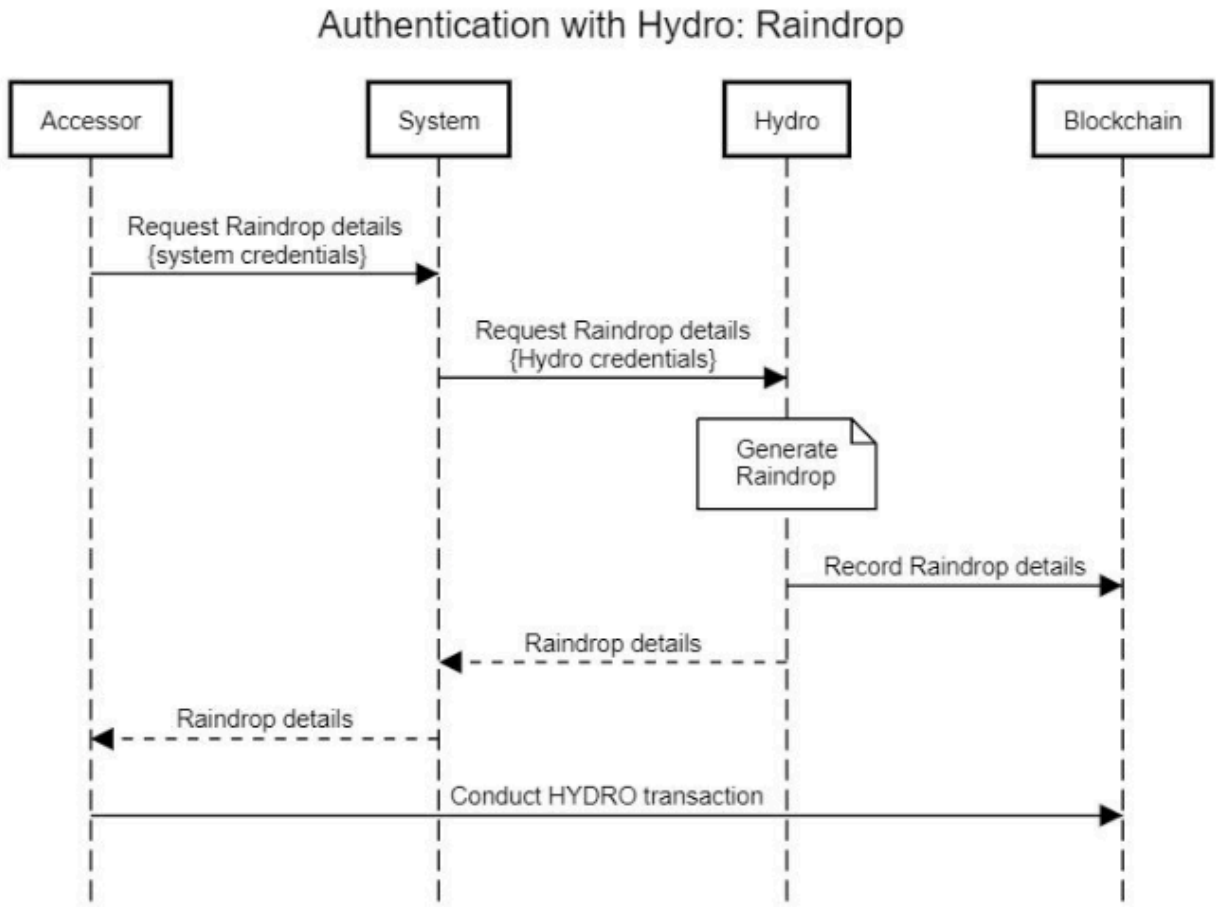
Initialisatie begint met een Systeem (bijvoorbeeld Hydrogen)welk registreert om Hydro te gebruiken en om identificatie gegevens te verkrijgen, door gebruik te maken van de Hydro module kan het

Systeem met de blockchain communiceren. Het Systeem neemt een Accessor aan boord (bijvoorbeeld een financiële instelling) welk met een openbaar adres registreert en dit geregistreerde adres doorgeeft aan Hydro. Dit adres is onveranderlijk en in de blockchain whitelist opgenomen welk is opgeslagen in een Hydro smart-contract. Het Systeem ontvangt een bevestiging dat het adres op de whitelist staat, en kan ook als openbaar event worden geverifieerd. Systeemregistratie hoeft slecht één keer te worden gedaan, terwijl Accessor whitelisting slechts eenmaal per Accessor gedaan hoeft te worden.

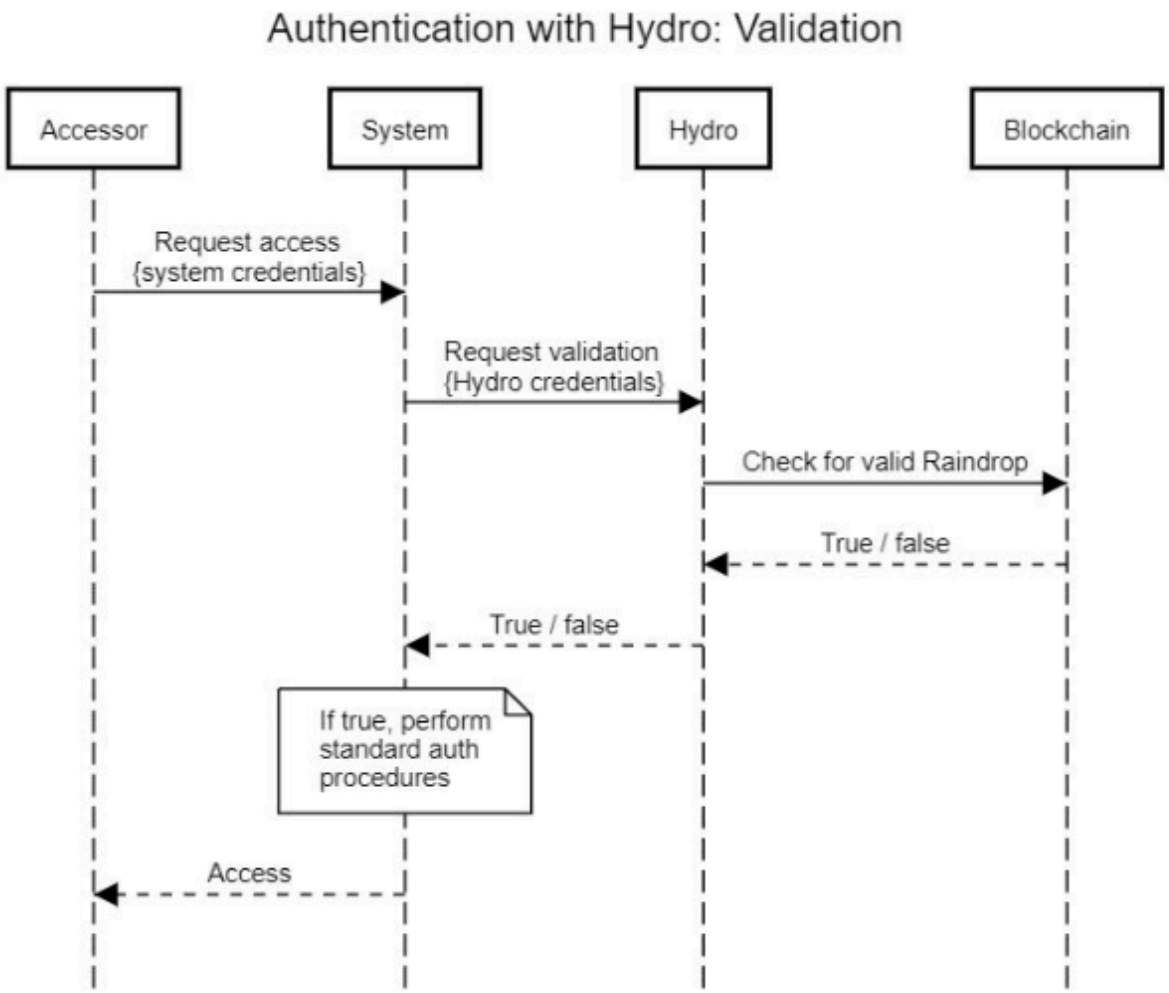


Nadat de initialisatie is voltooid, gaat de kern van de Hydro authenticatieproces van start. De Accessor, welk een Raindrop-transactie moet uitvoeren, start dit proces door een aanvraag te doen van de Raindrop-details uit het systeem, waarna het Systeem het verzoek vervolgens door stuurt naar Hydro. Hydro genereert een nieuwe Raindrop, bewaard bepaalde onveranderbare gegevens op de blockchain, en stuurt volledige details terug naar de Accessor via het Systeem. De Accessor, uitgerust met alle benodigde informatie, voert vervolgens een transactie uit van het geregistreerde adres naar een bepaalde methode in de Hydro smart contract. Wanneer het adres niet op de whitelist staat, wordt de actie gestopt - anders wordt deze opgenomen in de smart contract. Het is belangrijk om te beseffen dat deze transactie buiten het systeem zou moeten plaatsvinden, rechtstreeks van de Accessor naar de blockchain, aangezien ondertekening moet plaats vinden met de private key van

de Accessor (en welk alleen de Accessor zou moeten kunnen verkrijgen).



De laatste stap in het proces van Validatie. In deze stap, doet de de Accessor een officiële aanvraag tot toegang van het Systeem via de door het systeem ingestelde mechanisme. Voor het implementeren van de standaard authenticatieprotocollen, vraagt het Systeem Hydro of de Accessor een geldige Raindrop-transactie heeft voltooid. Hydro koppelt met de smart contract, controleert op geldigheid, waarna het antwoord met een waar/niet-waar. Het Systeem zal beslissen of de actie moet doorgaan op basis van het gegeven antwoord - als het antwoord niet-waar is, zal het Systeem de toegang weigeren. Pas als het antwoord waar is, zal het Systeem toegang verlenen.



Als we de inloggegevens van het basissysteem - welk ander bestaand systeemprotocol dan ook - beschouwen als een één verificatiefactor, dan is het belangrijk dat de Hydro laag een bruikbare tweede verificatiefactor biedt. Door de twee primaire aanvalsmogelijkheden te bekijken, kunnen we eenvoudig het nut ervan bevestigen:

- Mogelijkheid 1 - De aanvaller steelt de basisgegevens van het Accessor-systeem
    - De aanvaller probeert toegang te krijgen tot het systeem met geldige systeemreferenties
    - Dan volgt er systeemcontrole met Hydro, welk bepaald of een geldige transactie is uitgevoerd op de blockchain
    - Hydro antwoord met niet-waar en het systeem weigert toegang

- Mogelijkheid 2 - De aanvaller steelt de private key(s) van de Accessor zijn wallet

    - De aanvaller probeert met een Hydro-transactie uit te voeren vanaf het geregistreerde adres, zonder daar de vereiste Raindrop gegevens bij te gebruiken.
    - De aanvaller kan geen geldige blockchain-transactie maken

    - De aanvaller kan ook geen toegang krijgen tot het systeem, zonder de juiste systeemreferenties

Het is duidelijk dat de aanvaller beide, de referenties van het basissysteem en de private key(s) van de Accessor zijn wallet, zou moeten stelen om toegang te krijgen tot het Systeem. Met dit vooruitzicht, heeft Hydro met succes een extra authenticatiefactor toegevoegd.

Openstellen van The Raindrop

Hoewel deze blockchain gebaseerde authenticatieservice is ontworpen om het Hydrogen API ecosysteem te beveiligen, is er een brede toepasbaarheid op verschillende platforms en systemen mogelijk. Omdat we denken dat anderen mogelijk kunnen profiteren van deze verificatielaag, maken we het toegankelijk voor gebruik.

Net als dat de voorwaarde van integratie voor toegang tot zijn API ecosysteem bij Hydrogen, kan elk systeem dit toevoegen aan bestaande procedures en protocollen. Elk platform - of dit een API, applicatie, bedrijfssoftware, gamingplatform, etc. is - kan Hydro gebruiken voor authenticatiedoeleinden.
Officiële documentatie is beschikbaar op GitHub voor hen wie deze blockchain-laag zou willen opnemen in een authenticatie framework of REST API.

Case Study - Raindrop met OAuth 2.0

Er zijn vele manieren waarop de Raindrop kan worden gebruikt door private organisaties. Het afgelopen decennium hebben privé API's, databases en netwerken uitgebreide systemen van tokens, keys, apps en protocollen ontwikkeld in een poging om gevoelige gegevens te beveiligen. Bijvoorbeeld Google, welk een van de meest populaire aanbieders werd op de beveiligingsmarkt met de Google Authenticator-app. En zoals eerder genoemd, is er weinig tot geen reden om met deze te concurreren of bestaande protocollen te vervangen.

Als Case Study, is hier een kort overzicht over hoe Hydrogen de Hydro-authenticatie implementeert als beveiligingslaag over het API beveiligingsframework:

1. Hydrogen API partners moeten allereerst de IP-addressen van hun verschillende (werk)locaties op de whitelist zetten.
2. Partners moeten een aanvraag plaatsen om een openbaar Hydro adres op de whitelist te laten plaatsen.
3. Alle aanvragen betreft de Hydrogen API's en overdracht van data zijn gecodeerd en worden verzonden via het HTTPS-protocol.
4. Partners moeten een geldige Hydro Raindrop transactie uitvoeren vanaf het geregistreerde Hydro-adres.
5. Partners moeten OAuth 2.0 validatie gebruiken. OAuth (Open Authorization) is een open standaard voor token-gebasseerde authenticatie and authorisatie. Hydrogen ondersteunt de "Resource Owner Password Credentials"- en de "Client Credentials" -types en voor een authenticatie aanvraag moet elke API-gebruiker inloggegevens opgeven.
6. Als aan alle vijf van de bovenstaande elementen wordt voldaan, dan krijgt de Hydrogen-partner een unieke token toegewezen, welk bij elke API-aanvraag moet worden gecontroleerd en geverifieerd.
7. De token is 24 uur geldig, hierna zou de partner zichzelf weer opnieuw moeten valideren.

Mocht een van deze stappen niet met succes worden voltooid, dan wordt de gebruiker direct geblokkeerd voor API-toegang. Een hacker kan deze beveiligingsfactoren niet omzeilen door willekeurig te raden, omdat er ontelbaar unieke combinaties mogelijk zijn.

Hydro blockchain-gebaseerde authenticatie is een belangrijk componenten van het Hydrogen beveiligingsprotocol. Het Hydrogen-team adviseert partners om multi-signature wallets te gebruiken en private keys onafhankelijk op verschillende beveiligde locaties op te slaan los van andere inloggegevens. Zodat alles is voorkomen voor een eventueel falen. Een goed beveiligde multi-signature wallet is niet alleen moeilijk te stelen, maar het openbare karakter van de blockchain staat snelle herkenning van diefstal toe als het in verband staat met de veiligheid van de API.

Omdat iedereen een verificatiepoging tot het Hydro smart-contract kan bekijken, betekend dat het aanvallen van platforms voor maanden achter elkaar nu tot het verleden behoord. API-hackers kunnen nu direct worden tegengehouden, door onverwachte autorisatie pogingen in realtime kunnen worden gedetecteerd, waar ook ter wereld.

Risico's

Net als elke nieuwe technologie, zoals in de begin dagen van social media, e-mail en stream applicaties (welk afhankelijk waren van inbelverbindingen), is het belangrijk dat het core development team nieuwe ontwikkelingen op het gebied van Ethereum transacties en volumes nauwlettend in de gaten houdt. Zou je je kunnen voorstellen dat YouTube wordt lanceert in 1995? Of dat Instagram voor het eerst beschikbaar zou zijn op een Blackberry?

Het Ethereum core development team, zoals Vitalik Buterin en Joseph Poon hebben Plasma voorgesteld: een Scalable Autonomous Smart Contract upgrade op het Ethereum protocol:

> **Plasma is een voorgesteld framework voor gestimuleerde en gedwongen uitvoering van smart contracts welk schaalbaar zijn tot een significante hoeveelheid updates per seconde (mogelijk miljarden), waardoor wereldwijd de blockchain in staat is om een aanzienlijk aantal gedecentraliseerde financiële applicaties te runnen. Deze smart contracts worden gestimuleerd om zelfstandig te opereren via netwerk-transactiekosten, die uiteindelijk afhankelijk is van de onderliggende blockchain (zoals Ethereum) om transactionele state transitions af te dwingen.**

Anderen, zoals The Raiden Network, hebben off-chain scaling oplossing ontworpen om transactie te versnellen en kosten te verminderen. Op dit moment, zal de Raindrop het Ethereum framework **tot een minimum belasten.** Schaalbaarheid brengt dus een minimaal risico met zich mee voor het succes van de Raindrop technologie.

Conclusie

De immuniteit van een openbare blockchain biedt nieuwe kansen en mogelijkheden om de beveiliging te verbeteren van private systemen waaronder API's.

Deze whitepaper omschrijft drie belangrijke zaken:

1. Openbare blockchains kunnen waarde toevoegen aan de financiële diensten.
2. De Hydro Raindrop kan de beveiliging van private systemen verbeteren.
3. De Hydro Raindrop heeft een directe toepassing binnen het Hydrogen API-platform.

Het Hydro-team gelooft dat het beschreven framework de nieuwe standaard voor de beveiligingsinfrastructuur kan zijn voor een nieuw model van hybride private-publiekelijke systemen, waarbij alle belanghebbenden in de financiële-dienstverlening en daarbuiten zullen profiteren.

Bronvermelding:

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