Ang Hydro Raindrop:
Pampublikong Pagpapatotoo Sa Ang Blockchain

Enero 2018

TALAAN NG MGA NILALAMAN

Dukutin

HYDRO: Etimolohiya - Mula sa Laong Griyego ὑδρο- (*hudro-*), mula sa ὕδωρ (*húdōr*, "tubig")

Ang Hydro ay nagbibigay-daan sa mga bago at umiiral na mga pribadong sistema upang walang putol na pagsamahin at pakikinabangan ang hindi nababago at malinaw na dinamika ng isang pampublikong blockchain upang mapahusay ang aplikasyon at dokumento ng seguridad, pagkakakilanlan sa pamamahala, mga transaksyon, at artipisyal na katalinuhan.

Sa papel na ito, ang isang kaso ay gagawin para sa mga pribadong sistema, tulad ng mga APIs, upang gamitin ang Hydro pampubliko blockchain upang mapahusay ang seguridad sa pamamagitan ng pampublikong pagpapatunay.

Ang ipinanukalang teknolohiya ay tinatawag "Raindrop" - isang transaksyon na isinagawa sa pamamagitan ng isang matalinong kontrata na nagpapatunay sa pag-access ng pribadong sistema sa publiko, at maaaring umakma sa mga umiiral na pribadong paraan ng pagpapatunay. Ang teknolohiya ay inilaan upang magbigay ng karagdagang seguridad para sa sensitibong data sa pananalapi na lalong nasa panganib mula sa pag-hack at pag-crash.

Paunang pagpapatupad ng Hydro Raindrop ay isinagawa sa Hydrogen API Plataporma. Ang modular na hanay ng mga APIs na ito ay magagamit sa mga negosyo at mga developer sa buong mundo upang prototipo, magtayo, magpatotoo, at magpatupad ng mga sopistikadong plataporma ng teknolohiya sa pananalapi at mga produkto.

Ang Hydro Raindrop ay magagamit sa komunidad ng developer ng mundo bilang bukas na pinagmulan software, upang payagan ang mga developer na isama ang Hydro Raindrop sa anumang REST API.

Blockchain at Ethereum

Hydro ay ipinatupad sa Ethereum network. Bago magbigay ng karagdagang detalye sa proyekto, mahalaga na maunawaan ang ilang mga pangunahing ideya tungkol sa blockchain at Ethereum.

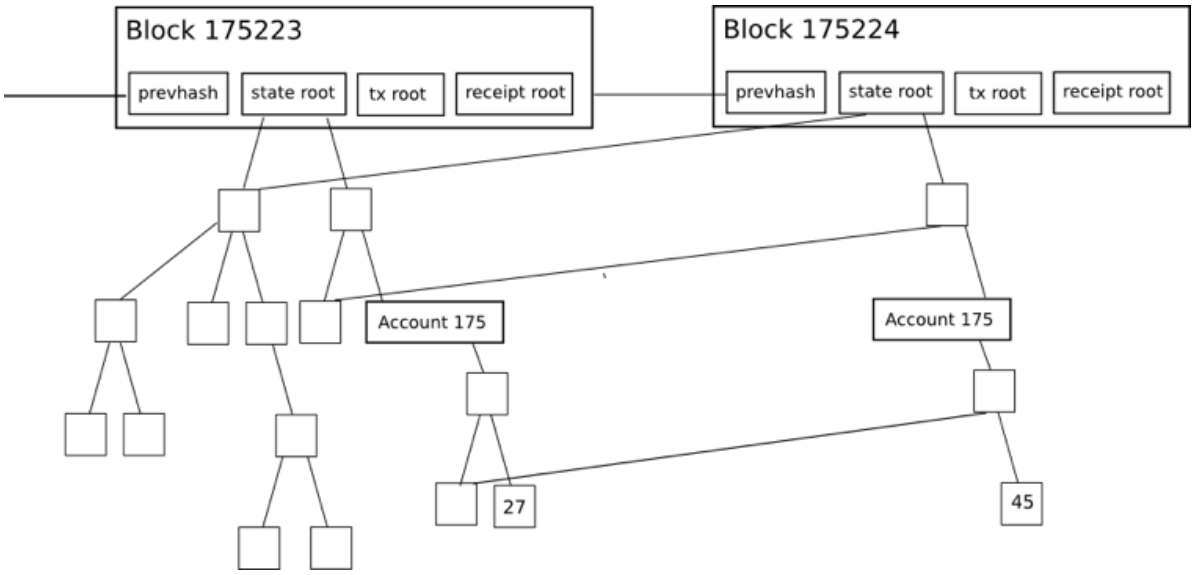
Gusali Sa Ethereum

Karamihan bilang mga app tulad ng Snapchat ay binuo na may Swift at iba pang mga tool na inaalok sa tuktok ng plataporma ng Apple iOS, upang maaari ring blockchain mga application na binuo sa tuktok ng Ethereum. Ang snap Inc. ay hindi kailangan upang bumuo ng iOS, ginagamit ito bilang imprastraktura upang ilunsad ang isang laro-pagbabago ng social media paggamit.

Katulad ng Project Hydro. Ito ay umaasa sa libu-libong mga developer sa buong mundo na nagtatrabaho upang gawing mas mabilis, mas malakas, at mas mahusay ang teknolohiya ng blockchain. Ang Hydro ay gumagamit ng patuloy na pagpapabuti ng imprastraktura sa pamamagitan ng pagbuo ng mga pakikipag-ugnayan na nakatuon sa produkto sa paligid ng teknolohiya ng blockchain na maaaring mag-alok ng mga mahahalagang benepisyo sa mga aplikasyon sa pananalapi na serbisyo.

Merkle Trees

Ang mga puno ng Merkle ay ginagamit sa mga sistema ng ipinamamahagi para sa mahusay na pag-verify ng data. Sila ay mahusay dahil ginagamit nila ang mga hash sa halip ng buong mga file. Ang mga latak ay mga paraan ng pag-encode ng mga file na mas maliit kaysa sa aktwal na file mismo.
Ang bawat bloke ng header sa Ethereum ay naglalaman ng tatlong Merkle Trees para sa mga Transaksyon, Resibo, at Estado:



Pinagmulan: [Merkling in Ethereum](); Vitalik Buterin, Ethereum Founder

Ginagawa nitong madali para sa isang light client upang makakuha ng napapatunayan na mga sagot sa mga query, tulad ng:

- Mayroon bang account na ito?
- Ano ang kasalukuyang balanse?
- Kasama ba ang isang transaksyong ito sa isang partikular na bloke?
- Nagkaroon ng partikular na pangyayari sa address na ito ngayon?

Mga Konkrata ng Smart

Ang isang pangunahing konsepto na pinagana ng Ethereum at iba pang mga network na batay sa blockchain ay ang mga smart na kontrata. Ang mga ito ay mga bloke ng sarili- isinasagawa ng kodigo na maaaring makipag-ugnayan sa maramihang mga partido sa, pagputol ng pangangailangan para sa mga pinagkakatiwalaang ahente. Ang kodigo sa isang matalinong kontrata ay maaaring makita bilang katulad sa mga legal na clauses sa isang tradisyonal na kontrata ng papel, ngunit maaari ring makamit ang mas malawak na pag-andar. Ang mga kontrata ay maaaring magkaroon ng mga patakaran, kondisyon, parusa para sa hindi pagsunod, o maaaring mag-kickstart ng iba pang mga proseso. Kapag na-gatilyo, ang mga kontrata ay nagsasagawa ng orihinal na ipinahayag sa panahon ng pag- lumawak sa pampublikong kadena, na nag-aalok ng mga naitayo-sa na elemento ng immutability at desentralisasyon.

Ang matalinong kontrata ay isang mahalagang kasangkapan para sa pagtatayo sa imprastraktura ng Ethereum. Ang pangunahing pag-andar ng layer ng Hydro blockchain ay nakamit sa pamamagitan ng mga pasadyang kontrata, tulad ng tinalakay sa bandang huli sa papel na ito.

Ethereum Talaga Mac

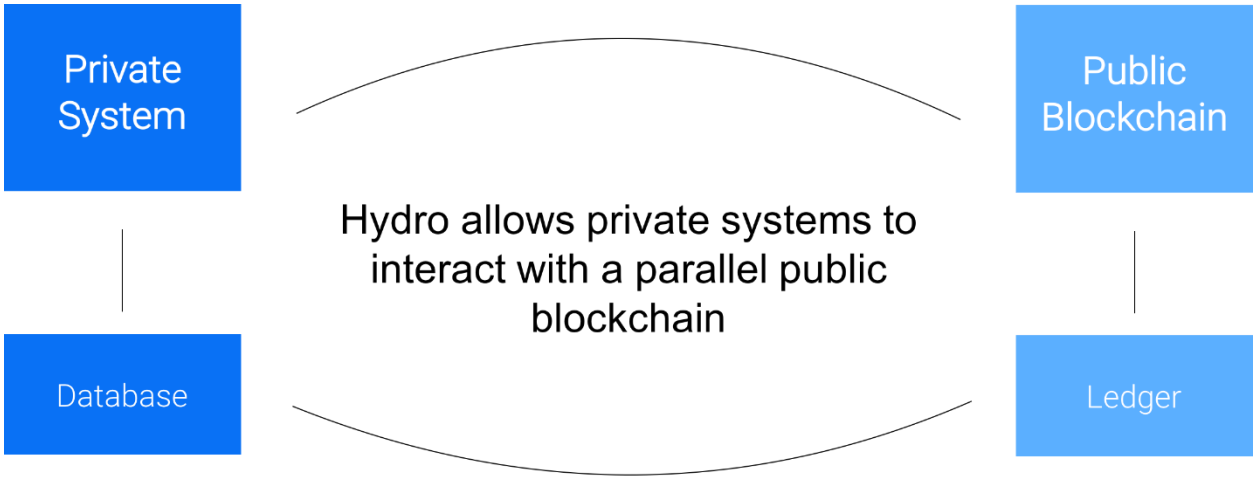
Ang Ethereum Virtual Machine (EVM) ay ang panahong tumatakbo na kapaligiran para sa matalinong kontrata sa Ethereum. Ang EVM ay nakakatulong upang maiwasan ang pag-atake ng Denial of Service (DoS), tinitiyak na ang mga programa ay mananatiling walang katayuan, at nagbibigay-daan sa komunikasyon na hindi maaaring maantala. Ang mga pagkilos sa EVM ay may mga gastos na nauugnay sa mga ito, na tinatawag na gas, na umaasa sa mga mapagkukunang computational na kinakailangan. Ang bawat transaksyon ay may isang pinakamataas na halaga ng gas na inilaan dito, na kilala bilang isang limitasyon ng gas. Kung ang gas na natupok ng isang transaksyon ay umabot sa limitasyon, ito ay titigil na magpatuloy sa pagproseso.

Pampubliko Ledger

Isang Pampublikong Ledger para sa Mga Pribadong Sistema

Ang mga sistema na nagbibigay kapangyarihan sa mga platporma ng pampinansyal na serbisyo, mga website, at mga paggamit ay madalas na inilarawan bilang mga daluyan ng daloy ng data - nagpapadala, nakakakuha, nag-iimbak, nag-a-magpabago, at nagpoproseso ng data para sa mga entidad na kanilang nauugnay. Dahil sa likas na katangian ng data na ito, at ng mga serbisyong pang-pinansya sa pangkalahatan, ang mga sistemang ito ay madalas na kumplikadong mga operasyon sa isang pribado at sentralisadong paraan. Ang pag-uumasa sa mga pribadong istruktura ay nagbubukas ng pinto para sa iba't ibang seguridad, aninaw, at kahusayan na nakuha sa pamamagitan ng pagsasama ng mga panlabas na pwersa na lumalampas sa abot ng panloob na sistema.

Ganiyan ang nangyayari Hydrogen's API Plataporma. Ang Hydro ay naglalayong mag-tap sa mga nabanggit na mga natamo sa pamamagitan ng pagpapahintulot sa mga gumagamit ng Hydrogen na mag-interface sa isang blockchain sa mga paraan na walang putol na isinama sa panimulang pribadong hydrogen ecosystem.



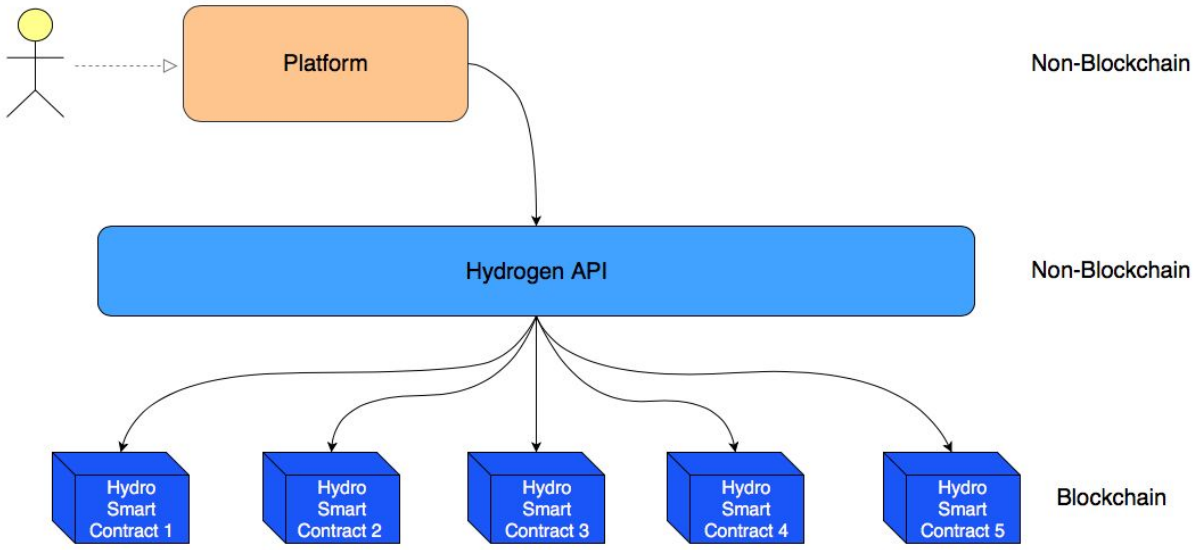
Maaaring mangyari ang mga operasyon na batay sa blockchain ng publiko bago, sa panahon, o pagkatapos ng mga pribadong operasyon. Ang pakikipag-ugnayan sa pagitan ng mga pribado at pampublikong elemento ay maaaring maglingkod upang patunayan, tatakan, itala, o pahusayin ang mga proseso sa loob ng isang ecosystem.

Ang mga etos ng modelong ito ay gumagawa ng mga proseso na mas matatag sa pamamagitan ng pagtapik sa mga benepisyo ng teknolohiya ng blockchain partikular na kung saan maaari itong makagawa ng pinaka-positibong epekto. Habang ang hybrid na balangkas ay maaaring hindi naaangkop sa lahat ng mga

platform, ang Hydro ay nakatuon sa pagbibigay ng halaga para sa mga kaso kung saan ito ay.

Arkitektura para sa Pag-aampon

Ang Hydro ay naiiba mula sa maraming mga umiiral na mga hakbangin sa blockchain, dahil maaaring ito ay umiiral nang nakapag-iisa at mag-ipon sa paligid ng mga bago o umiiral na mga sistema nang hindi nangangailangan ng sistematikong pagbabago. Sa halip na palitan, ang Hydro ay naglalayong dagdagan. Ang mga plataporma at institusyon na plug sa Hydrogen API ay maaaring awtomatikong ma-access ang blockchain.



Ang saklaw ng mga plataporma ng serbisyo sa pananalapi na maaaring magamit ang Hydrogen ay malawak. Ang mga plataporma na ito ay maaaring makapagbigay ng halos anumang karanasan, bahay ng anumang bilang ng mga pagmamay-ari na serbisyo, magsagawa ng anumang pribadong operasyon ng data, at lumawak sa anumang kapaligiran. Ito ay pinagana ng estruktural modularity ng Hydrogen at sinergistic sa Hydro, kumikilos bilang komplementaryong drayber ng pag-aampon.

Raindrop

Itinayo sa itaas ng Hydro pampublikong ledger na ito ay isang serbisyong pang-pagpapatunay na batay sa blockchain, na tinatawag na "Raindrop." Nag-aalok ito ng isang natatanging, hindi nababago, mundo tingnan suson ng seguridad na nagpapatunay ng isang kahilingan sa pag-pagpunta ay nanggagaling mula sa isang awtorisadong pinagmulan.

Pribadong mga protocol ng pagpapatunay tulad ng OAuth 2.0 nag-aalok ng iba't ibang mga antas ng katatagan at pagiging kapaki-pakinabang para sa spectrum ng mga kaso ng paggamit na umiiral. May maliit na pangangailangan upang makipagkumpetensya o pagtatangka na palitan ang mga protocol na ito - Nag-aalok ang Hydro ng isang paraan upang mapahusay ang mga ito sa pamamagitan ng pagsasama ng mga mekaniko ng blockchain bilang isang bahagi ng isang pamamaraan ng pagpapatunay. Ito ay maaaring magdagdag ng isang kapaki-pakinabang na layer ng seguridad upang makatulong na hadlangan ang mga paglabag sa sistema at kompromiso ng data.

Bago suriin ang mga teknikal na aspeto ng Raindrop, hayaan muna nating tingnan ang problema na sinusubukan na lutasin.

Ang Estado ng Seguridad sa Pananalapi

Ang pagtaas ng edad ng datos ay nagdala sa isang pagtaas sa kahinaan, at ito ay partikular na mahalaga para sa mga serbisyong pinansyal. Ang mga pampinansyal na plataporma ay madalas na gateway sa mga malalaking dami ng pribado at sensitibong data tulad ng mga numero ng ID ng pamahalaan, mga kredensyal ng managot, at mga kasaysayan ng transaksyon. Dahil sa kung gaano kahalaga ang data na ito, ang hindi mapagkakatiwalaan na pag-pagpunta ay karaniwang natutugunan ng mga sakuna na resulta.

Industriya ng pananaliksik kompanya Trend Micro lathala ng isang ulat na natagpuan ang mga bagay na ninakaw na linya ng Personal na Makikilalang Impormasyon (PII) na ibinebenta sa Deep Web sa kasing dami ng $1, ang mga pag-scan ng mga dokumento tulad ng mga pasaporte ay magagamit para sa kasing dami ng $10, at mga kredensyal sa pag- mag log in ng bangko para sa maliit na $200, ninakaw na data lalong pira-piraso at hindi maari bakas.

Sa kasamaang palad, ang umiiral na sistema ng pananalapi ay walang walang katapusang rekord ng subaybayan pagdating sa pagpigil, pag- suriin, at pakikipag-ugnayan sa mga paglabag sa data sa mga stakeholder nito.

- Ayon sa isang kamakailang pag-aaral ng Javelin Strategy & Research - *The 2017 Identity Fraud Study* - $16 bilyon ay ninakaw mula sa 15.4 milyong

mamimili ng U.S. sa 2016 dahil sa mga pagkabigo ng sistema ng pananalapi upang maprotektahan ang Personal na Makikilalang Impormasyon (PII).

- Noong Abril 2017, Symantec inilathala nito *Internet Security Threat Report*, na tinantiyang 1.1 bilyong piraso ng PII ay nakompromiso sa iba't ibang mga kapasidad sa kurso ng 2016.

- Ang *2016 Year End Data Breach Quickview* sa pamamagitan ng Risk Based Security, natagpuan na ang 4,149 na paglabag sa data ay nangyari sa mga negosyo sa buong mundo sa 2016, na naglalantad ng higit sa 4.2 bilyong talaan.

- Ang *2017 Thales Data Threat Report – Financial Services Edition*, isang pagsuri ng mga pandaigdigang propesyonal sa IT sa mga propesyonal na serbisyo, natagpuan na ang 49% ng mga organisasyong pampinansiyal na serbisyo ay nagdusa ng isang paglabag sa seguridad sa nakaraan, 78% ay gumagasta ng higit pa upang protektahan ang kanilang sarili, ngunit 73% ay naglulunsad ng mga bagong hakbangin na may kaugnayan sa AI, IoT, at mga teknolohiya ng ulap bago maghanda ng mga angkop na solusyon sa seguridad.

Paglabag Equifax

Noong Hulyo 29, 2017, na-hack ang Equifax, isang 118 taong gulang na U.S. ahensiya sa pag-uulat ng kredito. 143 milyong mamimili ang nakalantad sa PII, kabilang ang Mga Numero ng Sosyal Seguridad. Nakompromiso ang 209,000 mga mamimili ng data ng kredito kard.

Ano ang dahilan ng paglabag na ito?

Nagsisimula ito sa isa sa mga backend na teknolohiya na ginagamit ng Equifax. Ang Struts ay isang bukas na pinagmulan balangkas para sa pagbuo ng mga web paggamit sa Wika ng Java programming, na binuo ng Apache Software Foundation. CVE-2017-9805 ay isang kahinaan sa Apache Struts na may kaugnayan sa paggamit ng Struts REST plugin gamit ang handler ng XStream upang mahawakan ang mga kargamento ng XML. Kung pinagsasamantalahan, pinapayagan nito ang isang malayo na hindi awtorisadong pag-atake na magpatakbo ng malisyosong code sa munisiliyo ng paggamit upang kunin ang makina o maglunsad ng karagdagang pag-atake mula rito. Ito ay patched ng Apache dalawang buwan bago ang paglabag sa Equifax.

Ang Apache Struts ay naglalaman ng isang kapintasan sa REST Plugin XStream na nag-gatilyo bilang ang programa ay walang katiyakan deserializes pampasok na ibinibigay ng gumagamit sa mga kahilingan ng XML. Higit pang partikular, ang problema ay nangyayari sa XStreamHandler's toObject() na paraan, na hindi nagpapataw ng anumang mga paghihigpit sa papasok na halaga kapag gumagamit ng XStream deserializasyon sa isang bagay, na nagreresulta sa mga kahinaan ng hindi makatwiran na pagpapatupad ng code.

Kahit na naka-kompromiso ang REST plugin na ito, dapat ba itong mahalaga? Mayroon bang paraan upang gumamit ng blockchain technology upang ma-secure ang pinansyal na impormasyon ng mga 143 milyong mga customer habang umaasa pa rin sa kasalukuyang nanunungkulan REST API at Java-based na mga sistema?

Pagdaragdag ng Isang Blockchain Layer

Maliwanag na maaaring mapabuti ang integridad ng mga pinansyal na gateway data. Tingnan natin kung paano ang isang karagdagang layer ng seguridad ay nakamit sa pamamagitan ng Hydro.

Ang mga pangunahing mekanismo ng pinagkasunduan ng network ng Ethereum ay tiyakin ang transaksyon bisa dahil ang mga kalahok ay sama-sama nagproseso ng mga transaksyon na maayos na naka- tanda. Ang katotohanang ito ay humantong sa desentralisasyon at kawalan ng pagbabago, ngunit, mas mahalaga, nagbibigay ito ng isang vector para sa pagpapagaan ng hindi awtorisadong pag-pagpunta sa isang gateway na humahawak ng sensitibong data.

Sa Hydro, ang pagpapatotoo ay maaaring ipahayag na totoo sa transaksyon pagpapatakbo sa blockchain. Ang isang API, halimbawa, ay maaaring pumili upang patunayan ang mga nag-develop at mga aplikasyon sa pamamagitan ng pag-aatas sa kanila na simulan ang partikular na mga transaksyon, na may partikular na mga kargamento ng data, sa pagitan ng partikular na mga tirahan sa blockchain, bilang isang prekondisyon na nagtutulak ng isang pamantayan na pagpapatunay protokol.

Ang Hydro Raindrop

Ang ulan ay naglalaman ng mga pakete ng magpaikli tubig mula sa 0.0001 hanggang 0.005 sentimetro ang lapad. Sa isang karaniwang ulan ng bagyo, may mga bilyun-bilyong mga packet na ito, ang bawat random na laki, bilis, at hugis. Dahil dito, hindi maaaring mahulaan ng isa ang eksaktong katangian ng ulan. Katulad nito, ang bawat transaksyon sa pagpapatunay ng Hydro ay natatangi at halos imposible na magkaroon ng nangyari sa pamamagitan ng pagkakataon - ganito ang tawag namin sa kanila Raindrops.

Karaniwang ginagamit ng mga plataporma ng serbisyo sa pananalapi ang pag-mapatunayan ng micro- deposito upang patunayan ang mga managot ng kliyente. Ang konsepto ay payak: ang plataporma ay gumagawa ng maliliit na deposito ng mga random na halaga sa mga na-paghahabol na bangko managot ng isang gumagamit. Upang patunayan ang tunay na pagmamay-ari ng gumagamit ng nasabing managot, dapat na ipasa niya ang mga halaga ng deposito pabalik sa plataporma, na kung saan ay napatunayan na. Ang tanging paraan na maaaring malaman ng gumagamit ang mga wastong halaga (bukod sa paghula) ay sa pamamagitan ng pag-pagpunta sa mga bangko managot na pinag-uusapan.

Ang pag-mapatunayan na nakabatay sa raindrop sa Hydro ay kahalintulad. Kaysa sa pagpapadala ng gumagamit ng isang halaga at pagkakaroon ng ito nagpadala likod, tinutukoy namin ang isang transaksyon at ang gumagamit ay dapat isakatuparan ito mula sa isang kilalang pitaka. Ang tanging paraan na ang gumagamit ay maaaring magsagawa ng isang wastong transaksyon ay sa pamamagitan ng pag-pagpunta sa pitaka na pinag-uusapan.

Sa pamamagitan ng paggamit ng Raindrops, ang parehong sistema at ang accessor ay maaaring subaybayan ang mga pagtatangka ng awtorisasyon sa isang hindi nababago na pampublikong ledger. Ang transaksyon na nakabatay sa blockchain na ito ay na-decouple mula sa mga pangunahing operasyon ng sistema, nangyayari sa isang ipinamamahagi na network, at depende sa pagmamay-ari ng pribadong mga susi. Samakatuwid, nagsisilbing isang kapaki-pakinabang na pagpapatunay ng vector.

Isang Detalyadong Tumingin

May apat na mga entity na kasangkot sa proseso ng pagpapatunay ng Hydro:

1. *Accessor* - Ang partido na sinusubukang i-pagpunta ang isang sistema. Sa kaso ng Hydrogen, ang accessor ay isang pinansiyal na institusyon o app na gumagamit ng Hydrogen APIs para sa kanyang pangunahing digital na imprastraktura.
2. *System* - Ang sistema o gateway na ina-pagpunta ng Accessor. Para sa Hydrogen, ang sistema ay ang Hydrogen API mismo.
3. *Hydro* - Ang module na ginagamit ng System upang makipag-ugnay at mag-interface sa blockchain.
4. *Blockchain* - Ang ipinamamahagi pampublikong ledger na nagpoproseso ng mga transaksyon ng HYDRO at naglalaman ng mga smart na kontrata ng Hydro, kung saan ang impormasyon ay maaaring hunhon, hinila, o kung hindi man ay pinamamahalaan.

Ang bawat ulan ng yelo, sa kabuuan nito, ay isang itakda ng limang mga transaksyon na parametro:

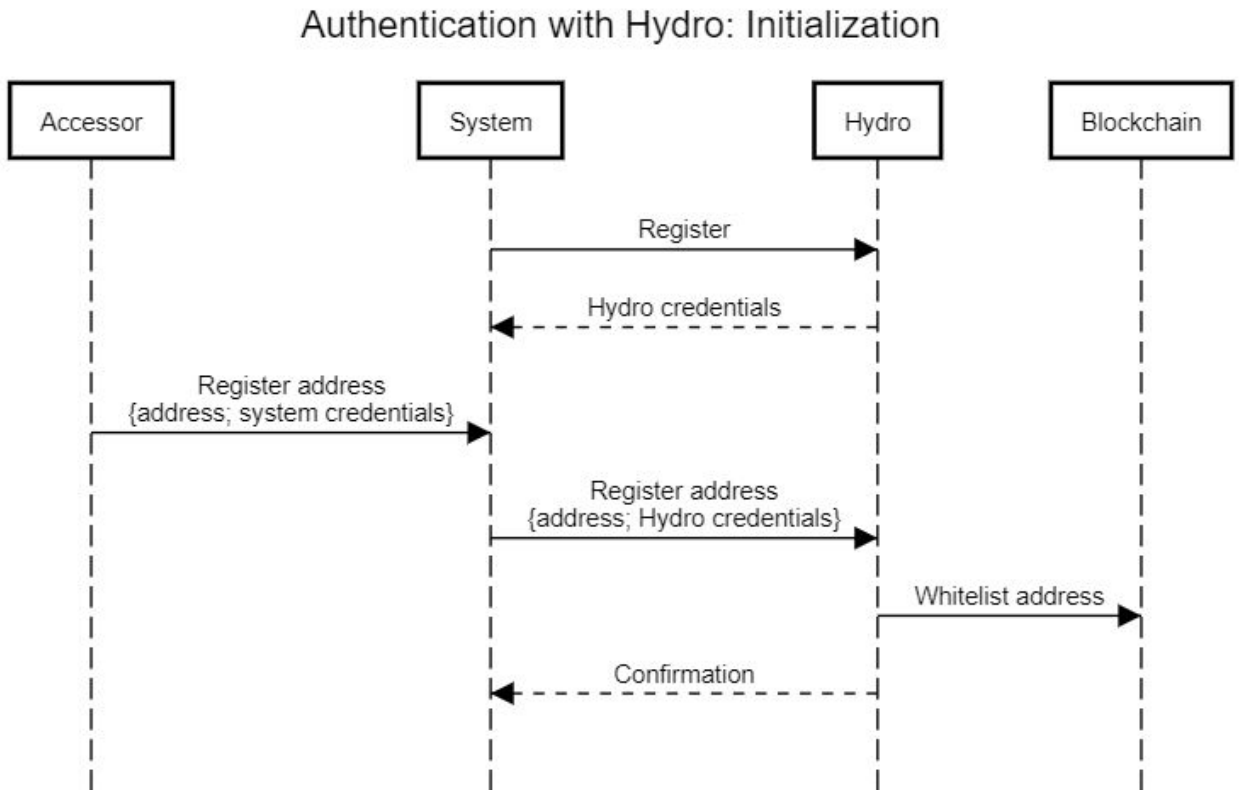
1. *Nagpadala* - Ang tirahan na dapat simulan ang transaksyon.
2. *Tatanggap* - Ang destinasyon ng transaksyon. Katumbas ito sa pagtawag sa isang paraan sa isang kontrata ng Hydro smart.
3. *ID* - Ang isang identifier na nauugnay sa System.
4. *Dami* - Isang tumpak na bilang ng HYDRO na ipapadala.
5. *Hamon* - Isang sapalaran na nabuong alphanumeric na pisi.

Sa ibaba ay isang outline ng proseso ng pagpapatunay, na maaaring pangkalahatan ay inuri sa tatlong yugto:

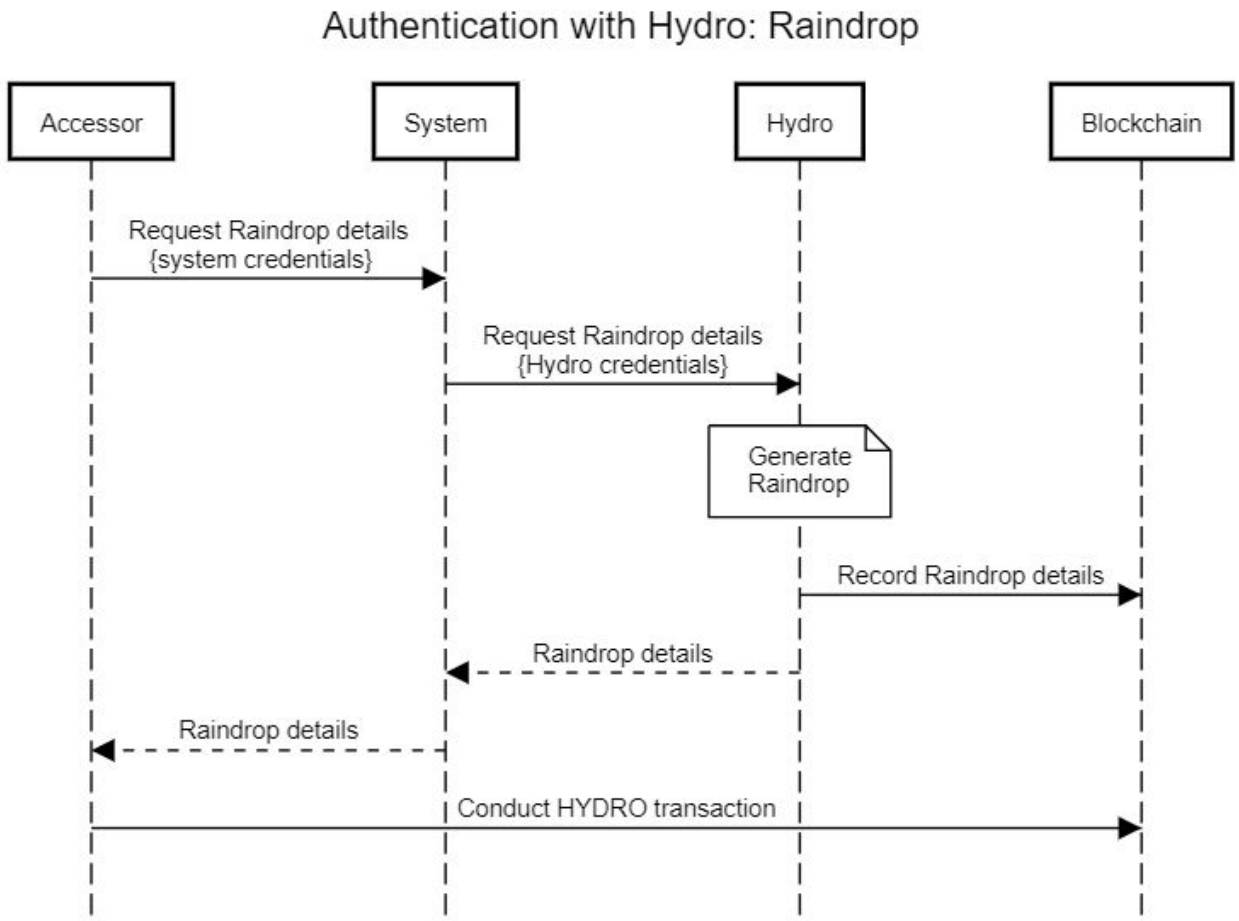
1. Magsimula

2. Raindrop
3. Pagpapatunay

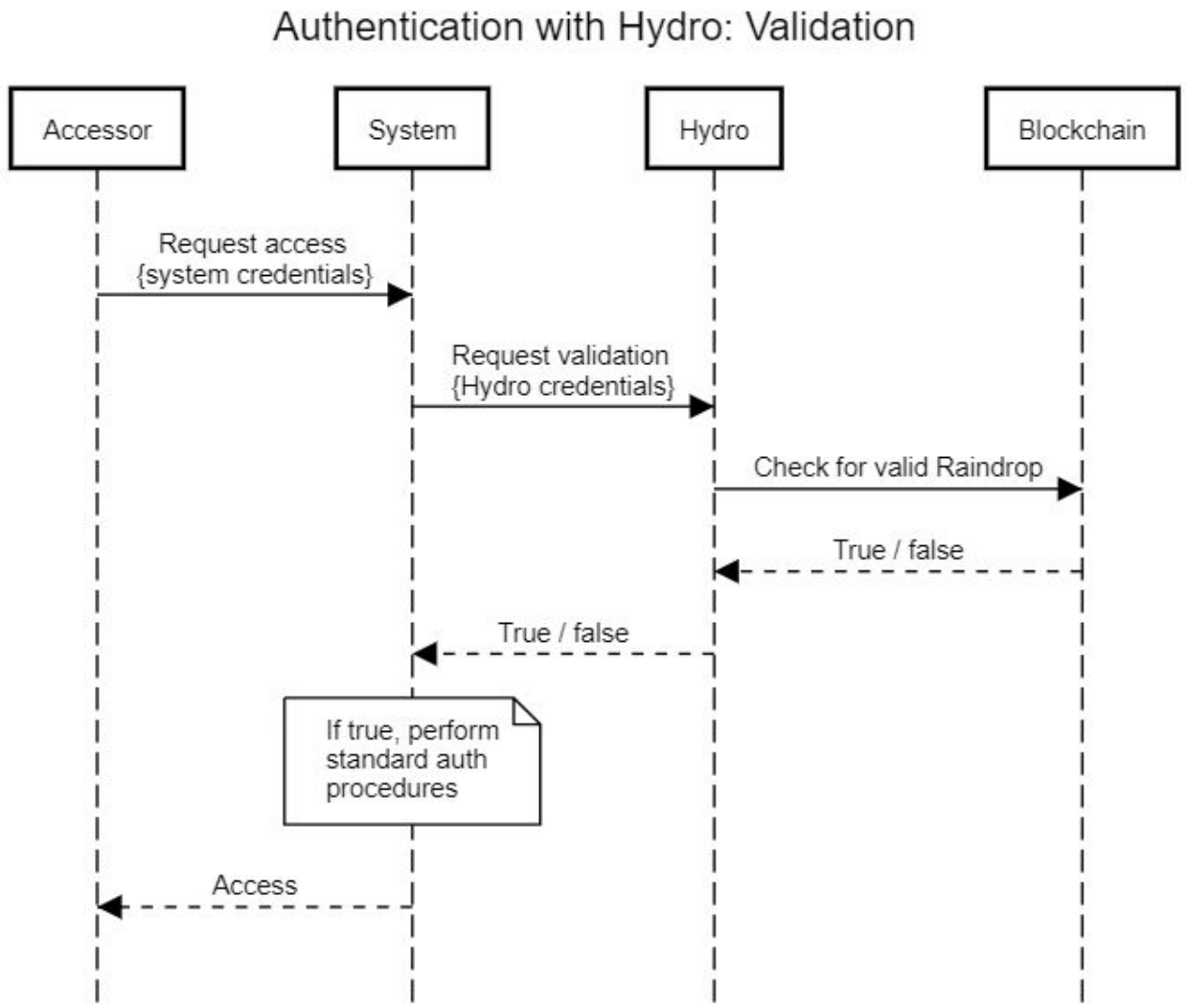
Magsimula nagsisimula sa isang System (hal. Hydrogen) na nagrerehistro upang gamitin ang Hydro at pagkuha ng mga kredensyal, na nagpapagana ng sistema upang makipag-ugnayan sa blockchain sa pamamagitan ng module ng Hydro. Ang System sakay isang Accessor (hal. Isang institusyong pinansyal) na nagrerehistro ng isang pampublikong tirahan, at pagkatapos ay ipinapasa ang rehistradong tirahan sa Hydro. Ang address na ito ay immutably nakasulat papunta sa blockchain sa isang whitelist naka-imbak sa isang Hydro smart kontrata. Ang System ay tumatanggap ng kumpirmasyon na ang tirahan ay whitelisted, na maaari ding ma-mapatunayan bilang isang pampublikong makikita na kaganapan. Ang pagpaparehistro ng sistema ay kailangang mangyari nang isang beses lamang, habang ang Accessor whitelisting ay kailangang mangyari nang isang beses bawat Accessor.



Matapos ang Inisyalisasyon, ang core ng proseso ng pagpapatunay ng Hydro ay maaaring magsimula. Ang Accessor, na dapat magsagawa ng isang transaksyon ng Raindrop, ay tumatalon sa prosesong ito sa pamamagitan ng paghiling ng mga detalye ng Raindrop mula sa System, at ang mga ruta ng System ang kahilingan sa Hydro. Ang Hydro ay bumubuo ng isang bagong Raindrop, nag-iimbak ng ilang mga detalye na walang pagbabago sa blockchain, at nagbabalik ng buong mga detalye sa Accessor sa pamamagitan ng System. Ang Accessor, nilagyan ng lahat ng kinakailangang impormasyon, ay nagsasagawa ng isang transaksyon mula sa nakarehistrong tirahan sa isang paraan sa hydro smart kontrata. Kung ang tirahan ay hindi whitelisted, ang pagkilos ay tinanggihan - sa kabilang banda, ito ay naitala sa matalinong kontrata. Mahalagang tandaan na ang transaksyon na ito ay dapat mangyari sa labas ng System, direkta mula sa Accessor sa Blockchain, dahil ito ay dapat na naka-sign sa pribadong key ng Accessor (na tanging ang Accessor ay dapat makuha).



Ang huling hakbang ng proseso ay Pagpapatunay. Sa hakbang na ito, ang Accessor ay opisyal na humiling ng pagpunta sa System sa pamamagitan ng itinatag na mekanismo ng System. Bago ang pagpapatupad ng alinman sa mga pamantayan na protokol ng pagpapatunay nito, tinatanong ng System Hydro man o hindi ang Accessor ay gumaganap ng wastong transaksyon ng Raindrop. Ang Hydro interface ay may matalinong kontrata, mga tseke para sa bisa, at tumutugon sa isang totoo / maling pagtatalaga. Ang System ay maaaring magpasya kung paano ito dapat magpatuloy batay sa pagtatalaga na ito - kung ito ay mali, ang System ay maaaring tanggihan ang pagpunta, at kung ito ay totoo, ang System ay maaaring magbigay ng pagpunta.



Kung isaalang-alang namin ang mga kredensyal ng System base - o anumang umiiral na protokol ng System na nasa lugar - upang malawak na maging isang kadahilanan ng pagpapatunay, mahalaga na ang Hydro layer ay nagbibigay ng isang kapaki-pakinabang na pangalawang kadahilanan. Sa pagsusuri sa dalawang pangunahing mga vectors ng pag-atake, maaari naming madaling kumpirmahin ang pagiging kapaki-pakinabang nito:

- Vector 1 - Pag-aatake ng magsasalakay ang mga kredensyal ng System ng Accessor's
    - magsasalakay nagtatangkang makakuha ng pagpunta sa System na may wastong mga kredensyal ng System

    - Sistema ng tseke sa Hydro upang malaman kung ang isang wastong transaksyon ay ginawa sa blockchain
    - o Bumalik ang hydro, at tinanggihan ng System ang pag-pagpunta
- Vector 2 - Pag-aatake ng atleta ang (mga) pribadong susi sa pitaka ng Accessor
    - Sinusubukan ng magsasalakay na magsagawa ng isang transaksyon ng Hydro mula sa nakarehistrong tirahan, nang walang kinakailangang mga detalye ng Raindrop
    - Hindi maaaring gumawa ng isang wastong transaksyon sa blockchain
    - Hindi rin maaaring humiling ng pag-pagpunta sa System nang walang tamang kredensyal ng System

Ito ay malinaw na ang magsasalakay ay dapat magnakaw sa parehong mga kredensyal ng System base at (mga) pribadong pitaka susi ng Accessor upang ma-pagpunta ang System. Sa bagay na ito, Matagumpay na nagdagdag ang Hydro ng isang karagdagang kadahilanan ng pagpapatunay.

Pagbubukas Ang Raindrop Sa Pampublikong

Habang ang serbisyong pang-pagpapatunay na batay sa blockchain ay naitala para tulungan ang pag-ligtas ng ekosistema ng Hydrogen API, malawak itong naaangkop sa iba't ibang mga plataporma at system. Dahil sa pakiramdam namin na maaaring makinabang ang iba mula sa layer ng pagpapatunay na ito, binubuksan namin ito para magamit.

Tulad ng pagsasama ng Hydrogen bilang isang prekondisyon para sa pag-pagpunta sa ekosistem API nito, kaya maaari ring idagdag ng system na ito sa mga umiiral na pamamaraan at protokol. Anumang plataporma - maging isang API, aplikasyon, software ng negosiyo, plataporma ng paglalaro, atbp. - Maaaring magamit ang Hydro para sa mga layunin ng pagpapatunay. Ang pormal na dokumentasyon ay magiging magagamit sa GitHub para sa mga nais na isama ang blockchain layer sa isang balangkas ng pagpapatunay o REST API.

Pag-aaral ng Kaso - Raindrop Sa OAuth 2.0

Mayroong dose-dosenang mga paraan na ang Raindrop palayain ay magagamit ng mga pribadong organisasyon. Ang mga pribadong API, database, at network ay lumikha ng mga detalyadong sistema ng mga token, mga susi, apps, at mga protokol sa nakaraang dekada, sa isang pagtatangkang ligtas ang sensitibong data. Halimbawa, ang Google ay naging isa sa mga pinakasikat na tagapagtustos ng produkto sa merkado sa Google Authenticator app. Tulad ng nabanggit kanina, diyan ay maliit na walang dahilan upang makipagkumpetensya sa o palitan ang mga umiiral na mga protokol.

Bilang isang aaral ng kaso, narito ang maikling pangkalahatang ideya kung paano ipinatupad ng Hydrogen ang authentication ng Hydro bilang isang layer ng seguridad sa pangkalahatang balangkas ng seguridad ng API:

1. Ang mga kasosyo sa hydrogen API ay dapat munang magkaroon ng mga IP address ng kanilang iba't-ibang mga napipintong kapaligiran.
2. Ang mga kasosyo ay dapat humiling na i-whitelist ang pampublikong tirahan ng Hydro.
3. Ang lahat ng mga tawag sa mga Hydrogen API at mga paglilipat ng data ay naka-encrypt at ipinadala sa pamamagitan ng HTTPS protokol.
4. Ang mga kasosyo ay dapat kumpletuhin ang wastong transaksyon ng Hydro raindrop mula sa nakarehistrong tirahan ng Hydro.
5. Dapat gamitin ng mga kasosyo OAuth 2.0 pagpapatunay. OAuth (Open Authorization) ay isang bukas na pamantayan para sa token-based na pagpapatotoo at awtorisasyon. Ang hydrogen ay sumusuporta sa mga uri ng "Mga Kredensyal ng May-ari ng Kredensyal ng May-ari ng mapagkukunan" at mga uri ng grant sa kliente, at ang bawat gumagamit ng API ay dapat magbigay ng mga kredensyal para sa kahilingan ng pagpapatunay.
6. Kung wala sa limang mga elemento sa itaas ang lumabag, ang kasosyo sa Hydrogen ay ipinagkaloob sa isang natatanging token, upang masuri at ma-mapatunayan sa bawat API tumawag.
7. Ang token ay may bisa sa loob ng 24 na oras, at pagkatapos ay dapat mapatunayan muli ng kasosyo ang kanilang sarili.

Kung ang alinman sa mga hakbang na ito ay lumabag, agad na naka-lock ang gumagamit mula sa pagpunta ng API. Ang isang Hacker ay hindi maaaring lampasan ang mga kadahilanang ito sa seguridad sa pamamagitan ng sapalaran na paghula, dahil may mga trillions ng mga natatanging mga kumbinasyon.

Ang hydro blockchain- batay na pagpapatunay ay isang mahalagang bahagi ng proteksyon ng hydrogen seguridad. Hinihikayat ng koponan ng Hydrogen ang mga kasosyo upang mag-magtayo ng mga marami-lagda pitaka, at mag-imbak ng mga pribadong susi sa maramihang mga ligtas na lokasyon nang nakapag-iisa mula sa iba pang mga kredensyal, kaya walang iisang punto ng kabiguan. Ang isang maayos na ligtas na marami-lagda pitaka ay hindi lamang mahirap na magnakaw, ngunit ang pampublikong likas na katangian ng blockchain ay nagbibigay-daan din para sa mabilis na pagkilala sa anumang pagnanakaw na may kaugnayan sa seguridad ng API.

Sinuman ay maaaring tumingin ng pagtatangka sa pagpapatotoo sa kontrata ng Hydro smart, na nangangahulugang ang mga araw ng mga plataporma na nakompromiso para sa mga buwan sa-end ay maaaring maging isang bagay ng nakaraan. Ang mga hacker ng API ay maaari na ngayong mapigilan ng mas madali dahil sa kakayahang makita ang mga hindi inaasahang mga pagtatangka ng awtorisasyon sa totoong oras, mula sa kahit saan sa mundo.

Mga Panganib

Karamihan tulad ng anumang nagbubuhat na teknolohiya, tulad ng mga unang araw ng social media, email, at mga anod na paggamit (na umaasa sa dumayal-pataas na pagkakakonekta), mahalaga na ang pangunahing koponan sa pag-unlad ay malapit na subaybayan ang mga bagong pagpapaunlad sa mga bilis at dami ng transaksyon ng Ethereum. Maaari mong isipin ang pagtatangkang YouTube na ilunsad noong 1995? O Instagram na unang inaalok sa Blackberry?

Buod Ethereum nag-develop tulad ng Vitalik Buterin at Joseph Poon ipinanukalang ang Plasma: Scalable Autonomous Smart Contracts mag-itaas sa protokol ng Ethereum:

> **Plasma ay isang iminungkahing balangkas para sa incentibo at pagpapatupad ng mga smart kontrata na kung saan ay nasusukat sa isang makabuluhang halaga ng mga pag-magpabago ng estado sa bawat segundo(potensyal na bilyon) na nagbibigay-daan sa blockchain upang makapagbigay ng isang malaking halaga ng desentralisadong mga paggamit sa pananalapi sa buong mundo. Ang mga smart na kontrata ay insentibo upang ipagpatuloy ang operasyon nagsasarili sa pamamagitan ng mga bayarin sa transaksyon ng network, na sa huli ay umaasa sa pinagbabatayan ng blockchain (hal. Ethereum) upang ipatupad ang transaksyonal na transisyon ng estado.**

Ang iba, gaya ng Ang Raiden Network, ay nagpanukala ng isang wala sa-kadena kaliskisan solusyon na dinisenyo upang mapabilis ang mabilis na transaksyon at mas mababang bayad. Sa oras na ito, ang Raindrop **maglalagay ng napakaliit na pilay** sa balangkas ng Ethereuem, kaya ang kakayahang sumukat ay isang napakaliit na panganib sa tagumpay ng teknolohiya.

Konklusyon

Ang walang pagbabago ng pampublikong blockchain ay nag-aalok ng mga bagong paraan upang mapahusay ang seguridad ng mga pribadong sistema tulad ng mga APIs.

Ang papel na ito ay nagpakita ng tatlong mahahalagang bagay:

1. Ang mga pampublikong blockchain ay maaaring magdagdag ng halaga sa mga serbisyo sa pananalapi.
2. Ang Hydro Raindrop ay maaaring mapahusay ang seguridad ng mga pribadong sistema.
3. May mga kagyat na paggamit ng Hydro Raindrop sa loob ng plataporma Hydrogen API.

Ang grupo ng Hydro ay naniniwala na ang balangkas na nakalagay ay maaaring maging pamantayan na imprastraktura ng seguridad para sa isang bagong modelo ng mestiso na pribadong sistema ng pampublikong, na makikinabang sa lahat ng mga namumuhunan sa industriya ng serbisyo sa pananalapi at higit pa.

Pinagmulan:

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