**Hydro Raindrop**

**Uthibitisho wa Umma Kwenye Blockchain**

Januari 2018

TABLE YA MAJILI

**Kikemikali**

HYDRO: Etymology - Kutoka Kigiriki cha Kale ὑδρο- (hudro-), kutoka kwa hisia (húdōr, "maji")

Hydro huwezesha mifumo mpya na iliyopo ya kibinafsi ili kuunganisha na kuimarisha mienendo isiyoweza kubadilika na ya uwazi ya blockchain ya umma ili kuongeza usalama na programu, usalama wa utambulisho, shughuli na akili za bandia.

Katika jarida hili, kesi itafanywa kwa mifumo binafsi, kama API, kutumia blockchain ya Hydro ya umma ili kuongeza usalama kupitia uthibitisho wa umma.

Teknolojia iliyopendekezwa inaitwa "Raindrop" - shughuli iliyofanywa kupitia mkataba mkali ambayo inathibitisha upatikanaji wa mfumo wa kibinafsi hadharani, na inaweza kusaidia njia zilizopo za kuthibitisha binafsi. Teknolojia inalenga kutoa usalama wa ziada kwa data nyeti za kifedha ambazo zinazidi kuwa hatari kutokana na hacking na uvunjaji.

Utekelezaji wa awali wa Hydro Raindrop hufanyika kwenye Jukwaa la API ya Hydrogen. Seti hii ya msimu ya API inapatikana kwa makampuni ya biashara na watengenezaji kimataifa kwa mfano, kujenga, kupima, na kupeleka majukwaa ya teknolojia ya teknolojia na kisasa.

Hydro Raindrop itafanywa kwa jumuiya ya waendelezaji wa ulimwengu kama programu ya chanzo cha wazi, kuruhusu waendelezaji kuunganisha Raidrop Hydro na REST API yoyote.

**Blockchain na Ethereum**

Hydro inatekelezwa kwenye mtandao wa Ethereum. Kabla ya kutoa maelezo zaidi juu ya mradi huo, ni muhimu kuelewa mawazo ya msingi kuhusu blockchain na Ethereum.

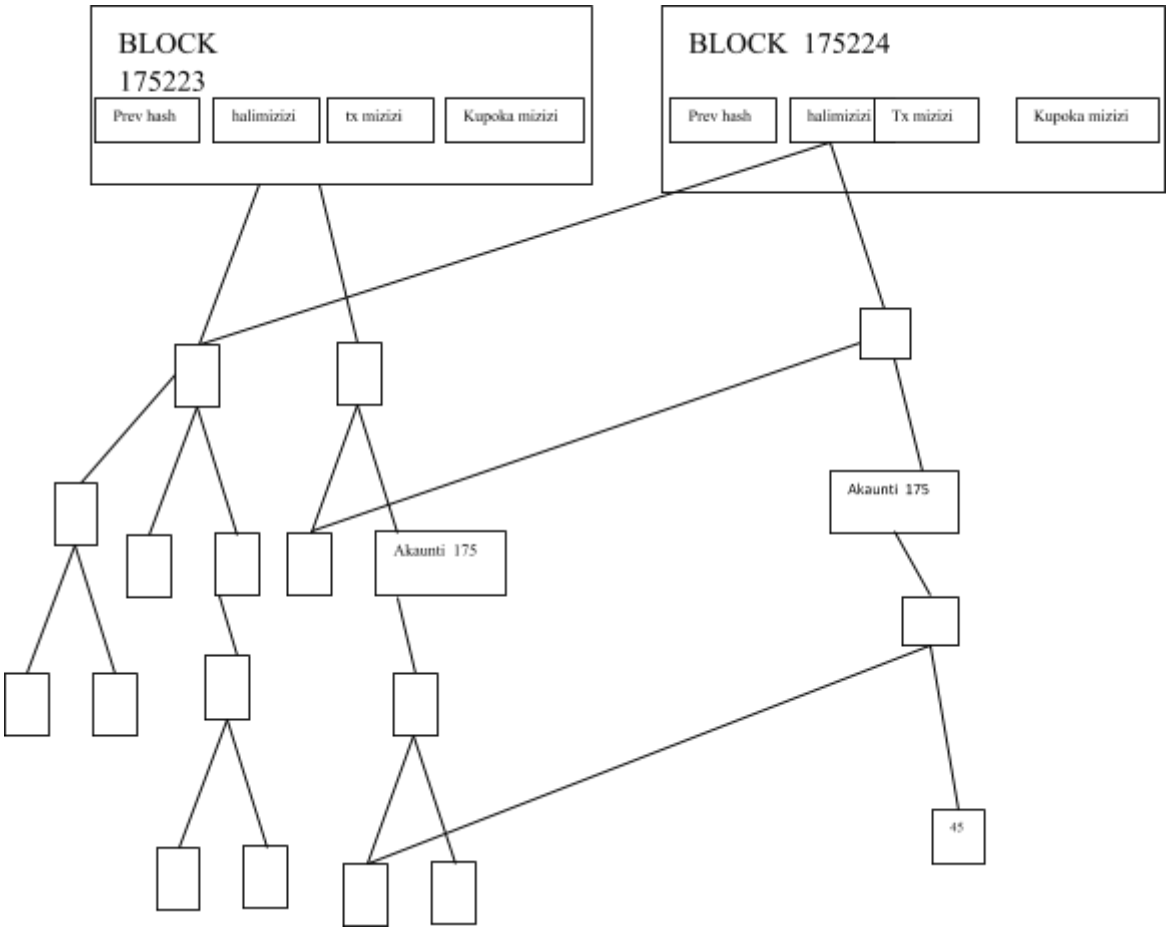
*Kujenga juu ya Ethereum*

Mengi kama programu kama Snapchat zilijengwa na Swift na vifaa vingine vinavyotolewa juu ya jukwaa la Apple iOS, hivyo pia block block inaweza kutumika juu ya Ethereum. Snap Inc haikuhitaji kujenga iOS, ilitumia kama miundombinu ya kuzindua maombi ya kubadilisha vyombo vya habari vya kijamii.

Mradi wa Hydro ni sawa. Inategemea maelfu ya watengenezaji duniani kote wanaofanya kufanya teknolojia ya msingi ya blockchain kasi, nguvu, na ufanisi zaidi. Hydro inaunganisha miundombinu hii ya kuboresha daima kwa kuendeleza mwingiliano wa bidhaa karibu na teknolojia ya blockchain ambayo inaweza kutoa faida inayoonekana kwa maombi ya huduma za kifedha.

*merkle miti*

Miti ya misombo hutumiwa katika mifumo iliyosambazwa kwa ufanisi wa ukaguzi wa data. Wao ni ufanisi kwa sababu wanatumia hasha badala ya faili kamili. Hashes ni njia za encoding files ambazo ni ndogo sana kuliko faili halisi yenyewe. Kila kichwa cha kuzuia katika Ethereum kina Miti ya Merkle mitatu ya Shughuli, Mapokezi, na Mataifa:




*Chanzo: Kuunganisha katika Ethereum; Vitalik Buterin, Mwanzilishi wa Ethereum*

Hii inafanya kuwa rahisi kwa mteja mwepesi kupata majibu kuthibitishwa kwa maswali, kama vile:

- Je, akaunti hii iko

- Nini usawa wa sasa
- Je, shughuli hii imejumuishwa katika block fulani
- Ina tukio fulani lililotokea katika anwani hii leo

*Mikataba ya Smart*

Dhana muhimu inayowezeshwa na Ethereum na mitandao mengine ya blockchain ni ya mikataba ya smart. Hizi ni vitalu vya kujitegemea vya kificho ambayo vyama vingi vinaweza kuingiliana na, kukataa haja ya watu waaminifu walioaminika. Kanuni katika mkataba mkali inaweza kuonekana kama sawa na kifungu cha kisheria katika mkataba wa jadi wa karatasi, lakini pia inaweza kufikia utendaji zaidi wa kupanua. Mikataba inaweza kuwa na sheria, masharti, adhabu kwa kutofuata, au inaweza kukata taratibu zingine. Ilipotokea, mikataba hufanya kama ilivyoelezwa mwanzoni wakati wa kupelekwa kwa mnyororo wa umma, kutoa vitu vya kujengwa katika hali isiyoweza kutengeneza na ugawaji wa madaraka.

Mkataba mkali ni chombo muhimu cha kujenga kwenye miundombinu ya Ethereum. Kazi kuu ya safu ya Hydro blockchain inapatikana kupitia mikataba ya desturi, kama ilivyojadiliwa baadaye katika karatasi hii.

*Mashine ya Ethereum*

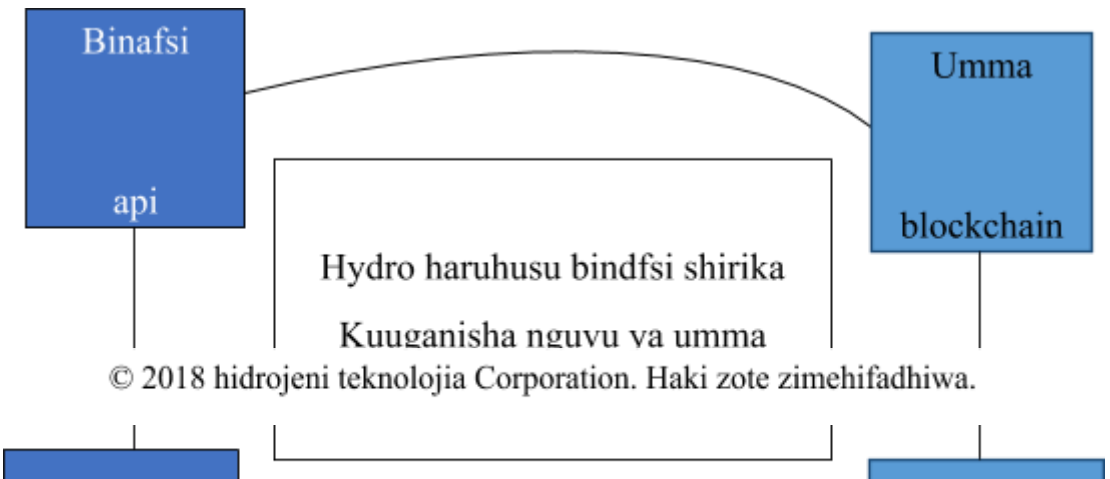
Mashine ya Ethereum Virtual (EVM) ni mazingira ya kukimbia kwa mikataba ya smart juu ya Ethereum. EVM inasaidia kuzuia mashambulizi ya Denial of Service (DoS), kuhakikisha mipango inabakia wasio na msingi, na itawezesha mawasiliano ambayo hayawezi kuingiliwa. Vitendo vya EVM vina gharama zinazohusiana nao, iitwayo gesi, ambayo hutegemea rasilimali zinazohitajika. Shughuli zote zina kiasi kikubwa cha gesi kilichopewa, kinachojulikana kama kikomo cha gesi. Ikiwa gesi inayotumiwa na manunuzi inakaribia kikomo, itaacha kusindika

**umma leja**

*ya umma kitabu kwa ajili ya binafsi mifumo*

Mifumo inayowezesha majukwaa ya huduma za kifedha, tovuti, na programu zinaweza kuelezewa kama miingiliano ya mtiririko wa data - hutuma, kurejesha, kuhifadhi, kusasisha, na kutengeneza data kwa vyombo ambavyo wanaunganisha. Kwa sababu ya hali ya data hii, na kwa huduma za kifedha zaidi kwa ujumla, mifumo hii mara nyingi hufanya shughuli nyingi za nyumba kwa njia ya faragha na ya kati. Kujiunga na miundo binafsi, kwa upande wake, hufungua mlango kwa ufanisi wa usalama, uwazi, na ufanisi wa kuwa na kuingiza nguvu za nje zinazozidi kufikia mfumo wa ndani

kama ilivyo kwa hidrojeni ya api ya jukwaa. Hydro inalenga bomba katika aforementioned faida kwa kuruhusu hidrojeni watumiaji wa interface na blockchain kwa njia ambazo ni seamlessly jumuishi ndani ya kimsingi binafsi hidrojeni mazingira.

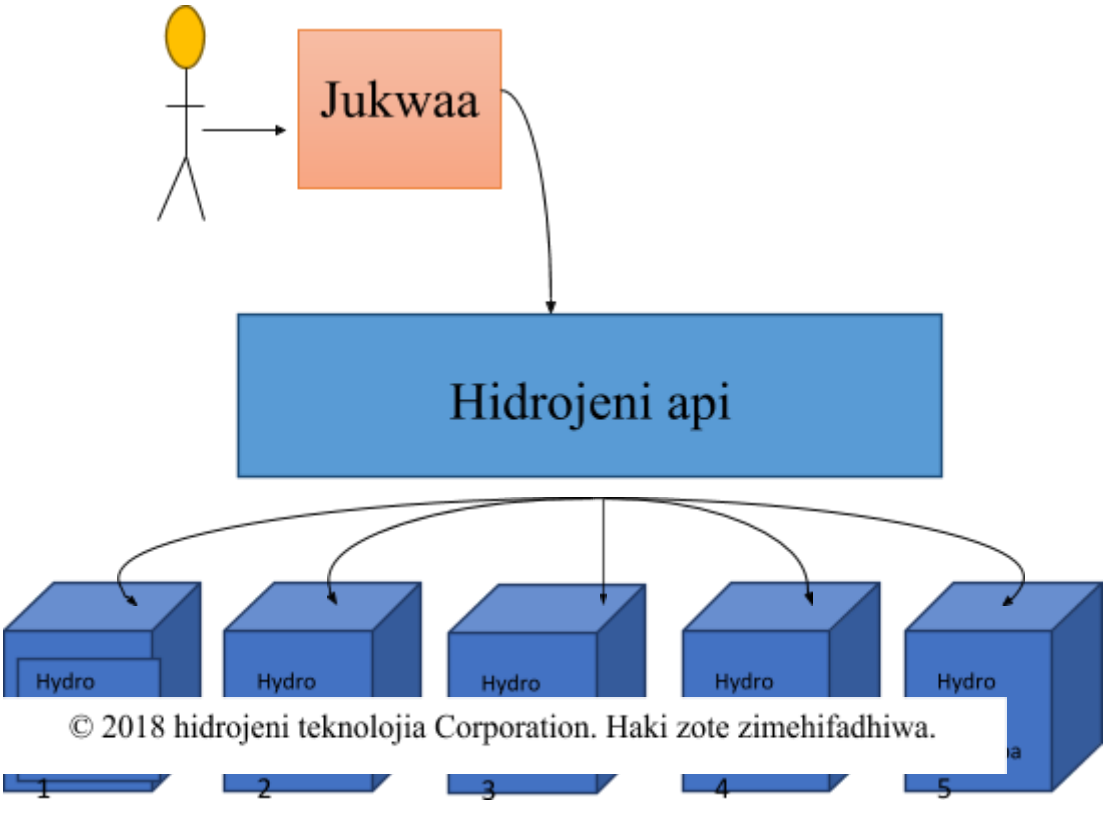


umma blockchain makao shughuli yanaweza kutokea kabla, wakati au baada ya binafsi shughuli. samspelet kati ya binafsi na ya umma mambo inaweza kutumika kuhalalisha, muhuri, rekodi, au kuboresha michakato ya ndani ya mazingira.

ya maadili ya mtindo huu ni maamuzi imara zaidi na tapping katika faida ya blockchain teknolojia hasa ambapo inaweza kuzalisha zaidi athari chanya. wakati huu hybrid mfumo inaweza kuwa zinazotumika kwa majukwaa yote, Hydro inalenga kutoa thamani kwa ajili ya kesi ambayo ni.

A*rchitecting mwanya*

Hydro tofauti na wengi zilizopo blockchain mipango, kwa sababu inaweza kuwepo kwa kujitegemea na safu kuzunguka mpya au zilizopo mifumo bila kuhitaji utaratibu mabadiliko. badala ya kuchukua nafasi, Hydro inalenga kuongeza. majukwaa na taasisi za kuziba ndani ya hidrojeni apis inaweza moja kwa moja kupata blockchain.



wigo wa huduma za kifedha majukwaa ambayo inaweza kujiinua hidrojeni ni pana. hizi majukwaa inaweza nguvu karibu yoyote uzoefu, nyumba idadi yoyote ya wamiliki wa huduma, kufanya yoyote binafsi data kazi, na kupeleka katika mazingira yoyote. hii ni kuwezeshwa na hidrojeni ya kimuundo modularity na ni synergistic na umeme wa maji, Kaimu kama nyongeza dereva wa kupitishwa.

**Raindrop**

kujengwa juu ya hii Hydro umma leja ni blockchain makao uthibitishaji huduma, inayoitwa "raindrop." hii inatoa tofauti, hayabadiliki, kimataifa viewable safu ya usalama kwamba inathibitisha na ombi la kufikia ni kuja kutoka mamlaka chanzo.

binafsi uthibitishaji itifaki kama vile oauth 2.0 kutoa ngazi mbalimbali ya robustness na manufaa kwa ajili ya wigo wa kesi ya matumizi ambayo kuwepo. ni kidogo haja ya kushindana na au kujaribu kuchukua nafasi hizi itifaki - Hydro inatoa njia ya kuongeza yao kwa kuchanganya blockchain mechanics kama sehemu ya uthibitishaji utaratibu. hii wanaweza kuongeza muhimu safu ya usalama wa kusaidia kuzuia mfumo ukiukaji na data Maafikiano.

kabla ya kuchunguza masuala ya kiufundi ya raindrop, Hebu kwanza kuangalia tatizo ni kujaribu kutatua.

*hali ya usalama wa kifedha*

kupanda kwa data umri umeleta na hayo kuongezeka kwa mazingira magumu, na hii ni muhimu hasa kwa ajili ya huduma za kifedha. kifedha majukwaa mara nyingi gateways kwa kiasi kikubwa cha binafsi na data nyeti kama vile serikali id idadi, sifa akaunti, na shughuli historia. kwa sababu ya jinsi muhimu sana data hii ni haifai upatikanaji kawaida alikutana na janga matokeo.

sekta ya utafiti wa kampuni ya mwenendo micro ilichapisha ripoti kuwa kupatikana kuibiwa line ya vitu ya binafsi zinazotambulika (pii) ni kuuzwa katika kina mtandao kwa ajili kidogo kama $ 1, scans ya nyaraka kama hati za kusafiria za kutosha kwa ajili kidogo kama $ 10, na benki ya kuingia kwa kama kidogo $ 200, na kufanya usambazaji wa kuibiwa data inazidi kugawanyika vipande vipande na hazieleweki.

kwa bahati mbaya, zilizopo mfumo wa fedha hana bila doa rekodi linapokuja suala la kuzuia, kupima, na kuwasiliana data ukiukaji na wadau wake.

- according kwa utafiti wa hivi karibuni na mkuki mkakati & utafiti - 2017 utambulisho udanganyifu utafiti - $ bilioni 16 kilichoibiwa kutoka 15.4 milioni ya Marekani ya walaji katika 2016 kutokana na kushindwa mfumo wa fedha za kulinda binafsi zinazotambulika (pii).
- n Aprili 2017, symantec kuchapishwa wake na internet usalama na tishio ripoti, ambayo makadirio bilioni 1.1 vipande vya pii walikuwa kuathirika katika mbalimbali uwezo juu ya mwendo wa 2016.

- the 2016 mwaka mwisho data uvunjaji quickview na riskbaserade usalama, kupatikana kuwa 4,149 data ukiukaji ilitokea katika biashara ya kimataifa katika 2016, kuwasababishia zaidi ya 4.2 bilioni rekodi.

- the 2017 thales data tishio ripoti - huduma za kifedha edition, utafiti wa kimataifa ni wataalamu katika huduma za kitaalamu, kupatikana kuwa 49% ya huduma za kifedha mashirika kuteswa uvunjaji wa usalama katika siku za nyuma, 78% ni matumizi ya zaidi ya kulinda wenyewe, lakini 73% ni uzinduzi mipango mipya kuhusiana na ai, iot, na wingu teknolojia kabla ya maandalizi sahihi ufumbuzi wa usalama.

*equifax uvunjaji*

Julai 29 2017, equifax, a 118 umri wa miaka ya Marekani ya mikopo Shirika la kuripoti, alikuwa hacked. 143 milioni watumiaji alikuwa pii wazi, ikiwa ni pamoja na usalama wa jamii idadi. 209,000 wateja alikuwa kadi data kuathirika.

nini kilichosababisha hii uvunjaji?

kuanza na moja ya backend teknolojia itatumika na equifax. struts ni chanzo wazi mfumo kwa ajili ya kuendeleza maombi ya mtandao katika java lugha ya programu, kujengwa na apache software Foundation. cve-2017-9805 ni mazingira magumu katika apache struts kuhusiana na kutumia struts wengine plugin na xstream handler kushughulikia xml payloads. kama kunyonywa, ni inaruhusu kijijini unauthenticated mshambuliaji kukimbia misimbo hasidi juu ya maombi server ama kuchukua juu ya mashine au uzinduzi mashambulizi zaidi kutoka humo. hii ilikuwa viraka na apache miezi miwili kabla ya equifax uvunjaji.

apache struts ina flaw katika maeneo mengine plugin xstream kwamba ni yalisababisha kama mpango insecurely de-serializes user-hutolewa pembejeo katika xml maombi. hasa zaidi, tatizo hutokea katika xstreamhandler ya toobject () mbinu, ambayo haina kuweka yoyote vikwazo juu ya zinazoingia thamani ya wakati wa kutumia xstream deserialization katika kitu, na kusababisha holela code utekelezaji udhaifu.

Hata kama hii mapumziko plugin alikuwa kuathirika, wanapaswa kuwa na mattered? Je, kuna njia ya kutumia blockchain teknolojia ya kupata taarifa za fedha kati ya hizi 143 ya wateja milioni wakati bado kutegemea anayemaliza wengine api na java makao mifumo ya?

*kuongeza blockchain safu*

ni wazi kwamba uadilifu wa data ya kifedha gateways inaweza kuboreshwa. Hebu kuchunguza jinsi safu ya ziada ya usalama ni mafanikio kupitia umeme wa maji.

ya msingi ya makubaliano ya mifumo ya ethereum mtandao kuhakikisha mapatano uhalali kwa sababu washiriki pamoja mchakato shughuli ambazo ni vizuri saini. ukweli huu husababisha madaraka na faradhi, lakini, muhimu zaidi, inatoa vector kukabiliana na kudhibiti kupata ruhusa gateway kwamba hushughulikia data nyeti.

na umeme wa maji, uthibitishaji inaweza vimesimama juu mapatano kazi tarehe ya blockchain. api, kwa mfano, unaweza kuhalalisha watengenezaji na maombi na wanaohitaji wao kuanzisha maalum shughuli, na hasa data payloads, kati hasa anwani za juu ya blockchain, kama sharti kwamba kickstarts kiwango uthibitishaji itifaki.

*Hydro raindrop*

mvua ina pakiti ya kufupishwa maji kuanzia 0.0001 kwa 0.005 sentimita katika kipenyo. katika kawaida mawimbi ya mvua, kuna mabilioni ya hizi pakiti, kila moja ya random kawaida, kasi, na sura. kwa sababu ya kwamba, mtu cannot reliably kutabiri hali halisi ya mvua. vile vile, kila Hydro uthibitishaji shughuli ni ya kipekee na karibu haiwezekani kuwa ilitokea kwa bahati - hiyo ni kwa nini tunawaita raindrops.

huduma za kifedha majukwaa kawaida kutumia ndogo za Amana uhakiki kuhalalisha akaunti ya mteja. dhana ni rahisi: jukwaa hufanya Amana ndogo ya random kiasi katika mtumiaji alidai akaunti ya benki. ili kuthibitisha mtumiaji hakika anamiliki alisema akaunti, yeye au yeye lazima relay Amana kiasi nyuma ya jukwaa, ambayo ni basi ilisahihishwa. njia pekee ya mtumiaji anaweza kujua halali kiasi (badala ya kubahatisha) ni kwa kupata akaunti ya benki katika swali.

raindrop makao ya ukaguzi na umeme wa maji ni sawa. badala ya kutuma mtumiaji kiasi na kuwa ni ilipeleka nyuma, sisi kufafanua shughuli na mtumiaji lazima kutekeleza ni kutoka inayojulikana Mkoba. njia pekee ya mtumiaji anaweza kufanya halali ya shughuli ni kwa kupata Mkoba katika swali.

kwa kutumia raindrops, wote wa mfumo na accessor wanaweza kufuatilia idhini majaribio juu ya hayabadiliki umma leja. hii blockchain makao shughuli ni decoupled kutoka msingi mfumo wa uendeshaji, hutokea kwenye kusambazwa mtandao, na hutegemea juu ya umiliki wa funguo binafsi. kwa hiyo, ni mtumishi kama muhimu uthibitisho vector.

*Kuangalia kwa kina*

kuna nne vyombo kushiriki katika Hydro uthibitishaji mchakato:

1. accessor - chama kujaribu kupata mfumo. katika kesi ya hidrojeni, ya accessor ni taasisi ya kifedha au programu kutumia hidrojeni apis kwa msingi wake digital miundombinu.
2. mfumo - mfumo au gateway kuwa ni kuwa kupatikana kwa accessor. hidrojeni, mfumo ni hidrojeni api yenyewe.
3. Hydro - moduli kwamba ni itatumika na mfumo wa kuwasiliana na interface na blockchain.
4. blockchain - kusambazwa umma leja kwamba taratibu Hydro shughuli na ina Hydro smart mikataba, kwa njia ambayo habari inaweza kuwa kusukuma, vunjwa, au vinginevyo kuendeshwa juu.

kila mmoja raindrop, katika ukamilifu wake, ni seti ya tano mapatano vigezo:

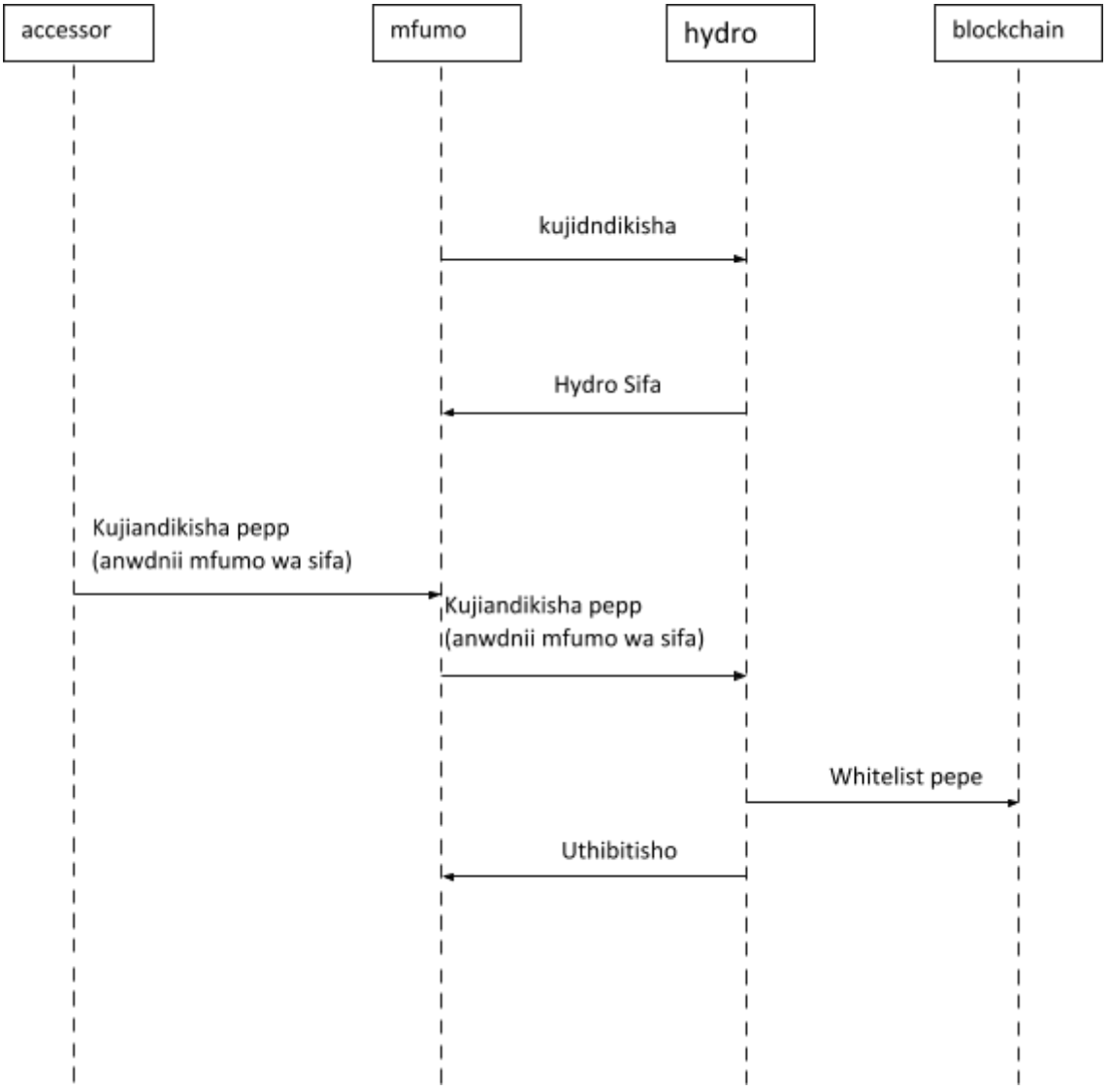
1. Sender - The address that must initiate the transaction.
2. mpokeaji - shughuli ya marudio. hii sambamba na wito njia katika Hydro smart mkataba.
3. id - wa kitambulisho kwamba ni kuhusishwa na mfumo.
4. 4. Wingi - sahihi idadi ya Hydro kutuma.
5. challenge - Nasibu yanayotokana alphanumeric kamba.

chini ni muhtasari wa uthibitishaji mchakato, ambayo inaweza kuwa kwa ujumla classified katika hatua tatu

1. initialization
2. raindrop
3. uthibitisho

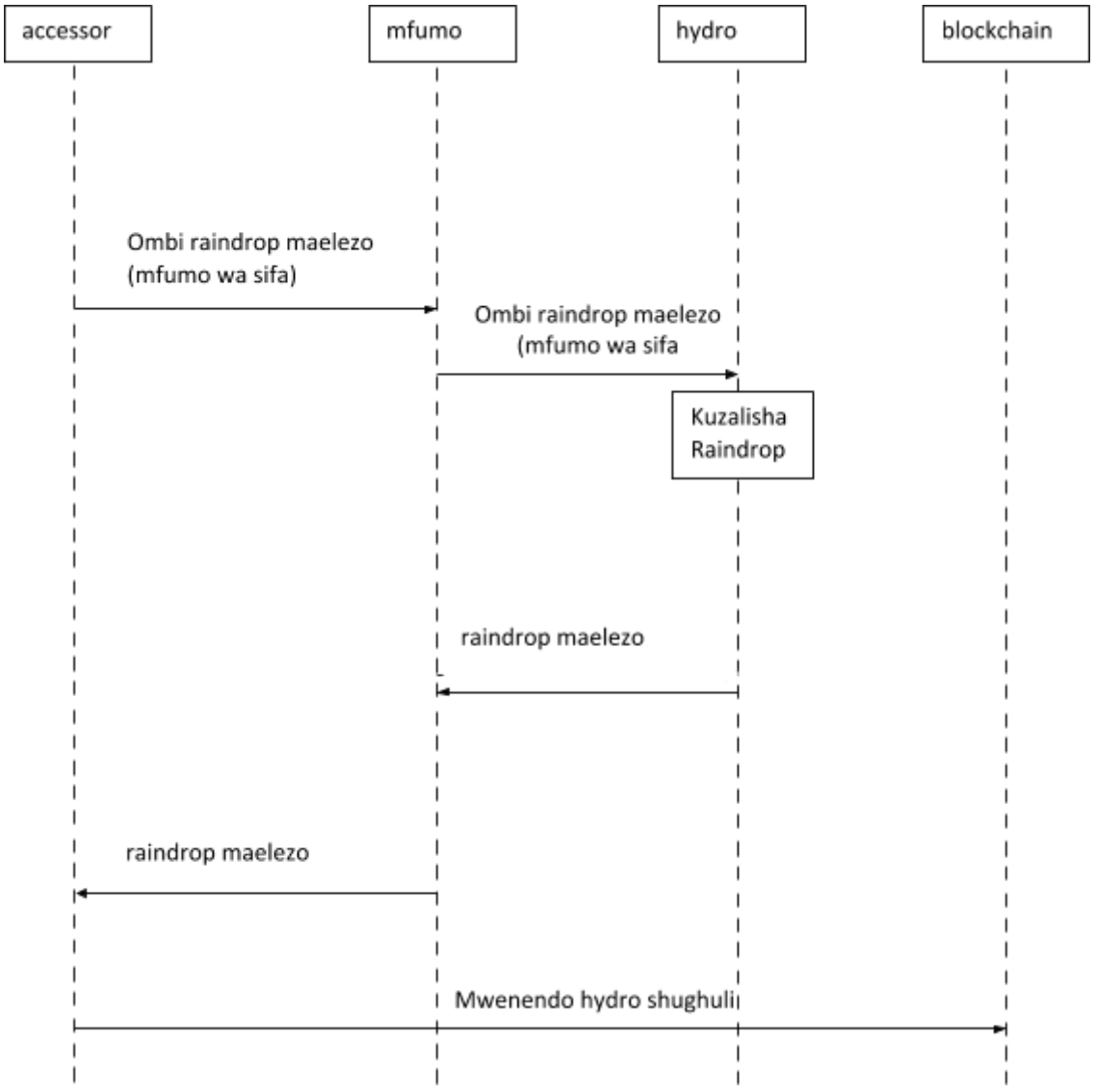
initialization huanza na mfumo (kwa mfano hidrojeni) kusajili kutumia umeme wa maji na kupata sifa, kuwezesha mfumo wa kuwasiliana na blockchain kupitia Hydro moduli. mfumo onboards an accessor (kwa mfano taasisi ya fedha) ambao madaftari ya umma ya mitaani, na kisha hupita waliosajiliwa anwani ya umeme wa maji. anwani hii immutably imeandikwa kwenye blockchain kwa whitelist kuhifadhiwa katika Hydro smart mkataba. mfumo anapata uthibitisho kwamba anuani mara imeidhinishwa, ambayo pia inaweza kuthibitishwa kama hadharani viewable tukio hilo. mfumo wa usajili haja tu kutokea mara moja, wakati accessor whitelisting haja tu kutokea mara moja kwa accessor

uthibitishaji na Hydro: initialization



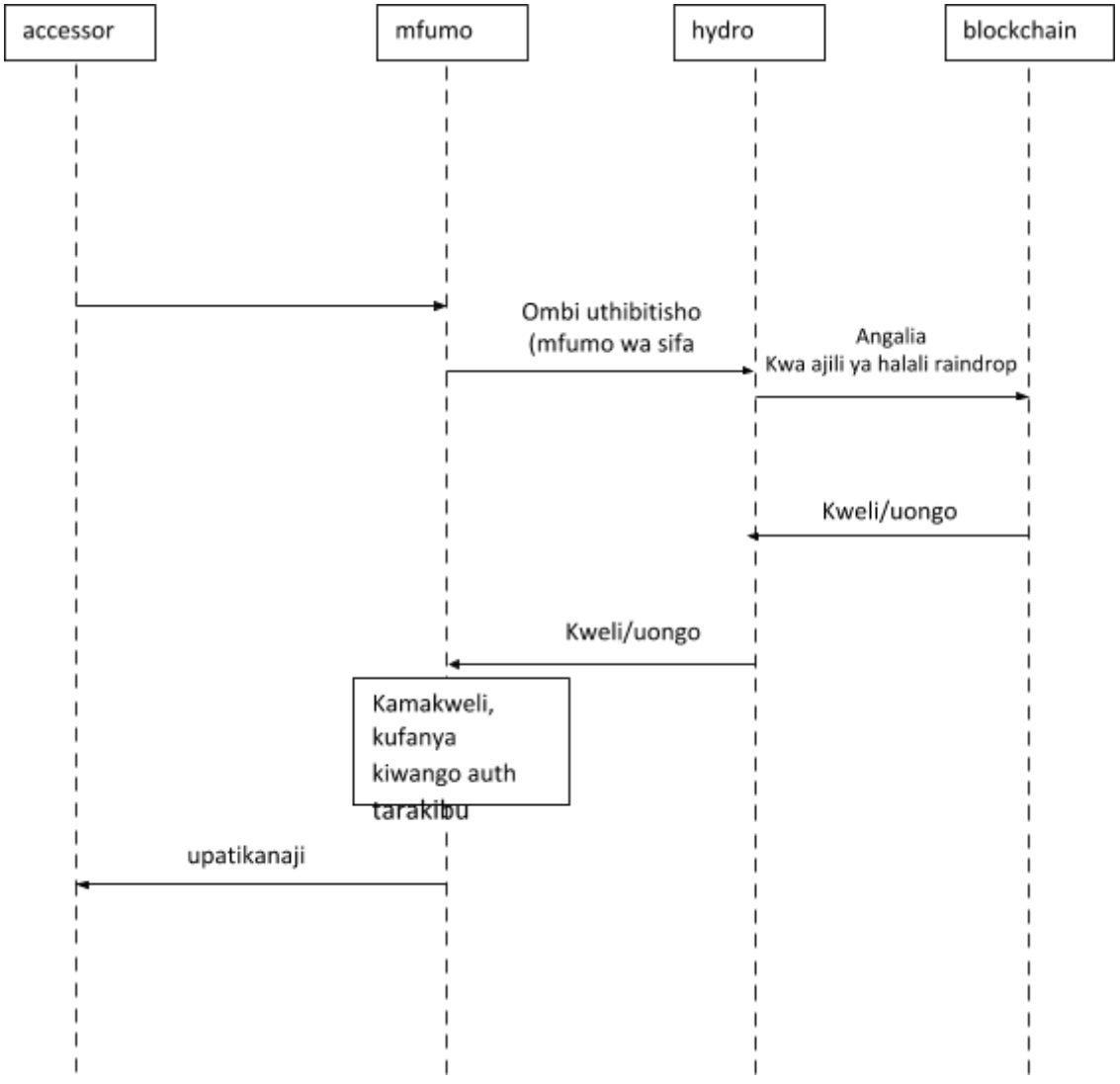
baada initialization ni kamili, msingi wa Hydro uthibitishaji mchakato unaweza kuanza. the accessor, ambaye lazima kutekeleza raindrop mapatano, jumpstarts mchakato huu na kuomba raindrop maelezo kutoka kwenye mfumo, na mfumo wa njia ombi Hydro. Hydro inazalisha mpya raindrop, maduka ya maelezo fulani immutably juu ya blockchain, na anarudi maelezo kamili na accessor kupitia mfumo. the accessor, vifaa na yote required habari, inafanya shughuli kutoka kusajiliwa pepe kwa njia katika Hydro smart mkataba. kama anuani si imeidhinishwa, hatua ni kukataliwa - vinginevyo, ni kumbukumbu katika smart mkataba. ni muhimu kutambua kwamba shughuli hii lazima kutokea nje ya mfumo, moja kwa moja kutoka accessor na blockchain, kama ni lazima saini na accessor ya ufunguo binafsi (ambayo tu accessor wanapaswa kuwa na uwezo wa kupata).

## uthibitishaji na Hydro: raindrop



hatua ya mwisho ya mchakato ni uthibitisho. katika hatua hii, ya accessor rasmi maombi ya upatikanaji wa mfumo kupitia mfumo imara utaratibu. kabla ya kutekeleza yoyote yake kiwango cha uthibitishaji itifaki, mfumo anauliza Hydro kama au ya accessor ina kazi halali raindrop manunuzi. Hydro interfaces na smart mkataba, hundi kwa uhalali na anajibu kwa kweli / uongo wajibu. mfumo ni uwezo wa kuamua jinsi ni lazima kuendelea misingi hii wajibu - kama ni ya uongo, mfumo inaweza kukataa kupata, na kama ni kweli, mfumo inaweza grant kufikia.

uthibitishaji na Hydro: uthibitisho



kama tunaona msingi mfumo sifa - au chochote mfumo uliopo itifaki hiyo ni katika nafasi - ili kwa upana kuwa moja ya sababu ya uthibitishaji, ni muhimu kwamba Hydro safu hutoa muhimu pili sababu. kwa kuchunguza mbili msingi mashambulizi ya wadudu, tunaweza urahisi kuthibitisha matumizi yake:

- vector 1 - mshambuliaji akiiba accessor ya msingi mfumo sifa
    - mshambuliaji majaribio ya kupata huduma ya mfumo na halali mfumo sifa
    - mfumo wa hundi na Hydro kuamua kama halali ya shughuli lilifanywa katika blockchain
    - mshambuliaji cannot kufanya halali blockchain shughuli
- vector 2 - mshambuliaji akiiba ufunguo binafsi (s) na accessor ya Mkoba
    - mshambuliaji majaribio ya kufanya Hydro shughuli kutoka kusajiliwa ya mitaani, bila required raindrop maelezo
    - mshambuliaji cannot kufanya halali blockchain shughuli
    - mshambuliaji pia cannot ombi upatikanaji wa mfumo bila sahihi mfumo sifa

ni wazi kwamba mshambuliaji lazima kuiba wote wa msingi mfumo sifa na accessor binafsi Mkoba muhimu(s) ili kupata mfumo. katika suala hili, Hydro ina mafanikio Aliongeza ziada sababu ya uthibitishaji.

*kufungua raindrop kwa umma*

wakati huu blockchain makao uthibitishaji huduma mara architected kusaidia kupata hidrojeni api ya mazingira, ni sana zinazotumika kwa majukwaa tofauti na mifumo. kwa sababu sisi wanaona kuwa wengine inaweza uwezekano wa kunufaika na ukaguzi huu safu, sisi ni kufungua it up kwa ajili ya matumizi.

kama vile hidrojeni itahusisha kama sharti kwa ajili ya kupata wake api ya mazingira, hivyo pia tunaweza mfumo wowote kuongeza kwa zilizopo taratibu na itifaki. jukwaa yoyote - iwe api, maombi, biashara programu, michezo ya kubahatisha jukwaa, nk - Je, kujiinua umeme wa maji kwa ajili ya uthibitishaji madhumuni. rasmi nyaraka itapatikana kwenye github kwa

wale ambao unataka kuingiza hii blockchain safu ndani ya uthibitishaji mfumo au mapumziko api.

*uchunguzi kifani - raindrop na oauth 2.0*

kuna kadhaa wa njia ya raindrop kutolewa inaweza kutumika na mashirika binafsi. binafsi apis, database, na mitandao tumemuumba kufafanua mifumo ya ishara, funguo, apps na itifaki katika muongo uliopita, katika jaribio la kupata data nyeti. google, kwa mfano, akawa moja ya maarufu bidhaa watoa katika soko na kithibitishaji cha google programu. kama ilivyotajwa hapo awali, ni kidogo kwa hakuna sababu ya kushindana na au nafasi hizi zilizopo itifaki.

kama uchunguzi kifani, hapa ni muhtasari wa jinsi hidrojeni zana Hydro uthibitisho kama usalama safu katika hali yake kwa ujumla api ya usalama wa mfumo:

1. hidrojeni api washirika lazima kwanza kuwa na anwani za ip zao mbalimbali mazingira ya idhini.
2. washirika lazima ombi whitelist umma Hydro ya mahali.
3. wito wote na hidrojeni apis na uhamisho wa data encrypted na kuambukizwa kwa https itifaki.
4. washirika lazima kukamilisha halali Hydro raindrop shughuli kutoka kusajiliwa Hydro ya mahali.
5. washirika lazima kutumia oauth 2.0 uthibitisho. oauth (Open idhini) ni wazi kiwango kwa ishara makao uthibitishaji na idhini. hidrojeni inaunga mkono "rasilimali mmiliki nenosiri sifa" na "mteja sifa" ruzuku ya aina, na kila api mtumiaji lazima kutoa sifa kwa ombi la uthibitisho.
6. kama hakuna Hata mmoja wa mambo ya tano juu zimekiukwa, hidrojeni Mpenzi ni nafasi ya kipekee ishara, kuchunguzwa na kuthibitishwa na kila api ya simu.
7. ishara ni halali kwa masaa 24, ambapo baada ya Mpenzi lazima kuthibitisha wenyewe tena

kama wapo ya hatua hizi ni kukiukwa, mtumiaji ni mara moja imefungwa kutoka kupata api. hacker cannot bypass hizi usalama na sababu na kubahatisha Nasibu, kwa sababu kuna matrilioni ya kipekee mchanganyiko.

Hydro blockchain makao uthibitishaji ni sehemu muhimu ya hidrojeni usalama itifaki. hidrojeni timu inahimiza washirika kuanzisha mbalimbali signature pochi, na kuhifadhi binafsi funguo katika mbalimbali salama locations kujitegemea kutoka nyingine sifa, hivyo hakuna Hata moja hatua ya kushindwa. vizuri kupata mbalimbali signature Mkoba ni si tu vigumu kuiba, lakini kwa umma asili ya blockchain pia inaruhusu kwa swift utambuzi wa yoyote wizi kama inahusiana na usalama wa api.

mtu yeyote anaweza mtazamo wa uthibitishaji jaribio Hydro smart mkataba, ambayo ina maana siku za majukwaa kuwa kuathirika kwa miezi juu-mwisho inaweza kuwa ni kitu cha zamani. api walaghai sasa inaweza kuzuiwa na zaidi immediacy kwa sababu ya uwezo wa kuchunguza zisizotarajiwa idhini majaribio katika muda halisi, kutoka mahali popote duniani.

**Hatari**

kiasi kama yoyote changa ya teknolojia, kama siku za mwanzo za kijamii vyombo vya habari, barua pepe, na Streaming matumizi (ambayo yalikuwa kujitegemea juu piga-up kuunganishwa), ni muhimu kwamba msingi timu ya maendeleo kwa karibu kufuatilia maendeleo mapya katika ethereum shughuli kasi na kiasi. Je, unaweza kufikiria youtube kujaribu kuanzisha mwaka 1995? au instagram kuwa kwanza inayotolewa juu ya blackberry?

msingi ethereum watengenezaji kama vile vitalik buterin Yusufu poon wamependekeza plasma: scalable autonomous smart mikataba ya itifaki ya:

plasma ni mapendekezo ya mfumo wa incentivized na kutekelezwa utekelezaji wa smart mikataba ambayo ni scalable kwa kiasi kikubwa cha hali updates kwa sekunde (uwezekano wa mabilioni) kuwezesha blockchain kuwa na uwezo wa kuwakilisha kiasi kikubwa cha madaraka kifedha maombi duniani kote. hizi smart mikataba incentivized kuendelea operesheni autonomously kupitia mtandao ada ya manunuzi,

ambayo ni hatimaye kujitegemea juu ya msingi blockchain (kwa mfano ethereum) kutekeleza mapatano hali mabadiliko.

wengine, kama vile raiden mtandao, na mapendekezo ya off-mnyororo scaling ufumbuzi iliyoundwa mamlaka kwa kasi zaidi shughuli na chini ada. kwa wakati huu, ya raindrop kuweka ndogo sana mzigo juu ya ethereuem mfumo, na hivyo scalability ni ndogo sana hatari kwa mafanikio ya teknolojia.

**Hitimisho**

faradhi ya umma blockchain inatoa njia mpya za kuimarisha usalama wa kibinafsi mifumo kama apis.

jarida hili umeonyesha tatu mambo muhimu:

1. umma blockchains wanaweza kuongeza thamani katika huduma za kifedha.
2. Hydro raindrop inaweza kuongeza usalama wa kibinafsi System.
3. kuna mara moja maombi ya Hydro raindrop ndani ya hidrojeni api ya jukwaa.

Hydro timu anaamini mfumo umeelezwa inaweza kuwa ya kiwango cha usalama miundombinu kwa ajili ya mtindo mpya wa mseto binafsi-public mifumo, ambayo watafaidika wadau wote katika huduma za kifedha viwanda na nje.

vyanzo:

ethereum: merkling katika ethereum
trend micro, Je, walaghai kufanya na yako kuibiwa utambulisho?
javelin mkakati & utafiti; 2017 utambulisho udanganyifu utafiti
symantec; na internet usalama na tishio ripoti
hatari ya msingi ya usalama, 2016 data uvunjaji mwenendo - mwaka katika mapitio
thales; 2017 thales data tishio ripoti - huduma za kifedha edition
apache.org; apache struts 2 nyaraka - s2-052
Joseph poon na vitalik buterin; plasma: scalable autonomous smart mikataba