हाइड्रो रेनड्रॉप

ब्लाकचेन पर सार्वजनिक प्रमाणीकरण

जनवरी 2018

विषय – सूची

सार

हाइड्रो: एटिमोलॉजी - प्राचीन यूनानी से ὑδρο- (*hudro* -), ὕδωρ (*húdōr*, "पानी") है

हाइड्रो नए और मौजूदा निजी प्रणालियों को आवेदन और दस्तावेज़ सुरक्षा, पहचान प्रबंधन, ट्रांसेकशन, और कृत्रिम बुद्धि को बढ़ाने के लिए सार्वजनिक ब्लाकचेन की अपरिवर्तनीय और पारदर्शी गतिशीलता को सहजता से एकीकृत और लाभ प्रदान करने में सक्षम बनाता है।

इस पत्र में, सार्वजनिक प्रमाणीकरण के माध्यम से सुरक्षा बढ़ाने के लिए हाइड्रो सार्वजनिक ब्लाकचेन का उपयोग करने के लिए API's जैसे निजी सिस्टम के लिए एक स्थिति बनायेगा ।

प्रस्तावित तकनीक को "रेनड्रोप" कहा जाता है - यह एक स्मार्ट कॉन्ट्रैक्ट के माध्यम से किया गया एक ट्रांसेकशन है जो निजी प्रणाली का सार्वजनिक रूप से उपयोग मान्य करता है, और मौजूदा निजी प्रमाणीकरण

विधियों का पूरक हो सकता है। इस तकनीक का उद्देश्य संवेदनशील वित्तीय डेटा के लिए अतिरिक्त सुरक्षा प्रदान करना है जो हैकिंग और उल्लंघनों से जोखिम में तेजी से बढ़ रहा है।

हाइड्रो रेनड्रॉप का प्रारंभिक कार्यान्वयन हाइड्रोजन API प्लेटफॉर्म पर किया गया। API का यह मॉड्यूलर सेट परिष्कृत वित्तीय तकनीकी प्लेटफार्मों और उत्पादों के प्रोटोटाइप, निर्माण, परीक्षण और तैनाती के लिए विश्व स्तर पर उद्यमों और डेवलपर्स के लिए उपलब्ध है।

हाइड्रो रेनड्रॉप दुनिया के डेवलपर समुदाय को ओपन सोर्स सॉफ्टवेयर के रूप में उपलब्ध कराया जाएगा, ताकि डेवलपर्स को किसी भी REST API के साथ हाइड्रो रेनड्रॉप को एकीकृत करने की अनुमति मिल सके।

ब्लाकचेन और एथेरियम

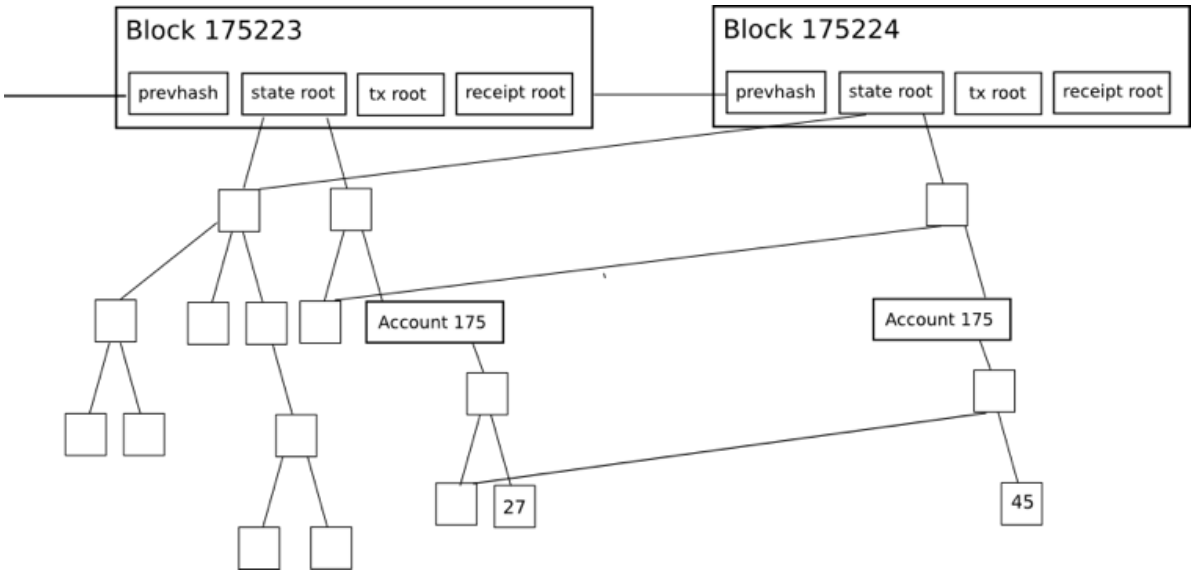
एथेरियम नेटवर्क पर हाइड्रो को लागू किया गया है। परियोजना पर अधिक जानकारी प्रदान करने से पहले, ब्लाकचेन और एथेरियम के बारे में कुछ मौलिक विचारों को समझना महत्वपूर्ण है। एथेरियम पर निर्माण

SNAPCHAT जैसे ऐप्स SWIFT और APPLE IOS प्लेटफार्म के शीर्ष पर पेश किए गए अन्य टूल्स के साथ बनाए गए थे, इसलिए एथेरियम के शीर्ष पर ब्लाकचेन के अनुप्रयोगों को बनाया जा सकता है। SNAP INC. को IOS बनाने की जरूरत नहीं थी, लेकिन उसने इसे गेम-चेंजिंग सोशल मीडिया एप्लिकेशन लॉन्च करने के लिए बुनियादी ढांचे के रूप में इस्तेमाल किया।

इसी समान प्रोजेक्ट हाइड्रो है। यह वैश्विक स्तर पर हजारों डेवलपर्स पर निर्भर करता है जो अवरुद्ध तकनीक को अंतर्निहित, मजबूत और अधिक कुशल बनाने के लिए काम कर रहे हैं। हाइड्रो ब्लाकचेन तकनीक के आसपास उत्पाद-केंद्रित इंटरैक्शन विकसित करके इस लगातार सुधारते बुनियादी ढांचे का लाभ उठाता है जो वित्तीय सेवाओं के अनुप्रयोगों के लिए ठोस लाभ प्रदान कर सकता है।

मर्कल ट्री

कुशल डेटा सत्यापन के लिए वितरित सिस्टम में मर्कल ट्री का उपयोग किया जाता है। वे कुशल हैं क्योंकि वे पूरी फाइलों के बजाय हैश का उपयोग करते हैं। हैश फाइलों को एन्कोड करने के तरीके हैं जो वास्तविक फ़ाइल से बहुत छोटे होते हैं। एथेरियम में प्रत्येक ब्लाक हेडर में लेनदेन, रसीदों और राज्यों के लिए तीन मर्कल ट्री होते हैं:



स्रोत: एथेरियम में मर्कलिंग; Vitalik Buterin, एथेरियम के संस्थापक

यह लाइट क्लाइंट के लिए प्रश्नों के सत्यापन योग्य उत्तर प्राप्त करना आसान बनाता है, जैसे कि:

- क्या यह खाता मौजूद है?
- वर्तमान संतुलन क्या है?
- क्या यह ट्रांसेकशन किसी विशेष ब्लॉक में शामिल किया गया है?
- आज इस एड्रेस में एक विशेष घटना हुई है?

स्मार्ट कॉन्ट्रैक्ट

एथेरियम और अन्य ब्लाकचेन-आधारित नेटवर्क द्वारा सक्षम एक महत्वपूर्ण अवधारणा स्मार्ट कॉन्ट्रैक्ट की है। ये कोड के स्वयं-निष्पादन ब्लाक हैं जिस से कई पार्टियां इंटरैक्ट कर सकती हैं, भरोसेमंद बिचौलियों की जरूरत के बिना । एक स्मार्ट कॉन्ट्रैक्ट के कोड को पारंपरिक पेपर कॉन्ट्रैक्ट में कानूनी खंडों के समान देखा जा सकता है, लेकिन यह अधिक विस्तृत कार्यक्षमता भी प्राप्त कर सकता है। कॉन्ट्रैक्ट में गैर-अनुपालन के लिए नियम, शर्तें, दंड हो सकते हैं, या अन्य प्रक्रियाओं को किकस्टार्ट कर सकते हैं। जब ट्रिगर किया जाये , तो सार्वजनिक श्रृंखला पर तैनाती के समय मूल रूप से शुरू किया गया कॉन्ट्रैक्ट, अपरिवर्तनीयता और विकेन्द्रीकरण के अंतर्निहित तत्वों की पेशकश करता है।

एथेरियम आधारभूत संरचना पर निर्माण के लिए स्मार्ट कॉन्ट्रैक्ट एक महत्वपूर्ण उपकरण है। हाइड्रो ब्लाकचेन परत की कोर कार्यक्षमता कस्टम कॉन्ट्रैक्ट के माध्यम से हासिल की जाती है, जैसा कि इस पेपर के बाद चर्चा की गई है।

एथेरियम वर्चुअल मशीन

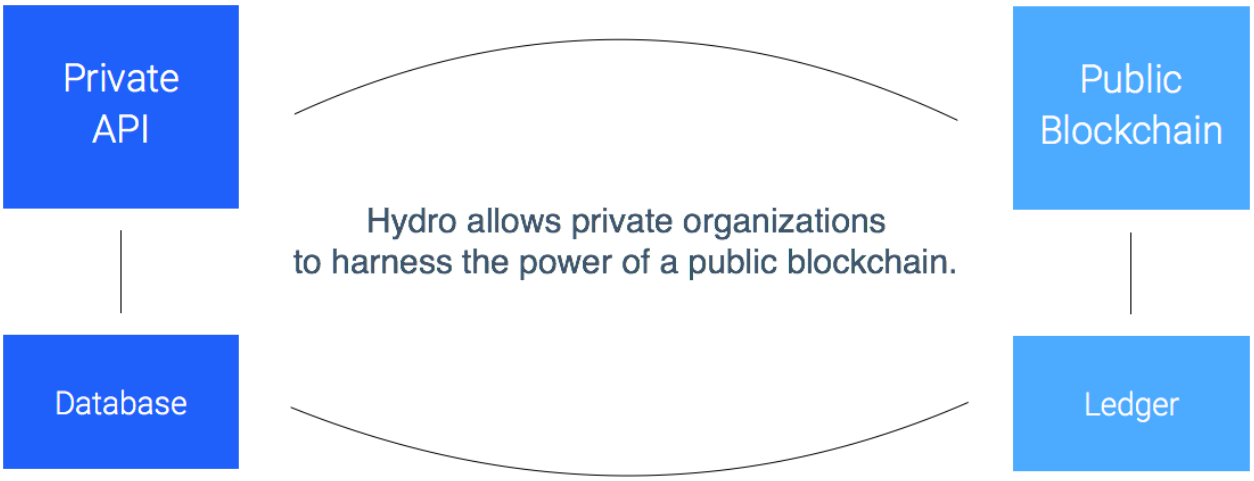
एथेरियम वर्चुअल मशीन (EVM) एथेरियम पर स्मार्ट कॉन्ट्रैक्ट के लिए रनटाइम पर्यावरण है। EVM सेवा अस्वीकार (DOS) हमलों को रोकने में मदद करता है, यह सुनिश्चित करता है कि कार्यक्रम स्टेटलेस बने रहें, और संचार को सक्षम किया जा सके जो बाधित ना हो सके । EVM पर कार्रवाइयों में उनके साथ जुड़ी लागत होती है, जिसे गैस कहा जाता है, जो आवश्यक कम्प्यूटेशनल संसाधनों पर निर्भर करता है। प्रत्येक ट्रांसेकशन में अधिकतम आवंटित गैस होती है, जिसे गैस सीमा के रूप में जाना जाता है। यदि ट्रांसेकशन से खपत गैस सीमा तक पहुंच जाती है, तो यह प्रसंस्करण जारी रखना बंद कर देता है ।

सार्वजनिक लेजर

निजी सिस्टम के लिए एक सार्वजनिक लेजर

सिस्टम जो वित्तीय सेवाओं के प्लेटफार्मों, वेबसाइटों और अनुप्रयोगों को पावर देते हैं उन्हें अक्सर डेटा प्रवाह के माध्यम के रूप में वर्णित किया जा सकता है - वे उन इकाइयों के लिए डेटा भेजते हैं, पुनर्प्राप्त करते हैं, स्टोर करते हैं, अपडेट करते हैं और प्रक्रिया करते हैं। इस डेटा की प्रकृति और वित्तीय सेवाओं की आम तौर पर, ये सिस्टम अक्सर निजी और केंद्रीकृत तरीके से जटिल परिचालन करते हैं। बदले में, निजी संरचनाओं पर रिलायंस आंतरिक प्रणाली की पहुंच से अधिक बाहरी बलों को शामिल करके विभिन्न सुरक्षा, पारदर्शिता और दक्षता लाभ के लिए दरवाजा खोलता है।

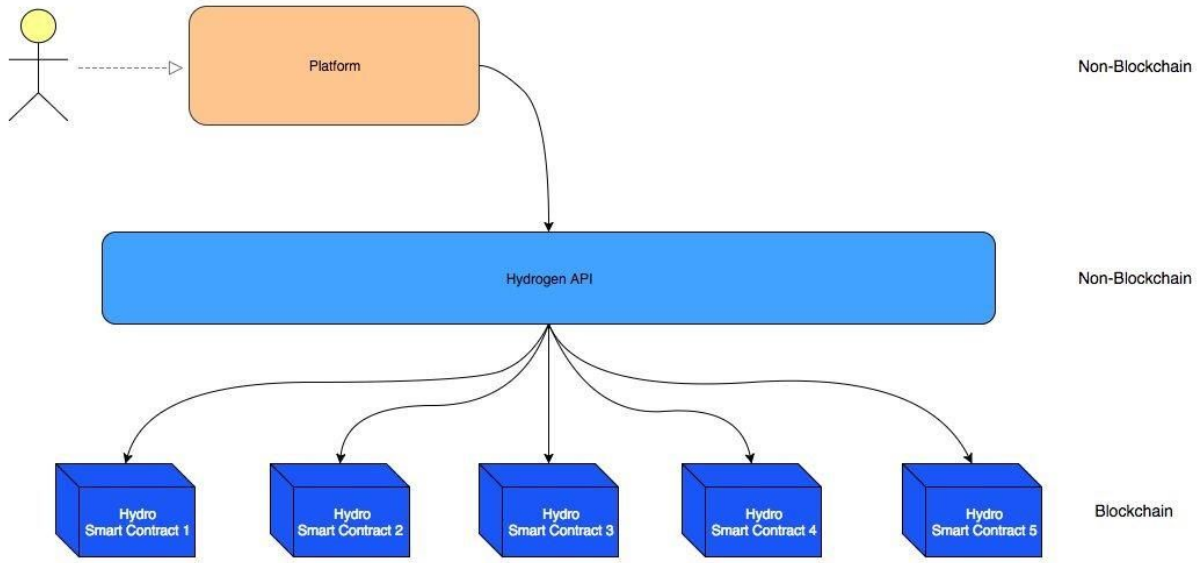
हाइड्रोजन के API प्लेटफ़ॉर्म के साथ ऐसा ही मामला है। हाइड्रो का उद्देश्य हाइड्रोजन उपयोगकर्ताओं को ब्लाकचैन के साथ इंटरफेस कराने के साथ साथ उपरोक्त लाभ उठाना है, जो मौलिक रूप से निजी हाइड्रोजन पारिस्थितिकी तंत्र में एकीकृत हैं।



सार्वजनिक ब्लाकचेन-आधारित संचालन निजी संचालन से पहले, उसके दौरान या उसके बाद हो सकते हैं। निजी और सार्वजनिक तत्वों के बीच अंतःक्रिया एक पारिस्थितिक तंत्र के भीतर प्रक्रियाओं को मान्य, मुद्रित, रिकॉर्ड या बढ़ाने के लिए काम कर सकती है। इस मॉडल का ethos ब्लाकचेन तकनीक के लाभ में टैप करके प्रक्रियाओं को और अधिक मजबूत बना रहा है, विशेष रूप से जहां यह सबसे सकारात्मक प्रभाव पैदा कर सकता है। हालांकि यह हाइब्रिड ढांचा सभी प्लेटफॉर्म पर लागू नहीं हो सकता है, लेकिन हाइड्रो उन मामलों के लिए मूल्य प्रदान करने पर केंद्रित है, जिनमें यह लागू है।

<u>स्वीकृति के लिए वास्तुकला</u>

क्योंकि यह स्वतंत्र रूप से मौजूद हो सकता है और व्यवस्थित परिवर्तन की आवश्यकता के बिना ये नए या मौजूदा सिस्टम के चारों ओर परत की तरह चढ़ सकता है



हाइड्रोजन का लाभ उठाने वाले वित्तीय सेवाओं के प्लेटफॉर्म का दायरा व्यापक है। ये प्लेटफार्म लगभग किसी भी अनुभव को शक्ति दे सकते हैं, मालिकाना सेवाओं की किसी भी संख्या का घर बना सकते हैं, कोई भी निजी डेटा ऑपरेशन कर सकते हैं, और किसी भी पर्यावरण में फ़ैल सकते हैं। प्रतिस्थापित करने

के बजाय, हाइड्रो का लक्ष्य बढ़ाना है। प्लेटफार्म और संस्थान जो हाइड्रोजन API में प्लग करते हैं, स्वचालित रूप से ब्लाकचेन तक पहुंच सकते हैं।

रेनड्रॉप

ये हाइड्रो पब्लिक लेजर के शीर्ष पर बनायी गयी एक ब्लाकचेन-आधारित प्रमाणीकरण सेवा है, जिसे "रेनड्रोप" कहा जाता है। यह सुरक्षा की एक विशिष्ट, अपरिवर्तनीय, वैश्विक रूप से देखने योग्य परत प्रदान करता है जो यह सत्यापित करता है कि एक अधिकृत स्रोत से एक एक्सेस अनुरोध आ रहा है।

OAuth 2.0 जैसे निजी प्रमाणीकरण प्रोटोकॉल मौजूदा मामलों के स्पेक्ट्रम के लिए मजबूती और उपयोगिता के विभिन्न स्तर प्रदान करते हैं। इन प्रोटोकॉल को प्रतिस्थापित करने या बदलने की कोशिश करने की बहुत कम आवश्यकता है - हाइड्रो एक प्रमाणीकरण प्रक्रिया के घटक के रूप में ब्लाकचेन यांत्रिकी को शामिल करके उन्हें बढ़ाने का एक तरीका प्रदान करता है। यह सिस्टम उल्लंघनों और डेटा समझौता को विफल करने में मदद के लिए सुरक्षा की एक उपयोगी परत जोड़ सकता है।

रेनड्रॉप के तकनीकी पहलुओं की जांच करने से पहले, आइए पहले उन समस्याओं को देखें जिन्हें ये हल करने का प्रयास कर रहा है। *वित्तीय सुरक्षा राज्य*

डेटा युग मे उदय, अपन साथ भेद्यता में वृद्धि लाया है , और यह वित्तीय सेवाओं के लिए विशेष रूप से महत्वपूर्ण है। वित्तीय प्लेटफार्म अक्सर सरकारी आईडी नंबर, खाता प्रमाण-पत्र और लेन-देन इतिहास जैसे निजी और संवेदनशील डेटा की बड़ी मात्रा के प्रवेश द्वार होते हैं। क्योंकि ये डेटा गंभीर रूप से महत्वपूर्ण होते है, इसलिए अनचाहे एक्सेस आम तौर पर विनाशकारी परिणाम लाते है।

इंडस्ट्री रिसर्च फर्म Trend Micro ने एक रिपोर्ट प्रकाशित की जिसमें व्यक्तिगत रूप से पहचाने जाने योग्य सूचना (PII) की चोरी लाइन वस्तुओं को $1 के रूप में DEEP WEB पर बेचा जाता है, पासपोर्ट जैसे दस्तावेज़ों के स्कैन को $10 जितना कम मे और बैंक लॉगिन प्रमाण-पत्र सिर्फ $200 मे उपलब्ध हैं ।चुराए गए डेटा का वितरण तेजी से खंडित और ना पता लगाने योग्य बन जाता हैं ।

दुर्भाग्यवश, जब मौजूदा हितधारकों के साथ डेटा उल्लंघनों को रोकने, निदान करने और संचार करने की बात आती है तो मौजूदा वित्तीय प्रणाली का ट्रैक रिकॉर्ड स्वच्छ नहीं है।

- Javelin Strategy & Research द्वारा हाल के एक अध्ययन के मुताबिक - 2017 पहचान धोखाधड़ी अध्ययन - व्यक्तिगत रूप से पहचाने जाने योग्य सूचना (PII) की रक्षा के लिए वित्तीय प्रणाली की विफलताओं के कारण 2016 में 15.4 मिलियन अमरीकी उपभोक्ताओं से $ 16 बिलियन चोरी किया गया था।

- अप्रैल 2017 में, Symantec ने अपनी इंटरनेट सुरक्षा धमकी रिपोर्ट प्रकाशित की, जिसका अनुमान है कि 2016 के दौरान विभिन्न क्षमताओं में 1.1 अरब PII के टुकड़े जोखिम मे थे।
- 2016 के अंत में *Data Breach Quickview* जोखिम आधारित सुरक्षा द्वारा पाया गया कि 2016 में दुनिया भर में कारोबार में 4,149 डेटा उल्लंघनों का आयोजन हुआ, जिसमे 4.2 बिलियन से अधिक रिकॉर्ड एक्सपोस हुए ।
- 2017 थाल्स डेटा धमकी रिपोर्ट - पेशेवर सेवाओं में वैश्विक IT पेशेवरों के एक सर्वेक्षण में वित्तीय सेवा संस्करण ने पाया कि 49% वित्तीय सेवा संगठनों को अतीत में सुरक्षा उल्लंघन का सामना करना पड़ा है, 78% खुद को बचाने के लिए और अधिक खर्च कर रहे हैं, लेकिन 73% उचित सुरक्षा समाधान तैयार करने से पहले AI, IoT, और cloud technologies से संबंधित नई पहल शुरू कर रहे हैं।

Equifax उल्लंघन

29 जुलाई 2017 को, 118 वर्षीय अमेरिकी क्रेडिट रिपोर्टिंग एजेंसी Equifax को हैक किया गया था। सामाजिक सुरक्षा संख्या सहित 143 मिलियन उपभोक्ताओं की PII एक्स्पोसे हुई । 209, 000 ग्राहकों का क्रेडिट कार्ड डेटा जोखिम मे था।

इस उल्लंघन का कारण क्या था?

यह Equifax द्वारा उपयोग की जाने वाली बैकएंड तकनीकों में से एक के साथ शुरू हुई । Struts जावा प्रोग्रामिंग भाषा में वेब अनुप्रयोगों के विकास के लिए एक ओपन सोर्स फ्रेमवर्क है, जिसे अपाचे सॉफ्टवेयर फाउंडेशन द्वारा बनाया गया है। XML पेलोड को संभालने के लिए XStream handler के साथ Struts REST प्लगइन का उपयोग करने से संबंधित Apache Struts में CVE-2017-9805 एक भेद्यता है। यदि शोषण किया जाता है, तो यह एक दूरस्थ अनधिकृत हमलावर को एप्लिकेशन सर्वर पर दुर्भावनापूर्ण कोड चलाने के लिए या तो मशीन पर ले जाने या उससे आगे के हमलों को लॉन्च करने की अनुमति देता है। यह Equifax उल्लंघन से दो महीने पहले अपाचे द्वारा पैच किया गया था।

Apache Struts में REST प्लगइन XStream में एक दोष होता है जो प्रोग्राम को अनिवार्य रूप से XML अनुरोधों में उपयोगकर्ता द्वारा आपूर्ति किए गए इनपुट को डी-सीरियलाइज करता है। विशेष रूप से, समस्या XStreamHandler की toObject () विधि में होती है, जो किसी ऑब्जेक्ट में XStream deserialization का उपयोग करते समय आने वाले मान पर किसी भी प्रतिबंध को लागू नहीं करती है, जिसके परिणामस्वरूप मनमाने ढंग से कोड निष्पादन में भेद्यता होती है।

यहां तक कि अगर इस REST प्लगइन से समझौता किया गया था, तो क्या यह महत्व रखता है ?

क्या इन 143 मिलियन ग्राहकों की वित्तीय जानकारी को सुरक्षित रखने के लिए ब्लाकचैन तकनीक का उपयोग करने का कोई तरीका है, पहले से मौजूदा REST API और जावा-आधारित सिस्टम पर निर्भर रहकर ?

एक ब्लाकचेन परत जोड़ना

यह स्पष्ट है कि वित्तीय डेटा गेटवे की अखंडता में सुधार किया जा सकता है। आइए देखें कि हाइड्रो के माध्यम से सुरक्षा की एक अतिरिक्त परत कैसे प्राप्त की जाती है।

एथेरियम नेटवर्क मौलिक सर्वसम्मति तंत्र मे ट्रांसेकशन की वैधता सुनिश्चित करता है क्योंकि प्रतिभागी सामूहिक रूप से उन ट्रांसेकशन को संसाधित करते हैं जो उचित रूप से हस्ताक्षरित हैं। यह वास्तविकता विकेन्द्रीकरण और अपरिवर्तनीयता की ओर ले जाती है, लेकिन, सबसे महत्वपूर्ण बात यह है कि यह एक गेटवे तक अनधिकृत पहुंच को कम करने के लिए एक वेक्टर प्रदान करता है जो संवेदनशील डेटा को संभालता है।

हाइड्रो के साथ, ब्लाकचेन पर ट्रांसेकशन संबंधी संचालन पर प्रमाणीकरण की भविष्यवाणी की जा सकती है। एक API, उदाहरण के लिए, विशेष प्रमाणीकरण प्रोटोकॉल को किकस्टार्ट करने वाली पूर्व कंडीशन के रूप में,ब्लाकचैन पर विशेष एड्रेस के बीच विशेष डेटा पेलोड के साथ विशेष ट्रांसेकशन शुरू करने के लिए डेवलपर्स और एप्लिकेशन को सत्यापित करने के लिए चुन सकती हैं।

हाइड्रो रेनड्रॉप

वर्षा में 0.0001 से 0.005 सेंटीमीटर व्यास तक घनत्व वाले पानी के पैकेट होते हैं।एक सामान्य बारिश के तूफान में, ऐसे अरबों पैकेट होते हैं, प्रत्येक यादृच्छिक आकार, गति, और रूप के । इसके कारण, कोई भी बारिश की सटीक प्रकृति की भरोसेमंद भविष्यवाणी नहीं कर सकता है। इसी प्रकार, हर हाइड्रो प्रमाणीकरण ट्रांसेकशन अलग और मौके से होने के लिए लगभग असंभव है - यही कारण है कि हम उन्हें रेनड्रॉप कहते हैं।

वित्तीय सेवा प्लेटफार्म आमतौर पर ग्राहक खातों को प्रमाणित करने के लिए माइक्रो-जमा सत्यापन का उपयोग करते हैं। यह विचार सरल है: मंच उपयोगकर्ताओं द्वारा दावा किए गए बैंक खातों में छोटी यादृच्छिक रकम को जमा करता है। यह साबित करने के लिए की उपयोगकर्ता द्वारा दिए गये खाते का वही स्वामी है , उसे जमा राशि को मंच पर वापस रिले करना होगा, जिसे तब वेलीडेट किया जाता है। केवल एकमात्र तरीका है जिस से उपयोगकर्ता वैध मात्रा (अनुमान लगाने के अलावा) को जान सकता है, उस बैंक खाते को एक्सेस करके जिसकी बात हो रही है ।

हाइड्रो के साथ रेनड्रोप-आधारित सत्यापन समरूप है। उपयोगकर्ता को एक राशि भेजने और इसे वापस रिले करने की बजाय, हम एक ट्रांसेकशन को परिभाषित करते हैं और उपयोगकर्ता को इसे ज्ञात वॉलेट से निष्पादित करना होगा। सिर्फ तभी उपयोगकर्ता एक वैध ट्रांसेकशन कर सकता है अगर वह उस वॉलेट एक्सेस कर सके जिसकी बात हो री है ।

रेनड्रॉप का उपयोग करके, सिस्टम और एक्सेसर दोनों एक अपरिवर्तनीय सार्वजनिक खाताधारक पर प्राधिकरण प्रयासों की निगरानी कर सकते हैं। यह ब्लाकचेन-आधारित ट्रांसेकशन मूल प्रणाली संचालन से निकलता है, वितरित नेटवर्क पर होता है, और निजी कुंजी के स्वामित्व पर निर्भर करता है। अतः यह एक उपयोगी वेलीडेशन वेक्टर के रूप में कार्य करता है।

एक विस्तृत द्रष्टि

हाइड्रो प्रमाणीकरण प्रक्रिया में शामिल चार इकाइयां हैं:

1. *एक्सेसर* - एक पार्टी जो सिस्टम को एक्सेस करने का प्रयास करती है। हाइड्रोजन के मामले में, एक्सेसर एक वित्तीय संस्था या ऐप है जो इसके मूल डिजिटल आधारभूत संरचना के लिए हाइड्रोजन API का उपयोग करता है।
2. *सिस्टम* - सिस्टम या गेटवे जिसे एक्सेसर द्वारा एक्सेस किया जा रहा है। हाइड्रोजन के लिए, प्रणाली ही हाइड्रोजन API है।
3. *हाइड्रो* - मॉड्यूल जिसका उपयोग सिस्टम द्वारा ब्लॉकचैन के साथ संवाद करने और इंटरफेस करने के लिए किया जाता है।
4. *ब्लाकचेन* - वितरित सार्वजनिक खाताधारक जो हाइड्रो के ट्रांसेकशन को संसाधित करता है और इसमें हाइड्रो स्मार्ट कॉन्ट्रैक्ट होते हैं, जिसके माध्यम से जानकारी को भेजा, लिया जा सकता है, या अन्यथा संचालित किया जा सकता है।

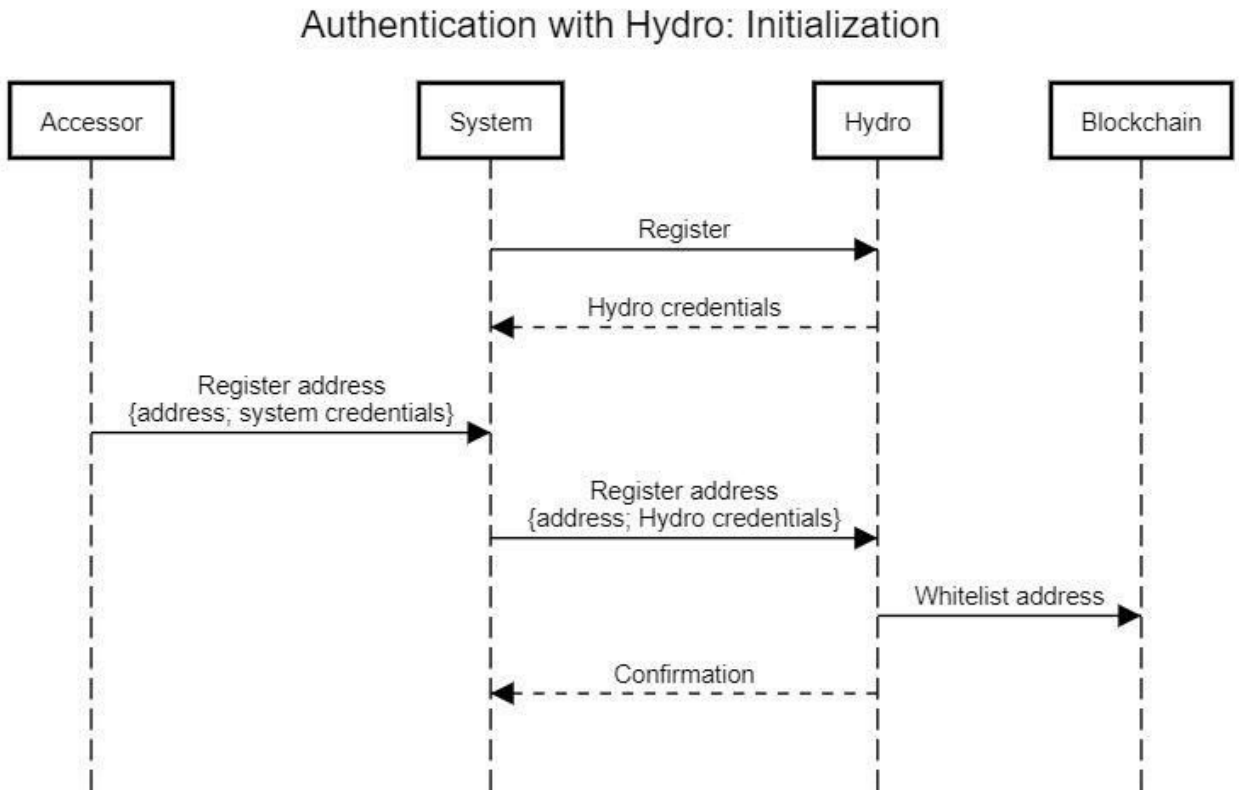
प्रत्येक रेनड्रॉप, पूरी तरह से, पांच ट्रांसेकशन मानकों का एक सेट है:

1. *भेजनेवाला* - वह एड्रेस जिसे ट्रांसेकशन शुरू करना होगा।
2. *पानेवाला* - ट्रांसेकशन का लक्ष्य। यह हाइड्रो स्मार्ट कॉन्ट्रैक्ट में एक विधि को पेश करने के अनुरूप है।
3. *आईडी* - एक पहचानकर्ता जो सिस्टम से जुड़ा हुआ है।
4. *मात्रा* - भेजने के लिए हाइड्रो की एक सटीक संख्या।
5. *चुनौती* - एक यादृच्छिक रूप से जेनरेट की गई अल्फान्यूमेरिक स्ट्रिंग।

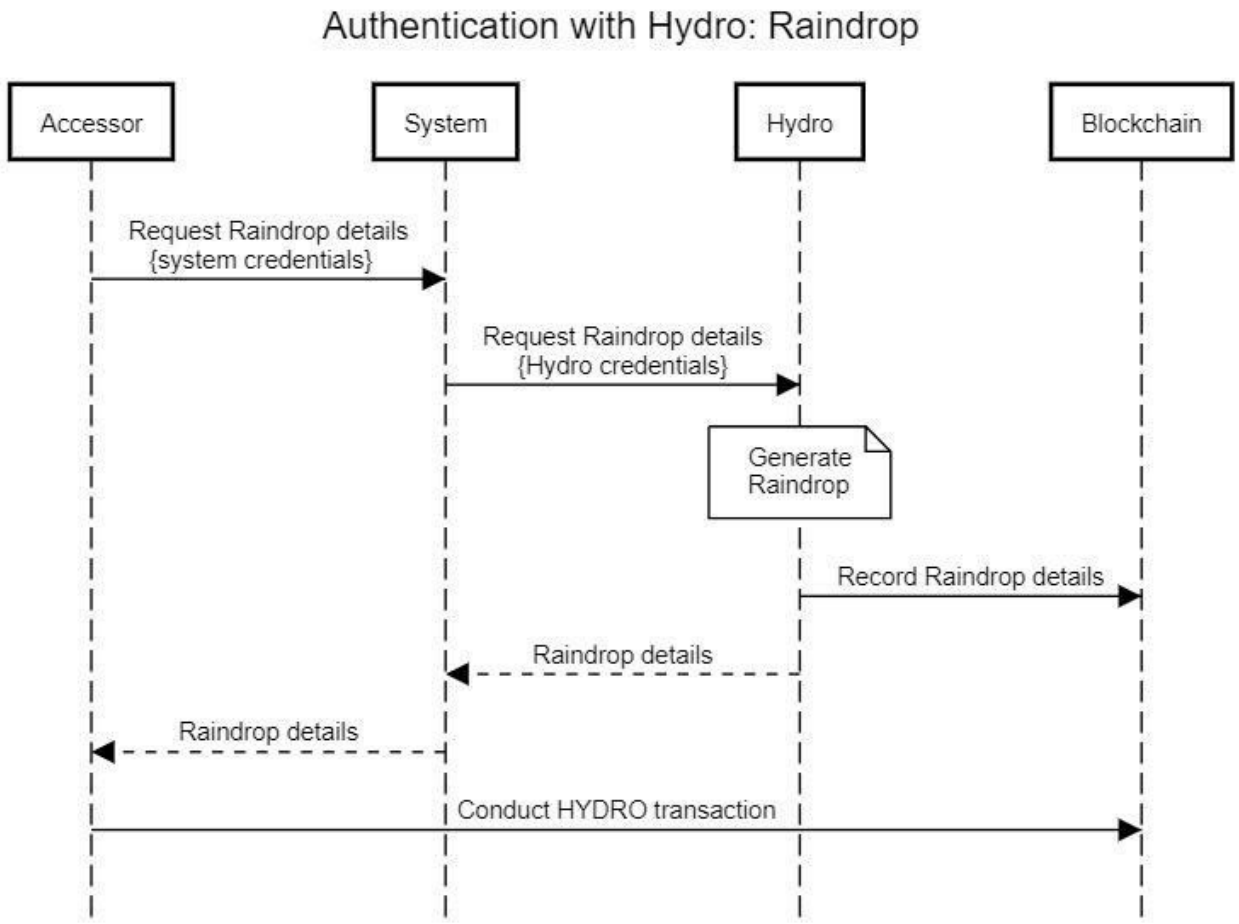
नीचे प्रमाणीकरण प्रक्रिया की एक रूपरेखा है, जिसे आम तौर पर तीन चरणों में वर्गीकृत किया जा सकता है:

1. प्रारंभ
2. रेनड्राप
3. वैलीडेशन

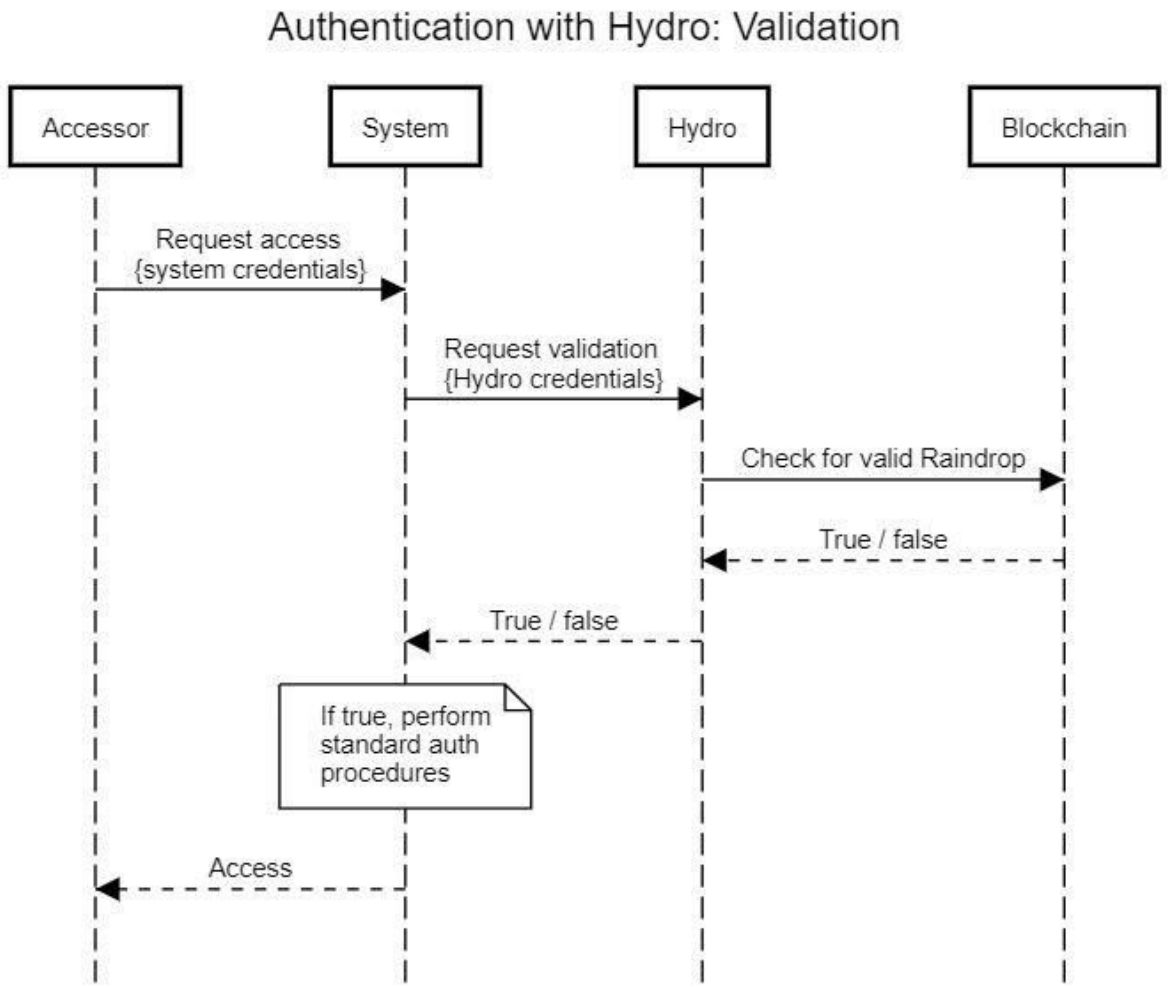
शुरुआत एक सिस्टम (जैसे हाइड्रोजन) के साथ शुरू होती है जो हाइड्रो का उपयोग करने और प्रमाण-पत्र प्राप्त करने के लिए पंजीकरण करती है, जिससे वह प्रणाली हाइड्रो मॉड्यूल के माध्यम से ब्लाकचेन के साथ संवाद करने में सक्षम होती है। सिस्टम एक एक्सेसर को ऑनबोर्ड (उदाहरण के लिए एक वित्तीय संस्थान) जो सार्वजनिक पते पंजीकृत करता है, और उसके बाद पंजीकृत एड्रेस हाइड्रो को पास करता है। यह पता एक हाइड्रो स्मार्ट कॉन्ट्रैक्ट में संग्रहीत वाइटलिस्ट में ब्लाकचेन पर अपरिवर्तनीय रूप से लिखा गया है। सिस्टम को एक पुष्टिकरण प्राप्त होता है कि यह पता वाइटलिस्ट किया गया था, जिसे सार्वजनिक रूप से देखने योग्य ईवेंट के रूप में भी सत्यापित किया जा सकता है। सिस्टम पंजीकरण केवल एक बार होता है, जबकि एक्सेसर वाइटलिस्ट प्रति एक्सेसर के आधार पर होती है।



प्रारंभिकरण पूरा होने के बाद, हाइड्रो प्रमाणीकरण प्रक्रिया का मूल शुरू हो सकता है। एक्सेसर, जिसे रेनड्रॉप ट्रांसेकशन को निष्पादित ज़रूर करना होगा, सिस्टम से रेनड्रॉप विवरण का अनुरोध करके इस प्रक्रिया को जंपस्टार्ट करता है, और सिस्टम अनुरोध हाइड्रो को रूट करता है। हाइड्रो एक नया रेनड्रोप उत्पन्न करता है, ब्लाकचेन पर अप्रत्याशित रूप से कुछ विवरण स्टोर करता है, और सिस्टम के माध्यम से एक्सेसर को पूरा विवरण देता है। सभी आवश्यक जानकारी से लैस एक्सेसर, पंजीकृत एड्रेस से एक ट्रांसेकशन को हाइड्रो स्मार्ट कॉन्ट्रैक्ट की एक विधि में आयोजित करता है। अगर एड्रेस वाइटलिस्ट नहीं है, तो कार्रवाई को खारिज कर दिया जाता है - अन्यथा, यह स्मार्ट कॉन्ट्रैक्ट में दर्ज किया जाता है। यह ध्यान रखना महत्वपूर्ण है कि यह ट्रांसेकशन सिस्टम के बाहर सीधे एक्सेसर से ब्लाकचेन तक होना चाहिए, क्योंकि इसे एक्सेसर की निजी कुंजी (जिसे केवल एक्सेसर प्राप्त करने में सक्षम हो) के साथ हस्ताक्षरित होना चाहिए।



प्रक्रिया का अंतिम चरण वैलीडेशन है। इस चरण में, एक्सेसर आधिकारिक तौर पर सिस्टम के स्थापित तंत्र के माध्यम से सिस्टम एक्सेस का अनुरोध करता है। अपने किसी मानक प्रमाणीकरण प्रोटोकॉल को लागू करने से पहले, सिस्टम हाइड्रो से पूछता है कि क्या एक्सेसर ने वैध रेनड्रॉप ट्रांसेकशन किया है या नहीं। स्मार्ट कॉन्ट्रैक्ट के साथ हाइड्रो इंटरफेस, वैधता के लिए जांच करता है, और एक सच्चे / झूठे पदनाम के साथ प्रतिक्रिया करता है। सिस्टम यह तय करने में सक्षम है कि इसे इस पदनाम के आधार पर कैसे एक्सेस देना चाहिए - यदि यह गलत है, तो सिस्टम एक्सेस से इनकार कर सकता है, और यदि यह सत्य है, तो सिस्टम एक्सेस प्रदान कर सकता है।



यदि हम आधार सिस्टम प्रमाण-पत्रों पर विचार करते हैं - या जो भी मौजूदा सिस्टम प्रोटोकॉल है, जो व्यापक रूप से प्रमाणीकरण का एक कारक है, तो यह महत्वपूर्ण है कि हाइड्रो की परत एक उपयोगी दूसरा कारक प्रदान करे। दो प्राथमिक वैक्टर हमलों की जांच करके, हम इसकी उपयोगिता की आसानी से पुष्टि कर सकते हैं:

- वेक्टर 1 - अटैकर एक्सेसर के आधार सिस्टम प्रमाण-पत्र चुराता है
    - अटैकर वैध सिस्टम प्रमाण-पत्रों के साथ सिस्टम तक पहुंच प्राप्त करने का प्रयास करता है
    - यह निर्धारित करने के लिए कि ब्लाकचेन पर वैध ट्रांसेकशन किया गया है, सिस्टम हाइड्रो के साथ जांच करता है
    - हाइड्रो झूठा रिटर्न देता है, और सिस्टम पहुंच से इनकार करता है
- वेक्टर 2 - अटैकर एक्सेसर के वॉलेट की निजी कुंजी चुरा लेता है
    - अटैकर पंजीकृत रेनड्रॉप विवरण के बिना पंजीकृत एड्रेस से हाइड्रो ट्रांसेकशन करने का प्रयास करता है
    - अटैकर वैध ब्लाकचेन ट्रांसेकशन नहीं कर सकता है

- अटैकर उचित सिस्टम प्रमाण-पत्र के बिना सिस्टम एक्सेस का भी अनुरोध नहीं कर सकता है

यह स्पष्ट है कि सिस्टम एक्सेस के लिए अटैकर को मूल सिस्टम प्रमाण-पत्र और एक्सेसर की निजी वॉलेट कुंजी दोनों को चुराने पड़ेंगे । इस संबंध में, हाइड्रो ने सफलतापूर्वक प्रमाणीकरण का एक अतिरिक्त कारक जोड़ा है।

जनता के लिए रेनड्रॉप खोलना

हालांकि इस ब्लाकचेन-आधारित प्रमाणीकरण सेवा को हाइड्रोजन API इकोसिस्टम को सुरक्षित रखने में मदद के लिए आर्किटेक्टेड किया गया था, यह विभिन्न प्लेटफार्मों और प्रणालियों पर व्यापक रूप से लागू होता है। क्योंकि हम महसूस करते हैं कि अन्य लोग इस सत्यापन परत से संभावित रूप से लाभ उठा सकते हैं, हम इसे उपयोग के लिए खोल रहे हैं।

जैसे ही हाइड्रोजन इसे अपने API इकोसिस्टम तक पहुंच के लिए पूर्व कंडीशन के रूप में एकीकृत करेगा, वैसे ही कोई भी प्रणाली मौजूदा प्रक्रियाओं और प्रोटोकॉल में जोड़ सकती है। कोई भी मंच - चाहे वह एक API, एप्लिकेशन, एंटरप्राइज़ सॉफ्टवेयर, गेमिंग प्लेटफॉर्म इत्यादि हो - प्रमाणीकरण उद्देश्यों के लिए हाइड्रो का लाभ उठा सकता है। औपचारिक दस्तावेज उन लोगों के लिए GitHub पर उपलब्ध होंगे जो इस ब्लाकचेन परत को प्रमाणीकरण ढांचे या REST API में शामिल करना चाहते हैं।

केस स्टडी - OAuth 2.0 के साथ रेनड्रॉप

निजी संगठनों द्वारा रेनड्रॉप रिलीज का उपयोग कई तरीकों से किया जा सकता है। संवेदनशील डेटा सुरक्षित करने के प्रयास में, निजी API, डेटाबेस और नेटवर्क ने पिछले दशक में टोकन, कुंजियो, ऐप्स और प्रोटोकॉल की विस्तृत प्रणाली बनाई है। गूगल,उदाहरण के लिए, गूगल Authenticator एप के साथ बाज़ार में सबसे लोकप्रिय उत्पाद प्रदाताओं में से एक बन गया। जैसा कि पहले उल्लेख किया गया है, इन मौजूदा प्रोटोकॉल के साथ प्रतिस्पर्धा करने या बदलने के लिए कोई कारण नहीं है।

एक केस स्टडी के रूप में, यहां एक संक्षिप्त अवलोकन है कि कैसे हाइड्रोजन हाइड्रो Authentication को अपने समग्र API सुरक्षा ढांचे में सुरक्षा परत के रूप में लागू करता है:

1. हाइड्रोजन API भागीदारों के पास पहले अपने विभिन्न वातावरण के IP एड्रेस वाइटलिस्ट करना होगा ।
2. साझेदारों को सार्वजनिक हाइड्रो एड्रेस को वाइटलिस्ट में डालने का अनुरोध करना होगा ।
3. हाइड्रोजन API और डेटा के स्थानान्तरण के लिए सभी कॉल एन्क्रिप्टेड हैं और HTTPS प्रोटोकॉल के माध्यम से प्रेषित हैं।
4. भागीदारों को पंजीकृत हाइड्रो एड्रेस से एक वैध हाइड्रो रेनड्रॉप ट्रांसेकशन पूरा करना होगा।
5. भागीदारों को OAuth 2.0 वैलीडेशन का उपयोग करना होगा। OAuth (ओपन प्रमाणीकरण) टोकन-आधारित authentication और प्रमाणीकरण के लिए एक खुला मानक है। हाइड्रोजन "संसाधन मालिक पासवर्ड प्रमाण पत्र" और "ग्राहक का समर्थन करता है
प्रमाण पत्र" अनुदान प्रकार, और प्रत्येक API उपयोगकर्ता को authentication अनुरोध के लिए प्रमाण-पत्र प्रदान करना होगा।
6. यदि ऊपर दिए गए पांच तत्वों में से कोई भी उल्लंघन नहीं किया जाता है, तो हाइड्रोजन साझेदारों को एक अद्वितीय टोकन दिया जाता है, जिसे प्रत्येक API कॉल के साथ चेक और सत्यापित किया जाता है।
7. टोकन 24 घंटों के लिए मान्य है, जिसके बाद साझेदार को खुद को फिर से वैलीडेट करना होगा।

यदि इनमें से किसी भी चरण का उल्लंघन किया जाता है, तो उपयोगकर्ता को तुरंत API एक्सेस से लॉक कर दिया जाता है। एक हैकर यादृच्छिक रूप से अनुमान लगाकर इन सुरक्षा कारकों को बाईपास नहीं कर सकता है, क्योंकि अनोखे संयोजन ट्रिलियन हैं।

हाइड्रो ब्लाकचेन-आधारित authentication हाइड्रोजन सुरक्षा प्रोटोकॉल का एक महत्वपूर्ण घटक है। हाइड्रोजन टीम भागीदारों को बहु-हस्ताक्षर वाले वालेट स्थापित करने के लिए प्रोत्साहित करती है, और अन्य क्रेडेंशियल्स से स्वतंत्र रूप से कई सुरक्षित स्थानों में निजी कुंजी स्टोर करने को कहती है, ताकि विफलता के लिए कोई भी स्थान ना रहे । एक उचित सुरक्षित बहु-हस्ताक्षर वॉलेट को चोरी करना मुश्किल नहीं है, लेकिन ब्लाकचेन की सार्वजनिक प्रकृति किसी भी चोरी की त्वरित पहचान के लिए भी अनुमति देती है क्योंकि यह API की सुरक्षा से संबंधित है।
जिसका मतलब है कि महीनों तक प्लेटफार्म जो जोखिम मे रहते थे वे दिन अब , अतीत की बात हो सकती है। API हैकर्स को अब दुनिया में कहीं से भी, वास्तविक समय में अप्रत्याशित प्राधिकरण प्रयासों का पता लगाने की क्षमता के कारण अधिक तत्कालता से विफल किया जा सकता हैं।

जोखिम

सोशल मीडिया, ईमेल और स्ट्रीमिंग एप्लिकेशन (जो डायल-अप कनेक्टिविटी पर निर्भर थे) के शुरुआती दिनों जैसे किसी भी नवजात तकनीक की तरह, यह महत्वपूर्ण है कि कोर डेवलपमेंट टीम एथेरियम ट्रांसेकशन की गति और वॉल्यूम में नए विकास को बारीकी से ट्रैक करे। क्या आप कल्पना कर सकते हैं कि YouTube ने 1995 में लॉन्च करने का प्रयास किया था? या Instagram पहली बार ब्लैकबेरी पर पेश किया जा रहा था ?

कोर एथेरियम डेवलपर्स जैसे कि Vitalik Buterin और Joseph Poon ने प्लाज्मा का प्रस्ताव दिया है: स्केलेबल स्वायत्त स्मार्ट कॉन्ट्रैक्ट एथेरियम प्रोटोकॉल में अपग्रेड करते हैं:

> प्लाज़्मा स्मार्ट कोन्त्रक्टों के प्रोत्साहन और लागू निष्पादन के लिए एक प्रस्तावित रूपरेखा है जो प्रति सेकंड (संभावित अरबों) के स्टेट अपडेटों की महत्वपूर्ण मात्रा के लिए स्केलेबल है, जिससे ब्लाकचेन दुनिया भर में विकेन्द्रीकृत वित्तीय अनुप्रयोगों की एक महत्वपूर्ण मात्रा का प्रतिनिधित्व करने में सक्षम हो सके। इन स्मार्ट कोन्त्रक्टों को नेटवर्क ट्रांसेकशन शुल्क के माध्यम से स्वायत्तता से संचालन जारी रखने के लिए प्रोत्साहित किया जाता है, जो अंततः ट्रांसेकशन संबंधी स्टेट संक्रमणों को लागू करने के लिए अंतर्निहित ब्लाकचेन (उदाहरण: एथेरियम) पर निर्भर करता है।

अन्य, जैसे कि Raiden नेटवर्क, ने ऑफ-चेन स्केलिंग समाधान का प्रस्ताव दिया है जो तेज ट्रांसेकशन और कम शुल्क को पावर करने के लिए डिज़ाइन किया गया है। इस समय, रेनड्रॉप एथेरियम फ्रेमवर्क पर बहुत ही कम तनाव डालेगा, अतः स्केलेबिलिटी तकनीक की सफलता के लिए एक बहुत ही छोटा जोखिम है।

निष्कर्ष

सार्वजनिक ब्लाकचेन की अपरिवर्तनीयता API जैसे निजी सिस्टम की सुरक्षा बढ़ाने के नए तरीके प्रदान करती है।

इस पेपर में तीन महत्वपूर्ण चीजें दिखायी हैं:

1. सार्वजनिक ब्लाकचेन वित्तीय सेवाओं में मूल्य जोड़ सकती हैं।
2. हाइड्रो रेनड्रॉप निजी प्रणालियों की सुरक्षा को बढ़ा सकता है।
3. हाइड्रोजन API मंच के भीतर हाइड्रो रेनड्रॉप का तत्काल अनुप्रयोग हैं।

हाइड्रो टीम का मानना है कि निर्धारित ढांचा हाइब्रिड प्राइवेट-पब्लिक सिस्टम के नए मॉडल के लिए मानक सुरक्षा आधारभूत संरचना हो सकता है, जो वित्तीय सेवाओं उद्योग और उससे बाहर के सभी हितधारकों को लाभान्वित करेगा।

सूत्र :

एथेरियम; एथेरियम में मर्कलिंग

Trend Micro; हैकर्स आपकी चोरी की पहचान के साथ क्या करते हैं?

Javelin Strategy & Research; 2017 पहचान धोखाधड़ी अध्ययन

Symantec; इंटरनेट सुरक्षा धमकी रिपोर्ट

Risk Based Security; 2016 डेटा उल्लंघन रुझान - वर्ष में समीक्षा

Thales; 2017 Thales डेटा धमकी रिपोर्ट-वित्तीय सेवा संस्करण

Apache.org; Apache Struts 2 प्रलेखन - S2-052

Joseph Poon and Vitalik Buterin; प्लाज्मा: स्केलेबल स्वायत्त स्मार्ट कॉन्ट्रैक्ट