Hydro Raindrop

المصادقة العامة على Blockchain

كانون الثاني 2018

جدول المحتويات

نبذة مختصرة

HYDRO: من القديمة - بسط و علل Greek ὑδρο- (*h udro-*), من عند ὕδωρ (*h údōr*, "ماء")

تمكن الأنظمة الخاصة الجديدة والقائمة من دمج ودمج ديناميكيات ثابتة وثابتة Hydro لتعزيز تطبيق وتوثيق الأمن ، وإدارة الهوية ، والمعاملات ، blockchain للجمهور بسلاسة والذكاء الاصطناعي.

عامة Hydro لاستخدام APIs ، في هذه الورقة ، سيتم إنشاء حالة للأنظمة الخاصة ، مثل blockchain لتعزيز الأمن من خلال المصادقة العامة.

معاملة يتم تنفيذها من خلال عقد ذكي يثبت - "Raindrop" التكنولوجيا المقترحة تسمى صلاحية الوصول إلى النظام الخاص بشكل علني ، ويمكن أن يكمل طرق التوثيق الخاصة القائمة. تهدف هذه التقنية إلى توفير حماية إضافية للبيانات المالية الحساسة التي تتعرض بشكل متزايد لخطر الاختراق والخرق.

برنامج. تتوفر هذه Hydrogen API يتم تنفيذ على Hydro Raindrop التنفيذ الأولي لل المجموعة المعيارية من واجهات برمجة التطبيقات للمؤسسات والمطورين عالميًا من أجل إنشاء نماذج للمنتجات والتقنيات المالية المتطورة وبناءها واختبارها ونشرها.

سيتم توفيرها لمجتمع المطورين العالمي كبرنامج مفتوح المصدر ، للسماح Hydro Raindrop للمطورين بدمج أي مع REST API.

Blockchain و Ethereum

يتم تنفيذها على Hydro شبكة الاتصال. قبل تقديم مزيد من التفاصيل حول Ethereum
.Ethereum و blockchain المشروع ، من المهم فهم بعض الأفكار الأساسية حول هذا المشروع

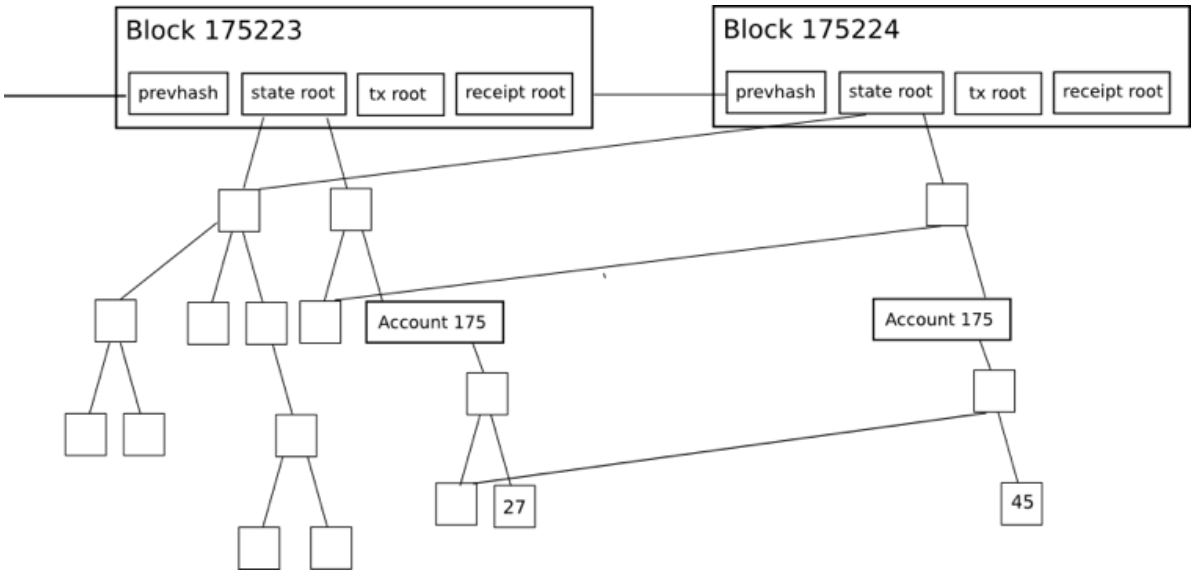
بناء على Ethereum

كما تم بناء تطبيقات مثل Snapchat باستخدام أدوات Swift وغيرها من الأدوات المقدمة على
منصة Apple iOS ، Ethereum. لم تكن blockchain على قمة لذا يمكن أيضًا بناء تطبيقات
شركة Snap Inc. بل استخدمته كبنية أساسية لإطلاق ، iOS بحاجة إلى إنشاء نظام التشغيل
.تطبيق وسائط اجتماعية يتغير قواعد اللعبة

مشروع Hydro إنه متشابه. وهو يعتمد على آلاف المطورين على مستوى العالم الذين يعملون
هذه Hydro الأساسية أسرع وأقوى وأكثر فاعلية. تعزز blockchain على جعل تقنية
البنية التحتية المتطورة باستمرار من خلال تطوير تفاعلات تركز على المنتج حول تقنية
blockchain التي يمكن أن تقدم فوائد ملموسة لتطبيقات الخدمات المالية

Merkle Trees

في الأنظمة الموزعة للتحقق من البيانات بشكل فعال. وهي تتسم Merkle يتم استخدام أشجار
هي طرق لتشفير Hash .بالكفاءة لأنها تستخدم علامات التجزئة بدلاً من الملفات الكاملة
الملفات التي تكون أصغر بكثير من الملف الفعلي نفسه
للمعاملات والإيصالات والدولMerkle trees على ثلاثة Ethereum يحتوي كل رأس كتلة في:



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

هذا يجعل من السهل على عميل خفيف الحصول على إجابات قابلة للتحقق من الاستعلامات ، مثل :

- هل هذا الحساب موجود؟
- ما هو الرصيد الحالي؟
- هل تم تضمين هذه المعاملة في كتلة معينة؟ ● هل حدث حدث معين في هذا العنوان اليوم؟

العقود الذكية

هو مفهوم blockchain والشبكات القائمة على Ethereum المفهوم الرئيسي الذي مكنته العقود الذكية. هذه هي كتل ذاتية التنفيذ من الكود يمكن أن تتفاعل معها أطراف متعددة ، مما يقلل الحاجة إلى وسطاء موثوق بهم. يمكن اعتبار الكود في عقد ذكي مشابهاً للبنود القانونية في العقد الورقي التقليدي ، ولكن يمكنه أيضًا تحقيق وظائف أكثر توسعية. قد يكون للعقود قواعد أو شروط أو عقوبات لعدم الامتثال أو يمكن أن يؤدي إلى بدء عمليات أخرى. عندما يتم تشغيلها ، يتم تنفيذ العقود كما هو مذكور أصلاً في وقت النشر على السلسلة العامة ، مما يوفر عناصر مدمجة من ثبات النظام واللامركزية.

يتم تحقيق الوظيفة .Ethereum العقد الذكي هو أداة حيوية للبناء على البنية التحتية عبر عقود مخصصة ، كما تمت مناقشته لاحقًا في هذه المقالة blockchain Hydro الأساسية لطبقة .

آلة افتراضية Ethereum

Ethereum. هي بيئة التشغيل للعقود الذكية في (EVM) الافتراضية Ethereum تعتبر آلة ويضمن بقاء البرامج عديمة الحالة ، على منع هجمات EVM يساعد (DoS)Denial of service

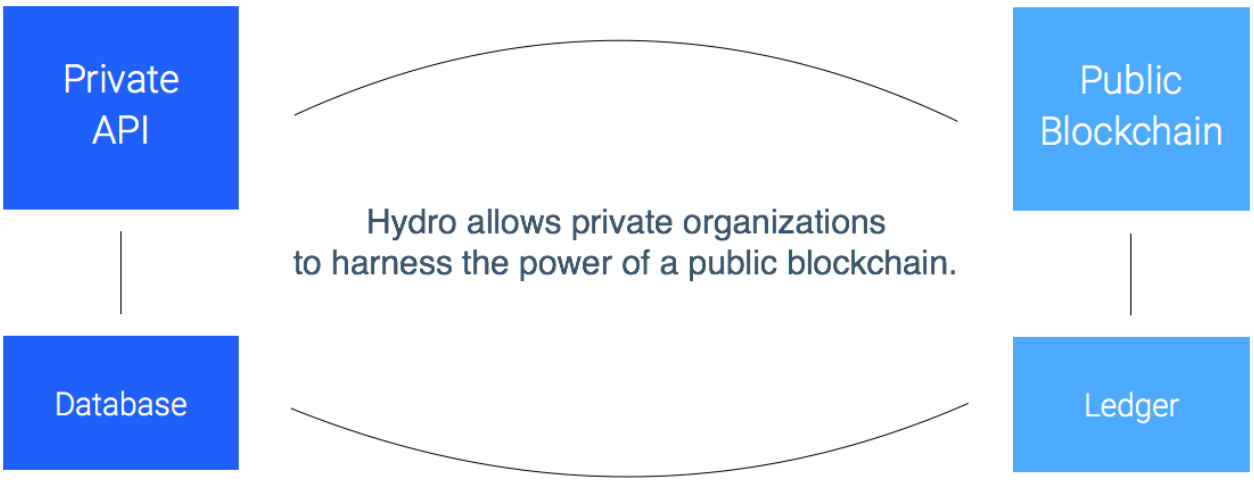
التكاليف المرتبطة بها ، EVM ، ويتيح الاتصال الذي لا يمكن قطعه. تتضمن الإجراءات على والتي تسمى الغاز ، والتي تعتمد على الموارد الحسابية المطلوبة. كل معاملة لها الحد إذا وصل الغاز المستهلك بواسطة معاملة g. الأقصى من الغاز المخصص لها ، والمعروف باسم .إلى الحد الأقصى ، فستتوقف عن متابعة المعالجة

دفتر الأستاذ العام

دفتر الأستاذ العام للأنظمة الخاصة

غالباً ما يمكن وصف الأنظمة التي تشغل منصات الخدمات المالية ومواقعها وتطبيقاتها على أنها وسائل لتدفق البيانات - فهي ترسل وتسترجع وتخزن وتحديث وتعالج البيانات للكيانات التي تتعامل معها. وبسبب طبيعة هذه البيانات والخدمات المالية بشكل عام ، فإن هذه الأنظمة غالباً ما تضم عمليات معقدة بطريقة خاصة ومركزية. وفي المقابل ، فإن الاعتماد على الهياكل الخاصة يفتح الباب أمام مجموعة متنوعة من الأمن والشفافية ومكاسب الكفاءة التي ..يمكن تحقيقها من خلال دمج قوى خارجية تتجاوز مدى وصول النظام الداخلي

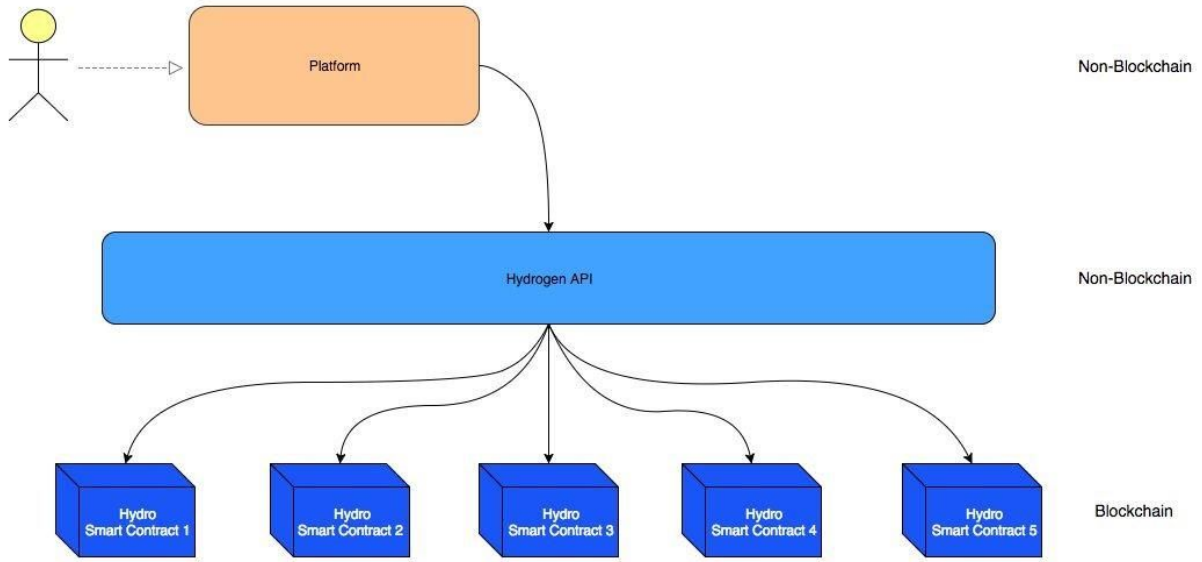
للاستفادة من المكاسب المذكورة أعلاه من Hydro الهيدروجين. تهدف API هذا هو الحال مع منصة بطرق يتم دمجها بسلاسة في blockchain خلال السماح لمستخدمي الهيدروجين بالتفاعل مع .النظام الأساسي الهيدروجين الخاص بشكل أساسي



قبل أو أثناء أو بعد العمليات blockchain يمكن أن تحدث العمليات العامة القائمة على الخاصة. يمكن أن يؤدي التفاعل بين العناصر الخاصة والعامة إلى التحقق من صحة أو ختم أو .تسجيل أو تحسين العمليات داخل النظام البيئي
تعمل روح هذا النموذج على جعل العمليات أكثر قوة من خلال الاستفادة من فوائد تقنية تحديدًا حيث يمكنها تحقيق التأثير الأكثر إيجابية. في حين قد لا ينطبق هذا الإطار blockchain .المختلط على جميع المنصات ، يركز هيدرو على توفير قيمة للحالات التي يكون فيها

الهندسة المعمارية للتبني

تختلف Hydro عن العديد من مبادرات blockchain الموجودة ، لأنها يمكن أن توجد بشكل مستقل وطبقة حول أنظمة جديدة أو موجودة دون الحاجة إلى تغيير نظامي. بدلا من الاستبدال ، يهدف Hydro إلى زيادة. يمكن للمنصات والمؤسسات التي يتم توصيلها إلى واجهات برمجة تطبيقات Hydrogen الوصول تلقائيًا إلى blockchain.



إن نطاق منصات الخدمات المالية التي يمكنها الاستفادة من الهيدروجين واسع. يمكن لهذه المنصات تشغيل أي تجربة تقريبًا ، وتضم أي عدد من الخدمات المسجلة الملكية ، وتنفيذ أي عملية خاصة للبيانات ، ونشرها في أي بيئة. يتم تمكين هذا من خلال النموذج الهيكلي لهيدروجين كمحرك متكامل للتبني ، Hydro وهو يتآزر مع.

Raindrop

ودعا ، blockchain بنيت على أعلى هذا دفتر الأستاذ العام هو خدمة التوثيق المستندة إلى "قطرة مطر". وهذا يوفر طبقة متميزة ، غير قابل للتغيير ، للعرض عالميا أن يتحقق من وصول الطلب يأتي من مصدر أذن.

مستويات متفاوتة من المتانة والفائدة في OAuth 2.0 توفر بروتوكولات المصادقة الخاصة مثل طيف حالات الاستخدام الموجودة. هناك حاجة ضئيلة للتنافس مع أو محاولة استبدال هذه كمكون في blockchain طريقة لتحسينها من خلال دمج ميكانيكا Hydro البروتوكولات - تقدم إجراء التوثيق. هذا يمكن أن يضيف طبقة مفيدة من الأمن للمساعدة في إحباط خرق النظام والوفاة بالبيانات.

دعنا أولاً نلقي نظرة على المشكلة التي تحاول ، Raindrop قبل دراسة الجوانب التقنية لـ حلها.

حالة الأمن المالي

جلبت زيادة عصر البيانات معها ارتفاع في الضعف ، وهذا مهم بشكل خاص بالنسبة للخدمات المالية. غالبًا ما تكون المنصات المالية عبارة عن بوابات لكميات كبيرة من البيانات الخاصة والحساسة مثل أرقام الهوية الحكومية ، وبيانات اعتماد الحساب ، وتاريخ المعاملات. بسبب مدى الأهمية الحاسمة لهذه البيانات ، فإن الوصول غير المبرر عادة ما يقابله نتائج كارثية.

قامت شركة الأبحاث الصناعية تريند مايكرو بنشر تقرير عن العثور على بنود مسروقة من على شبكة الويب المباشرة مقابل أقل من دولار أمريكي (PII) معلومات التعريف الشخصية واحد ، كما تتوفر نسخ من المستندات مثل جوازات السفر مقابل 10 دولارات كحد أدنى ، وبيانات اعتماد تسجيل الدخول البنكي مقابل 200 دولار أمريكي ، مما يجعل توزيع البيانات المسروقة مجزأة بشكل متزايد وغير قابلة للفك.

لسوء الحظ ، لا يمتلك النظام المالي الحالي سجلاً ناقصًا عندما يتعلق الأمر بمنع انتهاكات البيانات وتشخيصها والاتصال بها مع أصحاب المصلحة.

- وفقًا لدراسة حديثة أجرتها شرك Javelin Strategy & Research - *The 2017 Identity Fraud Study* - $16 15.4 مليار سرقت من million المستهلكين في الولايات المتحدة في عام 2016 بسبب فشل النظام المالي ل يحمي Personally Identifiable Information (PII).

- في أبريل 2017, Symantec نشرت لها *Internet Security Threat Report*, الذي يقدر أن 1.1 مليار قطعة من معلومات تحديد الهوية الشخصية قد تم اختراقها بمختلف القدرات على مدار عام 2016.

- كشف خرق بيانات نهاية العام 2016 من قبل الأمن القائم على المخاطر ، أن 4،149 مخالفة للبيانات حدثت في الشركات على مستوى العالم في عام 2016 ، وكشف أكثر من 4.2 مليار سجل.

- تقرير تهديد بيانات ثاليس لعام 2017 - إصدار الخدمات المالية ، وهو استبيان لمتخصصي تكنولوجيا المعلومات العالمية في الخدمات المهنية ، وجد أن 49 ٪ من منظمات الخدمات المالية قد عانت من خرق أمني في الماضي ، 78 ٪ تنفق أكثر لحماية

أنفسهم ، ولكن 73 ٪ يطلقون مبادرات جديدة تتعلق بتكنولوجيات الذكاء الاصطناعي ، إنترنت الأشياء ، والسحابة قبل إعداد الحلول الأمنية المناسبة.

خرق Equifax

وهي وكالة تقارير الائتمان الأمريكية ، Equifax في 29 يوليو 2017 ، تم اختراق شركة بما في ذلك أرقام الضمان ، PII البالغ عمرها 118 عامًا. تعرض 143 مليون مستهلك الاجتماعي. كان لدى 209000 عميل بيانات بطاقة ائتمان تعرضهم للاختراق.

?ما كان سبب هذا الخرق

هو إطار Equifax. Struts ويبدأ مع واحدة من التكنولوجيات الخلفية المستخدمة من قبل Apache التي تم إنشاؤها بواسطة ، Java مفتوح المصدر لتطوير تطبيقات الويب في لغة برمجة ذات Apache Struts عبارة عن ثغرة أمنية في Software Foundation. C VE-2017-9805 إذا .XML للتعامل مع حمولات XStream مع معالج Struts REST صلة باستخدام المكون الإضافي تم استغلاله ، فإنه يسمح لمهاجم بعيد غير مصادَق بتشغيل تعليمات برمجية ضارة على خادم التطبيقات إما للسيطرة على الجهاز أو إطلاق المزيد من الهجمات منه. تم تصحيح هذا قبل شهرين من خرق Apache بواسطة Equifax.

الذي يتم تشغيله حيث يقوم Xstream REST Plugin على خلل في Apache Struts يحتوي بشكل غير آمن. XML البرنامج بشكل غير آمن بتسلسل الإدخال الذي يقدمه المستخدم في طلبات والتي لا تفرض ، XStreamHandler () tostject وبشكل أكثر تحديدًا ، تحدث المشكلة في طريقة في كائن ، مما يؤدي إلى XStream أي قيود على القيمة الواردة عند استخدام إلغاء تسلسل نقاط ضعف تنفيذ تعليمات برمجية عشوائية.

فهل يجب أن يكون له أهمية؟ هل هناك طريقة ، REST حتى إذا تم اختراق هذا المكون الإضافي لتأمين المعلومات المالية لهؤلاء العملاء البالغ عددهم 143 blockchain لاستخدام تقنية الحالية وأنظمة جافا؟ REST API مليونًا مع الاستمرار في الاعتماد على

إضافة طبقة Blockchain

من الواضح أنه يمكن تحسين سلامة بوابات البيانات المالية. دعنا نفحص كيفية تحقيق Hydro. طبقة أمان إضافية عبر
صلاحية المعاملات لأن المشاركين يقومون بشكل Ethereum تضمن آليات التوافق الأساسية لشبكة جماعي بمعالجة المعاملات التي تم توقيعها بشكل صحيح. هذا الواقع يقود إلى اللامركزية والثبات ، ولكن الأهم من ذلك ، أنه يوفر ناقلات لتخفيف الوصول غير المصرح به إلى بوابة تتعامل مع البيانات الحساسة.

على سبيل .blockchain يمكن أن تستند المصادقة على عمليات المعاملات على ، Hydro مع التحقق من صحة المطورين (API) المثال ، يمكن أن تختار واجهة برمجة التطبيقات والتطبيقات من خلال مطالبتهم ببدء معاملات معينة ، مع حمولات بيانات معينة ، بين كشرط مسبق لبدء تنفيذ بروتوكول مصادقة قياسي ، blockchain عناوين معينة على.

Hydro Raindrop

يحتوي المطر على رزم من الماء المكثف يتراوح قطرها من 0.0001 إلى 0.005 سم. في عاصفة ممطر نموذجية ، هناك مليارات من هذه الحزم ، كل من الحجم العشوائي والسرعة والشكل. وبسبب ذلك ، لا يمكن للمرء أن يتنبأ بشكل موثوق بطبيعة المطر. وبالمثل ، فإن كل عملية تصديق هيدرو فريدة من نوعها ومن المستحيل افتراضيا حدوثها عن طريق الصدفة - وهذا هو السبب في أننا نسميها

للتحقق من m تستخدم منصات الخدمات المالية بشكل شائع التحقق من الودائع الإليكترونية حسابات العملاء. المفهوم بسيط: المنصة تقوم بإيداع كميات صغيرة من المبالغ العشوائية في الحسابات المصرفية التي يدعى المستخدم. ولإثبات امتلاك المستخدم بالفعل للحساب المذكور ، يجب عليه ترحيل مبالغ الإيداع إلى المنصة ، والتي يتم التحقق منها بعد ذلك. الطريقة الوحيدة التي يمكن للمستخدم من خلالها معرفة المبالغ الصالحة (إلى جانب التخمين) هي عن طريق الوصول إلى الحسابات المصرفية المعنية

هو مماثل. فبدلاً من إرسال المبلغ إلى المستخدم Hydro التحقق المستندة إلى قطرات المطر مع وإعادته مرة أخرى ، نحدد المعاملة ويجب على المستخدم تنفيذه من محفظة معروفة. الطريقة .الوحيدة التي يمكن للمستخدم من خلالها إجراء معاملة صالحة هي الوصول إلى المحفظة المعنية

مراقبة محاولات التخويل على دفتر accessor يمكن لكل من النظام و ، Raindrops باستخدام من عمليات blockchain أستاذ عام قابل للتغيير. يتم فصل هذه المعاملة القائمة على النظام الأساسية ، وتحدث على شبكة موزعة ، وتعتمد على ملكية المفاتيح الخاصة. لذلك ، .فإنه بمثابة ناقلات التحقق مفيدة

نظرة مفصلة

:هناك أربعة كيانات تشارك في عملية التوثيق Hydro

1. *Accessor* - الطرف الذي يحاول الوصول إلى النظام. في حالة ال Hydrogen, للبنية التحتية Hydrogen APIs هو مؤسسة مالية أو تطبيق يستخدم accessor الرقمية الأساسية.
2. *System* - النظام أو العبارة التي يتم الوصول إليها من قبل Accessor. إلى عن على Hydrogen, النظام هو API Hydrogen نفسه.
3. *Hydro* - الوحدة النمطية التي يستخدمها النظام للاتصال والتواصل مع blockchain .
4. *Blockchain* - دفتر الأستاذ العام الموزع الذي يعالج HYDRO المعاملات ويحتوي على العقود الذكية ، التي يمكن من خلالها دفع المعلومات أو سحبها أو تشغيلها Hydro بطريقة أخرى.

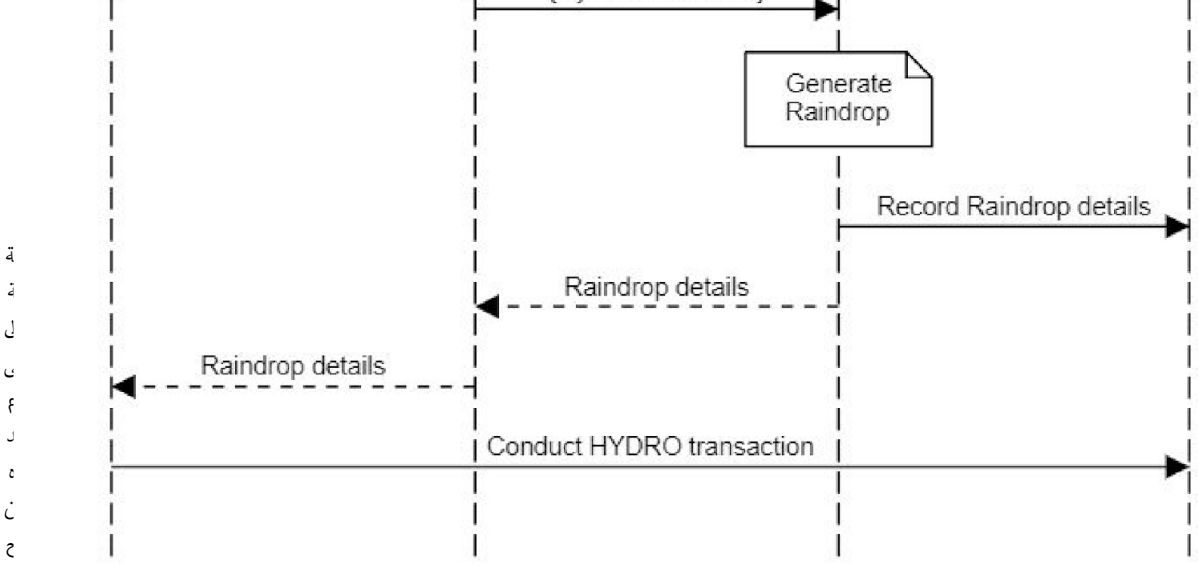
كل Raindrop, في جمله ، هي مجموعة من خمسة معاملات للمعاملات:

1. *Sender* - العنوان الذي يجب بدء المعاملة.
2. *Receiver* - عقد ذكي Hydro وجهة الصفقة. هذا يتوافق مع استدعاء طريقة في.
3. *ID* - معرف يرتبط بالنظام.
4. *Quantity* - عدد دقيق من HYDRO لإرسال.
5. *Challenge* - سلسلة أبجدية رقمية يتم إنشاؤها عشوائيًا.

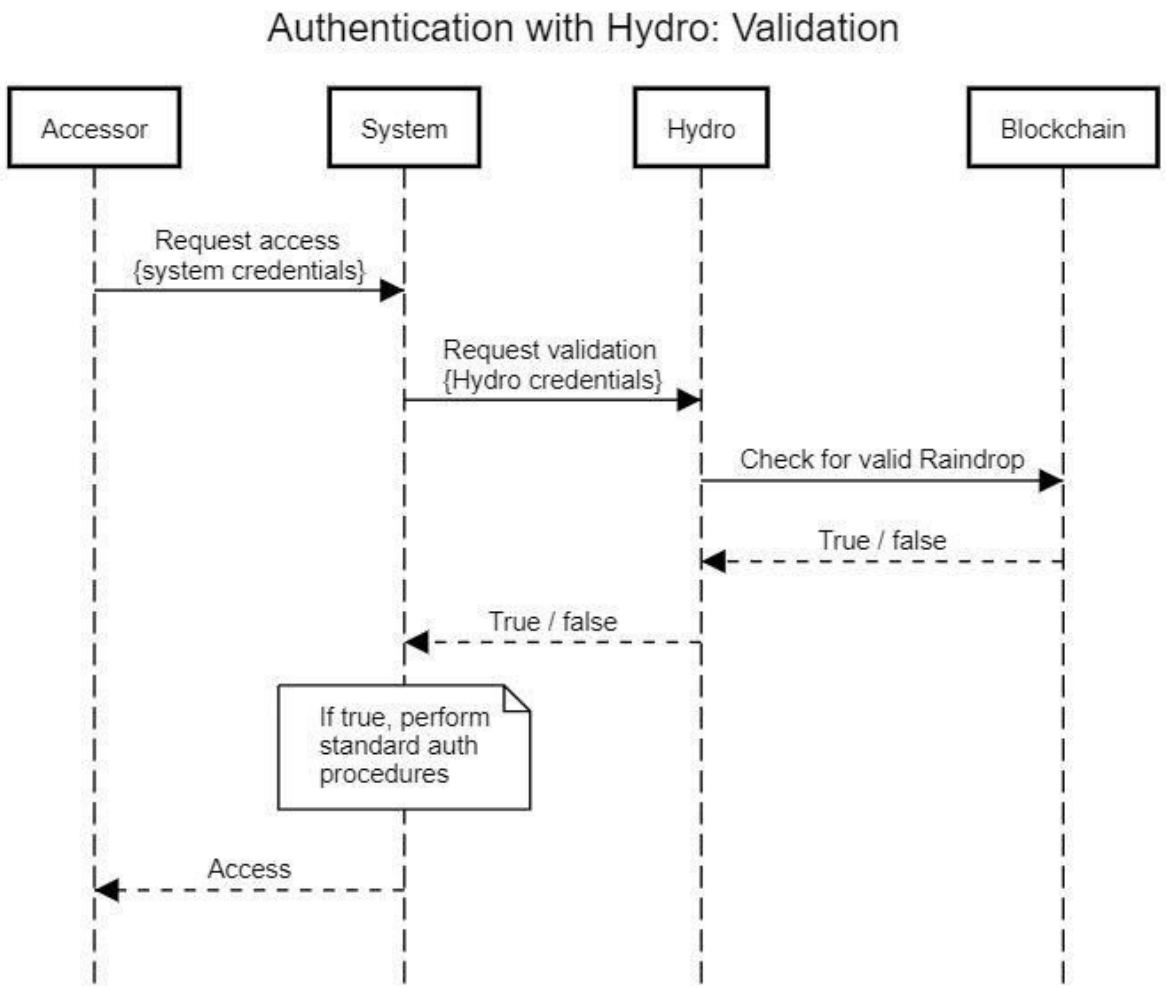
يوجد أدناه مخطط لعملية المصادقة ، والتي يمكن تصنيفها بشكل عام إلى ثلاث مراحل:

1. التهيئة
2. Raindrop
3. التحقق من صحة

والحصول على Hydro تبدأ عملية التهيئة من خلال نظام (مثل الهيدروجين) يسجل لاستخدام نظام (على .Hydro عبر وحدة blockchain بيانات الاعتماد ، مما يتيح للنظام الاتصال مع Hydro. سبيل المثال مؤسسة مالية) الذي يسجل عنوانًا عامًا ، ثم يمرر العنوان المسجل إلى إلى اللائحة البيضاء المخزنة في عقد blockchain هذا العنوان مكتوب بشكل مؤثر على الذكي. يتلقى النظام تأكيدًا على أن العنوان مدرج في القائمة البيضاء ، والذي Hydro يمكن التحقق منه أيضًا كحدث قابل للعرض العام. لا يحتاج تسجيل النظام إلا مرة واحدة Accessor. مرة واحدة فقط في Accessor فقط ، بينما يلزم أن تظهر القائمة البيضاء لـ



رسميًا Accessor الخطوة الأخيرة في هذه العملية هي التحقق من الصحة. في هذه الخطوة ، تطلب الوصول إلى النظام من خلال آلية النظام التي تم إنشاؤها. قبل تنفيذ أي من بروتوكولات بإجراء معاملة Accessor سواء قام Hydro المصادقة القياسية الخاصة به ، يسأل النظام صالحة أم لا. واجهات هيدروليكية مع العقد الذكية ، والتحقق من صحة ، Raindrop ويستجيب مع تعيين صواب / خطأ. النظام قادر لتحديد كيفية المضي قدمًا استنادًا إلى هذا التصنيف - إذا كانت خاطئة ، يمكن للنظام منع الوصول ، وإذا كان صحيحًا ، يمكن للنظام منح حق الوصول.



إذا اعتبرنا أن بيانات اعتماد النظام الأساسية - أو أي بروتوكول موجود في النظام - هو عامل واحد للمصادقة بشكل عام ، فمن المهم أن توفر الطبقة الهيدرولية عاملًا ثانيًا مفيدًا. من خلال فحص متجهي الهجوم الأساسيين ، يمكننا التأكد من فائدته بسهولة:

- Vector 1 - المهاجم يسرق بيانات اعتماد النظام الأساسي Accessor
  1. يحاول المهاجم الوصول إلى النظام باستخدام بيانات اعتماد النظام الصالحة
     - لتحديد ما إذا كانت هناك معاملة صالحة تمت على Hydro يتحقق النظام مع blockchain
     - ويرفض النظام الوصول ، إرجاع Hydro false
- Vector 2 - يسرق المهاجم المفتاح (المفاتيح) الخاصة إلى محفظة Accessor
  1. من العنوان المسجل ، دون تفاصيل Hydro يحاول المهاجم إجراء معاملة Raindrop المطلوبة
     - صالحة blockchain لا يمكن للمهاجم إنشاء معاملة
     - لا يستطيع المهاجم أيضًا طلب الوصول إلى النظام بدون بيانات اعتماد النظام المناسبة

من الواضح أن المهاجم يجب أن يسرق كلا من بيانات اعتماد النظام الأساسية والمفتاح من أجل الوصول إلى النظام. في هذا الصدد ، أضافت Access (المفاتيح) الخاصة بحافظة Hydro بنجاح عامل إضافي للمصادقة.

فتح Raindrop للعامة

للمساعدة في تأمين النظام الإيكولوجي blockchain في حين تم تصميم هذه الخدمة المستندة إلى الهيدروجين ، فإنه ينطبق على نطاق واسع على منصات وأنظمة مختلفة. ونظرًا لأننا API نعتقد أنه يمكن للآخرين الاستفادة من طبقة التحقق هذه ، فإننا نفتحها للاستخدام.

الخاص بها ، API وكما أن الهيدروجين سوف يدمجها كشرط مسبق للوصول إلى النظام الإيكولوجي كذلك يمكن لأي نظام أن يضيفه إلى الإجراءات والبروتوكولات القائمة. أي منصة - سواء كانت واجهة برمجة التطبيقات أو التطبيق أو برنامج المؤسسة أو منصة الألعاب وما إلى ذلك - لأولئك GitHub لأغراض المصادقة. ستتوفر الوثائق الرسمية على Hydro يمكنها الاستفادة من هذه في إطار المصادقة أو blockchain الذين يرغبون في دمج طبقة REST API.

دراسة الحالة - Raindrop مع OAuth 2.0

من قبل المنظمات الخاصة. Raindrop هناك العديد من الطرق التي يمكن من خلالها إطلاق سراح لقد أنشأت واجهات برمجة التطبيقات وقواعد البيانات والشبكات الخاصة أنظمة معقدة من الرموز والمفاتيح والتطبيقات والبروتوكولات على مدار العقد الماضي في محاولة لتأمين واحدة من أشهر مزودي المنتجات في Google بيانات حساسة. على سبيل المثال ، أصبحت كما ذكر سابقاً ، لا يوجد سبب يذكر .Google Authenticator السوق باستخدام تطبيق للمنافسة أو استبدال هذه البروتوكولات الموجودة.

كدراسة حالة ، إليك نظرة عامة مختصرة عن كيفية تنفيذ الهيدروجين للمصادقة المائية العام الخاص به (API) كطبقة أمان في إطار أمان واجهة برمجة التطبيقات:

1. لبيئاتهم IP يجب أن يكون لدى شركاء واجهة برمجة تطبيقات الهيدروجين أولاً عناوين المختلفة المدرجة في القائمة البيضاء.
2. يجب على الشركاء طلب إدراج عنوان هيدرولوجي عام في القائمة البيضاء.
3. يتم تشفير جميع المكالمات إلى واجهات برمجة تطبيقات الهيدروجين ونقل البيانات ونقلها من خلال بروتوكول HTTPS.
4. Hydro يجب على الشركاء إكمال معاملة سارية من قطرات المطر المائية من عنوان المسجل.

(Open Authorization) OAuth يعد .OAuth 2.0 يجب على الشركاء استخدام التحقق من صحة معيارًا مفتوحًا للمصادقة والتوثيق القائم على الرمز المميز. يدعم الهيدروجين "بيانات اعتماد كلمة مرور مالك الموارد" و "العميل

يجب أن توفر أنواع منح "الاعتماد" ، وكل مستخدم واجهة برمجة التطبيقات بيانات اعتماد لطلب المصادقة.

5. إذا لم يتم انتهاك أي من العناصر الخمسة المذكورة أعلاه ، يتم منح شريك الهيدروجين رمزًا مميزًا فريدًا ، ليتم التحقق منه والتحقق منه مع كل مكالمة من API.

6. الرمز صالح لمدة 24 ساعة ، وبعد ذلك يجب على الشريك التحقق من صحته مرة أخرى.

إذا تم انتهاك أي من هذه الخطوات ، فسيتم قفل المستخدم على الفور من الوصول إلى واجهة برمجة التطبيقات. لا يمكن للهاكر تجاوز عوامل الأمان هذه عن طريق التخمين بشكل عشوائي ، لأن هناك تريليونات من مجموعات فريدة.

المائي مكونًا مهمًا في بروتوكول أمان الهيدروجين. blockchain تعتبر التوثيق القائم على يشجع فريق الهيدروجين الشركاء على إنشاء محافظ متعددة التوقيع ، وتخزين المفاتيح الخاصة في مواقع آمنة متعددة بشكل مستقل عن أوراق اعتماد أخرى ، لذلك لا توجد نقطة واحدة للفشل. ليس من الصعب سرقة المحفظة متعددة التوقيع المضمونة بشكل صحيح فحسب ، بل إن الطبيعة العامة للكتلة تسمح أيضًا بالاعتراف السريع بأي سرقة من حيث صلتها بأمن واجهة برمجة التطبيقات.
الذكي ، وهو ما يعني أن أيام المنصات التي يتم Hydro يمكن لأي شخص عرض محاولة توثيق لعقد اختراقها لأشهر النهاية يمكن أن تكون شيئًا من الماضي. يمكن الآن إحباط متسللي واجهة برمجة التطبيقات بشكل فوري أكثر بسبب القدرة على اكتشاف محاولات تفويض غير متوقعة في الوقت الفعلي ، من أي مكان في العالم.

المخاطر

مثل أي تقنية ناشئة ، مثل الأيام المبكرة لوسائل التواصل الاجتماعي والبريد الإلكتروني وتطبيقات البث (التي كانت تعتمد على الاتصال الهاتفي) ، من المهم أن يقوم فريق التطوير الأساسي بتتبع التطورات الجديدة في سرعات وحجم المعاملات في Ethereum. هل يمكنك تخيل محاولة Blackberry؟ لأول مرة على Instagram لإطلاقه في عام 1995؟ أو عرض YouTube

اقترح مطورو Core Ethereum ، مثل Vitalik Buterin و Joseph Poon ، تحديث العقود الذكية ذاتية البلازما: القابلة للتحجيم إلى بروتوكول Ethereum:

> **تعد البلازما إطارًا مقترحًا لتحفيز وتنفيذ العقود الذكية القابلة للتطوير إلى حد كبير من تحديثات الدولة في الثانية (التي قد تكون بلايين من الدولارات) ، مما يتيح من تمثيل كمية كبيرة من التطبيقات المالية اللامركزية في جميع أنحاء blockchain تمكين العالم. يتم تحفيز هذه العقود الذكية على مواصلة التشغيل بشكل مستقل عن طريق الأساسي (على blockchain رسوم معاملات الشبكة ، والتي تعتمد في نهاية المطاف على لفرض التحولات الدولة المعاملات (Ethereum سبيل المثال.**

وقد اقترح آخرون ، مثل شبكة ريدن ، حلًا لتوسيع نطاق السلسلة يهدف إلى تشغيل معاملات Ethereuem حدًا ضئيلًا جدًا على إطار Raindrop أسرع وتخفيض الرسوم. في هذا الوقت ، ستضع وبالتالي فإن قابلية التوسع هي خطر صغير جدًا لنجاح التكنولوجيا ،.

Conclusion

توفر ثباتية blockchain مثل الأنظمة الخاصة أمان لتحسين طرقًا جديدة العام APIs.

لقد أظهرت هذه الورقة ثلاثة أشياء مهمة:

1. يمكن أن يضيف blockchains المالية في الخدمات قيمة العامة.
2. يمكن أن يعزز Hydro Raindrop الخاصة الأنظمة من أمن.
3. هناك تطبيقات فورية من Hydro Raindrop داخل منصة API الهيدروجين.

يعتقد الفريق الهيدرولوجي أن الإطار المبين يمكن أن يكون البنية الأساسية الأمنية القياسية لنموذج جديد من الأنظمة العامة الخاصة المختلطة ، والتي ستفيد جميع أصحاب المصلحة في صناعة الخدمات المالية وما بعدها.

Sources:

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

