Hydro Raindrop

Autenticación pública en el Blockchain

Enero 2018

TABLA DE CONTENIDO

Resumen

HYDRO: Etimología – de la antigua palabra griega ὕδρο (*hydro*), que proviene de la palabra ὕδωρ (agua).

Hydro permite que los sistemas privados nuevos y existentes integren y exploten impecablemente la dinámica inmutable y transparente de un blockchain para mejorar la seguridad de aplicaciones y documentos, la gestión de identidades, las transacciones y la inteligencia artificial.

En este documento, se hará referencia a los sistemas privados, como las API, que utilizarán el blockchain público de Hydro para mejorar la seguridad a través de la autenticación pública (public authentication).

La tecnología propuesta se denomina "Raindrop", una transacción que tiene lugar a través de un contrato inteligente (smart contract) que valida públicamente el acceso privado al sistema y puede complementar los métodos de certificación privada existentes. La tecnología tiene como objetivo proporcionar seguridad adicional para los datos financieros sensibles que están en mayor riesgo de piratería y violaciones.

La implementación inicial de Hydro Raindrop se lleva a cabo en la plataforma API de Hydrogen. Este paquete API modular está disponible para empresas y desarrolladores de todo el mundo para iniciar, construir, probar y desarrollar plataformas sofisticadas y productos de ingeniería financiera.

Hydro Raindrop estará disponible para la comunidad global de desarrolladores como software de código abierto (Open source software), para que los desarrolladores puedan integrar Hydro Raindrop con cualquier API REST.

Blockchain & Ethereum

Hydro se está implementando en la red Ethereum. Antes de analizar más detalles sobre el proyecto, es importante comprender algunas ideas fundamentales para blockchain y Ethereum..

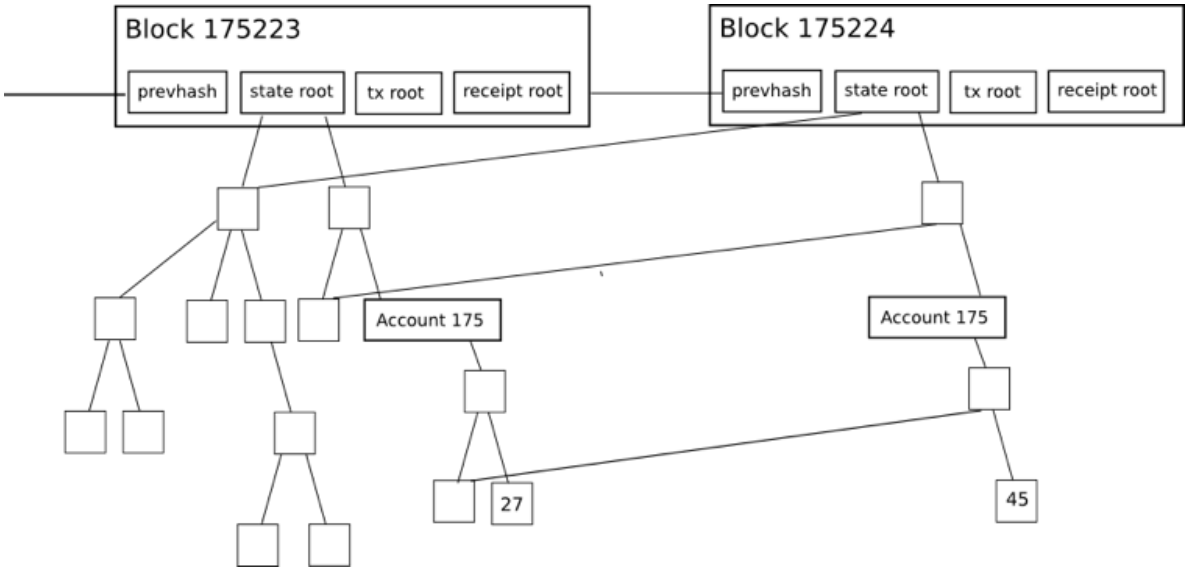
Basándose en Ethereum

Como las aplicaciones como Snapchat se crearon con Swift y otras herramientas ofrecidas por la plataforma Apple Ios, también se pueden construir aplicaciones de blockchain en Ethereum. Snap Inc. no necesitó construir Ios, lo usó como una infraestructura para lanzar una aplicación de redes sociales que cambiará las reglas del juego.

Proyecto Hydro es similar. Se basa en miles de desarrolladores en todo el mundo, que trabajan para que la tecnología blockchain subyacente sea más rápida, más potente y más eficiente. Hydro está utilizando esta infraestructura en constante mejora mediante el desarrollo de interacciones centradas en el producto en torno a la tecnología blockchain, que puede ofrecer importantes beneficios a las aplicaciones de servicios financieros.

Merkle Trees

Merkle Trees se utilizan en sistemas de validación de datos distribuidos. Son efectivos porque usan los llamados hash en lugar de registros completos. Los hashes son métodos de codificación de archivos mucho más pequeños que el archivo en sí. Cada encabezado de bloque en Ethereum contiene tres árboles de Merkle para transacciones, ganancias y estados:



Fuente: Merkling in Ethereum; Vitalik Buterin, Fundador Ethereum

Esto facilita que Light Client obtenga respuestas verificables a preguntas como:

- ¿Esta cuenta existe?
- ¿Cuál es el saldo actual?
- ¿Se ha incluido esta transacción en un bloque en particular?
- ¿Ha sucedido un evento en particular en esta dirección hoy?

Smart Contracts

Un concepto clave habilitado por Ethereum y otras redes basadas en blockchain es el de los contratos inteligentes. Estos son bloques de código autoejecutables con los que pueden interactuar múltiples partes, lo que elimina la necesidad de intermediarios de confianza. El código en un contrato inteligente puede verse como similar a las cláusulas legales en un contrato en papel tradicional, pero también puede lograr una funcionalidad mucho más expansiva.

Los contratos pueden tener reglas, condiciones, penalidades por incumplimiento o pueden impulsar otros procesos. Cuando se activan, los contratos se ejecutan como se estableció originalmente en el momento del despliegue en la cadena pública, ofreciendo elementos incorporados de inmutabilidad y descentralización.

El contrato inteligente es una herramienta vital para construir en la infraestructura de Ethereum. La funcionalidad principal de la capa de Hydro blockchain se logra a través de contratos personalizados, como se explica más adelante en este documento.

Máquina virtual de Ethereum

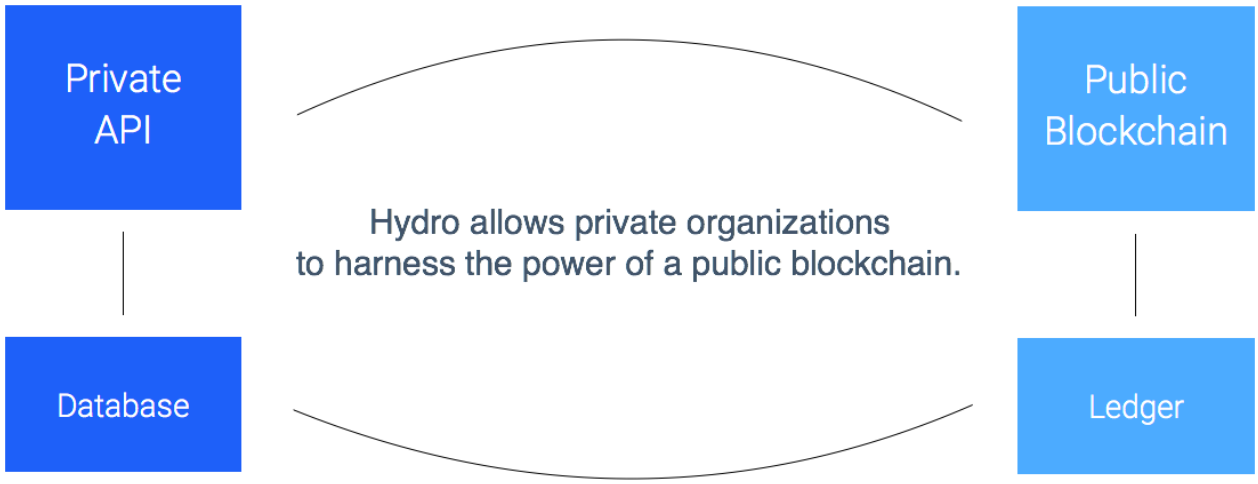
La máquina virtual Ethereum (EVM) es el entorno de tiempo de ejecución para contratos inteligentes en Ethereum. El EVM ayuda a prevenir los ataques de denegación de servicio (DoS), asegura que los programas permanezcan sin estado y permite la comunicación que no se puede interrumpir. Las acciones en el EVM tienen costos asociados con ellos, llamados gas, que dependen de los recursos computacionales requeridos. Cada transacción tiene una cantidad máxima de gas asignada, conocida como límite de gas. Si el gas consumido por una transacción alcanza el límite, dejará de continuar el procesamiento.

Public Ledger

Un Public Ledger para sistemas privados

Los sistemas que impulsan plataformas de servicios financieros, sitios web y aplicaciones a menudo se pueden describir como medios de flujo de datos: envían, recuperan, almacenan, actualizan y procesan datos para las entidades con las que interactúan. Debido a la naturaleza de estos datos y servicios financieros en general, estos sistemas a menudo tienen funciones complejas de forma privada y centralizada. La confianza en las estructuras privadas, a su vez, abre la puerta a una variedad de fusibles, la transparencia, así como las ganancias de eficiencia con el fin de adoptar la integración de las fuerzas externas que excederían el alcance del sistema interno.

Tal es el caso de la plataforma API de Hydrogen. Hydro apunta a aprovechar las ventajas antes mencionadas al permitir que los usuarios de Hydrogen interactúen con una cadena de bloques de manera que se integren perfectamente en el ecosistema de Hydrogen fundamentalmente privado.

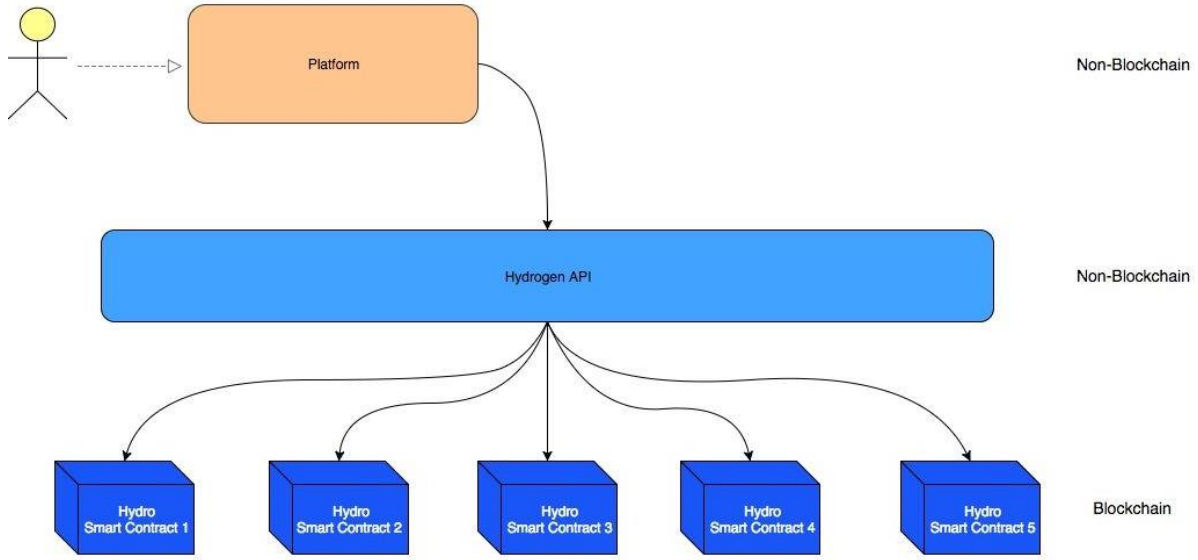


Las operaciones públicas basadas en blockchain pueden ocurrir antes, durante o después de operaciones privadas. La interacción entre elementos privados y públicos puede servir para validar, marcar, registrar o mejorar procesos dentro de un ecosistema.

El espíritu de este modelo fortalece los procesos al aprovechar los beneficios de la tecnología blockchain, especialmente donde puede producir los efectos más positivos. Si bien esta estructura híbrida puede no aplicarse a todas las plataformas, Hydro se centra en proporcionar valor para las situaciones en las que está en su lugar.

Plantilla arquitectónica

Hydro es diferente de muchas iniciativas existentes de blockchain porque puede ser independiente y colocarse en sistemas nuevos o preexistentes sin requerir un cambio sistemático. En lugar de reemplazar, Hydro apunta a aumentar. Las plataformas e instituciones que se conectan a las API de Hydrogen pueden acceder automáticamente a la cadena de bloques.



La amplitud de las plataformas de servicios financieros que pueden aprovechar el Hydrogen es amplia. Estas plataformas pueden alimentar virtualmente cualquier experiencia, alojar cualquier cantidad de servicios patentados, realizar cualquier operación de datos privados y crecer en cualquier entorno. Esto se logra a través de la adaptación estructural del Hydrogen y funciona con Hydro, actuando como una guía complementaria para la adopción.

Raindrop

Sobre la base de este libro público Hydro se encuentra un servicio de autenticación basado en blockchain, llamado "Raindrop". Esto ofrece una capa de seguridad distinta, inmutable y visible a nivel mundial que verifica que una solicitud de acceso proviene de una fuente autorizada.

Los protocolos de autenticación privados como OAuth 2.0 ofrecen diferentes niveles de solidez y utilidad para el rango de instancias de uso. Hay poca necesidad de competir o intentar reemplazar estos protocolos. Hydro ofrece una manera de reforzarlos mediante la integración de los mecanismos de blockchain como parte del proceso de autenticación. Esto puede agregar una capa de seguridad útil para ayudar a prevenir violaciones del sistema y filtración de información confidencial.

Antes de examinar el aspecto técnico de Raindrop, veremos el problema que es tratando de resolver.

El estado de la seguridad financiera

El aumento de la era de los datos trajo consigo vulnerabilidad a los sistemas, y esto es particularmente importante para los servicios financieros. Las plataformas financieras se pueden considerar como puertas de entrada a una gran cantidad de datos privados y confidenciales, como números de identidad, registros de cuentas e historiales de transacciones. Debido a la importancia de los datos de identificación, el acceso a ellos de fuentes no deseadas, a menudo se siguen resultados catastróficos.

La firma de investigación de la industria Trend Micro publicó un informe que encontró que las líneas robadas de Información de identificación personal (PII) se venden en la Web profunda por tan solo $ 1, escaneos de documentos como pasaportes están disponibles por tan solo $ 10 y credenciales de inicio de sesión bancario para tan poco como $ 200, haciendo que la distribución de datos robados se vuelva cada vez más fragmentada e imposible de rastrear.

Lamentablemente, el sistema financiero existente no tiene un historial impecable cuando se trata de prevenir, diagnosticar y comunicar infracciones de datos con sus grupos de interés.

- Según un estudio reciente de Javelin Strategy & Research titulado - *The 2017 Identity Fraud Study* - $16 billones fueron robados por 15.4 millones de consumidores estadounidenses en 2016 debido a fallas del sistema financiero para proteger los datos personales (PII).

- En abril de 2017, Symantec publicó su *Internet Security Threat Report*, que estima que en el transcurso de 2016, 1,1 mil millones de archivos de PII se pusieron a disposición de diversas fuentes.

- En el artículo *2016 Year End Data Breach Quickview* de Risk Based Security, se descubrió que en 2016 hubo 4.19 infracciones de datos en negocios en todo el mundo, lo que expone más de 4.200 millones de registros.
- En *2017 Thales Data Threat Report – Financial Services Edition*, una encuesta de profesionales de TI globales en servicios profesionales, encontró que el 49% de las organizaciones de servicios financieros han sufrido una brecha de seguridad en el pasado, el 78% está gastando más para protegerse, pero el 73% está lanzando nuevas iniciativas relacionadas con AI, IoT y tecnologías en la nube antes de preparar soluciones de seguridad apropiadas.

Equifax Breach

El 29 de julio de 2017, Equifax, una agencia de informes crediticios de 118 años de edad, fue hackeada, con 143 millones de usuarios de PII expuestos, incluidos los números de la seguridad social, ya que se han violado los datos de la tarjeta de crédito de 209,000 clientes.

¿Cuál fue la causa de esta violación?

Comenzó con una de las tecnologías de back-end utilizadas por Equifax. Struts es un marco de código abierto para el desarrollo de aplicaciones web en el lenguaje de programación Java, creado por la Apache Software Foundation. El CVE-2017-9805 es un punto vulnerable en Apache Struts sobre el uso del plugin Struts REST con el manejador XStream para manejar cargas XML. Si se infringe, le permite al atacante ejecutar código malicioso en el decorador de la aplicación, ya sea para encargarse del motor o para lanzar más ataques desde él. Esto fue parcheado por Apache dos meses antes de la violación de Equifax.

Apache Struts contiene un error en REST Plugin XStream que se desencadena a medida que el programa deserializa inseguramente la entrada proporcionada por el usuario en solicitudes XML. Más específicamente, el problema ocurre en el método toObject () de XStreamHandler, que no impone ninguna restricción sobre el valor entrante cuando se utiliza la deserialización de XStream en un objeto, lo que genera vulnerabilidades de ejecución de código arbitrarias.

Incluso si este plugin REST estuviera comprometido, ¿hubiera importado? ¿Existe alguna forma de utilizar la tecnología blockchain para asegurar la información financiera de estos 143 millones de clientes mientras se sigue confiando en la API REST y los sistemas basados en Java?

Agregar una capa de blockchain

Está claro que se puede mejorar la integridad de las puertas de datos financieros.

Veamos cómo se puede lograr un nivel extra de seguridad a través de Hydro.

Los mecanismos de consenso básicos de Ethhereum garantizan la validez de las transacciones porque los participantes procesan colectivamente las transacciones que están debidamente firmadas. Este hecho conduce a la descentralización y la estabilidad, pero, sobre todo, proporciona un vector para mitigar el acceso no autorizado a una puerta de enlace que maneja datos confidenciales.

Con Hydro, la autenticación puede depender de las operaciones de transacción en el blockchain. Por ejemplo, una API puede optar por validar desarrolladores y aplicaciones al exigirles que inicien transacciones específicas con una carga de datos particular entre direcciones específicas en la blockchain, siempre que se inicie un protocolo de autenticación.

Hydro Raindrop

La Rain ("lluvia") contiene paquetes de agua compactados que varían de 0,0001 a 0,005 cm de diámetro. En una tormenta típica, hay miles de millones de estos paquetes, cada uno con tamaño, velocidad y forma aleatorios. Debido a esto, uno no puede predecir con exactitud la naturaleza exacta de la lluvia. Del mismo modo, cada transacción de autenticación Hydro es única y prácticamente imposible de realizar al azar, por lo que la llamamos Gotas de lluvia.

Las plataformas de servicios financieros generalmente usan la verificación de microcrédito para validar las cuentas de los clientes. La idea es simple: la plataforma crea pequeños depósitos de cantidades aleatorias en cuentas bancarias declaradas por los usuarios. Para demostrar que el usuario posee realmente esa cuenta, debe transferir los montos de los depósitos a la plataforma, que luego se validan. La única forma en que el usuario puede conocer los importes válidos (excepto para adivinar) es el acceso a estas cuentas bancarias.

La verificación basada en Raindrop con Hydro es proporcional. En lugar de enviar una cantidad al usuario y retransmitirla, definimos una transacción y el usuario debe ejecutarla desde un monedero bien conocido. La única forma en que un usuario puede realizar una transacción válida es acceder a esta billetera.

Con las gotas de lluvia, tanto el sistema como el usuario pueden seguir los esfuerzos de autorización en un public ledger sin cambios. Esta transacción basada en blockchain se desconecta de las funciones básicas del sistema, aparece en una red distribuida y depende de la propiedad de las claves privadas. Por lo tanto, sirve como un valioso elemento de validación.

Una mirada cuidadosa

Hay cuatro elementos involucrados en el proceso de verificación de identidad de Hydro:

1. *Accessor* - El grupo busca acceso a un sistema. En el caso de Hydrogen, el accessor es una institución o aplicación financiera que utiliza las API de hidrógeno para su infraestructura digital central.
2. *System* - El sistema, o la puerta de enlace accesible para Accessor. Para el Hydrogen, el sistema es la API de Hydrogen en sí.
3. *Hydro* - El módulo utilizado por el Sistema para la comunicación y la interconexión con blockchain.
4. *Blockchain* – El public ledger distribuido que procesa las transacciones de HYDRO y contiene los smart contracts de Hydro, a través de los cuales se puede importar, recibir u operar informació.

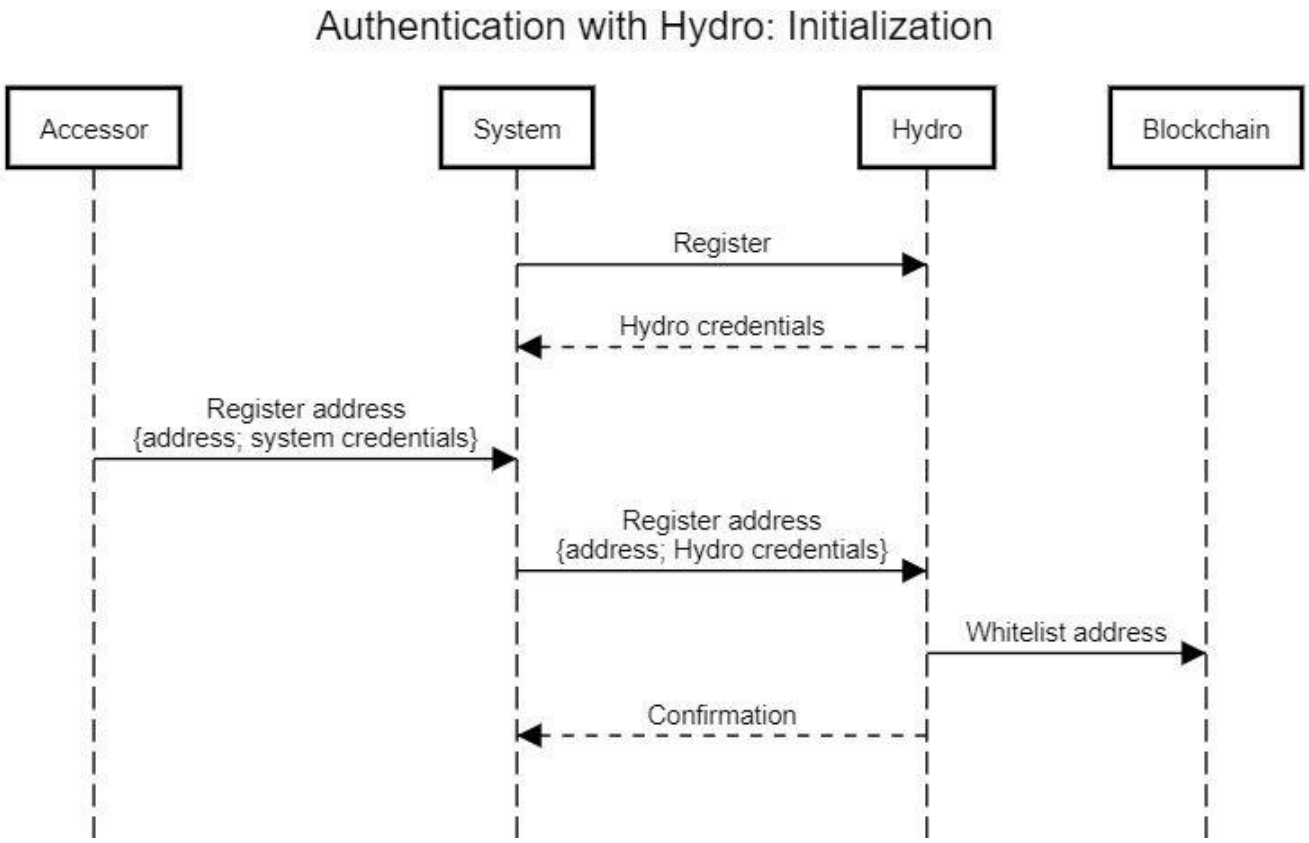
Cada de Raindrop consta de un conjunto de cinco parámetros de negociación:

1. *Sender* - La dirección para comenzar la transacción.
2. *Receiver* - El destino de la transacción. Esto corresponde a llamar a un método en un de Hydro Smart Contract.
3. *ID* - Un identificador asociado con el sistema.
4. *Quantity* - Un número HYDRO exacto seleccionado para el envío.
5. *Challenge* - Una serie alfanumérica producida al azar.

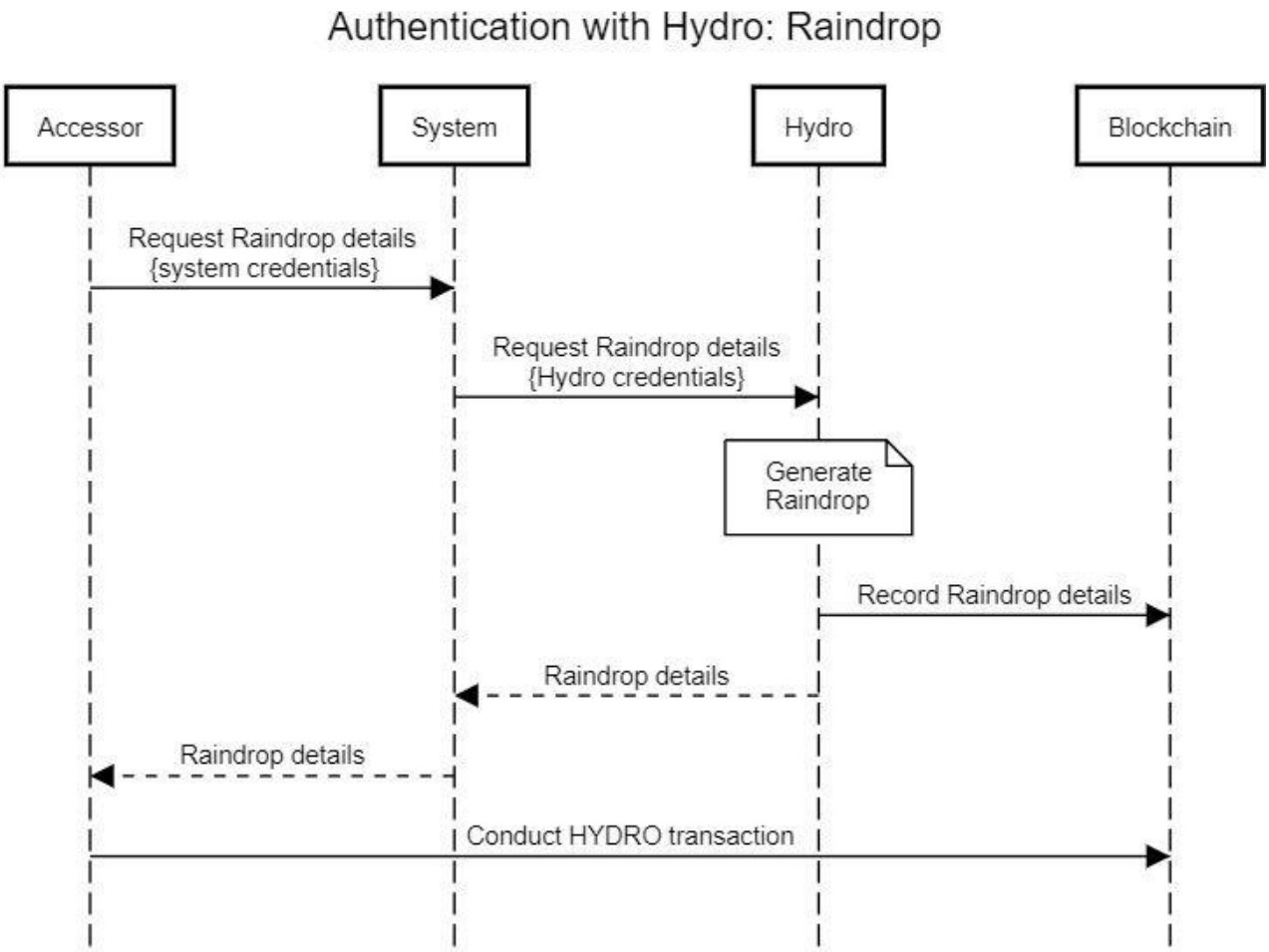
A continuación se muestra un resumen del proceso de autenticación, que generalmente se puede clasificar en tres etapas:

1. Initialization (Inicialización)
2. Raindrop
3. Validation (Validación)

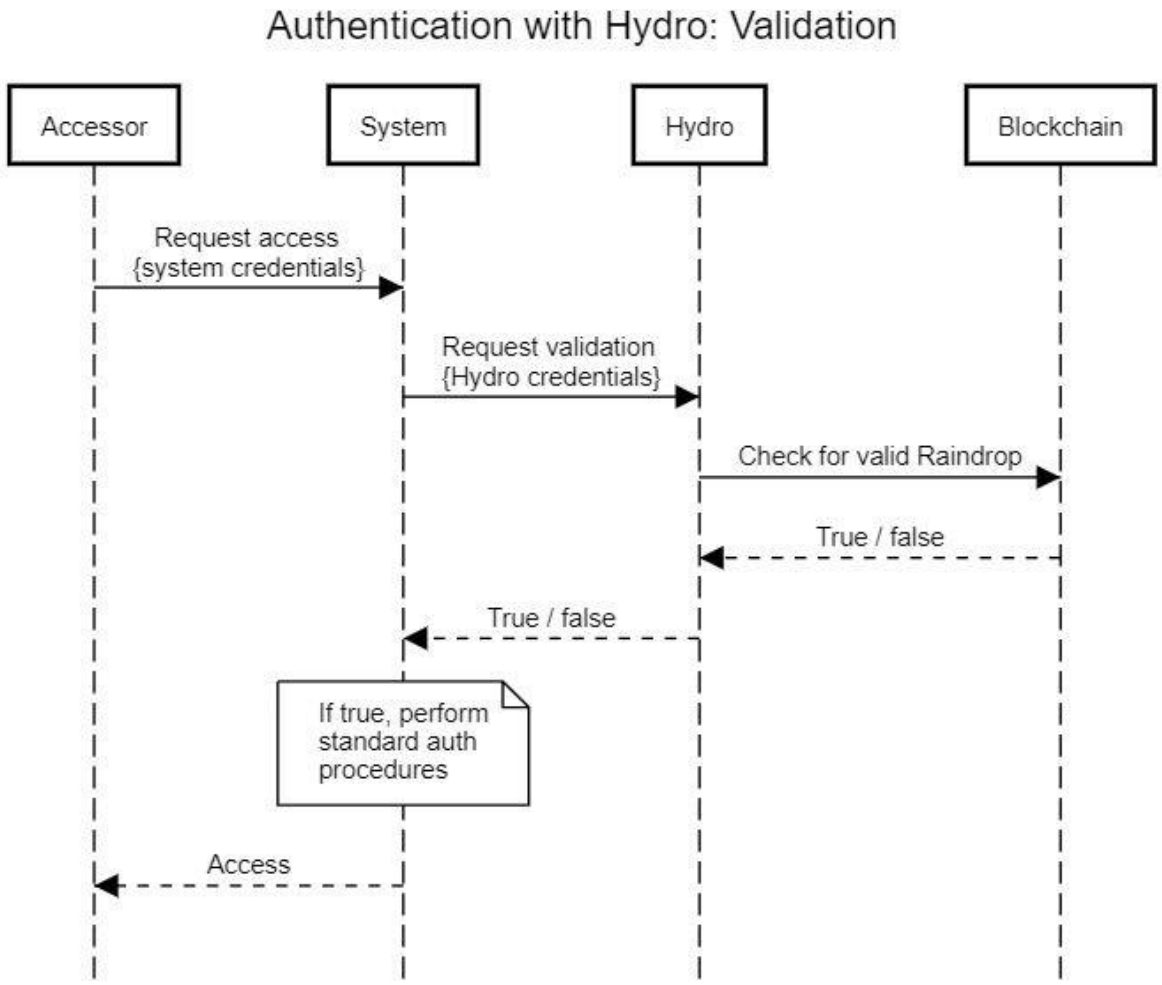
Inicialización comienza con un sistema (por ejemplo Hydrogen), registrado para utilizar el Hydro y recibir certificados, permitiendo que el sistema se comunique con blockchain por unidad Hydro. El sistema monitorea a un proveedor (por ejemplo, una institución financiera) que registra un libro público y luego transmite la dirección registrada a Hydro. Esta dirección se escribe sin cambios en el blockchain, en una whitelist almacenada en un smart contract de Hydro. El sistema recibe una confirmación de que la dirección se incluyó en la whitelist, que también se puede verificar a través de la vista pública. El sistema debe registrarse solo una vez, mientras que la whitelist de Accessor solo debe mostrarse una vez por Accesor.



Una vez que se completa la inicialización, el núcleo del proceso de autenticación Hydro puede comenzar. El descriptor de acceso, que debe llevar a cabo una transacción de la Raindrop se inicia este proceso preguntando detalles Raindrop del sistema y el sistema transfiere la solicitud a Hydro. El Hydro crea una nueva Raindrop, tiendas de detalles específicos blockchain sin cambios y devuelve todos los detalles Accessor a través del sistema. El proveedor, con toda la información requerida, realiza una transacción desde la dirección registrada a un método en el smart contract de Hydro. Si la dirección no figura en la lista blanca, la acción se rechaza; de lo contrario, se registra en el smart contract. Es importante tener en cuenta que esta operación debe tener lugar fuera del sistema directamente desde el de accessor a Blockchain, ya que deben ser firmados con la clave privada del de accessor (que sólo pueden ser adquiridos Accessor).



El último paso en el proceso es la Validación. En este paso, Accessor solicita acceso al sistema a través del mecanismo del sistema instalado. Antes de aplicar cualquiera de los protocolos de autenticación estándar, el sistema pregunta a Hydro si Accessor ha realizado o no una transacción válida de Raindrop. Hydro trabaja con el smart contract, verifica la validez y responde con una determinación verdadera / falsa. El sistema está en posición de decidir cómo proceder basándose en esta determinación: si es falso, el sistema puede denegar el acceso, y si es verdadero (verdadero), el sistema puede proporcionar acceso.



Teniendo en cuenta las credenciales del sistema central o el protocolo del sistema existente, como factor de autenticación, es importante que Hydro proporcione un segundo factor. Al examinar las dos agencias principales de ataque, podemos confirmar inmediatamente su utilidad:

- Vector 1 - El atacante roba las credenciales del sistema de accessor
    - El atacante intenta obtener acceso al sistema con credenciales de sistema válidas
    - El sistema verifica con Hydro para ver si hubo una transacción de blockchain válida
    - Hydro devuelve falso y el sistema niega el accessor
- Vector 2 – El atacante roba la clave privada de la billetera de Accessor
    - El atacante intenta realizar una transacción de Hydro desde la dirección registrada, sin necesidad de detalles de Raindrop
    - El atacante no puede realizar una transacción de blockchain válida

- El atacante tampoco puede solicitar acceso al Sistema sin las credenciales adecuadas del Sistema

Está claro que el atacante debe robar las credenciales del sistema clave de Accessor y la clave de billetera privada de Accessor para obtener acceso al sistema. En este sentido, Hydro ha agregado con éxito un factor de autenticación adicional.

Apertura de la Raindrop al público

Si bien este servicio de autenticación basado en blockchain fue diseñado para ayudar a proteger el ecosistema API de Hydrogen, es ampliamente aplicable a diferentes plataformas y sistemas. Debido a que sentimos que otros pueden beneficiarse potencialmente de esta capa de verificación, la estamos abriendo para su uso.

Así como Hydrogen lo integrará como una condición previa para el acceso a su ecosistema de API, también lo puede agregar cualquier sistema a los procedimientos y protocolos existentes. Cualquier plataforma, ya sea una API, una aplicación, un software empresarial, una plataforma de juegos, etc., puede aprovechar Hydro para fines de autenticación. La documentación formal estará disponible en GitHub para aquellos que deseen incorporar esta capa de cadena de bloques en un marco de autenticación o API REST.

Case Study – Raindrop With OAuth 2.0

Hay muchas maneras en que Raindrop puede ser utilizado por organizaciones privadas. Las API privadas, bases de datos y redes han creado sistemas de tokens procesados, claves, aplicaciones y protocolos durante la última década en un esfuerzo por proteger los datos confidenciales. Google, por ejemplo, se ha convertido en uno de los proveedores de productos más populares en el mercado con Google Authenticator. Como se mencionó anteriormente, no hay ninguna razón para competir o reemplazar estos protocolos existentes.

Como estudio de caso (Case Study), presentamos una breve descripción de cómo Hydrogen implementa la certificación Hydro como un nivel de seguridad en el marco general de seguridad de la API:

1. Los socios de Hydrogen API primero deben tener las direcciones IP de sus diversos entornos en la whitelist.
2. Los socios deben solicitar una whitelist de una dirección Hydro pública.
3. Todas las llamadas a las API de Hydrogen y las transferencias de datos se codifican y transmiten a través del protocolo HTTPS.
4. Los socios deben completar una transacción de Hydrogen válida desde la dirección Hydro registrada.

5. Los socios deben usar la validación de OAuth 2.0. OAuth (Open Authorization) es un estándar abierto para autenticación y autorización basada en tokens. Hydrogen admite los tipos de subvención "Credenciales de contraseña de propietario de recurso" y "Credenciales de cliente", y cada usuario de API debe proporcionar credenciales para una solicitud de autenticación.
6. Si no se infringe ninguno de los cinco elementos anteriores, al socio de Hydrogen se le concede un token único, que se comprobará y verificará con cada llamada API.
7. El token es válido por 24 horas, después de lo cual el socio debe validar de nuevo.

Si se infringe alguno de estos pasos, el acceso a la API bloquea inmediatamente al usuario. Un pirata informático no puede eludir estos agentes de seguridad asumiendo al azar porque hay trillones de combinaciones únicas.

La autenticación basada en Hydro Blockchain es un componente importante del protocolo de seguridad del Hidrógeno. El equipo de Hydrogen alienta a los socios a configurar carteras multi-firma y almacenar claves privadas en múltiples ubicaciones seguras independientemente de otras credenciales, por lo que no existe un solo punto de falla. Una billetera multi-firma debidamente asegurada no solo es difícil de robar, sino que la naturaleza pública de la cadena de bloques también permite el rápido reconocimiento de cualquier robo en lo que se refiere a la seguridad de la API.

Cualquiera puede ver un intento de autenticación en el smart contract de Hydro, lo que significa que los días en que las plataformas se ven comprometidas durante meses pueden ser cosa del pasado. Los piratas informáticos API ahora se pueden evitar con mayor inmediatez debido a la capacidad de detectar intentos inesperados de autorización en tiempo real desde cualquier parte del mundo.

Peligros

Al igual que cualquier tecnología incipiente, como los primeros días de las redes sociales, correo electrónico y aplicaciones de transmisión (que dependían de la conectividad de acceso telefónico), es importante que el equipo de desarrollo central siga de cerca los nuevos desarrollos en velocidades y volúmenes de transacciones de Ethereum. ¿Te imaginas YouTube intentando lanzar en 1995? ¿O que Instagram se ofreció por primera vez en Blackberry?

Los principales desarrolladores de Ethereum, como Vitalik Buterin y Joseph Poon, han propuesto actualizar el protocolo de Ethereum Plasma: Scalable Autonomous Smart Contracts :

> **Plasma es un marco propuesto para la ejecución incentivada e implementada de contratos inteligentes que es escalable a una cantidad significativa de actualizaciones estatales por segundo (potencialmente miles de millones), lo que permite que blockchain pueda representar una cantidad significativa de aplicaciones financieras descentralizadas en todo el mundo. Estos contratos inteligentes están incentivados para continuar su funcionamiento de manera autónoma a través de tarifas de transacción de red, que es en última instancia, depende de la cadena de bloques subyacente (por ejemplo, Ethereum) para hacer cumplir las transiciones de estados transaccionales.**

Otros, como The Raiden Network, han propuesto un alejamiento de la cadena (off-chain) diseñada para impulsar transacciones más rápidas y reducir los impuestos. En este momento, Raindrop ejercerá una presión mínima sobre el marco de Ethereuem, por lo que la escalabilidad es un riesgo muy pequeño para el éxito de la tecnología.

Conclusión

La inmutabilidad de un blockchain público ofrece nuevas formas de mejorar la seguridad de los sistemas privados como las API.

Este documento mostró tres cosas importantes:

1. Las public blockchain pueden agregar valor en los servicios financieros.
2. Hydro Raindrop puede mejorar la seguridad de los sistemas privado.
3. Hay aplicaciones directas de Hydro Raindrop dentro de la plataforma API de Hydrogen.

El equipo de Hydro cree que el marco establecido puede ser la infraestructura de seguridad estándar para un nuevo modelo de sistemas públicos privados híbridos, que beneficiará a todas las partes interesadas en la industria de servicios financieros y más allá.

Fuentes:

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