Hydro Raindrop

Public Authentication On The Blockchain

Januar 2018

INHALTSVERZEICHNIS

Zusammenfassung

HYDRO: Etymologie – Von altgriechischem Wort ὕδρο (*hydro*), was kommt aus dem Wort ὑδωρ.

Hydro ermöglicht neuen und bestehenden privaten Systemen, die unveränderliche und transparente Dynamik einer Blockchain zu integrieren und auszunutzen, um Anwendungs- und Dokumentensicherheit, Identitätsmanagement, Transaktionen und künstliche Intelligenz zu verbessern.

In diesem Dokument wird auf private Systeme wie APIs verwiesen, die die öffentliche Blockchain von Hydro zur Verbesserung der Sicherheit durch öffentliche Authentifizierung verwenden (public authentication).

Die vorgeschlagene Technologie wird "Raindrop" genannt - eine Transaktion, die durch einen intelligenten Vertrag erfolgt (smart contract), der den privaten Zugriff auf das System öffentlich validiert und bestehende private Zertifizierungsmethoden ergänzen kann. Technologie zielt darauf ab, zusätzliche Sicherheit für sensible Finanzdaten zu bieten, die zunehmend von Piraterie und Verstößen bedroht sind.

Die erste Implementierung von Hydro Raindrop erfolgt auf der Hydrogen API-Plattform. Dieses modulare API-Paket steht Unternehmen und Entwicklern weltweit zur Verfügung, um hochentwickelte Plattformen und Financial-Engineering-Produkte zu initiieren, zu konstruieren, zu testen und zu entwickeln.

Hydro Raindrop wird der weltweiten Entwicklergemeinschaft als Open-Source-Software zur Verfügung stehen, sodass Entwickler Hydro Raindrop mit jeder REST-API integrieren können.

Blockchain & Ethereum

Hydro wird im Ethereum-Netzwerk implementiert. Bevor Sie mehr über das Projekt erfahren, ist es wichtig, einige grundlegende Ideen zu Blockchain und Ethereum zu verstehen.

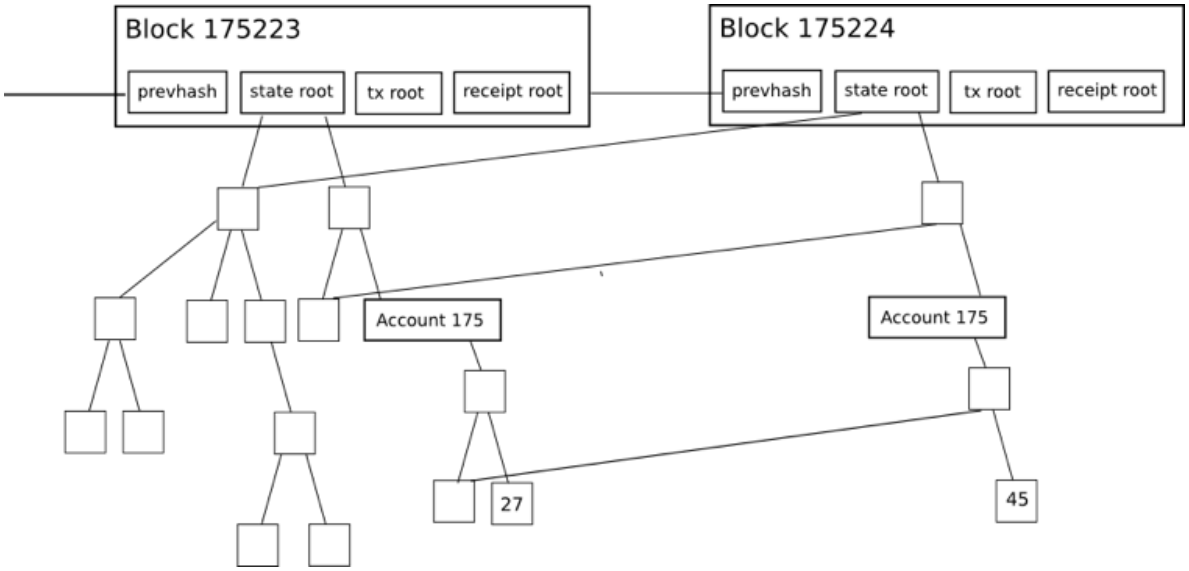
Aufbauend auf Ethereum

Da Apps wie Snapchat mit Swift und anderen Tools der Apple Ios-Plattform erstellt wurden, können Blockchain-Anwendungen auf Ethereum basieren. Snap Inc. musste Ios nicht erstellen und nutzte es als Infrastruktur, um eine bahnbrechende Social-Media-Anwendung zu starten.

Project Hydro ist ähnlich. Es basiert auf Tausenden von Entwicklern weltweit und arbeitet daran, die zugrundeliegende Blockchain-Technologie schneller, leistungsfähiger und effizienter zu machen. Hydro nutzt diese kontinuierlich verbesserte Infrastruktur durch die Entwicklung produktzentrierter Interaktionen rund um die Blockchain-Technologie, die Finanzdienstleistungsanwendungen erhebliche Vorteile bieten können.

Merkle Trees

Merkle Bäume werden in verteilten Systemen für eine effektive Datenverifizierung verwendet. Sie sind effektiv, weil sie die sogenannten Hashes anstelle von vollständigen Datensätzen verwenden. Hashes sind Dateicodierungsmethoden, die viel kleiner sind als die Datei selbst. Jeder Blockkopf in Ethereum enthält drei Merkle-Bäume für Transaktionen, Einnahmen und Status:



Quelle: Merkling in Ethereum; Vitalik Buterin, Ιδρυτής Ethereum

Dies erleichtert es einem Light Client, nachprüfbare Antworten auf Fragen wie:

- Ist dieser Account verfügbar?
- Wie ist das aktuelle Gleichgewicht?
- Wurde diese Transaktion in einen bestimmten Block aufgenommen?
- Ist an dieser Adresse heute ein bestimmtes Ereignis aufgetreten?

Smart Contracts

Ein Schlüsselmerkmal von Ethereum und anderen blockchain-basierten Netzwerken sind Smart Contracts. Hierbei handelt es sich um selbstausführbare Code-Blöcke, die mit mehreren Teilen interagieren können, wodurch die Notwendigkeit zuverlässiger Vermittler entfällt. Der Code in einem Smart-contract kann als ähnlich zu den gesetzlichen Klauseln eines Papiervertrags angesehen werden, aber es kann auch aufgrund erweiterter Funktionalität mehr erreichen. Solche Verträge können Regeln, Bedingungen und Strafen für Nichteinhaltung oder andere Verfahren enthalten. Wenn sie aktiviert sind, werden sie wie ursprünglich gemeldet ausgeführt, wenn sie in der öffentlichen Kette installiert werden, wobei eingebettete Daten bereitgestellt werden, die unverändert und dezentralisiert sind.

Intelligente Verträge sind ein wichtiges Instrument für den Aufbau der Ethereum-Infrastruktur. Die grundlegende Funktionalität der Hydro-Blockchain-Layer wird durch benutzerdefinierte Verträge erreicht, wie weiter unten in diesem Artikel beschrieben.

Virtuelle Maschine Ethereum

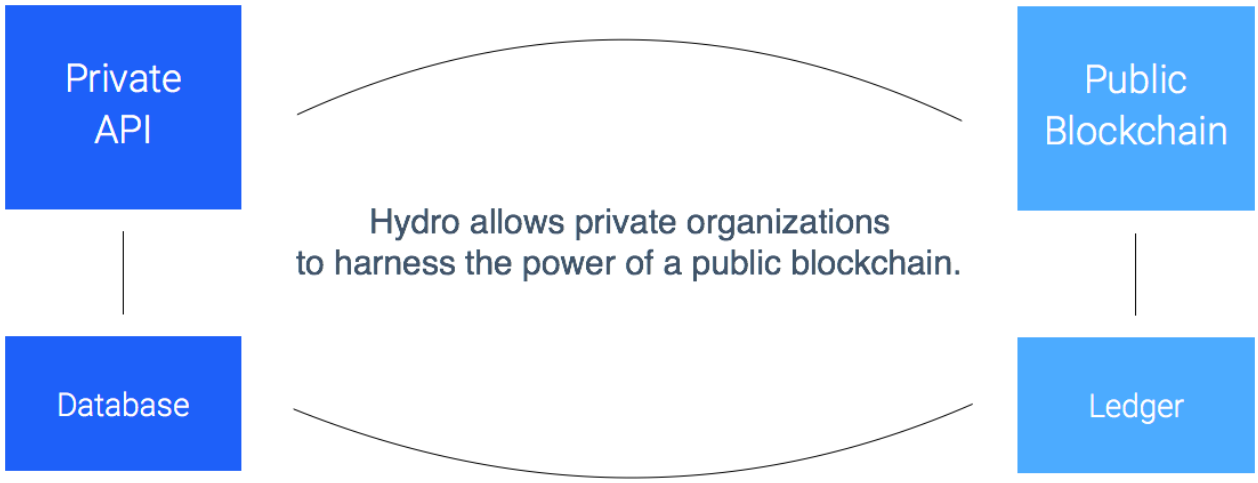
Die Ethereum Virtual Machine (EVM) ist die Ausführungsumgebung für Smart Contracts in Ethereum. EVM beugt Denial-of-Service-Angriffen (DoS) vor, stellt sicher, dass Programme unbeeinträchtigt bleiben und ermöglicht eine unterbrechungsfreie Kommunikation. Aktionen auf dem EVM haben mit ihnen verbundene Kosten, genannt Gas, die von den erforderlichen Rechenressourcen abhängen. Jede Transaktion verfügt über eine maximale Gasmenge, die als Gaslimit bezeichnet werden kann. Wenn das von einer Transaktion verbrauchte Gas das Limit erreicht, unterbricht es den Prozess.

Public Ledger

Public Ledger für private Systeme

Die Systeme, die Finanzdienstleistungsplattformen verwalten, Websites und Anwendungen können oft als Mittel der Datenfluss beschrieben - senden, empfangen, zu speichern, zu aktualisieren und Prozessdaten über die Personen, mit denen sie interagieren. Aufgrund der Natur dieser Daten und Finanzdienstleistungen im Allgemeinen haben diese Systeme oft komplexe Funktionen in einer privaten und zentralisierten Art und Weise. Das Vertrauen in privaten Strukturen, die wiederum öffnet die Tür zu einer Vielzahl von Sicherungen, die Transparenz sowie Effizienzgewinne, um die Integration von externen Kräften anzunehmen, die den Umfang des inneren Systems übersteigen würde.

Dies ist bei der Hydro API-Plattform der Fall. Hydro möchte die oben genannten Vorteile nutzen, indem es Hydrogen users ermöglicht, mit einer Blockchain auf eine Art und Weise zu interagieren, die nahtlos in das grundlegend private Wasserstoff-Ökosystem integriert ist.

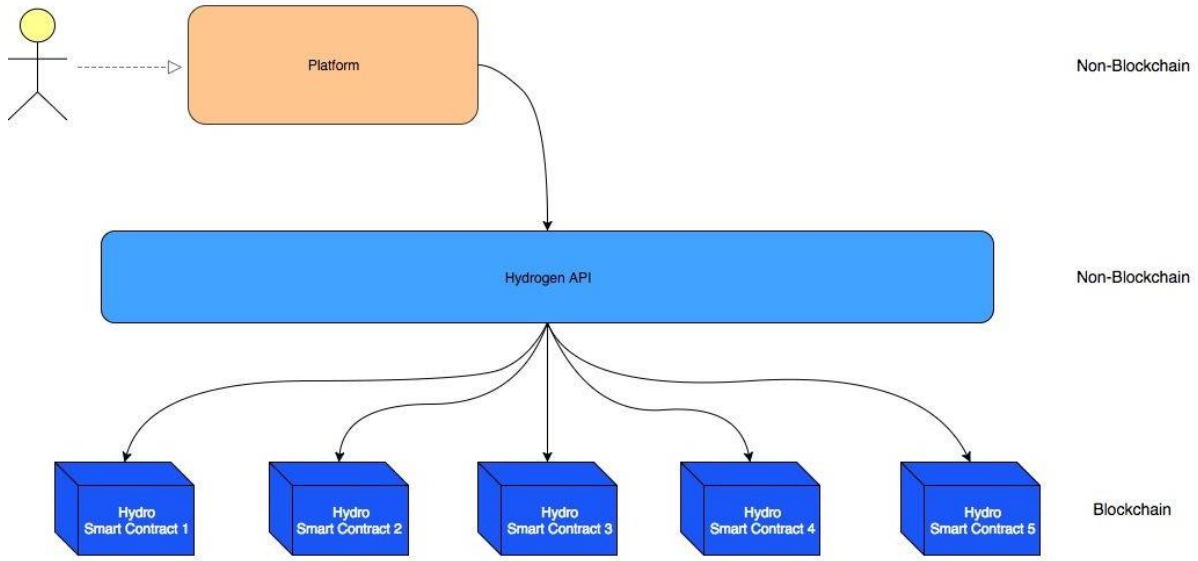


Blockchain-basierte öffentliche Funktionen können vor, während oder nach privaten Operationen ausgeführt werden. Die Interaktion zwischen privaten und öffentlichen Daten kann dazu dienen, Prozesse innerhalb eines Ökosystems zu validieren, zu versiegeln, aufzuzeichnen oder zu verbessern.

Der Ethos dieses Modells macht die Prozesse robuster, indem die Vorteile der Blockchain-Technologie genutzt werden, insbesondere dort, wo es die meisten positiven Effekte erzielen kann. Obwohl diese hybride Struktur möglicherweise nicht für alle Plattformen gilt, konzentriert sich Hydro auf die Bereitstellung von Werten für die Situationen, in denen es vorhanden ist.

Architecting for Adoption

Hydro unterscheidet sich von vielen bestehenden Blockchain-Initiativen, da es unabhängig und um neue oder bereits vorhandene Systeme herum platziert werden kann, ohne dass systematische Änderungen erforderlich sind. Anstatt zu ersetzen, versucht Hydro, sich zu verbessern. Die mit der Hydrogen API verbundenen Plattformen und Institutionen können automatischen Zugriff auf die Blockchain haben.



Die Bandbreite der Finanzdienstleistungsplattformen, die Wasserstoff nutzen können, ist breit. Diese Plattformen können nahezu jede Erfahrung bereitstellen, eine beliebige Anzahl von proprietären Diensten hosten, jede private Datenoperation ausführen und in jeder Umgebung wachsen. Dies wird durch die strukturelle Anpassung von Wasserstoff erreicht und arbeitet mit Hydro, das als ergänzender Leitfaden für die Einführung dient.

Raindrop

In das öffentliche Hauptbuch von Hydro integriert, gibt es eine Blockchain, die auf dem Authentifizierungsdienst "Raindrop" basiert. Dies bietet eine eindeutige, unveränderte, weltweit sichtbare Sicherheitsschicht, die überprüft, ob eine Zugriffsanforderung von einer genehmigten Quelle stammt.

Private Authentifizierungsprotokolle wie OAuth 2.0 bieten unterschiedliche Robustheits- und Nutzenniveaus für die vorhandenen Anwendungsbereiche. Es besteht kaum ein Bedarf, zu konkurrieren oder zu versuchen, diese Protokolle zu ersetzen. Hydro bietet eine Möglichkeit, diese zu verstärken, indem die Blockchain-Mechanismen als Teil des Authentifizierungsprozesses integriert werden. Dies kann eine nützliche Sicherheitsschicht hinzufügen, um Systemverstöße und den Verlust vertraulicher Informationen zu verhindern.

Bevor wir uns mit dem technischen Aspekt von Raindrop befassen, betrachten wir das Problem, das es zu lösen versucht.

Die Situation der finanziellen Sicherheit

Das Datenalter hat die Anfälligkeit für Systeme erhöht, und dies ist besonders wichtig für Finanzdienstleistungen. Finanzplattformen können als Gateways zu einer großen Anzahl von privaten und sensiblen Daten wie Identitätsnummern, Kontodaten und Transaktionshistorien angesehen werden. Aufgrund der Bedeutung von Identifikationsdaten, Zugriff auf diese aus unerwünschten Quellen folgen Sie oft katastrophalen Ergebnissen.

Trend Micro hat einen Bericht veröffentlicht, der besagt, dass gestohlene persönliche Identifikationsdaten, die als personenbezogene Daten bezeichnet werden, im Deep Web für nur 1 US-Dollar verkauft werden. Dokumentenscans wie Pässe sind für nur 10 US-Dollar verfügbar Verknüpfung mit Bankkonten von nur $ 200, so dass die Verbreitung von gestohlenen Daten leicht zugänglich ist.

Das bestehende Finanzsystem hat jedoch keine kristallklare Geschichte, wenn es um die Prävention, Diagnose und Kommunikation von Datenverletzungen mit Aktionären geht.

- Laut einer aktuellen Studie von Javelin Strategy & Research - *The 2017 Identity Fraud Study* - $ 16 Milliarden gestohlen von 15,4 Millionen US-Konsumenten im Jahr 2016 aufgrund von Ausfällen des Finanzsystems zum Schutz personenbezogener Daten (PII).

- Im April 2017 veröffentlichte Symantec den Bericht *Internet Security Threat Report*, Schätzungen zufolge wurden im Laufe des Jahres 2016 1,1 Mrd. PII-Dateien verschiedenen Quellen zur Verfügung gestellt.

- Im Artikel *2016 Year End Data Breach Quickview* von Risk Based Security wurde 2016 festgestellt, dass es weltweit 4,19 Datenverletzungen in Unternehmen gab, die mehr als 4,2 Milliarden Datensätze enthielten.

- Im *2017 Thales Data Threat Report – Financial Services Edition*, Eine Umfrage unter globalen IT-Experten im Bereich der professionellen Dienstleistungen ergab, dass 49% der Finanzdienstleistungsunternehmen in der Vergangenheit einen Sicherheitsverstoß begangen haben, 78% mehr für den Schutz selbst ausgeben, aber 73% neue Initiativen im Zusammenhang mit KI starten , IoT und Cloud-Technologien, bevor sie die richtigen Sicherheitslösungen vorbereiten.

Equifax Breach

Am 29. Juli 2017 wurde Equifax, eine 118-jährige US-Kreditberichterstattungsagentur, gehackt. 143 Millionen PPS-Nutzer waren betroffen, darunter Sozialversicherungsnummern, da die Kreditkartendaten von 209.000 Kunden verletzt wurden.

Was war der Grund für diesen Verstoß?

Es begann mit einer der von Equifax verwendeten Backend-Technologien. Struts ist ein Open-Source-Framework für die Entwicklung von Webanwendungen in der Programmiersprache Java, die von der Apache Software Foundation entwickelt wurde. Die CVE-2017-9805 ist ein Schwachpunkt in Apache Struts bei der Verwendung des Struts-REST-Plugins mit dem XStream-Handler zur Verarbeitung von XML-Ladevorgängen. Bei einem Verstoß kann der Angreifer dann Schadcode auf dem Decorator der App ausführen, um entweder die Engine zu übernehmen oder weitere Angriffe von ihr zu starten. Dies wurde von Apache gepatcht zwei Monate vor der Verletzung von Equifax.

Apache Struts enthält einen Fehler in der XSTREAM-Plugin-REST, der ausgelöst wird, wenn das Programm die Benutzereingabe für XML-Anforderungen verringert. Das Problem tritt insbesondere mit der toObject () -Methode von XStreamHandler auf, die bei der Verwendung der XStream-De-Segregation in einem Objekt keine Beschränkungen für den eingehenden Wert auferlegt, was zu willkürlichen Sicherheitsanfälligkeiten bei der Codeausführung führt.

Selbst wenn das REST-Plugin verfügbar wäre, wäre das von Bedeutung? Gibt es einen Weg zur Blockchain-Technologie, um die Finanzinformationen von 143 Millionen Kunden zu sichern und gleichzeitig auf bestehende REST-API- und Java-Systeme zu setzen?

Adding a Blockchain Layer

Es ist klar, dass die Integrität der Finanzdatengatter verbessert werden kann.

Schauen wir uns an, wie ein zusätzliches Sicherheitsniveau durch Hydro erreicht werden kann.

Die wesentlichen Konsensmechanismen von Ethereum stellen die Gültigkeit von Transaktionen sicher, da die Teilnehmer gemeinsam ordnungsgemäß signierte Transaktionen bearbeiten. Diese Tatsache führt zu Dezentralisierung und Stabilität, vor allem aber bietet sie einen Vektor, um unerlaubten Zugriff auf ein Gateway, das mit sensiblen Daten umgeht, zu mindern.

Bei Hydro kann die Authentifizierung von Transaktionen in der Blockchain abhängen. Eine API kann beispielsweise Entwickler und Anwendungen validieren, indem sie bestimmte Transaktionen mit einer bestimmten Datenlast zwischen bestimmten Adressen in der Blockchain starten, sofern ein Authentifizierungsprotokoll gestartet wird.

The Hydro Raindrop

Rain enthält konzentrierte Wasserpackungen mit einem Durchmesser von 0,0001 bis 0,005 Zentimetern. In einem typischen Sturm gibt es Milliarden dieser Pakete, jede mit zufälliger Größe, Geschwindigkeit und Form. Aus diesem Grund kann man die genaue Natur des Regens nicht genau vorhersagen. Genauso ist jede Hydro-Authentifizierungstransaktion einzigartig und praktisch unmöglich zufällig - wir nennen das also Raindrops.

Finanzdienstleistungsplattformen verwenden typischerweise die Mikrokreditverifizierung, um Kundenkonten zu validieren. Die Idee ist einfach: Die Plattform erzeugt kleine Einzahlungen von zufälligen Summen auf Bankkonten, die von Benutzern angegeben werden. Um nachzuweisen, dass der Benutzer dieses Konto tatsächlich besitzt, muss er die Einzahlungsbeträge zurück auf die Plattform überweisen, die dann validiert werden. Die einzige Möglichkeit, wie der Benutzer die gültigen Beträge kennen kann (außer zu raten), ist der Zugriff auf diese Bankkonten.

Verifizierung basierend auf Raindrop mit Hydro ist proportional. Anstatt einen Betrag an den Benutzer zu senden und weiterzuleiten, definieren wir eine Transaktion und der Benutzer muss sie aus einer bekannten Geldbörse ausführen. Die einzige Möglichkeit für einen Benutzer, eine gültige Transaktion durchzuführen, besteht darin, auf diese Brieftasche zuzugreifen.

Mit Hilfe von Raindrops können sowohl das System als auch der Accessor den Autorisierungsaufwand in einem unveränderten öffentlichen Hauptbuch verfolgen. Diese blockchain-basierte Transaktion wird von den grundlegenden Systemfunktionen getrennt, erscheint in einem verteilten Netzwerk und hängt vom Besitz der privaten Schlüssel ab. Daher dient es als nützliches Validierungselement.

Ein sorgfältiger Blick

Der Identitätsprüfungsprozess von Hydro umfasst vier Elemente:

1. *Accessor* - Die Gruppe sucht Zugang zu einem System. Im Falle von Wasserstoff ist Accessor eine Finanzinstitution oder Anwendung, die Wasserstoff-APIs für ihre digitale Kerninfrastruktur verwendet.
2. *System* - Es ist das System oder Gateway, auf das Accessor Zugriff hat. Für Hydrogen ist das System die Hydrogen API selbst.
3. *Hydro* - Das Modul, das vom System zur Kommunikation und Verbindung mit der Blockchain verwendet wird.
4. *Blockchain* – Das verteilte Public Ledger, das HYDRO-Transaktionen verarbeitet und die Hydro smart-Verträge enthält, über die Informationen importiert, empfangen oder betrieben werden können.

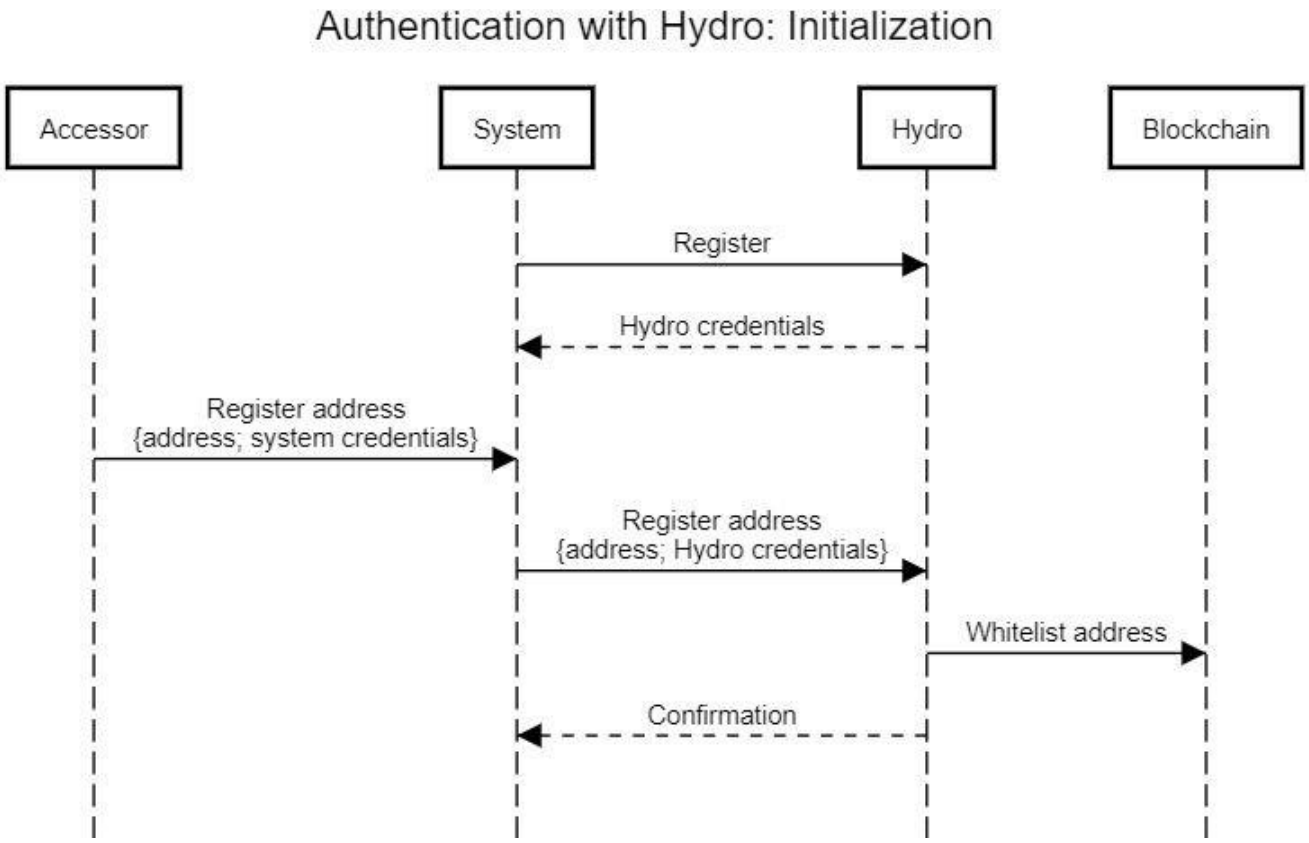
Jeder Raindrop besteht aus einer Reihe von fünf Handelsparametern:

1. *Sender* - Die Adresse, mit der die Transaktion beginnen soll.
2. *Receiver* - Das Ziel der Transaktion. Dies entspricht dem Aufruf einer Methode in einen Hydro Smart-contract.
3. *ID* - Eine Kennung, die dem System zugeordnet ist.
4. *Quantity* - Eine genaue HYDRO-Nummer, die für den Versand ausgewählt wurde.
5. *Challenge* - Eine zufällig produzierte alphanumerische Serie.

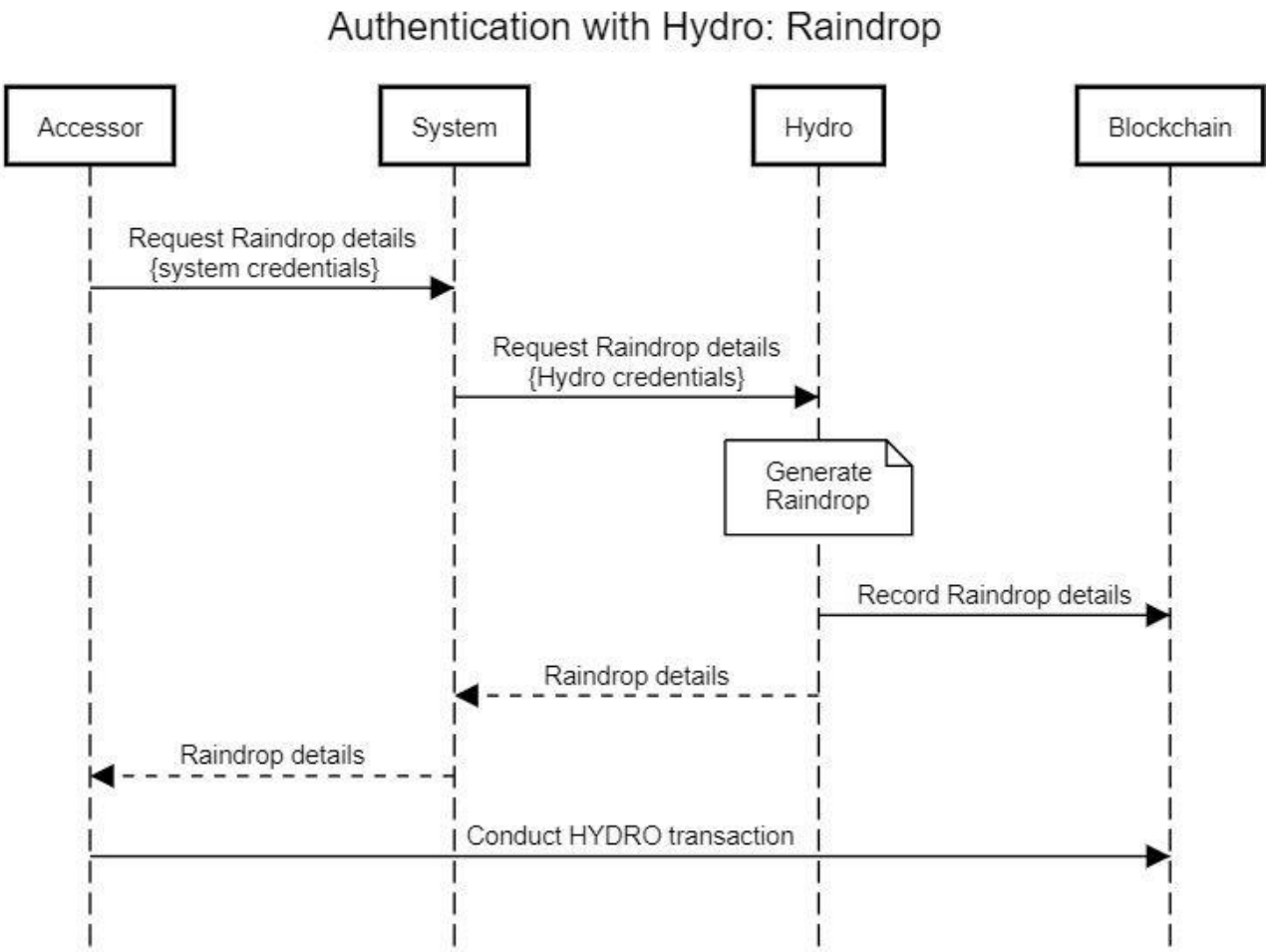
Im Folgenden finden Sie eine Zusammenfassung des Authentifizierungsprozesses, der im Allgemeinen in drei Phasen unterteilt werden kann:

1. Initialization (Initialisierung)
2. Raindrop
3. Validation (Validierung)

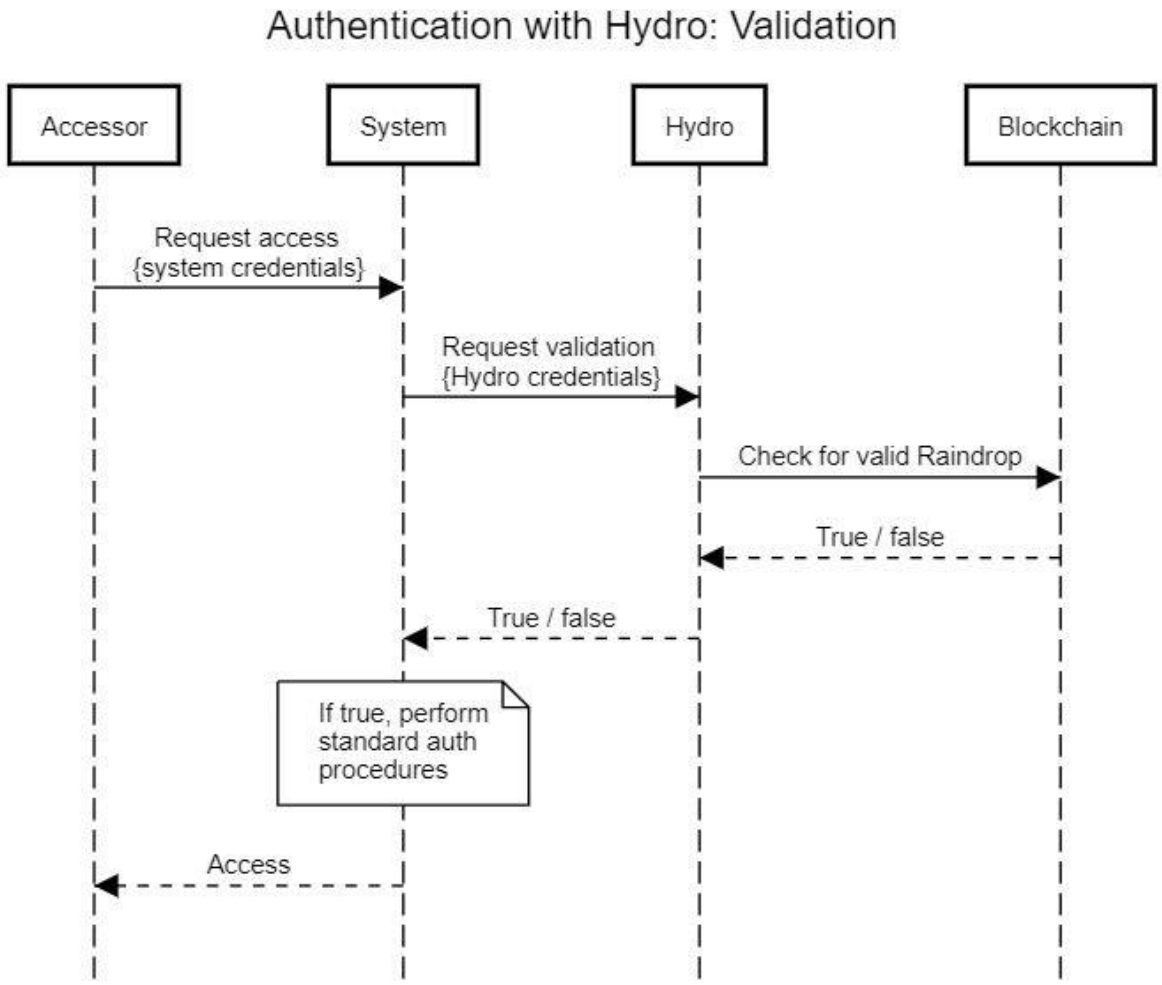
Die Initialisierung beginnt mit einem System (z. B. Wasserstoff), das für die Verwendung von Hydro registriert ist und Zertifikate empfängt, damit das System über die Hydro-Einheit mit der Blockchain kommunizieren kann. Das System überwacht einen Accessor (z. B. ein Finanzinstitut), der ein öffentliches Hauptbuch registriert und dann die registrierte Adresse an Hydro übermittelt. Diese Adresse wird unverändert in der Blockchain in einer Whitelist geschrieben, die in einem Hydro Smart-contract gespeichert ist. Das System erhält eine Bestätigung, dass die Adresse auf die whitelist gesetzt wurde, was auch durch die öffentliche Ansicht überprüft werden kann. Das System muss nur einmal registriert werden, während die Accessor-Whitelist nur einmal pro Accessor angezeigt werden muss.



Sobald die Initialisierung abgeschlossen ist, kann der Kern des Hydro-Authentifizierungsprozesses beginnen. Der Accessor, der eine Transaktion durchführen müssen Regentropfen beginnt diesen Prozess, indem Details Raindrop aus dem System fragen und überträgt das System die Anfrage an Hydro. Die Hydro schafft einen neuen Raindrop, speichert spezifische Details blockchain unverändert und gibt alle Details Accessor durch das System. Accessor führt mit allen erforderlichen Informationen eine Transaktion von der registrierten Adresse zu einer Methode im Hydro smart-contract durch. Wenn die Adresse nicht auf die whitelist gesetzt wird, wird die Aktion zurückgewiesen - andernfalls wird sie im Smart-contract aufgezeichnet. Es ist wichtig zu beachten, dass diese Transaktion außerhalb des Systems übernehmen sollte direkt aus dem Accessor Blockchain, da sie mit dem privaten Schlüssel von Accessor (die nur Accessor erworben werden können) zu unterzeichnen.



Der letzte Schritt in diesem Prozess ist die Validierung. In diesem Schritt fordert Accessor über den installierten Systemmechanismus Zugriff auf das System an. Bevor Sie eines der Standard-Authentifizierungsprotokolle anwenden, fragt das System Hydro, ob Accessor eine gültige Raindrop-Transaktion durchgeführt hat oder nicht. Hydro arbeitet mit dem Smart-contract, prüft die Gültigkeit und antwortet mit einer wahren / falschen Bestimmung. Das System ist in der Lage zu entscheiden, wie auf der Grundlage dieser Bestimmung gehen - wenn falsch (false), das System den Zugriff verweigern kann, wenn es wahr (true) ist, kann das System den Zugriff.



Unter Berücksichtigung der Anmeldeinformationen des Kernsystems oder des vorhandenen Systemprotokolls als Authentifizierungsfaktor ist es wichtig, dass Hydro einen zweiten Faktor bereitstellt. Durch die Untersuchung der beiden primären Angriffsagenturen können wir sofort ihre Nützlichkeit bestätigen:

- Attacker 1 - Der Angreifer stiehlt die Anmeldeinformationen des Accessor-Systems
    - Der Angreifer versucht, mit gültigen System Anmeldeinformationen auf das System zuzugreifen
    - Das System prüft mit Hydro, ob eine gültige Blockchain-Transaktion vorliegt
    - Hydro gibt false zurück und das System verweigert den Zugriff
- Attacker 2 – Angreifer stiehlt den privaten Schlüssel aus Accessors Brieftasche
    - Angreifer versucht, eine Hydro-Transaktion von der registrierten Adresse aus durchzuführen, ohne dass Raindrop-Details benötigt werden
    - Angreifer kann keine gültige Blockchain-Transaktion erstellen

- Der Angreifer kann den Zugriff auf das System auch nicht ohne ordnungsgemäße System Anmeldeinformationen anfordern

Es ist klar, dass der Angreifer sowohl die Zugangsdaten des Accessors als auch den privaten Zugangsschlüssel des Accessors stehlen muss, um Zugang zum System zu erhalten. In diesem Zusammenhang hat Hydro erfolgreich einen zusätzlichen Authentifizierungsfaktor hinzugefügt.

Opening the Raindrop to the public

Obwohl dieser Blockchain-basierte Authentifizierungsdienst entwickelt wurde, um das Hydrogen-API-Ökosystem zu gewährleisten, ist er weitgehend auf verschiedene Plattformen und Systeme anwendbar. Da andere von diesem Grad der Verifizierung und Sicherheit profitieren können, ist es offen für den Einsatz.

Genauso wie Hydrogen es als Voraussetzung für den Zugriff auf das API-Ökosystem einbaut, kann jedes andere System es zu bestehenden Prozeduren und Protokollen hinzufügen. Jede Plattform, ob API, Anwendung, Unternehmenssoftware, Spieleplattform usw., kann Hydro für Authentifizierungszwecke verwenden. Das Dokument wird in GitHub für diejenigen verfügbar sein, die diese Blockchain-Ebene in einen REST-Authentifizierungsrahmen oder eine API integrieren möchten.

Case Study – Raindrop With OAuth 2.0

Es gibt Dutzende von Möglichkeiten, wie Raindrop von privaten Organisationen genutzt werden kann. Private APIs, Datenbanken und Netzwerke haben in den letzten zehn Jahren verarbeitete Token systeme, Schlüssel, Anwendungen und Protokolle erstellt, um sensible Daten zu schützen. Google hat sich beispielsweise mit Google Authenticator zu einem der beliebtesten Produktanbieter auf dem Markt entwickelt. Wie bereits erwähnt, gibt es keinen Grund, diese bestehenden Protokolle zu konkurrieren oder zu ersetzen.

Als Fallstudie (Case Study) gibt es einen kurzen Überblick darüber, wie Hydrogen Hydro-Zertifizierung als Sicherheitsstufe im gesamten Sicherheitsrahmen der API implementiert:

1. Hydrogen-API-Partner sollten in erster Linie die IP-Adressen ihrer verschiedenen Umgebungen auf der whitelisted haben.
2. Οι συνεργάτες θα πρέπει να υποβάλουν αίτηση για μια λίστα επιτρεπόμενων επιδόσεων ως διεύθυνση Hydro.
3. Alle Aufrufe an Hydrogen-APIs und Datenübertragungen werden verschlüsselt und über das HTTPS-Protokoll übertragen.
4. Partner müssen eine gültige Hydro-Raindrop-Transaktion von der registrierten Hydro-Adresse durchführen.

5. Partner sollten die OAuth 2.0-Validierung verwenden. OAuth 2.0 (Open Authorization) ist ein offener Standard für Authentifizierung und tokenbasierte Autorisierung. Hydrogen unterstützt die Erteilungsarten "Besitzerkennwortzertifikate" und "Kundenzertifikate", und jeder API-Benutzer muss Anmeldeinformationen für eine Authentifizierungsanforderung angeben.
6. Wenn keiner der oben genannten Punkte verletzt wird, verfügt der Hydrogen Partner über ein eindeutiges Token, das bei jedem API-Aufruf überprüft und verifiziert werden muss.
7. Das Token ist 24 Stunden gültig, nach 24 Stunden wird der Partner erneut validiert.

Wenn einer dieser Schritte verletzt wird, wird der Benutzer sofort durch API-Zugriff gesperrt. Ein Hacker kann diese Sicherheitsagenten nicht umgehen, indem er zufällig annimmt, da es Billionen von einzigartigen Kombinationen gibt.

Die auf der Hydro-Blockchain basierende Authentifizierung ist ein wichtiges Element des Hydrogen Safety-Protokolls. Die Wasserstoffgruppe fördert seine Partner mehrere Signaturen Mappen (Multi-Signatur-Mappen) und speichern ihre privaten Schlüssel in mehreren sicheren Orten unabhängig von anderen Anmeldeinformationen zu erstellen, so dass es keine Schwachstelle. Ein Mehrfachsignaturen Portemonnaie ist richtig versichert ist nicht nur schwierig, gestohlen werden, aber die Öffentlichkeit der blockchain ermöglicht auch die schnelle Erkennung von Diebstahl, wie es um die Sicherheit API bezieht.

Jeder kann einen Versuch sehen, sich für den Hydro smart-contract zu authentifizieren, was bedeutet, dass die Tage der Plattformen, die auf dem Spiel stehen, schon seit Monaten vergangen sind. API-Hacker können jetzt direkter vermieden werden, weil sie von überall auf der Welt unerwartete Echtzeit-Autorisierungsversuche erkennen können.

Risks

Wie bei allen neuen Technologien, wie z. B. den Anfängen von Social Media-, E-Mail- und Streaming-Anwendungen (abhängig von der Einwahl), ist es wichtig, dass das zentrale Entwicklungsteam neue Entwicklungen bei Transaktionsgeschwindigkeiten und -volumen genau überwacht von Ethereum. Könntest du dir vorstellen, dass YouTube 1995 anfangen möchte? Oder bietet Instagram zum ersten Mal Blackberry an?

Οι κύριοι προγραμματιστές του Ethereum, όπως οι Vitalik Buterin και Joseph Poon, πρότειναν την ενημέρωση στο πρωτόκολλο Ethereum Plasma: Scalable Autonomous Smart Contracts :

> **Plasma ist ein vorgeschlagene Rahmen für die Anreize und Durchsetzung intelligente Verträge, die einen signifikanten Anteil Status-Updates pro Sekunde (vielleicht Milliarden) skalierbar ist, so dass der blockchain eine beträchtliche Anzahl von dezentralen Finanzanwendungen Liste vertreten. Diese intelligenten Verträge sind motiviert, weiterhin autonom über die Netztransaktionsgebühren zu betreiben (Netztransaktionsgebühren), die letztlich auf dem blockchain Subjekt abhängen (zB Astraleum) zur Einführung Übergangs-Handelssituation ändert.**

Andere, wie The Raiden Network, haben eine Off-Chain-Lösung vorgeschlagen, die schnellere Transaktionen und niedrigere Gebühren ermöglicht. Gegenwärtig wird Raindrop sehr wenig Druck auf Ethereuem ausüben, so dass die Skalierbarkeit ein sehr kleines Risiko für den Technologieerfolg darstellt.

Fazit

Der unterbrechungsfreie Betrieb einer öffentlichen Blockchain bietet neue Möglichkeiten, die Sicherheit privater Systeme wie APIs zu verbessern.

Dieses Dokument zeigte drei wichtige Dinge:

1. Öffentliche Blockchains können Finanzdienstleistungen einen Mehrwert verleihen.
2. Hydro Raindrop kann die Sicherheit privater Systeme verbessern.
3. Es gibt direkte Anwendungen von Hydro Raindrop innerhalb der Hydrogen API-Plattform.

Das Hydro-Team ist der Ansicht, dass der geschaffene Rahmen die Standard-Sicherheitsinfrastruktur für ein neues hybrid-öffentlich-privates Modell sein kann, von dem alle Akteure in der Finanzdienstleistungsbranche und darüber hinaus profitieren werden.

Quelle:

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