Hydro Raindrop
ブロックチェーン上での公開認証
2018年　1月

目次

1.要旨

HYDRO：語源-ギリシャ語の”　υδρο-”(hydro-)が由来である．”水(water)”を意味しています．

Hydroは,既存及び既存のプライベートシステムを,パブリックブロックチェーンの不変で透過的なダイナミクスをシームレスに統合・活用し,アプリケーションおよびドキュメントのセキュリティ,ID管理,トランザクション,及び人工知能の強化を可能とします．

本稿では，APIのようなプライベートシステムのため，公開認証を使ってセキュリティ強化のためHydroパブリックブロックチェーンを使用するケースが作成されます．その提案された技術は「Raindrop(雨滴)」と呼称される．これは，公にプライベートシステムへのアクセスを検証し，既存の個人認証方式を保管が可能なスマートコントラクトによって実施される．その技術は，ハッキングや規約違反からのリスクがますます高まっている機密性の高いフィナンシャルデータに対して，追加のセキュリティを提供することを意図しています．　Hydro Raindropの初期実装は，Hydrogen API Platform上で実施されます．このAPI群のモジュールセットは，最先端のフィナンシャル技術のプラットフォームや製品のプロトタイプ，構築，テスト，展開を世界中の企業や開発者が利用可能になります．Hydro Raindropは，開発者があらゆるREST APIとHydro Raindropを統合できるように，世界中の開発者コミュニティにオープンソースソフトウェアとして提供されます．

2.ブロックチェーンとイーサリアム

Hydroはイーサリアムネットワーク上に実装されています．プロジェクトの詳細を説明する前に，ブロックチェーンとイーサリアムに関するいくらかの基本的な考え方の理解が重要です．

2.1.イーサリアム上での構築

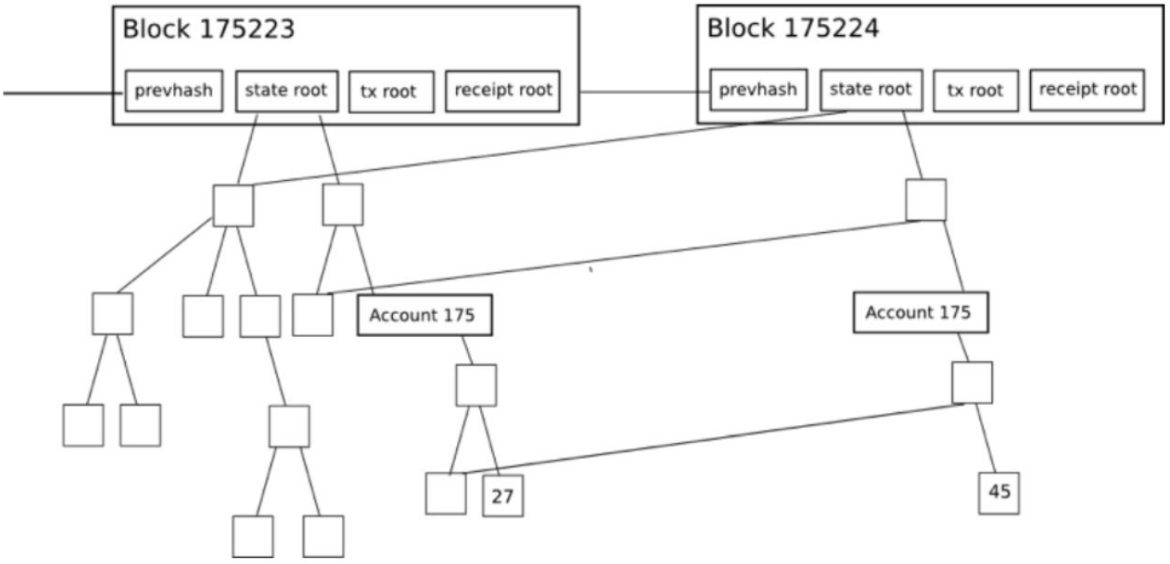
SnapchatのようなアプリケーションはApple　iOSプラットフォーム上に提供されるSwiftや他のツールを使用して構築されているが，Ethereum上にブロックチェーンアプリケーションとして構築することもできます．Snap　IncはiOSを構築する必要がなく，Ethereumは革新的なソーシャルメディアアプリケーションを立ち上げるためのインフラとして使われる．Hydroプロジェクトも同様です．それは基礎となるブロックチェーン技術をより早く，より強く，そして，より効率的にするために働いている世界中の何千という開発者に依存しています．Hydroは，フィナンシャルサービスアプリケーションに明確な利益をもたらすブロックチェーンテクノロジーを中心とした製品に焦点を当てた相互作用を開発することによって，この絶えずに改善されるインフラを活用します．

2.2.マークルツリー

マークルツリーは，効率的なデータ検証のために分散システムで使われています．それらは全てのファイルの代わりにハッシュ値を使用するため効率的です．ハッシュ値は，実際のファイルよりもより小さいファイルを符号化する方法です．Ethereumの各ブロックヘッダーには，トランザクション，受領高，状態の3つのマークルツリーが含まれます．

これは，簡単にライトクライアントが照会に対する検証可能な解答を得ることができます．

・このアカウントは存在しているか？
・現在の残高は？
・この取引は特定のブロックに追加されているか？
・特定のイベントが今日このアドレスで発生したか？



参考文献: Merkling in Ethereum; Vitalik Buterin, Ethereum Founder

2.3.スマートコントラクト

Ethereumや他のブロックチェンベースのネットワーウによって実現される重要な概念は，スマートコントラクトです．これらは，自動実行されるコードブロックで，複数の当事者は，信頼できる仲介者の必要性を排除して契約を結ぶことができます．スマートコントラクトのコードは，従来の紙面上での契約の法的条項と同様であるとして扱えますが，更に広範な機能として実現できます．契約はルール，条件，違反に対する罰則，または，他のプロセスを開始できます．引き金を引いた時，契約は，普遍性を持ち分散化された組み込み要素を提供するパブリクチェーン上で展開時に最初に述べたとおり実行されます．スマートコントラクトは，Ethereumインフラを構築する上で必要不可欠なツールです．
Hydroブロックチェーンのコア機能は，本稿の広範で説明するカスタム契約によって実現されます．

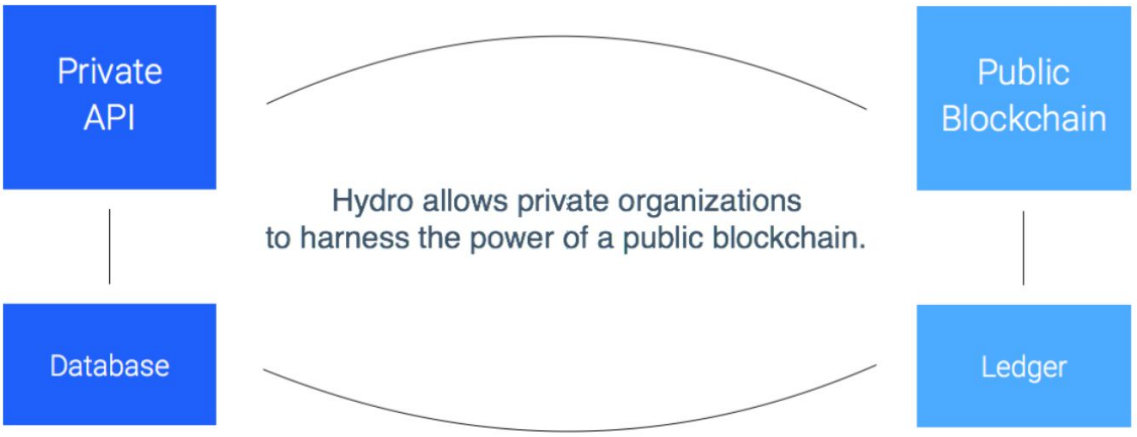
2.4.Ethereumバーチャルマシン

Ethereumバーチャルマシン(EVM)は，Ethereum上のスマートコントラクトのための実行環境です．EVMは，DoS攻撃を防ぎ，プログラムがステートレスを維持することを保証します．そして，中断することのできない通信を可能にする．EVMの振る舞いは，それらに関するコストを伴います．これを「ガス(gas)」と呼び，必要とされる計算資源に依存します．各トランザクションはそれのため「ガス制限(gas limit)」と呼ばれる最大量のガスが割り当てられます．もし，トランザクションによって消費されたガスが制限に達すると，取引は中断されます．

3.公開元帳(Public Ledger)

3.1.プライベートシステムのための公開元帳

フィナンシャルサービスプラットフォーム，Webサイト及びアプリケーションに動力を供給するシステムは，しばしばデータフローの媒体として記述することができます．それらは，実在するインターフェースのためにデータを送信，検索，格納，更新，及び処理をします．より一般的にデータとフィナンシャルサービスの性質により，それらのシステムはしばしばプライベート且つ中央集権的な方法で複雑な業務を提供します．プライベート構造上の依存は，内部システムの到達できない外的な力を組み込むことによって，多様な安全性，透明性，効率性を向上させます．

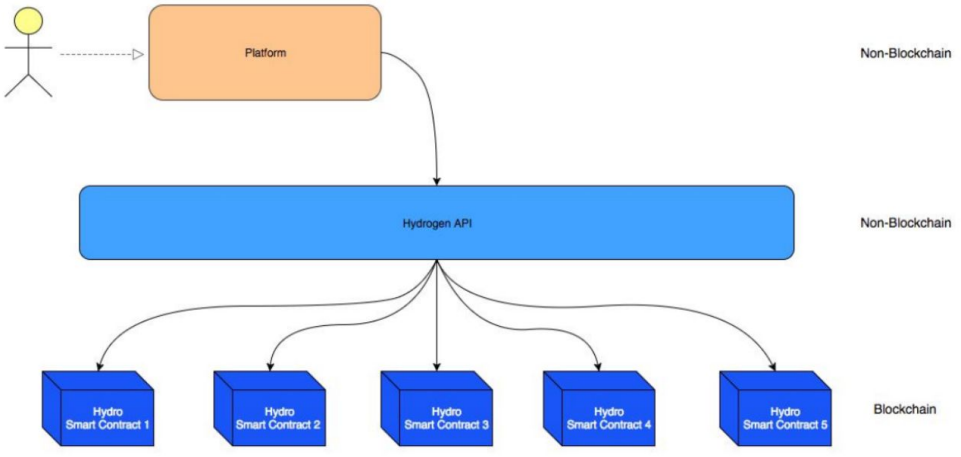


これはHydrogenAPIプラットフォームの場合です．Hydroは，基本的にプライベートなHydrogenエコシステムにシームレスに統合された方法でブロックチェーンと連携をユーザーとに許可することによって前述した多様な安全性，透明性，効率性の向上を得ることを目的としています．

パブリックブロックチェーンを基礎とした操作は,プライベートな操作の前,最中,後に行うことができます.そのプライベートとパブリックな要素間の相互作用はエコシステム内のプロセスの検証やスタンプ,記録または強化に役立ちます.このモデルの本質は,もっとも好ましい影響を生み出すブロックチェーン技術の利点を具体的に取り入れることでプロセスをより堅牢にしています.一方で,このハイブリッドフレームワークはすべてのプラットフォームに適用されるわけではありませんが,Hydroはそれが存在する場合に価値を提供することに重点を置いています.

3.2.採用のための設計

Hydroは多くの既存のブロックチェーンの取り組みとは異なります.なぜなら,独立して存在し,仕組みの変更を必要とせずに既存,又は,新規システム周辺に配置ができるからです.置き換えるのではなく,Hydroは増強を目指しています.プラットフォームとHydrogenAPIに接続する機関は自動的にブロックチェーンにアクセスできます.



Hydroを活用できるフィナンシャルサービスプラットフォームの範囲は幅広くあります.これらのプラットフォームは,事実上すべての経験を強化でき,任意の数の独自サービスを内包し,あらゆる環境に展開できます.これはHydroの構造的なモジュール性によって可能であり,Hydroと相乗的かつ採用の補完的な推進役として機能します.

4.Raindrop

Hydro public ledger(公開元帳)上に構築されたブロックチェーンを基盤とした認証サービス,これは「Raindrop」と呼ばれています.これは,アクセス要求が許可されたソースからきていることを検証する,明確かつ不変で世界中から視認可能なセキュリティ層を提供します.OAuth 2.0のようなプライベートな認証プロトコルまたは,存在するユースケースの範囲に様々なレベルの堅牢性と有用性を提供します.これらのプロトコルを置き換えるための試みや競合する必要はほとんどありません.Hydroは,認証手順の構成要素としてブロックチェーン技術を組み込むことによって,それらを強化する方法を提供します.これは,システムの侵害やデータの漏洩を防止するセキュリティを提供します.

Raindropの技術的側面の調査の前に,まずはその問題を解決しようとしています.

4.1.フィナンシャルセキュリティの状態

ビッグデータ時代の到来により,脆弱性が高まりました.そして,これはフィナンシャルサービスにとって特に重要です.フィナンシャルプラットフォームは,多くの場合,大量の個人や政府のID番号や口座資格情報,取引履歴のような機密データの出入り口です.このデータが非常に重要なため,不正アクセスは一般的に致命的な結果を伴います.

業界調査会社Trend Microでは,盗難された個人識別情報(PII)の項目の一部がディープウェブ上でわずか1ドルで販売され,パスポートなどのスキャンされたドキュメントは10ドル,そして,銀行へのログイン資格情報は200ドルで見つかったというレポートを出版した.盗まれたデータの配布はますます断片化され追跡不能になっています.

残念ながら,既存のフィナンシャルシステムはステークホルダーとのデータの漏洩を防止,診断,伝達する際に潔白な実績がありません.

- Javelin Strategy & Researchの調査による最近の調査-2017年個人情報漏洩調査-個人識別情報(PII)を保護するフィナンシャルシステムの不具合のため2016年に米国消費者1540万人から160億ドルが盗まれました.
- 2017年4月,Symantec社は2016年の間に個人識別情報(PII)の11億件が様々な方法で侵害されたと見積もったインターネットセキュリティ脅威レポートを出版しました.
- Risk Based Securityによる2016年末のデータ侵害クイックビューでは,全世界のビジネスで4149件のデータの漏洩が発生し,42億をこえるレコードが公開されています.
- 2017年Thalesデータ脅威レポート-専門サービスのグローバルIT専門家を対象に調査したフィナンシャルサービスエディションでは,フィナンシャルサービス組織の49%が過去にセキュリティ侵害を経験しており,その78%は自らを保護するために多くを費やしている.しかし,73%が適切なセキュリティ解決策を用意しないまま,AI,IoT,クラウド技術に関する新しい取り組みを開始しています,

4.2.エキファックス(米国の消費者信用情報会社)侵害

2017年7月29日,米国の消費者引用会社で118年の歴史を持つエキファックスはハッキングされ,1430万人の消費者の個人識別情報に加え社会保障番号,また,2万9千人のクレジットカード情報が暴露された.

どのケースが侵害になったのでしょうか？これはエキファックスによって利用されるバックエンド技術の1つから始まります.StrutsはApacheソフトウェア財団によって構築されたJava言語でWebアプリケーションを開発するためのオープンソースフレームワークです.CVE-2017-9805はXMLペイロードを処理するためのXStreamハンドラと共にStruts REST プラグインを使用する脆弱性です.もし悪用されると,遠隔で認証されていない攻撃者はアプリケーションサーバー上で悪意のあるコードを実行して,マシンを乗っ取るか.それ以上の攻撃を開始することができます.これは,エキファックス侵害の2カ月月前にApacheによって修正されました.

Apache Strutsは,XMLリクエスト内のプログラムがユーザー指定の入力を不安定に逆シリアライズするときに引き起こされるREST Plugin XStreamの欠陥が含まれています.具体的には,プログラムはXStreamハンドラーの持つtoObject() メソッドで引き起こされます.この

メソッドは,オブジェクトへのXstreamの逆シリアライズを使用するとき,引数上に制限を課さず,任意のコード実行に脆弱性を引き起こします.

例え,このRESTプラグインが侵害されたとしても,それは問題でしょうか？現時点のREST APIとJavaベースのシステムに依然として依存しながら,1億4300万人の顧客のフィナンシャル情報を保護するためにブロックチェーン技術を使用する方法がありますか？

4.3.ブロックチェーンレイヤの追加

フィナンシャルデータゲートウェイの統合性を改善できるのは明らかです.Hydroを介してセキュリティの追加レイヤーを達成する方法を見てみましょう.

Ethereumネットワークの基本的な合意形成メカニズムは,参加者が適切に署名された取引をまとめて処理するためトランザクションの有効性を保証します.この現実は非中央集権化と不変性につながりますが,更に重要なことは,それは機密データを取り扱うゲートウェイへの不正アクセスを緩和するためのベクトルを提供します.

Hydroを使用すると,認証はブロックチェーン上のトランザクション操作を前提とすることができます.例えばAPIは標準の認証プロトコルを開始する前提条件として,ブロックチェーン上の特定のアドレス間で特定のデータペイロードと共に特定のトランザクションを開始を要求することによって開発者とアプリケーションを検証することができます.

4.4.Hydro Raindrop

雨は直径0.0001から0.005cmの範囲の雨滴の集まりです.典型的な嵐の中には,何十億もの大きさ,速度,形状の雨滴があります.そのため,雨の正確な性質を確実に予測することはできません.同様に,すべてのHydro認証トランザクションは,一意で,偶然に発生することは事実上不可能です.そのため,我々はRaindrop(雨滴)と呼んでいます.

フィナンシャルサービスプラットフォームは,通常,顧客口座を検証するためのマイクロデポジット検証を利用します.このコンセプトはシンプルです.プラットフォームは,ユーザーの主張した銀行口座にランダムで少額を預金します.

ユーザーが実際にその口座を所有していると証明するためには,預金金額をプラットフォームに戻して検証しなければなりません.ユーザーが有効な金額（推測以外に）を知る唯一の方法は,問題の銀行口座にアクセスすることです.

Hydroを用いたRaindropベースの検証は,類似しています.ユーザーに金額を送って,それを送り返すのではなく,我々はトランザクションを定義し,ユーザーは既知のウォレットから実行する必要があります.ユーザーが有効なトランザクションを処理する唯一の方法はその問題のウォレットにアクセスすることです.

Raindropを使用することによって,システムと**アクセサの両方が不変の**公開元帳上で認証の試みを監視できます.このブロックチェーンベースのトランザクションは基本的なシステムの操作から独立し,分散ネットワーク上で発生します.そして,秘密鍵の所有権に依存します.従って,それは有効な検証ベクタとして機能します.

4.5.Raindropの詳細

Hydroの認証プロセスには4つの実体が関与しています：

1. アクセサ(Accessor)：システムにアクセスを試みる者.Hydrogenの場合,アクセサは主要なデジタルインフラのためHydrogen APIを利用する金融機関又はアプリケーションです.
2. システム(System)：アクセサによってアクセスされるシステムまたはゲートウェイの事.HydrogenのためシステムはHydrogen APIそのものです.
3. Hydro(Hydro)：システムがブロックチェーンと通信して連携するために使用するモジュール
4. ブロックチェーン(Blockchain)：Hydoroトランザクションを処理する分散された公開元帳で,情報をプッシュ,プル,又はその他の方法で操作できるHydroスマートコントラクトを含んでいます.

各Raindropは,全体として5つのトランザクションパラメータの集まりです.

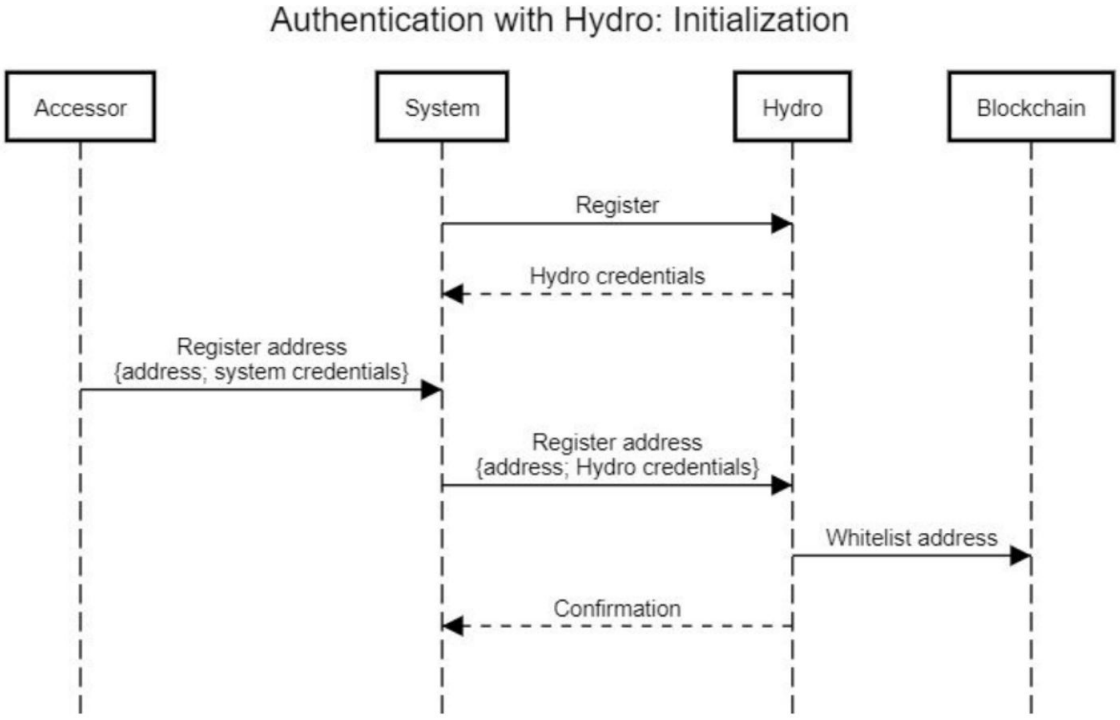
1. 送信者(Sender)：トランザクションを開始しなければならないアドレスです.

2. 受取人(Receiver)：トランザクションの送り先.Hydroスマートコントラクトでメソッドを呼び出すことに相当します.
3. 識別子(ID)：システムに関連付けられた識別子です.
4. 数量(Quantity)：正確なHydroの数を送信します.
5. 要求(Challenge):ランダムに生成された英数字の文字列です.

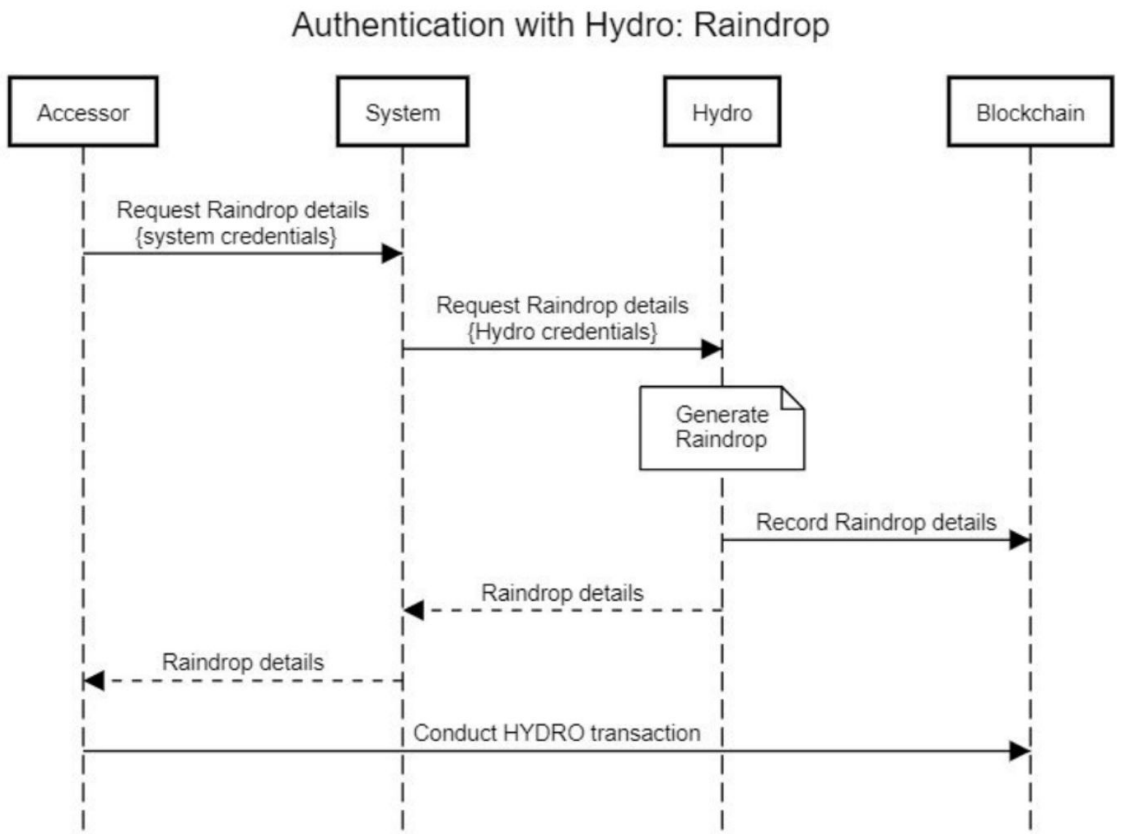
以下に認証プロセスの概要を示します.これは一般的に3つの段階に分類されます.

1. 初期化(Initialization)
2. 雨滴(Raindrop)
3. 検証(Validation)

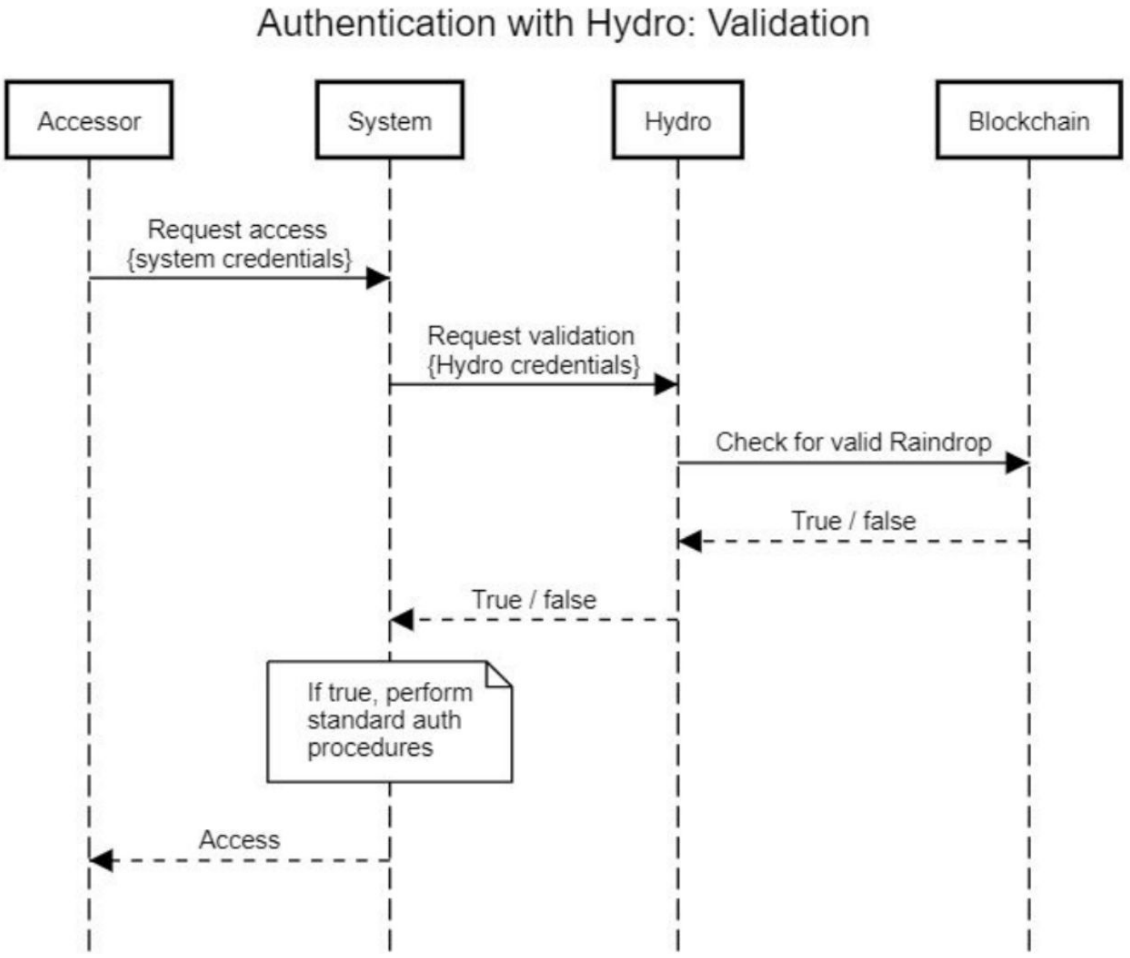
初期化は,登録されているシステム(例：Hydrogen)と共にHydroと取得している信用情報,Hydroモジュールを介してブロックチェーンと通信を可能にするシステムを使用することで開始する.システムは,パブリックアドレスを登録したアクセサ(例えば金融機関)を提供し,登録されたアドレスをHydroに渡す.このアドレスは,Hydroスマートコントラクトに格納されているホワイトリストのあるブロックチェーン上に永久に書き込まれます.システムは,アドレスがホワイトリストに登録されていることの確認を受信します.これは,一般公開されているイベントとしても確認できます.システム登録は,たった1度だけ必要ですが,一方でアクセサのホワイトリストへの登録はアクセサ毎に1度必要です.



初期化が完了すると,Hydro認証プロセスのコアが開始されます.Raindroトランザクションを実行する必要のあるアクセタはシステムからRaindropの詳細を要求することによってこのプロセスを開始し,システムは要求をHydroに転送します.Hydroは新しいRaindropを生成し,ブロックチェーン上に特定の詳細を永続的に格納し,そして,システムを介してアクセタに完全な詳細を転送します.全ての要求された情報を備えたアクセタは登録されたアドレスからHydroスマートコントラクトのメソッドへトランザクションを実行します.もしアドレスがホワイトリストになければ,その処理は拒否されます.それ以外は,スマートコントラクトに記録されます.このトランザクションはアクセタのプライベートキー(アクセタのみが取得できる)で署名する必要があるため,このトランザクションはシステムの外で,アクセタからブロックチェーン上に直接実行する必要があることに注意しなくてはなりません.



プロセスの最終段階は検証です.このステップではアクセタは公式にシステムの確立された仕組みを介してシステムへのアクセスを要求します.標準的な認証プロトコルのいずれかを実装する前に,そのシステムはアクセタが有効なRaindropトランザクションを実行したか否かを問い合わせます.Hydroはスマートコントラクトと結びつき,妥当性を確認し,真/偽の指示で応答をします.システムは,この指定に基づいてどのようにプロセスを進めるべきかを決定できます.これが偽であれば,システムはアクセスを拒否でき,真であればアクセスを許可することができます.



もし基本的なシステムの信用情報(または既存のシステムプロトコルが何であろうと)を広範囲に渡って認証の1つの要素であると考えるとき,それはHydroレイヤーは有用な2つの要素を提供することが重要です.2つの主要な攻撃ベクターを調査することにより,その有用性を容易に確認できます.

- ベクター1:攻撃者はアクセタの基本システムの信用情報を盗みます.
  - ◎ 攻撃者は有効なシステムの信用情報でシステムにアクセスを試みます.
  - ◎ Hydroのシステムチェックによりブロックチェーン上で有効なトランザクションが実行されたかを判定します.
  - ◎ Hydroは偽を返し,システムはアクセスを拒否します.

- ベクター2:攻撃者はアクセタのウォレットのプライベートキーを盗みます.
  - ◎ 攻撃者は要求されたRaindropの詳細なしに登録されたアドレスからHydroトランザクションの実行を試みます.
  - ◎ 攻撃者は有効なブロックチェーントランザクションを作ることができません.
  - ◎ 攻撃者は適切なシステムの信用情報なしでシステムへのアクセスを要求することもできません.

4.6.公開されているRaindropを開く

このブロックチェーンベースの認証サービスはHydrogen APIのエコシステムを保護するために設計されていますが,様々なアプリケーションやシステムに広く適用可能です.我々は他の人がこの検証レイヤーから潜在的に恩恵を受けることができると感じているため,私たちは他の人が使用できるよう公開をしています.

HydrogenはAPIエコシステムへのアクセスを前提として統合するのとまったく同じよう

に,どのシステムも既存の手順やプロトコルにそれを追加することができます.API,アプリケーション,エンタープライズソフトウェア,ゲーミングプラットフォームなどのプラットフォームは認証目的でHydroを利用できます.正式なドキュメントはこのブロックチェーンレイヤーを認証フレームワーク又はREST APIに組み込むことを希望する人々のためにGitHub上で入手できます.

4.7.事例研究:OAuth2.0におけるRaindrop

Raindropを民間企業が利用できる方法は数多くあります.プライベートAPI,データベース,そして,ネットワークは機密データを保護する試みとして過去10年間にトークン,キー,アプリケーションの複雑なシステムを作り出しました.例えばGoogleは,Google認証アプリケーションと共に市場で最も人気のある商品提供者の一つとなりました.前述のように,これらの既存のプロトコルと競合するか置き換える必要はほとんどありません.

事例として,ここで全体のAPIセキュリティフレームワークのセキュリティレイヤーとしてHydrogenがHydro認証をどのように実装するかについて簡単に説明します.

1. Hydrogen APIのパートナーは,まず,彼らの様々な環境のIPアドレスをホワイトリストに登録する必要があります.
2. パートナーはHydroの公開アドレスをホワイトリストに登録するように要求する必要があります.
3. Hydrogen APIへの全ての呼び出しとデータの転送は,HTTPSプロトコルを通して暗号化された送信されます.
4. パートナーは登録されたHydroアドレスから有効なHydro Raindropトランザクションを実行し,完了する必要があります.
5. パートナーはOAuth2.0検証を使用する必要があります.OAuth(公開認証)はトークンベースの認証と承認のためオープン標準です.Hydrogenは「Resource Owner Password Credentials」と「Client Credentials」のグラント種別をサポートしており,各APIユーザーは認証リクエストのための信用情報を提供する必要があります.
6. もし上記の5つの要素のいずれにも違反していない場合,Hydrogenパートナーには独自トークンが付与され,各API呼び出しで確認及び検証されます.
7. そのトークンは24時間有効です.その後,パートナーは自分自身を再度検証する必要があります.

もし,この手順のいずれかに違反すると,そのユーザーはAPIアクセスから直ぐにロックされます.ハッカーはこれらのセキュリティ要因を無作為に推測して回避することはできません.これは,何兆もの一意な組み合わせが存在するためです.

Hydoroブロックチェーンベースの認証はHydrogenセキュリティプロトコルの重要な構成要素です.Hydrogenチームは,パートナーに複数署名のウォレットを設定し,他の信用情報から独立した複数の安全な場所にプライベートキーを補完することを推奨しています.そのため,単一障害点はありません.適切に保護された複数署名ウォレットは,盗難が難しいだけでなく,ブロックチェーンの公開された性質によって,APIのセキュリティに関連するあらゆる盗難の迅速な認識も可能です.
誰もがHydoroスマートコントラクトへの認証を試みを見ることができます.つまり,何カ月もの間,プラットフォームが侵害された日が過去のものになる可能性があります.APIハッカーは,世界中のどこからでもリアルタイムに予期せぬ認証の試みを検出できるため,即時性を失うことになります.

5.リスク

ソーシャルメディアやEメール,ストリーミングアプリケーション(ダイアルアップ接続に依存していた)などの初期のテクノロジーのように,コア開発チームはEthereumのトランザクションと速度,スケーリングの新しい展開を詳しく追跡することが重要です.YouTubeが1995年に立ち上げようとしていることを想像できますか？また,Instagramが最初にBlackberryで提供されていますか？

Vitalik ButerinやJoseph PoonなどのコアEthereum開発者は,Plasma：Scalable Autonomous Smart ContractをEthereumにアップグレードすることを提案しています.

プロトコル：Plasmaはスマートコントラクトのインセンティブと強制実行のためのフレームワークとして提案されています.これは,1秒間あたりの大量の状態更新(潜在的には数十億回)のためスケーラビリティがあり,世界中の分散型フィナンシャルアプリケーションの相当量を表すことができます.これらのスマートコントラクトは,トランザクションの状態遷移を実行するために最終的に基礎となるブロックチェーン(例:Ethereum)に依存するネットワークトランザクションの手数料を介して自動的に動作し続けるようにインセンティブを与える.

Raiden Networkのような他の企業はより高速な取引と低い手数料のためオフチェーン・スケーリング・ソリューションを提案しています.現時点ではRaindropはEthereumフレームワーク上で最小限の負荷をかけるため,スケーラビリティはテクノロジの成功のために非常に小さなリスクです.

6.結論

パブリックブロックチェーンの不変性はAPIのようなプライベートシステムのセキュリティを高める新しい方法を提供します.

本稿では,3つの重要なことを示しています.

1. パブリックブロックチェーンはフィナンシャルサービスの価値を高めることができます.
2. Hydro Raindropはプライベートシステムのセキュリティを高めることができます.
3. Hydrogen APIプラットフォーム内のHydro Raindropがすぐに適用されます.

Hydroチームは,記載されたフレームワークがフィナンシャルサービス産業とそれを超えて全ての利害関係者に恩恵をもたらすプライベート-パブリックシステムの新しいハイブリッドモデルのための標準的なセキュリティインフラストラクチャであると考えている.

参考文献

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