Hydro Raindrop

BLOCKCHAIN의 공용 인증

일월 2018

목차

추상

HYDRO: 어원-고대로부터Greek ὑδρο- (*h udro-*), ...에서ὕδωρ (*h údōr*, “water”)

Hydro는 새로운 및 기존 사설 시스템이 공용 Blockchain의 불변하고 투명한 역학을 완벽하게 통합 및 활용하여 응용 프로그램 및 문서 보안, ID 관리, 트랜잭션 및 인공 지능을 향상시킵니다..

이 논문에서는 API와 같은 사설 시스템이 Hydro public BLOCKCHAIN을 사용하여 공개 인증을 통해 보안을 향상시키는 경우가있을 것이다.

제안 된 기술은 "RAINDROP"라고하며, 개인 계약 액세스를 공개적으로 확인하고 기존 개인 인증 방법을 보완 할 수있는 스마트 계약을 통해 수행되는 트랜잭션입니다. 이 기술은 해킹 및 침해의 위험이 점점 커지고있는 민감한 재무 데이터에 대한 추가 보안을 제공하기위한 것입니다.

Hydro raindrop의 초기 구현은 Hydrogen API Platform에서 수행됩니다. 이 모듈러 세트는 복잡한 금융 기술 플랫폼 및 제품의 프로토 타입, 구축, 테스트 및 배포를 위해 전 세계 기업 및 개발자가 사용할 수 있습니다.

Hydro raindrop는 개발자가 Hydro Raindrop를 REST API와 통합 할 수 있도록 오픈 소스 소프트웨어로서 세계 개발자 커뮤니티에서 사용할 수 있습니다..

Blockchain 과 Ethereum

Hydro는 Ethereum 네트워크에서 구현됩니다. 프로젝트에 대한 자세한 내용을 제공하기 전에 BLOCKCHAIN 및 Ethereum에 대한 기본적인 아이디어를 이해하는 것이 중요합니다..

에 건물Ethereum

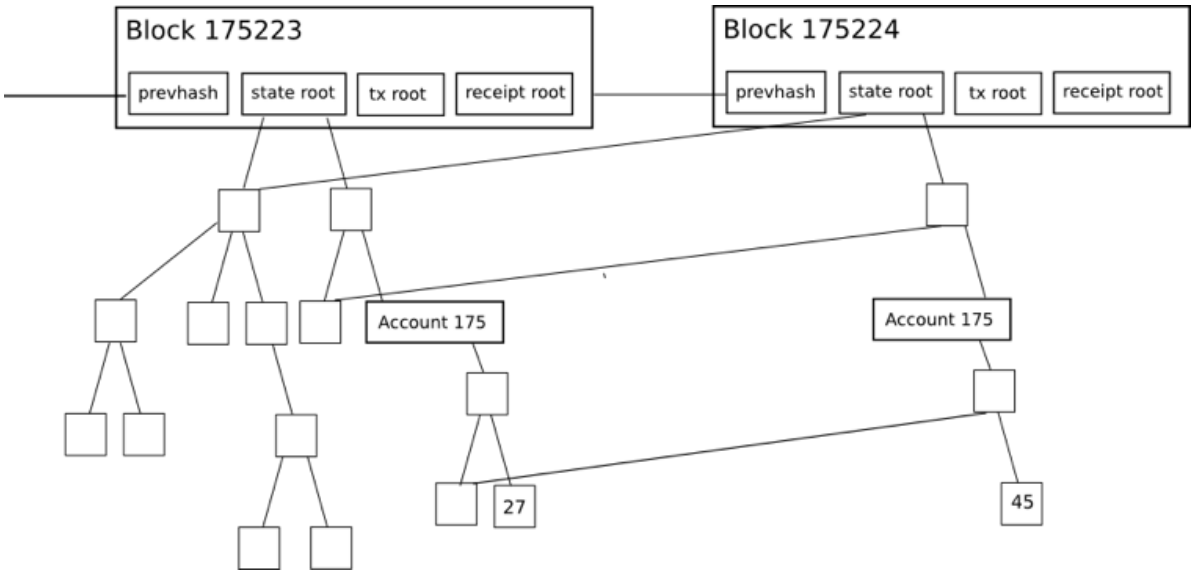
Snapchat과 같은 앱은 Apple의 iOS 플랫폼 위에 제공되는 Swift 및 기타 도구를 사용하여 제작되었으므로 Blockchain 응용 프로그램도 Ethereum 위에 구축 할 수 있습니다. Snap Inc.는 iOS를 구축 할 필요가 없었으며, 게임을 변화시키는 소셜 미디어 애플리케이션을 시작하기 위해 인프라로 사용했습니다.

프로젝트 하이드로도 비슷합니다. 기본 BLOCKCHAIN 기술을보다 빠르고, 강력하며, 효율적으로 만들기 위해 노력하고있는 전 세계 수천 명의 개발자에게 의존합니다. Hydro는 금융 서비스 응용 프로그램에 가시적 인 혜택을 제공 할 수있는 Blockchain 기술을 중심으로 제품 중심의 상호 작용을 개발함으로써 지속적으로 개선되는 인프라를 활용합니다..

Merkle Trees

머클 나무는 효율적인 데이터 검증을 위해 분산 시스템에서 사용됩니다. 전체 파일 대신 해시를 사용하기 때문에 효율적입니다. 해시는 실제 파일 자체보다 훨씬 작은 파일을 인코딩하는 방법입니다.

Ethereum의 모든 블록 헤더에는 트랜잭션, 수신 확인 및 상태를위한 3 개의 Merkle Tree가 있습니다.:



Source: Merkling in Ethereum; Vitalik Buterin, Ethereum Founder

이렇게하면 가벼운 클라이언트가 다음과 같이 쿼리에 대한 검증 가능한 답변을 쉽게 얻을 수 있습니다.:

- 이 계정이 존재합니까?
- 현재 잔고 란 무엇입니까?
- ●이 거래가 특정 블록에 포함 되었습니까? ● 오늘이 주소에서 특정 사건이 발생 했습니까??

스마트 계약

Ethereum 및 다른 BLOCKCHAIN 기반 네트워크에서 사용할 수있는 핵심 개념은 현명한 계약입니다. 이는 여러 당사자가 상호 작용할 수있는 자체 실행 코드 블록으로 신뢰할 수있는 중개자의 필요성을 없애줍니다. 똑똑한 계약의 코드는 전통적인 종이 계약의 법적 조항과 유사하지만 훨씬 더 광범위한 기능을 구현할 수도 있습니다. 계약에는 규칙, 조건, 위반에 대한 벌칙이 있거나 다른 프로세스를 시작할 수 있습니다. 시작될 때 계약은 공개 체인 배포시 원래대로 명시된대로 실행되며 내장 된 불변성 및 분권화 요소를 제공합니다.

현명한 계약은 Ethereum 인프라를 구축하는 데 필수적인 도구입니다. Hydro 블록 체인 레이어의 핵심 기능은이 문서의 뒷부분에서 설명하는대로 맞춤 계약을 통해 이루어집니다..

Ethereum가상 기기

Ethereum 가상 머신(EVM)은 Ethereum의 현명한 계약을위한 런타임 환경입니다. EVM은 DoS (Denial of Service) 공격을 방지하고 프로그램이 상태를 유지하며 중단 될 수없는 통신을

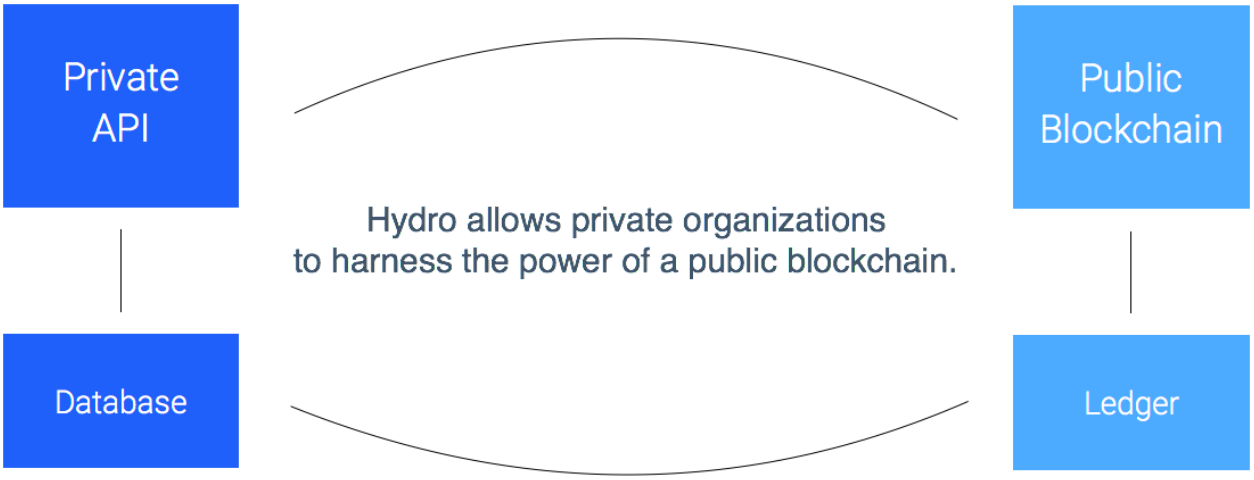
가능하게합니다. EVM에 대한 조치에는 가스와 관련된 비용이 소요되며 이는 필요한 계산 자원에 달려 있습니다. 모든 거래에는 최대 한도의 가스가 있으며이를 한계치 (g)라고합니다. 거래에 의해 소비 된 가스가 한도에 도달하면 처리를 중단합니다.

공인 원장

개인 시스템을위한 공인 원장

금융 서비스 플랫폼, 웹 사이트 및 응용 프로그램을 구동하는 시스템은 대개 상호 작용하는 엔터티의 데이터를 보내고, 검색하고, 저장하고, 업데이트하고, 처리하는 데이터 흐름의 매체로 설명 될 수 있습니다. 이 데이터의 성격과 금융 서비스의 특성으로 인해이 시스템은 종종 개인적이고 중앙 집중적 인 방식으로 복잡한 작업을 수행합니다. 사설 구조물에 대한 의존도는 내부 시스템의 도달 범위를 초과하는 외력을 통합함으로써 다양한 보안, 투명성 및 효율성 향상을위한 문호를 열어줍니다.

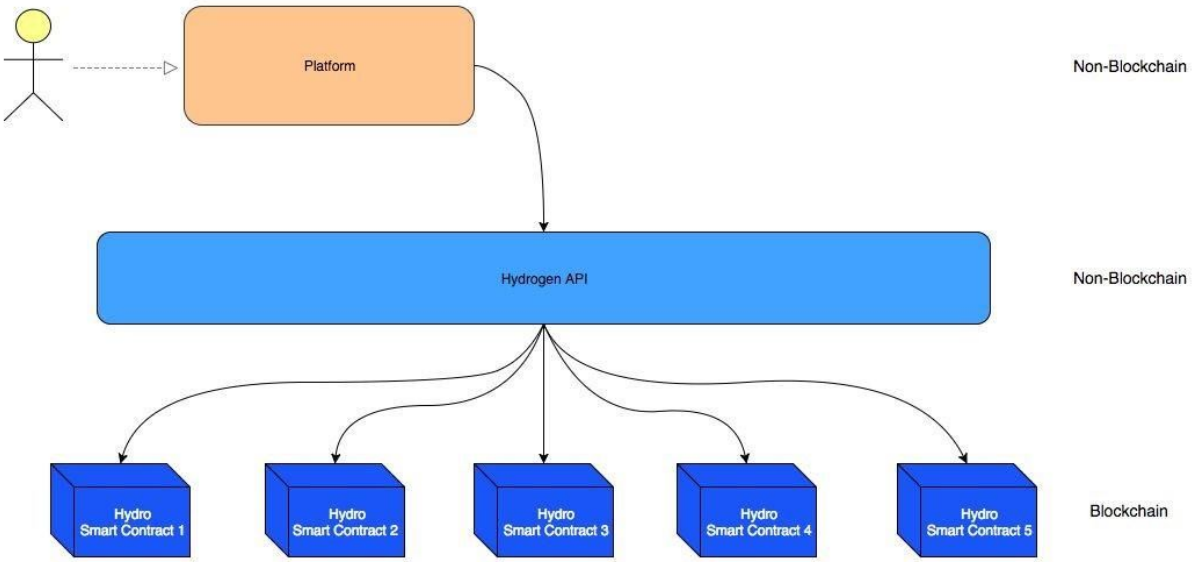
Hydrogen의 API 플랫폼의 경우입니다. HYDRO는 Hydrogen 사용자가 근본적으로 개인용 수소 생태계에 원활하게 통합되는 방식으로 블록 체인과 인터페이스 할 수 있도록하여 앞서 언급 한 이점을 활용하고자합니다.



공용 blockchain 기반 작업은 개인 작업 전, 도중 또는 후에 발생할 수 있습니다. 사적 요소와 공공 요소 간의 상호 작용은 생태계 내에서 프로세스의 유효성을 검사하고, 스탬프를 작성하고, 기록하고, 향상시키는 역할을합니다.
이 모델의 정신은 블록 체인 기술의 이점을 특히 긍정적 인 영향을 줄 수있는 곳으로 두드려 프로세스를 더욱 강력하게 만듭니다. 이 하이브리드 프레임 워크는 모든 플랫폼에 적용 할 수는 없지만 Hydro는 해당 플랫폼에 대한 가치 제공에 중점을 둡니다..

입양을위한 건축

Hydro는 기존의 많은 블록 체인 이니셔티브와는 달리 체계적으로 변경하지 않고도 독립적으로 존재하거나 새로운 시스템이나 기존 시스템을 둘러 쌀 수 있기 때문에 이와 다릅니다. 대체하기보다 Hydro는 기능 보강을 목표로합니다. 수소 API에 연결된 플랫폼 및 기관은 자동으로 블록 체인에 액세스 할 수 있습니다.



수소를 활용할 수있는 금융 서비스 플랫폼의 범위는 광범위합니다. 이러한 플랫폼은 사실상 모든 경험을 제공하고 독점적 인 서비스를 수용하며 개인 데이터 작업을 수행하고 모든 환경에 배포 할 수 있습니다. 이것은 Hydrogen의 구조적 모듈화에 의해 가능하며 Hydro와 함께 상승 작용을하며 보완 적 드라이버로 작용합니다.

Raindrop

이 Hydro 공공 주도 위에 구축 된 "Raindrop"이라는 블록 체인 기반 인증 서비스가 있습니다.이 도구는 권한이 부여 된 출처에서 액세스 요청이오고 있음을 확인하는 전역 적으로 볼 수있는 뚜렷한 불변의 보안 계층을 제공합니다.

OAuth 2.0과 같은 개인 인증 프로토콜은 존재하는 유스 케이스의 스펙트럼에 대해 다양한 수준의 견고 함과 유용성을 제공합니다. 이러한 프로토콜을 대체하거나 대체 할 필요는 거의 없습니다. Hydro는 블록 체인 메커니즘을 인증 절차의 구성 요소로 통합하여이를 향상시킬 수있는 방법을 제공합니다. 이를 통해 유용한 보안 계층을 추가하여 시스템 침해 및 데이터 손상을 방지 할 수 있습니다.

Raindrop의 기술적 인 측면을 검토하기 전에 먼저 해결하려고하는 문제를 살펴 보겠습니다..

금융 보안 상태

데이터 시대가 다가옴에 따라 취약성이 증가했으며 이는 특히 금융 서비스에 중요합니다. 금융 플랫폼은 종종 정부 ID 번호, 계정 자격 증명 및 거래 내역과 같은 사적이고 민감한 데이터를 대량으로 게이트웨이로 제공합니다. 이 데이터의 중요성이 매우 중요하기 때문에 부당 액세스는 대개 치명적인 결과를 낳습니다.

업계 조사 기관인 Trend Micro는 훔친 개인 식별 정보 (PII)의 항목이 딥 웹에서 최소 $ 1로 판매되고 있으며 여권과 같은 문서 스캔은 $ 10 정도이며 은행 로그인 자격 증명도 있음을 발견했습니다 적은 $ 200로 도난당한 데이터의 배포가 점차 단편화되고 추적 할 수 없게되었습니다..

유감스럽게도 기존 금융 시스템은 이해 관계자와의 데이터 유출 사고를 예방, 진단 및 전달할 때 현저한 성과를 거두지 못했습니다..

- Javelin Strategy & Research - 2017 년 Identity Fraud Study의 최근 연구에 따르면 2016 년 미국 소비자 1540 만 명에서 개인 식별 정보 (PII)를 보호하기위한 금융 시스템의 실패로 인해 160 억 달러가 도난당했습니다..
- 시만텍은 2017 년 4 월 인터넷 보안 위협 보고서를 발표했습니다.이 보고서는 2016 년 동안 11 억 개의 PII가 다양한 용량으로 손상되었다고 추정했습니다.
- 위험 기반 보안에 의한 2016 년 연말 데이터 유출 Quickview에서 2016 년 전세계 기업에서 4,149 건의 데이터 유출이 발생하여 42 억 건이 넘는 기록이 발견되었습니다..
- 전문 서비스 분야의 전 세계 IT 전문가를 대상으로 조사한 2017 Thales Data Threat Report - Financial Services Edition은 금융 서비스 조직 중 49 %가 과거에 보안 침해를 당했고 78 %는 자신을 보호하기 위해 더 많은 돈을 지출하고 있음을 발견했습니다. 적절한 보안 솔루션을 준비하기 전에 AI, IoT 및 클라우드 기술과 관련된 새로운 이니셔티브를 시작합니다..

Equifax Breach

2017 년 7 월 29 일, 118 세의 미국 신용 정보 기관인 Equifax가 해킹당했습니다. 사회 보장 번호를 포함하여 1 억 4,300 만 명의 소비자가 PII를 노출했습니다. 209,000 명의 고객이 신용 카드 정보를 손상 시켰습니다..

이 위반의 원인은 무엇입니까?

Equifax가 사용하는 백엔드 기술 중 하나에서 시작됩니다. Struts는 Apache Software Foundation에서 개발 한 Java 프로그래밍 언어로 웹 응용 프로그램을 개발하기위한 오픈 소스 프레임 워크입니다. C VE-2017-9805는 Struts REST 플러그인을 XStream 핸들러와 함께 사용하여 XML 페이로드를 처리하는 것과 관련된 Apache Struts의 취약점입니다. 악용되면 원격 인증되지 않은 공격자가 응용 프로그램 서버에서 악의적 인 코드를 실행하여 시스템을 인수하거나 시스템에서 추가 공격을 시작할 수 있습니다. 이것은 Equifax 위반 2 개월 전에 Apache에 의해 패치되었습니다..

Apache Struts에는 REST Plugin XStream의 결함이 포함되어 있는데, 이는 프로그램이 XML 요청에서 사용자 제공 입력을 안전하지 않게 직렬화 해제 할 때 트리거됩니다. 특히이 문제는 XStreamHandler의 toObject () 메서드에서 발생합니다.이 메서드는 개체로 XStream deserialization을 사용할 때 들어오는 값에 대한 제한을 두지 않으므로 임의 코드 실행 취약점이 발생합니다.

이 REST 플러그인이 손상된 경우에도 중요하게 받아 들여야합니까? 기존의 REST API 및 Java 기반 시스템에 여전히 의존하면서 이러한 1 억 4,300 만 고객의 재무 정보를 확보하기 위해 블록 체인 기술을 사용할 수있는 방법이 있습니까?

Blockchain 레이어 추가

재무 데이터 게이트웨이의 무결성이 향상 될 수 있음은 분명합니다. Hydro를 통해 추가적인 보안 계층을 구현하는 방법에 대해 살펴 보겠습니다.

Ethereum 네트워크의 기본적인 합의 메커니즘은 참가자들이 적절하게 서명 된 거래를 공동으로 처리하기 때문에 거래 유효성을 보장합니다. 이러한 현실은 분권화와 불변의 문제로 이어지지 만 더 중요한 것은 민감한 데이터를 처리하는 게이트웨이에 대한 무단 액세스를 완화하기위한 벡터를 제공한다는 것입니다.

Hydro를 사용하면 인증은 블록 체인의 트랜잭션 작업을 전제로 할 수 있습니다. 예를 들어, API는 표준 인증 프로토콜을 시작하는 전제 조건으로 블록 체인의 특정 주소 사이에서 특정 데이터 페이로드를 사용하여 특정 트랜잭션을 시작하도록 요구함으로써 개발자와 응용 프로그램의 유효성을 검사하도록 선택할 수 있습니다.

Hydro Raindrop

비에는 직경 0.0001 ~ 0.005 센티미터의 응축수가 포함되어 있습니다. 일반적인 폭풍우에는 무작위 크기, 속도 및 모양의 각각의 수십억 개의 패킷이 있습니다. 그렇기 때문에 비의 정확한 특성을 정확하게 예측할 수 없습니다. 마찬가지로, 모든 하이드로 인증 트랜잭션은 독특하고 실제로 우연히 발생하는 것이 불가능합니다. 이것이 우리가 R aindrops라고 부르는 이유입니다.

금융 서비스 플랫폼은 일반적으로 고객 계정의 유효성을 확인하기 위해 m 입금 확인을 사용합니다. 개념은 간단합니다. 플랫폼은 사용자가 주장한 은행 계좌에 임의의 금액을 조금씩 입금합니다. 사용자가 실제로 상기 계좌를 소유하고 있음을 증명하기 위해, 그 또는 그녀는 예금 금액을 다시 플랫폼으로 중계해야하며, 그 후에 플랫폼이 검증됩니다. 사용자가 추측 이외의 유효한 금액을 알 수있는 유일한 방법은 해당 은행 계좌에 액세스하는 것입니다.

Hydro를 이용한 빗방울 기반 검증은 유사합니다. 사용자에게 금액을 보내고 다시 전달하는 대신 트랜잭션을 정의하고 사용자는 알려진 지갑에서 트랜잭션을 실행해야합니다. 사용자가 유효한 트랜잭션을 수행 할 수있는 유일한 방법은 문제의 지갑에 액세스하는 것입니다.

Raindrops를 사용하여 시스템과 접근자는 불변의 공공 장부에 대한 인증 시도를 모니터 할 수 있습니다. 이 블록 체인 기반 트랜잭션은 기본 시스템 작업과 분리되며 분산 네트워크에서 발생하며 개인 키 소유권에 따라 달라집니다. 따라서 유용한 유효성 확인 벡터 역할을합니다..

상세보기

Hydro 인증 프로세스에는 4 개의 엔티티가 있습니다.:

1. *접근 자 - 시스템에 액세스하려는 당사자. Hydrogen의 경우 접근자는 핵심 디지털 인프라에 Hydrogen API를 사용하는 금융 기관 또는 앱입니다.*
2. *시스템 - 접근 자에 의해 액세스되는 시스템 또는 게이트웨이입니다. 수소의 경우 시스템은 Hydrogen API 자체입니다.*
3. *하이드로 (Hydro) - 시스템이 블록 체인과 통신하고 인터페이스하기 위해 사용하는 모듈.*
   4. 블록 체인 (Blockchain) - HYDRO 거래를 처리하고 하이드로 스마트 계약을 포함하는 분산 된 공공 장부.이를 통해 정보를 푸시, 당기거나 달리 조작 할 수 있습니다..

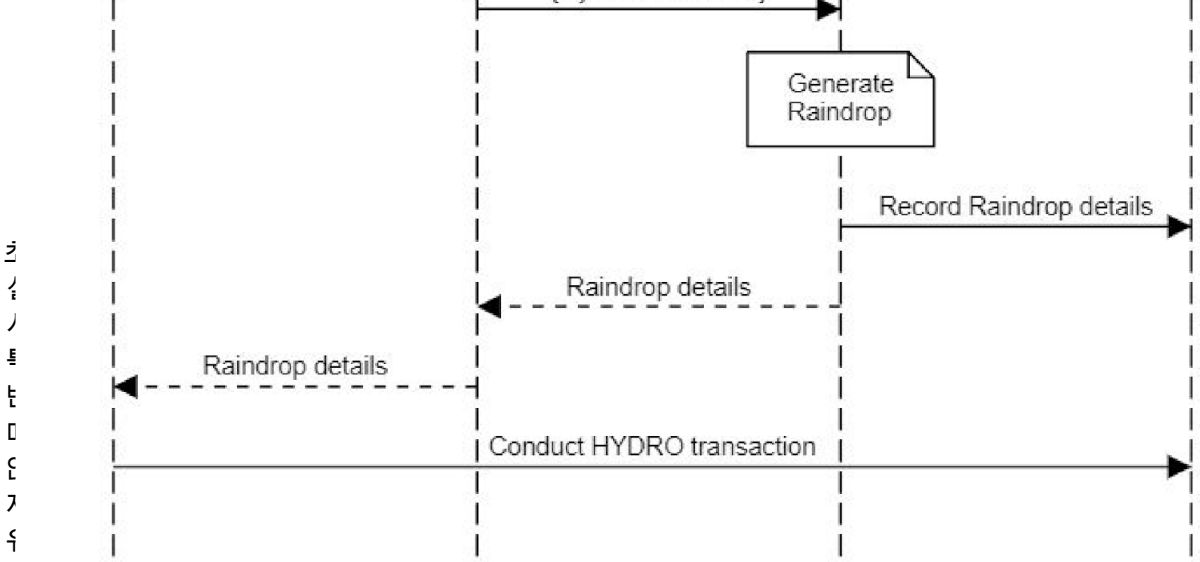
각 빗방울은 전체적으로 다섯 가지 거래 매개 변수 집합입니다.:

1. *발신자 - 거래를 시작해야하는 주소입니다.*
2. *수신자 - 거래의 목적지. 이는 Hydro 스마트 계약에서 메소드를 호출하는 것과 같습니다.*
3. *ID - 시스템과 관련된 식별자.*
4. *수량 - 보낼 수있는 정확한 수의 HYDRO.*
5. *도전 - 무작위로 생성 된 영숫자 문자열.*

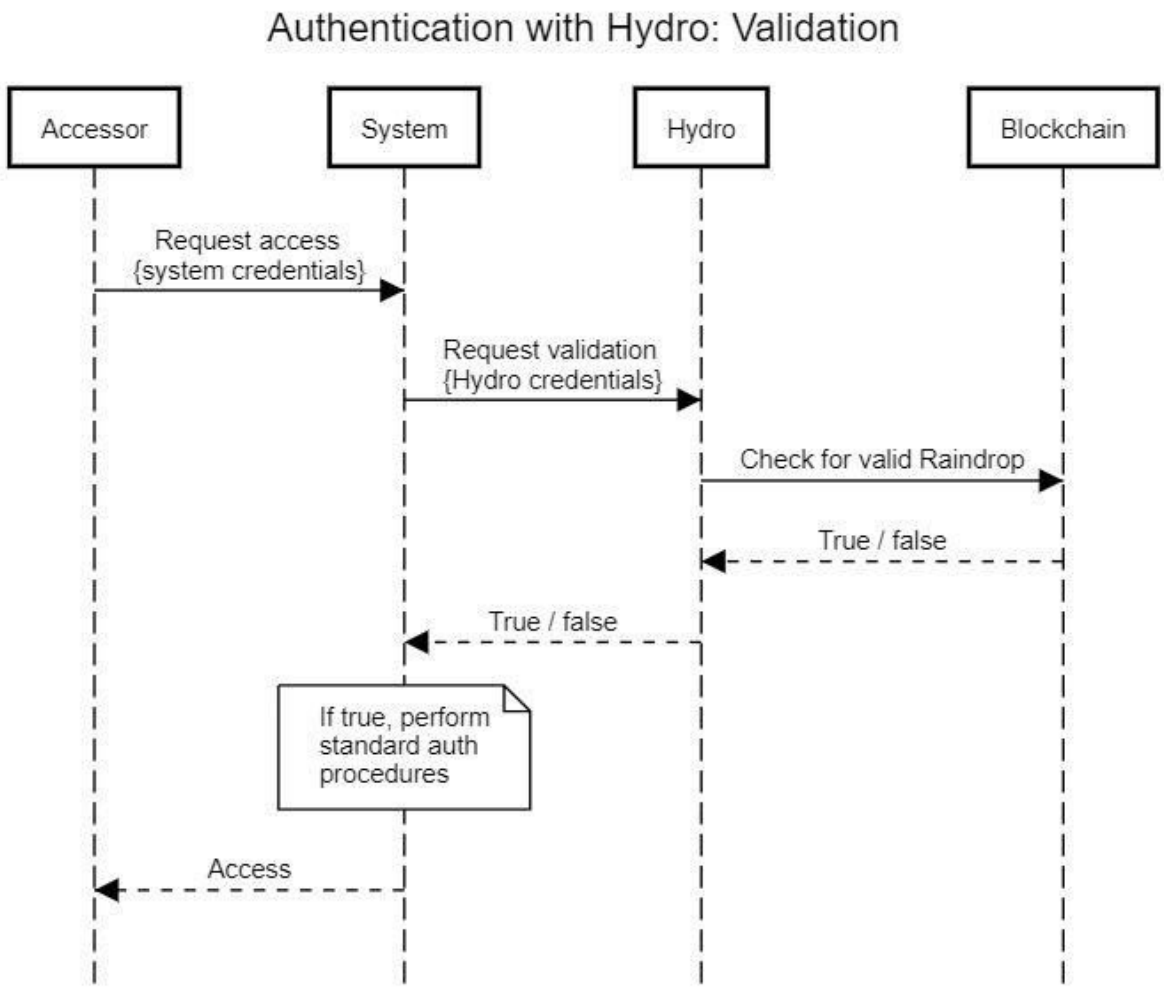
다음은 일반적으로 3 단계로 분류 할 수있는 인증 프로세스의 개요입니다.:

1. 초기화
2. 빗방울
3. 검증

초기화는 Hydro (하이드로)를 사용하고 자격 증명을 획득하도록 등록하는 시스템 (예 : 수소)으로 시작되어 시스템이 Hydro 모듈을 통해 블록 체인과 통신 할 수있게합니다. 이 시스템은 공공 주소를 등록한 접근 자 (예 : 금융 기관)에 탑재 한 다음 등록 된 주소를 Hydro로 전달합니다. 이 주소는 하이드로 스마트 계약서에 저장된 화이트리스트에 블록 체인에 영구히 기록됩니다. 시스템은 주소가 허용 목록에 포함되었다는 확인 메시지를 수신하며 공개적으로 볼 수있는 이벤트로 확인 될 수도 있습니다. 시스템 등록은 한 번만 수행하면되고 접근 자 화이트리스트는 접근 자 당 한 번만 필요합니다.



프로세스의 마지막 단계는 유효성 검사입니다. 이 단계에서 접근자는 공식적으로 시스템의 설정 메커니즘을 통해 시스템에 대한 액세스를 요청합니다. 표준 인증 프로토콜을 구현하기 전에 시스템은 접근 자 (Accessor)가 유효한 Raindrop 트랜잭션을 수행했는지 여부를 Hydro에 확인합니다. Hydro는 스마트 계약서와의 인터페이스를 통해 유효성을 확인하고참된/ 그릇된로 응답합니다. 시스템은 to이 지정에 기반하여 진행해야하는 방식을 결정하십시오. - 이것이 틀리면 시스템에서 액세스를 거부 할 수 있으며, 사실이라면 시스템이 액세스 권한을 부여 할 수 있습니다.



광범위하게 인증의 한 요소가되는 기본 시스템 자격 증명 또는 기존 시스템 프로토콜을 고려할 때 Hydro 계층이 유용한 두 번째 요소를 제공하는 것이 중요합니다. 두 가지 기본 공격 경로를 검토함으로써 우리는 그 유용성을 쉽게 확인할 수 있습니다:

- Vector 1 -공격자가 접근 자의 기본 시스템 자격 증명을 훔칩니다.
    1 공격자가 유효한 시스템 자격 증명을 사용하여 시스템에 대한 액세스를 시도합니다
    - 시스템은 Hydro와 점검하여 블록 체인에서 유효한 거래가 이루어 졌는지 판단합니다.
- Hydro는그릇된를 반환하고 시스템에서 액세스를 거부합니다.
- Vector 2 -공격자가 개인 키를 접근 자의 지갑으로 도용합니다.
    1 공격자는 Raindrop 세부 정보없이 등록 된 주소에서 Hydro 트랜잭션을 수행하려고 시도합니다.
- 공격자가 유효한 블록 체인 트랜잭션을 만들 수 없음
    - 공격자는 적절한 시스템 자격 증명 없이는 시스템에 대한 액세스를 요청할 수 없습니다.

공격자가 시스템에 액세스하려면 기본 시스템 자격 증명과 접근 자의 개인 지갑 키를 모두 훔쳐야합니다. 이와 관련하여 Hydro는 인증의 추가 요소를 성공적으로 추가했습니다..

대중에게 빗방울 열기

이 블록 체인 기반 인증 서비스는 Hydrogen API 생태계를 보호하기 위해 설계되었지만 다양한 플랫폼 및 시스템에 널리 적용 할 수 있습니다. 우리는 다른 사람들이 잠재적으로이 검증 레이어의 이점을 누릴 수 있다고 생각하기 때문에이를 사용하기 위해 개방하고 있습니다..

Hydrogen이 API 생태계에 액세스하기위한 전제 조건으로이를 통합하는 것과 마찬가지로 모든 시스템이 기존의 절차 및 프로토콜에도이를 추가 할 수 있습니다. API, 응용 프로그램, 엔터프라이즈 소프트웨어, 게임 플랫폼 등 모든 플랫폼이 인증 목적으로 Hydro를 활용할 수 있습니다. 이 블록 체인 계층을 인증 프레임 워크 또는 REST API에 통합하고자하는 사람들을위한 정식 문서가 GitHub에서 제공됩니다..

사례 연구 - raindrop 와 OAuth 2.0

빗방울 방출은 민간 단체에서 사용할 수있는 수십 가지 방법이 있습니다. 개인용 API, 데이터베이스 및 네트워크는 민감한 데이터를 보호하기 위해 지난 10 년 동안 토큰, 키, 응용 프로그램 및 프로토콜의 정교한 시스템을 만들었습니다. 예를 들어, Google은 Google Authenticator 앱을 통해 시장에서 가장 인기있는 제품 제공 업체 중 하나가되었습니다. 앞서 언급했듯이 이러한 기존 프로토콜을 경쟁하거나 대체 할 이유가 거의 없습니다.

사례 연구로, Hydrogen이 전체 API 보안 프레임 워크에서 보안 계층으로 Hydro 인증을 구현하는 방법에 대한 간략한 개요가 있습니다.:

1. 수소 API 파트너는 먼저 다양한 환경의 IP 주소를 허용 목록에 포함해야합니다.
2. 파트너는 공개 하이드로 주소를 허용 목록에 요청해야합니다..
3. Hydrogen API에 대한 모든 호출과 데이터 전송은 암호화되어 HTTPS 프로토콜을 통해 전송됩니다.
4. 파트너는 등록 된 하이드로 주소에서 유효한 하이드로 빗방울 거래를 완료해야합니다.
5. 파트너는 OAuth 2.0 인증을 사용해야합니다. OAuth (Open Authorization)는 토큰 기반 인증 및 권한 부여를위한 공개 표준입니다. 수소는 "자원 소유자 암호 자격 증명"및 "클라이언트자격 증명 "유형을 부여하고 각 API 사용자는 인증 요청에 대한 자격 증명을 제공해야합니다.
6. 위의 다섯 가지 요소 중 어느 것도 위반하지 않으면 Hydrogen 파트너에게 고유 한 토큰이 부여되어 각 API 호출을 통해 확인되고 확인됩니다..
7. 토큰은 24 시간 동안 유효하며, 그 후에 파트너는 자신을 다시 확인해야합니다..

위의 단계 중 하나라도 위반하면 사용자는 즉시 API 액세스로부터 잠김 상태가됩니다. 해커는 무수히 추측하여 이러한 보안 요소를 우회 할 수 없습니다. 수십억 가지의 고유 한 조합이 있기 때문입니다..

Hydro 블록 체인 기반 인증은 수소 보안 프로토콜의 중요한 구성 요소입니다. Hydrogen 팀은 파트너가 다중 서명 Wallet을 설정하고 다른 자격 증명과 독립적으로 여러 개의 안전한 위치에 개인 키를 저장하도록 권장하므로 단일 실패 지점이 없습니다. 적절히 보안이 설정된 다중 서명 지갑은 도용하기가 어렵지 않을뿐만 아니라 블록 체인의 공개 특성으로 인해 API의 보안과 관련된 모든 도용을 신속하게 인식 할 수 있습니다.

누구나 Hydro 스마트 계약에 대한 인증 시도를 볼 수 있습니다. 즉, 몇 달 동안 플랫폼이 손상된 날이 과거 일 수 있습니다. API 해커는 이제 전 세계 어느 곳에서나 예기치 않은 인증 시도를 실시간으로 감지 할 수 있기 때문에 즉시 처리 할 수 있습니다..

위험

소셜 미디어, 전자 메일 및 스트리밍 응용 프로그램 (전화 접속 연결에 의존하는)과 같은 초기 기술과 마찬가지로 핵심 개발 팀이 Ethereum 트랜잭션 속도 및 볼륨의 새로운 개발을 면밀히 추적해야합니다. 1995 년 YouTube의 출시를 상상해보십시오. 또는 Instagram이 Blackberry에서 처음 제공됩니까?

Vitalik Buterin 및 Joseph Poon과 같은 핵심 Ethereum 개발자는 Plasma : Scalable Autonomous Smart Contracts를 Ethereum 프로토콜로 업그레이드 할 것을 제안했습니다.:

> **Plasma는 스마트 계약의 인센티브 및 강제 실행을 위해 제안 된 프레임 워크로, 초당 상당량의 상태 업데이트 (잠재적으로 수십 억)로 확장 가능하여 블록 체인이 전 세계적으로 상당한 양의 분산 된 금융 응용 프로그램을 나타낼 수있게합니다. 이러한 현명한 계약은 네트워크 거래 수수료를 통해 자발적으로 계속 운영되도록 유도되며, 궁극적으로 트랜잭션 상태 전환을 시행하기 위해 기본 블록 체인 (예 : Ethereum)에 의존합니다.**

Raiden Network와 같은 다른 업체는 더 빠른 거래와 낮은 수수료를 제공하도록 설계된 오프 체인 (off-chain) 스케일링 솔루션을 제안했습니다. 현재 빗방울은 Ethereuem 프레임 워크에 최소한의 부담을 줄 것이므로 확장 성은 기술의 성공에 매우 작은 위험입니다.

결론

공용 블록 체인의 불변성은 API와 같은 사설 시스템의 보안을 향상시키는 새로운 방법을 제공합니다.

이 논문은 세 가지 중요한 것을 보여주었습니다:

1. 공공 블록 체인은 금융 서비스에 가치를 더할 수 있습니다..
2. 수력 빗방울은 사설 시스템의 보안을 향상시킬 수있다..
3. Hydrogen API 플랫폼 내에 Hydro Raindrop을 즉시 적용 할 수 있습니다..

Hydro 팀은 제시된 프레임 워크가 금융 서비스 업계의 모든 이해 관계자와 그 이상으로 이익을 얻을 수있는 새로운 하이브리드 사설 공용 시스템 모델의 표준 보안 인프라가 될 수 있다고 믿습니다.

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

