Hydro Raindrop

在区块链上验证公共身份

2018年1月

目录

摘要

HYDRO：词源 - 从古希腊文ὑδρο-（hudro-），ὕδωρ（húdōr，“水”）

Hydro使新的和现有的私有系统能够无缝整合和利用公共区块链的不变和透明动态，从而增强应用和文档安全性，身份管理，交易和人工智能。

在本文中，将对私有系统（如API）使用Hydro公共区块链通过公共身份验证来增强安全性进行说明。

所提议的技术被称为"Raindrop" - 通过智能合约执行的交易，公开验证私人系统访问，并且可以补充现有的私人认证方法。 该技术旨在为敏感的财务数据提供额外的安全性，这些数据越来越受到黑客攻击和违规风险的威胁。

在Hydro API平台上执行Hydro Raindrop的初始实施。 这套模块化的API可供全球的企业和开发人员用于原型，构建，测试和部署复杂的金融技术平台和产品。

Hydro Raindrop将作为开源软件提供给世界开发者社区，以便开发人员将Hydro Raindrop与任何REST API集成。

区块链和以太坊

Hydro在Ethereum网络上实施。 在提供有关该项目的更多细节之前，了解有关区块链和以太坊的一些基本概念非常重要。

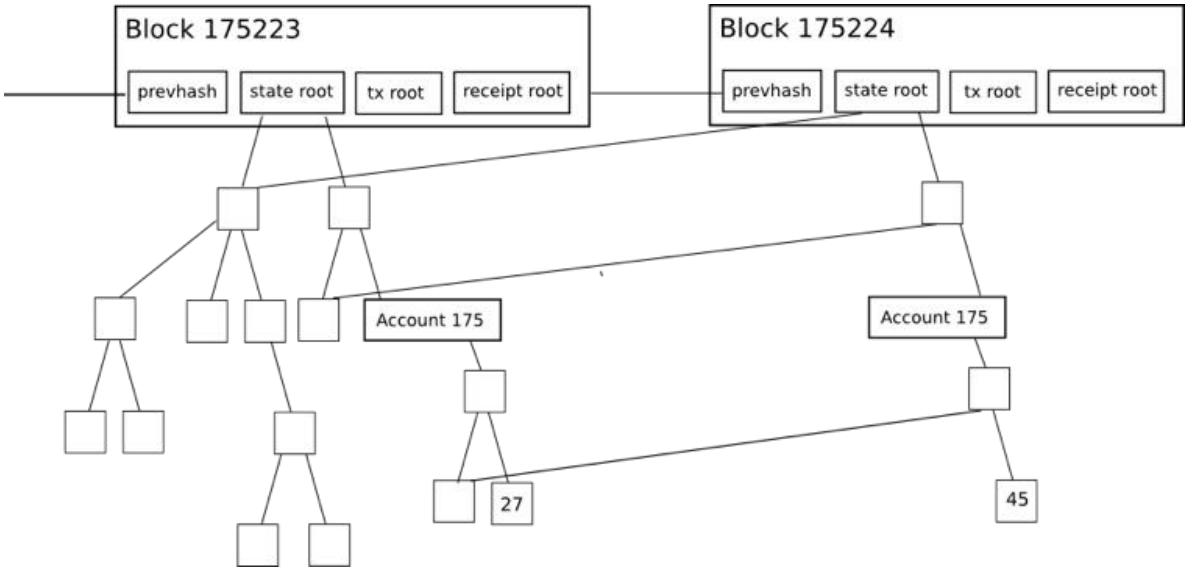
建立在以太坊上

就像Snapchat这样的应用程序是使用Swift和Apple iOS平台上提供的其他工具构建的，区块链应用程序也可以构建在以太坊之上。 Snap Inc.不需要构建iOS，而是将其作为基础设施来推出改变游戏规则的社交媒体应用程序。

Project Hydro与此类似。 它依靠全球数以千计的开发人员，致力于使底层区块链技术更快，更强大，更高效。 Hydro利用这种不断改进的基础设施，围绕区块链技术开发面向产品的交互，为金融服务应用提供实实在在的好处。

梅克尔树

Merkle树在分布式系统中用于高效的数据验证。 它们是有效的，因为它们使用散列而不是完整文件。 哈希是编码比实际文件本身小得多的文件的方式。
以太坊中的每个块头包含三个交易，收据和州的梅克尔树：



资源：[默克林在以太坊](#)； Vitalik Buterin，Ethereum创始人

这使轻量级客户机可以轻松获得可查证的查询答案，例如：

- 这个帐户是否存在？
- 目前的余额是多少？
- 此交易是否已包含在特定区块中？
- 今天在这个地址发生了一件特别的事件吗？

智能合约

以太坊和其他基于区块链的网络所启用的关键概念是智能合约。 这些是自我执行的代码块，多方可以进行交互，从而减少了对可信中间商的需求。 智能合同中的代码可以看作与传统纸张合同中的合法条款相似，但也可以实现更多的扩展功能。
合同可以有规则，条件，违规处罚或可以启动其他流程。 在触发时，合同按照原先在公开链上部署时的规定执行，提供不变性和分散化的内置要素。

智能合同是构建以太坊基础设施的重要工具。 Hydro区块链层的核心功能是通过定制合同实现的，如本文后面所讨论的。

以太坊虚拟机

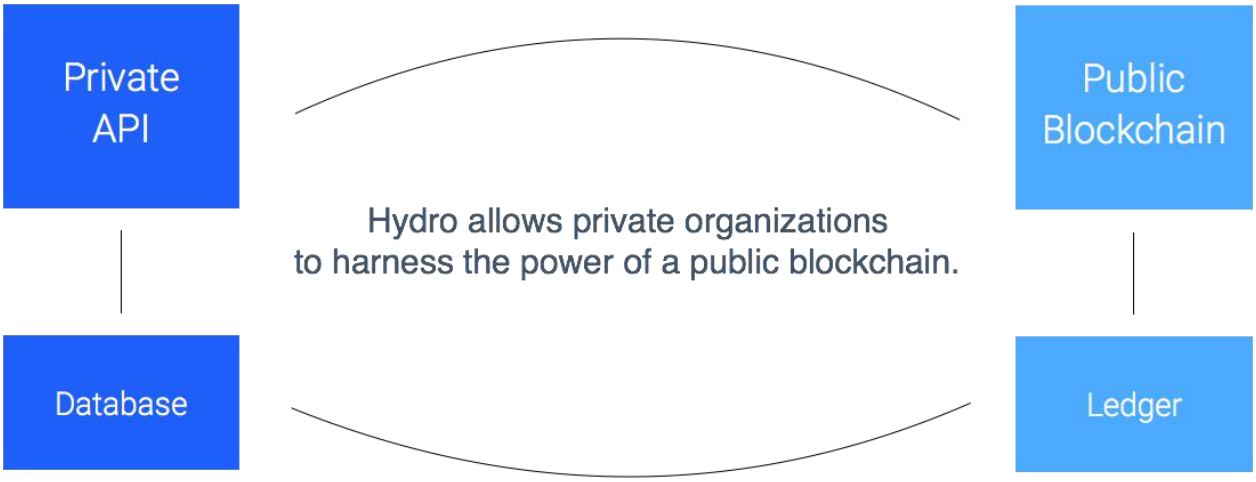
以太坊虚拟机（EVM）是以太坊智能合约的运行环境。 EVM有助于防止拒绝服务（DoS）攻击，确保程序保持无状态，并支持无法中断的通信。 EVM上的操作与其相关的成本（称为气体）取决于所需的计算资源。 每笔交易都有最大数量的气体分配给它，称为气体限制。 如果交易消耗的天然气达到限制，它将停止继续处理。

公共分布式账本

私人系统的公共总账

为金融服务平台，网站和应用程序提供支持的系统通常可以被描述为数据流的媒介 - 它们为它们所连接的实体发送，检索，存储，更新和处理数据。 由于这些数据的性质以及更普遍的金融服务的性质，这些系统通常以私人和集中的方式容纳复杂的操作。 反过来，依靠私人结构，通过合并超出内部系统范围的外部力量，为各种安全性，透明度和效率增加打开了大门。

Hydrogen的API平台就是这种情况。 Hydro旨在通过允许氢用户与区块链进行接口，以无缝方式集成到基本上私有的氢生态系统中，从而获得上述收益。

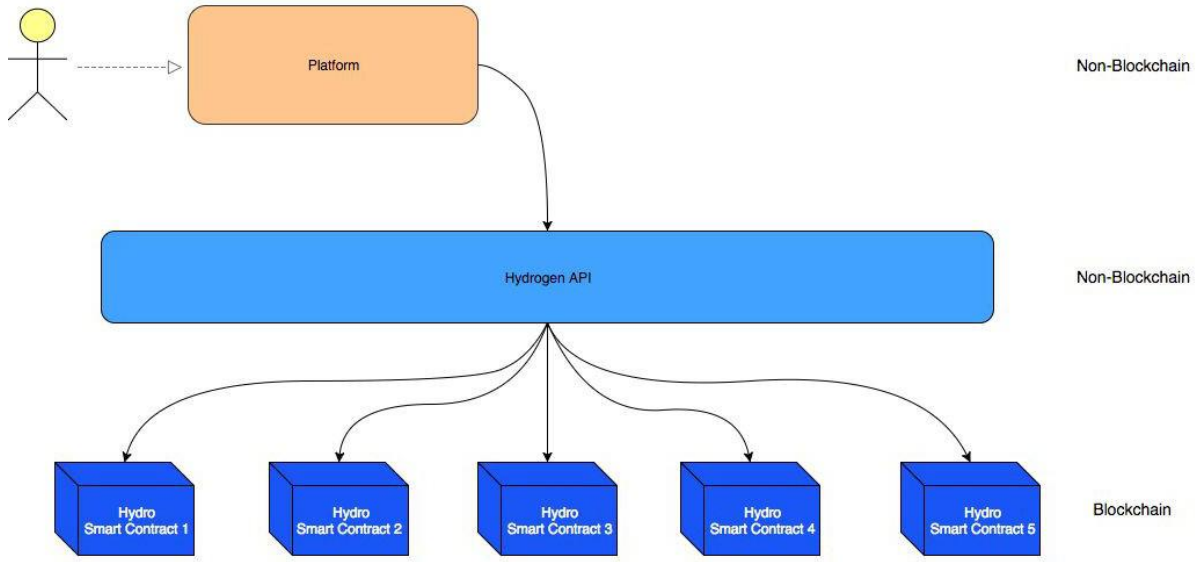


基于公共区块链的操作可以发生在私人操作之前，期间或之后。 私人和公共元素之间的相互作用可以用来验证，标记，记录或增强生态系统内的过程。

这种模式的特点是通过利用区块链技术的优势，特别是在可产生最积极影响的地方，使流程更加强大。虽然这种混合框架可能不适用于所有平台，但Hydro着重于为其提供价值。

采用的架构

Hydro与许多现有的区块链举措不同，因为它可以独立存在并围绕新的或现有系统分层，而不需要进行系统性更改。 Hydro不是要取而代之，而是要加强。 插入氢气API的平台和机构可以自动访问区块链。



可以利用氢气的金融服务平台的范围非常广泛。 这些平台几乎可以为任何经验提供动力，容纳任何数量的专有服务，执行任何私人数据操作，并在任何环境中部署。 Hydrogen的结构模块化使其成为可能，并与Hydro进行协作，作为采用的补充驱动器。

Raindrop

构建在Hydro公共账本之上的是基于区块链的身份验证服务，称为“Raindrop”。它提供了一个独特的，不可变的全球可见安全层，用于验证访问请求来自授权源。

诸如OAuth 2.0之类的私有认证协议为存在的一系列用例提供了不同级别的健壮性和实用性。 几乎没有必要与这些协议竞争或试图取代这些协议--Hydro提供了一种通过将区块链机制作为认证过程的组成部分来加强它们的方法。 这可以添加一个有用的安全层，以帮助防止系统泄露和数据泄露。

在研究Raindrop的技术方面之前，我们先来看看它正在试图解决的问题。

金融安全状况

数据时代的兴起带来了脆弱性的上升，这对金融服务业尤其重要。 金融平台通常是大量私人和敏感数据的门户，如政府身份证号码，账户凭证和交易记录。 由于这些数据非常重要，无保证的访问通常会遇到灾难性的结果。

行业研究公司Trend Micro发表了一份报告发现盗用的个人身份信息（PII）行项目在Deep Web上以低至1美元的价格出售，像护照这样的文档的扫描只需10美元，而银行登录凭证只需200美元，这使得被盗的数据日益分散和难以追查。

不幸的是，现有的金融系统在防范，诊断和沟通利益相关方的数据泄露方面没有一丝不苟的记录。

- 根据Javelin Strategy&Research最近的一项研究 -*2017年 身份欺诈研究*- 由于金融系统未能保护个人身份信息（PII），2016年有1500万美国消费者被盗，其中160亿美元被盗。
- 2017年4月，赛门铁克发布了它的*互联网安全威胁报告*，估计在2016年期间有11亿件PII受到各种能力的损害。

- 该*2016年年底数据违规快速查看*Risk Based Security发现，2016年全球企业发生了4,149起数据泄露事件，揭示了超过42亿条记录。

- 该*2017年泰雷兹数据威胁报告 - 金融服务版*对全球IT专业人士进行的专业服务调查发现，过去有49％的金融服务机构遭遇安全漏洞，78％的人花费更多的时间来保护自己，但73％的人正在推出与AI，物联网，和云技术，然后再制定适当的安全解决方

Equifax违规

2017年7月29日，拥有118年历史的美国信用报告机构Equifax被黑客入侵。 有1.43亿消费者接触过PII，包括社会安全号码。 209,000个客户的信用卡数据被泄露。

这种违规的原因是什么？

它始于Equifax使用的后端技术之一。 Struts是一个开源框架，用于开发由Apache软件基金会构建的Java编程语言的Web应用程序。CVE-2017-9805 是Apache Struts中与使用Struts REST插件和XStream处理程序处理XML负载有关的漏洞。 如果被利用，它允许未经身份验证的远程攻击者在应用程序服务器上运行恶意代码，以接管该计算机或发起进一步的攻击。 这是在Equifax违约前两个月由Apache修补的。

Apache Struts在REST插件XStream中包含一个缺陷，因为程序不安全地对用户提供的XML请求输入进行反序列化，所以会触发REST插件XStream。 更具体地说，问题出现在XStreamHandler的toObject（）方法中，当对对象使用XStream反序列化时，不会对传入值施加任何限制，从而导致任意代码执行漏洞。

即使这个REST插件受到了损害，它是否应该重要？ 有没有一种方法可以使用区块链技术来保护这些信息的财务信息
仍然依赖现有的REST API和基于Java的系统的1.43亿用户？

添加区块链图层

很显然，金融数据网关的完整性可以得到改善。 让我们来看看如何通过Hydro实现额外的安全层。

以太坊网络的基本共识机制确保交易有效性，因为参与者共同处理已妥善签署的交易。 这种现实导致了分权和不变性，但更重要的是，它为缓解对处理敏感数据的网关的未授权访问提供了一种载体。

借助Hydro，身份验证可以根据区块链上的事务操作进行预测。 例如，一个API可以选择验证开发人员和应用程序，通过要求他们启动特定事务，特定数据有效载荷以及区块链上特定地址之间的特定事务，作为启动标准身份验证协议的先决条件。

Hydro Raindrop

雨水包含直径在0.0001至0.005厘米范围内的浓缩水包。 在典型的暴雨中，有数十亿个这样的包，每个包都有随机大小，速度和形状。 因此，人们无法可靠地预测降雨的确切性质。 同样，每个Hydro认证交易都是独一无二的，几乎不可能偶然发生 - 这就是我们称之为Raindrop的原因。

金融服务平台通常使用微存款验证来验证客户账户。 这个概念很简单：该平台将小量的随机数量存入用户的银行账户。 为了证明用户确实拥有所述帐户，他或她必须将存款金额返还给平台，然后验证平台。 用户可以知道有效金额（除猜测外）的唯一方法是访问有问题的银行帐户。

使用Hydro进行基于Raindrop的验证是类似的。 我们定义了一个事务，而用户必须从一个已知的钱包中执行它，而不是向用户发送一个金额并将其返回。 用户可以进行有效交易的唯一方法是访问有问题的钱包。

通过使用Raindrops，系统和访问者都可以监视对不可变公共分类账的授权尝试。 这种基于区块链的交易与基本系统操作分离，发生在分布式网络上，并取决于私钥的所有权。 因此，它可以作为有用的验证向量。

详细的外观

Hydro身份验证过程涉及四个实体：

1. *访*问者 - 试图访问系统的一方。 就氢的情况而言，访问者是将氢气API用于其核心数字基础设施的金融机构或应用程序。
2. *系*统 - 访问者正在访问的系统或网关。 对于氢气，系统本身就是氢气API。
3. *Hy*dro - 系统利用该模块与区块链进行通信和连接的模块。
4. *区*块链 - 处理HYDRO交易并包含Hydro 智能合约的分布式公共分类帐，通过它可以推送，拉取或以其他方式操作信息。

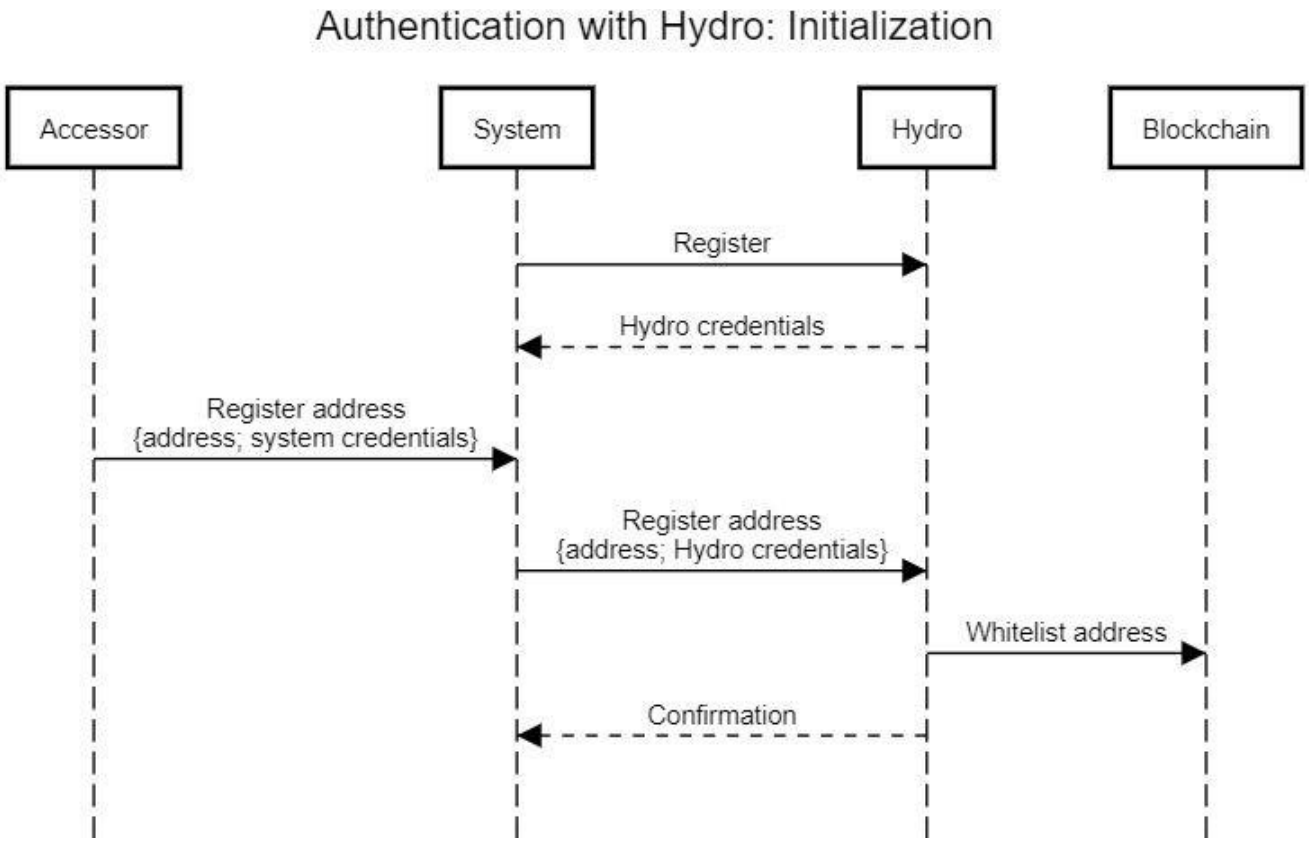
整个Raindrop是一组五个事务参数：

1. *发*件人 - 必须启动交易的地址。
2. *收*货人 - 交易的目的地。 这对应于在Hydro智能合约中调用方法。
3. *ID* - 与系统关联的标识符。
4. *数*量 - 要发送的精确数量的HYDRO。
5. *挑*战 - 随机生成的字母数字字符串。

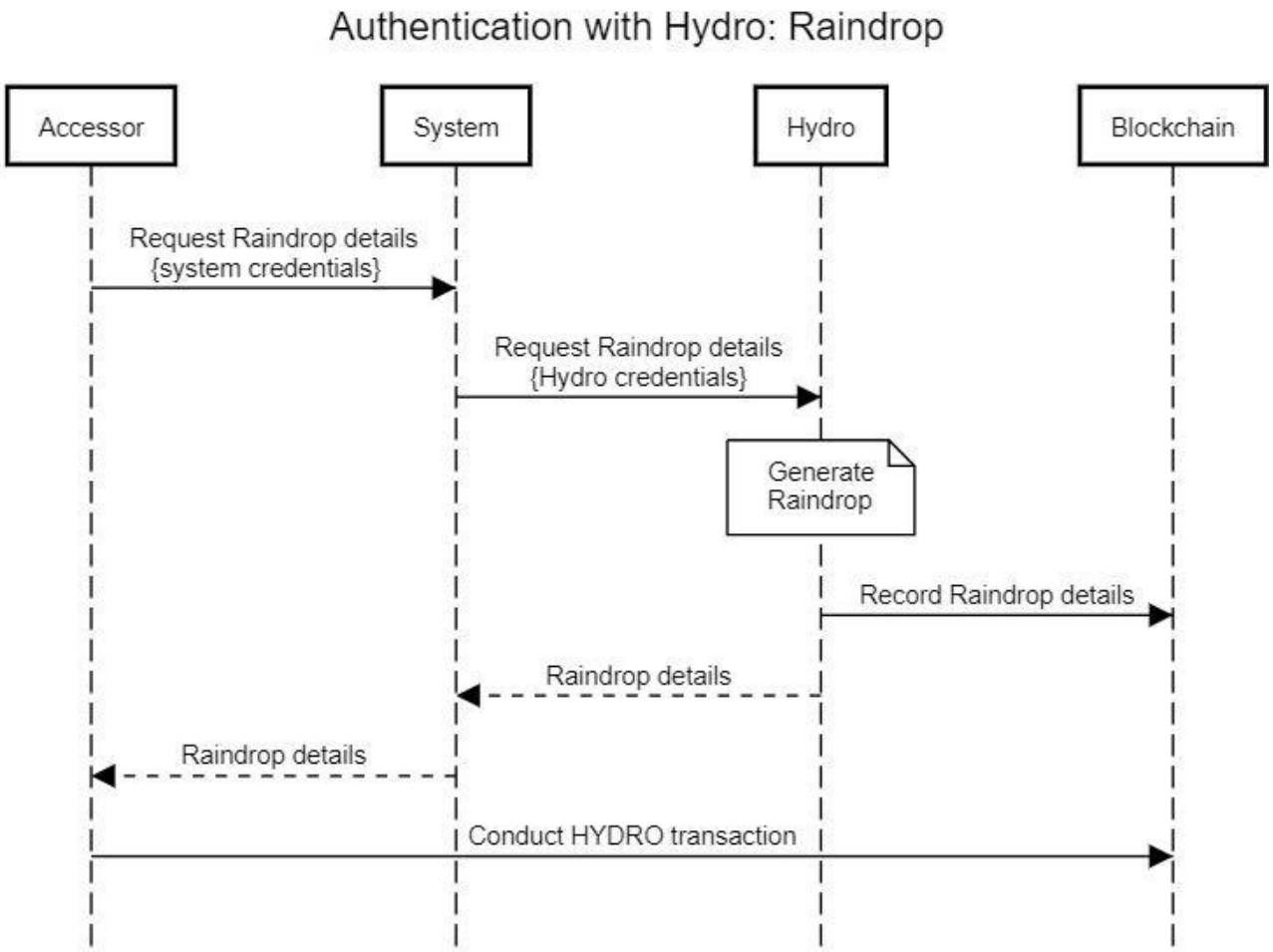
以下是认证过程的概述，通常可以分为三个阶段：

1. 初始化
2. Raindrop
3. 验证

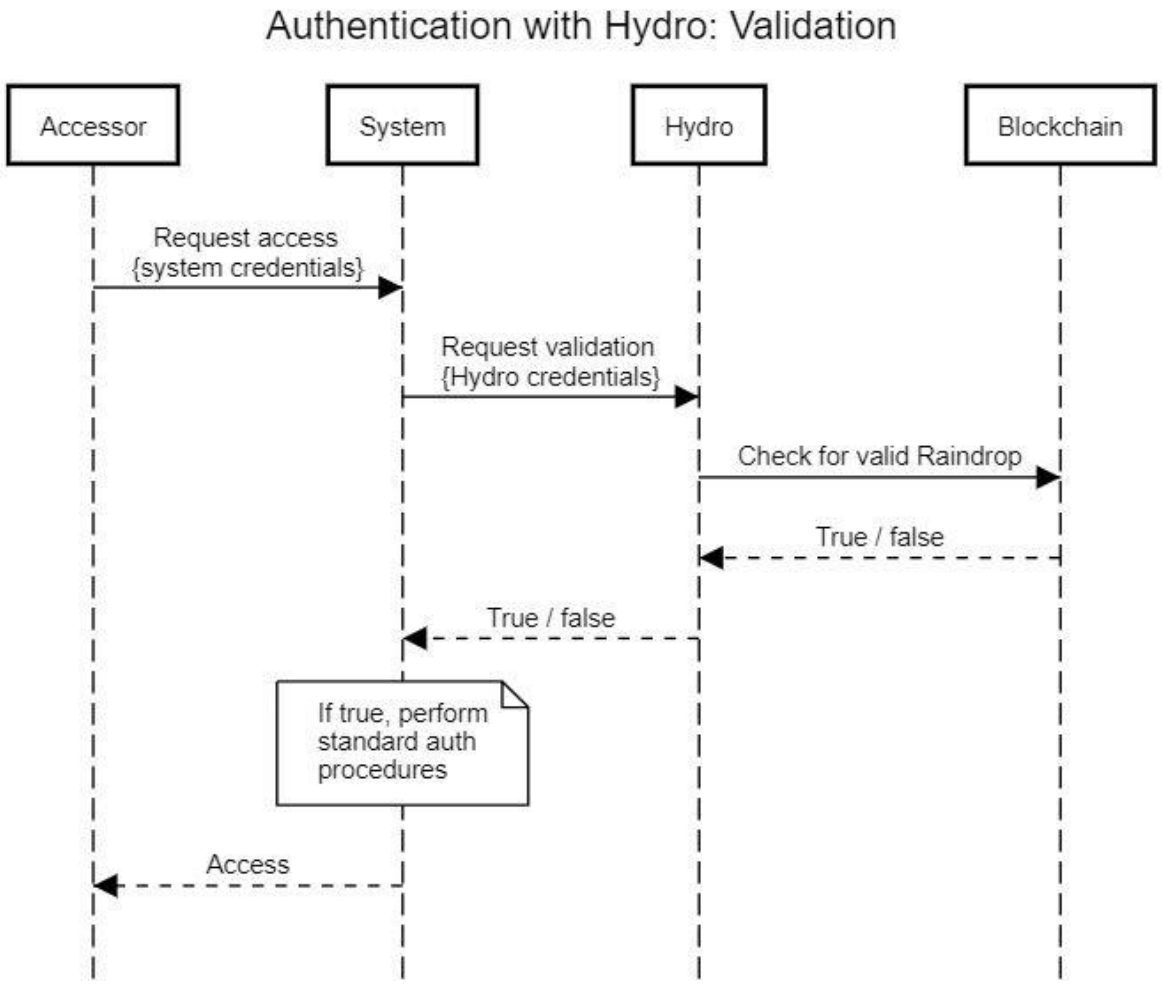
初始化从一个系统（例如氢气）注册到使用Hydro并获取凭据，使系统能够通过Hydro模块与区块链进行通信。 系统登录一个登记公共地址的访问者（例如金融机构），然后将登记的地址传递给Hydro。 该地址被永久地写入区块链，存储在Hydro智能合约中的白名单中。 系统收到确认地址已被列入白名单，也可以将其验证为公开查看的事件。 系统注册只需要进行一次，而访问者白名单只需要对每个访问者进行一次。



初始化完成后，Hydro认证过程的核心就可以开始了。 Accessor必须执行Raindrop事务，通过向系统请求Raindrop详细信息来启动此过程，系统会将请求路由到Hydro。 Hydro生成一个新的Raindrop，在区块链上不断存储某些细节，并通过系统将完整的详细信息返回给Accessor。 Accessor配备了所有必需的信息，从注册地址到Hydro智能合同中的方法进行交易。 如果该地址未列入白名单，则该操作将被拒绝 - 否则，会将其记录在智能合约中。 需要注意的是，这个事务应该在系统之外发生，直接从Accessor到Blockchain，因为它必须使用Accessor的私钥（只有Accessor应该能够获得）进行签名。



该过程的最后一步是验证。 在这一步中，访问者通过系统建立的机制正式请求访问系统。 在实施任何标准认证协议之前，系统询问Hydro是否访问者执行了有效的Raindrop事务。 Hydro与智能合约的接口，检查有效性，并以真/假指定作出响应。 系统能够根据这一指定决定应该如何进行 - 如果它是错误的，系统可以拒绝访问，如果它是真的，则系统可以授予访问权限。



如果我们考虑基础系统凭证 – 或者现有的任何现有系统协议 – 广泛地作为认证的一个因素，Hydro层提供有用的第二个因素是很重要的。 通过检查两个主要攻击媒介，我们可以很容易地确认它的有用性：

- 向量1 – 攻击者窃取访问者的基本系统证书
  - 攻击者尝试使用有效的系统凭证访问系统
  - 系统检查Hydro是否有效的交易
    在区块链上制作
  - Hydro返回false，系统拒绝访问
- 向量2 – 攻击者将私钥窃取到访问者的钱包
  - 攻击者尝试从注册地址进行Hydro交易，无需Raindrop细节
  - 攻击者无法进行有效的区块链交易

- 如果没有正确的系统证书，攻击者也不能请求访问系统

很明显，攻击者必须窃取基本系统凭证和访问者的私人钱包密钥才能访问系统。 在这方面，Hydro已成功添加了一个额外的身份验证因素。

向公众开放Raindrop

虽然基于区块链的身份验证服务的架构旨在帮助保护Hydrogen API生态系统，但它广泛适用于不同的平台和系统。 因为我们觉得其他人可能会从这个验证层受益，所以我们正在开放使用它。

正如Hydrogen将其整合为访问其API生态系统的先决条件一样，任何系统都可以将其添加到现有的程序和协议中。 任何平台 - 无论是API，应用程序，企业软件，游戏平台等 - 都可以利用Hydro进行身份验证。 正式的文件将是在GitHub上可用对于那些希望将此区块链层合并到认证框架或REST API中的用户而言。

案例研究 - Raindrop与OAuth 2.0

Raindrop发行版可以由私人组织使用的方法有很多种。 私有API，数据库和网络在过去的十年中创建了精巧的令牌，密钥，应用程序和协议系统，以保护敏感数据。 例如，谷歌凭借Google Authenticator应用成为市场上最受欢迎的产品提供商之一。 如前所述，几乎没有理由竞争或取代这些现有的协议。

作为案例研究，下面简要概述Hydrogen如何在其整个API安全框架中将Hydro认证实施为安全层：

1. 氢气API合作伙伴必须首先将各种环境的IP地址列入白名单。
2. 合作伙伴必须要求将公共Hydro地址列入白名单。
3. 所有对氢气API的调用和数据传输均通过HTTPS协议进行加密和传输。
4. 合作伙伴必须从注册的Hydro地址完成有效的HydroRaindrop交易。
5. 合作伙伴必须使用OAuth 2.0验证。 OAuth（开放授权）是基于令牌的认证和授权的开放标准。 Hydrogen支持“资源所有者密码凭证”和“客户端凭证”授予类型，并且每个API用户必须提供认证请求的凭证。

6. 如果上述五个元素均未被违反，则氢合作伙伴会被授予唯一标记，以便在每次调用API时进行检查和验证。
7. 令牌有效期为24小时，之后合作伙伴必须再次验证自己。

如果违反这些步骤中的任何一个，则用户立即被锁定以禁止API访问。 黑客无法通过随机猜测绕过这些安全因素，因为有万亿个独特组合。

基于Hydro区块链的认证是Hydrogen安全协议的重要组成部分。 氢气团队鼓励合作伙伴成立多签名钱包以及将私钥存储在与其他凭证无关的多个安全位置，因此不存在单点故障。 一个妥善保护的多重签名钱包不仅难以窃取，而且区块链的公共性质也可以迅速识别与API安全性有关的任何盗窃行为。

任何人都可以查看对Hydro智能合约的身份验证尝试，这意味着平台受到数月的损害的日子可能已成为过去。 由于能够从世界任何地方实时检测意外的授权尝试，因此API黑客现在可以更加直接地受挫。

风险

就像任何新兴技术一样，例如社交媒体，电子邮件和流媒体应用（依赖于拨号连接）的初期，核心开发团队紧密跟踪以太坊交易速度和数量的新发展，这一点非常重要。 你能想象YouTube试图在1995年推出吗？ 或者首次在黑莓上推出Instagram?

核心以太坊开发人员如Vitalik Buterin和Joseph Poon已经提出了这个建议等离子：可扩展的自主智能合约升级到以太坊协议：

> **等离子体是激励和强制执行智能合约的建议框架，可扩展到每秒大量的状态更新（可能为数十亿次），使区块链能够在全球范围内代表大量的分散式金融应用程序。 这些智能合约被激励以通过网络交易费用自主地继续运作，这最终依赖于底层区块链（例如以太坊）来强制执行交易状态转换。**

其他公司，例如Raiden Network，已经提出了一种链外扩展解决方案，旨在为更快的交易和更低的费用提供支持。 目前，Raindrop将对Ethereuem框架施加最小的压力，因此可扩展性对于该技术的成功来说是一个非常小的风险。

结论

公开区块链的不变性提供了增强API等私有系统安全性的新方法。

本文显示了三件重要的事情：

1. 公共区块链可以增加金融服务的价值。
2. Hydro Raindrop可以增强私人系统的安全性。
3. Hydro Raindrop在氢气API平台中有直接应用。

Hydro 团队认为，所提出的框架可以作为混合型私营 - 公共系统新模式的标准安全基础设施，这将有利于金融服务行业内外的所有利益相关方。

资料来源：

Ethereum;默克林在以太坊
Trend Micro;黑客用你被盗的身份做什么？
Javelin Strategy & Research;*2017年身份欺诈研究*
Symantec;*互联网安全威胁报告*
Risk Based Security;*2016数据泄漏趋势 - 年度回顾*
Thales;*2017年泰雷兹数据威胁报告 - 金融服务版*
Apache.org; Apache Struts 2文档 - S2-052
Joseph Poon和Vitalik Buterin;等离子：可扩展的自主智能合约