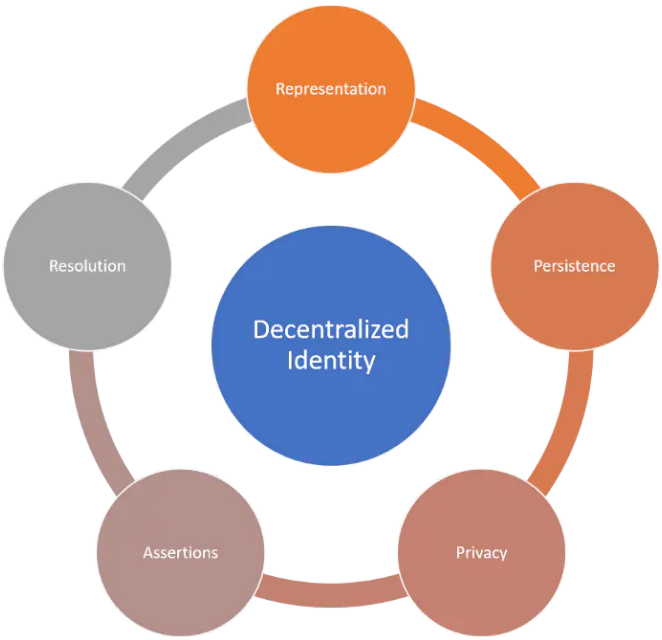
Sidetree - 去中心化身份管理协议

编程狂魔 关注
2019.05.31 11:54:33 字数 1,838 阅读 457

身份（Identity）管理是区块链应用的核心元素。在一个不可信、匿名的分布计算生态中，要实现去中心化身份管理并不是一件容易的事情。Sidetree是一个基于现有区块链平台的第二层（L2s）协议，专门用于去中心化身份管理。微软最新开源的ION项目，就是Sidetree协议基于比特币区块链的一个实现。本文将分6个部分介绍Sidetree去中心化身份管理协议：DID的核心要素、Sidetree协议的起源、概述、工作原理、设计约束与实现进展。

1、去中心化身份管理的核心要素

去中心化身份管理的挑战并不是单一模块的问题。在去中心化应用（DApp）中，一个身份的生命周期中，有一些需要考虑的关键因素：



did key elements

- 表示：用来描述主体身份的可迁移表示
- 持久化：用来存储、提取主体身份的机制，同时还需要保持其隐私
- 隐私：在去中心化账本中保护主体身份的模型
- 断言： 确定主体身份的特定语句
- 解析：解析、验证特定主体身份的机制

2、Sidetree协议的起源

2017年，去中心化身份组织（DIF）的一些成员开始讨论如何在全球级别实现去中心化身份系

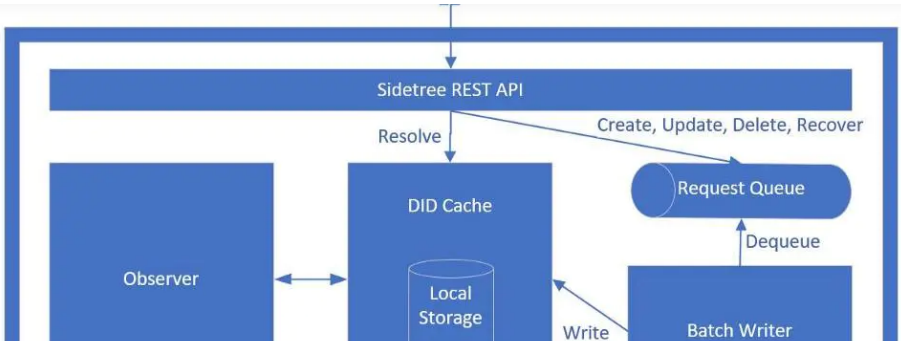
区块链的的可伸缩性不是小问题，但是目前已经存在一个有前途的思路来解决基于区块链的系统的伸缩性问题：第二层协议或L2s，例如：状态通道、侧链和比特币闪电网络。L2s通过确定性（Deterministic）处理与交易方案来实现可伸缩性，这些交易是在区块链之外完成的，只需要在与所依托的底层区块链交互时进行极少的共识处理。

要实现去中心化身份管理，就需要一个大规模运行的系统，同时具备一些核心特性，例如确定性状态解析以及差分持久化。在过去的18个月中，IDF成员间的思想交流最终形成了一个完整的第二层协议：Sidetree。

3、Sidetree协议概述

Sidetree协议本身并不是去中心化身份（DID）方法，它由一组代码层级的组件构成，包括确定性处理逻辑、内容寻址存储抽象以及可以部署到第一层的去中心化账本（例如：公有链）上的状态验证过程，从而实现无需许可的、第二层DID网络。通过使用特定链相关的适配器，Sidetree协议可以用来在不同的链上创建不同的第二层去中心化身份网络，这些特定链的适配器负责实现与底层区块链的读写交互。

无论底层采用哪种区块链，Sidetree协议的几乎所有实现代码都保持一致，这使得它可以适用于多种区块链平台。下面是Sidetree系统的总体结构，以比特币作为目标区块链，不过如前所述，这也适用于其他区块链：



sidetree arch

Sidetree协议基于一组模块化组件实现，最重要的包括：

- Sidetree**内核** / Sidetree Core ：
  Sidetree内核是主要的逻辑模块，它监听来自底层区块链的交易输入，并使用CAS模块（下面介绍）提取其中的DID操作，然后组合/验证每个DID的状态。

- **内容寻址存储** / Content Address Storage ：
  CAS（Content Address Storage）模块是一个基于哈希的存储接口，网络中的第二层节点使用该接口来交换彼此识别的DID操作批次，以便进行本地持久化和网络传播。该接口抽象自所使用的特定CAS协议，但是值得指出的是，DIF成员已经为此功能选择了IPFS。

- **区块链/账本适配器** / Blockchain/Ledger Adapter ：
  适配器中包含了任何需要读写特定区块链的代码，以便解除Sidetree主体对特定区块链的依赖。不同的底层链需要分别实现不同的适配器。

4、Sidetree**协议工作原理**

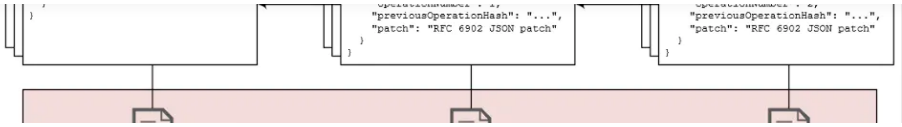
基于Sidetree的L2节点按如下步骤来创建、读取和处理DID操作：

1. 要将批操作写入基于Sidetree的L2网络的节点首先汇集尽可能多的DID/DPKI操作（基于确定性协议规则确定的上限），然后创建一个L1链上交易并在交易中嵌入该操作批次的哈希。

2. DID操作的源数据由发起节点本地存储，并推送到IPFS网络。当其他节点获知嵌入Sidetree操作的底层链交易后，这些节点将向原始节点或其他IPFS节点请求该批次数据。

3. 当一个节点收到某个批次后，它会将元数据固定到本地，然后Sidetree核心逻辑模块解压批次数据来解析并验证其中的每个操作。目标链的区块/交易体系是Sidetree协议唯一需要的共识机制，不需要额外的区块链、侧链或咨询权威单元来让网络中的DID达成正确的PKI状态。

下面是关于批次与操作嵌入目标区块链的更详细的示意图：



embed

5、Sidetree协议的设计约束

Sidetree协议在设计时做出了一些关键的假设：

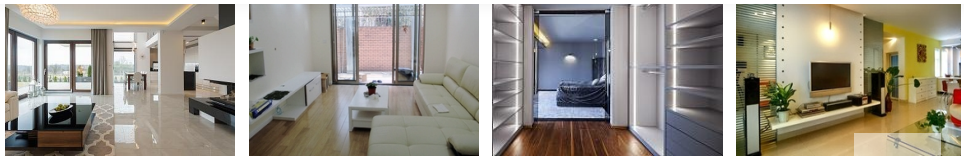
1. DIDs不可转让，协议没有提供一个逻辑实体转让、购买或获取其他逻辑实体的DID的途径。这对于DID/DPKI用例是可行的，但是不适用于资金的双花（double spend -- 讨厌这个名词的翻译，一种轻佻的感觉）。
2. 可以延迟揭示嵌入的批次数据，基于确定性规则集进行处理。
3. DID状态彼此独立，依次一个DID的持有者智能影响它自己的DID的状态。

6、Sidetree协议的实现进展

目前在DIF成员中，有两个团队分别使用Sidetree协议为比特币和以太坊开发L2层的去中心化身份网络。微软主要聚焦于比特币网络，而Transmute Industries则与ConsenSys合作在开发以太坊版本。你可以在这里
查看微软ION项目的实现代码。

原文： The Sidetree Protocol: Scalable DPKI for Decentralized Identity

汇智网 / Hubwiz.com 翻译整理，转载请标明出处。



被以下专题收入，发现更多相似内容

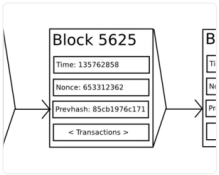
区块链 区块链大学 区块链研习社

推荐阅读

更多精彩内容 >

[中文] 以太坊白皮书

以太坊（Ethereum）:下一代智能合约和去中心化应用平台 翻译：巨蟹、少平 译者注：中文读者可以到以太坊爱...



车圣 阅读 2,870 评论 1 赞 7

iOS UIKit框架学习—UITableViewCell

UITableViewCell类定义了在UITableView对象出现时每个单元格的属性和行为。该类包括设置和管理...

Wynter_Wang 阅读 199 评论 0 赞 0

什么样的合同是电子合同

夫妻惊喜

老婆每次逛商场，都要抓几个娃娃，我发现了她这个爱好，决定给她一个惊喜。三八妇女节那天，我买了一台抓娃娃机！老婆却一...

有说有笑有情调 阅读 128 评论 2 赞 4

绝句五十六法

七言绝句"以其善言情而易合于乐"，"最合于诗人之陶写"，"自唐迄今千数百年，为之者众，好之者弥笃"（邵祖平《七...

墨兵书院 阅读 1,043 评论 5 赞 1

教案2018-08-27

1.明理篇：学习诗歌《二子乘舟》——诗经 邶风 2.作文篇：模仿李峤的《风》，练习白话文写作《咏日》 3.学习篇：...

愚者愚心 阅读 58 评论 0 赞 0

写下你的评论... 评论0 赞