

# PAI 数据

## Project PAI数据协议摘要

作者：

杜锦程<sup>1</sup>

方丹博士<sup>2</sup>

Mark Harvilla博士<sup>3</sup>

## 摘要

Project PAI数据协议（“PAI数据”）是对Project PAI区块链协议扩展的一个规范，其中包括一个对任意数据进行保护和提供访问的方法。在PAI币发展提案（PDP）2 [1]的背景下，本文定义了PAI数据支持的两种重要交易类型：存储交易（即便于数据存储和所有权证明的交易）和共享交易（即旨在实现授予和撤销指定接收人对数据访问权限的交易）。本文同时还提供了一个PAI数据协议与类似基于区块链的文件存储系统之间的比较分析。

<sup>1</sup> ObEN公司区块链研究员

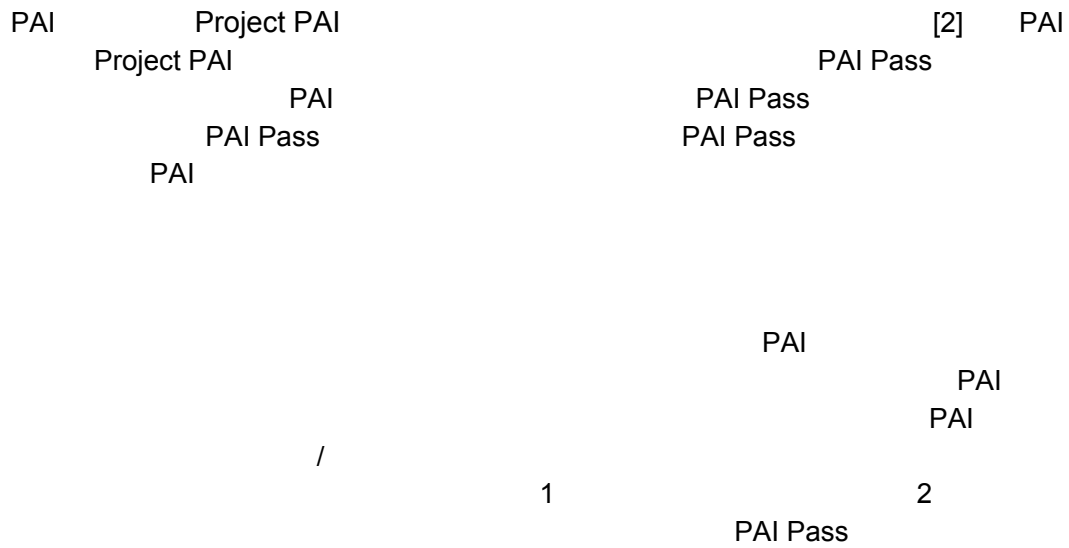
<sup>2</sup> ObEN公司区块链研究员

<sup>3</sup> ObEN公司首席工程师

# 介绍

Project PAI数据协议（“PAI数据协议”）是对扩展Project PAI区块链协议扩展的一个规范，其中包括一个保护和提供对任意数据进行保护和提供访问的方法。这是通过利用一个定制的OP\_RETURN数据协议和椭圆曲线加密（elliptical encryption），并结合数据存储（例如，用于去中心化存储的由种子节点组成的分段式网络或用于中心化存储的专有数据存储）来实现的 [1]。

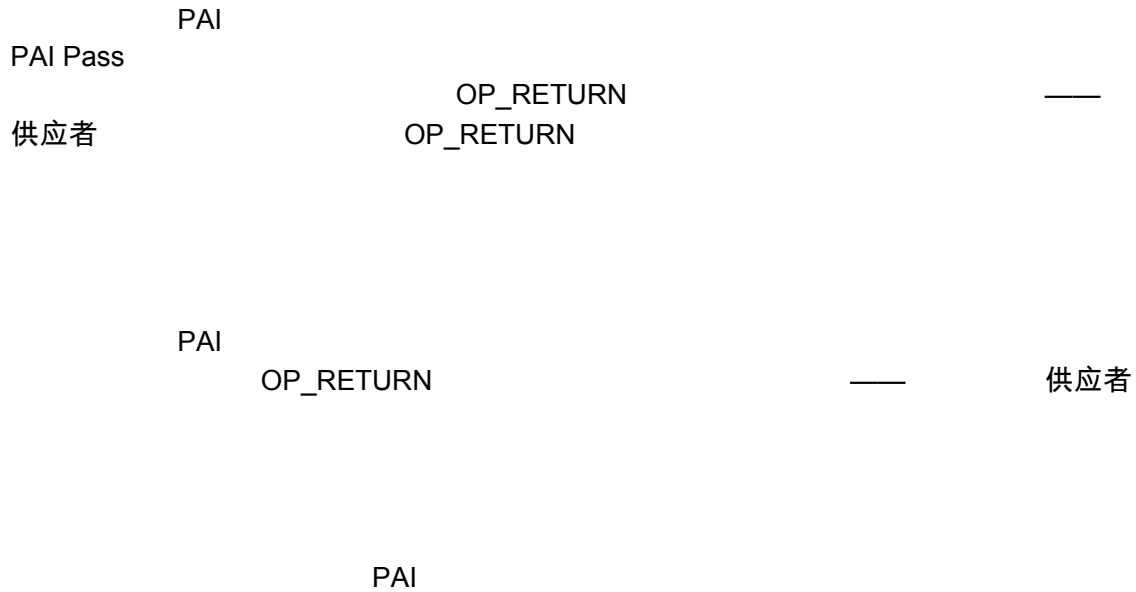
## PAI



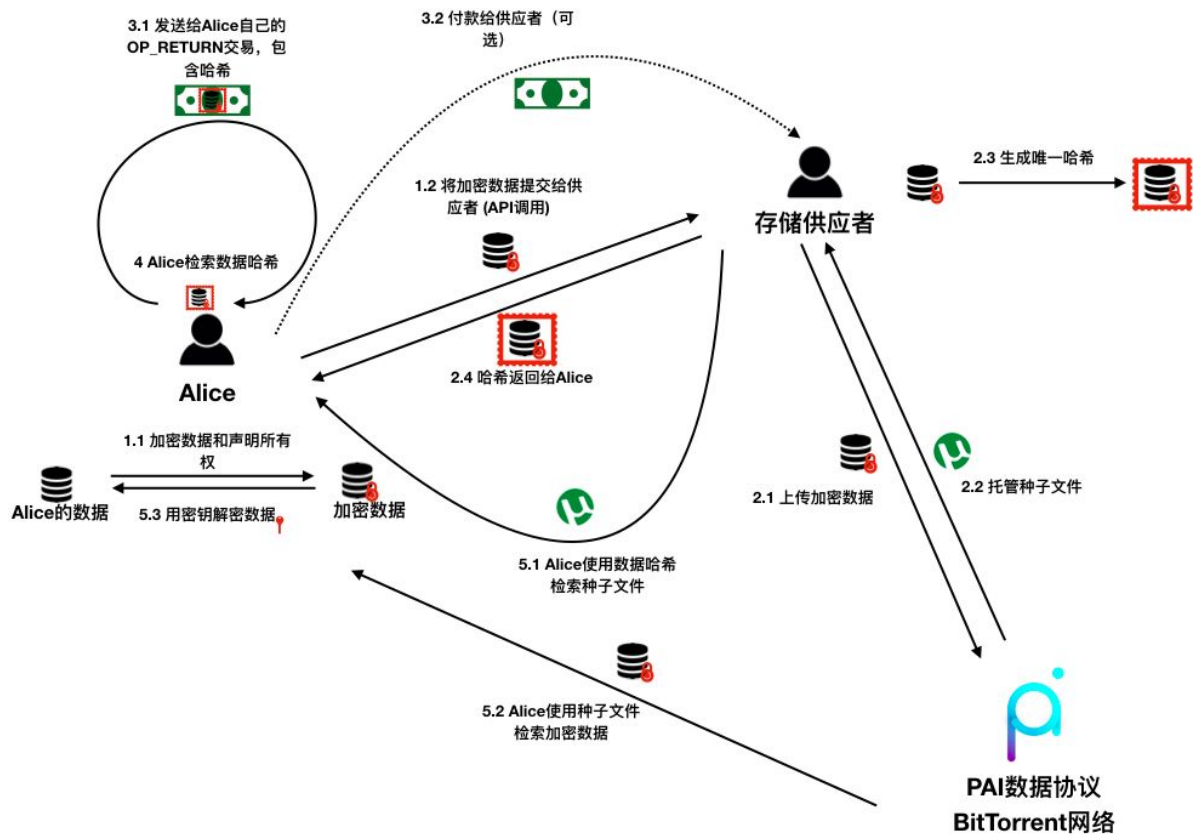
# 技术说明

PAI数据协议的主要构成有:

- Project PAI区块链
- OP\_RETURN操作码
- 椭圆曲线加密(Elliptical Encryption)
- (数据) 发送者 + (存储) 供应者 + (数据) 接收者
- 数据存储 (例如, 由种子节点组成的分段式网络)



<b>如果您需要...</b>	<b>那么您应该使用...</b>
存储和/或声明数据的所有权 (例如, 数字资产、知识产权)	PAI存储交易
授予接收人数据权限	PAI共享交易 (依据 PDP 2 [1], 带有一个“授予”操作ID (“grant” Operation ID) )
撤消收件人使用数据的权限	PAI共享交易 (依据 PDP 2 [1], 带有一个“撤消”操作ID (“revoke” Operation ID) )

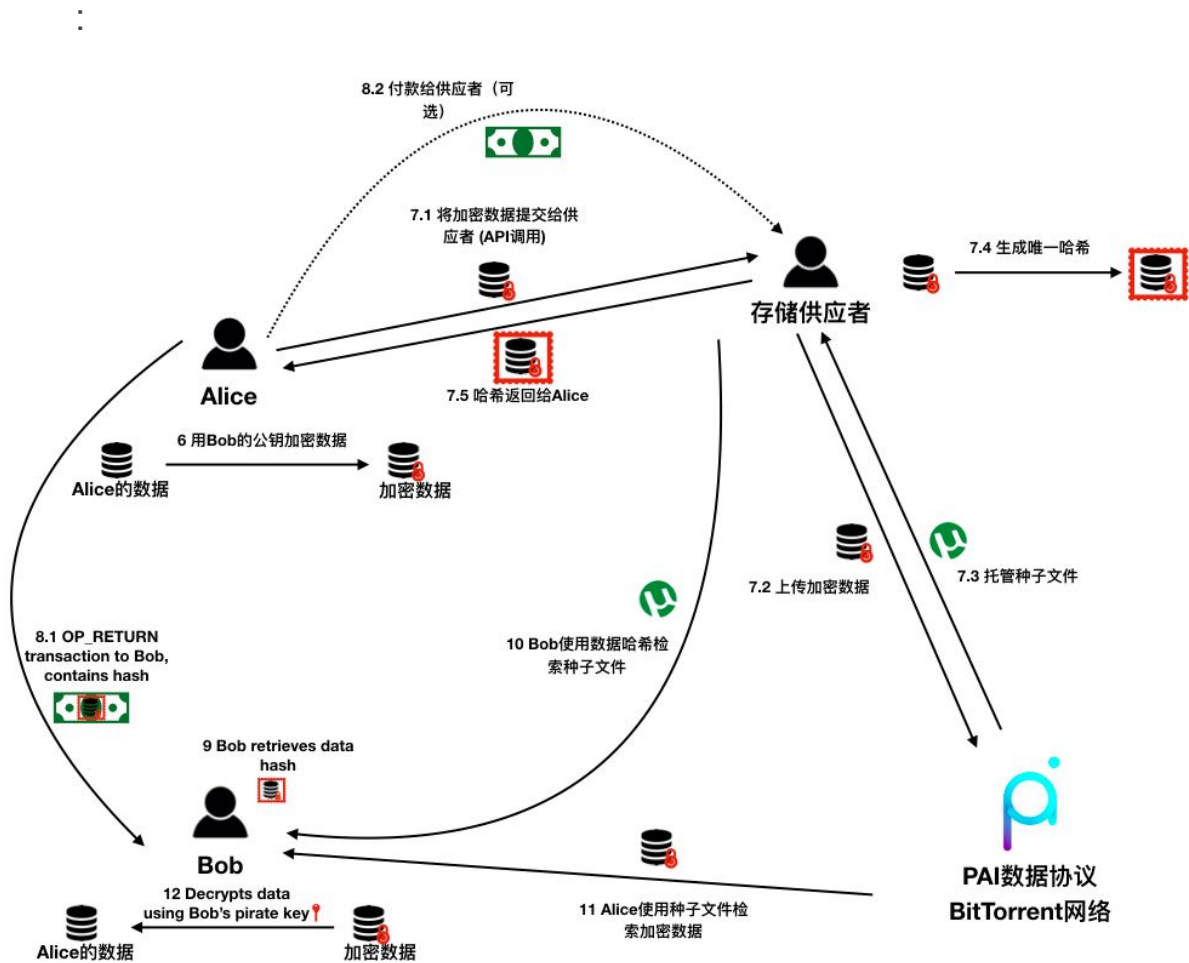


1.

如图1所示，一方（例如，Alice）可以通过PAI数据交易存储数据并声明对所存储数据的所有权。方法如下：

1. Alice用她的公钥加密数据，包括对所有权或作者身份的声明。此加密数据只能由拥有相应私钥的Alice进行解密。
2. Alice选择存储供应者，并且通过协议指定的一系列标准API调用（即“供应者API”），将加密数据提交给供应者。存储供应者：
  - a. 将数据上传到PAI数据BitTorrent网络。
  - b. 托管相应的种子文件。
  - c. 生成与数据关联的唯一哈希。
  - d. 哈希返回给Alice。
3. Alice创建一个PAI数据协议交易，有两个输出：
  - a. 发送给Alice自己的OP\_RETURN交易：此输出包含OP\_RETURN操作码字段中加密数据的哈希。
  - b. 付款给供应者（可选）：此输出根据各方之间的离线协议补偿存储供应者托管种子文件的服务。
4. Alice接收OP\_RETURN交易并检索数据哈希

- 如果Alice希望提出所有权声明或以其他方式检索数据，（1）使用数据哈希从存储供应者处检索种子文件；（2）从PAI数据BitTorrent网络处下载数据；（3）使用她的私钥解密数据。



2.

如图2所示，双方（例如数据发送者Alice和数据接收者Bob）可以以下文的方式通过PAI数据协议交易来互相分享数据。

- Alice用Bob的公钥加密数据。此加密数据只能由拥有相应私钥的Bob进行解密。
- Alice选择存储供应者，并且通过协议指定的一系列标准API调用（即“供应者API”），将加密数据提交给供应者。存储供应者：
  - 将数据上传到PAI数据BitTorrent网络。
  - 托管相应的种子文件。
  - 生成与数据关联的唯一哈希。
  - 哈希返回给Alice。
- Alice创建一个PAI数据协议交易，有两个输出：
  - 发送给Bob的OP\_RETURN交易：此输出包含OP\_RETURN操作码字段中加密数据的哈希。

- b. 付款给供应者（可选）：此输出根据各方之间的离线协议补偿存储供应者托管种子文件的服务。
9. Bob接收OP\_RETURN交易并检索数据哈希。
10. Bob利用数据哈希从存储供应者处取得种子文件。
11. Bob从PAI数据协议的BitTorrent网络处下载数据。
12. Bob用自己的私钥解密数据。

—

基于区块链的文件存储系统主要有两类 [3]：

1. 存储证明 / 容量证明（如 Permacoin, Spacemint）：单个节点没有足够空间存储完整数据集时，通过证明部分子集的持有真实性与完整性来生成新的区块
2. 维持一条区块链用以充当存储提供者与存储购买者之间的中间代理人（例如 Storj, Filecoin (IPFS)）

这些基于区块链的文件存储解决方案普遍修改了协议的共识机制；而PAI币并没有。例如，它们用到了以下共识机制：

- 存储证明（如 Permacoin, Spacemint, Burstcoin, Chia）：证明验证者保留了一定量的存储空间。
- 复制证明（如 Filecoin/IPFS [4]）：证明验证者在唯一的物理存储设备上复制了部分数据。
- 时空证明（Filecoin/IPFS）：证明部分数据被存储了一段时间。

在大多数其他基于区块链的数据存储解决方案中，一个节点供应存储的动机是区块奖励。节点可以供应的存储或带宽越多，它挖到下一个区块并获得区块奖励的概率就越高。这会导致节点之间的存储/带宽竞争，就像工作量证明（Proof of Work）中的哈希算力竞争一样，并且可能逐渐淘汰只具有小存储容量的节点。

相比之下，在PAI数据协议中，存储供应者通过数据提交者的交易被支付（可选）。如果与数据提交者达成了脱链协议，那么没有大量可用磁盘空间的单个存储供应者仍可以直接通过中继数据受益。这有助于降低存储供应者的进入门槛，从而鼓励更多的网络参与。无论数据本身是否继续由供应者提供，作为数据保管链的不可变记录，授予和撤销操作是永久嵌入区块链中的。

对于存储供应者的可选支付为分发费用提供了更大的灵活性。例如，供应者可以根据其可访问的空间，带宽，冗余级别和保留策略向存储供应者免费支付不同费用。或者，供应者可以基于中继的数据量向存储供应者付费。如果数据传输速度很慢，从接收者的角度来看，提交者可能会提高他们愿意支付的费用，从而鼓励更多的供应者参与并提高速度。

一旦数据接收者取得了数据，基于数据发送者与数据接收者之间的脱链协议，数据发送者可以通过撤销交易要求存储提供者（可能有多个）删除他们的本地备份。这可以极大地提高系统效率，因为存储供应者们可以复用他们有限的存储空间以支持不同的数据传输任务。请注意，在任何情况下数据都是用接收者的公钥加密的，因此对存储供应者来说是不可读的。

- [1] Alex Waters, Mark Harvilla, Patrick Gerzanics, PDP 2, "PAI Data Storage and Sharing," 2018, <https://github.com/projectpai/pdps/blob/master/pdp-0002.mediawiki>
- [2] Project PAI, "Project PAI Technical Whitepaper," <https://projectpai.com/assets/files/whitepaper/whitepaper-tech.pdf>, 2018
- [3] Paulus Nicolas Meessen, "Long term data storage using peer-to-peer technology," Radboud University, 2017
- [4] Protocol Labs, "Filecoin: A Decentralized Storage Network," <https://filecoin.io/filecoin.pdf>, 2017



