PAIデータ

プロジェクトPAIデータ・プロトコルの概要

著者: Jincheng Du[1]
Dan Fang博士[2]
Mark Harvilla博士[3]

概要

プロジェクトPAIデータプロトコル（「PAIデータ」）は、プロジェクトPAIブロックチェーンプ
ロトコルを拡張して、任意のデータへのアクセスを保護し、供給する方法を含むものであります。このレポートでは、PAIコイン開発提案（PDP）2 [1]について、PAIデータがサポートする2つの重要なトランザクションタイプを定義します。「ストレージトランザクション」はデータ保存と所有権の証明を可能にし、そして「共用トランザクション」は指定された受信者へのデータアクセスの付与と取
り消しを可能にします。ブロックチェーンベースのファイルストレージ・システムに対するPAIデータの比較分
析も示されています。

[1] ObEN, Inc.のブロックチェーン研究者
[2] ObEN, Inc.のブロックチェーン研究者
[3] ObEN, Inc.のチーフエンジニア

序論

プロジェクトPAIデータ・プロトコル（「PAIデータ」）は、プロジェクトPAIブロックチェーン・プロトコルを拡張して、任意のデータへのアクセスを保護し、供給する方法を含むものであります。これは、カスタムのOP_RETURNデータ・プロトコルと楕円暗号化（elliptical encryption）を、データストア（例：分散型ストレージ用のトレントノードのセグメント化されたネットワーク、または集中ストレージ用の独自のデータストア）と組み合わせて使うことによって実現できます。[1].

PAIデータのバックグラウンド

PAIデータは、持続可能でヒューマニスティックな情報経済を構築するためのプロジェクトPAIの取り組みの核心です[2]。 PAIデータを使用すると、ユーザーはプロジェクトPAIプロトコルを使用して自分のデータを保護し、データに許可を付けることができます。現在開発中のアプリケーションである「PAI Pass」は、PAIデータを活用する潜在的なユースケースの実例を提供します。 「PAI Pass」は統合されたSingle Sign onサービスおよびデータ管理アプリケーションです。「PAI Pass」プラットフォームは、PAIデータのような「PAI Pass」プラットフォームとは独立したユーザが選択する第三者データストアプロトコルを使用して、ユーザが自分のデータ（例えば、名前、年齢など）を入力して保護することを可能にします。

他のユースケース

PAIデータは知的財産を保護するための伝統的な方法（例えば、著作権登録）に代わるものではありません。しかしPAIデータは、著作権の証拠を維持しながらコンテンツを商品化したい知的財産を保有している開発者にとって非常に有用です。後述のように、PAIデータは第三者によって検証可能な不変のタイムスタンプを使用してデータを格納するための簡単な方法を提供します。
その結果、そのようなデータの作者または所有者のIDとともに、独自のデータ（企業秘密および/またはその他の知的財産）を保護するためにPAIデータを使用することは、タイムスタンプに反映され、その時またはその前に強い証拠を残すようになります。

（1）作品が生まれました。 （2）特定された著者がそのようなデータを作成したか、少なくとも知っていました。この機能は、認証システム（例えば、「PAI Pass」）によって強化されている場合に特に有用です。

技術的な説明

PAIデータプロトコルの主な要素は次のとおりです：

- プロジェクトPAIブロックチェーン
- OP_RETURN op code
- 楕円暗号化（Elliptical Encryption）
- 提出者 + プロバイダー + 受信者
- データストア (*例：* トレントノードのセグメント化されたネットワークなど)

トランザクション・タイプ

ストレージ・トランザクション

ストレージ・トランザクションは、PAIブロックチェーンを通してデータを保存するために使用されます。所有権を主張する当事者に関する情報が含まれている場合、または「PAI Pass」などのプラットフォームと組み合わせて使用される場合は、保存データの所有権を主張するために使用できます。 ストレージ・トランザクションは、ストレージのプロバイダーを介して検索するためのデータのハッシュされた識別子を含むOP_RETURN出力を用いて、トランザクションを自分にブロードキャストすることによって作成されます。あるいは、例えば、OP_RETURNは独自のデータストア内のデータへのマッピングに使用されるデータ自体のハッシュ、または他の識別子を含むことができます。

共有トランザクション

共有トランザクションは、PAIブロックチェーンを介して送信者と受信者の間でデータを共有するために使用されます。共有トランザクションは、ストレージのプロバイダーを介して検索するためのデータのハッシュされた識別子を含むOP_RETURN出力を使用して、トランザクションを対象受信者にブロードキャストすることによって作成されます。

ユースケース

このセクションではユーザーの必要性に応じてPAIコイン・プロトコルがどのように使われるのかについて概説します。

次の項目をしたい場合	***これを使わなければなりません***
データ（デジタル資産、知的財産など）の所有権を保存および/または主張する。	PAIストレージ・トランザクション
受信者に対するデータの許可	PAI共有トランザクション（PDP 2 [1] による、「grant」操作IDを含む）

受信者のデータ使用許可を取り消す	PAI共有トランザクション（PDP 2 [1]による、「取り消し」操作IDを含む）

例：ストレージトランザクション

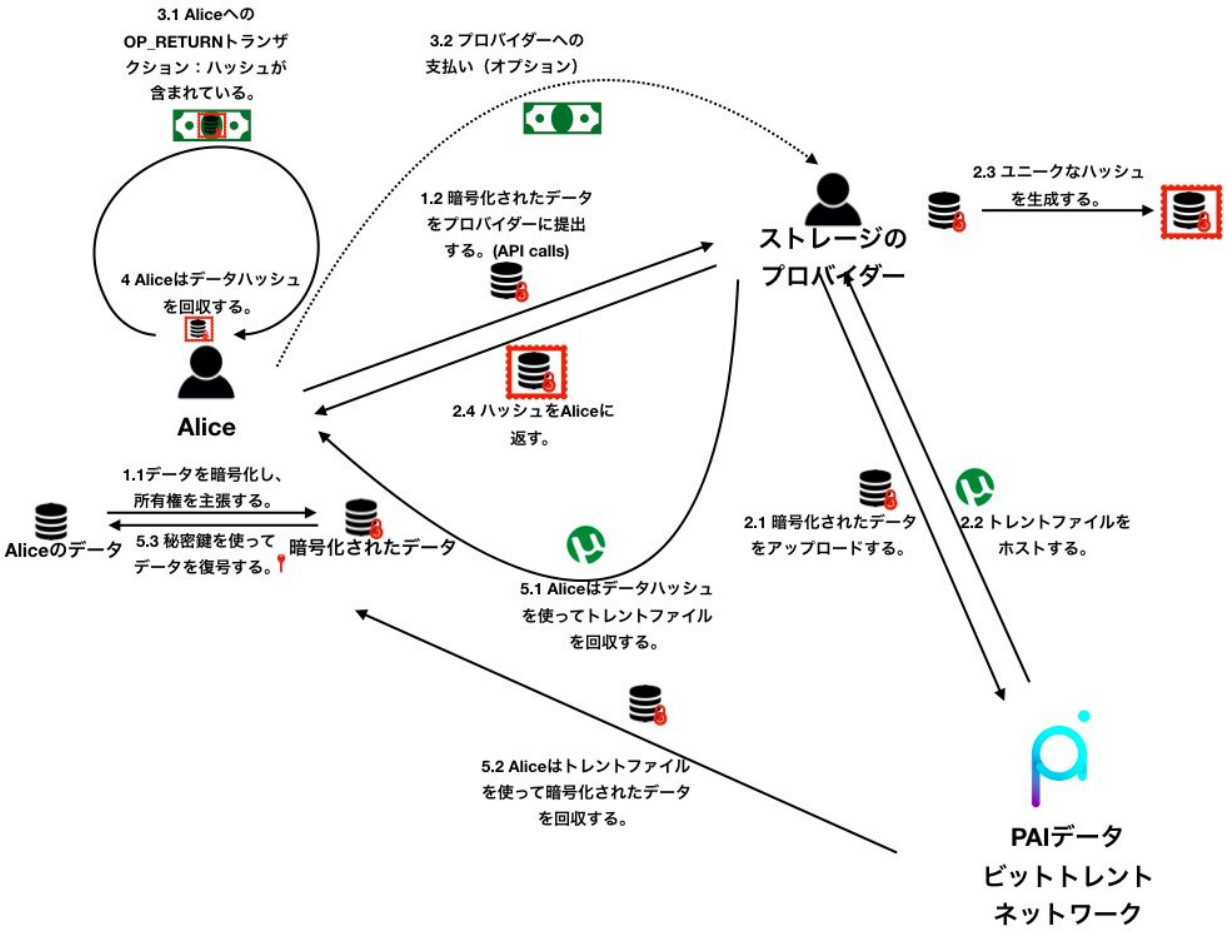

図 1. ストレージトランザクションのワークフロー

図１に示すように、当事者（例えば、プロバイダーAlice）は、以下の方法で、PAIデータトランザクションを通してデータを格納し、格納されたデータの所有権を主張することができます。

1. Aliceは所有権または著作権の主張とともにデータを自分の公開鍵で暗号化します。この暗号化されたデータは、対応する秘密鍵を持つAliceによってのみ復号できます。
2. Aliceは、ストレージのプロバイダーを選択し、プロトコルによって指定された一連の標準APIコール（例：「プロバイダーAPI」）を通して、暗号化されたデータをプロバイダーに提出します。ストレージのプロバイダーは：
    a. データをPAIデータ・ビットトレント・ネットワークにアップロードします。
    b. 対応するトレントファイルをホストします。
    c. データに関連付けられているユニークなハッシュを生成します。

d. ハッシュをAliceに返します。

3. Aliceは、2つの出力を持つPAIデータトランザクションを作成します：
    a. AliceへのOP_RETURNトランザクション：この出力には、OP_RETURN opcode field内の暗号化されたデータのハッシュが含まれています。
    b. プロバイダーへの支払い（オプション）：この出力は、すべての当事者間のオフチェーン合意に基づいて、トレントファイルをホストしているストレージのプロバイダーを補償します。
4. AliceはOP_RETURNトランザクションを受け取り、データハッシュを回収します。
5. Aliceが所有権の主張をするか、もしくはデータを検索することを望む場合、Aliceは、（１）データハッシュを使用してストレージのプロバイダーからトレントファイルを検索する。（2）PAIデータ・ビットトレント・ネットワークからデータをダウンロードする。（３）自分の秘密鍵を使ってデータを復号する。

例：共有トランザクション

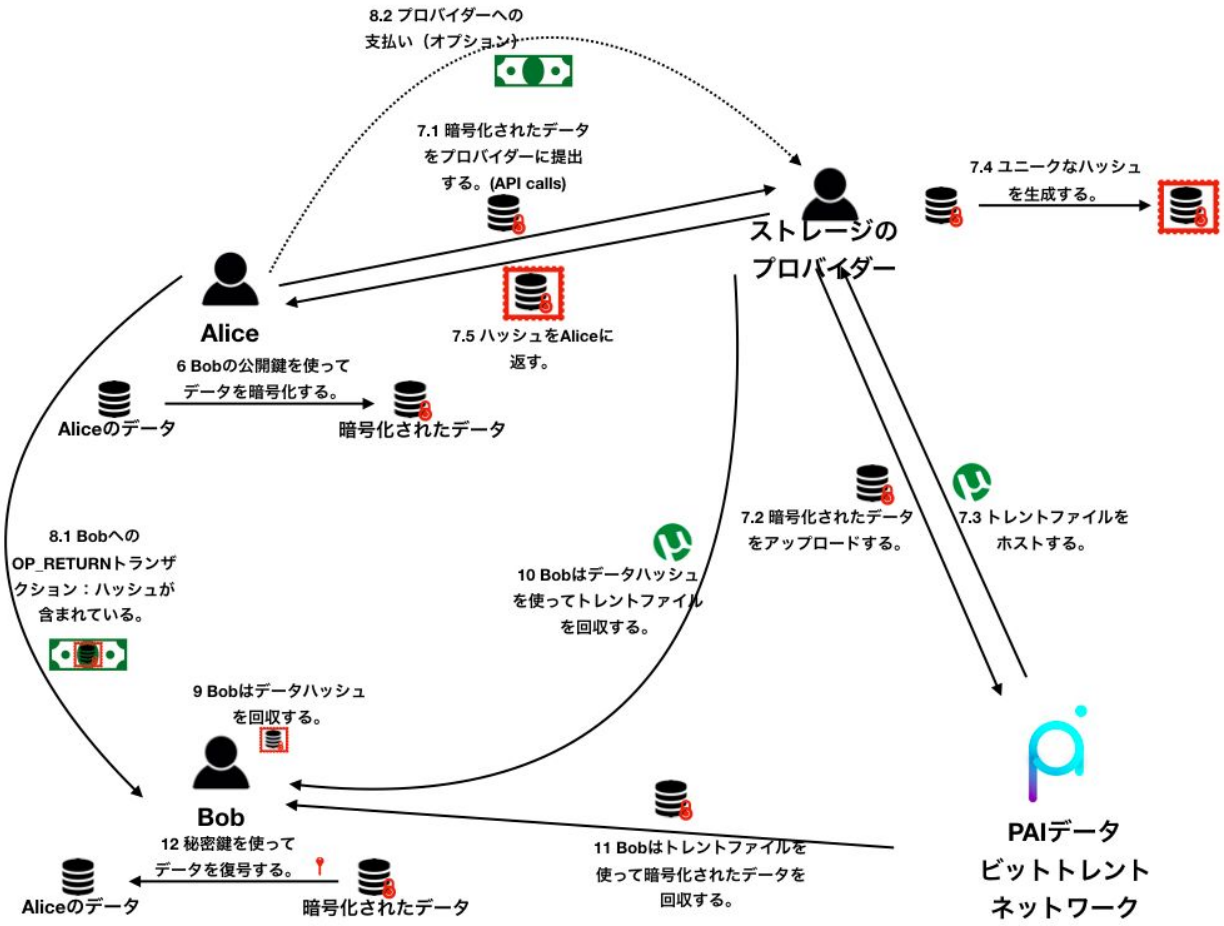

図２. ストレージトランザクションのワークフロー

図２に示すように、２つの当事者（例：Alice、提出者、Bob、受信者）は、以下の方法で、PAIデータトランザクションを通してデータを共有することができます：

6. AliceはBobの公開鍵でデータを暗号化します。この暗号化されたデータは、対応する秘密鍵を持つBobによってのみ復号できます。
7. Aliceは、ストレージプロバイダーを選択し、プロトコルによって指定された一連の標準APIコール（すなわち、「プロバイダーAPI」）を通して、暗号化されたデータをプロバイダーに提出します。ストレージプロバイダーは：
    a. データをPAIデータ・ビットトレント・ネットワークにアップロードします。
    b. 対応するトレントファイルをホストします。
    c. データに関連付けられているユニークなハッシュを生成します。
    d. ハッシュをAliceに返します。
8. Aliceは、2つの出力を持つPAIデータトランザクションを作成します：
    a. BobへのOP_RETURNトランザクション：この出力には、OP_RETURN opcode field内の暗号化されたデータのハッシュが含まれています。
    b. プロバイダーへの支払い（オプション）：この出力は、すべての当事者間のオフチェーン合意に基づいて、トレントファイルをホストしているストレージのプロバイダーを補償します。
9. BobはOP_RETURNトランザクションを受け取り、データハッシュを回収します。
10. Bobは、データハッシュを使用してストレージプロバイダーからトレントファイルを回収します。
11. Bobは、PAIデータ・ビットトレント・ネットワークからデータをダウンロードします。
12. Bobは、秘密鍵を使ってデータを復号します。

比較 — 他のブロックチェーンベースのファイルストレージ・システム

ブロックチェーンベースのファイルストレージ・システムには、主に2つの種類があります[3]：

1. Proof of Storage / Capacity (例： Permacoin, Spacemint):単一ピアが格納するにはデータセットが大きすぎるため、データセットの一部のサブセットの所有および完全性を証明することによってブロックが採掘できます。
2. ストレージの提供者とストレージの購入者との間を仲介するためにブロックチェーンを採掘します・（例：Storj, Filecoin (IPFS)

これらの代替のブロックチェーンベースのファイルストレージ・システムは通常、プロトコルの合意メカニズムを変更しますが、PAIコインはしません。例えば、以下の合意メカニズムが他のソリューションで使用されています。

- Proof of Storage (例： Permacoin, Spacemint, Burstcoin, Chia): 証明者が一定量のスペースを確保したことを証明する。
- Proof of Replication (例： Filecoin/IPFS [4]): いくつかのデータが独自の専用の物理ストレージに複製されていることを証明します。
- Proof of Spacetime (例：Filecoin/IPFS): ある期間を通してデータが保存されていたことを証明します。

PAIデータの利点

ストレージプロバイダーの参入障壁の低下

他のほとんどのブロックチェーンベースのデータストレージソリューションでは、ノードがストレージを提供する主な動機はブロック報酬です。ノードが提供できるストレージまたは帯域幅が多いほど、次のブロックを採掘してブロックの報酬を受け取る可能性が高くなります。これは、「Proof of Work」でのハッシュ力の競合と同じように、ノード間のストレージ/帯域幅の競合につながり、ストレージ容量がほとんどないノードは徐々に除外される可能性があります。

対照的に、PAIデータではストレージプロバイダーはオプションでデータ送信者からトランザクションを通じて支払いを受けます。大量の利用可能なディスク容量のない個々のストレージプロバイダーは、データ提出者とオフチェーンの合意が得られれば、データを中継することで直接利益を得ることができます。これは、ストレージプロバイダーの参入障壁を低下し、ネットワークへの参加を促進するのに役立ちます。付与および取り消しの操作はブロックチェーンに永続的に埋め込まれ、データ自体がプロバイダーによって提供され続けているかどうかにかかわらず、データの保護チェーンの不変の記録として機能します。

支払いシステム構築の融通性が向上

ストレージプロバイダーへのオプショナル支払いは、料金の分配においてより柔軟に対応することができます。たとえば、提出者はアクセス可能なスペース、帯域幅、冗長レベル、および保存ポリシーに基づいて、ストレージプロバイダーにさまざまな料金を自由に支払うことができます。あるいは、提出者は中継されたデータの量に基づいてストレージプロバイダーに支払うことができます。受信者から見てデータ送信が遅い場合、提出者は支払う意思のある料金を引き上げることにより、プロバイダーの参加を促進し、速度を上げることができます。

データ転送効率の向上

受信者がデータを取得すると、送信者と受信者の間のオフチェーン合意に応じて、送信者はストレージプロバイダーに取り消し呼び出しを介してローカルコピーを削除するよう依頼することができます。これによりシステム効率が大幅に向上し、データプロバイダーは限られたストレージスペースをさまざまなデータ送信タスクに再利用できます。いずれにせよ、データは受信者の公開鍵で暗号化されているため、プロバイダーは読み取れません。

参考

[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