2T-07

受益者のプライバシー保護と寄付者への透明性を両立する使途確約型の寄付プロトコル

平田 駿輔　　川原 圭博
東京大学

1 はじめに

寄付の透明性を担保する手段として、パブリックブロックチェーン上での暗号資産による寄付が注目されている。従来の現金寄付と比較して資金の流れが追跡可能になる一方、ブロックチェーンの完全な透明性は受益者のアドレスや消費行動を全世界に公開することとなり、プライバシー侵害のリスクを孕んでいる。特に、生活困窮者支援などの文脈では、支援を受けている事実自体がセンシティブな情報となりうる。そこで本稿では、寄付に関わる全ステークホルダー（寄付者、移転者、受益者、事業者）間のトランザクション詳細を秘匿しつつ、寄付者に対してのみ資金の追跡可能性を提供するプロトコルを提案する。本手法の特長は、ゼロ知識証明を用いた秘匿送金回路において、強制的に寄付者に取引内容の監査権限を付与する制約を設けた点にある。これにより、第三者に対するユーザのプライバシー保護と、資金拠出者である寄付者への透明性（説明責任）の両立を実現する。

2 Purpose Bound Money

本提案の基礎となる Purpose Bound Money (PBM) [1] とは、原資となる暗号資産を担保に発行される使途限定型のトークンであり、許可されたアドレス（事業者）のみがトークンと引換えに原資を出金（償還）できるスマートコントラクトによって管理される。一般的な暗号資産が無期限に循環するのに対し、PBM は以下の明確なライフサイクルを持つ。

1. **Mint（発行）:** 寄付者が原資（ERC-20 トークン）をロックし、ホワイトリストを設定して PBM トークンを発行する。
2. **Transfer（移転）:** 移転者や受益者間でトークンが流通する。
3. **Unwrap（償還）:** サービスの対価として PBM トークンを受け取った事業者は、自身がホワイトリストに含まれる場合に限り、トークンと引換えに原資を受け取る。引換えをもってトークンは消滅する。

本稿では、このライフサイクルを活用し、次章で述べるプライバシー保護手法を適用する。

3 提案手法

本章では、受益者のプライバシー保護と寄付者に対する透明性を両立する Purpose Bound Money トークンの移転プロトコルを提案する。本システムは、UTXO (Unspent Transaction Output) モデルを採用したゼロ知識証明回路により構成される。

3.1 強制的な寄付者用閲覧鍵の付与

本提案の新規性は、秘匿送金プロトコルの技術的基盤を活用しつつ、Purpose Bound Money に寄付者用の閲覧鍵をゼロ知識証明回路の制約として組み込むことで、寄付者にだけ寄付金（PBM トークン）の行方の透明性を技術的に担保する点である。

秘匿送金プロトコルである Zcash [2] や Aztec [3] は、暗号資産の取引を当事者間で暗号化することで、第三者から取引の当事者や金額を秘匿して当事者のプライバシーを保護する。これらは「閲覧鍵 (Viewing Key)」を提供し、所有者が自身の意思で取引内容を特定の第三者に開示する機能を備えている。しかし、これはユーザ自身のプライバシー保護には有効だが、寄付金のような「資金提供者に対す

Purpose Bound Money Protocol Achieving Both Beneficiary Privacy and Donor Transparency
Shunsuke HIRATA, and Yoshihiro KAWAHARA
The University of Tokyo

る説明責任」が求められるケースにおいては、ユーザの同意なしには寄付者が取引を監査できないという課題がある。本提案は、発行されてから償還されて消滅する PBM のライフサイクルに着目して、PBM トークンを発行した寄付者にだけ監査権限を与える仕組によってこの課題を克服する。

3.2 データ構造

本システムでは資産をノート $N = (v, id, h_{\text{owner}}, h_{\text{donor}}, r)$ と定義する。ここで v は PBM トークンの量、id はトークン ID、h_{owner} は現在の所有者の公開鍵ハッシュ、h_{donor} は寄付者の公開鍵ハッシュ、r はコミットメントと Nullifier を生成するための乱数 (Salt) である。ノートのハッシュ値がコミットメントとして Merkle Tree で管理される。

3.3 ゼロ知識証明回路の構成

提案するゼロ知識証明回路は、所有権の移転を検証すると同時に、取引内容を寄付者の公開鍵に対して暗号化したことを証明する。回路への主な入力と制約は以下の通りである。

3.3.1 トークン情報の一貫性とトークン量の保存

回路は、PBM の整合性を保つため、入出力間で以下の不変条件を課す。

$$id^{\text{in}} = id^{\text{out}}, \quad h^{\text{in}}_{\text{donor}} = h^{\text{out}}_{\text{donor}}, \quad \sum v_{\text{in}} = \sum v_{\text{out}}$$

これにより、PBM トークンが移転されても寄付者情報は引き継がれ、その資金の不正利用や改竄は不可能となる。

3.3.2 消費するノートの所有権と未消費の証明

回路は、トランザクション作成者 (sender) がこれから消費される入力ノート N^{in} の正当な所有者であること、およびそのノートが正当に台帳上に存在することを検証する。まず、sender の秘密鍵 sk_{sender} をプライベート入力として受け取り、公開鍵ハッシュ h_{sender} を導出し、これが N^{in} の所有者公開鍵ハッシュ $h^{\text{in}}_{\text{owner}}$ と一致すること、すなわち、sender は正当な秘密鍵を持っていることを検証する。また、Merkle Tree のルートと Merkle Path をプライベート入力として受け取り、N^{in} が正当に台帳上に存在することを検証する。

一般的な秘匿送金プロトコルでは、二重支払い防止のために、UTXO のノートが消費されるたびに対応する Nullifier がノートとトランザクション作成者の秘密鍵から導出され、Nullifier が使用済みフラグとして管理される。ここでは、Nullifier ν を $\nu = \text{Hash}(\text{Hash}(N^{\text{in}}), sk_{\text{sender}})$ で計算し公開する。この Nullifier ν の導出計算の正当性はゼロ知識証明回路で担保されるが、導出された Nullifier が使用済みかどうかの検証はゼロ知識証明回路の外（スマートコントラクトなど）で実行される。

3.3.3 寄付者の閲覧鍵の保証

本ゼロ知識証明回路は、寄付者が暗号化されたノートを確実に復号し、監査できるよう、寄付者の公開鍵を用いて正当に暗号化が行われたことを保証する。

具体的には、回路のプライベート入力（トランザクション作成者の一時秘密鍵 r、ノート暗号化用共通鍵 K）とパブリック入力（一時公開鍵 R、暗号化された共通鍵 $EncK_{\text{donor}}$）に対し、以下の整合性を検証する。

$$R = rG$$
$$S_{\text{donor}} = \text{ECDH}(r, PK_{\text{donor}})$$
$$EncK_{\text{donor}} = K + \text{Hash}(S_{\text{donor}})$$

ここで G は楕円曲線の生成元である。この制約により、寄付者の公開鍵によって正当に鍵共有および暗号化が行われたことが担保され、寄付者は自身の秘密鍵で K を復元できる。

謝辞 本研究は、JST 次世代研究者挑戦的研究プログラム JPMJSP2108 の支援を受けたものである。

参考文献

[1] Orchid-Dev, Victor Liew et al., ”ERC-7291: Purpose bound money,” Ethereum Improvement Proposals, 2023.

[2] Daira-Emma Hopwood et al, ”Zcash Protocol Specification”, 2025.

[3] Zachary J. Williamson, ”The AZTEC Protocol”, 2018.