

EC サイトにおける JPYC を用いた分散型エスクロー決済フローの設計と実装

電子商取引研究室 呉竹 權人

1. 序論

1.1 背景

EC 取引では、支払いと商品引き渡しの非同時性により、取引の信頼性確保が重要な課題となっている。従来はプラットフォーム運営者が第三者預託(エスクロー)を担うことで取引の安全性を確保してきたが、手数料の高さや利用条件、国・事業規模による制約、運営者への依存といった問題がある。

近年、分散型台帳技術とスマートコントラクトの発展により、中央管理者に依存しない決済・送金構造が注目されている。特に、円と価値が連動するステーブルコインである JPYC は、為替変動の影響を受けず、EC 決済への応用が期待されている。

1.2 問題点

既存の暗号資産決済では、宛先アドレスや金額の手入力による誤送金が発生しやすく、また PC ブラウザウォレットを前提とした方式では、マルウェアやフィッシングによる被害のリスクがある。

さらに、スマートフォンにウォレットを保有する利用者が多い一方で、PC で商品を購入し、スマートフォンで安全に決済するフローは十分に整理されていない。加えて、スマートコントラクトを用いた決済におけるガス代や処理時間が EC 運用に与える影響も明確に整理されていない。

1.3 提案手法

本研究では、JPYC を用いた分散型エスクロー決済フローを設計・実装する。PC 上の EC 購入画面で生成された支払い要求を QR コードとして提示し、スマートフォンのウォレットで署名・送信することで、秘密鍵を PC に露出させない安全な決済を実現する。

また、スマートコントラクトを用いて資金を一時的に預託し、取引成立時に送金、期限切れ時に返金を行う分散型エスクローモデルを構築する。

1.4 実験・評価内容

提案方式と従来方式を以下の観点から比較評価する。

- 操作ステップ数・手入力項目数の測定
- 誤送金防止率・注文紐付け成功率の算出
- トランザクションのガス代・処理時間の計測

2. 研究内容

2.1 分散型エスクローモデル

提案するエスクローは、INIT(初期状態) → FUNDED(入金済) → COMPLETED/REFUNDED(完了/返金) の状態遷移を持つ。購入者が JPYC をスマートコントラクトに預

託し、取引成立時に売り手へ送金、問題発生時には返金を行う。

2.2 決済フロー設計

PC 上の EC 購入画面で QR コードを表示し、スマートフォンのウォレットで署名・送金する方式により、秘密鍵を PC に露出させない安全な決済を実現する。

2.3 従来方式との比較

手動送金方式、PC ブラウザウォレット方式、提案方式を操作負担・安全性・コストの観点から比較する。

3. 今後の計画

本研究の実施スケジュールを表 1 に示す。

表 1 研究スケジュール

時期	内容
4 月前半	要件分析・関連研究調査
4 月後半	決済フローおよび仕様設計
5 月前半	スマートコントラクト実装
5 月後半	EC 側プロトタイプ実装
6 月前半	テスト・予備実験
6 月後半	実証実験・評価
7 月	論文執筆・まとめ

3.1 必要機材

- イーサリアム (テスト用の JPYC 等を受け取るため、前期中に準備)

参考文献

- 1) JPY Coin. Jpy coin (jpyc) white paper, 1 2021. 2025 年 1 月 6 日閲覧。