

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

近畿大学 情報学部 情報学科 呉竹 横人

1. 序論

EC サイトで買い物をする時、お金を払ってから商品が届くまでに時間がかかる。この間にトラブルが起きる可能性がある。今まで運営会社がお金を預かる方法が使われてきたが、手数料が高く、運営会社に頼るしかない問題がある^{*1)}。本研究では、日本円と同じ価値を持つ JPYC という暗号資産を使い、運営会社に頼らない安全な支払い方法を作ることを目的とする。PC で買い物をして、スマートフォンで安全に支払いができる仕組みを作る。

2. 提案方式

2.1 お金を預かる仕組み

買い手は JPYC を一時的に預ける。注文番号で取引を区別し、「最初」「預けた」「渡した」「返した」の 4 つの状態で管理する。商品が無事届いたら売り手にお金を渡す。期限を過ぎたら買い手にお金を返す。この仕組みで、お金を預ったのに商品が届かない時でも、ちゃんとお金が戻ってくる。

2.2 支払いの流れ

PC の画面に、注文番号・金額・売り手の情報が入った QR コードを表示する。買い手はスマートフォンで QR コードを読み取り、送り先と金額を確認してから送金する。大事な秘密の情報(秘密鍵)はスマートフォンの中だけに保管し、PC には入力しない。手で入力する項目を減らすことで、アドレスや金額を間違えて入力するミスを防ぐ。

3. 評価方法

この研究では、「コスト」と「資金ロック率」の 2 つを測る。比べる方法は、(a) 普通の送金と (b) 提案する方法の 2 つとする。

3.1 コスト

1 回の注文でかかる手数料を円で計算して比べる。普通の送金は送金 1 回分の手数料とする。提案する方法は、お金を預ける時と渡す時の 2 回分の手数料を合計する。それぞれの手数料を記録して、その時の円の価値で計算する。ネットワークの混み具合で手数料が変わるため、真ん中の値と高い方の値を示す。

3.2 資金ロック率

お金を預けた注文の中で、期限を過ぎてもお金が渡されず、返ってもこない割合を資金ロック率と呼ぶ。もしお金が動かなくなった時は、注文番号、状態、記録、理由を残して原因を調べる。資金ロック率が 0 に近ければ、この仕組みがちゃんと動くことを示せる。

4. 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	作業内容
4月	要件分析・関連研究調査
5月	決済フロー・仕様設計
6月	スマートコントラクト実装
7月	EC 側プロトタイプ実装
8月	テスト・予備実験
9月	実証実験・評価
10月-11月	論文執筆・まとめ

4.1 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)

5. 結論

本研究では、JPYC を使った安全な支払い方法と、PC で QR コードを表示してスマートフォンで支払う流れを提案する。評価は「コスト」と「資金ロック率」の 2 つに絞り、実際に使えるかどうかと信頼できるかを数字で示す。今後は実際に作って動かし、手数料がどのくらいかかるか、お金が動かなくなる条件は何かを整理する。

参考文献

- *1) JPYC. Jpycoin(jpyc) whitepaper, 1 2021. 2025 年 1 月 20 日閲覧。