

トークン取引と連携可能な電子商取引プラットフォームの検討 —購入者の支払いの利便性を向上する場合—

A Study on Token Payable E-Commerce Platform: In case of Increase in Convenience for Buyers

稲垣達大[†], 森山真光^{†‡}

Tatsuhiko Inagaki[†], and Masamitsu Moriyama^{†‡}

[†]近畿大学 総合理工学研究科

[‡]近畿大学 情報学研究所

[†]Graduate School of Science and Engineering, Kindai Univ.

[‡]Cyber Informatics Research Institute, Kindai Univ.

要旨

自治体ではデジタル地域通貨の活用が進んでいる。デジタル地域通貨には、ブロックチェーンの電子的な証票であるトークンが用いられることが多い。デジタル地域通貨は商品や体験を対面取引するため、電子的財布であるウォレットアプリケーションを開発する。本稿では、オンライン注文と店舗受け取りを実現するためにトークン取引を電子商取引プラットフォームに連携することを検討する。特に購入者の支払いの利便性について言及する。

1. はじめに

自治体や地域コミュニティではデジタル地域通貨の活用が進んでいる [1]。デジタル地域通貨には、ブロックチェーンの電子的な証票であるトークンを支払いに用いることが多い。デジタル地域通貨は商品（モノ）や体験（コト）を対面取引するため、電子的財布であるウォレットアプリケーションを用いてトークン支払いする。一方、実店舗では販売経路や顧客接点を増やすために、電子商取引プラットフォームを用いたオンライン注文と店舗受け取り (BOPIS: Buy-Online-Pickup-in-Store) が増加している [2]。これらのことから、本稿では安全な BOPIS の実現を目的としてトークン支払いする電子商取引プラットフォームについて検討する。特に、購入者の利便性を向上させるために、トークン支払いで通常用いられるウォレットに加えて、Web 拡張機能を用いたトークン支払いについて検討する。実際に Symbol ブロックチェーンのテストネットを用いて、トークン支払いする電子商取引プラットフォームのプロトタイプを試作し、ウォレットによるトークン支払いと Web 拡張機能によるトークン支払いを比較する。

2. トークン支払いする電子商取引プラットフォーム

2.1. トークン支払いに用いるブロックチェーンの検討

電子商取引プラットフォームのプロトタイプに用いるブロックチェーンは、3つのブロックチェーン Bitcoin と Ethereum と Symbol を検討した。Bitcoin では、トークン作成はカレードコインのように取引情報に独自に情報を書き込む必要がある。Ethereum では、契約を自動化する仕組みであるスマートコントラクトを用いることでトークンをプログラムで記述することができる。しかし、スマートコントラクトの不具合による資金流出が問題となっている [3]。Symbol では、モザイクと呼ばれるトークン作成機能をビルドイン機能として有している。これらのことから、プロトタイプに用いるブロックチェーンにはトークン作成機能をビルドイン機能として有している Symbol¹を用いることにする。

2.2. 電子商取引プラットフォームのプロトタイプ

電子商取引プラットフォームには、ショッピングモール型・クラウド型・オープンソース型などがある。トークン支払いする電子商取引プラットフォームを構築する場合、ショッピングモール型はプラットフォームの対応を待つ必要がある。クラウド型やオープンソース型は開発者向けアプリケーションやプラグインで実装することができる。トークン支払いの対応は、クラウド型の開発者向けアプリケーションやオープンソース型のプラグインでの実装を想定している。

その前段階として、トークン支払いする電子商取引プラットフォームについて、購入者が商品を選択しトークン支払いをするところまでのプロセスをプロトタイプとして試作する。商品の選択する画面を

¹<https://symbol-community.com/>

P_{select} 、ショッピングカートの画面を P_{cart} とする。商品を購入するために、ウォレットによりトークン支払いする画面を $P_{(buy|wallet)}$ 、Web 拡張機能によりトークン支払いする画面を $P_{(buy|webext)}$ とする。また、画面 A から画面 B に x というラベルのボタンをクリックして遷移するプロセスを $A \xrightarrow{x} B$ と定義する。商品を選択しショッピングカートに入れるプロセス $P_{select} \xrightarrow{items} P_{cart}$ は通常の電子商取引プラットフォームと同様である。ショッピングカートの画面から商品を購入するプロセスは、ウォレットによるトークン支払いのプロセス $P_{cart} \xrightarrow{wallet} P_{(buy|wallet)}$ と Web 拡張機能によるトークン支払いのプロセス $P_{cart} \xrightarrow{webext} P_{(buy|webext)}$ の2通りがある。 $P_{cart} \xrightarrow{wallet} P_{(buy|wallet)}$ は $P_{(buy|wallet)}$ にトークンの支払い先と量と取引のメッセージを情報とする QR コードを表示する。この QR コードをウォレットが読み取り、ウォレットからトークン支払いを実行する。 $P_{cart} \xrightarrow{webext} P_{(buy|webext)}$ は取引情報であるトランザクションを署名する Web 拡張機能をインストールして、その Web 拡張機能によりトランザクションを電子署名し、電子商取引プラットフォームからトークン支払いする。

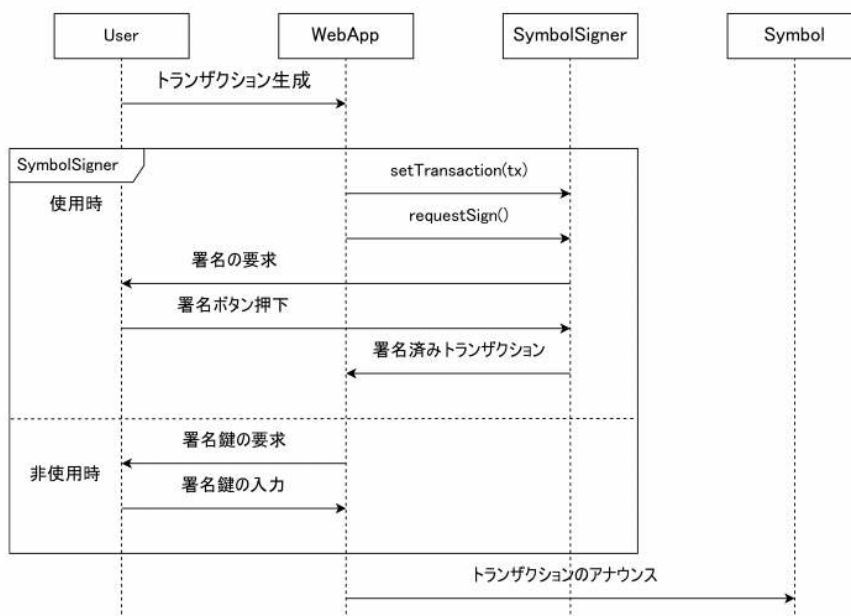


図 1: Web 拡張機能によるトークン支払いのシーケンス図

図 1 に Web 拡張機能によるトークン支払いのシーケンス図を示す。User が購入者、WebApp が電子商取引プラットフォーム、SymbolSigner が Web 拡張機能、Symbol がブロックチェーンである。User が商品購入するためのトークン支払いのトランザクションを WebApp で生成する。WebApp がトークン支払いを実行するためには、User の電子署名が必要となる。SymbolSigner は User の秘密鍵を保有し、WebApp からは秘密鍵を参照できないようにして電子署名する API である requestSign() を公開している。電子署名の際には、User の承認を必要とする。このようにすることで、WebApp は User の秘密鍵を知ることなく、User のトランザクションを電子署名することができる。加えて、WebApp は、電子署名されたトランザクションを Symbol に送信すると同時に、ショッピングカートの購入情報を WebApp に送信することができる。

3. 結果と考察

トークン支払いする電子商取引プラットフォームのプロトタイプを Web アプリケーションとして試作した。ブロックチェーンには Symbol のテストネット²を用い、トークン支払いや受け取りをするウォレットには Symbol Desktop Wallet (v1.0.12)³を用いた。Symbol のトランザクションを電子署名する

²https://symbolnodes.org/nodes_testnet/

³<https://github.com/symbol/desktop-wallet/releases>

Web 拡張機能には筆者らが開発している SSS Extension⁴を用いた。

図 2 と図 3 にそれぞれの試作した商品選択画面 P_{select} とショッピングカート画面 P_{cart} を示す。ここでは、商品 2 と商品 6 を選択して P_{select} の右上の購入ボタンを押すことで、 $P_{select} \xrightarrow{\text{購入}} P_{cart}$ に遷移している。ショッピングカート画面の P_{cart} には、Web 拡張機能である SSS Extension でトークン支払いする SSS 決済ボタンと、Symbol ウォレットでトークン支払いする QR 決済ボタンがある。

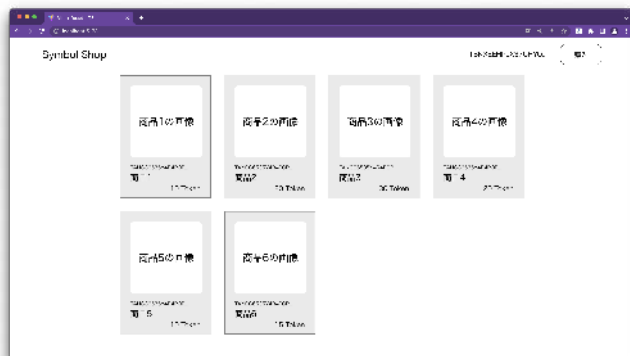


図 2: 商品選択画面 P_{select}

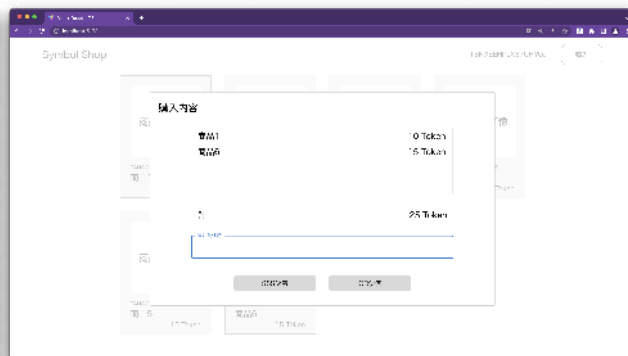


図 3: ショッピングカート画面 P_{cart}

ショッピングカート画面からウォレットによるトークン支払い画面へのプロセスは $P_{cart} \xrightarrow{\text{QR 決済}} P_{(buy|wallet)}$ となる。図 4 と図 5 に試作したウォレットによりトークン支払いする画面 $P_{(buy|wallet)}$ と QR コードを読み取った Symbol ウォレットを示す。 $P_{(buy|wallet)}$ には、トークンの支払い先と量と取引のメッセージを情報とする QR コードを表示している。この QR コードを Symbol ウォレットで読み取り、図 5 に示すようにトークン支払いができることを確認した。

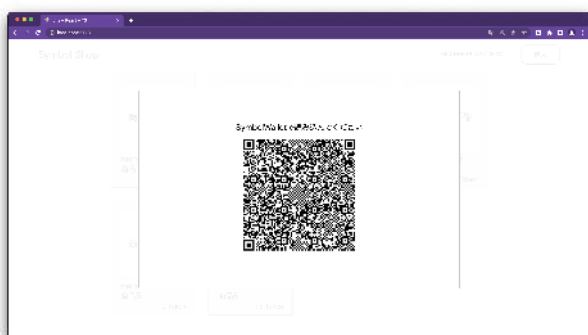


図 4: トークン支払いする画面 $P_{(buy|wallet)}$

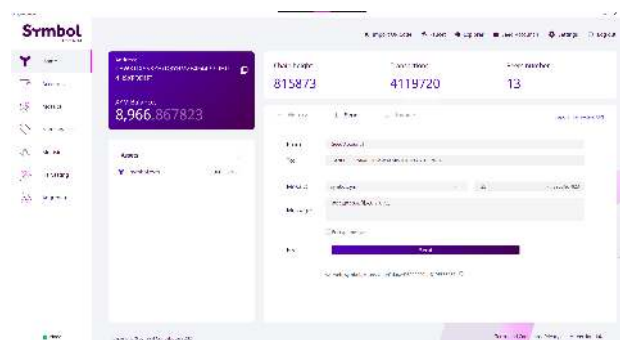


図 5: QR コードを読み取った Symbol ウォレット

ショッピングカート画面から Web 拡張機能によるトークン支払いのプロセスは $P_{cart} \xrightarrow{\text{SSS 決済}} P_{(buy|webext)}$ となる。図 6 に Web 拡張機能によりトークン支払いする購入者のログイン画面を示す。購入者はパスワードを入力することで秘密鍵を復号する。秘密鍵の復号に成功すると、 $P_{(buy|webext)}$ に遷移する。図 7 に、トークン支払いする画面 $P_{(buy|webext)}$ を示す。電子商取引プラットフォームである Web アプリケーションはトークン支払いするトランザクション Tx を生成する。次に、Web 拡張機能である SSS Extension から公開されている API である setTransaction(Tx) によりトランザクション Tx を SSS Extension に設定し、もう一つの API である requestSign() により SSS Extension に購入者の電子署名を依頼する (図 1)。SSS Extension が購入者の電子署名をするためには、購入者が図 7 の署名ボタンを押す必要がある。購入者が電子署名を承認すると、電子商取引プラットフォームである Web アプリケーションは電子署名されたトランザクションをブロックチェーン Symbol に送信すると同時に、ショッピングカートの購入情報を電子商取引プラットフォーム WebApp に送信する。図 7 に示されたトークンの支払い先と量と取引のメッセージが、Symbol ウォレットにも反映されていることを確認した。

⁴<https://chrome.google.com/webstore/detail/sss-extension/llldiojemakefgnhhkmiiiffonembcan?hl=ja>

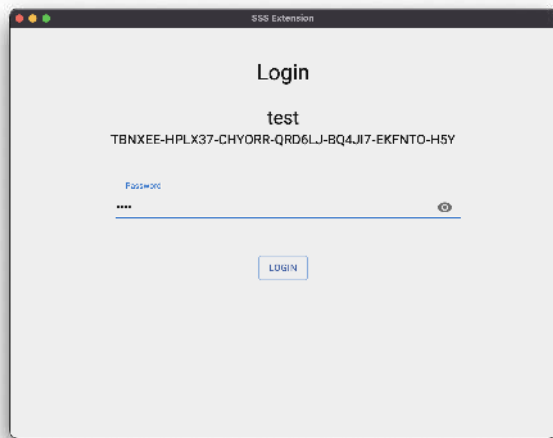


図 6: 購入者のログイン画面

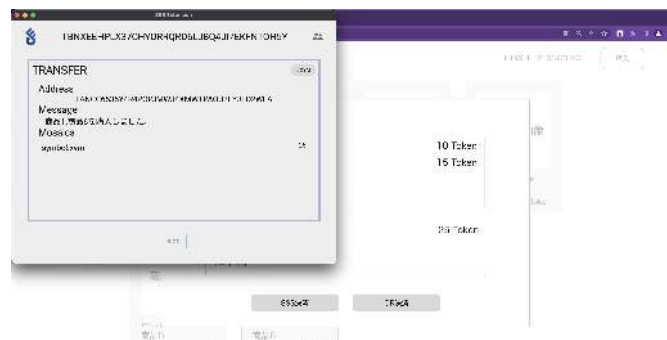


図 7: トークン支払いする画面 $P_{(buy|webext)}$

Web 拡張機能によるトークン支払い $P_{(buy|webext)}$ (図 6 と図 7) では、電子商取引プラットフォームである Web アプリケーションは電子署名されたトランザクションをブロックチェーン Symbol に送信すると同時に、ショッピングカートの購入情報を電子商取引プラットフォーム WebApp に送信できた。このため電子商取引プラットフォームはトークン支払いが確定した取引情報をシームレスに取得することができた。一方、ウォレットによるトークン支払い $P_{(buy|wallet)}$ (図 4) では、電子商取引プラットフォームである Web アプリケーションがショッピングカートの購入情報を受信し、ウォレットがトークン支払い情報を受信した。このため電子商取引プラットフォームは購入情報とトークン支払いを手動で紐づけるか、別途連携するシステムを構築する必要があった。また、Web 拡張機能によるトークン支払いは Web ブラウザで操作が完結し、購入者の利便性が向上したと考えられる。

4. まとめ

安全な BOPIS の実現を目的としてトークン支払いする電子商取引プラットフォームについて検討した。Symbol ブロックチェーンを用いて電子商取引プラットフォームのプロトタイプを試作し、ウォレットと Web 拡張機能によるトークン支払いを比較した。ウォレットによるトークン支払いでは電子商取引プラットフォームで購入情報とトークン支払い情報を紐付ける必要があったが、Web 拡張機能によるトークン支払いでは Web ブラウザで購入者の操作が完結し、電子商取引プラットフォームで同時に購入情報とトークン支払い情報を取得できることを確認した。今後の課題として、BOPIS でなく商品を発送する遠隔取引を実現するためにエスクローサービス [4, 5] の実装が挙げられる。

謝辞

本研究は JSPS 科研費 20K12087 の助成を受けたものである。

参考文献

- [1] “デジタル通貨広がる 行政・中小の DX の起爆剤に”, 日本経済新聞, 2022 年 5 月 31 日, 9 面.
- [2] Bart L. MacCarthy, et al., “Best Performance Frontiers for Buy-Online-Pickup-in-Store order fulfilment,” International Journal of Production Economics, vol. 211, May 2019, pp. 251-264.
- [3] “膨張する分散型金融 11 兆円市場、通貨の未来問う”, 日本経済新聞, 2021 年 10 月 18 日, 1 面.
- [4] S. Goldfeder, et al., “Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin,” International Conference on Financial Cryptography and Data Security, pp. 321-339, 2017.
- [5] A. Endurthi, et al., “Cheat Proof Escrow System for Blockchain,” 2021 5th international Conference on Intelligent Computing and Control System, 2021, pp. 294-298.