SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

プライバシーに考慮した身分証明を使ったトークン取引の新方式の提案と実証システムの試作

Design and evaluation of token trading system with privacy preserving identity disclosure mechanisms

佐藤 出 * 藤本 真吾 *
Izuru Sato Shingo Fujimoto

キーワード ブロックチェーン; トークンエコノミー; Hyperledger Indy; Hyperledger Cactus

あらまし

近年ブロックチェーン業界ではトークンエコノミーが注目されている。トークンエコノミーで取り扱う対象が広がるにつれ、法や提供する取引の性質によって取引を行う者の本人確認や取引対象者であることの確認が求められるケースが増えてくるものと考えられる。本人確認が必要とされる場合として携帯電話回線契約時、自動車の購入時、学生割引や従業員割引適用時などがある。

トークンエコノミーで身元確認が必要な取引で電子的な身分証明書を提示する場合、オンラインで送り記録されるかもしれない情報を最小限にしたいと考えるのが自然である。しかし証明書の関係ない部分を削除やマスクといった処理をすると、発行者が付けた電子署名の検証ができず、要求された事項の証明もできなくなってしまう。

取引の際必要最小限の事項だけを相手に提示することができれば、トークンエコノミーで実現できる取り引きの範囲を広げることができる。

本論文では、これを実現する方法として Hyperledger Indy、Hyperledger Fabric、Go-Ethereum、Hyperledger Cactus の各オープンソースソフトウェアを使い、必要な情報だけを相手に提示し、取引相手はその証明の検証結果によって分散台帳上の情報を操作する方式を提案し、この提案方式の実証システムを試作、有効性を評価した。

Hyperledger Cactus は複数のブロックチェーン技術を利用するアプリケーションを簡単に開発できるようにするミドルウェアである。Hyperledger Indy はブロックチェーンで利用できる Identity に関するツールやライブラリ群である。この Hyperledger Indy の分散台帳とゼロ知識証明に関するライブラリ機能を用いることで、自分の資格情報の一部だけを相手に証明することができる。本論文ではこれを用いて自動車を購入するシナリオで購入希望者が割引適用対象であることを証明する。Go-Ethereum は資金の移動を記録する分散台帳として利用し、Hyperledger Fabric は売買する自動車の所有権を記録する台帳として利用する。

本論文では 2 章でブロックチェーン連携取引での身分確認における課題を整理し、3 章でこの課題を Hyperledger Cactus を用いて解決する方式を検討し 4 章で前記方式の試作システムを評価し、最後にまとめと今後の課題について述べる。

* 富士通株式会社, 川崎市, Fujitsu Limited, Kawasaki-city