ブロックチェーンのプライバシー保護技術

～ブロックチェーンをより安心して利用するために～

大学院　情報科学研究科

○教授　田中俊昭（たなか としあき）

キーワード　**ブロックチェーン，プライバシー保護，匿名性，ミキシング，暗号プロトコル**

研究概要

ブロックチェーンは，取引データを参加者同士で確認するため信頼性が高く，改ざんが困難であるという特徴を活かして，暗号通貨に留まらず，スマートコントラクト，IoT（Internet of Things），サプライチェーン管理など様々な用途への応用が期待される．一方，ブロックチェーン上の参加者は，個人に紐づかない公開鍵に基づく識別子（ID）を用いて取引を行うので，一定の匿名性は保たれるものの，取引データなどの機微な情報が他の参加者に公開される．このため，特定の参加者の取引履歴を追跡できる，あるいは，他の取引と関連付けられる等のプライバシー漏洩の問題が指摘されており，これまで，本課題を解決する様々なプライバシー保護の手法が提案されている．本研究では，**参加者の特定，取引情報の追跡等，想定されるプライバシーの問題点を明確化し，さらに，その課題に対する対策技術について商用サービスや研究動向を整理する**．具体的には，複数のトランザクションを統合・混在させることにより追跡を困難にするミキシング技術，暗号プロトコルを用いて取引データを秘匿する技術，ブロックチェーンを拡張して取引を秘匿する技術等を比較・検証する．また，暗号通貨など一部の用途では，プライバシー保護技術が不正利用を助長することにもなるので，**プライバシー保護と不正利用対策を両立する手法等，今後，取り組むべき課題についても考察する**．

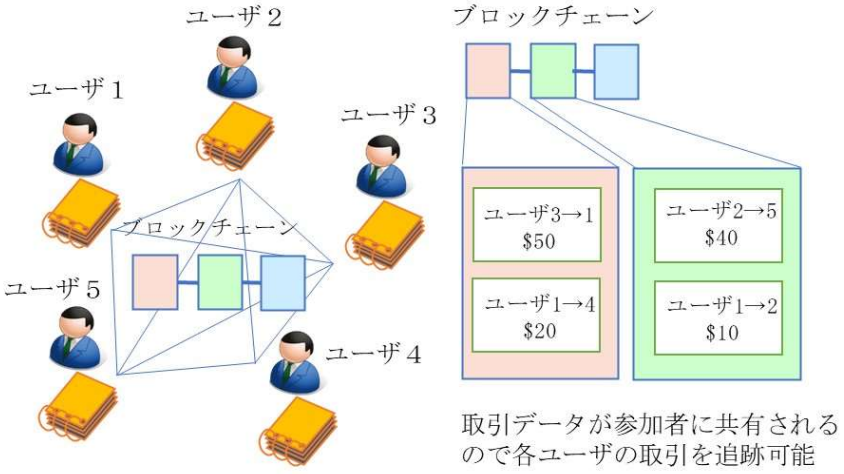

図１　ブロックチェーンの構成と取引データの例

図２　プライシー保護対策技術

アピールポイント

プライバシー保護技術は，健康・医療分野，企業間取引など機微な情報を扱うサービスにブロックチェーンを活用する際に解決すべき課題です．最新動向を知りたい方は是非お越しください．