

ブロックチェーンの鍵管理と応用に関する研究

研究分野: 暗号応用技術, ブロックチェーン, プライバシ保護

キーワード: ブロックチェーン, 鍵管理, 鍵紛失

貢献できるSDGsの区分:



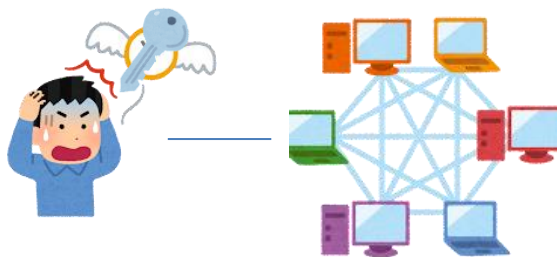
情報システム学部 情報セキュリティ学科 教授 松崎 なつめ

教員情報URL <https://sun.ac.jp/researchinfo/matsuzaki/>

研究概要

近年, 暗号資産の基盤技術である「ブロックチェーン」を用いた応用開発が盛んである. ブロックチェーンでは, 複数のノードに信頼を分散することでシステムの安全性を確保する一方, そこでやり取りされる価値の安全性は個々のユーザの秘密鍵管理にゆだねられる.

本研究では, 「**秘密鍵の紛失対策**」に着目し, 安全で利便性の高い方法を研究している. 具体的にはブロックチェーンの上で動作するプログラムを用いて, 自動的に鍵を退避する方法を考案し, 実装評価している.



産学連携の可能性(アピールポイント)

- ・ブロックチェーンの応用システム(例えば, サプライチェーンや認証など)の開発や, その安全性に関して提案・評価をします.
- ・安全で利便性の高い鍵管理方法を開発し, 実装評価します.
- ・鍵管理において, ユーザ自身のプライバシー保護にも配慮した方法を開発します.

外部との連携実績等

- ・科研基礎研究(C), 「ブロックチェーンに適した分散管理システム用鍵管理方法の設計と評価の研究, 2020.4~2024.3.
- ・長崎市個人情報保護審議会委員(2017年~現在)
- ・長崎県個人情報保護審査会委員(2023年~現在)