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

鍵紛失における非常ボタン式資産退避手法の実装と評価

An Implementation and Evaluation on "Emergency Button" Which Enables Crypto Asset Evacuation When Key Loss

松崎 なつめ * 喜多 義弘 *
Natsume Matsuzaki Yoshihiro Kita

キーワード 暗号資産　鍵紛失　非常ボタン　資産退避　Ethereum

あらまし

本論文では暗号資産の秘密鍵紛失対策について検討する．暗号資産において，秘密鍵は送金時のトランザクションに署名を施すために必要であり，秘密鍵の紛失は対応する暗号資産を紛失することに相当する．SCIS2020 で提案された「非常ボタン式資産退避手法」は，秘密鍵を保有しているときに，スマートコントラクトを準備しておき，公開情報のみで，事前に準備しておいたスマートコントラクトを起動することで，紛失した秘密鍵に対応した資産を，避難して救済する方法である．本論文では，この手法を Ethereum 上に実装して評価する．

* 長崎県立大学 〒 851–2195 長崎県西彼杵郡長与町まなび野 1 − 1 − 1 University of Nagasaki, 1-1-1, Manabino, Nagayo-cho, Nishi-sonogi-Gun, Nagasaki, 851–2195, Japan. {matsuzaki, kita}@sun.ac.jp