様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １０ 日現在

機関番号：２７３０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８１５

研究課題名（和文）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

研究課題名（英文）Research on key management methods for distributed systems suitable for blockchain

研究代表者
松崎　なつめ（Matsuzaki, Natsume）

長崎県立大学・情報システム学部・教授

研究者番号：１０７８１８９１

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究では，ブロックチェーンのような分散管理システムに適した鍵管理方法の，特に「秘密鍵紛失対策」をモデル化から設計し，安全性と実装性を評価することを目的とする．
2020年度はスマートコントラクトを用いた「非常ボタン式資産退避手法」のコンセプトを考案した．この方法は，鍵を紛失する前に暗号資産を退避するためのスマートコントラクトを用意し，秘密鍵紛失時に起動することで暗号資産を別の秘密鍵に紐づいた退避口座に退避する．2021年度は実装に向けた基礎検討を進め，2022年度には1名の研究協力者を追加して実装評価した．2023年度は提案方法のコンセプトから実装までを論文化しCANDARWにて発表した．

研究成果の学術的意義や社会的意義
ビットコインなどの暗号資産は公開鍵暗号をベースとしたブロックチェーン技術を用いて，価値ある資産情報を管理している．暗号資産管理においては，秘密鍵の漏洩対策と，対応する公開鍵の改ざんを防ぐ「鍵管理」が最重要事項である．2018年に起こったNEM鍵漏洩事件では，取引所に預けた秘密鍵が漏洩し，約580億円が不正流出した．この事件を教訓として，暗号資産を複数の取引所に分散管理することや，コールドウォレットを併用するなどの運用的対応策が提案されている．しかるに，鍵管理方法の技術的対応の検討は少なかった．本研究では，分散管理システムをモデル化し，分散管理システム向けの鍵管理を確立することを目的とする．

研究成果の概要（英文）：The purpose of this research is to design a key management scheme suitable for decentralized management systems such as blockchain, especially a “countermeasure against loss of private keys,” from modeling to design, and to evaluate its security and implementability.
In 2020, we considered the concept of an “emergency button method of asset evacuation” using smart contracts. In 2021, we conducted a basic study for implementation, and in 2022, we evaluated the implementation with one additional researcher. In 2023, we published a paper on the proposed method from concept to implementation and presented it at CANDARW.

研究分野：暗号技術

キーワード：暗号資産　鍵紛失　非常ボタン　資産退避　Ethereum

１．研究開始当初の背景

ビットコインなどの暗号資産は公開鍵暗号をベースとしたブロックチェーン技術を用いて，価値ある資産情報を管理している．この暗号資産管理においては，秘密鍵の漏洩対策と，対応する公開鍵の改ざんを防ぐ「鍵管理」が最重要事項である．2018 年に起こった NEM 鍵漏洩事件では，取引所に預けておいた秘密鍵が漏洩し，約 580 億円が不正流出した．この事件を教訓として，暗号資産を複数の取引所に分散管理することや，コールドウォレットを併用するなどの運用的対応策が提案されている．しかるに，鍵管理方法の技術的対応の検討は少なかった．

そこで，本研究では，分散管理システムをモデル化し，分散管理システム向けの鍵管理を確立することを目的とする．目指す鍵管理方法は，中央集権的な鍵管理である PKI（Public Key Infrastructure : 公開鍵暗号基盤）に対応する分散管理システム向けの鍵管理技術である．

２．研究の目的

研究期間の１年目に，本研究における取り組むべき研究テーマを「秘密鍵紛失対策」と絞り込んだ．秘密鍵は，暗号資産を支出する場合に必要となる情報であり，この紛失は対応する暗号資産を支出できないことを表す．このテーマに絞った理由は２つある．１つ目は秘密鍵の紛失については，例えば暗号資産を分散管理するなど万が一鍵を紛失してもそのリスクを低減したり，カストディなどの機関に委託するなど運用的な対策はあるものの，安全でユーザの利便性を確保した技術対策が提案されていないからである．２つ目はブロックチェーンを用いた主となるアプリである暗号資産においては，匿名性が必要であり，一方，紛失した鍵を回復するためには何らかの認証が必要と考えられ，この矛盾する２つの特性を両立することに学術的な興味を抱いたからである．

本研究では「秘密鍵紛失対策」をモデル化から具体的な方法まで設計し，安全性と実装性を評価して，現行システムへの適用を検討することを目的とする．秘密鍵紛失とは，所定の暗号資産を使うための秘密鍵を本人が有していないことと定義する．この秘密鍵紛失対策における要件としては次を想定する．

【安全性】方式を悪用されないこと．

【鍵の個人管理】秘密鍵を主に個人で管理する場合を想定する．取引所やカストディに秘密鍵の管理を任せる方法は，比較的ユーザ利便性はある一方，NEM 鍵漏洩事件のようなリスクは残り，またコストもかかる．

【即応性】鍵を紛失し，すぐに対応できる方法であること．例えば，鍵を分散して周りに預託する場合は，分散鍵を集めればもとの鍵を復元できるが，分散鍵の持ち主であることを証明して閾値以上を集めるには，時間がかかると想定する．

【匿名性】通常の法廷通貨のように，匿名で暗号通貨を利用する場合も想定する．この場合，例えば鍵を他に預託しておいたとしても，鍵の持ち主であることを認証して鍵を回復することは困難である．

【ユーザ利便性】鍵紛失前には，ユーザの利便性を損なわないこと．また，鍵の紛失に気が付いたら，ユーザの利便性を確保しつつ即対応可能である対策であること．

【暗号資産を回復】紛失した鍵の復元よりも，対応する暗号資産を本人に戻すことを目指す．

３．研究の方法

(1) 研究体制

研究は研究代表の松崎（全体推進，方式設計），研究分担者の喜多氏（方式設計，実装評価）と 2022 年より加わった福光氏（方式設計，実装評価）の３人で議論し，分担して進めた．

(2) 研究経過

2020 年 : 既存技術を調査し，解決すべきテーマを「秘密鍵紛失対策」に絞り込み，スマートコントラクトを用いた「非常ボタン式資産退避手法」のコンセプトを考案した．

2021 年 :「非常ボタン式資産退避手法」の詳細プロトコルと実装検討を進め，より実践的な方式に拡張した．

2022 年 : 福光氏が加わり，実装に関し復号オラクル Chainlink を用いて安全性と使いやすさを向上する方法を検討した．イーサリウムを用いて実装評価完了．

2023 年（１年延長）これまでの検討結果を整理して，英論文化．国際会議 CANDARW（The Eleventh International Symposium on Computing and Networking Workshops, Nov. 28 2023 to Dec. 1 2023, Matsue, Japan）に採録されて発表完了．

４．研究成果

(1) 提案方法の要約

上記要件を考慮して本研究で提案した「秘密鍵紛失対策」は，秘密鍵に対応する暗号資産を，所定の退避用アカウントに移動するスマートコントラクトを「非常ボタン」として事前に作っておき，秘密鍵を紛失した場合に，このスマートコントラクトを起動することにより，暗号資産を救済する．より詳細に述べる．避難先の口座 B を生成し，対応した秘密鍵を金庫に保存するとともに，もとの口座 A から B に暗号資産を移動するトランザクションを生成する．そして，口座 A の（紛失前の）秘密鍵 sk を用いてトランザクションに署名を施す．さらに，この署名付きトランザクションを実行・記録するスマートコントラクト SC を準備する. 鍵紛失を認識した後, 速やかに SC を起動し，口座 A に紐づいた暗号資産を口座 B に移動する．その後退避先の口座 B に対応した秘密鍵を取り出して，対応する暗号資産を利用可能とする．

さらに，提案方法の最終形では，次の３点を特徴としている．

1) トランザクションを暗号化 : 署名付きのトランザクションをユーザが定めた鍵で暗号化して記録することにより，攻撃者による悪用のリスクを削減している．復号時には Chainlink と外部アダプタで実装される復号オラクルを用いてトランザクションを復号する．
2) トランザクションを Value 分割して記録 : Value を分割して準備することにより，スマートコントラクト準備後に，暗号資産を消費したり追加して Value が変化した場合にも，最初に準備したトランザクションを用いることができる．
3) トランザクションを IPFS に保存 : Value 分割したトランザクションを（ブロックチェーンではなく）分散型ストレージ IPFS に記録することにより手数料（GAS 代）を節約する．

(2) 発表論文

・CSS2020（Computer Security Symposium 2020：2020.10.26-29）のパネルセッションでの発表（DPS-07:ブロックチェーンに適した鍵漏洩対策の検討）:「秘密鍵紛失対策」に関する従来方法と，技術的解決の必要性を示した．この議論の中で，この課題解決の重要性を確認

・SCIS2021（The 38th Symposium on Cryptography and Information Security：2021.1.19-22）での発表（2E1-3：鍵紛失時における非常ボタン式資産退避手法の考察）：鍵紛失の非常時に，匿名性を確保したまま，紛失した鍵に対応した暗号資産を避難するスマートコントラクトを導入して提案し，その有用性について議論した．

・電子情報通信学会情報セキュリティ研究会（ISEC：2021.7）での発表（鍵紛失時における非常ボタン式資産退避手法の実用化に関する考察，ISEC2021-28）：退避先の鍵を分散管理し，それを収集して復元するもう１つのスマートコントラクトを導入した．

・SCIS2022（The 39th Symposium on Cryptography and Information Security：2022.1.18-21）での発表（鍵紛失時における非常ボタン式資金退避手法の実装と評価，4D2-5）：イーサリアムを用いたスマートコントラクトの実装にあたり，その基礎検討を行った．

・SCIS2023（The 40th Symposium on Cryptography and Information Security：2023.1.24-27）での発表（鍵紛失における非常ボタン式資産退避手法の再実装，3C3-2）：退避する暗号資産を小銭に分割することで利便性を高めるとともに，ブロックチェーン上のデータを暗号化することで安全性を向上した．

・CANDARW2023（The Eleventh International Symposium on Computing and Networking Workshops，28 November - 1 December 2023, Matsue, Japan）での発表（Emergency Button: Evacuation of Crypto Asset When Key Loss）：非常ボタン式資産退避手段のコンセプトから実装までを論文化した．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 松崎なつめ，喜多義弘，福光正幸
２．発表標題 鍵紛失時における非常ボタン式資金退避手法の再実装
３．学会等名 SCIS2023 (The 40th Symposium on Cryptography and Information Security)
４．発表年 2023年

１．発表者名 松崎なつめ，喜多義弘
２．発表標題 鍵紛失時における非常ボタン式資産退避手法の実用化に関する考察
３．学会等名 電子情報通信学会　情報セキュリティ研究会（ISEC）
４．発表年 2021年

１．発表者名 松崎なつめ，喜多義弘
２．発表標題 鍵紛失時における非常ボタン式資金退避手法の実装と評価
３．学会等名 SCIS2022 (The 39th Symposium on Cryptography and Information Security)
４．発表年 2022年

１．発表者名 松崎なつめ，喜多義弘
２．発表標題 ブロックチェーンに適した鍵漏洩対策の検討
３．学会等名 CSS2020（Computer Security Symposium 2020）パネルセッション
４．発表年 2020年

１．発表者名
松崎なつめ，喜多義弘

２．発表標題
鍵紛失時における非常ボタン式資産退避手法の考察

３．学会等名
SCIS2021 (The 38th Symposium on Cryptography and Information Security)

４．発表年
2021年

１．発表者名
Natsume Matsuzaki Masayuki Fukimitsu and Yoshihiro Kita

２．発表標題
Emergency Button: Evacuation of Crypto Asset When Key Loss

３．学会等名
The Eleventh International Symposium on Computing and Networking Workshops (CANDARW) (国際学会)

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	喜多　義弘 (Kita Yoshihiro) (00758089)	長崎県立大学・情報システム学部・准教授 (27301)	
研究分担者	福光　正幸 (Fukumitsu Masayuki) (10736119)	長崎県立大学・情報システム学部・准教授 (27301)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関