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　５ 年　 ６ 月 １４ 日現在

機関番号：３４４１９
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１２０８７

研究課題名（和文）複数の暗号資産ウォレットと連携可能なマルチシグ対応コールドストレージの基盤開発

研究課題名（英文）Development of infrastructure for multisig cold storage inked to multiple crypto asset wallets

研究代表者
森山　真光（Masamitsu, Moriyama）

近畿大学・情報学部・准教授

研究者番号：００２８３９５３

交付決定額（研究期間全体）：（直接経費）　　1,700,000円

研究成果の概要（和文）：暗号資産の市場は成長を続けている。一方で暗号資産の秘密鍵の紛失や盗難は後を絶たない。個人で秘密鍵を管理する方法には、ペーパーウォレットやハードウェアウォレットがある。暗号資産取引所で数万人の秘密鍵を管理する方法は一般的に非公開であるがコールドウォレットやマルチシグを用いている。本研究では個人と暗号資産取引所の中間にある同一敷地内に配置された100個程度の暗号資産ウォレットにおいて利便性と安全性のバランスのとれた秘密鍵の管理手法としてマルチシグ対応のコールドストレージの基盤開発を行った。

研究成果の学術的意義や社会的意義
暗号資産ウォレットの秘密鍵の管理手法は数万人を扱う取引所もしくは個人で実践されている。本研究はその中間に位置し未だ標準技術のない同一敷地内に配置された100個程度の暗号通貨ウォレットを対象としている。さらに策定したプロトコルをEコマースサービスに実際に適用し検証している。暗号通貨のソフトウェアにとって重要な分散化を実践することで、本研究の成果は暗号資産に留まらずブロックチェーンが応用されるスマートコントラクト(自動的な契約)等の分野でも有効となることが期待される。

研究成果の概要（英文）：The market for crypto-assets continues to grow. On the other hand, there is no end to the loss or theft of private keys for crypto-assets. Personal methods of managing private keys include paper and hardware wallets. The method of managing tens of thousands of private keys on crypto-asset exchanges is generally undisclosed but uses cold wallets and multisig. In this study, we developed the infrastructure for multisig cold storage as a method of managing private keys with a balance between convenience and security in about 100 crypto-asset wallets.

研究分野：情報学

キーワード：暗号資産　ブロックチェーン　コールドストレージ　マルチシグ　ウォレット

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
(1) 暗号資産は P2P（Peer-to-Peer）技術と公開鍵暗号などの技術を用いて実現されている。暗号資産は、円やドルなどの法定通貨を発行する中央銀行を経由せず、利用者にとっては送金時に負担する手数料が数円ですむ利点がある。暗号資産の種類は研究開始当初で 600 以上あるとされていた。インターネット上で最も多く取引されている暗号資産は 2008 年に発明された Bitcoin である。研究開始当初の時価総額は約 100 億ドル（１兆円）で市場全体の 8 割を占め、利用者は世界で 1300 万以上、国内では数万人であった[1]。

(2) 暗号資産は暗号技術や分散システムの組み合わせで実現され、特に分散台帳技術であるブロックチェーンと通貨発行である分散マイニングの研究がなされている[2]。また代表者は国際電子商取引のシステム開発やその P2P 技術への応用に取り組んでいる。

(3) しかしながら、暗号資産の運用においては、次のような課題がある。
① 安全性: 2014 年当時最大の取引所であったマウントゴックスで約 5000 億円相当が消失、2016 年香港の取引所で約 66 億円が盗難、違法取引や資金洗浄の犯罪への利用[3]。
② 人材: ブロックチェーンをゼロから組める技術者は国内で 150 名程度[4]。
③ 投資: 日本の対フィンテック投資（2015 年）は約 65 億円と米国の 0.5%、中国の 30 分の 1[5]。

(4) 課題１．の暗号資産の安全性は分散型台帳であるブロックチェーンが書き換えられたのではなく、利用者の秘密鍵の紛失もしくは盗難にあったために発生している。暗号資産の支払い機能であるデスクトップおよびモバイルウォレットはインターネットに接続したハードウェアに秘密鍵を保持している。これは取引データであるトランザクション Tx を電子署名するときに秘密鍵が必要となるためである。しかしながら、ハードウェアがマルウェアなどのウィルスに感染していると秘密鍵が盗まれる危険性がある。

(5) 個人で秘密鍵を管理する方法は、紙に秘密鍵を印刷したペーパーウォレットや専用端末であるハードウェアウォレットがある。暗号資産取引所で数万人の秘密鍵を管理する方法には、2 段階認証ログインをはじめ暗号資産ウォレットをネットワークにつながっていない安全な場所で管理するコールドストレージと複数の秘密鍵で署名しないと送金できないマルチシグの組み合わせがある。一般的に暗号資産取引所のセキュリティ施策は非公開である。

２．研究の目的
(1) 暗号資産関連のソフトウェア開発者にとって、最も重要な原則は分散化である[6]。E コマース構築パッケージの運用やブロックチェーン教育はともに同一敷地内に配置された 100 個程度の暗号資産ウォレットの秘密鍵を管理する必要がある。本研究では暗号資産において利便性と安全性のバランスのとれた同一敷地内の 100 個程度の秘密鍵の管理手法を確立することを目的とする。

３．研究の方法
(1) 複数の暗号資産ウォレットで共通に利用できるコールドストレージのプロトコルを策定する。暗号資産では秘密鍵で電子署名された取引データであるトランザクション Tx が分散マイニングという分散化合意形成の仕組みによって信用され、最後に分散型台帳であるブロックチェーンに記録される。ウォレットソフトウェアは支払い先を Web ブラウザや QR コードから読み取りトランザクション Tx を作成する。次にウォレットソフトウェアは端末がインターネットに接続していないことを確認した後にコールドストレージにある秘密鍵で Tx の電子署名の要求を送信し、電子署名を受け取る。最後にコールドストレージに接続していないことを確認した後にインターネットに電子署名された Tx を送信する。以上のデータ形式や通信方法を策定する。

(2) 策定したプロトコルの E コマースへの適用と検証を行う。代表者が分析している E コマースパッケージに策定したプロトコルを組み込み、複数の暗号資産で実際に送金入金処理の動作検証を行う。特に、暗号資産が銀行の発行する確約書である信用状（Letter of Credit: L/C）の代理になり得るか検証する。

４．研究成果
(1) 初年度は暗号資産ウォレットとコールドストレージとのマルチシグに対応したプロトコルについて Bitcoin と Ethereum に調査し、この 2 つの暗号資産の 1-of-1 マルチシグを抽象化したコールドストレージを試作し検証した。安全性から有線やネットワーク接続でなく、エアギ

ャップとなる QR コードを媒介としたカメラと NFC タグを媒介とした NFC リーダ・ライタを採用することとした。

(2) 2 年度は策定したプロトコルを Bitcoin と Ethereum のウォレットと連携可能な m-of-n マルチシグに対応するコールドストレージ機能に拡張した。Ethereum はビルドインでマルチシグ機能を有していないためスマートコントラクトで実装した。図 1 に策定したプロトコルのシーケンス図を示す。ウォレットが自身で Tx に電子署名する（図 1-1）。ウォレットがコールドストレージに識別士を送信する（図 1-2）。ウォレットは自身で署名した Tx をコールドストレージに送信する。コールドストレージは Tx をマルチシグとなる電子署名する（図 1-4）。ウォレットはマルチシグ Tx を受信しブロックチェーンにブロードキャストする（図 1-4，5）。シングルボードコンピュータで実装した。m-of-n マルチシグでは n 個の署名者の暗号資産ウォレットを識別して署名する必要がある。そのため図 1 のように暗号資産ウォレットを識別するワンタイムパスワードや個体識別番号により署名者を識別するプロトコルを追加した。通常の暗号資産ウォレットは取引情報であるトランザクション(Tx)を QR コードで入出力する機能を有する。図 2 にコールドストレージのインタフェースを示す。図 2 のようにコールドストレージに QR コードを読み取るバーコードリーダと QR コードを出力するディスプレイを接続して、通常の暗号資産ウォレットと連携できるようにした。

(3) 3 年度は暗号資産ウォレットとコールドストレージ間の Tx を NFC で送受信できるように拡張した。暗号資産として Symbol を追加した。通常の暗号資産ウォレットは NFC による Tx の送受信機能がない。そこで各暗号資産について NFC で Tx を送受信できるウォレットアプリケーションを開発して検証した。独自にウォレットアプリケーションを開発することで署名者の識別情報と Tx を同時に送信できるため利便性が向上した。QR コードを媒介としたエアギャップと NFC タグを媒介とした NFC リーダ・ライタのエアギャップは、ともにエアギャップを実装しているため安全性を高めている。QR コードは通常のウォレットアプリケーションを利用できるが、NFC は独自のウォレットアプリケーションを用いる必要がある。利用者の利便性を検討し使い分けが必要である。加えて、本プロトコルを E コマースアプリケーションと連携し、マルチシグによるエスクロー取引の機能を実装し、第三者預託が実現できることを確認した。

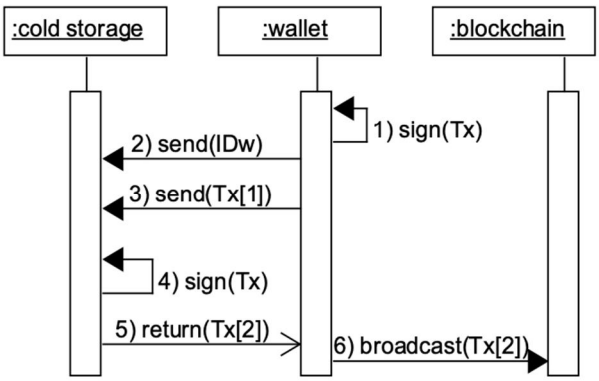

図 1 策定したプロトコルのシーケンス図

図 2 コールドストレージのインタフェース

<引用文献>

[1] “ビットコイン 通貨の位置づけ明確に 取引時、消費税課さず”,日経新聞，2016/10/12，1 面.
[2] F. Tschorsch et al.: “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies”, IEEE Communications Surveys & Tutorials, 18(3), 2084 - 2123, 2016.
[3] “リアルフィンテック下「紙幣がなくなる日」日銀備え”，日経新聞，2016/9/3，5 面.
[4] “リアルフィンテック中 メガ銀猛追 高まる存在感”，日経新聞，2016/9/2，5 面.
[5] “低金利の恩恵中小に 売掛金電子債券ですぐに現金”，日経新聞，2016/8/29，11 面.
[6] A. A. Antonopoulos: “Mastering Bitcoin”, Oreilly & Associates Inc., 239-241, 2014.

5．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 森山真光
2．発表標題 サプライチェーンマネジメントにおけるブロックチェーン技術マルチシグの適用に関する一考察
3．学会等名 日本生産管理学会 第55回全国大会
4．発表年 2022年

1．発表者名 白濱敬也，森山真光
2．発表標題 ブロックチェーン秘密鍵のバックアップエコシステムについて ーデータ作成および検証プロトコルの実装ー
3．学会等名 2021年電子情報通信学会総合大会「ジュニア&学生ポスターセッション」
4．発表年 2021年

1．発表者名 白濱敬也，森山真光
2．発表標題 ブロックチェーン秘密鍵のバックアップエコシステムの提案
3．学会等名 第16回情報システム学会全国大会・研究発表大会
4．発表年 2020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

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