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　２ 年　 ６ 月　 １ 日現在

機関番号：３４４１９
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００４４５

研究課題名（和文）複数の暗号通貨ウォレットで共通に利用できるコールドストレージ機能に関する研究

研究課題名（英文）Study on function of common cold storage using multiple cryptocurrency wallets

研究代表者
森山　真光（Moriyama, Masamitsu）

近畿大学・理工学部・准教授

研究者番号：００２８３９５３

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：　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は実践されている。本研究ではその中間に位置した未だデファクトスタンダードのない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を対象に利便性と安全性のバランスの取れた秘密鍵の管理手法の確立を目指す。
　ワンボードマイコンをコールドストレージとして、複数の暗号資産ウォレットと取引情報であるトランザクションを送受信するプロトコルを策定し、実証実験を行った。通信手段としてはUSBとBluetoothのシリアル通信方式、microSDカードとNFCの記憶媒体方式を提案した。

研究成果の学術的意義や社会的意義
　暗号資産の市場規模は20兆円以上で利用者数は3,000万人以上であるが、暗号資産の紛失や盗難は後を立たない。暗号資産の紛失や盗難はほとんどが、基盤技術であるブロックチェーンや分散型台帳技術のデータが書き換えられたのではなく、利用者の秘密鍵が紛失もしくは盗難にあったため発生している。
　本研究では、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手法を提案した。さらに暗号資産の秘密鍵を管理する教材を作成し、学生や社会人を対象にブロックチェーンのセミナーで活用した。ユースケースとして、ブロックチェーンや分散型台帳技術の教育やEコマース運営者の決済への活用が期待される。

研究成果の概要（英文）：　The private key management of a crypto-assets wallet is using practically in both cases of a personal use and tens of thousands of people use in crypt-assets exchanges. If the personal use and the crypto-assets exchanges use are a small case and a large case respectively, the private key management of 100 pieces of crypto-assets wallet placed in same site is a medium case. However, a de facto standard of the private key management in the medium case does not exist. We aim to establish a private key management method in the medium case for keeping balance of usability and security.
　We have developed the protocol that transfer transactions between multiple crypto-assets wallets and a cold storage, and experimented by using one-board microcomputer as the cold storage. we have proposed serial communications such as USB and Bluetooth, and communications by recording mediums such as microSD card and NFC.

研究分野：情報学

キーワード：ブロックチェーン　秘密鍵　分散型台帳技術

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

１．研究開始当初の背景

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。円やドルなど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。暗号資産の種類は当時で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通貨は2008年に発明されたBitcoinである。当時の時価総額は約100億ドル（1兆円）で市場全体の8割を占め、利用者は世界では1,300万以上で国内では数万人であった。

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、特に分散型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。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470億円相当が消失、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等の犯罪へ利用
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
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

２．研究の目的

暗号資産の紛失や盗難はほとんどの場合が、基盤技術であるブロックチェーンや分散型台帳技術のデータが書き換えられたのではなく、利用者の秘密鍵が紛失もしくは盗難にあったため発生している。

個人で秘密鍵を管理する方法には、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、二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を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。このように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は実践されている。

本研究ではその中間に位置した未だデファクトスタンダードのない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を対象に利便性と安全性のバランスの取れた秘密鍵の管理手法の確立を目指す。ユースケースとしてはブロックチェーンや分散型台帳技術の教育やEコマース運営者の決済への活用を想定している。

３．研究の方法

本研究ではワンボードマイコンをコールドストレージとして、複数の暗号資産ウォレットと取引情報であるトランザクションを送受信するプロトコルを策定し、実証実験を行う。通信手段としてはUSBとBluetoothのシリアル通信方式、microSDカードとNFCの記憶媒体方式を提案する。

４．研究成果

(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プロトコルの策定

暗号資産では秘密鍵で電子署名された取引情報であるトランザクション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。図1に暗号資産ウォレットとコールドストレージ間の通信に用いるメッセージを、表1にそのメッセージの概要を示す。通信に用いるメッセージを固定することによって、コールドストレージの動作を制限し、安全性を向上させている。また定められたメッセージ以外は一切受け付けないようにしている。メッセージ内に暗号資産ウォレットとクライアントの識別子を記述するため、1つのコールドストレージで複数の暗号資産ウォレットを共通で利用できるようになっている。

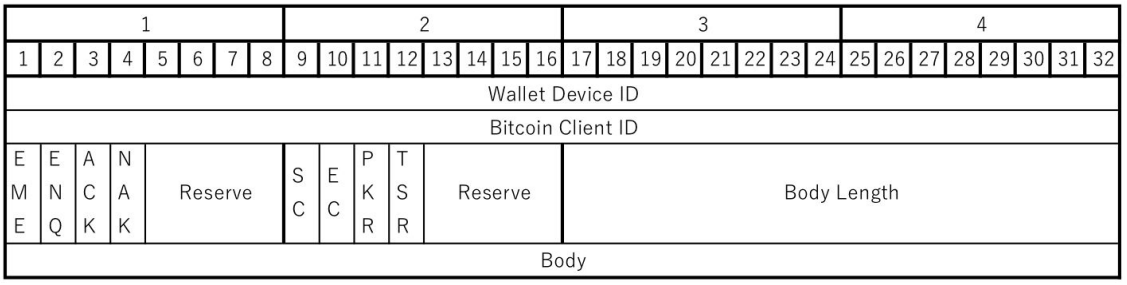

図1 暗号資産ウォレットとコールドストレージ間の通信に用いるメッセージ

表1 暗号資産ウォレットとコールドストレージ間の通信に用いるメッセージの概要

Wallet Device ID		製造段階で発行されたウォレットデバイスの ID
Wallet Application ID		ウォレットアプリケーションの ID (コネクション終了まで有効な ID)
Control Code	EME	緊急データ (最優先に実行すべき事項，ハードウェア独自実装可)
	ENQ	問い合わせ
	ACK	肯定応答
	NAK	否定応答
	Reserve	予約 (常に 0)
Operation Code	SC	コネクションの開始
	EC	コネクションの終了
	PKR	公開鍵の要求
	TSR	トランザクション署名の要求
	Reserve	予約 (常に 0)
Body Length		ボディ部のバイト長
Body		ボディ部

図2に記憶媒体媒介方式による暗号資産ウォレットとコールドウォレットの電子署名の流れを示す。コールドストレージはインターネットと直接接続しないようにエアギャップでの接続を実装している。コールドウォレットはシード値を生成し、階層的決定性ウォレットを用いて親秘密鍵から木構造を構成しこ秘密鍵を生成する。これにより複数の暗号資産ウォレットの取引情報の電子署名を管理することができる。

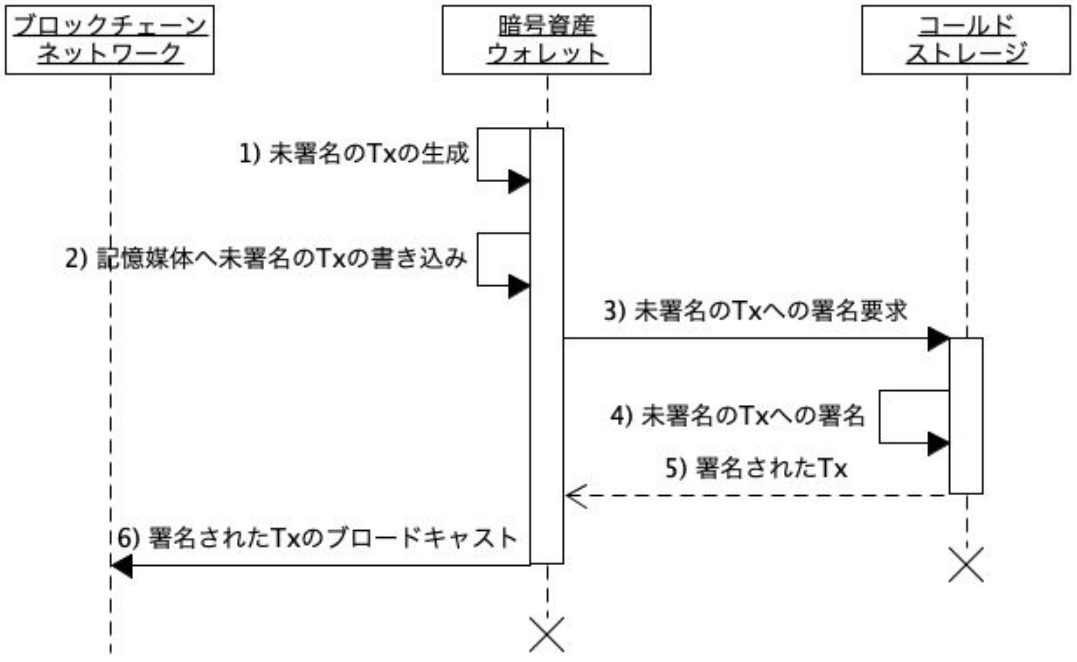

図2 記憶媒体媒介方式による暗号資産ウォレットとコールドウォレットの電子署名の流れ

図3に実験に用いた暗号資産ウォレット(図中BC)とコールドストレージ(図中HW)の配置図を示す。暗号資産としてビットコインのテストネットを用いた。暗号資産ウォレットはインターネット経由でビットコインのテストネットに接続できる。コールドストレージにはワンボードマイコンを用いた。暗号資産ウォレットとコールドストレージはUSBのシリアル通信方式と、microSDとNFCの記憶媒体媒介方式を実装した。USBのシリアル通信方式ではインターネットに接続した暗号資産ウォレットとコールドウォレットを常時接続することは避け、暗号資産ウォレットのインターネットの切断を確認してから、暗号資産ウォレットとコールドストレージを接続するようにした。

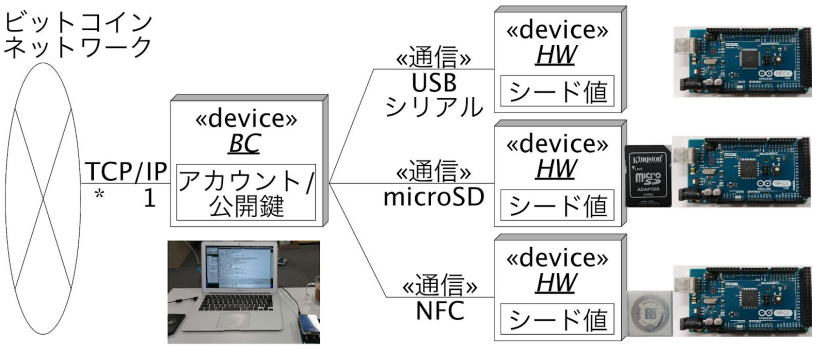

図3 暗号資産ウォレットとコールドストレージの配置図

図4に取引情報と暗号資産ウォレットの起動からコールドストレージを介して5つの署名された取引情報を受信するまでの時間を示す。USBのシリアル通信方式とNFCの記憶媒体媒介方式は同程度の生成時間であったが、NFCの記憶媒体媒介方式は常時エアキャップであるため安全性の面で、USBのシリアル通信方式よりも優れていると考察する。

```
kos@kos:~$ bitcoin-cli -testnet decoderawtrans
action $(bitcoin-cli -testnet getrawtransactio
n 585d1bc8f71f262f1c6e3743cd7d6e6d9efe690fce0c
6770d736fc902d02c361)
{
  "txid": "585d1bc8f71f262f1c6e3743cd7d6e6d9ef
e690fce0c6770d736fc902d02c361",
  "hash": "585d1bc8f71f262f1c6e3743cd7d6e6d9ef
e690fce0c6770d736fc902d02c361",
  "version": 1,
  "size": 225,
  "vsize": 225,
  "locktime": 0,
  "vin": [
    {
      "txid": "3aa8420fb6777e3642f0b853788cf5d
```

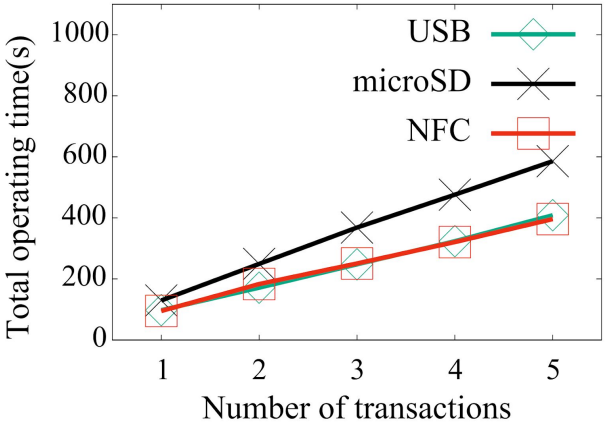

図4 取引情報と暗号資産ウォレットからコールドストレージを介して電子署名を生成するまでの時間

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 沼田幸輔，森山真光
２．発表標題 NFCを用いたビットコインウォレットの秘密鍵管理手法の提案と評価
３．学会等名 情報システム学会 第14回全国大会・研究発表大会
４．発表年 2018年

１．発表者名 森安昭太、森山真光
２．発表標題 暗号通貨ウォレットの秘密鍵管理手法の提案と評価
３．学会等名 経営情報学会秋季全国研究発表会
４．発表年 2017年

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の活用に関する考察 --ブロックチェーンの入門セミナーの実施事例について--
３．学会等名 日本生産管理学会第51回全国大会
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