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

Proposal and evaluation of private key management method of Bitcoin wallet using NFC

沼田幸輔 †, 森山真光 †
Kosuke Numata†, and Masamitsu Moriyama‡
† 近畿大学　理工学部
†Faculty of Science and Engineering, Kindai Univ.

要旨

近年，問題となっている暗号通貨の流出事件では取引所の秘密鍵管理の安全性に原因があるとされている．我々は安全にビットコインウォレットの複数の秘密鍵を管理する手法として，シリアル通信方式と記憶媒体媒介方式の 2 つを提案した．しかし，提案した microSD を用いた記憶媒体媒介方式は安全性は高いが，多くの操作時間を要するという問題がある．そこで，安全性を保ちつつ操作時間の短縮を目的として NFC を用いた秘密鍵管理手法を提案する．本研究では，トランザクションに署名を行うまでの時間を計測して有効性を評価する．結果，NFC を用いた秘密鍵管理手法は安全性を保ちつつ microSD の 0.676 倍で操作できることを確認した．

1 . 序論

ビットコインという 3,000 万人以上のユーザ[1] が利用する暗号通貨がある．近年，問題となっている暗号通貨の流出事件[2] の主な原因として，取引所の秘密鍵管理は安全性に問題があると考える．秘密鍵管理は大きく 3 つに分けられる．1 つ目は紙による管理のペーパーウォレット，2 つ目はソフトウェアで管理するソフトウェアウォレット，3 つ目はデバイスで管理するハードウェアウォレット (以降 HW とする) である．3 つ目のハードウェアウォレットは市販されているが，問題点として複数のビットコインクライアントで利用ができない．そこで我々は，ビットコインウォレットの秘密鍵管理手法として複数のビットコインクライアントで利用できる HW のシリアル通信方式と記憶媒体媒介方式の 2 つを提案した [1]．1 つ目のシリアル通信方式はインターネット上に晒される危険 [2] があるが，累計操作時間が短いという利点がある．2 つ目の記憶媒体媒介方式はインターネット上に晒されないエアギャップだが，データのやり取りに用いる microSD の抜き差しに時間を要するという問題がある．そこで，ビットコインウォレットの秘密鍵管理の安全性を保ちつつ，操作時間の短縮を目的として NFC を用いたデータ通信を提案する．そして，複数のビットコインクライアント (以降 BC とする) で利用できるエアギャップ端末の HW を実装する．本研究では，提案する手法を実装した HW と BC を用いて，BC 起動時から取引情報であるトランザクション (以降 Tx とする) に署名を行うまでの時間を計測して，有効性を評価する．

2 . 研究内容

提案する手法に使う HW はインターネット上に晒されないエアギャップ端末を実装する．従来手法では，秘密鍵を HW のプログラム上に記述している．よって，使用するユーザを増やす時はプログラム上に追記する必要があり，ユーザ追加毎にプログラムを変更する必要があった．そこで，本提案手法では階層的決定性ウォレット [3] を実装することにより従来手法の複数の秘密鍵管理の改善をする．本提案手法の HW はシード値を生成し，階層的決定性ウォレットを使用してシード値から任意の秘密鍵の生成を行う．階層的決定性ウォレットは親秘密鍵から子秘密鍵，孫秘密鍵を木構造的に生成することができるため，複数の BC においての利用を可能にする．

図 1 に BC と HW の配置図を示す．BC とビットコインネットワークはインターネットで接続される．BC と HW は USB のシリアル通信方式と microSD と NFC の記憶媒体媒介方式でデータ通信を行う．USB のシリアル通信方式ではインターネットと接続されている BC と USB で繋がるため，BC ではインターネットの切断を確認してから通信を行う．

[1] Blockchain Wallet Users - Blockchain, https://www.blockchain.com/ja/charts/my-wallet-n-users, 閲覧 2018-11-12

[2] 「Zaif」、不正アクセスで約 67 億円相当の仮想通貨が流出–入出金を一時停止, https://japan.cnet.com/article/35125870/, 閲覧 2018-11-12

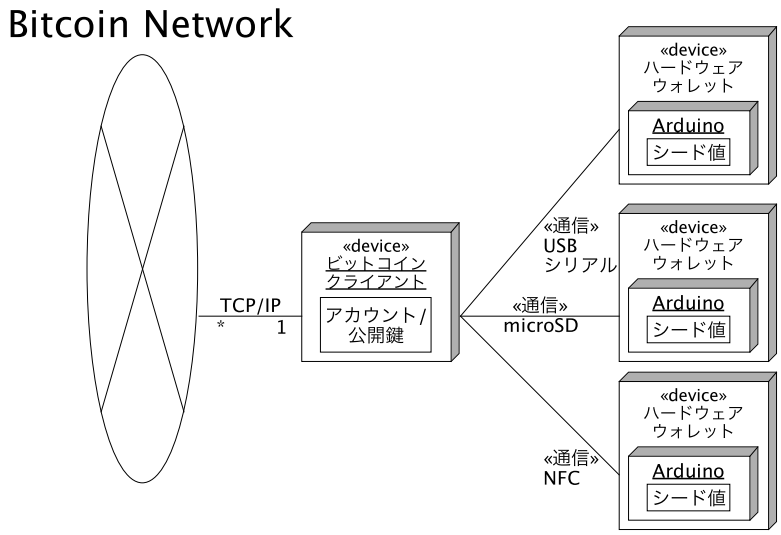

図 1: *BC* と *HW* の配置図

3 . 結果・考察

3.1. ユーザの操作時間の計測

実験は，提案手法を実装した *BC* と *HW* を用意し，5 つの署名された *Tx* が *BC* で生成されるまでの時間を計測した．*BC* を動作させる環境として，MacBook Air 2015 を用いた．OS は macOS High Sierra，CPU は Intel Core i5 1.6GHz，RAM は DDR3 4GB 1600MHz を用いた．*HW* は Arduino Mega 2560 Rev3 を用いた．*BC* と *HW* は USB のシリアル通信方式と microSD と NFC の記憶媒体媒介方式でデータ通信を行った．図 2 に実際に用いた実験機器を示す．図 2 の *HW* はインターネットに繋がっておらずエアギャップ状態である．

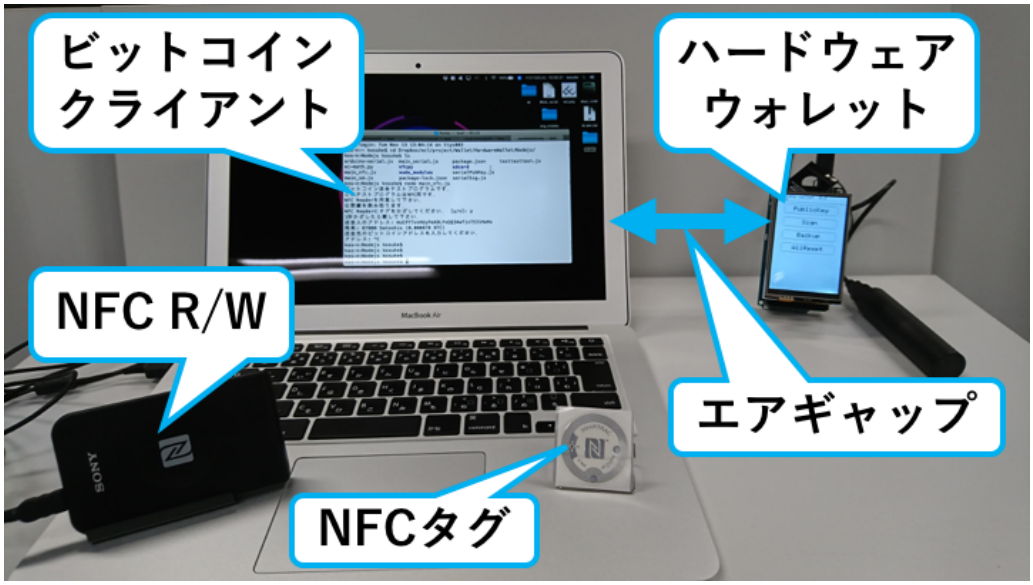

図 2: 実際に用いた実験機器

図 3 にブロックチェーンに組み込まれた *Tx* を示す．*Tx* はブロックチェーンに組み込まれており，提案手法の実装が正しいことが確認された．図 4 に 5 つの署名された *Tx* が *BC* で生成されるまでの時間を示す．X 軸は署名された *Tx* の数を，Y 軸は累計操作時間 (秒) を示し，各点は X 軸に対応する数の署名された *Tx* が生成された時点の累計操作時間を示している．5 つの署名された *Tx* を生成するまで，USB は 408.748 秒，microSD は 585.926 秒，NFC は 396.290 秒であった．1 つあたりの平均操作時間は，USB

は 81.749 秒，microSD は 117.185 秒，NFC は 79.258 秒であった．記憶媒体媒介方式において，microSD と NFC を用いたデータ通信の 1 人あたりの累計操作時間の差は 37.927 秒であった．NFC は microSD の 0.676 倍で通信できると確認された．

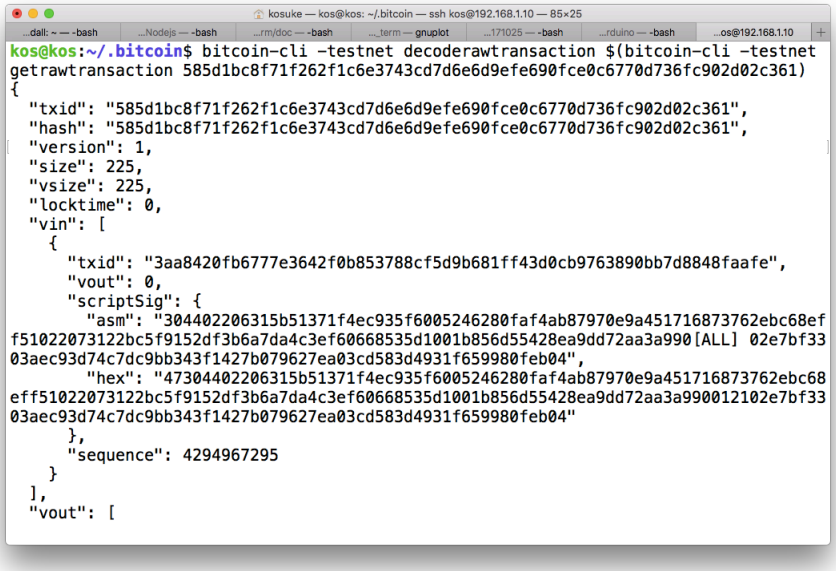

図 3: ブロックチェーンに組み込まれた Tx

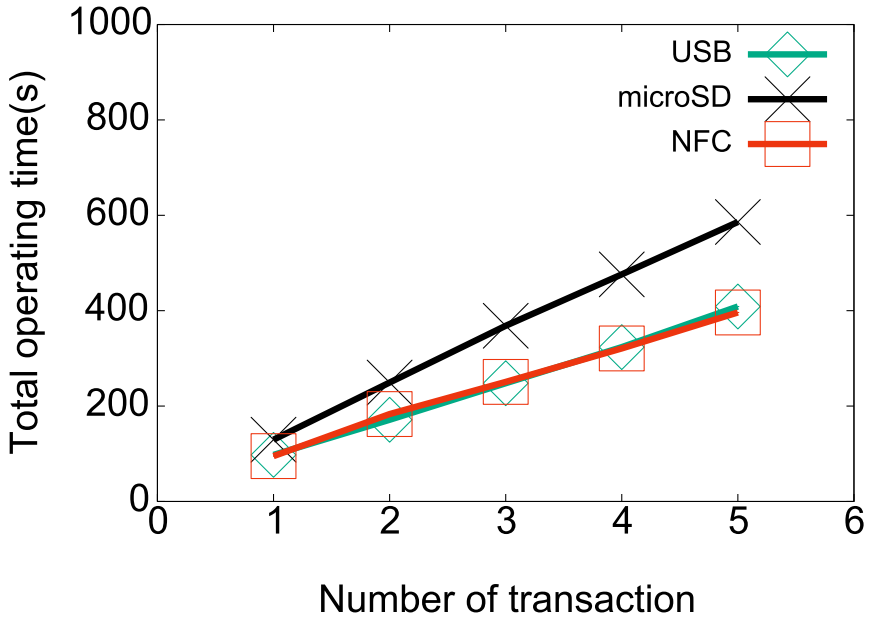

図 4: 5 つの署名された Tx が BC で生成されるまでの時間

3.2. HW の計算時間の計測

HW の処理時間は鍵の生成に 10.500 秒，署名に 4.159 秒要した．署名時は鍵の生成から行うので，累計 25.159 秒要した．処理時間にディスプレイ描画の時間も含めると鍵の生成に 13.400 秒，署名に 6.157 秒要し，累計 32.957 秒要した．処理時間とディスプレイ描画も含めた処理時間の差は 7.798 秒である．それぞれの 5 つの署名された Tx が BC で生成されるまでの平均操作時間からディスプレイ描画を含めた処理時間を引くと，USB は 48.792 秒，microSD は 84.228 秒，NFC は 46.301 秒であった．処理時間よりも操作時間に多くの時間を要していることが確認された．

4 . 結論

ビットコインウォレットの秘密鍵管理の安全性を保ちつつ，操作時間の短縮を目的として NFC を用いたデータ通信を提案した．そして，複数の BC で利用できるエアギャップ端末の HW を実装した．実験内容は 5 つの署名された Tx が生成されるまでの時間の計測である．NFC は microSD の 0.676 倍で通信できることを確認し，有効性を評価した．また，NFC の記憶媒体媒介方式はエアギャップであるため，秘密鍵管理の安全性は保たれた．また，階層的決定性ウォレットを用いることによって従来手法よりも秘密鍵管理の容易化を図った．今後は二重支払いを防止する Segwit の対応と HW と BC の操作方法の簡略化を図りたい．また，ウォレットの機能として，アカウントの判別方法の実装や UTXO の複数選択の実装を行う．

参考文献

[1] 森安 昭太, 森山 真光, “暗号通貨ウォレットの秘密鍵管理手法の提案と評価, ” 経営情報学会　全国研究発表大会要旨集, Vol.2017f, 2017, pp.55-58.

[2] Tejaswi Volety,Shalabh Saini,Thomas McGhin,Charles Zhechao Liu, Kim-Kwang Raymond Choo, “Cracking Bitcoin wallets : I want what you have in the wallets, ” Future Generation Computer Systems, Vol.91, 2019, pp.136-143.

[3] Marek Palatinus, Pavol Rusnak, “Multi-Account Hierarchy for Deterministic Wallets, ” https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki, 閲覧 2018-11-12