仮想通貨アドレスの真正性の検証
Verification of authenticity for virtual currency address

著者 1 高木豊* 著者 2 森邦彦** 著者 3 小田謙太郎**
(鹿児島大学 *理工学研究科 **学術情報基盤センター)

1 はじめに

2009 年よりビットコイン(Bitcoin)[1]が仮想通貨として運用を開始した. ユーザー数は年々増え続け全世界で 500 万人以上にものぼり, またビットコインの価値も他の仮想通貨に比べて大きく上回っており 1BTC は 8 月現在, 約 6 万円で取引されていて非常に高額(BTC はビットコインの単位で, 最小額は 0. 00000001BTC)である.

このビットコインだが, 実際に運用するとなると問題点が出てくる. ビットコインをやりとりする為にはユーザーは 58 種類の英数字の中から 26～35 文字で構成されているビットコインアドレスを受領者から送金者に教えなければならない. しかしインターネット経由で得られるビットコインアドレスは受領者から送金者に渡る間に第三者に改竄される可能性が考えられる. 本研究の目的は利用者が取引を安全に行う際に与えられたビットコインアドレスが取引先の人物の本物のビットコインアドレスであるかどうかの検証をするための方法を提案することにある.

これをビットコインアドレスの真正性の検証と呼ぶ.

2 外部状況

仮想通貨の中に BitShares[2]というものがある. この仮想通貨はビットコインアドレスのような 58 種の英数字によって構成されているのではなく, 人間にも読めるアカウント名を用いている. しかし改竄可能であるので仮想通貨アドレスの真正性を保証するには不十分だと考える.

また, ビットコインを管理するソフトウェア, 通称ウォレットというものがあり, Bitcoin-Core[3]を代表するそれらの中にはビットコインアドレスに自己署名をすることによって真正性を確保しようとしているものがある. しかしこれは署名が誰のものかわからないという点が不十分である.

3 提案手法

3. 1 提案手法1

提案手法を 3 つ提示する.

1 つ目は Public Key Infrastructure(公開鍵基盤)[4][5][6], 認証局設置によるビットコインアドレスが誰のものであるかの確認を行う手法である.

利点は認証局によって広い範囲でビットコインによる送金受領の保証をすることができる. これは後述する信頼の輪を用いた手法よりも範囲は大きくなると考えられる.

欠点としては手数料[7]の増加, 第三者機関の介入などでビットコインのメリットが薄れてしまうことである.

3. 2 提案手法 2

2 つ目は信頼の輪を利用して, ビットコインアドレスに問題がないことを友人や知人により証明してもらい, 正当なものであることを確認する.

利点は時間が経つ毎に拡大すると考えられ, それに伴い信頼できる取引可能な相手も増えていく. また, 先に述べた公開鍵基盤を用いた手法と違い手数料が必要ないのが大きな利点である.

欠点としては 1 つのビットコインアドレスに取引が集中して, 第三者から現在保有しているビットコインの総量を推測されるおそれがある.

3. 2 提案手法 3

3 つ目は最小額を本命の決済前に送金し, 現実世界で反応を返してもらい相手の確認を行う.

この方法の利点としては先に提案した 2 つの手法とは違い, 第三者を必要とせず一対一で取引を行うことができる点である. これはビットコインが持つ特徴である, 中央機関が存在せず一対一でやりとりを行える利点を損なっていない.

欠点は, この方法では相手の現実世界での反応による確認が必要なので物理的距離は近くなることである.

4 まとめ

本研究ではビットコインアドレスの真正性の判断に重点を置き, それを保証することによって利用者の利便性向上を目的とし, 解決のために 3 つの手法を提示した.

今後の課題としては, ビットコインのメリットを損なわせずに, 今回で提案された方法よりも汎用性の高い手法の構築が必要だと考えられる.

謝辞

本論文を作成するにあたりご指導, ご指摘を頂いた森邦彦教授, 小田謙太郎助教に深く感謝いたします.

参考文献

[1] Satoshi Nakamoto, “Bitcoin:A Peer-to-Peer Electronic Cash System” https://bitcoin. org/bitcoin. pdf
[2] BitShares : 入手先(https://bitshares. org/), (参照 2016-08-10)
[3] Bitcoin project, Bitcoin, BitcoinCore, 入手先 (https://bitcoin. org/ja/download), (参照 2016-08-10)
[4] 青木隆一, 稲田龍, 村井純 :PKI と電子社会のセキュリティ, 共立出版(2001/10/25)
[5] 牧野二郎, 日本ボルチモアテクノロジーズ, 城所岩生 : 電子署名のしくみとPKIの基本, 毎日コミュニケーションズ(2003/08)
[6] R. Hously, W. Ford W. Polk, D. Solo, “Internet X. 509 Public Key Infrastructure, Certificate and CRL Profile,” RFC 2459 1998.
[7] 日立 : 公開鍵基盤 PKI 価格, 日立製作所, 入手先(http://www. hitachi. co. jp/Prod/comp/soft1/pki/info/price/index. html), (参照 2016-08-10)