Reality of less trust than expected to trustless financial system

Yuta Takanashi[1,2], Shin'ichiro Matsuo[1], Pindar Wong[3], and Eric Burger[1]

[1] Georgetown University
[2] Financial Services Agency
[3] VeriFi Ltd.

Abstract. After the original publication of the Bitcoin paper [1], cryptocurrency exchange was born to connect the cryptocurrency world to fiat currency world. Although most persons believe that the cryptocurrency exchange plays the simple role of exchange, several security incidents raise a big question on the reality of the cryptocurrency exchange. That is, what kinds of operations are conducted, whats are the informational asset to be protected, and what kinds of security postures are required.
In this paper, we report the results of investigation of 16 registered and 16 quasi-registered cryptocurrency exchanges by Japanese regulators, then analyze the reality of functionalities, implementation and operations of real cryptocurrency exchanges. Then, we conduct analysis from the information security management system (ISMS) standard point of views, to clarify the required actions to secure the implementation and operation of cryptocurrency exchanges. They includes analysis on blockchain protocol, cryptographic key management, system security, and operation. We shows the current activities in IETF and ISO to have a common document on security of cryptocurrency exchange.
Keywords: Cryptocurrency exchange, Information security management, Standards

1 Introduction

1.1 Background

Eliminating the trusted party in realizing network based services is one of the biggest dreams in financial cryptographic research, hence this is the main subject in this world. The main reason why we seek to eliminate the trusted party is, it is too difficult to realize expected trusted party. Such difficulties are caused by operator's mistakes, malicious activities and collusion with other parties. Many cryptographic techniques like secret sharing scheme, threshold cryptography and multi party computation protocol are well studied to realize many network based services without trusted parties. The sentence, "An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." is the explanation of Bitcoin - one of the most attractive cryptographic protocols

- described in the original paper [1]. Bitcoin is the one of the most excellent cryptographic protocols which claimed to realize payment scheme among cryptographic protocols which try to eliminate the trusted party.

In spite of this attractive claim of Bitcoin, there is a fundamental assumption in the claim. That is, it holds only when the payment is conducted by Bitcoin, and no exchange to any other payment methods exits.

References

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *https://bitcoin.org/bitcoin.pdf*.
2. M. Sato, M. Shimaoka, and H. Nakajima, " General Security Considerations for Crypto Assets Custodians," *https://tools.ietf.org/html/draft-vcgtf-crypto-assets-security-considerations-02*
3. S. Matsuo and A. L. Castro (ed.), "ISO TR 23576: Blockchain and distributed ledger technologies – Security of digital asset custodians," under development, *https://www.iso.org/standard/76072.html*