Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography

Huaqun Wang, Debiao He, Yimu Ji

PII: S0167-739X(17)31350-X
DOI: http://dx.doi.org/10.1016/j.future.2017.06.028
Reference: FUTURE 3526

To appear in: *Future Generation Computer Systems*

Received date : 14 December 2016
Revised date : 10 April 2017
Accepted date : 25 June 2017

Designated-Verifier Proof of Assets for Bitcoin Exchange Using Elliptic Curve Cryptography

Huaqun Wang[1,2]

1. Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China
2. State Key Laboratory of Information Security,Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Debiao He

State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China

Yimu Ji[1,2,3]

1.School of Computer Science, Nanjing University of Posts and Telecommunications,Nanjing, China
2.Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nan-jing University of Posts and Telecommunications, Nanjing, China
3.College of Software, Nanjing College of Information Technology, Nanjing, China

Abstract

Based on the core technique of blockchain, bitcoin is designed for the first time. Bitcoin is a digital currency and a payment system. The blockchain is a digital ledger that records every bitcoin transaction that has ever occurred. The users' privacy is preserved in the bitcoin exchange by using the blockchain. In some application scenarios, it is important to show the buyer's assets strength in order to avoid the troublemakers. At the same time, it is also necessary to preserve the buyer's assets privacy. In this paper, we propose the novel concept of DV-PoA (designated-verifier proof of assets) for bitcoin exchange. Since bitcoin exchange's signature takes use of the elliptic curve cryptography, we design the first concrete DV-PoA scheme by using elliptic curve cryptography in order to be consistent with it. Then, we prove the security of the proposed DV-PoA scheme. After that, we analyze its efficiency from the two cases: theory and implementation. Our analysis shows that the designed DV-PoA scheme is