Information Sciences 509 (2020) 290–303

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Toward conditionally anonymous Bitcoin transactions: A lightweight-script approach

Lun Li[a,b], Jiqiang Liu[a,b,*], Xiaolin Chang[a,b], Tianhao Liu[b], Jingxian Liu[b]

[a] Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, 3 Shangyuancun, Haidian, Beijing 100044, China

[b] School of Computer and Information Technology, Beijing Jiaotong University, 3 Shangyuancun, Haidian, Beijing 100044, China

ARTICLE INFO

Article history:
Received 24 October 2018
Revised 5 September 2019
Accepted 9 September 2019
Available online 11 September 2019

Keywords:
Conditional anonymity
Bitcoin
Privacy-preserving
Internet of Things
Signature algorithm

ABSTRACT

Bitcoin is being explored for applications in various Internet of Things (IoT) scenarios as a peer-to-peer payment platform. However, security and anonymity problems exist with Bitcoin, which threaten vulnerable IoT facilities. This paper aims to achieve conditional anonymity inside Bitcoin transactions. We first propose an identity-based conditionally anonymous signature (ICAS) algorithm and then design a lightweight Bitcoin script scheme (named pay-to-public-key-hash-with-conditional-anonymity or P2PKHCA), which applies the ICAS algorithm to make conditionally anonymous Bitcoin transactions. P2PKHCA allows the identity manager to trace the real identity of users while preserving users' anonymity. Furthermore, P2PKHCA is backward compatible in terms of being able to work seamlessly with the existing Bitcoin script scheme pay-to-public-key-hash (P2PKH) in the Bitcoin network. We conduct a security analysis to verify the security features of P2PKHCA and employ a performance evaluation in terms of the cryptographic time and space costs by comparison with P2PKH. The simulation results demonstrate the effectiveness of P2PKHCA in reducing both time cost and data size.

1. Introduction

Currently, peer-to-peer payment [16] has played an essential role in various Internet of Things (IoT) systems, such as an electric vehicle (EV) charging network [19]. Anonymity is one of the basic IoT security requirements from the user's perspective. Using Bitcoin transactions as the peer-to-peer payment is promising and attractive in IoT scenarios because of its anonymity [6]. The past few years have witnessed broad applications of Bitcoin in online sale websites, offline products/energy companies [39,40], and precious metal dealing [1].

Notably, Bitcoin anonymity is controversial and needs to be enhanced in IoT. Although the blockchain-based networks usually claim to be self-anonymous, leveraging blockchain in IoT is somehow an exception, and its anonymity cuts both ways [11,27,35,36]. On the one hand, adversaries can make use of frequently dispersed Bitcoin addresses to construct destructive or problematic transactions that infest IoT applications, which makes it challenging to manage criminal activities (e.g., unexplained money laundering) [20,28]. On the other hand, users usually do not change their Bitcoin addresses periodically. Therefore, users are threatened by identity guessing in these IoT scenarios because physical sensors/devices often relate to the users' identities, which makes the currently controversial anonymous features in Bitcoin are difficult to work

* Corresponding author.
E-mail address: jqliu@bjtu.edu.cn (J. Liu).

https://doi.org/10.1016/j.ins.2019.09.011
0020-0255/

out. This threat is more serious in IoT trading systems connected with physical facilities, such as the vehicle-to-grid system [38]. Thus, a more secure conditional anonymity in the Bitcoin transaction is unsurprisingly demanding in those IoT scenarios.

For a further explanation of the necessity of improving Bitcoin's anonymity, we consider a scenario where a user is driving an EV. He/she prepares to use an unmanned charging pile to charge his/her car. He/she hopes to pay through Bitcoin since he/she does not want to expose himself/herself in an unacquainted location for security reasons. However, the provider company wants to ensure that the charging pile is not damaged, which requires the user to provide a real identity (e.g., the driving license number or the vehicle identification number) so that the provider can trace the initiator/attacker of the transaction and is prepared for the worst. The rapidly increasing number of IoT applications creates demands of solving the contradiction between users' privacy concerns and IoT companies that hope to guarantee the security of their facilities and capital sources.

Although new blockchain-based systems for solving security problems have been proposed (e.g., [5,23,37,42,43]), Bitcoin has nevertheless currently hit the highest market share by over 50% of the entire peer-to-peer blockchain-based trading [34], which highlights the necessity of balancing anonymity and tracing inside Bitcoin itself. Conditional privacy/anonymity has been explored to achieve anonymity while preserving the feature of tracing in various scenarios [15,26]. Currently, how to achieve conditional anonymity in Bitcoin is still an open question, especially in an unobtrusive way.

This paper aims to achieve conditional anonymity in Bitcoin transactions while preserving the transaction's security attributes. Conditional anonymity is defined as the fact that transactions of a user remain anonymous, but the transactions can be traced to obtain the real identity by the authorized third party (named the identity manager) in this paper. The authorized tracing can be used for future audits, dispute resolution, and so on. We design a Bitcoin script scheme in transactions, referred to as pay-to-public-key-hash-with-conditional-anonymity (P2PKHCA). It is a lightweight scheme with an easily applied script structure in Bitcoin transactions, including three types of scripts: locking, unlocking and tracing scripts. Compared to existing Bitcoin script schemes such as pay-to-public-key-hash (P2PKH), Additionally, P2PKHCA achieves conditional anonymity and traceability in IoT scenarios. Also, P2PKHCA preserves a series of security attributes in the existing Bitcoin script schemes. The attributes include identity privacy-preserving, transaction integrity, unlinkability, and modification resistance.

The major contributions from the perspective of the P2PKHCA scheme are summarized as follows:

- P2PKHCA can preserve the user's privacy through locking and unlocking scripts. In this paper, we propose a novel identity-based conditionally anonymous signature (ICAS) algorithm to generate new script values and new opcodes for P2PKHCA, including OP_CHECKCASIG, $<$pseudonym$>$, $<$PseHash$>$ and $<$casig$>$. Locking and unlocking scripts allow a user to generate a new pseudonym through a tamper-proof device in each P2PKHCA transaction. Therefore, identity guessing attacks can be effectively resisted.
- P2PKHCA can achieve identity traceability through the tracing script. With the new opcode OP_TRACEID in the tracing script, the identity manager traces the user's real identity from the unlocking script of a P2PKHCA transaction while the user is still anonymous to other users. Thus, the IoT payees are able to require P2PKHCA transactions for significant deals.
- P2PKHCA is backward compatible and can be compatible with P2PKH in the Bitcoin network.

We carried out a detailed security analysis of P2PKHCA. Additionally, simulations were conducted to evaluate P2PKHCA by comparison with the current widely used P2PKH. Performance evaluation indicates that P2PKHCA achieves good performance while also achieving conditional anonymity, demonstrating its practicality in the Bitcoin network. To the best of our knowledge, we are the first to make an improvement to Bitcoin script with an ICAS algorithm, aiming to enhance the privacy and traceability in Bitcoin script scheme. Note that P2PKHCA can also be implemented in those blockchain-based IoT networks that have the same specification as Bitcoin. For example, tracing criminal activities are required in wireless sensor networks[8, 12, 45] and financial systems for the risk management [42].

The remainder of this paper is organized as follows. Section 2 gives the preliminaries of the Bitcoin script scheme (e.g., P2PKH) and the other cryptographic primitives used in this paper. Section 3 presents a survey of related work. Section 4 presents the detailed scheme of P2PKHCA and detailed security analysis. Section 5 conducts performance evaluations and comparisons. Finally, Section 6 concludes this paper.

2. Preliminaries

This section first introduces fundamental preliminaries used in presenting the proposed P2PKHCA, including the general transaction structure in Bitcoin and the structure of the current Bitcoin script. Then, we present the combined public key algorithm related to the key management in our scheme.

2.1. Transaction structure in Bitcoin

In the Bitcoin network, the subject of a dealing system is the transaction. All transactions are in open record and formed as many transaction *flows*. Thus, the coin and balance of an account are just concepts without the data structures in Bitcoin.

The transaction structure of Bitcoin is composed of three main functional parts, namely the unique transaction identification (ID), transaction inputs, and transaction outputs. Each output and input contain a unique address, which is usually