

## Research Article

# BNRDT: When Data Transmission Meets Blockchain

Hongjian Jin<sup>1</sup>, Xingshu Chen<sup>1,2</sup>, Xiao Lan<sup>2</sup>, Hui Guo<sup>3</sup>, Hongxia Zhang<sup>1</sup>, and Qi Cao<sup>1</sup>

<sup>1</sup>College of Cybersecurity, Sichuan University, Chengdu 610065, China

<sup>2</sup>Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China

<sup>3</sup>State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

Correspondence should be addressed to Xingshu Chen; chenxsh@scu.edu.cn and Xiao Lan; lanxiao@scu.edu.cn

Academic Editor: Chenquan Gan

Copyright © 2020 Hongjian Jin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Data transmission exists in almost all the Internet-based applications, while few of them consider the property of nonrepudiation as part of data security. If a data transmission scheme is performed without the endorsement of a trusted third party (TTP) or a central server, it is easy to raise disputes while transmitting valuable data, especially digital goods, because a dishonest participant can deny the fact of particular data transmission instance. The above problem can be solved by signing and encrypting. However, digital signature schemes usually assume public key infrastructure (PKI), increasing the burden on certificate management and are not suitable for distributed networks without TTP such as blockchain. To solve the above problems, we propose two new schemes for nonrepudiation data transmission based on blockchain (we call it BNRDT): one for short message transmission and the other for large file transmission. In BNRDT schemes, nonrepudiation evidence of data transmission is generated and stored on the blockchain to satisfy both the properties of nonrepudiation (including nonrepudiation of origin and nonrepudiation of receipt) and data confidentiality. We implement and test the schemes on Hyperledger Fabric. The experimental results show that the proposed schemes can provide appealing performance.

## 1. Introduction

An overwhelming majority of Internet-based applications are inseparable from data transmission, may be short messages, videos, or even confidential government documents. In most cases (e.g., online chatting and video-on-demand service), data transmission processes rely on a trusted third party (TTP) or a central server, which acts as a data source (or a transmission relay station) and the security provider. With such a trusted platform, data security including confidentiality, integrity, authenticity, and even nonrepudiation when required are easily implemented. However, in some specific scenarios, such as P2P (Peer to Peer) digital goods trading, schemes are in lack of endorsements by trusted platforms; thus, nonrepudiation is no longer easy to achieve. Concretely, we consider that a digital goods seller needs to transmit the commodity over the Internet to an online buyer. Since the data transmission instance affects the parties' own interests, thus both the seller and the buyer want to ensure that the whole process can be

undeniable, if they are honest. In other words, the buyer cannot deny having received the data so as to refuse to pay for it, and the seller cannot deny having sent it to the buyer so as to refuse to refund or be responsible for it if any problem arises after purchasing.

Nonrepudiation services [1] have been introduced for a long time to prove the nonrepudiation of user behaviour including the case of data transmission, which can effectively solve the above problem. By now, many nonrepudiation approaches have been proposed, but most of the existing work on nonrepudiation is still based on trusted third parties [2–5]. Such TTP-based implementations usually offer higher efficiency but may suffer from single-point failures. Moreover, a proper TTP is usually not available in distributed environments. Non-TTP-based nonrepudiation approaches are traditionally implemented by increasing interactions between users and gradually releasing secrets [6–8]. However, this kind of technique always leads to lower execution efficiency and cannot provide fairness for every participant equally. Beyond that, with the rapid development of































