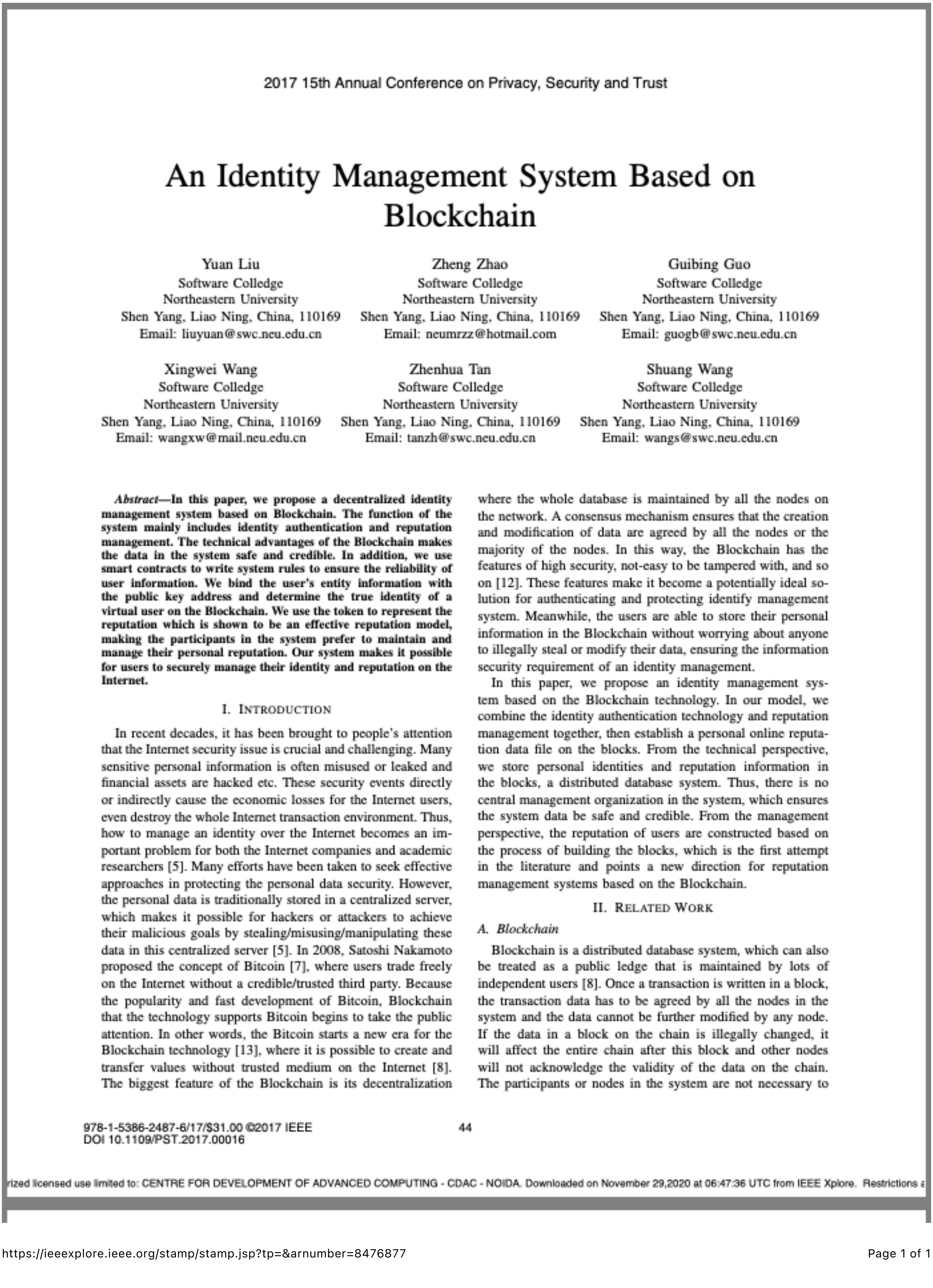

2017 15th Annual Conference on Privacy, Security and Trust

An Identity Management System Based on Blockchain

Yuan Liu
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: liuyuan@swc.neu.edu.cn

Zheng Zhao
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: neumrzz@hotmail.com

Guibing Guo
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: guogb@swc.neu.edu.cn

Xingwei Wang
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: wangxw@mail.neu.edu.cn

Zhenhua Tan
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: tanzh@swc.neu.edu.cn

Shuang Wang
Software Colledge
Northeastern University
Shen Yang, Liao Ning, China, 110169
Email: wangs@swc.neu.edu.cn

***Abstract*—In this paper, we propose a decentralized identity management system based on Blockchain. The function of the system mainly includes identity authentication and reputation management. The technical advantages of the Blockchain makes the data in the system safe and credible. In addition, we use smart contracts to write system rules to ensure the reliability of user information. We bind the user's entity information with the public key address and determine the true identity of a virtual user on the Blockchain. We use the token to represent the reputation which is shown to be an effective reputation model, making the participants in the system prefer to maintain and manage their personal reputation. Our system makes it possible for users to securely manage their identity and reputation on the Internet.**

I. Introduction

In recent decades, it has been brought to people's attention that the Internet security issue is crucial and challenging. Many sensitive personal information is often misused or leaked and financial assets are hacked etc. These security events directly or indirectly cause the economic losses for the Internet users, even destroy the whole Internet transaction environment. Thus, how to manage an identity over the Internet becomes an important problem for both the Internet companies and academic researchers [5]. Many efforts have been taken to seek effective approaches in protecting the personal data security. However, the personal data is traditionally stored in a centralized server, which makes it possible for hackers or attackers to achieve their malicious goals by stealing/misusing/manipulating these data in this centralized server [5]. In 2008, Satoshi Nakamoto proposed the concept of Bitcoin [7], where users trade freely on the Internet without a credible/trusted third party. Because the popularity and fast development of Bitcoin, Blockchain that the technology supports Bitcoin begins to take the public attention. In other words, the Bitcoin starts a new era for the Blockchain technology [13], where it is possible to create and transfer values without trusted medium on the Internet [8]. The biggest feature of the Blockchain is its decentralization where the whole database is maintained by all the nodes on the network. A consensus mechanism ensures that the creation and modification of data are agreed by all the nodes or the majority of the nodes. In this way, the Blockchain has the features of high security, not-easy to be tampered with, and so on [12]. These features make it become a potentially ideal solution for authenticating and protecting identify management system. Meanwhile, the users are able to store their personal information in the Blockchain without worrying about anyone to illegally steal or modify their data, ensuring the information security requirement of an identity management.

In this paper, we propose an identity management system based on the Blockchain technology. In our model, we combine the identity authentication technology and reputation management together, then establish a personal online reputation data file on the blocks. From the technical perspective, we store personal identities and reputation information in the blocks, a distributed database system. Thus, there is no central management organization in the system, which ensures the system data be safe and credible. From the management perspective, the reputation of users are constructed based on the process of building the blocks, which is the first attempt in the literature and points a new direction for reputation management systems based on the Blockchain.

II. Related Work

A. Blockchain

Blockchain is a distributed database system, which can also be treated as a public ledge that is maintained by lots of independent users [8]. Once a transaction is written in a block, the transaction data has to be agreed by all the nodes in the system and the data cannot be further modified by any node. If the data in a block on the chain is illegally changed, it will affect the entire chain after this block and other nodes will not acknowledge the validity of the data on the chain. The participants or nodes in the system are not necessary to

978-1-5386-2487-6/17/$31.00 ©2017 IEEE
DOI 10.1109/PST.2017.00016