International Journal of Digital Crime and Forensics
Volume 13 • Issue 1 • January-February 2021

Detection of Suspicious or Un-Trusted Users in Crypto-Currency Financial Trading Applications

Ruchi Mittal, Netaji Subhas Institute of Technology, New Delhi, India
https://orcid.org/0000-0001-6818-2355

M. P. S. Bhatia, Netaji Subhas Institute of Technology, New Delhi, India

ABSTRACT

In this age, where cryptocurrencies are slowly creeping into the banking services and making a name for them, it is becoming crucially essential to figure out the security concerns when users make transactions. This paper investigates the untrusted users of cryptocurrency transaction services, which are connected using smartphones and computers. However, as technology is increasing, transaction frauds are growing, and there is a need to detect vulnerabilities in systems. A methodology is proposed to identify suspicious users based on their reputation score by collaborating centrality measures and machine learning techniques. The results are validated on two cryptocurrencies network datasets, Bitcoin-OTC, and Bitcoin-Alpha, which contain information of the system formed by the users and the user's trust score. Results found that the proposed approach provides improved and accurate results. Hence, the fusion of machine learning with centrality measures provides a highly robust system and can be adapted to prevent smart devices' financial services.

KEYWORDS

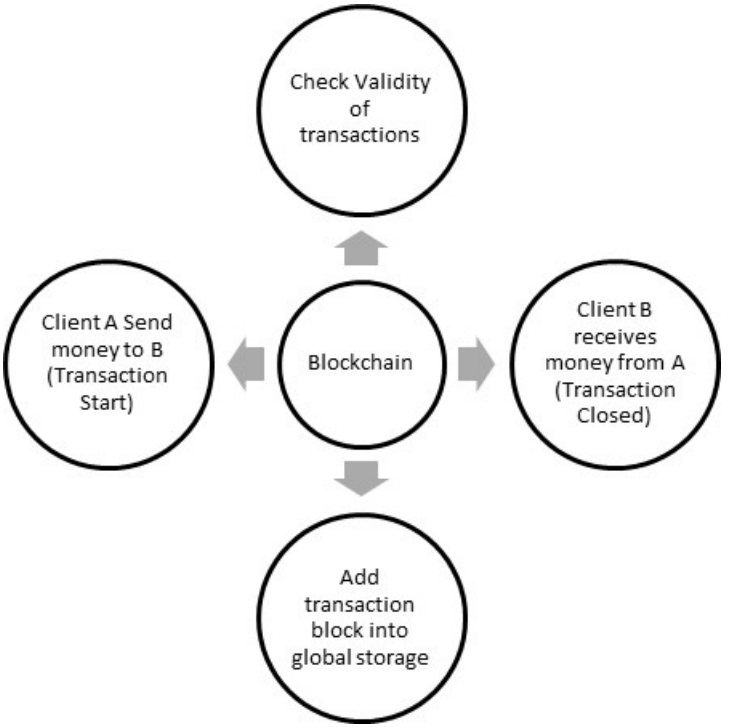
Anomaly Detection, Banking, Centrality Cryptocurrency, Deep Fraud Detection, Financial Services, Machine Learning, Random Forest, Security, Smart Devices, Social Network

INTRODUCTION

Due to advancements in technologies, online banking services via mobile applications and desktop applications hold continued growth among customers (Teutsch, Jain, & Saxena, 2016). This growth may increase the complexity of the banking system and raise security concerns among users. Also, there are many currencies exhibit in the real world, and each country has its currency, which again increases the complexity of the financial system (Sklavos, & Koufopavlou, 2005). To bypass the banking systems' complexity, a new type of currency came into the picture called cryptocurrency (Ahmad, Kumar, Shrivastava, & Bouhlel, 2018), which has no walls or boundaries and used globally anywhere in the world. The concept of cryptocurrency is new; it may raise security concerns when using mobile applications or desktop applications to prevent fraud and protect personal information.

DOI: 10.4018/IJDCF.2021010105

Figure 1. Cryptocurrency workflow



A cryptocurrency is a decentralized form of money compared to any central banking system. In this age, where cryptocurrencies are slowly creeping into the banking services and making a name for them, it is becoming crucially essential to figure out the security concerns when users make transactions. With the high instability of cryptocurrencies and highly competitive central bank currencies, most of the population is hesitant when investing in cryptocurrencies and skeptical of how to differentiate the trusted user, untrusted users. Cryptocurrencies are mainly working with blockchain mechanism, initially proposed by Satoshi Nakamoto in 2009. Satoshi Nakamoto named the proposed bitcoin (Schwartz, Youngs, & Britto, 2014) cryptocurrency. Figure 1 shows the basic workflow of the cryptocurrency using the blockchain mechanism. Here, client A sends money to B without the involvement of any other thirst party.

This paper investigates the untrusted users of cryptocurrency transaction services, which are connected using smartphones and computers. Though the cryptocurrency users are anonymous, it is necessary to maintain the users' reputation information to identify risky users.

As technology is increasing, transaction frauds are growing, and there is a need to detect vulnerabilities in such systems. Several types of risk exist in financial systems, such as hacking, fraud, password leak, and so on (Niu, Ji, & Tan, 2005). Various kinds of attacks can be conducted by attackers to breach smart devices' security and obtain illegal access (Upadhyaya, & Jain, 2016). Such as existing web pages are replaced with fraudulent web pages, broken firewalls for mobile apps using financial services, old desktop apps that are not updated with technologies, and encourage fraud security parameters. Many third parties are involved in financial services that may promote risks, Hackers, or un-trusted users. Hence, authors pick up one of such risks involved in the latest cryptocurrency financial system, i.e., identifying untrusted users from the networks. Such problems motivate us to find chances by collaborating with different domains to find the optimal and reliable