Chapter 7
Developing a Model to Highlight the Relation of Digital Trust With Privacy and Security for the Blockchain Technology

Subhodeep Mukherjee
GITAM University, India

Venkataiah Chittipaka
https://orcid.org/0000-0002-7804-0796
GITAM University, India

Manish Mohan Baral
Birla Institute of Technology, India

ABSTRACT

Digitalization uses digital technology to change a business model and provide new revenue models and value-producing opportunities. Blockchain is a type of database that stores various kinds of information in blocks that form a chain of information. It is one of the secured ways of transferring and storage of data. Blockchain is helping in creating trust for digitalization among its users. This research aims to study the impact of trust in blockchain by analyzing the privacy and security concerns that can impact the user attitude and its intention to the adoption process. For this structure, literature review is performed. Five variables are used, and they are attitude, privacy, trust, security, and intention. A questionnaire is developed for survey-based research in the software firms, banking sector, and digital marketing companies. For analysis, exploratory factor analysis and structural equation modeling are used. A model is developed that shows a good fit, and the parameters are satisfied.

DOI: 10.4018/978-1-7998-8081-3.ch007

INTRODUCTION

Over the last few years, blockchains (BC) have undergone exponential growth (Kshetri, 2018). BC applications range from healthcare, banking, transport, risk management, and media to public and social services, as BC goes beyond being just another buzzword (Grover et al., 2019). Addressing the security risks affecting BC seems to be the key to further development (D. H. Shin, 2017). The success of BC has been a critical problem in maintaining privacy and protection in BC (Du et al., 2019). There is an absence of exploration on security in BC, notwithstanding the expanding weakness issue, prompting a restricted comprehension of what security issues and trust mean for the BC experience. How many clients trust the administrations, cooperation's, and associations behind them becomes progressively critical as BC develops (Bancroft and Scott Reid, 2017). As clients collaborate with BC, they expect the merchandise they have paid to acquire, and their information won't be controlled (D. Shin & Ibahrine, 2020). Even though unmistakably trust matters in computerized settings, there has been an absence of explanation concerning what trust is, how it works/can be set up, and what advanced trust comprises. Various research has inspected client protection issues and firm assurance rehearses in a complex mechanical setting. It has stayed obscure how parts of protection/security influence an individual's psychological acknowledgment measure in the advancing BC setting (Casino et al., 2019). BC innovation is crucial for security and protection since it can work without an affirmed outsider. BC security issues are firmly associated with protection worries in BC (Kshetri, 2018). It isn't put away in an isolated area, while dispersed record innovation is scrambled. Firms don't have complete oversight over the subtleties. User data could be diverted via several servers when stored in BC due to this decentralized structure (Coita et al., 2019). In a BC, data is vulnerable, and other entities in the chain may access it. When information is deliberately or erroneously encrypted before being sent to a chain, no one can access it unless decoded (Fortuna & Risso, 2019). BC transactions are vulnerable to hacking through chain nodes, despite privacy-enhancing technologies. For this study, five variables are being used and they are attitude (AT), privacy (PR), trust (TR), security (SEC), and intention (IN).

The research questions that will be addressed are:

RQ1: Is BC addressing the trust issues of the users.
RQ2: How much secured is the usage of BC?
RQ3: Whether BC is providing privacy to its users?