The Effect of Blockchain Security on Intention to Use

Introduction

Bitcoin, or cryptocurrency, has been one of the most wanted products (DeVries, 2016). The trend of bitcoin in the world market has allowed its investors to ask for more (DeVries, 2016). The cryptocurrency is powered by Blockchain technology. Blockchain was first introduced in 2008 by Satoshi Nakamoto. The main purpose of blockchain is to prevent financial institutions to interfere with transactions. It is almost like a public ledger that everyone knows but does not know the details of the said ledger. It works by using encryption and peer-to-peer networks. The encryption method is similar to that of RSA. The user is given a public key and private to encrypt and decrypt the blockchain. Whenever a user is trying to make a transaction, it uses the public key of the user to encrypt the information. The information stored in the blockchain may include information of previous hash, amount of money being sent, the receiver's name, and the transaction timestamp. All of the information is then encrypted into a jumble of letters and numbers and can be used for the next transaction. As the name suggests, it is all linked transactions between users in the web of the ledger. To verify that the previous hash has not been tampered with, blockchain checks other's previous hash. If the previous hash of the current transaction is equal to the previous transaction, then it is considered that it is correct. If it does not equal the previous transaction's hash, then it fails to confirm that the previous hash is valid (Nakamoto, 2008). The problems with blockchain are that it would eventually run of space for transactions and encryption, all data is vulnerable when things go wrong, and it is not protected against hacking.

Transactions need to be kept to prove proof of work. The hash needs to be stored somewhere in the user's device as proof for future transactions (Nakamoto, 2008). The transactions that are run by the consumer may hit the limit of the storage capacity of the device of their choosing. Transactions would be too huge for some to keep using the cryptocurrency. Although they may purchase a new device, the question arises as to what happened with the recent transactions of users. It verifies the hash to continue with future transactions. The loss of previous owner's transactions may result in the disoriented ledger and have holes or gaps that do not allow further back into the ledger. Nakamoto's (2008) proposed solution is to use Merkle Tree. Once the hash is buried deep enough, there is no need for that information so the user can save space. The problem with the proposed solution is that the recent hash will no longer be available. The data must be backed up in a device to ensure that in an unforeseen event, there is a way to save the transactions held by the users.

The data is always vulnerable if blockchain technology fails to keep up with new technologies. Shortly, there may be a way to get around the current encryption method. It is most unlikely that

it will happen but if it did then there must be a way to protect the data. A malicious code can be sent to data in the form of valid data and it can cause loss of a huge amount of sum.

Technologies are vulnerable to hacking. With zero-day vulnerability, no one can know if the system can be breached. The CIA triangle of cybersecurity further explains how systems can be vulnerable (Nweke, 2017). The CIA triangle, or Confidential, Integrity, and Availability triangle claim that no system will have all three of these. If the system is mostly focused on Confidential, the users might find it difficult to access necessary information. The same goes for Integrity, Integrity might be the highest value of a system but it might lack Confidentiality or Availability. Each company has different values and aspects but when it comes to security, they choose for their data to be secure as possible by minimizing pivotal points of entry and maximizing the availability for users. A company's needs for its networking system or overall system can be determined by using Authentication, Authorization, and Accounting (AAA or triple-A) (Nweke, 2017). Each part of AAA corresponds to

The purpose of this study is to find the correlation between blockchain security and its intention to be used. With knowing the perceived risk, the consumer ought to be able to determine if blockchain can be trusted or not. The security of the blockchain of each company might not be publicly available but the base design was from (Nakamoto, 2008). The simple design can then be elaborated into a grander design that can protect people. By having a basic understanding of blockchain security and system, the question arises as to what extent does blockchain security can influence the intention to use?

Theoretical Background

This paper will use the Theory of Reasoned Action (TRA) and Social Exchange Theory (SET) to find the correlation between intention to use and blockchain security. Expectation-Confirmation Model (ECM) can be used, however, ECM is focused on predicting the entity or service use (Anderson & Sullivan, 1993). Technology Acceptance Model was not used because it does not provide a framework for finding security and intention to use. It finds, however, perceived usefulness toward the behavioral intention to use (Albayati et al., 2020). TRA, on the other hand, proposes the idea that the user's reasoning might contribute to the intention to use. Social Exchange Theory (SET) finds the effect of influence towards intention to use (Shin, 2019). Thus using TRA and SET is effective because one can determine the intention to use through the factor of system's security or blockchain security. Moreover, the SET contributes to the attitude of the consumer being influenced by outside factors (Shin, 2019). The knowledge before an examination will contribute greatly to finding the correlation between attitude and intention.

Proposed Research Model and Research Hypothesis

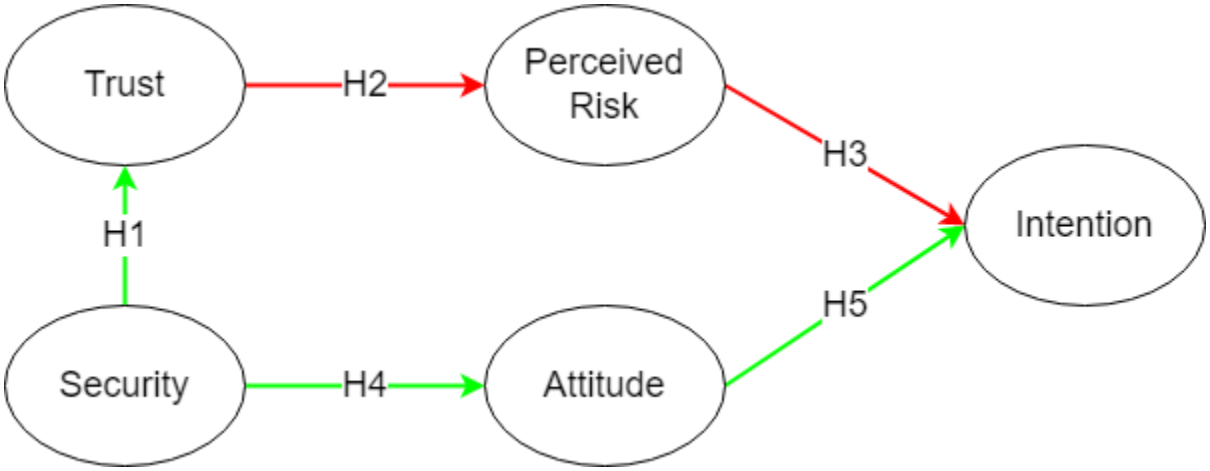

Figure 1. Proposed Research Model

As blockchain technology progress into Research and Development, it is bound to be vulnerable at some point. With the international market being interested in cryptocurrency, it ought to find itself to be improved so that it can be used internationally. Through the security of blockchain, the attitude and trust of consumers will greatly affect the intention to use.

Security

The concern of blockchain technology is mostly about its security. The security refers to the ability to protect its consumers' information and the product that they are sharing. The bitcoin can be cracked through a powerful computing power (Lin & Liao, 2017). However, the security of blockchain help ensure the safety of consumers. Users would want to have a safe platform that can protect itself from any attack while ensuring that bitcoin has a value. The use of security can be influenced by outer factor that can cause security to positively or negatively affect other factors and so the SET was used to asses the idea of outer factors.

H1: Consumers' perceived security will positively influence their trust in the blockchain.
H4: Consumers' perceived security will positively influence their attitudes towards the use of blockchain technology.

Trust

User's trust rely on the interaction between the blockchain and the user (Shin, 2019). Even though blockchain does not require a middleman, it still requires trust that the value of bitcoin would be equal of the value it give. Like how the citizen trusts the government that the value of a paper is equal to the labor given. Trust have a relation with perceived risks as the user have to weigh the benefits and the risks when trusting a service. Users who trusts system easily does not check for any authentication that the system is fake (Shin, 2019).

H2: Consumers' trust will negatively affect their perceived risk of a transaction.

Perceived Risk

The risks needs to be verified before using a service due to information gathering by large companies. Thus resulting consumer to be being hesistant when it comes to online transactions. The perceived risks of blockchain can negatively affect the intention to use due to consumer being well aware of scenarios that can possibly happen. Perceived risks is often seen as negative because it brings consumers doubt about a product (Shin, 2019).
H3: Consumers' perceived risk will negatively affect their intention to use.

Attitude

User Attitude on blockchain is based on their perception of blockchain and outside factors. Therefore influencing the intention to use of blockchain (Shin, 2019). TRA expands on the relationship between attitudes and action (Shin, 2019). The user evaluation contributes to the attitude but is not used because it's a prefactor of attitude and does not focus on the subject of security towards the intetion to use. The application of attitude contributes to the intention to be used by allowing consumers viewpoint to affect their intent. The attitude of consumer on new product can be positive but with past experience with companies it might be negative. The attitude have an influence on the user intent to use a technology.
H5: Consumers' attitudes toward blockchain technology have a positive influence on their intention to adopt the blockchain.

References

Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. *Technology in Society*, 101320. https://doi.org/10.1016/j.techsoc.2020.101320

Anderson, E. W., & Sullivan, M. W. (1993). The Antecedents and Consequences of Customer Satisfaction for Firms. *Marketing Science*, *2*, 125–143. https://doi.org/10.1287/mksc.12.2.125

DeVries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal of Business Management and Commerce*, *1(2)*, 1–9.

Ham, J. V. D. (2021). Toward a Better Understanding of "Cybersecurity." *Digital Threats: Research and Practice*, *3*, 1–3. https://doi.org/10.1145/3442445

Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19(5)*, 653–659.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal*, *6*, 1–2.

Shin, D. D. H. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, 101278. https://doi.org/10.1016/j.tele.2019.101278