# ENHANCING CYBERSECURITY THROUGH BLOCKCHAIN TECHNOLOGY

**Joseph Meynard G. Ogdol**[1]
*https://orcid.org0000-0003-3149-1183*
*meynard@nmsc.edu.ph*

**Bill-Lawrence T. Samar**[2]
*https://orcid.org/0000-0002-2240-9929*
*bill.samar@nmsc.edu.ph*

[1,2]Northwestern Mindanao State College of Science and Technology
Tangub City, Misamis Occidental, Philippines

**Charmalyn Cataroja**[3]
*charmdum@yahoo.com*
Zaria International, Inc.
Chicago, USA

## ABSTRACT

*Centralized server systems have been popular in the industry of modern IT services. It allowed the deployment of various large-scale applications to aid the needs of the modern society. However, centralized systems have been common targets for cyberattacks and the need to explore novel ways to secure our systems has always been of utmost importance. As a response, this paper explores the applications of Blockchain Technology to the Cybersecurity paradigm specifically on Phishing attacks. A simulation has been conducted to test the effectiveness of an application that implements a blockchain. A combination of 998 randomly generated phishing messages has been fed to a simulation environment for the application. The results of the simulations show that out of 998 randomly generated phishing messages, a prevention rate of 100% has been performed by the application that implements a blockchain. The study, therefore implies that the blockchain technology is a very viable option to improve Cybersecurity aspects of modern information systems.*

***Keywords:*** *Blockchain, Cybersecurity, Phishing Attack, Hash, Cryptography*

## 1.0 Introduction

Ensuring Cybersecurity is a critical aspect that needs to be addressed in modern computing technologies found in various contexts. Due to the society's prevalent reliance and usage of electronic information systems, implementing solutions to improve the robustness of existing information systems is key to maintaining the stability of day to day computing transactions. According to a study conducted by Hong (2012) Phishing is one of the top most common yet prevalent threats to Cybersecurity. Phishing is a form of cyber-attack wherein an attacker

impersonates credible companies and or institutions by replicating legitimate e-mail messages, instant messages and or websites in an attempt to expose sensitive data from victims such as usernames, passwords, credit card information and others. Blockchain is a common distributed ledger that facilitates recording and tracking of transaction that can be traced back in 1976 on a paper published by Diffie entitled "New Directions in Cryptography". Systems that use blockchain utilizes a network of several nodes wherein each member of the network has access to the latest copy of an encrypted ledger so that they can validate a new transaction.

Existing studies showed that 50 percent of phishing is done through email (Vishwanath, 2011). It was also found that banks and card issuers in the U.S. had indirect losses of an amount of $1.2 billion in 2003 when approximately two million users gave information to spoofed websites (Litan, 2004). On the other hand, studies to improve data security states that Blockchain technology can be used to store an important piece of data in a secure way as long as it implements a relatively numerous number of nodes (Matanovic, 2017). It is also claimed that any application that implements a Blockchain builds trust in distributed systems and ultimately promote cyber peace (Shackelford, 2017). Instead of saving your data in a Cloud Based Data Center, Blockchains are able to provide the same service while enhancing the security aspect (Kshetri, 2017).

Based on the literature review conducted during the conduct of this study, it was found that works related to the field of Blockchain Technology directed to Cybersecurity has been explored by other authors. On the works of Ahram et. Al (2017) surveying the applications of Blockchain Technology, it has been found that blockchain technology has the potential capability of securing various paradigms such as the IoT *(Internet of Things)*, Social Media Networks and other industry paradigms apart from computing such as Healthcare, Finance and Marketing. This is supported and indirectly confirmed by Kropela et. Al (2017) which explored and successfully applied the blockchain technology in digital supply chain systems while taking interoperability into account. The latest study by Tischhauser et. Al (2018) applied blockchain technology in the paradigm of cybersecurity intrusion detection, and have found that blockchain technology is applicable for the purpose of intrusion detection.

Synthesizing upon the given background on the blockchain technology through a literature review, it can be safely implied that although the applicability of blockchain technology has been proven in a wide a array of practical applications including cybersecurity. There has not been an actual test or at least a simulation conducted to test the effectiveness of blockchain technology. In order to address the identified gaps, this paper incorporates the methods in Blockchain Technology in an attempt to further enhance Cybersecurity by improving existing procedures to prevent phishing and enhancing data security and integrity.

## 2.0 Conceptual Framework

This study is anchored on the Blockchain Theory, which states that it is an unchangeable digital ledger of transactions that can be used to record not just financial transactions but everything of a value (Tapscott et. Al, 2016). With this claim, it is implied that the same Blockchain technology may be used to secure systems from phishing. Therefore, to test the theory for its capability to enhance Cybersecurity, the conceptual framework illustrated in figure 1 will be used to guide the methodology of this study. An electronic message will be fed into a hashing algorithm which produces a fixed length hash that is unique to reduce the size of the message, the message will then be added to the blockchain together with a private key provided by the legitimate user in order to allow other users to confirm the authenticity of the message. After a new message has been added to the blockchain, a unique hash ID will be produced and be embedded to the final message to be sent to the recipient of the message.

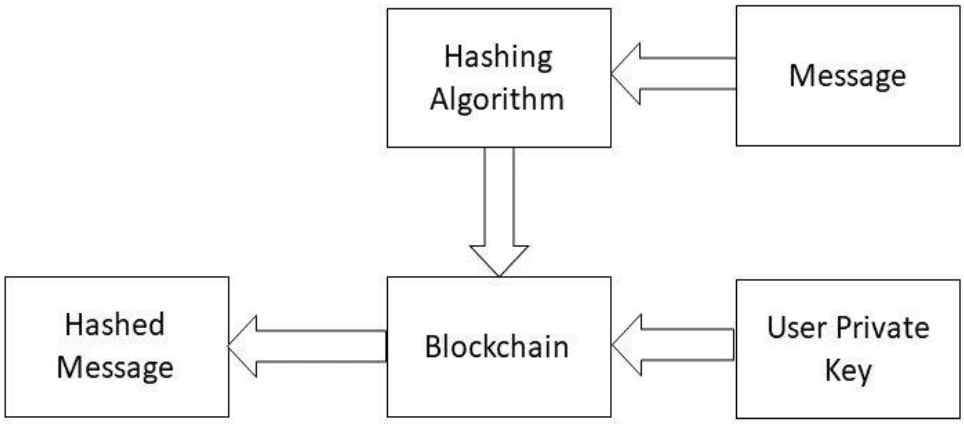


**Figure 1: Conceptual Framework**

In the setting of this study, the message is the raw and unsecured data to be processed which can be in the form of emails or instant messages. To process the unsecured data, a hashing algorithm will be utilized, a Hashing Algorithm is defined as a cryptographic algorithm that processes data and returns a unique series of characters representing the data, several hashing algorithms exist which provides different levels of security having different processing power requirements. Hashes are widely used as a mechanism to sign text files or data files to prevent tampering. To supply authenticity to each message, users are mandated to give a Private Key to be used by the Hashing Algorithm. The user's Private Key is a unique key that is only known by the user and is used to encode the message, it is found to mathematically

irreversible using the resulting hash message. After securing the message, it is appended to the blockchain and spread to other blockchain networks. The Blockchain is a constantly growing list of records called blocks which is linked and secured by hashes using cryptography based on available hashing algorithms. A hashed message is the output of the newly created block in the updated blockchain where in every created block will have a unique hash id to be appended to the final message before it will be sent to its recipient. Although cryptography has its drawbacks, this study includes the selection of a hashing algorithm that proves to offer the highest degree of security against hacking.

## 3.0 Research Methodology

*Research Design*

This study utilizes a descriptive method and a programming simulation. A Mersenne Twister pseudorandom number generator by Matsumoto, et. al (1997) will be utilized to randomly determine whether the test code would generate a valid or an invalid message simulating a phishing attack.

*Research Method*

A selection process has been done to identify a hashing algorithm that is suitable for the blockchain implementation. A number of hashing algorithms have been benchmarked for security based on the number of hash possibilities and hash complexity an algorithm is able to produce. The selection process has identified the SHA256 algorithm as a suitable hashing algorithm for the blockchain implementation. A computer simulated environment is then developed to simulate legitimate and phishing email senders and email receivers. The development used the Javascript as the base runtime environment for the simulation for a less language technical and straightforward code implementation of the simulation. The simulation is used to test the concept of this study applying blockchain to detect phishing content. Upon executing the simulation for a number of 2000 iterations, the results of the simulation program are then logged to measure the performance of the block chain concept applied to protect against phishing.

## 4.0 Results and Discussion

Depicted on the screenshot shown on figure 2, is the successful processing of adding blocks to the blockchain. Each line on the command line interface (CLI) represents adding a new block in the blockchain. Each block is composed of a public key, timestamp, hash of the message, a hash of the previous block, and a hash that points to the next block. The blockchain will be used as a reference to detect simulated phishing attacks fed into the simulation environment. In analogy an added block

represents a single email, and or chat message that is secured by a SHA 256 hashing algorithm.


*Figure 2. Adding Blocks to the Blockchain*

After the successful insertion of a new Block, theBlockchainn is tested by feeding a randomly generated collection of both legitimate and phishing messages. The setup simulated blockchain worked as expected, detecting the legitimate and phishing messages through the hash algorithm used in the blockchain. The execution of the message verification is shown below in figure 3.


*Figure 3. Verification of messages simulation*

Depicted on the pie chart shown on figure 4, out of 2000 iterations 985 or 49.25% valid messages as legitimate messages were generated by the test environment leaving 1015 or 50.75% invalid messages as phishing attacks.

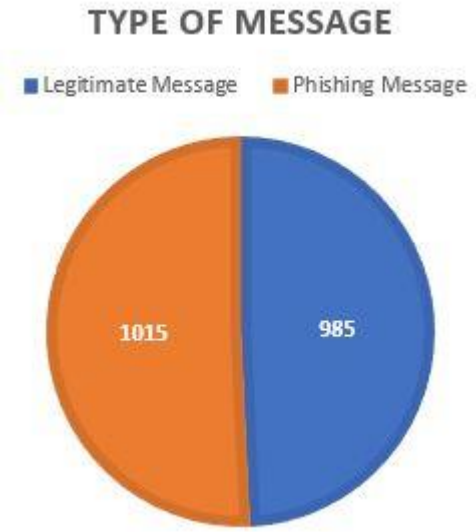


*Figure 4. Randomly generated types of messages*

Out of 1015 simulated phishing attacks, 1015 were intercepted and prevented. Based on the conducted simulation, it is found that by applying the blockchain technology, 100% of the simulated phishing attacks have been detected and prevented by the system. Safely, within the context of this study it is assumed that the theory of Tapscott et. Al, 2016 is accepted as the blockchain technology effectively performed its task of phishing detection. Thus, the technology can be applied to various facets including the problem of phishing in cybersecurity.

## 5.0 Conclusion

Results revealed that the blockchain technology is a viable option to improve Cybersecurity aspects of modern information systems. Depending on the scale and context of the target system, blockchains can be used widely for a variety of decentralized or peer-to-peer systems. Although, the study confirms the theory of Tapscott (2016), further development on the technical implementation of the blockchain technology may be integrated resulting in an increased of bandwidth usage of the proposed e-mail server platforms during the distribution of the updated ledger. However, there is a slight delay on the distribution of the emails

**References:**

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In Technology & Engineering Management Conference (TEMSCON), 2017 IEEE (pp. 137-141).

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?.

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In ECIS (p. ResearchPaper153).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590). ACM.

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. In proceedings of the 50th Hawaii international conference on system sciences.

Litan, A. (2004). Phishing attack victims likely targets for identity theft.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. Ieee Access, 6, 10179-10188.

Pilkington, M. (2015). Blockchain technology: principles and applications. Browser Download This Paper.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586.