A Literature Survey on Improving Sapiens Chain: An Improved Blockchain-based Cyber-security Framework

Ahubele, Betty O.
Department of Computer Science,
University of Port Harcourt, Nigeria
Email:betty4diamond2019@gmail.com

Abstract - The constant usage of the internet has necessitated the need to improve current cyber-security frameworks. This is because; majority of the current cyber-security frameworks are still vulnerable to cyber-attacks, and also lack trustable measures. In this paper, we addressed the aforementioned issue through a blockchain-based approach termed as an improved Sapiens Chain. Our approach encompassed an in-depth illustrative model on how Sapiens chain can be improved for a more robust cyber-security framework.

Index Terms -: Blockchain, Cyber-security, Sapiens Chain

1 INTRODUCTION

Cyber-security is a unique concept which involves protecting a computer system from theft, malicious hack, hardware damages, and disruption or misdirection of the services they provide. According to [1], [2], [3], [4]; the Sapiens Chains cyber-security framework can protect the privacy of an anonymous user in order to ensure immutable transactions and provision of decentralized and trustable services.

Furthermore, transactions between parties in present approaches are usually carried out in a centralized form which requires the participation of parties that are trusted. This could create serious security issues such as single point of failure and high transaction cost. Distributed ledger technology emerged to tackle these issues by allowing un-trusted parties to interact with each other without the need for a third-party intermediary. Distributed platforms have attracted a lot of attention from individuals, commercial organizations, national and international institutions, thereby enhancing the possibility of securing record of information in a distributed way. Building on this, it is highly possible to construct distributed databases and also to record the results of transactions that have financial value, especially in crypto-currencies.

Ledger technologies have numerous applications which encompass finance, medicine, data sharing and anti-money laundering. Furthermore, another importance of a DLT (Distributed Ledger Technology) is the ability to create trust in an untrusting ecosystem.

Blockchain's inherently decentralized nature makes it the perfect technology for cyber-security. The ledger technology has virtually endless uses in everything from medical and financial data sharing to anti-money laundering monitoring and encrypted messaging platforms. This process creates trust while also maintaining a high level of data integrity. In essence, the distributed nature of blockchain provides no "hackable" entrance or point of failure that detrimentally exposes entire datasets.

2 CHARACTERISTICS OF BLOCKCHAIN

[10] listed the following blockchain characteristics which include:

i) Decentralization:

In conventional centralized transaction systems, each transaction needs to be scrutinized through a centralized trusted party e.g., the central bank. With decentralization, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network.

ii) Persistency:

This is a unique blockchain feature in which transactions can be scrutinized and accessed by means of a centralized trusted party. Invalid transactions within the blocks could be discovered immediately. Persistency refers to the inability of deleting or altering (rollback) the transactions after they are recorded in the ledger.

iii) Anonymity:

This is a process where users communicate with the blockchain through a given address that hides the real user's identity.

iv) Auditability:

Specified by [11] enables the storage of information about user balances that relies on a model identified as unspent transaction output. Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. Auditability in the sense of public availability of the blockchain helps to verify and trace all previous transactions

Figure 2.1 is an illustration of how blockchain works.

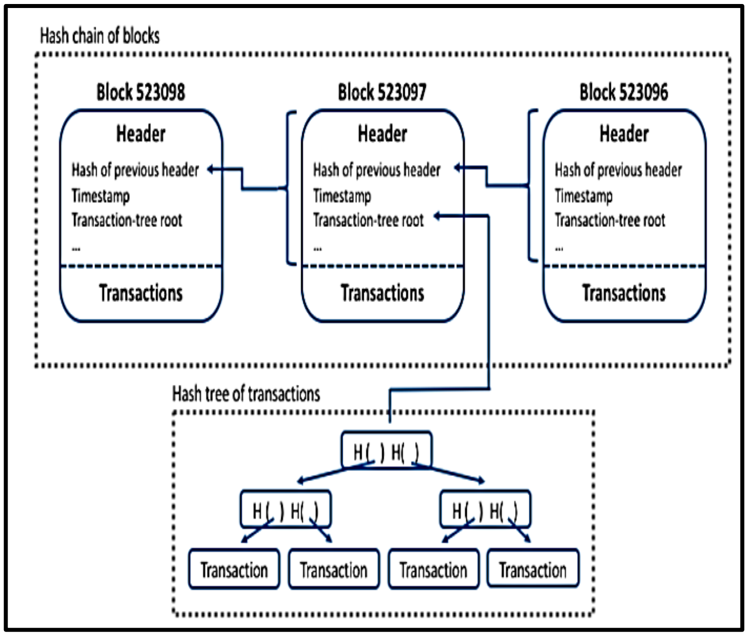

Fig. 2.1: Illustration of how blockchain works
(Source: [12])

2.1 Current Implementation Issues associated with Blockchain

Blockchain technology has great potentials for the construction of future Internet systems. However, it has been faced with a lot of technical challenges. A similar study by [13] identified some quality issues such as security, privacy, size and bandwidth, performance, usability, data integrity and scalability that affect the implementation of blockchain.

It was revealed that the Blockchain has a possibility of 51% attack. In such a case, one miner can have full control of the majority of the network which is a serious problem.

[14] also analyzed cases of breaches in security that took place in bitcoin. Furthermore, continuous testing strategy can be applied to block chain technology in order to ensure reliability and security of the software. Such blockchain quality improvement were recently presented by IBM [15]

In the same perspective, [16] highlighted one of the biggest challenges such as data storage capacity limitation which is prevalent in the current Blockchain implementations.

3 OVERVIEW OF SAPIENS CHAINS

Sapiens Chain is a decentralized security detection platform, including the decentralized vulnerability platform and the automatic vulnerability detection system (figure 3.1). It contains two kinds of nodes which are the ordinary nodes and fog nodes respectively [5],[6],[7][8][9]

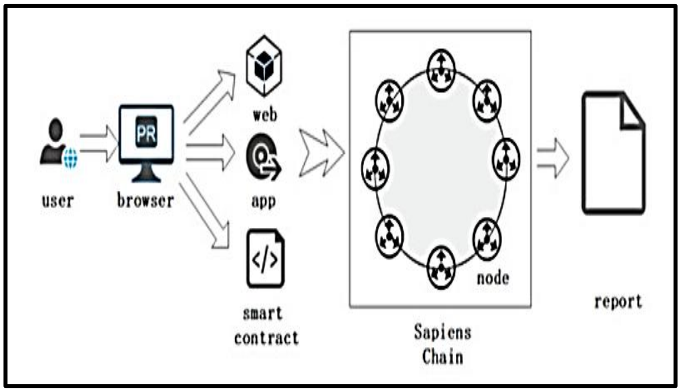

Fig. 3.1: Sapiens Chains Overview
(Source: [1])

The computing nodes of the Sapiens Chain are decentralized and thus each node won't be affected by others. The users submit their tasks including website tasks, application tasks, and smart contract tasks through the browser, the fog nodes in Sapiens Chain first distinguish the type of the task, and then segment tasks into several parts, running the algorithms to select proper nodes to deal with the task, and finally gather the results into a report.

3.1 PROPOSED IMPROVED SAPIENS CHAINS

Our approach for improving the existing system encompasses the addition of an enhanced verifier platform that uses multimodal biometric technique (see figure 3.2). The need for the improvement is due to the fact that smart contracts testing are complicated because of the critical nature of applications and its immutability if deployed on a blockchain. Secondly, manual test generation is likely to form an important component but inevitably is limited; there is a need for effective automated test generation and execution techniques.

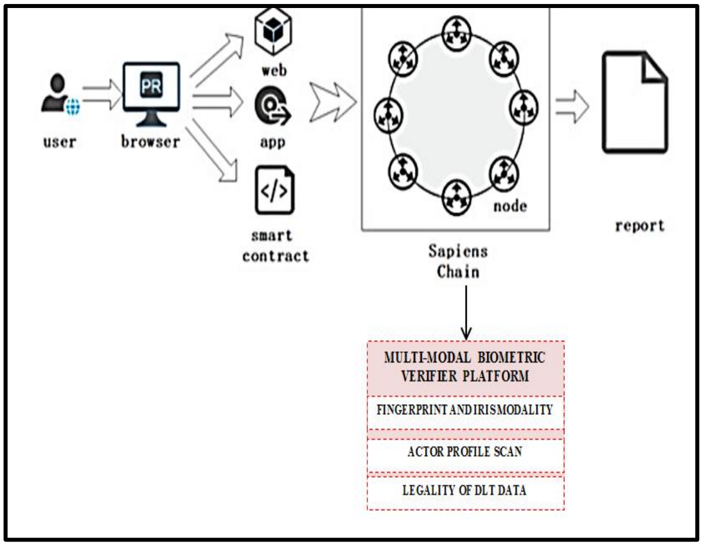

Fig. 3.2: An Improved Sapiens Chains Overview

From figure 3.2, our proposed improvement will aid efficient and robust verification process that relies on a hybridized biometric process which includes fingerprint and iris technology. Furthermore, there are other sub-components such as actor-profile scan and legality of the shared DLT (Distributed Ledger Technology) data. The actor-profile scan involves verifying the profile of the actors when there is suspicion of any actor with malicious intent in the system. In addition, DLTs are backed-up by certain ethics and conditions. Hence, the legality of DLT data is a unique platform that also verifies whether any shared transaction does not compromise the existing ethics and condition.

4 CONCLUSION

In this paper, we proposed an Improved Sapiens Chains Blockchain-based framework for cyber-security.

The importance of multimodal biometrics to distributed ledger systems encompasses verification and security. The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geo-spatial continuum from set of acquired data.

In addition, a homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

5 REFERENCES

[1] Yu H. (2018), Sapiens Chains: A Blockchain-based Cybersecurity framework,https://airccj.org/cscp/ vol8/csit89509.pdf

[2] Zhongru W. (2018), Sapiens Chains: A Blockchain-based Cybersecurityframework, https://airccj.org/cscp/ vol8/csit89509.pdf

[3] Qiang R. (2018), Sapiens Chains: A Blockchain-based Cybersecurity framework,https://airccj.org/cscp/ vol8/csit89509.pdf

[4] Binxing F. (2018), Sapiens Chains: A Blockchain-based Cybersecurity framework,https://airccj.org/cscp/ vol8/csit89509.pdf

[5] Jinyu S. (2018), Research on CRO'S Dilema in Sapiens Chain: A game Theory Method, Natarajan Meghanathan et al. (eds): DaKM, SIPP, CCSIT, NCWMC – 2018, PP 113 – 122, 2018 © CS & IT-CSCP 2018, DOI: 10.5121/CSit.2018.81508

[6] Zhongru W. (2018), Research on CRO'S Dilema in Sapiens Chain: A game Theory Method, Natarajan Meghanathan et al. (eds): DaKM, SIPP, CCSIT, NCWMC – 2018, PP 113 – 122, 2018 © CS & IT-CSCP 2018, DOI: 10.5121/CSit.2018.81508

[7] Qiang R. (2018), Research on CRO'S Dilema in Sapiens Chain: A game Theory Method, Natarajan Meghanathan et al. (eds): DaKM, SIPP, CCSIT, NCWMC – 2018, PP 113 – 122, 2018 © CS & IT-CSCP 2018, DOI: 10.5121/CSit.2018.81508

[8] Yue W. (2018), Research on CRO'S Dilema in Sapiens Chain: A game Theory Method, Natarajan Meghanathan et al. (eds): DaKM, SIPP, CCSIT, NCWMC – 2018, PP 113 – 122, 2018 © CS & IT-CSCP 2018, DOI: 10.5121/CSit.2018.81508

[9] Binxing F. (2018), Research on CRO'S Dilema in Sapiens Chain: A game Theory Method, Natarajan Meghanathan et al. (eds): DaKM, SIPP, CCSIT, NCWMC – 2018, PP 113 – 122, 2018 © CS & IT-CSCP 2018, DOI: 10.5121/CSit.2018.81508

[10] Zheng Z, S. Xie, H.NDaiandH. Wang (2016), Blockchain challenges and opportunities: A survey. International Journal Web Grid Services 14(4), 352-375

[11] Nakamoto S. (2008), Bitcoin: A peer-to-peer electronic cash system. 100-121

[12] Narayanan A., J. Bonneau, E.Felten A. Miller and S. Goldfeder. (2016), Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press

[13] Bojana K., K.E lena and A. Mavridou (2017). Blockchain Implementation Quality and Challenges: A Literature Review.
11-13

[14] Lim L.,Y.Kim,J. Lee,L. Jae-Pil L.,H. Nam-GungandL. Jae-Kwang. (2014), The Analysis and Counter-measures on Security Breach of Bitcoin, International Conference on Computational Science and Its Applications, Springer, 720–732

[15] Ojha Varun, (2017).Unit-testing your Blockchain chaincode in Go for HyperledgerFabric v0.6. https://www.ibm.com/developerworks/ cloud/library/

[16] Xu X., I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass. P. Cesare and P. Rimba (2017), A Taxonomy of Blockchain-Based Systems for Architecture Design in Software Architecture (ICSA). IEEE International Conference, 243–252.