International Journal of Scientific Engineering and Science
Volume 6, Issue 9, pp. 43-49, 2022. ISSN (Online): 2456-7361

Blockchain Based Techniques for Several Network Security Services and Their Challenges

Jeremiah Tashie Wosu[1], Njumoke N. Abiola-Oseni[2]
[1, 2]Department of Computer Engineering Technology, Port Harcourt Polytechnic, Rumuola, Port Harcourt, Nigeria

***Abstract*—*Network security services such as privacy, data provenance, authentication, encryption, and integrity assurance are imperative for today's decentralized applications, especially due to sizeable volume of data being processed over the networks and the use of cloud computing. At present, these security services are provided by centralized controllers or by adopting weak distributed approaches. Thus, they are apt to suffer malicious attacks. On the contrary, blockchain is a secured and distributed ledger that can provide a fully distributed, provably secure, and consensus solution. This paper x-rays different potentials as well as some challenges of proposed blockchain-based approaches for several network security services. To this end, theoretical underpinnings of numerous papers published in high ranked scientific journals are utilized in the research for streamlining our assessment and capturing the continuously expanding blockchain domain. Based on a structured, systematic review and thematic content analysis of the discovered literature, we present some blockchain-based techniques for providing security services. Furthermore, we experimentally determined the individual efficiency of some blockchain-based techniques providing security services. This is achieved by employing TestRpc and AppDetectivePro to evaluate the performance of each technique. The results show that blockchain-based techniques are over 90% efficient in providing security services. Finally, foreseeable challenges associated with blockchain-based security service are also discussed to prod further research.*

Keywords*—*Blockchains, encryption, authentication, data provenance, privacy, integrity assurance, security challenges, centralized controllers, distributed approaches.

I. INTRODUCTION

A. Background Information

A blockchain is a system that enables a network of computers to communicate and exchange resources directly without involving a centralized authority as a transaction intermediary. It establishes a distributed or decentralized network of computers through which values can be exchanged forthwith, stored securely, and at a very low cost. The data is forwarded to many computers in the network and each of these computers runs a copy of the blockchain. Blockchain also store data immutably in chains. Thus, blockchain reduces to the minimal the chances of the digital records being lost. It also reduces cases where documents are altered, as well as situation where information becomes unavailable just because one computer in the network is unreachable. Furthermore, blockchain system is based on smart contracts and cryptographic algorithms as well as distributed consensus algorithms such as proof-of-work (PoW), Proof of Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof of Burn (PoB) and Proof of Authority (PoA) [1].

Over the last few years, blockchain technology has attracted colossal interest from the government, educational sector, finance sector, manufacturing sector, marketing sector, legal sector and advertising industries. Blockchain currently extends across many applications that are in vogue and spurring research in computer networking domain. Such applications include crypto currency, healthcare [2], peer to peer ridesharing, trusted crowd funding, disk space renting system, Internet of Things (IoT) [3], cloud storage, supply chain systems and security services such as authentication, confidentiality, privacy, integrity, and provenance. The term authentication refers to the confirmation of user identity. Confidentiality ensures that information cannot be accessed by persons that have not been granted approval to do so. A privacy service enables data owners to have absolute control over the divulgence of their information. Integrity involves maintaining data accuracy and consistency throughout the life-cycle of the data. Data or resource provenance refers to the metadata that traces and records the ingenuity of the data as well as the operations associated with them.

Currently, the aforementioned network security services are provided by trusted centralized authorities or by employing inefficient distributed methods. Consequently, security is a serious challenge for most of these applications. On the other hand, blockchain being a fully decentralized, distributed, secure, and consensus-based innovative technology, provides security measures that are capable of handling many challenges associated with trusted third party brokers.

B. Research Objectives

The aim of this research is to analyse different potentials and challenges of proposed blockchain-based approaches for several network security services. The specific objectives are as follows:

1. To carry out a structured, systematic review and thematic content analysis of literature in blockchain security domain.
2. To present some blockchain-based techniques for providing security services.
3. To experimentally determine the performances of different blockchain-based techniques for providing security services.
4. To highlight some challenges associated with blockchain-based security services in order to provoke further research in this area.

The remainder of this research is structured as follows; Section II reviews works on decentralized approaches for

providing security services, Section III presents different blockchain-based techniques for providing security services, Section IV discusses the techniques employed to experimentally determine the individual efficiency of some blockchain-based techniques as well as the results obtained, Section V highlights some challenges associated with blockchain-based security services, and finally, the research is drawn to a conclusion in section VI.

II. Review of Related Literatures

A. Related Works on Blockchain-Based Security Services

Numerous works that involves the application of blockchain-based techniques for providing security services such as privacy, data provenance, authentication, encryption, and integrity assurance exist. A review of some recent studies is presented in this section.

The authors in [4] conducted a systematic literature review to acquire knowledge on the latest application of blockchain technology and to establish some challenges contributing to low integrity, anonymity and adaptability of the technology. They presented many uses of blockchain, but only very few of them were specifically designed for Internet of Things. The authors also discovered many issues in the integrity, anonymity and adaptability. With respect to anonymity, it was realized that in blockchain systems only pseudonymity is guaranteed. They also established that the integrity of substantial blockchain systems is the most secure; meanwhile inherent issues associated scalability make it undesirable for Internet of Things applications. Nevertheless, blockchain based techniques for providing network security and their challenges were not examined.

In the research titled "Blockchain Technology: A Survey on Applications and Security Privacy Challenges" [5] carried out a survey to make available a broad analysis on several applications of blockchain technology for researchers in various institutions and research centres. The authors of the work also investigated the difficulties experienced when executing blockchain systems and its related authentication, integrity, provenance and privacy issues.

The work in [6] systematically reviewed some literature on blockchain-based applications putting into consideration present-day status, category and open challenges. On the basis of methodical review, they provided a completely broad method for grouping blockchain-enabled applications covering many areas such as digital currency, peer to peer ridesharing, trusted crowd funding, disk space renting system, supply chain systems, and data management. The work also explained some challenges affecting blockchain technology and proffered solutions to such issues.

As presented in the paper titled "A Survey on the Security of Blockchain Systems," [7] carried out a thorough analysis on the security threats to blockchain. The work examined the corresponding security attacks by examining well known blockchain systems. They also considered the techniques to improve security solutions for blockchain, with the hope of utilizing them in the implementation of several blockchain systems.

The work in [8] carried out a structured and very broad examination of the most ubiquitous blockchain techniques for enhancing security applications. Their result reveals that, amongst other things, Internet of Things (IoT) lends itself well to novel blockchain applications. Furthermore, networks and machine visualization, public-key cryptography, web applications, certification schemes, cloud storage, supply chain systems, and the secure storage of Personally Identifiable Information (PII). Finally, the work examined many the blockchain based approaches for combating cyber security threats.

The authors in [11] presented Instant Karma PKI (IKP), a system that automatically responds to illegal certificates and motivates certificate authorities (CAs) to act in the right manner. The proposed system also report potentially unauthorized certificates. Domains in IKP determine factors for their certificates, whereas certificate authorities (CAs) determine reactions such as financial penalties that are automatically carried out when an unauthorized certificate is issued. By leveraging smart contracts and blockchain-based consensus, they decentralized IKP while still providing automated incentives. They also presented a conceptual framework for payment flows and executed IKP in Ethereum platform to prove that decentralizing and automating public-key infrastructures (PKIs) with financial stimulus is both cost effective and practical.

A trust-aware blockchain based seamless authentication with privacy-preserving (TABSAPP) for handling crucial security issues was presented in [10]. TABSAPP consists of unprecedented data traffic pattern was employed to manage user identity as well as to prove that the developed system is highly efficient in increasing users' connectivity to enhance information exchange metrics such as packet delivery ratio and mobility speed.

The authors in [11] proposed a decentralized conceptual structure for identity and trust management in the Internet of Vehicles ecosystem. The main aim of the proposed framework is to ensure that software updates are highly secure. The proposed concept is made up of two processes: the identification and registration of objects in the system, and the authentication of the objects which depends on essential benchmarks for determining provable certificate presentation, confirmation, and rescission. The authors demonstrated the workability of their proposed method with a prototype. Results obtained show that the system is highly efficient for identity and trust management.

The work in [12] developed a decentralised signature storage system to guarantee trust among system entities, which could also be applied to many other decentralized Cyber-physical Systems (CPS) approaches. Ethereum network and Docker Tools were utilized in the implementation of the developed solution. The solution also ensures security properties such as participant identification, provenance, integrity, and non-repudiation. Furthermore, it abates the cost and volume of information storage than the normal usage of distributed system in CPS.

In [13] Hierarchical Identity Based Encryption (HIBE) was adopted to implement a name-based security approach meant

for codifying content. Each participant in the proposed system sustains his Unique Private Key Generator that is used for creating the master secret key and the public system parameters suitable for Hierarchical Identity Based Encryption mechanism. Hence the proposed system is not prone to the problem of key bond, which is intrinsic in several related mechanisms. Decentralized approach was adopted in order to spread the system properties of a content user in a completely distributed way.

A blockchain based mechanism for tracing, recording and regulating what program constituents are distributed between users over several security domains was developed in [14]. The decentralized mechanism depends on function-based and feature-based access regulates and averts disapproved data accesses. The system also ensures the integrity of provenance data on software module updates and the associated details such as the location and time of update as well as the entity that carried out the update. Moreover, the developed system tracks data leakages, secretly implemented by approbated system users, to unapproved entities. The developed mechanism is very efficient for data forensics/provenance, where the identity of users that accessed/ updated/ transferred the delicate cyber data or vital software is detected. It also guarantees that all the transactions in the universal cooperative software development environment are registered in the decentralized and distributed ledger, and can be confirmed in the future. Finally, the system guarantees that transactions cannot be rejected by invokers.

A decentralized system for Data Integrity Service was designed in [15]. The system provides highly efficient data integrity verification mechanism for data owners as well as for data consumers, independent of any trusted centralized party. The authors also presented essential protocols and a prototype system, which was tested to ascertain the feasibility and performance of the proposed system. The results obtained assessment were presented and thoroughly analysed. The work would spur further research and subsequent system proposals on data security in distributed environment.

The work in [16] designed a revocable and privacy-preserving distributed data security framework (RPDDSF) by implementing a sizeable global and multiple-authority system. The proposed system enables completely secluded access policy for trusted data distribution in Internet of Things schemes. Thus, it is capable of guaranteeing entity attribute privacy maintenance with unrestrained attribute global and key bond resistance appropriate for sizeable blockchain based systems. Consequently, RPDDSF enables users to easily track, detect, reveal and punish traitors by applying forward/backward secure rescission. Moreover, the proposed system is capable of securing data integrity and confidentiality for data owners as well as for data users to withstand misbehaving cloud.

In [17] the researchers designed a very efficient system, called SUBLμME, which stands for Safe Universal BLockchain as a μservices-based Method for internet of things Environments. The system combines BaaS and microservices technologies. Hence, it is capable of providing reconfigurable and reusable data security attributes executed as separate services that can be use severally for many internet of things schemes. The developed system was tested and authenticated by a simulated intelligent home environment. The results obtained from the performance evaluation reveals that SUBLμME guarantees many security enhancements such as access control, data integrity, data packages' validation and efficient and secure data transmission and storage.

The work in [18] designed a decentralised method for generating a privacy-preserving and confirmable query scheme to participants in Industrial Internet-of-Things (IIoT) systems. The proposed work applies blockchain to save data. It also uses the cloud to store extensive data (e.g., image) as off-chain data and provisioning search services to users by executing a query in both on-chain and off-chain data and creating an aggregated result. Furthermore, the system instituted a novel privacy-preserving query approach for quaranteeing delicate data privacy during query execution. A data owner encrypts both on-chain and off-chain data in the privacy-preserving query mechanism before sending it to the blockchain and cloud. A prototype query verification model was also developed for the blockchain. The prototype permits each blockchain user to endorse the query result individually and a user to verify the endorsement of the query result before use. The evaluation performance tests revealed that the work is highly efficient and scalable.

A framework for safely storing patient health records exchange (SPHRS) was designed in [19]. The system is fully controlled by the patient in terms of giving and rescinding access as well as creating access policies for care providers. The framework achieves security by applying participants' identity authentication and verification. Decentralised IPFS storage was applied to store the encrypted patient health records and ensure immutability. In addition, The framework's performance was evaluated by testing metrics such as blockchain transactions' gas consumption, throughput, average response time, and average bytes.

Sequel to the review of related works thus far, it is evident that much attention has not been given to the potentials and challenges associated with blockchain-based techniques for providing security services. Moreover, our work is different from other similar works in that it is based on a structured, systematic review and thematic content analysis of the discovered literature. Also, this work fits better to up-to-the-minute advancement in blockchain technology and elucidates with high accuracy the future blockchain trends. Thus, taking into account the existing and future heterogeneity of blockchain-based approaches, the potentials and challenges of these approaches for providing network security services are presented in a simple but very clear manner.

B. Research Gaps

Thus far, considering the related literatures reviewed, the following research gaps have been identified as regards the application of blockchain-based techniques for providing network security services:

1. None of the works reviewed experimentally determined the individual efficiency of some blockchain-based techniques for providing security services.

2. Attention has not been given to challenges associated with blockchain-based security services with a view to goading more research in the area.

C. Research Contribution

This work proposes to carry out a structured, systematic review and thematic content analysis of literature in blockchain security domain as well as experimentally determine the individual efficiency of different blockchain-based techniques for providing security services, and present some of their challenges. This is achieved by employing TestRpc and AppDetectivePro to evaluate the performance of different decentralized approaches for providing security services.

III. Blockchain Technology Based Techniques for Security Services

Some blockchain-based techniques for providing security services such as privacy, data provenance, encryption, authentication and integrity assurance are presented in this section.

A. Blockchain-Based Data Privacy Techniques

A privacy service gives data owners the power to regulate the divulgence of their information. Each participant defines his access control list (ACL). Blockchain technology is utilized to deliver distributed end-to-end data privacy solutions. To be specific, it offers the data proprietorship solutions and continuously varies the access dibs as required. The real essence of decentralized data privacy is to develop a blockchain stratum on top of the data storage stratum, thereby enabling data holder create his choice of ACL via smart contracts, as well as promulgate the ACL and the data as blockchain transactions [20]. Next, we present some blockchain-based solutions that offer data privacy services.

(1) Fair Access: It leverages on smart contracts to create polices that regulates data access and make permission resolutions. Fair Access, considers blockchain as a database that stores all the policies that regulates data access for both the resource and the requester in form of transactions. It also considers blockchain as an archive that guarantees auditing functions. Furthermore, it averts counterfeiting of token by carrying out transactions integrity inspections, and tracks token reuse using the double spending discovery scheme [21]. Fair Access functions comprise of resource registration, grant access, request and revoke access.

(2) Zyskind's Approach: This is a decentralized data privacy technique that enables users to regulate access and sue of their data. This technique utilizes blockchain blocks in storing the data as well as the ACL. The system makes this possible by integrating a blockchain, which serves as an access-control regulator, to an offblockchain storage medium [22]. The system is made up of three basic elements namely users, providers and the blockchain network.

(3) Decentralized Runtime Access Monitoring System (DRAMS): This technique applies blockchain technology to confirm access regulation records for clouds in a federated cloud environment. The main design applies the smart contracts in determining the access rights as well as in gathering the access records from various clouds. A thorough comparison of the access rights and the access records is carried out by the miners; if a discrepancy is observed, access will not be granted [23].

B. Blockchain-Based Data Provenance

Data or resource provenance is a security service that enables data or resource to be tracked as well as be audited. It refers to the metadata that tracks and reports the originality of the data and the operations associated with them. The metadata comprises of the inputs records, the users, the platforms, and the functions that made use of or processed the data of interest. Blockchain technology being a distributed ledger that logs the transactions in the system is, therefore, able to offer data provenance service by logging the details of the data ingenuity and the transactions in the blockchain platform [20]. Some techniques that utilize blockchains to offer data and resource provenance service are highlighted in the succeeding paragraphs.

(1) Prov Chain: It is mechanism to gathert and confirm cloud data provenance, by attaching the provenance data to blockchain transactions. Prov Chain functions basically in three stages: (1) provenance data assemblage, (2) provenance data storage, and (3) provenance data authentication. [24]. It makes use of the blockchain database as a distributed database that offers the confidentiality and non-reputability guarantees. The authentication of the data provenance is carried out off-chain by a distributed provenance auditor (PA).

(2) Data Prov: This is an architecture that harnesses blockchain technology as well as smart contracts to deliver data provenance services for critical cloud information. Changes to documents are made via versioning in the Data Prov system model. Each modification that is related to a document is recorded as a separate new version. The platform considers that only current version of the document/data file is used for modification. The system verifies the condition that any information which contains modification that is not recorded in the provenance data is discarded [25].

(3) A Blockchain-Based Approach for Data Accountability and Provenance Tracking (DAPT): The three vital components of DAPT are: data subjects, data controllers, and data processors. In DAPT platform, the controller generates a contract details the shared constraints on the application and redistribution of any explicit or implicit data derived from all subjects that acquiesces with the controller. The contract behaves as a repository of the configurable policy templates that will be instantiated for all subjects and do not store anything except the list of subjects [26].

C. Encryption and Authentication Services Using Blockchain-Based PKI

Encryption and authentication are very crucial security services that certainly need to be offered in any network platform. To this end, public key infrastructure (PKI) is among the most common methods for ensuring that key management is made available for global key cryptography. The distributed, the event-recording and non-reproducibility

International Journal of Scientific Engineering and Science
Volume 6, Issue 9, pp. 43-49, 2022. ISSN (Online): 2456-7361

features of the blockchain technology make it a desirable technique for PKI. Thus, we will present some techniques to accomplish blockchain-based PKI.

(1) Blockstack: This approach uses Namecoin to create a distributed PKI platform. In Namecoin, data storage is carried out within the blockchain transactions. It is achieved by determining a name-value pair that stores usernames, and can be registered in the transactions. Blockstack ID modifies Namecoin by including a second namevalue pair that is reserved only for the public keys. Blockstack creation ties the user identity to an elliptic curve public key which is considered to be one of the best public key cryptography techniques [27].

(2) Gan's Approach: It is a key-based authentication system that utilizes private blockchain for recording the nodes' current public keys, confirming the keys, and letting other users to apply for the nodes' keys. The detail of this technique is shown in Figure 1, where a Centralized CA (CCA) is considered to be completely secured. Several validators, donated as Device Manufacturer Validators (DMVs), are connected to the CCA [28].

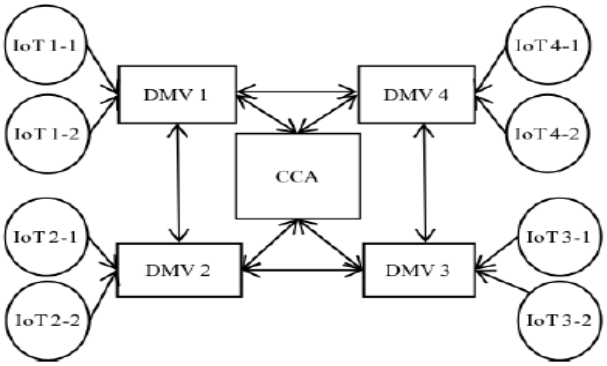

Fig. 1. The architecture of Gan's technique

(3) Distributed PKI (DPKI): This technique leverages on blockchain technology as a decentralized, trustless database that removes the use of a CA and grants the nodes total control and ownership of their data. It harnesses a Web registration domain, where the user produces its public/private key and forwards the public key to the blockchain plateform as a transaction. Security is achieved by connecting the current key of the user to his/her identity [20].

(4) Instant Karma PKI (IKP): The Instant Karma PKI (IKP) technique stores the certificate authorities (CA) features in the blockchain database. It is a system that automatically responds to illegal certificates and motivates certificate authorities (CAs) to act in the right manner. The system also report potentially unauthorized certificates. Domains in IKP determine factors for their certificates, whereas certificate authorities (CAs) determine reactions such as financial penalties that are automatically carried out when an unauthorized certificate is issued. By leveraging smart contracts and blockchain-based consensus, IKP can be decentralized while still providing automated incentives [29].

(5) Guardtime Solution: Guardtime is a technique for secure authentications of the IoT devices harnessing blockchain technology as well as physically unclonable functions (PUFs). A PUF is a digital fingerprint hardware that is considered a unique identifier of the nodes. PUF based techniques offer an offline method with a tamper resistant ID and resiliency. PUFs utilize the unique features of each node to create its unique private/public keys. It also uses PUFs to derive the public/private keys. The public keys are forwarded to the blockchain in transactions. IoT devices use small memory; therefore, they are unable to store sizeable private/public keys. Obviously, the solution offered by PUF and Guardtime helps such nodes to reproduce the same key each time it is needed [30].

(6) Pemcor: It harnesses blockchain database as a decentralized and secure data store. In Pemcor, the CA is allowed to issue an unsigned certificate. The hash value of the certificate is recorded in the blockchain which is regulted by authorities, such as banks or governments. Such authorities share two blockchain databases, one for the generated certificates and one for the revoked certificates. During verification, the authority verifies its maintained blockchain data stores. If the hash of the certificate exists in the stored certificate blockchain and is not in the revoked certificates blockchain, the certificate is valid; otherwise, it is not. This idea offers many benefits such as an easy confirmation with minimal delay guarantees [31].

D. Blockchain-Based Integrity Assurance

Blockchains have inherent integrity regulator as transactions are signed by the sender and confirmed by the miners. The data cannot be altered if it is committed to the blockchain database. Thus, harnessing blockchain transactions to forward the data or any asset guarantees the integrity service. Most importantly, blockchain technology can be utilized to offer evidence for when the data has been modified. In the succeeding paragraphs, we present some integrity approaches harnessing the blockchain technology.

(1) Storj: It allows data to be stored off-chain while the metadata referring to the original data is stored in the transactions. The metadata has the location of the data and the hash of the data. Whenever the user wants to access the data, it inquires the blockchain network. The network confirms the data stored off-chain and brings back the metadata that is required to regain the original data. In this way, the integrity is managed efficiently. [20].

(2) Ericsson Blockchain-Based Integrity Assurance: It offers integrity services that let the application developers to confirm the integrity of their users' data and assets. They make use of Keyless Signature Infrastructure (KSI) to create signatures for the resources [32]. Guardtime offered a scalable, decentralized, efficient and provably secure blockchain-based KSI approach. Ericsson harnesses Guardtime's approach to offer integrity rather than authentication [30].

Generally, Ericsson service needs two important steps: signing the data and verifying the signature. To sign data requires forwarding them to the blockchain, where the signature is simply returned to the user. The signature is kept in the blockchain transactions as well as at the user's system. To verify the data, the stored signature is forwarded to the blockchain network for verification purposes. The blockchain

nodes will confirm the signature and presents the expected hash value if the signature is valid. The user compares its hash value with the submitted one to determine whether the data was modified [32].

IV. Efficiency of Some Blockchain-Based Techniques

In this section, we will experimentally determine the individual efficiency of some blockchain-based techniques providing security services. This is achieved by employing TestRpc and AppDetectivePro to evaluate the performance of each technique.

Testrpc is a Node.js based Ethereum client for system implementation and testing. It harnesses ethereumjs to simulate full client behaviour thereby making it very easy and fast to develop Ethereum solutions. It also involves all commonly known RPC operations and characteristics, and can be run deterministically to accelerate system development. It has been adopted for simulating a good number of blockchain-based approaches for offering security services.

AppDetectivePRO is a database and Big Data scanner that can instantly reveals configuration errors, identification and access regulation problems, missing patches, or any poisonous fussion of settings that could lead to escalation of privileges attacks, data leakage, denial-of-service (DoS), or unauthorized modification. It was utilized in scanning for vulnerabilities in the different decentralized techniques providing security services.

The result of the comparison of various blockchain-based techniques used for network security services such as privacy, data provenance, encryption and authentication (implemented with PKI), and integrity assurance are presented in tables 1, 2 and 3.

TABLE 1: A Comparison of Blockchain-based Techniques for Data Privacy

S/N	Technique	Does It Modify Implementation?	Scalable Solution?	Efficiency
1	FairAccess	Yes	No	97%
2	Zyskind	Yes	No	96%
3	DRAMS	No	No	94%

TABLE 2: A Comparison of Blockchain-based Techniques for Data Provenance

S/N	Technique	Does It Modify Implementation?	Efficiency
1	ProvChain	No	92%
2	DataProv	No	94%
3	DAPT	Yes	91%

TABLE 3: A Comparison of Blockchain-based Techniques for Integrity

S/N	Technique	Can it Verify Multiple Chunks?	Cryptographic Technique	Effi-ciency
1	Storj	No	PKI	90%
2	Ericson	Yes	KSI	94%

V. Challenges Associated with Blockchain Security Services

Certainly, blockchain-based security applications have many potential benefits. Nevertheless, it still has some challenges that affect its implementation for the security services considered in the previous section. In this section, we discuss some of these security challenges with a view to goad further research.

A. Vulnerabilities in Smart Contracts

When a program is implemented in a decentralized platform, a smart contract can have security vulnerabilities caused by a defect in that program. A typical example is that some smart contracts are prone to bugs such as mishandled exceptions, transaction-ordering dependence, timestamp dependence, and reentrancy vulnerability [33].

B. Transaction Malleability

During contracted transactions, the agreement does not instantly cloak all the data in the hashed transaction; therefore, it is uncommon but possible for transactions to be intercepted, altered, and rebroadcast, hence making the transaction legal entity to think that the original transaction was not verified [34].

C. Computations and Mining Nodes

In most of the latest applications, it is expedient for the blockchain entities to be simple so as to ensure that low computation performance demands are met. However, the security services generally require high computations in encryption, decryption, and signature [20].

D. Privacy Leakage and Anonymity

Among of the most rated features of blockchain is its ability to provde pseudo-user anonymity. This is vital for security purpose as public blockchains are open, thereby exposing user information to malicious attackers. Unfortunately, for most of the blockchain-based techniques considered in the previous section, the transactions relate the user identity to their public key, the ACL, or the provenance data; therefore, the users are no longer anonymous [35].

E. Scalability

Applications utilizing blockchain technology are believed to scale better than traditional centralized techniques. Conversely, the technology performs poorly as the number of users and networking nodes increases. This is a serious issue, especially with network security applications, where thousands of users need to be served and the network scales up fast [20].

VI. Conclusion

In this paper, we did a systematic presentation of some network security services that are based on blockchain technology. These security services include data privacy, data and resource provenance, authentication, confidentiality, and integrity assurances. Techniques involved in providing each of the security applications were thoroughly analyzed and clearly presented. TestRpc and AppDetectivePro were employed to experimentally determine the performance of different blockchain-based techniques for providing security services.

In conclusion, it is obvious that decentralized approaches are very efficient in providing network security services. Nevertheless, there are challenges associated with blockchain based techniques. These security challenges affecting the

implementation of decentralized approaches were highlighted with a view to goading further research.

REFERENCES

[1] M. Pilkington, “Blockchain technology: Principles and applications,” in Research Handbook on Digital Transformations. Cheltenham, U.K.: Edward Elgar, 2016. Accessed: Feb. 13, 2018. [Online]. Available: https://ssrn.com/abstract=2662660.

[2] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Services (Healthcom), Munich, Germany, 2016, pp. 1–3.

[3] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[4] M. Conoscenti, A. Vetrò, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in Proc. IEEE/ACS 13th International Conference on Computer System Application (AICCSA), Agadir, Morocco, 2016, pp. 1–6.

[5] B. K. Mohanta, D. Jena, S. S. Panda and S. Sobhanayak. Blockchain technology: A survey on applications and security privacy Challenges Internet of Things Volume 8, December 2019, 100107 www.sciencedirect.com/science/article/abs/pii/S2542660518300702.

[6] F. Casinoa, T. K. Dasaklisb and C. Patsakisa. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics 36, pp. 55–81, 2019.

[7] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” International Journal on Network Security, vol. 195, no. 5, pp. 653–659, 2017.

[8] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi and K. R. Choo. A systematic literature review of blockchain cyber security. Digital Communications and Networks 6 (2020) 147–1562021.

[9] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI Around with Decentralized Automated Incentives," 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 410-426, doi: 10.1109/SP.2017.57.

[10] B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, W. Wang and N. M. F. Qureshi, "TAB-SAPP: A Trust-Aware Blockchain-Based Seamless Authentication for Massive IoT-Enabled Industrial Applications," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3159164.

[11] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger and S. Steinhorst, "Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem," 2020 Global Internet of Things Summit (GIoTS), 2020, pp. 1-6, doi: 10.1109/GIOTS49054.2020.9119623.

[12] B. K. Mohanta, U. Satapathy, M. R. Dey, S. S. Panda and D. Jena, "Trust Management in Cyber Physical System using Blockchain," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225272.

[13] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 415-420, doi: 10.1109/INFCOMW.2016.7562112.

[14] D. Ulybyshev et al., "(WIP) Blockhub: Blockchain-Based Software Development System for Untrusted Environments," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 582-585, doi: 10.1109/CLOUD.2018.00081.

[15] B. Liu, X. L. Yu, S. Chen, X. Xu and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," 2017 IEEE International Conference on Web Services (ICWS), 2017, pp. 468-475, doi: 10.1109/ICWS.2017.54.

[16] J. Zhang, J. Ma, Y. Yang, X. Liu and N. N. Xiong, "Revocable and Privacy-Preserving Decentralized Data Sharing Framework for Fog-Assisted Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 13, pp. 10446-10463, 1 July1, 2022, doi: 10.1109/JIOT.2021.3122949.

[17] D. Hasan and M. Driss, "SUBLμME: Secure Blockchain as a Service and Microservices-based Framework for IoT Environments," 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), 2021, pp. 1-9, doi: 10.1109/AICCSA53542.2021.9686757.

[18] M. S. Rahman, I. Khalil, N. Moustafa, A. P. Kalapaaking and A. Bouras, "A Blockchain-Enabled Privacy-Preserving Verifiable Query Framework for Securing Cloud-Assisted Industrial Internet of Things Systems," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 5007-5017, July 2022, doi: 10.1109/TII.2021.3105527.

[19] M. Abouali, K. Sharma, O. Ajayi and T. Saadawi, "Performance Evaluation of Secured Blockchain-Based Patient Health Records Sharing Framework," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795759.

[20] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka. Security Services Using Blockchains: A State-of-the-Art Survey. IEEE Communications Surveys & Tutorials, Vol. 21, No. 1, First Quarter 2019.

[21] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in IoT,” in Proc. Europe MENA Cooperation Advance Information Communication Technology Conference, 2017, pp. 523–533.

[22] R. G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Security Privacy Workshop, San Jose, CA, USA, 2015, pp. 180–184.

[23] M. S. Ferdous, A. Margheri, F. Paci, M. Yang, and V. Sassone, “Decentralised runtime monitoring for access control systems in cloud federations,” in Proc. IEEE 37th International Conference on Distributed Computer Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 2632–2633.

[24] X. Liang et al., “ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in Proc. 17th IEEE/ACM International Symposium Cluster Cloud Grid Computer (CCGRID), Madrid, Spain, 2017, pp. 468–477.

[25] A. Ramachandran & M. Kantarcioglu. “Using blockchain and smart contracts for secure data provenance management,” Computer Repository arXiv preprintarXiv:1709.10000, 2017.

[26] R. Neisse, G. Steri, and I. Nai-Fovino, “A blockchain-based approach for data accountability and provenance tracking,” in Proc. 12th International Conference on Availability Rel. Security, Reggio Calabria, Italy, 2017, pp. 1–10.

[27] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Proc. USENIX Annual Technology Conference (USENIX ATC), Denver, CO, USA, 2016, pp. 181–194.

[28] S. Gan, “An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain,” M.S. thesis, Indian Institute of Technology at Kanpur, Kanpur, India, 2017. Accessed: Feb. 13, 2018. [Online]. Available: https://security.cse.iitk.ac.in/node/240.

[29] S. Matsumoto and R. M. Reischuk, “IKP: Turning a PKI around with decentralized automated incentives,” in Proc. IEEE Symposium on Security Privacy (SP), San Jose, CA, USA, 2017, pp. 410–426.

[30] Guardtime. Internet of Things Authentication: A Blockchain Solution Using SRAM Physical Unclonable Functions. May 2017. Accessed: Feb. 13, 2018. [Online]. Available: https://www.intrinsicid.com/wpcontent/uploads/2017/05/gt_KSI-PUF-web-1611.pdf.

[31] F. Corella, Implementing a PKI on a Blockchain, Pomcor Res. Mobile Web Technol., Carmichael, CA, USA, Oct. 2016. Accessed: Feb. 13, 2018. [Online]. Available: https://pomcor.com/2016/10/25/implementing-a-pki-on-a-blockchain/.

[32] Ericsson. Data Integrity Assurance User Guide—I Implementation of Service in Predix User Guide. 2016. Accessed: Feb. 13, 2018. [Online]. Available: https://www.ericsson.com/globalassets/digital-asset-integrityservice-user-guide_rev0726.pdf.

[33] J. McKendrick. (2017). 9 Reasons to be Cautious With Blockchain. [Online]. Available: https://www.zdnet.com/article/9-reasons-to-becautious-with-Blockchain/

[34] A. Moinet, B. Darties and J. L. Baril. “Blockchain-based trust & authentication for decentralized sensor networks,” IEEE Security Privacy. 2018.

[35] D. Christian and D. Wattenhofer, ``Bitcoin transaction malleability and MtGox," in Proc. European Symposium on Res. Computer Security, 2014, pp. 31 - 326.