A Conceptual Framework for Augmenting the Security of Digitized Academic Records in Nigerian Tertiary Institutions using Blockchain Technology

Ayei E. Ibor[1], Ofem A. Ofem[1], Julius N. Obidinnu[2]
[1]Department of Computer Science, University of Calabar, Calabar, Nigeria
[2]Department of Computer Science, Cross River University of Technology, Calabar, Nigeria
Email: ayei.ibor@gmail.com, ofem_ajah@yahoo.com, obijulius@yahoo.com

Abstract *- All academic activities produce records such as statements of result, testimonials, certificates and transcripts, most of which are stored in manual file cabinets and relational databases. With the growing importance of academic records in Nigeria, it has become imperative to protect them from falsification and accidental modification. Though the use of relational databases has been the de facto standard for storing academic records in recent years, the digitized contents are always under the control of a single administrator who has authoritative access with full rights and privileges to them. However, authoritative access is likely to introduce instances of unauthorized alteration of records due to centralized control of the database. With blockchain technology, the storage, modification, distribution and verification of academic records will be based on distributed consensus. This will allow all authorizing parties to be notified of changes, and can either confirm or reject the status of any update on an earlier stored academic record using its hash. This paper presents a conceptual framework based on blockchain technology for the security of digitized academic records with digital signature scheme and timestamps. It is envisaged that the proposed approach will be valuable to tertiary institutions in Nigeria for the security of academic records in terms of modification and verification processes.*

Keywords: ***data security, blockchain technology, academic records, cryptographic hash function***

1. INTRODUCTION

The security of digitized academic records depends on the accuracy of processing and storage. Processing usually precedes storage, and the stored records are used as valid contents in relation to the individual performances of students. The storage of academic records has never been a complicated task. The complicated part of the process usually arises when the initially stored contents are modified, distorted, lost and/or destroyed due to a plethora of conditions such as sheer committing of fraud, natural disaster, and system breakdown. Due to the sensitivity and position of academic records in the general structure of a tertiary institution, and their relevance to the professional development of students, it has become increasingly necessary to employ more sophisticated yet low cost methods of keeping them secure in all circumstances.

Transcript processing and certificate verification are major aspects of academic record processes that are frequent. Several studies have been focused towards transcript processing such as Onwudebelu et al in [1], Mbam and Odachi in [2], and Okikiola and Samuel in [3]. For instance, [2] proposed a web-based approach for transcript processing. However, this approach did not consider the various levels of authorization for enhancing the security of the processed transcripts including the possibility of unauthorized modification of contents. Similarly, a system for optimizing the generation of transcripts from students' results was proposed in [3].

Onwudebelu et al in [1] had in an earlier research posited that the significance of academic records such as transcripts leaves the management and administration of Nigerian tertiary institutions with no option than to provide an improved and convenient way of storing and accessing them. While most of these researches centered more on the convenience of access, little or no details are given about the secure process of managing these academic records such that accidental modification and distortion is completely eliminated. Although the tradeoff between ease of access and security may come with some overheads, a secured database of records provides for confidentiality, integrity and availability. These three main goals of security are relevant in any context of information use.

Having considered the administrative and implementation problems currently plaguing the management of academic records, this paper presents a conceptual framework for the use of blockchain technology in implementing a secured and distributed access to academic records for which instances of unauthorized modification and distortion of records is eliminated. The approach suggests the use of digital signature scheme and timestamps based on blockchain technology to deliver a highly transparent system for achieving the security of digitized academic records underpinned by low cost implementation and maintenance.

II. REVIEW OF RELATED LITERATURE

The storage and retrieval procedures for digitized academic records require robust implementation strategies. Digitized academic records are basically stored on relational database management systems such as Oracle, PostgreSQL SQL Server, or MySQL [2], [3]. These databases are either used in web-based or desktop academic information systems, and has become a conventional practice in most academic institutions and some production environments. Lemieux in [4] opines that authenticity and reliability are major considerations of the trustworthiness of digitized records. These considerations largely depend on the security of the database.

Utami and Raharjo in [5] discussed database security for academic information systems populated with data of transcripts, certificates and statements. This implementation was based on the use of table constraints and relationships as well as role based access control. One of the problems that necessitated the work of [1] and [6] is the improper security and poor management of academic records. However, their proposed approach did not have an explicit security component that addresses the problem of accidental record modification and distortion. At the same time, the various levels of authorization for accessing the stored contents were not defined.

The use of a single database usually promotes authoritative access for the administrator, which can create room for the manipulation of academic records in a way not authorized after storage. Blockchain technology, which has been widely used for the creation of decentralized currencies, self-extracting digital contracts and intelligent assets over the Internet [7], [8], [9], [10], [11], can serve as a replacement for centralized control over academic records. Sharples and Domingue in [12] proposed a system that uses blockchain (the core mechanism for bitcoin digital payment system) to store permanent distributed record of intellectual effort as well as reputational reward. The use of blockchain in this context is geared towards instantiating and decentralizing educational records.

Furthermore, [9], [11], and [13] assert that blockchain provides a mechanism for creating a database of distributed records. These distributed records are executed and shared among participating parties, who permit updates on the records based on the distributed consensus method. In distributed consensus, updates can only be permitted when a majority of the participating parties agree for such an update to be effected, and once an update is made, it cannot be erased by a single participating party. Pilkington in [8] and Raval in [13] discussed that blockchain as a replicated database of transactions (or records) paves way for the building of massively scalable and profitable applications with a high level of security. Further uses of the blockchain technology are given in [7], [10] and [14].

III. BLOCKCHAIN TECHNOLOGY: AN OVERVIEW

Blockchain delivers decentralized control over transactions and data. This technology has been used for bitcoin cryptocurrency and has recently found applications in several other fields. Raval in [13] posits that blockchain technology has come as the future of massively scalable and profitable applications, which will be more flexible, transparent, distributed and resilient. The idea of decentralized applications is a representation of the cryptographically stored ledger, scarce-asset model implemented over a peer-to-peer network technology.

Blockchain technology has found relevance in decentralized validation of transactions, which are stored with a quasi-anonymous framework using some form of storage called public ledgers. Validating transactions over a decentralized peer-to-peer technology has been shown to provide strong confidentiality, data integrity, and non-repudiation services [15]. Transactions over blockchain

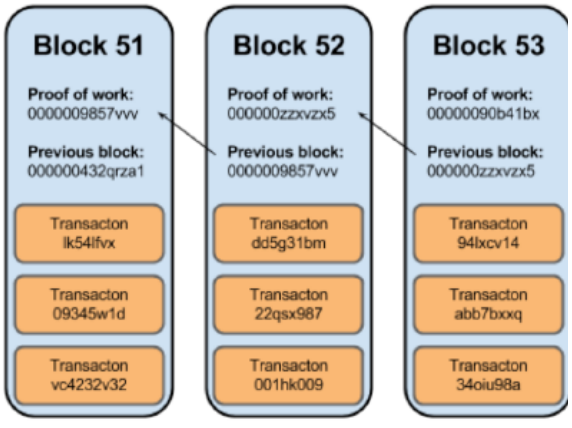

Figure 1. A representation of a blockchain [15].

technology are authenticated over public-key cryptography for the participating parties such that the public-key is mapped as the participant's account number while the private key depicts the ownership credentials of the participant. To ensure data integrity and non-repudiation, digital signatures are used. A typical representation of a blockchain is illustrated in Figure 1.

In [16], blockchain is described as a model of state machine replication. State machine replication permits that a service preserves some state, which can be transformed by the operations invoked by clients. Subsequently, outputs are generated, which can then be verified by the clients. Blockchain is implemented over Internet-connected nodes using a distributed protocol. In this way, blockchain acts as a trusted computing service in either a permission-less or permissioned mode. In a permission-less blockchain, participation is based on the ability to spend CPU cycles, and as well demonstrate proof-of-works – a requirement, which ensures that expensive computations are performed so that transactions on a blockchain are facilitated. Conversely, a permissioned blockchain exerts control over the participation in validation and protocol using already defined node identities, which exist in a block.

According to [17], the technology of blockchain, though considered as a public ledger, has the potential to become a globally decentralized record of digital assets. In a blockchain architecture, each computer or node connected to it with a client that participates in validating and relaying transactions, automatically has a downloaded copy of the shared ledger or database. The information stored in the blockchain database is always complete and includes all records of transactions from the point of origin of the transactions. This means that there is the possibility to create a chain of connected records, which are transparent to all validating parties such that changes or modifications can only be effected when authorized by a majority of them. Queries are also easy to implement on any block explorer to confirm the transactions on any connected node.

The disruptive nature of blockchain is demonstrated in its capacity to enforce trustless proof mechanism for all transactions initiated and validated by all nodes connected to it. For trustless proof mechanism, the users can trust the public blockchain database of records stored globally on decentralized nodes without including any trusted intermediaries [11], [17], [18], [19], and [20]. Similarly, blockchain delivers tamper-proof digital platforms of distributed trust as well as substituting the frequent requests for actively intermediated synchronization of data and concurrency control. These enhanced features of blockchain technology make it usable in all sectors and layers of the society in diverse ways.

Blockchain technology is both decentralized and distributed as shown in Figure 2. Decentralization here has to do with the fact that the failure of a single node cannot affect the operation of the entire blockchain architecture. Moreover, the timestamped public database or ledger is stored on multiple connected nodes or computers over the Internet to create a distributed environment easily accessible to all participating parties [13].

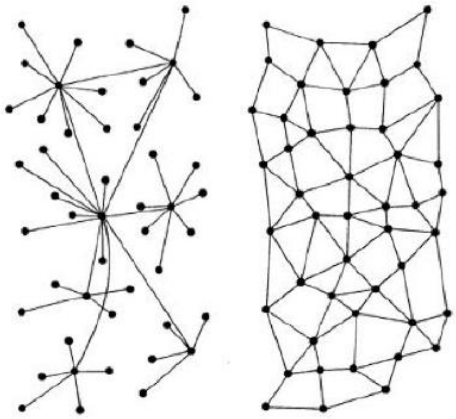

Figure 2. Illustrating blockchain technology as both decentralized and distributed [13]

Peer-to-peer technology in blockchain allows nodes to talk to each other directly. This provision uses smart contracts to effect decentralized consensus since the blockchain record is available to every node. The smart contract, which is a piece of code triggered based on some preprogrammed conditions lives in the blockchain, completely eliminating the issue of a central point of failure. Beck et al in [18] posits that the smart contract is a piece of code, which is executed on a blockchain through an Ethereum Virtual Machine (EVM). The piece of code is then available for the network participants to implement. For the smart contracts to be successfully executed, the Turing-complete programming languages are used to create EVM bytecode form the smart contracts. The Turing-complete programming languages used for creating smart contracts in a blockchain are Solidity, Serpent, Mutan and LLL (Low-level Lisp-like) programming languages respectively. Furthermore, smart contracts are identified through addresses and use the data they receive to execute the code it contains [18].

IV. THE PROPOSED APPROACH

The proposed approach uses the distributed consensus of blockchain technology to enhance the security of stored

academic records. In this approach, all processed academic records are stored on a public blockchain. A cryptographic hash function is then applied on the stored records and the output is stored in a blockchain with the transaction generated being signed by the private key of the tertiary institution. This creates a high level of security for the stored academic record as the blockchain cannot be modified without a majority consensus of the participating parties who serve as the validators of the stored transaction.

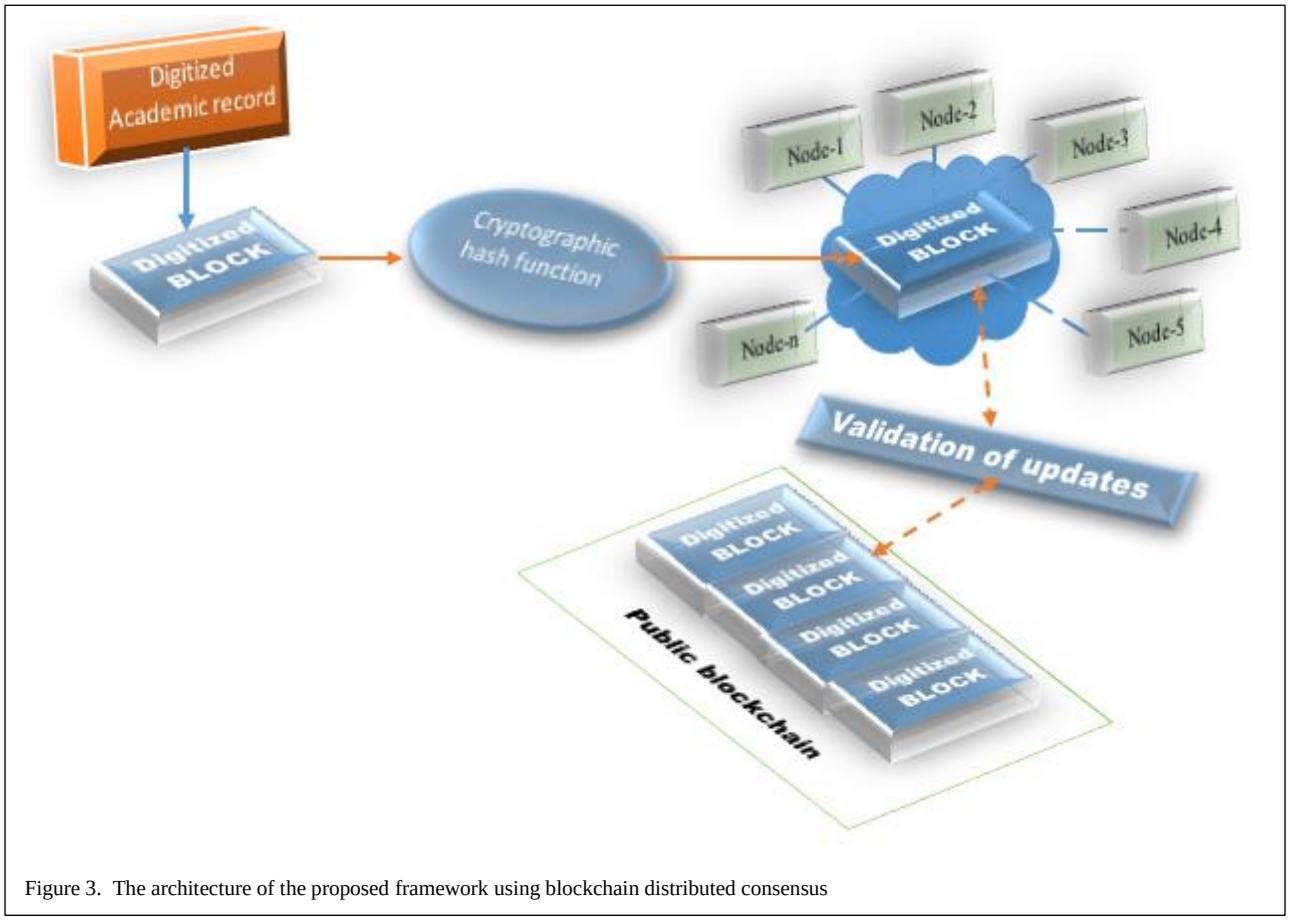

Figure 3. The architecture of the proposed framework using blockchain distributed consensus

As depicted in Figure 3, each validator on a connected node (represented as Node-1 ... Node-n), in this case, a member of the institution privy to the academic records, must agree on an update, where necessary, before changes can be effected on an earlier version of the stored academic records. These changes are then effected across the replicated blockchain database for all validators to be aware of further reviews of the records. Additionally, the tertiary institution can deploy the digital signature scheme of blockchain to add the signatures of the authorized validators such that updates can be based on an initially agreed condition. This condition can be the minimum number of authorized validators or signatures for an update to be effected.

As illustrated in Figure 3, the cryptographic hash function plays an important role in the security and validity of the stored academic records. Security in this case is enhanced through the replacement of authoritative access with distributed consensus. This implies that it is practically impossible to have a single validator having complete control of access to academic records in such a way that fraudulent activities can be perpetrated. For verifying the originality of academic records, the timestamp attached to the digital signature can be used for this purpose. The timestamp is automatically created at the time the cryptographic hash function is applied on the academic record to create a transaction that is stored in public blockchain. The preferred hash function in this case is the secure hash algorithms (SHA-256), which makes the blockchain database immutable.

The choice of SHA-256 is to ensure that all blocks in the blockchain are well formed and not tampered with, in which case the blockchain becomes unbreakable throughout its use [18] and [21]. As depicted in Figure 1, the blockchain is replicated across all the nodes

participating in the processing of an academic record, and all network participants have a copy of the data in the blockchain and work together in updating it. This transparent process augments the security of the records by creating a trust-free layer that uses distributed consensus to authenticate and validate the contents of the processed and stored academic records.

The digitally signed transaction contains the date the academic record was stored on the public blockchain, and as such the record is publicly verifiable by users owing to the decentralized nature of a blockchain. Where academic records are directly signed, and recorded on the blockchain using a well-structured data format without the use of a cryptographic hash function, it is also possible to use an encryption algorithm to protect the records from public access. The encryption process is based on public/private key cryptography, which allows a public/private key pair to be created for a certain record stored on the blockchain. The public key is given to those who should have access to the public blockchain while the private key is used by the validator to access the blockchain database whenever necessary [17].

The key pair is created using Elliptic Curve Digital Signature Algorithm (ECDSA) based on the mathematics underpinning elliptic curves. This asymmetric key can also be used for digitally signing a document to validate that an update is approved by a network participant. The network participant's private key when generated can be added to the stored academic record for encrypting and each user that requires access to the public blockchain uses a public key, which is cycled through additional layers of encryption using SHA-256 and RIPEMD-160 (Race-integrity Primitives Evaluation Message Digest) [17]. Access to the public key is based on consensus between a

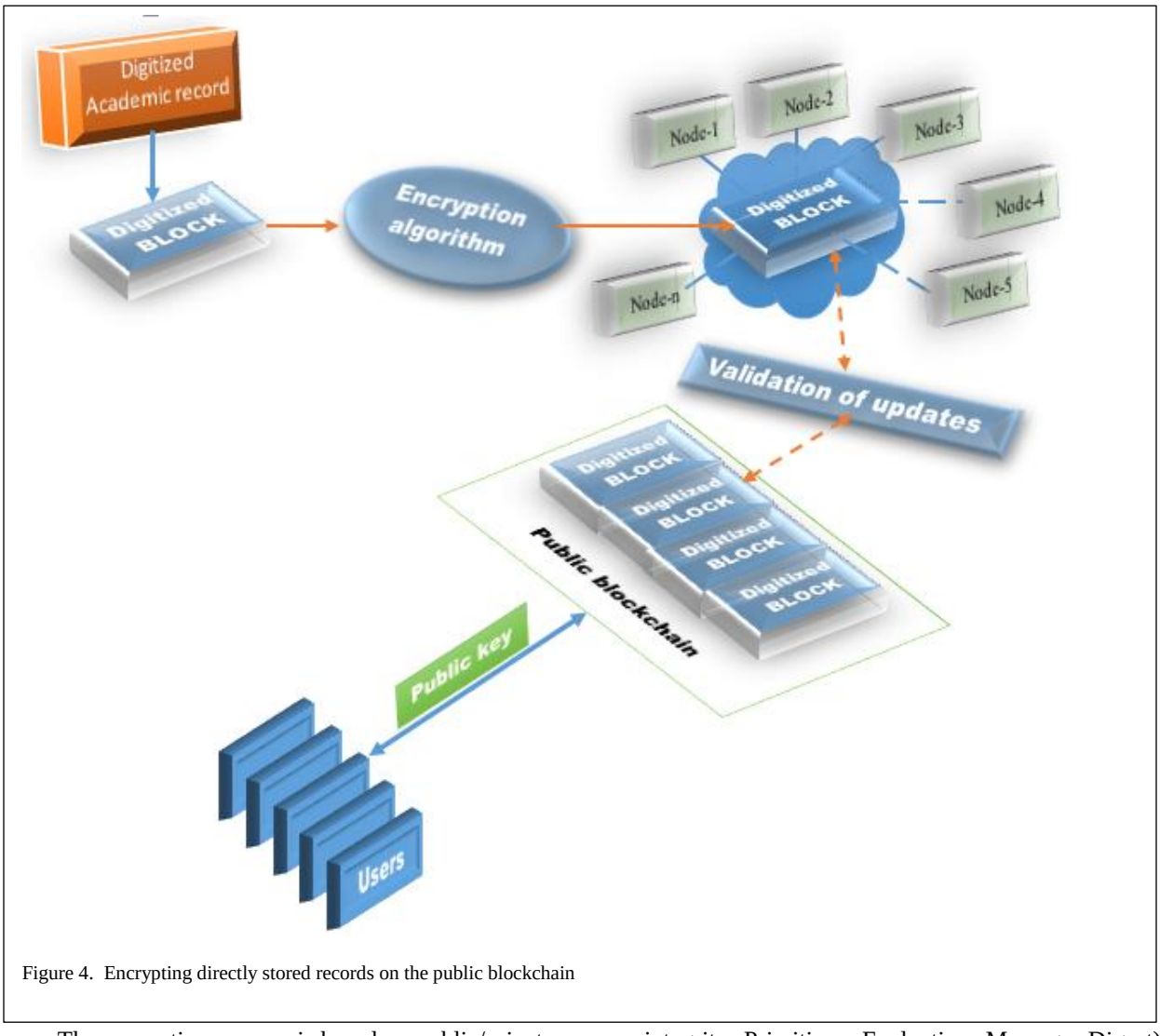

Figure 4. Encrypting directly stored records on the public blockchain

validator and users for viewing the contents of the blockchain database in a bid to prevent unauthorized access to academic records. This is illustrated in Figure 4.

Using ECDSA, which primarily is underpinned by elliptic curve cryptography, a relatively short encryption key can be generated, which is faster thus requiring less computing power especially when implemented over wireless devices with limited computing power, memory and battery life [22], [23], and [24]. Similarly, RIPEMD has higher levels of security against preimage attacks and has the property of being one way involving the irreversible transformation of identification data [25], [26], and [27].

V. CONCLUSION

This paper highlights an alternative approach to authoritative access to the database of academic records of tertiary institutions in Nigeria. The approach discusses the use of blockchain technology including distributed consensus for authorizing changes to stored academic records, the use of digital signature scheme and timestamp for signing and verifying the authenticity of the stored academic record as well as encryption algorithms for enforcing the integrity of the stored contents. The proposed framework has the potential, if implemented correctly, to eliminate the common issues of the centralized database approach, which allows an administrator to have so much control of classified data such as certificates, transcripts, testimonials and statements.

The digital signing of the transaction generated from the cryptographic hash of the original academic record creates a timestamp that can be used to verify that it is authentic in the future. This will eliminate illegal modification and falsification of academic records, and as such deliver an enhanced security standpoint at all times. Each network participant has a copy of the blockchain database locally stored and any intended update of the digitized academic record is communicated to all parties, which must validate such an update before it is implemented on a blockchain. This added layer of security and transparency augments the security of the digitized academic records through the implementation of the blockchain.

REFERENCES

[1] Onwudebelu, U., Fasola, S., & Williams, E. O. (2013). Creating Pathway for Enhancing Student Collection of Academic Records in Nigeria-a New Direction. *Computer Science and Information Technology*, *1*(1), 65-71.

[2] Mbam, B. C. E., & Odachi, G. N. (2014). Web-Based Virtual Transcript Processing and Transfer for Nigerian Universities. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, *9*(4), 15-20.

[3] Okikiola, M. A., & Samuel, F. (2016). Optimizing the Processing of Results and Generation of Transcripts in Nigerian Universities through the Implementation of a Friendly and Reliable Web Platform. *Imperial Journal of Interdisciplinary Research*, *2*(12).

[4] Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal*, *26*(2), 110-139.

[5] Utami, E., & Raharjo, S. (2014). Database security model in the academic information system. *International Journal of Security and Its Applications*, *8*(170).

[6] Afolayan, O. A., & Absalom, E. E. S. (2012). Design and Implementation of Students' Information System for Tertiary Institutions Using Neural Networks: An Open Source Approach. *International and Interdisciplinary Studies in Green Computing*, 193.

[7] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? —a systematic review. *PloS one*, *11*(10), e0163477.

[8] Pilkington, M. (2016). 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.

[9] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10.

[10] Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17.

[11] Mattila, J. (2016). *The Blockchain Phenomenon–The Disruptive Potential of Distributed Consensus Architectures* (No. 38). The Research Institute of the Finnish Economy.

[12] Sharples, M., & Domingue, J. (2016, September). The blockchain and kudos: A distributed system for educational record, reputation and reward. In *European Conference on Technology Enhanced Learning* (pp. 490-496). Springer, Cham.

[13] Raval, S. (2016). *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. " O'Reilly Media, Inc.".

[14] Wright, A., & De Filippi, P. Decentralized blockchain technology and the rise of lex cryptographia, 2015. *URL https://papers. ssrn. com/sol3/papers. cfm*.

[15] Herbert, J., & Litchfield, A. (2015). A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology. In *Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)* (Vol. 27, p. 30).

[16] Cachin, C. (2016, July). Architecture of the Hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

[17] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

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

[19] Gabison, G. (2016). Policy Considerations for the Blockchain Technology Public and Private Applications. *SMU Sci. & Tech. L. Rev.*, *19*, 327.

[20] Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Europe and MENA operation Advances in Information and Communication Technologies* (pp. 523-533). Springer, Cham.

[21] Gupta, P., & Kumar, S. (2014). A comparative analysis of SHA and MD5 algorithm. *architecture*, *1*, 5.

[22] Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications*, ////*11*(1), 62-67.

[23] He, D., Chen, J., & Chen, Y. (2012). A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. *Security and Communication Networks*, *5*(12), 1423-1429.

[24] Galbraith, S. D., & Gaudry, P. (2016). Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, *78*(1), 51-72.

[25] Ghosh, R. (2014). The Techniques behind the Electronic Signature based upon Cryptographic Algorithms. *International Journal of Advanced Research in Computer Science*, *5*(3).

[26] Zeb, M. A. (2014). Enhancement in TLS Authentication with RIPEMD-160. *International Journal*, *2*(2), 402-406.

[27] Smart, N. P. (2016). Hash functions, message authentication codes and key derivation functions. In *Cryptography Made Simple* (pp. 271-294). Springer, Cham.