A Note on Blockchain Authentication Methods for Mobile Devices in Healthcare

George-Mircea GROSU, Silvia-Elena NISTOR
Distributed and Parallel Computer Science - Faculty of Automatic Control and Computers
Bucharest, Romania
george_mircea.grosu@stud.acs.upb.ro, silvia_elena.nistor@stud.acs.upb.ro

Emil SIMION
Center for Research and Training in Innovative Applied Mathematical Engineering Techniques "Traian Lalescu"
Faculty of Applied Sciences - Politehnica University of Bucharest
Bucharest, Romania
emil.simion@upb.ro

Abstract: The past couple of decades witnessed a tremendous expansion in the IoT world that gathers now billions of devices, sensors, users and transactions. The aspirations of ubiquitous computing have drastically changed the computing world, from a parallel point of view, to distributed, then grid and cloud computing – all these just to keep up with the proliferation of devices and the users' expectations. Alongside with this fast development, many issues appeared, especially in terms of scalability and security. Regardless of protocols, devices, applications or technologies used, critical data will be involved and, therefore, vulnerabilities that can affect the performance of the system or allows them to be maliciously exploited. The higher the number of devices, the more constraints appear and along with these constraints the existing models and technologies become overwhelmed and simply not enough. The size of the IoT and its autonomous character make it impossible to sustain and implement a centralized authentication system. Therefore, to allow reliable peer authentication and to approach a trust level management, we propose discussing a model based on blockchain technology. Blockchain is a revolutionary technology, modeled by a linear sequence of blocks, considered to be the future of wireless networks security (Li et al., 2018). We rely on this new data structure to address two major components of security in mobile networks: authentication and trust.

Keywords: Cryptographic Authentication, Trust, Anonymity, Wireless, Mobile, Hash Functions, Healthcare, Blockchain

INTRODUCTION

Wireless networks are widely used nowadays and electronic devices all over the world are interconnected. The amount of data that is sent across the network must be validated and transferred securely, to ensure its integrity. To overcome the limitations of a centralized authentication system, we propose the analysis of a new model based on the revolutionary technology called blockchain (Songara et al., 2018). Motivated by its success in cryptocurrency, blockchain technology has become a hot topic nowadays and has been studied in the environment of wireless networks. These types of networks are vulnerable to a large variety of attacks, such as spoofing or eavesdropping and are also prone to limited resources and higher

http://doi.org/10.54851/v4i1y202209

constraints in terms of energy and memory capacity, which makes it even more difficult to implement advanced security solutions (Hammi et al., 2018). We rely on the decentralization, anonymity and proof of security characteristics of blockchain to help us create a model of secure authentication and authorization for mobile decentralized networks (Wu et al., 2018). The authentication step acts as a gateway access towards the device, followed by the authorization, which determines which transactions and operations are permitted. In this article, our purpose is to provide a new authentication and authorization scheme, based on blockchain technology in a typical health-care scenario.

BLOCKCHAIN

Blockchain technology is known as the underlying technology for cryptocurrencies, but in-depth knowledge upon this subject has not yet reached the majority of population. Blockchain is still at the beginning of its expansion and shows great potential in various domains. Research upon cryptographically secured chain of blocks has begun in 1991 by Stuart Haber and W Scott Stornetta, but the real break- through was made by Satoshi Nakamoto in 2008, when he released a model for the first real application of blockchain – Bitcoin. Fast forwarding to our days, more than 10 years later, this technology proved its potential by becoming more and more popular in the financial and investment world, especially amongst cryptocurrency enthusiasts around the world. Before discussing the ongoing research on how this technology can be used in other domains as well, let us introduce the concept and characteristics of blockchains.

Blockchain is a distributed database, shared among the nodes of a computer network, that stores information in digital format, more specifically, permanent and tamper-proof records of transactional data (Hammi et al., 2018). The innovation brought by the blockchain technology consists of removing the single point of failure from centralized models and generates trust without involving third-parties.

A. BLOCK

Unlike a traditional database, where information is stored in tables, a blockchain collects it in blocks with certain storage capacities, that are chained to previous filled blocks. A block consists of the block header and body (Figure 1). The first block in a blockchain is called "genesis block" and therefore, does not have a parent block.

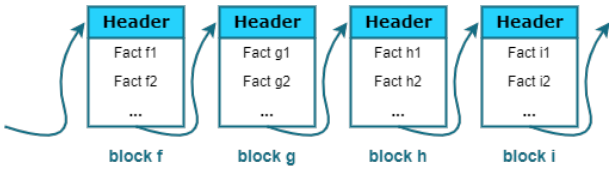

Fig 1.: *Blocks structure (Hammi et al., 2018)*

B. HASHING

Because all the data is timestamped, the blockchain becomes inherently immutable – the longer the chain, the harder it is to alter it. Blocks are stored linearly, in chronological order, so if an entity would want to alter a block, they would have to change all the following blocks and all the copies from all the nodes. Blocks are linked through their hash codes, which are altered whenever any change is inflicted upon a block. An attacker could perform such a malicious alteration only when it obtains a control of 51% (for reaching consensus) or more of the copies of the blockchain, which would require a tremendous amount of resources. Moreover, the output of the hashing function is determined by the input, but given the hash, it is impossible to determine the input.

C. MERKLE TREE

As previously mentioned, a block is formed of a header and a body. Amongst other fields, the header contains a timestamp, a hash that refers to the previous block and a hashed list of the transactions occurred since the last block. A hash tree, also known as Merkle Tree (Figure 2), is used to encrypt data in blockchain.

- Leaf node → hash of a block
- Non-leaf node → hash of its child nodes' hashes

The top of the tree is called Merkle ROOT, which is exactly the hash function applied on all of the transactions that took place since the creation of the last block. The advantage of enabling this data structure is a quick and secure data validation across big datasets.

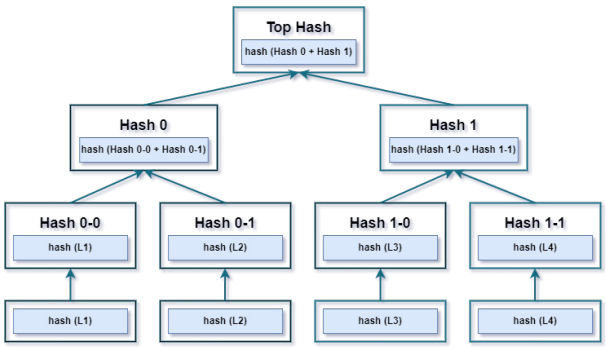

Fig 2.: *Blocks structure (Lim et al., 2018)*

D. CONSENSUS

In a blockchain, there are mainly two types of nodes:

- Nodes that perform read operations – passive nodes
- Nodes that perform read and write operations – active nodes. These nodes are called MINERS.

It is compulsory for miners to perform a consensus protocol in order to prove that the transactions are valid. Consensus algorithms come as a solution to the famous Byzantine Generals' Problem, where a group of nodes tries to make a decision despite the fact that the credibility of some of the nodes might be altered.

Consensus algorithms are generally measured by determining their tolerance to faulty/ questionable processes. In the synchronous case with known participants, no existent solution tolerates more than (n-1)/3 byzantine faults. For the asynchronous approach, Paxos algorithm can tolerate (n-1)/5 byzantine faults, the phase algorithm (Attiya, Doyev, Gill) can tolerate (n-1)/4 faults and the BFT-CUP no more than (n-1)/3, even with unknown participants.

The validation process in blockchain is based on different criteria, depending on the mechanism of consensus adopted, be it competitive, voting or luck-based (European Union, 2016). Among the most popular mechanisms involved in transaction validation and consensus protocols are (Lim et al., 2018):

- **Proof of Work** – solve mathematical puzzles to validate new blocks of data. It is a random process and requires a great amount of computational power, electricity and bandwidth, which can become a concerning disadvantage.
- **Proof of Stake** – by alleviating the downsides of Proof of Work, this approach seeks to make a correlation between the power of a node and its stake. In this case, the user must prove its investment in the network in terms of stake, not in computing power. The goal is to alleviate concerns regarding the environmental sustainability and scalability associated with Proof of Stake.
- **Proof of Importance** – this algorithm values the nodes in regard to their activities and utility in the network. The concept is similar to Proof of Stake, but the metrics and criteria involved are different: net transfer, currency vested, cluster nodes.

E. BITCOIN

Bitcoin (Nakamoto, 2009) is a peer-to-peer digital, decentralized cryptocurrency created by Satoshi Nakamoto in 2008. In terms of structure, the first block ever created in Bitcoin is called "Genesis block ". The fields stored in a Bitcoin block are:

- block size
- block header
  - previous block hash
  - Merkle root
  - timestamp
  - difficulty target
  - nonce
- counter
- transactions

Regarding the mining process in Bitcoin, any machine in the network can have the role of miner and use its processing power to solve the mathematical puzzle required for the proof of work. In this regard, various hardware are used: CPU, GPU, FPGA mining, etc. The more miners there are, the more difficult the challenge becomes, therefore, a new block is added in the average of 10 minutes. The miner that managed to mine a block receives a reward in Bitcoins.

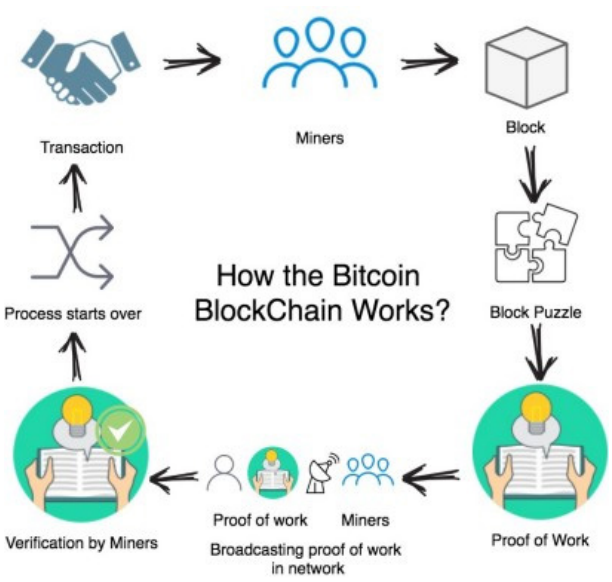

Fig 3.: *Bitcoin Blockchain Workflow (Ghimire & Selvaraj, 2018)*

The proof of work is based on a cryptographic puzzle, that searches for a value called NONCE. Afterwards, this value is hashed with SHA-256 and the result begins with the number of zero bits (Nakamoto, 2009). The work needed to achieve this proof of work is exponential with regards to that number of zeroes, which shows indeed the great computational costs required from the miners. The miner computes the hash of a block with different values for nonce until the result reaches a certain target value, which consists of a 256-bit number, shared between the miners.

F. ETHEREUM

The second most well-known open source application of blockchain technology is Ethereum. Bitcoin requires a lot of resources and is non-Turing complete (Alilwit, 2020), so Ethereum was built to compensate these limitations. Vitalik Buterin proposed it in 2013, in his whitepaper, "Ethereum: A Next Generation Smart Contract and Decentralized Application Platform".

This blockchain-based application is a platform built for smart contracts, which are Turing complete programs, executed by Ethereum Virtual Machine (EVM) in bytecode, in order to manage digital units of value in a decentralized fashion. The mining operation is very much alike the one in Bitcoin, based on Proof of Work, creating and validating blocks. However, the block size is shorter in Ethereum and it takes about 14 seconds to validate a block in Ethereum, unlike 10 minutes in Bitcoin. As a consensus protocol, Ethereum uses GHOST protocol, Ethereum Greedy Heaviest Observed Subtree (Hammi et al., 2018). To execute the smart contracts, a small fee is required, which is called "gas ". This fee is proportional to the size of the instructions, so bigger instructions involve more gas required. The topology of the Ethereum network is formed as a peer-to-peer network, where each node runs an Ethereum client, and is responsible for synchronization with other clients.

Whereas Bitcoin is mainly used as an alternative to traditional currencies, Ethereum finds many more applications besides cryptocurrencies (ETH), such as smart contracts, non-fungible tokens (NFT) or decentralized finance (DeFi).

STATE OF THE ART

In the past decade, we have witnessed a growing interest in the blockchain technology, since it proved its potential in various domains. The literature discusses major future development in the blockchain ecosystem, regarding possible applications meant to face the numerous challenges that occur inherently. Scalability and privacy leakage are major points of concern that are often addressed in research studies and proposals. Indeed, it is difficult to alter a block in a blockchain, by the very definition of this technology, but that does not necessarily mean that transactional privacy is completely secure and the small possibility of linking the real identity of the user with its addresses and transactions still remains. However, considering some major key characteristics of blockchain, such as decentralization, anonymity, persistency, traceability and transparency, the potential is tremendous and research continues to leverage it in different areas of application - healthcare, finance, business or even real estate.

In the financial area, the European Union Agency for Network and Information Security (ENISA) saw the opportunity of distributed ledger technology being used in improving

cybersecurity (European Union, 2016). The authors manifest their goal to optimize time and cost resources for operation, to minimize human interaction with the system and to remove third-party or central entities through blockchain. Cost and speed efficiency are the highlight of the 21st century and the finance sector is heavily dependent nowadays on digitalization. Therefore, it runs at the parameters offered by the underlying technology. The challenges identified by ENISA that are associated with blockchain refer to some traditional concerns: key management, privacy, cryptography but also to some technology-related issues: consensus hijack, sidechains, DDoS, scalability, wallet management, lack of anti-fraud tools, and some others. For each and every one of these concerns, the authors propose a book of good practices, meant to alleviate the possible attacks on the system.

Although the blockchain has a strong degree of security when it comes to the chain itself, a major concern remains regarding the storage and management of private keys. In "BIDaaS: Blockchain Based ID as a Service", the author (Lee, 2018) identifies this concern and proposes a new blockchain based ID as a service solution to provide identity and authentication management from providers to partners. This infrastructure is based on a private blockchain, managed by the provider, whereas the partners have read-only permissions. A user is generally registered to the provider and requires access to one or more services offered by the partners, without giving away personal information directly to the partner. The provider then proceeds to register a form of unique identification for the user, generally by signing a virtual ID and public key of the user with the private key of the provider. Based on the data written on the BIDaaS blockchain and the user's public key information, the partner can confirm the identity of the user and begin the mutual authentication process. Therefore, the user no longer needs to create unnecessary accounts for different services that may be scarcely used and, on the other hand, the service provider no longer needs to maintain a local authentication and identity management infrastructure.

Due to the rising expansion of IoT, a centralized authentication system is a matter of utopia. In the article "Bubbles of Trust", the authors (Hammi et al., 2018) envision a decentralized authentication system to meet the needs of mutual authentication in an interconnected system of systems as IoT, where many devices are almost or fully autonomous. The name refers to the creation of virtual trusted zones, where devices can identify and trust each other, based on the technology of blockchain. The solution assumes that the underlying network is unreliable and potentially lossy, without some strong mechanisms to ensure integrity or authentication and therefore is prone to malicious attacks, such as alteration, dropping or injection of messages / packets. Inside a bubble of trust there is a Master and the Followers, who receive a ticket in the form of a lightweight certificate, signed by the Master. Once the Master is chosen, the group is defined and the Followers are given the tickets - initialization phase. The next step consists of transposing the bubble created onto the blockchain. This process translates as a transaction that contains the Master's ID and the group ID and after the validation of the transaction, the bubble is created. In this approach, a public blockchain is used, so anyone can create a bubble. Then, the Followers send transactions to adhere to a certain group, through their tickets. Objects with fake tickets or with no ticket at all are not permitted and thanks to the signature of transactions, data is secure and bubbles are completely isolated from each other.

Needless to say, the blockchains can be used in many approaches, depending on our goals and architecture of the system, on the requirements, constraints and users' expectations. In the following we describe our proposed solution that aims to complement the existing ideas and provide a reliable scheme to authenticate and identify users, while also considering some of the guidance points formulated by ENISA and the five main security goals: availability, scalability, nonrepudiation, identification and mutual authentication.

USE CASE

We propose a model of authentication and authorization that will support the medical system. The digitalization of medical prescriptions is necessary in the fast-moving society we live in. It is inconceivable in the 21st century to wait in line for a piece of paper in order to buy your usual medicines. In this sense, the digitalization of the process of issuing and using a medical prescription resides in the authentication of the individual and his authorization for the use of certain services.

The main factors that delay this digitalization process are related to security. Security issues include threats such as:

- **abuse →** endangering human lives by abusively accessing drugs or services which can be life threatening in case of improper use. Both the fraudulent issuance of prescriptions and the repeated use of the same prescription are considered to be a breach in the authorization process.
- **tax evasion →** the system can be tricked by using false prescriptions to fraudulently obtain medical services.
- **breach of privacy →** if the process of anonymizing the information is reversible or weakly secured, sensitive information can be leaked. This information could be used for malicious purposes: blackmail, espionage, tampering the public image or even murder.
- **identity theft →** the authentication module may contain security breaches that facilitate the misuse of another individual's identity. Thus, we may end up using the wrong or unwanted permissions or authorizations in order to access or provide medical services without a specialist's recommendation.

The proposed model aims to solve these problems by anonymizing the personal data of the end user, authorizing it by certified entities in the field (medical staff), and consuming resources (medicine and medical services) – based on the authorization obtained. The whole process will be based on the innovative technology provided by blockchain.

The main steps of the system are described in Figure 4:

- The person goes to the general practitioner (GP) and requests a virtual identity (Virtual ID), empowered by GP authorization level;
- The virtual identity is uploaded and confirmed in the blockchain, thus becoming permanent;
- The GP creates a virtual identity signed authorization for that person, then signs it with his own virtual identity, and uploads it to the blockchain;
- The person goes to the service provider institution and, based on virtual identity, obtains the services for which he/she has been authorized.

1) A request is created based on patient virtual identity for the requested service;

2) The request is uploaded to the blockchain for validation;

3) If there is a match with a block able to authorize the current request, then the person will be able to benefit from services.

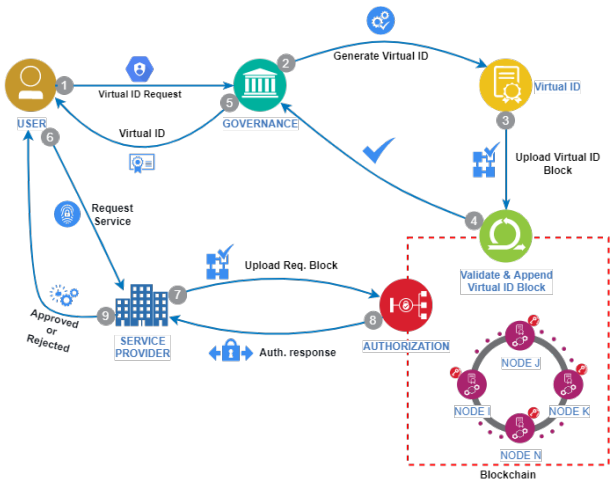

Fig 4.: Medical Prescriptions Model

SOLUTION

The proposed solution is based on two main components: the user authentication module in the virtual space and the authorization module that empowers a virtual entity to access a set of services (Alilwit, 2020).

A. AUTHENTICATION

It is based on the notion of virtual identity (Virtual ID), which transparently identifies a person in the online world. The generation of Virtual ID requires a centralized, reliable

creator entity that validates the real identity of the individual and creates and guarantees the virtual one (Gao et al., 2018).

Virtual ID is a digital certificate obtained by aggregating several information about the person:

- **Government Identity Number →** to verify the real identity of the person, the creator will verify the document issued by a trusted institution (the government);
- **Biometric Information →** for an increased entropy, we can include biometric data such as fingerprint or an iris scan;
- **Smart card or device →** the device based on which the Virtual ID is generated, and on which it will be stored;
- **User interaction →** without the physical interaction of the person holding the virtual identity, it cannot be used.

Once the digital certificate is generated, it is signed with the certificate of the creator entity and then submitted to the blockchain system for acceptance.

Using 4 types of information, we obtain a redundancy that allows the loss of at most 1 component, having the possibility to invalidate and create a new identity. Thus, the given solution aims to facilitate the ability to invalidate a virtual identity. This would be possible using a request made by the owner of the deprecated Virtual ID and signed with a new certificate generated based on the other 3 available means of identification.

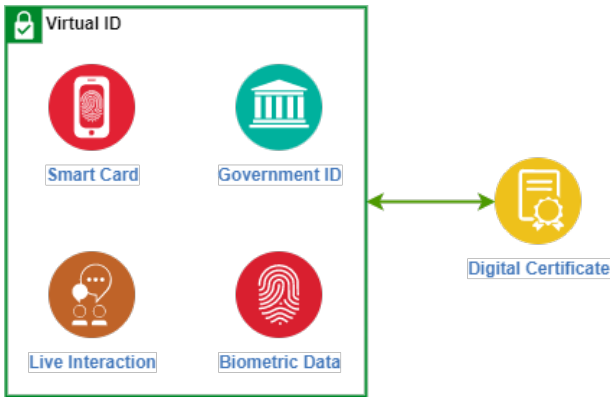

Fig 5.: *Virtual ID Model (Gao et al., 2018)*

B. AUTHORIZATION

This is the process of determining whether a user has the privilege to access the requested services. Thus, each service is characterized by a required level of authorization in order to use it (Lim et al., 2018).

In the proposed solution, the authorization is equivalent to the quantification of the access to certain medical services offered to patient by an authorized GP. In this respect, the process can be divided in two stages: provide quantum and consume quantum.

1) **Provide quantum →** following a basic service, such as a medical consultation, the authorized entity will make a request, based on the user's Virtual ID and signed with its privileged certificate, which provides the user with the required quantum of services. The request is submitted and recorded in the history of the blockchain;

2) **Consume quantum →** the service provider checks the authenticity and authorization level of the user. In this respect, the provider makes a request for accessing the services, signs it with the user's Virtual ID and submits it for validation. If the request is validated, it is recorded in the history of the blockchain in order to demote the Virtual ID privileges for consumed services. Otherwise, the Virtual ID will be marked for fraudulent intent and its trust will diminish.

Thus, our solution can achieve a decentralized authorization process, accessible for any provider willing to participate in the blockchain network, and managed within the limits of the law by certified staff, i.e., medical staff.

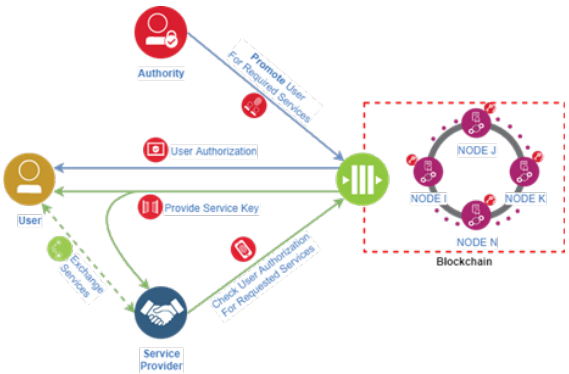

Fig 6.: *Authorization Process Model*

C. VULNERABILITIES

- **Identity hijacking →** the ability to access another person's identity without his/her consent. Our solution makes this type of attack more difficult by conditioning the virtual identity with the biometric data of the owner;
- **Man-in-the-Middle →** the attack is possible, not the alteration of the blocks, because they are signed with the private key of the source, a key that exists only on the user's smart card and which is not exposed to the internet;
- **Data breach →** blockchain transactions are public, which makes this vulnerability possible. If the owner of a virtual identity can be identified, then the entire medical history can be leaked and used in undesirable ways;
- **Data integrity →** once the blocks are in the blockchain, they are difficult to alter;
- **Data confidentiality →** the anonymization of the data is not treated. Thus, if sensitive data is included in the virtual identity, then it could be seen by anyone;
- **Human errors →** it is possible to lose the smart card, the identity card or to alter the biometric data. Therefore, we propose a system to replace the existing identity, based on the other 3 remaining components.

CONCLUSIONS

With in this paper, we have proved that a viable solution for optimizing the digitalization of healthcare services could be an authentication and authorization system based on blockchain technology, that leverages its main characteristics: anonymity, transparency, decentralization. Healthcare contains highly sensitive data, with heavy consequences upon users in the event of a malicious attack, which is why solutions involving blockchain have such a great potential in improving security.

Nevertheless, some problems still stand and need to be addressed in the future work: who participates in the network, how exactly an authorized node, capable of writing on the blockchain, can be identified, what consensus mechanism should be implemented for mobile devices, notoriously known for their limited computational resources, and how the data will be anonymized.

REFERENCE LIST

Alilwit, N. (2020). Authentication Based on Blockchain. In 2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC) (pp. 1-6). DOI: 10.1109/ipccc50635.2020.9391553

European Union. Agency for Network and Information Security. (2016). Distributed Ledger Technology & Cybersecurity. ENISA.

Gao, Z., Xu, L., Turner, G. Patel, B., Diallo, N., Chen. L. & Shi, W. (2018). Blockchain-based Identity Management with Mobile Device. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (pp. 66-70). DOI: 10.1145/3211933.3211945

Ghimire, S. & Selvaraj, H. (2018). A Survey on Bitcoin Cryptocurrency and its Mining. In 2018 26th International Conference on Systems Engineering (ICSEng), (pp. 1-6), DOI: 10.1109/icseng.2018.8638208

Hammi, M. T., Hammi, B., Bellot, P. & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, Computers & Security, 78, 126–142. DOI: 10.1016/j.cose.2018.06.004

Kim, H. W. & Jeong, Y. S. (2018). Secure Authentication- Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain, Human-centric Computing and Information Sciences, 8(1): 11. DOI: 10.1186/s13673-018-0136-7

Lee, J. H. (2018). BIDaaS: Blockchain Based ID As a Service, IEEE Access, 6, 2274–2278. DOI: 10.1109/access.2017.2782733

Li, D., Peng, W., Deng, W. & Gai, F. (2018). A Blockchain-Based Authentication and Security Mechanism for IoT. In 2018 27th International Conference on Computer Communication and Networks (ICCCN), (pp. 1-6). DOI: 10.1109/icccn.2018.8487449

Lim, S. Y., Fotsing, P., Almasri, A., Musa, O., Mat, K., Miss, L., Ang, T. & Ismail, R. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey, International Journal on Advanced Science, Engineering and Information Technology, 8(4–2): 1735. DOI: 10.18517/ijaseit.8.4-2.6838

Moinet, A., Darties, B. & Baril, J. L. (2017). Blockchain based trust & authentication for decentralized sensor networks. ArXiv, arXiv:1706.01730v1 [cs.CR]. Available at: <https://allquantor.at/blockchainbib/pdf/moinet2017blockchain.pdf>.

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: <https://metzdowd.com. https://www.researchgate.net/publication/228640975_Bitcoin_A Peer-to-Peer Electronic Cash System>.

Songara, A., Chouhan, L. & Kumar, P (2018). Blockchain Security for Wireless Multimedia Networks. In Ramakrishnan, S. (eds.), Cryptographic and Information Security, pp 28.

Tan, H. & Chung, I. (2020). Secure Authentication and Key Management with Blockchain in VANETs, IEEE Access, 8, 2482–2498. DOI: 10.1109/access.2019.2962387

Wu, L., Du, X., Wang, W. & Lin, B. (2018). An Out- of-band Authentication Scheme for Internet of Things Using Blockchain Technology. In 2018 International Conference on Computing, Networking and Communications (ICNC), (pp. 769-773). DOI: 10.1109/iccnc.2018.8390280