Computer Systems Science & Engineering
DOI:10.32604/csse.2021.05480
Article

Tech Science Press

Using Blockchain Technology in Mobile Network to create decentralized Home Location Registry (HLR)

Behnam Kiani Kalejahi[1,2,*], Ruslan Eminov[1] and Aga Guliyev[1]

[1]Department of Computer Science, School of Science and Engineering, Khazar University, Baku, Azerbaijan
[2]Department of Biomedical Engineering, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
*Corresponding Author: Behnam Kiani Kalejahi. Email: bkiani@khazar.org
Received: 22 June 2020; Accepted: 22 January 2021

Abstract: Blockchain can mean many things to many people. It is a set of protocols and encryption technologies for securely storing data on a distributed network for the developers. It is a distributed ledger for business and finance and the technology underlying the explosion of new digital currencies. For technologists, it is the driving force behind the next generation of the internet. On the other hand, it is a transformational technology facilitating large-scale human progress in previously unimagined ways for the rest of the people, a tool for radically reshaping society and economy. Some view it as a disruptive technology that can be the source of a great deal of fraud, illegal activity, where others see opportunities to bring into existing systems by providing decentralization, transparency, and efficiency. This complex technological, economic, and social phenomenon has been the subject of fervent debate. It calls into question what might have been seen to be established parameters of the modern world like currency, economics, trust, value, and exchange. It is a revolutionary new computing paradigm and one of the most significant, fundamental digital platforms' advances since the internet. It is an emergent technology experiencing very rapid evolution, and so is our understanding of what it is and what it can be. This paper is subject to the use of Blockchain concepts in mobile networks to strengthen the Home Location Registry (HLR) database and make it decentralized for secure transactions and in banking and financial centers. Blockchain also holds potential implications for global commerce. It could make trade more efficient by removing the manual and paper-based processes and introducing streamlined and automated processes.

Keywords: Blockchain; Mobile Network; Home Location Registry; Mobile Technology

1 Introduction

Dramatical increase in Bitcoin prices at the beginning of 2017 attracted people's attention, and Blockchain technology was considered one of the best and trending innovations of the 21st century. However, most people still don't know that Blockchain's invention was originally in the early 1990s. The idea behind Blockchain technology was created in 1991 by Stuart Haber and W. Scott Stornetta,

where they aimed to develop a cryptographically secured chain of blocks that the timestamp could not be tampered with.

As an upgraded version of the idea, the Merkle tree is applied to the concept where multiple documents could be merged into a single block to improve efficiency. For years, this technique remained useless until a person or organization called Satoshi Nakamoto conceptualized Blockchain as cryptocurrency and got involved in many other applications after that.

1.1 Blockchain Explanation

In this new information technology, distributed computing is combined with cryptography to create a model for a secure database that can keep an immutable record of transactions. The things that make this database new and different from traditional record-keeping technologies are the following: This database is open to all Blockchain network members [1].

All members are equally privileged in this network, and there is no such thing as privileged access to the database. There is no central authority or trusted third party to validate, verify, or audit the database. Instead, the database is managed autonomously using a peer-to-peer network and distributed timestamping server. No one member of the Blockchain network is trusted, and no one member needs to be trusted. There is no central storage where the database is stored. Every member of the network has a copy of the Blockchain database [2].

There is no "official" copy of the database as there is no one member in this network whose version of the database is "trusted" more than any other member. The same information is distributed to every member of the Blockchain network.

The block's changes are validated by most network members' consensus and added to a new block by miners. This new block reflecting the changes made to the block is then added to the Blockchain. Miners update the Blockchain using specialized software and their computers' processing power after verifying the validity of the changes [3].

Thousands and thousands of network members confirm the addition of a new block to the Blockchain, making it highly unlikely for anyone to beat the combined computing power of the network to add a "bad" block to the chain. Such a design removes the characteristics of infinite reproducibility from a digital asset and facilitates a robust workflow where participants' uncertainty regarding data security is marginal. Trust between network members is established collaboratively using protocols (Distributed Consensus Algorithms) and cryptography instead of a trusted third party [4].

Instead of using tables, this new database stores data in data structures called blocks. Data that is stored inside a block can be anything depending upon the type of the Blockchain and what it is used for. Each block contains a cryptographic hash from the previous block linking the two. A hash uniquely identifies the block and its contents. Hash is useful to detect any changes made to the block. A link created between blocks is called a chain. The chain is a hash of the previous block inside any given block. The chain is not the only thing that is stored inside a block. Each block contains data about a transaction and a timestamp in addition to the chain. Blocks store records of valid transactions that are hashed and encoded into a Merkle tree [5]. The chain between blocks makes any alteration or change to any block affect all subsequent blocks. This means records cannot be altered retroactively without the alteration of all subsequent blocks. This allows network members to verify and audit transactions independently and relatively inexpensively. A timestamp serves the purpose of keeping track of the creation time of a record in a database. The first block in a database is called a genesis block. The previous block's integrity is confirmed to the genesis block [6].

New blocks are added linearly and authenticated by mass collaboration. They are powered by collective self-interest. The structure of the block alone does not guarantee that data stored inside a block is tamper-proof. As with the power of today's computing technology, it is possible to compute millions of hashes in

a second and make your Blockchain valid again. To mitigate this, Blockchain uses proof-of-work. It is a mechanism that slows down the creation of new blocks. It takes about 10 minutes to calculate the required proof-of-work in bitcoin's case and add a new to the chain. This mechanism makes it very hard to tamper with the blocks because if you tamper with one block, you'll need to recalculate hashes for all the subsequent blocks. The security of Blockchain comes from its creative use of hashing and the proof-of-work mechanism.

But there are other ways that Blockchain secures itself, and that is by being distributed and decentralized. This decentralization and distribution of a database eliminates the risk of centralized points of vulnerability and replaces the middleman between parties in a transaction with mathematics. All these Blockchain database properties work in conjunction to make a Blockchain to be trusted as a single source of truth. It is thanks to these properties; it is called a trust machine. Blockchain is not only a distributed database. It is a protocol to define the rules of communication between computers using the same distributed database. Just as the open communications protocol created profitable business services by catapulting innovation, the Blockchain protocol offers a similar foundation for businesses to create value-added chains [7]. Heretofore, we viewed Blockchain simply as a distributed database, which is what it was originally intended to be.

1.2 Blockchain in Banking

Blockchain was invented as a peer-to-peer network that enabled keeping records of bitcoin's two-way payment transactions. (Blockchain 1.)

But Blockchain soon outgrew its original purpose. It now can become a system of records for all internet transactions, in other words. It can become a foundational technology creating a new technological infrastructure for our entire economic and social systems.

During its evolution up to now, Blockchain has passed through developmental stages (Blockchain1, Blockchain2, and Blockchain3) from essentially being a distributed database to becoming a fully-fledged globally distributed cloud computing. The first Blockchain (Blockchain1.0) was conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto. The concept and technicalities were described in the white paper "Bitcoin. A Peer-to-Peer Electronic Cash System" [8].

These ideas were first implemented in 2009 as a core component supporting bitcoin, where it served as a public ledger for all transactions. The Blockchain's invention for bitcoin made it the first digital currency to solve the double-spending problem without the need for a trusted authority or central server. It was only later that we came to separate a Blockchain concept from its specific implementation as a digital currency. It was seen that the underlying technology had more general applications beyond digital currency and could be used as a distributed ledger tracking and record the exchange of any form of value. It has been called a value-exchange protocol owing to its inherent design characteristics [9].

Within just a few years, the second generation of the Blockchain (Blockchain2.0) emerged, which was designed as a network on which developers could build applications was essentially the beginning of Blockchain's evolution into the distributed virtual computers. This was made technically possible by the development of the Ethereum platform. Ethereum is an open-source, public, Blockchain-based distributed computer platform featuring Smart Contract functionality. It provides a decentralized Turing-complete virtual machine that can execute computer programs using a global network of computers. Initially described in a white paper in 2013, Ethereum's goal was to build distributed applications. Two years later, the system was implemented, attracting a large and dedicated community of developers, supporters, and enterprises.

Ethereum's important contribution to Ethereum was that it worked to extend Blockchain technology's capacity from being primarily a database supporting bitcoin to becoming a general platform of value-exchange on a global scale. While Blockchain2.0 is a big step forward, it has performance issues when handling an increased number of transactions. The volume of transactions it can efficiently handle is a

significant constraint on its way. The speed of handling transactions is measured in transactions per second. As of 2018, Ethereum can handle 15 transactions per second by comparison to a credit card network capable of handling more than 24.000 transactions per second [10].

Another essential factor to consider is the cost of handling these transactions. While for a limited number of large transactions, it works efficiently for a large number of small transactions, it simply cannot be done in the existing form of Blockchain technology (Blockchain2.0). Such a large number of small transactions would require enabling a high volume of machine-to-machine exchanges. It would prove too expensive to operate in this kind of economy that involves many small exchanges. But this is exactly what many people want to use Blockchain for in the future.

In response to these constraints, the third generation of Blockchain is currently under development (Blockchain3.0). Many different organizations build this next-generation Blockchain infrastructure, such as NEO, Ethereum, and Lighting Network, and many others using different approaches to overcome existing constraints. Lightning Network is one such project that seeks to extend the capacity of existing Blockchains [11]. The main idea is that a small and nonsignificant transaction does not have to be stored on the main Blockchain. This is what is called an off-chain approach where small transactions are recorded off of the main Blockchain. It works by creating small communities where the record of those small transactions can occur without each transaction handled by the main Blockchain.

A payment channel is opened between a group of people with a fund being frozen on the main Blockchain. Those members can then transact with each other using their private keys to validate the transactions.

This is like having an IOU (I owe you) with the shop where you just mark down what you have exchanged so that you do not have to update the main record each time you make a purchase. The records stay local between the members involved until finally setting the finances and update the main record. This only requires two transactions on the main Blockchain. One for opening a transaction channel and one for closing. All other small transactions take place on the small network without being registered on the main Blockchain. This reduces the workload on the main Blockchain and makes it possible to run many small transactions fast within the subnetwork. As of the start of 2018, there was proof of concept running on the bitcoin test network [12].

IOTA is another example of the Blockchain sequential chain and where blocks are added in a regular, linear, and chronological order. The data structure of the IOTA system can achieve high transactional throughput by having parallel operations. The data structure is more like a network than a linear chain, where processing and validation can take place alongside each other. The other big difference is that there are no specialized miners in this network.

Every node uses the network functions as the miner. In the IOTA network, every node making a transaction also actively participates in forming the consensus. That is to say, every member of the network does the mining instead of having specialized miners. There is no centralization of the mining, which works to create bottlenecks and demands lots of energy. Likewise, there are no transaction fees for validation in the IOTA network. Because it is user-generated content, the more people use the network, the faster it becomes, which is the opposite of existing systems, making IOTA very scalable.

There are lots of other approaches to overcome the existing constraints of Blockchain technology. But suffice it to say the Blockchain should be understood as an emerging technology whose existing implementation is like a large-scale proof of concept running on a very inefficient system. Hopefully, through experimentation, in the coming years, it will evolve into globally distributed cloud computing.

As Melanie Swan writes in her book: “First there were mainframes and PC paradigms, and then the internet revolutionized everything. Mobile and social networking was the most recent paradigm. For this

decade, the current emerging paradigm could be the connected world of computing, relying on Blockchain cryptography" [13].

Blockchain first started to be used for cryptocurrency, Bitcoin. Then alternative usages are derived from the cryptocurrency example. The first extensive use of the Blockchain was suggested by the programmer and co-founder of Bitcoin, Vitalik Buterin, in 2013. He suggested using the technology to build a decentralized application by adding scripting language to Bitcoin; however, he could not get the community's agreement. After that, Vitalik developed its own distributed computer platform, Ethereum, which introduced Smart Contracts. That was the first trigger to spread Blockchain into many different areas such as healthcare, trade, insurance, notary, e-payment, copyright protection, supply chain management, government, etc. Smart contracts, which are executed on the Ethereum platform, consist of programs or scripts running on a decentralized Ethereum virtual machine (EVM). The program or script in Smart Contract creates different conditions, and if those conditions are met, then transactions are processed [14].

Ethereum platforms also provide flexibility for developers to build and publish their applications inside the Ethereum Blockchain, which are called DApps or Decentralized Applications. We consider the home location registry using the modified Blockchain concept to prevent the possible risks and weaknesses and provide secure servers with more complexity in front of attacks [15,16].

2 Concept of Home Location Registry

HLR (Home Location Registry) is considered the main user information database in the mobile network, containing all permanent information related to 2G, 3G, 4G, or 5G subscribers. HLR contains user identity information such as billing details, IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Station International Subscriber Directory Number), Subscribed Services (Missed Call Alert, Caller Tone or any other services), Authentication Information, etc. [17,18].

HLR has another version that holds temporary user information called Visitor Location Register (VLR). VLR holds user information such as subscriber location, mobile status on or off, etc., to decrease the number of queries to HLR when the subscriber is roaming at Home or Visiting Public Land Mobile Network (PLMN).

Missing or abduction of information from HLR may result in catastrophically for the Mobile Network Operator (MNO), which makes it a critical node in the network. Usually, operators keep their HLR separated into different nodes to have geographical redundancy. In this case, if one of the HLRs is failed, the other one can take the load. The common solution to protect the HLR system from outside attacks is limiting the access to the HLR from outside of the network and just providing access from the Local Area Network (LAN).

But there is no specific firewall or protection mechanism against possible attacks on the specified node from the security side. The behavior of those attacks can be both for stealing information from the HLR or interrupting the functionality of the network equipment and network accordingly [19–22].

3 Proposed Method

The current mobile network provides information security by using Authorization, Authentication, and Encryption, which verifies user and users' privileges then encrypts the messaging so that the message can only be read by using a specific key between them network nodes or between user and network. Also, most mobile operators build their networks with geographical redundancy from the redundancy side. If any of the critical nodes are out of services that affect the service's performance, then other nodes can take a full load of the network. Depending on the resources and geographical area that the operator serves, they may include 2 or more backup nodes on their networks. These backup nodes can serve as load sharing or active/standby, depending on the operator's choice.

Above mentioned specifications help to build a secure network with redundancy and are widely used by mobile operators. However, the increasing speed of technological development also improves hacking mechanisms, requires protection techniques, and reduces weaknesses. Some of the weaknesses of traditional HLR on mobile networks are given below.

Weaknesses on the current HLR node:

1. Single point of failure: Most MNOs are using 1 or 2 separate HLRs in their network. But it still does not avoid the risk because usually, data in these nodes are different, and if the node is failed, the second one will keep working but will not carry the information those were existing on the failed node.
2. No specific protection if the attacker had access to the local network.
3. No protection if someone from inside the network tries to change user data.

This paper suggests using a modified Blockchain concept on the HLR node to prevent the above risks or weaknesses. As described in Section 2.1, Blockchain requires different servers to provide security, and more servers mean more complexity against attacks [23,24].

Using this approach, different servers are considered different HLR nodes that are working together as a pool. Each HLR holds a portion of the total data, which is only hosted by this specific node. When they all come together, they create one unique HLR database.

Other than user information belonging to it, each HLR also holds a portion of data from all other nodes. For example, if there are 10 HLR nodes on the network working together on Blockchain logic together as a single HLR, each node consists of its data and one-ninth (1/9) of data from every other node. Fig. 1 shows the data structure design of a node in the chain. Having a portion of the other nodes on every node gives sustainability to the network as if any of these nodes fail, then the data can be restored from other nodes.

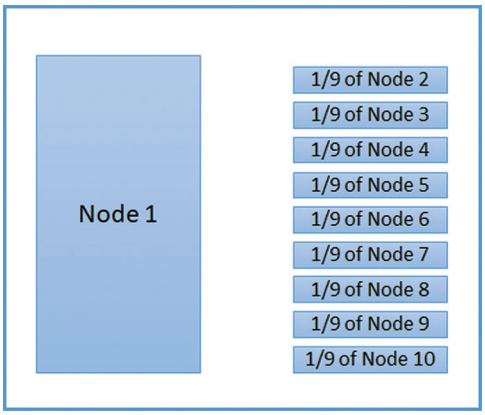

Figure 1: Example design of data structure in a node

but consistency is not the only reason to use multiple nodes. Multiple nodes are used for multiple levels of authentication of the inserted data as well. This specification prevents the database from incorrect data insertion because, regarding the Blockchain theory, before adding a block to the chain, the block should be verified by all nodes, which were called Proof of Work (PoW) in the Blockchain. The verification process will be done according to defined standards. One of the main reasons to use multiple validators in the Blockchain is to create a database where the timestamp cannot be tampered with. The same concept applies to HLR practice, as well. Similar to the Blockchain, a hash will be calculated for each generated new block. The hash is calculated based on an algorithm that takes the content of newly added data as

the input and encodes it cryptographically. The HLR block includes its hash and the hash of the previous block, similar to Blockchain. All nodes have the full HLR chain, including all generated blocks with the hash and hash of previous data but not the server's actual data.

4 Advantages and Disadvantages of the Proposed Method

All new methods are invented to overcome some difficulties or weaknesses, and it also brings disadvantages to themselves. This section is aimed to analyze the advantages of the suggested methods and disadvantages it brings compared to the traditional HLR concept. The suggested solution mainly avoids a single point of failure by having a decentralized network of HLRs. Also, by having multiple split copies of the data, it is easier to restore the failed node data. Additionally, all blocks are timestamped, and each block carries a hash of the previous block, which means if any backdated data is tried to be modified, all blocks after that created block needs to be changed one by one. In Fig. 2 the block's hash is generated using an encryption algorithm, which changes automatically if any previous content in the database is changed. So, if any old data is tired to be changed, the hash will be changed automatically, which will not match the hash in the next block and as a result system will decline the change. But the method also brings some disadvantages to the current network if applied on a traditional network of the MNO.

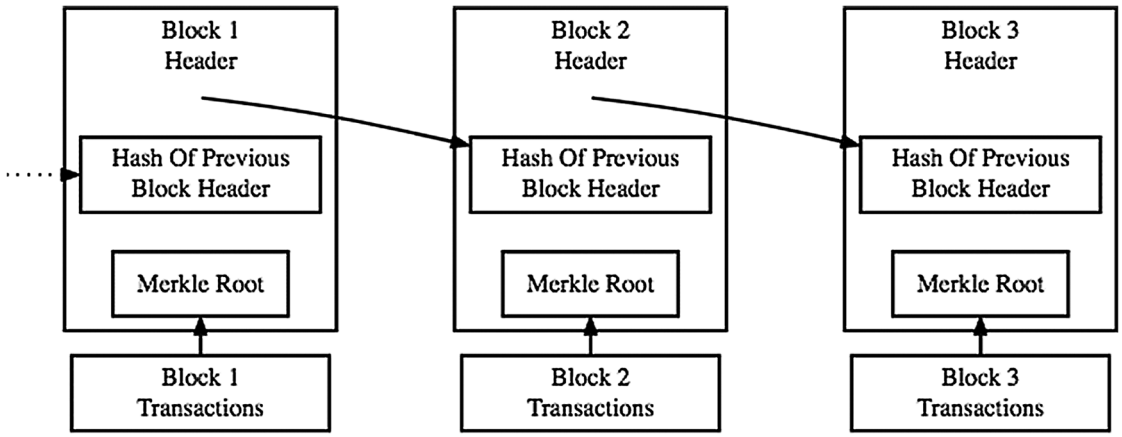

Figure 2: Hash of the Block

One of the disadvantages is that currently, MNOs are using one or two HLRs on their network, which means the additional cost will be charged for using additional nodes to improve complexity from the hardware side. This additional cost includes different server and hosting costs. Another downside of using multiple HLRs in different geographic locations is transmission cost. Especially for operators that host equipment in different regions of the country, the cost of renting a transmission medium can be undesirable, and building this medium will be even higher depending on the type of medium.

5 Possible Solutions

This section concentrates on possible solutions to the problems that come with the suggested method.

5.1 5G Core Implementation

5G is a trend that became popular in the last few years, which is the next evolution of mobile networks after 4G LTE (Long-term Evolution). Some mobile operators have built a 5G network for testing it, and some of them have already launched the network despite a minority of the mobile devices that support 5G. The new generation of mobile networks promises higher speeds (more than 1Gbps) and less latency with higher bandwidth to support new technologies, such as the Internet of Things (IoT) devices. Providing the promised features requires some changes and additions on traditional networks such as Edge Cores [25].

A traditional network is built on one main core, where all major network elements are connected to this core directly or alternatively. This means even if the element is far away from the core, it should connect to the core directly or over another equipment that is directly connected using transmission media. The long-distance transmission caused additional delay and latency from the technical side and additional medium-cost from the financial side. To overcome this problem, a new Edge-Core idea is introduced with 5G, which works as a sub-Core, and it connects to nearby nodes directly. Edge-Core does not require the transmission of the data to the central core in most cases and handles the traffic by itself [26].

The usage of Edge Cores benefits and support the HLR chain solution that is recommended in this paper by eliminating the transmission cost. As a result, multiple HLR nodes can connect to the nearest Edge core and operate without contacting Central Core.

5.2 Virtualization of Hardware Saving

Virtualization is another trend which increases its usability and uses cases every passing day. Flexibility and price saving make it more attractive for companies, and most of the big companies have already switched or started switching to a virtual environment. Virtualization allows administrators to use their resources more flexible and productive by separating hardware resources, virtually no physical. For example, each application used its server to store its data and operate using its Central Processing Unit (CPU). However, by building a virtual environment on common use servers, administrators can now launch multiple applications with multiple characteristics on the same server Fig. 3. The server supports the total requirements of the applications. In the future, if one of the applications is removed from the environment for any reason, another one can be used on the space that is left after the removed application [27].

The benefits of using a virtual environment are a lot, and this environment also supports suggested solutions in this paper. Using a virtual environment, the operators can separate a small portion of their resources for the application and save from buying separate hardware for multiple HLR nodes.

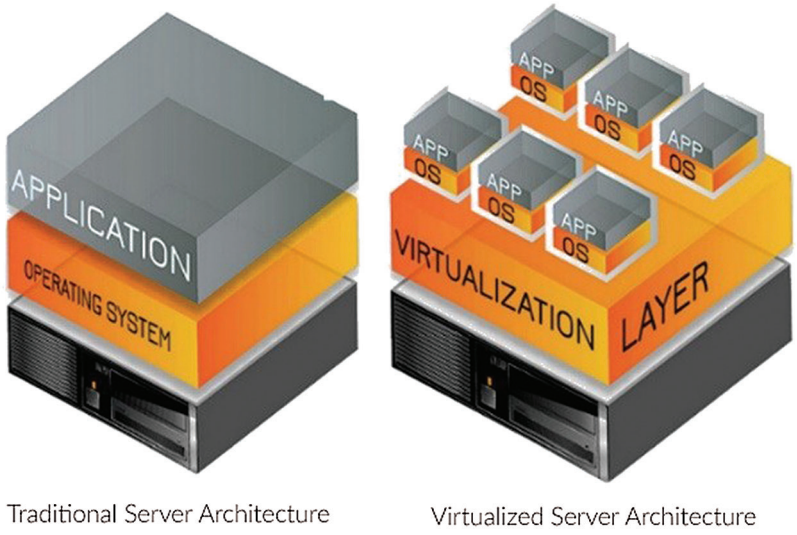

Figure 3: The physical savings of virtualization

6 Conclusion

With information security brought to another level by the increasing rate of technology and hacking mechanisms, it's critical to provide extra protection on one of the main nodes, the HLR database, in the mobile networks, which include key user information. This paper offered another level of HLR protection by enriching its security with Blockchain design. Until that point, HLR protection was measured by encryption algorithms' complexity level between network equipment. However, in this paper, the security of the node itself has been investigated, and improvements suggested. The suggested method is analyzed through the paper by stating the advantages or solutions for traditional architecture's weaknesses and the disadvantages of using the new method together with possible options to avoid the disadvantages. As a result of this analysis, the paper's method is considered successful and feasible for modern mobile networks for improving database security and sustainability.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," *2016 IEEE Int. Conf. on Communications (ICC)*, 14 July 2016, pp. 1–6, 2016.

[2] C. K. Han and H. K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. on Mobile Computing*, vol. 13, no. 2, pp. 457–468, 2014.

[3] D. Katz, "Build a blockchain and a cryptocurrency from scratch," 2018. [Online]. Available at: https://www.udemy.com/course/build-blockchain.

[4] L. Ghiro, L. Maccari and R. L. Cigno, "Proof of networking: can Blockchains boost the next generation of distributed networks?," in *2018 14th Annual Conf. on Wireless On-demand Network Systems and Services (WONS)*, Isola, pp. 29–32, 2018.

[5] D. B. Rawat and A. Alshaikhi, "Leveraging distributed Blockchain-based scheme for wireless network virtualization with security and QoS constraints," in *2018 Int. Conf. on Computing, Networking and Communications (ICNC)*. Maui, HI, 332–336, 2018.

[6] H. Yang and Y. Lee, "Blockchain-based trusted authentication in cloud radio over fiber network for 5G," *2017 16th Int. Conf. on Optical Communications and Networks (ICOCN)*, 01 December 2017, pp. 1–3, 2017.

[7] O. Alphand, IoTChain, "A Blockchain security architecture for the internet of things," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, pp. 1–6, 2018.

[8] B. Paramasivan, M. Johan, V. Prakash and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks," *Journal of Commun. and Networks*, vol. 17, no. 1, pp. 75–83, 2015.

[9] Intel. 2020. [Online] Available at: https://www.intel.com/content/www/us/en/products/docs/wireless-products/mobilecommunications/mobile-software.html.

[10] Christos Xenakis, "Security measures and weaknesses of the GPRS security architecture," *International Journal of Network Security*, vol. 6, no. 2, pp. 158–169, 2008.

[11] X. Ban, R. Sarkar and J. Gao, "Local connectivity tests to identify wormholes in wireless networks," *ACM 12th Int. Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc)*, ACM, pp. 13, 2011.

[12] S. Brands and D. Chaum, "Distance-bounding protocols," *Advances in Cryptology — EUROCRYPT '93, 1994*, Springer, vol. 765, pp. 344–359, 1994.

[13] D. G. Baur, K. H. Hong and A. D. Lee, "Bitcoin: Medium of exchange or speculative assets?," *Journal of International Financial Markets, Institutions and Money*, vol. 54, no. 4, pp. 177– 189, 2018.

[14] A. Biryukov, D. Khovratovich and I. Pustogarov, "Deanonymisation of clients in a bitcoin p2p network," in *Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security*, New York, NY, USA, pp. 15–29, 2014.

[15] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, 2014.

[16] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy- reserving smart contracts," in *Proc. of IEEE Symp. on Security and Privacy (SP)*, San Jose, CA, USA, pp. 839–858, 2016.

[17] M. Jawad Alam and M. Ma, "DC and CoMP Authentication in LTE-Advanced 5G HetNet," in *GLOBECOM 2017 - 2017 IEEE Global Commun. Conf.*, Singapore, pp. 1–6, 2017.

[18] Mobile Station - Base Station System (MS-BSS) interface; Data Link (DL) layer specification, Technical specification (TS), 3rd Generation Partnership Project, 2014. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=512.

[19] N. V.-Rodriguez, A. Aucinas, M. Almeida, Y. Grunenberger, K. Papagiannaki *et al.,* "RILAnalyzer: A comprehensive 3G monitor on your phone," in *Internet Measurement Conf.*, Barcelona, Spain, 2013.

[20] J. Cichonski, J. M. Franklin and M. Bartock, "Guide to LTE security," *Special Publication (NIST SP)*, pp. 800–187, 2018.

[21] S. Djahel, F. Naitabdesselam and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 13, no. 4, pp. 658–672, 2011.

[22] C. Decker, J. Seidel and R. Wattenhofer, "Bitcoin meets strong consistency," in *Proc. of the 17th Int. Conf. on Distributed Computing and Networking (ICDCN)*, Singapore: ACM, pp. 13, 2016.

[23] T. P. Anithaashri and R. Baskaran, "Enhancing the network security using amalgam game," *International Journal of Information Security*, vol. 2, no. 1, pp. 45–57, 2012.

[24] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," Wireless Network, pp. 1–5, 2016.

[25] M. Imran, F. A. Khan and H. Abbas, "Detection and prevention of black hole attacks in mobile ad hoc networks," in *2014 Int. Conf. on Ad-hoc and Wireless Networks (AdHocNets)*, Springer, pp. 111–122, 2014.

[26] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. on Mobile Computing*, vol. 4, no. 5, pp. 502–516, 2005.

[27] X. Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," *IET Information Security*, vol. 7, no. 2, pp. 61–66, 2013.