SHA-256 in Parallel Blockchain Technology: Storing Land Related Documents

Fariha Jahan
Department of CSE,
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh

Mayel Mostafa
Department of CSE,
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh

Shahrin Chowdhury
Department of CSE,
American International University-Bangladesh (AIUB)
Dhaka, Bangladesh

ABSTRACT
Everyday many land documents are stored in an offline process. This process is challenging because it is done manually; for registration and storing, it needs many papers too. However, there is also a lack of security because anyone can see the document. Safety problems can be solved by creating a secure digitized system and the successful implementation of the system. The digitalization of the land registry system through Block-chain could be the only solution to serve a helpful, more secure, and corruption-free solution. In this paper, a new block-chain architecture called parallel block-chain by Satellite Chain Formation algorithm specially designed to store land-related documents with the SHA-256 hash algorithm has been implemented. Polynomial equations also show the numbers of generated blocks and times. And this research also indicates that the proposed system is secure, scalable, and fast.

General Terms
Block-chain, Information Security, Algorithm

Keywords
Parallel Blockchain, Bitcoin, SHA-256, Satellite chain formation, Polynomial Equation, Python.

1. INTRODUCTION
Every day people are communicating with one another in this world. In communication, the essential asset is data. Data can be audio, video, graphics, text, etc. Nowadays, data security is fundamental, so the most critical concern is to secure/protect the data; violation of data security can take place in many ways, and using various types of attacks. Man-in-the-Middle (MiM) attack is one of the common attacks to breach data security. Land transaction records are one of the essential records produced by an organization. Indeed, Hernando de Soto argues that they are the cornerstone of today's society [5]. Nowadays, Blockchain is the most secure technology in recent technology trends [1], which integrates decentralization, distributed computation, asymmetric encryption, timestamp, and consensus algorithm. Block-chain is a chain that consists of many tamper-proof blocks [2]. This chain is secure because every block has a hash algorithm of the previous block, so if any non-verified block enters into the chain, the whole chain will be destroyed to protect the data. Block-chain is also scalable because of block size, and block size depends on the hash algorithm. For example, MD5 is a 128-bit hash function, digest value of SHA-1 is 160 bit, SHA-224, SHA-256, SHA-384, SHA-512 produces hash values of 224 bit, 256 bit, 384 bit, 512 bit respectively[3] which overcomes the storing and transferring issue of IoT[2]. The block-chain can influence the way several internet applications are designed today as an innovative tool.

Block-chain's decentralized aspects are one of its most important sights. Companies are usually no longer democratic entities and want to control their systems to implement specific business logic and policies. Distributed block-chain technology is expected to change land registration by providing secure land storage architecture using cryptographic protocol usage transactions [10]. It will bring the benefits of increased security and productivity in production and cost reduction. In some countries worldwide, steps were taken to test possibilities to use block-chain land registry technology or even to incorporate block-chain land registers from a socio-economic point of view reflected in the strict formal legal requirements for the transfer of real rights. What needs to be emphasized is that, because of the complicated complexity of land transfer, contracting parties also need legal assistance.

Block-chain can be used in many sectors. Here are the essential benefits of block-chain that may prove useful, e.g. Supply chain management, Quality assurance, Banking transactions, E-Voting, Immutable records, Secure access and storage, Easy and secure business tread, Stock exchange, Peer-To-Peer global transaction.

The purpose of land registry procedures is to ensure that practitioners are not advertising itself, but still sale assurance. And it will be considered the position of the block-chain in the land area registration and, in particular, whether it could be an option for structures of property registry currently running. In this paper, the authors proposed and developed a new block-chain architecture called parallel architecture by Satellite Chain Formation algorithm specifically designed to store land-related documents with the SHA-256 hash algorithm. The numbers of generated blocks and times are also shown by two polynomial equations in this research.

2. LITERATURE REVIEW
N.S. Tinu proposed a Survey on Blockchain Technology, and here the author described the taxonomy, Consensus Algorithms, and Applications of Blockchain. There are three types of Blockchain called Public, Private, and Consortium or Hybrid Blockchain. The author presented a comparison between these three types of Block-chain characteristics very precisely. PoW is a compromise technique used in Bitcoin. It's easy to use in an open network, validate a block, and build a new block hash. To avoid the rapid generation of new blocks, Bitcoin formulated two characteristics. In PoW, per network node calculates a block header hash value. Proof of stake is a better solution for energy conservation and stability than PoW. Anyone picked by evidence of a stake algorithm will build blocks. DPoS is a democratic representative and an improvement in the face of direct democratic PoS. A replication algorithm that can tolerate byzantine errors is PBFT (Practical Byzantine Fault Tolerance). Byzantine error is the case in which multiple

witnesses have symptoms. Every network operation interruption caused by Byzantine malfunction is a byzantine one [1].

Shitang Yu et al. proposed a High-Performance Blockchain Platform using technologies such as distributed network architecture with the PBFT-DPOC consensus algorithm. Here, the authors proposed a three-layer architecture, including the intelligent device layer, block-chain layer, and DAPP layer for achieving efficiency and security for the connection of smart devices through node-to-node mapping [2].

Wenting Li et al. proposed the Satellite chain formation algorithm and integrated it with the Hyperledger Fabric v0.6 to create a novel block-chain architecture for industrial standards. This is a parallel network in which various consensus protocols can be used privately in a simultaneous way. Existing block-chain deployments depend on the availability and order of the transactions to all system nodes. It goes contrary to current business standards, which prohibit the sharing and dissemination of information to the relevant stakeholders. Whereas some solutions promote encryption of transactions selectively, such strategies require subtle critical management infrastructure and still allow the device's ultimate nodes to analyze a single system exchange prevalence. They also proposed an algorithm named Cross-chain Asset Transfer algorithm for transferring assets. Assets must move through satellite chains between stakeholders. For instance, this will help cross border transfers between financial institutions in different areas of administration [4].

The model, constructed by UML diagrams and tested using statistical models of usage, was proposed by Cleverence et. al. to digitize the land records and compare them to fingerprint for authentication. The system is protected as it will not require more than one proprietor on one piece of land and time; the cost would also decrease for registration of land titles. The model is included with the Integrated Land Management Information System (ILMIS) with bitcoin block-chains.
The criteria for their model were collected from 200 responde nts [9].

Another paper analyzed three block-chain approaches to record land ownership transfer and evaluated them using a theoretical archival science lens. The paper discussed relevant legal and financial problems related to land recordkeeping based on block-chain. At the same time, the potential benefits of block-chain technology can be significantly increased inland registrations–improved performance, reduced transactional friction, improved protection, etc. [5].

M. Kaczorowska discussed the possible benefits and risks of land automation. All transactions and practical experience in the application of block-chain in land registration for selected countries. The ability of block-chain to increase the recording rate is recognized notably for developing countries in which the land is situated inefficient and inefficient identification schemes. This is because block-chain is a digital archive storage tool. Also, it is essential to establish the issue about the anonymous block-chain character. It is assumed that electronic IDs connected to public keys can address these difficulties [10].

This magazine discussed a blockchain-based parking network that allows pay parking between car parking owners and users. They removed the need for a reputable third-party agency instead of current parking schemes as the consortium chain ensures consumer security. No territorial constraints, the method facilitates adjustable up and down. BCOS cash can be used to watch each other, trace each transaction, and use additional virtual payment. The future analysis involves an automated program to incorporate and test the system and operate with a parking operator [11].

A study has been developed on a smart parking solution that uses block-chain technology to integrate an infrastructure. It also set an innovative, intelligent parking scenario that enables the data security and trust of different stakeholders. This model allows urban drivers to find a suitable place to park. The providers of parking services can also share sensitive information without having a trusted third party. This model is mostly aimed at enhancing security and privacy [12].

3. RESEARCH METHODOLOGY

To store the land record in a Digitalized System through Blockchain, the authors implemented a Satellite Chain Formation algorithm with the SHA-256 hash Algorithm by python language and integrated it with Bitcoin.

3.1 Satellite chain formation

By this algorithm, the authors established a parallel block-chain. In this algorithm, the satellite chains are the sub-chains created in a parallel manner. This system is more secure because different consensus protocols can be used in different satellite chains in parallel [4], making this system safe. The algorithm is given below:

Definitions:

ID_i: registered ID of node i in the block-chain

$CList_i$: proposed consensus protocol list from node i

procedure PROPOSE_CHAIN

send ID_i,$CList_i$ to all nodes

……...

……....

$chain_{id}$ ← getName({IDk})

consensus ← select({$CList_k$})

……...

……...

COORDINATE(chain_info)

else ACKNOWLEDGE(chain_info)

end if

end procedure

……...

……

send (chain_info,sig_i) to all nodes

wait and collect {sig_k} from all nodes

……

……

return (chain_info,{sig_k})

columns

end if

end function

.....

……..

if isInitiator(j,{ID_k}) & valid(sig_j,chain_info') **then**

if chain_info = chain_info' **then**

……

……...

wait for {sig_k} from initiator j

if valid(sig_k) for all nodes k **then**

……

……...

end if

end if

end function [4]

3.2 Bitcoin

Bitcoin is a decentralized, public, and permission less block-chain like Ethereum. It means the ledger is public. All miners can determine the Consensus and the read permission is public here it means the organizations, miners, everyone can read the ledger. However, the benefit of Bitcoin block-chain is where the identity is anonymous/pseudonymous

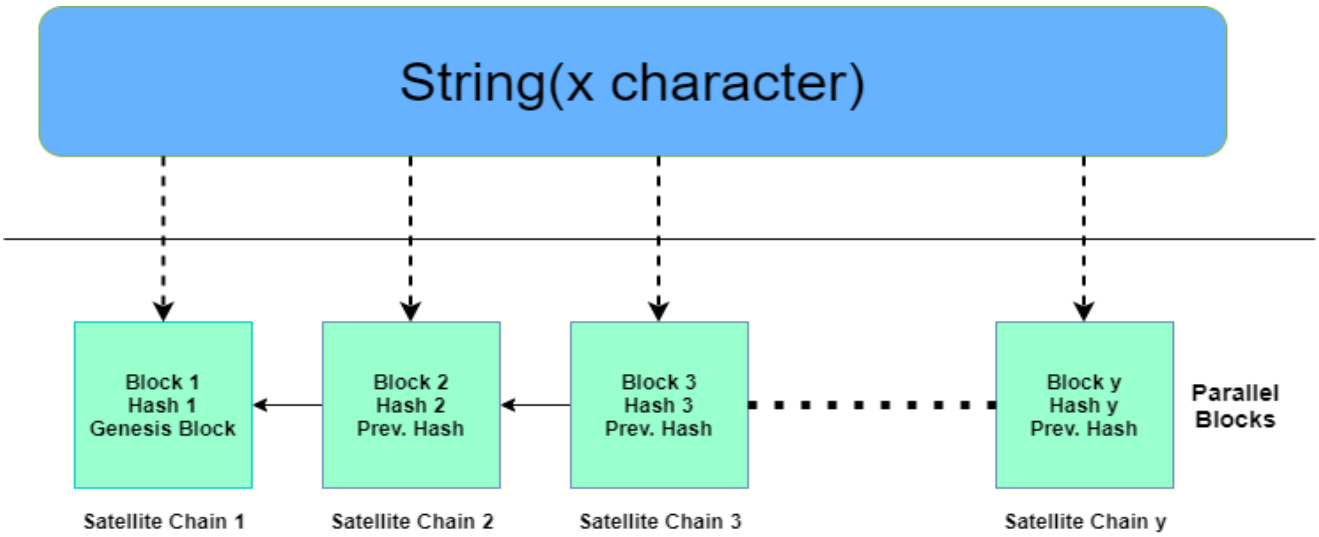

Fig 1: Proposed System's Architecture

and in terms of immutability it is nearly impossible to tamper [1].

3.3 SHA-256

SHA stands for Secure Hash Algorithm and is designed by the National Security Agency (NSA) [8]. SHA-256 is derived from SHA-2. It is not encryption but a hash algorithm. It is a one-way cryptographic hash. It is highly secured because the encrypted message by this algorithm can never be decrypted [6]. Also, it is a 256-bit block cipher algorithm [7]. SHA-256 turns the 64 characters of hexadecimal string into 256-bit characters length. That is why it is called SHA-256.

In this research, if the user provides any string which contains x no of character, that string will be stored in y no of blocks parallelly.

4. RESULTS AND DISCUSSION

Authors have stored string data through parallel block-chain by the Satellite chain formation algorithm with the SHA-256 hash algorithm. For storing land records, this research has used four strings considering the data sample. While storing this string, the number of blocks and time took (in minutes) for blocks are shown below:

Table 1. Data sample and parameters of each string.

Serial No	Strings	Total No. of Letters (including space)	Total Number of Blocks	Total time Taken (in minutes)
1	I am the best president. Ever.	30	3,475,450	202
2	This land costs twenty lakh tk.	31	3,591,299	209
3	These case files cover land entries in all 30 public land states.	65	7,530,142	438
4	There are over ten million such individual land transactions in the custody of the National archives.	101	11,700,682	681

It has been observed that with the increment of no of letters in the string the number of blocks and time both are increasing. It means block number and time is dependent on letter number. In our system, the relationship of letters and block numbers is described by a general polynomial equation:

y = -2E-05x2 + 115848x + 0.2636; (1)
where y= number of blocks and x= number of letters.

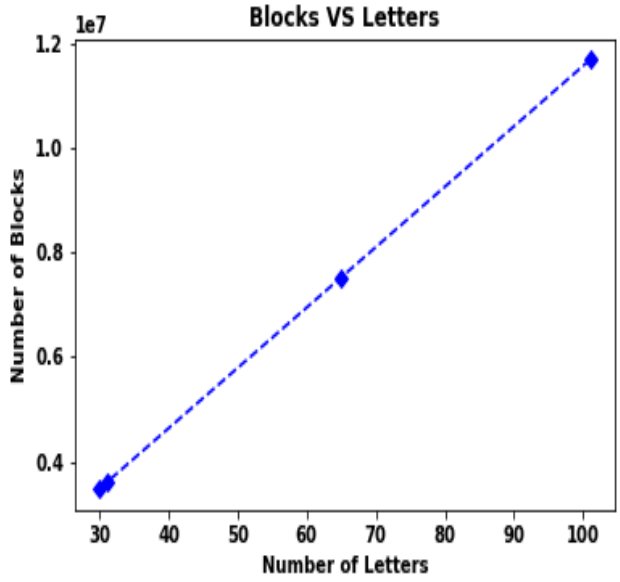

Fig 2: Graph of blocks vs letters of four strings.

Following (1) equation, in this system blocks are stored. The number of blocks depends on the number of letters when it is used.

Meanwhile, in this system the relationship of letters and time is also described by a general polynomial equation:

y =0.0001x2 + 6.7255x + 0.2342; (2)

Where y= total time taken (in min) and

x= no. of letters.

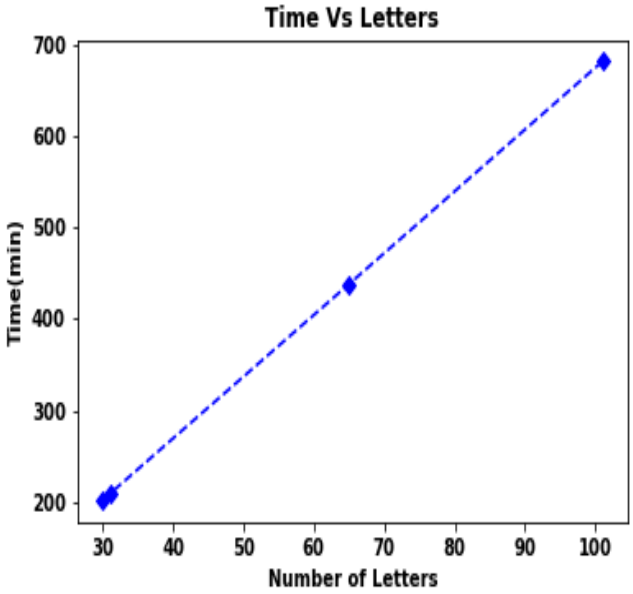

Fig 3: Graph of Time vs letters of four strings

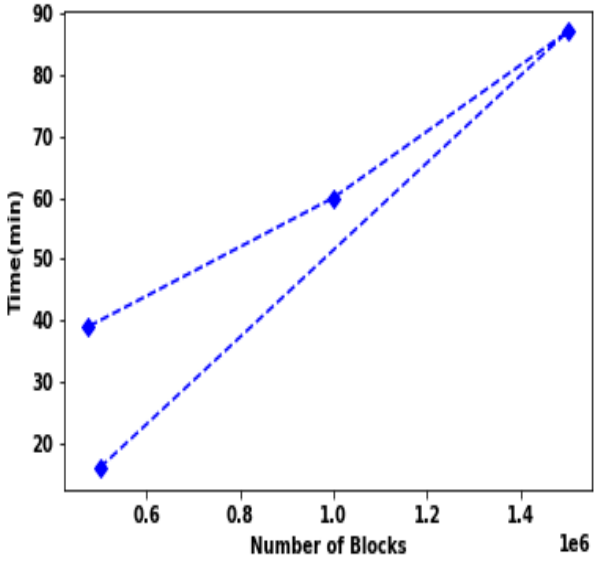

Fig 4: Result of storing a string "I am the best president. Ever."

From Fig 4, it is observed that in the first 16 minutes, it was required to create 500,000 blocks in parallel. Next, 1,500,000 parallel blocks were made by utilizing 87 minutes, which was expected because the number of blocks in round 2 is three times bigger than the number of blocks in round 1. Subsequently, 10,00000 blocks are generated using 60

minutes, which takes less time than the round 2 times as the number of blocks is less. Finally, the time taken to make 475,450 blocks and check the whole system is 39 minutes; hereafter creating 475,450 blocks, our system checks the whole chain, which is why the total time is 39 minutes.

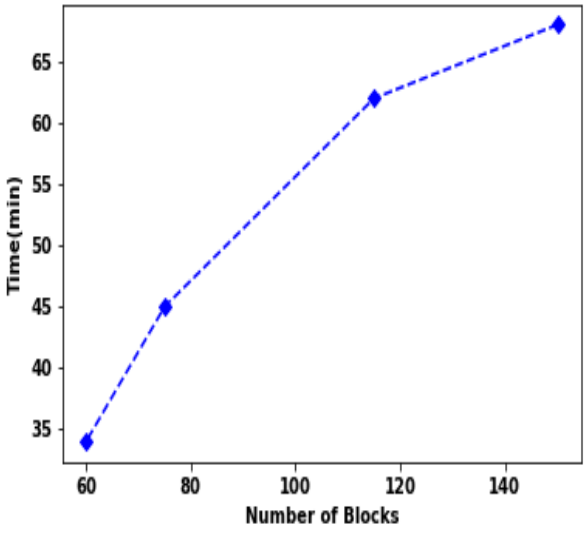

Fig 5: Result of storing a string "This land costs twenty lakh tk."

From Fig 5, it can be seen that 150 blocks have been generated parallel in the first 68 minutes. Subsequently, it takes 62 minutes to build 115 parallel plates. It takes 45 minutes to create 75 blocks parallel. Since 75 blocks are less than 115 blocks, so it takes 17 minutes less time. Finally, it takes 34 minutes to make 60 blocks and to test the entire system

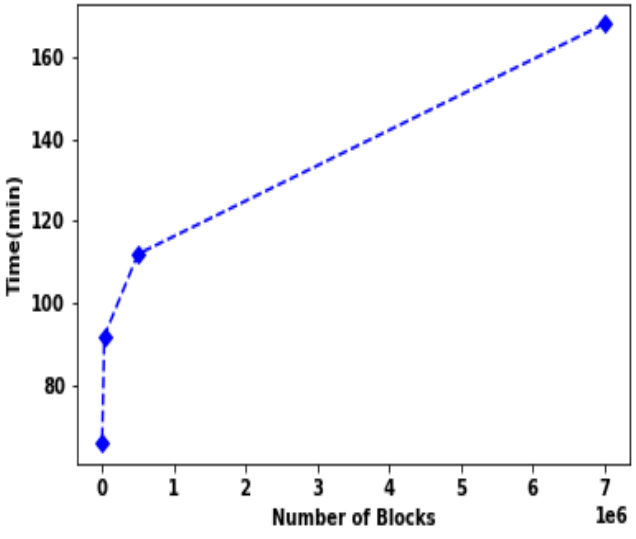

Fig 6: Result of storing a string "These case files cover land entries in all 30 public land states."

Fig 6 illustrates that it takes 168 minutes for 7000000 blocks to be formed simultaneously. Following that, 500000 parallel blocks are created in 112 minutes. It takes 92 minutes to make 30,000 blocks in parallel. Finally, to inspect the entire system and also to create 142 blocks; 66 minutes is used.

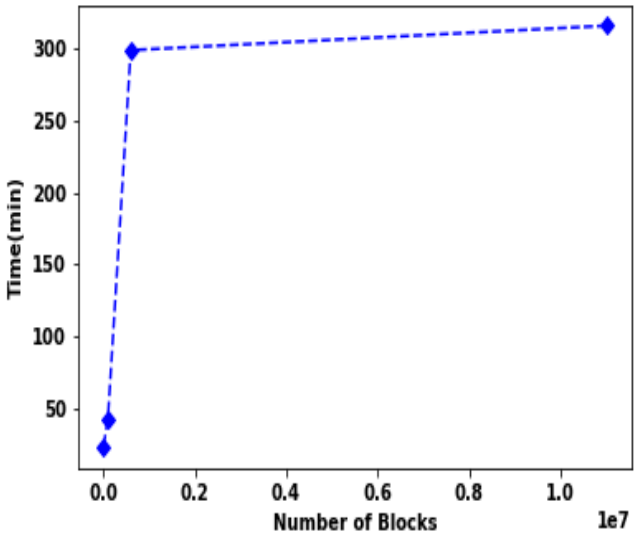

Fig 7: Result of storing a string "There are over ten million such individual land transactions in the custody of the National archives."

It is evident from Fig 7, that the formation of 11,000,000 blocks is taken parallel at the first 316 minutes. Following this, 299 minutes are taken as planned to create 600,004 parallel blocks. It took 43 minutes to generate 100,139 blocks in parallel. Finally, it takes 23 minutes to make 100 blocks and to test the entire system.

Since the system has stored string data by satellite chain formation algorithm and the SHA-256 algorithm in a parallel block-chain it can be said that using this method; land records can also be stored. The analysis clearly understood that the parallel block-chain is more scalable because there are more blocks than a single block-chain. It is faster because data is stored in parallel, not sequentially. Each satellite chain can privately run different consensus protocols in parallel, which makes the model secure. It is also efficient because after creating the blocks the whole system is checked.

5. FUTURE WORK

After all, authors have stored string data in a parallel block-chain using a satellite chain formation algorithm with the SHA-256 hash algorithm and integrated it with public block-chain Bitcoin. The future work will be storing string data in a private Blockchain e.g. Hyperledger Fabric, MONAX, etc. and Consortium Blockchain e.g. R3, EWF, etc.

6. CONCLUSION

As land records are so sensitive, it is imperative to ensure that records for land transactions are established and maintained in a manner that ensures long-term availability, quality of evidence, and law enforcement management. Transparency, financial stability, and human rights can be at risk without adequate treatment and care for land transaction records. Block-chain is an electronic database through which, using a consensus protocol, users can preserve digital records, events, or transactions that are encrypted, authenticated, and managed via a shared network of participants. Land and property management provides a wide range of documentation and supporting data. To secure land records in a digitized way,

Block-chain is the most secure technology till now. In this paper, the authors have developed a parallel block-chain through the Satellite chain formation algorithm with the SHA-256 hash algorithm to store string data. Using this novel approach, land records can also be stored quickly, scalable and secure way.

7. REFERENCES

[1] N. Tinu, "A Survey on Blockchain Technology-Taxonomy, Consensus Algorithms and Applications", International Journal of Computer Sciences and Engineering, vol. 6, no. 5, pp. 691-696, 2018. Available: 10.26438/ijcse/v6i5.691696.

[2] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, "A High Performance Block-chain Platform for Intelligent Devices," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 260-261, doi: 10.1109/HOTICN.2018.8606017.

[3] S. Debnath, A. Chattopadhyay and S. Dutta, "Brief review on journey of secured hash algorithms," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-5, doi: 10.1109/OPTRONIX.2017.8349971.

[4] Wenting Li, Alessandro Sforzin, Sergey Fedorov, and Ghassan O. Karame," Towards Scalable and Private Industrial Blockchains", In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts (BCC '17), New York, 2017, pp. 9-14, doi: https://doi.org/10.1145/3055518.3055531

[5] V. Lemieux, "Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective", European Property Law Journal, vol. 6, no. 3, 2017. Available: 10.1515/eplj-2017-0019 [Accessed 29 June 2020].

[6] 2. Chris Veness, "SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts", Movable-type.co.uk, 2020. [Online]. Available: https://www.movable-type.co.uk/scripts/sha256.html.

[Accessed: 29- Jun- 2020].

[7] Iwar.org.uk, 2020. [Online]. Available: http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf. [Accessed: 29- Jun- 2020].

[8] B. Roy, Advances in cryptology. Berlin: Springer, 2005.

[9] Kombe, Cleverence, Manyilizu, Majuto, Mvuma,"Design of Land Administration and Title Registration ", Journal of Information Engineering and Applications, vol. 7, no. 1, pp. 8-15, 2017. Available: https://www.iiste.org/Journals/index.php/JIEA/article/view/35154/0

[10] M. Kaczorowska, "Blockchain-based Land Registration: Possibilities and Challenges", Masaryk University Journal of Law and Technology, vol. 13, no. 2, p. 339, 2019. Available: 10.5817/mujlt2019-2-8.

[11] J. Hu, D. He, Q. Zhao and K. R. Choo, "Parking Management: A Blockchain-Based Privacy-Preserving System," in IEEE Consumer Electronics Magazine, vol. 8, no. 4, pp. 45-49, July 2019, doi: 10.1109/MCE.2019.2905490.

[12] S. Ahmed, Soaibuzzaman, M. S. Rahman and M. S. Rahaman, "A Blockchain-Based Architecture for Integrated Smart Parking Systems," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 2019, pp. 177-182, doi: 10.1109/PERCOMW.2019.8730772.Journal, 2012. Available: 10.2139/ssrn.2097443.