Paper No: SC-11 **Smart Computing**

Minimization of fraudulent activities in land authentication through Blockchain-based system

L. W. D. C. Jayabodhi*
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
jdinith72@gmail.com

Chathura Rajapakse
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
chathura@kln.ac.lk

J. M. D. Senanayake
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
janakas@kln.ac.lk

***Abstract*: In Sri Lanka, the land administration process has not been digitized, which has led to plenty of conflicts in determining the real ownership of lands and drastically increasing the land transaction processing time, which has resulted in many fraudulent activities concerning land management. The existing system is majorly paper-based and centralized. Administrators who have the powers to alter the system according to their wishes hold a huge threat for information security and is a centralized system that bears the risk of a single point of failure. Hence, transitioning into another system that could mitigate the drawbacks in the current land authentication system has become a vital need and currently, the knowledge regard this area is very much limited. The decentralized nature of the blockchain-based system has the potential of diluting major limitations in the current system. The overall objective of this research is to mitigate fraudulent activities in land authentication systems through the blockchain-based technological approach. A prototype of a smart contract-based model has been created and verified with the involvement of the actual users. Since the smart contract-based land authentication model verifies the land ownership within a short period, the transaction processing time narrows down from a few months to a couple of minutes. The results show signs of considerable improvements in the efficiency and the security of the land authentication process, the users who interacted with the prototype and presented positive comments.**

Keywords: *Blockchain mining, Land authentication, Smart contract*

I. INTRODUCTION

The study will consider the applicability of the blockchain technology to the land authentication and the land ownership transfer process. The existing system is very much of a paper-based system. The land ownership transfer documentation (creation of a deed) takes about a month to go through the process. This arises space for the many fraudulent activities in land ownership.

Also, the process for identifying the real owner of the land can become a complex process when there are disputes in the deed. Therefore, the general public cannot do it by themselves and they have to rely on the services of a legal officer. Even though the legal officer with his expertise may take several days for verification. If the land had undergone many transactions and alterations to the geographical dimension the process becomes extremely complex. So that the legal officers would be reluctant to go ahead of such transactions as the real owner of the land is doubtful.

Therefore, considering these drawbacks it would be best to have a digitalized system for land authentication. Through the digitalized system, the land ownership transfers will be tracked and the sensitive data such as the land boundaries will be stored in terms of the geo-locations. Hence the information such as the land location and the ownership of the land will be available for the public with a matter of few clicks.

But the digitalized system has its drawbacks as all the information is stored in the central location, it provides too much power on the administrator. Also, there would be a disastrous situation if the digitalized system is damaged due to some external factor. Since the land authentication information is highly sensitive, it would very much risky to store the land information in the digitalized system with central information storage. So the problem of lack of a robust highly secure system for the land authentication is remaining unsolved.

Hence to mitigate the above drawback, a blockchain-based system is used to store highly sensitive land information such as the land ownership details and the dimension information. A proof-of-concept is constructed and tested in a controlled environment. The immutable and distributed properties of the blockchain would address the abovementioned problems related to the Land Authentication System.

II. LITERATURE REVIEW

A. The legal framework in Sri Lanka related to land authentication

Roman-Dutch Law, Islamic Law, Thesawalamai Law, and European Law existing in the pre-British period, influenced the crafting of Sri Lankan land law. In the period of the British ruling, these laws were amended according to the common English Law. After independence in 1948, they have been many reforms regarding the land administration put forward by each of the governments ruling at that time [1]. According to Perera, the number of court cases with unsolved lands is listed below.

The major reason for land disputes to drag so long is the complication of the land laws and the issues regard to determine the real legal ownership of the land.

According to Perera many people would not bring the land dispute to the court but would try to resolve them by themselves using the methods such as “forceful trespassing and evictions, informally compromising in between parties to discussions “. These complications regard to land ownership have caused many bottlenecks in acquiring the best use of the land and hence hindering the economic development of the country.

TABLE1. NO OF COURT CASES PENDING

District Courts	No of years Pending					Unclassified	Total
	5	10	20	30	>30		
Colombo	877	194	62	2			1135
Mt Lavinia	472	49	1				522
Moratuwa	152						152
Homagama	238	144					382
Avissawella	677	426	605	145	24		1877
Panadura	389	72	5	8		8	482
Gampaha	841	362	235	5		3	1446

Source: Sri Lanka Study on Land Markets, Ministry of Lands, 2000

According to the evaluations made under the Implementation Completion and Result Report in 2007 published by the world bank, the Land Titling Project which was implemented with an investment of $5 million from the World Bank funds has been categorized as unsatisfactory [2].

B. Land authentication management with blockchain

The major issue which is arising from the existing land authorization system is that there is room for creating fraudulent deeds and illegally selling the land to another party. This is a basic use case of double-spending which blockchain heavily used in providing solutions.

Cleverence Kombe identifies several functional requirements that are to be fulfilled in an Integrated Land Management Information System (ILMIS). According to him, those functions are:

- Validation of the Land Title Information
- Validation of the Land Title Transactions
- Notarization of the Legal Registration process [3].
- Distribute the fingerprint information stored in the Integrated Land Management Information System using the blockchain technology.

Kombe also mentions about the importance of an ILMIS in the face of the natural disaster and the importance of using the blockchain in order to increase the availability of the system. Their research is more focused on the usage of the Fathom blockchains. A third-party company which is providing blockchain-based API to manage the blockchains. Also, the legislative framework covered in that research is the legislative framework of Tanzania [3].

Blake and Sanders address the issue of interconnecting the Land Information System with the other digitalized services such as the mortgage banks. Financial institutions and also other public bodies. That research is based on Nigeria where most of the government services are digitalized. But considering the Sri Lankan context, there is still a large amount of room for digitalization [4]. Therefore, that kind of integration can be focused on the later phases of the implementation.

C. Mitigation of double-spending with the use of Blockchain

There have been several attempts to mitigate the frauds is caused related to the double-spending, by the use of the blockchain technology.

Hissu Hyvärinen discusses the use of blockchain in the taxation process through his research, “A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services”. In the taxation process, many individuals taxed twice for the incomes they earn in offshore. But most of the tax authorities in different countries have got together and have created tax relief schemes to prevent this kind of double taxation. But many of the public illegally used these tax relief schemes. The people use it for their advantage due to the easily forgeable legal documentation and due to the insufficient exchange of information between the international tax authorities [5]. Hissu Hyvärinen intends on creating a blockchain-based prototype to mitigate the tax frauds and also increase the transparency of the flow of dividends.

George Foroglou in his paper titled Further applications of the blockchain explain several other use cases of the blockchain. Some of them are providing a solution to the double-spending issue. Voting or Election is another area where the double-spending happens in a form of casting votes by an individual. George Foroglou mentions about the BitCongress where the Ethereum network has been used to create a blockchain-based voting system. In that, each of the individuals is entitled to “vote coin” which he may use only one time to vote. The casted vote would be recorded on the blockchain after verifying it. There are several other voting technologies that George Foroglou mentions in his paper. They are Remotengrity, a voting system that provides every physical vote with a cryptographic code to verify the authenticity of every physical vote and Agora Voting [6].

Foroglou speaks about another system called “Smart property” in order to prevent people from overspending their properties (a form of double-spending) with the integration of the internet of things. Many of the appliances that we use today can be controlled through the internet. A smart home can be designed in a way that the the owner needs a digital key to open the doors of the house.

A blockchain system can be built such that it stores the information about the owner and also the digital key to open the smart home. If the house owner fails to pay the rental fee to the smart home, the digital keys would be updated and his access to the smart home will be revoked. In this way ownership of the applications can be controlled with the use of the internet of things and also Blockchain [6].

D. Blockchain mining process

Blockchain mining is the process through which the transactions are verified in the Blockchain. It is a high-cost operation that includes a tremendous amount of computing power. In a public blockchain, any user can sign up as a miner and he would be rewarded for each of the blocks that he has mined.

- Cryptographic Hash Function - It is a function, which generates a binary number when a string is passed into it, and that number is unique to that particular string. Also, the number cannot be reverse calculated and obtained the initial input value.
- SHA256 Algorithm - This provides a 256-bit binary Cryptographic Hash number for each of the inputs given.
- Consensus - The majority of the nodes in the Blockchain come in agreement that a particular block is a legitimate block.

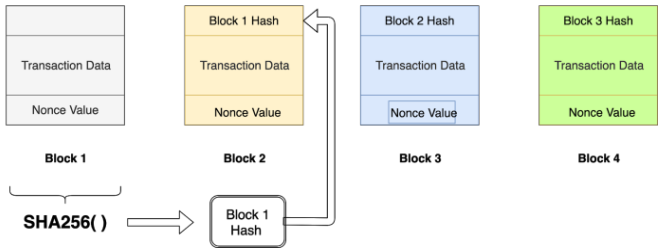

Fig. 1. Structure of a Blockchain

As shown in the above diagram the blockchain is a collection of data nodes known as blocks. Each of the blocks contains

- Previous blocks hash
- Transactional Information
- Nonce Value

The nonce value is an arbitrary value inserted by the miner. In the Block 2 hash value is generated by sending the Block.

1's hash, Transaction data in Block 2 and the Nonce value to the SHA256 function. The Blockchain specifies the difficulty number in which the generated hash should not exceed. The duty of the miner is to generate that hash value altering the nonce value. As the SHA256 cannot be reverse-engineered the only mechanism to derive the relevant nonce value is through guessing. Once the miner successfully derived the nonce value it is sent to the other nodes for the approval. When the Blockchain reaches consensus, the block is added to the Blockchain and the miner is rewarded.

If malicious users altered the transaction data in the Block 2 the resulting hash would be changed, and the Block 2 should be reminded. Also, as Block 2 hash is present in Block 3 it would be changed, and it also should be reminded. Similarly, all the Blocks after Block 2 should be reminded. So the need for a continuous chain of remaining makes impossible for a malicious user to alter the data in the blockchain.

Several algorithms are being used to perform the consensus in the Blockchain.

1) Practical Byzantine Fault Tolerance Algorithm (PBFT)

This algorithm works in three phases,

- The leader broadcast a new request.
- The validators (miners) sign and broadcasts the prepare message for each of the requests.
- If the necessary, amount of prepare messages are received the validators broadcasts commit messages. When the required commit messages level is received the validators commit the changes [7].

If more than one-third of the nodes get corrupted this algorithm would fail.

2) Tendermint

It is a secure state machine replication algorithm operating similar to the PBFT algorithm. It has overcome the limitation of the failure to operate if one-third of the nodes failed. In Tendermint each of the validators is identified through their private key and each of them keeps a full copy of the replicated state. Each of the blocks is assigned an incremental number known as the height, in each of the rounds the validators take rounds to nominated block suitable for each of the height. Each of the rounds contains only one valid block [8].

The voting mechanism is depicted in the following figure.

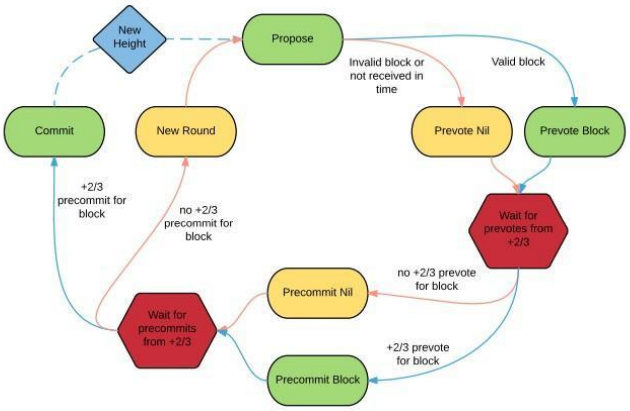

Fig. 2. Tendermint algorithm

The validators first vote for block by *Prevote Block*. If *Prevote Block* receives more than two-thirds of votes it will broadcast the *Precommit Vote*. If it also received more than two thirds the mentioned block will be added to the height. If not, a new round is started and continued until the block is successfully committed [8].

A. Consortium blockchains

The consortium blockchain is similar to the typical blockchain but the mining power of it vests on several entities [9]. The consortium blockchain bears the following characteristics.

- It is only available to a specific set of users.
- It is semi-decentralized: the members of the blockchain could supervise it and control it [9].
- The verification of the operations is done by the special pre-approved set of nodes [10].
- The data is immutable, but there is the chance for the blockchain rollback.

The consensus algorithms that are used in the public blockchain mining process are very resource-intensive and time-consuming [10]. But that kind of complex consensus algorithms is very much necessary in the public blockchains because the miners are anonymous.

But in a consortium blockchain, the miners are trusted entities and are known for some degree. So that the security is lowered to an acceptable level by reducing the complexity of the consensus algorithms [9]. Thus, the efficiency can be increased, and the transactions throughput cab be increased up to several thousand transactions per second.

As a in a public blockchain for a new block to be added to the blockchain the newly added block should be confirmed by the supermajority of the nodes [10].

III. RESEARCH METHODOLOGY

This study is conducted to minimize the fraudulent activities occurring in the land authentication system and thereby making it a more accurate, fast and resilient system. The principles presented in blockchain technology have been used to minimize the effect of double-spending as well as to make the land information system's most secure system. A methodological review of the literature has been carried out to identify the features of the other land authentication systems implemented in foreign countries. Data is collected about the existing processes in the land authentication system and information is gathered about the loopholes that exist in the current land authentication system. Personal interviews with legal officers, as well as the informal interviews with the people working in the land registry, have been used in the gathering of the data and information. Also, the land registry had been visited by the researcher and the process had been observed to a permissible extent.

Then a model is developed portraying the existing system. The loopholes present in the existing system are identified. Then those loopholes are evaluated in order to make the blockchain-based process free from those loopholes. After that, a model based on Blockchain technology is developed. The owner who wants the transfer of land ownership creates an e-request. The e-request is stored in the blockchain, which is stored in the land transfer smart contract. Then the legal officer takes those e requests and approves them. Once they are approved the land information is sent to the smart contract containing the land ownership information and the owner's details are amended in the smart contract. Before modification of the owner's information, the smart contract checks whether the user who generated the request is the current owner of the land. Also, it checks for the validity of the legal officer who authorized the transaction.

The above system requires a blockchain environment to operate. In the demonstration phase the Ganache blockchain, which is a blockchain running on the localhost, is used. In the commercial phase, a consortium blockchain is set up having several governmental organizations as the mining nodes. Each of the successful proof of stake would generate Ether. Private organizations also could join in the mining process. So that the mining responsibility is shared between both the state and the private sector. The private sector could reimburse the Ether by selling them off to the state. The public and the legal officers would be needing Ether to perform their land ownership transactions and the ownership confirmations. The required Ether could be purchased from the state.

IV. IMPLEMENTATION

The Etherium blockchain environment is used for the development of the blockchain. The smart contracts were developed through the Solidity language. Remix IDE (Integrated Development Environment) is used to test and develop smart contracts.

Then they were compiled to Application Binary Interface and then deployed to the Etherium network with the use of the Truffle. Truffle is a development framework that allows the user to create a smart contract project at a click of a button. The developer is being provided with a project structure, files, and directories by the Truffle development framework which makes the development and testing much easier.

The Etherium Blockchain framework is demonstrated with the use of the Ganache tool. It is a private Etherium blockchain that allows the user to run tests and would act as a platform to test all the actions performed on the main blockchain without an additional cost. It has been used by many developers to test their smart contracts with frontend interactions.

The relevant functions of the smart contract are called from the frontend application using Web3js library. It is a collection of JavaScript libraries that helps the user to interact with the blockchain and to perform actions like reading from the smart contract data and writing into the smart contract. The Etherium nodes also provide an RPC interface but this is very much error-prone and difficult to work with. The web3js provide a layer of abstraction on top of the Etherium RPC which makes it more user-friendly and less error-proned.

The users will be accessing the system through a special wallet named the metamask, It provides a digital wallet and provides the user interface to manage the identities in different sites and sign the blockchain transactions. It allows the user to visit the distributed web.

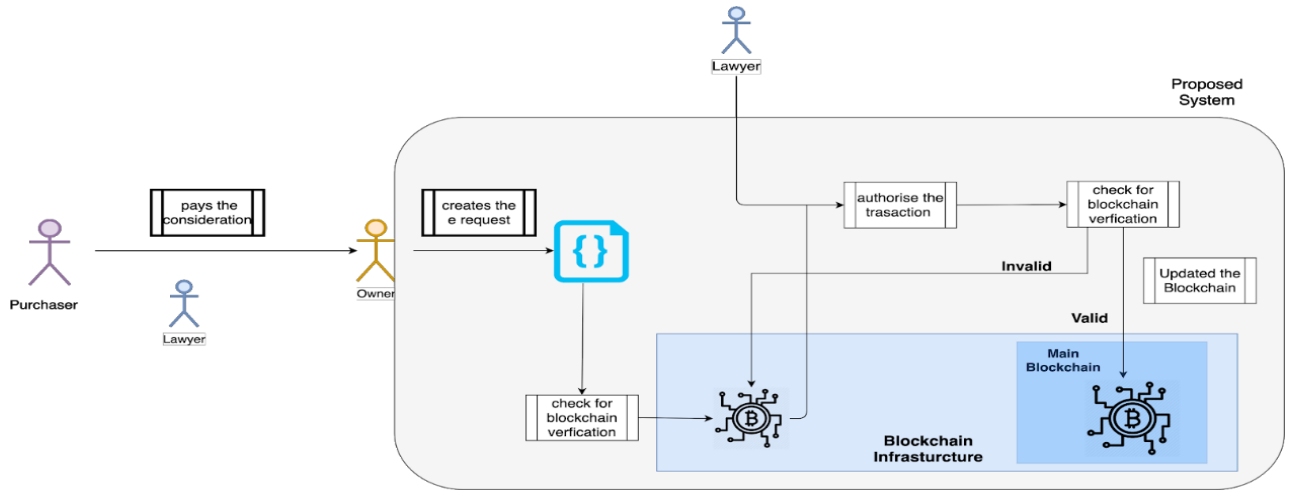

Fig. 3. Proposed Model

The interaction of all those tools is portrayed in the following architectural diagram in Fig. 4.

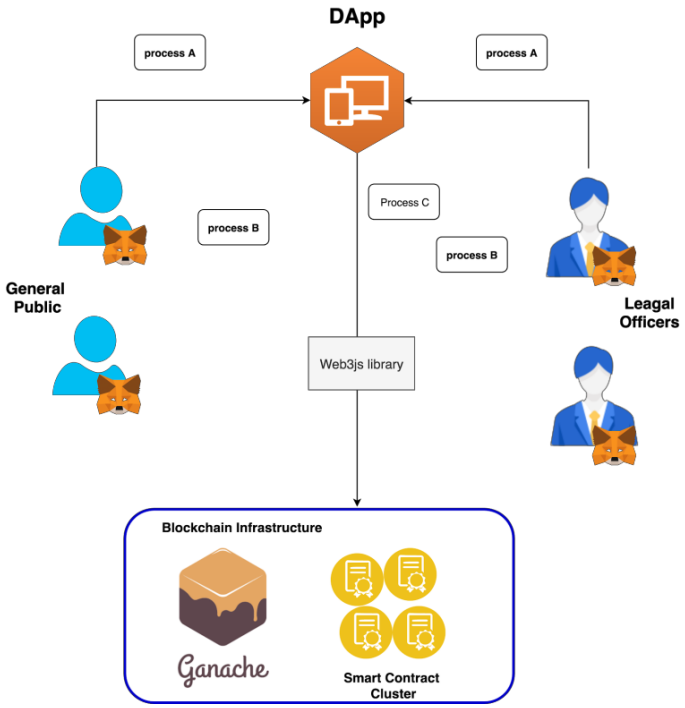

Fig. 4. Integration of tools in Blockchain

Process A - The users (legal officers / general public) Metamask browsers will be connecting with the Blockchain for the authentication process

Process B - The users (legal officers / general public) will be communicating with the DApp to perform the land authentication transactions.

Process C - The DApp will be connecting to the Ganache blockchain to write the transactions to the blockchain.

There are three smart contracts are created for the smooth functioning of the application.

- Land information - this contains all the information on the lands such as a list of previous owners, the next land.
- Land collection - this consists of the information of all the lands. All that information is stored as a mapping of Land
- Legal officer - This consists of the information of the Legal officers.
- Ownership change request - This consists of the information of the requests to transfer ownership of the Land before it is accepted by the legal officer.

V. TEST PLAN AND RESULTS

The user (both the landowner and the legal officer) should log in with the metamask account and confirm his identity.

In the testing phases, the Ganache local test network is being used. It would generate sample accounts with 100 ETH on each of the accounts as shown in figure 5. The Ether would be consumed when performing the change of ownership and confirmation of land ownership transactions. The transactions can be seen in figure 6.

Fig. 5. Testing Accounts in Ganache

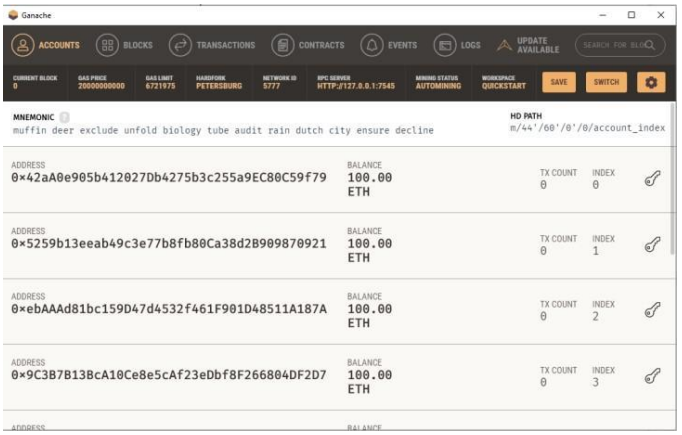

Fig. 6. Transactions in Ganache

The landowner creates the transaction for change of the ownership of the land through his mobile device. Then it is being saved on the ownership change request side until it has been approved by the legal officer. The legal officer uses the platform to approve the request and thus the verified request is sent to the land collections smart contract and the relevant land smart contract would be updated with the information of the new landowner there.

A. Case Study: Change of Land Ownership

The hypothetical owner of the land logs into the system. Then he successfully creates a land transfer to the hypothetical purchaser, which is approved by the hypothetical legal officer.

1. The Owner of the land log into the system
2. Then he selects the relevant land and creates land ownership transfer requests.

In the application, the land and the user in which the land is transferred would be selected from the user interface and ids of the land and the user that the land is transferred to will be extracted. But in the prototype, the above information should be entered as shown in the below interface.

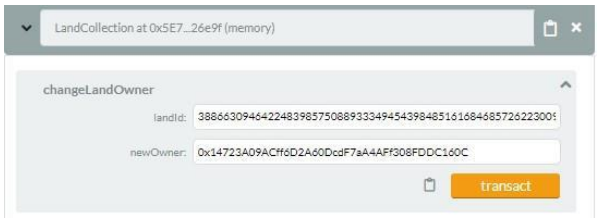

Fig.7. Change Landowner Interface

3. Then the legal officer logs into the system and approves the above-created request if the contents are legitimate.

The legal officer would have the capability to authorize or reject the transaction. The legal officer would have the ability to view the land information and the owner in which the land is transferred. Once the details are found satisfactory the legal officer can confirm the land transfer. In application legal officer could do that by selecting the Land. But in the prototype, the land id should be entered to proceed with the confirmation.

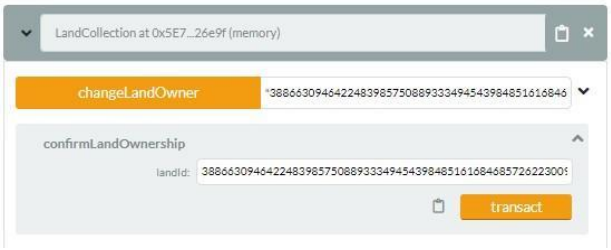

Fig.8. Confirm Land Transfer Interface

B. Verification of the Land ownership

The confirmation of a particular land is owned by the mentioned user.

1. The prospective purchase logs into the system as a general user.
2. Then he searches the information of the land interested in.

In the application, he would have the luxury of selecting on the land itself. But in the prototype, the landId should be entered by the user as shown below.

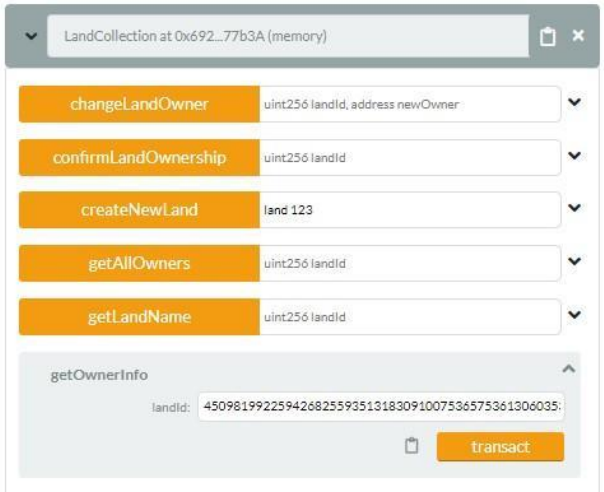

Fig.9. Getting Landowner Information

3. The information of the current owner is displayed.

The Blockchain-based application is returning the address of the current owner of the Land as shown below.

Fig.10. Land Current Owner Information

Then the application could combine the user profile information and presents it interactively.

4. If more information is needed ownership details of the previous five owners can be viewed.

VI. CONCLUDING REMARKS AND FUTURE WORK

The architecture of this model combines the requirements of the land authentication system in Sri Lanka with the modern technological advancement of the blockchain. The paper covers the gap of a lack of knowledge regarding Blockchain-based land authentication systems for the Sri Lankan context. This paper presents a model, which can be used to reduce the fraudulent activities occurring in the Land Authentication System in Sri Lanka and a prototype developed using Blockchain technology for the testing purpose of the model. This section is focused on the benefits and the limitations of such an approach.

A. Benefits

The major issue on the Land Authentication system lack of transparency in the authentication process and the complexity of identifying the real user. But being a digitalized system, it has been reduced to a significant level.

Also due to the vast amount of time that has been taken to validate a land transaction in the existing system, there is a lot of room for the fraudulent activity. But here a land transaction can be validated within a span of a few minutes. This reduces the window for fraudulent activities.

Also, the existing system can be altered by various parties being a paper system, and also a digitalized system would vest too much power on the administrator of the system. But being a blockchain system, which is decentralized, a group of administrators.

B. Drawbacks

The existing system would be subjected to natural wear and tear is a paper-based system. but the proposed system being digitalized would be tolerant for those.

This system can be linked with land-based other service providers such as the mortgage banks and finance companies. This would ensure that the middle loan approval and other processes in those systems would be very much streamlined. Further, if the middle person legal officer is removed then this system becomes highly immune to the fraudulent activities.

REFERENCES

[1] T. G. U. P Perera, "Implementing Land Registration Systems in Sri Lanka: Being Pragmatic*"* In Sri Lanka Journal of Real Estate, 2010

[2] "Implementation Completion and Result Report on Sri Lanka Land Titling Related Services Project", World Bank, March 2007

[3] Mr. Cleverence Kombe, Dr. Majuto Manyilizu and Prof. Aloys, "Design of Land Administration and Title Registration Model Based on Blockchain Technology", Journal of Information Engineering and Applications, February 2017, pp 8-10.

[4] Blake Sanders and Daniel Steeves, "Scheduled Private Token Sale & Token Distribution Event", March 2018.

[5] H. Hyvärinen, M. Risius and G. Friis "A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services", Business & Information Systems Engineering, November 2017, pp. 441-456

[6] G. Foroglou and A. Tsilidou, "Further Applications of the Blockchain", 12th Student Conference on Managerial Science and Technology, September 2018

[7] A. Baliga, "Understanding Blockchain Consensus Models", April 2017, pp. 8-9.

[8] E. Buchman, "Tendermint: Byzantine Fault Tolerance in the Age of Blockchains", June 2016, pp 17 – 20.

[9] O. Dib, K. Brousmiche, A. Durand, E. Thea and E. B. Hamida, "Consortium Blockchains: Overview, Applications and Challenges", International Journal on Advances in Telecommunications, September 2018, pp. 51-63

[10] Denys, "How the Consortium Blockchain Works", [Online] Available:https://blockchain.intellectsoft.net/blog/how-theconsortium-blockchain-works, [Accessed 25-Dec-2019].