IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Survey On Creating A Land Administration System Using Blockchain And Cryptography

Saurabh Jain, Atharva Papinwar, Sarang Pathak, Vaibhav Patil, Prof. Arivanantham Thangavelu

Abstract:

It is important to maintain accurate records for any type of property, whether it is land or a home. Such a record can be used to locate the current owner of the property and indicate that he is the true owner, thereby preventing unauthorized, fraudulent changes. The current property verification and transfer procedures are inefficient, prone to errors, ambiguous, and occasionally corrupt. Using blockchain technology, the proposed system enables us to provide a more transparent system for document registration and ownership transfer. To ensure the trustworthiness of the property registration process, we employ the digital signature concept. The attempt to use the IPFS decentralized file-sharing platform provides even more secure data transfer by eliminating the reliance on a single point of storage. It helps in reducing the risk of data loss or destruction.

Keywords: Property Registration Process, Ownership Transfer, Blockchain Technology, Digital Signature, Decentralized Platform, Transparent System, Trustworthiness.

1. Introduction:

Substantial efforts have been made by scholars across the world to compute the economic benefits of secure ownership. However, there is currently no system in place to effectively manage all aspects of property ownership records. The concern of proprietorship is so critical that almost all financial institutions rely heavily on property ownership to ensure their security. At present, people trust various third-party users. E.g., A government agency may be tasked with the responsibility of maintaining a record of ownership information.

Sometimes, these records are not preserved systematically. Since the ownership rights are uncertain, it becomes more difficult for financial institutions to work properly and comfortably, preventing the nation's economic development. As real estate is high-value property so, maintaining the correctness and completeness of such property is important. Moreover, it is essential to have the correct records that recognize the current owner and be responsible for the proof that he is the real owner.

Issues Faced in Property Ownership Transfer:

- Lack of transparency
- Risk of data manipulation
- Poor user experience and education
- Ineffectual protection of the owners' rights (e.g., in case of theft)
- Risks with transfer and sale fraud

Property Registration and Ownership Transfer using Blockchain as a new technology, the blockchain's security, speed, and transparency have made it an attractive option to facilitate ledger-based processes. By using a distributed system like blockchain technology we can keep track of property ownership information systematically.

Blockchain technology can store an absolute history of transnational histories, so nobody can ever doubt the genuineness; records are eternally linked to the system so not even a single entity can manage interfere and manipulate the record.

1.1.1 Aim:

- Have all the property-related documents available at any given point of time just by providing the Aadhaar card number of the owner through a decentralized platform along with the authentic blockchain security.
- Have a transparent system for document registration and transfer of ownership.
- Have a less turnaround time for registration document preparation and signing.
- Digitally sign all documents to maintain the trustworthiness of the property registration process.

2. Literature Survey:

According to Miroslav Stefanovic et al. [1], blockchain and smart contracts could be used to register real estate transactions in land administration systems (LASs).

The Cooperative Search Scheme in the Blockchain-based Data Market was presented by Suhan Jiang et al. [6]. Using Ethereum's contract and gas system, the cost of a query can be divided into two parts: one for data owners, and one for miners. We also use grouping strategies to help our customers save time and money. There is also an equitable way to split the total cost among users, based on the grouping result. For example, it provides proof of group strategy and a sharing incentive to discourage free-riders.

In China, a blockchain-based framework for microfilms has been proposed by Wei-Tek Tsai, et al. [3]. As a result, a BC provides an ideal environment for intellectual property (IP) protection. In [4] [7], a comprehensive literature review of blockchain technology's operation and features is provided. [8] outlines a practical application for blockchain technology. [10] The functioning of blockchain technology and the potential use or impact on current Land Registry systems that it may have, according to Jacques Vos and colleagues [10].

Distributed consensus in the blockchain can be improved by using the epidemic algorithm, according to Pasu Poonpakdee et al. [11]. The goal is to use epidemic protocols to distribute information using unicast communication patterns, whereas blockchain uses broadcast communication patterns. Epidemic protocols, according to early findings, can disseminate information at an optimal rate. However, there are numerous factors to consider, including message overhead, network topology, and more.

An extreme-scale network problem can be solved by using the epidemic protocol [11], randomization of communication, and computation. When it comes to a fixed cycle length for epidemic protocols, this is the norm. Every cycle, a random peer receives the local value sent by each node. They've proven useful in large networks for disseminating information and gathering data. Epidemic membership protocol offers a peer sampling service. The fault tolerance, scalability, decentralization, and lightweight properties of epidemic protocols make them preferable to centralized paradigms when compared to consensus protocols.

Two billion unbanked or underbanked adults around the world could benefit from the blockchain-based Everex capital transfer system, which is described in Alex Norta et al. [12]. For this reason, the novel concept of eFiat, a cryptocurrency whose value is tied to and whose name is derived from a fiat currency, was introduced. Everex users use a currency exchange to convert local currencies to eFiat, then transfer

the coins to their account via their wallet. By using eFiat, the Everex system allows its users to access financial services without the volatility problems that currently plague other, less stable cryptocurrency systems.

For blockchains that make use of the account and multi-asset models, Donghui Ding et al. Anonymous addresses and anonymous asset metadata are incorporated into the transaction structure in order to facilitate asset transfer and double-spending detection. The zero-knowledge proof is generated and verified using the zk-SNARKs algorithm. Finally, we put our plan to the test through a series of experiments.

3. Fundamentals of Blockchain:

A blockchain is a distributed ledger technology that is shared among the nodes of a computer network. As a database, a blockchain stores information in digital format. Blockchains play a vital role in the cryptocurrency ecosystems, such as Bitcoin, Ethereum, etc., to create and maintain a highly secure and decentralized ledger of transactions. The upheaval with a blockchain is that it has the potential to cater to the need for fidelity and security of a record of data and yields trust without the need for a trusted third party.

The fundamental distinction between a typical database and a blockchain is the structuring of data. A blockchain accumulates information together in chunks, known as blocks, that contain sets of information. Each block can hold only a specific amount of data and, when topped up, will be closed and linked to the previously loaded block, composing a chain of data togetherly known as the blockchain. Whatever information that will be added newly will be compiled into a block formed at the later stage which will then proceed towards the addition to the primary blockchain once they're completely filled.

In a database, the structure of the data usually comprises rows and columns forming tables, while in blockchain as its name suggests, is a network of interconnected blocks. This leads to devising a data structure when implemented in a decentralized nature will lead to a completely irreversible timeline of data. As soon a block reaches its maximum capacity, it is etched in stone and permanently becomes a part of the main timeline where each and every block contains an exact timestamp when it is linked to the main blockchain.

4. Proposed Methodology:

Property registration and ownership transfer can be more secure and transparent thanks to the blockchain's data transfer security and transparency. Using a distributed and shared database, secure data transfer can be accomplished. This means that the documents cannot be tampered with and there is no need for third-party verification. When we take into account all these factors, we're motivated to develop a system that uses Blockchain to ensure the integrity of Digitally signed documents in the property registration process. The same is represented in Figure 1, which depicts the design.

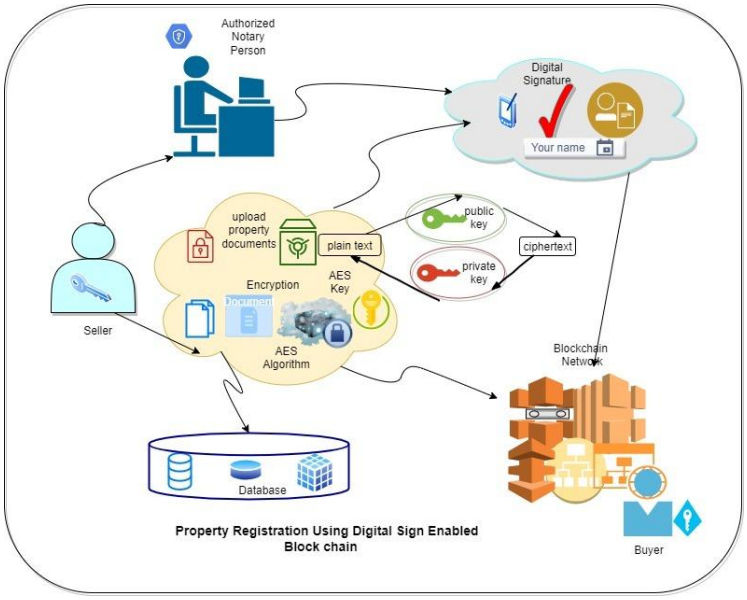

Figure. 1

Proof of Ownership:

In order to prove that you are the rightful owner of a piece of property, you will need to provide proof of ownership. Encrypted documents and metadata are uploaded to a decentralised platform by the data owner or seller. Every single document pertaining to the property is signed digitally. Authorized users should be able to make changes to all related documents.

Proof Of Authentication:

An individual user's username and password are used to verify their identity. Uploading property documents necessitates the use of a unique digital e-sign for each user.

Upload Property file With Digital Signature:

Digitally sign each document before uploading it to the property. Electronic documents, transactions, and messages containing digital signatures can provide additional assurances to their signers by acknowledging their informed consent and providing proof of the document's origin, identity, and current status. That's why uploading property files requires a digital signature.

Upload property File & Grant permissions:

Let's say the owner or seller of the data uploads documents containing real estate information in encrypted format with a digital signature. With its permissions, an authorised person can grant XYZ user access to this property document that has been uploaded by XYZ user. This is important because security is becoming increasingly important in today's world. Read, Write, and Append are the three permissions.

Share Property File:

This decentralised platform enables document owners and sellers to share data with other users. Different types of permissions are granted to users by this system.

Store Property File Using Blockchain:

The digitally signed property file is stored sequentially in blocks in a decentralised, distributed system. IPFS is a protocol created specifically for the storage of distributed file storage that is peer-to-peer in nature. While an unauthorised third party cannot read encrypted data, a trusted individual can decrypt encrypted data and gain access to it in its original form. Popular encryption and decryption methods exist, but the key is not a proprietary algorithm. Encryption keys must be kept secret so that only trusted parties have access to them. Encrypt all of your data so that each property file is stored in an Encrypted Format, which is more secure.

4.1 Algorithms:

1. The Inter-Planetary File System (IPFS):

It is a decentralized file-sharing platform used for storing files, blocks, and raw pieces of data and aims to recognize the content based on the content id.

After uploading the file to IPFS, it divides the files into two parts, each of which contains the most 256 KB of data.

Each portion is identified by a cryptographic hash called QM hash or Content Identifier (CID).

2. AES:

The prime purpose of the AES algorithm is to encrypt large-size data.

AES is a kind of symmetric key block cipher algorithm widely used around the world for data encryption.

It's a particular structure of encrypting and decrypting data make it more secure so that it cannot be hacked.

AES can deal with different key sizes such as AES 128, 192, and 256 bit and each of these ciphers have a block size of 128-bits.

AES system goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys to retrieve the original plain-text

For 128-bit keys, before reaching the final round, this output goes through nine rounds, during each round four transformations are performed:

1) Sub-bytes

2) Shiftrows

3) Mix-columns

4) Add round Key. In the 10th round, there is no Mix-column transformation.

3. RSA:

The RSA algorithm is a public key encryption technology that is widely regarded as the most secure. Rivest, Shamir, and Adleman devised the RSA algorithm in 1978, hence the name.

The following characteristics are present in the RSA algorithm:

The RSA algorithm is a popular finite field exponentiation over integers, including prime values.

This approach uses sufficiently large integers, making it challenging to solve.

In this algorithm, there are two types of keys: private and public.

The data sent by the sender is encrypted with the receiver's public key and the receiver decrypts the data with their own private key.

Conclusion:

Here, an effort is made to provide a transparent and robust security system for the registration and transfer of ownership of property. We no longer have to rely on a third party to verify property transfers when they are secured by the blockchain. Encrypted documents are first uploaded to the blockchain by a user with a digital signature. The public RSA key is used to encrypt the symmetric key. When a third-party user requests access to a document, the data owner is notified. The user decrypts the symmetric key using the RSA private key after receiving permission from the data owner. Documents are unencrypted after he obtains the key.

The data is even more secure because there is no central point of storage, which reduces the risk of it being lost or destroyed as it travels over the blockchain.

References:

[1] Prof. Arivanantham Thangavelu, Prof. Poonam Deokar, Prof. Preeti Patil, "Explicating the Trust and Scaling Issues in the Blockchain Cryptocurrency Ecosystem", ©2021 IJRAR November 2021, Volume 8, Issue 4

[2] Miroslav Stefanovic´, Sonja Ristic´, Darko Stefanovic´, Marko Bojkic´ and ore Przˇulj, "Possible Applications of Smart Contracts in Land Administration", ©2018 IEEE.

[3] Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, "Blockchain challenges and opportunities: a survey", Int. J. Web and Grid Services, Vol. 14, No. 4, 2018.

[4] Wei-Tek Tsai, Libo Feng, Hui Zhang, Yue You, Li Wang, Yao Zhong, "Intellectual-Property Blockchain-based Protection Model for Microfilms", 2017 IEEE Symposium on Service-Oriented System Engineering.

[5] Ibrar Ahmed1, Shilpi2, Mohammad Amjad, "Blockchain Technology A Literature Survey", IRJET Volume: 05 Issue: 10 — Oct 2018.

[6] Merlinda Andoni,Valentin Robu David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, Andrew Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Elsevier 2018.

[7] Suhan Jiang, Yubin Duan, Jie Wu, "A Client-biased Cooperative Search Scheme in Blockchain-based Data Markets", 2019 IEEE.

[8] Pauliina KRIGSHOLM, Kaisa RIDANPA¨ A¨ and Kirsikka RIEKKINEN, Finland, "Blockchain as a Technological Solution in Land Administration –What are Current Barriers to Implementation", Geospatial information for a smarter life and environmental resilience- Hanoi, Vietnam, April 22–26, 2019.

[9] Saranya A1, Mythili R, "A Survey on Blockchain Based Smart Applications", International Journal of Science and Research (IJSR), 2019.

[10] https://chromaway.com/papers/A-blockchain-based-property-registry.pdf

[11] Jacques Vos, "BLOCKCHAIN-BASED LAND REGISTRY: PANACEA, ILLUSION OR SOMETHING IN BETWEEN?", 7th Annual Publication, October 30 2016).

[12] Pasu Poonpakdee; Jarotwan Koiwanit; Chumpol Yuangyai; Watchara Chatwiriya, "Applying Epidemic Algorithm for Financial Service Based on Blockchain Technology", 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST).

[13] Alex Norta; Benjamin Leiding; Alexi Lane, "Lowering Financial Inclusion Barriers with a Blockchain-Based Capital Transfer System", IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).

[14] Donghui Ding; Kang Li; Linpeng Jia; Zhongcheng Li; Jun Li; Yi Sun, "Privacy protection for blockchains with account and multi-asset model", China Communications (Volume: 16, Issue: 6, June 2019).