JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Empirical Approach Towards Improving Operational Efficiency Of Land Acquisition System Utilizing The Blockchain Technology

Saurabh Jain, Atharva Papinwar, Sarang Pathak, Vaibhav Patil, Prof. Harshal Mahajan

Abstract:

The land is a non-liquid, immovable asset with a high value. The integrity and accurate tracking of land ownership/transfer records is a difficult task. The existing property registration process has several problems, and people take advantage of them to cheat people and the authorities involved. While land ownership can change over time, and often quite frequently, preserving detailed and lengthy ownership transfer documentation can be a difficult task. The majority of the problems originate from the fact that present land registration systems either have legacy paper document trails or are poorly maintained non-transparent centralized systems. To modify the property ownership record, fraudulent users may try to fabricate physical documents or edit computer information. This paper presents a safe record-keeping technique that addresses these difficulties by utilizing a Blockchain-based system that can produce physical asset records into immutable liquid blockchain-based token assets. This new blockchain token asset can now be utilized to maintain a clearly visible and digitally secure ownership record. Unlike today's centralized cadastral methods, blockchain allows for the creation of a decentralized, transparent database.

Using blockchain-based decentralized storage services, which can create a new paradigm for safe data outsourcing and correct remote search, many of the present cloud-based data marketplaces' privacy and security difficulties will be eliminated. The use of blockchain technology, specifically smart contracts, may improve the process of registering transactions in property management systems. We focused on performing a comprehensive analysis of blockchain technology. Further, we studied the concept of digital signature, various algorithms i.e., AES, DES, and the use of the IPFS decentralized file-sharing platform to provide 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. The security issue is greatly reduced by implementing land registration using blockchain technology.

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

1. Introduction:

A land administration system mainly records data consisting of the said property's location, ownership status, valuation, and usage. Additionally, the land administration system also maintains the record of physical, topographical, and spatial data of the location. This data can be categorized as legal and spatial data. The property's location, ownership status, valuation, and usage fall into the category of legal data stored in the land register. The physical, topographical, and spatial data come under spatial data which is usually stored in a cadastre.

A record that contains the legal situation regarding a specific unit of land that contains the record of land or its deeds is known as a land register. Whereas, an official record of data consisting of the specifics about the particular unit of land that is generally obtained by surveying the property's boundary is known as a cadastre. The land register contains the information about the owner of the property along with the documentation of the property. On the other hand, the cadastre consists of details including the address, usage of the land, nature, construction details, and taxation value.

It is suggested to integrate two LAS subsystems but LAS still majorly have got two separate subsystems. The main reason behind separation is an inconsistency between these two subsystems which occurs during the process of integration. Incorrectness in LAS can be detected using these inconsistencies.

There are several other reasons which are needed to be addressed in the traditional LAS, which include but are not limited to the incorrect state of LAS caused as a reason of the digitization and poor quality of cadastral maps or because of human errors. These issues are of extreme importance as they can lead to unreliability in any systems that get their data from any LAS and in turn hamper the decision-making of those systems. It can also give rise to numerous legal complications as the data from LAS is mostly presumed to be in the correct state. Hence, ensuring the correctness of this data is quite important for the stakeholders.

In this paper, we focus on addressing these problems using blockchain technology, particularly smart contracts and their possible applications that can assist in solving the above-mentioned issues by utilizing the technology to its fullest.

The purpose of using blockchain in the property registration process is rather easy to justify in the countries where the land administration systems are not trusted, as a consequence of corruption, bad governance, or due to the lack of quality of that register. Undoubtedly, blockchain technology in these cases would be the answer for organizing the process of property registration and ownership transfer in a more efficient and trustworthy manner.

2. Related Work:

2.1 Blockchain:

Blockchain is being referred to as the fifth disruptive innovation in the field of computing.

The term blockchain was pioneered by a pseudonymous entity under the alias of Satoshi Nakamoto in the paper titled "Bitcoin: A peer-to-peer electronic cash system", published in the year 2008.

A study shows that as of 2017 only 69 peer-reviewed papers were published that discussed the applications of blockchain technology in other fields rather than just focusing on cryptocurrency.

Decentralization, immutability, transparency, and smart contracts are pinpointed as the main characteristics of blockchain technology.

Blockchain creators' initial idea was to eliminate the need for some trusted third party included in a financial transaction. In the first blockchain use case, which is bitcoin, asymmetric cryptography, cryptographic hash functions & Proof-of-Work were used to achieve this target. In the asymmetric cryptography technique, public & private pair keys are used to authenticate & encrypt the messages.

The process of a transaction from one owner to another implies that the cryptocurrency's owner uses his private key to sign the hash of the previous transaction and the new owner's public key, and this data is converted into coins. Transactions performed in this fashion are added to blocks which are then added to the blockchain.

The consensus algorithm is used to add a new block to the blockchain. The consensus algorithm tackles the problem of double-spending by acting as a timestamp server. Every new block in the blockchain is made up of three parts: new transactions, the preceding block's hash, and the nonce. Only the nonce can be modified because the hash of the preceding block and transactions are constants at the block level. The nonce's purpose is to allow network nodes to generate a hash of a new block that is lower or equal to the current blockchain's target hash. The number of transactions that a peer-to-peer network can complete in a given length of time is determined by the target hash. Nodes in a peer-to-peer network running a certain blockchain perform the computations required to determine the nonce that will result in a "valid" hash. These nodes are contending to be the first to find the

proper nonce and receive the reward for their contributions. The chances of finding nonce are determined by the consensus algorithm used by the blockchain. Proof-of-work is the most frequent consensus algorithm, and in this event, the probabilities of obtaining this nonce are solely dependent on the computational capability of a single node. Proof-of-stake, where the probabilities of discovering the nonce is depending on the amount of currency a node has or practical byzantine fault tolerance, delegated proof of stake, ripple, or thundering are examples of less frequent consensus methods.

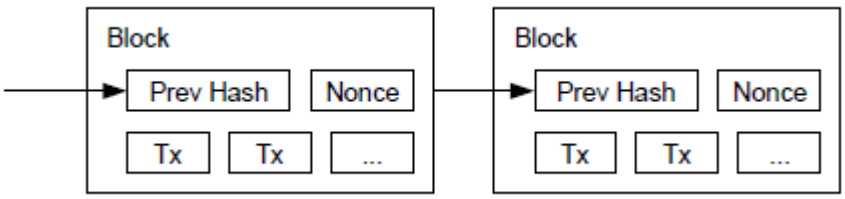

Figure 1: Graphical representation of the process of formation of blockchain

2.2 Smart Contracts

The smart contracts were originally introduced by Nick Szabo in the year 1996. Later with the appearance of the Ethereum blockchain created by Vitalik Buterin, which was the first Turing complete language for smart contracts, they came into the limelight.

A smart contract is a solution that utilizes blockchain technology for creating contracts between two or more parties in a decentralized environment. In layman's terms, a smart contract can be considered as a coded program that provides the capability to be read and also executed automatically if a certain pre-defined set of provisions is fulfilled. If contracts are made in a blockchain-based decentralized environment, they can be executed safely even without trust between the parties involved. Smart contracts have the potential to lower transaction costs (using a trusted third-party verification has costs) as well as to decrease frauds and other malpractices.

3. Implementation Details:

3.1 Proposed System Architecture:

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 2, which depicts the design.

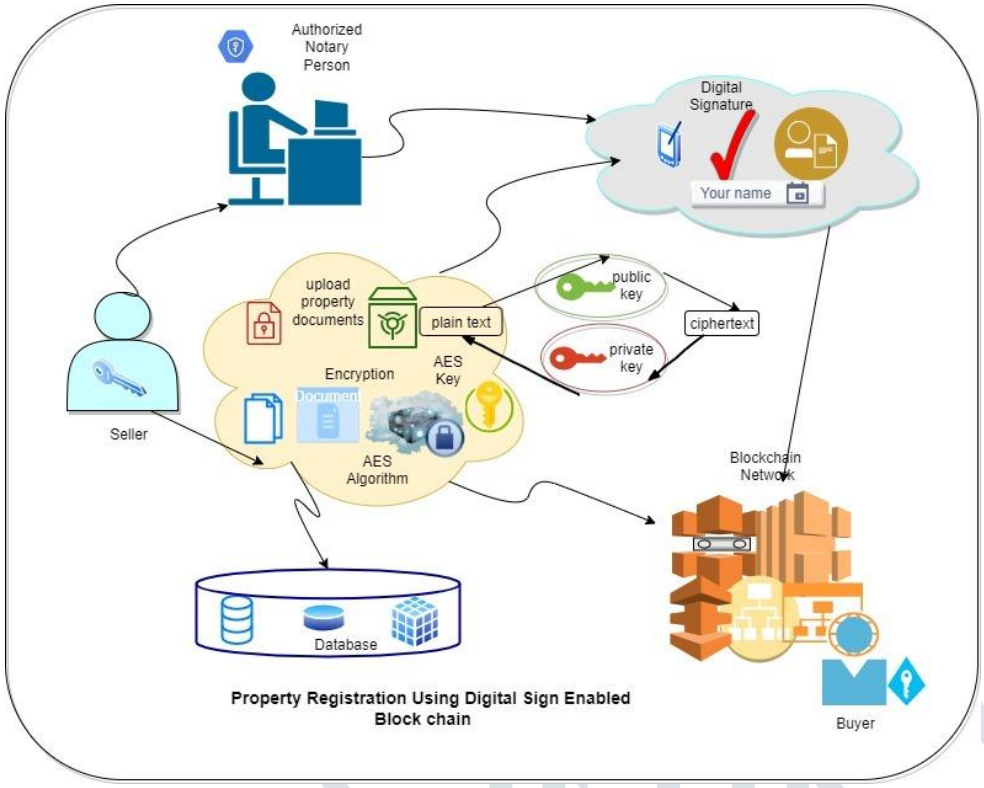

Figure 2: Proposed System Architecture

3.2 Algorithms Used:

I. IPFS:

The Inter-Planetary File System also known as "IPFS" is a decentralized distributed system, which provides the ability to store and access data, websites, applications, and any other files.

When a file is uploaded to IPFS, it is broken down into different chunks. Each chunk contains a maximum of 256 kilobytes of data and/or links to the additional chunks of data.

Every chunk is identified by a cryptographic hash, also known as a content identifier (CID), that is computed from its content.

A node can either pin the content to preserve it forever or discard it when isn't used for a while in order to save space.

This means each node stores only content it is interested in with some indexing information that ensures which node stores what kind of information.

The files on the IPFS network are resistant to censorship and tampering. Along with all these functionalities, the user does not need to remember the long strings of CIDs. In order to map these CIDs, DNSLink is used along with the IPFS decentralized naming system which converts them to human-readable names.

Identifiers:

- **Node IDs:**

Public Key Hash. Routing in DHT, based on:

1. Other peer's network addresses.

2. Object names.

- **Distributed Hash Table (DHT):**

S/Kademlia:

It stores two different types of information.

1. Every time a new file is uploaded through a node, the latter registers itself as a supplier of the chunks of the file.

2. The DHT contains information on how to connect to a node with a specific identifier, for example by providing an IP address.

- **Object Merkle Directed Acyclic Graph (DAG):**

1. The Merkle Directed Acyclic Graph helps us in identifying the entire file by using the root hash only.

2. On top of DHT/block exchange.

3. Objects are immutable.

4. Generalization of Git data structure.

- **File sharing:**

IPFS provides the utilisation of complicated Merkle-Linked structures with the data addressability of peer-to-peer file-sharing systems. The content is further distributed over a peer-to-peer network.

II. RSA:

RSA is one of the best-known public-key cryptosystems for key exchange or encryption of blocks of data or digital signatures. RSA uses a variable size key along with a variable size encryption block. It is a number theory based asymmetric (public key) cryptosystem, which is a block cipher system. Two prime numbers are used for the generation of the public key and private key. These two different keys are used for encryption and decryption purposes. The sender encrypts the message using the Receiver's public key and when the message gets transmitted to the receiver, the receiver can decrypt it using his own private key. RSA operations can be decomposed into three broad steps; key generation, encryption, and decryption.

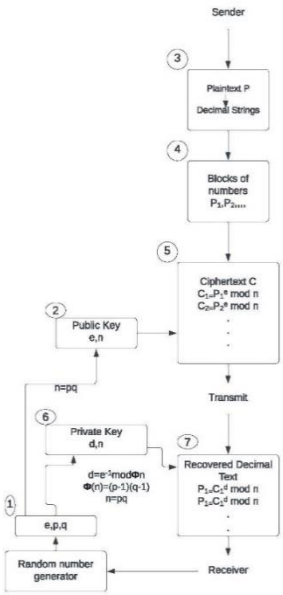

Figure 3: RSA processing of Multiple blocks

- **Key Generation Procedure:**

1. Choosing two distinct large random prime numbers p & q such that $p \neq q$.

2. Compute $n = p \times q$.

3. Calculate: phi (n) = (p-1) (q-1).

4. Choose an integer e such that 1<e<phi(n)

5. Compute d to satisfy the congruence relation $d \times e = 1 \bmod \text{phi}(n)$; d is kept as a private key exponent.

6. Here, the private key is (n, d) and the public key is (n, e). The values d, p, q, and phi must be kept a secret.

- **Encryption:**

Plaintext: P < n

Ciphertext: C = Pe mod n.

- **Decryption:**

Ciphertext: C

Plaintext: P = Cd mod n.

III. AES:

AES algorithm supports multiple combinations of data along with key lengths of 128, 192, and 256 bits and is referred to as AES-128, AES-192, or AES-256, depending on the length of the key. During the encryption and decryption process, the AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys. This in turn allows it to deliver the final output in the form of cipher-text or to retrieve the original plain text. The data length of AES is 128-bits, which can be further categorized into four operational blocks. These blocks are treated as an array of bytes and organized as a matrix of the order of 4×4 that is called the state.

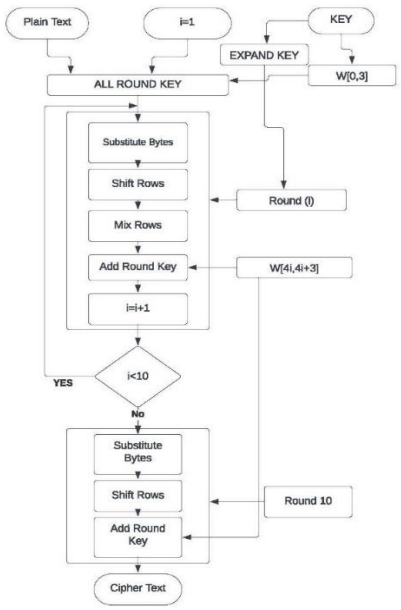

Figure 4: AES (Advanced Encryption Standard) Process

A. Encryption:

The steps of AES encryption for a 128-bit block are as follows:

1. The set of round keys is to be derived from the cipher key.

2. Initializing the state array with the block data (plaintext).

3. The initial round key is then added to the starting state array.

4. Performing nine rounds of state manipulation.

5. Performing the tenth and final round of state manipulation.

6. Copying the final state array out as the encrypted data (ciphertext).

A series of steps are required by each round of the encryption in order to alter the state array.

Four types of operations are involved in these steps:

1.Sub-Bytes

2.Shift-Rows

3.Mix-Columns

4.XOR-Round Key

B. Decryption:

The process of decryption consists of performing all the steps of encryption in a reverse manner along with the inverse functions:

1.InvSub-Bytes

2.InvShift-Rows

3.InvMix-Columns

Operation in decryption is:

1. Perform initial decryption round:

XOR-Round Key

InvShift-Rows

InvSub-Bytes

2. Perform nine full decryption rounds:

XOR-Round Key

InvMix-Columns

InvShift-Rows

InvSub-Bytes

3. Perform final XOR-Round Key:

XOR-Round Key

InvMix-Columns

InvShift-Rows

InvSub-Bytes

4. Mathematical Model:

S = {U, C, V, I, T, F, FT, Ds, Ss} where,

– U = {U1, U2, U3. . . . .Un | Here 'U' is a Set of all USERS}

U is the user of the system. Users of the system may grow as more and more people use the system. The user is an infinite set.

– ES = {E REG, E ENC, E DEC | 'ES' is a Set of Encryption Service}

C is the camera to capture the imaging system. This service uses the AES & RSA algorithm for encrypting a file. Primarily, three services are provided by this ENCRYPTION SERVER. Hence, it's a Finite Set as the number of attributes are limited.

– SS = {S REG, S LOGIN, S UPLOAD, S DOWNLOAD| SS is a Set of Storage Service}

STORAGE SERVER will provide four services like Registration, Login, Upload, and Download. This set also has finite attributes, so this is also a Finite Set.

– K= {K1, K2, K3. . . . . .Kn | K is the Set of Keys }

This set is used for storing the keys may be encryption or decryption. As there may be a number of files so there may be a number of keys also. This is also an infinite set.

– DE = {UID, PUB KEY, PRV KEY | DE is a Set of a data table for storing of Keys on Encryption /Decryption Server}

Encryption / Decryption Server will be used to temporarily store data for the separate encryption-decryption process.

– DS = {USERINFO, USERDATA | DS is a Set of a data tables for permanent storing of data on server}

– USERINFO = {User ID, Password, FULL NAME, Email ID, contact | USERINFO is a set for storing User}

Activities / Events:

- **EVENT 1**

User will make registration on Encryption Server & Storage Server.

Let's consider f(U) as the function of the User

Thus, f(U) → {Es ∪ Ss}

- **EVENT 2**

User will log in to both the server.

Let's consider f(U) as the function of the User

Thus, f(U) → {Es ∪ Ss}

- **EVENT 3**

User will be authenticated.

Let f(Es) be a function of the Encryption Server.

Thus, f(Es) → {U1, U2, U3....Un} ε U

- **EVENT 4**

The data owner will encrypt the file initially using AES

Let f(Es) be a function of the Encryption Server.

Thus, f(Es) → {F1, F2, F3.....Fn} ε F

- **EVENT 5**

Data owners upload files with a digital signature to the Encryption Server.

Let's consider f(Un) as the function of 'n' number of Users.

Thus, f(Un) → {E s} ε U

The digitally signed property file is stored using blockchain technology.

Let f(S) be a function of the System

Thus, f(S)→ {Es}

- **EVENT 6**

The exchange of the keys takes place using the DIFFIE-HELLMAN method of key exchange.

Let's consider f(Un) as the function of 'n' number of Users.

Thus, f(Un) → {Es} ε U

- **EVENT 7**

The encryption server will decrypt the file using the same keys

Let f(Es) be an Encryption Server.

Thus, f(Es) → {F1, F2, F3. . . ..Fn} ε F

EVENTS FOR RETRIEVAL OF FILE:

- **EVENT 8**

The user will Log in. Let f(U) be a function of the User

Thus, f(U) → {Es ∪ Ss}

- **EVENT 9**

The user will send the request to the authorized person.

Let's consider f(U) as the function of the User.

Thus, f(U) → {F1, F2, F3. . . . . Fn} ε F

- **EVENT 10**

Let f(G) be a function to grant permission to access the file.

Thus, f(G) → {F1, F2, F3. . . .Fn} ε F

- **EVENT 11**

Decryption keys will be used here for Decrypting files.

Let f(Es) be an Encryption Server.

Thus, f(Es) → {K1, K2, K3. . . . . .Kn} ε K

- **EVENT 12**

The user will decrypt the file and can use it.

Let f(Un) be a set of N Users.

Thus, f(Un)→ {F1, F2, F3. . . .Fn} ε F

Venn Diagrams:

As described in activity 1 following Venn diagram is drawn

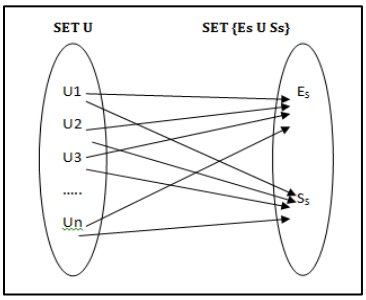

Figure 5: Venn diagram 1

As described in activity 3 following Venn diagram is drawn

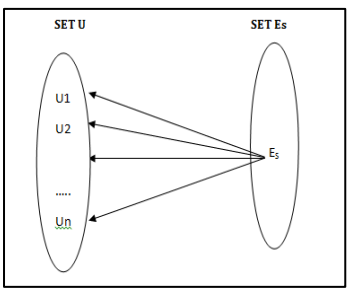

Figure 6: Venn diagram 2

As described in activity 4 following Venn diagram is drawn

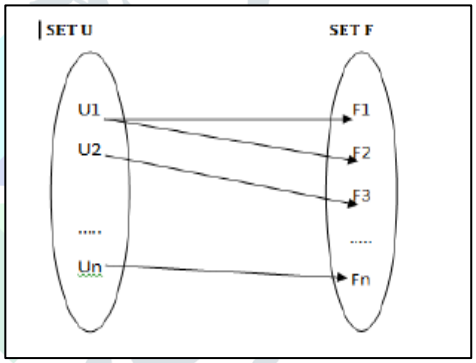

Figure 7: Venn diagram 3

As described in activity 5 following Venn diagram is drawn

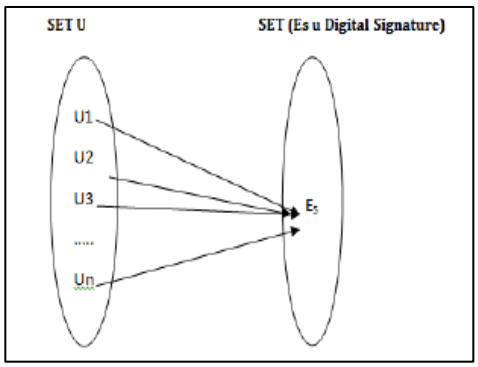

Figure 8: Venn diagram 4

As described in activity 7 following Venn diagram is drawn

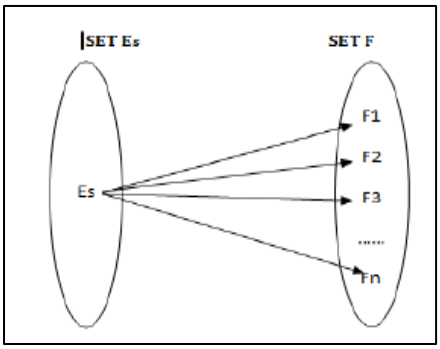

Figure 9: Venn diagram 5

As described in activity 10 following Venn diagram is drawn

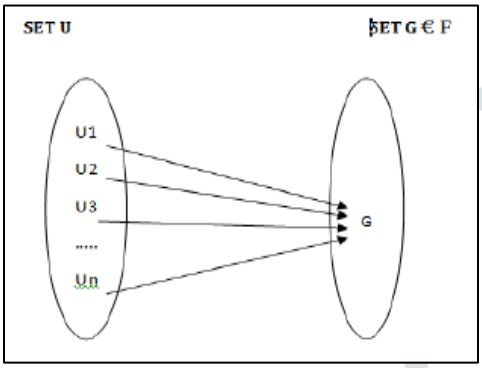

Figure 10: Venn diagram 6

As described in activity 11 following Venn diagram is drawn

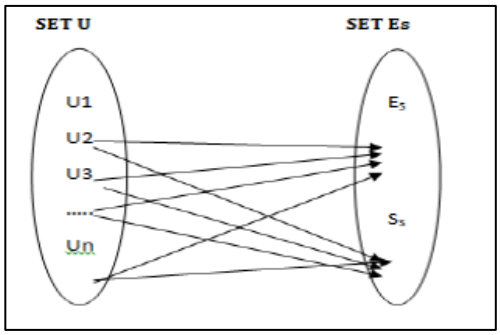

Figure 11: Venn diagram 7

As described in activity 12 following Venn diagram is drawn

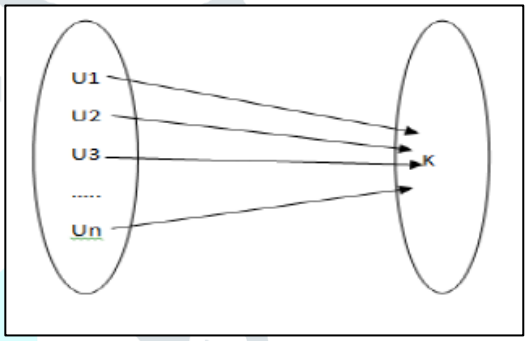

Figure 12: Venn diagram 8

5. Result Analysis:

In the proposed system, we used the AES algorithm to encrypt and decrypt files/data for secure file transfer. Firstly, before uploading to a decentralized platform, we use the AES algorithm for encrypting the user's data and digitally signing it. We are using the AES algorithm as it takes less time for data encryption compared to DES and ECC (Elliptic-curve cryptography) algorithms.

Algorithm Comparison		
Sr. No.	Algorithm	Time(ms)
Encryption	DES	24
	AES	7
	ECC	17
Decryption	DES	28
	AES	12
	ECC	20

Figure 13: Algorithm Comparison

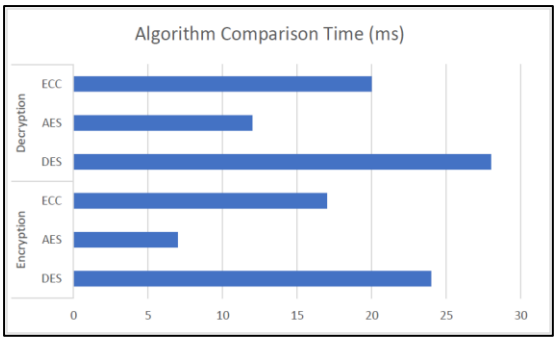

Figure 14: Graphical Representation of Algorithm Comparison

Figure 13 gives the algorithm comparison for AES, DES, and ECC algorithms in terms of encryption and decryption in a tabular form. The visual illustration of the table is shown in figure 14.

Here the RSA algorithm is used for key encryption. After uploading the encrypted document over blockchain, the symmetric key of the uploading is encrypted by using the RSA public key of the user. It can be known by everyone. Figure 15 gives the comparison of operation time required for RSA and ECDSA for 512, 256, and 1024 bits of input in tabular form. The graphical representation of the table i.e., comparison of the RSA and ECDSA for 256, 512, and 1024 bits is given in figure 16.

Input size(bits)	Algorithm Name Key Size	Encryption	Decryption
256	RSA 1024	1.26239	3.282019
	ECDSA 192	5.06889	4.404533
512	RSA 1024	2.263075	5.23173
	ECDSA 192	4.84413	6.494078
1024	RSA 1024	3.92709	33.765234
	ECDSA 192	6.264871	44.315245

Figure 15: Operation Time for Different Key Sizes

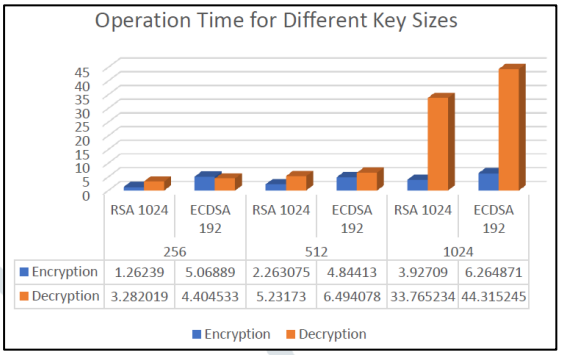

Figure 16: Graphical Representation of Operation Time for Different Key Sizes

The property which is available for the sell is sent for the verification process to a higher authority by the seller. The figure shows the verified property details like ID, property number, Survey, area, address, and registrar.

After verification of the property, the seller can transfer the ownership to the buyer. The transfer of ownership contains the property details that are to be transferred and details of the new owner along with the seller details like selling cost, stamp duty, property area, and market value.

Conclusion:

Blockchain technology seems to be quite disruptive and shows phenomenal potential in the domain of land administration. In this paper, we proposed a flawless, feasible, and hassle-free solution that can be handy in making the land registration process easier. There are many challenges involved in this process such as broker margin, time delays, etc. We can get rid of such problems associated with land registration in India as well as the rest of the world by using this system.

The major issue in the Land Acquisition system lack of transparency in the authentication process and the complexity of identifying the real owner. But being a digitalized system, it has been reduced to a significant level. This system can secure the ownership documents from man-made as well as natural disasters by making the process of land registration paperless also making the process easier & eco-friendly at the same time.

It takes a lot of time to validate the transaction in the conventional system, there is a very high possibility of getting fraud. But in this system transaction occurs in a few minutes. This gives so much less room for fraudulent activities. Also, in the existing system, there are chances of papers being altered by various parties being based on the paper system. On the other hand, too much power will be vested in the hands of the system administrator. But the decentralized nature of blockchain would divide it among several groups of administrators. Because of all the above advantages, there is wide scope for this platform there can be many use cases of the platform created.

References:

[1] Saurabh Jain, Atharva Papinwar, Sarang Pathak, Vaibhav Patil, Prof. Arivanantham Thangavelu, "Survey On Creating A Land Administration System Using Blockchain And Cryptography", © 2022 IJRAR February 2022, Volume 9, Issue 1

[2] 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

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

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: May 17, 2021].

[5] 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.

[6] 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.

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

[8] 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.

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

[10] 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.

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

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

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

[14] 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).

[15] 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).

[16] 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).