ISSN No:-2456-2165

# Blockchain Technology

STELLA MARIS COLLEGE

(Autonomous)

17, Cathedral Road,

Chennai-600086.

Bachelor of Computer Application

(Affiliated to University of Madras)

ISSN No:-2456-2165

# BONAFIDE CERTIFICATE

This is to certify that this is a bonafide report of the Critical Analysis done by:-

Sonali. M

Shakthi Nivedha. G

Ms. Rajalakshmi. S (Assistant Professor )

# TABLE OF CONTENTS

ISSN No:-2456-2165

## ABSTRACT

**Blockchain is a peer-to-peer decentralized distributed ledger technology that 20provides the records of any digital asset transparent and unchangeable and works without any third-party intermediaries. Blockchains are tamper-resistant digital ledgers distributed in a distributed fashion. It is a digital collection of information about the transaction. Blockchain was initially invented as a way of verifying the contents of a document using immutable timestamps. It was designed as a way of ensuring authentication, immutability, and privacy. This paper consists of core concepts like proof of work, proof of stack, Round Robin Consensus Model, BDAS working Algorithm, Agriculture Traceability Tools and Technology Solutions, and an introduction to Ethereum in Blockchain.**

ISSN No:-2456-2165

# CHAPTER ONE
# INTRODUCTION

Blockchains are digital ledgers that exhibit tamper-evident qualities and resistance to tampering. They are created and maintained digitally without reliance on a central repository or authority. At a fundamental level, blockchain technology empowers a community of users to document transactions and distribute ledgers among a select group of individuals. The paramount aspect of blockchain is its inherent immutability, ensuring that once a transaction is recorded, it cannot be altered, thereby safeguarding data integrity. Blockchains serve as decentralized ledgers that store transactions securely through cryptographic signatures, organizing them into interconnected blocks to enhance their resistance against tampering. In 2008, blockchain technology was integrated with various innovations and ideas to establish cryptocurrencies, which serve as digital currencies secured by cryptographic methods, rather than relying on a central authority or repository. This technology garnered substantial attention in 2009 when the Bitcoin network was introduced. Within the Bitcoin system, users have the capability to digitally sign and transfer ownership of data to another party, and the Bitcoin blockchain effectively records this transfer, enabling all network participants to independently verify the validity of these transactions.

Blockchain Technology changed the working pattern of real estate and the e-governments involved in it; it changed the entire perspective of government contracts, and as a result, we now have upgraded rights, laws, and contracts. In this modern era, blockchain revolutionized the ownership of properties and introduced the concepts of tokenization, smart contracts, titles, and smart laws. These concepts explain the basic mechanism of blockchain in real estate and the security that makes the technology indestructible and tamper-resistant. As the conclusion reduces the physical kinetic energy of an organization and increases transparency along the way the document is processed, it helps to minimize the human errors and chaos or catastrophe involved with ownership.

ISSN No:-2456-2165

# CHAPTER TWO
# LITERATURE REVIEW

Blockchains are digital ledgers characterized by their resistance to tampering and lack of a central repository or authority. At a foundational level, they empower a user community to document transactions and distribute ledgers among a specified group of individuals.

At the forefront of modern cryptocurrency progress lies Ethereum, a blockchain implementation that places a strong emphasis on smart contracts. Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ethereum is open source and is used primarily to support the second-latest cryptocurrency in the world, known as Ether. Ethereum enables the smart contacts and applications built on its blockchain to run smoothly without fraud, downtime, control, or any third-party interference.

Biometric authentication systems exhibit significant security vulnerabilities, including the potential for biometric data leaks, the inconsistency of authentication modules, and the lack of transparency in managing biometric information. We will discuss the BDAS, a new biometric authentication system using blockchain that provides a decentralized and distributed mechanism for processing_biometric authentication and an auditable mechanism for managing biometric information. BDAS's evaluation demonstrates that it provides reliable and secure authentication compared to existing methods while introducing negligible performance overhead in real-world scenarios. BDAS (Blockchain-based Distributed Biometric Authentication System), a new biometric authentication system using blockchain,

Traceability, often referred to as the "one step back, one step forward" principle, entails the capability to retrieve comprehensive information regarding the source and history of a food product. It is the "ability to follow the movement of a feed or food through specified stages of production, processing, and distribution. Traceability encompasses data regarding food ingredients, their sources, processing, transportation, and storage conditions. It includes both quantitative and qualitative information pertaining to the ultimate food product and its origins.

The blockchain serves as an immutable, decentralized public ledger for the management of ownership records, including land titles and various property rights. Managing the property and even performing peer-to-peer transactions have been made possible with the DLT system.

A token, a blockchain-based record representing property rights, is a unit of account that is connected to the user's address and showcases exclusive control over the given address enabled by the user's private key.

A token is mapped with cadastral data and property rights such as leases, mortgages, superficies, etc. The linkage between real estate and property rights with the title record is established by entities possessing the authorization to validate ownership, deeds, and other property rights transactions.

ISSN No:-2456-2165

# CHAPTER THREE
# METHODOLOGY

A critical literature review analysis is conducted, focusing on advancements in finance, Ethereum, Securing a biometric authentication system, Agriculture traceability systems, and Real estate tokenization.

*A. Blockchain Components*

➢ *Cryptographic Hash Functions:*

It is one of the most important components of blockchain technology. Hashing is one of the methods in the cryptographic hash function to get unique Data. Even the smallest change to the input will result in a completely different output digest.

| Input | SHA 256 Digested Value |
|---|---|
| 2022 | b1ab1e892617f210425f658cf1d361b5489028c8771b56d845fe1c62c1fbc8b0 |
| Technology! | 86acff5d3a8c46144dcb6f5528da96ac5d5ded243b66fd22bec77fe8c763c091 |

Fig 1 Sample Input Texts and Corresponding SHA-256 Digests

- *Cryptographic Hash Functions have these Important Security Properties:*

✓ They are preimage-resistant. It means that it is computationally infeasible to compute the correct input value given some output value.
✓ They are second-preimage resistant. This means one cannot find an input that hashes to a specific output.
✓ They are collision-resistant. This means that one cannot find two inputs that hash to the same output.

➢ *Cryptographic Nonce:*

A cryptographic nonce is a random number employed exclusively for a single purpose. When combined with data, it can generate distinct hash digests.

- Nonce: Hash (Data + Nonce) = Digest

➢ *Transactions:*

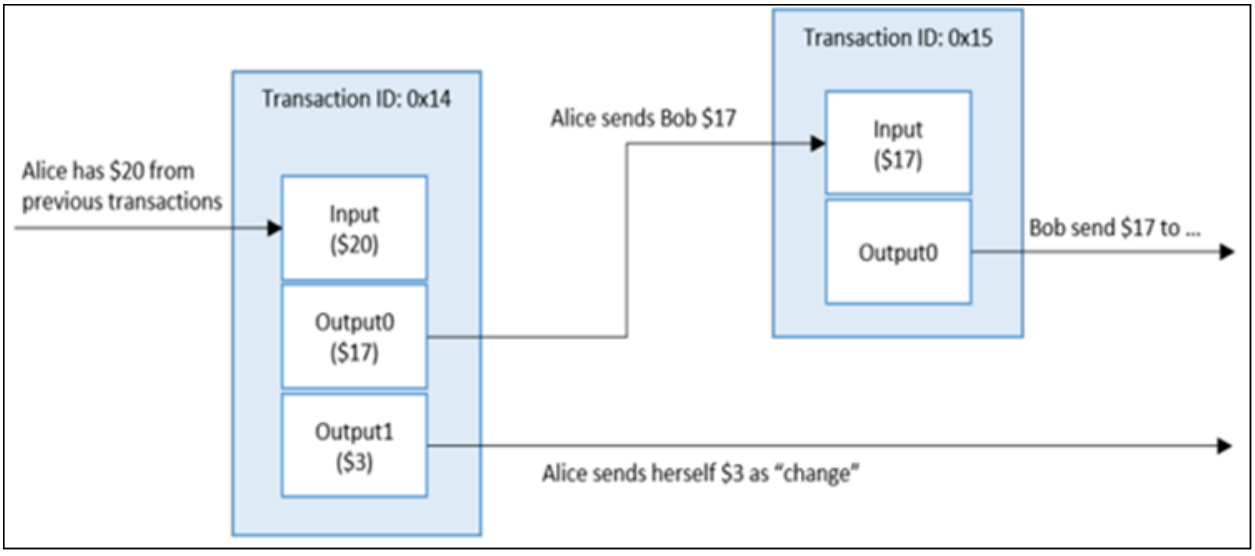


Fig 2 Example of Crypto Currency Transaction

- *In this, we talk about two Concepts, Input and Output:*

✓ *Inputs:*

Typically, transactions involve a list of digital assets slated for transfer. When conducting a transaction, there is a need to pinpoint the source of these digital assets, which is achieved by referencing either the preceding transaction where the sender acquired them or the current transaction. It's important to note that in the blockchain realm, once values are recorded, they become

immutable and cannot be altered. To validate their authority over the referenced inputs, the sender usually provides proof through digital signatures.

✓ *Outputs:*

Typically, the outputs represent the accounts set to receive digital assets and indicate the quantity of digital assets they will obtain. Each output explicitly states the number of digital assets to be conveyed to the new owner(s).

➢ *Asymmetric-Key Cryptography:*

Asymmetric-key cryptography uses a pair of keys: a public key and a private key that is related to each other. The public key is made public without reducing the security of the process, but the private key must remain secret. Even though there is a relationship between the two keys, the private key cannot efficiently be determined based on knowledge of the public key. These keys function in a manner that verifies the credibility and genuineness of transactions while also ensuring their visibility to the public. This is accomplished through a procedure referred to as "digital signing." Essentially, digital signing entails using a private key to encrypt a transaction, enabling anyone with the corresponding public key to decrypt it. The party initiating the transaction holds the essential private key for this encryption operation.

➢ *Addresses and Address Derivation:*

Certain blockchain networks employ an address, which is a concise and alphanumeric sequence of characters. This address is generated from the public key of a user within the blockchain network through the application of a cryptographic hash function. Most blockchain implementations make use of addresses as the “to” and “from” endpoints in a transaction. Addresses are shorter than the public keys and are not secret. One method to generate an address is to create a public key, apply a cryptographic hash function to it, and convert the hash to text. Addresses frequently serve as the outwardly visible identifier for a user within a blockchain network, and it's common practice to transform an address into a QR code.

➢ *Ledgers:*

A ledger is a collection of transactions. In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralized, trusted third party.

➢ *Blocks:*

Transactions are added to the blockchain when a publishing node publishes a block. A block contains a block header and block data. The block header contains metadata for this block. The block data contains a list of validated and authentic transactions that have been submitted to the blockchain network. Validity and authenticity are ensured by checking that the transaction is correctly formatted and that it has been cryptographically signed. Within the blockchain network, fellow full nodes engage in a meticulous review of all transactions within a published block, rejecting any block that contains transactions lacking validity. This practice is crucial for upholding the integrity of the timestamp.

- *Block Data:*

A list of transactions and ledger events is included within the block.

- *Private Key Storage*

In blockchain networks, the private key should be stored by the respective user. Private key storage is done with the use of software, which is also called a wallet. A wallet has the capability to retain private keys, public keys, and their corresponding addresses. It also carries out computations to determine the total amount of digital assets owned by the user. Security surrounding the private key is of paramount importance, which is why users often resort to specialized secure hardware for storage. This practice is facilitated by the emerging private key escrow services industry, which not only ensures security but also complies with KYC regulations by securely storing the private key.

➢ *Chaining Blocks:*

Blocks are interconnected by including the hash digest of the previous block's header within each block, thereby creating the structure known as the blockchain.

ISSN No:-2456-2165

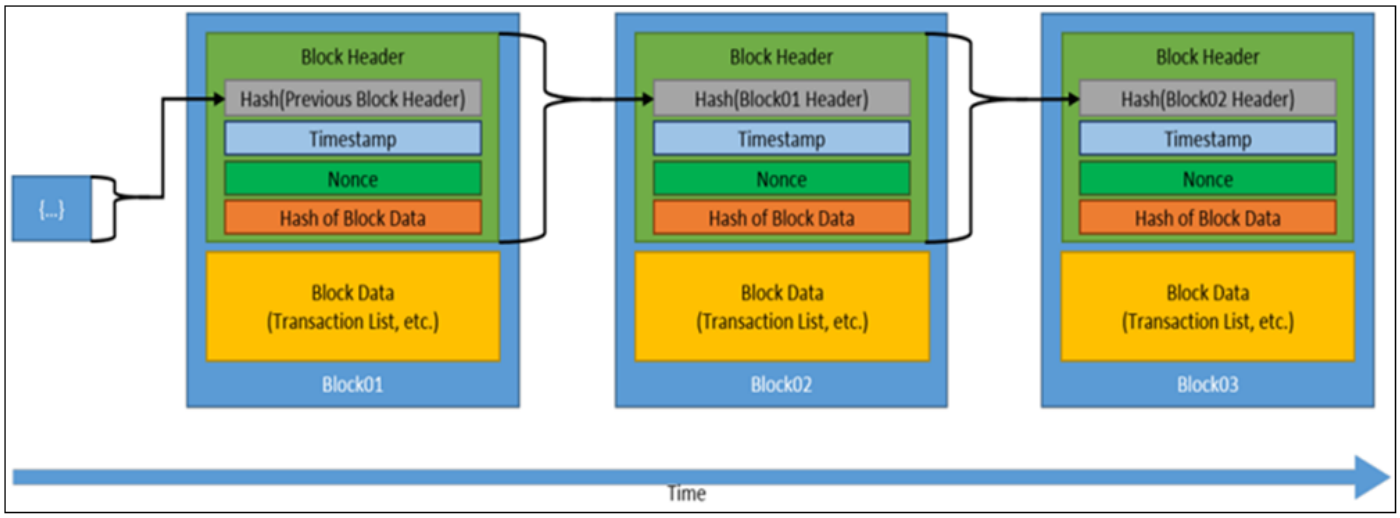


Fig 3 Standardized Sequence of Blocks

*B. Consensus Model*

A permissionless blockchain does not have to be restricted to a specific set of users based on its role; it is available in public for every user of the blockchain technology to view. In a permissionless blockchain network, numerous publishing nodes vie with both time and each other to simultaneously release the next block. It is done by the block miner in order to win direct cryptocurrency or transaction fees as a reward for adding the respective block to the blockchain.

Blockchain technologies employ consensus models to facilitate collaboration among a collective of users who may not trust each other. So while working together, there are various properties for publishing the block. Initially, the system establishes consensus on its initial state, which is referred to as the genesis block. Subsequently, users must collectively endorse the adoption of a consensus model for adding blocks to the system. Each block added through this consensus model is connected to the preceding block by incorporating the previous block's headers into the hash digest. However, the very first genesis block lacks any prior block headers, typically initialized as zero. This approach enables users to autonomously verify the integrity of each block.

➢ *Proof of Work:*

In a Proof-of-Work system, each node tasked with verifying transactions must engage in resource-intensive computations to demonstrate their validity as network participants. This process remains secure as long as the combined computational power of honest nodes surpasses that of potential attackers. A block is formed by combining a set of transactions with the hash of the preceding block and a nonce. A timestamp server then generates a hash for the block and publicly announces it, providing proof that the data within the block must have existed at the time of hashing. To maintain consistency, the timestamp server also verifies that the block's timestamp is greater than that of the previous block in the blockchain. These hashes are linked in a chain, which is called a blockchain. The important property of the blockchain is that the transactions can be traced back to any time in history.

In the proof-of-work system, a nonce within the block is continuously incremented until it produces a value with the required number of leading zero bits in the block's hash. If this hash is tampered with by a malicious attacker, it will render all subsequent blocks invalid hashes. The governing principle is that the longest chain, enjoying majority consensus in the network, is deemed the correct one. Therefore, for an attacker to alter a block, they must wield sufficient computational power to override the consensus established by the majority of honest nodes. Transactions within a block are structured and protected through the use of a Merkle tree. This tree structure resembles a binary tree and comprises numerous leaf nodes. The root of this tree is a hash that is derived from the hashes of its child nodes.

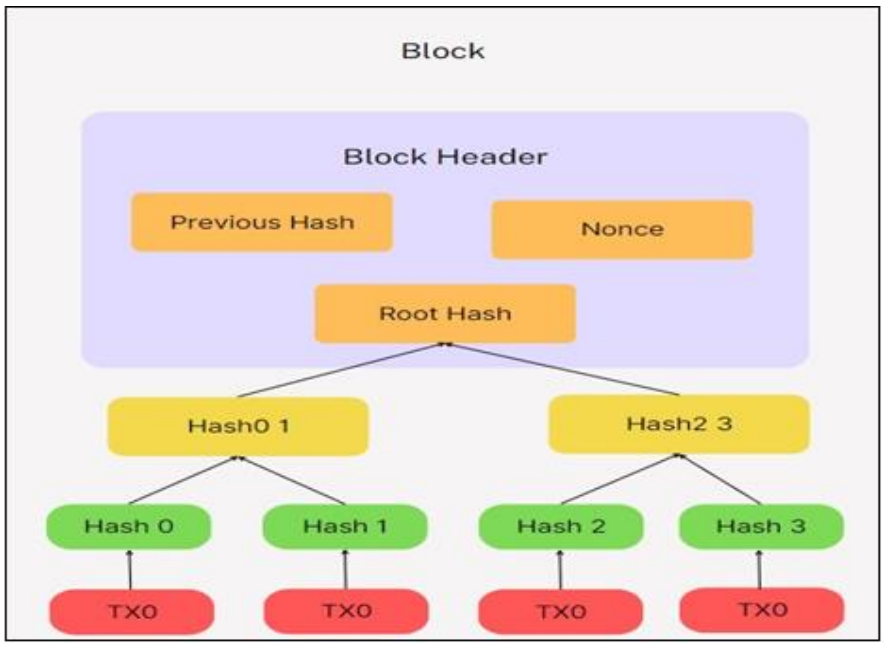

Fig 4 Bitcoin Block Transactions are Organized in a Merkle Tree Structure

➢ *Proof of Stack:*

The proof-of-stake model operates under the premise that users who invest a greater stake in the system are more inclined to actively support the system's success. A stack in this model is nothing but the amount of crypto currency that the blockchain network user has invested in the system. Proof of stake uses the amount of stake a user has as a determining factor for publishing new blocks, so there is no need to perform resource-intensive computations in this model compared to the proof of work model.

In this proof of stack, the crypto currency is already distributed among users rather than new crypto currency being generated at a constant pace, and the reward for block publication is just the earnings of the user provided by the transaction fees given for publishing the respective block. There are various methods to select stack users in blockchain.

First is the random selection of stack users; the user is selected based on their stack; if the user has a stack of, say, 42%, then the probability of selecting that user is considered 42%, so as the stack increases, the probability of being selected also increases.

The second is multi-round voting, also called Byzantine fault tolerance proof of stake. In this method, several stack users create proposed blocks, and all these proposed blocks are then voted on by the stack user, Via this method, all the stack users have a voice in addressing the block to be made public. This method is considered complex and time-consuming compared to the random selection of stack users.

The third is coin aging systems, also known as coin age proof-of-stacks. In this method, the staked cryptocurrency has an age property, and the staked crypto currency can count towards the owner being selected to publish the next block. The staked crypto currency then has its age reset, and it cannot be used again until after the requisite time has passed. This method allows users with a larger stack to publish more blocks without overpowering the system. Additionally, it incorporates a cooldown timer associated with each crypto currency coin used in block creation. Coins that are older and form larger groups enhance the likelihood of being selected for publication.

Next, there are delegate systems, where users cast votes to select nodes that will act as publishing nodes responsible for creating blocks on their behalf. The voting influence of nodes is directly linked to their stake, meaning that nodes with a larger stake hold more substantial voting power. This voting process for selecting publishing nodes is an ongoing affair, and the competition to maintain one's status as a publishing node can be intense. The constant risk of losing this status, along with the associated rewards and reputation, serves as a powerful incentive for publishing nodes to avoid engaging in malicious behavior.

➢ *Round Robin Consensus Model:*

Round Robin is a consensus model utilized by specific permissioned blockchain networks. Under this consensus mechanism, nodes take turns creating blocks, which can occasionally lead to the same node having multiple chances to publish blocks. To mitigate potential problems, these systems frequently include a time constraint, permitting active nodes to publish blocks and preventing inactive nodes from hindering block publication. This approach is designed to prevent any single node from dominating the creation of the majority of blocks. However, it's important to note that Round Robin is not well-suited for permissionless blockchain networks, which are the foundation of most crypto currencies. In these networks, malicious nodes could exploit the system by continually adding more nodes to increase their chances of publishing new blocks.

➢ *Proof of Elapsed Time Consensus Model:*

In the Proof of Elapsed Time (PoET) consensus model, every node vying to become a publisher requests a waiting duration from a secure hardware time source that is part of their computer system. This secure hardware time source generates a random waiting period and supplies it to the node's software. Subsequently, the node enters an inactive state for the predetermined duration. After emerging from this inactive state, the node proceeds to craft a new block and disseminate it to the blockchain network, alerting fellow nodes about the addition. Once a node has broadcasted its block, any other nodes still in idle mode will cease waiting, and the entire process repeats. Crucially, this model hinges on the use of genuinely random wait times. If the wait time were not randomly determined, a malicious publishing node could exploit the system by consistently opting for the shortest possible wait time, potentially disrupting the network's balance.

*C. Introduction to Ethereum in Blockchain:*

The foundation of contemporary cryptocurrency development centers around Ethereum and the incorporation of blockchain technology, with a particular emphasis on smart contracts. Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ethereum is open source and is used primarily to support the second-latest cryptocurrency in the world, known as Ether. Ethereum enables the smart contacts and applications built on its blockchain to run smoothly without fraud, downtime, control, or any third-party interference.

➢ *Bitcoin and Blockchain Technology:*

- *Bitcoin Essentials:*

Satoshi Nakamoto introduced a system proposal that revolves around a peer-to-peer distributed timestamp server. This server plays a crucial role in generating computational proof to establish the chronological order of transactions. In this framework, an electronic coin is essentially a sequence of digital signatures. Each transaction is structured as a collection of digitally signed hashes from previous transactions and the public key of the next recipient. The private key is employed for transaction signing, whereas the public key is utilized for transaction verification. These public keys are stored in wallets, which can be implemented using software, hardware, or online platforms. The Bitcoin ledger is characterized as a state transition system, encompassing a state that reflects the ownership status of all existing bitcoins.

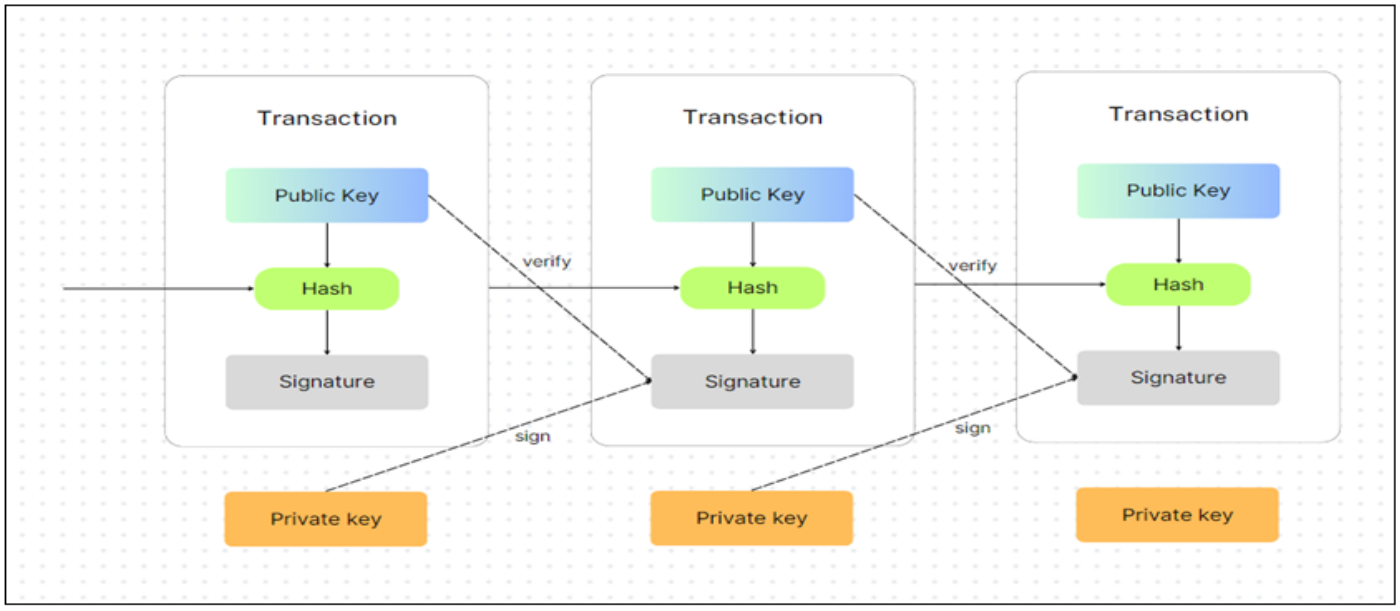


Fig 5 Transaction Structure in Bitcoin Block Chain

- *Bitcoin Transactions:*

Each transaction in the system is uniquely identified by its hash value, which serves as a transaction identifier and encompasses a set of inputs and outputs. It's essential to note that each output from a transaction can only be employed once as an input throughout the entire blockchain. Attempting to reference the same output more than once gives rise to the double-spending problem and is strictly prohibited within the network. Transactions consist of inputs and outputs, with each transaction potentially having multiple inputs and up to two outputs. The inclusion of multiple inputs allows for the consolidation of smaller coin amounts being transferred, while the outputs represent the amount sent to the recipient.

The Bitcoin distributed ledger meticulously records all transactions and ownership changes across the network. Every node within this peer-to-peer network maintains a copy of this ledger. When a user wishes to send coins to another party, they achieve this by publicly announcing the transaction.

- *Bitcoin Network and Mining:*

The inception of each block involves a primary transaction, referred to as a coin-based transaction, where a new coin is generated and owned by the creator of that block. This incentive encourages nodes to diligently verify transactions and inject new coins into circulation, as there isn't a central authority responsible for issuing them. The Bitcoin network aims to produce a block roughly every ten minutes and to maintain this pace despite increasing computational power, the system gradually elevates the difficulty of generating new blocks. Each node assembles transactions into a block and engages in the process of finding proof-of-work. Once successful, it broadcasts its completed block to the network, with acceptance contingent on the correctness of all enclosed transactions. If the network approves the block, the blockchain advances by generating the next block, appending the hash of the previously added block to it. Beyond the reward tied to creating a block, nodes are also rewarded with coins for verifying transactions. This process of adding new blocks and validating transactions is known as mining. The very first block within the blockchain is the genesis block, serving as the source of the initial 50 BTC (Block Reward) to initiate the network. However, considering the decentralized nature of distributed systems, there are instances where multiple nodes nearly simultaneously broadcast identical blocks but possibly with different transaction sets. This scenario, termed a fork, results in an inconsistent state within the network.

- *Bitcoin Scalability Problem:*

Bitcoin faces significant scalability problems due to its small 1MB block size. This means it can only handle less than seven transactions per second. In contrast, Visa, a popular payment network, managed to process a whopping 47,000 transactions per second during the 2013 holiday season and currently handles hundreds of millions of transactions daily. To match Visa's speed with Bitcoin's 1MB block size, would result in the creation of more than 400 terabytes of data every year.

- *Segwit and Lightning Segwit (Segregated Witness):*

This proposed solution aims to address the scalability challenge in Bitcoin while tackling the issue of transaction malleability. Transaction malleability arises because the transaction signature doesn't cover all the transaction data, making it possible for a malicious node to alter a transaction and invalidate its hash. Segregated Witness (SegWit) resolves this by allowing an increase in the block size, up to a maximum of 4MB, and introducing an additional layer on top of the existing network. It achieves this by separating the signature data from other transaction data, and it paves the way for the Lightning Network, a second-layer protocol hailed as the next significant advancement in the Bitcoin network. The Lightning network is designed to facilitate micropayments through a network of micropayment channels. These channels represent an agreement between two parties to delay broadcasting the transaction to the network while still executing the transaction.

➢ *Ethereum:*

To address the limitations inherent in Bitcoin, Ethereum was introduced, offering solutions to several shortcomings in Bitcoin's scripting language. Its primary breakthrough lies in its full Turing completeness, granting Ethereum the capability to support all types of computations, including loops. Ethereum also improves the blockchain structure by introducing features like transaction state tracking. Ethereum essentially serves as a blockchain with an integrated Turing-complete programming language. This framework provides an abstract layer that empowers individuals to establish their own rules for ownership, transaction formats, and state transition functions. These rules are encoded in smart contracts, which are cryptographic instructions executed only under specific conditions. Ethereum's consensus mechanism relies on a modified GHOST protocol (Greedy Heaviest Observed Subtree) designed to tackle the issue of stale blocks in the network. Stale blocks, which do not become part of the Bitcoin blockchain because they are preceded by orphan blocks, deprive miners of rewards. The GHOST protocol addresses this by awarding block rewards to stale blocks, with the stale block receiving 87.5% of the reward, and the nephew (a related block) of the stale block getting the remaining 12.5%. This ensures that miners still receive compensation, even if their blocks do not make it into the main blockchain.

➢ *Ethereum Transactions and Messages:*

A transaction is a solitary instruction that is securely signed using cryptographic techniques. Transactions in the context of cryptocurrency can be categorized into two types based on their outcomes: those that trigger message calls and those that establish new accounts. Each transaction can be described as a digitally signed data package originating from an externally owned account. These transactions contain essential components, including the recipient of the message, a sender's signature for identification, the specified amount of Ether to be transferred, an optional data field, as well as STARTGAS and GAS-PRICE values. The STARTGAS and GAS-PRICE fields play a pivotal role in safeguarding the network against potential attackers. "Gas" serves as the fundamental unit of computation within the system. Every transaction necessitates a specific amount of computational work, and the STARTGAS field signifies the maximum number of computational steps that the transaction is permitted to consume. Typically, the price is set at 1 gas for every computational step, with an additional fixed charge of 5 gas for each byte in the data area. However, the GASPRICE field allows for variations in this value, which can be higher depending on user preferences. Miners are incentivized to process transactions with higher GAS-PRICE values because they receive greater rewards for doing so. This mechanism encourages efficient use of computational resources and ensures that miners prioritize transactions based on the fees offered by users. The Ethereum state transition function, which changes the states of the sender and the recipient by executing a transaction, starts with verifying the correctness of the transaction. If this is correct, then it calculates the transaction fee as STARTGAS * GAS-PRICE subtracts this value from the sender's account balance, and increments his nonce. If this is correct, the

fee is paid and the requested amount is transferred to the recipient. The receiving account is created if it doesn't already exist, and if it is a contract, then the contract's code is executed. One contract can send a message to another in the Ethereum network. The message is akin to a transaction but is generated by a contract. Much like standard transactions, this message initiates the recipient account to execute its linked code.

- *ERC20 Token:*

Ethereum serves as an ideal platform for creating tokens, and these tokens are typically implemented as smart contracts following the ERC20 Token Standard. These tokens have the flexibility to represent a wide range of assets or digital assets on the Ethereum network. The ERC20 standard outlines a specific contract structure that must be adhered to, encompassing six functions and two events that collectively provide a comprehensive description of an account's behavior and properties.

```
contract ERC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint
balance);
    function allowance(address tokenOwner, address spender) public constant
returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool
success);
    function transferFrom(address from, address to, uint tokens) public returns
(bool success);
    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender,
uint tokens);
}
```

Fig 6 ERC20 Token

➢ *Ethereum Blockchain:*

An Ethereum blockchain exhibits similarities to the Bitcoin blockchain, but a significant difference lies in the content of Ethereum blocks. Ethereum blocks include essential elements such as block number, difficulty, and nonce, but they also contain a list of transactions and the most up-to-date state. Each transaction in this list contributes to the creation of a fresh state by implementing alterations to the preceding state. The Ethereum blockchain's header includes the mining fee recipient's address, hashes of state, transaction, and receipt tries, the difficulty level, the block's current gas limit, a total gas usage count for the block's transactions, a timestamp, a nonce, and extra hashes for verification purposes. Ethereum employs Ethash as its memory-intensive proof-of-work algorithm, a modification of the Dagger-Hashimoto algorithm. Every node within the Ethereum network operates under an Ethereum virtual machine (EVM) and executes its instructions. Solidity is one of the most widely used programming languages for crafting smart contracts. Ethereum's block time typically hovers around 15 seconds, occasionally reaching up to 30 seconds during peak periods. Despite concerns about scalability, Ethereum has demonstrated its capacity by successfully handling over one million unique transactions within a 24-hour window, averaging around 11 transactions per second, when using the Geth blockchain client with fast sync. Ethereum finds diverse applications, including token systems, financial derivatives, identity and reputation systems, file storage, insurance, cloud computing, and prediction markets. However, its primary use case revolves around decentralized applications (DApps). DApps are digital applications or programs that operate on a blockchain or a peer-to-peer network of computers rather than a single centralized computer. Some notable examples of DApps include Golem (supercomputing), Augur (prediction markets), Civic (identity verification and protection), OmiseGO (public blockchain-based exchanges), and Storj (renting hard drive space).

*D. Securing a Biometric Authentication System using Blockchain:*

Security weaknesses are prevalent in biometric authentication systems, with notable concerns such as the potential for biometric data exposure, the questionable reliability of authentication modules, and the absence of transparency in the management of biometric information. We will explore BDAS, a novel biometric authentication system that leverages blockchain technology to address these issues.BDAS presents a decentralized and distributed method for performing biometric authentication while delivering an accountable system for managing biometric data. BDAS, which stands for the Blockchain-based Distributed Biometric Authentication System, incorporates blockchain technology to enhance the secure management of biometric data.It achieves this by partitioning each biometric template into fragments and storing them separately across the blockchain for various clients. BDAS guarantees dependable authentication by harnessing the decentralized characteristics of blockchain, enabling all network clients to conduct transactions independently, free from dependence on a central authority. Moreover, BDAS meticulously records each transaction on the blockchain, complete with timestamps, establishing a permanent record of all authentication activities. This heightened transparency and traceability significantly bolster the system's security. Importantly,

BDAS provides reliable authentication in comparison to current methods, all while introducing minimal performance impact in real-world situations.

➢ *Biometric Authentication:*
Conventional biometric systems consist of four modules:

- A sensor collects the Biometric Data.
- A feature extractor analyzes the biometric data to identify specific characteristics and generates a biometric template.
- The administrator manages the enrolled templates
- The Authenticator identifies the similarity between the input and enrolled templates.

- *With these Modules, Biometric Authentication Operates in Two Steps:*

✓ *Enrolment:*
A user registers their biometric data using a sensor. This information is then transformed into a predefined format known as a template, which is subsequently stored by the administrator.

✓ *Authentication:*
A user attempts to authenticate by providing her biometric information via a sensor, and then the information is compared with the enrolled templates.

➢ *A Brief History of the BDAS Working*
BDAS, an innovative biometric authentication system leveraging blockchain technology, introduces a decentralized and distributed method for biometric authentication, eliminating the need for reliance on a central authentication module. Within BDAS, every client autonomously handles template fragments and carries out authentication operations without depending on any particular central entity. This decentralized methodology guarantees robust authentication by reducing the potential for single-point failures. To enhance the security of biometric information, each template is divided into fragments, with different clients responsible for managing these segments. This segmentation strategy minimizes the potential exposure of the entire template. BDAS carries out its core functions, including template management and authentication recording, through the utilization of a smart contract embedded in the blockchain. It's important to highlight that BDAS necessitates a minimum of three clients, each of which operates a blockchain node, to ensure secure distributed information management. BDAS is designed as a permissioned blockchain, allowing only verified nodes to participate. Using the smart contract, a client identifies the designated clients responsible for overseeing the necessary fragments. Every authentication operation within the BDAS system is systematically recorded as a transaction on the blockchain network, ensuring a high degree of transparency and traceability.

- *BDAS's Enrollment Process Operates in the following order:*

✓ Request enrolment: A client acquires a user's biometric data using a sensor, extracts relevant features, and then creates a template.
✓ Split Template: Each template undergoes division into three fragments, and the specific types of fragments are determined based on their respective timestamps.
✓ Identify Nodes: A client identifies the nodes linked to its associated node.
✓ Select Clients: In BDAS, when there are n clients, the number of stored copies for each template's fragments is [n/3], and a total of [3 * (n/3)] clients are selected at random. For instance, if there are eight clients, each fragment will have two copies and six different clients will be randomly chosen to oversee them.
✓ Store Templates: The designated template fragment(s) are placed in storage on the selected clients.

- *BDAS's Authentication Operates in the following order:*

✓ Request Authentication: A client collects a user's biometric data using a sensor and then initiates an authentication request.
✓ Run Contract: A client executes a smart contract to determine the locations of the necessary template fragments.
✓ Return Information: The client receives information regarding the locations of the fragments.
✓ Request Templates: The client requests and obtains the relevant fragments through separate client communications.
✓ Compare Templates: A client combines the fragments to form a complete template and then compares it with the requested information.

*E. Traceability*
Traceability, often referred to as the "one step back, one step forward" principle, represents the capacity to retrieve comprehensive details concerning the origin of a food product. It encompasses the ability to track the journey of a feed or food item through specific phases of production, processing, and distribution. Traceability encompasses a wealth of information,

including data about food ingredients, their sources, the production process, transportation, and storage conditions. This information comprises both quantitative and qualitative aspects related to the final food product and its provenance.

➢ *Level of Traceability*

Traceability operates on two distinct levels: the intra-company level, or internal level, where a single entity, such as a company or organization, traces the origins of a product's ingredients and packaging, and the supply chain level, also known as the external level, which encompasses both intra-company processes and a reconstructive process that traces the complete history of a specific product.

Voluntary traceability pertains to the freedom of choice granted to every participant within the supply chain regarding the data they opt to collect. One of the primary challenges in voluntary systems is their inherent complexity, as each participant may employ their own set of standards and methods for tracking and tracing products, resulting in a wide array of collected data.

➢ *Agriculture Traceability Tools and Technology Solutions*

The swift advancement of IoT (Internet of Things) and sensor technology has greatly facilitated the process of data collection, providing efficient and dependable methods. Among these methods, barcodes, QR codes, RFID (Radio-Frequency Identification), and wireless sensor networks (WSNs) stand out as the most prevalent and widely recognized technologies within supply chains.

- RFID supply chain provides safe information and data management system by tracing and monitoring.
- Supply chains integrated with WSNs encompass wireless sensors and actuators, including devices like humidity sensors and temperature sensors. These devices collect data, which is subsequently processed and transmitted to higher-level systems to facilitate decision support.

➢ *Ethereum*

The Ethereum protocol specifies that every participant within the network is interconnected ; according to the author, there are three levels of decentralisation logical decentralization, political decentralization, and architectural decentralization.

Ethereum is especially used to support smart contracts. The primary vision behind smart contracts was to establish a decentralized ledger for contract storage. Smart contracts prove highly beneficial for facilitating transactions among farmers, suppliers, and distributors. Essentially, smart contracts resemble real-world contracts but with the distinctive feature of being entirely digital. They are essentially small script programs housed on the blockchain, characterized by tamper-proof logic code. The key characteristics of smart contracts lie in their immutability and distribution, as they are securely stored within the blockchain network. Blockchain is used for storing smart contracts because, during distribution, smart contracts secure a validation certificate, so tampering with the code of the contract is not possible.

In a blockchain, when a block (or transaction) is scanned and sourced in a completely digitized way, the specific transaction is confirmed and the block is appended to the chain. After the execution of the contract, a certificate is issued and the client receives the smart contract as follows:

- *History of all Smart Contracts*
- *History of all Transactions*
- *The Current State of all Smart Contracts*

*F. Tokens*

The blockchain serves as an immutable and decentralized public repository for recording land titles and property rights, effectively managing ownership. Managing the property and even performing peer-to-peer transactions have been made possible with the DLT system.

A token, a blockchain-based record representing property rights, is a unit of account that is connected to the user's address, which showcases exclusive control over the given address enabled by the user’s private key.

A token is mapped with cadastral data and property rights such as leases, mortgages, superficies, etc. The linkage between real estate and property rights with the title record is established by entities possessing the authorization to validate ownership, deeds, and other property rights transactions.

Smart contracts are the driving mechanism for managing ownership. Blockchain transactions are valid similarly to legal deeds. Blockchain transactions produce token records, starting from the creation of the token to its various transfers and deactivating the token .

Tokens resemble digital versions of titles. Title tokens serve as the foundation for various derivative tokens, which, while not titles themselves, are intricately linked to them and establish diverse economic property relationships.

Tokenizing land titles and property rights involves an initial interaction with land authorities, followed by anchoring the title to the blockchain. This process eliminates the necessity for registering each transaction individually.

A cross-blockchain protocol is employed to handle legal matters through a framework known as "smart laws." These smart laws are specifically crafted to tackle various issues, including inheritance, dispute resolution, token access restoration in case of lost keys, and other enforcement-related matters that involve multiple trusted third parties. The cross-blockchain protocol allows for the utilization of multiple blockchains within a bundled framework. As a result, users have the flexibility to choose which blockchain they prefer to manage their property rights. The security standards mandated by the government ensure the reliability of the cross-blockchain database. Blockchains that adhere to the criteria of immutability and decentralization in maintaining a public ledger can be part of the property registry bundle.

➢ *Legal Side of Tokens:*

Tokens serve as a means of facilitating ownership and property management via peer-to-peer transactions. This information is encoded within the blockchain.

- The The title is associated with the address, followed by the registration process for the title.
- The title is an outcome of a transaction, representing a subsequent transaction that references and inherits the preceding one. Consequently, a chain of deeds is also accessible.

Blockchain can fit both conventional systems of keeping records in a public registry as a chain of deeds and maintaining the registry of title records for the title and its current owner.

➢ *Converting a Token to a Title*

A title is considered evidence of ownership, it is mostly a combination of various legal documents and legal acts, such as:

- *Certificate of Ownership,*
- *A Title Deed*
- *Court Decision.*
- *Evidence of Ownership*

The title is used to represent the property as it contains the cadastral number for identification, and a title can always point to the object of ownership in one document.

Through the process of data insertion, a token becomes a record that has legal meaning and is hence considered an economically valuable asset.

- *There are two ways to Legitimize any Immovable Property and assign rights and obligations:*

✓ *By Declaration and Agreement of Private Parties.*
✓ *By Public Acknowledgment.*

The title rights and token work together, during the sale of the token, ownership gets transferred to the relevant token and the buyer accepts the token and gets declared the new owner, This procedure may also incorporate a trusted third party, like the government, to validate whether the token accurately represents the associated property.

Presently, the proprietor initiates a record in which they assert their title, while the governing body generates a separate record to authenticate the owner's rights. Consequently, in the event of the owner losing their private key, they have the option to request the authority to amend their record. This update serves to determine the token's status, which would otherwise be rendered invalid, and includes certification as well as a link to a newly issued title record, effectively reinstating ownership.

The title owner possesses complete authority over the token, allowing them to engage in peer-to-peer transactions. In contrast, the government, having control over its own token, is responsible for regulating relationships in accordance with legal requirements. In the event of any disputes, the land authority will enforce a court decision, which will be documented, and such records are irreversible.

ISSN No:-2456-2165

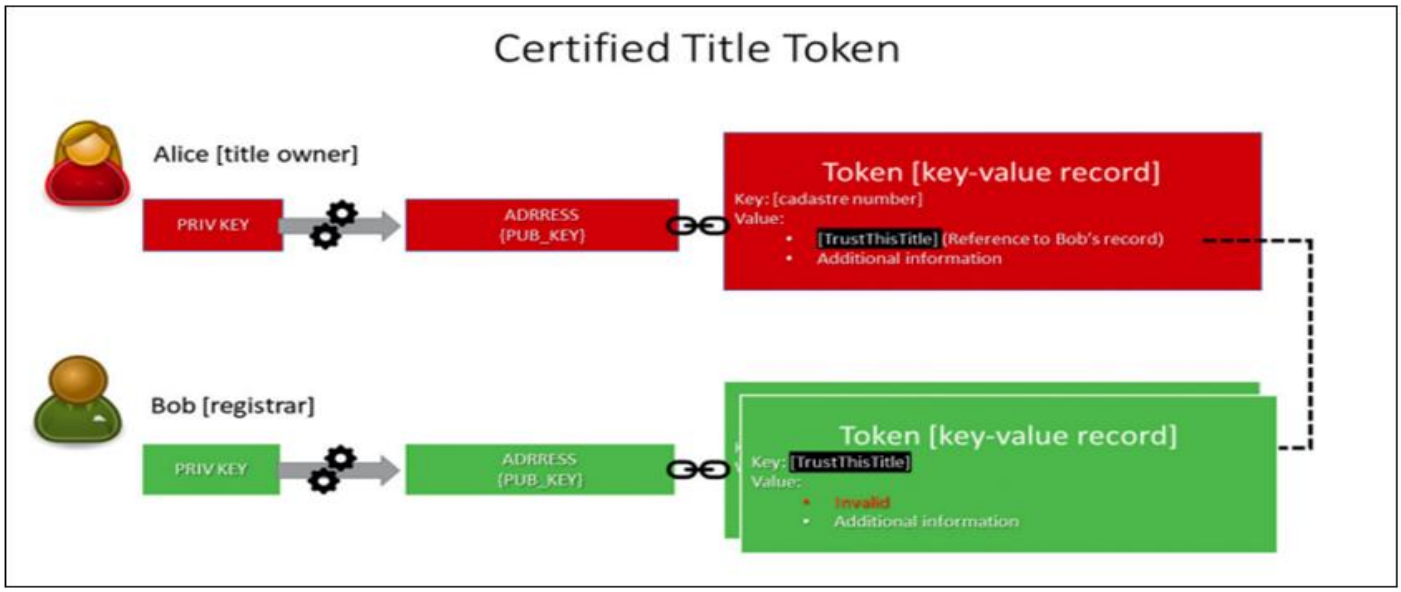


Fig 7 A title token, endorsed by a registrar's token, is established. Alice generates a token in which the primary identifier is the cadastral number (an exclusive key), and the content consists of a link to Bob's token. Subsequently, Bob produces a token using the same key referenced by Alice, and within this token, he inserts information about the status of Alice's token, marking it as 'valid' in the 'Value' field.

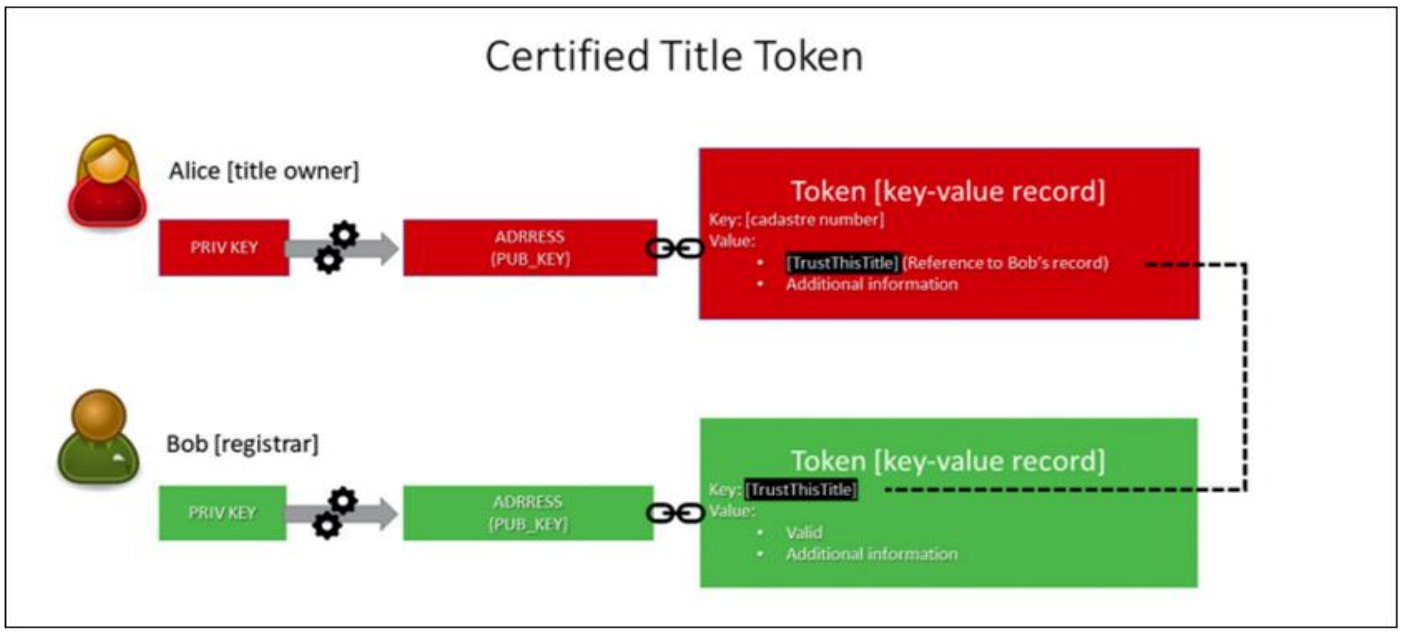


Fig 8 Invalidation of the Title Token: Bob modifies his token by adding a fresh 'invalid' status to the 'Value' field. This revised entry from Bob functions as an authentication for Alice's token

➢ *Authorization*

The owner possesses complete autonomy over the token, with only the private key required to conduct a transaction. Nevertheless, the owner's actions undergo multiple verifications by the authorities. The Title token transaction is endorsed by multiple governing bodies.

- Notary acts can take a basic form, including traditional paper documents. In such cases, the notary issues a token confirming the completion of the act, and this token includes metadata detailing the act itself.
- The survey report could be recorded on the blockchain or provided as a hyperlink to a file hosted on a remote server, which may have either public or restricted access.
- Building permits, much like surveys, can be either published on the blockchain or stored on an external server maintained by a third party.

ISSN No:-2456-2165

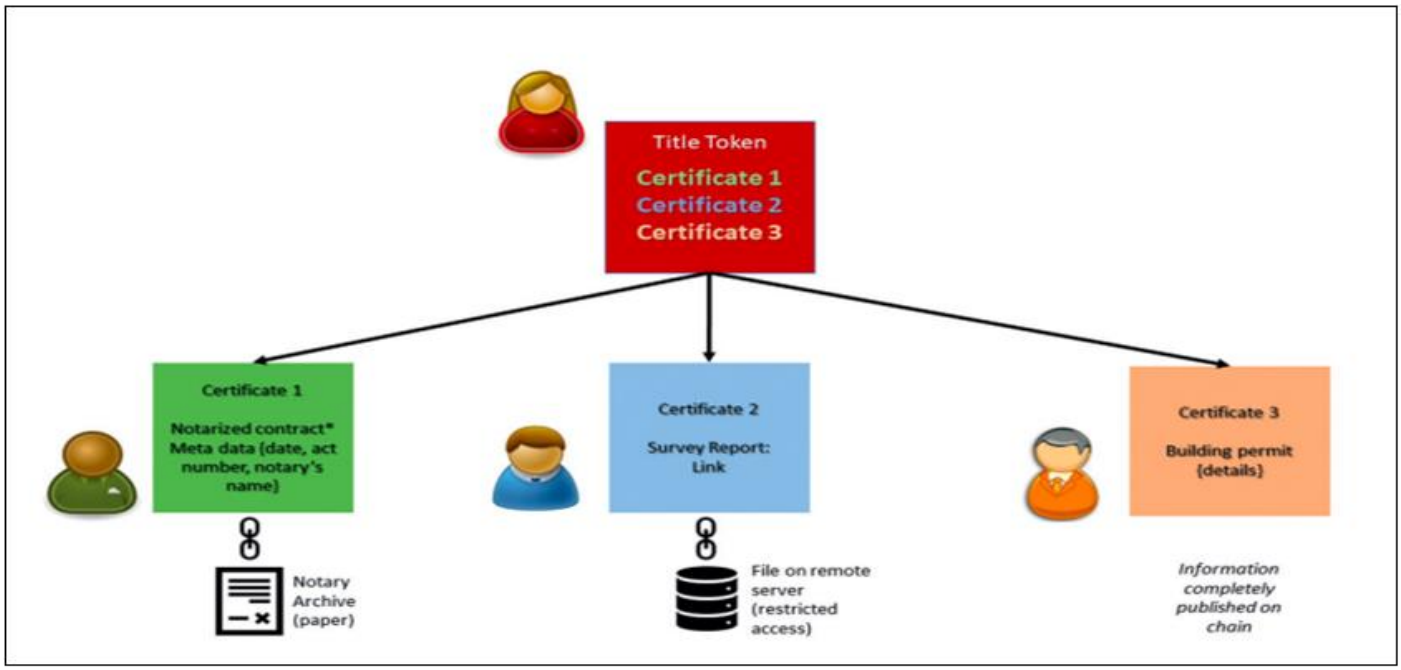


Fig 9 Transactions involving Title Tokens with Authorization from Multiple Entities: Notarial procedures can take a basic form, often documented on paper. Consequently, the notary issues a token confirming the completion of the action, which includes metadata pertaining to the act. Survey reports can either be directly recorded on the blockchain or linked through anchoring and/or hashing to a file on a remote server, with accessibility options ranging from public to restricted. Likewise, building permits, much like survey reports, can either find their place on the blockchain or be stored on an external server.

ISSN No:-2456-2165

# CHAPTER FOUR
# CONCLUSION

In summary, blockchain technology has rapidly evolved since its inception, offering secure and decentralized solutions for various applications. It began with Bitcoin and has grown to encompass a multitude of cryptocurrencies and innovative use cases. The foundation of blockchain technology lies in its cryptographic principles, which ensure the security and immutability of transactions recorded on a global ledger. While the technology is still relatively young, it has generated significant interest, although it is likely that the initial hype will subside, leaving blockchain as a valuable tool for specific scenarios. Blockchain's strength is in its ability to leverage existing technologies in novel ways, allowing organizations to weigh the advantages and disadvantages before implementation. The challenge of immutability, while beneficial in some cases, can also pose obstacles to adoption.

Bitcoin and Ethereum stand as prominent examples of blockchain's potential to establish trust in peer-to-peer networks. However, the landscape has expanded with numerous cryptocurrencies, each addressing specific needs. Blockchain's immutable public repository, governed by decentralized interactions, has opened the door to tokenization and smart contracts. These features enable ownership, record-keeping, and the creation of a repository of evidence for various property rights and legal matters. Trusted third parties play a vital role in certifying legal facts and ensuring enforceability in blockchain-based systems. The concept of referenced tokens, governed by smart laws, enhances the reliability of blockchain-based property registries. Governments must take a leading role in blockchain reform, ensuring citizens have the option to choose between traditional property rights protection and blockchain-based systems. Cross-blockchain infrastructure and security standards will promote competition and drive technological advancements.

In conclusion, blockchain technology offers significant promise, but it should be implemented judiciously in appropriate contexts. Its evolution has led to diverse applications beyond cryptocurrencies. Ongoing research should focus on addressing challenges, scalability, and expanding the use of blockchain technology in various domains, accompanied by objective evaluations of proposed solutions. As blockchain continues to mature, it has the potential to revolutionize industries while upholding principles of security, privacy, and transparency.

## REFERENCES

[1]. Blockchain Technology Overview by Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone
[2]. Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview by Dejan Vujicic
[3]. Securing biometric authentication system using blockchain by Youn Kyu Lee & Jongwook
[4]. Blockchain in Agriculture Traceability Systems: A Review by Konstantinos Demestichas
[5]. General Concept of Real Estate Tokenization on Blockchain by Oleksii Konashevych
[6]. Youn Kyu Lee, Jongwook Jeong. "Securing biometric authentication system using blockchain", ICT Express, 2021.
[7]. https://www.mdpi.com
[8]. https://www.degruyter.com
[9]. https://www.researchgate.net
[10]. https://doaj.org
[11]. https://portal.dnb.de/opac.htm
[12]. https://www.mdpi.com/
[13]. https://www.slideshare.net/
[14]. 14 .http://archives.univ-biskra.dz/handle/123456789/2471
[15]. https://www.igi-global.com/
[16]. https://owasp.org/
[17]. https://www.grin.com/de/
[18]. https://medium.com/
[19]. https://csrc.nist.gov/
[20]. https://www.ugc.gov.in/
[21]. https://vdoc.pub/
[22]. Blockchain Application in IOT Ecosystem Springer Science and Business Media LLC, 2021
[23]. Younis A. Younis, Abdulsalam Sami, Salma Naje. "Blockchain and Cryptocurrencies in Libya: a Study ", The 7th International Conference on Engineering & MIS 2021, 2021
[24]. Dejan Vujicic, Dijana Jagodic, Sinisa Randic "Blockchain technology, bitcoin, and Ethereum: A brief overview", 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), 2018.
[25]. https://encyclopedia.pub/entry/24357
[26]. https://sdlccorp.com/post/blockchain-technology-complete-guide/
[27]. https://dev.to/manyorock/cryptographic-hash-function-and-the-blockchain-56de
[28]. https://dev.to/manyorock/cryptographic-hash-function-and-the-blockchain-56de
[29]. https://nirolution.com/proof-of-work-vs-proof-of-stake/
[30]. https://www.investopedia.com/terms/b/blockchain.asp
[31]. https://docs.venom.foundation/learn/consensus/
[32]. https://blog.logrocket.com/permissioned-vs-permissionless-blockchains-dapps/
[33]. https://builtin.com/blockchain
[34]. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain
[35]. https://dev.to/yuryoparin/smart-contracts-in-10-minutes-risks-nfts-storage-options-4865
[36]. https://www.coolearth.com/traceability-and-woke-product-choices/