Vehicle Register Management System Using Blockchain

Saba Khanum[#], Himanshu, Ujjwal, Mayank
Department of Information & Technology,
Maharaja Surajmal Institute of Technology
[#] Corresponding Author, Email: *saba@msit.in*

***Abstract*— Blockchain provides a transparent record to the entire business network, allowing buyers and sellers of each vehicle to track where the vehicle is in its lifecycle. The platform benefits many stakeholders, including car manufacturers, dealers, regulators, insurance companies, buyers, sellers, and even garages, providing transparency and trust in vehicle transactions, preventing disputes and lowering the cost of services. It tracks ownership, sale, and accident history to create smart, more efficient systems for supply chains. This ensures availability of consistent data across various departments and also solves the obsolete data problem. The research paper shed light on role of blockchain in enhancing the experience of vehicle registration system. It will positively influence both the local and regional car markets, and the car manufacturing industry as a whole.**

***Keywords*— Blockchain, security, vehicle registration, Smart contract**

1. INTRODUCTION

The Motor vehicle agencies need to collaborate with external organizations like the Departments of Justice and Insurance to register vehicles. Maintaining the most updated information is essential to enable these organizations to register and track vehicles accurately. It is a time taking process where multiple parties are involved and also poses a risk of information manipulation, data duplication and various errors. In such a scenario, critical information can get highly vulnerable to frauds and data tampering or even become non-traceable. By bringing Blockchain into the picture and moving the entire vehicle registration process on to Blockchain, a lot of these issues can easily be taken care of. Blockchain comes to the rescue by reducing the average turnaround time [1]. Blockchain will enable parties to push data as a smart contract that eventually becomes a single source of immutable data to all parties. Not only this, Blockchain in vehicle registration ecosystem, will help reduce the risk of frauds and attacks, as data updates are only possible by authorized personnel using a private key. In fact, any tampering of data can also be easily tracked on Blockchain. The best part is, Blockchain will provide a single and easy view of the vehicle lifecycle which is not available today.

2. LITERATURE SURVEY

Blockchain's promise is the decentralization of trust, enabling value flow without intermediaries. It allows financial transactions to be verified and cleared without the need for a trusted third party sitting between market participants, removing requirements of market participants, intermediaries reduce costs and complexity.

The distributed ledger approach means that the members of a financial market (the network) share an identical system of record, rather than each maintaining their own proprietary view of it. This replicated, shared ledger provides consensus, provenance, immutability and finality for the transactions concerned payments, asset transfers, etc. This shared approach removes the need for reconciliations. New transactions are only accepted for posting to the distributed ledger (through the creation of new blocks for the chain) once all the computers in the network achieve consensus as to their validity. The verification of transactions by all network users reduces error rates and queries. At the heart of blockchain is a new type of distributed database. This provides for the exchange of

information in a synchronous and even manner, as well as allows it to be updated constantly, providing near-instant clearing and settlement. The provision of faster settlement means less risk in the financial system and so reduces the capital.

The new distributed database functionality also allows code to run with the blockchain to modify data (both on and off the chain) automatically. This enables the blockchain to support self-enforcing or smart contracts, allowing the automation of a variety of business functions. The blockchain's security and privacy protocols are based on the use of a cryptographic hash function each block (of transactions) in the chain is identified by its own hash key. This approach was developed to prevent the double spending of Bitcoins. The complexity of the crypto hash function reduces the blockchain's susceptibility to fraud [2].

Blockchains may be either: - Public or private, meaning they can be open to everyone or restricted to a defined group of users (e.g., institutions) - Permissioned or permission-less, meaning that either anyone can offer their services to add blocks to the chain or only a restricted group of users can do so - Bitcoin functions on a public, permission-less model and hence experiences performance issues with new blocks taking a long time to be added to the chain. Most blockchain use cases for other financial applications are based on the private, permissioned model which is less prone to performance issues, as the number of users can be controlled.

2.1 Origin Blockchain

Blockchain was first proposed in 2008 by Satoshi Nakamoto. Blockchain is essentially a public- ledger, in which all transactions are stored in a chain of data packages (blocks) and distributed across a peer-to-peer network. All involved nodes in the network hold a copy of the blocks. Every transaction or digital event in the public ledger has to be validated using a consensus mechanism by the majority of those participating nodes in the network. If agreed, then the transaction is recorded in a new block. A timestamp is applied to the new block along with a hash pointer as a link to the previous block and a nonce, which is a random number for verifying the hash. After that, the new block is added to the previous chain of blocks and distributed across the network. In this way, blockchain provides a secure, decentralized, persistent, fault-tolerant and auditable transaction platform which allows a transaction to take place in a decentralized fashion without the need of a central intermediary [3]. In general, blockchain has the following key characteristics:

2.1.1 Decentralization

Unlike a traditional transaction which is validated through a central trusted agency, every node in the network can validate transactions and has an identical copy of the ledger. This mechanism causes transactions in a blockchain to have advantages in fault tolerance, data consistency, higher user control, attack resistance, transparency and it also enables the removal of third-party intermediaries, such as a notary or financial institution.

2.1.2 Persistency

The use of a consensus mechanism, a time-stamp, and a cryptographic seal mean that invalid transactions will not be admitted and it becomes impossible to edit, delete or copy transactions that are already recorded in the blockchain. These blockchain features provide for data consistency, fraud protection, ownership assurance and immutable records of the transactions

2.1.3 Anonymity Interactions based on blockchain technologies take place between two individuals using public-key cryptography, by which their identities are covered by pseudonyms. In this way, user privacy will be better protected than in classic electronic transactions.

2.1.4 Auditability All transactions in a blockchain are stored in a chronological order, including the previous block's hash and storage of the hash of the current transaction which is meant to connect the next block when added. With this mechanism, transactions can be easily verified and tracked [4].

3. DESIGNS AND IMPLEMENTATION

3.1. Complexity

Blockchain technology involves an entirely new vocabulary. It has made cryptography more mainstream, but the highly specialized industry is chock-full of jargon. Thankfully, there are several efforts at providing glossaries and indexes that are thorough and easy to understand.

3.2. Transaction Speed and Cost

Bitcoin currently has notable transaction costs after being touted as 'near free' for the first few years of its existence. As of late 2016, it can only process about seven transactions per second and each transaction costs about $0.20 and can only store 80 bytes of data.

There's also the politically charged aspect of using the bitcoin blockchain, not for transactions, but as a store of information. This is the question of "bloating' and is often frowned upon because it forces miners to perpetually reprocess and rerecord the information.

4. METHODOLOGY

4.1. Blockchain

A blockchain, originally block chain, is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash). By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks.

Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. This allows the participants to verify and audit transactions inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Blocks hold batches of valid transactions that are hashed and encoded into a

Merkle tree: Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block [5].

4.2. React-JS

React makes it painless to create interactive UIs. Design simple views for each state in your application and React will efficiently update and render just the right components when your data changes. React is an open source JavaScript library which is declarative, efficient, and flexible. It is maintained by top IT firms like Facebook. ReactJS mainly works on the aspect of MVC

(Model View Controller). It is used for building User interface. Web developers have to crate components in react from which they can use it and build a performance-oriented application.

React components plays a very important role in web development. If a web developer is using reactjs in their project they need to create component in react and then use it. React components use the render method to for data input and output. React offers all the flexibility which can be expected from an open source java-script library. A React element is a plain object describing a component instance or DOM node and its desired properties. Instances only contain information about component type, their properties and any child elements in it. The element is a mode of communication which tells react that what the user wants to see on the screen. It is an immutable description object with two fields – type: (string ReactClass) and props: Object. A DOM node is represented by type of elements in a string with particular name and properties that define the attributes. DOM elements are very light because they are just objects on ReactJS and they don't have to be parsed. Elements can be nested as parent and child when creating as an element tree, but it is not actual instances but descriptions. ReactJS is the one-way data flow which begins with properties. Flux is recommended as application architecture for React. Flux is a kind of data flow programming style. Properties cannot be directly modified by the component but have to be passed as callback functions to modify values. This way, properties flow down and action flows up. ReactJS is the dynamic element in web application development as it provides extensive support for apps that require constant data update. React does not attempt to provide a complete 'application framework'. It is designed specifically for building user interfaces and therefore does not include many of the tools some developers might consider necessary to build an application. This allows the choice of whichever libraries the developer prefers to accomplish tasks such as performing network access or local data storage. Common patterns of usage have emerged as the library matures. To support Reacts concept of unidirectional data flow (which might be contrasted with Angular's bidirectional flow), the Flux architecture represents an alternative to the popular model-view-controller architecture.

4.3 Node JS

Node.js is a JavaScript runtime built on Chrome's V8 JavaScript engine. Node.js uses an event-driven, nonblocking I/O model that makes it lightweight and efficient. Npm is a Node.js package of open source library which is largest in the world. It's an asynchronous event driven JavaScript runtime, which is designed to build scalable network applications. It can handle many concurrent connections at a time, where when connection request is made concurrently for each connection a callback is fired. If there is no task to be performed node will go to sleep [6].

Node.js connection handling mechanism is super-efficient than our existing classical thread-based model Thread-based networking is relatively inefficient and very difficult to use. Furthermore, users of Node are free from worries of dead-locking the process, since there are no locks. Almost no function in Node directly performs I/O, so the process never blocks. Because nothing blocks, scalable systems are very reasonable to develop in Node. Node.js was first conceived in 2009 by Ryan Dahl and was developed and maintained by Ryan who then got sponsored and supported by Joyent**.** Dahl was not happy the way Apache Http server used to handle the lot of concurrent connections and the way code was being created which either blocked the entire process or implied multiple execution stacks in the case of simultaneous connections.

4.4. Web3.js

The web3.eth.Contract object makes it easy to interact with smart contracts on the ethereum blockchain. When you create a new contract object you give it the json

interface of the respective smart contract and web3 will auto convert all calls into low level ABI calls over RPC for you. The web3.js library is a collection of modules which contain specific functionality for the ethereum ecosystem.

- The web3-eth is for the ethereum blockchain and smart contracts
- The web3-shh is for the whisper protocol to communicate p2p and broadcast
- The web3-bzz is for the swarm protocol, the decentralized file storage
- The web3-utils contains useful helper functions for Dapp developers [4, 7].

4.5. Solidity

Solidity is a contract-oriented, high-level language for implementing smart contracts. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

4.6. *Architecture*

Transactions are those that give a blockchain purpose. They are the smallest building blocks of a blockchain system. Transactions generally consist of a recipient address, a sender address, and a value. This is not too different from a standard transaction that you would find on a credit card statement. A Bitcoin transaction moves the value of some bitcoin from one address to another address. A transaction changes the state of the agreed-correct blockchain. A blockchain is a shared, decentralized, distributed state machine. This means that all nodes (users of the blockchain system) independently hold their own copy of the blockchain, and the current known "state" is calculated by processing each transaction in order as it appears in the blockchain [8].

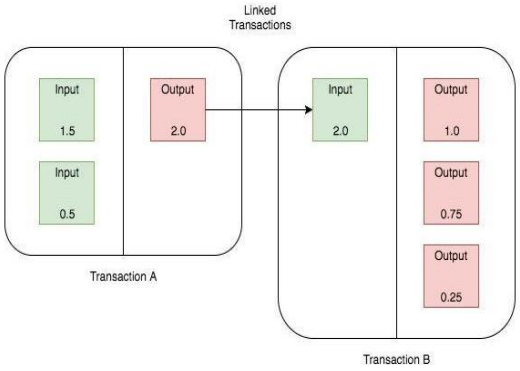

Fig.1: Linked transaction

Transactions are bundled and delivered to each node in the form of a block. As new transactions are distributed throughout the network, they are independently verified and "processed" by each node. This constant movement of coin is what constitutes the data within any blockchain architecture, while the ways in which transactions are handled and verified varies by implementation. An input always references a previous transaction's output. This continual pointer of inputs to previous transactions outputs allows for an uninterrupted, verifiable stream of value (represented by the bitcoin currency) amongst addresses.

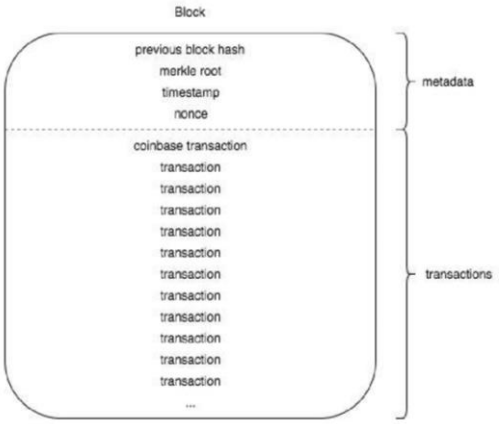

Fig.2: Block details

Blocks are data structures whose purpose is to bundle sets of transactions and be distributed to all nodes in the network. Blocks are created by miners (discussed in more detail below). It's important to realize that each miner (and more generally, each user of a blockchain) is allowed to act however they want within this blockchain system. Consensus rules dictate that only

valid changes to the blockchain will be accepted by everyone else [9]. This result in a system that economically guarantees that only valid blocks will be worked on, submitted to the network, and accepted by the greater community. Blockchains are probabilistic systems, by design. Nodes, or the computers in the network, independently decide and concur upon which "chain of blocks" is the longest and most valid. As a block is created and set around the network, each node processes the block and decides where it fits into the current overarching blockchain ledger. Side branch blocks are particularly interesting. They might not currently exist in the main branch, but if more work is done on them (meaning other blocks are mined that reference them as a parent), there is the possibility that that a particular side branch will be reorganized into the main branch. As new blocks are appended to the blockchain, it becomes increasingly difficult to "overwrite" existing blocks because the most valid chain is the one that has had the most work done on it [10].

Manufacturer-Dealer Workflow:

- The Dealer can initiate vehicle sale contract. A smart contract can then automatically send out requests for registration and insurance.
- The manufacturer adds new vehicle to the blockchain network as smart contract can by adding basic details like make, model, variant, chassis number, engine number etc.
- Executes the sale of the vehicle to the dealer on the smart contract, which automatically transfer ownership to the dealer.

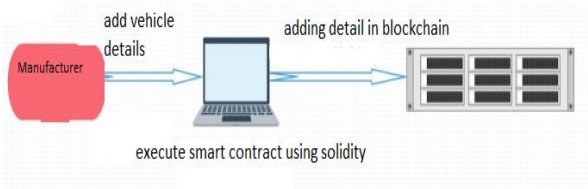

Fig. 3: Flow diagram of smart contract execution

Vehicle sale/registration workflow:

- The RTO and insurance agency can validate required data about vehicle and customer from Blockchain and provide registration and insurance respectively.
- On successful processing of the above step, the vehicle ownership can be automatically transferred to the customer by the smart contract

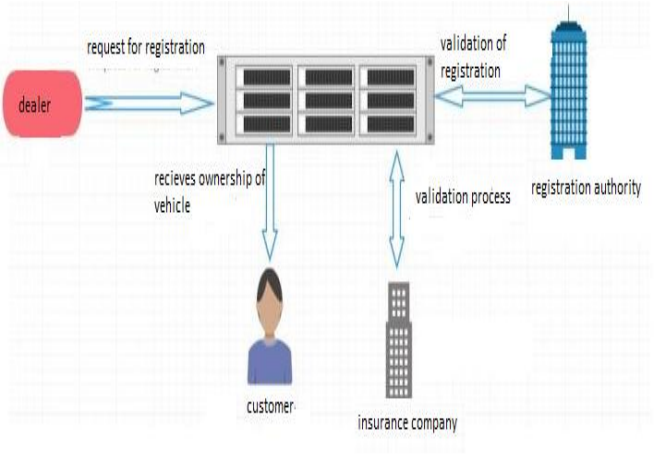

Fig. 4: Flow diagram of vehicle registration

5. RESULT

The User Interface of the Vehicle register platform for the vendor and insurance agent is done using ReactJS framework which can be deploy on local host. The back-end which consists of database and various API is done using MongoDB and NodeJS respectively which is used to interact with front-end/ User Interface. Ethereum blockchain is used to make the decentralized system of the registered vehicle in which smart contract is written on solidity which is a contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms.

The ABI, Application Binary Interface, is basically how you call functions in a contract and get data back. An Ethereum smart contract is bytecode deployed on the Ethereum blockchain. There could be several functions in a contract. An ABI is necessary so that you can specify which function in the contract to invoke, as well as get a guarantee

that the function will return data in the format you are expecting. The ABI, Application Binary Interface, is basically how you call functions in a contract and get data back. An Ethereum smart contract is bytecode deployed on the Ethereum blockchain. There could be several functions in a contract. An ABI is necessary so that you can specify which function in the contract to invoke, as well as get a guarantee that the function will return data in the format you are expecting.

Web3.js is used to interact with ethereum node using various connections; it is a library with collection of modules which contain specific functionality for the ethereum ecosystem. EVM (Ethereum Virtual Machine) is a system designed to operate as a runtime environment for Ethereum based smart contracts.

6. FUTURE SCOPE

Blockchain has literally enabled the technology ecosystem to take a significant leap of innovation. Along the years, as Bitcoin has managed to take prominence and grabbed attention from all over the world (and rightly so), people took to studying all about cryptocurrency and Blockchain- the very platform that enabled crypto transactions to take place. By identifying the need to make transactions more secure and recording them seamlessly, Satoshi Nakamoto came up with Bitcoin- the digital, cryptocurrency and Blockchain, the technology Bitcoin works on. To put it simply, Blockchain is a shared, distributed ledger for recording transactions and tracking both tangible and intangible assets across a trusted network. This digital ledger records transactions publically as well as validates all transaction data seamlessly. Blockchain, with its potential uses and benefits, has already intrigued many.

7. CONCLUSION

The main conclusion of this research paper is blockchain has affected a large number of applications in last decade. Vehicle registration system designed by us has great potential to mark there presence in today's scenario.

REFERENCES

[1] Alharby, M., Moorsel, V.A. (2017), "Blockchain-based smart contracts: A systematic mapping study", arXiv preprint arXiv:1710.06372.

[2] Iansiti, M., Lakhani, K. R. (2017), "The truth about blockchain", Harvard Business Review, 95(1), 118-127

[3] Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system"

[4] Tikhomirov, S. (2017, October), "Ethereum: state of knowledge and research perspectives", In International Symposium on Foundations and Practice of Security (pp. 206-221) Springer, Cham

[5] Lemieux, V. L. (2016), "Trusting records: is Blockchain technology the answer?", Records Management Journal, 26(2), 110-139

[6] Anjum, A., Sporny, M., Sill, A. (2017), "Blockchain standards for compliance and trust", IEEE Cloud Computing, 4(4), 84-90

[7] Sporny, M. (2017, April), "Building Better Blockchains: Linked Data in Distributed Ledgers", In Proc. 26th Int'l Conf. World Wide Web Companion (p. 1429)

[8] Singh, S., Singh, N. (2016, December), "Blockchain: Future of financial and cyber security", In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on (pp. 463-467), IEEE

[9] Buterin, V. (2014), "A next-generation smart contract and decentralized application platform", white paper.

[10] Morabito, V. (2017),"Smart contracts and licensing; In Business Innovation through Blockchain", (pp. 101-124) Springer, Cham