

## Decentralized Vehicle Registry on Blockchain

Harshit Khanna, Himanshu Mehta

Software Engineer, Delhi, India

### ABSTRACT

#### Article Info

Volume 6, Issue 5

Page Number: 134-140

Publication Issue :

September-October-2020

The main aim of this project is to meliorate the experience of the customers by providing them with the complete authentic history of a vehicle – from the manufacturer till the time it reaches to scrap yard. In vehicle registration management system we store the details in a decentralized and distributed database with the help of which various departments can access vehicle details. Any renovation in the vehicle details will be reflected in every department. By using blockchain we can track the whole lifecycle of the vehicle like selling or buying because it provides transparent of the entire business. Blockchain provides us transparency and is very trustworthy in vehicle transactions, preventing all the disputes and also lowers the cost of service because of which many stakeholders, including car manufacturers, buyers, sellers, dealers, regulators and even garages ae benefited. By the help of blockchain we can track ownership, sale and accident history and helps in maintaining proper system for supply chains. It also ensures that the data remains consistent among various departments and also eliminate false data problem. The regional and local carmakers as a whole are also influenced.

#### Article History

Accepted : 01 Oct 2020

Published : 07 Oct 2020

Keywords : Ethereum, Vehicle Registry, Blockchain, Smart Contracts, Decentralization

---

### I. INTRODUCTION

The process of vehicle registration the motor vehicle agencies need to collaborate with the external organizations like Department of Justice and Insurance. For correct tracking and registration the information is updated constantly. Maintaining the most updated information is essential to enable these organization to register and track vehicles accurately. Vehicle registration process is a very cumbersome and time taking process and has multiple parties involved in it by which there is a risk of information

manipulation, data duplication and various other errors and because of the above risks the important information can get highly susceptible to frauds and data tampering or even become non traceable. By using blockchain and by putting all the vehicle registration management system on blockchain it can easily take care of such issues and can be handled easily. Blockchain also helps us to reduce the turnaround time which was a negative aspect earlier. Also the data us updated only by authorized private key which reduces the risk of frauds and attacks and any tampering in data can be identified. It will

provide a easy structure which can be used in the project.

## II. LITERATURE SURVEY

### The Promise of Blockchain

The promise of blockchain is “the decentralization of trust, enabling value flow without intermediaries. The concept of third parties is removed by allowing financial transactions to be allowed and cleared in turn reduces the costs and complexity. In the distributed ledger concept one identical record is maintained by members of financial market rather than maintaining different records. By maintaining the distributed ledger the data is replicated which provide acceptance, beginning and non changeable platform for transaction like payments, transfer, assets etc. Once all the computer in the network accepts the new transaction is added in a form of new block in the chain. By verifying the transactions the risk of error and queries are reduced. Blockchain is a new type of distributed database. Information in blockchain is updated constantly and information is exchanged at the same time in a good manner providing instant clearing of transactions. Fast settlements also reduces the risk in the financial system which in turn reduces the capital requirements. The code simultaneously runs with the blockchain which is a new functionality in distributed databases which helps in modifying the data automatically. Smart contracts which is supported by blockchain automates variety of business functions. A “Cryptographic hash functions” is used for the security and privacy protocols in which each block in the chain is identified by its own unique “hash” function. Double spending of blockchain was prevented using this technique. The fraud was also reduced because of the complexity of the hash function. Blockchain can be either : Private or Public so it can be open to all or restricted to a particular group of users. Permission or Permission less so anyone can add a block or a group of people

are restricted from doing so. Blockchain works on public permission less model that’s why it takes time to add a new block o chain also faces performance issues. Other blockchain uses private, permissioned applications in which number of users can be controlled.

### Origin of Blockchain

In 2008, Satoshi Nakamoto first proposed the concept of blockchain which is essentially a public ledger. All the transactions are stored in a chain of data packages or blocks and distributed across a peer-to-peer network. The nodes involved in a network hold a copy of the blocks. Each and every transaction or digital event in the blockchain has to be approved using a acceptance mechanism by the majority of these participating nodes in the network. If approved, then the transaction is reduced in a new block. Along with a hash pointer a timestamp is applied to the new block. It acts as a link to the previous block and a nonce which is a random number for checking the hash. After that the new block is add to the previous chain of blocks and distributed across the network. Therefore blockchain provides a safe, decentralized, fault tolerance and auditable transaction platform. The key feature of blockchain is that it allows transaction to take place in a decentralized manner without any central party. Decentralization: In blockchain no third party is there in between the transaction, every node in the network can validate transactions and maintains a identical copy of the transaction. This makes blockchain fault tolerant, data consistent, attack resistant, transparent and free from notary or financial institutions. Persistency: By using a acceptance mechanism, time stamp and a cryptographic seal, an invalid transaction is not admitted. The transactions already recorded in blockchain cannot be edited, deleted or copied. This helps in data consistency, fraud protection and fixed records of the transactions. Anonymity: The user privacy is protected because the interactions which

are based on blockchain technologies take place between two individual using public key cryptography. Auditability: It is very easy to verify check or track the transactions because in a blockchain the transactions are stored in a chronological order.

### Design and implementation constraints

**Complexity:** A complete new vocabulary is involved in blockchain technology. Cryptography is more mainstream but the highly specialized industry is chock full of jargon. There are many efforts at providing glossaries and indexes that are simple and easy to understand.

**Transaction speed and cost:** Bitcoin currently has important transaction cost after being touted as “near free” for first few years of its existence. As of late 2016 it can process seven transactions in a second. Each transaction costs about \$0.20 and can store 80 bytes of data. The politically charged feature of using the bitcoin blockchain also acts as a store of information and is called bloating. It focuses to recheck and record the information.

## III. METHODOLOGY

### Blockchain

Cryptography is used in blockchain which is used for linking of growing list of record called “blocks”. Cryptographic hash of the previous block, timestamp and transaction data together join up to form a block. Modification of data is not possible in blockchain. It is a distributed ledger which help in permanent and verifiable transaction between two parties. A peer-to-peer network is used in blockchain which is used for inner node communication and validating new blocks. No one can change the data in any block without the acceptance of network majority. If any data in the blocks are changed automatically the data of subsequent blocks are altered. In blockchain records cannot be altered and it also have a good

design with high byzantine fault tolerance. In blockchain records cannot be altered without the alteration of all subsequent blocks and acceptance of the network, so blockchain is decentralized, distributed and public ledger. Participants can verify and audit transactions without paying money. Distributed time stamping server and a peer-to-peer network is used in managing blockchain database. Batches of valid transactions are first hashed and then encoded into a Merkle tree. For linking two blocks the block should have the hash of the prior block forming a chain. The integrity of the previous block is confirmed all the way back to original block.

### ReactJS

React is used in making interactive UIs. React help us to efficiently update and render the components when we design a simple view for application. React is an open source JavaScript library which is very easy, declarative to use. React is maintained by It firms like Facebook. ReactJS mainly works on MVC(Model View Controller) which is used for building user interface. Performance oriented applications can be made from components which are present in react. Components of react plays a very important role in web development. For using Reactjs in project, web developers need to create component in react and then use it. Render method is used by react components in input and output. React element contains component instance or DOM node and its desired properties. Element is a node of communication which tells react that what the user want to see on screen. It is unchangeable description object with two fields – type :(string React class) and props: object. The type of elements in a string with particular name and properties that define the attribute help in the representation of a DOM node. The elements of DOM are very light as they are just objects on ReactJS and they don't have to be analyzed. While creating an element tree, elements can be nested as parent and child, but it is not actual

instances it is descriptions. The one way data flow which begins with properties is known as ReactJS.

**NodeJS**

Node.js, a JavaScript runtime which is built on Chrome’s V8 engine. It uses non-blocking I/O, an event-driven model which makes both efficient and lightweight. There is an open source library package of Node.js known as Npm which is largest in the world. Also it is an asynchronous event driven JavaScript runtime which is designed to build scalable network applications. Many concurrent connections at a time can be handled easily by it, here a callback is fired for each connection on concurrently connection request. Node would go to sleep when there is no task performed. Other than our existing classical thread based model one of the connection handling mechanism is Node.js which is super efficient comparatively. Networking, thread based is quite difficult to use and relatively inefficient. Furthermore, due to no locks Node users are free from worries of dead-locking the process. Since in node there is no function exists which performs I/O, hence the process never blocks. In node scalable systems are very reasonable to develop because of nothing blocks. In 2009, Ryan Dahl was first conceived Node.js. After got developed and maintained by Ryan it got sponsored by Joyent. Due to lot of concurrent connections and the way of code was being created Dahl was not happy with Apache Http server. It might get blocked the entire process.

**Web3.js**

In order to interact with smart contracts on Ethereum blockchain, web3-eth contract object makes it easy to do so. Instead of creating a new contract object one could give it json interface of smart contract respectively, also conversion of all calls into low level ABI over RPC would easily be done by web3. This library i.e. web3.js, contains

specific functionality for Ethereum ecosystem which includes a collection of modules.

This library includes the following:

- Web3-shh means whisper protocol in order to communicate p2p and broadcast
- Web3-eth stands for Ethereum blockchain and smart contracts
- Web3-bzz stands for swarm protocol which is decentralized file storage
- Web3-utils functions for Dapp developers

**Solidity**

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

**IV. ARCHITECTURE**

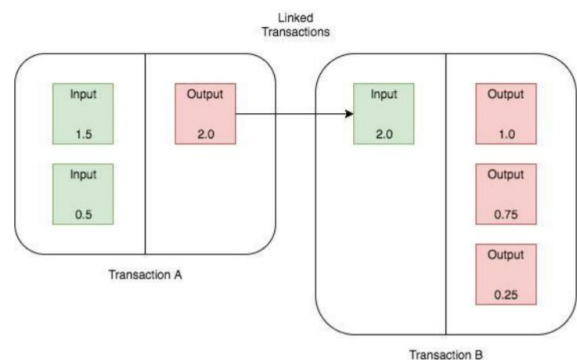


FIG.1 LINKED TRANSACTIONS

Transactions are the smallest building blocks of blockchain system which generally consist of a recipient address, a value and a sender address. It is similar to standard transaction that could be found recorded on a credit card statement. In a Bitcoin

transaction the transaction exist only if the value of some bitcoin moves from one address to other. The Blockchain is shared, distributed and decentralized state machine which means all the nodes, also called users of blockchain system independently record their own copy of the blockchain and the current known state is observed by processing each transaction individually in order as it appears in the blockchain.

In the form of a block, transactions are bundled and delivered to each node. On the distributed network, new transactions are distributed, also independently verified and processed by each node. In any blockchain architecture this constant movement of coin constitutes the data within it. Here an input always refers to a previous transaction's output. This pointer of continual of inputs to previous transactions output allows for uninterrupted, verifiable stream of value amongst addresses.

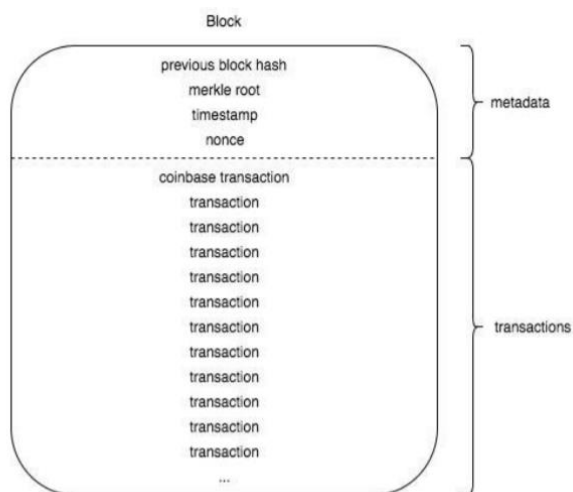


Fig.2 BLOCK DETAILS

Blocks are Data structures which shows its purpose to bundle sets of transactions and to be distributed to all the nodes in the network. Miners create the blocks in the blockchain. In each blockchain system each miner has the equal rights to act as they want to act in the system. Blockchain also includes consensus

rules which is necessary for everyone to accept the changes which occur in the complete blockchain, also it dictates only valid changes in the system to be accepted by everyone else. Hence, this complete system results in economically guaranteeing only valid blocks will be worked on, submitted on the network and also accepted by higher community. Blockchain is a probability based system, by design. Nodes in the complete network independently decide and lie upon which decides "chain of blocks" is the longest and most valid. In blockchain ledger, each node processes the block and decides where it would place into the current overarching blockchain. In the blocks, there exist, a side branch block which might not currently exist in the main branch, but if some work is done on them then there is a chance of existing that particular side branch into the main branch of the blockchain. It becomes increasingly difficult to overwrite existing blocks as soon as new blocks are added to the blockchain because the most valid chain is one which has the most work done on it

### Manufacturer Dealer Workflow

Manufacturer adds all the details of new vehicles to the blockchain network as a smart contract by adding basic details like make, color, model number, variant, chassis number, engine number etc.

Smart contract can automatically transfer ownership to the dealer by execution of the sale of vehicle to the dealer

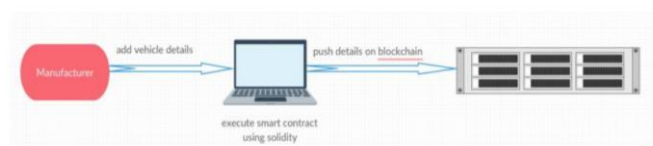


FIG.3 FLOW DIAGRAM OF SMART CONTRACT EXECUTION

### Vehicle Registration / Sale Workflow:

The vehicle sale contract can be initiated by dealer through smart contract which can then send out requests for registration and insurance. From blockchain data about customer and vehicle, the Insurance company and RTO can validate required data.

Without any error on running above processes, vehicle ownership can be transferred automatically by the smart contract. Fig.4 Flow diagram of vehicle registration

### V. 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 consist 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. It can be used for implementing smart contracts on various blockchain platforms.

ABI, the Application Binary Interface, is basically how you call functions in a contract and get data back. Ethereum smart contract is bytecode deployed on Ethereum blockchain. This smart contract is very useful due to its benefits such as Accuracy, which is primary requirements of a smart contract to record all terms and conditions in all details. Another big benefit is transparency, it facilitates total transparency of all transactions among all parties. There is now clear communication which benefits as there is no room for miscommunication or misinterpretation. As these contracts easily runs on software code and live on internet as a result, they

can execute transactions very quickly. Efficiency level is now high which results in more value generating transactions processed per unit time. This removes the need of vast use of papers.

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. For Ethereum based smart contract EVM (Ethereum Virtual Machine) is a system designed to operate as a runtime environment.

### VI. FUTURE SCOPE

Blockchain has enabled the technology ecosystem to take a significant leap of innovation. In many years passed by, Bitcoin has managed to grabbed attention of many people or almost of all over the world, people started studying about cryptocurrency and their own blockchain. Smart contracts allows many people in all ways as in speed and direct communication with the clients, it eliminate the need of mediators and allows for transparent, clear, direct relationships with clients. Through smart contract execution there is also reduction of fraud execution in this platform. Last and very efficient use of smart contract is immutable which ensures that once block is added to the blockchain it cannot be broken or tampered in any case. Satoshi Nakamoto once came up with the Bitcoin (the digital cryptocurrency) and blockchain technology makes the need of transactions more secure and recording seamlessly. In short, Blockchain is a technology which is growing very vastly or rapidly without seeing it's end and people are working and exploring more about it to achieve something better then ever.

### VII. REFERENCES

- [1] 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.
- [2] Alharby, M., & van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. arXiv preprint arXiv:1710.06372
- [3] Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing*, 4(4), 84-90.
- [4] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, 95(1), 118-127.
- [5] 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.
- [6] Sporny, M. (2017, April). Building Better Blockchains: Linked Data in Distributed Ledgers. In *Proc. 26th Int'l Conf. World Wide Web Companion* (p. 1429)
- [7] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- [8] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper.
- [9] Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer?. *Records Management Journal*, 26(2), 110-139.
- [10] Morabito, V. (2017). Smart contracts and licensing. In *Business Innovation Through Blockchain* (pp. 101-124). Springer, Cham.

**Cite this article as :**

Harshit Khanna, Himanshu Mehta, "Decentralized Vehicle Registry on Blockchain", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)*, ISSN : 2456-3307, Volume 6, Issue 5, pp.134-140, September-October-2020. Available at doi : <https://doi.org/10.32628/CSEIT206530>  
Journal URL : <http://ijsrcseit.com/CSEIT206530>