Supply Chain Management in E-Commerce Using Blockchain

Vaibhav D. Dhore and Neha Mishra

Abstract With the increase in the Internet and online shopping era, online shopping and E-commerce have become the most convenient way for customer and seller to buy and sell the product online using Internet. With this increasing E-commerce services, it has become mandatory to provide the trusted proof of delivery system to the customer and seller. Existing system is centralized system which completely relies on the third party for the proof of delivery which can lead to a single point of failure. Existing proof of delivery systems leads back in credibility, transparency, and traceability. Blockchain is the decentralized distributed ledger which provides the system to be transparable, traceable, and creditable. Supply chain management using Ethereum blockchain is one of the solutions that can be given. This system is the decentralized proof of delivery system that uses Ethereum smart contract to prove the delivery of a shipped item between seller and buyer. Each customer, seller, and courier services registers on the Web application. Later, seller uploads catalog of the commodities to be sold which customers choose to buy. Courier services are assigned this parcel based on the sentiment analysis, and later, at the time of delivery, payment is done using ethers.

Keywords Blockchain · Ethereum · Smart contracts · Supply chain

1 Introduction

With the widespread of technology and Internet, it has become a new trend for buying and selling the commodities online using Internet via E-commerce. This online shopping service provides customers to compare, review, and check the current trends in the market. Hence, they get a wide range of options over the different brands. E-commerce shopping is getting more favored with time especially with the increase

V. D. Dhore (✉) · N. Mishra
VJTI, Mumbai University, Mumbai, India
e-mail: vddhore@ce.vjti.ac.in

N. Mishra
e-mail: Nbmishra_m17@ce.vjti.ac.in

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2020

D. Patel et al. (eds.), *IC-BCT 2019*, Blockchain Technologies,
https://doi.org/10.1007/978-981-15-4542-9_6

in the use of cell phones and Internet. Hence, it has given rise to increase in the demand of the different commodities. Hence, delivery is provided by the third party to increase the supply of the mandatory demand. Therefore, proof of delivery of physical item and product has become mandatory and need of the current time. Hence, it is needed to facilitate the shipment in a way that is trusted, transparent, and traceable mostly for the seller, buyer, and transporters that are located around the globe.

Proof of delivery helps to provide the assurance of shipped items has reached from source to destination without being tampered. This process provides each entity involved with trust. Existing proof of delivery falls back in providing the transparency, traceability, and credibility. Most of the current system is centralized and depends on the paper document which is carried by the courier services. With the advancement of the cell phones, handheld devices also being used to share the report along with the commodities. Hence, this system relies on the support of the trust on the courier services. These third-party service providers are mostly unreliable and untrusted and cost much more for delivery.

Blockchain is a decentralized distributed ledger which is immutable. A blockchain uses log which is ordered and each event, i.e., transaction is being recorded which helps to trace and audit. Hence, using Ethereum blockchain would help to create smart contract and allow the execution of the code. Blockchain transaction is being irreversible, i.e., one cannot change once the transaction is being done and created. These transactions are being stored in the form of blocks. Each block consists of the data, timestamp, and the hash value of the previous block. These blocks are being organized in the form of the Merkle tree.

An optimized proof of delivery solution should provide the requirement which are mandatory for the trade are accountability which means the entities involved cannot deny any action taken i.e. it is irreversible, penalty and incentivization which means it provide trust between entities by giving them incentive hence they are being forced to act honestly else penalty is being paid, auditability which provides proper to trace and track the system, integrity where each transaction, logs and events are being tampered proof, authentication and authorization these provide the access and authority to legitimate users, time bound which ensures the shipped item is placed within the time frame [4].

In this paper, we provide the solution for the proof of delivery system using blockchain technology. In the given framework solution, the defined system involves single or multiple courier services. This solution provided mainly focuses on the eradicating the problems faced with the current centralized system which is based on the third party for the delivery. Here, the given proof of delivery system is being implemented between seller and buyer irrespective of the number of the courier services. Payments are being done in the form of the ethers which force entities to act honestly. Interplanetary file system do provide the integrity between entities and the contract with the help of the defined hash being stored.

2 Related Work

In this section, we review and summarize work related to proof of delivery algorithms and techniques that make use of blockchain.

In [1], blockchain is a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the ledger is verified by consensus of a majority of the participants in the system. The entered records cannot be deleted. The popular example that uses blockchain technology is Bitcoin; it is a peer-to-peer decentralized digital currency. The digital currency Bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found a wide range of applications in both financial and non-financial world. Various applications on healthcare, identity management, cloud, Iota, security, banking, and supply chain are being en-cooperated with blockchain.

In [2], it is being explained that various aspects of blockchain can be used in different fields. Various new consensus protocol can be build such as proof of intelligence which can be later used in AI. Here, how the blockchain works logically and smart contracts can be used to gain the verified blocks.

In [3], a blockchain is a public ledger distributed over a network that records transactions executed among network participants. Each transaction is verified by network nodes according to a majority consensus mechanism before being added to the blockchain. Recorded information cannot be changed or erased and the history of each transaction can be recreated at any time. Blockchain can be used in various fields which can give better way for recoding the records such as identity management such as records of voter Id, Aadhar card data, and driving licence. Blockchain can provide various advantages like trust between the participating entities, transparency, decentralization, and automation. The basic transaction of records is shown as below.

In [4], blockchain is a distributed ledger which means all the parties taking part in the transaction or the parties present on the blockchain has the copy of the ledger and there is no centralized database. In case of any failure of the centralized database, it may lead to data loss but with blockchain this problem is solved. Another important advantage provided is the transparency of the transactions. Blockchain has found application in many new technologies with its promising features. Digital identity management can be done by blockchain where we can control our identity without depending on any central authority. It enables us to share our identity according to the need and can protect user's consent. One Name is one of the companies providing such digital authentication. In 2015, Bitcoin Foundation started a new project on the blockchain-based voting system to ensure transparency in the voting system with every vote being recorded on the blockchain. Immutability, cryptographic hash, and transparency are the advanced features provided for the blockchain based voting system. In supply chain management, blockchain enabled us to keep the track of the origin of the products. We can ensure the quality of the end products by maintaining the immutable record on the blockchain. Further, blockchain is also used with IoT, medical services, baking, real estate, etc.

In [5], various protocols are used in blockchain for adding the new block in the chain by the form of verification. This verification is done by the consensus protocol. Consensus protocol is of two major types: proof of work and proof of stake. Depending on the type of blockchain, these protocols changed. Blockchain can be of permissioned and permissionless. Access privacy of both protocols depends on the type of the blockchain.

In [6], blockchain is a new technology for data sharing between untrusted peers. However, it does not work well with massive transactions. Besides, there are high barriers between heterogeneous blockchain systems. In this paper, it is proposed that an innovative component-based framework is for exchanging information across arbitrary blockchain system called interactive multiple blockchain architecture. In given architecture, a dynamic network of multi-chain is created for inter-blockchain communication. Here, it is proposed that the inter-blockchain connection model is for routing management and messages transferring. Additionally, their proposed protocols provide transactions with atomicity and consistency in crossing-chain scene.

In [7], proof of delivery plays a major role in the delivery of any physical assets. In this paper, to maintain the trust of each entity, double collateral has been taken in the form of ethers. An automated system has been implemented which on successful delivery of the product will return ethers to the entities depending upon the given share. An automated dispute solver has also been implemented in order to gain the minimum dispute among the entities.

Each entity is managed by the smart contract which helps to develop the proper solution for the courier services. Here, more than one courier service might be required for the delivery based on the address of the delivery point. Hence, each product has the verification key which is being shared to each other for the purpose of the authentication. When the seller gives the courier service for delivery, it first checks whether the address is near me or not. If it is near it then the delivery is done by the same courier service where the customer verifies the keys given to it and then the delivery is being confirmed. If the address does not fit in the location of the courier service, then it transfers to other courier services, and key verification is done and later the delivery takes place. Here, more than one courier services might be engaged for the delivery based on the address. An arbitrator manages any dispute among the courier services and seller for the purpose of the ether transfer. If dispute happens then the whole transaction being made is failed and then the whole process is repeated again. Easy return policy has also been implemented for the purpose of better services than the traditional method of relying on the third party.

In [8] paper solution related to maintenance of whole agri-food details using RFID tags from raw materials to the final products like vegetables and meats, and fruits like for e.g. meat of pig contains details of pig, its parents, any disease related to pig, their slighter details is stored in the block chain in various units like from production to distribution to end users. Each RFID sends signal data information using sensor and network to blockchain database. These data would help to get track of the origin of the product and final delivery destination. If any major issue such as poisoning

due to rotten food happens, then the further delivery can be stopped as we would know the source and destination where food has been supplied.

In [9], current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. Single point storage, processing and failure are the problems in this architecture. Solutions to these problems have provided blockchain technology. This paper proposes a supply chain system for detection of counterfeiting attack which is a decentralized supply chain with the help of blockchain and near-field communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security. Simulation in the paper shows that the proposed protocol has good performances as well as gives nice security compared with the state-of-the-art consensus protocol Tendermint.

In [10], RFID is being used in order to perform the log of the ownership of the product; hence, due to the log creation of the system, a customer can refuse the product if the manufacturing company fails to give the ownership of the product hence helped to reduce the anti-counterfeits. Hence, here, post-supply chain ownership management is important. After the defined system of the supply chain, at the later point, it can be disrupted at the retailer where the product can be mixed with the duplicate product or the forged product. Hence, every entity can be stored on the blockchain and it can help to gain the proper verification of the genuineness of the product.

In [11], smart city has all data over the network. A smart city uses information technology to integrate and manage physical, social, and business infrastructures in order to provide better services to its dwellers while ensuring efficient and optimal utilization of available resources. With so many technologies as cloud computing, Internet of things (IoT), and interconnected networks, more innovative solution, direct interaction, and collaboration between local government and citizens can be delivered by smart cities. Even though there are many potential benefits, disruption causes many problems related to information security and privacy. This paper presents a system with a security framework that is a combination of blockchain technology and smart devices for a secure communication platform in smart cities.

Here, we are using the Ethereum smart contract service to create the smart contracts for the data management. Here, the shipment is sent and the front of the mobile app tracks the data using Bluetooth LE sensor and keeps track of the temperature, and when the shipment reaches, these temperature records are then sent to the smart contract, i.e., Ethereum node, for keeping log and taking the method for verification of the proper environment.

Current existing system includes third party for the delivery and there is no transparency for the owner of the product. Each transaction made during the process of buying and selling of a particular item can be tampered without any proof which may cause primary dissatisfaction to customer. Data log of the current system is reversible. Anyone can change the details of the item and the transaction log.

3 Proposed Solution

In the proposed blockchain solution, the main focus is given on the proof of the delivery of the commodities between seller and buyer. We are using Ethereum blockchain smart contract to maintain the proof of delivery between courier services and customer. The main entities of the system are:

- Customers: Customers are the main entities of the defined system. Each customer is provided to register at the Web-based application. These details are being stored on the blockchain in the form of the identity management. For being more concern, we can even put know your customer format of the bank by using the system such as Aadhar number.
- Seller: Seller is the major role player who sells their product on these sites and helps to maintain the E-commerce. The seller has the item to be packaged for transfer to the interested buyer. The seller creates the first contract in the chain. Therefore, the seller is the owner of the first contract created.
- Courier services: Courier services are the entities which help to deliver the product over the defined time period. Multiple couriers are available to deliver the item from the seller to the buyer if needed based on the geolocation of the seller and buyer. The transporter creates the next contract in the chain (Fig. 1).

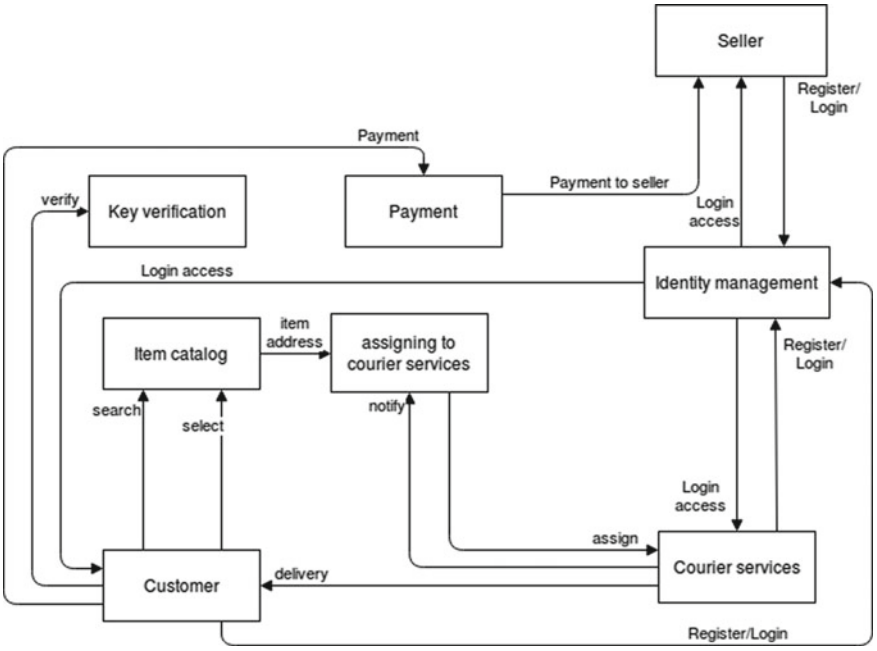

Fig. 1 Supply chain management in E-commerce using blockchain proposed system

In our system, customer registers to the blockchain using the Web application where their data is stored in the form of blocks. Each customer gets access to the item catalog from where they can choose the item to buy. Seller registers to the blockchain similar to the customer, and even courier services get registered.

Once any register customer requests for the product, that product is set for delivery by seller. Using sentiment analysis on the user review for the courier services, delivery is assigned to that service.

During the process of assignment, the key is generated and provided to the courier services which would be required at the time of verification. Customer gets the details and key as well. During the part of delivery, customer verifies the key and then the delivery is confirmed. Payment is done in the form of ethers, later which is transferred to the seller. Each transaction is recorded and maintained for future references.

In order to achieve the needed functionality with transparency and tracing the item as it moves through the chain of contracts, the smart contracts contain the following:

- Methods: Methods are used in smart contracts to create function calls. Each function is responsible for executing and implementing a desired action. Hence, in this work, some of the important functions we have created include methods to deposit the collateral, perform the key verification between any two parties as well as settle the payment and handle the dispute. All public variables have automatic getter functions created for them. However, setters have to be created as required. Hence, to change the state of a contract, a setter function was created to allow only its parent or its own child to alter its state.
- Modifiers: Modifiers are used in the smart contracts to create a requirement before the execution of a function. For instance, the collateral should be certain agreed upon amount. This is checked using a modifier. Other modifiers were also used to restrict the execution of a function based on the Ethereum address of the function caller. Therefore, certain functions can only be executed by the seller, others by the transporters and buyer, respectively.
- Events: Events act as notifications and are used as logs which can help in tracing back in case of dispute. Therefore, any function that is executed creates an event that updates all entities about the status of the item and contract until now.
- Variables: Variables are used to store information that might change as the transaction progresses or that are needed for certain checks and functionalities. Therefore, the main variables in the contracts are used to store Ethereum addresses of the participating entities, the key hash that is used in the key verification comparison, the item price, the contract state, IPFS hash, and the address of the child contract for each parent contract in the chain.

Following is an interface contract declaring the required functions for the customer. The data structures used are structure and map. The contract's customer's data structure will contain the following information:

- *custmerName* will store the name of the customer,
- *customerAddress* will store the address of the customer which will be required for the delivery purpose.
- *custmerHashReport* stores the hash for the report which will be given during the delivery process.
- *custmerAdd,* the blockchain account address.

The customer Registration(…) function is used to store the customer's details. To register the customer, the function will be executed as follows,

customerRegistration(0x1111111111111111111111111111111111111111, Customer1, Mumbai, customer1@gmail.com)

The function viewHistory() returns the historical customer data which the customer wants to view.

```
Contract CustomerContract {
        struct Customer {
address customerAdd;
string customerName;
uint age;
string email;
bytes32 custmerHashReport;
string addr;
}
        mapping(address => Customer) public customer;
function customerRegistration(address customerAdd, string customerName, string customerAddress, string customeremail) public view returns (bool success);
        function viewHistory() public view returns (Customer[] c);
}
```

Following is an interface contract declaring the required functions for the seller. The data structures used are structures and mapping. The contract's seller data structure will contain the following information:

- *sellerName*, stating the seller name.
- *sellerAddress*, the location address of the seller.
- *sellerAdd,* the blockchain account address.
- *sellerEmail* mail id for contact.

The sellerRegistration(…) function registers the seller. The function is as follows,

sellerRegistration(0x3333333333333333333333333333333333333333, Seller1, Mumbai, seller1@gmail.com)

The updateItem(…) function uploads the hash generated of the details of the item and a brief description of the item. This can be done as follows,

updateItem(0x1111111111111111111111111111111111111111, "Mi LED TV 4X PRO 138.8CM", QmYqSCWuzG8Cyo4MFQzqKcC14ct4ybAWyrAc9qzdJaFYTL)

"QmYqSCWuzG8Cyo4MFQzqKcC14ct4ybAWyrAc9qzdJaFYTL" is the hash of the item details.

```
contract SellerContract {
      struct Seller {
address sellerAdd;
string sellerName;
string sellerAddress;
string sellerEmail;
}
       mapping(address => Seller) public sellers;
function sellerRegistration(address sellerAdd, string sellerName, string sellerAddress, string sellerEmail) public view returns (bool success);
function updateItem (address sellerAdd, string itemDesc, bytes32 itemHashReport ) public returns (bool success);
}
```

Following is an interface contract declaring the required functions for the courier services. The data structures used are structures and mapping. The contract's courier services data structure will contain the following information:

- *courierServicesName* takes the courier services' name who will deliver the product to customer.
- *courierServicesEmail* takes the mail id of the courier services.
- *courierServicesAddress,* it stores the address of the courier service's address.
- *courierServicesAdd,* the blockchain account address.

The courierServicesRegisration(…) function registers the courier services into the network.

courierServicesRegisration(0x4444444444444444444444444444444444444444, CourierServices1, courierservices1@gmail.com, Mumbai)

```
contract CourierServicesContract {
        struct CourierServices {
address courierServicesAdd;
string courierServicesName;
string courierServicesEmail;
string courierServicesAddress;
}
        mapping(address => CourierServices) public courierServicess;
function CourierServicesRegisration (address courierServicesAdd, string courierServicesName, string courierServicesEmail, string courierServicesAddress) public view returns (bool success);

}
```

Following is an interface contract declaring the required functions for the item datastore. The data structures used are structures and mapping. The contract's item datastore data structure will contain the following information:

- *itemHashReport* is the hash of the details of the item

The function itemRegistration(…) registers the item details. The function is,

itemRegistration(1, Item1) will return the status of the registered item.

The item detail is requested using requestItemData(…) function. It can be done as follows,

requestItemData(1), the item data is returned.

```
Contract ItemContract {
        struct Item{
uint itemId;
bytes32  itemHashReport;
}
mapping(uint => Item) public items;
function itemRegistration (uint itemId, string itemName) public view returns (bool success);
function requestItemtData (uint itemId) public view returns (Item[] I);
}
```

4 Conclusion

In this paper, we have provided a solution for the centralized E-commerce site which can be tampered. This solution helps to give the system to be decentralized and provide it with the proper proof of the delivery of the commodities in the single as well as the multiple courier services. This solution eliminates the third-party reliability of the system for the delivery. It creates benefit for the customer. Each and every transaction is being recorded, and hence, it cannot be tampered as blockchain has the property of being irreversible. This system provides transparency to the customer and has a record of the ownership of the item.

References

1. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: beyond bitcoin. Appl Innov 2:6–10
2. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V (2018) To blockchain or not to blockchain: that is the question. IT Professional 20(2):62–74
3. Henry R, Herzberg A, Kate A (2018) Blockchain platforms: a compendium. Blockchain Access Privacy, IEEE, pp 38–45
4. Kan L, Wei Y, Muhammad AH, Siyuan W, Linchao G, Kai H. A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) 2018 Jul 16. IEEE, pp 139–145
5. Tian F (2016) An Agri-food supply chain traceability system for china based on RFID & Blockchain Technology. IEEE
6. Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T (2017) A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access 5:17465–17477
7. Alzahrani N, Bulusu N. Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain. In: Proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems 2018 Jun 15. ACM, pp 30–35
8. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: High performance computing and communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on 2016 Dec 12. IEEE, pp 1392–1393
9. Hasan HR, Salah K (2018) Blockchain-based proof of delivery of physical assets with single and multiple transporters. IEEE Access 6:46781–46793
10. Consumers are now doing most of their shopping online. Accessed 13 Jun 2018
11. UPS study: purchases from marketplaces nearly universal retail now global as e-commerce shoppers cross borders. Accessed 13 Jun 2018. Available: http://fortune.com/2016/06/08/onlineshopping-increases/