Hindawi
Security and Communication Networks
Volume 2023, Article ID 9853410, 1 page
https://doi.org/10.1155/2023/9853410

Retraction

Retracted: Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract

Security and Communication Networks

Received 3 October 2023; Accepted 3 October 2023; Published 4 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. M. Khan, N. T. RoJa, F. A. Almalki, and M. Aljohani, "Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract," *Security and Communication Networks*, vol. 2022, Article ID 2213336, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2213336, 8 pages
https://doi.org/10.1155/2022/2213336

Research Article

Revolutionizing E-Commerce Using Blockchain Technology and Implementing Smart Contract

Mohammad Monirujjaman Khan[1], **Nesat Tasneem RoJa**[1], **Faris A. Almalki**[2] **and Maha Aljohani**[3]

[1]*Department of Electrical and Computer Engineering, North South University, Bashundhara, Dhaka-1229, Bangladesh*
[2]*Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[3]*Software Engineering Department, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia*

Correspondence should be addressed to Mohammad Monirujjaman Khan; monirujjamanqmul.khan@gmail.com

Received 25 February 2022; Revised 6 April 2022; Accepted 25 April 2022; Published 31 May 2022

Academic Editor: Muhammad Arif

The days of storing data manually are behind us. We are opting for the online form of data storage and transfer. The new era of data digitization comes with its own perks and detriments. Cybersecurity is still a crucial concern today. As more data transfer occurs through an online medium, the risks of a breach and cyberattacks are inevitable. The whole foundation of e-commerce is based on the online transfer of goods and transactions without the need to travel. Transferring transactional data and transactions in e-commerce are prone to cyber threats. Our research's major objective is to develop a system that protects against such mishaps, especially during the transfer of transactional data, and also implement an automated system that ensures these transactions occur without any errors. To implement this, we are taking advantage of new emerging technologies called blockchain and smart contract. Blockchain allows a decentralized, immutable digital ledger to safely store and transfer data across the network. Blockchain technology is used in e-commerce to transfer transactions in a safe, secure, and faster way. Blockchain enables a peer-to-peer transaction system and data encryption that enables the safe transfer of transactional data. Blockchain is used to transfer transactional data. A smart contract is a special program that enables, verifies, and enforces the terms of a contract digitally. It provides transactional security as the contact is in place. The blockchain, coupled with smart contracts, will revolutionize the future of e-commerce. We have combined blockchain technology to ensure data security and user privacy with smart contracts to ensure that the protocol for the transaction is maintained. The results are presented by building and implementing the proposed system that provides the solution for transactional data privacy.

1. Introduction

As the world is advancing into a more digitalized version of itself, people's needs and luxuries are evolving with it. People are gravitating towards online shopping rather than visiting shops physically. In e-commerce, most of the interactions between the buyer and seller occur through an online medium. So, it is essential to have a secure form of interaction between them. Online interactions, particularly online transactions, are not always completely secure [1]. There has been an increase in recorded security breaches in which a third party gains possession of large amounts of data [2, 3]. Most likely, some people are constantly trying to breach security and exploit certain weaknesses in the network. This is where blockchain comes in. Blockchain is a peer-to-peer, decentralized, trustless network with a public ledger and automated access-control manager, where members can interact without any trusted intermediaries and any form of malicious activities [3, 4]. Blockchain used heavy cryptography which gives the interactions between

each node of the network a sense of authoritativeness [4]. Smart contracts are self-executing programs on the blockchain which allows proper, distributed, and heavily automated workflows [4]. We can protect the network from malicious intrusion by third parties, using cryptographic and other protection techniques [5].

Blockchain is a fairly new technology, which was introduced by Satoshi Nakamoto in January 2009 as part of the bitcoin technology to decentralize currency [6]. Blockchain has sparked up an interest in numerous applications in finance, health care system, reputation system, banking industry, Internet of Things (IoT), public and social service, and so on [4, 7–9]. It is a type of decentralized database that is distributed across the whole network and is more secure than traditional databases. All transactions are kept in the blocks. As new transactions occur, if the transaction is verified by the consensus proof-of-work (PoW) algorithm, it appends to the blockchain [7]. A smart contract is a hidden contract between a buyer and a seller that is written as a program and is automated. Security issues for e-commerce and finance pose a major threat these days [10].

As the world of e-commerce is rapidly growing, the need for a secure and protected form of interaction between a buyer and a seller is becoming more essential by the day. While we enjoy the benefits of a data-driven culture, we must consider how our data is stored, used, and spread. Centralized organizations hold a large amount of personal data of their users and the users have no control over how these organizations are using and manipulating these [3]. Research conducted by Yli-Huumo et al. shows that out of 41 blockchain-related papers, 80% of the research is solely based on bitcoin, whereas only 20% of the research work has been performed on smart contracts and other applications of blockchain [11].

In paper [11], the authors conducted research and it was found that out of 41 research papers based on the blockchain topic they had surveyed, 33 of them were focused on bitcoin applications and only 8 of them focused on other applications of blockchain. Bitcoin is not the sole application of the blockchain. In the paper [12], the author discusses the application of blockchain technology to medical data. Blockchain can be used to keep medical records of patients for easier access during a medical emergency. In paper [13], the author discusses the implementation of blockchain in banking industries in China. In papers [1, 3], the authors focused on the security issues that we are dealing with in online data and information transferring systems. In papers [4, 5, 14] and [15], the authors proposed a smart contract application to implement automated programs to control and secure relationships over computer networks. In paper [2], the authors discuss the issues with security breaches in the Internet of Things (IoT) devices. IoT devices are prone to hacks, and the issue can be solved using blockchain technology and smart contract, which are also discussed in [4]. In papers [16], the authors discuss how the existing system lacks transactional privacy and propose a solution using Hawk, where we can use private smart contracts without using cryptography. In the study [17], the author presented an Ethereum-based solution for transactional privacy. In the paper [18], the authors surveyed the benefits and drawbacks of online shopping. The research conducted by the authors of [10] stated that there is a security need for transaction data and user data for e-commerce platforms. In the paper [19], the authors propose a solution to transaction insecurity by implementing cryptocurrency. However, it was discovered that the transaction confirmation process for transferring funds was very slow. Implementing blockchain in online services such as e-commerce is difficult due to its scalability. Also, bitcoin transactions use 3 to 4 times the amount of energy as 100,000 VISA transactions [18]. The authors of the paper [20] developed a blockchain-based electronic health record monitoring system and data security. Smart supply chain management using the blockchain and smart contract has been developed in the paper [21].

The main application of blockchain is still considered to be bitcoin [11]. Implementation of blockchain technology along with smart contracts has not yet been adopted by many e-commerce platforms. A transaction on an e-commerce platform is made secure, easier, and faster with blockchain. Users can not only make safer transactions but also store digital assets under the security of the blockchain. In a traditional form of online transaction, a third party (i.e., banks and credit cards) is required to confirm the transaction [11], but if we use a smart contract, the need for a third party is discarded. All the processes that require human interaction to complete the transaction are replaced by computer programs, thus making it safer, more secure, and faster. Blockchain, coupled with smart contract technology, can not only improve the experience of online shopping but make it safer. To the best of the author's knowledge, no work has been performed merging blockchain and smart contracts in e-commerce in the literature study stated above. The objective of this research is to use blockchain technology in e-commerce to transfer transactions in a safe, secure, and faster way. We used blockchain technology to assure data security and user privacy as well as smart contracts to ensure that the transaction protocol is maintained.

In the next section of this paper, the authors describe the methods and methodologies used to implement blockchain technology in e-commerce. In section 3, the authors have described the results that were obtained from the research and the analysis of the results. In section 4, the authors have discussed the conclusion of the research and how that can further improve and extend the current research.

2. Method and Methodology

This section of the paper discusses the methodologies that were used to implement the proposed model. In the proposed model, the authors solve the problem that people face on e-commerce platforms. We are displaying the transaction flow on a website. The coding part of the blockchain was written in JavaScript, and Postman was used to send HTTP requests via an API call. The smart contract was coded using solidity. The website code was written using HyperText Markup Language (HTML), Cascading Style Sheets (CSS), Structured Query Language (SQL), and Hypertext Preprocessor (PHP).

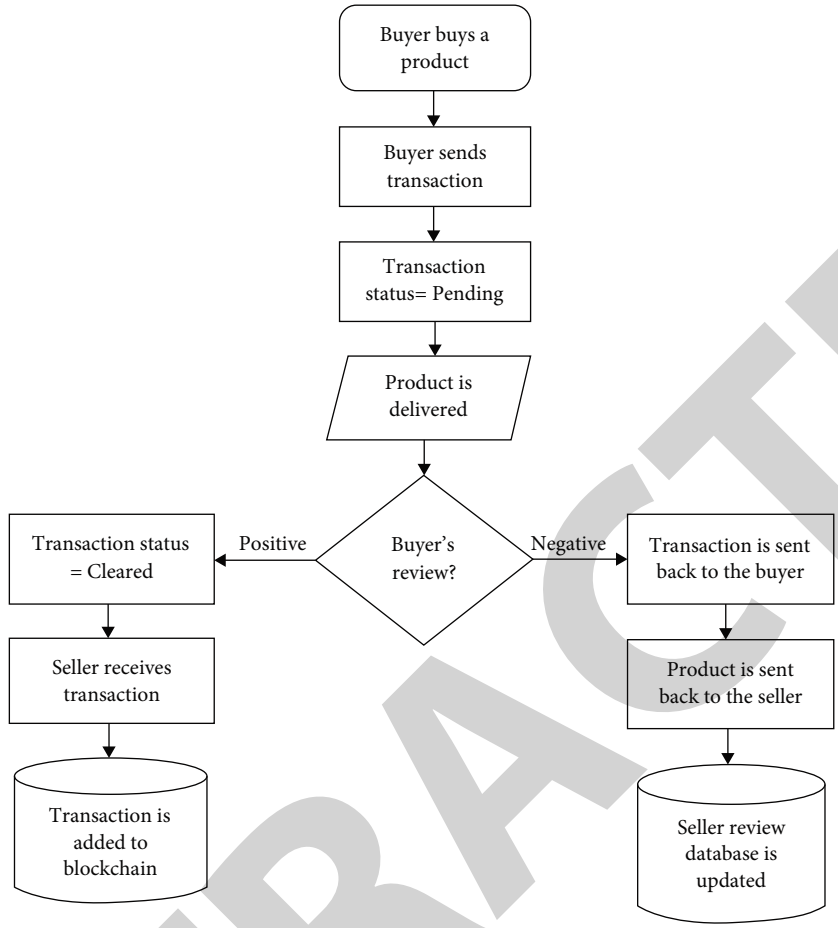


Figure 1: Flow diagram to show how our system works.

2.1. Outline of the Proposed System. Figure 1 shows the schema of how our proposed system works. When a buyer buys a product, they confirm the purchase by making the transaction. As the buyer makes the transaction, the transaction status is set to pending until the buyer receives the purchased product in good condition. After the transaction is completed, the product is sent to the buyer's address. When the buyer receives the product, they are required to submit a prompt review of the product so that the transaction can occur.

If the buyer receives the product in good condition and there is no fault with the product, the buyer leaves a positive review and the transaction status is cleared. The seller receives the transaction. The blockchain containing the transaction information is updated. If the buyer somehow does not receive the product or receives it in poor condition, the buyer leaves a negative review and the transaction status is not cleared. The transaction is sent back to the buyer, the product is sent back to the seller, and the database containing the seller's review is updated.

2.2. Blockchain. A blockchain is a type of decentralized, peer-to-peer database that is distributed across each node of the trustless blockchain network. As the name suggests, a blockchain is a chain of blocks. Each block in the blockchain contains some attributes that are very important to maintain the integrity of the whole blockchain. The blockchain uses heavy cryptography to maintain this integrity [4]. If an attribute of any block is tampered with, the block becomes invalid. If one of the blocks collapses or is invalid, the whole blockchain becomes invalid. This is because each block contains the last hash, which refers to the previous block. So, changing any attribute of the block will change its hash, and the next block cannot refer back to the invalid block. To prevent this, we have used an algorithm called proof-of-work (PoW). Proof-of-work is a decentralized consensus process that allows each node of the network to spend time, solving a complex computational or mathematical problem to prevent the system from being hacked.

Figure 2 shows the data for the genesis block and also the attributes of a block. Each block in the blockchain contains a timestamp, the last hash, a hash, the difficulty, and nonce and data. The timestamp is the time of block creation, the last hash is the hash of the previous block, the hash is the cryptographic hash of the current block that is calculated by hash functions (such as SHA-256), the difficulty is used to maintain the mining rate of each block, a nonce is a pseudorandom number that the miners calculate, and the data is simply the data the block will store (it is the

```
const GENESIS_DATA = {   // SCREAM
    timestamp: 1,
    lastHash: '-----',
    hash: 'hash1',
    difficulty: INITIAL_DIFFICULTY,
    nonce: 0,
    data: []
};
```

Figure 2: Data for the genesis block.

```
const crypto = require ('crypto');

const cryptoHash = (...inputs) => {
    const hash = crypto.createHash('sha256')

    hash.update(inputs.sort().join(' '));

    return hash.digest('hex');   // So that
};
```

Figure 3: Generating hash using SHA-256.

```
static mineBlock( { lastBlock, data }) {
    const lastHash = lastBlock.hash;
    let hash, timestamp;
    let { difficulty } = lastBlock;
    let nonce = 0;

    do{
        nonce++;                          // nonce is adjusted until it meets condition
        timestamp = Date.now();           // once nonce is created block is generated so
        difficulty = Block.adjustDifficulty ( { originalBlock: lastBlock , timestamp});
        hash = cryptoHash( timestamp , lastHash, data, nonce, difficulty)          //
    } while (hexToBinary(hash).substring( 0 , difficulty) !== '0'.repeat(difficulty));
```

Figure 4: mineBlock function in Block class.

```
class Blockchain{

    constructor (){
        this.chain = [Block.genesis()];     // chain arr
    }

    addBlock( {data} ){
        const newBlock = Block.mineBlock({
            lastBlock:this.chain[this.chain.length - 1],
            data
        });
    this.chain.push( newBlock );        // adds a new bl

    }
```

Figure 5: Blockchain class and 'addBlock' function.

```
> redis-server --daemonize yes

[nodemon] 1.18.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching: *.*
[nodemon] starting `node index.js`
Listening to localhost:3000
```

Figure 6: Redis server running localhost: 3000.

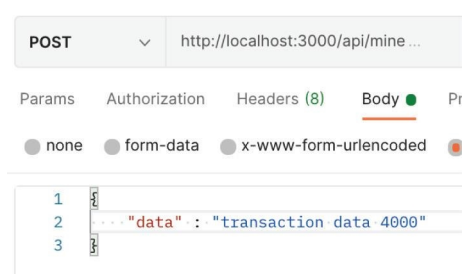


Figure 7: Mining transactional data using Postman API call.

transactional data for our research). The first block in the blockchain is called the "genesis block." Since there were not any blocks before the genesis block in the blockchain, it does not have the last hash. All the attributes for the genesis block are hardcoded.

Figure 3 shows how a hash is generated using a hash function. A hash function satisfies the cryptographic demands required for a blockchain computation to be solved. A cryptographic hash function called SHA-256 is used to generate a hash for each block during the mining of each block. Hash functions are very sensitive to changes. The same data will produce the same hash. A slight change in any attribute of the block will change the hash code and the block will not match. Since it is almost impossible to estimate the length of a hash if someone were trying to crack the blockchain, hashes are of a fixed length.

Figure 4 shows the 'block' class contains a 'mineBlock' function which mines a new block upon receiving new transaction information. Mining a block is a competitive process. To mine a block, the program needs to compute complex mathematical calculations to find the nonce. This requires a huge amount of resources and energy. There is no exact way to calculate the nonce value. So, the miner (the one who mines the block) needs to iterate and reiterate to find the nonce value that matches the criteria in the 'mineBlock' function. To find the nonce value is not enough to mine a block. However, miners cannot simply add a block to the blockchain without proof-of-work. The miner has to show proof-of-work. Proof-of-work checks the whole blockchain for any discontinuity before adding the next block. Each node in the network checks the nonce value that was calculated and verifies it. This verification takes less time than computing the actual proof-of-work algorithm. If all the nodes in the network verify that the nonce value is correct, only then can the new block be mined.

Figure 5 shows the constructor and function of the blockchain class. The constructor constructs a blockchain and adds the genesis block as the first block. The 'addBlock' function is used to add a new block to the blockchain. When a block is successfully mined, it is appended at the end of the blockchain. This is done using the 'addBlock' function. The new block is added at the end of the blockchain, and the hash of the previous block is linked with the current block. The new blockchain is then updated across the whole blockchain network. Each node of the network will receive an identical blockchain.

Figure 6 shows a Redis server running. We have implemented a network through the Redis server with a default localhost:3000, which allows a real-time messaging system. Postman is used for API mine call through an HTTP request. We created a POST request to send data to the block class for the mining block. We created a GET request to access the blockchain, read the blockchain, and display the

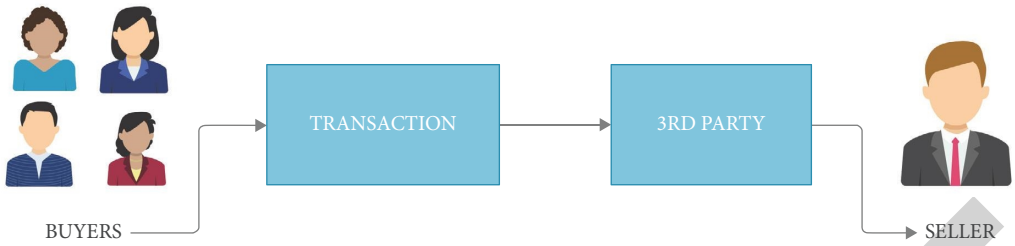


Figure 8: A simple transaction without using a smart contract.

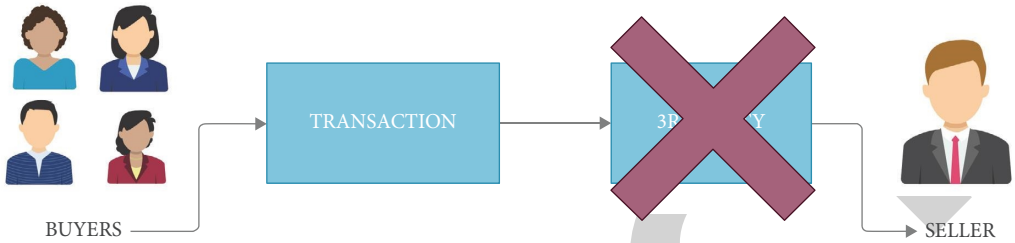


Figure 9: A simple transaction using a smart contract.

blockchain. Figure 7 shows that the data passed during the HTTP POST request was the transaction data, and it was in its corresponding JSON format. This was passed to the 'mineBlock' as an attribute. When the transaction status is cleared by the buyer, the block is mined. The mined block is used to sync the blockchain all over the blockchain network.

2.3. Implementation of Smart Contract. A smart contract can solve numerous problems that occur during a traditional transaction between a buyer and a seller. Figure 8 shows a visual representation of how a simple transaction occurs between a buyer and seller without the use of smart contract technology. Without using a smart contract, a third party (i.e., banks or credit cards) has to connect the transaction between the buyer and the seller. It can be time-consuming and the company might take commissions that further increase the price of the product, which is not ideal for a buyer.

Figure 9 shows a visual representation of how a simple transaction occurs between a buyer and seller using smart contract technology. When a smart contract is used to complete a transaction, the need for a third party to link the buyer and seller is eliminated. The buyer and seller will execute the transaction directly. The transaction takes place as soon as the buyer clears the transaction status and the seller receives the transaction.

3. Results and Analysis

3.1. Frontend. All of our system's front-end activities will be regulated by our website. Figure 10 shows our website's front end, which includes a homepage and Figure 11 shows the login page. The homepage has a few options to link to our support page (such as Facebook, Google Plus, Twitter, and LinkedIn). The "Login tab" has a login prompt where the user can choose one of three account categories to log into. There will be an "Admin Account" for the administrator of

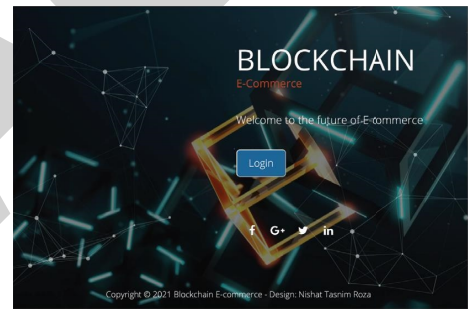


Figure 10: Website home page.

the system, "Buyers Account" for the buyers, and "Sellers Account" for the sellers. Each user requires a fixed e-mail address or username and a password to log in to their corresponding accounts. A "Logout" initiates a logout system and returns to the home page of the website.

Figure 12 shows the administrator's dashboard. When a system administrator logs in, they will be taken to an admin dashboard. The administrator has complete power over all accounts. Separate tabs on the admin dashboard show all of the buyers and sellers. The "Buyer Accounts" and "Seller Accounts" tabs show all the buyers and sellers, respectively. The "Transaction" tab keeps track of all the transactions that have taken place. The administrator has real-time access to all the transaction data and can control it. The "Create Account" tab in the admin account allows them to fill out a registration form to create a new user of some kind.

Figure 13 shows the user registration form. The admin account has a "Create Account" tab, where they can fill out a registration form to create a new user of any type. The admin enters the user's first and last names, gender (male, female, or other), account type (admin, buyer account, or seller account), password, and address. The new user must read the terms and conditions before selecting the boxes. After inputting all the required fields in the form, the account will be created.

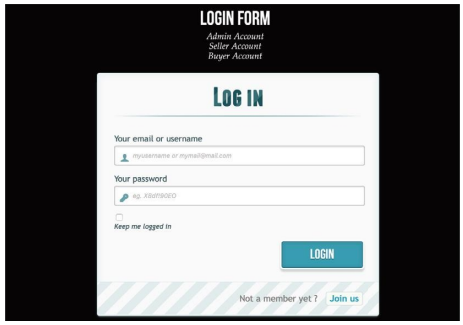


Figure 11: Website login page.

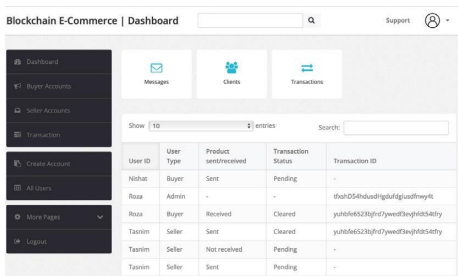


Figure 12: Admin dashboard.

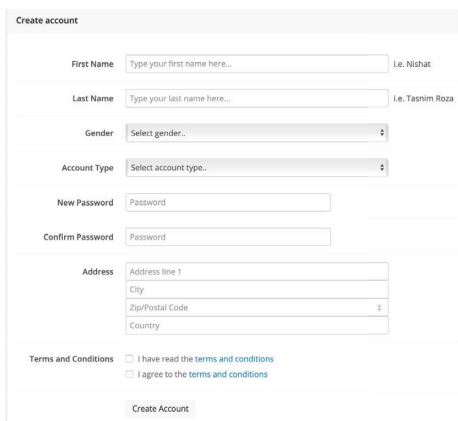


Figure 13: User registration form.

The sellers will log in to the seller dashboard. The seller's dashboard has a tab that displays all the products they have sold, a tab that shows all the product details, a tab that shows the transaction status of the products, and a tab that stores the seller's reviews.

Figure 14 shows the buyer's dashboard. The buyers will log in to the buyer's dashboard. The buyer's dashboard has a tab that displays all the products they have purchased, a tab that shows the transaction status of the products, and a tab where they can post their reviews of the products and the buyer they have purchased from. Figure 15 shows the buyer's review form. This review is important for the smart contract to function. If the review sent by the buyer is positive, implying the product they received was received in good condition, the transaction status will be cleared. After clearance, the transaction will successfully take place. As the

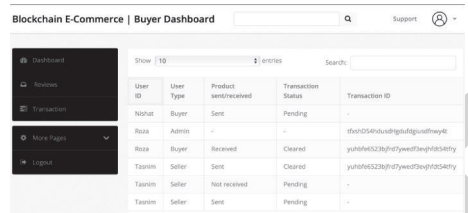


Figure 14: Buyer dashboard.

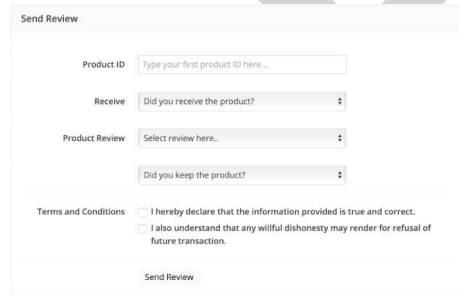


Figure 15: Buyer review form.

transactional data is passed to the Postman API function, a new block will be mined following the steps discussed in section 2.2. However, if the review sent by the buyer is negative, the transaction status will not be cleared, the product will be sent back to the seller, a new block will not be created, and the seller review database will be updated. The seller will not receive any transaction.

3.2. Backend. The backend is where we implemented the blockchain aspect of the system. Figure 16 shows the blockchain after mining a few transactions. The data for mining the transaction block is obtained from the website. After the transaction status is cleared for a transaction, the transactional data is posted via an API mine call using an HTTP request by Postman. This data is used as an attribute for mining the block. After the block is successfully mined, it holds all the attributes a block should have. The last hash of the current block correctly refers to the previous block. Furthermore, the blockchain needs to be validated by the other nodes of the network before the new block can be added and the blockchain can be replaced.

We have implemented the proof-of-work system by writing a script that checks how well the dynamic difficulty adjusted the system to approach the mining rate. After successful mining and successfully showing the proof-of-work, the new block is appended to the end of the blockchain. The whole chain is checked before updating the whole blockchain. The old blockchain is replaced with a new chain. Figure 17 shows that the blockchain is replaced by the most recently updated blockchain.

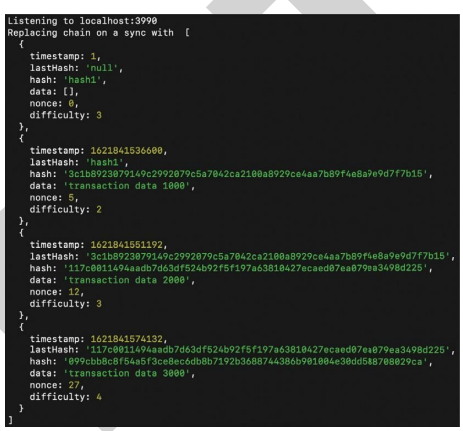
We have created a broadcast function that broadcasts the whole blockchain across the network. Using that function, everyone across the blockchain network is synced with the updated blockchain. Figure 18 shows a new instance of a new user who is synced with the updated blockchain even though they joined the network after the blockchain was already

```
[
    "timestamp": 1,
    "lastHash": "null",
    "hash": "hash1",
    "data": [],
    "nonce": 0,
    "difficulty": 3
},
{
    "timestamp": 1621841536600,
    "lastHash": "hash1",
    "hash": "3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15",
    "data": "transaction data 1000",
    "nonce": 5,
    "difficulty": 2
},
{
    "timestamp": 1621841551192,
    "lastHash": "3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15",
    "hash": "117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225",
    "data": "transaction data 2000",
    "nonce": 12,
    "difficulty": 3
},
{
    "timestamp": 1621841574132,
    "lastHash": "117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225",
    "hash": "099cbb8c8f54a5f3ce8ec6db8b7192b3688744386b901004e30dd588708029ca",
    "data": "transaction data 3000",
    "nonce": 27,
    "difficulty": 4
}
```


Figure 16: The blockchain after mining the third transaction.

```
Replacing chain with new blockchain: [
  {
    timestamp: 1,
    lastHash: 'null',
    hash: 'hash1',
    data: [],
    nonce: 0,
    difficulty: 3
  },
  {
    timestamp: 1621841536600,
    lastHash: 'hash1',
    hash: '3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15',
    data: 'transaction data 1000',
    nonce: 5,
    difficulty: 2
  },
  {
    timestamp: 1621841551192,
    lastHash: '3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15'
,
    hash: '117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225',
    data: 'transaction data 2000',
    nonce: 12,
    difficulty: 3
  },
  {
    timestamp: 1621841574132,
    lastHash: '117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225'
,
    hash: '099cbb8c8f54a5f3ce8ec6db8b7192b3688744386b901004e30dd588708029ca',
    data: 'transaction data 3000',
    nonce: 27,
    difficulty: 4
  }
]
```


Figure 17: Blockchain is replaced with new blockchain.



```
Listening to localhost:3990
Replacing chain on a sync with  [
  {
    timestamp: 1,
    lastHash: 'null',
    hash: 'hash1',
    data: [],
    nonce: 0,
    difficulty: 3
  },
  {
    timestamp: 1621841536600,
    lastHash: 'hash1',
    hash: '3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15',
    data: 'transaction data 1000',
    nonce: 5,
    difficulty: 2
  },
  {
    timestamp: 1621841551192,
    lastHash: '3c1b8923079149c2992079c5a7042ca2100a8929ce4aa7b89f4e8a9e9d7f7b15',
    hash: '117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225',
    data: 'transaction data 2000',
    nonce: 12,
    difficulty: 3
  },
  {
    timestamp: 1621841574132,
    lastHash: '117c0011494aadb7d63df524b92f5f197a63810427ecaed07ea079ea3498d225',
    hash: '099cbb8c8f54a5f3ce8ec6db8b7192b3688744386b901004e30dd588708029ca',
    data: 'transaction data 3000',
    nonce: 27,
    difficulty: 4
  }
]
```


Figure 18: Everyone on the network has the updated blockchain.

created. This will happen to any future users. Even if a new user joins the network with a different PORT, they will instantly receive the most recently updated blockchain. The system is optimized to prevent redundant interactions.

The blockchain, joined with the smart contract, will revolutionize the future of e-commerce. We have combined blockchain technology to ensure data security and user privacy with smart contracts to ensure that the protocol for the transaction is maintained. Our design system can be used by any e-commerce website. It will run smoothly and efficiently to prevent issues concerning data security and integrity from the traditional transaction process. All the transactional data is transferred securely and efficiently.

Table 1: Comparison chart.

	Transactional privacy
This paper	Smart contract
Ref [16]	Hawk
Ref [17]	Ethereum
Ref [20]	Ethereum
Ref [21]	Smart contract

Table 1 shows the comparison between this paper and other research papers. This paper only implements smart contract for providing transactional privacy. Kosba et al. [16] use Hawk, a decentralized smart contract that provides transactional privacy as the smart contract is written privately without any cryptography. Wood [17] uses the Ethereum platform to provide transactional privacy. In [20], blockchain has been applied for electronic health record security. Smart contract has been used for smart supply chain management in [21].

4. Conclusion

The system that was designed uses blockchain technology and smart contract to maintain transactional data integrity and security for any e-commerce platform. Our system was successfully developed and implemented, and it is capable of resolving data security and integrity issues with an existing framework by utilizing Blockchain Technology and the Smart Contracts feature. The transactional data is safely transmitted across the network.

As demonstrated in our research, blockchain technology coupled with smart contracts is a very powerful tool. Blockchain provides us with a decentralized and distributed network and the ability to transmit data across the whole network in a trustless manner without third party interference. Smart contract enabled us to program complicated processes and reduce redundant work.

Our system is not only confined to e-commerce platforms it can be implemented across a variety of applications. With enough resources, we can build a state-of-the-art structure that will be sufficient to minimize cyber security complications in the future. Blockchain technology has the potential to be used for a variety of other applications in the future, including telemedicine, healthcare, banking, and others.

Data Availability

No data were utilized to support these research findings.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This research was funded by the Deanship of Scientific Research at Taif University, Kingdom of Saudi Arabia, through Taif University Researchers Supporting Project Number (TURSP-2020/265).

References

[1] K. Roy, N. Islam, T. Khan, and M. M. Khan, "A novel approach to data storage using blockchain technology," *International Conference on Information Technology (ICIT)*, pp. 245–250, 2015.

[2] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[3] G. Zyskind, O. Nathan, and A. '. Pentland, "Decentralizing privacy: using blockchain to protect personal data," *Security and Privacy Workshops*, pp. 180–184, IEEE, San Jose, CA, USA, 21 May 2015.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[5] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[6] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 2014–2026, 2014.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the International Congress on Big Data (BigData Congress)*, pp. 557–564, IEEE, Honolulu, HI, USA, 25 June 2017.

[8] R. Dennis and G. Owen, "Rep on the block: a next generation reputation system based on the blockchain," in *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 131–138, IEEE, London, UK, 14 December 2015.

[9] S. Fujimura, H. Watanabe, A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "Bright: a concept for a decentralized rights management system based on blockchain," in *Proceedings of the 5th International Conference on Consumer Electronics-berlin (ICCE-Berlin)*, pp. 345-346, IEEE, Berlin, Germany, 6 September 2015.

[10] X. Zhu and D. Wang, "Research on Blockchain application for e-commerce, finance and energy," *IOP Conference Series: Earth and Environmental Science*, vol. 252, no. 4, pp. 1–6, Article ID 042126, 2019.

[11] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?-A systematic review," *PLoS One*, vol. 11, no. 10, 2016.

[12] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *Proceedings of the 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30, IEEE, Vienna, Austria, 22 August 2016.

[13] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, 2016.

[14] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Wang, "An overview of smart contract: architecture, applications, and future trends," in *Proceedings of the Intelligent Vehicles Symposium (IV)*, pp. 108–113, IEEE, Changshu, China, 26 June 2018.

[15] P. Ryan, "Smart contract relations in e-commerce: legal implications of exchanges conducted on the blockchain," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 14–21, 2017.

[16] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the Symposium on Security and Privacy (SP)*, pp. 839–858, IEEE, San Jose, CA, USA, 22 May 2016.

[17] G. Wood, "Ethereum: a secure decentralized generalised transaction ledger," http://gavwood.com/paper.pdf.

[18] Yi Lim, H. Hashim, N. Poo, D. Poo, and H. Nguyen, "Blockchain technologies in E-commerce: social shopping and loyalty program applications," https://www.researchgate.net/publication/332977375_Blockchain_Technologies_in_E-commerce_Social_Shopping_and_Loyalty_Program_Applications.

[19] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, "Have a snack, pay with Bitcoins," in *Proceedings of the International Conference on Peer-to-Peer Computing*, pp. 1–5, IEEE, Trento, Italy, 9 September 2013.

[20] K. T. Akhter Md Hasib, I. Chowdhury, S. Sakib et al., "Electronic health record monitoring system and data security using blockchain technology," *Security and Communication Networks*, vol. 2022, pp. 1–15, Article ID 2366632, 2022.

[21] M. D. Turjo and M. M. Khan, "Smart supply chain management using blockchain and smart contract," *Scientific Programming*, vol. 2021, pp. 1–12, Article ID 6092792, 2021.