Hindawi
Journal of Advanced Transportation
Volume 2020, Article ID 8854082, 14 pages
https://doi.org/10.1155/2020/8854082

WILEY | Hindawi

Research Article

Research on a Shared Bicycle Deposit Management System Based on Blockchain Technology

Daozhi Zhao,[1] Di Wang ,[1] and Baosen Wang[2]

[1]*College of Management and Economics, Tianjin University, Tianjin 300072, China*
[2]*School of Economics, Beijing Wuzi University, Beijing 101149, China*

Correspondence should be addressed to Di Wang; wangdi666@tju.edu.cn

Received 17 June 2020; Revised 23 July 2020; Accepted 21 August 2020; Published 3 September 2020

Academic Editor: Aijun Liu

As a green travel mode, bike sharing is developing rapidly across China. At present, charging deposits from users is the common operation mode adopted by shared bicycle enterprises. The large number of shared bicycle enterprises generates fierce market competition, and the eliminated enterprises always refuse to return user deposits. Even regular running enterprises still have trouble with the immediate return of deposits. This situation severely affects the reputation of shared bicycle enterprises, and concerns have been shared widely across the society. Meanwhile, there is a general expectation among users that their deposits could be refunded timely and a broad appeal for technical management to resolve this problem. This article uses blockchain technology to reform the current management mode for shared bicycle deposits and constructs a decentralized, user information and deposit visualized, and multidimensional supervised management system. The proposed management system makes the real-time flow direction supervision of user deposits to be realized. Furthermore, a smart contract of shared bicycle deposits with punishment mechanism is also designed. Finally, the differences between the proposed deposit management mode and the current deposit management mode are analyzed, and a simulation experiment is conducted. In the simulation experiment, the deposit theft rate of our deposit management system is 0%, which is far better than the two existing bike deposit management systems. The results show that the outstanding advantages of the proposed deposit management mode, which include improving deposit supervision and guaranteeing user deposit security, are also conducted. This article has made effective technical management exploration to reduce deposit management risks and improve deposit management institutions for shared bicycles. It has important practical reference value for accelerating the sustainable development of shared bicycle enterprises.

1. Introduction

After its introduction to the China market at 2016, bike sharing, with vigorous support from the government, has become an indispensable part of urban green public transport system [1]. According to the statistics, shared bikes are distributed in over 200 cities in China; the highest daily usage of shared bikes has surpassed 700 million person-times [2]. Shared bicycles positively affect low-carbon transportation and environmental protection. Nevertheless, the common drawbacks such as not open, not transparent, not visible, and delay refund of the current deposit management mode of shared bicycles have aroused the anxiety of users. In this situation, the reputation damages and widespread criticisms toward shared bicycle enterprises are inescapable.

After fierce competitions for the occupation of market shares among numerous shared bike enterprises, the failed enterprises exit markets and refuse to return user deposits. According to the statistics, up to 25 million-yuan deposits belong to about 125,000 users which could not be returned after the bankruptcy of "Xiao Ming" shared bikes in June 2018. The well-known company OFO has also been exposed as having difficulty for the deposit refund. According to the incomplete statistics, the number of active users of shared bikes in China had grown to 221 million [3], and the deposit scale of shared bikes can reach 40 billion yuan. Meanwhile, several shared bike enterprises have embezzled user deposits

to invest and manufacture more bicycles [4]. This situation has raised concerns among the majority of users.

Currently, the lack of a scientific deposit management mode is a common problem among shared bicycle companies. The drawbacks of deposit management have caused social contradictions between enterprises and users, severely impaired the reputation of shared bike enterprises, and restricted the sustainable, healthy development of the bike-sharing industry. Meanwhile, there is a widespread appeal for protecting the legitimate rights and interests of bicycle users. Thus, establishing a wholesome, scientific management system for shared bike deposits has aroused great concern from the government and the academic community.

On May 16, 2019, "user deposit administrative measures for the new industry forms of communication and transportation (trial)" was jointly issued by the Ministry of Transport, People's Bank of China, National Development and Reform Commission, Ministry of Public Security, State Administration for Market Regulation, and China Banking Regulatory Commission (http://www.mot.gov.cn/zxft2019/xinyetgl/). This measure enacted detailed regulations toward the management of user deposit and advance fund for internet bicycle rental and made requests such as "store and manage by special account, earmark funds for specified purpose only" and "immediate deposit for rental, immediate refund for return." Meanwhile, this measure pointed out that detailed management measures for user deposits should be carried out as soon as possible, and the rights and obligations of all parties should be clarified to strengthen the management of user deposits, prevent user deposit risks, guarantee legitimate rights and interests of users, and promote the healthy development of new industry forms of communication and transportation.

Under these circumstances, it is widely expected that the deposit management mode of shared bicycle enterprises will be reshaped with advanced technology. As the underlying technology of bitcoin [5, 6], blockchain has the characteristic of decentralized data storage and tamper-resistant data [7, 8]. Due to its outstanding advantages for supervising digital asset trading, the blockchain technology has been used to build transparent information management platforms for financial and medical institutions [9, 10]. At the Politburo Meeting, Jinping Xi pointed out that "we should take blockchain as an important breakthrough in independent innovations of core technologies and accelerate the promotion of technological reform and industrial innovation"(http://paper.people.com.cn/rmrb/html/2019/10/26/nw.D110000renmrb201910262-01.htm). Evidently, how to develop and apply blockchain technology has been appreciated at the national level of China.

If the system can be equal and without privilege, it can reduce the opportunism behavior of relevant enterprises. Trading information in blockchains cannot be tampered, and it is traceable. Users could check their balance at any time by using a private key. Meanwhile, supervision organizations have access via a public key to monitor the trading data and capital pools. These merits solve the asymmetrical problems of trade information and effectively ensure the safety of user deposits. Furthermore, this paper designs a smart contract to regulate the behavior of enterprises and users in real time. Finally, with a simulation experiment, this paper shows the deposit theft rate of the system which is 0%, which verifies its security and effectiveness.

This article is organized as follows: in Section 1, we introduce the research background and main research content. In Section 2, we introduce related research reviews of shared bicycle deposit, blockchain technology, and smart contract. In Section 3, we construct a management system of shared bicycle deposits based on blockchain technology and introduce the process of data upload and encryption, transaction data storage, verification methods of payment information, and smart contract. In Section 4, the safety performance index of the management system for shared bicycle deposits is illustrated, and experimental simulation and numerical analysis are conducted. Section 5 gives the research conclusion. Section 6 gives future research and applications.

2. Literature Review

2.1. Shared Bicycle Deposits. Since shared bicycle services entered the China market, collecting user deposits has become a common operation procedure for shared bicycle enterprises [11, 12]. For example, Mo-bike charges 299 yuan as deposit from each user [13], and the deposits charged by OFO and Bluegogo are 199 yuan and 99 yuan, respectively [14, 15]. Different viewpoints for the property of shared bicycle deposit are held by the academic community. Deemed by Chen et al. [16], users and shared bicycle enterprises formed a rental relationship, and the deposit was the guarantee fund for users to rent bikes. The property of deposit was discriminated from a legal perspective by Marselli [17], and charging deposit was deemed to be a disguised form of financing. Hence, fund custody regulations should be carried out to provide supervision for the shared bicycle deposits. Deemed by Nakamura and Abe [18], the manufacturing and operating costs of shared bicycles were very high, and normal running of related enterprises could not be maintained merely by charging low use fee. And deemed by Vallurupalli and Bose [19], using the deposits to reinvest is the main source of profit for the enterprises.

According to this paper, the purpose of enterprises for charging deposits is to insure proper and reasonable use of shared bicycles by the users and guarantee priority compensation to enterprises when bicycles are deliberately damaged by the users. However, the supervision system for shared bicycle deposits is outdated, which has created a series of problems.

First of all, different with the common rental mode, shared bicycle users not always apply for deposit refund immediately after they return shared bicycles. This situation will result in a shared bicycle is bounded with multiple user

deposits. It brings enormous sum of funds to the deposit pools of enterprises. Secondly, the flow directions of huge deposits are opaque, and there is a risk of corporate misappropriation. Furthermore, the current shared bicycle deposit system fails to achieve the purpose of restraining misconducts of users, and the phenomena of damaging and hiding shared bicycles occur occasionally.

Deemed by us, the reasonability of charging user deposits remains controversial and should be determined by the current industry conditions and legal institutions. However, users have the rights to check the flow direction of deposits, and enterprises should refund deposits timely under the requests of users. Therefore, the realization of the transparency and publicity of deposit flow direction is a problem demanding prompt solution. This article uses blockchain technology to resolve the shortcomings of the current shared bicycle deposit management system. It sets up a specified account for deposit, prevents enterprises from concealing and transferring user deposits, and fulfills the user demands of checking the flow direction of deposit in real time.

2.2. Blockchain. Blockchain is the underlying technology of bitcoin developed by Nakamoto [20]. Its essence is that everyone participated and is trustworthy, secure, and a shareable encrypted distributed account book [21]. Each new transaction is packaged into a block and linked to the previous block after being confirmed by the majority or all nodes in the system. It forms a valid, tamper-proof part of the data layer [22]. Also, there is no central institution with special rights in the application of blockchain technology, and there are no privileges between participants [23]. Blockchain technology could provide strong technical support for the establishment of safe and transparent application systems in this age of gradual virtualization of money and gradual digitization of assets [24–26]. The blockchain technology has the following advantages.

(i) Decentralization [27]: blockchain-based applications could eliminate the intermediate links of transaction processes, and they do not need the arbitration and management of a third party. Meanwhile, any node could participate in the process of information validation; however, no node could control blockchain individually. (ii) Tamper resistance: blockchain technology uses hash algorithm to store data information, that means the data is hard to tamper with [28]. Any node that tampers or adds invalid data will be detected by the system as a potential threat. (iii) Transparency: information on blockchain is open and transparent due to system-validated nodes could view data in the data layer at any time [29].

The blockchain technology is changing the application of digital currency. In 2017, the donation query system was established based on blockchain technology by Alipay charity donation platform to guarantee the reasonable use of donation (http://www.sohu.com/a/122224160_254472). In 2018, based on the real transaction data and running resources in a supply chain scenario, by the use of blockchain technology, Tencent company released "Tencent blockchain + supply chain finance solutions," which enabled to improve the financing difficulties of small, medium, and microcompanies and support the transformation and upgrade of local industries (https://tech.qq.com/a/20180413/012603.htm). Li et al. [30] proposed P2P cloud storage network, which could realize transfer and sharing of data by users without having to rely on third-party data providers. Zyskind and Nathan [31] proposed cloud storage solutions based on blockchain to improve the data storage security.

2.3. Smart Contract. Smart contract is a contract performed automatically on blockchain and programmed in the form of code [32]. The essence of the smart contract is a digital formally defined commitment containing trigger conditions and execution results [33]. The data storage and reading processes of blockchain are transparent and tamper-resisted. These merits of blockchain could provide underlying technical support for running of the smart contract [34, 35], and the development of the smart contract makes it possible to monitor digital currencies in real time.

The smart contract based on blockchain technology could replace original arbitration and enforcement processes, not only reduce the arbitration enforcement costs but also avert the interference of human factors, and minimize fraud losses. The nodes in blockchain conform to the vested provisions of the smart contract and are punished by the smart contract based on the performance of violations.

This article establishes a deposit management system for shared bicycles by the use of blockchain and smart contract technologies, with aims to monitor the conducts of enterprises in real time, eradicate the misconducts of enterprises, eliminate the possibility of disguised financing in the bike-sharing industry, and guarantee scientific running of the shared bicycle service system.

3. Shared Bicycle Deposit Management System

The core which sets shared bicycle use right as exchange exists in the shared bicycle system [36]. This section constructs a blockchain deposit management system for shared bicycles based on different authorities and responsibilities for the three nodes of enterprises, users, and supervisory organizations around this core. As shown in Figure 1, this system contains a data layer, network layer, and consensus layer.

As can be seen from the figure, in the data layer, the blocks constitute a blockchain according to the occurrence of the time sequences of transactions and guarantee the safety of data stored in the blockchain by the utilization of SHA256 algorithm [37] and Merkle hash value [38]. In the network layer, the nodes are connected with a flat topological structure, and there is no centralized node. Meanwhile, related nodes could view data of any node in the network layer by using a public or private key. As shown in the consensus layer, all the nodes of the network layer should comply with the enacted rules and conform to the identical smart contract. This section individually introduces the four important composing structures: uploading and encryption

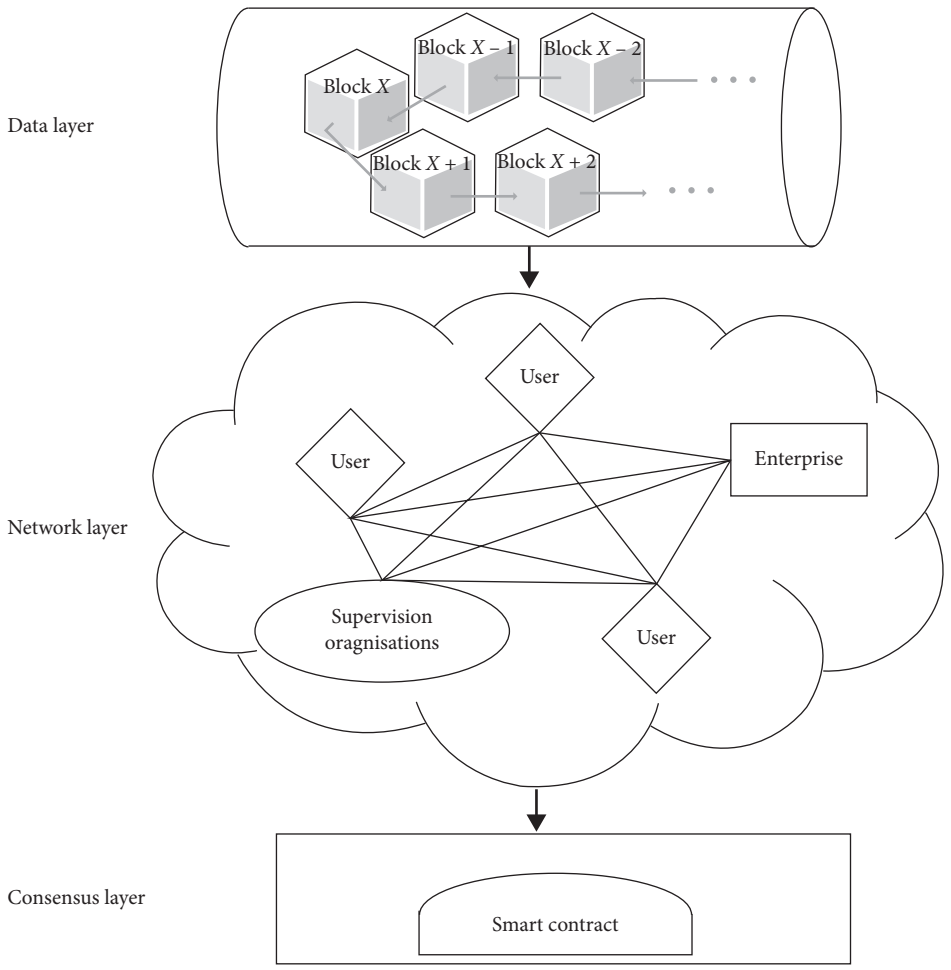

Figure 1: Blockchain shared bicycle deposit management system.

of the data of shared bicycle users, transaction data of users use shared bicycle store, verification of payment information for deposit refund, and smart contract for deposit transfer according to the usage flow of shared bicycles.

3.1. Uploading and Encryption of the Data for Shared Bicycle Users. After shared bicycle users log in and access the nodes of the client, the basic information containing user identities, locations, and so on, is compressed as 32 MB file package and stored in the node block of users. The submitted deposits of registration, the resulting cost record, and transaction data for bicycle using are also preserved in the user block. As shown in Figure 2, each block is composed of a block head and a block body [39]. The block head contains block number, hash value of the previous block, Meckel root, and time stamp [40], and the block body contains all the target transaction lists [41]. The hash value of the previous block ensures the trading order of blockchain, and the Meckel root hash value ensures the authenticity of the transaction record in the blocks. The blocks link together orderly according to the order of trading time, and each block cites the previous block via the "hash value of previous block" of its block head, in turn creating an integral chain of blocks.

The encryption and decryption processes of blocks rely on the RSA and elliptic curve cryptosystem [42]. In our deposit management system for digital signatures and the locking and unlocking of script, the generation of private and public keys is realized with the secp256k1 curve asymmetric encryption algorithm that was proposed by Pote et al. [43]. Encryption code for the private key and public key is given in Algorithm 1.

The private key is secretive, and the public key is available systemwide. The nodes after identity authentication could view data information by the utilization of the public key for the verification of integrity degree and reliability. Especially, this proposed system implants privacy into the permission design of nodes. In this situation, the basic information of users could only be consulted by themselves, and other nodes could only check trading information by the use of the public key. Hence, the privacy of personal information, asset status, and credit status of users could be guaranteed. Decryption code for the private key and public key is given in Algorithm 2.

3.2. Store Transaction Data for Shared Bicycle Using of Users. Merkle tree is used to store transactions taking place in the user node blocks in the proposed deposit management

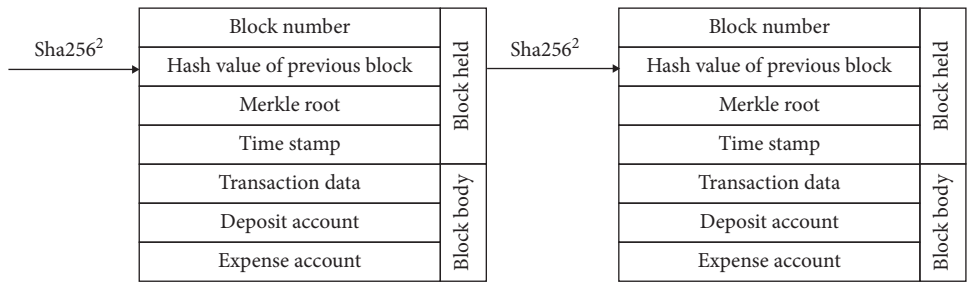

Figure 2: Block structure.

```
Package encryp
import {
    “crypto/rand”
    “crypto/rsa”
    “crypto/x509”
    “encoding/pem”
    “errors”
}
    var privateKey = []byte(`
    —begin RSA private key—
    var publicKey = []byte(`
    —begin public key—
    —end public key—
```

Algorithm 1: Encryption code for private key and public key.

```
//Decry the public key in pem format
    block, _ := pem.Decode (publicKey)
    if block == nil {
        return nil, errors.New (“public key error”)
    }
    // Parsing the public key
    pubInterface, err := x509.ParsePKIXPublicKey(block.Bytes)
    if err != nil {
        return nil, err
    }
    // Type discriminant
    pub := pubInterface.( * rsa.PublicKey)
    //Encryption
    return rsa.EncryptPKCS1v15 (rand.Reader, pub, origData)
}
// Decryption
func RsaDecrypt (ciphertext []byte) ([]byte, error) {
    // Decryption
    block, _ := pem.Decode (privateKey)
    if block == nil {
        return nil, errors.New (“private key error!”)
    }
    //Resolves the private key in PKCS1 format
    priv, err := x509.ParsePKCS1PrivateKey (block.Bytes)
    if err != nil {
        return nil, err
    }
    // Decryption
    return rsa.DecryptPKCS1v15 (rand.Reader, priv, ciphertext)
}
```

Algorithm 2: Decryption code for private key and public key.

system. Merkle tree is a kind of hash binary tree, which could conclude and check the integrity of large-scale data rapidly [44]. As shown in Figure 3, six transactions are hypothesized to exist in a user node block, with hash values of H_1~H_6. Each hash value is stored in a "leaf" node [45], and all nodes of the same level are divided into groups with two nodes. The hash values of nodes in the same group are tandem calculated by the hash algorithm until the top root node is only left over. The hash value stored in the root node is the Meckel root hash value. The above procedure is described by formulas as follows:

$$H_{12} = \text{sha256d}\ (H_1 + H_2)$$
$$H_{34} = \text{sha256d}\ (H_3 + H_4)$$
$$H_{56} = \text{sha256d}\ (H_5 + H_6)$$
$$H_{1234} = \text{sha256d}\ (H_{12} + H_{34})$$
$$H_{123456} = \text{sha256d}\ (H_{1234} + H_{56})$$

The system performs Algorithm 3 for the hash calculation of each transaction to generate leaf hashes. Merkle tree like Figure 3 is established, and Merkle root is also calculated according to the leaf hashes.

As shown in Figure 4, differing from the current bike-sharing system, the trading information of the proposed deposit management system is not stored in shared bicycle enterprises or specific nodes but in the node blocks where transactions are taking place. The number of blocks is a series of hash values without regularity [46]. The hash values of the previous blocks are stored in the current blocks and are used to connect all blocks to form a chain structure.

When a new block is generated in the system, all nodes will add it to their own blockchains to guarantee data integrity. The heights of blocks are associated with their sequential order of joining blockchain. Block joined earlier has less height, and blocks joined later have more height. The data storage of the chain structure is orderly as the traditional account book and could give early warning towards the modification of block data. By checking the previous block hash value stored in the latter block, users could estimate whether the block data have been tampered.

The hash values of block heads are obtained by calculating the trading information of block bodies, and the hash values of block heads change accordingly when trading information is deleted or tampered. Thus, nodes could check the account security by observing hash values, which can reduce the probability of data tampering. As can be seen in the program, when certain information is deleted, the Merkle root of a block body changes, and the hash value of a block head varies accordingly (Algorithm 4).

The blockchain technology makes the transaction conducts between users and enterprises to be a distributed account book and solve the opacity problem of information between users and enterprises. Consequently, introducing blockchain technology to the deposit system of shared bicycles could realize the tamper-proof property of trading information.

In the proposed system, all transactions related to shared bicycles could be caught, and supervision organizations could comprehend the using condition of any user at any time and location, as well as the flow direction of any fund. Hence, this system could provide technical support to supervision organizations for authenticity checking of deposit refund for enterprises.

3.3. Verification of Payment Information for Deposit Refund. In the current bike-sharing system, purchasing and selling of shared bicycle use rights have nothing to do with supervision organizations. Comparing with the nodes of enterprises and users, the nodes of supervision organizations are incomplete with the function of payment information checking. The proposed system endows the nodes of supervision organizations with Simplified Payment Verification (SPV) permission [47] so that supervision organizations could check the existence of any payment in the network, as shown in Figure 1.

As indicated in Section 3.2, the transactions between users and enterprises will be saved in the transaction data package of block bodies and in the block heads as the hash values of the Merkle root by virtue of the hash algorithm. If the deposit is really refunded to user A by a related enterprise, the resulting transaction record will be saved in the block body, and the hash value of this block and the "hash value of the previous block" stored in the latter block head will change simultaneously. As shown in Figure 5, supervision organizations need to verify the hash value authenticity of H_{1234}, H_{12}, and H_3 to check the authenticity of Transaction 4. If the calculated hash value, according to the Meckel number path of the latter block by related supervision organization, is identical with the hash value of the user A block, Transaction 4 is verified.

The supervision organizations perform Algorithm 5 to compare the Merkle root of user A calculated by them with the Merkle root submitted by the shared bicycle enterprise. If the two Merkle roots are equal, confirming no transaction was false, returning of deposit to user A could be verified. On the contrary, if the two roots are not equal, a selective packet dropping attack would take place in the enterprise reports, confirming the enterprise has not returned the deposit to user A. Original hash sent by the shared bicycle enterprise is denoted with the symbol (').

Overall, the verification of enterprises' deposit refunds conducted by supervision organizations is simplified as verifying whether the two Merkle roots are equal. Therefore, this system provides a scientific, convenient checking mode to supervisory organizations. Simplified Payment Verification (SPV) could enhance the supervisory force of the government and remove the advantage of information asymmetry from enterprises.

The shared bicycle deposit management system based on blockchain technology could ensure visuality of trading data, tamper-proof property of generating the transaction, and checking of the authenticity of payment information. It could also realize automatic supervision of the conduct of enterprises and users via the vsmart contract to guarantee their legitimate rights and interests.

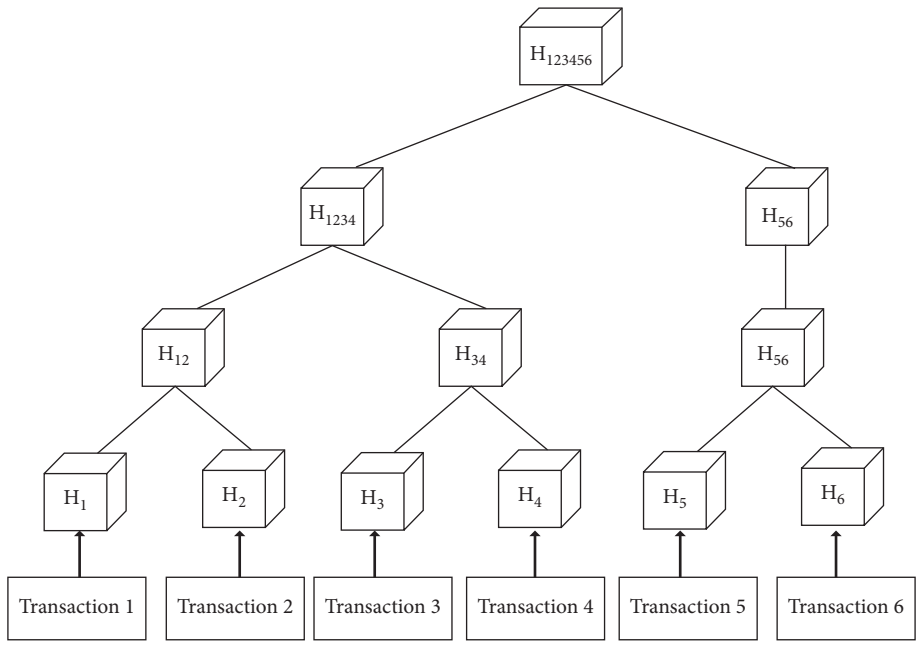

Figure 3: Merkle tree.

```
(1) READ: Transactions
(2) For all transactions
(3) hash[i]=create Hash(transaction[i])
(4) For all hashes in each level
(5) if number of hashes = even then
(6)     Hash[i]=create Hash(hash[i]+hash[i])
(7) else
(8)     if! Last Hash then
(9)         hash[i]=create Hash(hash[i]+hash[i+1])
(10)    else
(11)        hash[i]=create Hash(hash[i]+hash[i])
(12)    end if
(13)    if level=last then
(14)        rootvalue=hash[i]
(15)    end if
(16) end if
```

Algorithm 3: Hash each transaction, build Merkle tree, and compute the Merkle root.

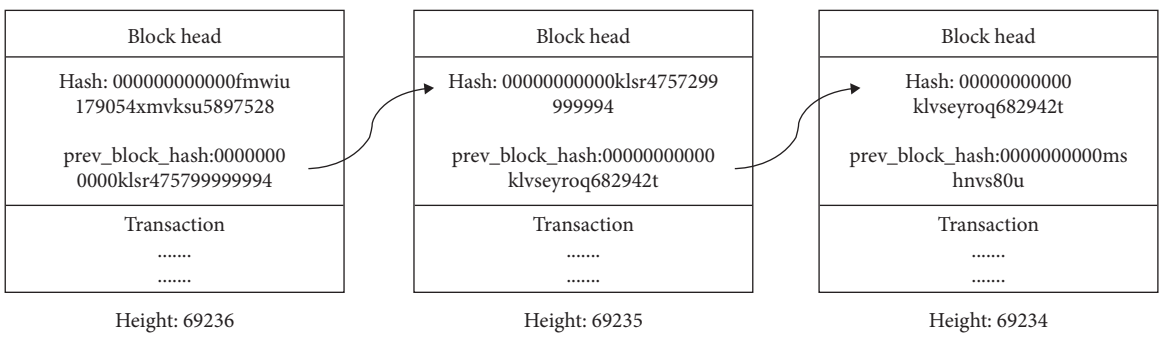

Figure 4: Blockchain structure.

```
#Delete the last transaction in the block transaction
>>>block.txs.pop()
>>>block
#The hash value of the block has changes
Block(hash:4r4i4nv5ny6m6iiih6i390u68b690b5m388569j40)
#The hash value of Meckel root has changes
>>>block.merkle_root_hash
'4n4u4nt843t3nv5394mtvj5m9vj54854v9i8v9vm034,f0j538'
```

Algorithm 4: Check the account security.

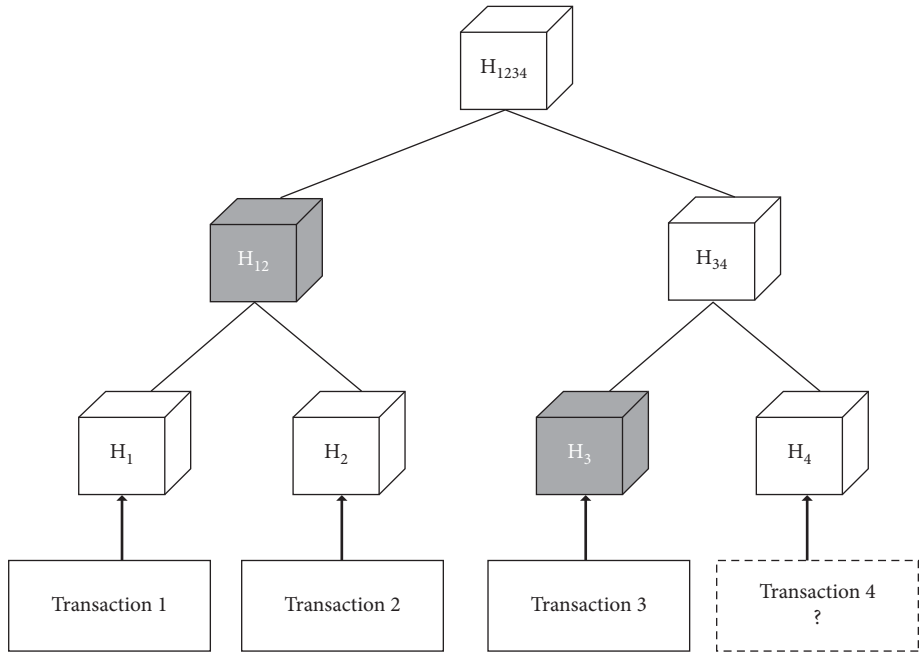

Figure 5: Supervision organizations verify transaction payments.

```
(1) READ: merkleRoot'
(2) if merkleRoot= merkleRoot' then
(3)     Transactions are all legitimate
(4) else
(5)     A selective transaction dropping attack has happened
(6) end if
```

Algorithm 5: Identify malicious paths.

3.4. Smart Contract for Deposit Transfer. Smart contract is the executed agreement among nodes in the blockchain technology [48]. Smart contract typically consists of properties, which contain statements and values and contract terms, trigger conditions, and corresponding response actions of which are linked by "if-then" conditionals [49, 50]. Ethereum uses gas to prevent unlimited contract execution as well as DoS attacks [51]. An account must enclose adequate amounts of gas to successfully call a contract function. Although the proposed system should be carried out based on a platform similar to Ethereum, the blockchain-based shared bicycle deposit management system designed by us theoretically supports all smart contract frameworks. For this reason, detailed gas consumption is not our primary consideration. However, we still optimized the system implementation to minimize operating costs.

In this system, the contract terms related to the enterprise and the users are designed in detail. Every transaction

between users and enterprises will be broadcasted in the blockchain network layer, which will be verified by each node and stored in the block. The operating mechanism diagram of the system smart contract is shown in Figure 6.

The smart contract could automatically supervise the flow direction of deposits. Specifically, enterprises can only use the deposits of users for predetermined purposes. As shown in trigger condition 1, if a deposit goes into a nondesignated account, the smart contract would automatically execute a punishment mechanism, locking deposit accounts of enterprises and recording negative information. Meanwhile, the smart contract could also be used to supervise trading information. When an enterprise updates a transaction record, the smart contract could verify it and the deposit value automatically and release this information to the network. Moreover, each transaction record is added to the node blocks when the conformity of the transaction and deposit value are verified by users. A smart contract could also automatically trigger a punishment mechanism, freeze circulating funds, and record negative information, as shown in the corresponding action 2. As shown in Contract Terms 1 and 2, this article demonstrates how a smart contract can be used to supervise capital flow directions and control the deposit usage permissions of enterprises. Smart contract could be used to supervise transaction information and standardize the operating behavior of enterprises. Thus, the possibility of disguising financing for shared bicycle enterprises can be ruled out, and the risk of out-of-control deposit management can be significantly reduced.

In addition, the supervision mechanism for the user conduct is also set in the smart contract. Users purchase the right to shared bicycle usage, not shared bicycle ownership. Thus, users are obliged to avoid damaging the shared bicycles, and maliciously damaging shared bicycles is strictly forbidden in the use rules of enterprises. Nevertheless, the damage conduct to shared bicycles of users occurs occasionally. In this situation, the proposed system binds the behavior of users with their deposits and sets conditions for permitting enterprises to transfer user deposits. After use, the shared bicycle will be checked. If a returned bicycle is not damaged, enterprises could transfer the use fee of users according to the corresponding action 3. Conversely, as shown in the corresponding action 4, if a shared bicycle is returned damaged, the smart contract can deduct a partial deposit from the user to compensate the account of the enterprise according to the damage level of the shared bicycle. Contract Term 5 shows the smart contract would transfer the entire user deposit of anyone who does not return a bicycle or seriously damages it in order to compensate the enterprise. The core code for smart contracts is shown in Appendix A.

4. Experiment and Analysis

This article sets the theft rate of deposit as the evaluation index of safety. The safety and effectiveness of the proposed system are analyzed by comparing its deposit theft rate with the current deposit management system of shared bicycles. In the following section, the experiment settings are first introduced. Then, the parameters of the deposit theft rate are introduced. Finally, simulation experiment is carried out, and related results are compared.

4.1. Experimental Setup. The experiment is conducted with Java1.8 on a desktop computer (Inter(R) Pentium(R) G34603.5 GHz, RAM4 GB, DISK1 TB, bandwidth100 MB/s) equipped with Windows 7 operating system.

4.2. Deposit Theft Rate of the Shared Bicycle Deposit Management System

4.2.1. The Current Deposit Management System for Shared Bicycles. The current deposit management systems for shared bicycles are mainly managed by enterprises or comanaged by enterprises and signing banks. These deposit management systems ensure the security of deposits by establishing an allopatric disaster preparedness system [52]. However, these systems have only one or two centralized nodes with high risk of being stolen since the breakdown of a single node will lead to the crash of the whole system [53]. The basic symbols of the deposit management system for shared bicycles are shown in Table 1.

In enterprise-led deposit management systems, deposits are stored in a central node. Once the node crashes, all deposits will be stolen, and the enterprise and users will suffer huge losses. The number of hacker attacks is shown as follows:

$$NAT_1 = f \cdot U \cdot p, \quad (0 \le NAT_1 \le CN). \tag{1}$$

The central node crashes when $NAT_1 = CN$; the deposit theft rate of the enterprise-led deposit management system is shown as follows:

$$T_1 = NAT_1 \cdot A. \tag{2}$$

In the deposit management system jointly managed by the enterprise and its signatory bank, the deposits are randomly stored in two central nodes and subject to a Poisson distribution with parameter $\lambda_1 = A/CN \cdot p$. In this system, the number of hacker attacks is shown as follows:

$$NAT_2 = \sum_{k=1}^{f \cdot U} \frac{\lambda_1^k \cdot e^{-\lambda_1}}{k!}, \quad (0 \le NAT_2 \le CN). \tag{3}$$

The deposit theft rate of system T_2 can be obtained by calculating the number of central nodes CN, the total amount of deposit accounts A, the probability of nodes attacked successfully p, and system security parameter η:

$$T_2 = NAT_2 \cdot \frac{A}{CN} \cdot p\eta. \tag{4}$$

According to (2) and (4), as the amount of deposit accounts increases, the rate of deposit theft increases. Thus, the two current types of the deposit management model are extremely insecure.

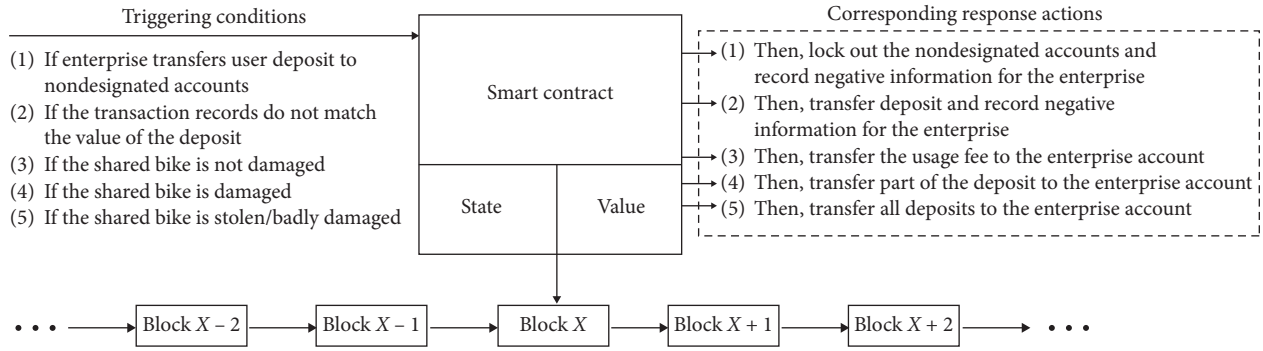

Figure 6: Operational mechanism of the smart contract.

Table 1: Basic symbols of the deposit management system for shared bicycles.

Symbol	Meaning
T	Deposit theft rate
NAT	Number of attacks
CN	Number of node centers
f	Percentage of malicious nodes
U	Number of users
p	Probability of a successful attack on a node
A	Amount of deposit accounts
m	Number of blocks
r	Number of copies of deposit accounts
n	Number of nodes
q	Number of fake blocks forged by an attacker
$m - q$	Actual number of blocks
Q	Probability of successful attacks on all blocks

4.2.2. The Deposit Management System for Shared Bicycles Based on Blockchain Technology. In the deposit management system for shared bicycles based on blockchain technology, there is no central node for storing user deposits. User deposits are stored in the deposit account of each block, and the copy of each user deposit account is randomly stored in the nearby block. In this system, the crash of a block does not affect the whole system; only more than half of the system blocks crashing at the same time would affect the whole system. In this system, the number of deposit accounts that hackers need to attack simultaneously is at least $m/2$, and the probability of correctly attacking the copy of each deposit account is $(r/m)^m$. If the number of blocks in the system is large enough, the probability of tampering the password to steal the deposit by a hacker is infinite close to 0.

To compare the proposed system with the two existing systems, this paper assumes that a hacker has successfully tampered the block with a serial number of z. The probability of tampering all blocks and stealing all deposit accounts by the hacker is as follows:

$$Q = \begin{cases} 1, & \text{if} m - q \le q, \\ \left(\dfrac{q}{m-q}\right)^z, & \text{if} m - q \le q. \end{cases} \tag{5}$$

According to the above formula, when the number of real blocks in the system is greater than the number of fake blocks, the probability of all deposit accounts being stolen by attackers decreases exponentially with the increase of blocks. When the number of real blocks is less than the number of fake blocks, suppose the process of forging fake blocks by the hacker obeys a Poisson process with parameter $\lambda_2 = z \cdot q/m - q$, the number of attack times needed by the hacker to tamper with the whole system NAT_3 is as follows:

$$NAT_3 = 1 - \sum_{k=0}^{z} \frac{\lambda_2^k \cdot e^{-\lambda_2}}{k!} \cdot \left[1 - \left(\frac{q}{m-q}\right)^{z-k}\right]. \tag{6}$$

The deposit theft rate of the blockchain shared bicycle deposit management system is

$$T_3 = NAT_3 \cdot \left(\frac{r}{n}\right)^m. \tag{7}$$

4.3. Simulation and Analysis. In the simulation experiment, the number of central nodes in the enterprise-led deposit management system CN is equal to 1. The probability of hacking the center node successfully by an attacker is set to 0.1. The number of central nodes in the deposit management system led by enterprises and signing banks CN is equal to 2, the security parameter of the deposit η is set to 0.9, and the probability of hacking the center node successfully by an attacker is set to 0.1. The number of copies of deposit accounts in the deposit management system of shared bicycles using blockchain technology is set to 3. As an extreme case, we set the number of blocks forged by the attacker as $q = n/3$. With the increase in the number of deposit accounts, the deposit theft rates for the three systems are shown in Figure 7.

As shown in Figure 7, when the amount of deposit accounts increases from 50 to 500, the deposit theft rates of three deposit management systems for shared bicycles T_1, T_2, and T_3 vary greatly. The security of the deposit management system led by enterprises is very low. Once the only deposit storage node is breached, the deposit theft rate T_1 is almost 100%, the system will crash, and all deposits will be stolen. For the deposit management system led by enterprises and signing banks, the deposit theft rate T_2 gradually increases with the increase in the amount of

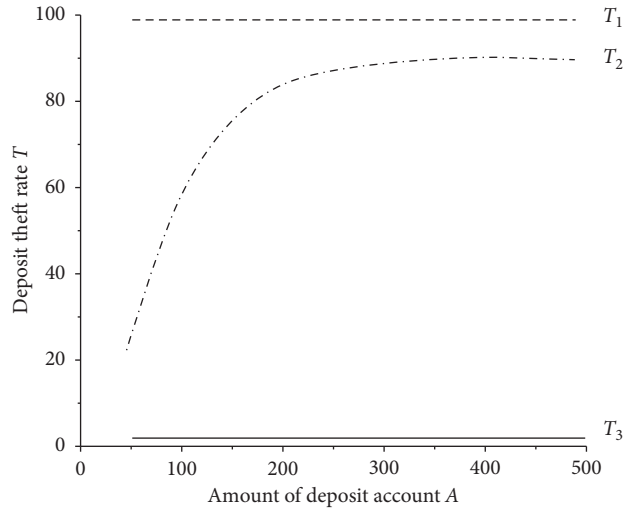

Figure 7: Operational deposit theft rate of the shared bicycle deposit management system.

deposit accounts. When the amount of deposit accounts is more than 200, the deposit theft rate tends to be 90%. For the blockchain-based shared bicycle deposit management system, the deposit theft rate T_3 is almost 0%, showing an outstanding performance in security.

5. Conclusion

As a green transportation mode, shared bicycles are experiencing rapid development all over China. However, the current management mode of shared bicycle deposits has several defects, such as the nonpublic storage of deposit, the opaque flow directions of deposit, and the delay in deposit refunds. These issues have aroused the dissatisfaction of shared bicycle users and wide attention from the society. To correct these defects in the deposit management mode of shared bicycles and promote the sustainable development of the service, this paper combines the concept of blockchain with the shared bicycle system. It is the first time this type of research has been undertaken, to our knowledge. This paper creatively constructs a deposit management system for shared bicycles based on the blockchain technology. In the deposit management system for shared bicycles built in this paper, the user deposit accounts, personal information, and transaction data are stored in blocks of the same specification. Asymmetric encryption algorithm and SHA256 algorithm are used to guarantee the security of blocks, and Merkle algorithm is used to ensure that transaction data, deposit value, and other information could not be tampered. Moreover, this system endows the supervision organizations with SPV permission to verify the authenticity of deposit refunds. Meanwhile, the smart contract of the consensus layer can monitor the transaction behaviors and deposit flows of enterprises and users in real time. It can punish enterprises transferring user deposits illegally and punish users who damage shared bicycles. Finally, in the simulation experiment, the deposit theft rate of our deposit management system is 0%, which is far better than the two current deposit management systems. Thus, the security and effectiveness of our shared bicycle deposit management system are verified. Our system eliminates the problem of information asymmetry among enterprises, users, and supervision organizations, eradicates the possibility of enterprises transferring user deposits unilaterally, and realizes the visualization of deposit accounts, the transparency of deposit whereabouts, and the management requirement of immediate deposit refunds.

The research results of this article improve the theoretical system of deposit management for the shared bicycle industry and design a set of operational programs for the scientific management of shared bicycle deposit. Meanwhile, these results are also endowed with important theoretical significance and practical value for the guarantee of user deposit security, improving the industry supervision system, reinforcement of antecedent and real-time scientific and effective supervision conducted by the government, and accelerating the innovative development of shared bicycle enterprises.

Firstly, the system proposed in our paper eliminates the centralization advantage of shared bicycle enterprises and eradicates the possibility of transferring users' deposits by enterprises at will. In this system, the transfer of deposit needs to meet the trigger conditions stipulated in the smart contract. Also, each deposit is transferred automatically by the smart contract, which means the enterprises have no right to transfer the deposits. If the deposit transfer records meet the trigger conditions, the smart contract will automatically review the rationality of related deposit transfer and publish the transaction record, and block the status and deposit value on the network layer in the form of broadcast. Therefore, users and the supervision organizations can verify the rationality of any deposit transfer in real time. Thus, our system puts an end to the transfer of user deposits caused by false transaction and finally guarantees the legitimate rights and interests of users.

Secondly, our deposit management system realizes the management requirements of deposit account visualization and the immediate deposit refunds. The deposit of the user is kept in the deposit account of the user block body. Technically, enterprises have no right to interfere with the deposit accounts of users, and the users can withdraw the deposits without waiting for the review of the enterprise or regulatory agency. At the same time, the smart contract designed by our system can monitor the user behavior in real time. If a user intentionally damages shared bicycles, the smart contract will withdraw part of the deposit to compensate related enterprise, thereby protecting the legitimate rights and interests of the enterprise.

Moreover, the proposed system increases the capability of supervision organizations to check deposit returns and realizes a multidimensional deposit supervision management mode. In this system, the deposit return record is saved in the block head by generating a hash value with the hash algorithm. Adding or deleting a deposit return record will affect the hash value. By checking the hash values between users and enterprises, the supervision organizations could verify the authenticity for deposit refunds by enterprises, in

turn guaranteeing the legitimate rights and interests of related enterprises and users.

Finally, the blockchain deposit management system for shared bicycles constructed in this paper eliminates the management shortcomings of the current shared bicycle industry and reconstructs its management system. This system could record the behavior of enterprises and users comprehensively and provide real and reliable data support for the supervision of the shared bicycle market. In general, this paper provides blockchain technical support and a creative management mode for building a shared bicycle system that features honest operations of enterprises, standardized user conducts, and multidimensional regulation of supervision organizations.

6. Prospective Directions

The decentralization, visualization, and information tamper-proof characteristics of the blockchain technology could realize the openness and transparency of the industrial transaction mode and social management structure. Thus, implementation of blockchain technology can help meet the technical requirements for the revolution of the industrial structure and form in the context of supply-side reforms. In this paper, the deposit management system for shared bicycles constructed with the blockchain technology complies with the development of the society, solves the problem of unreliable enterprise deposit management credit, ensures the reasonable use of user deposits, and provides scientific technical support for the sustainable development of shared bicycles. Beyond the management of shared bicycle deposits, the proposed system still has many other aspects that deserve attention and are worth expanding. In future research, we will seek to predict user demand and plan bike delivery quantity by utilizing user transaction records stored in this system in combination with cloud computing and other technologies.

Appendix

A

```
pragma solidity ^0.4.2;
contract Token { //Account query
//issue Function can recharge the contract account
//transfer Function can send tokens to other accounts
//getBalance Function gets the token balance for an account
  address issuer;
  mapping (address => uint) balances;
  event Issue(address account, uint amount);
  event Transfer(address from, address to, uint amount);
  function Token() {
    issuer = msg.sender;
  }
  function issue(address account, uint amount) {
    if (msg.sender != issuer) throw;
    balances[account] += amount;
  }
  function transfer(address to, uint amount){
    if (balances[msg.sender]<amount)throw;
    balances[msg.sender] −= amount;
    balances[to] += amount;
    Transfer(msg.sender, to, amount);
  }
  function getBalance(address account)constant returns (uint) {
    return balances[account];
  }
}
contract LockAccount {//
  mapping(address => uint) private userBalances;
  function transfer(address to, uint amount){
    if (userBalances[msg.sender] ≥amount){
      userBalances[to]+=amount;
      userBalances[msg.sender] −= amount;
    }
  }
  function withdrawBalance()public{
    uint amountToWithdrew = userBalances[msg.sender];
    if (!(msg.sender.call.value(amountToWithdrew))) { throw; }
    userBalances[msg.sender] = 0;
  }
  _mapping (address => uint)private userBalances;
  mapping(address => bool)private claimedBonus;
  mapping (address => uint) private rewardsForA;
  function untrustedWithdrew(address recipient) public{
    uint amountToWithdrew = userBalances[recipient];
    rewardsForA[recipient] = 0;
    if (!(recipient.call.value(amountToWithdrew) ())) { throw; }
  }
  function untrustedGetFirstWithdrewalBonus(address recipient)public{
    if (claimedBonus[recipient]) { throw; }
    claimedBonus[recipient] = true'
    rewardsForA[recipient] += 100;
    untrustedWithdrew(recipient);
  }
```

```
    function deposit() payable public returns(bool){
      if (!lockBalances) {
        lockBalances = true;
        balances[msg.sender] += msg.value;
        lockBalances = false;
        return true;
        {throw;}
    }
    function withdraw(uint amount) payable public
returns(bool){
      if (!lockBalances && amount>0 && balances
[msg.sender] ≥ amount) {
        lockBalances = true;
        if (msg.sender.call(amount)()) {// Normally
insecure, but the mutex saves it
          balances[msg.sender] −= amount;
      }
      lockBalances = false;
      return true;
      {throw; }
    }
}
contract StopContract{//
      bool private stopped = false;
      2address private owner;
      modifier isAdmin(){
        if (msg.sender != owner){throw;}
        }
      }
      function toggleContractActive() isAdmin public{
        stopped =! stopped;
      }
      modifier stopInEmergency{if (!stopped)_;}
      modifier onlyInEmergency{if (!stopped)_;}
      function deposit()stopInEmergency public{
      }
}
```

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

All the authors contributed to the idea of this paper. D. Z. supervised the overall work. D. W. wrote the whole manuscript and polished the language of this paper. B. W. provided constructive advice to improve the manuscript.

Acknowledgments

This research was funded by the National Natural Science Foundation of China (Grant no. 71472134) and School-level major project of Beijing Wuzi University in 2020—design and function of hedging strategy calculator (Grant no. 035200120918).

References

[1] D. Zhao and D. Wang, "The research of tripartite collaborative governance on disorderly parking of shared bicycles based on the theory of planned behavior and motivation theories-a case of Beijing, China," *Sustainability*, vol. 11, no. 19, p. 54, 2019.

[2] Y. Cao and D. Shen, "Contribution of shared bikes to carbon dioxide emission reduction and the economy in Beijing," *Sustainable Cities and Society*, vol. 51, p. 10, 2019.

[3] L. Gao, Y. Ji, X. Yan et al., "Incentive measures to avoid the illegal parking of dockless shared bikes: the relationships among incentive forms, intensity and policy compliance," *Transportation*, vol. 51, pp. 1–28, 2020.

[4] B. Bachand-Marleau, *Better Understanding of Factors Influencing Likelihood of Using Shared Bicycle Systems and Frequency of Use*, Transportation Research Record, New York, NY, USA, 2018.

[5] S. Ølnes, *Beyond Bitcoin Enabling Smart Government Using Blockchain Technology*, Springer, Berlin, Germany, 2016.

[6] R. Beck, "Beyond bitcoin: the rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.

[7] D. Zhao, L. Feng, and G. Liang, "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 958–967, 2018.

[8] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, p. 2541, 2016.

[9] D. Knezevic, "Impact of blockchain technology platform in changing the financial sector and other industries," *Montenegrin Journal of Economics*, vol. 14, no. 1, pp. 109–120, 2018.

[10] Z. Shae and J. J. P. Tsai, *On the Design of a Blockchain Platform for Clinical Trial and Precision medicine*, IEEE, New York, NY, USA, 2017.

[11] J. Zhao, W. Deng, and Y. Song, "Ridership and effectiveness of bikesharing: the effects of urban features and system characteristics on daily use and turnover rate of public bikes in China," *Transport Policy*, vol. 35, pp. 253–264, 2014.

[12] B. Shen, Y. Shan, Y. Jia, D. Xie, and S. Zhu, "Modeling the cashflow management of bike sharing industry," Springer, Berlin, Germany, 2019.

[13] X. Liu, T. Gao, and X. B. Wang, *From High-Tech to Business Model Innovation. Regional Innovation Index of China*, Springer, Singapore, 2018.

[14] H. Xu and X. Liu, *Research on Social Governance Innovation of Shared Bikes*, Atlantis Press, Berlin, Germany, 2018.

[15] D. Yu and L. Shang, "Opportunities and challenges faced by share economy: taking sharing bicycle as an example," *DEStech Transactions on Environment, Energy and Earth Sciences*, vol. 47, 2017.

[16] M. Chen, D. Wang, Y. Sun, E. O. D. Waygood, and W. Yang, "A comparison of users' characteristics between station-based

bikesharing system and free-floating bikesharing system: case study in Hangzhou, China," *Transportation*, vol. 47, no. 2, p. 689, 2018.

[17] R. Marselli, "Treasury financing and bank lending-reserves causality: the case of Italy, 1975–1990," *Journal of Post Keynesian Economics*, vol. 15, no. 4, pp. 571–588, 1993.

[18] H. Nakamura and N. Abe, "Evaluation of the hybrid model of public bicycle-sharing operation and private bicycle parking management," *Transport Policy*, vol. 35, pp. 31–41, 2014.

[19] V. Vallurupalli and I. Bose, "Rabbit or tortoise? Rethinking customer acquisition at dravya bank," *Communications of the Association for Information Systems*, vol. 43, no. 1, pp. 378–403, 2018.

[20] S. B. Nakamoto, "A peer-to-peer electronic cash system," *Consulted*, vol. 43, 2008.

[21] S. Bogart and K. Rice, *The Blockchain Report: Welcome to the Internet of Value*, Needham Insights, New York, NY, USA, 2015.

[22] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 05, pp. 1–10, 2016.

[23] M. Attaran and A. Gunasekaran, "Blockchain-enabled technology: the emerging technology set to reshape and decentralise many industries," *International Journal of Applied Decision Sciences*, vol. 12, no. 4, pp. 424–444, 2019.

[24] M. L. D. Silvestre, P. Gallo, J. M. Guerrero et al., "Blockchain for power systems: current trends and future applications," *Renewable and Sustainable Energy Reviews*, vol. 10, 2019.

[25] V. K. Chattu, A. Nanda, S. K. Chattu, S. M. Kadri, and A. W. Knight, "The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security," *Big Data and Cognitive Computing*, vol. 3, no. 2, p. 25, 2019.

[26] S. Fernandez-Vazquez, R. Rosillo, and D. De La Fuente, "Blockchain in FinTech: a mapping study," *Sustainability*, vol. 11, no. 22, p. 6366, 2019.

[27] Q. Priore and K. Li, "Decentration transaction method based on blockchain technology. 2018 international conference on intelligent transportation, big data & smart city (ICITBS)," *IEEE*, vol. 11, pp. 416–419, 2018.

[28] A. Hari and T. V. Lakshman, "The internet blockchain: a distributed, tamper-resistant transaction framework for the internet," *ACM*, vol. 11, pp. 204–210, 2016.

[29] J. Hwang, M.-i. Choi, T. Lee et al., "Energy prosumer business model using blockchain system to ensure transparency and safety," *Energy Procedia*, vol. 141, pp. 194–198, 2017.

[30] J. Li, J. Wu, and L. Chen, "Block-secure: blockchain based scheme for secure P2P cloud storage," *Information Sciences*, vol. 465, pp. 219–231, 2018.

[31] G. Zyskind and O. Nathan, "Decentralizing privacy: using blockchain to protect personal data," *IEEE*, vol. 465, pp. 180–184, 2015.

[32] R. Wang, W. T. Tsai, J. He, C. Liu, Q. Li, and E. Deng, "Logistics management system based on permissioned blockchains and RFID technology," *White Paper*, vol. 465, 2019.

[33] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, p. 37, 2014.

[34] R. Lai and D. L. K. Chuen, "Blockchain–from public to private," *White Paper*, vol. 2, pp. 145–177, 2018.

[35] T. Bocek and B. Stiller, *Smart Contracts–Blockchains in the Wings*, Springer, Berlin, Germany, 2018.

[36] P. DeMaio, "Bike-sharing: history, impacts, models of provision, and future," *Journal of Public Transportation*, vol. 12, no. 4, p. 41, 2009.

[37] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Image encryption algorithm based on discrete logarithm and memristive chaotic system," *The European Physical Journal Special Topics*, vol. 228, no. 10, pp. 1951–1967, 2019.

[38] M. Szydlo, *Merkle Tree Traversal in Log Space and Time*, Springer, Berlin, Germany, 2004.

[39] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: a secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, 2019.

[40] Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[41] B. Wang, J. Park, and J. H. Park, "A lightweight hash-based blockchain architecture for industrial IoT," *Applied Sciences*, vol. 9, no. 18, p. 3740, 2019.

[42] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[43] S. Pote, V. Sule, and B. K. Lande, "Arithmetic of koblitz curve SECP256K1 used in bitcoin cryptocurrency based on one variable polynomial division," 2019.

[44] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems*, vol. 102, pp. 902–911, 2020.

[45] S. Philippe, A. Glaser, and E. W. Felten, "A cryptographic escrow for treaty declarations and step-by-step verification," *Science & Global Security*, vol. 27, no. 1, pp. 3–14, 2019.

[46] A. Aggarwal, P. Chaphekar, and R. Mandrekar, "Cryptanalysis of bcrypt and SHA-512 using distributed processing over the cloud," *International Journal of Computer Applications*, vol. 128, no. 16, pp. 13–16, 2015.

[47] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, and H. Jin, "SBLWT: a secure blockchain lightweight wallet based on trustzone," *IEEE Access*, vol. 6, pp. 40638–40648, 2018.

[48] G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor, and X. Xu, "On legal contracts, imperative and declarative smart contracts, and blockchain systems," *Artificial Intelligence and Law*, vol. 26, no. 4, pp. 377–409, 2018.

[49] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-Enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[50] N. Liu, M. Xu, B. Gao, and G.-Q. Liu, "A novel intelligent classification model for breast cancer diagnosis," *Information Processing & Management*, vol. 56, no. 3, pp. 609–623, 2019.

[51] W. Qi, Z. Wang, X. Wang, K. Qiu, C. Jia, and C. Jiang, "LSC: online auto-update smart contracts for fortifying blockchain-based log systems," *Information Sciences*, vol. 512, pp. 506–517, 2020.

[52] D. Wang, D. Zhao, B. Wang et al., "Industrial engineering and engineering management," 2019.

[53] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & internet of things," 2017.