A Study on Blockchain-based Circular Economy Credit Rating System

Hsin-Te Wu[1], Yi-Jen Su[2], Wu-Chih Hu[1]

[1] Department of Computer Science and Information Engineering,
National Penghu University of Science and Technology, Taiwan
[2] Department of Computer Science and Information Engineering, Shu-Te University, Taiwan
wuhsinte@gms.npu.edu.tw, iansu@stu.edu.tw, wuchih.hu@gmail.com

Abstract

Circular economy is distinct from the linear economy model in the past. Circular economy emphasizes regeneration instead of possession of resource, and proposes using shared resources to create new supply chains and new economies. When practicing circular economy, prior to collaboration, each economic entity must learn of each other's credit rating. This study applies the blockchain technology to establish each economic entity's transaction details, and then employs confidence level algorithms to calculate each entity's credit rating; the method utilizes the concept of decentralization to reduce third party broker fees, which, aside from decreasing transaction costs, provides effective credit rating of public economic entities.

Keywords: BlockChain, Circular economy, Sharing economy

1 Introduction

Blockchains can alter our future lifestyles. For the Internet of Vehicles, vehicles will be able to utilize blockchains to perform parking and toll payments while also being able to directly pay and download music or multimedia videos. For real estate management, users will be able to use blockchains to lease spare spaces and automatically calculate payments. In the future, blockchains will not only contribute to the Internet of Things or corporations, but also towards food safety, e-voting, intellectual property, and healthcare. Blockchains will completely alter past business models. For financial institutes, consumers will not longer need to conduct procedures such as money transfer personally at the bank during business hours; instead, they will be able to utilize the blockchain technology to perform digital currency transactions. Banks will save up on physical rent fees and labor costs while consumers enjoy secure transaction at any time, any place. The sharing economy can also apply blockchains. Take the ride sharing service platform Lazooz as an example; users can use the app to search for nearby available vehicles for ride sharing, all the while eliminating the need for an intermediate. We can see from the above why countries around the globe are devoting manpower to researching and developing blockchains because the blockchain technology will bring new economic drive.

Circular economy has risen to become the new generation's economic issue. Circular economy involves leasing, instead of purchasing, idle properties or reusing waste for resource recycling to achieve the goal of sustainable resource management. There are five key concepts to circular economy: (1) redesigning product material: opting for non-disposable and recyclable material for sustainable use of resources; (2) employing ownership transferring innovative commercial models: changing past linear economy models to substitute buying with leasing; (3) creating higher values through the power of internal circulation: maintaining a product's maximized value by way of circulation, such as utilizing repair, upgrade, reproduction, remarketing to maintain a product's economic value; (4) turning waste into resource: recycling discarded goods and returning them to another product's circulation; (5) establishing industrial symbiosis: bringing different industries to the same region so they may exchange resources, share infrastructures, reduce disposable waste, and lower production costs. This study proposes a trust mechanism for the sharing economy. Many industries currently hold idle machinery or idle space; through a sharing economy, they can increase corporate profits by substituting buying with leasing. However, mutual trust is required in realizing sharing economy; moreover, in order to enable enterprises to share resources at any time and place, trust between enterprises must be transparent and non-modifiable; hence, this study proposes a trust verification mechanism based on blockchain technology that can help realize sharing economy.

*Corresponding Author: Hsin-Te Wu; E-mail: wuhsinte@gms.npu.edu.tw
DOI: 10.3966/160792642019052003026

This study employs blockchains in establishing the buyer's and seller's credit rating so that the two parties may utilize credit ratings to select a trustworthy business partner. This study utilizes public key cryptography from blockchains to ensure a transaction's non-repudiation; each party to the transaction can acquire their counterparty's credit ratings by means of verification. Our proposed rating system holds different calculation methods for the buyer and the seller: the seller's involves calculation of corporate capital, transaction amount, and completed transaction progress while the buyer's involves calculation of corporate capital, transaction amount, and payment status, and as for the rating part, the two parties provide ratings for each other. The proposed credit rating system aims to create a better transaction environment for the sharing economy and enable the buyer and seller to choose better business counterparties through transparent credit ratings.

2 Related Work

Ever since Bitcoin's development in 2009, many businesses have dedicated themselves towards Bitcoin. However, because Bitcoin has undergone serious fluctuations in stock prices, some Bitcoin companies experienced bubble burst. Reference [1] offers an analysis model for Bitcoin price prediction to help investors in their Bitcoin investments. Reference [2] offers simulation of the Bitcoin system model; it also simplifies blockchains and avoids double spending risks. Reference [2] simulates blockchains' execution efficiency, and its experiment showed promising results. Reference [3] discusses Bitcoin mining efficacy in Bitcoin software and hardware. Bitcoin has launched digital currency in many countries, and has even established Bitcoin e-payment systems in convenient stores. Reference [4] analyzes the advantages of digital currency and takes a look at Bitcoin's usage of zk-SNARK transaction authentication system. Bitcoin has drastically matured since its introduction in 2009, which has also served as a motivation for blockchain development.

Reference [5] mentions using data envelopment analysis to analyze and verify the effects of circular economy. Reference [6] elaborates on the definition of sharing economy and emergent collectives, and provides case studies of sharing economy. Reference [7] proposes a sharing economy model for public enterprises and private companies that allows resources to be adequately allocated by means of accords and thus increases the scale of sharing economy. Meanwhile, Reference [8] posits the required conditions for a complete transaction and, after analyzing them, concludes that trust is the foremost condition among all. Reference [9] utilizes location sharing to achieve privacy protection and trust, and is mainly applied in social networking sites.

Reference [10] proposes a fully decentralized, collaborative reputation based computational model that conducts ratings based on two factors: first, contract fulfillment situation, and, second, parties involved in the process. This method reduces one sided buyer/seller malicious ratings and enhances the reputation system's accuracy. In Reference [11], Web service recommendation systems searches for webpages suitable for the user from a myriad of webpage services. This study uses bloom filtering to enhance its recommendation performance. Reference [12] suggests a dependable trust management scheme — GroupTrust — to avoid dishonest or maliciously fabricated ratings; it also calculates the truthful rating from the fabricated ones. Meanwhile, Reference [13] proposes VANET, which utilizes the Boneh-Boyen-Shacham short group signature scheme to accomplish message ratings; it also relies on signatures o ensure the credibility of ratings. Reference [14] focuses on a pragmatic rating system: for each rating, it provides two to three genuine options and adds a few false ones, a method that should identify truthful ratings from fabricated ones. Reference [15] introduces privacy preserving decentralized reputation systems that employ privacy protection to prevent information leaks and ensure personal reputation.

This study employs blockchains to store users' (corporate) transaction conditions. It utilizes bilinear pairing to verify the origin and integrity of transaction details; any user can use the blockchains to collect information on their transaction counterparty's credit condition. The reputation system relies mainly on transaction conditions between sellers and buyers to conduct rating. This reputation system can optimize the search for business partners in a sharing economy.

3 Background

This chapter introduces the blockchain model's operation model and the encryption/decryption methods. This study is based on bilinear pairing and uses ID based cryptography to ensure authenticity of the message's origin and integrity.

3.1 Blockchain Model

The development of blockchains can be divided into four phases: in 2009, Bitcoin started its operations; Blockchains 1.0 emerged afterwards and was dubbed "digital currency;" Blockchain 2.0 added smart contracts that stored commercial contracts such as stock transactions, securities registration, futures, and loans; Blockchain 2.5 added distributed data, data layer blockchains, artificial intelligence, and exchange less international finance networks; Blockchain 3.0 employed even more complex smart contracts and was applied to government affairs, medicine, science, culture, and the justice system.

BlockChain mainly employs a distributed architecture. In the past, information used to be stored in centralized management system; while such servers possess the functions of adding new data or editing existing data, centralized management systems are susceptible to malicious attacks, such as distributed denial of service attack (DDOS) [16]. Once a centralized management system experiences a meltdown, all its services come to a halt, and many services are no longer available. Hence, the blockchain technology employs distributed ledgers, and for its security key management features, it calls for distributed security key management. The blockchain model is illustrated in Figure 1. Each user has their public/private key; when User A and User B engage and complete a transaction, User A will run the transaction details through hash technology to confirm the transaction details' integrity and non-repudiation. User A will then add TimeStamp to the transaction details to verify its validity and sign it using their private key. Following that, signed transaction details are transmitted to each node on the Internet. Every node can use User A's public key for authentication; every node can also help maintain the same ledgers since ledgers are made public and subject to authentication by everyone. Hence, when a certain node is under malicious attacks, other nodes can still carry on operation of ledgers. In sum, blockchains bear the following advantages: (1) decentralization, with data being stored in a distributed database; (2) joint effort in maintaining the public ledger; (3) employment of hash technology ensures the information's non-repudiation; (4) the hash block has a TimeStamp that ensures the information's validity.

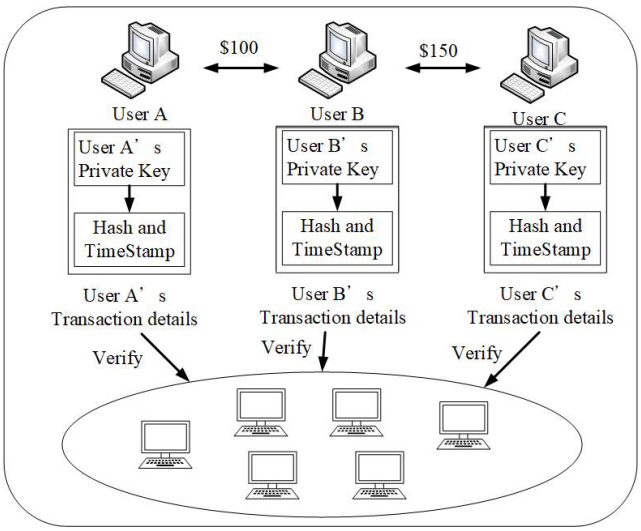

Figure 1. Blockchain model

The blockchain technology has been utilized in all kinds of applications. For instance, it has been used in IoT's point to point data collection and network security protection. The Internet of Vehicles has also used the blockchain technology in parking fee payment using digital currency. Additionally, given our current IoT and smart healthcare status, all information must be stored and not deleted, medical information also require permanent preservation; as a result, centralized databases can no longer handle such rapid growth in data volume. This is why we must turn to distribute database for storage needs. Distributed database has been in development for years (Reference [24]), and we are now able to realize its algorithms and system implementation. We have also advanced significantly in peer to peer algorithm and techniques, including the DHT algorithm and the content addressable network (CAN). We have also witnessed the launch of variegated related software.

3.2 Bilinear Pairing

This study uses bilinear pairing to authenticate message origin, non-repudiation, and integrity. The use of bilinear pairing's encryption/decryption allows for more flexibility. Suppose G_1 and G_2 are, respectively, additive and multiplicative groups and apply the prime order q; suppose P is G_1's generator, and the bilinear mapping is $e: G_1 \times G_1 \to G_2$. The features of bilinear pairing are as follows:

I. Bilinear: $e = (aP, bP) = e(P, P)^{ab}$,

$e(a \cdot P + b \cdot P, P) = e(a \cdot P, P)e(b \cdot P, P)$, for all $P \in G_1$ and $a, b \in Z_q^*$.

II. Non-degeneracy: $P \in G_1$ such that $e(P, P) \neq 1$. That is, the mapping does not send all pairs in $G_1 \times G_1$ to the identity in G_2.

III. Computable: There exists an efficient algorithm to compute $e(P, P)$ for all $P \in G_1$.

In this study, to realize bilinear map e, we have applied pairing methods from Weil [17] and Tate [18] pairings. The data amount of G_1 and q are respectively 161 bits and 160 bits.

3.3 ID Based Cryptography

This study utilizes ID based cryptography (IBC) [18] for private communication. IBC's advantage lies on the premise that it does not require either party to provide certificate for identity authentication. Suppose that the private key generator (PKG) selects a random number as its master key. Any user's real ID is ID_u, the user's public key is $\mathcal{PK}_{\mathbb{ID}_u} = \mathbb{ID}_u \cdot P$ and their private key is $\mathcal{PR}_{\mathbb{ID}_u} = s \cdot \mathcal{PK}_{\mathbb{ID}_u}$. When User A and User B engage in message communication, they can establish a common session key using the following algorithm:

$$\mathcal{SK}_{\mathbb{ID}_A \leftrightarrow \mathbb{ID}_B} = e\left(\mathcal{PK}_{\mathbb{ID}_B}, \mathcal{PR}_{\mathbb{ID}_A}\right) = e\left(\mathcal{PK}_{\mathbb{ID}_B}, s \cdot \mathcal{PK}_{\mathbb{ID}_A}\right) \quad (1)$$

In Equation (1), the user on both sides can user their own private key and their counterparty's public key to establish a common session key ($\mathcal{SK}_u$). Given that

$\mathcal{PR}_{\mathbb{ID}_u}$ is only known to oneself, while s is secret and inaccessible, this ensures the security and origin of the message.

4 The Proposed Scheme

4.1 System Model

This study proposes a blockchain based sharing economy credit rating system. The blockchain technology part focuses on utilizing bilinear pairing public key cryptography to authenticate transaction details. Suppose every user has a true ID ($\mathbb{ID}_u$), a public key ($\mathcal{PK}_{\mathbb{ID}_u}$), and a private key ($\mathcal{PR}_{\mathbb{ID}_u}$). As shown in Figure 2, when Seller A sends out transaction items to each user on the Internet, the user can choose freely whether or not to engage in transaction. For instance, if Buyer B and Buyer F are interested in a certain transaction item and send out responses to Seller A, then Seller A, upon receiving such responses, will query the credit ratings of Buyer B and Buyer F. Although each user maintains their ledger, in order to confirm that the ledger is up to date, messages requesting the credit ratings of Buyer B and Buyer F will be issued. In order to confirm that the ledger is authentic, origin authentication is performed; additionally, to prevent malicious conspired attacks, authenticity of credit ratings are only confirmed after receiving t sets of user information. When Seller A decides to engage in transaction with Buyer B and Buyer F, they will use smart contracts for their transaction contract [20] because smart contracts are not only legally binding but also public, which ascertains fairness of transaction between both parties. Table 1 illustrates the symbols used in this study.

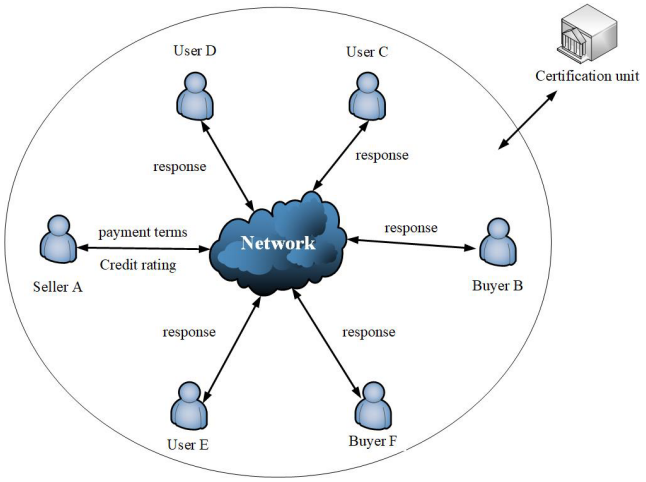

Figure 2. System model

Table 1. Notation

Notation	Description
P	the generator of G_1.
$\mathbb{ID}_u$	the real ID of the user u.
G_1	the additive group.
G_2	the multiplicative group.
s	A random number $s \in Z_q^*$ chosen as the master key where Z_q^* is a finite field of order q.
$\mathcal{SK}$	the common session key.
$\mathcal{TM}_{\mathbb{ID}_u}$	the total transaction amount between Seller and the buyer
$\mathcal{TR}_{\mathbb{ID}_{b,B}}$	the transaction result between between Seller and the buyer
e	the bilinear map.
H_1	$H_1 : \{0,1\}^* \to G_1$.
H	the hash function.
M	the message or smart contract.
$\mathcal{PR}_{\mathbb{ID}_u} = H_1(\mathbb{ID}_u \cdot s \cdot P)$	the private key of user u.
$\mathcal{PK}_{\mathbb{ID}_u} = H_1(\mathbb{ID}_u \cdot P)$	the public key of user u.
$\mathcal{TA}_{\mathbb{ID}_u}$	the transaction amount between Seller and the buyer

4.2 Message Transmission and Authentication

Figure 2 is an illustration of when a seller posts a transaction's details to the Internet. Seller A ($ID_{s,A}$) uploads the transaction content to the Internet and encrypts the message using $\mathcal{PR}_{\mathbb{ID}_u}$; other users receive such message and user their public key to decipher the message. When users Buyer B and Buyer F become interested in the transaction, they will utilize IBC and $ID_{s,A}$ to conduct private communication, and notify their transaction demands to $ID_{s,A}$; $ID_{s,A}$ will then respond to Buyer B and Buyer F, a process of which is shown in Figure 3.

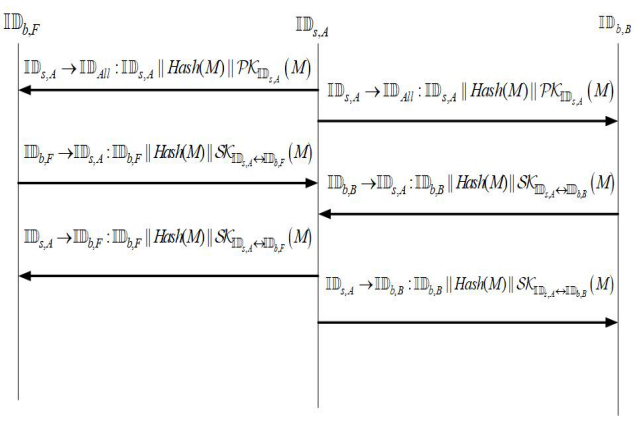

Figure 3. Illustration of transaciton query process

When $ID_{s,A}$ receives Buyer B and Buyer F intent of transaction, $ID_{s,A}$ will then issue messages to every

user, inquiring the credit ratings of Buyer B and Buyer F. When other users receive such request, they will search for ledgers concerning information of Buyer B and Buyer F, and use IBC and $ID_{s,A}$ to conduct private communication and message transmission. The process is as follows:

After completing credit rating query, $\mathbb{ID}_{s,A}$ will use the algorithm in Section 4.3 to compute credit rating. Upon completing the computation, $\mathbb{ID}_{s,A}$ will then select a business partner, and then employ BlockChain 4.0 technology's smart contracts to establish a contract and make the contract public so as to allow other users to conduct authentication. Smart contracts are legally binding; when the transaction is complete, $\mathbb{ID}_{s,A}$ will utilize the private key to encrypt the transaction details and smart contracts, process the message using hash functions and TimeStamp, and then disclose the information on the Internet for authentication purposes. The equation is as follows:

$$\mathbb{ID}_{s,A} \| Hash(M) \| \mathcal{PR}_{\mathbb{ID}_{s,A}} \| T_i \quad \textbf{(2)}$$

Buyer B and Buyer F will also encrypt the transaction details and smart contracts using private keys, process the messages using hash functions and TimeStamp, and then make the information public on the Internet for authentication to improve buyer credit rating.

4.3 Credit Rating Computation

Each time a seller and buyer engage in a successful transaction, the following in-formation ensues:

$$\mathcal{M}_{\mathbb{ID}_{s,A}} = \mathbb{ID}_{s,A} \| \mathbb{ID}_{b,B} \| .. \| \mathcal{TR}_{\mathbb{ID}_{b,B}} \| .. \quad \textbf{(3)}$$

$$\mathcal{M}_{\mathbb{ID}_{b,B}} = \mathbb{ID}_{s,A} \| \mathbb{ID}_{b,B} \| \mathcal{TM}_{\mathbb{ID}_{s,A}} \| \mathcal{TA}_{\mathbb{ID}_{b,B}} \| \mathcal{TR}_{\mathbb{ID}_{b,B}} \quad \textbf{(4)}$$

Equation (3) concerns the transaction status between the seller and the buyer; $\mathcal{M}_{\mathbb{ID}_{s,A}}$ stands for the information of Seller $\mathbb{ID}_{s,A}$; stands for the true identity of Seller $\mathbb{ID}_{s,A}$; $\mathcal{TM}_{\mathbb{ID}_{s,A}}$ is the total transaction amount between Seller $\mathbb{ID}_{s,A}$ and the buyer $\mathbb{ID}_{b,B}$; $\mathcal{TA}_{\mathbb{ID}_{b,B}}$ is the transaction amount between $\mathbb{ID}_{b,B}$ and $\mathbb{ID}_{s,A}$; $\mathcal{TR}_{\mathbb{ID}_{b,B}}$ is the transaction result between $\mathbb{ID}_{b,B}$ and $\mathbb{ID}_{s,A}$, which includes message transaction status, payment time, and completion time. The seller and buyer upload the transaction result to each node. The algorithm is as follows:

$$\mathbb{ID}_{s,A} \| Hash(M) \| \mathcal{PR}_{\mathbb{ID}_{s,A}} \| T_i \quad \textbf{(5)}$$

$$\mathbb{ID}_{b,B} \| Hash(M) \| \mathcal{PR}_{\mathbb{ID}_{b,B}} \| T_i \quad \textbf{(6)}$$

In Equation (5), $\mathbb{ID}_{s,A}$ sends out transaction details to every user on the Internet; upon receiving the information, the user will compute $\mathbb{ID}_{s,A}$'s public key ($\mathcal{PK}_{\mathbb{ID}_{s,A}} = H_1(\mathbb{ID}_{s,A} \cdot P)$), and then use $\mathbb{ID}_{s,A}$'s public key to decipher and conduct verification of the message's integrity and validity. In Equation (6), $\mathbb{ID}_{b,B}$ sends out transaction details to every user on the Internet after the transaction is completed; upon receiving the information, the user will compute $\mathbb{ID}_{b,B}$'s public key ($\mathcal{PK}_{\mathbb{ID}_{b,B}} = H_1(\mathbb{ID}_{b,B} \cdot P)$), and then utilize $\mathbb{ID}_{b,B}$'s public key to proceed with deciphering and verification.

When $\mathbb{ID}_{s,A}$ wishes to compute the credit ratings of $\mathbb{ID}_{b,B}$ and $\mathbb{ID}_{b,F}$, it will send out a credit rating query in a process as illustrated in Figure 4. Following that, when $\mathbb{ID}_{s,A}$ receives the credit rating sent by the user, it will verify the origin and integrity of each one of them and avoid maliciously conspired, fabricated credit ratings. When the received credit ratings have identical content and exceed *t* in number, it indicates that the credit rating is genuine. The computation is as follows:

```
//determine whether the content of credit rating is identical
For i=1~n
//determine whether the message is identical
If message_i == message_i+1
Count=Count+1;
End
End
//determine whether it is higher than the threshold
If Count > t
//credit rating bears high credibility
Correct=True
Else
Correct=Flase
  End
```

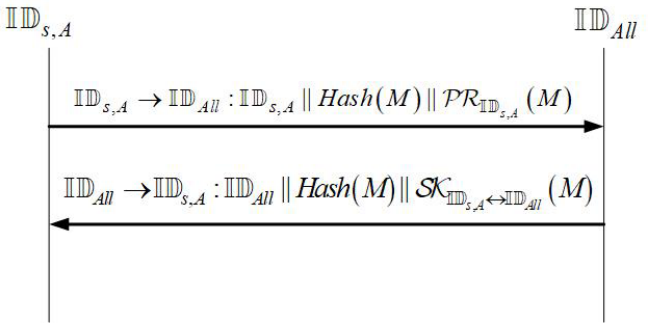

Figure 4. Illustration of Credit Rating Query

When Correct is True, $\mathbb{ID}_{s,A}$ can use relevant information in credit ratings for computational purposes, such as: When another user, $\mathbb{ID}_{b,B}$, wishes

to join $\mathbb{ID}_{s,A}$ in a sharing economy transaction, $\mathbb{ID}_{b,B}$ can utilize $\mathbb{ID}_{s,A}$'s true ID to calculate each transaction amount's credit rating; the calculation is as follows:

$$\mathcal{R}_{\mathbb{ID}_{s,A},i}=\begin{Bmatrix}\left(\mathcal{T}_{\mathbb{ID}_{s,A}}*0.3\right)+\left(F_{\mathbb{ID}_{s,A},i}*0.7\right),TR_{\mathbb{ID}_{s,A},i}=1\\0,TR_{\mathbb{ID}_{s,A},i}=0\end{Bmatrix} \quad (7)$$

$$\mathcal{T}_{\mathbb{ID}_{s,A},i}=\begin{Bmatrix}1,\dfrac{\mathcal{TM}_{\mathbb{ID}_{s,A},i}}{\mathcal{CA}_{\mathbb{ID}_{s,A}}}>1\\\dfrac{\mathcal{TM}_{\mathbb{ID}_{s,A}}}{\mathcal{CA}_{\mathbb{ID}_{s,A}}},\dfrac{\mathcal{TM}_{\mathbb{ID}_{s,A}}}{\mathcal{CA}_{\mathbb{ID}_{s,A}}}<=1\end{Bmatrix} \quad (8)$$

$$\mathcal{CR}_{\mathbb{ID}_{s,A}}=\sum_{1}^{n}\mathcal{R}_{\mathbb{ID}_{s,A},i}/n \quad (9)$$

Equation (7) calculates single transaction ratings of Seller $\mathbb{ID}_{s,A}$ and focuses on the completed transaction of $TR_{\mathbb{ID}_{s,A},i}$. Hence, if $TR_{\mathbb{ID}_{s,A},i}$ is 0, then the transaction rating is 0; if $TR_{\mathbb{ID}_{s,A},i}$ is 1, then the transaction completion time $\mathcal{F}_{\mathbb{ID}_{s,A},i}$ is used to calculate whether it falls within the allotted transaction time; adding the above to the calculation of whether transaction amount $\mathcal{TM}_{\mathbb{ID}_{s,A},i}$ falls within the capital $\mathcal{CA}_{\mathbb{ID}_{s,A}}$, we can obtain the seller's rating $\mathcal{R}_{\mathbb{ID}_{s,A},i}$ for a single transaction. Equation (9) calculates the seller's overall rating; Seller $\mathbb{ID}_{s,A}$ can also use Equations (7)~(9) to calculate Buyer $\mathbb{ID}_{b,B}$'s rating, so that the two parties may understand each other's past number of transactions and their ratings to facilitate their selection of optimal transaction counterparties.

5 Performance Analysis

This chapter proposes: 5.1.security analysis, 5.2.performance analysis, and 5.3.credit rating analysis of differential comparison between our proposed scheme and other literature.

5.1 Security Analysis

Given that our proposed scheme is based on blockchain technology, when it comes to security analysis, we must satisfy requirements of authentication, integrity, non-repudiation, and message time validity. The following is an analysis of our proposed scheme:

I. Authentication: our proposed public key is obtained via users' real ID; if one can falsify a public key, they cannot falsify the private key because the master key s is kept secret and unattainable.

II. Integrity: this study applies hash technology to ensure message integrity.

III. Non-repudiation: the public key used by users are created through real IDs; private keys are created using public keys and s. Hence, by using public/private key for encryption/decryption, we can ensure the origin of the message.

IV. Message time validity: each message bears a TimeStamp that ensures its time validity.

5.2 Performance Analysis

This study provides a performance analysis of our proposed system as well as References [13] and [15]. The analysis focuses on factors including authentication, integrity, non-repudiation, and private communication. In Table 2, we ilustrate the encryption/decryption computation time based on the encryption/decryption execution time of [21-23]. Following that, Table 3 conducts performance analysis based on computation time obtained in Chart 2. Results indicate that our proposed scheme requires less amount of computation. Reference [15] uses share key, which requires collecting *t* sets of keys before deciphering the ciphertext. Hense, we presume that each key's computation calls for *2* TP* for signing and verification.

Table 2. Execution time in milliseconds

Nottions	Descriptions	Execution Time(ms)
TP	Pairing operation	≈ 4.5
TM	Point Multiplication	≈ 0.6
TE	Field Exponentiation	≈ 0.54
H	HMAC	0.002
SE	AES encryption	<0.19
SD	AES decryption	<4.65

Table 3. Performance analysis

Method Property	[13]	[15]	proposed method
Authentication	Signing: 2**TM*+1**TP* Verification: 2**TM*+1**TP*	Signing: n**TP* Verification: n**TP*	Signing: 1**TM*+1**TP* Verification: 1**TM*+1**TP*
Spending time	11.4 ms	*n**9 ms	10.2 ms
Integrity	Signing: *H* Verification: *H*	Signing: *H* Verification: *H*	Signing: *H* Verification: *H*
Spending time	0.002 ms	0.002 ms	0.002 ms
non-repudiation	Signing: 3**TM*+3**TP* +3**TE* Verification: 3**TM*+3**TP* +3**TE*	Signing: n**TP* Verification: n**TP*	Signing: 1**TM*+1**TP* Verification: 1**TM*+1**TP*
Spending time	60.84 ms	*n**9 ms	10.2 ms
Private communication	N/A	N/A	Signing: *SE* Verification: *SD*
Spending time	N/A	N/A	4.84 ms

5.3 Credit Rating Analysis

Our proposed credit rating system calls utilizes blockchains to conduct distributed data storage of transaction details and openly provides verification of each user on the Internet, which helps elevate information validity and credibility. Moreover, it employs smart contracts to establish electronic contracts. Smart contracts are currently widely used by financial institutes for their client contracts, and they are also legally binding. This study applies smart contracts to ensure protection for both sides of a transaction and, hence, enhances the credibility of our system's credit ratings. Our proposed credit rating system focuses on the transaction amount between the buyer/seller and whether the transaction was completed within time frame; the transaction amount and contract fulfillment situation can shed light on the credit conditions of both the buyer and the seller. On a sharing economy platform, credit rating is the best condition to finding a trustworthy business partner. This study's proposed credit rating system is based on blockchain technology, which facilitates information verification and safety and benefits the promotion of sharing economy.

6 Conclusion

This study has here proposed a blockchain based circular economy credit rating system. In the future, circular economy will be a key point in the government's promotions; however, circular economy's sharing mechanism requires the addition of a credit rating mechanism. In the past, enterprises had to rely on credit checking to obtain information on the other party's credit status, yet this can be time consuming and cost increasing for a transaction. This study's proposed credit rating system uses blockchains to conduct network verification; the system's decentralization feature reduces costs of credit investigation while also enabling two parties to a transaction to conduct inquiries at any time and place and facilitate their transaction.

Acknowledgments

This work was partly supported by the Ministry of Science and Technology, Taiwan, under grants MOST106-2622-E-346-001-CC3, MOST107-2622-E-346-001-CC3, and MOST107-2221-E-346-007-MY2. The authors also gratefully acknowledge the helpful comments and suggestions of reviewers, which have improved the quality and presentation.

References

[1] X. Li, C. A. Wang, The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin, *Elsevier Decision Support Systems*, Vol. 95, pp. 49-60, March, 2017.

[2] F. Tschorsch, B. Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 3, pp. 2084-2123, Third Quarter, 2016.

[3] H. Vranken, Sustainability of Bitcoin and Blockchains, *Elsevier Current Opinion in Environmental Sustainability*, Vol. 28, pp. 1-9, October, 2017.

[4] R. Agrawal, R. Srikant, Fast Algorithms for Mining association Rules in Large Databases, *Proceedings of the 20th International Conference on Very Large Data Bases*, Santiago, Chile, 1994, pp. 487-499.

[5] Y. Wang, B. Liang, Efficiency Evaluation of City Circular Economy Based on the Super-Efficient Mixed DEA Cluster Model, *Proceedings of the 2010 International Conference on Management and Service Science*, Wuhan, China, 2010, pp. 3697-3700.

[6] C. Petrie, Emergent Collectives Redux: The Sharing Economy, *IEEE Computer Society*, Vol. 20, No. 4, pp. 84-86, July-August, 2016.

[7] J. M. García, P. Fernández, A. R. Cortés, S. Dustdar, M. Toro, Edge and Cloud Pricing for the Sharing Economy, *IEEE Internet Computing*, Vol. 21, No. 2, pp. 78-84, March-April, 2017.

[8] E. Viardot, Trust and Standardization in the Adoption of Innovation, *IEEE Communications Standards Magazine*, Vol. 1, No. 1, pp. 31-35, March, 2017.

[9] R. Schlegel, C. Y. Chow, Q. Huang, D. S. Wong, Privacy Preserving Location Sharing Services for Social Networks, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp. 811-825, September- October, 2017.

[10] S. Kraounakis, I. N. Demetropoulos, A. Michalas, M. S. Obaidat, P. G. Sarigiannidis, M. D. Louta, A Robust Reputation Based Computational Model for Trust Establishment in Pervasive Systems, *IEEE Systems Journal*, Vol. 9, No. 3, pp. 878-891, September, 2015.

[11] S. Wang, Z. Zheng, Z. Wu, M. R. Lyu, F. Yang, Reputation Measurement and Malicious Feedback Rating Prevention in Web Service Recommendation Systems, *IEEE Transactions on Services Computing*, Vol. 8, No. 5, pp. 755-767, September-October, 2015.

[12] X. Fan, L. Liu, M. Li, Z. Su, GroupTrust: Dependable Trust Management, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 28, No. 4, pp. 1076-1090, April, 2017.

[13] L. Chen, Q. Li, K. M. Martin, S. L. Ng, Private Reputation Retrieval in Public- A Privacy Aware Announcement Scheme for VANETs, *IET Information Security*, Vol. 11, No. 4, pp. 204-210, June, 2017.

[14] P. Naghizadeh, M. Liu, Perceptions and Truth: A Mechanism Design Approach to Crowd Sourcing Reputation, *IEEE/ACM Transactions on Networking*, Vol. 24, No. 1, pp. 163-176, February, 2016.

[15] M. R. Clark, K. Stewart, K. M. Hopkinson, Dynamic Privacy Preserving Decentralized Reputation Systems, *IEEE*

Transactions on Mobile Computing, Vol. 16, No. 9, pp. 2506-2517, September, 2017.

[16] P. Chris, *eWeek*, DDoS Attack Volume Escalates as New Methods Emerge, 2014.

[17] M. Scott, Computing the Tate Pairing, *Proceedings of the 2005 international conference on Topics in Cryptology*, San Francisco, CA, 2005, pp. 293-304.

[18] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, M. Scott, Efficient Algorithms for Pairing-based Cryptosystems, *Proceedings of 22nd Annual International Cryptology Conference*, Santa Barbara, CA, 2002, pp. 354-368.

[19] D. Boneh, M. K. Franklin, Identity Based Encryption from the Weil Pairing, P*roceedings of 21st Annual International Cryptology Conference*, Santa Barbara, CA, 2001, pp. 213-229.

[20] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, *IEEE The Plethora of Research in Internet of Things*, Vol. 4, pp. 2292-2303, May, 2016.

[21] Efficient Implementation of Cryptographic pairings, http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf.

[22] M. Scott, Implementing Cryptographic Pairings, *Lecture Notes in Computer Science*, Vol. 4575, pp. 177-196, July, 2007.

[23] M. Long, C. H. J. Wu, J. D. Irwin, Reducing Communication Overhead for Wireless Roaming Authentication: Methods and Performance Evaluation, *International Journal of Network Security*, Vol. 6, No. 3, pp. 331-341, May, 2008.

[24] R. Agrawal, R. Srikant, Fast Algorithms for Mining Association Rules in Large Databases, *Proceedings of the 20th International Conference on Very Large Data Bases*, Santiago, Chile, 1994, pp. 487-499.

Biographies

Hsin-Te Wu is an Assistant Professor of Department of Computer Science and Information Engineering from National Penghu University of Science and Technology, Taiwan. He received the Ph.D. Degree in Department of Computer Science and Engineering from National Sun Yat-Sen University, Taiwan, in 2013. His research interests include computer networks, wireless network, speech compression, network security and Internet of things.

Yi-Jen Su received his Ph.D. degree in electrical engineering from the National Cheng Kung University, Tainan, Taiwan, in 2007. From 2007, he worked at the Shu-Te University for 11 years. He is currently a Associate Professor of the Department of Computer Science and Information Engineering, respectively. He has published more than 50 papers in journal and conference proceedings since 2007. His current research interests includs social network analysis, sentiment analysis, data mining, artificial intelligence, e-Learning and image processing.

Wu-Chih Hu received his Ph.D. degree in Electrical Engineering from the National Taiwan University of Science and Technology, Taiwan, in 1998. From 1998, he worked at the National Penghu University of Science and Technology for 20 years. He is currently the Dean and Professor in the College of Marine Resource and Engineering and the Department of Computer Science and Information Engineering, respectively. He has published more than 130 papers in journal and conference proceedings since 1998. He obtained the Best Paper Awards of ICGEC2010, RVSP2011, ACIIDS2012, ISIC2012, and ICGEC2013. His current research interests include image processing, pattern recognition, visual surveillance, IoT, Blockchain, and Deep learning.