sustainability

MDPI

Article

Blockchain-Based One-Off Address System to Guarantee Transparency and Privacy for a Sustainable Donation Environment

Jaekyu Lee [1,†], Aria Seo [2,†], Yeichang Kim [3,*] and Junho Jeong [4,*]

[1] Department of Techno-Management Cooperation Course, Dongguk University, 123 Dongdae-ro Gyeongju-si, Gyeongsangbuk-do 38066, Korea; jaekyulee@dongguk.ac.kr
[2] Electronic Commerce Institute, Dongguk University, 123 Dongdae-ro, Gyeongju-si, Gyeongsangbuk-do 38066, Korea; seoaria@dongguk.ac.kr
[3] Department of Information Management, Dongguk University, 123 Dongdae-ro Gyeongju-si, Gyeongsangbuk-do 38066, Korea
[4] Electronic Commerce Institute, Dongguk University, 123 Dongdae-ro, Gyeongju-si, Gyeongsangbuk-do 38066, Korea
* Correspondence: kimyc@dongguk.ac.kr (Y.K.); yanyenli@dongguk.edu (J.J.)
† These authors contributed equally to this work.

Received: 28 September 2018; Accepted: 22 November 2018; Published: 26 November 2018

Abstract: The problem of transparency in donation systems has long been a topic for discussion. However, the emphasis on transparency raises privacy concerns for donors and recipients, with some people attempting to hide donations or the receipt of money. Therefore, a donation system that guarantees transparency and privacy is required to avoid negative side effects. In this study, we developed a system that protects personal information by using a one-time account address system based on a blockchain while emphasizing transparency. The developed system could contribute to the creation of a sustainable and safe donation environment and culture.

Keywords: donation system; transparency guarantee; privacy protection; blockchain; disposable address system

1. Introduction

With the development of social consciousness, a culture of donation has formed in Korea. However, the transparency within a donation system has been an issue for a long time; for example, donors typically want to know the details of how their donation is being used. However, an emphasis on transparency can lead to privacy concerns for donors and recipients. Therefore, a donation system that guarantees both transparency and privacy should be developed [1].

People who receive donations from or provide them to the donation system may not want their donations to be disclosed. Users would be able to create contracts and use the system using addresses that are not easily recognizable, if they used a donation system with a blockchain featuring security. However, in such a blockchain system, the log can be analyzed to see when the same type of address repeats the same specific action. Therefore, it is possible for a privacy issue to occur, because the user's behavior can be analyzed. That is, the donation system can track the record of donations received or provided, leading to the exposure of privacy.

In this study, we propose an address update system that avoids leaving logs that can be analyzed using a system that can update the address of a user who maintains a specific form. This system protects privacy by applying a blockchain-based peer-to-peer (P2P) mixing method that updates the address log between peers and simultaneously enhances transparency.

We review related research and analyze existing sponsorship and identity management systems in order to design our proposed system. We then employ MetaMask in the Chrome environment to create a network environment for testing sample data using our design system. The web-based Remix integrated development environment (IDE) is implemented using the Solidity language as a JavaScript virtual machine (VM) environment. The system developed in this research protects the privacy of the users of the donation system by not recording donations by a specific donor to a specific person.

2. Background Research

2.1. Donation System

2.1.1. Donation Culture

With the development of a donation culture in Korea, the total amount of donations to major private donation organizations has more than quadrupled, from 2.19 billion won in 1999 to 12.48 trillion won in 2013. Among these donations, the amount raised in the social welfare sector in 2014, as reported to the National Tax Service, was approximately 1.777 trillion won, consisting of 1485 public benefit corporations.

Individual donations account for 32.1% of all donations, or approximately 570 billion won. Based on resident registration demographics, the total adult population is approximately 41.65 million; thus, the annual donation per adult is less than 14,000 won (Figure 1). Therefore, it is necessary for individual donations to become more active in the future [2].

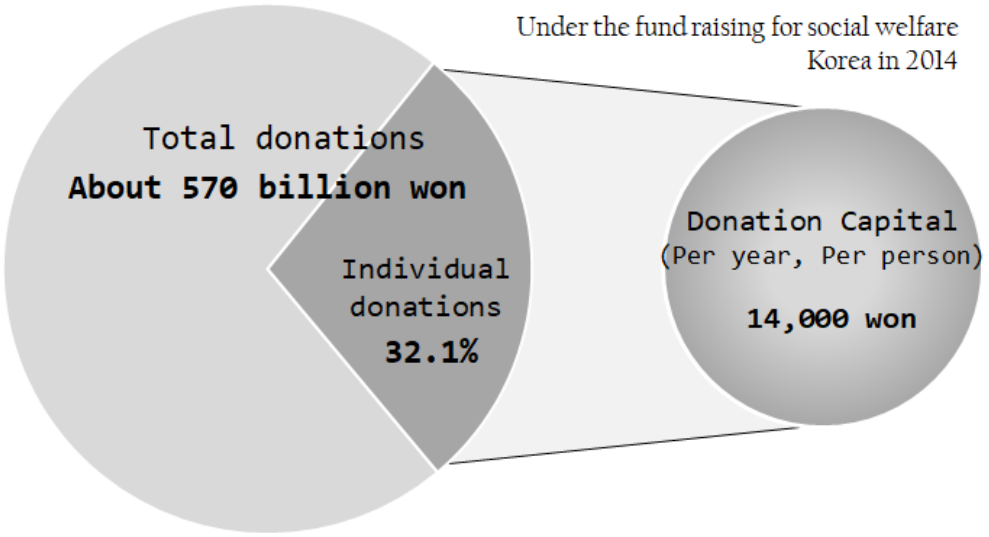

Figure 1. Percentage of individual donations among all donations in Korea.

In addition, among the 1485 fundraising institutions, the top 18 raised 77.3% of the total amount. The reason for this phenomenon is that many fundraising institutions do not properly manage regular donors, and there is a lack of information, human and material resources, and opacity of operations. Regarding the management of donors, they often want to know the details of how their contributions are being used, which requires periodic reminders. Moreover, the opacity of operations occurs either when the institution inflates the costs of in-kind donations or donation spending and contributes minimally to aid recipients or when the funding of the operating organization is fully disclosed, yet the recipient uses the donation abnormally [3,4].

Thus, the management and operation of individual donors requires substantial manpower and operating expenses; this manpower must operate ethically, so that donations can be correctly executed. Therefore, it is necessary to manage registered donors on a regular basis, recommend and connect relevant aid recipients, and provide aid recipients with the majority of funds. An audit system

for all of the activities of the system operator is supported, and—if the system is managed by a trusted organization such as a government office—effective and transparent system operation will be achievable.

In addition, existing donation systems can expose the personal information of supporters and donors and greatly violate their privacy if personal information is exposed to the operator of the donor system. Therefore, it is necessary to ensure the anonymity of donors and aid recipients from the internal operators, with only authorized persons given access to search technology for the encrypted data used to access personal information.

2.1.2. Private Support System Research

A traditional personal donation system sponsors aid recipients through fundraising organizations. However, fundraising organizations are not always transparent. Some donors do not want to disclose their donations to others. Moreover, the total amount sponsored by fundraising organizations is not made transparent because some people do not even want to know about the sponsorship [5]. Therefore, as shown in Figure 2, all personal information of donors and aid recipients must be encrypted so that it cannot be read by anyone other than the user [6–10].

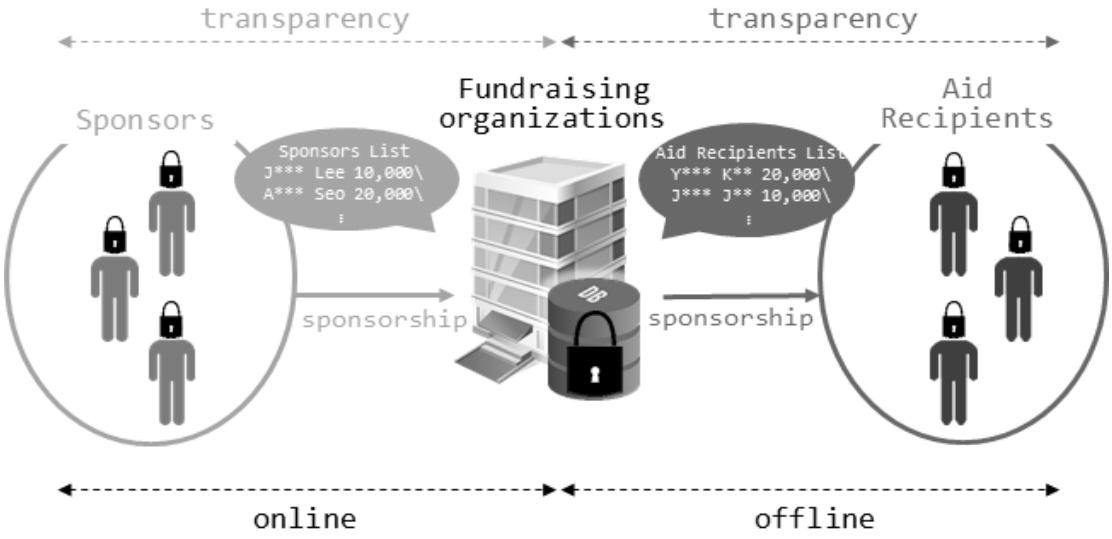

Figure 2. Encryption-based personal support system.

Fundraising organizations disclose the donations sponsored and delivered to aid recipients, yet donors cannot recognize each other through the donor list; information is provided in a form that only the donor can recognize [11–13]. For example, a sponsor named Jaekyu Lee can find himself in the form of J*** L** in the list of donors, which is open to the public, and can confirm that their donation in the amount of 10,000 won was delivered to an aid recipient named J*** L**. This allows donors to transparently handle the total amount of the donations sponsored by fundraising organizations without suffering from anonymity or privacy concerns [14,15]. In this study, we develop a one-off address system based on a blockchain that can protect the transparency of the system and the privacy of the donor and recipient to establish a sustainable donation environment.

2.2. Related Technological Research

2.2.1. Blockchain Concept

Blockchain technology is an important platform technology in the era of the fourth industrial revolution. It is designed to distribute a ledger that records transaction information to a P2P network instead of a central server, so that participants in the network can collectively record and manage

transaction details as core technology that prevents the double payment of electronic transactions. In a broader sense, it is also classified as distributed ledger technology. A blockchain is a data distribution processing technique. As shown in Figure 3, a block-to-block connection relationship is defined by the next block containing the cipher-based hash value of the previous block. Blocks contain a blockchain consisting of a block header and block body. The block header contains the hash value of the transaction contained in the hash value block of the previous block header, the Merkle root, the timestamp, bits, and nonce. Moreover, the block body contains the transaction information contained in the block and the Merkle tree of the transaction [16–18].

Blockchain technology is developed and implemented slightly differently for each platform. However, all blockchains are managed by distributed nodes and have the same appearance in the overall system due to a defined protocol. It is characterized by the fact that it is difficult to arbitrarily modify the recorded information, because each block must be computed to be recognized as a valid block. Therefore, it is increasingly being used in various systems to ensure the confidentiality of transaction details and to prevent the falsification and tampering of data. In this study, we construct a donation system that enhances transparency of a donation system, while protecting against the falsification and tampering of transaction details by using a blockchain [19–21].

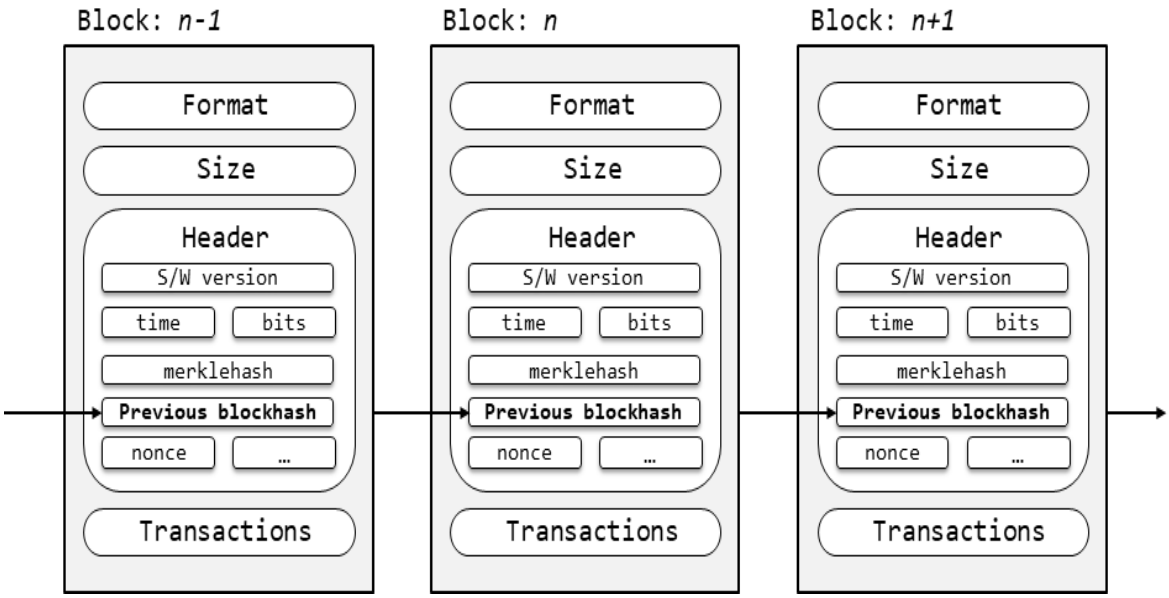

Figure 3. Concept and structure of a blockchain.

2.2.2. Smart Contract

Ethereum is a distributed computing platform for implementing smart contract functionality based on blockchain technology. Furthermore, Ethereum is the first blockchain-based smart contract platform, with the largest number of smart contracts, and a public blockchain designed to operate smart contracts based on the virtual currency "Ether". A smart contract in Ethereum operates on an open blockchain; therefore, all information is shared among all of the nodes in Ethereum. It is difficult to manipulate the information written in smart contracts because there are more than 30,000 Ethereum nodes, globally. Ethereum has an externally owned account controlled by a secret key and a contract account controlled by code. Users can create transactions through external ownership accounts to distribute smart contracts or execute code contained in smart contracts. Ethereum was the first to implement the concept of a "smart contract", providing scalability to transparently operate a variety of applications such as contracts, SNS, e-mail, and electronic voting as well as transactions and payments [22].

Smart contracts implement certain conditions with executable code. As shown in Figure 4, the contract code is executed when a message is sent to a specific address. In addition, the state

of the Ethernet is changed, or the message is sent to another smart contract. For example, when one public key and its corresponding secret key are divided into parts among n persons and each message is signed with its own private key, only k or more signatures must be authenticated through the public key. Therefore, there is a "k of n threshold signature technique" that can be used. In this study, we generate a voting contract model to change users' addresses using smart contracts and construct donation contracts to receive donations. We also build a donation system that protects the privacy of donors and recipients [23,24].

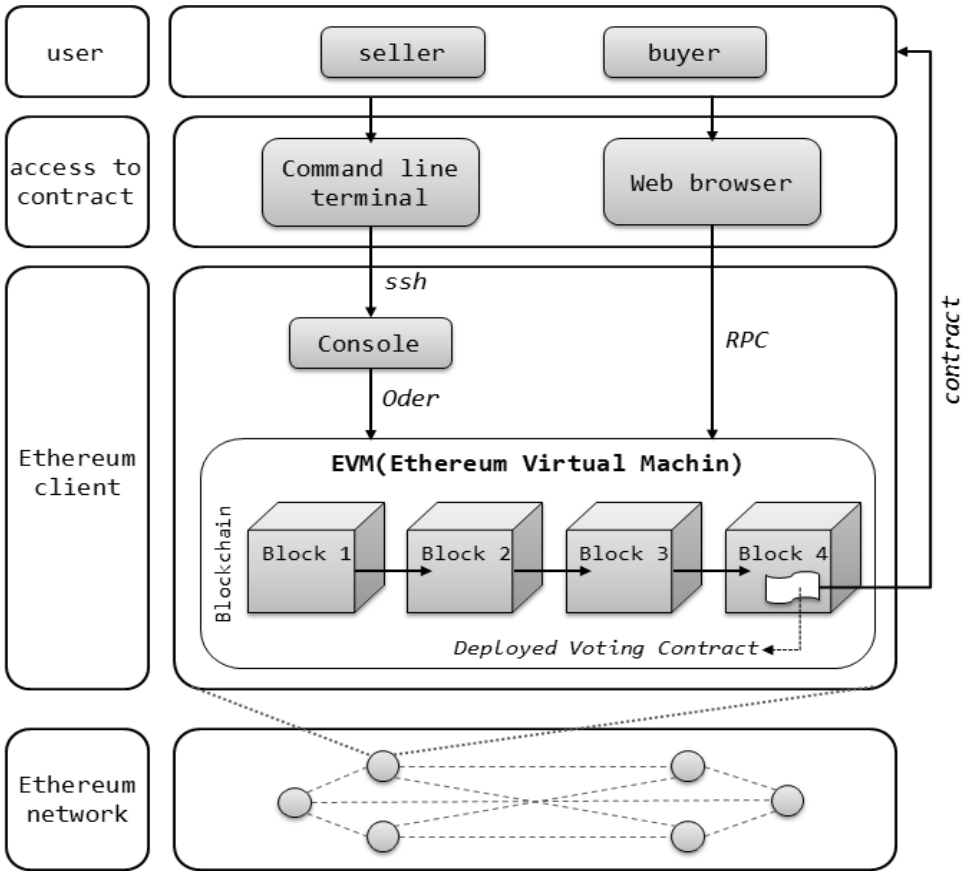

Figure 4. Smart contract operation method with Ethereum.

2.2.3. Password Currency Mixing

Cryptographic mixing has emerged to overcome the anonymity problem that occurs in blockchain-based cryptographic systems. It mixes multiple users' passwords and sends them to the target withdrawal address; thus, the source becomes ambiguous, as the transactions are processed several times because the passwords of several users have been mixed. As the number of users participating in mixing and the amount of money used for mixing increase, it becomes more difficult to trace the source.

There are two main methods of mixing. In one, a user who wants to mix cryptographic money deposits their cryptographic money into an intermediary and sends the intermediary's cryptographic money to the target address instead. The other is P2P mixing, which is a protocol in which users who want cryptographic mixing combine their cryptograms using a P2P client without intermediaries. As shown in Figure 5, the cryptographic money of user A deposited in transaction 2, in which mixing is performed, is the same as the amount of cryptographic money of user B. Therefore, it is impossible to know which user withdrew cipher money at a target address. In this study, we apply the privacy protection method using the P2P mixing method to construct a privacy protection system [25].

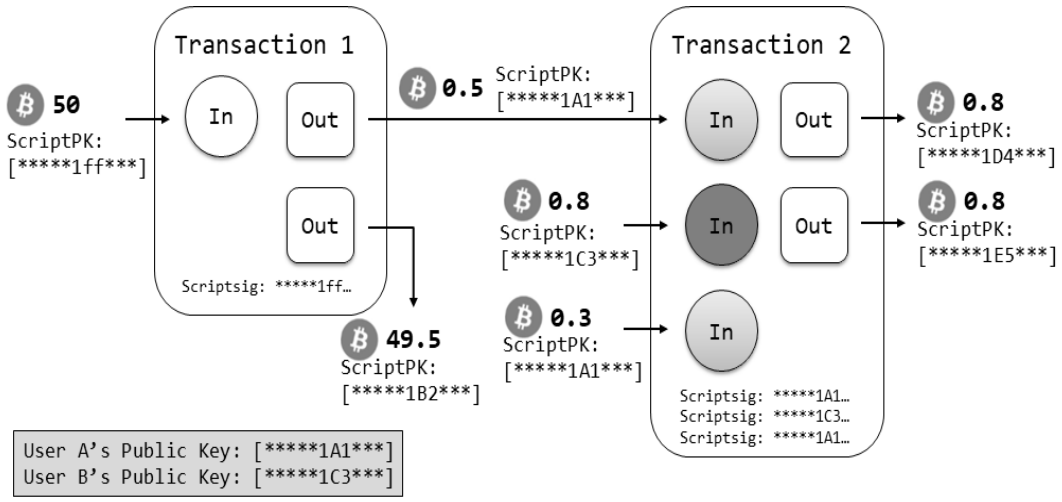

Figure 5. P2P-based cryptographic mixing technique.

2.2.4. User-Centric Identity Management Service

Figure 6 shows the structure of a user-centric identity management system using a blockchain-based smart contract that allows users to create and manage their own identities without centralized management. The system consists of an identity contract that represents the user identity, an owner account that owns the identity contract, a user that creates transactions through the owner account, a revocation contract that can revoke and renew the address of the owner account, a voter account that transfers transactions to the revocation contract, and a voter group that controls the company.

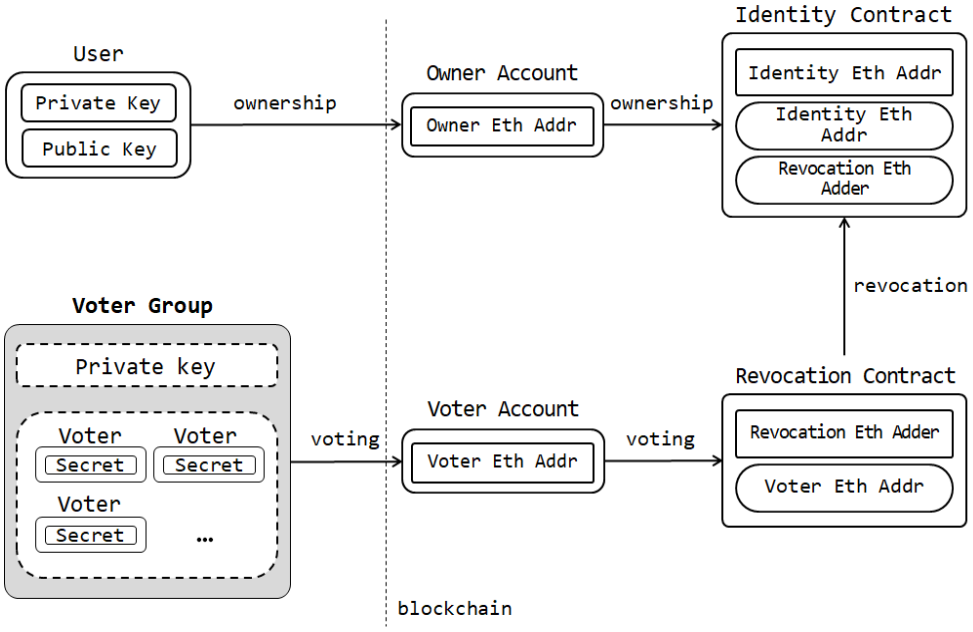

Figure 6. Blockchain-based identity management system architecture.

The user creates a pair of private and public keys. They create their own account using the generated key and obtain an address, which they use to create an identity contract that represents their identity. As the identity contract contains the address of the revocation contract, the revocation contract must be implemented to execute the identity contract. A revocation contract is a smart contract that revokes or renews an account address and is created through the voter account. The voter account is the account of the members of the voter group, which comprises the system users. If the user needs

to update the account address, the voter group sends a message to the revocation contract via the voter account. The revocation contract is executed when the number of messages is k or more on the basis of the k-out-of-n (k of n threshold signature) technique. The identity contract is then executed to update the user's address. In this study, we refer to a system that updates the user's address to protect their privacy in the donation system. A user-centric identity management service designs a system to update the user's address by constructing a smart contract on the basis of voting.

3. System Design

In this work, we develop a donation system that can increase transparency while ensuring privacy in order to solve the problems of existing sponsorship systems. The system is designed with reference to the P2P-mixing-technique-based blockchain. Therefore, donors and receivers cannot be identified by other donors and receivers. Figure 7 illustrates the process of converting an account address when sending donations. In this section, we describe the algorithm for generating the detailed structure of the system and updating the address.

1. The donor sends a donation to the receiver's account address (B) using their account address (A).
2. Voters in the voting group change their account address on the basis of the voting results using the account address (C).
3. The donor sends their donation to the changed account address (B') of the receiver using the changed account address (A').

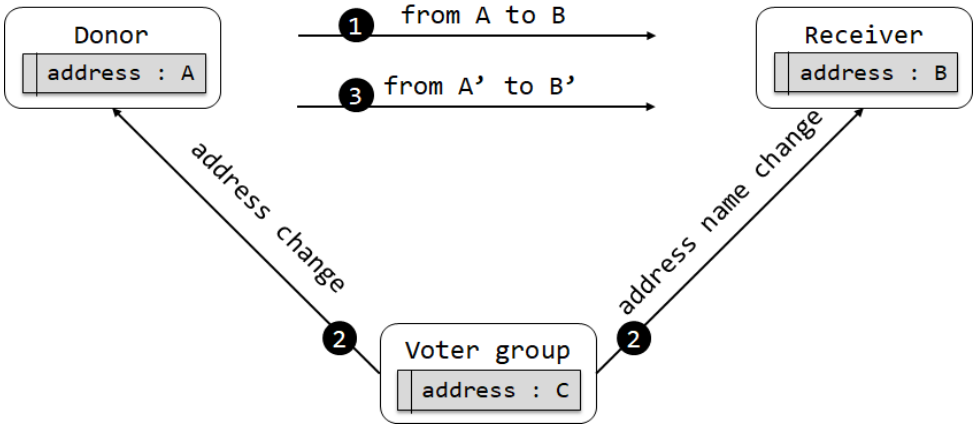

Figure 7. Process of converting an account address.

3.1. Overall System Architecture

The structure of the blockchain-based disposable address system, which provides a sustainable donation environment by protecting transparency and privacy, is as follows.

- The donor is a system user who makes donations and has a private key and a public key.
- The donor account is an account created by the donor using the public and private keys. The donor owns the donor address (Donor Eth Addr) created on the basis of the account. Addresses can be used to create and access smart contracts. The receiver is a system user who receives donations and owns a private key and a public key. The receiver account is created using the private key and public key of the receiver and owns the receiver's address (Receiver Eth Addr).
- The voter group consists of all users who use the system, and its account is termed the voter account. A renew contract is a smart contract that has the authority to execute an identifier contract through voting by the voter group. The renew contract includes the address of the renew contract (Renew Eth Add) and voter's address (Voter Eth Addr). The identifier contract is a smart contract that can modify the user's information and includes the address of the identifier contract

(Identifier Eth Addr), the user's address (Donor Eth Addr or Receiver Eth Addr), and the address of the renew contract (Renew Eth Addr). The identifier contract contains the address of the renew contract, and therefore contains the condition that the renew contract must be executed before the identifier contract.

- A donation contract is a smart contract that the donor can implement and is created by the receiver. Therefore, the donation contract includes the address of the donation contract (Donation Eth Addr) and the address of the receiver account (Receiver Eth Addr).

In Figure 8, ①~⑥ show the order in which the structure is generated in the smart-contract based one-time address system developed in this study.

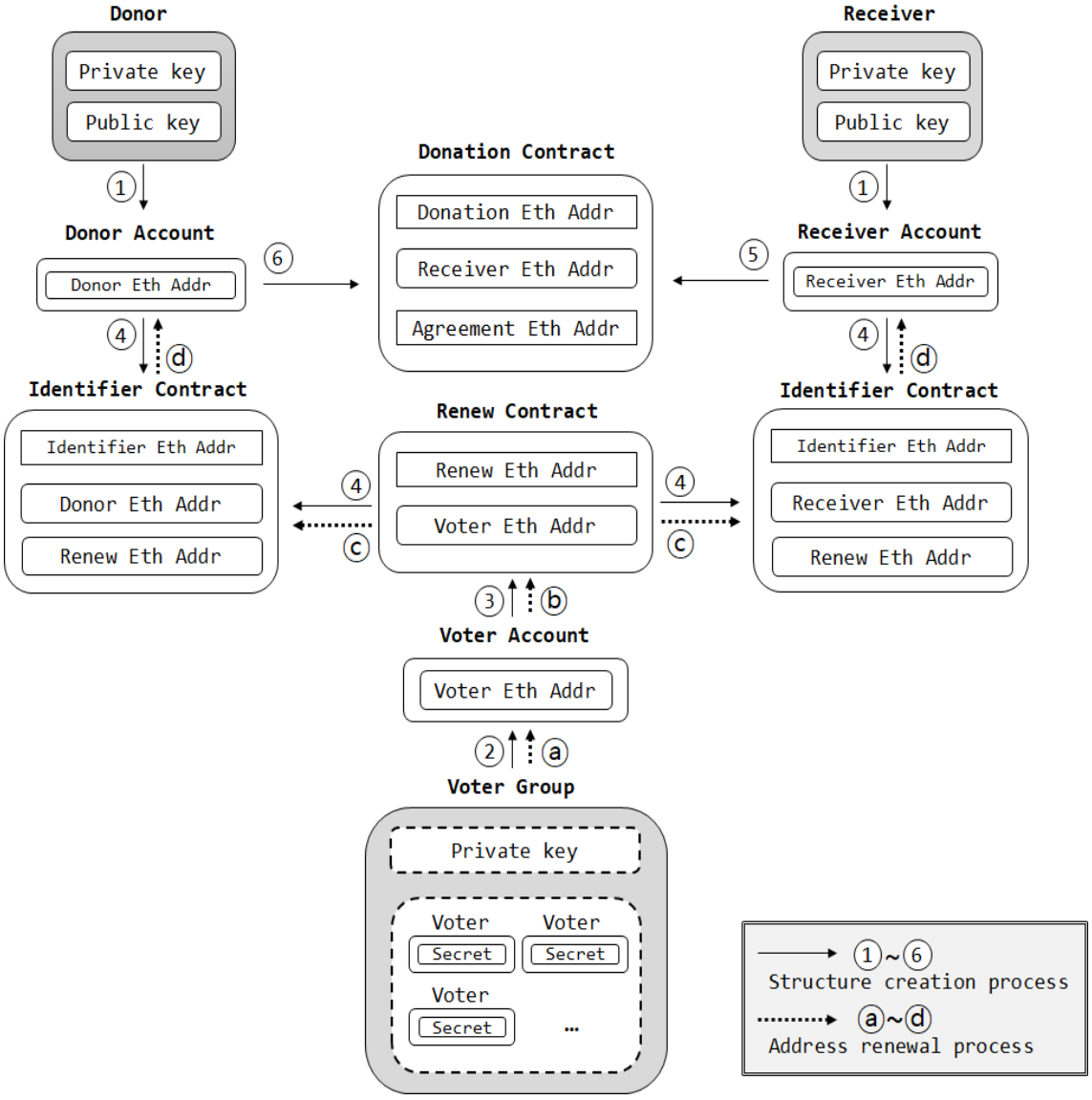

Figure 8. System processes. From ① to ⑥ shows the order in which the structure is generated, and from ⓐ to ⓓ shows the method for updating addresses.

1. The donor and receiver generate their private and public keys. Each person creates an account using the public key, and the created account holds the address.
2. The voter group accesses their own account.
3. A renew contract is created to update the account address.

4. The donor and receiver create an identity management contract that specifies the address of the renew contract (Renew Eth Addr).
5. The receiver creates the donation contract.
6. The donor donates to the receiver through the donation contract.

3.2. Address Update Technique

In Figure 8, ⓐ~ⓓ show the steps for updating addresses in the smart-contract based one-time address system.

1. When the system is configured, each voter group accesses their own account.
2. A message is sent to the renew contract to update the address.
3. When more than half of the voting group sends a message, the renew contract is executed.
4. When the address renewal contract is executed, the identifier contract is executed, and all donor and receiver addresses are updated with new addresses.

4. Sample Data Test

The system implemented in this study employs a network environment using MetaMask in Chrome. The Solidity language is used as a JavaScript VM environment in the web-based Remix IDE.

4.1. Creation of Renew and Donation Contracts

Figure 9 shows the debugging screen after the creation of the code for creating a renew contract. The generated contract is a contract renewing the addresses of the donor and receiver and corresponds to ②~③ in Figure 8. Figure 10 shows the debugging screen after the creation of the code for creating a donation contract. The generated contract is the contract that the donor will use to donate to the receiver. Donation contracts will continue to be donated records and correspond to ⑤ in Figure 8.

Figure 11 shows the results of renewing the addresses of the donor and receiver, which satisfy the execution conditions of the identifier contract by executing the renew contract. It is not easy to analyze the behavior of a user through the action of the repeated address, as the address is renewed. For this reason, this results in a reduction in the risk of privacy exposure. Figure 11 shows the results of ⓐ–ⓓ in Figure 8. In Figure 11, it is confirmed that the addresses of users A and B are changed through the renew contract created by the voting group. It can be seen that the address (0xd72d . . .) of user A (Account2) is changed to address A' (0x1e91 . . .) in Figure 11a. Furthermore, the address (0xc927 . . .) of user B (Account3) has been changed to address B' (0x6e87 . . .) in Figure 11b. The actual address changed for each user is as follows:

- Account2(A): 0xd72d684581676**********b7042f3798d8c0ffc
- Account2(A'): 0x1e919c196255b**********cf4a23b1ac261e12d
- Account3(B): 0xc92757aa17d3c**********e760d537db717d161
- Account3(B'): 0x6e877dc1e9ab8**********91d9bdfe48b5df69d

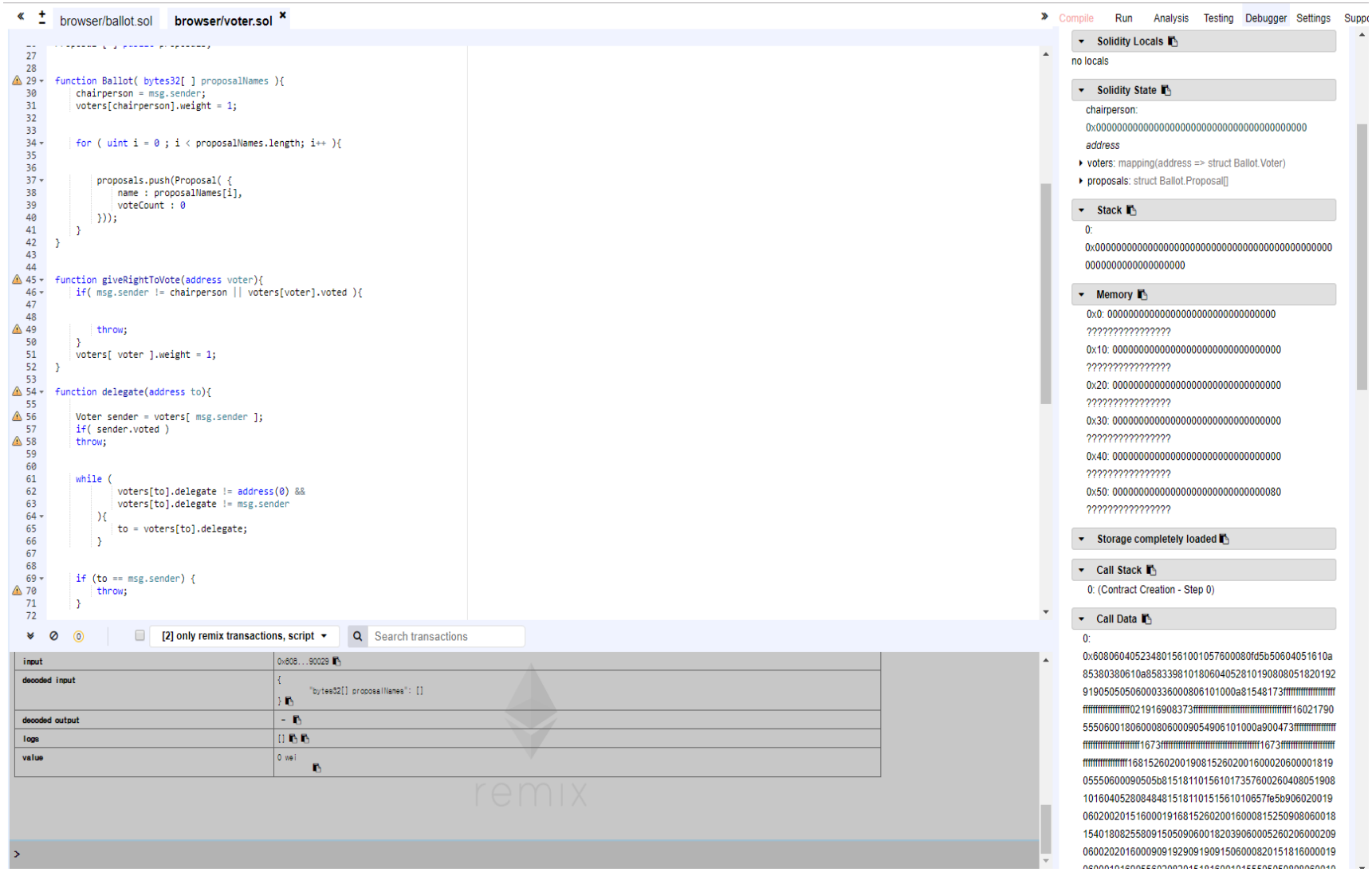

Figure 9. Code for the creation of a renew contract.

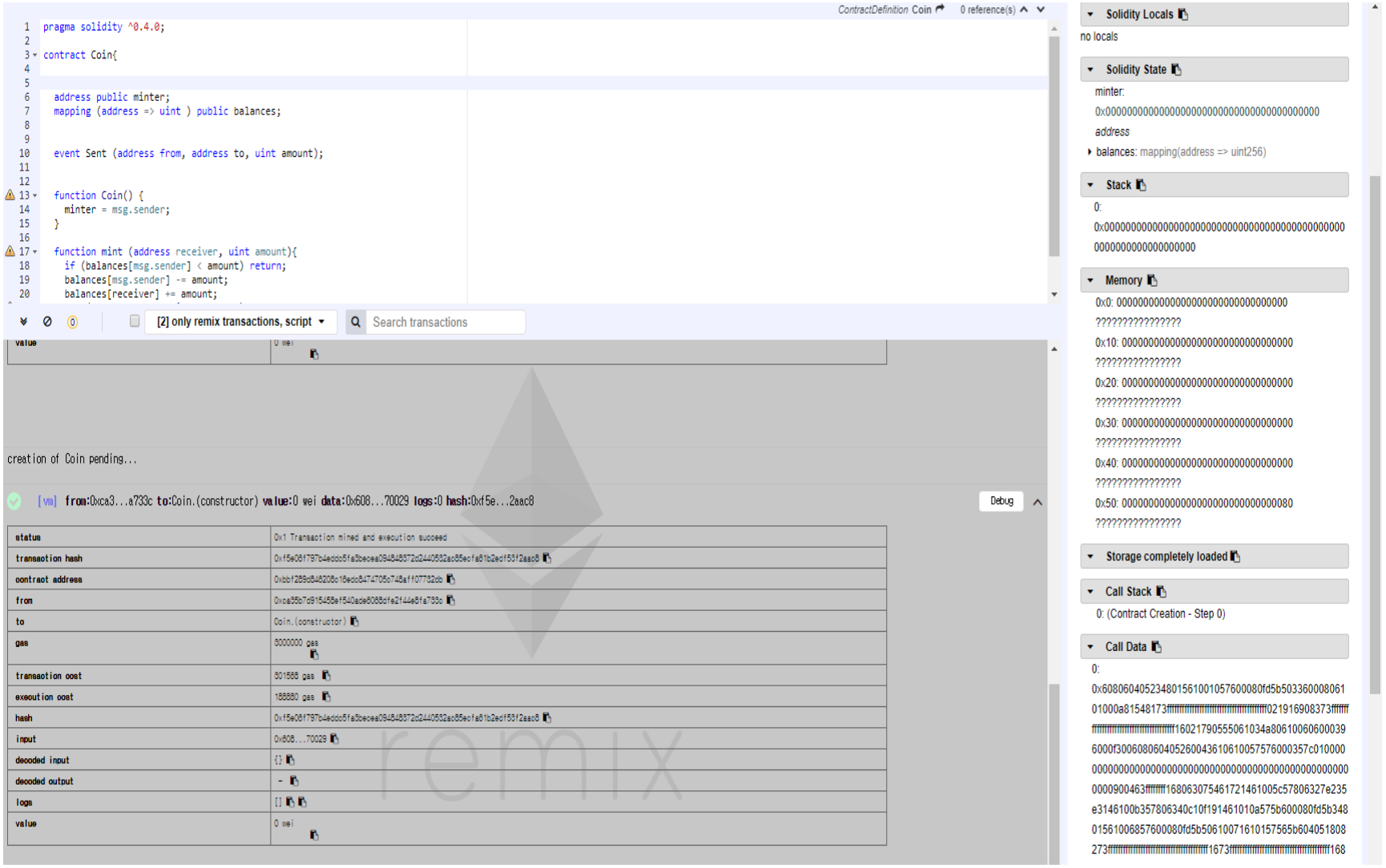

Figure 10. Code for the creation of a donation contract.

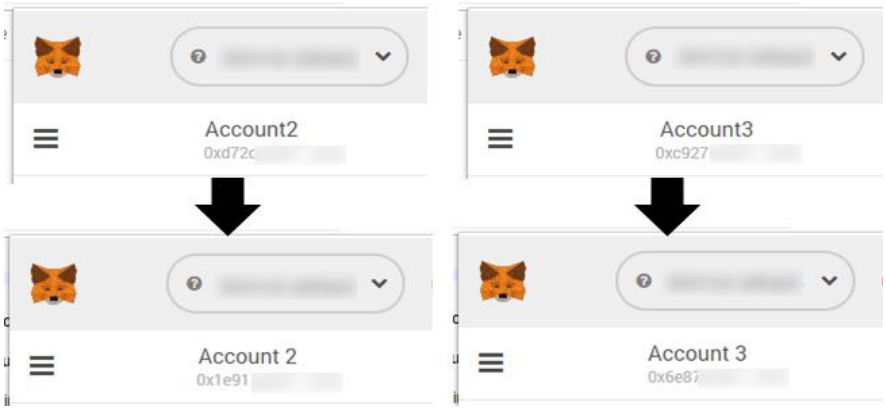

Figure 11. Confirmation of the update of (**a**) user A's address (Account 2) and (**b**) user B's address (Account 3).

4.2. Test Results

Figure 12 shows the result of testing the sample data in this study. In Phase Pharse00, A provides a donation to B through Donation Contract using the existing address. In phase Pharse01, the Voting Group creates a Renew Contract and changes the addresses of A and B. In Pharse02, A accesses the donation contract using the changed address A′ and provides a donation to the changed address B′ of B. The Pharase01 step is repeated again. The Voting Group uses the Renew Contract to change the addresses of A′ and B′. Then, Pharse02 step is performed. A′ accesses the Donation Contract using the changed address A″, and B′ provides the contribution to the changed B″.

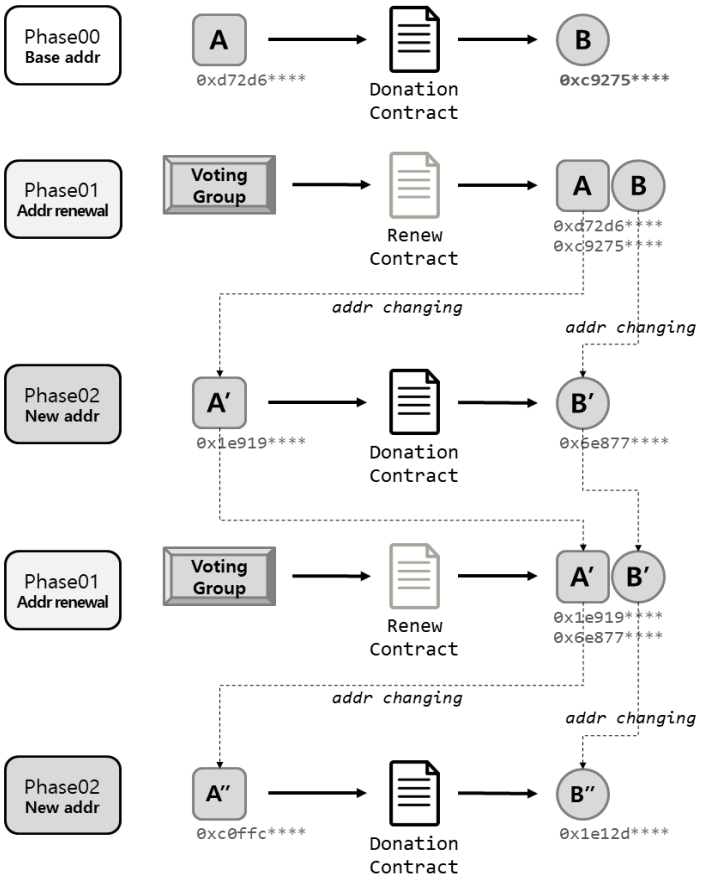

Figure 12. Sample data test results.

5. Conclusions

The existing centralized donation systems in Korea involve problems related to the transparency and privacy of users. In this study, we designed a donation system using a smart contract based on a blockchain for transparency. Through this process, donations are made transparent. We also designed a one-off address system using a smart contract to protect privacy. This protects the privacy of the users of a donation system by not recording the donation from a specific donor to a specific person.

We compare the proposed system and existing donation systems (offline and online) in Table 1. To do this, the system management technology, system management type, system transparency, privacy protection, and security assurance were compared. The proposed system can be utilized in various application system domains other than donation systems.

Table 1. Comparison of existing and the proposed systems.

Division	Existing Offline Systems	Existing Online Systems	Proposed System
System management technology	Offline ledger	An existing database-based donation system	Blockchain
System administration	Centralized system using paper ledger	Centralized system with central server	Decentralization system of P2P format
Transparency	No transparency at all	Provide transparency but lack confidence in transparency	Transactions can be browsed, and transparency reliability is assured by agreement algorithm
Privacy	No open records on the Internet	Opened for others to view transaction history or locked for nobody to see	Privacy is protected because nobody knows where the transaction originated
Integrity	Integrity is not guaranteed at all	It is a risk that data will be altered by third parties	Data cannot be altered by third party due to agreement algorithm
Security	No security	Variable security by security system in the system	Very secure with user-to-user blockchain system

Author Contributions: J.L., A.S., Y.K. and J.J. designed the overall system. J.L. and A.S. also implemented the overall system, performed experiments, and wrote the original draft. In addition, J.J. contributed to supervision and writing—review & editing.

Funding: This research was funded by the Korean Ministry of Education (NRF-2017R1D1A3B03029906).

Acknowledgments: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jeong, J.; Seo, A.; Lee, J.; Kim, Y. A Study of Private Support System Model Design for Guarantee the Privacy of Sponsors and Aid Recipients. In *Proceedings of the ISIS2017, Korean Institute of Intelligent Systems: KIIS*; 2017; pp. 1–7.
2. Kang, M.; Park, M.; Kwon, T. User-Centric Idetity Management System Using Smart Contract. In *Proceedings of the JCCI, The Korean Institute of Communications and Information Sciences: KICS*; 2016; pp. 1–2.
3. Hyeon, L.S.; Ri, K.H.; Hong, S. A Study on Blockchain Data Design Considering Personal Information Protection. *Proc. Symp. Korean Inst. Commun. Inf. Sci.* **2018**, *1*, 478–479.
4. Yang, Y.H. An Exploratory Study on the Determinants for Individual Donation in Korean Society. *J. Hum. Stud.* **2015**, *30*, 37–64.
5. Kang, C.-H.; Park, T.-K.; Oh, J.-Y. A Study on Regular Donors' Giving Duration: Application of Survival Analysis Method. *J. Korean Soc. Welf. Adm.* **2016**, *18*, 153–175.
6. Dong, Z.; Luo, F.; Liang, L. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 98–967. [CrossRef]

7. Hwang, C.-S. Activation Policies of Giving Culture to Solve Cultural Disparities. *J. Cult. Policy* **2010**, *23*, 27–43. [CrossRef]
8. Lee, M.-Y.; Yun, M.-H. A qualitative study of fundraisers'ethical dilemma and conflict in the NGOs. *J. Korean Soc. Welf. Adm.* **2015**, *17*, 247–275.
9. Son, Y.; Jeong, J.; Ko, S.; Oh, S. A Study on the Intelligent Business Matching System Using Celebrity Relationship Graph. *Int. J. Softw. Eng. Its Appl.* **2016**, *10*, 117–124. [CrossRef]
10. Debnath, S.; Ganguly, N.; Mitra, P. Feature weighting in content based recommendation system using social network analysis. In *Proceedings of the ACM 17th International Conference on World Wide Web, Beijing, China*; 2008; pp. 1041–1042.
11. Burke, R. Hybrid recommender systems: Survey and experiments. *User Model. User-Adapted Interact.* **2002**, *12*, 331–370. [CrossRef]
12. Pazzani, M.J.; Billsus, D. Content-based recommendation systems. In *The Adaptive Web*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 325–341.
13. Bellare, M.; Boldyreva, A.; O'Neill, A. Deterministic and efficiently searchable encryption. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 535–552.
14. Abdalla, M.; Bellare, M.; Catalano, D.; Kiltz, E.; Kohno, T.; Lange, T.; Malone-Lee, J.; Neven, G.; Paillier, P.; Shi, H. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 205–222.
15. Boneh, D.; Di Crescenzo, G.; Ostrovsky, R.; Persiano, G. Public key encryption with keyword search. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 506–522.
16. Jeong, J.; Hong, Y.S. An Efficient Searchable Encryption Scheme using Multi-Indices in Cloud Computing Environments. *Asia Life Sci. Suppl.* **2016**, *13*, 151–162.
17. Chen, G.; Xu, B.; Lu, M.; Chen, N. Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.* **2018**, *5*, 1. [CrossRef]
18. Sun, J.; Yan, J.; Zhang, K. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financ. Innov.* **2016**, *2*, 26. [CrossRef]
19. Nguyen, G.; Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
20. Sharma, P.K.; Moon, S.; Park, J. Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. *J. Inf. Process. Syst.* **2017**, *13*, 184–195.
21. Xiong, L.; Shi, Y. On the Privacy-Preserving Outsourcing Scheme of Reversible Data Hiding over Encrypted Image Data in Cloud Computing. *CMES* **2018**, 17. [CrossRef]
22. Young-Seek, C.; Jae-Sang, C. The Security Risk and Countermeasures of Blockchain based Virtual Currency Trading. *J. Korea Inst. Inf. Electron. Commun. Technol.* **2018**, *7*, 100–106.
23. Minhyeok, K.; Minkyung, P.; Taekyoung, K. User-Centric Identity Management System Using Smart Contact. *Annu. Conf. Korean Inst. Commun. Sci.* **2017**, *2*, 604–605.
24. Seo, A.; Jeong, J.; Kim, Y. Cyber Physical Systems for User Reliability Measurements in a Sharing Economy Environment. *Sensors* **2017**, *17*, 1868. [CrossRef] [PubMed]
25. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information* **2017**, *8*, 44. [CrossRef]