Mehran University Research Journal of Engineering and Technology
Vol. 40, No. 2, 305 - 313, April 2021
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.2102.05

Privacy Preservation for On-Chain Data in the Permissionless Blockchain using Symmetric Key Encryption and Smart Contract

Riaz Ahmad Ziar[1], Syed Irfanullah[2a], Wajid Ullah Khan[2b], Abdus Salam[2c]

RECEIVED ON 07.01.2020, ACCEPTED ON 15.09.2020

ABSTRACT

Blockchain technology provides several suitable characteristics such as immutability, decentralization and verifiable ledger. It records the transactions in a decentralized way and can be integrated into several fields like eHealth, e-Government and smart cities *etc*. However, blockchain has several privacy and security issues, one of them is the on-chain data privacy. To deal with this issue we provide a privacy-preserving solution for permissionless blockchain to empower the user to take control of transaction data in the open ledger. This work focuses on designing and developing the peer-to-peer system using symmetric cryptography and ethereum smart contract. In this scheme, we create smart contracts for the interaction of the data provider, data consumer, and access control list. Data providers register authorized users in the access control list. Data consumers can check their validity in the access control list. After successful validation, data consumers can request the security key from data providers to access secret information. Based on successful validation, a smart contract that is created between the data provider and data consumer is executed to send a key to the data consumer for accessing the secret information. The smart contracts of this proposed model are modeled in solidity, and the performance of the contracts is assessed in the Ropsten test network.

Keywords: Blockchain, Permissionless Blockchain, On-Chain Data Privacy, Smart Contract, Privacy, Ethereum.

1. INTRODUCTION

A blockchain can be described as a distributed records database. It is comprised of encrypted blocks of smaller datasets that serve as a public ledger of all digital events or transactions executed and shared by participating parties. The transactions in the ledger are verifiable by consensus of the participants of the systems at any future time upon request [1]. The information is also undeletable. The verifiable records of the transactions are used to coordinate actions and verify events without compromising the privacy of the parties or digital assets involved [2]. We can divide blockchain generally into public (permissionless) and private (permission) blockchain. In a permissionless blockchain, there is no restriction for the execution of any operation. All users have sufficient rights of reading, auditing, writing, and reviewing the operation of the blockchain such as Bitcoin cryptocurrency. A private or permissioned blockchain network is mainly designed and developed for exchanging data and information within an organization or between a group of listed people. In private blockchain the new or unknown users cannot access the blockchain till they receive a special offer from the authorized entity which controls the private blockchain, so the mining

[1] Department of Computer Science, Kardan University, Kabul, Afghanistan.
Email: r.ziar@kardan.edu.af (Corresponding Author)
[2] Department of Computing and Technology, Abasyn University, Peshawar, Pakistan.
Email: [a]syed.irfanullah@abasyn.edu.pk, [b]arbabwajid.ullah@abasyn.edu.pk, [c]dr.salam@abasyn.edu.pk

process is fully controlled by the owner of the private blockchain [11]. Because of the excellent features, the blockchain technologies can be integrated into several fields like smart grid, Internet-of-Things (IoT) and Virtual Networks (VNs) *etc*. [12]. Blockchain offers distributed transactional ledger functionalities that function autonomously and do not require a centralized trusted authority. The history of blockchain technology dates back to 2008 when it was the backbone of the bitcoin cryptocurrency. The recorded ledger updates are cryptographic and time stamped. The immutable nature of blockchain transactions increases their attractiveness to the global financial systems. Over the years, the competitiveness and cost-effectiveness of blockchain technology applications are expected to grow as a result of Moore’s Law, Kryder’s Law, and Nielsen’s Law [3]. According to Moore’s Law, the time required to process data halves every 18 months. Kryder asserts that data storage halves annually, and Nielsen observes that bandwidth doubles. every second-year.

Different sectors have the potential of taking advantage of blockchain technology in improving their efficiencies and creating sustainable development. Even though blockchain technologies facilitate the transparency and democratization of data, it poses the challenge of privacy, and therefore, a need exists for the innovation of effective solutions.

The smart contract is used as an agreement between two parties, ethereum blockchain allows users to create a smart contract for different problems. There are more than I million smart contracts on the ethereum network [3]. On the blockchain network, all the users have share of data and the entire log file of the system. This feature of the blockchain confirms availability and integrity, however, this makes data public on the network, which breaks confidentiality. Several researchers have provided solutions to mitigate the breach of information privacy on the blockchain. A pseudonym-based anonymity solution is provided by bitcoin to protect secret, but all the transaction data are present as plain text that is vulnerable to relationship analysis attack. Several other privacy-preserving models such as Monero, Zcash, and others improve the confidentiality of currency transfer but skip the support of smart contracts and programmability.

The future of several fields is optimistic about a sustainable future with the application of blockchain technology. The distribution of database management, for instance, is among several actors that increases the fficulty of system-wide data manipulation. As a result of the distribution, data integrity is maintained in baseline agricultural information, consequently safeguarding it from fraudulent activities and biases from individual groups of stakeholders, decision-makers, consumers, and non-governmental organizations [4]. Blockchain technology also eliminates chances of single-point failures due to the increased immutability and data transparency, which is transformative for an organization [5, 6]. All in all, even though the main advantage of blockchain and smart technologies lies in the decentralization of information and the reduction of failure points, the issue of privacy and security remains a concern, especially when sharing the data to open ledger. The individuals and companies are still worried about the privacy of their data to integrate blockchain in their business as the data shared is in a public network and present as plain text [17]. Privacy is still an issue that requires effective solutions, especially due to the availability of information among various parties.

2. LITERATURE REVIEW

In [6], a decentralized system has been proposed for ride-sharing on the public blockchain, the system enables drivers to share information without a trusted third party. The trip information is shared on a public blockchain, the information includes private data such as location, Date, Time, and Price. The privacy of information in the public blockchain is not guaranteed, the system uses zero-knowledge of membership proof to keep private information confident in the public blockchain. However, the system provides privacy only for trip information and cannot be used for general purposes.

A smart contract-based privacy preservation system is proposed in [7] for retrieving a sensitive record from the cloud. The authors used smart contract and blockchain technologies for authorization purposes only. This mode does not store data on the blockchain network. The data is stored in a separate database, the user can retrieve date from the database only if the user is authorized otherwise the smart contract will avoid the user from retrieving the record from the database. But the model is not used for on-chain data privacy, it is used only for off-chain data privacy. A decentralized system is proposed in [8] for electronic health record. The system has five components: Data owner, Data provider, cloud server, blockchain, and data requester. The data provider is the doctor who shares encrypted record to the cloud, the data requester is the user of the data who requests for the data to be used. This model uses re-Encryption techniques for the privacy of shared data. This model was implemented in the consortium blockchain which is not transparent as a public blockchain.

In [14], "A Smart Contract-based PKI and Identity System (SCPKI) " is proposed that is based on Public Key Infrastructure (PKI) using decentralized design through the web-of-trust model and smart contract. The system contains two main components, the first one is a smart contract which is used to provide an interface to the blockchain and manages the identity and attributes of the entity. And the second part is the clients, which interacts with the smart contract and another system. The model does not provide on-chain data privacy and the data is accessible on an open ledger. A "blockchain-based access control ecosystem" is introduced in [15] that provides data owners with a high right to control access for private data and preserve data integrity. They implement the smart contract and their functions in the Hyperledger composer tool. However, the system does not provide data privacy on the public ledger in the blockchain. In [16] the supply chain traceability system is presented based on blockchain ethereum smart contracts. In this system, each producer is required to list the ingredients of their products as recipes. This mechanism protects the raceability of each product transaction. This system is used for the traceability of the product information but it is not used for the privacy of the product data, the product data is visible for every user of the public ledger. In [18], a decentralized system is proposed that enables users to keep their privacy in permissioned blockchain. The system implements two smart contracts, the first smart contract is used by the user to upload their documents to the Inter Planetary File System (IPFS) storage, and through the second smart contract, the admin registers the users into the system. This system provides privacy for the users of permissioned blockchain but it is not usable in the permissionless blockchain. In [19], the author proposed a model for alerting the users on sharing Personally Identified Information (PII). The author used a smart contract to check PII in the information which is requested by the devices to be shared. This system reduces the risk of information sharing to the third party. However, the system does not provide privacy of information in the open ledger of blockchain technologies.

A decentralized scheme is proposed in [10] for the intelligent transport system. The authors used pseudonym management and shuffle operations to protect the identity and location of the vehicle. However, the model was used in the transportation system. It was not usable for general purpose and did not provide on-chain data privacy in the public blockchain. In [13], a decentralized model called midchain has been proposed. The model combines blockchain, midchain, and structure P2P networks to achieve privacy for health data. This model used both offline and on streaming data sharing to provide privacy for health care records. This model does not store data on the public blockchain. The privacy of individual devices in the blockchain cannot be confirmed due to the shared transactions and transmissions, which opens a loophole for third-party entities to view and analyze the transactions as well as infer the identities of the senders [9].

In the literature review, we evaluated different papers that proposed models for the privacy of data in blockchain technology but reference to the above literature, no such work is done to provide data privacy for on-chain data in permissionless blockchain using access control list and smart contract. As data sharing is the main characteristics of blockchain, and data is not protected in the public ledger. In our work we propose a model to create an environment in which data will be seen in the open ledger of public blockchain but it will be encrypted for unauthorized

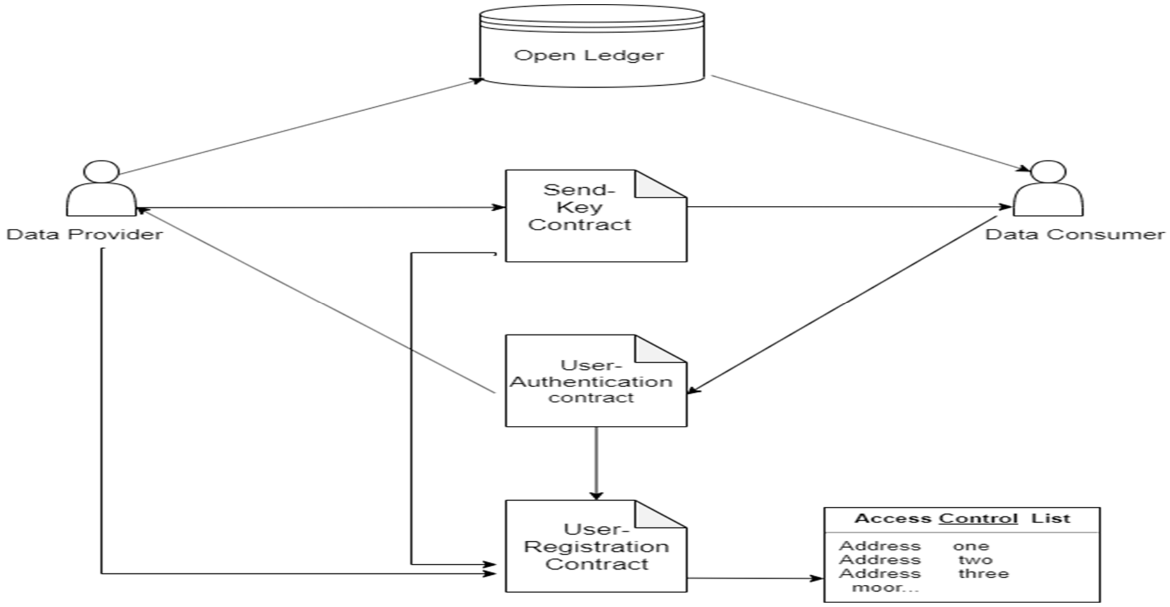

Fig. 1: Proposed Model

users while it will be accessible for authorized users with a provided decryption key.

3. PROPOSED MODEL

This section provides detailed information about the proposed model. This model focuses on the privacy of on-chain data in open ledger of public blockchain. In this model, encrypted data is shared on the open ledger and only authorized users can access that data through decryption key. The components of this model are Data provider, Data consumer, Access control list and Open ledger, as shown in Fig. 1. The model also contains three smart contracts, namely User-Registration, User-Authentication, and SendKey contracts. We first elaborate on the above components which are the parts of the proposed model.

1. Data Provider (DP): Data provider is the object (*e.g.* person, business, and process). Data providers encrypt private data using the symmetric key algorithms and share encrypted data to open ledger of permissionless blockchain network.
2. Data Consumers (DCs): These are the entities that want to access the data shared by the data provider to the permissionless blockchain networks. The consumers seek for the decryption key to decrypt data. Only the DP has the power to send the decryption key to the authorized Data consumer.
3. Access control list: This list is created by the data provider to add the addresses of all those data consumers who are allowed to decrypt the private data. The data provider can add, delete, update, and search data consumers' addresses in this list. If the address is not added in the list, the user cannot request for the decryption key.
4. Open Ledger: It is a shared database in a permissionless blockchain used to record transactions between two users. This ledger is synchronized, and each user of the network can access the copy of data from the open ledger.
5. User-Registration smart contract: is created for data provider. It is used to Add, Delete, Update, and Validate users in the Access control list. This contract will only be executed by the data provider.
6. User-Authentication smart contract: is created by the data consumer between itself and data provider. Data consumers use this contract to request a decryption key from the data provider.
7. SendKey smart contract: SendKey Contract is created by data providers between itself and Data consumers. DP uses this contract to send the decryption key to the authorized data consumer.

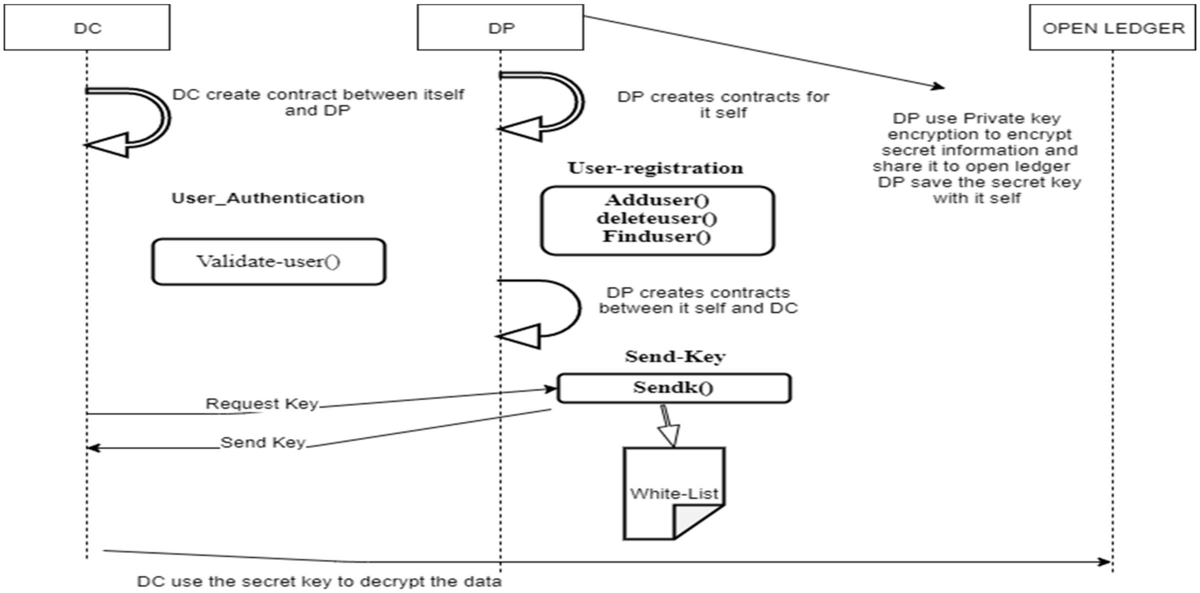
DC
DP
OPEN LEDGER
DC create contract between itself and DP
DP creates contracts for it self
DP use Private key encryption to encrypt secret information and share it to open ledger DP save the secret key with it self
User-registration
Adduser()
deleteuser()
Finduser()
User_Authentication
Validate-user()
DP creates contracts between it self and DC
Send-Key
Sendk()
Request Key
Send Key
White-List
DC use the secret key to decrypt the data

Fig. 2: Workflow of the system

The decryption key is encrypted by the public key of data consumers once it is received. The data consumer can decrypt that key with his/her private key. Fig. 2 explains the workflow of the proposed model in which DP and DC interact with each other through the smart contract defined below, to achieve privacy.

1. DP and DC must create Externally Owned ccounts (EOA) in Ethereum blockchain to communicate in the Ethereum network.
2. DP uses the symmetric key encryption algorithm to generate a key and encrypts private information. DP transfers encrypted data through the Ethereum network. DP also creates two contracts one is for itself, and the second is created between itself and DC. The first contract is used to add delete and find users from the access control list, and the second one is used to
3. DC creates a smart contract between itself and DP. This contract is used by DC to check his/her address in the access control list. After the successful validation, DC requests a key from DP. DP sends key only to those users whose address is registered in the access control list**.**
4. Finally, DC uses his private key to decrypt the security key which is encrypted by his public key and uses that security key to decrypt the secret information.

3.1 Algorithm of User-registration contract created by data provider for itself

<u>**Algorithm 1:** User-registration smart contract</u>
Input: Data consumer's Address
Output: True/False
Required: Valid data consumer Address

```
Function Adduser(Address u) onlyowner
If u is not added before
Add user to List-of-users
Return   True
Else
User already exists
     Return False
End function

Function Deleteuser(Address u) onlyowner

If u is in the List-of-users
Delete the user from the List-of-users
    Return True
   Else
     Not found
     Return False
```

```
End function

Function  Finduser (Address u)

   If u is in the List-of-users
      Return true
   Else
      Return false
End function
End
```

3.2 Algorithm for User-Authentication contract. It is created by data consumer between itself and data provider

Algorithm 2: User-Authentication smart contract
Input: Data Consumer Address
Output: True/False
Required: User Address and connection with user registration smart contract

```
Function Validate-User (Address DC)

f DC is present in the list-of-users
       Send security key to DC
       Return True
     End
     Else
       Return False
     End
End
```

3.3 Algorithm for contract Send-key. This contract is created by data provider between itself and data consumer

Algorithm 3: Send-Key smart contract
Input: DP and DC address and Encrypted Key
Output: Encryption Key
Required: DC Address and encryption key
Required: encryption of security key with the public key of DC

```
Function sendkey(Address DC, Address DP,
encrypted-key)
Send Key to Data consumers
           Return true
  End
```

A smart contract is an agreement between two parties. It provides several security benefits such as authorization, authentication, and audit. Similarly, when the transaction is executed between DP or DC, the authentication is sure and only the authorized DP and DC users have the right to perform the transaction. Second, the Users-Authorization contract will achieve the authorization when the DC requests the Encryption key. The encryption key will be sent only if the address of DC is present in the access control list. Third, one of the features of blockchain is to store data permanently. With the help of this feature, people can easily audit the transaction information in the future. Finally, the public and private keys are assigned for each DP and DC, and the hacker cannot decrypt the transaction data between DP and DC without having the prior knowledge of the private key. However, the proposed model is deployed by those smart contracts that we have described in the previous section.

4. RESULTS AND DISCUSSION

This section provides detailed information about the deployment charge of smart contracts and the execution cost of their functions. We used the Ropsten test network for the experiment of this system. The solidity programing language is used for the development of smart contracts, practicing remix online IDE. We finished the development of this system in September 2019. On the mentioned date, 1 ether =173.12 USD dollars and 1 gas =1e9 ether, which is the lower cost of a transaction. For less expenses, the transaction will take a long time to be executed and vice versa.

The deployments of smart contracts and the execution of their functions have charges. The following figures contain the deployment cost of the contract and the execution costs of their functions. The one-time cost of smart contract creation for User-Registration, User-Authentication, and Send-key are 0.000594826, 0.000174, and 0.000218 ether respectively. After the conversion of ether to USD dollar, the costs are respectively 0.10, 0.03, and 0.04 US$. The cost of contract creation is lesser than the execution cost of their functions. The execution cost of the function is not fixed, it is changeable based on the length of input data.

In Fig. 3, we calculate the total cost of smart contract deployments. Three smart contracts are designed for the proposed system. The user registration smart contract has four functions that are used for Create, Read, Update, and Delete (CRUD) operations. The sendkey contract is used to send the decryption key for the authorized users and a user-authentication smart contract is used for the authentication of users.

In Fig. 4, the execution cost of AddUsers() function is presented. The function consumes gas on the user is added to the access control list. The result shows that the function consumes very less gas per transaction which shows the proposed model is more suitable and inexpensive.

In Fig. 5, the gas consumption for the Deleteuser() function is presented. This function uses gas for user deletion from the access control list. The figure shows that it uses a very limited gas. From the simulation result we observe that our system is efficient and the operation is not expensive.

Fig. 6 shows the execution cost of the sentkey function. This is used by the admin user to send the decryption key to authorized users. The function is designed to consume less gas. The figure shows the cost of the function which is approximately zero dollars.

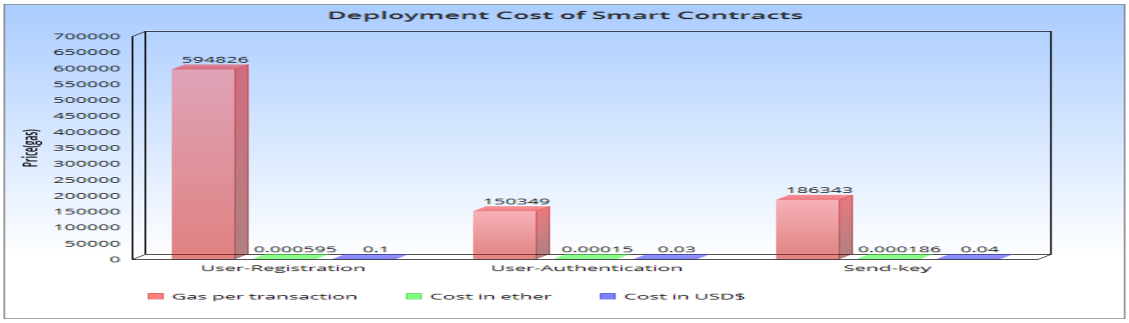

Fig. 3: Deployments Cost of Smart Contracts

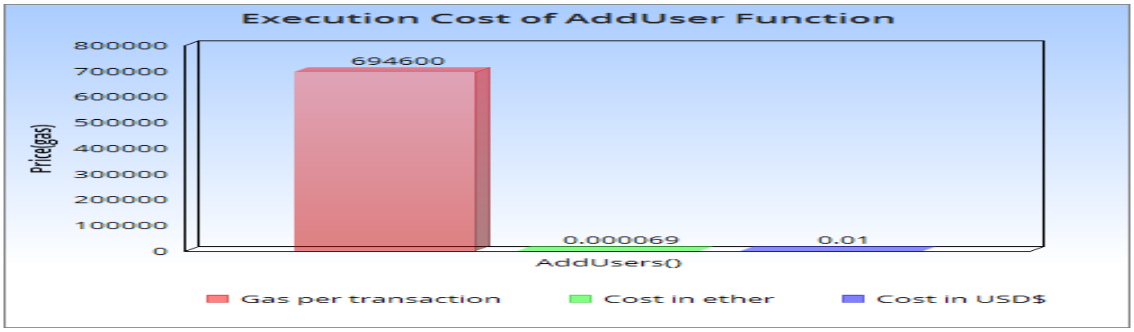

Fig. 4: Execution Cost of Add Users function

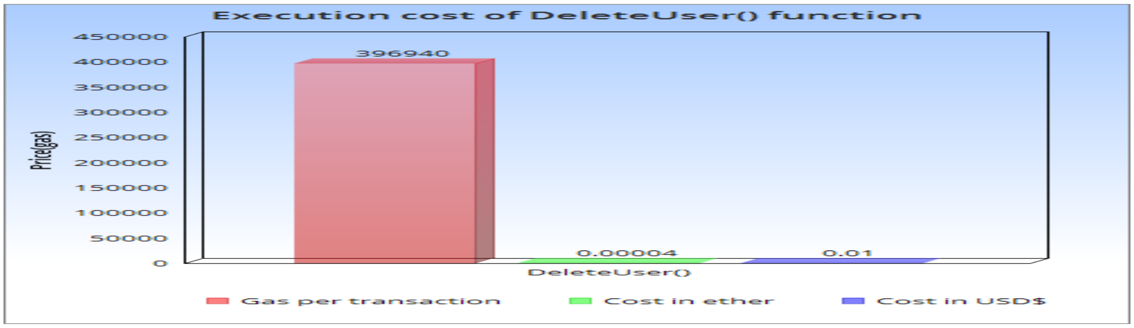

Fig. 5: Execution Cost of DeleteUser() function

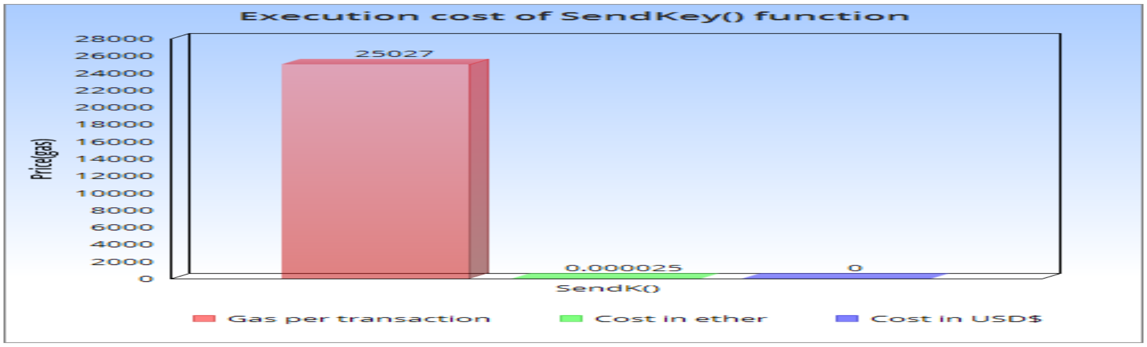

Fig. 6. Execution Cost of SendKey() function

4.1 Safety Analysis

This system combines the use of the access control list, Ethereum smart contract, and private key encryption to provide privacy and security. In a permissionless blockchain, the transaction data is shared on the open ledger and presented as plain text. All users of the network can easily access the data from the open ledger. In the proposed model the data providers have full control over their private data, the data is encrypted by the symmetric key algorithm and not readable for the unauthorized users, no third party has access to collect private information about the data provider. The DP also has the power to issue decryption key for data consumers, as only authorized data consumers can request the decryption key. In our system, we use an access control list to keep a record of authorized users. The access control list is used by both the data provider and data consumer to validate the users. Moreover, we use the Ethereum blockchain network for the implementation to provide communications for all participants and stored records permanently. Stored records will support users to backtrack the records or transactions if they are needed for verification purposes.

5. CONCLUSION

Data privacy is an important issue for the individual and organization who/which want to use permissionless blockchain for data sharing. As the data is public in the blockchain network and each user of the network access the copy of data, therefore a solution is needed to provide data privacy in permissioneless blockchain. In this work, we propose privacy-preserving smart contracts for the permissionless blockchain to secure any private information between blockchain users. The DP share data in encrypted form in the open ledger and unauthorized users cannot access the pieces of information. Only those users who have the decryption key can access the information. DP has the authority to issue the Private key for authorized users. The smart contracts for DP and DC are programmed in the Ethereum blockchain using solidity language. The proposed model is tested in the Ropsten test network.

REFERENCES

1. Hassan M. U., Rehmani M. H., Chen J., "Privacy preservation in blockchain-based loT systems: Integration issues, prospects, challenges, and future research directions", *Future Generation Computer Systems*, Vol. 97, pp. 512-529, 2019.
2. Galvez J. F., Mejuto J. C. Simal-Gandara J., “Future challenges on the use of blockchain for food traceability analysis”, *Trends in Analytical Chemistry*, Vol. 107, pp. 222-232, 2018.
3. Yuan R., Xia Y., Chen H., Zang B., Xie J., "ShadowEth: Private Smart Contract on Public Blockchain", *Journal of Computer Science and Technology*, Vol. 33, No. 3, pp. 542-556, 2018.
4. Sun J., Yan J., Zhang K. Z. K., "Blockchain-based sharing services: What blockchain technology can contribute to smart cities", *Financial Innovation*, Vol. 2, No.1, pp. 1-9, 2016.
5. Davidson S., De Filippi P., Potts J., “Blockchains and the economic institutions of capitalism”, *Journal of Institutional Economics*, Vol. 14, No.4, pp. 639- 658, 2018:
6. Baza M., Lasla N., Mahmoud M., Srivastava G., Abdallah M., "B-Ride: Ride Sharing with

Privacy-preservation, Trust and Fair Payment atop Public Blockchain", *IEEE Transactions on Network Science and Engineering*, pp. 1-1, 2020.

7. Siraj M. N., Udzir N.I., Asmawi A.M.D.H.A., "SmartCoAuth: Smart-Contract privacy preservation mechanism on querying sensitive records in the cloud", *arXiv preprint arXiv:2004.02543*, 2020.
8. Wang Y., Zhang A., Zhang P., Wang H., "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain", *IEEE Access*, Vol. 7, pp. 136704-136719, 2019.
9. Fabiano N., "The Internet of Things ecosystem: the blockchain and data protection issues", *Advances in Science, Technology and Engineering Systems Journal*, Vol. 3, No. 2, pp. 01-07, 2018.
10. Bao S., Cao Y.. Lei A., Asuquo P., Cruickshank H, Sun Z., Huth M.. "Pseudonym Management Through Blockchain: Cost-Efficient Privacy Preservation on Intelligent Transportation Systems", *IEEE Access*, Vol. 7, pp. 80390-80403, 2019.
11. Peng L., Feng W., Yan Z., Li Y., Zhou X., Shimizu S., "Privacy Preservation in the permissionless blockchain: A survey", Digital Communications and Networks, 2020.
12. Javed M., Rehman M., Javaid N., Aldegheishem A., Alrajeh N., Tahir M., "Blockchain-Based Secure Data Storage for Distributed Vehicular Networks", *Applied Sciences*, Vol. 10, No. 6, p. 2011, 2020.
13. Shen B., Guo J., Yang Y., "MedChain: Efficient Healthcare Data Sharing via Blockchain", *Applied Sciences*, Vol. 9, No. 6, p. 1207, 2019.
14. Al-Bassam M., "SCPKI: A Smart Contract Based PKI and Identity System", *Proceedings of the ACM Workshop on Blockchain, Cryprocurrencies and Contracts,* pp. 35-40, 2017.
15. Uchibeke U.U., Schneider K.A., Kassani S.H., Deters R., "Blockchain Access Control Ecosystem for Big Data Security", *Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing and IEEE Smart Data,* pp. 1373-1378, Halifax, NS, Canada, 2018.
16. Westerkamp M., Victor F., Kupper A., "Blockchain Based Supply Chain Traceability: Token Recipe Model Manufacturing Processes", *Proceeding of the IEEE Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Smart Data*, pp. 1595-1602, Halifax, NS, Canada, 2018.
17. Bernabe J.B., Canovas J. Hernandez-Ramos R., Moreno T., Skarmeta A., "Privacy-Preserving Solutions for Blockchain: Review and Challenges", *IEEE Access*, Vol. 7, pp. 164908-164940, 2019.
18. Kapsoulis N., Psychas A., Palaiokrassas G., Marinakis A., Litke A., Varvarigou T., "Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy- Oriented Decentralized Architecture", *Future Internet*, Vol. 12, No. 2, p. 41, 2020.
19. Ziar R., Irfanullah S., Omar R., "Smart Contract-Based Alert System for Reduction of Information Privacy Paradox and Fatigue in IoT", *Kardan Journal of Engineering and Technology*, Vol. 1, No. 1, pp. 37–47, 2019.