SCDP: Smart Contract-based Decentralized Privacy System for Securing Data Ownership Management

Yunmin He*†, Yu-Chi Chen†, Zhong-Yi Guo†, Raylin Tso‡, Shaozhen Ye*
*College of Math. and Computer Sci., Fuzhou University, Fuzhou, China
Emails:hymgy@foxmail.com, yeshzh@fzu.edu.cn
†Dept. of Computer Science and Engineering, Yuan Ze University, Taoyuan, Taiwan
Emails:wycchen@saturn.yzu.edu.tw, b3751282@gmail.com
‡Dept. of Computer Science, National Chengchi University, Taipei, Taiwan
Email:raylin@cs.nccu.edu.tw

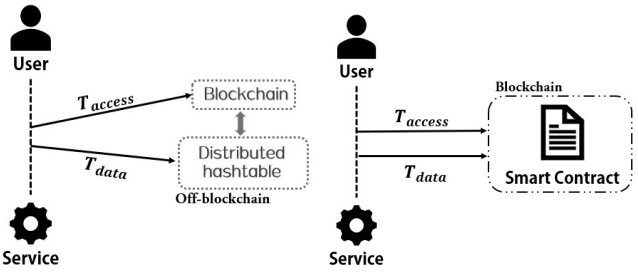
***Abstract*—Secure data ownership management is significant for realizing personal and private data sharing, which can be widely used with consumer electronics. The notion of the decentralized privacy (DP) is introduced by Zyskind et al., and accordingly the first DP system is implemented through blockchain and off-blockchain distributed hashtable. To address the efficiency and overhead issues, we present a conceptually simple solution directly from smart contracts with cryptographic primitives. Our system is called the smart contract-based decentralized privacy (SCDP) system. We propose the basic SCDP system as a warm-up to introduce the design principle based on symmetric encryption. Moreover, the strong SCDP system is provided by using ciphertext-policy attribute-based encryption for supporting more flexible scenarios of access control and also eliminating some limitations of the basic system.**

***Index Terms*—Decentralized privacy, Smart contracts, Encryption, Ownership, Access control**

I. Introduction

With the trend of information technology and users' activities, the size of data has gradually blown up, and accordingly IT has also entered the era of big-data. Explicitly, *data* plays an extremely important role as a row material to bring plenty of advantages beyond imagination. Therefore, privacy and security issues about user data also attract research attentions. Recently, Zyskind et al. [5] proposed a decentralized personal data management system implemented by blockchain [2] and off-blockchain storage to solve privacy problems. Their decentralized privacy (DP) system helps users ensure data ownership and fine-grained access control. As shown in Fig. 1.(a), there are two types of transactions in DP system: T_{access}, for access management; and T_{data}, for data transmission and usage. However, we found that this system decouples the main functionality into two functions where the permission power is delegated to blockchain and the users' data are stored in the off-blockchain distributed hashtable. Thus, this really induces a few communication overhead to connect these two distinct functions.

In this paper, to overcome the above-mentioned issues, we propose a smart contract-based decentralized privacy (SCDP) system. The overall architecture of this system is shown in Fig. 1.(b). This system is mainly composed of three entities: user, wants services and provides personal data; service, provider of corresponding functions; and smart contract



(a) Overview of DP system. (b) Overview of SCDP system.

Fig. 1. Comparison of two systems.

(SC) [3], achieves interaction between the user and service. Obviously, in this SCDP system, both T_{access} and T_{data} are implemented through SC to avoid extra connection overhead.

II. Smart Contract-based Decentralized Privacy Systems

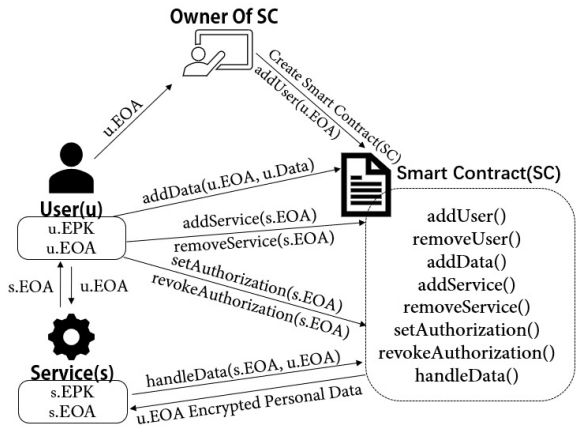


Fig. 2. Specific execution of the basic SCDP system.

Firstly, combining the SC and symmetric encryption technology, we propose the basic smart contract-based decentralized privacy (SCDP) system. The specific process of this basic system is shown in Fig. 2. For a clear illustration, we show an example: the owner of SC will create an SC and deploy it upon the blockchain initially. Then, the owner adds a user

978-1-7281-3575-5/19/$31.00 ©2019 IEEE

into the system when he/she signs up. After that, the SC will send relevant permissions and user's externally owned address (u.EOA) to the blockchain through T_{access}. Meanwhile, the personal data of the user will be encrypted and sent to the SC through T_{data}. The encryption of data uses the symmetric encryption scheme and the encryption key is Shared between the user and service. The user in the system can add required service and the service's externally owned address (s.EOA) into the SC, and then grant a set of permissions about data to the service through T_{access} if needed. Moreover, the user can also revoke the permissions if he/she wants. Once being authorized, the service can obtain the encrypted personal data through T_{data} and decrypt it with the shared key to provide corresponding services. Ultimately, the user can remove the service from the system. And if the user applies to revoke his/her account, the owner of SC can also remove the user from the system.

The basic SCDP system solves the efficiency and overhead problems of [5] to certain extent, but introduces some new defects: the owner of SC is given excessive unnecessary privileges; multiple users and services in a single SC and so on. In order to address these issues and enhance the security of the system, we reconstruct the basic SCDP system with the ciphertext-policy attribute-based encryption (CP-ABE) [1]. The reconstructed strong SCDP system is shown in Fig. 3. In this system, the user itself becomes the owner of the SC who controls the additions and removals of multiple services.

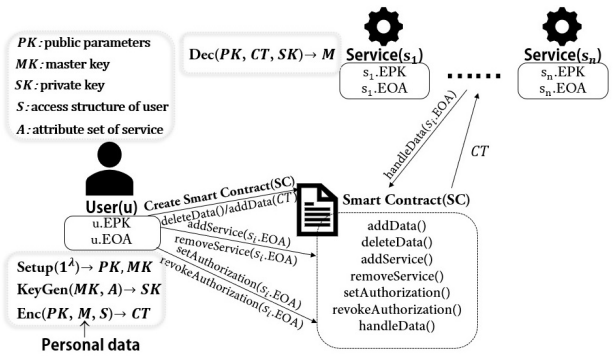


Fig. 3. Specific execution of the restructured strong SCDP system.

Our strong SCDP system is mainly composed of the following four functions: $Initialization$ achieves the initialization of the entire system; $DataProcessing$ encrypts and transfers personal data of the user; $Authority$ is related to grants and revocations of data permissions; $DataDecryption$ eventually achieves data decryption and service provision. The specific descriptions of the four main steps are as follows:

- $Initialization$: The user u initially creates and deploys the personal SC on blockchain. Then, u generates the public parameters PK and master key MK.
- $DataProcessing$: The personal data M of the user u is encrypted into the ciphertext CT which then can be sent to the SC through T_{data}. In addition, u also can delete related personal data in the system through T_{data}.
- $Authority$: When she/he needs a third-party service, u as the owner of the SC adds the service s_i $(1 \leq i \leq n)$ and the service's externally owned address (s_i.EOA) into the system, then can grant or revoke a set of permissions to s_i through T_{access} at any time. In addition, u can also succinctly remove s_i from this system.
- $DataDecryption$: The service s_i can correctly decrypt the ciphertext CT and obtain the personal data of u if and only if its own attribute set A satisfies the access structure S of u. Finally, s_i can provide functions which u needs through the obtained data.

III. Analysis

We compare our SCDP system with the original DP system in terms of different attributes. The specific comparisons of the two systems are shown in Table I. Also, we evaluate the costs where in Ethereum all operations require Ether and gas [4]. Up to May 2019, 1 Ether ≈ 249.95 USD, and 1 gas ≈ 1 wei (0.000000001 eth). The costs of executing various functions of SC in this system are shown in Table II (costs of data-related functions are affected by data size).

TABLE I
Comparison of two DP systems

Two DP Systems	Main Attributes			
	Data ownership	Access control	Blockchain	Off-blockchain
DP	Achieved	Achieved	Required	Required
SCDP	Achieved	Achieved	Required	Not required

TABLE II
Costs of Different Functions

Function	Gas Used	USD
Deploy Contract	1820106	0.4549
addService	111533	0.0279
removeService	23698	0.0059
setAuthorization	30677	0.0077
revokeAuthorization	30941	0.0077

IV. Conclusions

In this paper, we present SCDP systems. Conceptually, they combine SC with cryptographic techniques to achieve our goals for functionality, and moreover avoid some overhead issues in the previous DP system.

Acknowledgements

This work supported in part by Taiwan Ministry of Science and Technology under grant 106-2218-E-115-008-MY3.

References

[1] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE, 2007.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] Nick Szabo. Smart contracts. *Unpublished manuscript*, 1994.

[4] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32, 2014.

[5] Guy Zyskind and Oz Nathan. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.