The Private Key Sharing of Blockchain and Its Applications for Digital Assets

Elisha Tseng
Wagor International School
Taichung, Taiwan

Kate Tseng
Wagor International School
Taichung, Taiwan

***Abstract*—The purpose of this paper is to discuss the problems of private keys stolen and lost, and how it influences the wallet security of digital assets. On basis of Secret Sharing by Adi Shamir, this paper indicates the methods and future development of private key trusteeship and wallet supervision.**

Keywords——Private Key, Wallet, Blockchain, Smart Contract, Secret Sharing

I. INTRODUCTION

As digital assets and virtual currency have been rising recently, blockchain wallet security has also received more attention progressively. Private key is the only and the most crucial defense to the wallet. Yet private key may face the risk of being lost or stolen. Once the private key to the wallet is lost or stolen, chances are that digital assets might not be reclaimed. Therefore, the solution to secure the private key is essential.

The main issue with current blockchain systems is that users will not be able to access their keys due to damaged or lost devices. Although blockchain technology is decentralized, key management has become the sole responsibility of the user. Key management is distinct from the centralized approach of general account passwords which require administrators and IT personnel to reset or create passwords. Nonetheless, the current systems lack of this function, and the loss of assets will occur. The New York Times stated that it had caused loss of up to 220 million US dollars by forgetting passwords of the private key to the Bitcoin encrypted wallet. According to Chainalysis, approximately 20% of Bitcoins, which worth about $210 billion US dollars, have not moved in the past five years or more. Hence, they were considered lost.

Currently, there are tools on the market to protect private keys, such as Cold Wallet and Hot Wallet [1]. Howbeit, they have advantages and disadvantages. For Cold Wallet, it can be well protected, but there are many restrictions on use. Also, there may be problems with the hardware itself being broken. As for Hot Wallet, it may be at risk of being hacked. In addition, some users are willing to host assets in centralized institutions, such as cryptocurrency exchanges, etc. However, this practice violates the uniqueness of decentralization and anonymity of the blockchain. Assets locked or lost prove the that the exchange securities trustee of private keys is uncertain.

On basis of the Secret Sharing (SS) scheme by Adi Shamir [2], the project states that the private key can be split through the SS scheme when the user would like to use the private key. If it is just a general SS scheme, there will must be a center role, whom may cause the leakage of private key fragments or even crack it. With the modified SS scheme by Smart Contract of the blockchain, the demander can call Smart Contract to generate the key, distribute it and provide Master Secret Key while using private keys. Subsequently, the system will generate a sub-key and segment it. The sub-key will be restored according to the t-n setting, which can solve the above defects. The following questions are to be explored and solved in this paper: security storage of splitting private keys, seizure of illegal gains, and inheritance and transfer of digital assets.

1. Security Storage of Splitting Private Keys

The private key to the wallet is indispensable. Once it is stolen or lost, it will result in irreparable loss. In consequence, the security of the private key to the user's wallet must be guaranteed. In the first year of this paper, it is expected to propose an effective solution to divide the private key through Smart Contract of the blockchain.

2. Seizure of Illegal Gains

After supervisor seize the criminals' private keys to wallets, it is possible for supervisors to cooperate with other criminals to move keys and assets or steal wallets. This paper has adopt the first-year private key fragments to encrypt and decrypt the trusteeship of keys. Smart Contract of the blockchain is used as a platform to trustee private keys and extended to the related applications. Afterwards, this paper was expected to seize illegal gains from digital assets in the second year. Private keys should be trusteed after supervisors' seizure, and splitting private keys through Smart Contract can achieve a safer supervision mechanism, preventing abettors from moving keys and assets in a short time. Besides, it prevents stealing from supervisory personnel.

3. Inheritance and Transfer of Digital Assets

If information, such as the private key, is not provided to the family, the encrypted assets cannot be transferred to the family, and the family cannot withdraw the assets smoothly while the holder passing away. Expectedly, Smart Contract in the first year will be able to preset the receivers. Triggered by Smart Contract, the keys will be sent to the preset receivers in order to achieve an effective mechanism for digital assets inheritance. In the third year of this paper, it is to be used for the application of digital asset inheritance to solve the problem of digital asset inheritance by Smart Contracts.

II. MOTIVATION AND BACKGROUND

1. Frequent Private Key of Wallet Stolen

Recently, private key management has received more attention since it is essential and confidential information of personal privacy. With the upsurge of investments in cryptocurrencies and NFT (Non-Fungible Token), the problem of capital security has arisen. For instant, the private key is lost or stolen, especially for personal digital asset wallets. Therefore, a more secure and proper key management mechanism is needed. When storing the management key, it can provide higher security to ensure the security of private key management.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

2. Improved Secret Sharing proposed by Shamir

Shamir proposed the key sharing method of "Secret Sharing." Private key segmentation refers to dividing a private key, which is the master key, into several fragments, and least one part of them is required to restore the master key. This method is to prevent unauthorized persons from obtaining the entire private key, which can be used for digital signing and messages decryption. Similar to the joint security box, it requires many people to recover the private key and unlock it, and the problem of private key management would be solved. Since this private key split is generated by the administrator or a third party, this centralized operation would lead to frauds of keys. Additionally, Smart Contracts would be developed to improve "Secret Sharing" proposed by Shamir.

3. Solve the Problem of Private Key Trustee by Smart Contract

Most of the traditional key trusteeship have some defects. As long as the devices storing the private key or the auxiliary tools for retrieving the private key are lost, the user can no longer retrieve the wallet. In addition, it is vulnerable to intrusion, so that intruders can discover the key through any mechanism such as brute force cracking and weak encryption [3], or even the vicious bankruptcy of the custodian or the exchange [4], resulting in the failed trusteeship of the private key. Therefore, this paper used blockchain technology to prevent tampering and key outflow to protect the private key of the entire wallet, and develop a better private key trustee to achieve decentralization and decrease the risk of being hacked.

4. Solve Application Scenarios Related to Asset Finance of Wallet

More criminal cases of crypto assets occur, so that the seizure of supervisors is required. Due to the decentralization of cryptocurrencies, it cannot be directly seized as ordinary bank accounts. This legally illegal seizure scenario uses public power to directly detain the criminal, and transfer assets to a new supervised wallet. How prevent supervisors and criminals from colluding secretly to transfer money is an urgent problem to be solved in the future of digital asset finance. In addition, most of us purchase or invest in cryptocurrencies in present. Once the holder of the assets passes away, the assets would not be transferred while the owner not leaving the private key related information to the relatives, which is an inheritance problem of digital asset. This paper used the master key mechanism generated in the first year to develop automatically triggering Smart Contract technology to complete the transfer of assets.

III. METHOD

We would like to solve the problems of the general private key split, and propose a feasible solution to protect the private key. By designing a Smart Contract through the blockchain, it can prevent the frauds and theft of the sub-key.

First of all, the user received Mainkey through the *(t, n)* mechanism at the beginning. Supposedly, it is segmented into ten sub-keys. Then ten private keys are generated and one-to-one correspondingly encrypted. Each encryption could only be encrypted and decrypted by one private key, and the encrypted results have been stored on the blockchain. These ten private keys would generate ten wallets. When they need to be restored, they would collect these ten wallets with one-to-one correspond to summon these ten keys on the blockchain. The master key would not be restored until the collection satisfies the setting of *(t, n)* value, which can achieve a higher level of security.

With the solidity by Ethereum, it takes advantages of implement the test and set the permissions. Only those with permissions can operate the wallet, and once the contract is published, it cannot be changed. In addition, alliance chains can also be used. The alliance chain would register user credentials, which can only be used by pre-set individuals and nodes.

The popularity of digital assets and cryptocurrencies has the characteristics of anonymity, speed, and difficulty in cross-border tracking, which are easy to become criminal tools. Recently, fraud cases related to blockchain and virtual assets have increased, leading to crimes such as money laundering and fraud. The criminals' wallets seized by the government must use the *(t, n)* Shamir scheme to achieve the security of keys. Howbeit, chances are that keys would be stolen by the supervisors, and be transferred by the accomplices. This research is on the basis of the blockchain key trustee mechanism and develops the anti-escape seizure mechanism for illegal gains of virtual currency. Previous research [5] approaches secure ways to store and restore backed-up keys in an external repository, using an end-to-end secure connection, and a reliable method of backing up these keys as an independent share stored in multiple locations. An application of this technology would be implemented on Social Wallet as a part of future key backup mechanism. The problem of different wallet applications has not been solved in the past, such as loss of keys or damage to the device. These types of issues can result in users losing access to their cryptocurrencies, or users trust certain service providers, such as wallet exchanges, to back up their keys and set security protocols in place to recover lost keys. There are many risks associated with the security of private keys used in blockchain transactions related to the potential hacking of the software used in the device. For example, if passwords are used to protect keys, hackers can guess and look up keylogging history to restore those passwords. Also, hackers can then use the passwords to access to the user's private key. The followings are two phases of designing a Smart Contract through the blockchain:

- Shared-building Phase

1. The dealer chooses a secret *s*, a large prime number p>n, and considers a polynomial *f(x)* of degree.

t-1 = a0 + a1x + a2x2 + ... + at-1xt−1 (mod p), where the coefficient aj ∈ Zp = {0, 1, 2, …, p−1} for j = 1, 2, …, t−1 and a0 = f(0) = s.

The dealer as a miner builds a genesis block, which contains its identity, public key and related parameters (p), the total number of participants n, hash, identity of the signature algorithm, and related parameters.

2. Dealer do the following steps:

A. Generate n shares *(i, f(i))* for *i = 1,2,...,n* and secretly transmit them to n participants.

B. Prepare a list *(i, hash(f(i)))*, including *(IDdealer, hash(s))*, and store them in the transaction part of the second block.

C. Calculate hash (genesis - block header), list Merkle tree *(i, hash(f(i)))* and current timestamp, and create a second block header flag.

D. Broadcast the blockchain consisting of the genesis block and the second block to n participants.

- Secret-reconstructing phase

1. Any set of t participants secretly exchanges their shares.

2. Each participant uses the blockchain to verify the secret received from other t-1 participants, and proceeds to the next step. If verification fails, verification can be terminated.
3. Each participant uses the Lagrange polynomial interpolation formula to reconstruct the polynomial f(x). In order to prove that it is valid, they record the hash of the reconstruction secret in the blockchain, that is, the hash (s=f(0)) . If the check is met, the correct secret can be reconstructed.

Seizure of cryptocurrency by criminal suspects can be carried out by copying the private key that exists in a specific data set to the storage device of the prosecutor's office, and deleting the electromagnetic records on the storage device of the relevant person [6]. If the criminal's cryptocurrency should be transferred to the public key of the government, the private key can be kept securely. If the relevant person still holds a copy of the private key (Kopien), it avoids the risk of the relevant person transferring the assets. Furthermore, the encrypted currency is under the trusteeship of the relevant government office at this time, which is different from the deposit currency. The latter is not placed under the custody of the government office, but it is still deposited in the bank account, and only the relevant person is prohibited from disposing of it.

In another case, the criminal handed over all his virtual currency to the online electronic wallet provided by the transaction service provider for management. This situation has the technical specificity, which the virtual currency may be the private key and be not stored on the device of the perpetrator or participant, but on the server of the transaction service provider. Meanwhile, there is a debt-obligatory relationship between the transaction service provider and the criminal actor or participant legally. Accordingly, the perpetrator or participant in the crime retains a right to require the transaction service provider to deliver the bitcoin or virtual currency stored in its online wallet. Regarding the confiscation of the property, it is stipulated that the false confiscation is carried out, that is, the private key is confiscated. Afterwards, the currency is transferred to the public key owned by the government office to achieve the security of seizure.

IV. FUTURE DEVELOPMENT

Firstly, uploading from the user's private key to the blockchain and studying how to store and encrypt can ensure the security and efficiency of the user's private key fragment. Secondly, to complete the relevant application, the supervisors can use the private key splitting method and execute the seizure of illegal gains of criminal suspects. Thirdly, it can solve the problem of inheritance and transfer of digital assets, and the developed Smart Contract of blockchain mechanism can transfer assets to designated heirs.

Steps are displayed in Figure1.

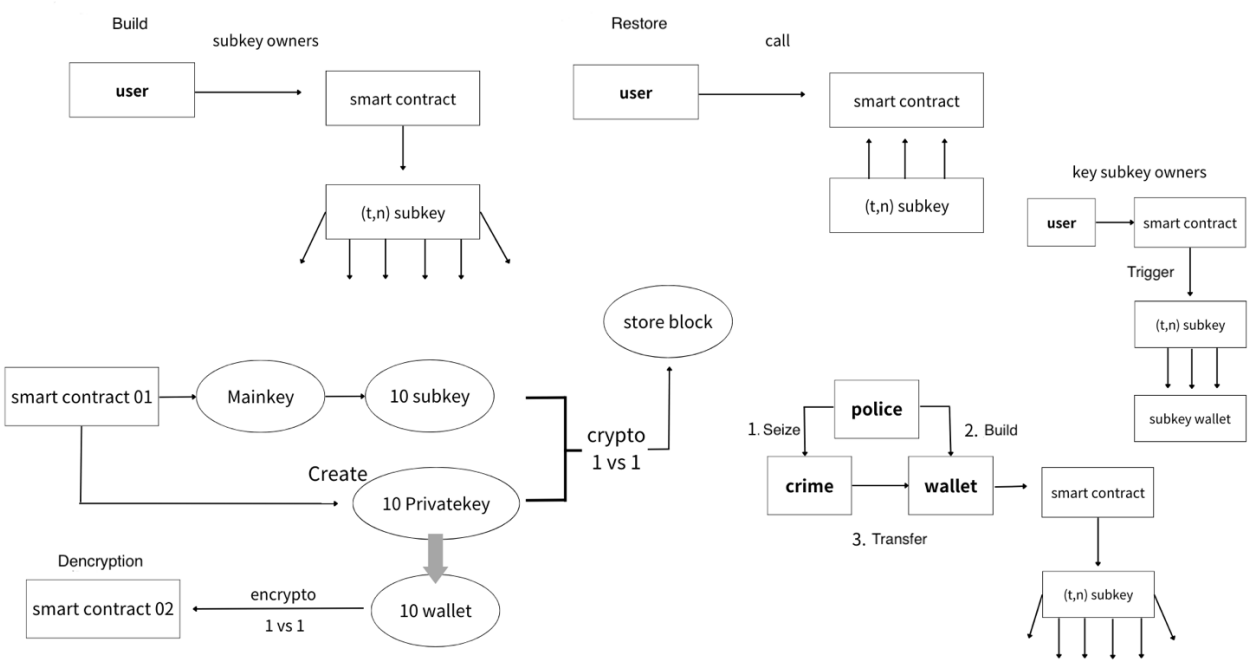

Fig. 1. The Architecture of Research Methods

1. Research and Development on the Prevention of Escape and Seizure of Illegal Proceeds of Virtual Currency

The seizure of illegal gains in law is mainly due to the increasing crimes related to virtual currency recently. Assuming that the criminal suspect's wallet is seized now, the relevant police supervisors need to create a new wallet, and the wallet will have the key. The relevant police supervisor will determine to whom split the key and transfer the criminal's wallet to a new wallet for seizure. Then they return it or compensate the victim after the investigation is concluded. In the second year of this paper, we have developed a legal seizure mechanism for virtual currency illegal gains to solve this problem.

A. Solve the Security Problem of Wallet Trusteeship

To prevent criminals from colluding with their accomplices and provide private keys to remove the illegal gains, it is expected that effective supervision mechanism will be designed to transfer the illegal gains to the supervision

wallet of the supervisors, so it can be well controlled.

B. Solve the Internal Control Problems of Inspectors

To prevent supervisors from guarding and stealing, the security of the wallet cannot be guaranteed if only one person has the key to the wallet. Therefore, a mechanism for safe storage of encrypted assets is designed, and private keys are jointly held by multiple people to solve the security problem of seizing wallets.

2. Research and Development on the Safe Transfer of Digital Asset Heritage

We who live in the digital generation hope to transfer digital assets to relatives through the triggering smart contracts, and decide whom to give to in advance by making a will after passing away in the future. Only when the holder passes away, it will be distributed to the respective wallets of whom has access to use while Smart Contract trigger condition is activated. Also, these people need to show it to withdraw it later, so as to achieve the fairness of digital asset distribution and integrity. However, with the increase of data on the chain, the scale of the chain will become larger, which consumes a lot of cost and resources for nodes.

V. REFERENCES

[1] P. Das, S. Faust, J. Loss, “A Formal Treatment of Deterministic Wallets,” CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 651–668, November 2019.

[2] A. Shamir, “How to share a secret,” Communations of ACM, vol. 22, pp. 612–613, 1979.

[3] O. Pal, B. Alam, V. Thakur, S. Singh, “Key management for blockchain technology,” ICT Express, Vol. 7, pp. 76–80, 2021.

[4] B.-Y. Lin. “Research for Recovery and Saving Private key,” Master Thesis, Tamkang University, Taiwan 2021.

[5] N. Lehto, K. Halunen, O. -M. Latvala, A. Karinsalo and J. Salonen, "CryptoVault - A Secure Hardware Wallet for Decentralized Key Management," 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS), Barcelona, Spain, 2021, pp. 1-4, doi: 10.1109/COINS51742.2021.9524133.

[6] W.-Z. Zheng, “Study on Criminal Confiscation and Seizure of Virtual Currency: BitCoin as Application Example,” The Journal of Business Law and Finance, Vol. 3, pp. 93–113, 2020.