Trust Your Wallet: a New Online Wallet Architecture for Bitcoin

Fangdong Zhu*, Wen Chen*, Yunpeng Wang*, Ping Lin*, Tao Li*, Xiaochun Cao† and Long Yuan‡
*College of Computer Science, Sichuan University, Chengdu, China
†State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
‡School of Computer Science and Engineering, University of New South Wales, Sydney, Australia

***Abstract*—Online wallet has become an important method to manage Bitcoin. In a Bitcoin transaction, online wallet manages the private key automatically, and stores the encrypted private key in remote to ensure the accessibility of Bitcoin anywhere. In the traditional online wallet, the private key is stored centrally in a storage unit. However, if the storage unit is collapsed or hacked, users will suffer the risk of losing their Bitcoins. Motivated by this, in this paper, we propose a new online wallet architecture: HA-eWallet. In HA-eWallet, the transaction of Bitcoin is signed by multiple private keys rather than one, and private keys are stored separately in different places. In addition, we introduce a second service unit to construct the Active-Active architecture to rotate the capability and workload. Besides, we adopt a disaster recovery strategy in our proposed architecture in case of any disaster. According to the running states of each service unit, HA-eWallet have three operation models, and can be switched smoothly. Theoretical analyses and experiments show that: HA-eWallet can achieve higher availability compared with the traditional online wallet architecture, and users will not suffer a loss as long as the number of lost private keys are less than 50% of the users' total number of private keys.**

***Index Terms*—Bitcoin, multi-signature, disaster recovery, high availability, online wallet, Active Active architecture**

I. Introduction

Bitcoin was proposed by Satoshi Nakamoto in November 2008 [1]. Over the past years, Bitcoin has become an attractive cryptography currency in the world. Until now, the price of Bitcoin has increased rapidly from less than 1 dollar in 2010 to 4900 dollars in 2017 [2]. Furthermore it has been accepted by some government agencies and banks. For instance, on 19 August 2013, the German Finance Ministry announced that Bitcoin was now essentially a "unit of account" and could be used for the purpose of tax and trading in German [3]. In another example, UK banking giant Barclays has announced it will take its first step toward supporting the use of Bitcoin as an alternative payment method by allowing charities to accept donations in the digital currency [4].

Due to the convenience, online wallet, which manages private keys of the Bitcoin in a web site, has become a popular way, in particular in managing a small amount of Bitcoin. In the Bitcoin world, a private key determines the ownership of Bitcoin. Although the private key is encrypted in users' web browser or App, centralized storage of the encrypted key will lead to serious security issues, since online wallet cannot offer services when the storage units are cracked or collapsed. In recent years, there has been a lot of medium of Bitcoin exchange compromised. For example, an online wallet *Inputs.io* lost 4100 BTC and went bankrupt, because private keys were cracked by attackers in 2013 [5].

Recently, online wallet has become a hot research topic and much work has been devoted to improve its security and availability. In 2014, Bamert et al. [6] created a proof-of-concept Bitcoin hardware token: BlueWallet. It communicates using Bluetooth Low Energy and can protect the Bitcoin private keys. In 2015, Eskandari et al. [7] contributed an evaluation framework for comparing Bitcoin key management approaches, and conducted a broad usability evaluation of six representative Bitcoin clients. Goldfeder et al. [8] presented the first threshold signature scheme compatible with Bitcoins ECDSA signatures and showed how distributed Bitcoin wallets could be built using this primitive. In 2016, Zhou et al. [9] proposed a Distributed Bitcoin Account Management (DBAM) framework that realized joint management of Bitcoin accounts applied especially to enterprises and companies. The framework incorporates secret sharing and attribute based encryption schemes compatible with the existing bitcoin protocols. In 2017, Wu et al. [10] investigated how to jointly manage the Bitcoin trading when the Bitcoin account is possessed by multiple participants and how to simultaneously guarantee the anonymity of the multiple owners.

The aforementioned methods mainly focus on the security of private keys. However, the availability of online wallet is not very concerned. Motivated by this, we propose a novel online wallet architecture, HA-eWallet, in this paper, which considers both security and availability. Regarding security, we propose a multiple private keys paradigm which is compatible with the multi-signature schemes of the Bitcoin protocol. Regarding availability, we introduce a second service unit and adopt a disaster recovery strategy in our online wallet architecture. The contributions of this paper can be summarized as follows.

- We propose a multiple private keys paradigm. In our new paradigm, a transaction has to be signed by multiple private keys and they are stored separately in different places. Compared with the single and centrally stored private key strategy used in traditional online wallet, our

Correspondence should be addressed to Wen Chen; wenchen@scu.edu.cn.

978-1-5386-1978-0/17/$31.00 ©2017 IEEE

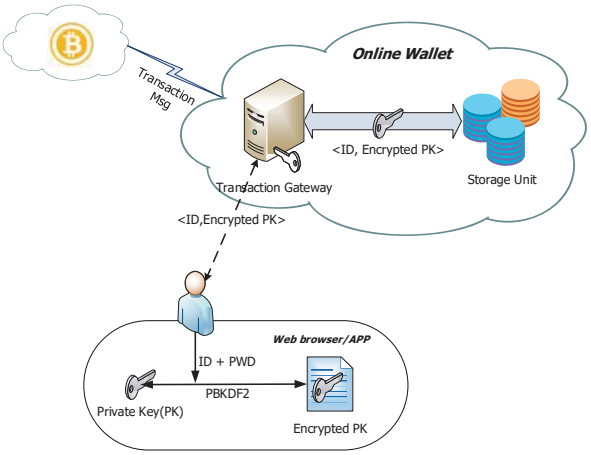

Fig. 1: The architecture of Coinpunk.

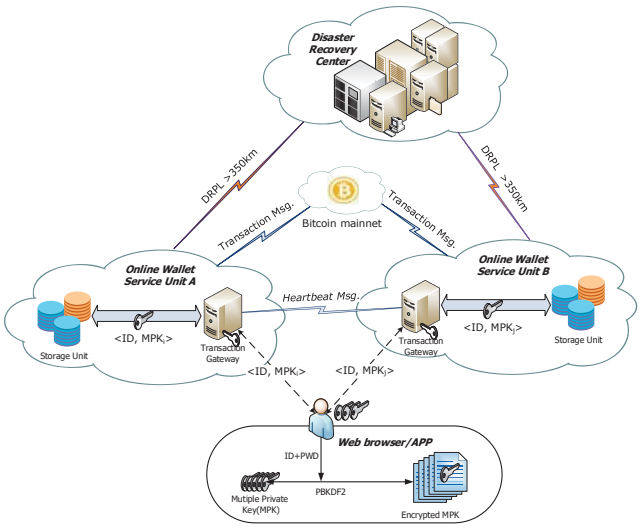

Fig. 2: The architecture of HA-eWallet.

new paradigm can significantly improve the security of the online wallet.

- We construct an Active-Active architecture by introducing a second service unit in HA-eWallet. The benefits of constructing the Active-Active is that the availability of HA-eWallet is improved through rotating the capability and workload between services units.
- We adopt a disaster recovery strategy to further improve the availability of HA-eWallet. With the disaster recovery, our online wallet architecture can resist the serious data loss in disaster events.
- We conduct theoretical and experimental analyses in terms of the availability of HA-eWallet and the results show the HA-eWallet can achieve a higher availability compared with the traditional online wallet architecture.

II. Traditional online wallet architecture

In this section, we take Coinpunk as an example to demonstrate the traditional online wallet architecture. Coinpunk is a famous DIY online wallet. It was funded by Bitcoin Foundation in 2013 [11]. Furthermore, the codes of Coinpunk are partly adopted in most online wallet providers. The architecture of Coinpunk is shown in Fig.1.

As shown in Fig.1 , users' ID and password (PWD) are concatenated to encrypt the private key by PBKDF2 algorithm. The procedure is processed on users' web browser or App. After encrypted, the private key is sent to the online wallet and stored centrally. When a new transaction comes, the encrypted private key is sent back from online wallet and decrypted by ID and password on the web browser or APP. Then the transaction message can be signed and broadcast.

In Coinpunk, users do not need to keep private keys in an encrypted form or clear text. Therefore, Bitcoin can be transacted conveniently. However, as the encrypted key is stored centrally, it is hard to guarantee the availability and security. If the transaction gateway is broken down, the transaction will be unavailable or delayed. Moreover, if the storage unit is collapsed or cracked, users' Bitcoin will inevitably suffer a loss.

III. The details of HA-eWallet

In this section, we first give an overview of HA-eWallet, and then we present the operation models in detail. In the last part, *Live-Detection scheme*, which is responsible for detecting the running state of HA-eWallet, is described.

A. Overview of HA-eWallet

The architecture of HA-eWallet is shown in Fig.2. To improve the availability, we introduce a second online wallet service unit whose internal composition is similar to the first service unit. Both service units are running simultaneously. Hence they can constitute an *Active-Active architecture* [12] , which means the capability and workload can be rotated to accelerate incident response time and increase confidence. Each service unit mainly consists of two parts: a transaction gateway and a storage unit. The transaction gateway handles users' transaction and monitors the running state of the storage unit. The storage unit is responsible for storing users' private key in database. In order to protect against earthquakes, terrorist attacks and other disasters, each online wallet service unit connects with the disaster recovery center using DRPL (the disaster recovery private line). The data stored in each service unit should be backed up to the disaster recovery center regularly. With the disaster recovery center, even if the data are completely destroyed in disasters, it can also be restored with zero loss.

Regarding the management of the private keys, HA-eWallet adopts the *multi-signature technology* [13]. Multi-signature refers to requiring more than one key to authorize a transaction and is supported by the Bitcoin protocol, and it has a great many of varieties, such as 2 of 3, 3 of 5, and 5 of 7 multi-signature. In HA-eWallet,*3 of 5 multi-signature* is used, which

means a transaction must be signed by any 3 private keys of 5. Compared with the traditional online wallet architecture which adopts the single and centrally stored private key strategy, our multiple and distributed stored private key strategy can significantly improve the security of the online wallet.

B. Operation models

HA-eWallet has three operation models: the dual-master model, simplex model and recovery model. According to the states of service unit, the operation models can be switched seamlessly.

1) Dual-master model: In this model, both service units are running in normal condition. 5 private keys are randomly generated in users' web browser or App. 2 private keys are randomly selected and encrypted by users' ID and password, and then they are sent to each transaction gateway separately. After the encrypted private key is received, the transaction gateway stores the private key in the storage unit, and backs it up to the disaster recovery center timely. When a new transaction comes, 2 private keys of online-wallet providers and a private key of users could sign the transaction.

2) Simplex model: In this model, one of service units fails. The failed service unit will be restored from the disaster recovery center immediately. While, the function of transaction will not be affected. When there is a transaction to receive Bitcoin, users generate 5 private keys as usual. The only difference is that users send the encrypted key to the normal service unit rather than the both two service units. When there is a transaction to send Bitcoin, users only need to provide 2 private keys, combined with the private key in the normal service unit, the transaction can be signed. When the failed service unit is recovered successfully, the normal service unit will send one private key to the recovered service unit.

3) Recovery model: In this model, both service units fail. This is the worst condition and the transaction will be suspended. However, we can guarantee that the Bitcoin still safe. For one thing, the service units can be restored from the disaster recovery center. For another, users still control their Bitcoin by providing 3 private keys. Even when both keys are stolen and cracked by attackers, they cannot sign a transaction to spend users' Bitcoin.

Fig.3 shows the switch scheme of the operation models in HA-eWallet. The operation models are decided by the states of service unit. For example, in dual-master model, both service units work normally. If one of the service units fails, the operation model will be switched from dual-master model to simplex model. And then if the other service unit fails, the operation model will be switched from simplex model to recovery model. If both service units recover from the disaster recovery center, the operation model will be switched from the recovery model to dual-master model.

C. Live-Detection scheme

As seen from above, the operation models of HA-eWallet depend on the running states of each service unit. Therefore, an efficient live detection scheme is an important part of the system. In particular both service units perceive each other's work states in this scheme. In order to address this problem, we introduce the *Live-Detection scheme* in this section. In this scheme, the transaction gateway of each service unit is responsible for monitoring the operating states of the storage unit in the service unit and communicating with the other transaction gateway. The rules of communication are listed as follows.

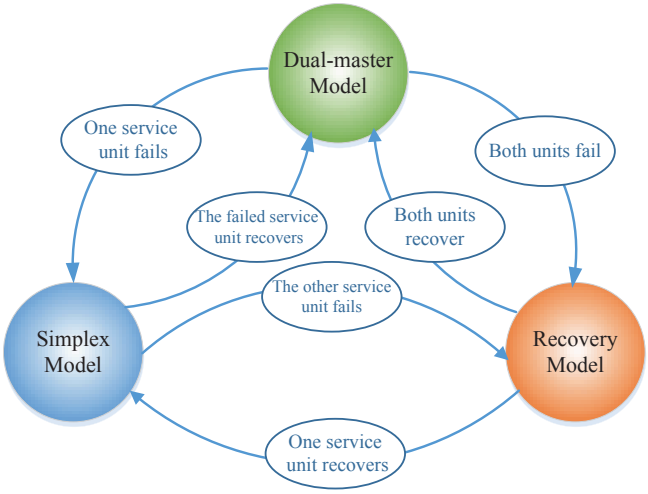

Fig. 3: The operation model of HA-eWallet.

- If the storage unit works normally, the transaction gateway in the same service unit will send one heartbeat packet to the other transaction gateway in the fixed *timeslot*.
- If a *heartbeat packet* is received, the transaction gateway will consider the other service unit works normally. Otherwise, if no heartbeat packet is received after given timeslot, the transaction gateway will consider the other service unit fails.
- If the storage unit fails, the transaction gateway will send a *reset packet* immediately.
- If the transaction gateway receives a reset packet, the transaction gateway will consider the other service unit fails.

Fig.4 shows an example of the Live-Detection scheme. The black continuous lines represent the heartbeat package sent from the transaction gateway A to B. The grey continuous lines represent the heartbeat package sent from the transaction gateway B to A. All heartbeat packages should be sent in one unit interval per timeslot. The blue dashed line represents the reset package sent from the transaction gateway A to B. It means that the transaction gateway A detects a deadly error from storage unit in the same service unit. After the transaction gateway B receives the reset packet, the operation model will be switched from dual-master model to simplex model.

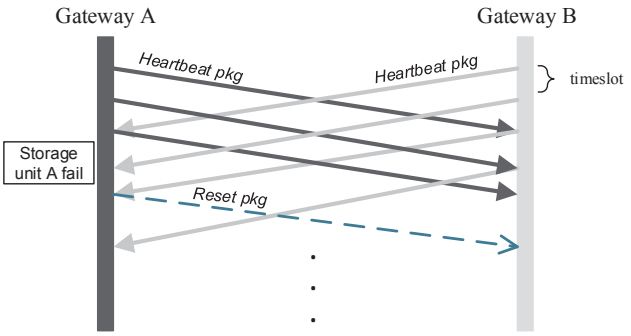

Fig. 4: The Live-Detection scheme of HA-eWallet.

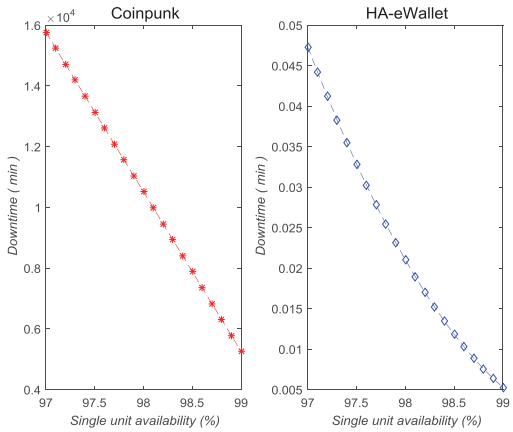

Fig. 5: Downtime per year.

IV. Discussion

A. The availability of HA-eWallet

Suppose that the availability of a service unit is p, and the availability of the disaster recovery center is q. According to the operation models of HA-eWallet, it is unavailable only when all service units and the disaster recovery center fail. So the availability of HA-eWallet can be expressed in Eq(1).

$$\varphi_H = 1 - (1-p)^2(1-q), \tag{1}$$

where φ_H is the availability of HA-eWallet.

Downtime is a crucial criterion to evaluate the high availability system. In order to study the availability of HA-eWallet, we design an experiment to simulate the downtime per year. The parameters are set as follows: the availability of a service unit ranges from 97% to 99%, and the availability of the disaster recovery center is 99.99%. The downtime can be calculated by Eq(2).

$$T_d = \varphi_H T_{total}, \tag{2}$$

where T_d is the downtime, and T_{total} is the sum of elapsed time. The results of experiment are shown in Fig.5.

As shown in Fig.5, compared with Coinpunk, HA-eWallet's downtime is lower by five orders of magnitude. When the availability of single service unit is 97%, the downtime of HA-eWallet per year is 0.0473 minutes, which is lower than Coinpunk's (15,768 minutes) by 99.9997%. This phenomenon can be explained as follows: the availability of Coinpunk only relates to one service unit. If the key stored in the service unit is stolen or collapsed, it will be unavailable. Unlike Coinpunk, HA-eWallet will be available as long as any service unit or the disaster recovery center is alive. Therefore, the availability can be much improved.

B. The scalability of HA-eWallet

To satisfy further requirements for high availability and security, HA-eWallet can be extended in the following areas.

1) The scalability of service unit: According to the above section, the availability and security can be improved by the increasement of the service unit. Meanwhile, the multi-signature technology should be evolved to correspond with the number of the service unit. Assuming the number of the service unit is k, then the *m of n multi-signature* will satisfy Eq(3) and Eq(4).

$$m \geq (n+1)/2, \tag{3}$$

where n and m are integers.

$$k = n - m, \tag{4}$$

where k is the number of the service unit.

The scheme of key management will be improved too. In users' web browser or App, the n private keys are generated. Then k keys are randomly selected and encrypted to be sent to each service unit. Similarly, the transaction can be signed by m private keys in service unit and users. It is not difficult to infer that the improved HA-eWallet can tolerate k private keys lose.

2) The scalability of disaster recovery center: The disaster recovery center is an important part of ensuring the availability of HA-eWallet. Using a single disaster recovery center is only due to the cost considerations. If each service unit can back up data to multiple disaster recovery centers, the reliability of the data will be further enhanced.

C. The security of HA-eWallet

According to the procedure of HA-eWallet, HA-eWallet can tolerate a loss of k private keys. It means that even if attackers steal or crack k private keys, they cannot forge a signature of the users Bitcoin. In particular when the k private keys are all stored in the services units, they can be restored through the disaster recovery center. So, HA-eWallet can tolerate the ratio of lost keys η will satisfy Eq(5).

$$\eta = k/n = (n-m)/n. \tag{5}$$

Substitute Eq(3) into Eq(5), we get

$$\eta \leq (n-1)/2n < 1/2. \tag{6}$$

Therefore, users will not suffer a loss as long as the number of lost private keys are less than 50% of the users total number of private keys.

V. Conclusion

In this paper, we propose a high availability architecture of online wallet in Bitcoin: HA-eWallet. In HA-eWallet, a Bitcoin transaction must be signed by any 3 private keys rather than one. Besides, the private keys are stored separately in different places: 3 private keys are stored in the user node, while the other 2 encrypted private keys are stored in the service units separately. According to the multi-signature mechanism, even though both of the two private keys in online wallet providers are stolen or cracked by attackers, they cannot forge a signature of the users' Bitcoin. In addition, each online wallet service unit connects with the disaster recovery center, and backs up the private keys timely. In this way, our system can be always available unless all service units and the disaster recovery center fail.

Acknowledgement

This work was supported by the National Key Research and Development Program of China (Grant No.2016YFB0800605 and No.2016YFB0800604) and Natural Science Foundation of China (Grant No.61402308 and No.61572334). Furthermore, thank editors and reviewers for all the valuable advice.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] "Average usd market price across major bitcoin exchanges," https://blockchain.info/charts/market-price/, accessed Sep 11, 2017.
[3] "Wikipedia:legality of bitcoin by country or territory," https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory/, accessed Sep 11, 2017.
[4] "Barclays to set bitcoin rolling," https://www.thetimes.co.uk/article/barclays-to-set-bitcoin-rolling-dstptmhllmn/, accessed Sep 11, 2017.
[5] "Hackers steal $1.2 million of bitcoins from inputs.io, a supposedly secure wallet service," http://www.coindesk.com/hackers-steal-bitcoins-inputs-io-wallet-service/, accessed Sep 11, 2017.
[6] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, *BlueWallet: The Secure Bitcoin Wallet*. Cham: Springer International Publishing, 2014, pp. 65–80. [Online]. Available: https://doi.org/10.1007/978-3-319-11851-2_5
[7] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management." Workshop on Usable Security (USEC, 2015.
[8] S. Goldfeder, R. Gennaro, H. Kalodner, J. Bonneau, J. A. Kroll, E. W. Felten, and A. Narayanan, "Securing bitcoin wallets via a new dsa/ecdsa threshold signature scheme," 2015.
[9] X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, "Distributed bitcoin account management," in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug 2016, pp. 105–112.
[10] Q. Wu, X. Zhou, B. Qin, J. Hu, J. Liu, and Y. Ding, "Secure joint bitcoin trading with partially blind fuzzy signatures," *Soft Computing*, vol. 21, no. 11, pp. 3123–3134, Jun 2017. [Online]. Available: https://doi.org/10.1007/s00500-015-1997-6
[11] "Bitcoin foundation funds diy bitcoin wallet coinpunk," http://www.coindesk.com/bitcoin-foundation-funds-diy-bitcoin-wallet-coinpunk/, accessed Sep 11, 2017.
[12] C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, "Symmetric active/active high availability for high-performance computing system services: Accomplishments and limitations," in *2008 Eighth IEEE International Symposium on Cluster Computing and the Grid (CCGRID)*, May 2008, pp. 813–818.
[13] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.