ASTES

*Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 1, 36-42 (2021)*

www.astesj.com

*Special Issue on Multidisciplinary Sciences and Engineering*

**ASTESJ**

**ISSN: 2415-6698**

# An Anonymity Preserving Framework for Associating Personally Identifying Information with a Digital Wallet

Qazi Mudassar Ilyas*, Muhammad Mehboob Yasin

*College of Computer Sciences and Information Technology, King Faisal University, Al Ahsa, 31982, Saudi Arabia*

ARTICLE INFO

*Article history:*
*Received: 23 October, 2020*
*Accepted: 19 December, 2020*
*Online: 10 January, 2021*

*Keywords:*
*Anonymity*
*Cryptocurrency*
*CryptoRegistry*
*Digital Wallet Ownership*
*Lost Digital Wallet*

ABSTRACT

*Growing adoption of cryptocurrencies by institutional investors coupled with recurring incidents of loss of access to digital wallets have resulted in emergence of custodial services for high net worth individuals and institutions. However, such services are not economically feasible for the wider community of crypto owners who are left with no recourse for recovery of lost funds. This paper proposes a framework, AFAP, for associating certain personally identifying information with a digital wallet so that a user may prove ownership of the said wallet. Thus, the owner is able to establish his/her claim over funds associated with such a wallet in case of loss of access to it. We show that the proposed scheme has no adverse effect on anonymity, privacy and forgetfulness of personal information of the wallet owner.*

## 1. Introduction

Cryptocurrencies are gaining much traction in the mainstream economic activity because of their global and fully decentralized nature, promise of freedom from political influence, and peer to peer nature of transactions [1]. The blockchain does not carry any information pointing to the owner of a particular digital wallet. Further, the use of Hierarchical Deterministic (HD) wallets [2] makes it harder to even group individual transactions carried out by one individual. The pseudo-anonymity thus provided by blockchain is one of the major factors contributing to the popularity of digital currencies. However, a drawback of this characteristic is the inability to associate a digital wallet address with an individual in order to prove ownership of a lost digital wallet.

The value of Bitcoin, leader of the pack, recently climbed to an all-time high of USD 24,058 on CoinDesk Bitcoin Price Index beating the earlier high of USD 20,000 reached on December 2017 [3]. Several businesses have already embraced digital currencies, while governmental entities are also preparing to bring them into mainstream financial systems [4]. Hence, cryptocurrencies are on track to become an important part of all financial transactions in future. However, digital currencies are in their infancy and several issues need to be resolved before they can become part and parcel of a common individual's life [5].

*Corresponding Author: Qazi Mudassar Ilyas, College of CS&IT, King Faisal University, PO Box 400, Al Ahsa, 31982, Kingdom of Saudi Arabia, qilyas@kfu.edu.sa

The Achilles' heel of Cryptocurrencies is the fact that access to all funds owned by an individual is tied to a complex long number that is almost impossible to remember. Therefore, this complex number, known as private key of a digital wallet, needs to be stored safely. Also, the private key needs to be kept in a secure manner because anyone with knowledge of this number can use the funds stored in the respective wallet.

A private key can be lost owing to hardware or software failure, personal carelessness in safekeeping the keys, or in some cases even death of the owner. Several users have reported losing their private keys thus making their funds inaccessible to them. A survey reported that a significant fraction of respondents had experienced loss of Bitcoin keys at least once [6]. According to careful estimates, about 4 million Bitcoins had been lost till 2017 [7]. More recently, more than 100,000 individuals lost Bitcoins worth nearly USD 190 million owing to the death of the owner of a cryptocurrency exchange QuadrigaCX [8]. Since there is no inherent mechanism in the Bitcoin framework to recover lost keys, a lost private key simply means all Bitcoins associated with that key are lost forever. Hence, there is need for a mechanism to restore access to funds in case respective private keys become permanently inaccessible.

Since a mnemonic passphrase is easier to memorize or record as compared to a complex number, it is widely used by digital wallets to create the private key [9, 10]. Though, this improves the user experience, yet this does not absolve the user from

responsibility of storing her/his passphrase in a safe and secure manner. As in the case of loss of private keys, loss of a passphrase implies loss of access to the respective digital wallet. In the following, we address the problem of loss of access to a digital wallet which may be because of loss of a private key or loss of the corresponding mnemonic passphrase.

We propose a two-step solution to this problem. As the first step, the owner is afforded the ability to prove ownership of a lost wallet. Subsequently, either the funds stored in the lost wallet may be returned to the rightful owner or he/she may be suitably compensated. In this paper, a framework for proving ownership of a wallet is proposed, while the second step of solution is subject of future work. The proposed framework, "Anonymity Preserving Framework for Associating Personally Identifying Information (PII) with a Digital Wallet (AFAP)", can be used to associate the PII of owner with a digital wallet in a secure fashion while maintaining the same level of anonymity as provided by the current cryptocurrency ecosystem.

The proposed framework comprises three entities, namely CryptoRegistry, PII Associating Transaction (PAT) and PII Wallet. CryptoRegistry is a trusted long-lived entity that registers a given PII against a digital wallet by digitally signing this association and helps in validating the same when required to do so. A PII Associating Transaction (PAT) stores the aforementioned association on the blockchain by embedding the said CryptoRegistry signature in an outgoing transaction. A PII wallet is a specialized digital wallet that facilitates the registration and validation processes.

Rest of the paper is organized as follows. The next section summarizes the related works. The proposed framework is presented in Section 3 detailing key components and schemes for registration of a digital wallet and claiming its ownership. A case study is provided in Section 4 that shows feasibility of the proposed framework. The paper is concluded with the discussion and future work.

## 2. Related Work

The issue of loss of access to a digital wallet has gained attention of researchers owing to an increasing number of incidents resulting in loss of digital currency worth millions of dollars belonging to thousands of individuals [11,12]. The solutions proposed till date focus on safekeeping of digital wallets to ensure continued availability of private keys as and when needed. These solution approaches can be divided into two main categories, namely user-centric approaches that facilitate one in safekeeping of one's digital assets and custodial approaches that transfer the responsibility of safekeeping to a trusted third party.

User-centric approaches include cold storage, offline wallets and specialized hardware wallets. Cold storage refers to safely storing the private key of a digital wallet on an offline medium ranging from secondary storage to plain paper [13,14]. An offline wallet is an air-gapped device that can generate transactions for export to a hot wallet, thus providing an improved user experience. A specialized hardware wallet incorporates Hardware Security Modules (HSM) to store the private keys in a protected area of microcontroller storage which cannot be accessed from outside the device [15]. As suggested in [16], one can derive two values from the private key and store one of these value on a remote server. Protection against brute force password attacks is provided by keeping the second value on the local machine. A shortcoming of this scheme is that one needs to remember password to retrieve the value from the server. Further, damage to the local machine can result in permanent loss of access to the key.

Though all aforementioned approaches provide varying levels of protection against loss of private keys, yet the possibility of damage to or loss of access to physical medium still exists, which will result in loss of access to the respective digital wallet.

Another class of solutions relies on Shamir's secret sharing scheme, as adapted by [17], based on semi-trusted social network comprising friends of an individual. However, such schemes are more suitable for corporate clients since social networks of individuals are quite fluid and cooperation of "friends" cannot be guaranteed for unforeseeable future.

In custodial approaches, such as a browser-based wallet, an online account is maintained with a service provider that is used for storing and retrieving digital assets; examples include CoinBase*, Kraken† and BitStamp‡. However, several instances have been reported where many clients lost access to their digital assets owing to the service provider going out of business. For an exposè, the reader may refer to [18,19]. To overcome this issue, clients are usually facilitated to backup their private keys as an assurance against the possibility of the service provider ceasing to exist. Although these online services relieve the owner from the responsibility of safekeeping digital assets, they are exposed to a multitude of vulnerabilities such as internal or external theft and cyber-attacks. Recently, specialized custodial service providers have also emerged that claim improved security against aforementioned vulnerabilities by utilizing air-gapped devices and employing higher standards of security. Two of the well-known examples of such service providers are Fidelity Digital Assets§ and Ledger Vault** . However, these services have high associated costs and thus are suitable only for institutional clients or high net-worth individuals. It needs to be emphasized that privacy and anonymity are obviously compromised in all custodial services as digital assets in custody need to be associated with identity of respective owners.

One may conclude that none of the solutions proposed so far gives absolute guarantee against loss of access to a digital wallet while maintaining privacy and anonymity. Another perspective is to accept the occurrence of such eventuality as an inherent weakness of the blockchain technology and devise mechanisms to handle such situations. One such mechanism may be to prove ownership of a lost digital wallet and claim compensation for unspent amount stored in that wallet.

Various initiatives have been proposed for using blockchain to prove existence or ownership of a digital asset at a certain point in

* https://www.coinbase.com/
† https://www.kraken.com/
‡ https://www.bitstamp.net/
§ https://www.fidelitydigitalassets.com/
** https://www.ledger.com

time. For example, the online service named "Proof of Existence" [20] stores cryptographic hash of a digital document on blockchain that can be used to prove that the said document existed at a particular point in time. Further, integrity of the document is also established. Additionally, various schemes, referred to as Colored Coins [21], exploit the immutable characteristic of blockchain technology to store real world asset manipulation information on the blockchain [22, 23]. In [24] a DNS like naming system is proposed that associates human-readable names with respective internet resources by storing mapping information on the blockchain. In all such schemes, non-financial data is made part of the blockchain by embedding it into script of an OP_RETURN output; a special output of a blockchain transaction [25]. We also exploit the said scripting feature of OP_RETURN output to associate PII with a digital wallet by storing requisite metadata on the blockchain. The details of the proposed framework follow.

## 3. Proposed Framework

In order to overcome the wallet ownership issue, one may associate some Personally Identifying Information (PII), such as national ID, driving license or passport number with the digital wallet using the aforementioned output script of a transaction. In the following, we first introduce some obvious extensions of the use of aforementioned scripting feature for storing PII on the blockchain and point out that anonymity and privacy of the wallet owner may be compromised by using such simple schemes. We then present our framework to associate PII with a digital wallet and show that it preserves anonymity and privacy of the wallet owner.

### *3.1. Simple schemes for storing PII on blockchain*

In this section, we present three ways of storing PII on blockchain to associate ownership of a digital wallet in the order of increasing complexity.

#### *3.1.1. Plaintext PII*

In this scheme, the owner of a digital wallet constructs a transaction and embeds his/her PII in one of the output scripts. This transaction is then sent on the network for processing. Since output script of a transaction can only be created by the originating digital wallet and cannot be tampered with after the transaction has been broadcast, the said information is irrevocably tied to the corresponding digital wallet. The wallet owner may record ID of the said transaction (TxID) for future reference. Once this transaction is confirmed, it becomes part of the blockchain, thus permanently associating PII with the issuing wallet.

In case of losing access to the private key of a digital wallet, henceforth referred to as a lost wallet, blockchain will be scanned to extract the aforementioned transaction using TxID and identify the rightful owner of the issuing wallet from the embedded PII. This scheme may be used to serve as a basic naming system for digital wallets akin to BitAlias [26] and OneName [27] etc. However, this scheme violates one of the basic principles of blockchain technologies, namely, ensuring anonymity of parties to a transaction. Therefore, this way of associating PII with a wallet may not be of general appeal.

#### *3.1.2. Encrypted PII*

To preserve anonymity of the wallet owner, one may create a public-private key pair and encrypt the PII with this public key before embedding it into the script. Now, to prove ownership of a digital wallet, one needs to locate the corresponding transaction on the blockchain and decrypt the PII using the respective private key. This requires the corresponding private key to be readily accessible when needed. This problem is akin to safely storing the private key, of the digital wallet, itself. Hence, this scheme does not reduce the responsibility of the wallet owner in safeguarding a private key.

An alternate way to relieve the owner of this added responsibility is to use pubic key of a well-known entity, such as a coin exchange, for encrypting the PII. Now, one needs to approach the said entity for decrypting the PII in order to establish one's claim of ownership. Though a wallet owner is absolved from responsibility of safekeeping any private keys, this scheme suffers from two drawbacks.

Firstly, the well-known entity may not be aware of such use of its public key. Also, it is not bound to maintain all its public private key pairs for foreseeable future. Therefore, it may not be in possession of the required private key when approached. Hence, owner claim may not be substantiated based on the encrypted PII. Secondly, since public key is supposed to be widely available, the encrypted PII is prone to dictionary attack.

#### *3.1.3. Hashed PII*

This method requires PII to be hashed using a well-known hashing algorithm and the resulting hash to be embedded in the script of a transaction in blockchain. To establish the claim of ownership, one may create hash of one's PII and validate it against the hash recovered from the respective transaction. In order to avoid dictionary attack, a sufficiently large random, commonly called salt, may be added to the PII. However, PII validation process now depends upon availability of the salt used. Therefore, the wallet owner is made to bear the responsibility of safekeeping the salt. Though, the salt may be in the form of hash of a memorable passphrase, the situation is reduced to a problem that is akin to safely storing the private key of a digital wallet.

### *3.2. An Anonymity Preserving Framework for Associating PII with a Digital Wallet*

By now, the need has been established for a long-lived trusted third party with the responsibility of safekeeping the information required for proving association of a given PII with a digital wallet in an anonymous way. We call this entity a CryptoRegistry and propose a framework that preserves owner's anonymity and privacy as long as the CryptoRegistry is deemed trustworthy. We call this framework AFAP - An Anonymity Preserving Framework for Associating Personally Identifiable Information (PII) with a Digital Wallet.

The proposed AFAP framework comprises three components, namely a CryptoRegistry, a PII Associating Transaction (PAT) and a PII wallet. In the following, we give the details of each one of these components.

### 3.2.1. CryptoRegistry

We introduce the concept of a CryptoRegistry that is a trusted long-lived entity. A CryptoRegistry is required to perform the following functions:

- To provide an Application Programmer Interface (API) for registering the PII provided by a wallet owner
- To provide an API for making available the following information:
  - A public key $K_{Pub,CR}$
  - Registration fee, $F_{CR}$
  - A wallet address, $W_{CR}$
  - A sufficiently large random number, also known as salt, for defense against dictionary attack as discussed below, $S_{CR}$
  - A hashing algorithm along with its parameters, $\mathcal{H}$
  - Hash of (PII || $S_{CR}$), $H_{ID}$
  - Digital signature on PII, $S_{CR}$, $F_{CR}$, $W_{CR}$, $\mathcal{H}$ and $H_{ID}$ using $K_{Priv,CR}$
  - The digital certificate to the effect that the said CryptoRegistry is owner of the respective public key, $K_{Pub,CR}$

It may be noted that the proposed scheme introduces a random salt to preserve anonymity since use of hash of PII alone may be linked to the original PII by brute force attack.

- To ensure availability of the PII, $S_{CR}$, $TxID_{PAT}$, and respective public-private key pair, once a PAT constructed by a PII wallet paying the fee $F_{CR}$ to the wallet $W_{CR}$ is confirmed on the blockchain. By virtue of its digital signature, the CryptoRegistry is bound to the PAT. As a trustee, the CryptoRegistry is also required to ensure confidentiality and security of information entrusted with it throughout its life time.
- To provide a list of PATs and corresponding digital wallet addresses associated with a given PII. It is to be noted that, in the interest of anonymity and privacy, the aforementioned information will only be provided to the rightful owner of PII or any authorized legal entity.
- Optionally, a CryptoRegistry may advertise special prefix to be used with OP_RETURN to facilitate searching a particular PAT on the blockchain.

### 3.2.2. PII Associating Transaction (PAT)

Generally a PII Associating Transaction (PAT) consists of three outputs. Firstly, an output transferring Registration fee $F_{CR}$ to CryptoRegistry wallet $W_{CR}$. Secondly, an output transferring change to the wallet owner's change address. Thirdly, a zero valued output with OP code OP_RETURN and output script comprising the following information:

- Special prefix provided by the CryptoRegistry (if any)
- $\mathcal{H}$(PII || $S_{CR}$), $H_{ID}$
- Digital signature on PII, $S_{CR}$ ,$F_{CR}$, $W_{CR}$ and $H_{ID}$ using $K_{Pub,CR}$

It is to be noted that since every Bitcoin transaction is tied to the originating wallet and cannot be tampered with after it has been confirmed, thus the above information, by virtue of being embedded in the transaction, becomes irrevocably tied to the corresponding digital wallet.

### 3.2.3. PII Wallet

PII wallet is a specialized digital wallet capable of constructing and verifying PAT transactions for associating itself with PII. For this purpose, it needs to communicate with a CryptoRegistry and perform a number of functions as detailed below:

- Accepting and storing PII of the wallet owner in a secure way
- Providing a list of available CryptoRegistries to the wallet owner
- Initiating the process for registration of given PII with the selected CryptoRegistry
- Accepting response from CtyptoRegistry comprising $S_{CR}$, $F_{CR}$, $W_{CR}$, $H_{ID}$ , a hashing algorithm $\mathcal{H}$ and a digital certificate
- Verifying digital signature and hash value, $H_{ID}$
- Constructing PAT as described above and transmitting to the network
- Sending $H_{ID}$ and transaction ID of PAT to CryptoRegistry after confirmation of PAT
- Periodically querying the said CryptoRegistry for confirmation of $H_{ID}$ registration in its database
- When required, querying all CryptoRegistries for registration status of provided PII
- Displaying to the user a list of CryptoRegistries with whom provided PII is registered

### 3.2.4. Associating PII with a digital wallet

The sequence of steps for the purpose of registering a PII of the owner of a digital wallet is depicted in Figure 1.

The details of each step are as follows:

1. The user provides his/her PII to the wallet.
2. The wallet sends the provided PII for registration with the selected CryptoRegistry.
3. The CryptoRegistry selects a wallet ($W_{CR}$) for receiving registration fee ($F_{CR}$), chooses a random salt ($S_{CR}$) and calculates $H_{ID}$ which is hash of PII concatenated with $S_{CR}$. It saves this information in its database for future reference with registration status as 'Not Confirmed'.
4. The CryptoRegistry sends PII, $S_{CR}$, $F_{CR}$, $W_{CR}$ and $H_{ID}$ , its signature on this information and its corresponding digital certificate to the PII wallet.
5. The wallet creates a PII Associating Transaction (PAT) using the received information and transmits it to the Bitcoin network.
6. The wallet periodically queries the blockchain for confirmation of PAT.

7. Once PAT is confirmed, the wallet notifies the CryptoRegistry of the confirmation by sending transaction ID of PAT ($TxID_{PAT}$) and $H_{ID}$
8. The CryptoRegistry queries the blockchain for confirmation of $TxID_{PAT}$
9. Upon confirmation, The CryptoRegistry updates PII registration status as 'Confirmed' and records corresponding $TxID_{PAT}$
10. The wallet periodically queries the CryptoRegistry for PII registration status
11. Upon confirmation, the wallet notifies the user that the provided PII has been successfully registered with the selected CryptoRegistry and records $TxID_{PAT}$ for future reference.

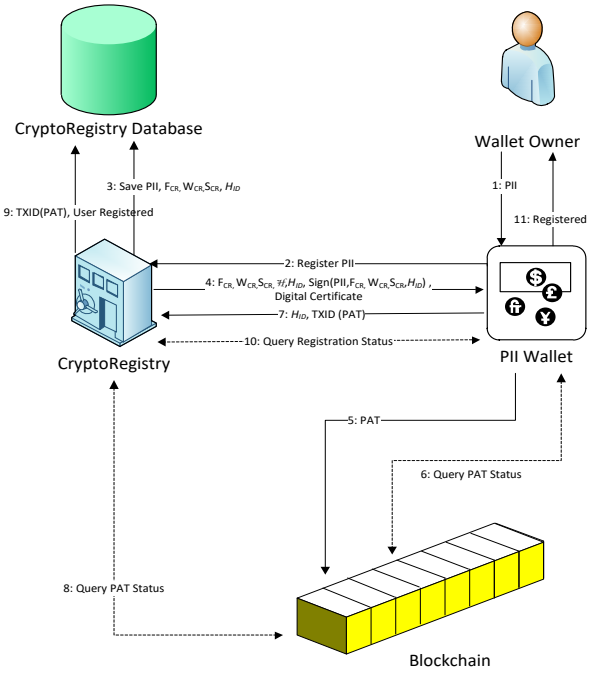


Figure 1: PII Registration in AFAP Framework

### 3.2.5. *Claiming ownership of a lost PII Wallet*

In the event of loss of a PII wallet, a PII wallet is installed and its recovery mode is initiated. The following sequence of events may follow (see Figure 2).

- The user enters her/his PII used for querying the registration status of the lost wallet.
- The wallet queries all known CryptoRegistries one by one using the provided PII.
- PII wallet receives response from the CryptoRegistries and displays the list of CryptoRegistries with affirmative response.

In the interest of owner's anonymity, the CryptoRegistry shall not reveal any information other than whether the subject PII is registered with it or not. The said CryptoRegistry may now be approached by the owner to obtain the transaction ID of the corresponding PAT along with the salt.

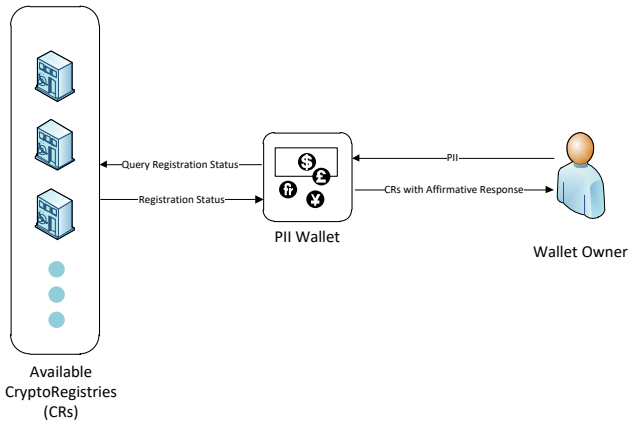


Figure 2: Claiming ownership of a lost wallet

The hash of given PII concatenated with salt is computed and matched against the one extracted from PAT. A successful match proves that the said PII was used to construct the PAT and that the wallet from which this PAT was broadcast is the wallet associated with the said PII. This way the ownership of the wallet, and any unspent funds associated with it, is established.

### 3.2.6. *Right to be forgotten*

One of the important principles incorporated into General Data Protection Regulation (GDPR) is a user's right to be forgotten (RtbF) allowing for retroactive erasure of all personal data. Considering the immutable nature of blockchain, it may appear that storing association of PII with a digital wallet may be in violation of the RtbF. However, the said right is safeguarded on two counts. Firstly, PII itself is not stored on the blockchain in any way, i.e., neither in plain text nor in encrypted form. Secondly, proving association of a particular PII with a digital wallet requires knowledge of the corresponding salt, which is a cryptographically strong random number. Hence, if the salt is forgotten, this association becomes unprovable. The right to forget this salt and any associated personal data can be exercised by the user with a request to CryptoRegistry. In [28], it has been shown that integration of such requirements into the current computing infrastructures is practically feasible.

## 4. Case study

In order to validate the proposed framework, a sample PAT was constructed by simulating interaction between a client and a typical CryptoRegistry as detailed below. The resulting transaction was successfully broadcast on Bitcoin Testnet. This was followed by simulating the situation of loss of this wallet. The lost wallet address was successfully retrieved from the blockchain by presenting only the PII. The following is the detail of interactions among the various components of the proposed AFAP framework.

### 4.1. *PII Association with a digital wallet*

The example client wishes to associate his PII "ABC1234567" with his digital wallet. The CryptoRegistry generates a salt, calculates hash of PII concatenated with this salt and returns the following information to the client along with his signature on the same:

CryptoRegistry Prefix = TESTPII

Salt: $S_{CR}$ = 9586311452

SHA1 (PII || Salt): $H_{ID}$ = d49cdc68c804114b402bbaa108d324a80a19e354

Registration Fee: $F_{CR}$= 5mBTC

Wallet address for receiving registration fee:

$W_{CR}$ = mpvkKZ6ysUYEGZuXR1FYRCKzykvMmtovyv

Signature:

Sign(PII,$F_{CR}$, $W_{CR}$,$S_{CR}$,$H_{ID}$) = AAwPRuNFlPvKCaic12aFRLYXf9ZbytXjBowXeKZm0kGNETcplSyEE268401jgS8=

The client constructs the PAT with three outputs. Firstly, paying registration fee to $W_{CR}$, secondly the change to be returned to itself and finally a null data transaction with the script comprising prefix, hash and signature of the CryptoRegistry. The resulting script is given below:

Script: TESTPIId49cdc68c804114b402bbaa108d324a80a19e354AAwPRuNFlPvKCaic12aFRLYXf9ZbytXjBowXeKZm0kGNETcplSyEE268401jgS8=

This example transaction was broadcast on Bitcoin Testnet and can be found with the transaction id "985b15d99baf20facc67f1f925e51b7dd49b34dcbdc0a64bc0607adc9100e0d7". Figure 3 shows the details of the said transaction as depicted by Bitcoin Block Explorer.

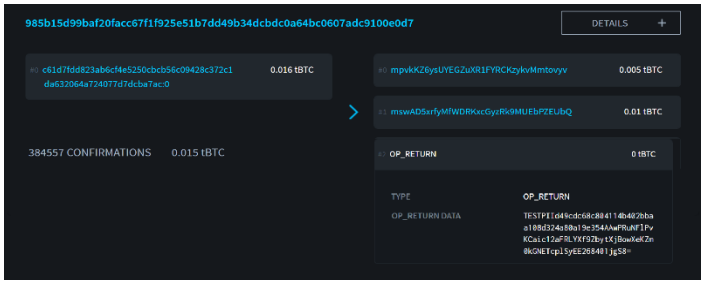


Figure 3: Details of PAT as shown by Bitcoin Block Explorer

It may be noted that the CryptoRegistry is required to store the transaction ID of PAT and other associated information in its database, as depicted in Figure 1.

### *4.2. Claiming ownership of a digital wallet*

Assuming the owner knows the transaction ID of PAT and the salt used to construct the script of PAT, firstly PAT may be retrieved from blockchain using transaction ID. Then, the PII association may be proven by calculating hash of PII concatenated with salt and validating it against the script of null data output of PAT.

Since the main purpose of the proposed AFAP framework is to relieve the wallet owner from maintaining access to the private key of a digital wallet in a secure, safe and anonymity preserving manner, the owner is not assumed to maintain transaction ID of PAT and the respective salt. In such a case, the owner may present her/his PII to the CryptoRegistry to confirm association of the said PII with a digital wallet.

## 5. Discussion

The proposed AFAP framework uses blockchain itself to store the association of the Personally Identifying Information (PII) of the owner with her/his digital wallet. The proposed framework requires a persistent entity, called CryptoRegistry, which is mandated to maintain record of transaction IDs of PII Associating Transactions (PATs) and associated information in a secure way. The proof of ownership of a digital wallet lies in hash of PII and a random number, called salt, stored in a PAT.

In case of loss of a digital wallet, the owner may query available CryptoRegistries to confirm registration of her/his PII against a PAT from their databases. Once a confirmation is received, the owner may prove her/his identity to the satisfaction of the respective CryptoRegistry in order to retrieve transaction ID of PAT and respective salt. The hash extracted from PAT validates the PII and ownership of legal claimant of the PII is established. The proposed scheme, therefore, depends on long term availability of the CryptoRegistry used to register a digital wallet. In the interest of anonymity and privacy of the wallet owner, the CryptoRegistry may require due legal process in identifying the claimant before releasing transaction ID of PAT and respective salt.

From the aforementioned requirements of a CryptoRegistry, one may draw parallel with crypto exchanges or custodial services as trusted third parties for safekeeping of users' crypto assets. However, it may be noted that in the latter case, clients' funds are stored in the wallets owned by the trusted third party functioning as a custodian. Thus a user may lose all his/her funds in the event of hacking or bankruptcy of the custodian. In contrast, in the event of bankruptcy of a CryptoRegistry, the hash values stored in respective PATs cannot be verified owing to unavailability of corresponding salts, whereas the user funds remain intact. A user may safeguard against this eventuality by choosing to register with multiple CryptoRegistries. Though, the cost of registration may discourage registration with multiple CryptoRegisteries, it is expected that existing crypto exchanges will offer CryptoRegistry services and they may waive off these fees to increase their customer base.

The proposed framework brings the cryptocurrency ecosystem a step closer to the conventional banking system where an account holder may prove ownership of funds after losing access to corresponding checkbook or card. It may be noted that the protection afforded to an individual by AFAP is stronger than that of traditional banks since the funds and proof of ownership are stored in an immutable blockchain and there is no risk akin to bankruptcy.

## 6. Future Work

Although a user may claim ownership of her/his lost funds in the above manner, the process for recovery/compensation may involve legal procedures. One possible way of compensating the owner of a lost wallet is to create a compensation fund for such eventualities. Alternatively, a special transaction to credit the required funds to claimant's new wallet akin to the mechanism proposed for managing deflation of cryptocurrencies by [29]. Further, similar to the expiration flag proposed by them, the old wallet needs to be flagged as invalid in a way that blocks any future access to it or funds associated with it.

## References

[1] Capgemini, BNP Paribas, "World Payments Report 2018," 55, 2018.
[2] V. Buterin, "Deterministic Wallets, Their Advantages and their Understated Flaws," Bitcoin Magazine, 2013.
[3] D.Z. Morris, "Bitcoin Hits a New Record High, But Stops Short of $20,000

| Fortune," Fortune, 2017.
[4] R. Krygier, "Venezuela launches the 'petro' its cryptocurrency," The Washington Post, 2018.
[5] M. Raskin, D. Yermack, Digital currencies, decentralized ledgers and the future of central banking, 2018, doi:10.4337/9781784719227.00028.
[6] K. Krombholz, A. Judmayer, M. Gusenbauer, E. Weippl, "The other side of the coin: User experiences with bitcoin security and privacy," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, doi:10.1007/978-3-662-54970-4_33.
[7] J.J. Roberts, N. Rapp, "Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says," Fortune, 2017.
[8] T. Bult, "Thesis - Security analysis of blockchain technology Security analysis of blockchain technology."
[9] M. Palatinus, P. Rusnak, A. Voisine, S. Bowe, (bip-0039) Mnemonic code for generating deterministic keys, GitHub, 2013.
[10] Y. Liu, R. Li, X. Liu, J. Wang, L. Zhang, C. Tang, H. Kang, "An efficient method to enhance Bitcoin wallet security," in Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID, 201-207, 2018, doi:10.1109/ICASID.2017.8285737.
[11] M. Conti, K.E. Sandeep, C. Lal, S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys and Tutorials, 2018, doi:10.1109/COMST.2018.2842460.
[12] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, R. Brooks, "A brief survey of Cryptocurrency systems," in 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016, 1-5, 2016, doi:10.1109/PST.2016.7906988.
[13] S. Eskandari, D. Barrera, E. Stobert, J. Clark, A first look at the usability of bitcoin key management, ArXiv, 2018, doi:10.14722/usec.2015.23015.
[14] R.N. Akram, K. Markantonakis, D. Sauveron, "Recovering from a lost digital wallet: A smart cards perspective extended abstract," Pervasive and Mobile Computing, 2016, doi:10.1016/j.pmcj.2015.06.018.
[15] O. Boireau, "Securing the blockchain against hackers," Network Security, 2018, doi:10.1016/S1353-4858(18)30006-0.
[16] E.M.D.W. Brickell, SECURE STORAGE OF PRIVATE KEYS, United States, 2005.
[17] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, Y. Li, "A Social-Network-Based Cryptocurrency Wallet-Management Scheme," IEEE Access, 2018, doi:10.1109/ACCESS.2018.2799385.
[18] L.J. Trautman, "Virtual Currencies: Bitcoin & What Now after Liberty Reserve and Silk Road?," SSRN Electronic Journal, 2014, doi:10.2139/ssrn.2393537.
[19] U. Chohan, "The Problems of Cryptocurrency Thefts and Exchange Shutdowns," SSRN Electronic Journal, 2018, doi:10.2139/ssrn.3131702.
[20] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V. Kalyanaraman, "Blockchain Technology - BEYOND BITCOIN," Berkley Engineering, 2016.
[21] M. Rosenfeld, "Overview of colored coins," 13, 2012.
[22] L. Bell, W.J. Buchanan, J. Cameron, O. Lo, "Applications of Blockchain Within Healthcare," Blockchain in Healthcare Today, 1-7, 2018, doi:10.30953/bhty.v1.8.
[23] H. Min, "Blockchain technology for enhancing supply chain resilience," Business Horizons, 2019, doi:10.1016/j.bushor.2018.08.012.
[24] M. Ali, J. Nelson, R. Shea, M.J. Freedman, "Bootstrapping Trust in Distributed Systems with Blockchains," USENIX ;Login:, 2016.
[25] M. Bartoletti, L. Pompianu, "An analysis of bitcoin OP_RETURN metadata," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, doi:10.1007/978-3-319-70278-0_14.
[26] Y.G. Malahov, "BitAlias I Aka Usernames for Bitcoin," Medium, 2015.
[27] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, A. Narayanan, "An empirical study of Namecoin and lessons for decentralized namespace design," 14th Annual Workshop on the Economics of Information Security (WEIS), 2015.
[28] E. Politou, E. Alepis, C. Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, Journal of Cybersecurity, **4**(1), tyy001, 2018, doi:10.1093/cybsec/tyy001.
[29] H. Gjermundrød, I. Dionysiou, "Recirculating lost coins in cryptocurrency systems," Lecture Notes in Business Information Processing, 229-240, 2014, doi:10.1007/978-3-319-11460-6_20.