Secure Cryptocurrency Depository

Dr. Praveen Baratam

Background:

Crypto-currencies in general are secured with public-key cryptography where a public-key or a derivative of it serves as wallet/address containing funds/tokens in the underlying ledger and the owner proves to the corresponding network and community that he is in possession of the respective private-key with a cryptographic signature and authenticates himself as the rightful owner of the respective funds/tokens to transfer/spend the same.

From an end-user's perspective it boils down to keeping his private-keys safe and away from prying eyes to secure his funds/tokens. If one misplaces/loses his private-keys, his funds/tokens are lost forever. Similarly if anyone can steal his private-keys, his funds/tokens can also be stolen without any chance of recovery.

While securing one's private-keys might seem trivial at first but ensuring safety i.e. preventing data loss (lost private-key) along with absolute security i.e. preventing data theft is very difficult if not impossible.

Several methods and devices were proposed and implemented to alleviate this problem at least partially but none are as flexible and secure as one would desire them to be.

On an individual level, one can generate and/or store their private-keys in a secure electronic device frequently referred to as a Hardware Wallet that only signs transactions on his behalf but never gives access to the said private-keys inside it. Assuming these devices have no exploitable defects/backdoors, they can alleviate several attack vectors such as trojans, man-in-the-middle, etc. However, one real cause for concern here is that these hardware wallets can malfunction like any other electronic device out there or be lost and hence cannot assure data safety. As a result, they are in turn backed up for safety and these backups (often referred to as seed phrases) effectively become one's new secret which in turn can be lost or stolen.

On the other hand, many currently resort to multi-signature arrangements where more than one signature (m-of-n or n-of-n) from different entities, with corresponding private-keys, are needed to authenticate and unlock specific funds/tokens in the underlying blockchain/ledger. Here the assumption is that the probability of multiple entities losing their respective private-keys or malicious entities gaining access to them is exponentially lower than the same thing happening with a single entity. However, a malicious entity in possession of the given end-user's private-key might be able to pose as him over network to the other parties in this multi-signature scheme and still steal the said funds/tokens. BitFinex, a cryptocurrency exchange, was compromised in a similar attack in spite of multi-signature security arrangements with BitGo, a company providing non-custodial multi-signature

security to businesses and entities dealing in cryptocurrencies, and Bitcoin worth 70 Million USD were stolen from it. All that can be done in such arrangements is that the other/securing parties can impose limits on spends/transfers in a given time frame and contain fraud. On another note, the other parties can become hostile or disappear; effectively holding one's funds/tokens hostage until such situation is resolved.

To sum it up, we either risk losing access to our own funds/tokens and/or risks theft and we have to choose one or more methods depending on the compromises we are willing to make in this regard.

Solution:

The following describes an arrangement and method, in its simplest form, between two parties (First Party and Second Party) participating in a cryptocurrency network/system to effectively reduce the probability of loss or theft of the First Party's funds/tokens. Here the Second Party is acting as Secure Cryptocurrency Depository for the First Party. This arrangement and method can be similarly and analogously extended to even more parties as may be necessary.

The method presumes that unrecoverable hardware wallets without any provision to recover the private-keys stored inside it in case of loss or malfunction of the device, hereafter referred to as hardware tokens, and time-locks for transaction outputs are available for the crypto-currency system of interest. Relative time-locks (CheckSequenceVerify) similar to the one described in Bitcoin Improvement Proposal 112 are more desirable than absolute time-locks (CheckLockTimeVerify) similar to the one described in Bitcoin Improvement Proposal 65. The subsequent discussion assumes relative time-locks are available for the cryptocurrency of interest even though similar functionality can be devised using absolute time-locks too.

The method and arrangement proceeds as follows:

1. At inception, the First Party creates a transaction similar to the one depicted in Figure 1, hereafter called the Deposit Transaction, in which the First Party transfers an arbitrary sum of funds/tokens in its control to a multi-signature address but does not yet sign or broadcast it. The multi-signature address in the Deposit Transaction requires the following signatures to authenticate and spend/transfer from it:

    a. First Party's Private Key generated Signature
    b. First Party's Hardware Token generated Signature
    c. Second Party's Private Key generated Signature

2. Then, the First Party creates a second transaction, hereafter referred to as Provisional Transaction, as depicted in Figure 2, spending all the funds/tokens sent to the multi-signature address in the Deposit Transaction, and sends a copy of the Provisional Transaction without any signed inputs or signatures, to the Second Party. Please note that the Provisional transaction is spending from an unconfirmed Deposit

Transaction.

3. Then, the Second Party adds its Private Key generated signature to the unsigned Provisional Transaction received from the First Party and then sends the partially signed Provisional Transaction back to the First Party.

4. In the meantime, the First Party also adds its Private Key generated signature and the signature generated by the hardware token in its possession to the unsigned copy of the Provisional Transaction it created and sends the partially signed Provisional Transaction to the Second Party.

   Note: The signatures used in this scheme sign the transaction similar to SIGHASH_ALL or SIGHASH_SINGLE in BitCoin protocol where the corresponding output of the transaction cannot be modified once signed.

5. At this point in time, the First Party is in possession of the partially signed Provisional Transaction with Second Party's Private Key generated signature added to it and the Second Party is in possession of the partially signed Provisional Transaction with First Party's Private Key generated signature and the signature generated by the hardware token in First Party's possession added to it.

6. Then, the First Party signs and broadcasts the Deposit Transaction it created to the cryptocurrency network/system completing the setup process. The whole process in outlined in **Figure 3**.

7. Once the Deposit Transaction is confirmed, both First Party and Second Party start monitoring the Cryptocurrency network directly and/or using third party services for transactions referencing the Multi-Signature output address described above from the Deposit Transaction to detect any breach of security or foul play.

8. Subsequently, the First Party, at its discretion, can add its Private Key generated signature and the signature generated by the hardware token in its possession to the partially signed Provisional Transaction with the Second Party's Private Key generated signature and broadcast the fully signed Provisional Transaction to the cryptocurrency network/system when necessary.

9. Similarly, the Second Party can add its Private Key generated signature to the partially signed Provisional Transaction with the First Party's Private Key generated signature and the signature generated by the hardware token in possession of the First Party and broadcast the fully signed Provisional Transaction to the cryptocurrency network/system when necessary.

10. To sum it up, either parties can add missing signatures to the partially signed Provisional Transaction in their possession and broadcast them when necessary.

11. As soon as the Provisional Transaction is broadcasted, the cryptocurrency monitoring systems prompt both parties to initiate recovery if it is not broadcasted by them to begin with. Either ways First Party or the Second Party in coordination with the other or optionally unilaterally create and broadcast a transaction using the respective options of the Provisional Transaction transferring the funds/tokens to a desired address terminating the arrangement.

Description

Common attacks on data safety and security include ransomware, trojans, man-in-the-middle, etc. Most attacks either compromise **data-safety** by denying/destroying access to one's private-keys/secrets (ransomware, computer-virus, etc.) or **data-security** by gaining access to one's private-keys through whatever means (trojans, man-in-the-middle, cloud backdoors, etc.) or both.

To defend against the aforementioned attack vectors, one needs to plan for situations where one's private keys are lost and/or stolen. In case of multi-factor authentication schemes such as Multi-Signature Cryptocurrency Wallets, we also need to plan for situations where one, multiple or all parties' private-keys are lost and/or stolen. While most existing arrangements/systems rely on one-more factor and m-of-n factor arrangement to harden the offered protection, they are still knowledge based proof systems in the end and can be compromised.

One of the salient features of the proposed system is out-of-band authentication with Hardware Tokens, that are not knowledge-based and require physical access to complete the step. Hardware Tokens are a special kind of Hardware Wallets, that do not allow a backup or recovery of any sort providing true out-of-band authentication and device failure is already accounted for in the proposed scheme.

The above discussed scheme/protocol with deposit and unconfirmed provisional transactions allows for many contingencies such as loss and/or breach of either party's private-keys and malfunction, loss and/or possible theft of either party's hardware tokens while reducing the probability of loss of First Party's funds/tokens to a great extent. There will be an opportunity to recover the funds/tokens in a majority of situations thereby removing the incentive and consequently motive to steal First Party's funds/tokens in the first place.

Whenever First Party and/or Second Party realize that they have lost their respective private-keys and/or hardware tokens, one of them can add the missing signatures to the partly signed Provisional Transaction with them and broadcast the same to initiate recovery of funds/tokens.

Also, whenever there is any breach, the adversary, in most situations needs the partly signed provisional transaction along with the private-key in case of Second Party or both private-key and hardware token in case of First Party to steal the funds. In which case the adversary will add the missing signatures to the stolen partly signed Provisional Transaction using the stolen private-keys (and hardware token as the case may be) and broadcast the

same hoping that no action will be taken by either parties until he gets a chance to transfer the funds/tokens to an address in its control. But, as soon as the provisional transaction is broadcasted cryptocurrency network monitoring systems, either internal or external, will signal the First Party and Second Party to initiate recovery as exemplified below.

For instance, when the First Party's private-key is breached, its funds/tokens remain safe and can be recovered by adding his signatures (using his private-key and hardware token) to the half-signed provisional transaction in its possession and broadcasting the fully signed provisional transaction to the respective cryptocurrency network. In this particular case it can recover its tokens in coordination with the Second Party before 5000 blocks are created on the respective blockchain after the block confirming the broadcasted provisional transaction.

Or in another instance, when the Second Party (Depository) is completely compromised and all its private-keys and hardware tokens are lost/stolen, the First Party and other parties with similar arrangement and relationship with Second Party can recover their funds/tokens before 2000 blocks are created on the respective blockchain after the block confirming the broadcasted provisional transaction (either by them or the adversary) as discussed previously as long as their private-keys and hardware tokens are safe and secure. In the above situation, even if the First Party's private-keys are breached, it can still recover its funds/tokens before 500 blocks are created as long as its hardware tokens are safe.

The **Confusion Matrix** in **Figure 4** enumerates the options available and outcomes of situations where private-keys and/or hardware tokens of First Party and/or Second Party are compromised or stolen. It also enumerates situations where respective private-keys are lost by First Party but not Second Party.

Since Second Party is an organized entity that can employ data-safety measures such as multi-site replication, offline storage, etc. this method does not explicitly specify the process and enumerate options available when Second Party's private-keys are lost for simplicity and brevity. This method can be analogously extended to this scenario and more or simplified if desired by reordering/adding/removing options in the Provisional Transaction accordingly when planning and accounting for certain contingencies are deemed necessary or unnecessary. Also the timelocks mentioned in the Provisional Transaction are one of the many possible values for them exemplifying a particular order and can be adjusted as necessary to suit a particular arrangement.

It should be noted here that in certain situations where the First Party has lost its private-key and/or hardware token as enumerated in the Confusion Matrix from Figure 3, the Second Party can steal First Party's funds/tokens but will not do so because such unilateral actions will result in loss of trust/business from other parties as well as legal proceedings by the First Party. Hence, the incentive and motive to cheat the First Party of its funds/tokens is non-existent. But if such participating entities are compromised either by an internal or external adversary, they still have recourse and can reconcile the situation by taking remedial steps available.

Finally, even if Hardware Tokens are not available and we have to rely on relative/absolute timelocks only, the method and scheme described above can be scaled down as depicted in **Figure 5** and still offer better protection than currently practiced multi-signature arrangements.

Figure 1


DEPOSIT TRANSACTION
Alice
Depository
From Alice
5 BTC
Signatures:
Alice
To Alice Depository
5 BTC
Required to Unlock:
Alice
Depository
***
Private Key
Based Signatures
Hardware Token
Based Signature

Figure 2

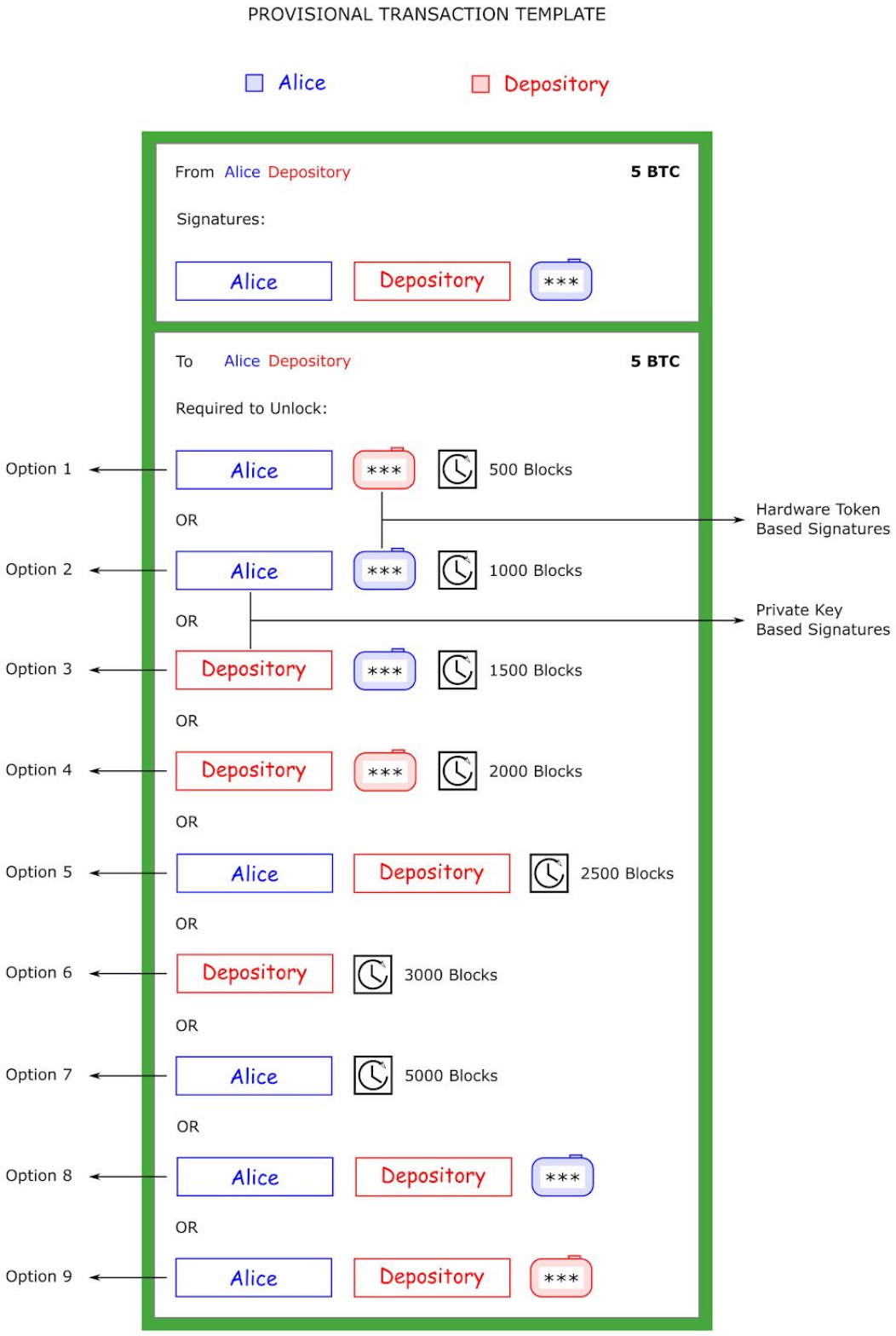

PROVISIONAL TRANSACTION TEMPLATE
Alice
Depository
From Alice Depository
5 BTC
Signatures:
Alice
Depository
***
To Alice Depository
5 BTC
Required to Unlock:
Option 1
Alice
***
500 Blocks
OR
Hardware Token
Based Signatures
Option 2
Alice
***
1000 Blocks
OR
Private Key
Based Signatures
Option 3
Depository
***
1500 Blocks
OR
Option 4
Depository
***
2000 Blocks
OR
Option 5
Alice
Depository
2500 Blocks
OR
Option 6
Depository
3000 Blocks
OR
Option 7
Alice
5000 Blocks
OR
Option 8
Alice
Depository
***
OR
Option 9
Alice
Depository
***

Figure 3

COINVAULT

Alice creates a **Deposit Transaction** transferring Bitcoin to a Multisig Address requiring Signatures generated by Alice's Private Key, Depository's Private Key and Alice's Hardware Token* to spend from it

t_0

Alice creates a **Provisional Transaction** as per **Provisional Transaction Template** provided by **CoinVault** spending all the Bitcoin from the Deposit Transaction and transmits a blank copy of the Provisional Transaction without any signatures to Depository

t_1

Depository receives a blank copy of **Provisional Transaction** without any signatures from Alice

Alice adds **Signatures** generated using her Private Key and Hardware Token* to the Provisional Transaction and transmits it to Depository

t_2

Depository adds **Signatures** generated using its Private Key to the Provisional Transaction and transmits it back to Alice

Alice receives **Partially Signed Provisional Transaction** from Depository

t_3

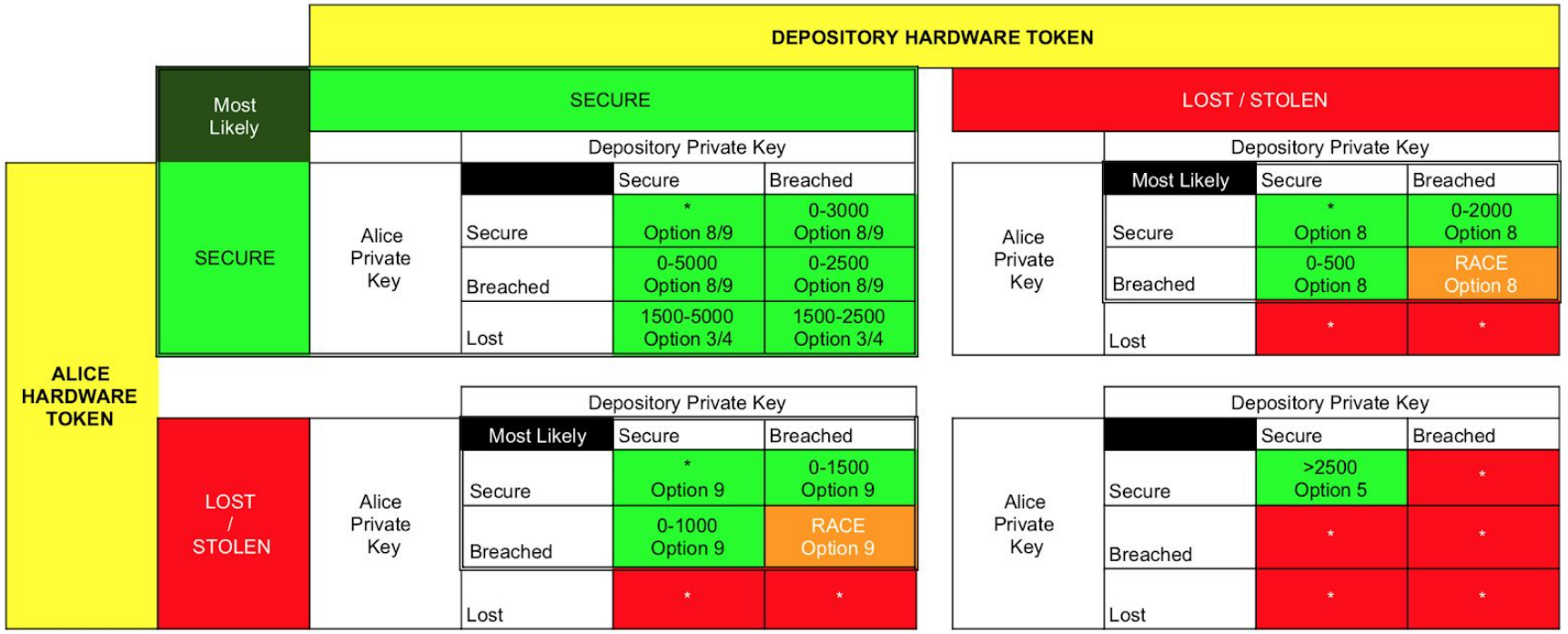
Depository receives **Partially Signed Provisional Transaction** from Alice

Alice broadcasts the Signed **Deposit Transaction** to **Bitcoin Network**

t_4

* Hardware Token is a special Hardware Wallet without any seed phrase to recover the keys

Figure 4



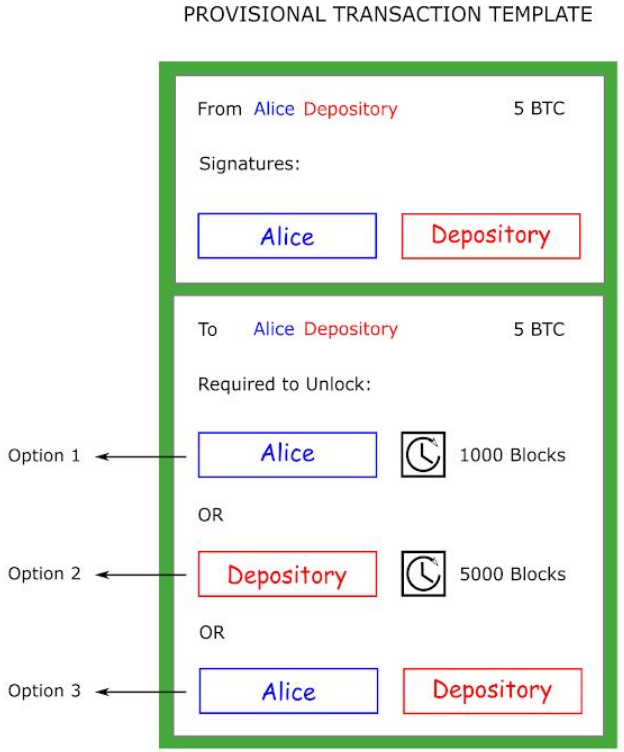
Note: When a **Private Key** is lost, it is assumed as breached. When a **Hardware Token** is lost, it is assumed malfunctioning, lost or stolen.

Note: Green squares indicate situations where recovery is possible within the mentioned window period in blocks of the blockchain. **Red** blocks indicate situations where remedial steps might fail to recover Alice's funds. **Orange** Blocks indicate situations where neither Alice+Vault nor the adversaries have an advantage over one another in claiming Alice's funds.

Note: Options as depicted in **Provisional Transaction Template**

Secure Vault without Hardware Tokens

Figure 5



Confusion Matrix

Alice Private Key \ Depository Private Key	Secure	Breached
Secure	* Option 3	0-5000 Option 3
Breached	0-1000 Option 3	*
Lost	*	*

Note: Lost Private Keys are assumed stolen.