Secure Cryptocurrency Exchange & Wallet

Dr. Praveen Baratam

Background:

Cryptocurrencies in general are both acquired and traded on an electronic exchange that lists different cryptocurrencies/crypto-assets often with other assets such as fiat currencies issued by central banks of various countries and enables trading between them. Most of these exchanges are custodial in nature and act as trusted third parties where trading parties transfer both cryptocurrencies and other assets in their control/possession to the exchange controlled addresses/accounts and get notional limits on the exchange to trade. All this works well as long as there is no security breach on the exchange.

Since most cryptocurrencies are secured by public-key encryption which is knowledge based, any security breach on the exchange's systems can be disastrous. And any adversary gaining access to exchange's private-keys can irreversibly steal the cryptocurrencies in its custody leading to huge loss of wealth for trading parties and loss of trust within the ecosystem. We have seen this scenario playout with many cryptocurrency exchanges all over the world at some point or the other and approximately 15 Billion USD worth cryptocurrencies were stolen from them as of Dec 2017. This has become the Achilles heel of the cryptocurrency world off late.

Over time cryptocurrency exchanges have evolved several strategies such as Hot-Wallets coupled with Cold/Offline Storage, Multi-Signature arrangements with third-parties that serve as gatekeepers to enforce limits on transactions, insurance for hot funds, etc. But most of these strategies have proved inadequate and/or were circumvented over the past few years by increasingly sophisticated attacks. eg: BitFinex lost $71 Million USD worth of Bitcoin in spite of Multi-Signature arrangements with BitGo.

The same is true for Custodial Cryptocurrency Wallet Services, hereafter referred to as Cryptocurrency Wallets, that store users' funds/tokens with them and allow their users to make transactions like a bank. They then settle these transactions on their users' behalf. Most Cryptocurrency Exchanges also double up as Cryptocurrency Wallets for their users allowing transacting parties to pay/accept in cryptocurrencies/assets of their choice and managing the conversion for them when necessary.

There is an urgent need for securing cryptocurrency exchanges and wallets to prevent further losses and bolster general faith in the cryptocurrency ecosystem.

Solution:

The following describes an arrangement and method, in its simplest form, between two parties (First Party and Second Party where the Second Party is acting as Secure

Cryptocurrency Exchange and/or Wallet for the First Party) participating in a cryptocurrency network/system to effectively reduce the probability of loss or theft of the First Party's funds/tokens while guaranteeing settlement between trading/transacting parties by the Second Party. Hereafter, the term Cryptocurrency Exchange, shall also imply Cryptocurrency Wallet wherever relevant.

The method presumes that unrecoverable hardware wallets (or rendered unrecoverable by not-recording / discarding the backup/seed) without any provision for recovery of the private-keys/secrets 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

Cryptocurrency Exchanges act as custodial escrow agents for the trading entities participating on their platforms to minimize counter party risk and guarantee settlement. However, this escrow mechanism, with respect to cryptocurrencies, creates a new problem of keeping third party funds/tokens in their custody safe and secure. A security breach on the

respective Cryptocurrency Exchanges' systems can compromise the private-keys securing the funds in its custody and lead to loss/theft of respective funds/tokens.

In the proposed scheme/arrangement a Cryptocurrency Exchange can enforce settlement albeit with a predefined delay and does not need exclusive custody of the said funds/tokens beforehand to guarantee settlement. Moreover, in the event of a security breach on one or both sides, there are remedial steps that the Cryptocurrency Exchange and/or First Party can take to prevent loss or theft of respective funds/tokens.

Generally, First Party will cooperate with Second Party in the settlement process and in situations where it disagrees or refuses to cooperate, the Cryptocurrency Exchange (Second Party) can get exclusive custody of the respective funds/tokens and enforce settlements as per the terms of the contractual service agreement with the First Party.

For instance, when the First Party is in disagreement with a proposed settlement for a trade, the Cryptocurrency Exchange (Second Party) can use the Option 2 as depicted in Figure 2 and take exclusive custody of the respective funds/tokens to enforce settlement. This option allows the Cryptocurrency Exchange to function as a regular custodial escrow between trading parties as is the case with most exchanges and in general.

In another instance, if a Cryptocurrency Exchange suffers a security breach and its private-keys are compromised/stolen, it can use Option 1, 2, 3, 7 or 8 depicted in Figure 2 to transfer the funds/tokens to another secure address or back to the First Party as may be desired. Cryptocurrency Exchanges can even prevent loss/theft using Option 7 depicted in Figure 2 and transfer the respective funds/tokens away from the compromised address even when its hardware tokens are lost/stolen in the above described situation.

Also, the Cryptocurrency Exchange (Second Party) can use Option 2 depicted in Figure 2 and transfer the respective funds/tokens to a secure address when First Party's private-key and/or hardware token are compromised/lost/stolen.

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 or 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 the Second Party always gets first claim on the respective funds/tokens as it is accepting a liability on First Party's behalf and 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 by Second Party is non-existent. But if First Party and/or Second Party 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

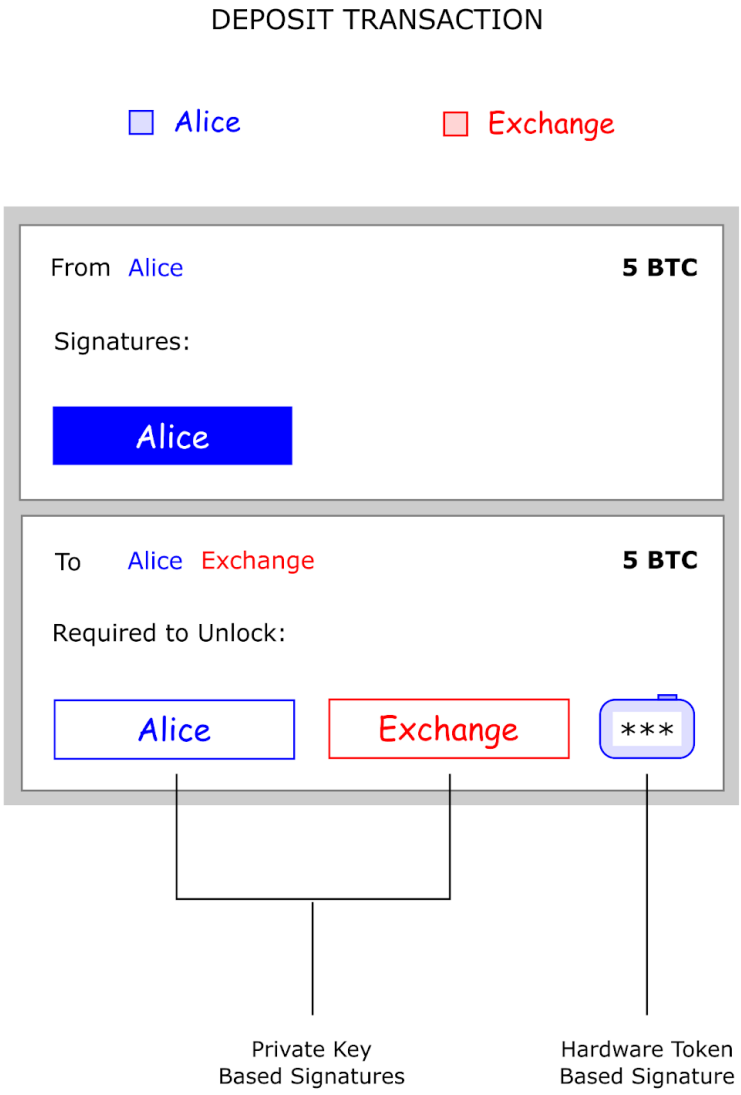

DEPOSIT TRANSACTION
Alice
Exchange
From Alice
5 BTC
Signatures:
Alice
To Alice Exchange
5 BTC
Required to Unlock:
Alice
Exchange
***
Private Key
Based Signatures
Hardware Token
Based Signature

Figure 2

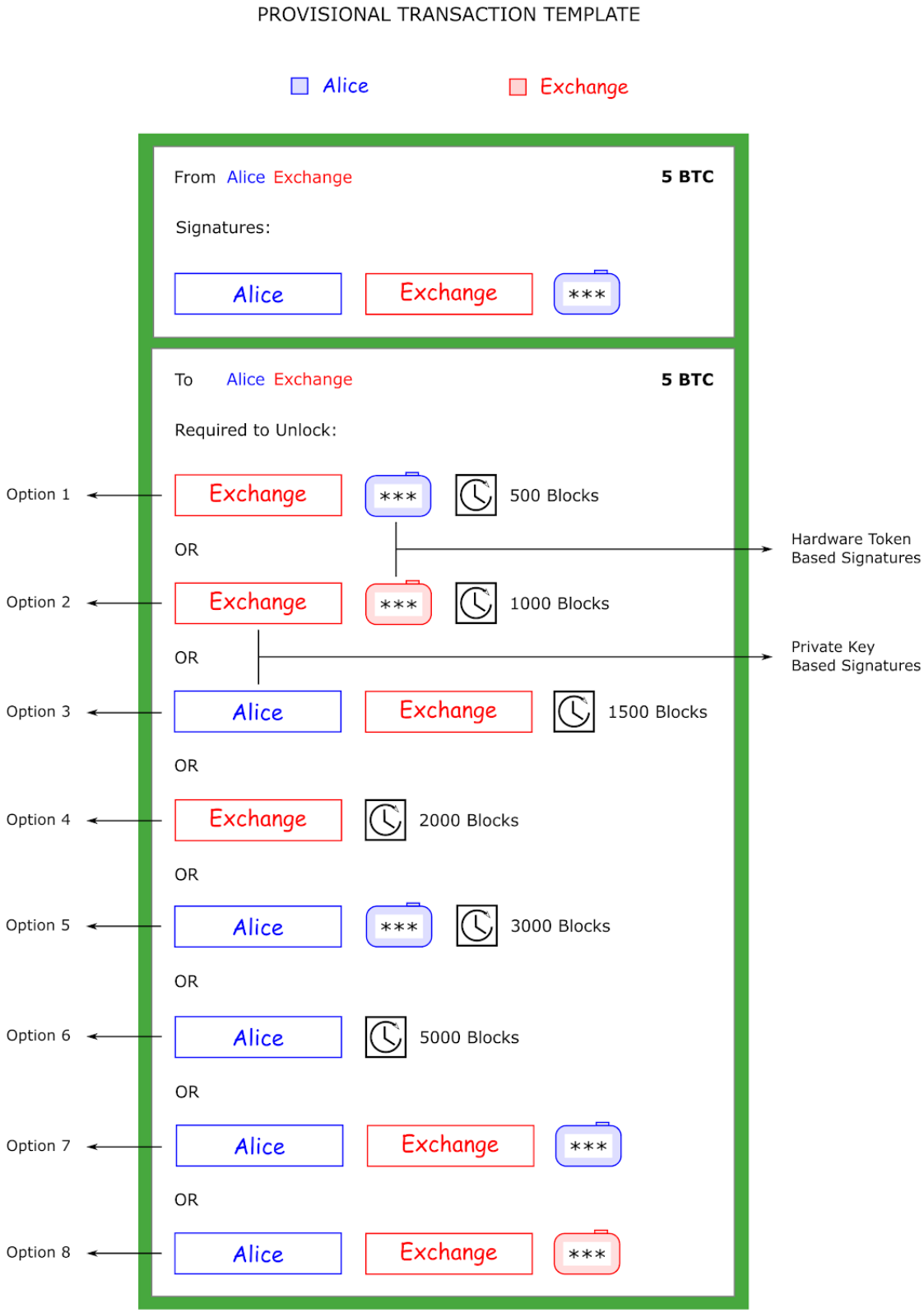

PROVISIONAL TRANSACTION TEMPLATE
Alice
Exchange
From Alice Exchange
5 BTC
Signatures:
Alice
Exchange
***
To Alice Exchange
5 BTC
Required to Unlock:
Option 1
Exchange
***
500 Blocks
OR
Hardware Token Based Signatures
Option 2
Exchange
***
1000 Blocks
OR
Private Key Based Signatures
Option 3
Alice
Exchange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

Figure 3

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

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 Exchange

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

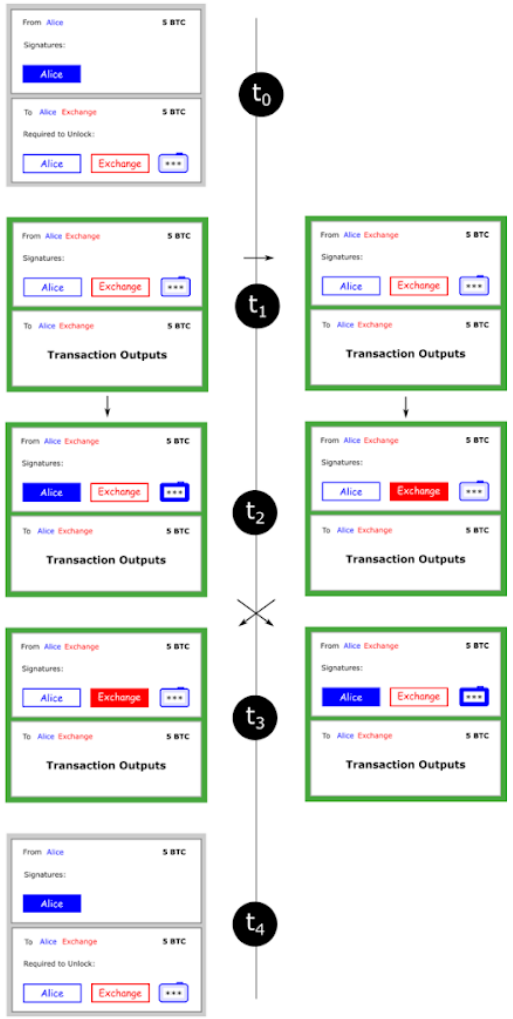
Alice adds **Signatures** generated using her Private Key and Hardware Token* to the Provisional Transaction and transmits it to Exchange

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

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

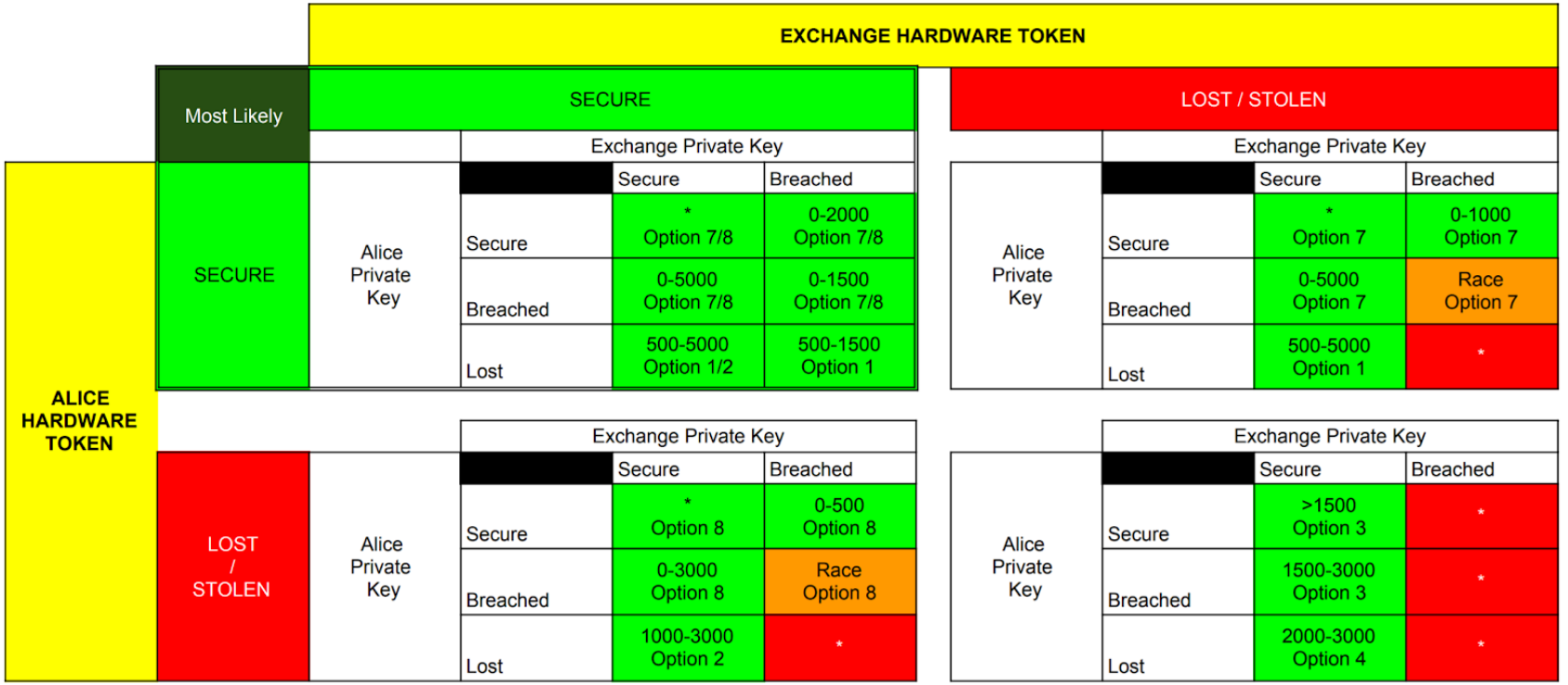
Exchange receives **Partially Signed Provisional Transaction** from Alice

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



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

Figure 4



Note: When a **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 & Exchange nor the adversaries have an advantage over one another in claiming Alice's funds.

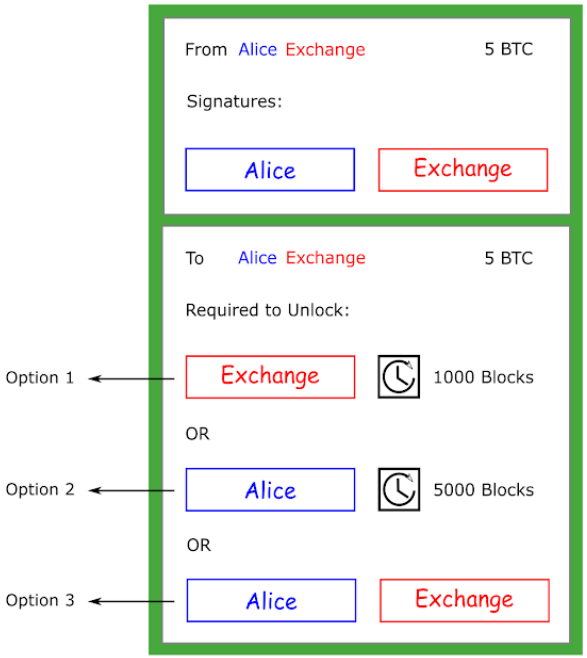
Note: Options as depicted in **Provisional Transaction Template** in **Figure 2**.

Figure 5

Secure Exchange without Hardware Tokens

DEPOSIT TRANSACTION

PROVISIONAL TRANSACTION TEMPLATE



Confusion Matrix

Alice Private Key	Exchange Private Key: Secure	Exchange Private Key: Breached
Secure	* Option 3	0-1000 Option 3
Breached	0-5000 Option 3	*
Lost	1000-5000 Option 1	*

Note: Lost Private Keys are assumed stolen.