Hybrid Custody using Smart Vaults for Hot Wallets

Dr. Praveen Baratam
CoinVault.tech
Updated 28th Aug, 2024

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 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. Any adversary gaining access to the exchange's private-keys can irreversibly steal the cryptocurrencies in its custody leading to a huge loss of wealth for trading parties and a loss of trust within the ecosystem. We have seen this scenario play out with many cryptocurrency exchanges and service providers all over the world and approximately 77 Billion USD worth of cryptocurrencies were stolen from them as of Oct 2023. This has become the Achilles heel of the cryptocurrency world of 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. However, most of these strategies have proved inadequate and/or were circumvented over the past few years by increasingly sophisticated attacks. eg: WazirX was recently hacked (July 2024) and lost 231 Million USD worth of cryptocurrencies despite state-of-the-art security practices.

The same is true for Custodial Cryptocurrency Wallet Services, hereafter referred to as Cryptocurrency Wallets, which 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.

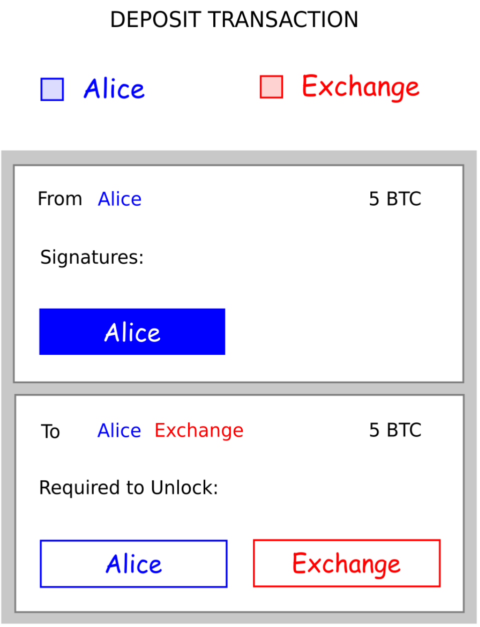
There is an urgent need for securing cryptocurrency exchanges and wallets to prevent further losses and bolster general faith in the cryptocurrency ecosystem.

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 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.

Figure 1



Setup:

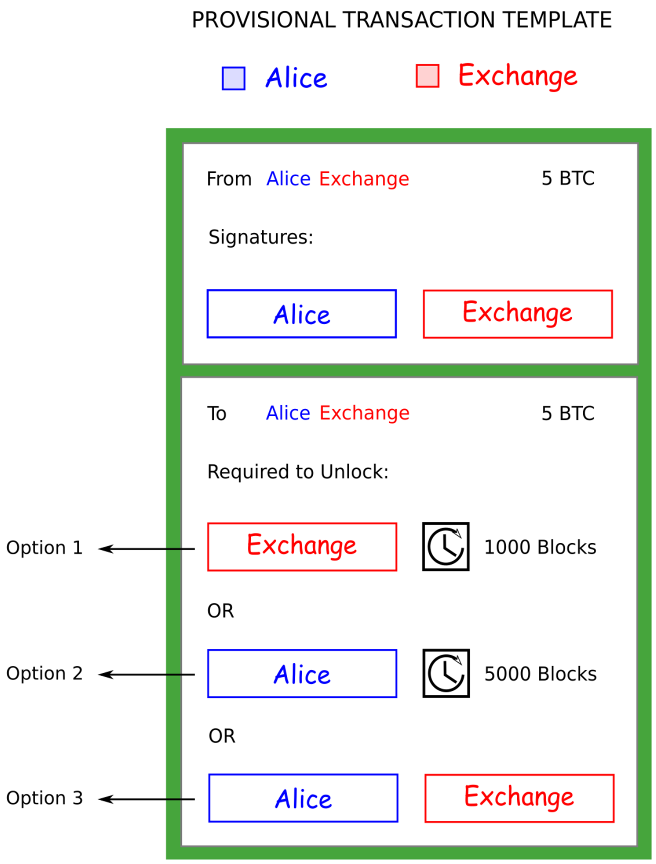
1. At inception, the First Party creates a transaction similar to the one depicted in **Figure 1** (Alice as the First Party and Exchange as the Second Party)**,** hereafter called the Deposit Transaction, in which the First Party transfers an arbitrary sum of tokens it owns to a multi-signature address 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. 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** (Alice as the First Party and Exchange as the Second Party), spending all the tokens sent to the multi-signature address in the Deposit Transaction, and sends a copy of the unsigned Provisional Transaction to the Second Party. Please note that the Provisional transaction is spending from an unconfirmed Deposit Transaction.

Figure 2



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

4. Parallelly, the First Party also adds its Private Key generated signature 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 transactions similar to SIGHASH_ALL or SIGHASH_SINGLE in Bitcoin protocol.

5. At this point, the First Party has the partially signed Provisional Transaction with the Second Party's Private Key generated signature already added to it and the Second Party has the partially signed Provisional Transaction with the First Party's Private Key generated signature already 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 is outlined in **Figure 3** (Alice as the First Party and Exchange as the Second Party).

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

8. Subsequently, the First Party, at its discretion, can add its Private Key generated signature to the partially signed Provisional Transaction with the Second Party's Private Key generated signature already added to it and broadcast a fully signed and valid Provisional Transaction to the cryptocurrency network/system when necessary.

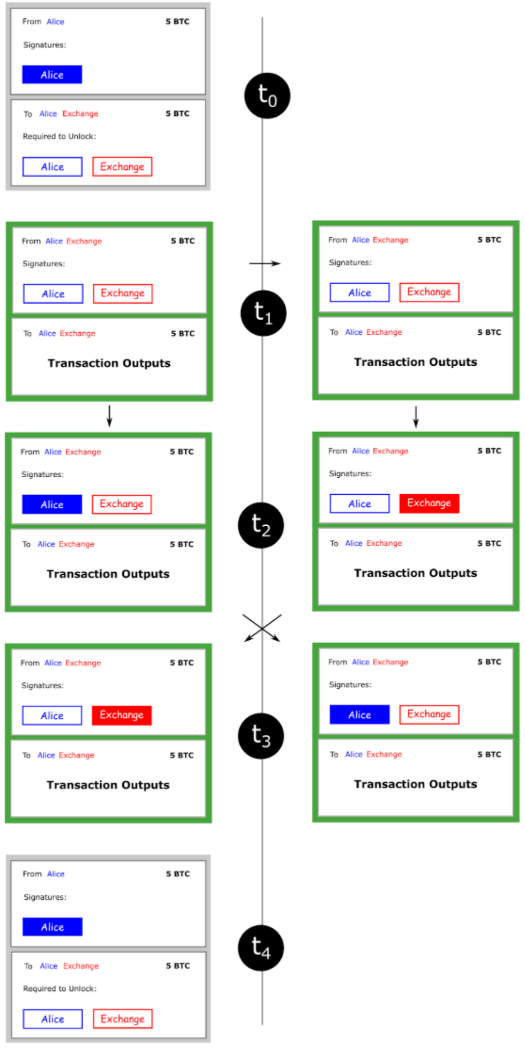
9. Similarly, the Second Party can add its Private Key generated signature to the partially signed Provisional Transaction with the First Party's Private Key generated signature already added to it and broadcast a fully signed and valid Provisional Transaction to the cryptocurrency network/system when necessary.

10. To sum it up, either party can add missing signatures to the partially signed Provisional Transaction in their possession, broadcast the same when necessary, and unlock the Smart Vault.

11. Whenever the First Party or the Second Party wants to terminate this arrangement and transfer the tokens from the Smart Vault created above, it can sign (add the missing signatures) the partially signed provisional transaction with it and broadcast a fully signed and valid provisional transaction to the network and unlock the Smart Vault. Either party can also ask the other party to do the same if its private-key is lost.

12. Once the provisional transaction is confirmed, the First Party or the Second Party, either unilaterally or in coordination with the other if they suspect foul play, can create and broadcast another transaction transferring the tokens from the Provisional Transaction to a desired address using the respective options of the Provisional Transaction.

Figure 3



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

Alice creates a **Provisional Transaction** as per Smart Vaults **Provisional Transaction Template** spending all the Bitcoin from the Deposit Transaction and transmits a copy of the Unsigned Provisional Transaction to the Exchange

Exchange receives a copy of the Unsigned **Provisional Transaction** from Alice

Alice adds the **Signature** generated using her Private Key to the Unsigned Provisional Transaction and transmits it to the Exchange

Exchange adds the **Signature** generated using its Private Key to the Unsigned 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**

Description

Cryptocurrency Exchanges act as custodial escrow agents for the trading entities participating on their platforms to minimize counterparty risk and guarantee settlement. However, this escrow mechanism 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.

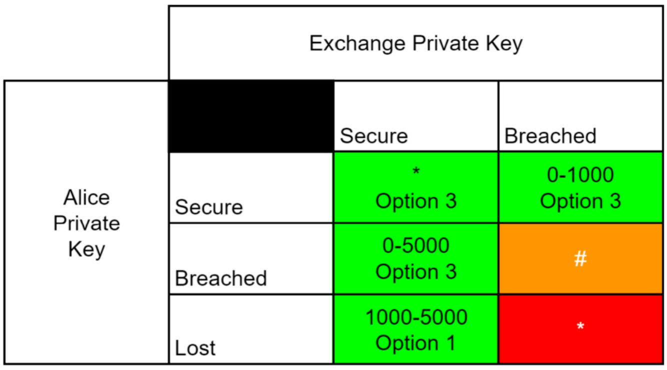
In the proposed scheme/arrangement a Cryptocurrency Exchange can enforce settlement albeit with a predefined delay and does not need exclusive custody of the said funds/tokens beforehand to guarantee settlement. Moreover, in the event of a security breach on one or both sides, there are remedial steps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

Generally, the First Party will cooperate with the 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 pre-agreed terms and conditions 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 **Option 1** as depicted in **Figure 2**, and take exclusive custody of the respective funds/tokens to enforce a settlement. This option allows the Cryptocurrency Exchange to function as a regular custodial escrow between trading parties as is the case with most exchanges.

In another instance, if the Cryptocurrency Exchange suffers a security breach and its private-keys are compromised/stolen, it can use **Option 3** of the Provisional Transaction as depicted in **Figure 2** to cosign a recovery transaction with the First Party and transfer the funds/tokens to another secure address or back to the First Party.

Figure 4



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

Note: Lost Private Keys are assumed stolen.

Hackers need to collaborate to steal the funds

* Slim chances of recovery

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 the First Party but not the Second Party.

Since the Second Party is an organized entity that can employ data-safety measures such as multi-vault diversified backups, 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 that are deemed necessary or unnecessary. Also, the timelocks mentioned in the Provisional Transaction are one of the many possible combinations 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 the first claim on the respective funds/tokens as it is accepting liability on the First Party's behalf and can steal the 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. There is no scope for plausible deniability too as failure to initiate recovery and corrective measures confirms maleficence. Hence, the incentive and motive to cheat the First Party of its funds/tokens by the Second Party is non-existent. But if the 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.