Figure 1

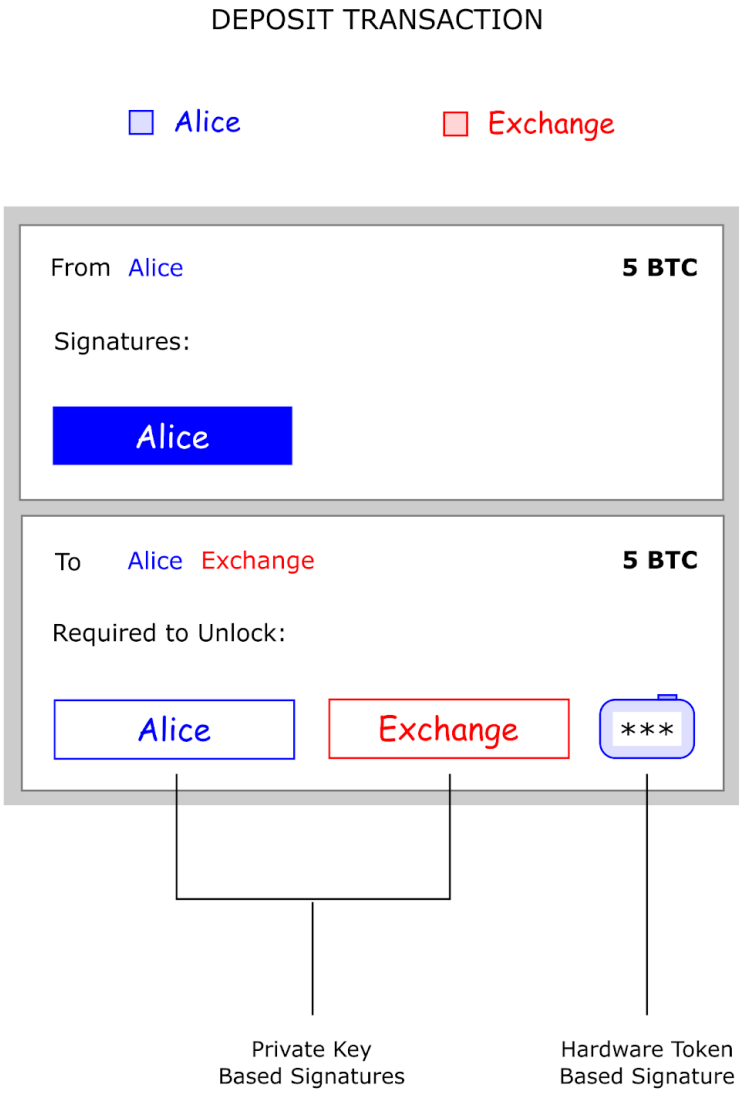

DEPOSIT TRANSACTION
Alice
Exchange
From Alice
5 BTC
Signatures:
Alice
To Alice Exchange
5 BTC
Required to Unlock:
Alice
Exchange
***
Private Key
Based Signatures
Hardware Token
Based Signature

Figure 2

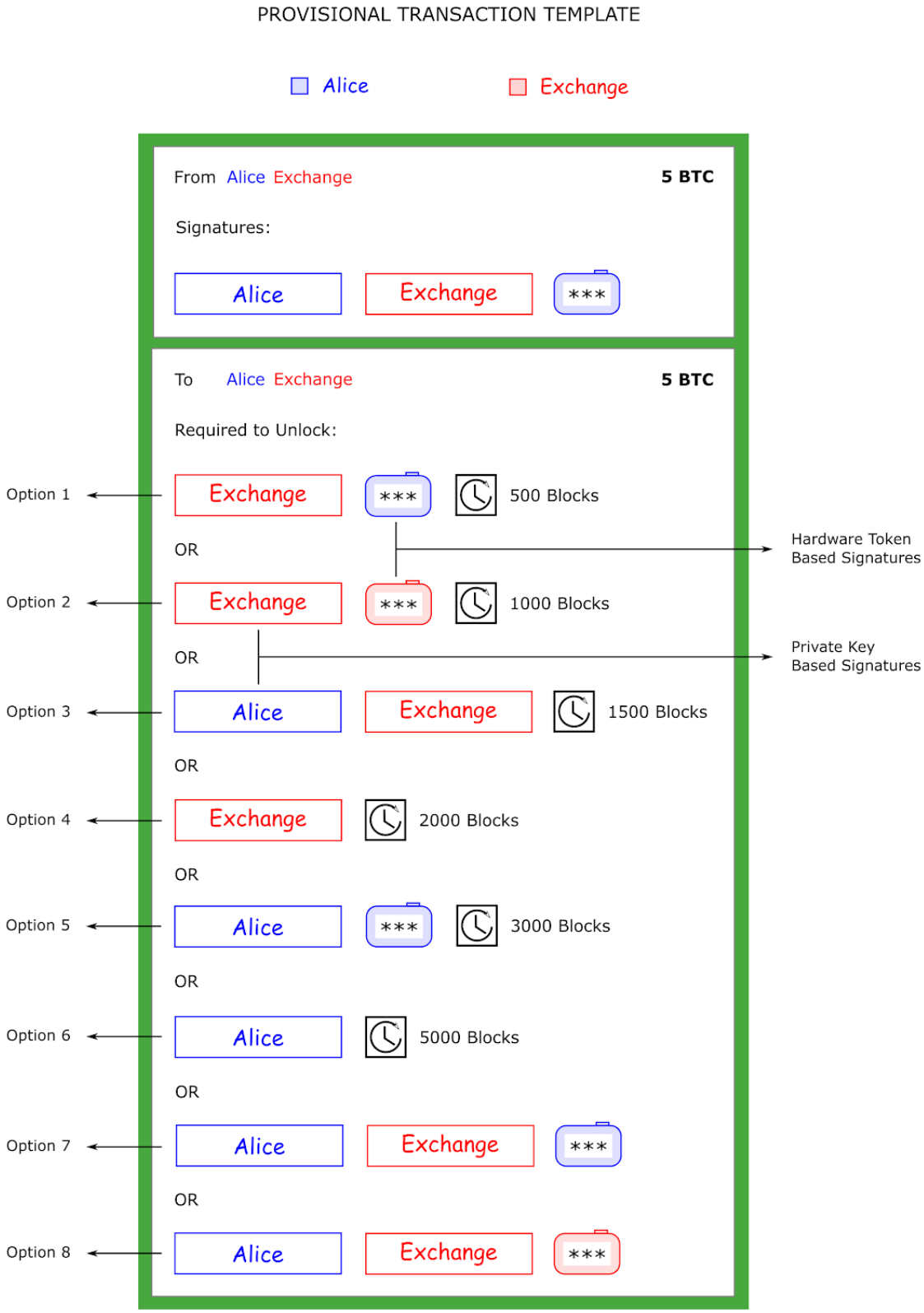

PROVISIONAL TRANSACTION TEMPLATE
Alice
Exchange
From Alice Exchange
5 BTC
Signatures:
Alice
Exchange
***
To Alice Exchange
5 BTC
Required to Unlock:
Option 1
Exchange
***
500 Blocks
OR
Hardware Token Based Signatures
Option 2
Exchange
***
1000 Blocks
OR
Private Key Based Signatures
Option 3
Alice
Exchange
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

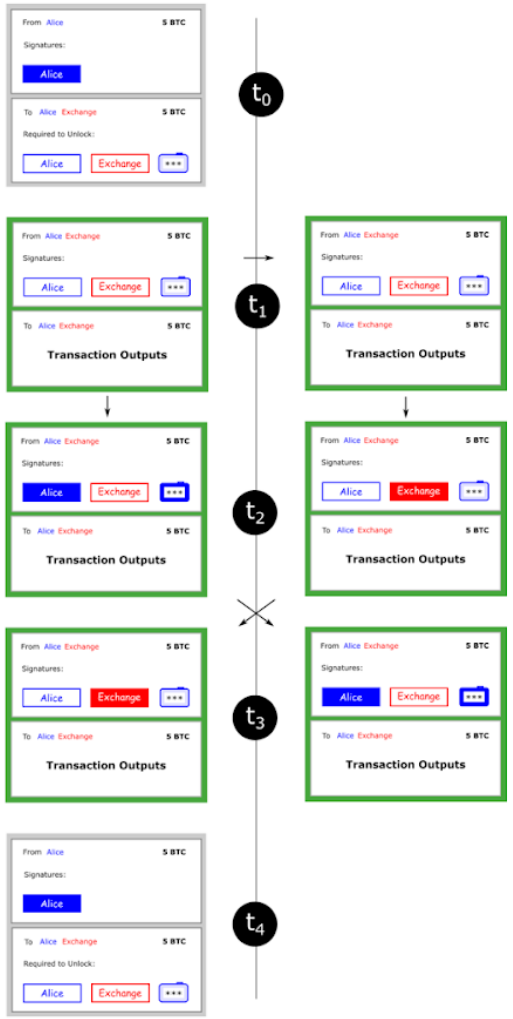
Alice adds **Signatures** generated using her Private Key and Hardware Token* to the Provisional Transaction and transmits it to Exchange

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

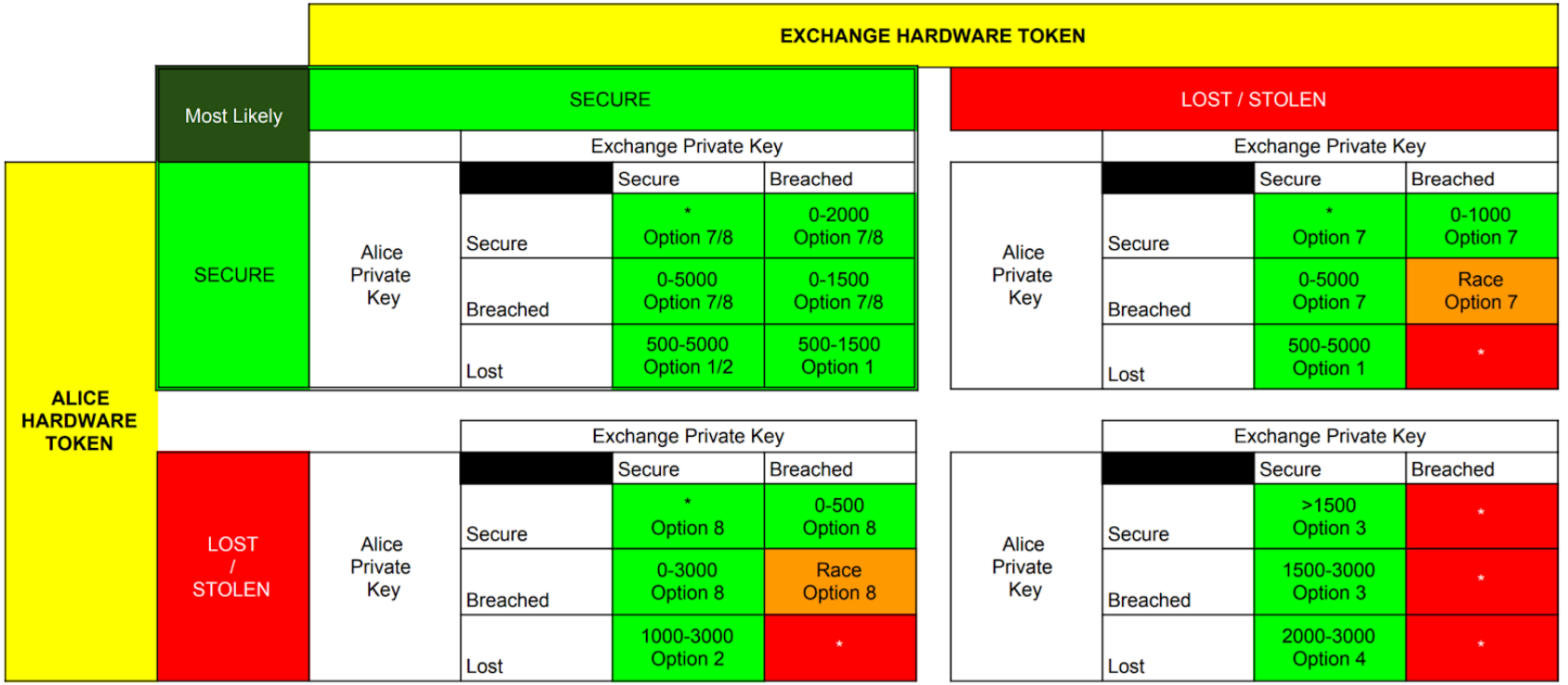
Exchange receives **Partially Signed Provisional Transaction** from Alice

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.

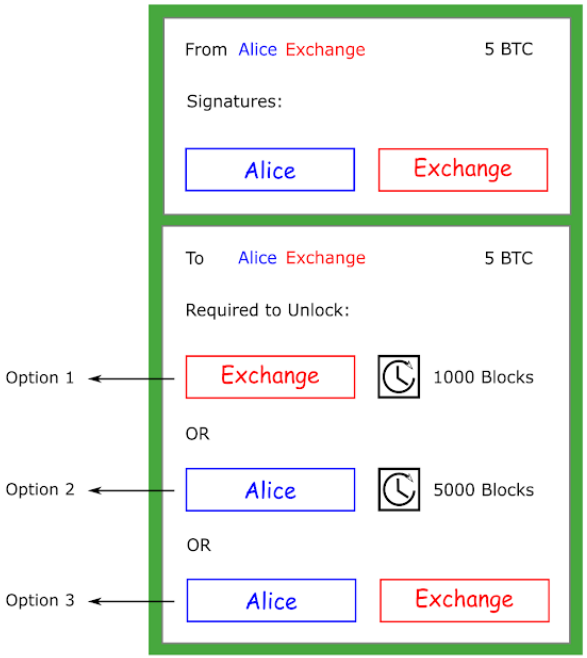
Note: Options as depicted in **Provisional Transaction Template** in **Figure 2**.

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.