Vardiz OTC Storage Setup Service Documentation

Last Updated October 2018

VARDIZ

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

1. Introduction

This document aims to supplement clients of Vardiz OTCs Storage Setup Service on proper procedures to setup, deposit, withdraw, recover, maintain and troubleshoot issues related to their Bitcoin assets.

While the gamut of available options are limitless, the tiers of implementation that we recommend have been carefully selected as a suitable compromise between security and convenience.

The procedures within this document are specific to the particular combination of hardware and software offered by Vardiz OTC, and it is imperative that they are followed with diligence. We make no guarantees on the applicability of this document should users deviate from steps herein.

Many of the concepts have been simplified to what we deemed sufficient for layman understanding, however they do require a modicum of proficiency in computer operations. The more esoteric terms are *italicized*, and summarized in a glossary. We also used colour-codes for notable items as follows:-

- **Red** - Denotes critically sensitive data; knowledge of which can be used to steal your funds. Great care must be taken to ensure such data remains secret. In particular you must never paste or type it into any computer or smartphone, take pictures of it, or share it with untrusted parties.
- **Gold** - Denotes moderately sensitive data; knowledge of which cannot be used to steal your funds, however can be used to know how many Bitcoins you own, the transactions you send and receive, and your counterparties. Adherence to the prescribed discipline should help you keep an acceptable level of privacy.

Vardiz OTC Storage Setup Service uses commercially or freely available hardware and software, and we monitor vendor updates to the components we use. Vendor-specific procedures are provided via hyperlinks, as steps may change between versions of this document.

Please keep eye out for the latest version of this document, available for download from our website.

1.1. Addresses & Keys

Your current Bitcoin balance is not stored within your device, they exist instead within *addresses* on the Bitcoin blockchain.

Think of *addresses* as a public locked box with all your Bitcoins in it. Anyone can see the box, but only you have the key (called a *private key*) to spend its contents.

1.2. Wallets, Trezor hardware & CryptoSteel

Wallets are what we use to interface with the Bitcoin network. There are many kinds, but they are interoperable as long as they adhere to specifications. The wallets we recommend differ based on different tiers of implementation.

Multi-signature wallets are similar to joint bank accounts. They are suitable for use by legal entities who not only require protection from compromised personnel, but also require an added level of redundancy in case of key loss.

Trezor hardware is a device that complements wallets we by serving as secure storage of your *private keys*. Using such a device prevents theft in case of computer viruses or hacking.

CryptoSteel is a metal widget to store the *mnemonic seeds* used to back up your Trezor hardware. Typically mnemonic seeds are stored on paper, but such an arrangement does not protect against fire or floods.

The combination of wallets, Trezor Hardware & CryptoSteel offered in our implementation tiers are as follows:-

Tier	Wallet	Trezor hardware	CryptoSteel
Tier 1	Trezor wallet	Used	-
Tier 2	Trezor wallet	Used	Used
Tier 3	3 Electrum multi-signature wallets	3 devices, one for each Electrum multi-signature wallet	3 widgets, one for each Trezor hardware

1.3. Transactions

Only a valid *transaction* may be *broadcasted* by your wallet to the Bitcoin network. Validity includes having sufficient balance, sending to correct cryptocurrency address, and signed by all required private keys. You can enter any transaction into a block explorer to see its status.

A *transaction fee* is a component of your transaction used to entice miners to confirm it. The fee is a free market, and estimates are obtainable from your wallet itself, or through online tools such as Bitcoinfees. Transactions with fees that are too low will take time to confirm.

A valid transaction that is just broadcasted will have 0 confirmations, sufficient for petty purchases. After it is included

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

in a block by a miner, the transaction will have 1 confirmation. The more blocks that get appended to the blockchain afterwards, the more confirmations that transaction will have.

Confirmations can be monitored using wallets or *Block explorers*; 6 is widely accepted as good enough for even the highest value transactions.

1.4. Fund segregation

The implementation we recommend are meant for funds held in storage, where the focus will be on security and privacy as opposed to user experience. The procedures associated with such funds are correspondingly more involved.

For petty funds, these procedures are overkill. They may be kept in more user-friendly app wallets such as Samourai (for Android) or BRD (for IOS) and topped up from time to time. Note that usage procedures for app wallets are outside the scope of this document.

2. Procedures (Tier 1 & Tier 2)

These implementation tiers are for individual users who are not expecting to co-manage their Bitcoin assets with other people. Security and redundancy will be reliant on having trusted heirs.

2.1. Setup procedures

Setup procedures will be carried out by Vardiz OTC personnel on your premises. Our steps are included here should you need to replicate the procedures yourself.

2.1.1. Choose computers that are only accessible by you and kept in a secure location; like your office.

2.1.2. Your computers communicate with your Trezor hardware via a software tool called a Trezor bridge, downloadable here.

2.1.3. Your Trezor hardware needs to be initialized prior to first use. Connect it to your computer and follow instructions here.

2.1.4. Backup your Trezor hardware by following instructions here. Remember to write down the **mnemonic seeds** clearly on paper, and in the right sequence.

2.1.5. Name your Trezor hardware by following instructions here, and physically label the device name using a sticker.

2.1.6. For Tier 2 clients only: Transfer the first 4 characters of each **mnemonic seed** onto your CryptoSteel in sequence. You will need small screwdriver to use the widget as shown here. Physically label the widget with the name of your Trezor hardware using stickers.

2.1.7. Setup a PIN for your Trezor hardware by following instructions here.

2.1.8. Check the accuracy of your **mnemonic seeds** by following instructions here.

2.1.9. Fore Tier 2 clients only: Once your **mnemonic seeds** are confirmed accurate, seal your CryptoSteel using a zip-tie and destroy any paper based copies of the **mnemonic seed**. Store your CryptoSteel in a safe location off-site.

2.1.10. The Trezor wallet is browser-based, but the vendor have no access to your data. All identifying information is kept within your Trezor hardware, so keep it out of sight when not in use.

2.2. Deposit procedures

To deposit funds into your Trezor wallet, follow instructions here. The ***address*** (or its ***QR code***) may be shared in an email, printed or simply shown to your counterparty. It is good discipline to use new addresses each time a deposit is made.

2.3. Withdrawal procedures

To transfer funds from your Trezor wallet, follow instructions here. A good discipline is to only transfer funds from your storage wallet to periodically top up your petty funds wallet, and using your petty funds wallet for all 3rd party transactions.

2.4. Recovery procedures

Typical recovery scenarios are as follows:-

2.4.1. **Your main computer is compromised / lost**: Use a new computer and install the Trezor bridge tool. Since the Trezor wallet is browser-based, nothing is actually stored within the computers.

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

2.4.2. **You forgot your PIN**: Plug in your Trezor hardware, wipe the device following instructions here, and follow recovery procedures using your **mnemonic seeds** based on instructions here.

2.4.3. **Your Trezor hardware is compromised / lost**: Purchase a new Trezor hardware and follow recovery procedures using your **mnemonic seeds** based on instructions here.

2.4.4. **Your mnemonic seeds are compromised / lost:** Immediately initiate withdrawal procedures to a temporary wallet. Wipe your Trezor hardware following instructions here, re-initiate setup procedures and deposit funds into the new wallet.

2.4.5. **Both your main computer & Trezor hardware are compromised / lost:** Use a new computer and install Trezor bridge. Purchase a new Trezor hardware and follow recovery procedures using your **mnemonic seeds** based on instructions here.

2.4.6. **Both your Trezor hardware & mnemonic seeds are compromised / lost:** This is the worst case scenario. Your funds are lost.

2.5. Estate planning procedures

Only the **mnemonic seeds** are pertinent for estate planning.

2.5.1. Leave instructions within a sealed envelope containing the location of your **mnemonic seeds.** Include information on the **exact type and rough quantum of your assets**: E.g. contains ~ 1 BTC worth of Bitcoin.

2.5.2. Instruct your heirs to initiate recovery procedures as per Section 2.4.5.

2.6. Maintenance procedures

It is recommended that maintenance procedures are performed annually.

2.6.1. For Tier 2 clients only: Ensure the zip-tie of your CryptoSteel is intact. If it is not, follow instructions in Section 2.4.4. Always ensure to re-seal your Cryptosteel with a new zip-tie before storage.

2.6.2. Re-check the accuracy of your mnemonic seeds following instructions in Section 2.1.8. If it doesn't match, follow instructions in Section 2.4.4.

2.6.3. Ensure information in Section 2.5.1 is up to date.

3. Procedures (Tier 3)

This implementation tier is meant for legal entities who are required to co-manage their Bitcoin assets not only with internal staff, but also with 3rd-party service providers. Security and redundancy will be reliant on having a robust process.

Ideally, legal entities who are interested to hold Bitcoin must have a member of staff that is sufficiently competent about Bitcoin to keep abreast with latest developments. Our procedures are a good foundation, however there are many applications to explore for those who are willing to experiment.

Core to this implementation will be 2-of-3 multi-signature Electrum wallets, combined with Trezor hardware and CryptoSteel for **mnemonic seed** storage. Two signers will be needed for every outgoing transaction, however any number of people may be granted **watch-only access** to the wallets.

As an example, we shall use the fictional legal entity "SPV Sdn Bhd" whose CEO and CFO have been authorized by the BOD to access company funds.

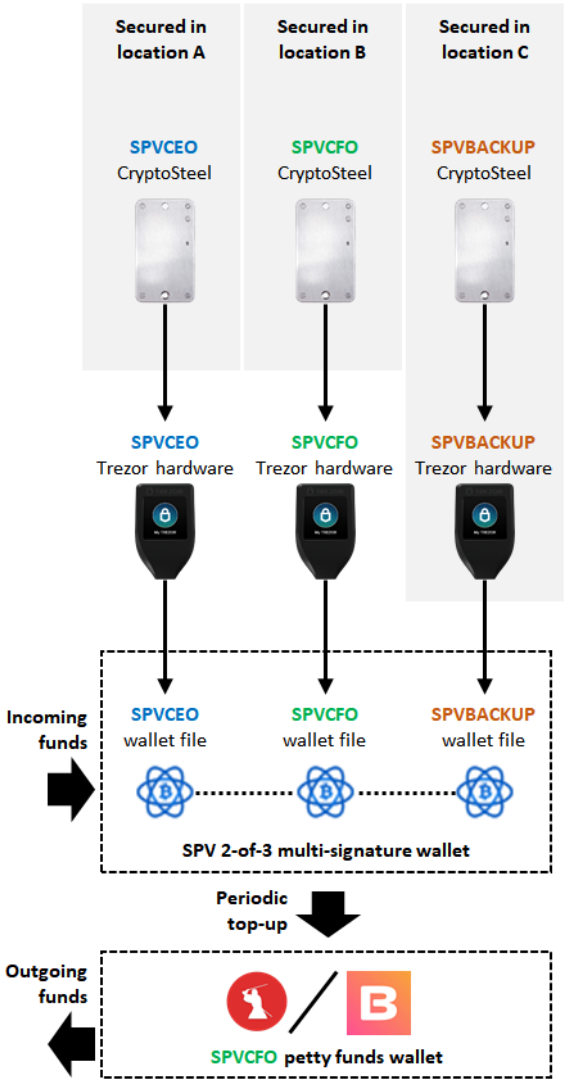
Fund segregation is particularly important for multi-signature wallets; as withdrawal procedures are more tedious. In most cases, the only counterparty for the multi-signature wallet will be the petty funds wallet controlled by the CFO.

A general outline of our Tier 3 implementation are as follows:-

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

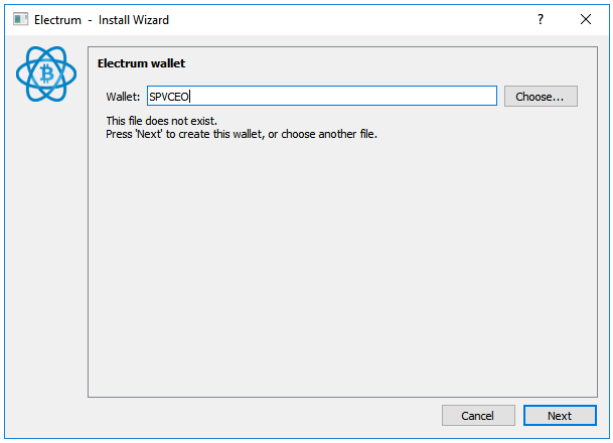


3.1. Setup procedures

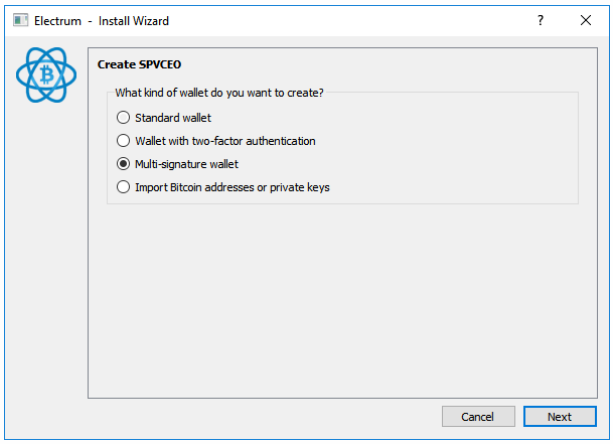
Setup procedures will be carried out by Vardiz OTC personnel on your premises. Our steps are included should you need to replicate the procedures yourself.

3.1.1. The first few steps of our Tier 3 implementation is to create “dummy” Trezor wallets. Steps are identical to our Tier 2 implementation from Section 2.1.1 until Section 2.1.10. While the resulting wallets are entirely usable, they may be disregarded. Follow all the steps separately for SPVCEO, SPVCFO & SPVBACKUP.

3.1.2. Download the Electrum wallet onto the CEOs computer from here. Open Electrum and create a new wallet with the name “SPVCEO”:-



3.1.3. Choose “Multi-signature-Wallet”:-

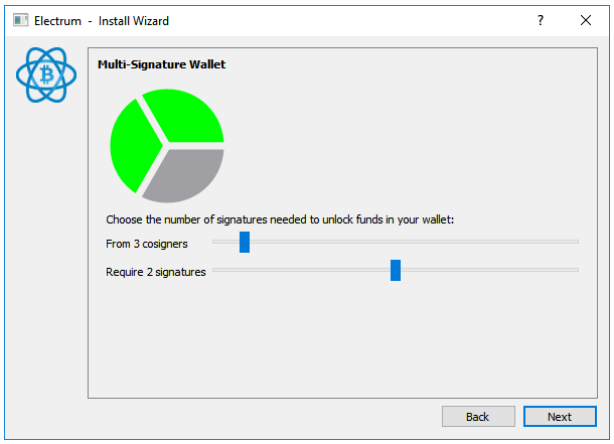


1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

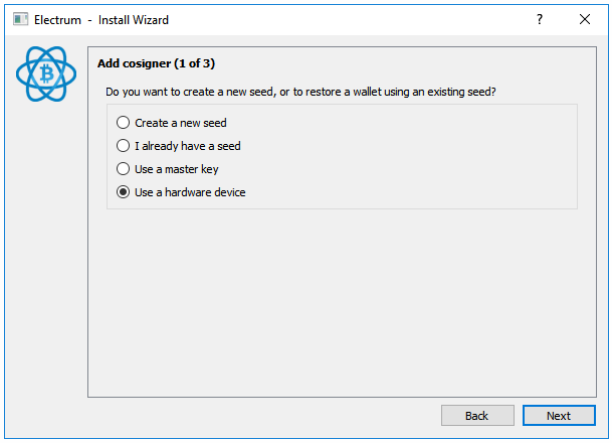
enquiries@vardiz.com
vardiz.com

VARDIZ

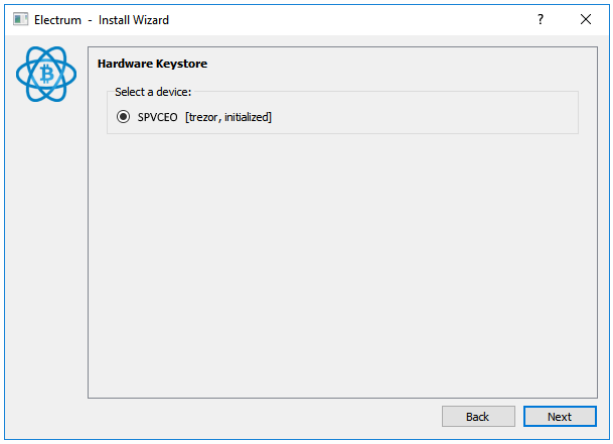
3.1.4. Choose “From 3 cosigners, require 2 signatures”:-



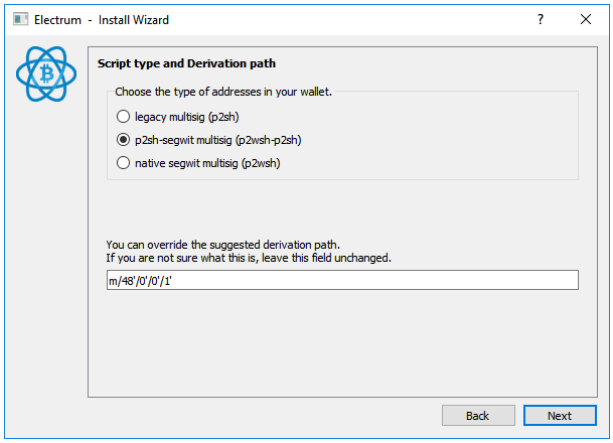
3.1.5. Connect the Trezor hardware and Choose “Use a hardware device”:-



3.1.6. Select the Trezor hardware:-



3.1.7. Choose “p2sh-segwit multisig”:-

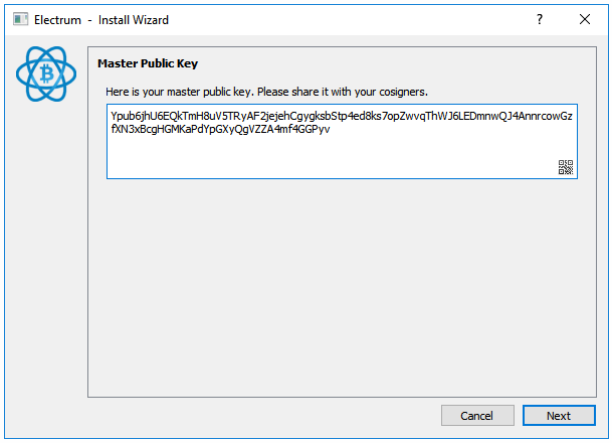


3.1.8. The following is the **Master Public key** (also called ***XPUB***) for SPVCEO. Copy this information into a text file and share with SPVCFO and SPVBACKUP.

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

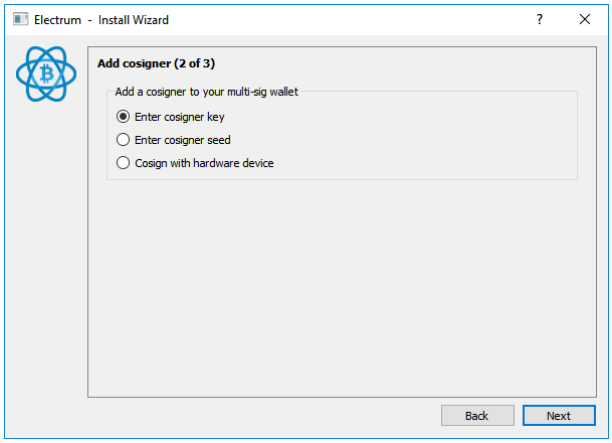
enquiries@vardiz.com
vardiz.com

VARDIZ

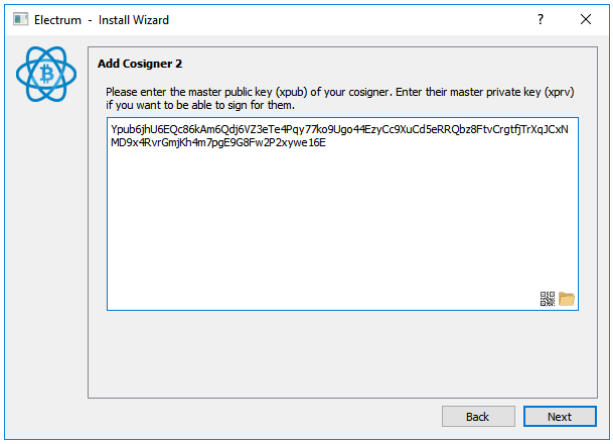


3.1.9. Repeat steps from Section 3.1.2 to Section 3.1.8 for SPVCFO & SPVBACKUP.

3.1.10. Chose “Enter cosigner key”:-



3.1.11. Enter the ***XPUB*** for SPVCFO or SPVBACKUP:-

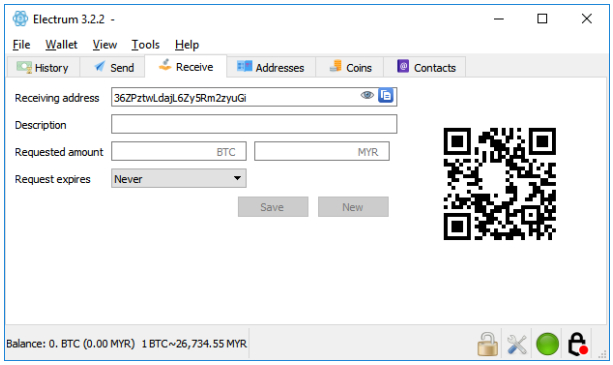


3.1.12. Enter the ***XPUB*** for the remaining cosigner.

3.1.13. A wallet file called SPVCEO is now created. This can be found at the %APPDATA%\Electrum\wallets directory. Copy each version of this file (SPVCEO / SPVCFO / SPVBACKUP) and save in the folder within the other computers so that all three computers have access to all three files.

3.2. Deposit procedures

To deposit funds into your multi-signature wallet, follow instructions in this tab:-



The ***address*** (or its ***QR code***) may be shared in an email, printed or simply shown to your counterparty. It is good practice to use new addresses each time a deposit is made.

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

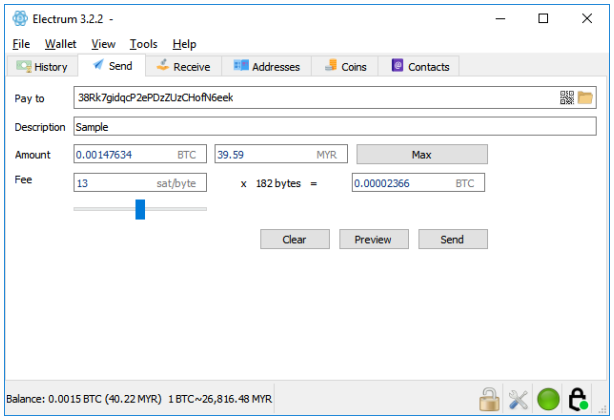
enquiries@vardiz.com
vardiz.com

VARDIZ

3.3. Withdrawal procedures

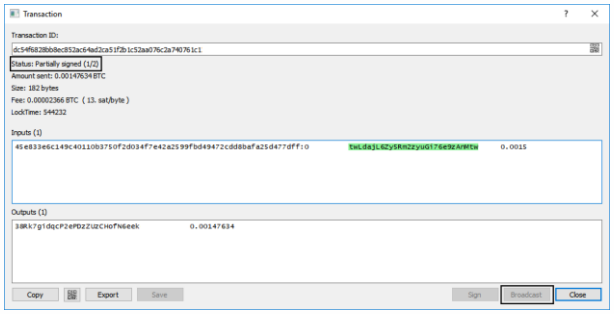
3.3.1. To transfer funds from your multi-signature wallet into your petty funds wallet, you will need first need the latter's **address**.

3.3.2. At SPVCEO, insert or scan the address in this tab:-

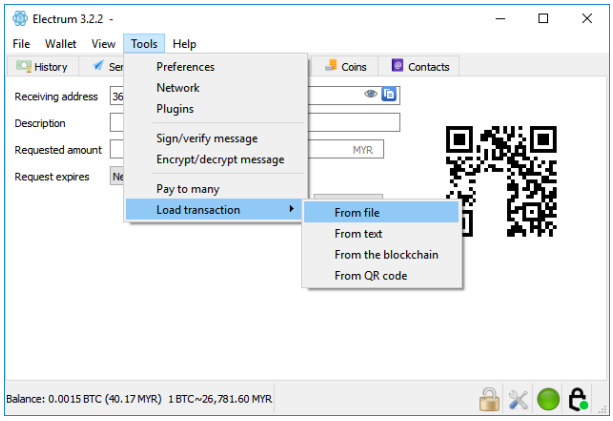


3.3.3. Ensure the SPVCEO Trezor hardware is connected, set the description, amount & fee, click send, and confirm on the Trezor hardware.

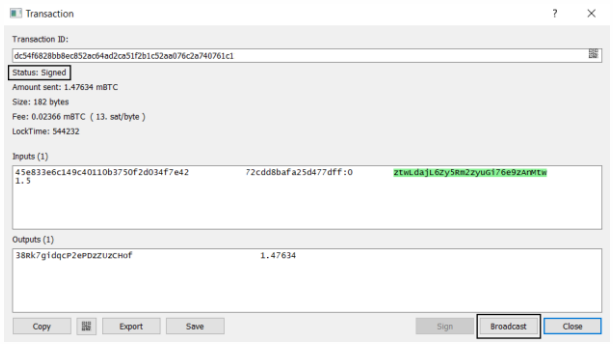
3.3.4. Note that the transaction status denotes "*partially-signed*" and it may not be broadcasted. Click on Export, save the **partially-signed transaction** file, and share it with SPVCFO.



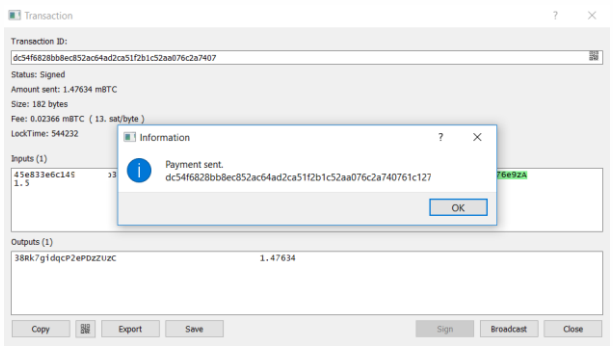
3.3.5. At SPVCFO, load the transactions, click send and confirm on the Trezor hardware.



3.3.6. The transaction may now be broadcasted for confirmation by the Bitcoin Network:-



3.3.7. You may share the corresponding transaction ID with your counterparties for their reference:-



3.3.8. Electrum works on the basis of wallet files and not on computers. This means if you open 2 separate instances of Electrum with 2 (out of 3) of the required wallets, the whole withdrawal process can be completed within one computer, as long as 2 (out of 3) of the Trezor hardware is present for

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

signing. This is convenient, however a physical security compromise, as a bad actor on-site is may steal funds.

3.4. Recovery procedures

Recovery scenarios for our Tier 3 implementation is similar to those from Section 2.4.1 to Section 2.4.5. However, the multi-signature arrangement provides plenty of additional redundancies.

Worst case scenario will only arise if 2 (out of 3) Trezor hardware **AND** 2 (out of 3) CryptoSteels are compromised or lost at the **SAME TIME**. As long as you keep this in mind, most other scenarios are recoverable.

3.5. Succession planning procedures

Unlike individuals, legal entities must be cognizant of the impact of staff turnover on security arrangements. Access to company Bitcoin assets must be treated with the same severity as bank accounts, with mandates approved by the BOD.

3.5.1. Mandate should be attached to positions as opposed to individuals. Upon handover, only the Trezor hardware needs to be inherited, however its associated **PIN** must be changed.

3.5.2. It is recommended to keep **mnemonic seeds** in separate bank safe deposit boxes, with access restricted to BOD members.

3.5.3. If the BOD suspects rogue staff may have access to **critical** or **moderately sensitive data**, the BOD may migrate entire company funds into a temporary wallet, wipe all existing devices and widgets, and setup a fresh arrangement.

3.6. Maintenance procedures

It is recommended that maintenance procedures are performed annually with all BOD members present.

3.6.1. Ensure the zip-tie of your CryptoSteels are intact. If it is not, follow instructions in Section 2.4.4. Always ensure to re-seal your CryptoSteels with a new zip-ties before storage.

3.6.2. Re-check the accuracy of **mnemonic seeds** following instructions in Section 2.1.8. If it doesn't match, follow instructions in Section 2.4.4.

4. Glossary

Addresses

A modified version of a public key, this is what you share with people to receive Bitcoin. A wallet can manage many addresses, and it is good practice to use a fresh one each time. Looks like this:-

37RX7nozdfQEA57APExZKLBR8q9xjYw7TL

Or in QR code form:-

Block explorers

Online services which continually parse and report on the Bitcoin blockchain. Used to check balances and monitor the confirmation of transactions. Examples include **Blockchain** & **Blockcypher**.

CryptoSteel

A metal widget used to store mnemonic seeds in a way that's flood-proof and fire-proof. Important for our Tier-2 and Tier-3 implementations.

Mnemonic seed

A set of 12 to 24 words that can be used to generate a Root Seed by any BIP39 compliant wallet. The sequence matters, but cases do not. Looks like this:-

1	struggle	7	funny
2	oxygen	8	rare
3	blood	9	enact
4	public	10	govern
5	cross	11	describe
6	forest	12	frozen

In all our implementations, mnemonic seeds are used to recover your Trezor hardware.

1278728-P
Vardiz Commerce Sdn Bhd
Level 3 Lot 74 Jalan Mamanda 1
Ampang Point 68000 Ampang
Selangor Malaysia

enquiries@vardiz.com
vardiz.com

VARDIZ

Multi-signature wallet	A special type of wallet whose addresses require multiple signers before transactions become valid for broadcasting. Used in our Tier-3 implementation via Electrum.
QR code	A method to convert between a string of characters and a graphic scanable by a camera. Prevents copy errors.
Public key	A string of characters used to generate an address that can be signed using a private key. Each public key-private key pair is unique. Looks like this:- 02a1633cafcc01ebfb6d78e39f687a1f0995c62fc95f51ead10a02ee0be551b5dc The associated complexities are handled by your wallet.
Private key	A string of characters used to sign outgoing transactions from an address. Addresses used in multi-signature wallets require multiple private keys to sign. Looks like this:- b221d9dbb083a7f33428d7c2a3c3198ae925614d70210e28716ccaa7cd4ddb79 The associated complexities are handled by your wallet.
Partially-signed transactions	Pertinent to multi-signature wallets. These are transactions which have not yet been signed by all required signers, hence may not be broadcasted. Needs to be shared manually for signing, and maybe broadcasted after all required signatures obtained.
PIN	A set of numbers used to unlock your Trezor Hardware. If you forget your PIN, you will need to initiate the appropriate recovery procedures
Transactions	What broadcasted by your wallet to the Bitcoin network when you spend Bitcoin. Looks like this:- cf160e073e930333481ffe2575c9c42ef811c816c1195e46c4bc1daa02d987b8
Wallet	Various software implementation that users use to interface with the Bitcoin network. Examples include:- **Bitcoin Core** - The reference implementation of Bitcoin meant for sophisticated users. Most wallets are modified, user-friendly versions of Bitcoin Core. **Electrum** - Desktop-based client used in our Tier-3 implementation for storage funds. **Trezor wallet** - Browser-based client used in our Tier-1 & Tier-2 implementations for storage funds. **Samourai** - Android-based client recommended for petty funds. **BRD** - IOS-based client recommended for petty funds.
Trezor hardware	A device used to store private keys and sign transactions securely. Pertinent to all our implementations. Comes in two variants:- **Model One** - No touch screen, meaning PINs and seeds entered through the computer. **Model T** - Touch screen, meaning PINs and seeds entered through the device.
XPUB	Extended public keys pertinent to our Tier 3 implementation. Used to ensure multiple signers in different computers refer to the same multi-signature wallet.

5. Resources

5.1. Trezor wiki: https://wiki.trezor.io/

5.2. Electrum documentation: http://docs.electrum.org/en/latest/

5.3. Bitcoin BIP depository: https://github.com/bitcoin/bips/blob/master/README.mediawiki