

Instructions for TripleShibe

CONTENTS

Introduction

Creating a One Party TripleShibe Account

Creating a Three Party TripleShibe Account

Spending from a TripleShibe Multisig Account

APPENDIX A - Create a Dogecoin Address (public & private keys)

APPENDIX B - Disclaimer

INTRODUCTION

This document is intended to be a practical introduction for learning how to use the TripleShibe freeware from [dogecoinmultisig.org](https://github.com/tomcarbon/dogecoinmultisig.org), available at <https://github.com/tomcarbon/dogecoinmultisig>. The user will learn how to create Dogecoin Addresses, the TripleShibe account from those new addresses, and then how to spend from the resultant multisigs.

The reader will learn about the following two Basic Types of TripleShibe configurations:

a) **The one party account:** This is a where one person (or group) owns all three keys.

Typical use cases include **Personal** and **Business**.

b) **The three party account:** This is where the three keys are distributed between three people (or groups). Typical use case might include **Charity** functions where multiple persons holding the funds is more appropriate than a single person holding the funds.

After learning to create a Triple Shibe account to their desired level of security, **the reader will next learn how to spend from any of the addresses from the related TripleShibe funds.**

In the Appendixes A and B, more stuff.

This is a living document. Find the latest copy at github.com/tomcarbon.

Creating a One Party TripleShibe Account

You must have three public keys. To acquire three public keys, one must create a new Dogecoin Address, three times. To learn how to create a new Dogecoin address, see *Appendix A* of this document.

Public keys are created along with the creation of a Private Key for a new Dogecoin Address. Place your new public keys into the three available places on the TripleShibe screen:



TripleShibe Dogecoin 2/3 Multisig

[Click Here for Instructions!](#)

Place three Public Keys into the boxes below and click Next

Three empty text input boxes for entering public keys.

Sort PubKeys Alphabetically?

Next

They are automatically arranged into alphabetical order (default). (advanced: public keys can be arranged into another order if desired - this will create a different set of multisig addresses)

For extra security, create the addresses on an offline computer. Store the information for your three private keys onto encrypted memory sticks and/or hard copies.

For even more security, you could store each of the private keys in different physical locations.

You are now ready to use your new Dogecoin Multisig Addresses.

Creating a Three Party TripleShibe Account

The reader must have access to three public keys to create a TS account. Typically, for a 3 party account, the public keys are provided from three independent people or parties.

Each party controls one Private Key, and then provides the corresponding Public Key to her/his other two colleagues.

Place the three public keys into the TripleShibe and click Next:



TripleShibe Dogecoin 2/3 Multisig

[Click Here for Instructions!](#)

Place three Public Keys into the boxes below and click Next

Sort PubKeys Alphabetically?

Next

The link from the resultant TripleShibe Account can then be copied and shared between the members and folks outside the group(s) as deemed appropriate.

(To acquire a public key, one must create a new Dogecoin Address (when you do, save the Private Key). To learn how to create a new Dogecoin address, see *Appendix A* of this document)

For extra security, create the address on an offline computer. Store the information for your Address/public/private key onto encrypted memory sticks and/or hard copies.

You are now ready to use your new Dogecoin Multisig Addresses.

Spending from a 1/3 Multisig Account

1) Press the 'Spend' button of the account that you would like to spend from:



TripleShibe Dogecoin 2/3 Multisig

[Click Here for Instructions!](#)

Address:



Confirmed Balance: 12315.1995202

Shareable URL for this page

<http://dogecoinmultisig.org/multisigmain/?tripleshibe=04a>

Spend

Pay Spot

Verify

Reddit

more

2) You will be brought to the following screen. Enter the **DESTINATION ADDRESS** and the **AMOUNT** that you want to pay.

Spend Pay Spot Verify Reddit

more

To Address:

Amount:

(the mining fee will be added on top of this amount, unless full amount, then it's subtracted)

Next

3) Click Next.

4) You will be brought to the following “WITHDRAW” screen.



WITHDRAW (redeem) from your Multisig (or your regular Dogecoin Address)

[Reset Everything and Start Over](#)

Address to pay from:

A2kRGaYUC9FXnuZPGpAXyXKTU9fxicwBLM

Confirmed Balance: 98.01

Destination Address to pay to:

9zByhQgSg3Xsz9MqDGsMGJNrdshys9BCjQ

Amount:

50

(the mining fee will be added on top of all this, unless full amount, then it's subtracted!)

Your Private Suite Key or One Private Signature (or check the box so you can sign offline):

Show

Do not sign the transaction (for offline use)

Warning: if this is a large transaction you're gonna have to copy/paste instead of using the buttons. It's still fully functional this way, just the buttons will fail because there's about a 3K limit to transaction size supported by html.

Put your Private Key, or your Private Suite Key (which is just two Private Keys appended together), into the indicated area, and click Next

Your Private Suite Key or One Private Signature (or check the box so you can sign offline):

.....

Show

Do not sign the transaction (for offline use)

Successful Sign

The dogecoin transaction below has been signed one time.

```
0100000014bece443d0aaebd9ff26cdadb7f87f917a1903e317d366b90a1cc91b66a8177d0000000900048304:
c9189449714a97c8d3102204f0ab55083f1b7926f289b1969f112ebc155607995b9e0e2ad2eabb4aeaede470145:
050326b2441c1364d0de4cbdd4c289996311eeb31924c0be32c2a46026d96960cf19bede3c852a493ce51aefffff
5a862f48e35b6870084d717000000017a914711fedff0960e6d71e9af3e75306057612f000838700000000
```

BROADCAST (online) MAKE VERIFY URL

If one signature is required for this multisig, the next step will be 'broadcast'. Press the **broadcast** button to transmit the transaction onto the Dogecoin network. You will receive a success message (or an error message).

Your Private Suite Key or One Private Signature (or check the box so you can sign offline):

.....

Show

Do not sign the transaction (for offline use)

Another Successful Sign!

The dogecoin transaction below has been signed twice.

If this is a 3/3 Lockdown Multisig you'll need to sign it again

Otherwise, click the BROADCAST button to send the transaction to the dogecoin network.

```
0100000013a1895385a2db25053249efbd1599bc83db9e7e4a211c2e3061ef0559c502db70000000fd5e010
58d99faf96b76cd6bc3c1b7e72502201d63f7f935cd30372152fe3157e87524be3d525f3be9a9b4b5e5d3b52feb
3ce3cd5c27f20a872fe87e2be7ffb24902203c7eb21bc11b8c8ef1e23177d959b6cdf4159103f98332732ec72cdf
2aa978327e0df050326b2441c1364d0de4cbdd4c289996311eeb31924c0be32c2a46026d96960cf19bede3c85
e8696ae80fd42a4d2dd735258889919738a5179fdf50c69135b4224f30711b8fe359c761672c456c39ee295a41
a497aae1e4f03942227b3c1028ca7f416529eb35ca9ed1241c04dad37f347179ac3cfa193ac6153aeffffff02002
98e8178b08700a90dae0400000017a9147ea5708d1555ae5d3c0986e214aeb8ecfd7067338700000000
```

BROADCAST (online) MAKE SIGN URL (or sign again)

If two signatures are required, you will need to sign the transaction again before the Broadcast step. Follow the instructions as indicated on the buttons (again, if this transaction is larger than about 3K, you'll need to copy/paste from the verify->sign_transaction buttons, this is a limitation of the POST functionality).

If three signatures are required, you'll need to add the third sign step.

If you wish to generate a transaction (sort of like an invoice), but not sign it, check the box. You can then copy the resulting transaction data onto a memory stick (in a .txt file), or an email, facebook IM, and/or sign it offline, etc.

APPENDIX A - How to Create a New Dogecoin Address

- a) From dogecoinmultisig.org/multisigmain, go to **New->New Dogecoin Address**.
- b) You will be brought to the following screen:



New Dogecoin Address create a new address

Any keys used you will need to manually store safely as they will be needed later to redeem the Dogecoins.

Address (Share)

Public key (Share)

Private key (WIF key)

Show

Add random information here:

Make New Address (offline is OK)

- c) The “Add random information here” box is optional. Any information in this box will be ADDED to the entropy used in the original randomizing algorithm. As one can press the ‘Make New Address’ button multiple times on this screen, the reader can press this one time to obtain some nice randomized data which can then be arbitrarily copy/pasted into the random information box.
- d) Press the button that says “Make New Address (offline is OK)”. Your new Dogecoin Address will be generated.
- e) Save the three pieces of information (Address, Public Key, Private Key).

You are now ready to use your new Dogecoin Address.

APPENDIX B - DISCLAIMER

Dogecoin is a joke and the economic infrastructure is a joke and dogecoinmultisig.org and this document are also a joke too Hahaha! And with its oddball predictable inflationary model! Haaha!

So what if the the joke is perfectly functional, and we can understand what dogecoin will probably be doing in the year 2069. The inflationary economic model is understandable. And it's good for internet tipping and also for charity things too. That it retains its value over time, apparently. That the dogeconomy is really there, that it is gaining mass.

Have fun with it. Do Good Things. Hold not the developers nor community responsible for this SILLY 'toy' currency that is nevertheless operational worldwide 24/7. Which happens to be really fast, and quite inexpensive to send. And is not a commodity because of its nearly 5% rate of inflation. And is helping people with its charitable endeavors.

IT'S A DOG ON A COIN. Of course, it's a joke. Tee hee hee. <jaws music>

reddit.com/r/dogecoin

wow