Securing a Bitcoin seed phrase in stainless-steel washers (abridged).

An article on securing a 24-word seed phrase backup with a 3D printed Blockmit jig and stress testing the backup.

This is the abridged version of my more detailed article which covers generating a 24-word seed phrase on a verified ColdCard. If you want the

more detailed article, it can be found here. This version only covers the stamping of the seed phrase into the washers and stress testing the backup. It is assumed you already have your seed phrase.

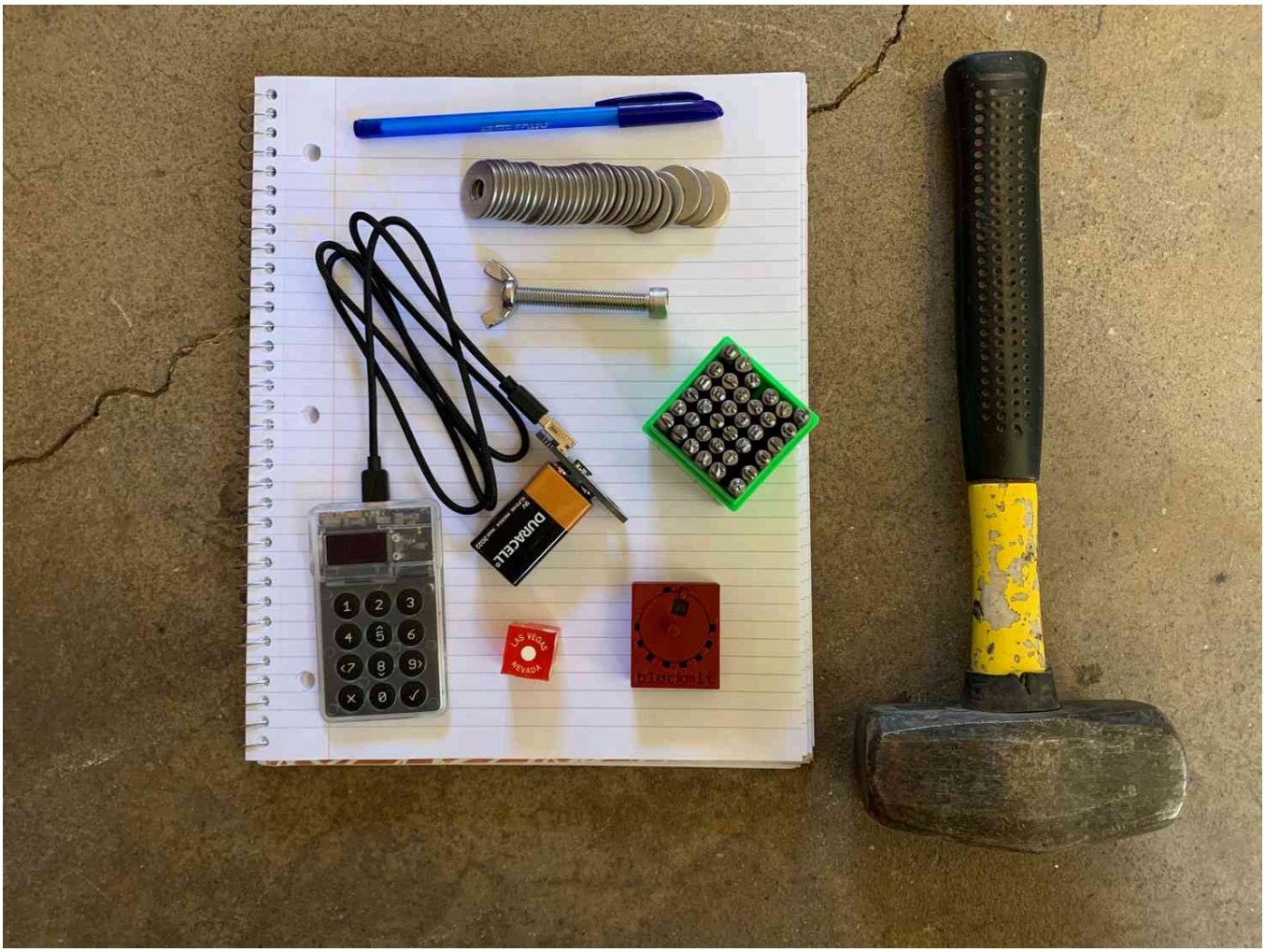
Having a reliable backup of a seed phrase is an important part of self-custody. There are many ways to backup a seed phrase, but there is no way to get bailed out if the backup is lost or damaged beyond recognition. This level of radical responsibility can be shocking to some people; there is no Bitcoin customer support desk, or Bitcoin chargebacks, or Bitcoin card-lock feature, those who are righteous enough to take custody into their own hands take the full responsibility of their Bitcoin with them.

So why would someone be crazy enough to self-custody their bitcoin, with all the pitfalls, scams, & hackers? Wouldn't people be better off just leaving custody to the pros? The short answer is "no", the long answer is "fuck no!". In this article, I aim to demonstrate how to create and verify a simple, robust, and inexpensive backup so that you can rest assured that your bitcoin is better off in your hands, not the custodians.

Self-custody is an important aspect of censorship-resistance. Self-custody enables a person to interact with the world however they choose. Because of censorship-resistance, people have the freedom to donate to any cause they find value in, obtain goods & services that may not align with a banker's vision of the world, and secure their wealth in a manner that mitigates confiscation. There are several disadvantages when a person hands over control of their bitcoin to someone else like creating a permissioned relationship, introducing counter-party risk, and diminishing privacy through KYC.

That's enough rambling from me about self-custody, let's get on with the article. The following describes how to backup a seed phrase into stainless steel washers using the Blockmit 3D printed jig; and stress testing the backup. To get started, there are few necessities. If you're

following along at home, gather the following items:



1. Hammer.
2. Blockmit 3D Printed Jig. Available at CryptoCloaks.com
3. Letter & Number Stamp Set. 3mm (1/8").

4. Stainless Steel Washers. 8mm I.D. x 24mm O.D. x 2mm thick.
5. Stainless Steel Wingnuts. M8-1.25
6. Stainless Steel Bolts. M8-1.25 x 60mm.

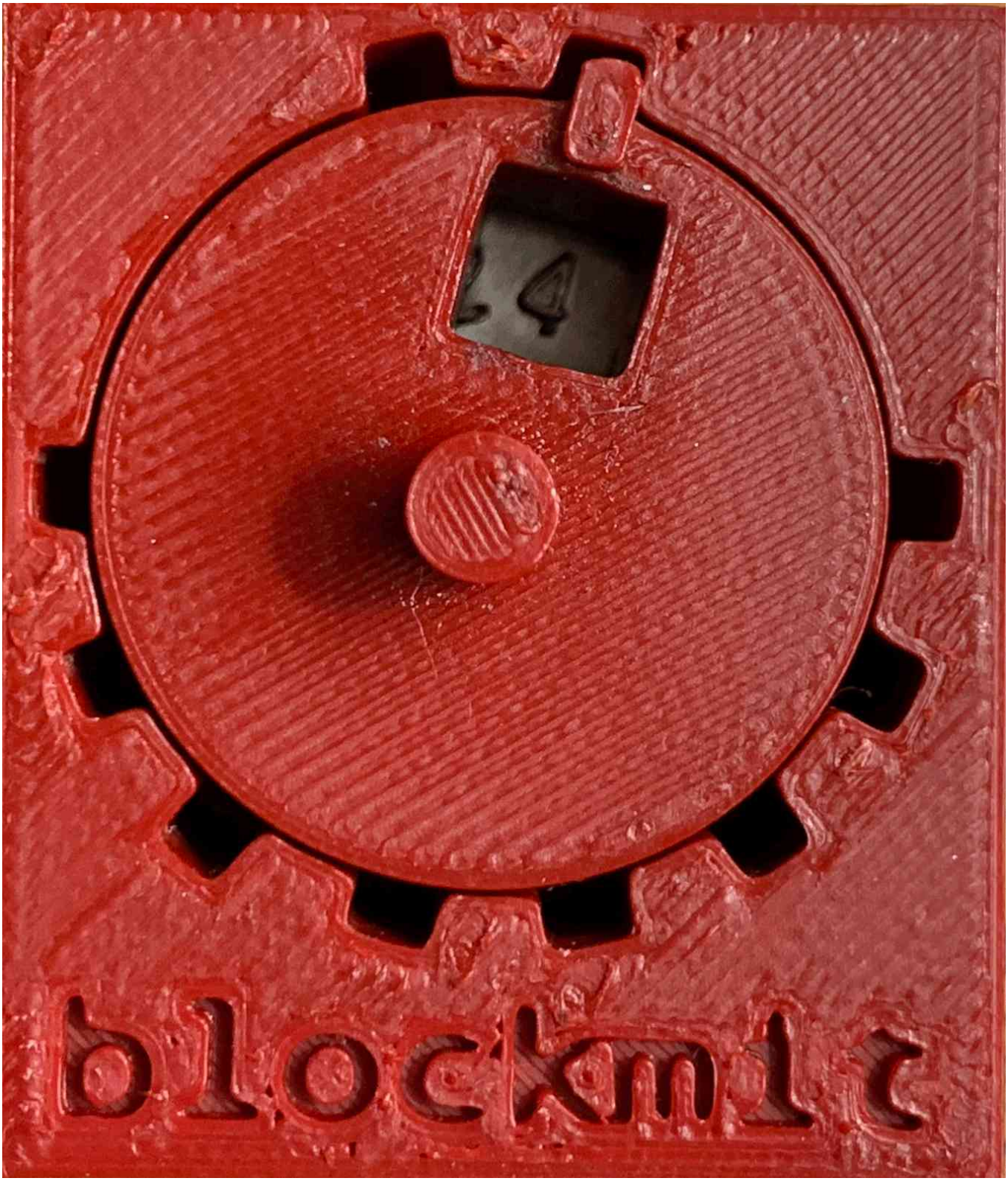
The following steps assume that you already have a 24-word seed phrase, a BIP39 passphrase, and your wallet fingerprint.

The 24-word seed phrase, the BIP39 passphrase, and the wallet fingerprint can be stamped into stainless steel washers for a simple backup that can withstand fire, flooding, and other harsh environments. Having a robust backup helps ensure that in the event the hardware wallet or other device is lost or stolen that the Bitcoin wallet can still be restored later from the information stamped into the backup washers.

To help with this, Blockmit came up with a really cool idea for a 3D printed jig. This jig allows the user to center the washer and the stamps in a clean way that keeps everything uniform and legible. Be sure to check out Blockmit's guide on using this jig here. Thank you to @Multicripto for originally bringing this awesome idea to my attention.

If you don't have a 3D printer, you can purchase these jigs from CryptoCloaks on their website here.


24
SENTENCE
blockmic



Make sure to source all the materials correctly, this jig was designed to use metric hardware. It is recommended to use double sided tape to keep the washers and jig aligned while stamping, but I didn't use any double sided tape and I was still very pleased with the results. My son helped supervise me to make sure I got the stamping done right.

Once finished, you will have a robust stainless steel backup of your 24-word seed phrase.


05
PROSE
15
14
REFUSE
13
22
21


05
BIRTH
PROSPER
BRONZE
15
OTHER
14
REFUSE
13
DIAGRAM
22
21


P1
C05 5KY6 M
P2
H 3V90 ER A


P1
C05 5KL6M
P2
H3V90ERY


FP
B7069DB


FP
B1069 5DB


CM 1 2 3 4 5 6 7 8 9
U.S.A
9 5 4 3

I was curious how well a stainless steel washer backup would be able to withstand extreme heat. So I heated up the backup until it was white hot and just starting to melt. Then took the washers apart and found that they were all still totally legible.


REFUSE
RUDDER
SILVER
SEVERENCE


02
CLERK
05
BIRTH
07
BRONZE
09
CHIMNEY
10
CLOG
11
DIVIDE
12
NEGLECT
13
DIAGRAM
14
REFUSE
15
OTHER
16
SUDDEN
17
18
SWEET
19
SHOP
20
WINTER
21
SMART
22
MANGO
23
SHUFFLE
24
SENTENCE
P1
P2
FP


BIRTH
PROSPER
BRONZE
13
DIAGRAM
14
REFUSE
15
OTHER
21
SMART
22
MANGO
23
SHUFFLE


BIRTH
PROSPER
BRONZE
13
DIAGRAM
14
REFUSE
15
OTHER
21
SMART
22
MANGO
23
SHUFFLE


SWEET
SHOP
WINTER

Then I decided to mix up some salt-water and throw the backup into the jar, I'm planning on letting it sit in the salt-water until Christmas (40 days) and then I'll open it and see if any corrosion has occurred. I'm not expecting much, since it is stainless steel, but I will post the results here at that time anyways.

40 days later...

After sitting in the salt-water mix for 40 days, I opened the jar on Christmas day. The stainless steel backup was rinsed off with fresh water and then taken apart and the individual washers were dried out. As I

suspected, since this is stainless steel, there was no sign of deterioration. The information was still fully legible and the seed phrase was still 100% recoverable.


01 SUGAR
02 CLERK
03 DERIVE
04 WHISPER
05 BIRTH
06 PROSPER
07 BRONZE
08 FRINGE
09 CHIMNEY
10 CLOTH
11 DIVIDE
12 NEGLECT
13 DIAGRAM
14 REFUSE
15 OTHER
16 SUDDEN
17 ZIP
18 SWEET
19 STOP
20 WINTER
21 SMART
22 MANOR
23 SHUFFLE
24 SENTENCE


14
REFUSE
15
OTHER
23
13
DIAGRAM
27
MANGO
21

Thank you for reading! I hope this got you thinking about backing up your seed phrases with stainless steel washers. Self-custody is a way to interact with Bitcoin in a way that protects the user from the downfalls of third parties. There are tradeoffs to all choices, but I hope this made you realize that self-custody can be easy and is not frightening.

If you enjoyed this content, leave me a tip here: Donate.

This article can be found on Twitter as a thread here.