SEED CIPHER #888888

Stackchain Magazine EP. 6 cover art by Asanoha

The front and back cover of this magazine is an artistic study created by Asanoha in the eternal quest to conceptualize bitcoin. If one were to say that bitcoin is the knowledge of a private key that allows an individual to transact with the balance of a seed on the Timechain, then both in essence, and in actuality, this magazine has the potential to *be* bitcoin.

The artwork on the front cover is the Cipher Key, the back cover is the Ciphertext. It is a hybrid transposition cipher that must be user-loaded, and is reusable.

There are 96 glyphs in the Cipher Key, each glyph representing one letter of a 24 word truncated seed phrase. All BIP39 seed phrases can be truncated down to the first 4 letters of each word.

The value of the glyphs remains arbitrary until they are assigned a letter by the user based on a seed phrase they have generated. Once assigned according to the order of glyphs on the Cipher Key, the letters are written next to their corresponding glyph on the Ciphertext in a scrambled order. The cover of the magazine is the key that decrypts the order of the letters, and thus the seed phrase.

Since the letters are scrambled on the Ciphertext, the words are unrecognizable. This provides security, since anyone finding the Ciphertext would have a hard time decrypting it without the Cipher Key. In order to decrypt the seed phrase, one needs both the Cipher Key and the Ciphertext, making this a type of seed XOR.

If the Ciphertext is used to encrypt an address that contains bitcoin, it must of course still be securely hidden. What is interesting, is that the Cipher Key itself can be displayed publicly, and without knowing what value the glyphs have been assigned, the chance of someone cracking a seed phrase that has been encrypted to it is the same as randomly guessing any 256-private key. The odds of guessing a 256-bit private key are approximately 1 in 115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000. In an attempt to understand how large that number is, consider that it is more than the approximate number of atoms in the observable universe.

ASANOHA

There is something magical about the process of rolling dice in the physical realm, using the entropy of the universe to pick a seed that a private/public key pair is derived from in order to sign digital transactions of a monetary unit backed by time itself. It is utterly fascinating to then take this modern wonder of digital cryptography in the form of a mnemonic phrase and encrypt it using the art on the cover of a magazine depicting an ancient glyph-based transposition cipher.

Combining simple cryptographic methodology developed over a thousand years ago with some of the most advanced cryptography of today, this cover art eloquently bridges the past and present, the physical and digital. It is also an interactive art study, a collaboration between the artist and the viewer, as one might say it is not complete until the cipher on this magazine has been used to secure a small amount of bitcoin, hidden within its paper surface.

Along with a variety of Bitcoin symbology, iconography, and cryptography, Asanoha creates geometric artwork. The shapes and patterns he paints and draws speak to the same mathematical truth bitcoin is built upon.

Transcending the borders, ideology and flaws of man, both bitcoin and sacred geometry honor the fundamental structure of all life and the universe itself. Whether perceived from a scientific or spiritual perspective, they both remind us that everything is connected. As bitcoin is the newest and purest form of time storage and transference, sacred geometry is the oldest and purest form of illustrating and contemplating the mysterious and wonderful formula known as life, the universe and everything.

Whether tattooing or painting, Asanoha primarily works by hand. Utilizing oil-based metallic paint pens, gold leaf, and acrylic on canvas, he also creates fine art limited edition archival prints of select pieces. Asanoha does not create any form of NFTs, ordinals, or inscriptions; instead, he focuses solely on physical artwork. Working to conceptualize the mystery of bitcoin in an elegant fashion, Asanoha inspires the viewer to ponder its intricacies while simultaneously promoting the sound money values of scarcity, integrity and honesty.

Asanoha is the Art Director at Bitcoin Trading Cards (btc-cards.com), and he is the Ops Director at simplestbitcoinedu.com

You can view more of his artwork at SovereignRemnant.com
primal.net/asanoha // twitter.com/asanoha_gold

ASANOHA

HOW TO ENCRYPT YOUR SEED

Step 1.

- Orientate yourself with the following pages:
  Plaintext Cipher Key Template, Cipher Key, Ciphertext.
- Make a few photocopies of each of these pages so that you can keep your magazine in mint condition.

Step 2.

- Perform all following steps in a room with no electronics of any kind.
- Generate a BIP39 bitcoin seed phrase using a wallet of your choice, or by rolling your own seed using the tutorial by D++ and Keysa found in this magazine.
- Write the seed down.
- Send a test transaction to this seed. Confirm that it goes through.
- Wipe the seed from whichever wallet you used to create it.

Step 3.

- Rewrite your seed on another piece of paper truncating it down to the first 4 letters of each word.

Step 4.

- Using the Plaintext Cipher Key Template, assign the first letter of your first word to the first symbol in the Plaintext Cipher Key Template, as read top left to right.
- Continue until all letters are assigned to their corresponging symbols in consecutive order.
- Go slowly, and double check your accuracy.

Step 5.

- Once all letters are assigned to their corresponding symbols on the Plaintext Cipher Key, find the first letter's symbol on the Ciphertext itself. Fill in the first letter of your first word next to it. Find the second letter's symbol.
- Continue until all letters have been paired with their corresponding symbols.
- Congratulations, you have just encrypted your seed phrase by scrambling all 96 characters necessary to access your bitcoin.

Step 6.

- Remove your Plaintext Cipher Template from eyesight.
- Using the Cipher Key, start with the first symbol, and locate it on your encrypted Ciphertext. On a seperate piece of paper write down the corresponding first letter of your first seed word.
- Using the second symbol on the Cipherkey, find and write down your second letter.
- Continue until you have decrypted the order of all 96 letters of your truncated seed phrase.
- Congratulations, if you followed these instructions correctly, you have successfully decrypted your seed phrase.

Continued on next page...

HOW TO ENCRYPT YOUR SEED

Step 7.
- Input the decrypted seed phrase into a bitcoin wallet of your choice.

Note Some wallets may require you to use the whole words. Use a copy of the BIP39 wordlist if needed to aqcuire the remaining letters.

Step 8.
- Confirm you have access to the bitcoin you sent to the seed in Step 1.

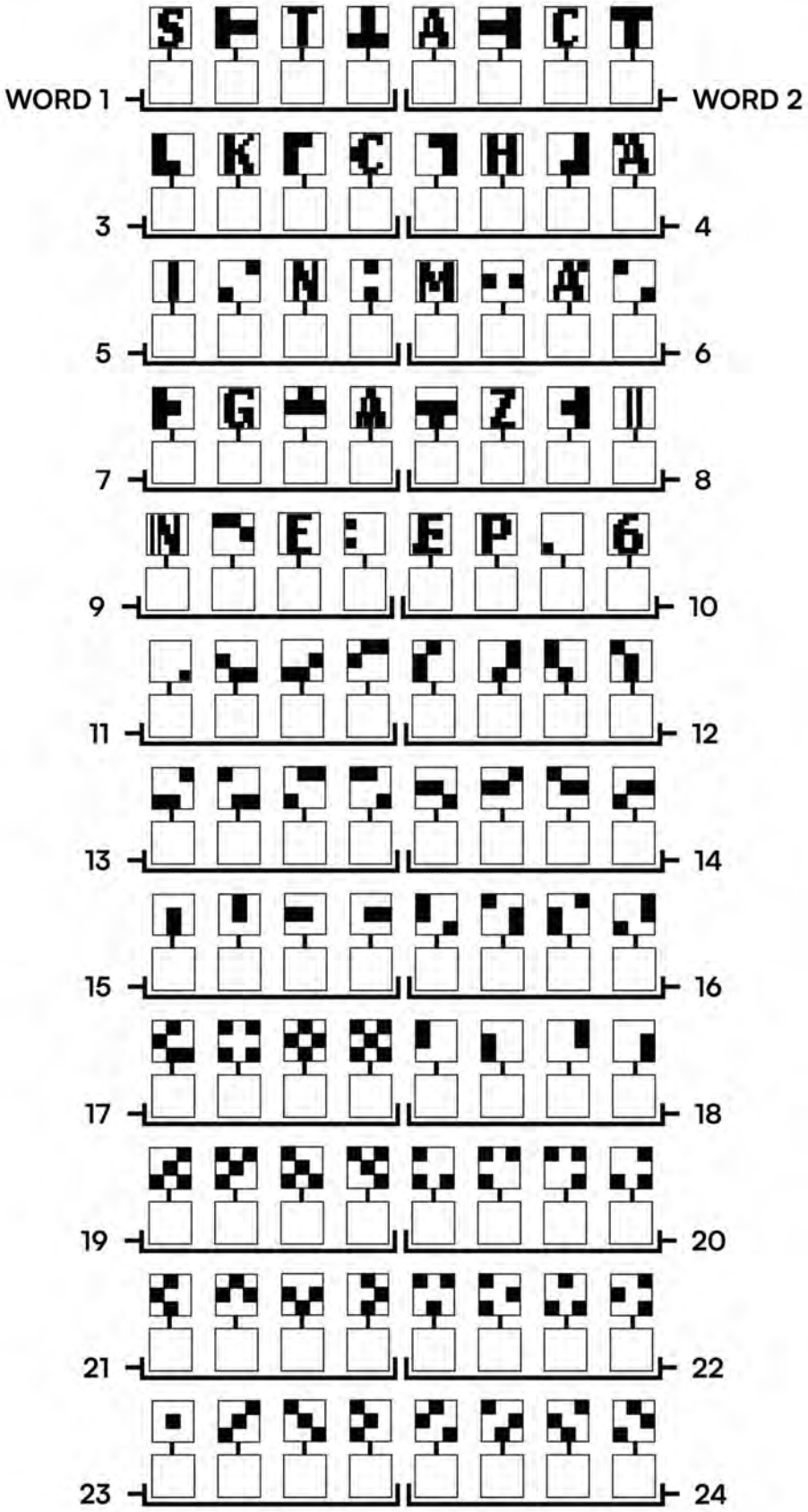
Step 9.
- It is reccomended to repeat Step 5 to Step 8, to ensure you understand how this works.

Step 10.
- Once you have confirmed that you followed all steps correctly and you have verified you are able to use the Cipher Key to decrypt the order of your scrambled seed letters on the Ciphertext, you may destroy the Plaintext Cipher Key Template.
- If you have have destroyed the Plaintext Cipher Key Template, and any other backups you wrote down during this process, your seed now only exists as Ciphertext. The only way to decrypt the order of the seed letters is using the Cipher Key.
- Be sure to securely hide your Ciphertext.

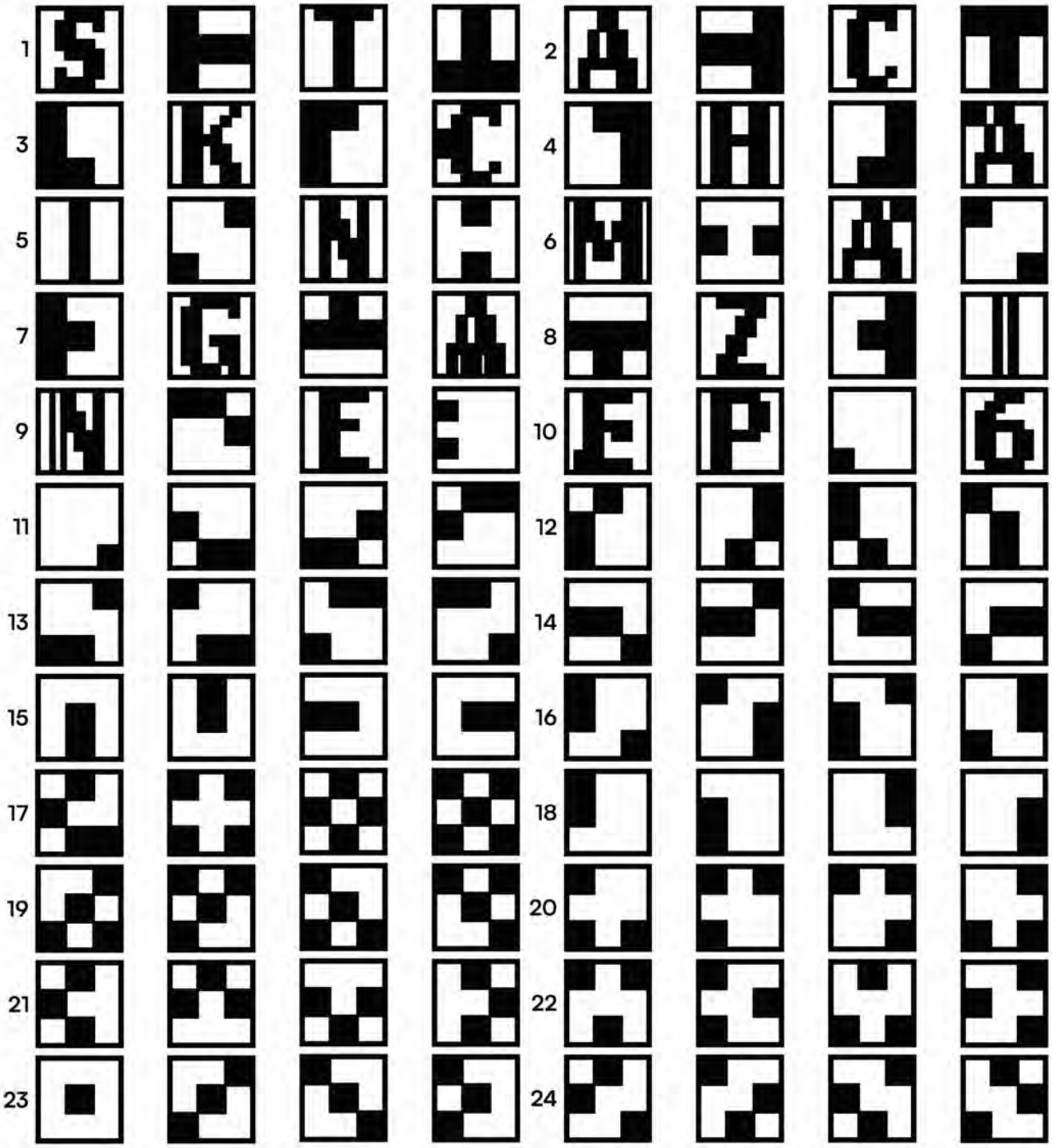
Step 11.
- Congratulations shadowy super coder, you have now learned how to encrypt and decrypt a bitcoin seed phrase entirely offline, using only pen and paper.

DISCLAIMER: This tutorial is for educational and artistic purposes only. Seed storage experimentation is fascinating, and there is debate on the security of using a plain text seed back up. It is recommended by industry standard to NOT encrypt a bitcoin seed phrase containing any signifigant amount of bitcoin. The general consenus for secure seed storage is to stamp your plain text seed into a solid plate of titanium, with a total of two backups hidden seperately. Do not use seed storage solutions with physically moving parts. Utilizing a passphrase, multisig, or any encryption method should only be attempted by an advanced user for self custody bitcoin storage. The most common cause of lost bitcoin is due to user error. Keep it simple stupid xoxo
Each persons' ideal setup is situational and based on personal variables.
Stackchain Magazine, Asanoha, and all of their affiliates are not in any way responsible for any bitcoin that may be lost in any attempt to encrypt it.

PLAINTEXT CIPHER KEY TEMPLATE



CIPHER KEY



CIPHERTEXT