Building Your Own Bank

or...

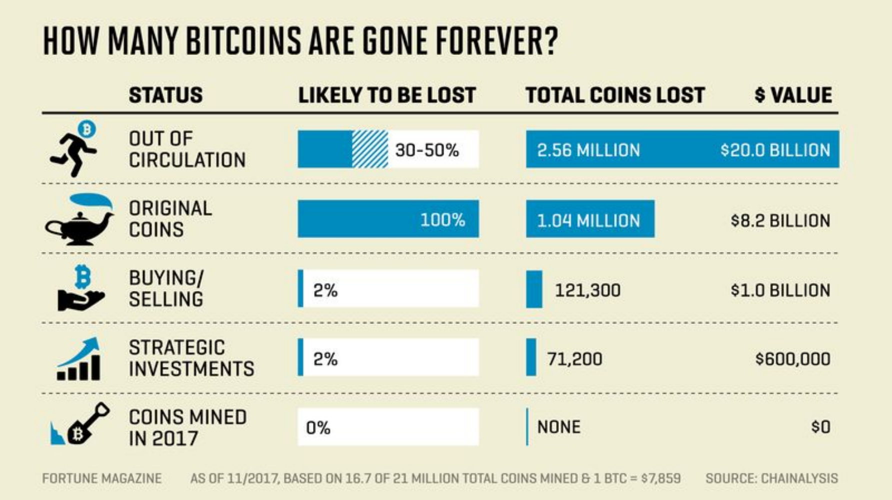
Constructing Crypto Castles

Jameson Lopp
Infrastructure Engineer

Casa

Jameson@team.casa
https://keys.casa
https://lopp.net
@lopp

A History Rife with Failure



HOW MANY BITCOINS ARE GONE FOREVER?

STATUS	LIKELY TO BE LOST	TOTAL COINS LOST	$ VALUE
OUT OF CIRCULATION	30-50%	2.56 MILLION	$20.0 BILLION
ORIGINAL COINS	100%	1.04 MILLION	$8.2 BILLION
BUYING/ SELLING	2%	121,300	$1.0 BILLION
STRATEGIC INVESTMENTS	2%	71,200	$600,000
COINS MINED IN 2017	0%	NONE	$0

FORTUNE MAGAZINE AS OF 11/2017, BASED ON 16.7 OF 21 MILLION TOTAL COINS MINED & 1 BTC = $7,859 SOURCE: CHAINALYSIS

An estimated 4,000,000+ BTC lost.

An estimated 2,000,000+ BTC stolen.

Issues of Personal Responsibility

- Few folks think about self defense because they aren’t big targets
- Few folks have much more protecting them at home than a few walls and doors that are easily breached by a motivated attacker
- No way to reverse theft of bearer assets means more motivated attackers
- If everyone fails at securing their assets, they won’t be worth much

Attacks	Defenses
Physical Theft	Safes, hidden storage, guards
Digital Theft	Offline storage
Physical disaster	Redundant storage
Social Engineering	Education, Paranoia
Collusion	Trust Minimization

Key Holding Risks

User holds key **OR** Service holds key

User holds key	Service holds key
● Malware	● Malware
● Weak password	● Hacks
● Coercion	● Insider theft
● Death of owner	● Fractional reserve
● Data loss	● Government seizure
● Forgotten password	● Data loss
● Phishing	● Frozen by service
	● Phishing

Key Holding Risks

User holds key **AND** Service holds key

(2-of-2)

User holds key

- ~~Malware~~
- ~~Weak password~~
- ~~Coercion~~
- Death of owner
- Data loss
- Forgotten password
- Phishing

Service holds key

- ~~Malware~~
- ~~Hacks~~
- ~~Insider theft~~
- ~~Fractional reserve~~
- Government seizure
- Data loss
- Frozen by service
- Phishing

Key Holding Risks

User holds multiple keys **AND** Service holds key

(2-of-3, 3-of-5…)

- ~~Malware~~
- ~~Weak password~~
- ~~Coercion~~
- ~~Death of owner~~
- ~~Data loss~~
- ~~Forgotten password~~
- Phishing

- ~~Malware~~
- ~~Hacks~~
- ~~Insider theft~~
- ~~Fractional reserve~~
- ~~Government seizure~~
- ~~Data loss~~
- ~~Frozen by service~~
- Phishing

Security Engineering Objectives

1. Protect users from trusted third parties.
2. Protect users from attackers.
3. Protect users from themselves.

It’s preferable for a user to temporarily lose access to their funds than for an attacker to temporarily gain access.

Security Engineering Objectives

1. Protect users from trusted third parties.
2. Protect users from themselves.
3. Protect users from attackers.

If we push security out to the edges of the network, users are more likely to experience loss due to negligence rather than attack.

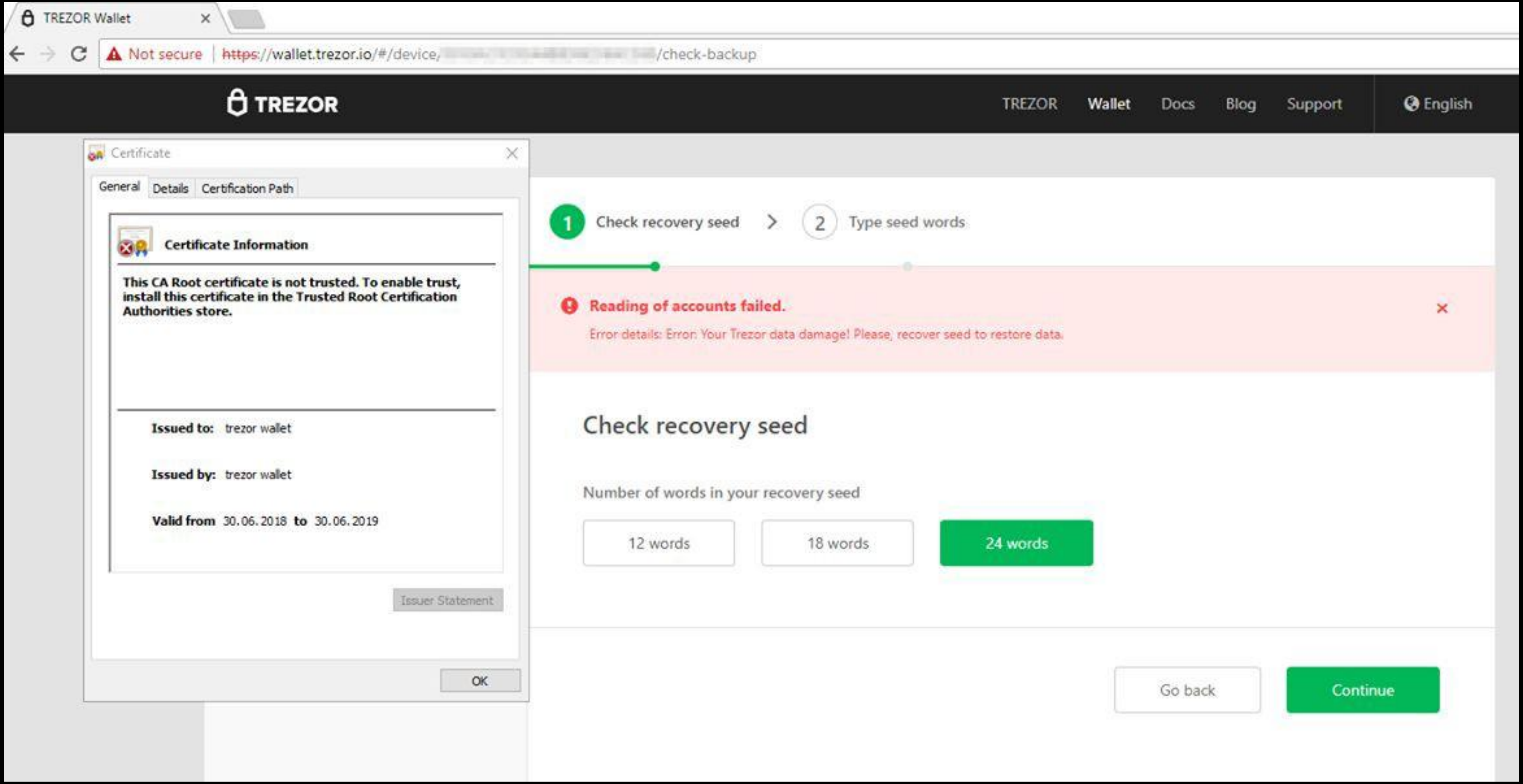
How to Build a Bitcoin Bank

Step 1: Write down this 24 word seed phrase and keep it safe.

How to Build a Bitcoin Bank

Step 1: Write down this 24 word seed phrase and keep it safe.

Users Shouldn't Handle Seeds



Not secure | ~~https~~://wallet.trezor.io/#/device/[redacted]/check-backup

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: trezor wallet

Issued by: trezor wallet

Valid from 30.06.2018 **to** 30.06.2019

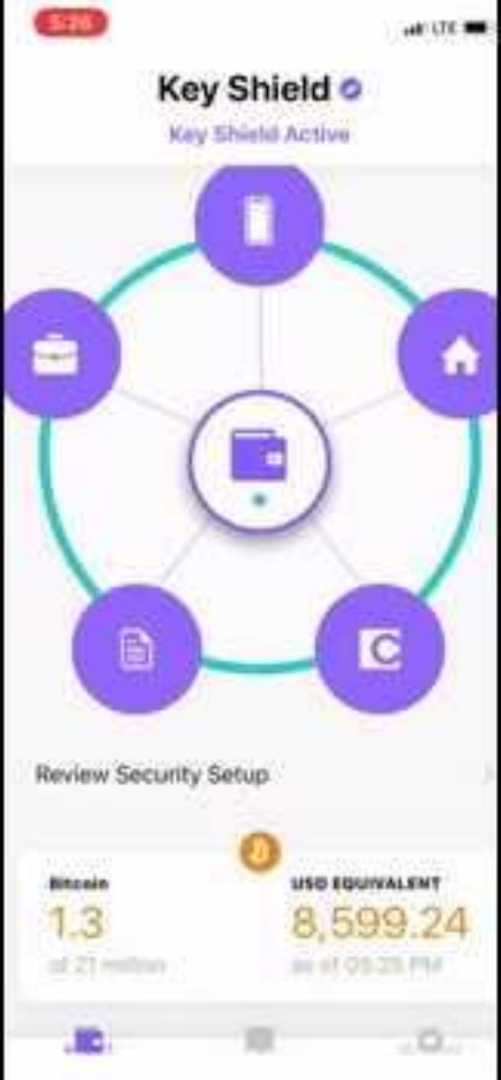
Reading of accounts failed.

Error details: Error: Your Trezor data damage! Please, recover seed to restore data.

Check recovery seed

Number of words in your recovery seed: 24 words

Seedless Recovery



Key Shield

Key Shield Active

Review Security Setup

Bitcoin

1.3

of 21 million

USD EQUIVALENT

8,599.24

as of 03:25 PM

Paper Wallets are Prone to Failure

- Hard to generate private keys securely
- Loss to physical attackers if unencrypted
- Loss due to environmental factors
- Loss due to improper transaction construction / single key sweeping

Metal Wallets are Prone to Failure

- Loss to physical attackers if unencrypted
- Loss due to environmental factors
- Loss due to improper transaction construction / single key sweeping

Add Redundancy: Eliminate SPoF

Multi-signature
Multi-device
Multi-location

My Personal (pre-Casa) Solution

1. Create encrypted file container on airgapped machine with VeraCrypt
2. Encrypt container with a randomly generated long passphrase that you generate via rolling dice
3. Use ssss to split the decryption passphrase into your preferred setup. This mainly depends upon how many trusted friends and family you're willing to store the encrypted data and decryption shards with. You also want enough redundancy that your M of N scheme doesn't become useless if a member or two loses their data or dies / is no longer able to participate in a recovery ceremony.
4. Copy file onto N USB drives and place one ssss shard on each drive
5. Hand out USB drives in faraday bags to will executors.
6. Update annually to protect against bitrot.
7. Write down what you have done and provide detailed step-by-step instructions for how to recover the data if you're no longer around.
8. **MAKE SURE YOU TEST YOUR INSTRUCTIONS**.

Complexity is the Enemy of Security

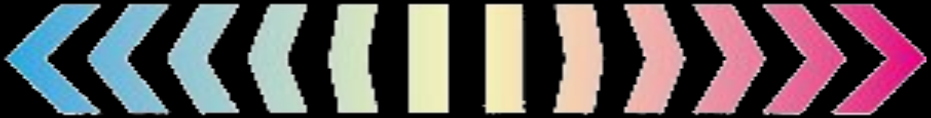
We aren’t just engineering financial applications for motivated, enthusiastic users. We’re also engineering them for the less savvy heirs who may have to execute a recovery.

How to Build a Bitcoin Bank / Crypto Castle

Use the basic building blocks:

- Air gaps are the moat
- Strong crypto / multisig are the stone walls
- Hardware key managers are the portcullis
- Wallet software is the gatehouse
- Automated alerts are the watchtowers
- A simple duress kill switch is the drawbridge

Trust Minimization



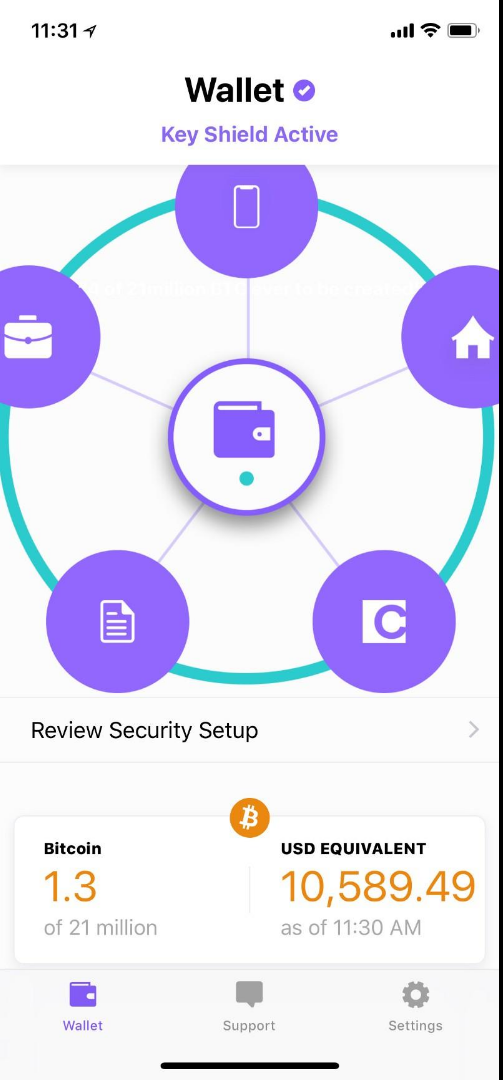
Low Trust
Low Convenience

High Trust
High Convenience

Push security to the edges

Simple full node integration is preferable

User Friendliness



11:31

Wallet

Key Shield Active

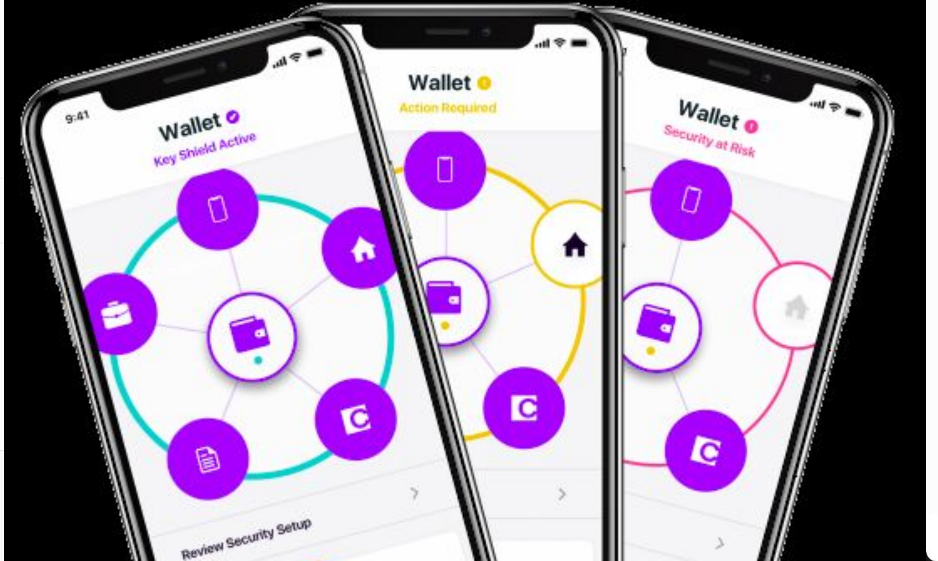
Review Security Setup

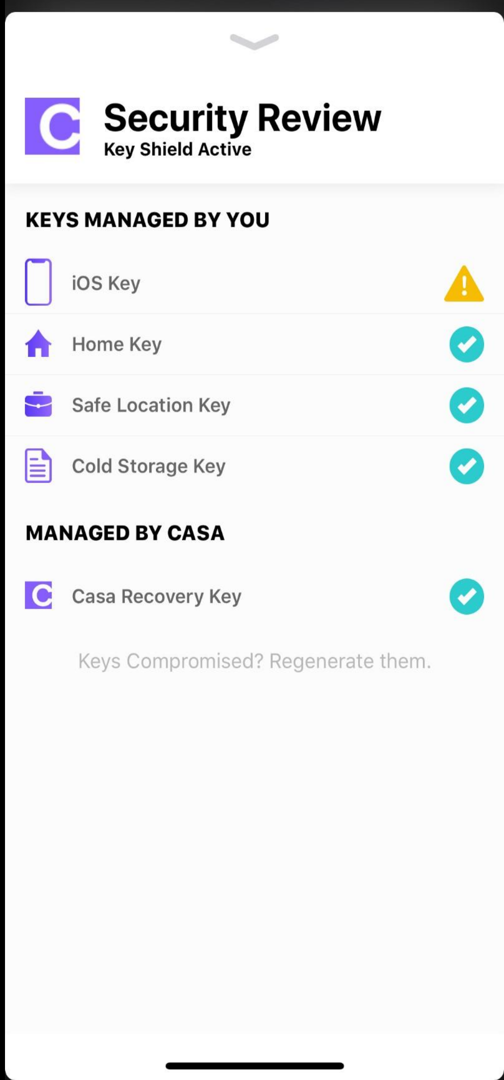
Bitcoin
1.3
of 21 million

USD EQUIVALENT
10,589.49
as of 11:30 AM

Software should bake in best practices to educate & guide the user.

Visual representations of security make it more real.





Security Review

Key Shield Active

KEYS MANAGED BY YOU

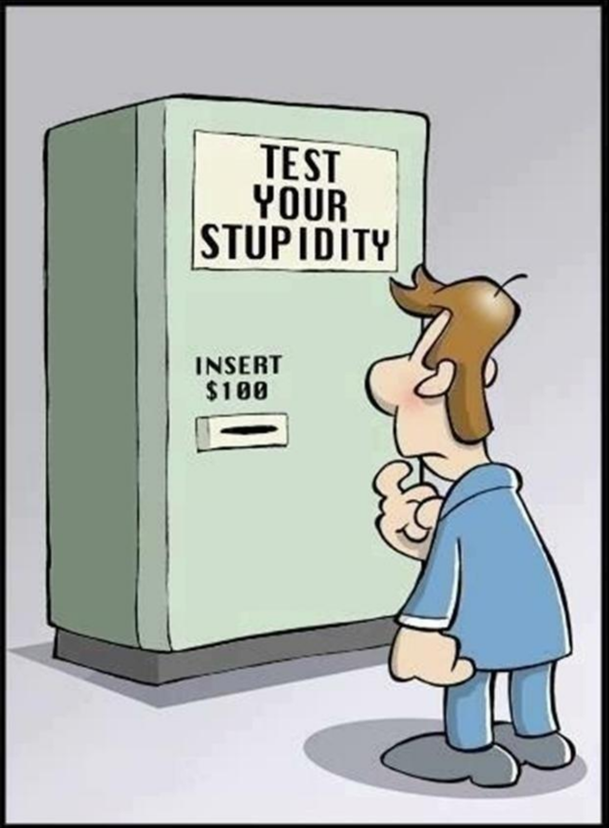
iOS Key	⚠
Home Key	✓
Safe Location Key	✓
Cold Storage Key	✓

MANAGED BY CASA

Casa Recovery Key	✓

Keys Compromised? Regenerate them.

Ignorance Protection



Some users will get tricked or otherwise compromised. It’s hard to stop social engineering.

Solutions:

Remind user to verify address out of band with counterparty.

OP_CHECKLOCKTIMEVERIFY

Malware blacklists

Reputation features & covenants

Begin Building Your Crypto Castle Today!

Questions?

Jameson Lopp
Infrastructure Engineer

Casa

Jameson@team.casa
https://keys.casa
https://lopp.net
🐦 @lopp