BITSAGA

SECURING BITCOIN

BITSAGA

IN ORDER TO UNDERSTAND

HOW

WE MUST FIRST DETERMINE

WHY

SECURITY IS NOT...

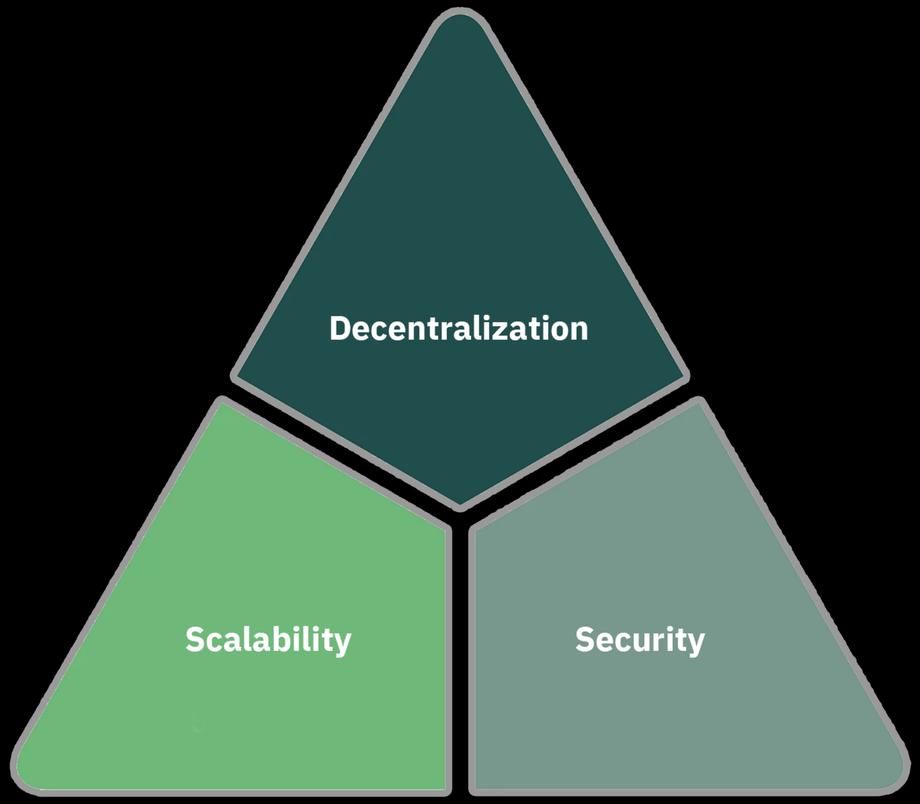
A DESTINATION BUT
AN EVER ONGOING PROCESS

SECURITY IS NOT...

ABOUT OWNING THE RIGHT TOOLS
IT'S ABOUT USING THEM CORRECTLY

BITSAGA

SECURITY IS NO...



...SINGLE POINTS OF FAILURE

BITSAGA

DISTRUST & CAUTION ARE THE PARENTS OF SECURITY

- Benjamin Franklin

BITSAGA

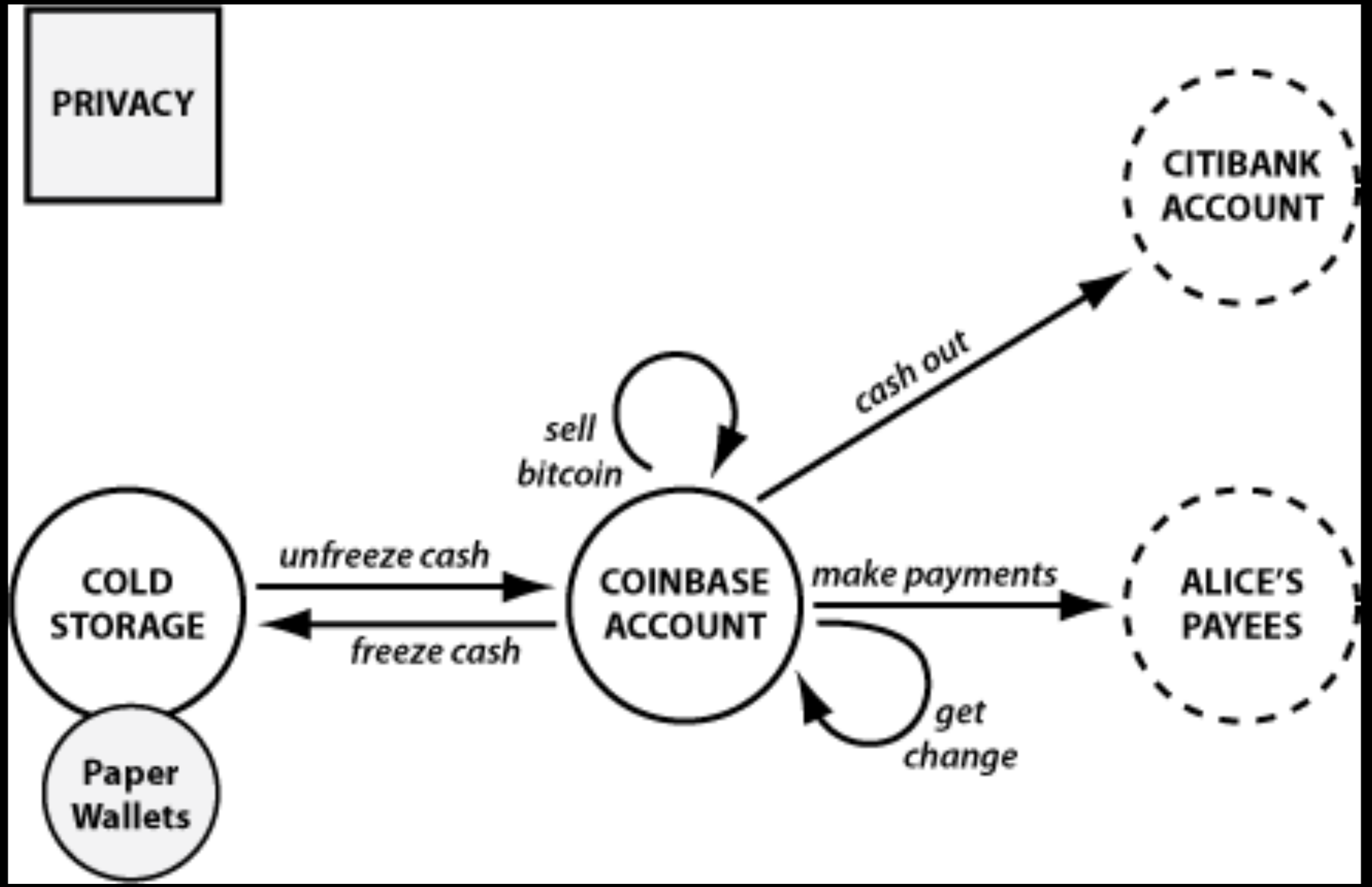
SECURITY = MANAGING RISKS

RISK MODELLING

- Identify & value your assets
  (including privacy, compartmentalisation, UX)
- Diagram your process (risks when storing ≠ risks when moving)
- Risk characterisation
  - Interface vulnerabilities (wrong / spoofed address)
  - Custody vulnerabilities (threats & hazards)
  - Non-physical vulnerabilities (compartmentalisation loss)
  - Consequences & likelihoods
  - Consider valuation changes

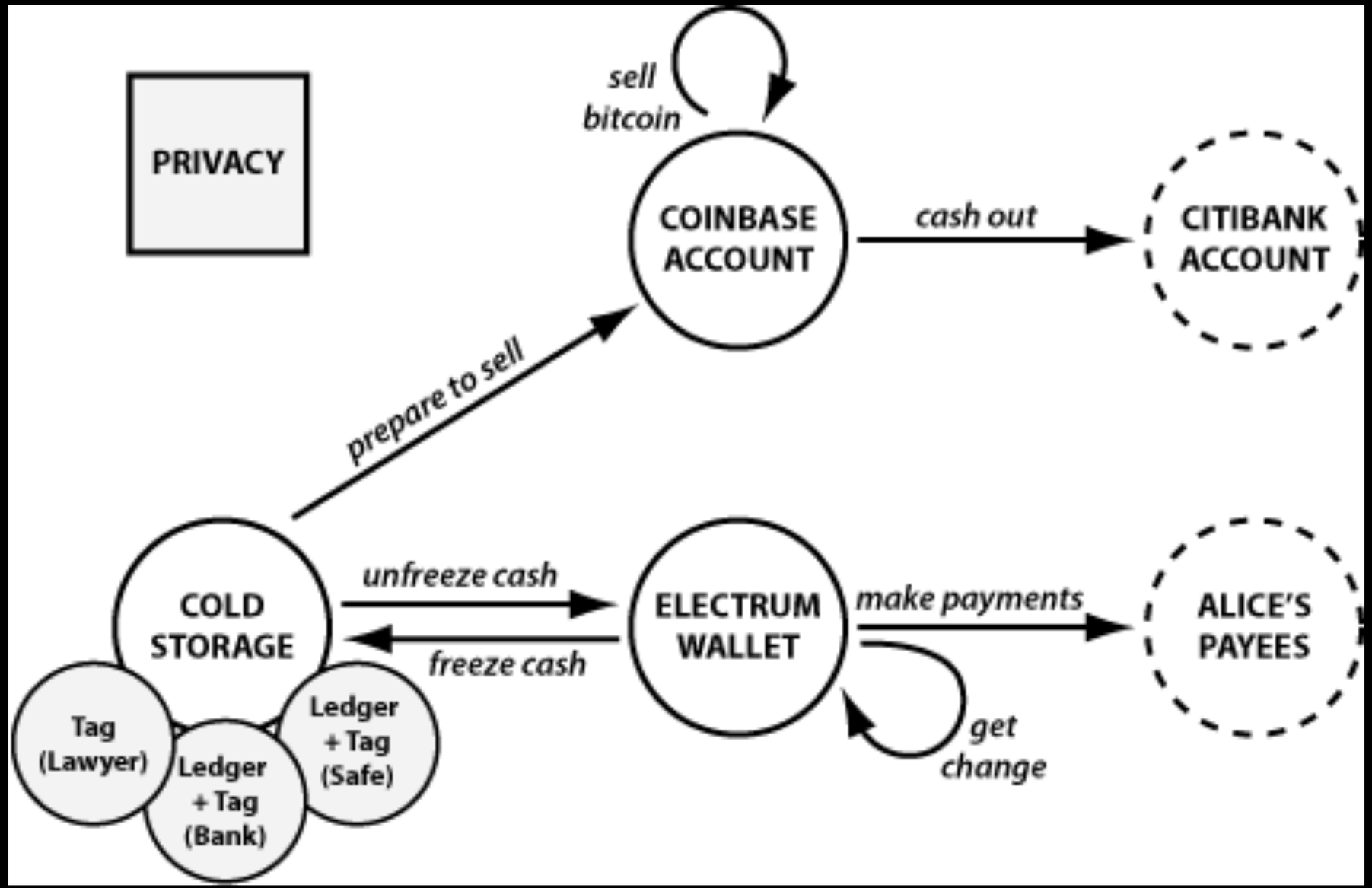
BITSAGA

RISK MODEL



BITSAGA

REVISED RISK MODEL



BITSAGA

RISKS

bitrot, blackmail, censorship, coercion, convenience, correlation, incapacitation, denial of access, disaster, institutional & internal theft, key fragility, legal forfeiture, loss of fungibility, nation-state actor, network & personal attacks, process fatigue, social engineering, supply chain attack, systemic key compromise, transaction & user error

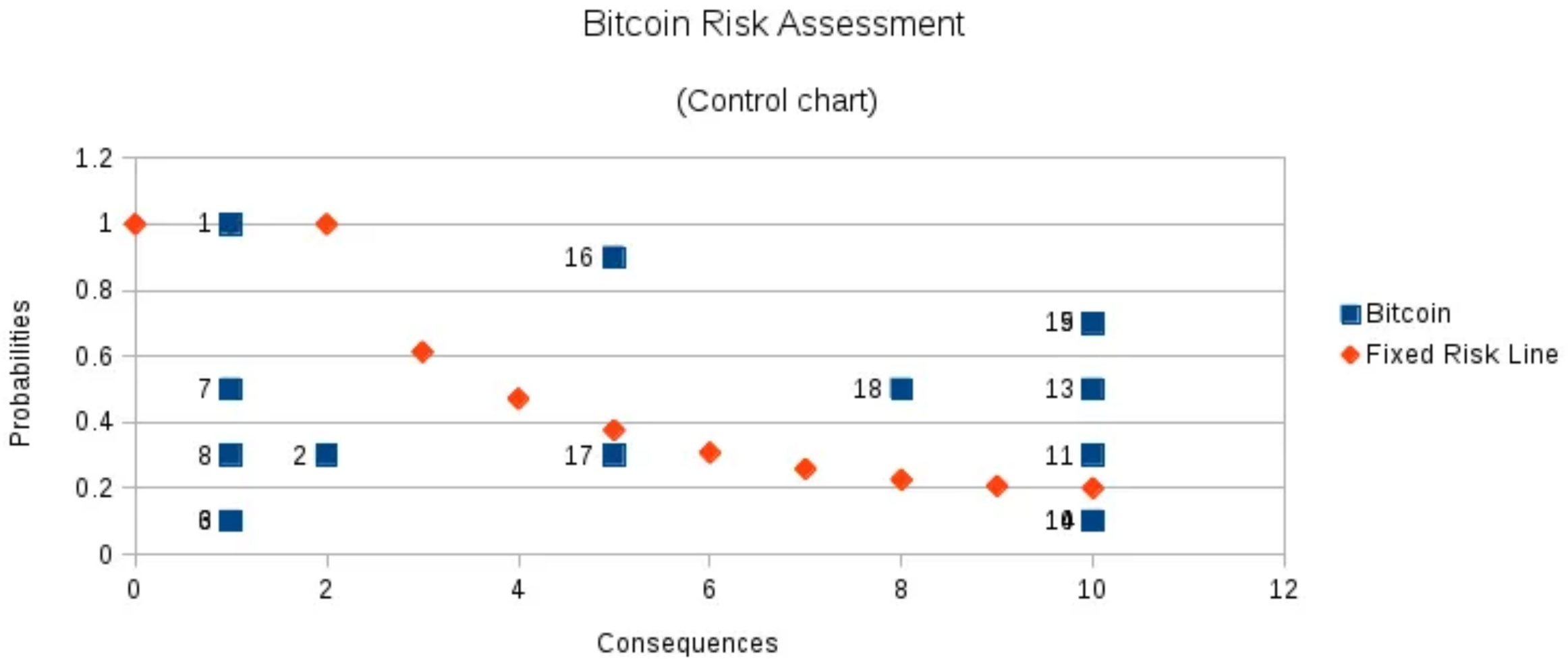
RISK

vulnerability consequence

x

vulnerability likelihood

PORTFOLIO SECURITY RISK ASSESSMENT



BITSAGA

SECURITY UP
RISK DOWN

21 BITCOIN SECURITY LEVELS

Level 0 - 4: basic security

- Level 0: bitcoin on an exchange
- Level 1: hot storage on closed-source multicoin wallet
- Level 2: hot storage on open-source bitcoin wallet
- Level 3: cold storage np multicoin USB hardware wallet
- Level 4: cold storage on a bitcoin USB hardware wallet

21 BITCOIN SECURITY LEVELS

Level 5 - 9: single seed improvements

- Level 5: air gapped hardware wallet, verifiable firmware
- Level 6: analog-only air gapped stateless cold storage
- Level 7: single seed + passphrase
- Level 8: Shamir’s secret sharing
- Level 9: Shamir’s secret sharing, steel backups

21 BITCOIN SECURITY LEVELS

Level 10 - 15: basic multi-sig

- Level 10: 2/3 hybrid multi-sig, 1 hot key
- Level 11: 2/3 full cold multi-sig
- Level 12: full cold multi-sig, encrypted/offline descriptor
- Level 13: 3 key decaying/expanding multi-sig
- Level 14: 3/5 hybrid multi-sig, 1 hot key

21 BITCOIN SECURITY LEVELS

Level 16 - 21: advanced multi-sig

- Level 16: 3/5 multi-sig with self-generated seeds
- Level 17: 3/5 taproot multi-sig
- Level 18: 3/5 multi-sig, conjoined UTXOs
- Level 19: own node, TOR
- Level 20: tamper evident sealing, multiple jurisdictions, decoys, health checks

21 BITCOIN SECURITY LEVELS

- Level ... : dedicated air gapped coordinator, dead-man switch, red team testing, on-location security, network separation & hardening, glacier protocol, fallback networking, layered encryption, redundant power backups and much more...

SECURING THE NETWORK

WHY TO RUN A NODE

- Privacy (surveillance companies run nodes)
- Validation transactions (counterfeit bitcoin)
- Changing rules of the game (forks)
- Strengthening the network
- Lightning
- Knowledge

SECURING THE NETWORK

HOW TO RUN A NODE

- Bitcoin Core
- DIY (Raspberry Pi)
  - Raspiblitz, MyNode, Umbrel, Citadel, StartOS
- Pre-built
  - Raspiblitz , MyNode One, Nodl, Start9 Server One

Gitea
A painless self-hosted Git service.

SimpleX Server
An instant messenger without user IDs

Core Lightning
An implementation of the Lightning Network protocol by Blockstream.

File Browser
Simple cloud data storage and sharing

Nextcloud
A safe home for all your data

Synapse
Synapse is a battle-tested implementation of the Matrix protocol, the killer of all messaging apps.

Alby Hub
Self-custodial Lightning wallet with integrated node.
Installed

SearXNG
Privacy-preserving internet metasearch engine.

Ride the Lightning
A full function, device agnostic, web user interface for managing lightning node operations

FreeGPT-2
FreeGPT-2 is a tool for running large language models locally.
Installed

Lightning Terminal
Your Home for Lightning Liquidity

noStrudel
A sandbox for exploring nostr

Jam
Jam - A friendly UI for JoinMarket

BTCPay Server
Bitcoin and cryptocurrency payment processor and POS system.
Installed

LNBits
Free and open-source lightning-network wallet/accounts system.

Ghost
A self-hosted blogging platform

Mempool
Be your own explorer

RoboSats
A simple and private p2p bitcoin exchange

Jellyfin
The Free Software Media System

Start9 Pages
Create Tor websites, hosted on your personal server.

Vaultwarden
Secure password management

Bitcoin Core
A Bitcoin Full Node by Bitcoin Core
Installed

electrs
An efficient re-implementation of Electrum Server in Rust
Installed

LND
A complete implementation of a Lightning Network node by Lightning Labs
Installed

Nostr RS Relay
A Nostr relay, written in Rust.
Installed

Burn After Reading
Share messages and files that are destroyed after they are viewed

Wasabi
Wasabi - Desktop Wallet In Your Browser

Monero
A Monero Full Node

Bitcoin Core (testnet4)
A Bitcoin Full Node by Bitcoin Core

Datum Gateway
Make block templates and issue work to your miners

Bisq
Buy and sell bitcoin for fiat (or other cryptocurrencies) privately and securely.

LNDg
Web UI for LND developed specifically for LND Routing Node Operators

Helipad
View boosts & boostagrams from Podcasting 2.0 apps

Public Pool
Public Pool - Fully Open Source Solo Bitcoin Mining Pool
Installed

Balance of Satoshis
A Tool for working with the balance of your satoshis on LND

Syncthing
Synchronizes files between devices in real time, safely protected from prying eyes

Webtop
Webtop - A Linux Desktop Environment In Your Browser

CryptPad
Collaboration suite, end-to-end encrypted and open-source.

IPFS Podcasting
Crowd-host podcasts over IPFS

Photoview
An easy way to organize and share your personal photos

Specter
A user-friendly web GUI for Bitcoin Core with a focus on multisignature setup using hardware wallets and airgapped devices.

Uptime Kuma
Uptime Kuma - A fancy self-hosted monitoring tool

Dojo
Your private backend server for Ashigaru, Samourai Wallet and other light wallets.

Bitcoin Knots
A Bitcoin Full Node by Bitcoin Knots
Installed

Sparrow
Sparrow - Desktop Wallet In Your Browser
Installed

Remote
Use Tor Browser to Remotely control your Core Lightning nodes using Remote.

MySpeed
Speed test analysis software that tests your internet speed periodically for up to 30 days

Lightning Jet
Fully automated rebalancer for LND Lightning nodes

ThunderHub
LND Lightning Node Manager in your Browser
Installed

EPIC Node Server
EPIC Node Server

Sphinx Chat
Chat on the Lightning Network.

Cups Messenger
Real private messaging

IPFS
InterPlanetary File System

Mastodon
A free, open-source social network server

CONNECTING YOUR NODE TO YOUR WALLET

SECURITY IS AN EVER ONGOING PROCESS...

- Bitcoin.org: securing your wallet
- Jolly Roger's security guide for beginners
- Casa: Do's and don'ts of bitcoin key management
- Nau: triple Sec
- EFF: surveillance self-defense
- NSA: Hardening network devices