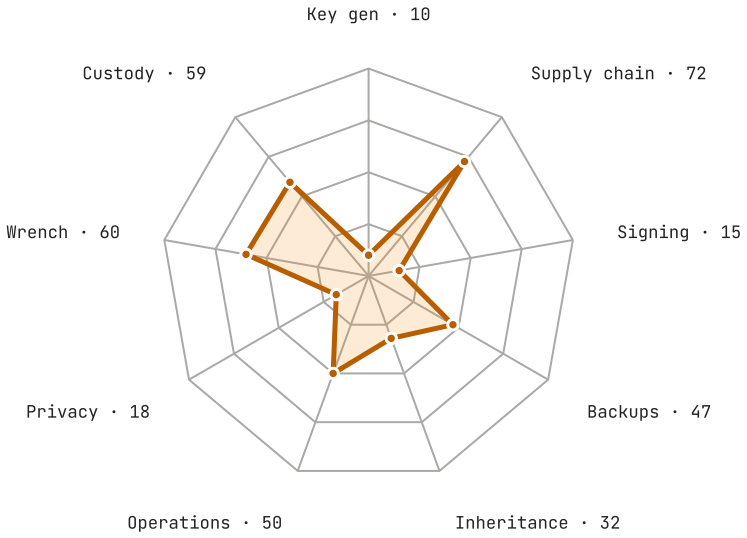
FICTIONAL SEEDED RANDOM EXAMPLE · 69/69 RUBRIC QUESTIONS

Bitcoin Safety Vector

Yes · Hardware · Multisig · Model 2.0.0 · Schema 2

Not a security certification. Printed results are sensitive.

Score web



OVERALL RUBRIC SCORE

35 /100

CRITICAL

Weakest-link cap: Key generation · 43 → 35

01 Dimension scores

Key generation 10 /100	Supply chain & device integrity 72 /100
Signing-time security 15 /100	Backup resilience 47 /100
Inheritance & incapacitation 32 /100	Operational competence 50 /100
Privacy & targeting exposure 18 /100	Physical coercion (wrench) 60 /100
Custodial / counterparty exposure 59 /100	

02 Critical findings

- Key generation: Score is below the critical threshold of 35.
- Signing-time security: Score is below the critical threshold of 35.
- Inheritance & incapacitation: Score is below the critical threshold of 35.
- Privacy & targeting exposure: Score is below the critical threshold of 35.
- Key generation: Brainwallet/web-generated seed is in a known-weak enumerable class (~98% historical brainwallet drain rate); dimension capped at 10 until funds migrate.
- Signing-time security: Seed words entered into a website/app must be considered exposed; dimension capped at 15 until funds migrate.

03 Prioritized actions

1. **Signing-time security**
   If seed words were entered into a website, app, message, or support tool, treat the seed as exposed. Verify a fresh backup and destination, test with a small amount, then migrate the remainder.
   trezor.io

2. **Signing-time security**
   Adopt the device-screen rule: confirm addresses, amounts, and approvals on the signing screen, checking the full address for large sends. This reduces clipper, poisoning, and interface-swap risk.
   nccgroup.com

3. **Backup resilience**
   Make a second physical copy in a different building to reduce single-location destruction risk.
   jlopp.github.io

4. **Backup resilience**
   Upgrade one copy to stamped stainless steel (a plate that passes Lopp's stress tests): ~$30-80; survives fire/flood/crush.
   jlopp.github.io

5. **Operational competence**
   Adopt a test-transaction rule: send a small amount and confirm receipt before a large transfer to reduce wrong-address and wrong-amount risk.
   coindesk.com

04 Method

Scoring

Ordinal self-assessment. Not a probability of loss, guarantee, certification, or substitute for professional advice. The overall score uses profile-adjusted weights and a weakest-link cap.

Key generation	6.8%
Supply chain & device integrity	8.5%
Signing-time security	11.9%
Backup resilience	18.4%
Inheritance & incapacitation	6.8%
Operational competence	18.4%
Privacy & targeting exposure	6.8%
Physical coercion (wrench)	6.7%
Custodial / counterparty exposure	15.5%

Caveats

- This is an ordinal self-assessment, not a probability of loss, guarantee of safety, or substitute for professional legal, tax, custody, or physical-security advice.
- Wrench-attack datasets are floors: all sources undercount (Lopp states his registry is non-comprehensive; CertiK counts only confirmed incidents). Trends are reliable; absolute rates are minimums.
- The visibility-to-victim link is a documented pattern, not a measured rate: no source publishes a precise share of victims who were publicly known holders; the dominance of founders, influencers, and their relatives in named cases is strong qualitative evidence, but the exact fraction is an inference.
- The inheritance share of lost coins rests on survey and case-study evidence: no rigorous study isolates death-without-plan on-chain; the dimension leans on the Cremation Institute 2020 survey (behavioral gap) plus cases like QuadrigaCX, the thinnest evidence base of the model.

Action sources

1. Signing-time security
   trezor.io
2. Signing-time security
   nccgroup.com
3. Backup resilience
   jlopp.github.io
4. Backup resilience
   jlopp.github.io
5. Operational competence
   coindesk.com

```
SAMPLE PROVENANCE
Fictional seeded random example · 69/69 rubric questions · Revision seeded-sample-v1
Seed btc-safety-vector-seeded-sample-v1
Algorithm sha256-domain-separated-rejection-v1 · Model 2.0.0 · Schema 2
Rubric fingerprint 3e00ddf6c5ed0a656840af3c52b3e3a566a5766aee6af6f9a5bf7604b7841738
Manifest SHA-256 bdaa1e791b2233ffe8b78bc55fbb64b2619a13dc6729b83f9a6e37e325fc39cb
```