Great Wall: Reinventing Coercion-Resistance

"I have never seen an unworried Bitcoiner"

The 2023-2026 Bitcoin cycle has been witnessing a terrifying rise in the frequency and gravity of **wrench attacks** (theft of crypto assets through robbery or kidnapping), and, embarrassingly, crypto community doesn't have a simple, effective and affordable solution for it. Yet. Meet **Great Wall**, an innovative self-custody protocol for coercion-resistance. It is **the only** to combine the following four properties below:

Key Features

1 Deviceless / KBA

No gadget, metal plate, vault, physical address, etc (additional points of failure) are necessary for the key derivation.

2 Non-Shared Custody

You don't compromise Bitcoin's foundational premise of **individual** custody.

3 Non-Obscurity

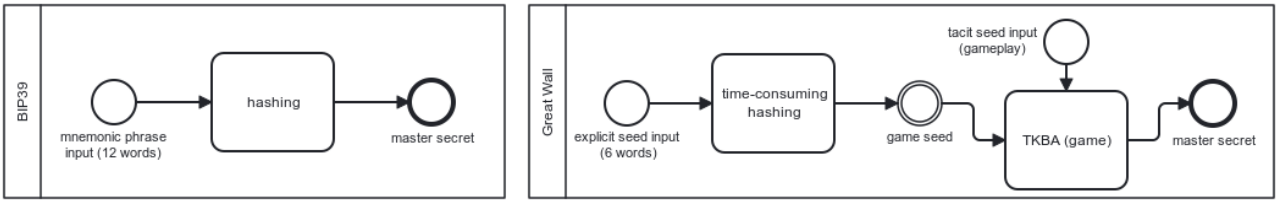
You don't need to hide in shadows, nor wish on your lucky start that your secret trick (like decoy wallet) is never learned by the bad guys.

4 Coercion-Resistance

Commitment or threat of violence on user yields no material benefit to the attacker in any circumstance.

How It Works

Simply put: "1) It's all in your brain; 2) in nobody else's; 3) the attacker knows about it; and 4) they are, nevertheless, unable to coerce you into giving away your keys". Let's see how to deliver all that, and 5) monetize it!



Comparative BPMN diagrams representing BIP39 and Great Wall key derivation schemes.

Likewise BIP39, it's just a key derivation scheme that can run 100% offline in any device. The simple way to describe the Great Wall protocol is to say:

1. You input an initial seed equivalent in strength to 6 BIP39 words into an hours-long hash;
2. Hash specifies a seed to your 'private game', which admits a near-infinity of possible 'gameplays';
3. Bits of your 'private gameplay' of your 'private game' are added to the entropy of the master secret;

The catch is that the knowledge of 'gameplay' is easy to memorize but impossible to put into words. Because of that, you, kept alive and well, are strictly necessary during the entire process, which can be set up to take hours, days, or even weeks. As a result, stealing your stash becomes at least as difficult as conducting a kidnapping that takes as long. Similarly to Anki and Duolingo, an **integrated memory coach** prevents user *forgetting* their seeds due to *insufficiently* exercising brain memory of them; but also user *fatigue* due to *overdoing* it. Replaying this half minute game-like UX on average once a week comfortably cements your lifelong coercion-resistant access to your stash.

Monetization — first-mover lock-in

1. **branded merchandise** — likewise security companies' warning signs, it dissuades would-be wrench attackers and propagate virally;
2. **convenience** — for a small price, without compromise of security properties, you can choose to outsource the hours-, days- or weeks-long inconvenience of keeping your own device very busy;
3. **hardware** — for premium UX, high-end users will prefer dedicated air gapped hardware;
4. **inheritance protocol** — same market and similar mechanism to 2, also recurrent micropayment;

Visit linktr.ee/greatwallt3 to verify all claims and learn more.