Startup FAQ / Q&A

Last updated: October 12, 2025

General Questions

Q: What problem does your startup solve?

A: Great Wall, the protocol, app and startup solve the terrifyingly rising problem of **wrench attakcs** on custody of crypto assets.

Q: How is your approach different from competitors?

A: Great Wall is, the first to combine 4 crucial information security properties, namely:

1. **Devicelessness / Stateless / Kowledge-Based Authentication**: AKA **KBA**. This refers to the attainment of secret at hand, in our case, the private keys of a wallet, is not depending on any physical object except user's own brain, in contrast to PBA (**P**ossession-**B**ased **A**uthentication). Namely, by having access to a piece of information (the 'knowledge', in knowledge-based authentication) that is possible to memorize, user can attain their wallet in any device. There is no particular external device, metal plaque, object, physical address that, user depends on, therefore becoming an additional point of failure;

2. **Individual, non-Shared Custody**: This is the foundational premise of Bitcoin. Compromising on that premise negates the core valeu proposal of Bitcoin / crypto. As our saying goes "be your own bank" means you don't rely on anybody else or any company for the custody of your assets.

3. **Non-Obscurity**: This is a direct consequence of one of the most widely accepted paradigms in cryptology and protocol design, the Kerckhoffs's principle. The principle states: 'Knowledge inevitably diffuses, so a security system cannot rely on adversaries' ignorance on how it works, but on the secrecy of each instance.'. Put simply: 'A good security system is not one based on a secret trick (that one just *hopes* adversaries never get to learn), but on the secrecy of each user's keys'.

4. **Coercion Resistance**: It's the main point: to render attempts of using violence or threats thereof on custodians to compel them to give up their stashes (or any private information whatsoever). Not only that, system has to be such that an attacker cannot even threaten the integrity of the user's stash to try to obtain something else.

Q: Why are this specific combination of 4 properties so important?

A: The importance of that specific combination of properties becomes clear once we analyse the shortcomings of systems lacking or compromising each one individually, as described below:

1. **Individual, Non-Obscure, Coercion Resistant, but not KBA**: This setup describes solutions that are intensive in physical elements, such as sharding your key and distributing shards accross multiple addresses as well as the elements for physical security of each such address, like physical vaults, surveilance, home defense, alarm, geographic separation, etc. The shortcoming of that approach is the **astronomically high costs** of setup, maintenance and update. Put simply: 'Bitcoin is reduced to a glorified gold'.

2. **KBA, Non-Obscure, Coercion Resistant, but not Individual**: This setup describes solutions in which owner depends on services of shared custody. As explained above, that completely negates the foundational premise of Bitcoin. Companies offering said services, are themselves liable to state regulations, judicial subpoenas, and are themselves, additional points of failure. Put simply: 'Bitcoin is reduced to a glorified fiat currency';

3. **KBA, Individual, Coercion Resistant, but based on Obscurity**:

4. **KBA, Individual, Non-Obscure, but Coercion Vulnerable**:

Technical Questions

Business Model