Summary

I want to explore how a single wallet can upgrade smoothly from a temporary burner wallet up to a big account or DAO treasury. If that works, the interface could eventually be standardized.

Consider a wallet with tiers of capability. Capabilities range from “spend up to x ETH per day” to “full admin rights, including ability to modify the tiers”. Each tier would have a list of keys which can exercise those capabilities, optionally requiring m-of-n signers from that list.

Example user story

Our user creates a new Ethereum wallet. Initially, the wallet has a single tier with full admin rights and a single authorized key listed in that tier. (A wallet app would do both automatically-- create an initial keypair + deploy the smart wallet contract controlled by that key.)

Later, our user adds a second device–say a phone, if the first was a laptop. Rather than moving the same key over via seed phrase, they add the phone as a second, separate authorized key. (In an app, this would show up in more descriptive phrasing like “Add an authorized device”.) Both devices now have full admin capabilities.

Later, the wallet accumulates significant asset value. To protect against malware or other theft, the owner creates a second tier. The first tier contains [phone key, laptop key] as authorized keys, and can spend up to 1 ETH per day. The second tier has full admin capabilities and contains [phone, laptop, plus a friend’s phone] as authorized keys, with at least two

signatures required to take an action.

Notice the user never had to change their public address, update ENS or similar. The same wallet went from (quick burner) to (big account with social recovery). And unlike, say, a Gnosis Safe or a hot/cold wallet setup, they can still conveniently use the account for everyday activity (spending up to 1 ETH per day) from either of their two devices.

Also, the user never had to write down a seed phrase: each private key was generated on a device and never left that device. They are still protected if they lose one of their devices.

Finally, a DAO treasury would use the same mechanism but with more tiers and more approved addresses. They might have 50 people who are each authorized for small expenses, plus some higher tiers culminating in a core-team multisig admin tier.

Goals

- Good new-user experience. New Ethereum users should not have to set up things like social recovery immediately–they should be able to start right away.
- Upgradeability. Allow smooth upgrade from a starter wallet to a secure wallet, keeping the same address.
- Better security. Avoid seed phrases in typical usage. This removes a primary avenue for loss and theft. Instead, treat keys as immovable, never leaving the device on which they’re generated.
- Transparency, particularly for group accounts. Create a uniform way for interfaces such as wallet apps to show who’s authorized to spend or take other actions from a shared account.

Relationship to account abstraction

The big shortcoming of the idea above, if we implemented it today, is that each authorized key also

needs to hold a balance separate from the wallet balance in order to initiate transactions and pay for gas.

So in the example above, the owner would have to keep three piles of ETH: the main pile in the wallet, plus a bit of ETH on the phone and a bit on the laptop.

EIP-2938 / EIP-4337 may fix this in the future. Alternately, a wallet like this could be implemented on L2 to benefit from both account abstraction and lower fees.

Comparison to tradfi

Smart wallets in general (and this idea specifically) recreate the idea of tiered verification from tradfi. For example, if I spend $5 at a gas station, I can wave my card in front of the reader and the transaction completes immediately. Above $10 or so, I might have to enter a PIN or sign. Above a few thousand dollars, the card doesn’t work at all and I have to make a wire transfer. In that case, someone from the bank calls me and asks me security questions.

The details are silly and archaic, but the general principle (frictionless small payments, tiers of added verification for large ones) is important! Unfortunately the path of least resistance for Ethereum users today is to use a single EOA thru metamask or similar. This allows frictionless instant payments of any size, which is not

what you want and often results in people getting burned.

Comparison to crypto prior art

We have a number of smart wallets (Gnosis Safe, Argent Vault etc) but I have not yet seen one that allows both

frictionless (= single-signer) spending for small amounts and secure (= multisig) for large amounts and administration, from a single wallet.

Also, as far as I'm aware, there's not yet an ERC standard way for a wallet to expose information on who's authorized to do what.

Such a standard would allow greater transparency. With the proliferation of DAOs managing treasuries, I would like an easy way to see who the signers are and the spending limits (if any) for each tier.