

Smart contract wallets

Managing crypto funds individually and collectively



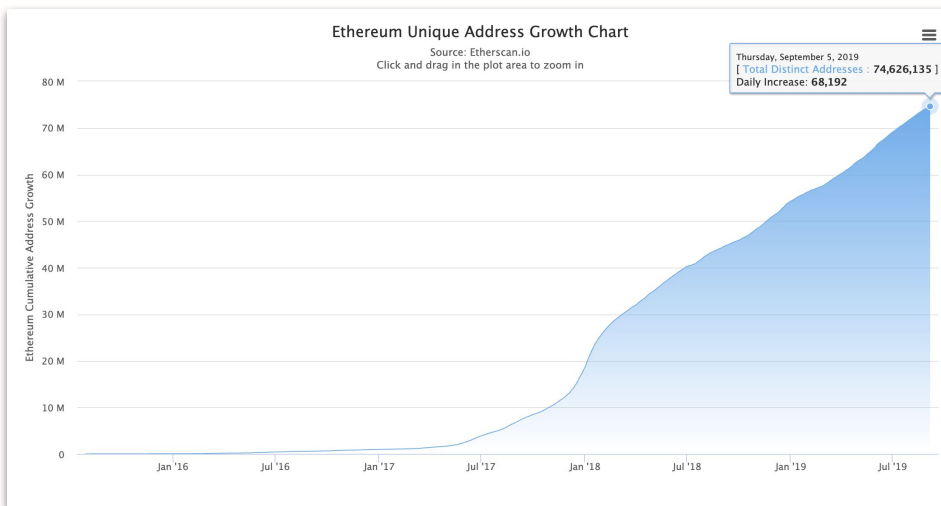
Overview

1. Why smart contract wallets?
2. Where are we now?
3. Where are we going?



Explosion in accounts & funds held

- ~74,000,000 accounts on Ethereum
- ~36,000,000,000 USD in value (ETH + top 100 ERC20s)



Source: <https://etherscan.io/> on September 6, 2019



How are users storing their funds?



 kraken

coinbase


BINANCE

BITFINEX 





People that work in crypto?

- 67% make a transaction weekly or more often
- 77% use MetaMask
 - 6/10 comfort level storing funds
- 82% own a hardware wallet
 - 7.6/10 comfort level storing funds
- 85% have a mobile wallet installed
 - 44% hold no more than \$30 in this wallet



Today: **Externally owned accounts** (EOAs)



Issues with EOAs

- Backups of **seed phrase** required!
- **No access control**: Access all or nothing.
- **Limited** on features.
- Users are **not ready** for it:

Posted by u/pelebel 1 year ago 📄

Help needed! Lost private key TIFU

So I installed the wallet on my computer last year, mined quite a bit, did transactions and everything was fine. I copied my public key to a secure location, thinking I was securing my wallet.

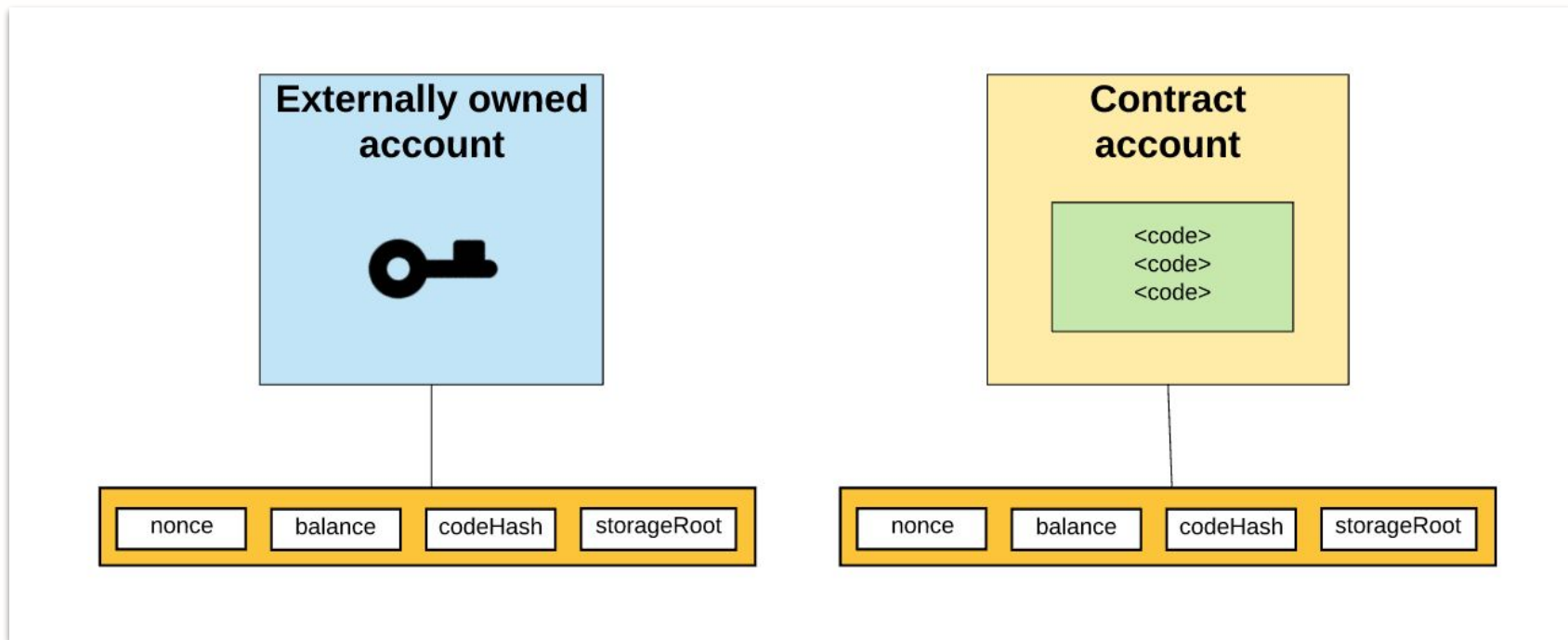


Hardware wallets

- Still an externally owned account
- Air gapped to not expose private key
- People feel comfortable
- Still, if seed is lost, everything is gone...
- **This doesn't scale**



Ethereum account types



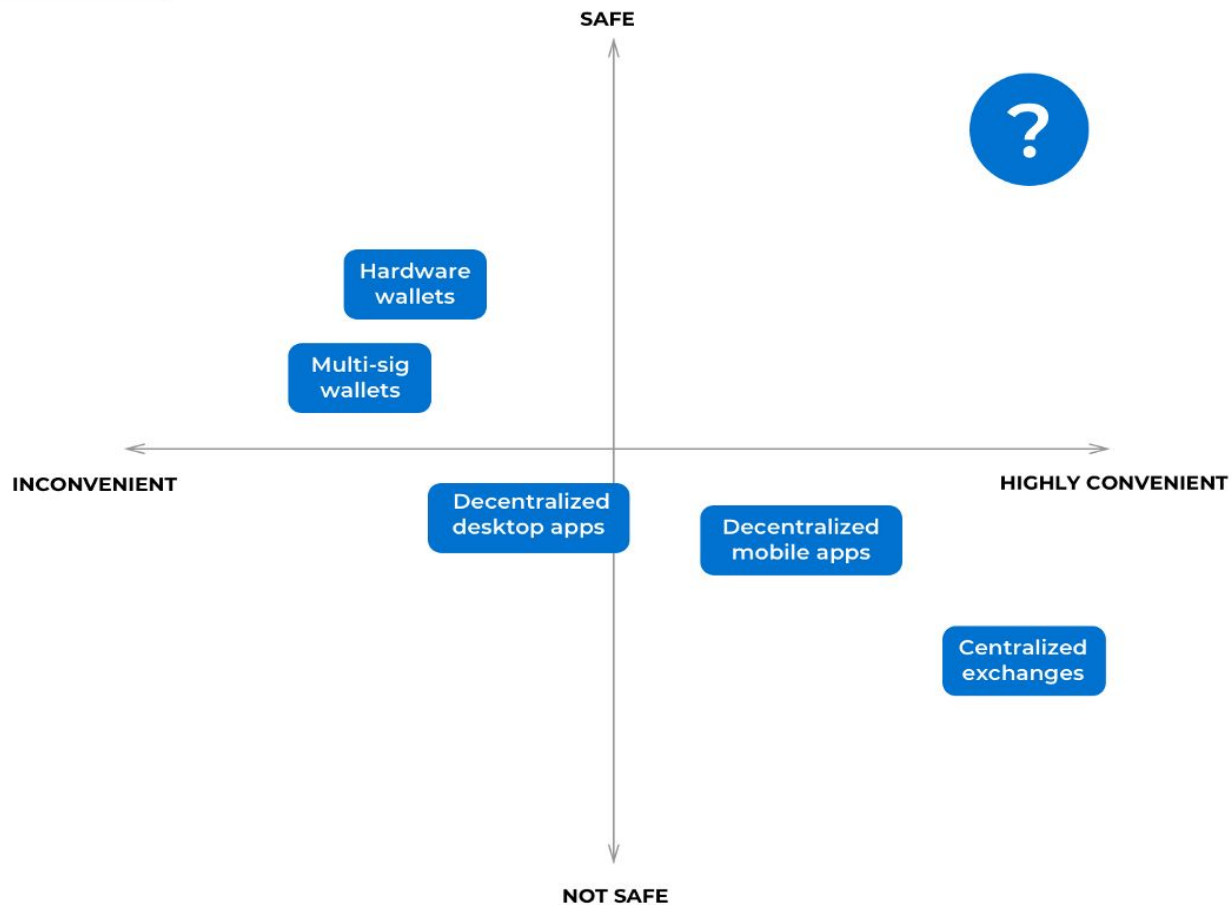
What can smart contract wallets enable?

- Improved access control:
 - Multi-factor authentication
 - Transfer limits
 - Whitelists
 - Seedless recovery
- Allow 3rd parties to submit transactions (“Meta transactions”)
 - “Gas less” transactions / let dapps pay fees
 - Pay transaction fees in ETH or ERC20 tokens
- Simplified interaction with other contracts
 - Batching of transactions



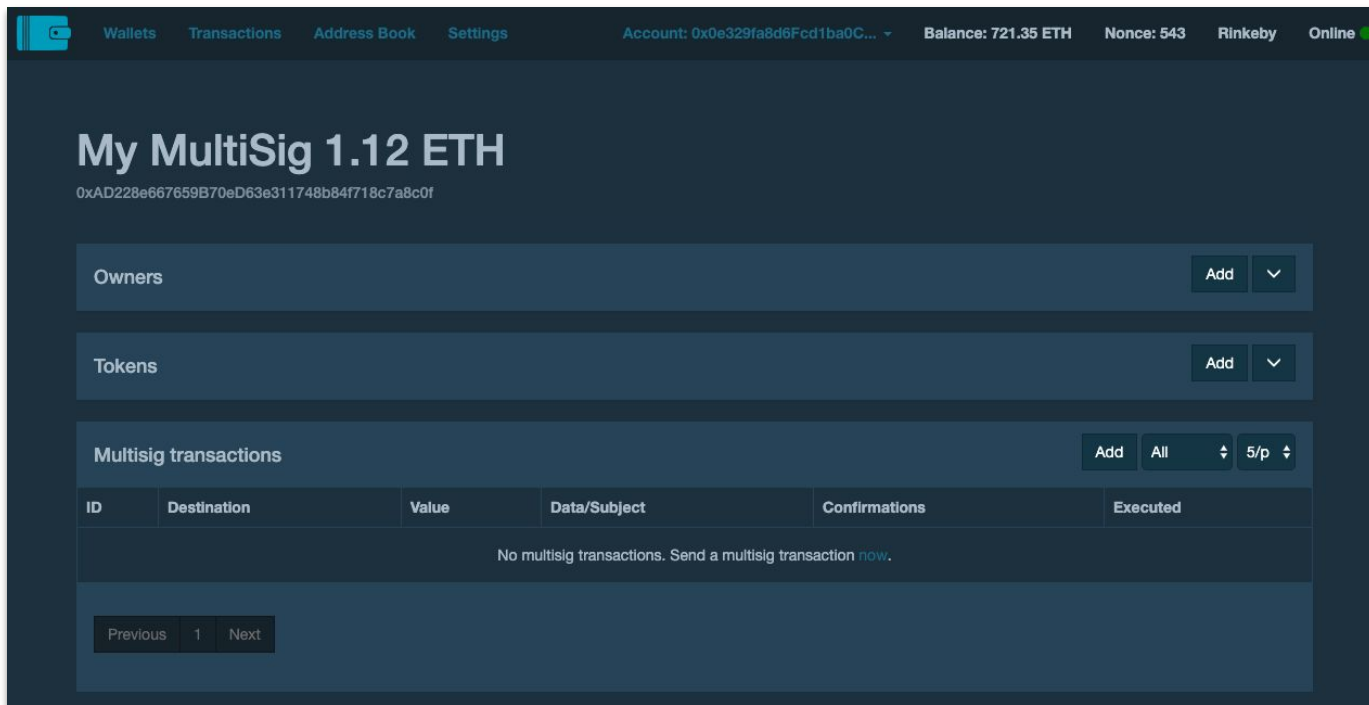
THE CURRENT STATE OF STORING FUNDS ON ETHEREUM

Convenience = UX, Mobile, Availability



Background: Gnosis MultiSig

- > 2,500 deployed instances, the top 25 alone holding more than 1.4M ETH
- Predecessor of the Gnosis Safe



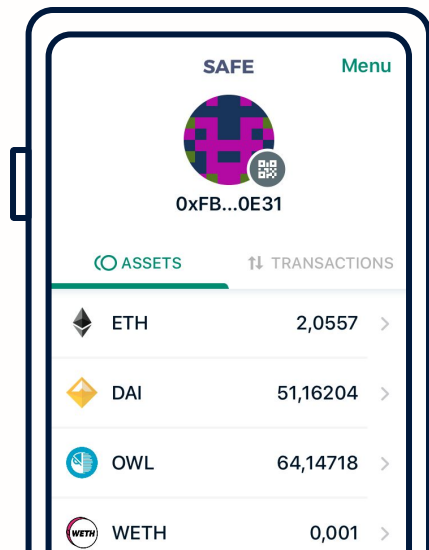
The screenshot displays the Gnosis MultiSig web interface. At the top, a navigation bar includes links for Wallets, Transactions, Address Book, and Settings. The account information shows: Account: 0x0e329fa8d6Fcd1ba0C..., Balance: 721.35 ETH, Nonce: 543, Rinkeby network, and Online status. The main content area is titled "My MultiSig 1.12 ETH" with the address 0xAD228e667659B70eD63e311748b84f718c7a8c0f. Below this are three sections: "Owners" with an "Add" button, "Tokens" with an "Add" button, and "Multisig transactions" with "Add", "All", and "5/p" controls. A table with headers ID, Destination, Value, Data/Subject, Confirmations, and Executed is shown, but it is empty. A message states: "No multisig transactions. Send a multisig transaction [now](#)." At the bottom, there are "Previous", "1", and "Next" pagination controls.

Where are we now?



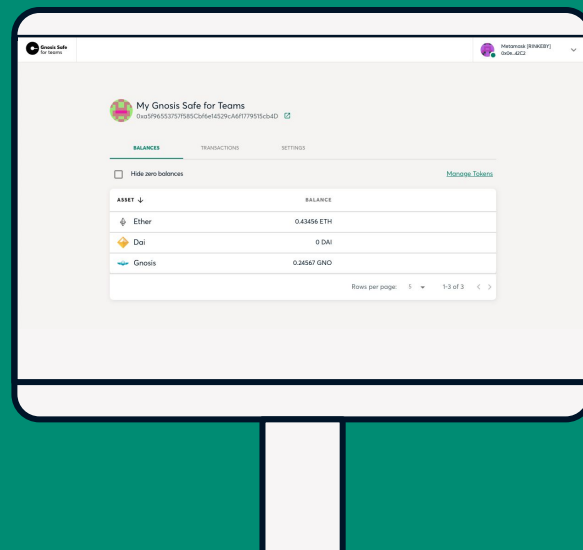
Gnosis Safe

- For individuals managing funds



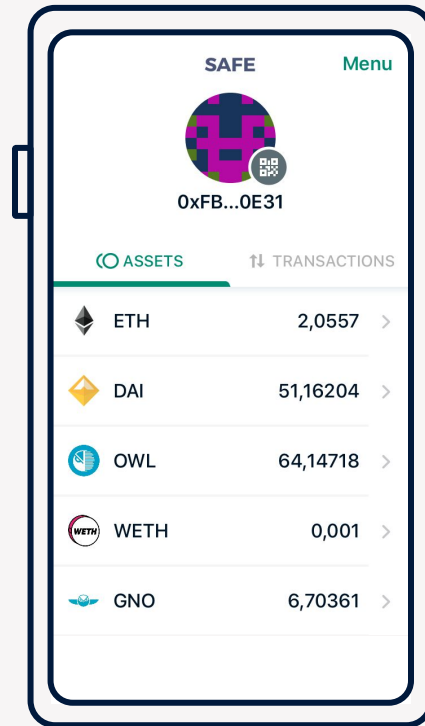
Gnosis Safe for Teams

- For teams managing funds collectively



Gnosis Safe

- For individuals managing funds
- Mobile app for Android & iOS
- 2 devices: Mobile phone + 2nd factor
 - All transactions have to be confirmed
- Key never leaves the device
- Pay transaction fees in ETH or ERC20 tokens
- Dapp interaction via WalletConnect
 - Mobile to desktop
 - Mobile to mobile



 0xFB...0E31 2,0557 ETH

↓ -0,01 ETH

 0xFB...0E31

Balance after transfer 2,0457 ETH

Network fee [?] 0,4646 OWL

Balance after transfer 63,96153 OWL

Confirmed

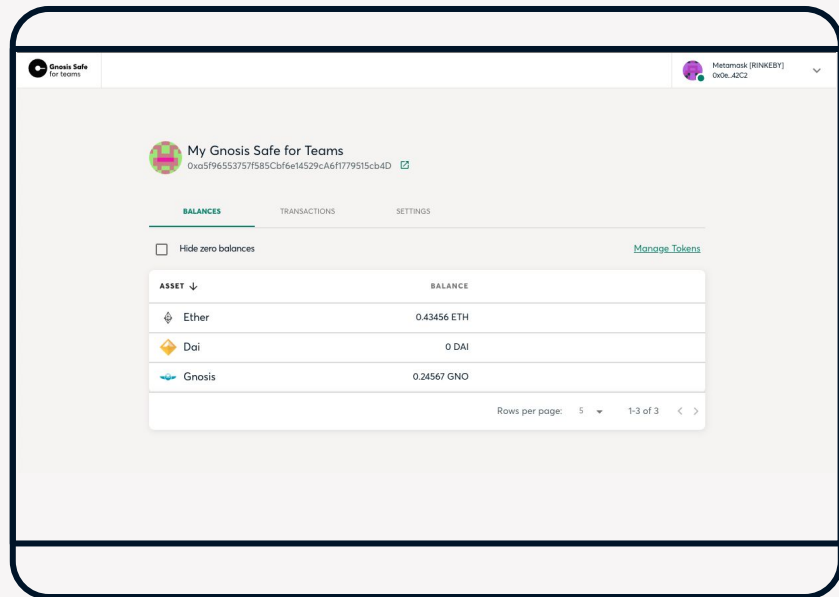
The Authenticator has approved this transaction.



Submit

Gnosis Safe for Teams

- For teams managing funds collectively
- Direct successor of the Gnosis MultiSig
- Webapp
- Flexible owner setup
- Wallet agnostic via WalletConnect
- Sign up for beta at safe.gnosis.io/teams



Replace owner

1 of 2



Review the owner you want to replace from the active Safe. Then specify the new owner you want to replace it with:

Current owner



Other owner

0x091D6309FD31f1facAB29BDF236454De23FA29a

New owner

Owner name*

Owner address*

Cancel

Next

Add new owner

What are the current challenges for smart contract wallets?



Why haven't we seen more adoption?

- Smart contract wallets are still relatively new
- Users are more comfortable with what they were first presented
- “It won’t happen to me” syndrome
- Fears over security (Parity multi-sig hack)
 - Gnosis Safe has been audited and formally verified
 - Trust will come with time
- **Full potential is not yet leveraged**

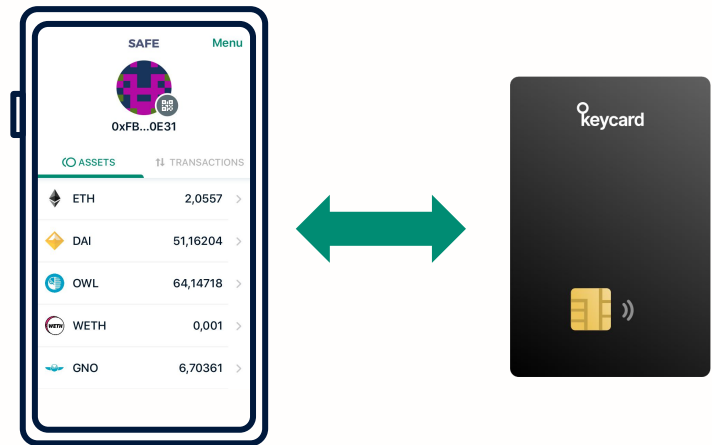


Where are we going?



- Hardware wallets
 - Status Keycard
 - Ledger Nano S/X

More convenient 2FA options

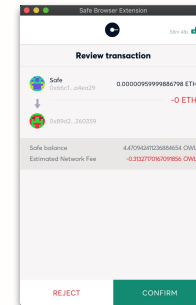
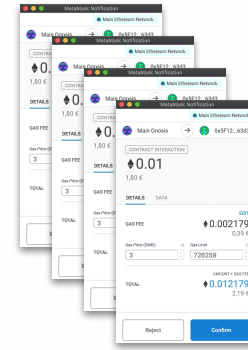


Pay transaction fees?

- Who should pay transaction fees in trustless, decentralized systems?
 - For new user onboarding?
 - Long term?

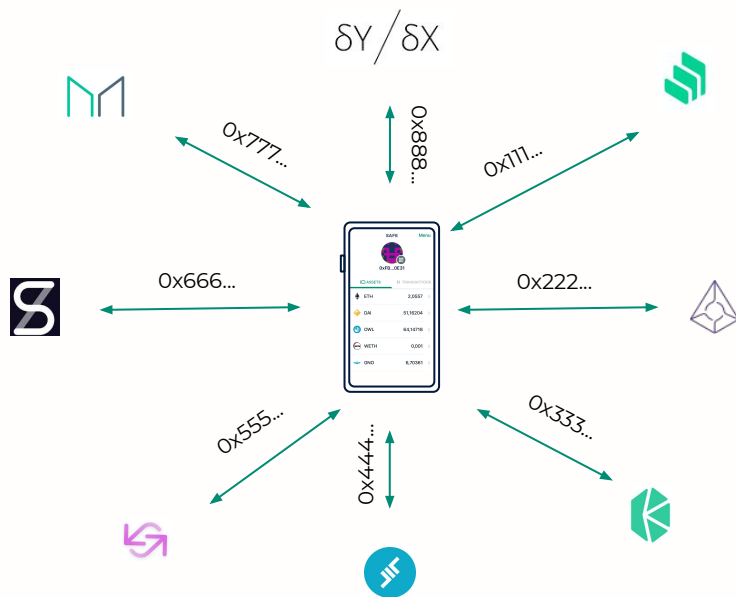


Leverage batched transactions



Contain risks of transactions

- Spending limits
- Whitelisted contracts
- Dapp specific accounts



More DeFi integrations for the Gnosis Safe for Teams

- Trading
- Lending
- Fund insurance



Crypto wallets

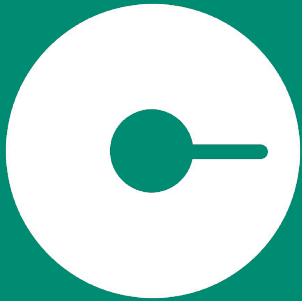
Crypto bank accounts

Crypto authenticators

- Is the term “wallet” outdated?
- Should wallets be bank accounts?
- Is earning interest a dapp?
- Should wallets just be authenticators?



Thank you!



Tobias Schubotz

@tschubotz