The Consumer Crypto Stack

The 100x unlock in consumer crypto applications.

Nicholas
@nnnnicholas
web3galaxybrain.com

October 3, 2023

The Problem

Self-custodied crypto experiences have been too hard

- High cognitive overhead
  - Gas, Tokens, Wrapped tokens, Approvals
- Need a wallet
- Desktop-oriented
- Many footguns
  - Seed phrase phishing, malicious signature requests
- Custodial solutions are not the future we want

The Consumer Crypto Stack's Values

Make crypto experiences accessible to everyone with a phone.

- Self-custody
- Mobile-first
- Application-first
- One-click transactions
- L2-first
- New-to-crypto friendly
- Lazy KYC

The Consumer Crypto Stack

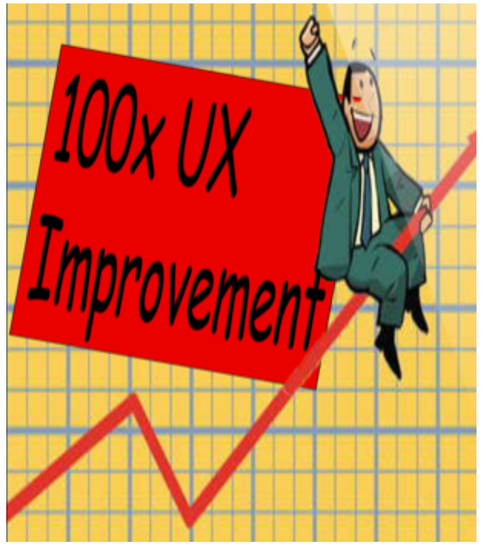
App wallets, cheap transactions, and mobile notifications

Client

1. **PWA / App**
2. **Smart Contract Wallets**

Transaction

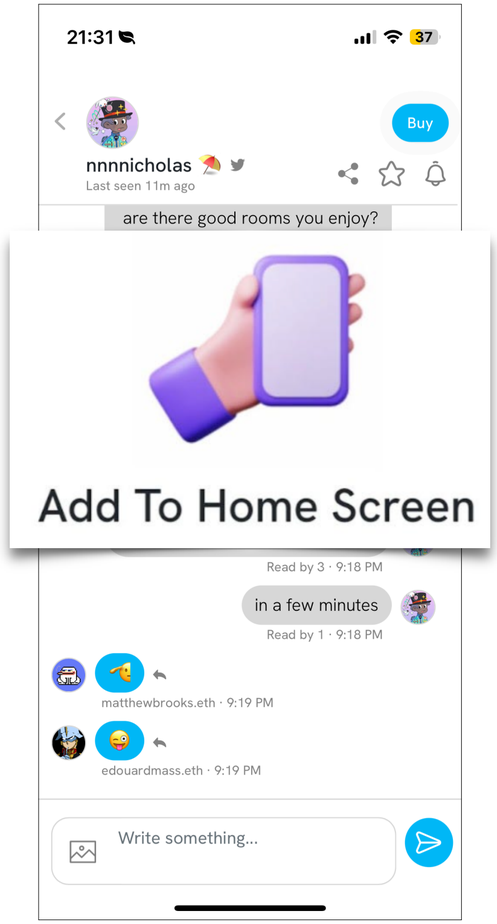
3. **L2**
4. **Gasless**



1. PWA / App

Goodbye Discrete Software Wallets (for Most New Users)

- Progressive Web Apps (PWA) on iOS are good now
  - Notifications
  - Home screen icon
- Passkeys available everywhere
  - Private public key pairs generated on-device
  - WebAuthn API in iOS, Android, Windows, Chromium, and Firefox
  - Embedded Passkey signers on AA
  - iCloud Keychain is State of the Art PK backup for 99%
  - Sessions
- EU *Digital Markets Act* will jailbreak iOS in March 2024
  - Sideloaded apps
  - No 30% tax
  - No App Store Guildelines
  - Big Q: How many people will sideload and where?



2. Smart Contract Wallets

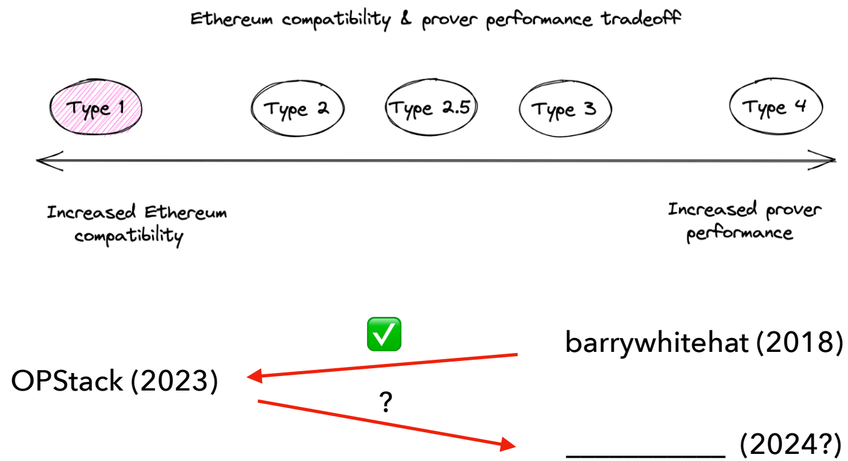
Account Abstraction (EIP-4337)

- BYO Authentication
  - Passkeys, Facebook, Gmail, Magic, SMS
  - Rotate signers without moving assets
- New ways to pay gas
  - Pay in an ERC-20
  - Sponsor by MEV, Dapp, or L2 Sequencer
- Tx Bundling
  - E.g. Approve/Swap ERC-20 in one tx
  - Batch send all assets
- Upgradeable (optional)
- Drawbacks
    - Permissions changes don’t automatically propagate to every chain
    - Passkeys’ secp256r1 verification requires EIP-7212 or MPC DKG EOA

3. L2

Suitable for consumer app experiments

- Much cheaper txs
  - L2s will fight for top apps with subsidies
- 1:1 EVM equivalent L2s “just work”
- Appchain Rollups
  - RaaS let some apps cut out markup on L1 block space
- Pendulum swinging back to specialized L2s
- Drawbacks
  - L2 decentralization is not fully baked



4. Gasless

Get transaction cost out of the way of users adoption

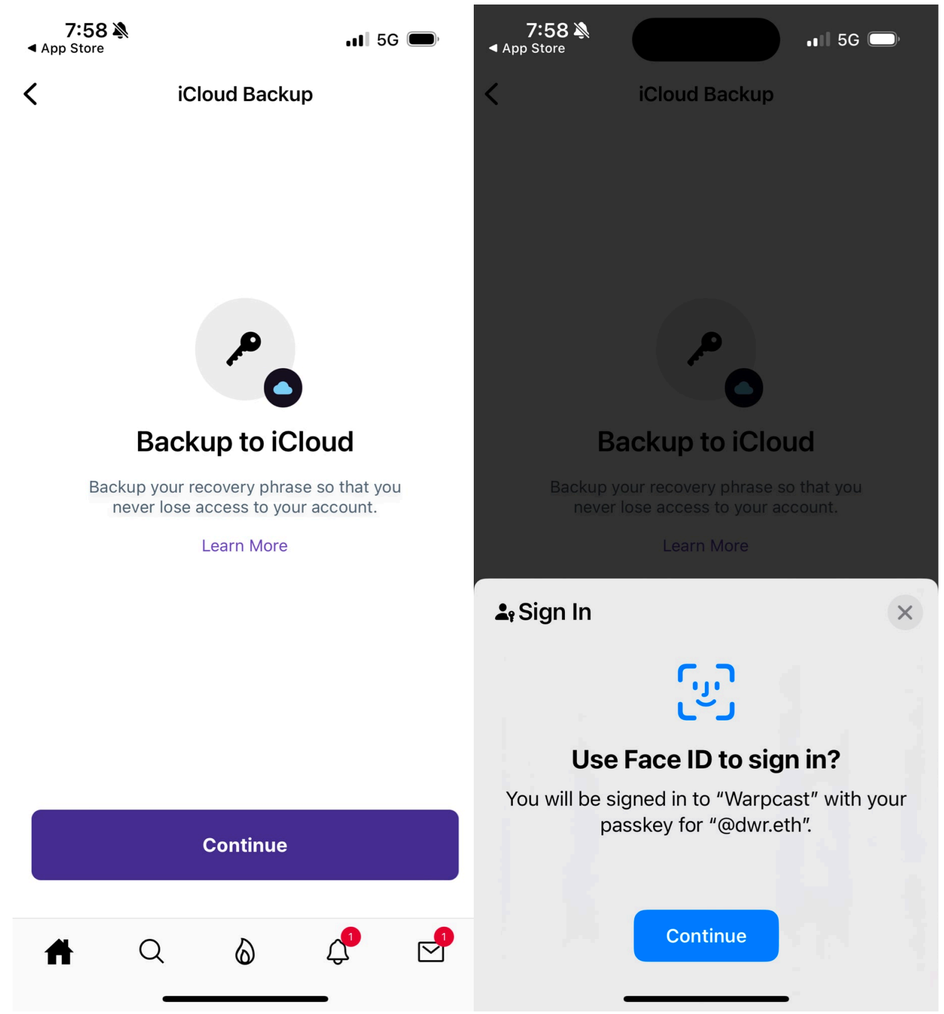
- Goal: Delay onramping friction
- Sponsored transactions
  - Paid for by Paymasters, Sequencers, or MEV
- Lazy maxi
  - Offchain orderbook of Intents
  - Paid for by Intent “Taker”

nnnnicholas irl

Case Study: Warpcast

Farcast Recovery Phrase in iCloud Keychain

- Sign in with FaceID
- Store Farcaster EOA recovery phrase in largeBlob alongside Passkey
- Passkeys + largeBlob can be backed up to iCloud Keychain
- If user loses their device, they can recover their Farcaster signing key to a new device thanks to iCloud Keychain



Warpcast October 2023

The Consumer Crypto Stack

App wallets, cheap transactions, and mobile notifications

1. **PWA / App**
2. **Smart Contract Wallets**
3. **L2**
4. **Gasless**

Consumer crypto is here.

I am hiring.

Subscribe to web3galaxybrain.com.

@nnnnicholas on X

@nicholas on W