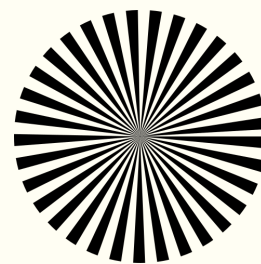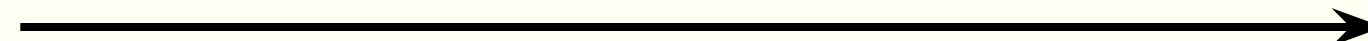# WALLETS, PLATFORMS... WTF?

It's easy to miss how fast the wallet game is changing if you're not paying attention to shifting platform economics.

- What does it mean for wallets to "own" their customers?
- What do wallets *owe* their customers in return?
- Are we ready for wallets to be as interchangeable as browsers?
- Who gains from raising UX standards?

01/15

CROSS-PLATFORM WALLETS WEN?

1. INTRO: BROWSER WARS 3.0

2. THE REDHEADED STEPCHILD

3. SOME PATHS FORWARD:

   COINBASE, METAMASK, WALLET CONNECT, PENUMBRA, C.A.K.E.

4. ...PROFIT?

← Slides at

https://bit.ly/ wallets_ platforms_ wtf

PRESENTED BY BUMBLEFUDGE @WEB3SUMMIT BERLIN, AUG 2024

CROSS-PLATFORM WALLETS WEN?
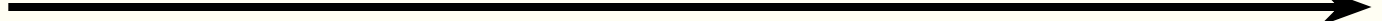
1. INTRO: BROWSER WARS 3.0

2. THE REDHEADED STEPCHILD

3. SOME PATHS FORWARD:

   COINBASE, METAMASK, WALLET CONNECT, PENUMBRA, C.A.K.E.

4. ...PROFIT?

← Slides at

https://bit.ly/ wallets_ platforms_ wtf

PRESENTED BY BUMBLEFUDGE @WEB3SUMMIT BERLIN, AUG 2024

#GOALS

- Community venue, open governance
- Open-source, public specifications that enable and encourage chain-agnostic engineering and UX
- CAIPs - Improvement Proposals spanning multiple systems
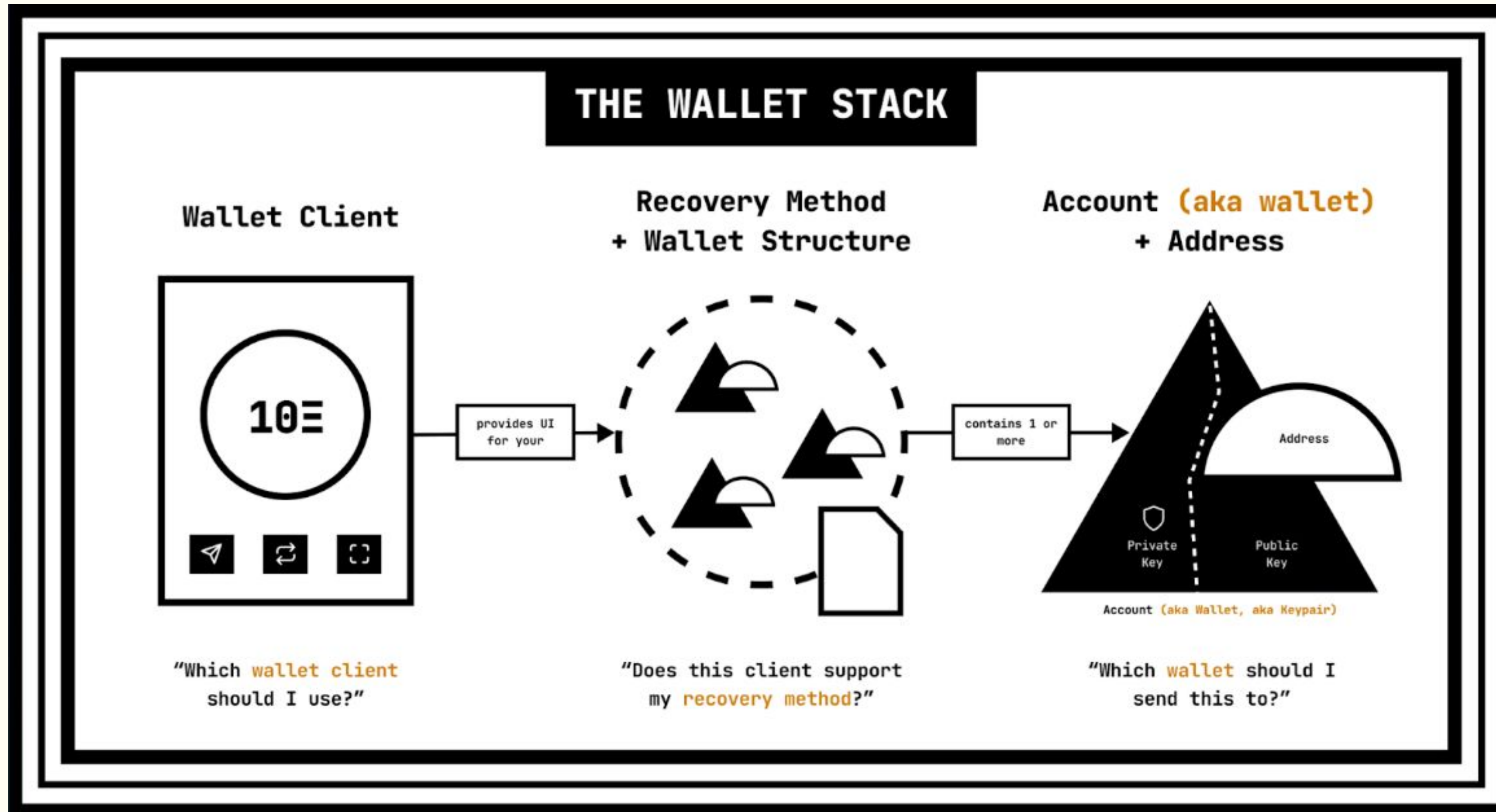- CANs - Documentation of each L1's RPC & addressing syntaxes *for external consumption*

#VISION

- User Agency > Sovereignty
- Buidl for an open web[3] that comes after the "browser wars" era
- Think of web3 as a cohesive design space and meta-platform, not competing VMs & platforms

YO WHY ARE THEY SHARING RESOURCES

WITH NO PROFIT INCENTIVE

03/15

C.A.S.A.

THE WALLET STACK

Wallet Client

provides UI for your

Recovery Method + Wallet Structure

contains 1 or more

Account (aka wallet) + Address

Address

Private Key   Public Key

Account (aka Wallet, aka Keypair)

"Which wallet client should I use?"

"Does this client support my recovery method?"

"Which wallet should I send this to?"

04/15

NEUTRAL WEB PLATFORM (ONCE STANDARDIZED, ANYWAYS)

HTTP Request

Accept-Language: en-US
Content-Length: 423
User-Agent: [...] **Chrome/71.0** [...]
[...]

User Agent

USER SPACE

Server

BUSINESS LOGIC

PayPal

ANYONE WANNA BOLT ON PAYMENTS?

Your browser is not currently supported.

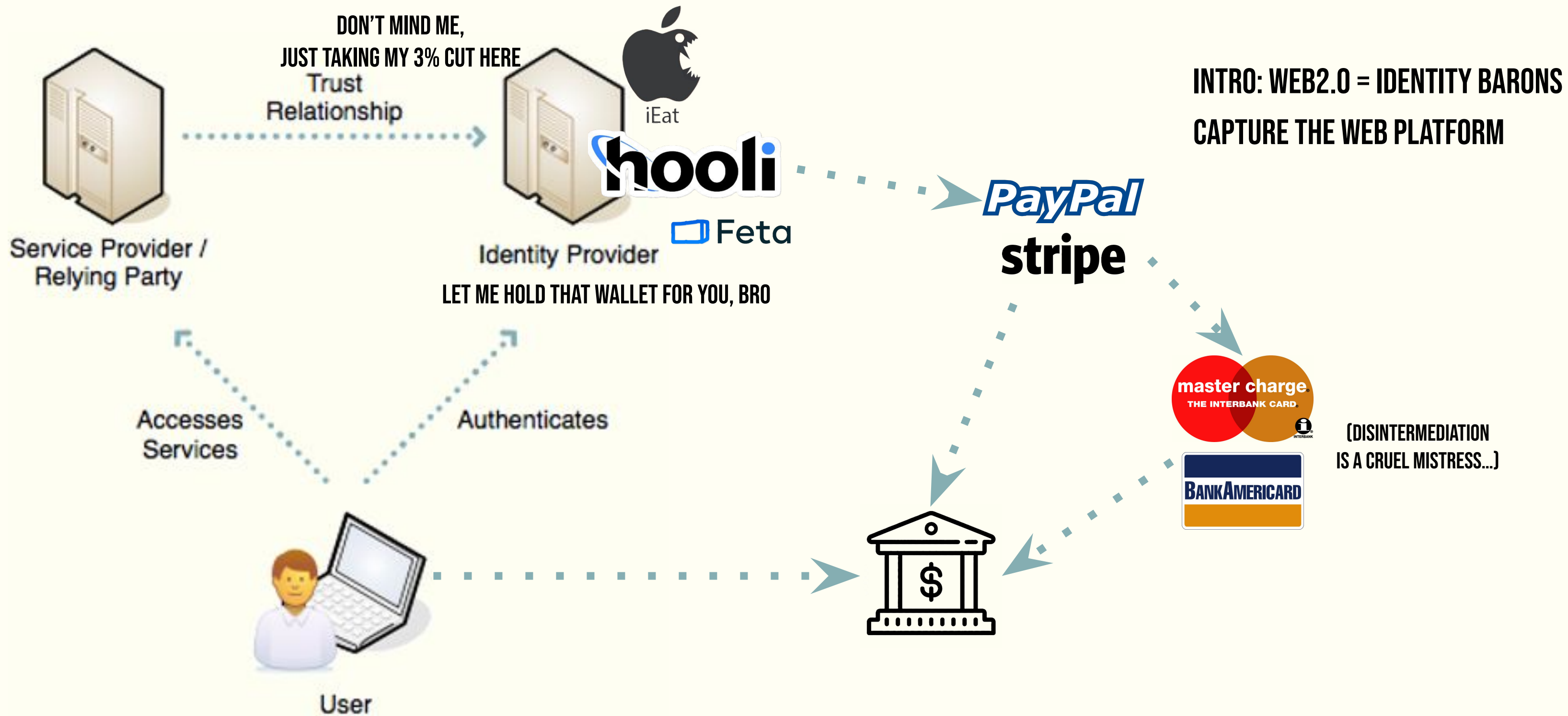Please use the latest version of Chrome, Opera, Firefox, or Safari.

UNTIL BROWSERS COULD AGREE ON STANDARDIZED CORE FEATURES,
    EACH BROWSER WAS ITS OWN OVERLAPPING BUT DISTINCT PLATFORM MATCHMAKING SURFERS 🏄 TO WAVES 🌊

WHAT ARE THE CORE UX AND SECURITY FEATURES OF THE WEB3 PLATFORM?
ARE WE WARNING USERS IF THEIR WALLETS DON'T HAVE THEM?

05/15

C.A.S.A.

DON'T MIND ME,
JUST TAKING MY 3% CUT HERE

Trust
Relationship

iEat

hooli

Feta

Service Provider /
Relying Party

Identity Provider

LET ME HOLD THAT WALLET FOR YOU, BRO

INTRO: WEB2.0 = IDENTITY BARONS

CAPTURE THE WEB PLATFORM

PayPal
stripe

master charge
THE INTERBANK CARD

BANKAMERICARD

(DISINTERMEDIATION
IS A CRUEL MISTRESS...)

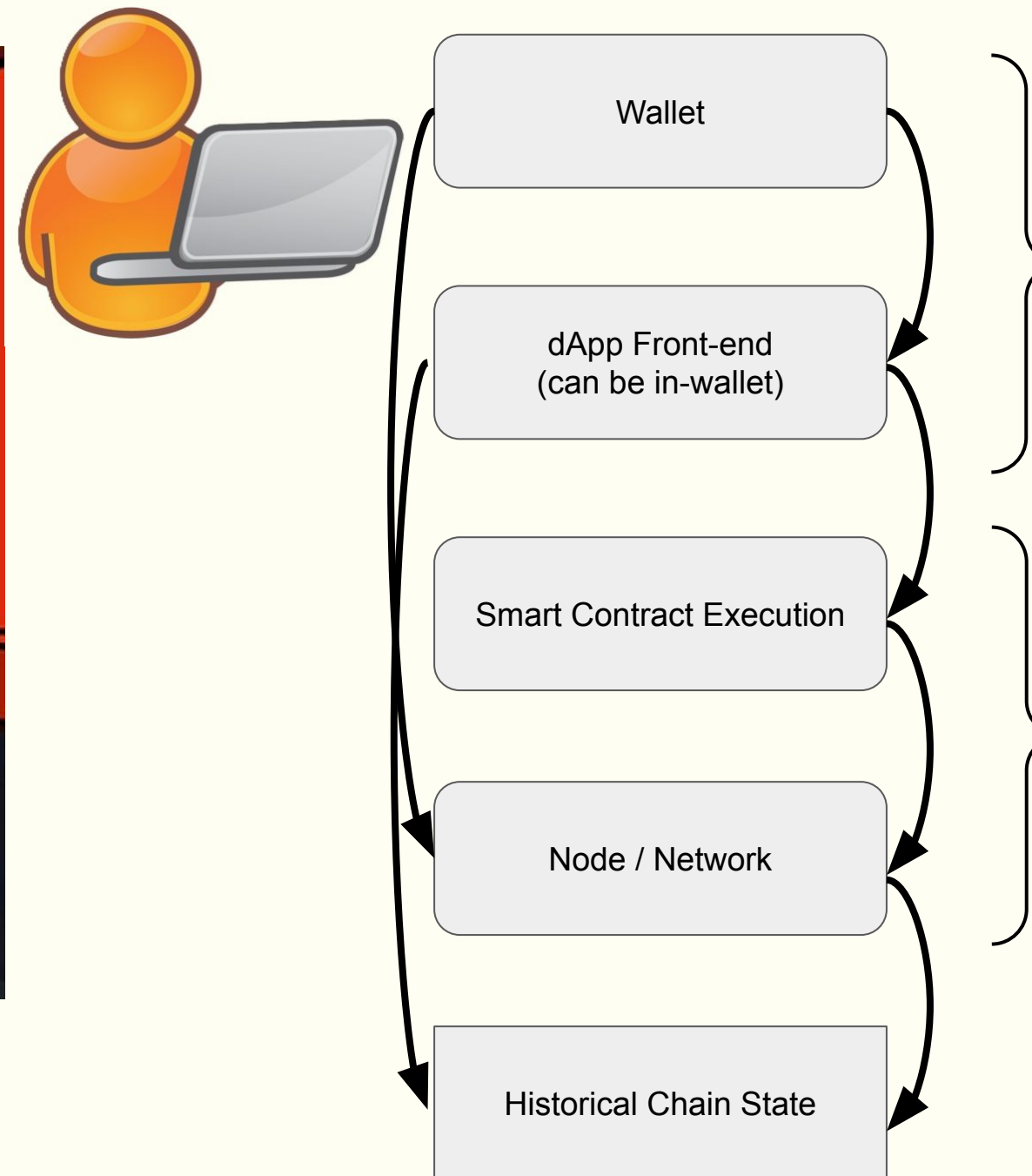Accesses
Services

Authenticates

User

BOLTING ON AN "IDENTITY LAYER" TO THE INTERNET CREATED THE MOST POWERFUL AND PROFITABLE MONOPOLIES IN HISTORY

HEALTHY MARKET ENJOYERS CALL THIS A FAILURE MODE, NOT A COMMON CARRIER MODEL

06/15

SEE: THE VERGE'S ANTITRUST PAGE OR WALLET NEWS; DECENTRALIZED.ID; K. PISTOR

C.A.S.A.

Wallet

dApp Front-end
(can be in-wallet)

Smart Contract Execution

Node / Network

Historical Chain State

USER-SPACE AND BUSINESS LOGIC ARE BOTH
PRECARIOUSLY SQUATTING IN THE
CENSORABLE, VULNERABLE, AND CAPTURED
WEB2 PLATFORM

WEB3 IS MOSTLY PAYING ATTENTION
TO WHAT IT CAN CONTROL, HERE,
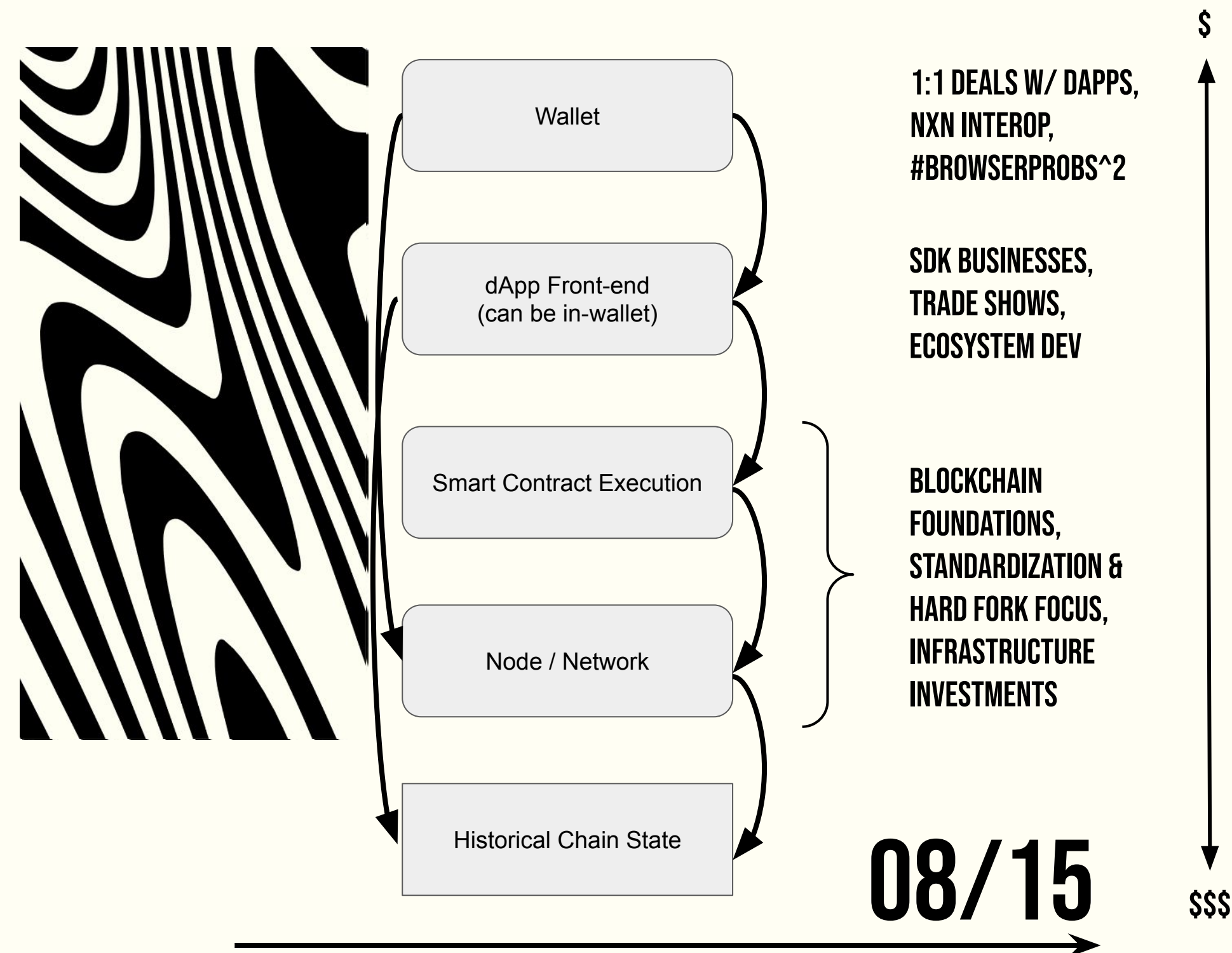ON VERY SHORT TIMELINES

07/15

SEE ALSO: WEB2 VULNS, NETLIFY CVE, WEB3AUTH (ARVIX), ETC ; CAIP-282 (PR); EIP-6963

PROGRESS... SOME DAY?

Wallets are the hardest layer to improve:

- **Coordination**: what market actor is incentivized to coordination adoption of wallet features or flows?

- **Compliance risk**: Wallets anonymizing their users keeps dapp liability low and protocol neutral, but they are a kind of fiduciary, tricky relationship

- **Control points:** Mobile OS app stores, browser security models, and soon even browser extension registries can all effectively cripple a wallet

- **Consolidation**: Vertical integration (dapps buying or provisioning wallets) disincentivizes wallet progress
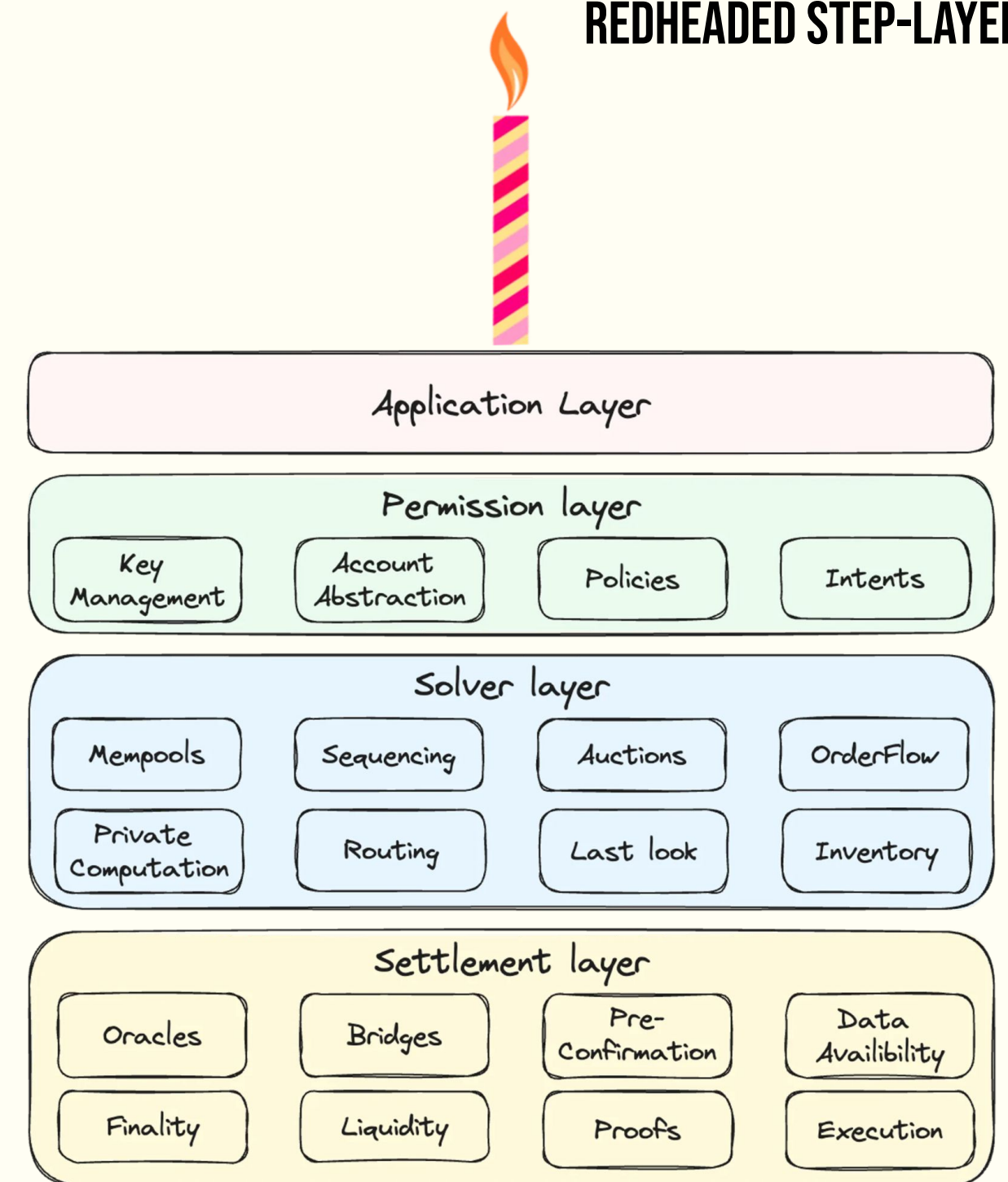
"THE MARKET WILL SORT WALLETS OUT" – EVERYONE SINCE 2015

$

Wallet

1:1 DEALS W/ DAPPS, NXN INTEROP, #BROWSERPROBS^2

dApp Front-end (can be in-wallet)

SDK BUSINESSES, TRADE SHOWS, ECOSYSTEM DEV

Smart Contract Execution

Node / Network

BLOCKCHAIN FOUNDATIONS, STANDARDIZATION & HARD FORK FOCUS, INFRASTRUCTURE INVESTMENTS

Historical Chain State

08/15

$$$

SRC: LOL, ME; SEE ALSO ETH WALLET WG PROPOSAL

TODAY, SOLVERS & INTENTS!

Compare the amount of business-model and technological innovation everywhere below the individual user... which is even reaching into the green zone (theoretically user-space).

We have so over-engineered the concept of "intents" that we forgot the legal meaning of the word, and the "meaningful consent" needed for **any** of this stuff to be scalable, street-legal for the next billion, or ethical.

Wallets need to be where permission and consent are enforced... the wallet is the end-user's **trusted advocate**.
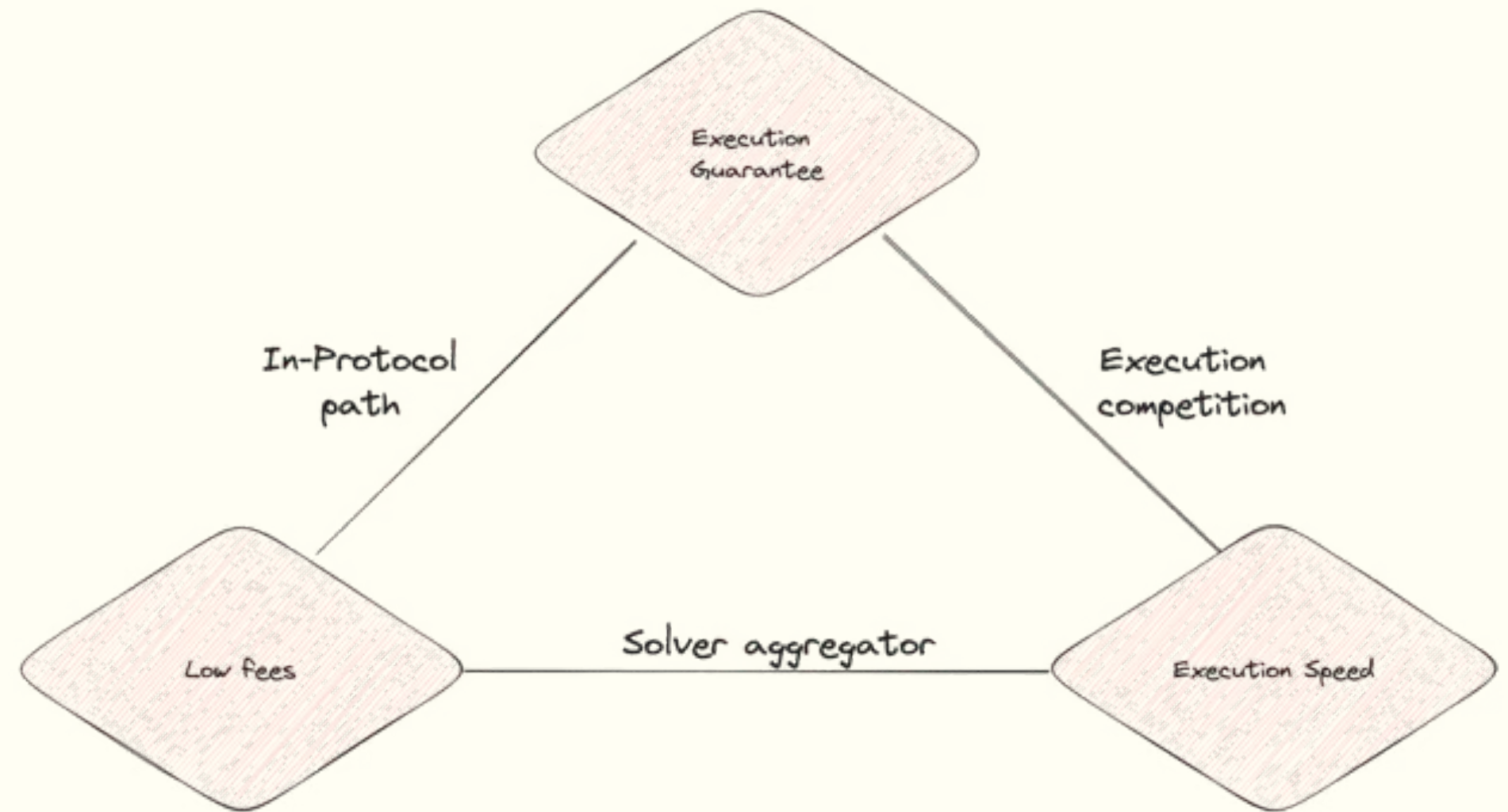
Application Layer

Permission layer

| Key Management | Account Abstraction | Policies | Intents |

Solver layer

| Mempools | Sequencing | Auctions | OrderFlow |
| Private Computation | Routing | Last look | Inventory |

Settlement layer

| Oracles | Bridges | Pre-Confirmation | Data Availability |
| Finality | Liquidity | Proofs | Execution |

09/15

SRC: FRONTIER.TECH; COMPARE TO ADTECH SOLVER DSLS

FRONTIER.TECH:

C.HAIN A.BSTRACTION

K.EY E.LEMENTS

When you're holding a DeFi solver, everything looks like an opportunity for arbitrage and routing hijinx.
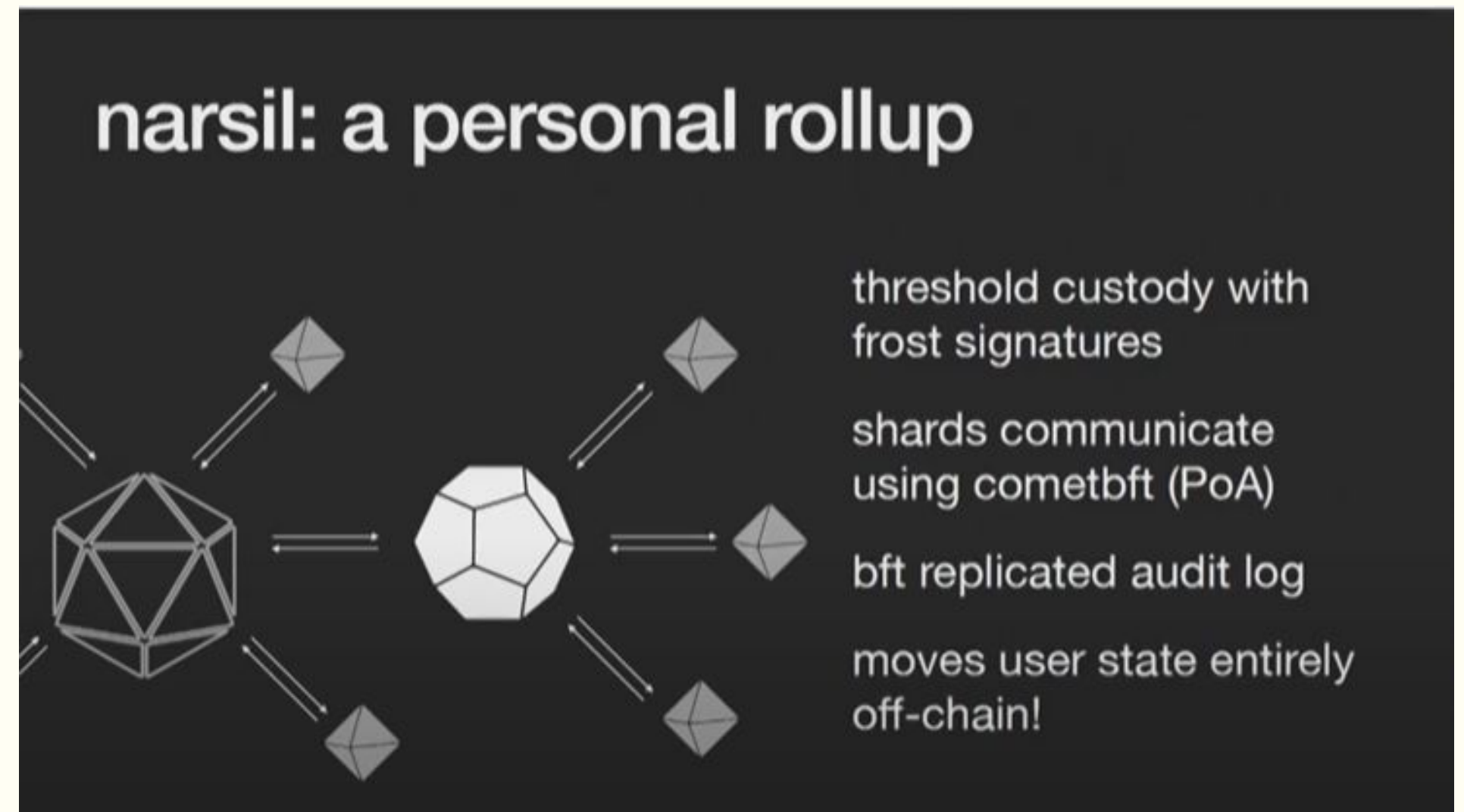

10/15

PENUMBRA:

PER-USER ROLLUPS?!

The end-state of all onchain maximalism is all human activity is made legible to nodes, even if proved off-chain and managed by squishy human wallets off-screen
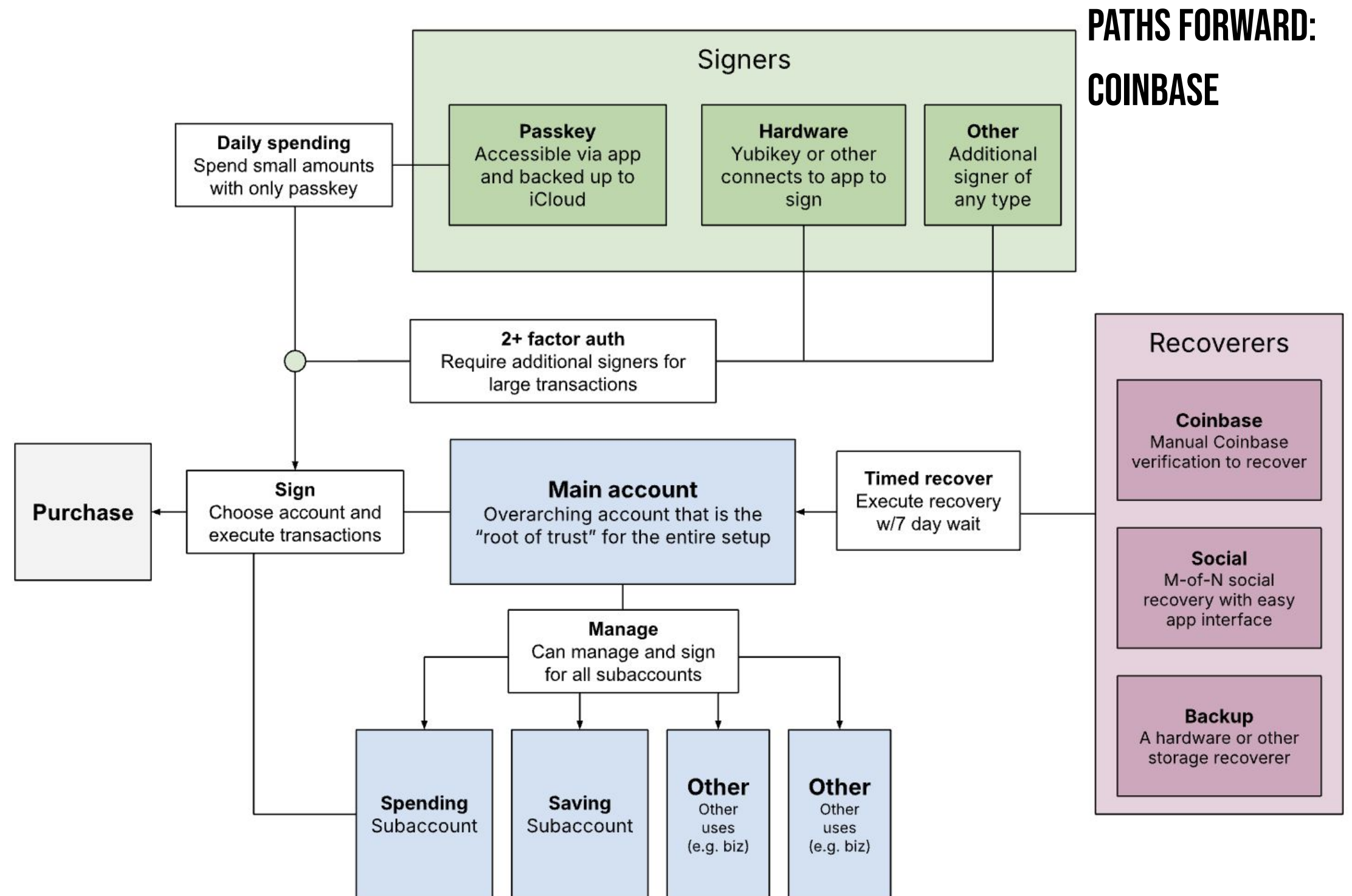
FROM THE TALK "SHIELDED TRANSACTIONS ARE ROLLUPS", ETHCC 2023
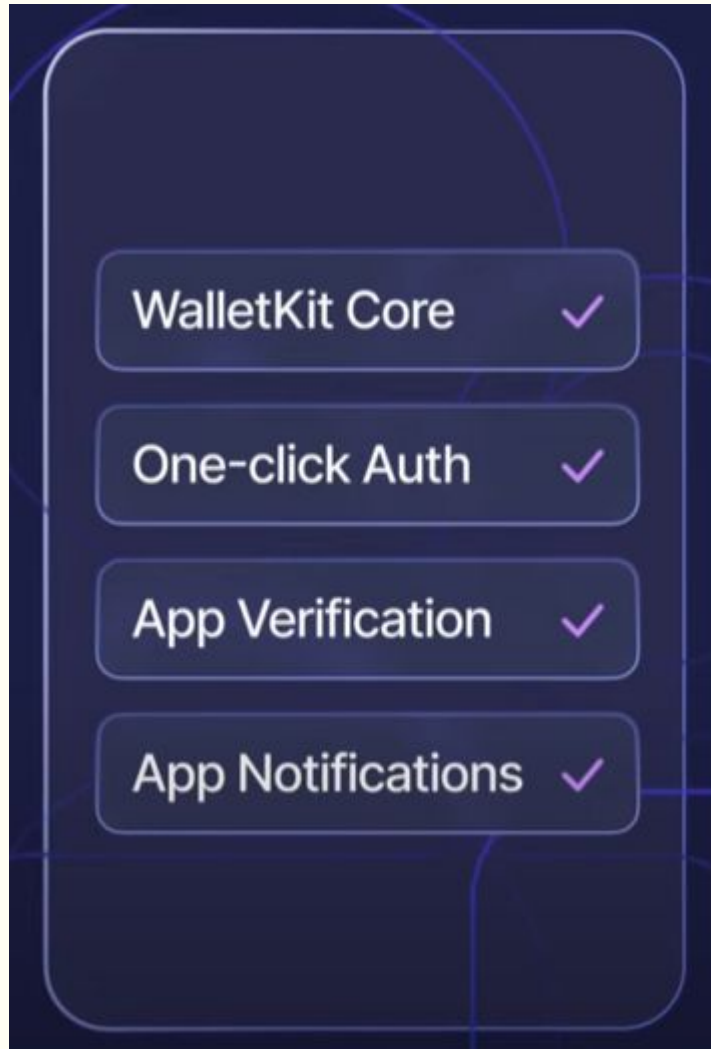

narsil: a personal rollup

threshold custody with frost signatures

shards communicate using cometbft (PoA)

bft replicated audit log

moves user state entirely off-chain!

11/15

C.A.S.A.

COINBASE:
THE EVERYTHING APP

Props to team #standardOil, honestly

Signers

Daily spending
Spend small amounts with only passkey

Passkey
Accessible via app and backed up to iCloud

Hardware
Yubikey or other connects to app to sign

Other
Additional signer of any type

2+ factor auth
Require additional signers for large transactions

Purchase

Sign
Choose account and execute transactions

Main account
Overarching account that is the "root of trust" for the entire setup

Timed recover
Execute recovery w/7 day wait

Recoverers

Coinbase
Manual Coinbase verification to recover

Social
M-of-N social recovery with easy app interface

Backup
A hardware or other storage recoverer

Manage
Can manage and sign for all subaccounts

Spending
Subaccount

Saving
Subaccount

Other
Other uses (e.g. biz)

Other
Other uses (e.g. biz)

12/15

WALLET CONNECT:

WALLETKIT SDK + CERTIFIED
= UX BASELINE SCRUM

By giving wallets an SDK of standardized features that dapps are demanding, a "baseline" of wallet UX features and flows can be coordinated...cooperatively!
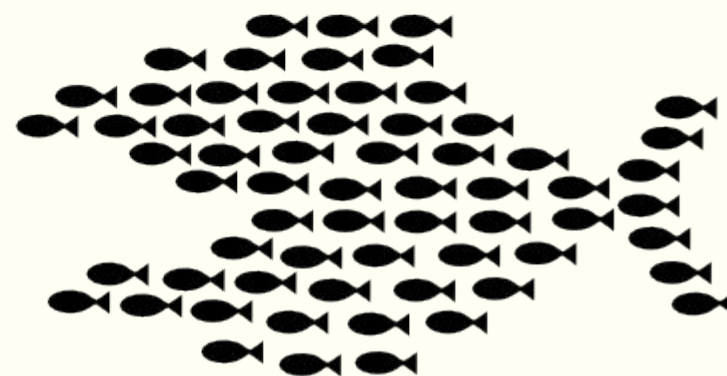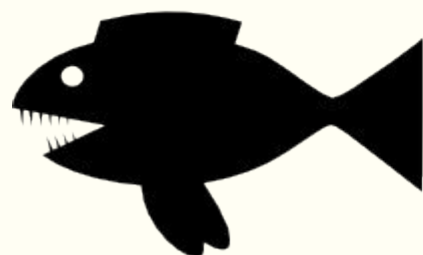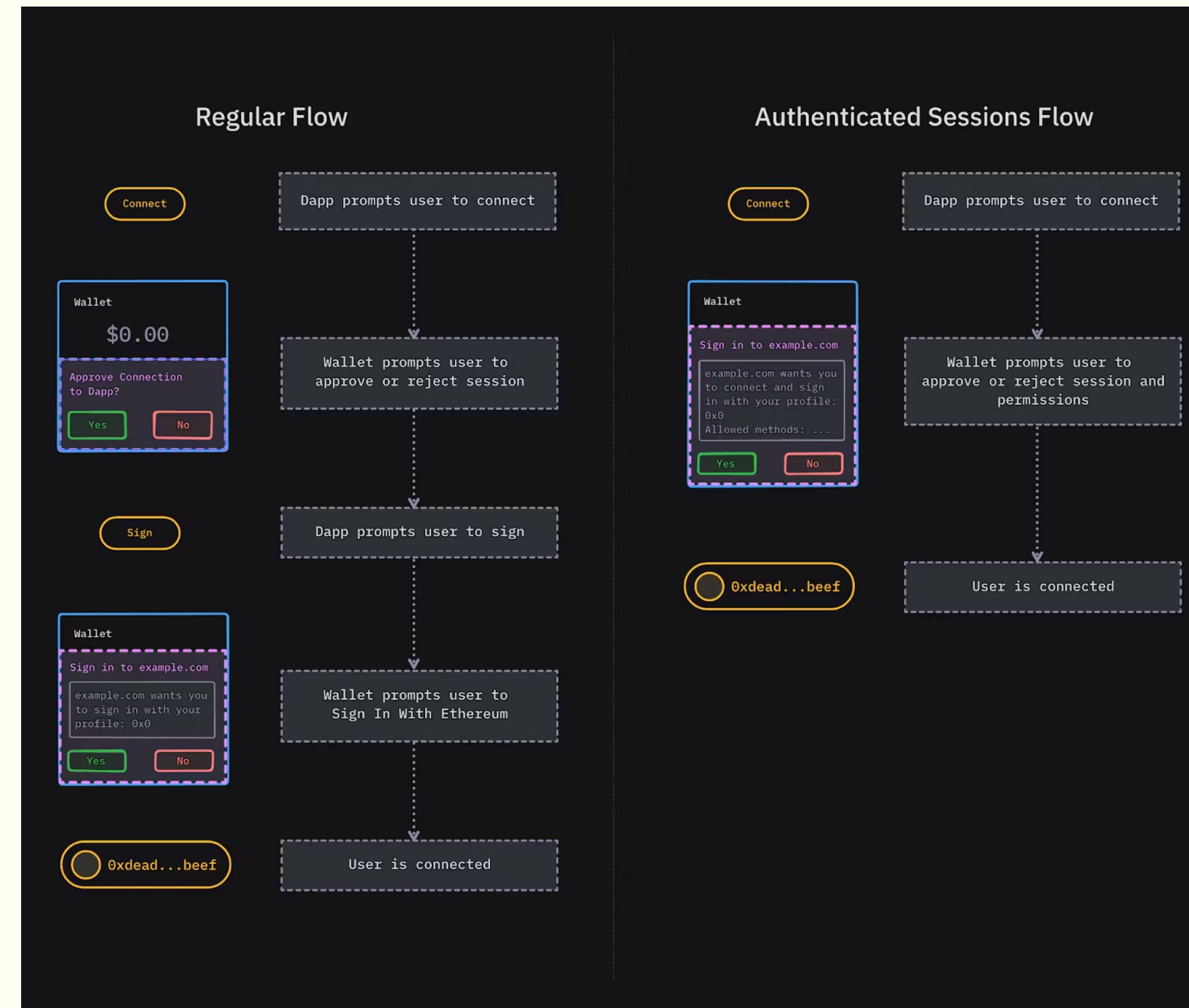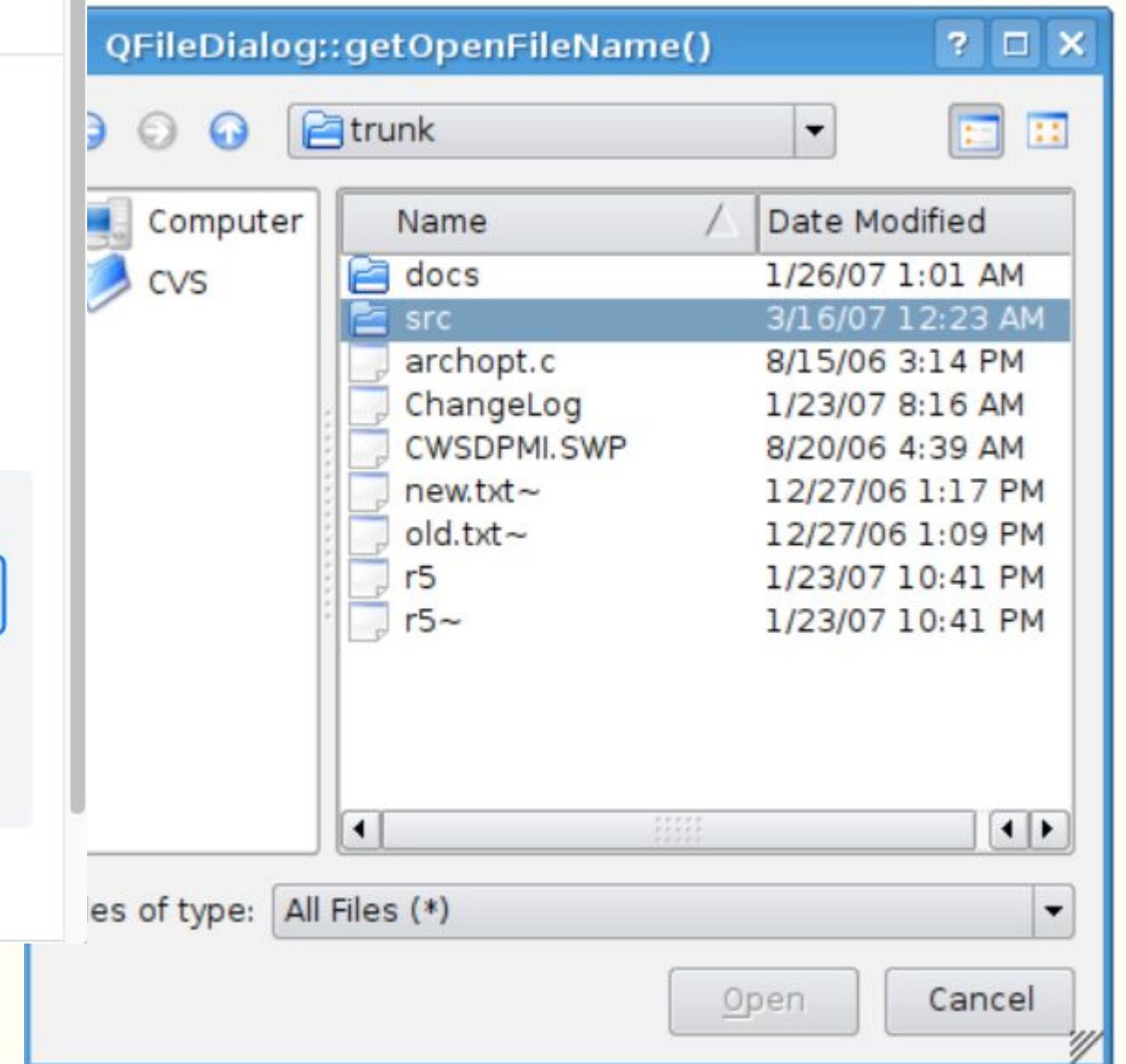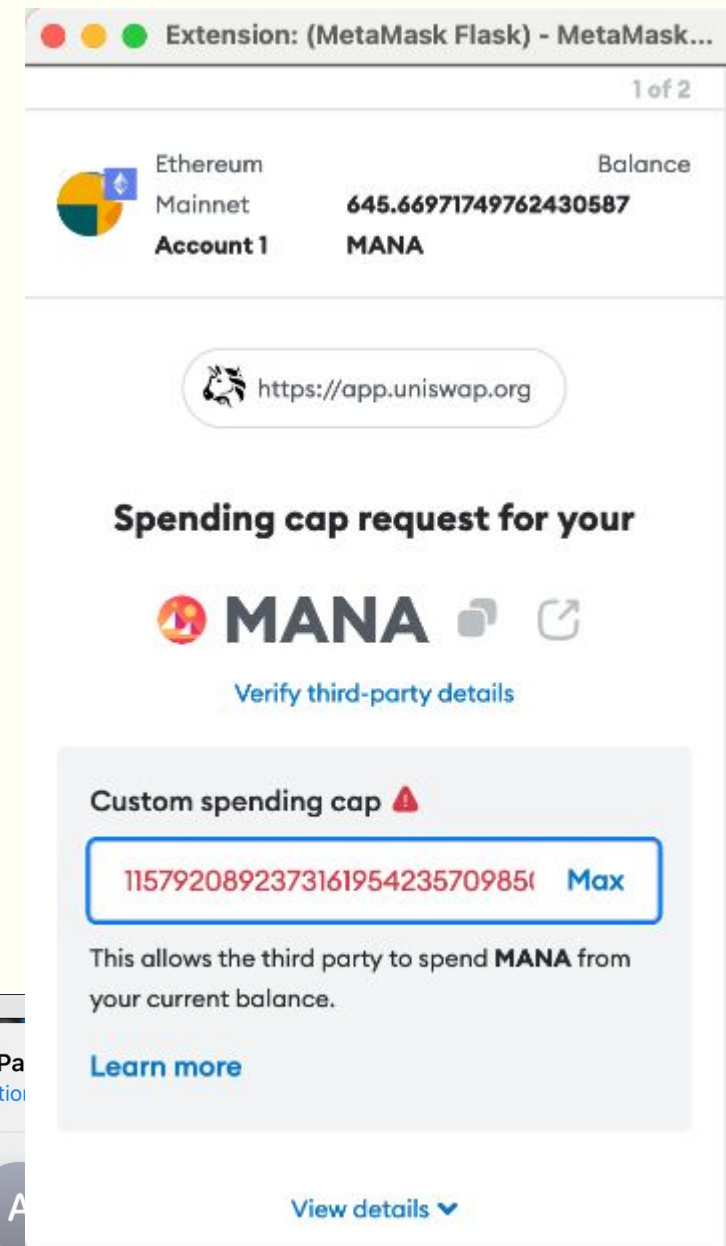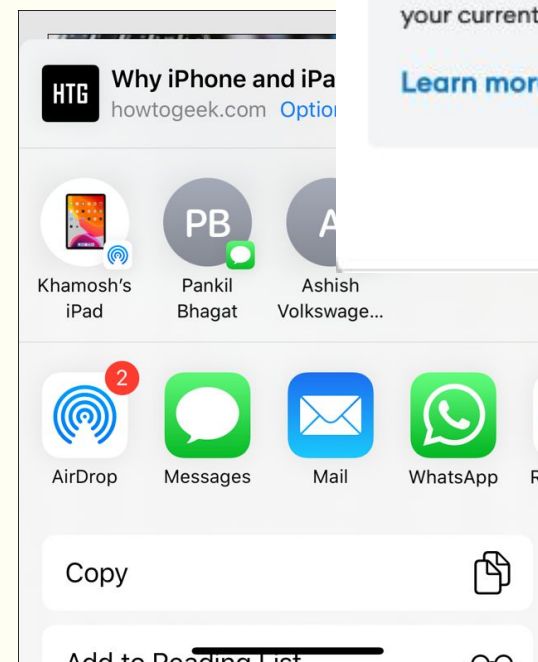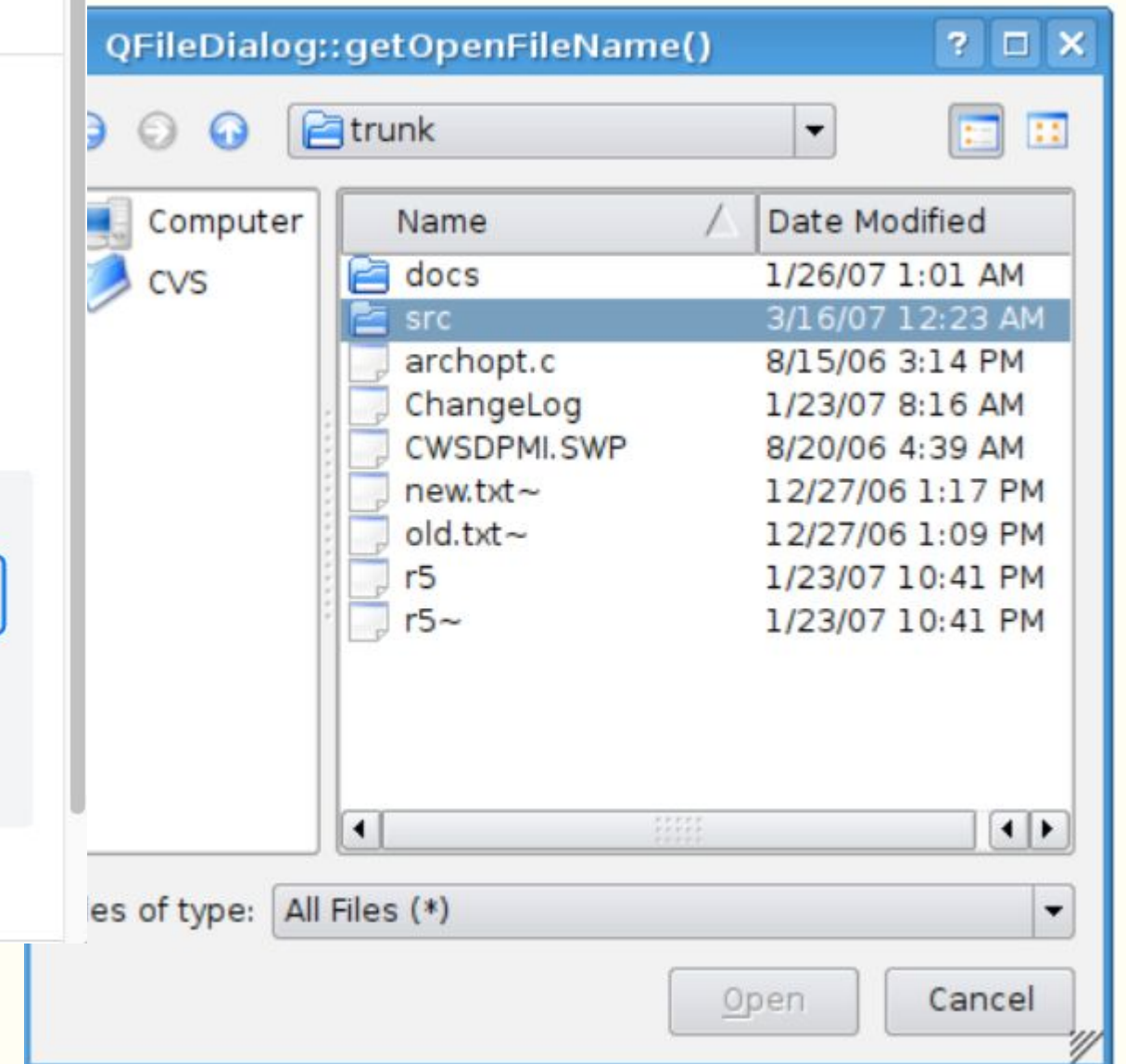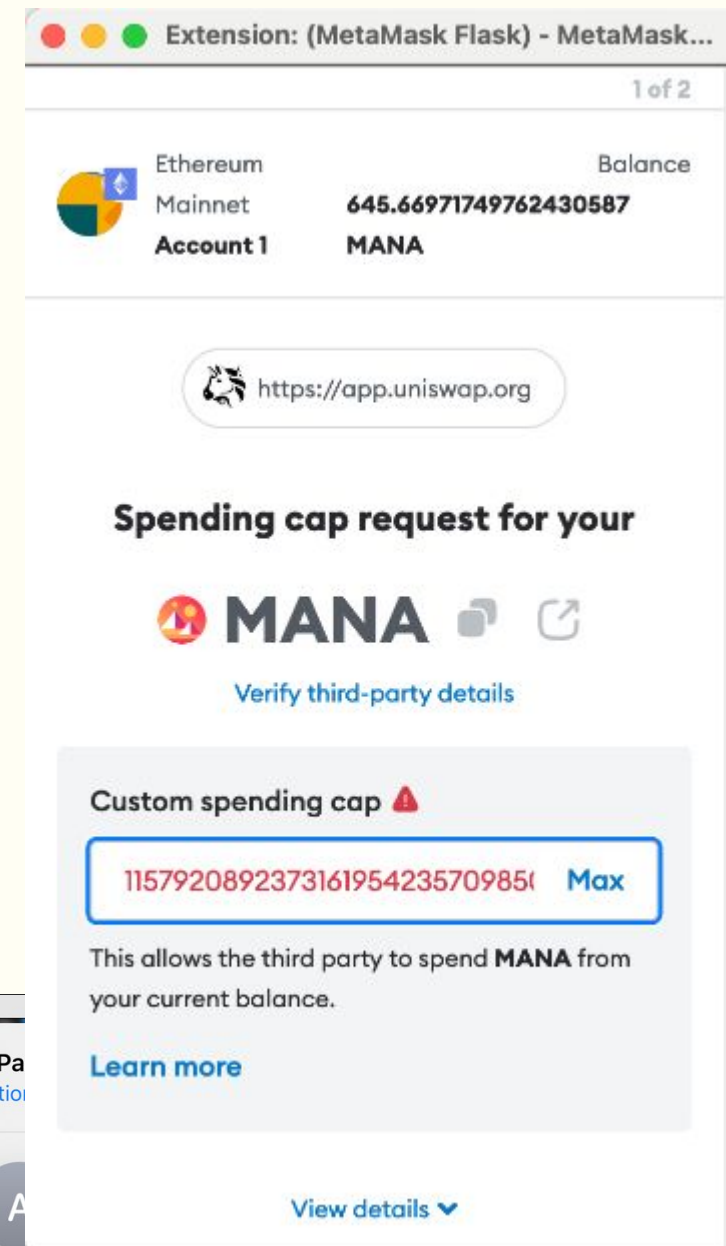

13/15

METAMASK:

ASSET ABSTRACTION

Will the next billion *want* to know, much less *manage*, most of their 200 addresses or even know what chain anything is "on"?
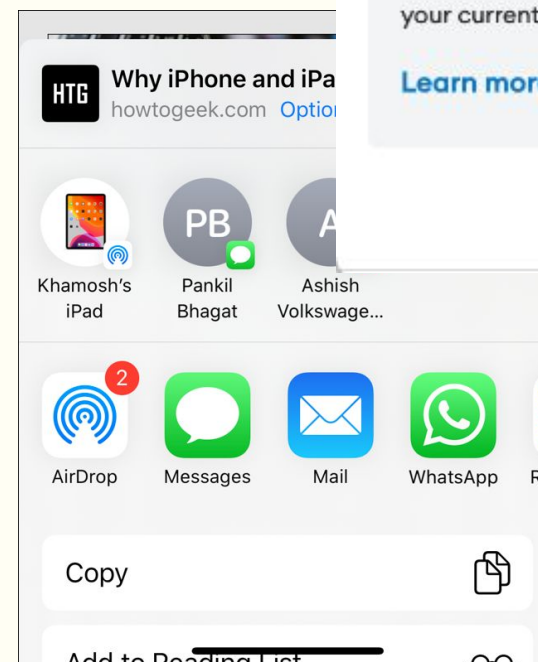
METAMASK:

ASSET ABSTRACTION

Will the next billion *want* to know, much less *manage*, most of their 200 addresses or even know what chain anything is "on"?

14/15

THE END

Koans to ponder:

- What does it mean for wallets to "own" their customers?
- What do wallets *owe* their customers in return?
- Are we ready for wallets to be as interchangeable as browsers?
- Who gains from raising UX standards?

@chainagnostic

chainagnostic.org

15/15