Taylor Monahan

MetaMask

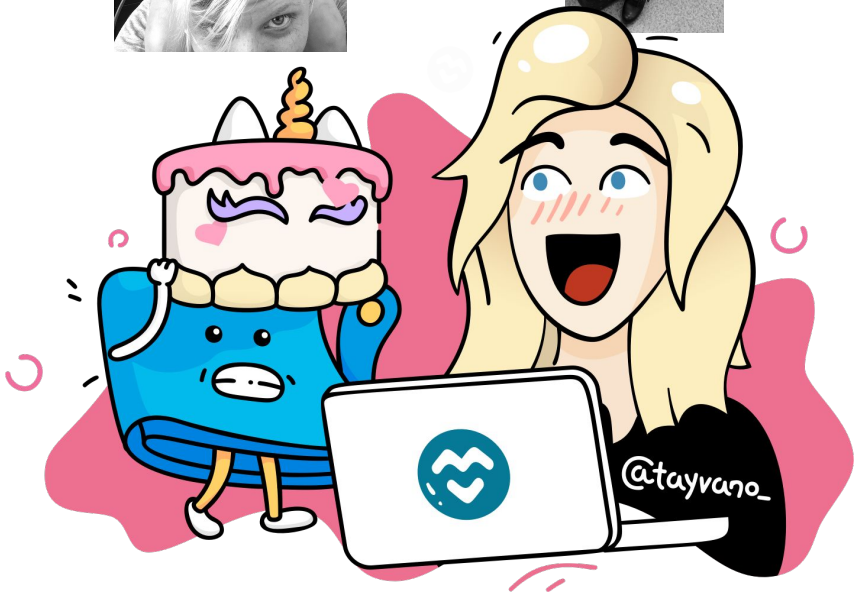
The Original Sin

Our early choices shaped the world we live in today.

What's worth changing for tomorrow?

Who am I?

Taylor Monahan



Been in this space since 2013.

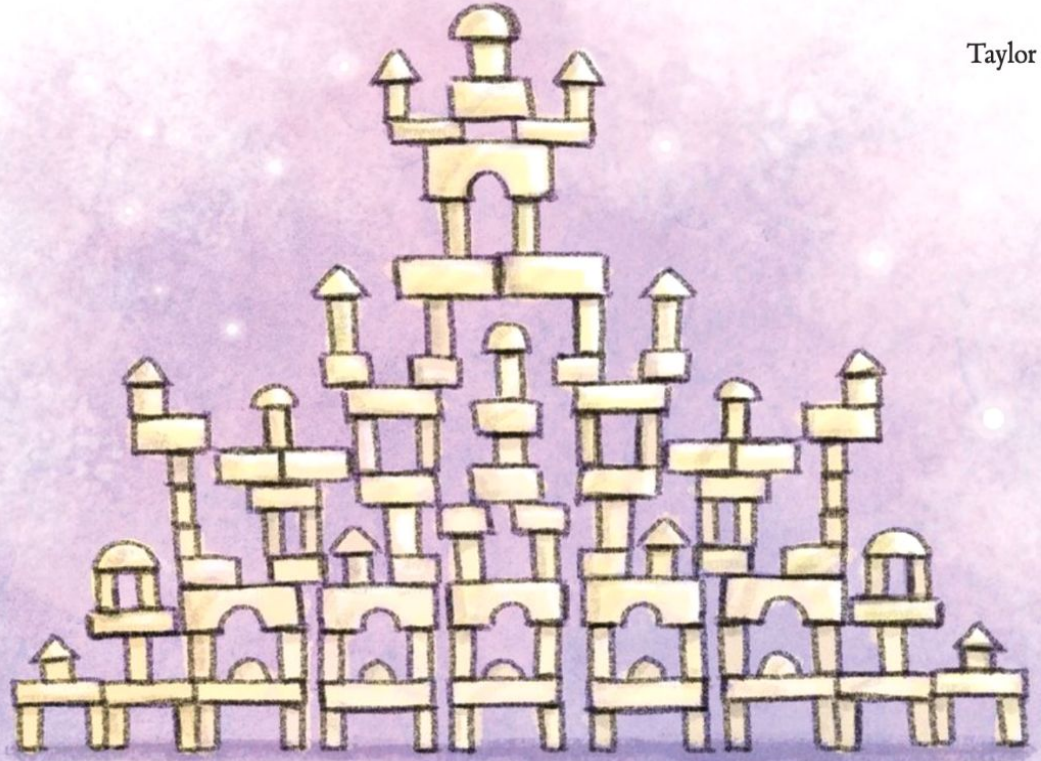
Been building **wallets** since 2015.

Been building **MetaMask** since Feb 2022.

@tayvano_ on Twitter.

Something amazing.

Taylor was so proud.



“The Rabbit Listened” by Cori Doerrfeld

METAMASK

This shit is amazing.

the world computer
trustless computing
making your own money
unique and unstoppable
permissionless
how cool are consensus mechanisms?!
digital self-sovereignty
financial innovation
trust layer for a better society
composability
programmable money
innovation
inclusive community
genius people & good vibes

"The Rabbit Listened" by Cori Doerrfeld

METAMASK

This shit is also hard.

We fail people all the time.

We fail people who are relying on us to access the **wonders of Web3**.

We are failing newcomers who enter the space **hopeful** and **optimistic**.

We have failed those who **trust** us.

METAMASK

This shit is fucked up.

My world is one where our long-standing reliance on private keys means **billions of dollars** have been stolen from **real people.**

It means billions of dollars **will be** stolen from real people in the coming years.

Building

METAMASK

tayvano commented on `7d4a184` on Jan 7, 2018 Member

That my single biggest regret in my entire fucking goddamn life is telling people to enter their fucking private keys on our website. It was shortsighted, stupid, ignorant, harmful and I will never, ever be able to go back in time to change that. Regardless of all the good we do or how much people tell us we are responsible for the usability of Ethereum, **we are responsible for creating and encouraging and to this day allowing a terrible practice which ultimately resulted in more loss than I can comprehend.**

This community deserves better and those who encourage it without education, myself included, should be called out and chastised for their decision. I feel this way partially because I wish someone had educated my ass earlier about the risks and what I was encouraging. My naivety was the cause of this decision. I figured that the reason people shouldn't enter their keys is because at any point someone could push a bad commit and exit scam with the keys. I knew we wouldn't do that and therefore it wasn't a worry. What I failed to realize, and hope those building tools in this space do realize, is that **the reason you don't fucking have users enter keys on websites is because you are training them that it's okay to enter fucking keys on fucking websites.** Oh yeah, and the entire internet is fucking insecure as fuck and we are relying on the DNS system which was built by pioneers building the future who were just as naive as we are today.

METAMASK

"We're basically at the **eating poisonous mushrooms** phase of product development.

The pioneers are often taking a total leap of faith...just leaping into the abyss...and then letting us know if it hurt."

– Dan Finlay
Founder, MetaMask

METAMASK

New Paradigms

METAMASK

New Paradigms

The incentive to gain access to people's **private keys / secret recovery phrases** is so large, everyone from script-kiddies to state-sponsored hackers dedicate limitless time and energy to infiltrating, evolving, and executing increasingly creative attacks.

What's the problem?

METAMASK

Scams
Social Engineering
Phishing
Account Takeovers
Supply Chain Attacks
DNS & BGP Hijacks
XSS/Injection Attacks
ECDSA Nonce Reuse

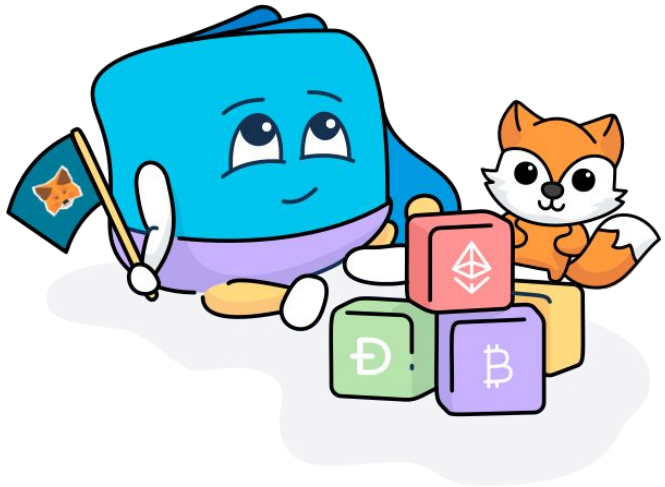
METAMASK

People don't understand.

Most people **don't even realize** that losing their private key—or having it stolen—means they've lost **all** their...

- digital assets
- future airdrops
- collectibles
- soulbound tokens
- access
- identity

...and there's no path of recourse.



METAMASK

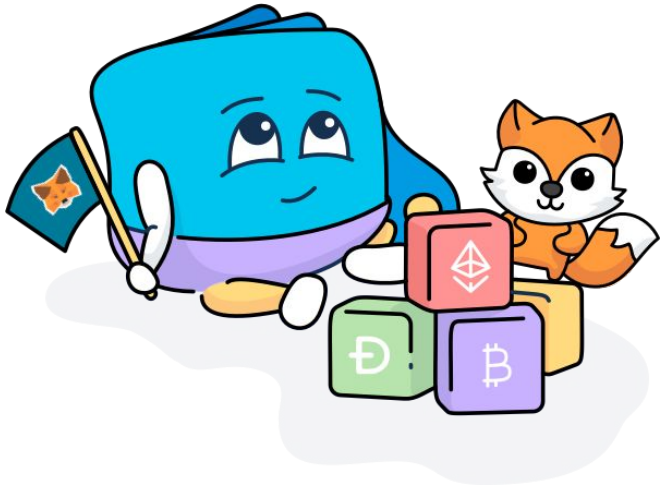
People shouldn't need to understand.

The problem isn't ignorance or janky interfaces.

The problem is this entire ecosystem is built on top of **irrevocable private keys.**

A single string of **immutable** characters has **full, unlimited**, **irrevocable** control over...
- everything you've ever done...
- every asset you've ever held...
- every permission you've ever granted....

across every single network...



afdfd9c3d2095ef696594f6cedcae59e7
2dcd697e2a7521b1578140422a4f890

brain surround have swap horror body response double fire dumb bring hazard

METAMASK

Incentives

In an ecosystem full of experts in game theory, incentives, and cryptonomics, it boggles my mind that so many fail to see that, **in order for people to be safe and successful,** we need to incentivize them to do so.

We need to lower the cost of being safe.

METAMASK

Incentives

Migrating from one account to another is neither fun nor cheap.

It **punishes** those most engaged with the ecosystem.

It has a **real cost**—transaction fees, closing/opening DeFi positions, tax implications, immovable assets, user error, time, stress, energy.

It shouldn’t be like this.

We can do better than this.

METAMASK

We are responsible for our creations.

The original sin is thinking technology lives in an **amoral**, **apolitical**, **inhumane** bubble.

It's conflating **private keys** with **people's identities**.

It's believing that **immutability is better.**

It's seeing the **technology** as the solution.

It's refusing to tackle the hard, messy, **human** problems.

It's undervaluing **people.**

The Original Sin

METAMASK

The ostrich: "Gulp!
Let's hide and pretend
nothing happened!"

METAMASK

New Paradigms

METAMASK

New Paradigms

This is mine.

It **cannot** be hacked or stolen.

I have full **control** over it. I can **use** it. I can **revoke** it. I can **recover** it.

I give full, informed, enthusiastic **consent** to the things that are done with it.

I **choose** how I interact with the world.

I choose how I impact the world.

What's the solution?

METAMASK

ERC-4337

Account abstraction without Ethereum protocol changes

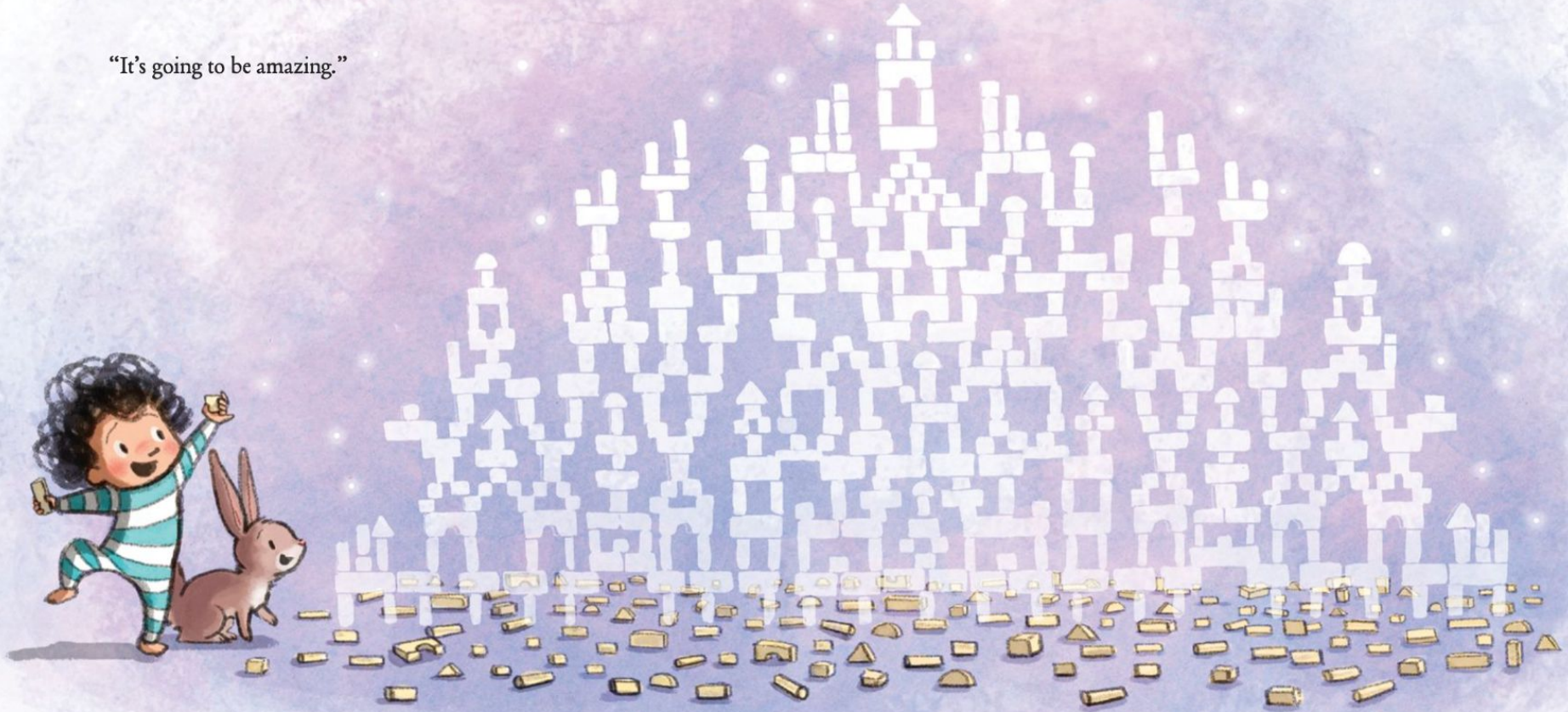
EIP-3074

Allow externally owned accounts to delegate control to a contract

EIP-5003

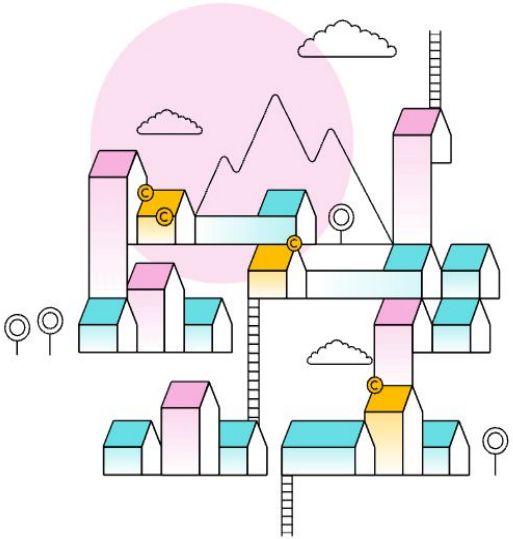
Allow migrating away from ECDSA by deploying code in place of an externally owned account

"It's going to be amazing."



VillageDAO

Better Customer Care for Web3



VillageDAO mobilizes communities into incentivized success teams! The VillageDAO platform allows the community to support itself by installing trust, transparency, and incentive alignment between the community and the brands they support.

You can learn more by checking out their site (joinvillagedao.com) or their Twitter (@VillageDAO_). MetaMask is excited to be the first partner of VillageDAO!

Decentralized Infrastructure Network

A self-sustaining, reliable, and robust network of infrastructure providers built to serve a high-throughput of API blockchain requests

- Remove single point of failure
- Collaborative Web3 spirit
- Improve reliability for users
- Guarantee towards 100% uptime
- Same, easy-to-use Web2 UX

Apply via QR Code

Infura is seeking strong Web3 infrastructure providers to work together towards a decentralized future

METAMASK

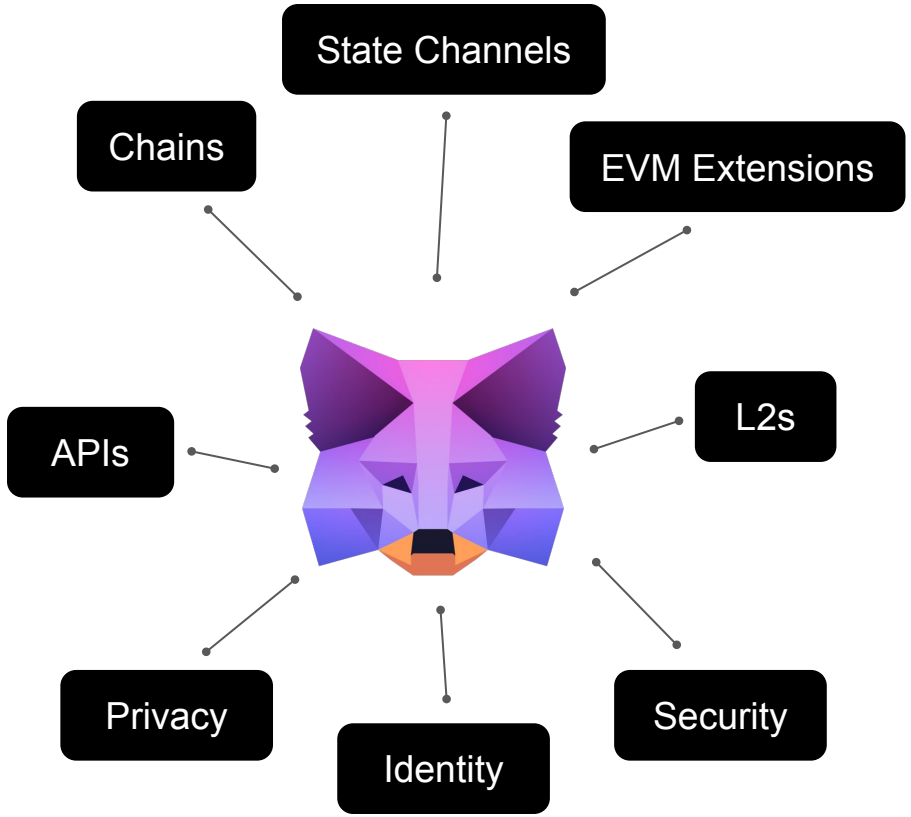
MetaMask Snaps

Ever wished MetaMask did something to make your users' experience better?

MetaMask is now an **extensible platform** for **permissionless innovation**.

Bring your own solutions to make Web3 easier to use into MetaMask with Snaps—an open platform for **anyone** to extend the functionality of MetaMask.

metamask.io/snaps/



❤️ Thank You!

@MetaMask

@tayvano_