

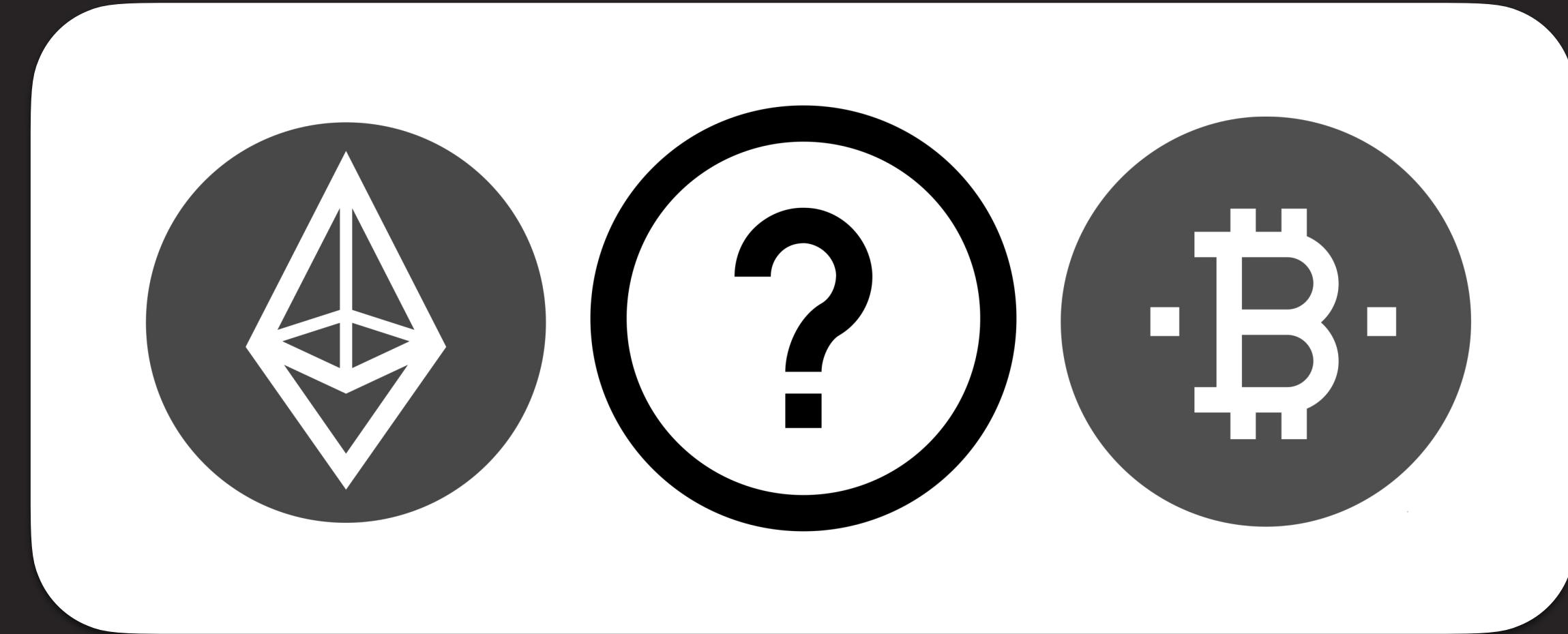
# 1729

## Lecture 14: Open Problems in Web3

A brief tour of some open problems in web3.

# Summary

- People have asked what they can do
- While I'm writing, you can write too :)
- If any of these problems interests you, write a review



# Open Problems in Web3 Infrastructure

What's important and valuable, but falling through the cracks?

# **Overview: Blog, GitHub, Microsite, Startup**

Open Problems

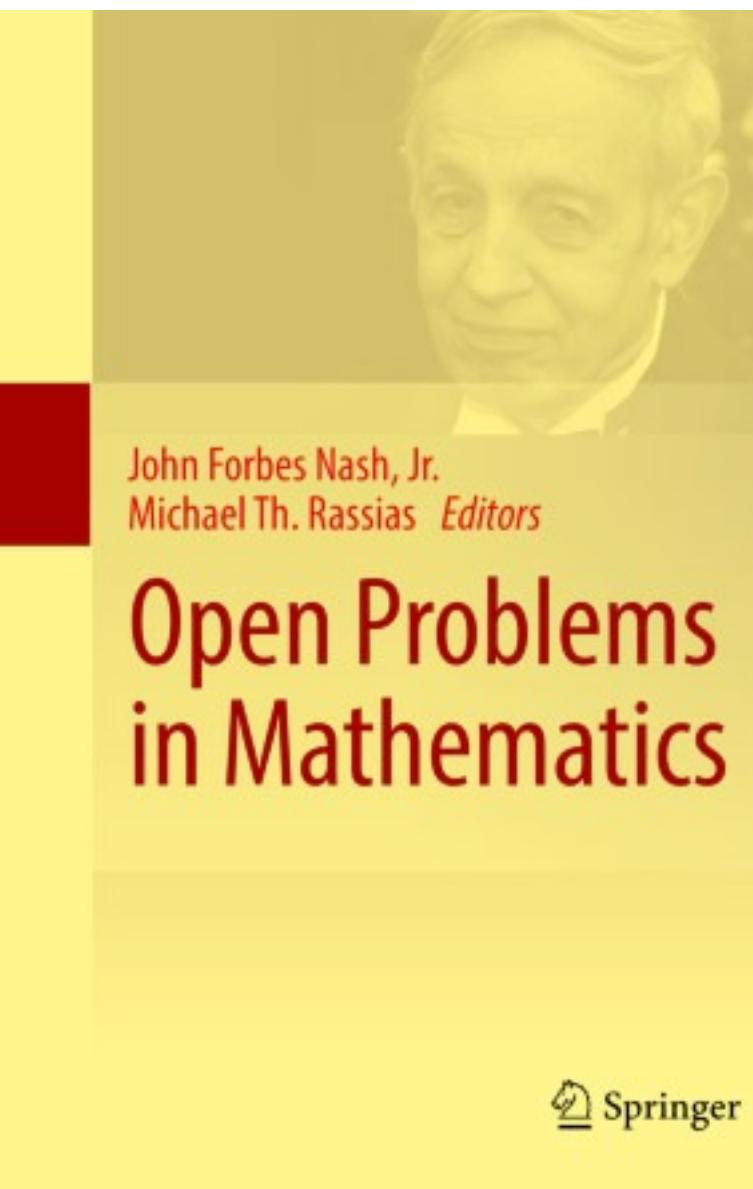
# Updated Request for Startups

## Motivation

Request-for-startups are like open problems in math.

Example: prize competition at [1729.com/inflation](http://1729.com/inflation)

Today's talk is on a series of such (unsexy) problems, where funding is available if you solve them



By Kat Mañalac

Y



### Millennium Problems

#### Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the solution to the quantum versions of the Yang-Mills equations. But no proof of this property is known.

#### Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. The Riemann hypothesis tells us about the deviation from the average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious' zeros of the zeta function are complex numbers with real part 1/2.

#### P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.

#### Navier–Stokes Equation

This is the equation which governs the flow of fluids such as water and air. However, there is no proof for the most basic questions one can ask: do solutions exist, and are they unique? Why ask for a proof? Because a proof gives not only certitude, but also understanding.

#### Hodge Conjecture

The answer to this conjecture determines how much of the topology of the solution set of a system of algebraic equations can be defined in terms of further algebraic equations. The Hodge conjecture is known in certain special cases, e.g., when the solution set has dimension less than four. But in dimension four it is unknown.

#### Poincaré Conjecture

In 1904 the French mathematician Henri Poincaré asked if the three dimensional sphere is characterized as the unique simply connected three manifold. This question, the Poincaré conjecture, was a special case of Thurston's geometrization conjecture. Perelman's proof tells us that every three manifold is built from a set of standard pieces, each with one of eight well-understood geometries.

#### Birch and Swinnerton-Dyer Conjecture

Supported by much experimental evidence, this conjecture relates the number of points on an elliptic curve mod p to the rank of the group of rational points. Elliptic curves, defined by cubic equations in two variables, are fundamental mathematical objects that arise in many areas: Wiles' proof of the Fermat Conjecture, factorization of numbers into primes, and cryptography, to name three.

BUILD

## A \$100k Prize for a Decentralized Inflation Dashboard

Build a censorship-resistant inflation dashboard. If we pick your project, we'll fund it with \$100k.



1729

Aug 5, 2021 • 12 min read



Inflation is a [monetary phenomenon](#), a function of money printing. But it is also in part a social phenomenon, a function of mass psychology. If enough of the right people believe that inflation is going to happen, it will. As such, when inflation is happening, there is often a push to *censor* discussion of inflation itself, under the grounds that discussing the problem actually causes it in the first place. That is exactly what happened in [Argentina](#) and [Venezuela](#) over the last decade.

And that is why the world needs a global, decentralized, censorship-resistant inflation dashboard. Enter the next 20 days, where you can submit ideas for this

# Example: A Decentralized Inflation Dashboard

This one is written up completely at [1729.com/inflation](https://1729.com/inflation)

# Do a Review, a GitHub, a Microsite, *then* Startup

A startup is a multiyear commitment.

You can start with a technical review, a simple blog post on the area. Then set up a GitHub that you start poking at. Then deploy a microsite. Finally, if the initial traction works, do a startup.

This gives you stopping points and lets you test the waters.

1 Decentralized Social Networks  
Comparing federated and peer-to-peer protocols

Jay Gruber Follow Jan 10, 2020 · 9 min read

Twitter Facebook LinkedIn Email Print

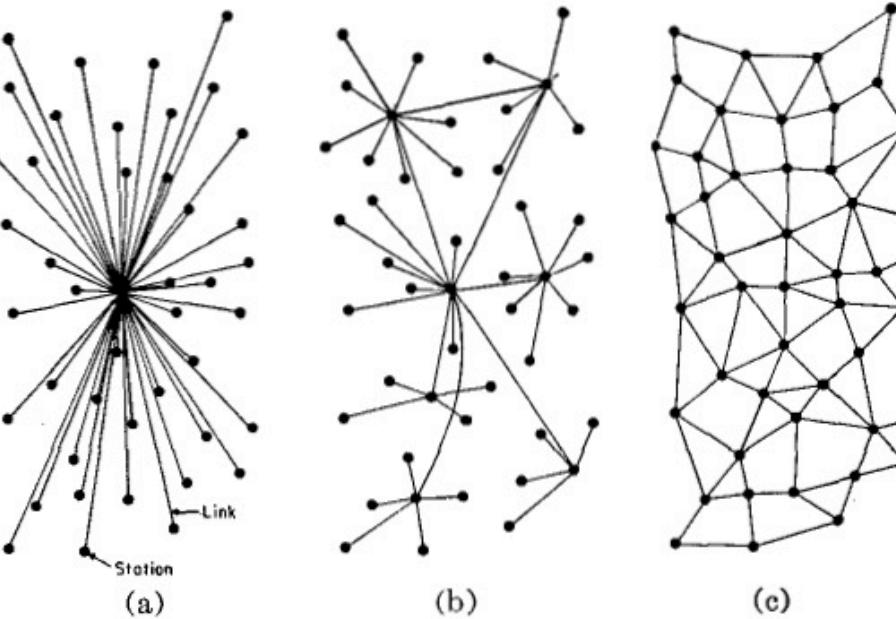


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Or, centralized, federated, and peer-to-peer

3 Carrd

## Build one-page sites for pretty much anything

Whether it's a personal profile, a landing page to capture emails, or something a bit more elaborate, Carrd has you covered. Simple, responsive, and yup – totally free.

Choose a Starting Point

Profile Landing Form Portfolio Sections

2 ConsenSys/rimble-app-demo

React Ethereum dApp demonstrating onboarding and transaction UX

4 Contributors 5 Issues 29 Stars 19 Forks

A GitHub repository card for 'rimble-app-demo' under the 'ConsenSys' organization. It shows 4 contributors, 5 issues, 29 stars, and 19 forks. A yellow progress bar is at the bottom.



Overview: Blog, GitHub, Microsite, Startup

## **Open Problems**

# Instant DAOification of a GitHub project

First open problem is related to what we just talked about: how do you instantly DAOify a GitHub project?

[twitter.com/balajis/status/1326313315044192256](https://twitter.com/balajis/status/1326313315044192256)

## How I Stumbled Upon The Internet's Biggest Blind Spot

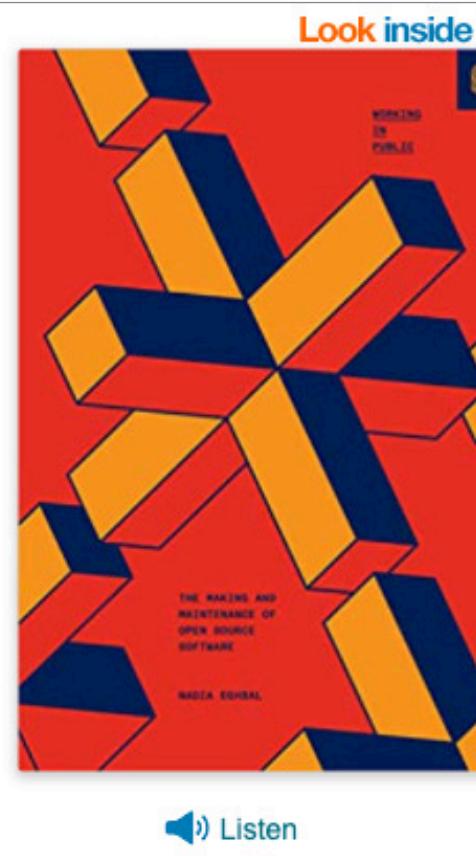
Let's make software even better.



Nadia Eghbal

Jan 14, 2010

I left my job in venture capital, which is something that I initially joined College of the hard knocks. I joined a non-venture fund, but I'm still here. (I'm not sure what goes.)



Look inside

Working in Public: The Making and Maintenance of Open Source Software Hardcover – August 4, 2020

by Nadia Eghbal (Author)

★★★★★ 248 ratings

See all formats and editions

Kindle  
\$9.99

Audiobook  
\$0.00

Hardcover  
\$18.42

Read with Our Free App

Free with your Audible trial

6 Used from \$13.50

1 New from \$18.42

An inside look at modern open source software developers--and their influence on our online social world.

"Nadia is one of today's most nuanced thinkers about the depth and potential of online communities, and this book could not have come at a better time." --Devon Zuegel, director of product, communities at GitHub



Balaji Srinivasan  
@balajis

...

A new way to fund open source?

- Be open source dev
- Issue a token
- Hold X% of it
- Has 0 value initially
- Award (100-X)% of it over time to folks who contribute code
- Companies then buy token to prioritize bugs & features
- Suddenly, an economy arises!

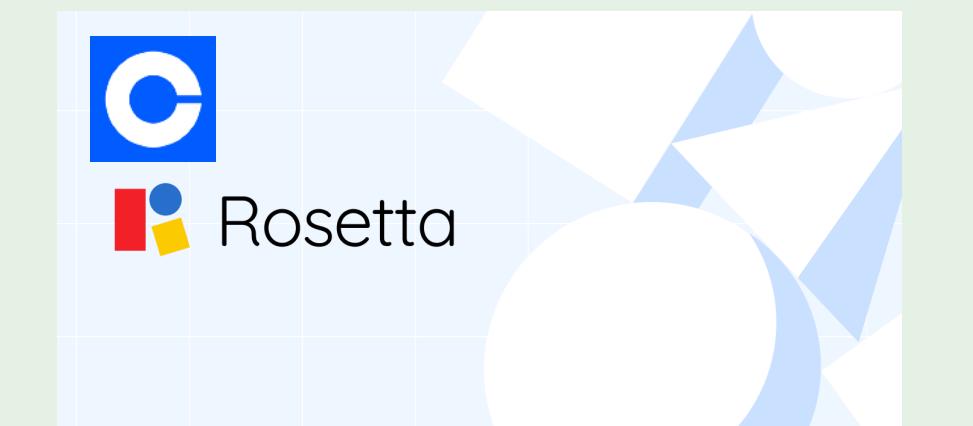
7:58 AM · Nov 11, 2020 · Twitter Web App

337 Retweets 128 Quote Tweets 2,251 Likes

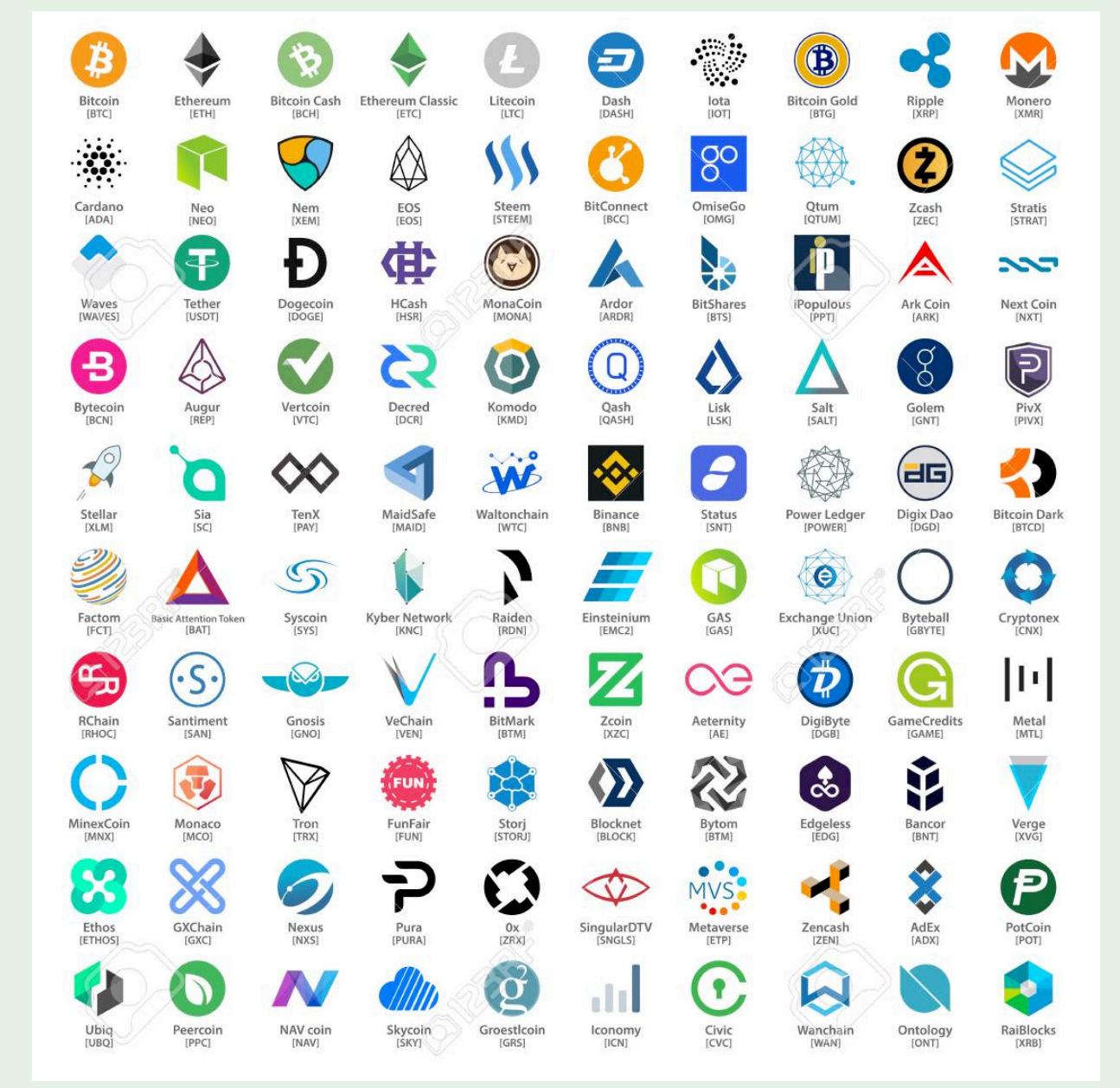
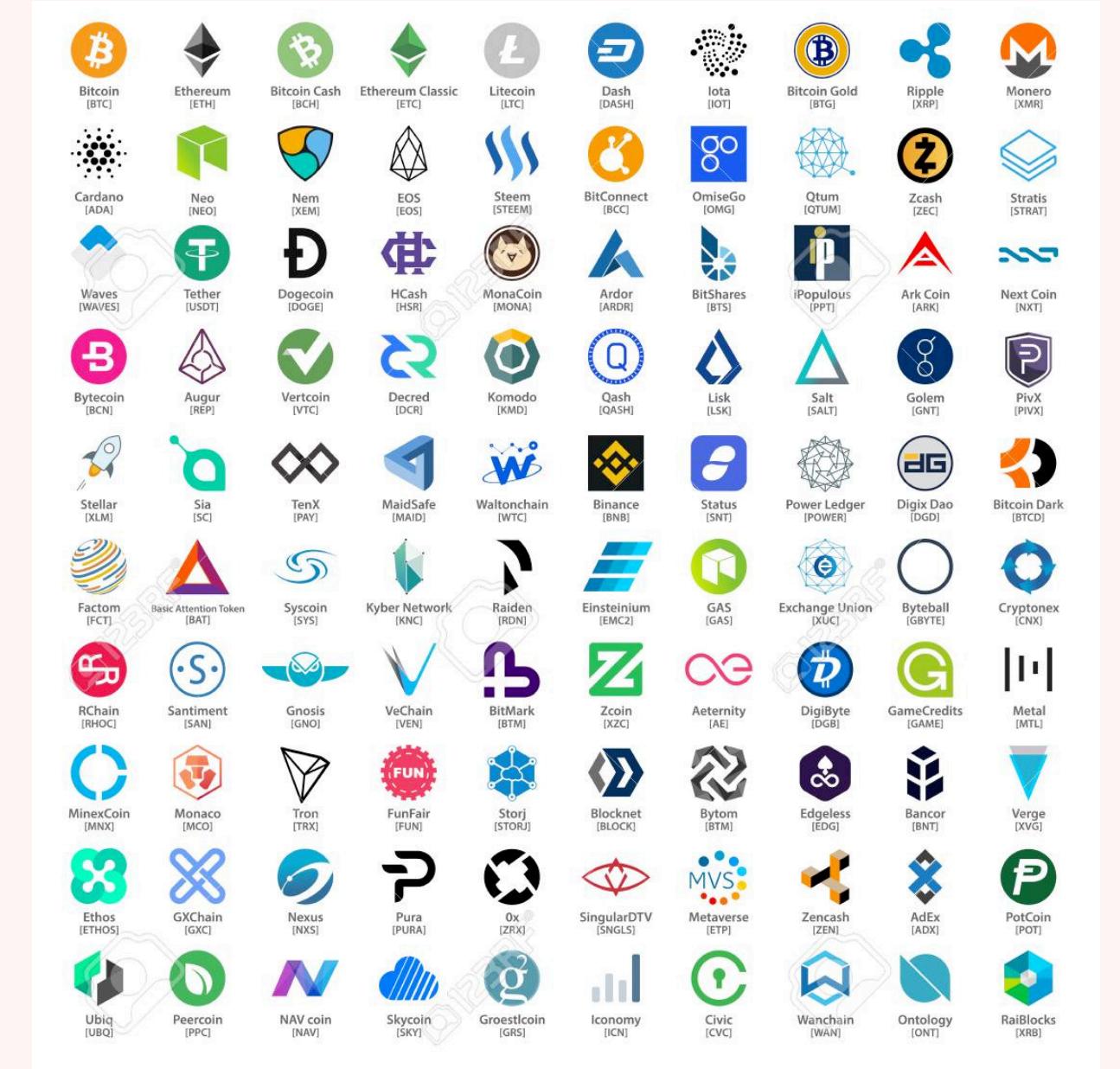
# Postchain: PostGIS, but for web3

Everyone building anything in  
web3 ends up reinventing the  
bridge between PostgreSQL and  
blockchains. What if we solve  
that once and for all?

[postgis.net](http://postgis.net)  
[bit.ly/2ULcimi](https://bit.ly/2ULcimi)  
[bit.ly/3mBbn3l](https://bit.ly/3mBbn3l)



for



# Chain Migration and Interoperation

How do we start on a centralized database, or on a token, and move some assets (or all of them) to the other?

Can we systematize this?

## Why Blockstack is migrating to the Bitcoin blockchain

by [Muneeb Ali](#) — September 15, 2015



Since earlier this year, we have been planning to migrate Blockstack's underlying blockchain from Namecoin to Bitcoin. This process started with the [experimental release of Blockstack Core](#), which includes a decentralized DNS system built on the Bitcoin blockchain, and since then we've been running tests to ensure that we could perform a migration without incident and that Blockstack Core could perform at scale.

### Recent Posts

SEC Filing Update  
Stacks Cryptocurrency No Longer Treated as a US Security by Blockstack PBC  
JANUARY 21, 2021

See the Stacks.co Blog for latest Stacks Ecosystem Updates!  
JANUARY 11, 2021

Hiro: Dedicated To The Builders of A Better Internet on Bitcoin  
DECEMBER 22, 2020

### Categories

APP MINING (17)

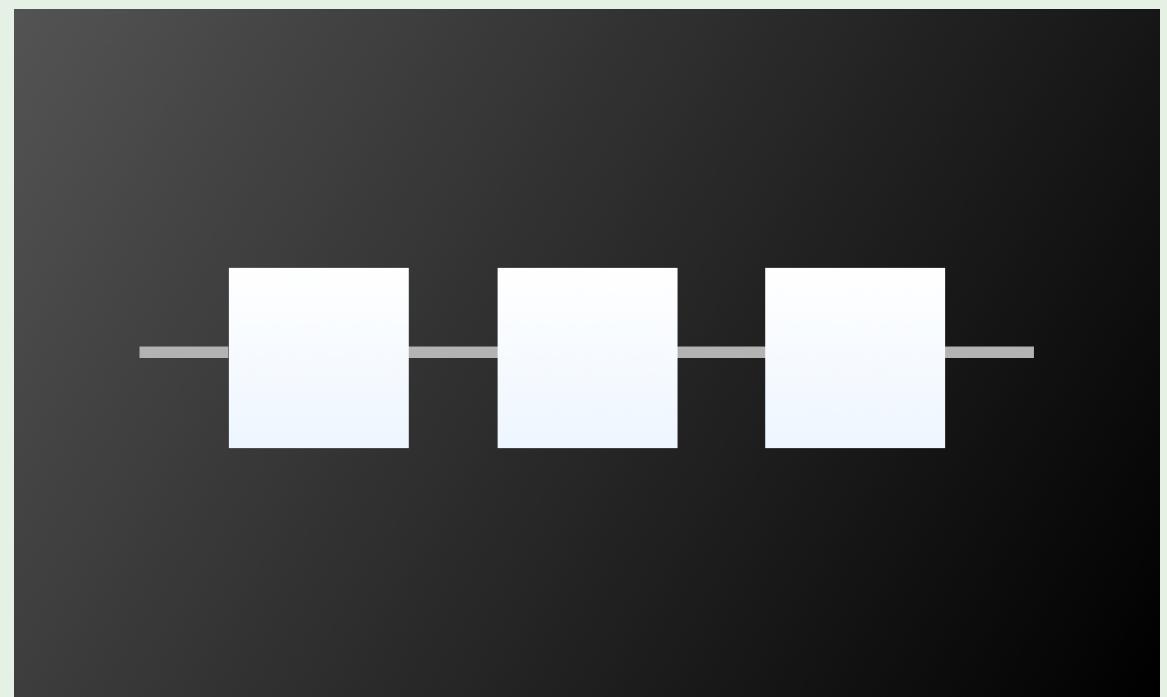
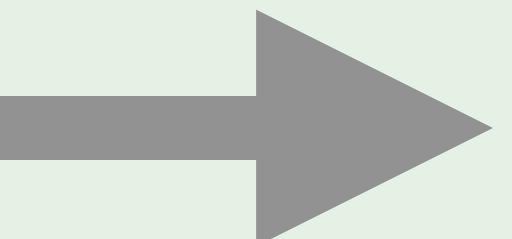
ASIA (6)

BLOCKCHAIN (31)

BOUNTIES (4)

CENSORSHIP (1)

## Binance Reveals Timeline for BNB Cryptocurrency's Move Off Ethereum

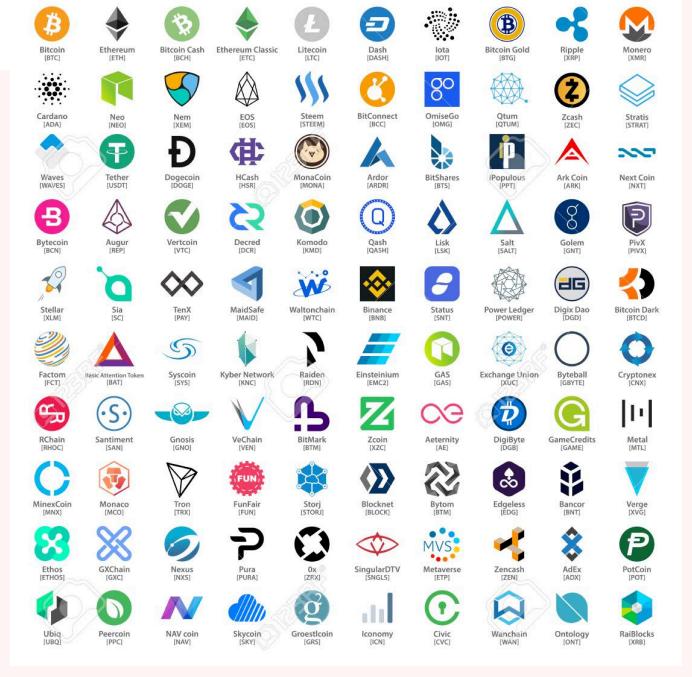
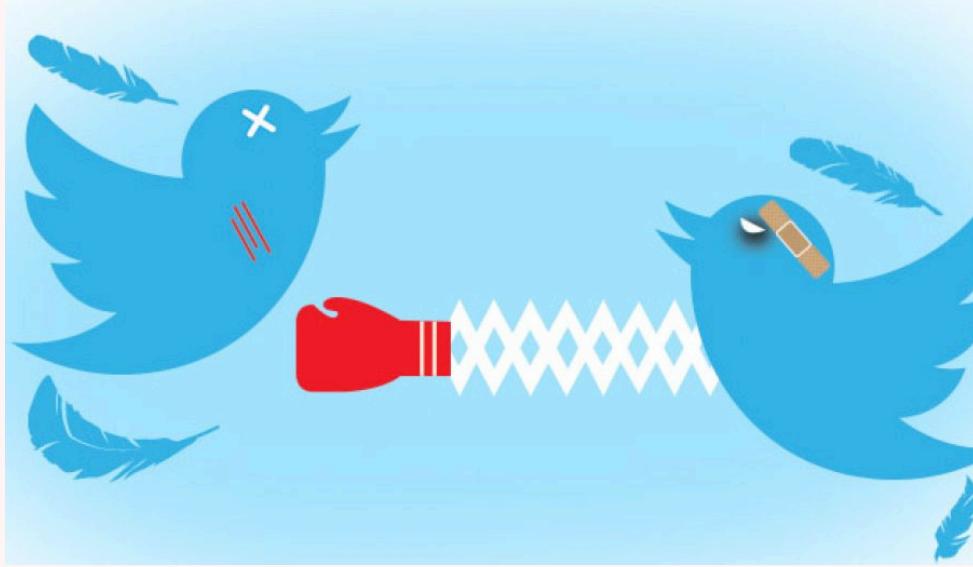


# Quantifying & Optimizing Decentralization

How do we move from shouting slogans at each other to actually framing the problem of quantifying decentralization?  
Then we can optimize given scarce resources.

[news.earn.com/quantifying-decentralization-e39db233c28e](http://news.earn.com/quantifying-decentralization-e39db233c28e)

But this also points the way to when a digital asset transaction may no longer represent a security offering. If the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract. Moreover, when the efforts of the third party are no longer a key factor for determining the enterprise's success, material information asymmetries recede. As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful.



## Quantifying Decentralization

We must be able to measure blockchain decentralization before we can improve it.

Given a subsystem  $s$  with  $K$  entities, let  $p_1 > \dots > p_K$  be the proportions of the subsystem controlled by each of the  $K$  participants such that  $\sum_i^K p_i = 1$ . Then we define the Nakamoto coefficient as:

$$N_s := \min \left\{ k \in [1, \dots, K] : \sum_{i=1}^k p_i \geq 0.51 \right\}$$

In other words, the Nakamoto coefficient of a subsystem  $N_s$  is the minimum number of entities whose proportions one can sum to get to 51% control. If we assume a decentralized system is composed of  $S$  such subsystems, where  $N_s$  denotes the Nakamoto coefficient of subsystem  $s$ , the minimum Nakamoto coefficient  $N_{\min}$  is defined as:

$$N_{\min} := \min \{N_1, \dots, N_S\}$$

So the minimum Nakamoto coefficient of a decentralized system is the *minimum* number of entities to compromise to get to 51% control of at least one subsystem.

Minimize:

$$f(x)$$

Subject to:  $g_j(x) \geq 0, j = 1, \dots, J;$

$$h_k(x) = 0, k = 1, \dots, K;$$

$$x_i^{(L)} \leq x_i < x_i^{(U)}, i = 1, \dots, N;$$



Anatoly Yakovenko @aeyakovenko · Aug 21

how is solana trading decentralization? the key facet we are focusing on is the **Nakamoto Coefficient**, aka the min set of nodes that add up to 33%. Eth2 is not focusing on that facet, instead on minimizing the cost of the honest majority to detect fraud proofs.

3

1

25

↑

# The Coin Table and the Cap Table

Right now, many entities have a cap table plus one (or more) coin tables. Can we set up a *combined* web dashboard for these, perhaps using APIs?

[twitter.com/balajis/status/1364626032771272706?  
lang=en](https://twitter.com/balajis/status/1364626032771272706?lang=en)

The collage includes:

- Carta logo (blue mountain icon)
- Coinbase logo (blue text)
- AngelList logo (handshake icon and text)
- A list of CEX (Centralized Exchange) logos: Binance, HitBTC, OKEX, Kraken, Bitmax, coindesk, POLONIEX, Bakkt, CEX.IO, and BITTREX.
- A screenshot of the AngelList platform showing a cap table summary for "OperiaEq". It displays 25 total shareholders, 1,084,500 total shares, 0% held by the user, and \$2,450,000 in total cash raised.
- A screenshot of the CoinTikka interface showing real-time price data for Bitcoin (BTC) and Ethereum (ETH). BTC is at \$9,516.04 (+4.69%) and ETH is at \$234.09 (+5.24%).

# Automated Accounting, Triple-Entry Bookkeeping, Streaming Financials

Now that many businesses are running in part on USDC, can we show toy examples of what fully automated accounting might look like?

Streaming financials: realtime income statement, etc.

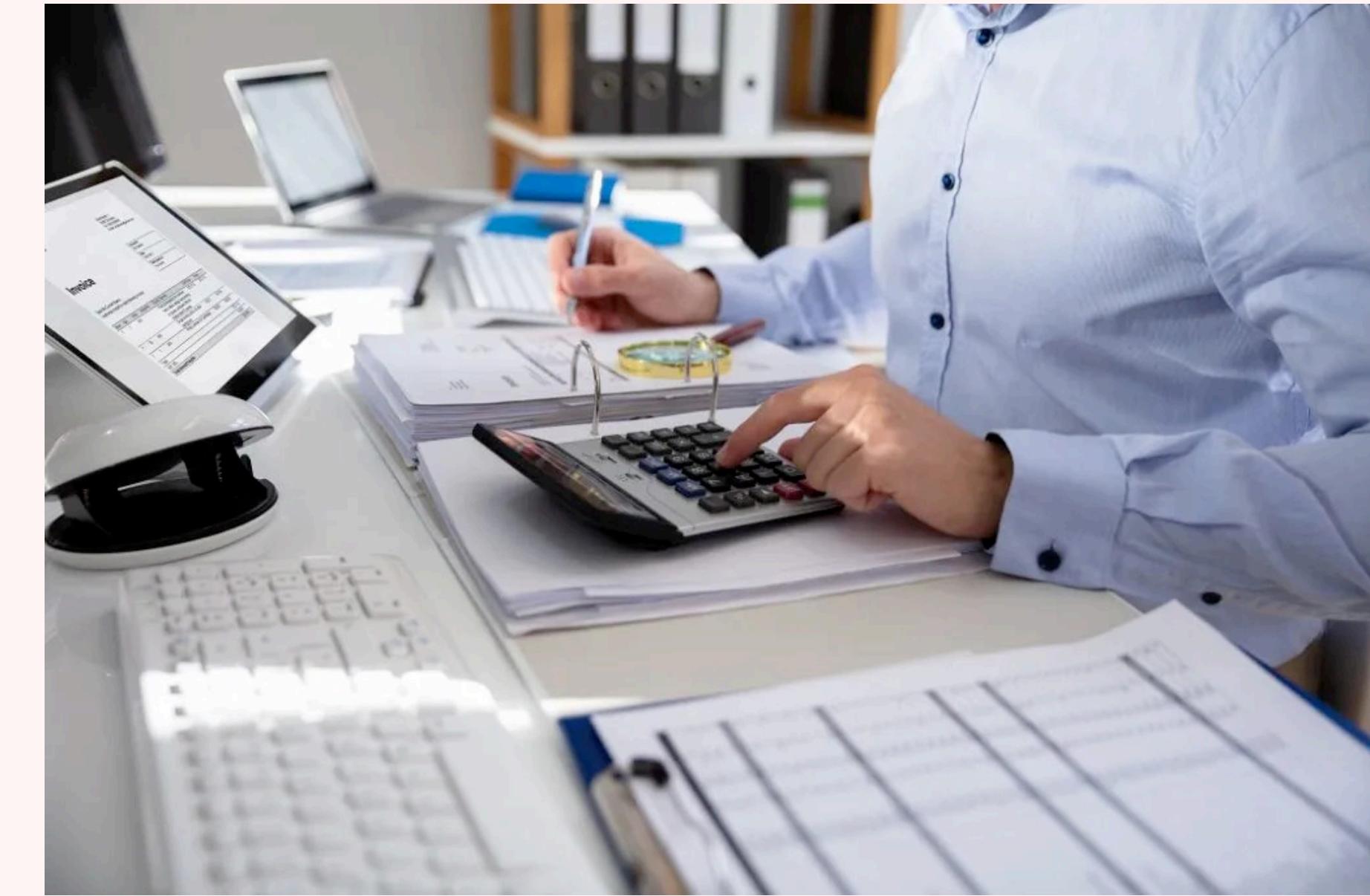
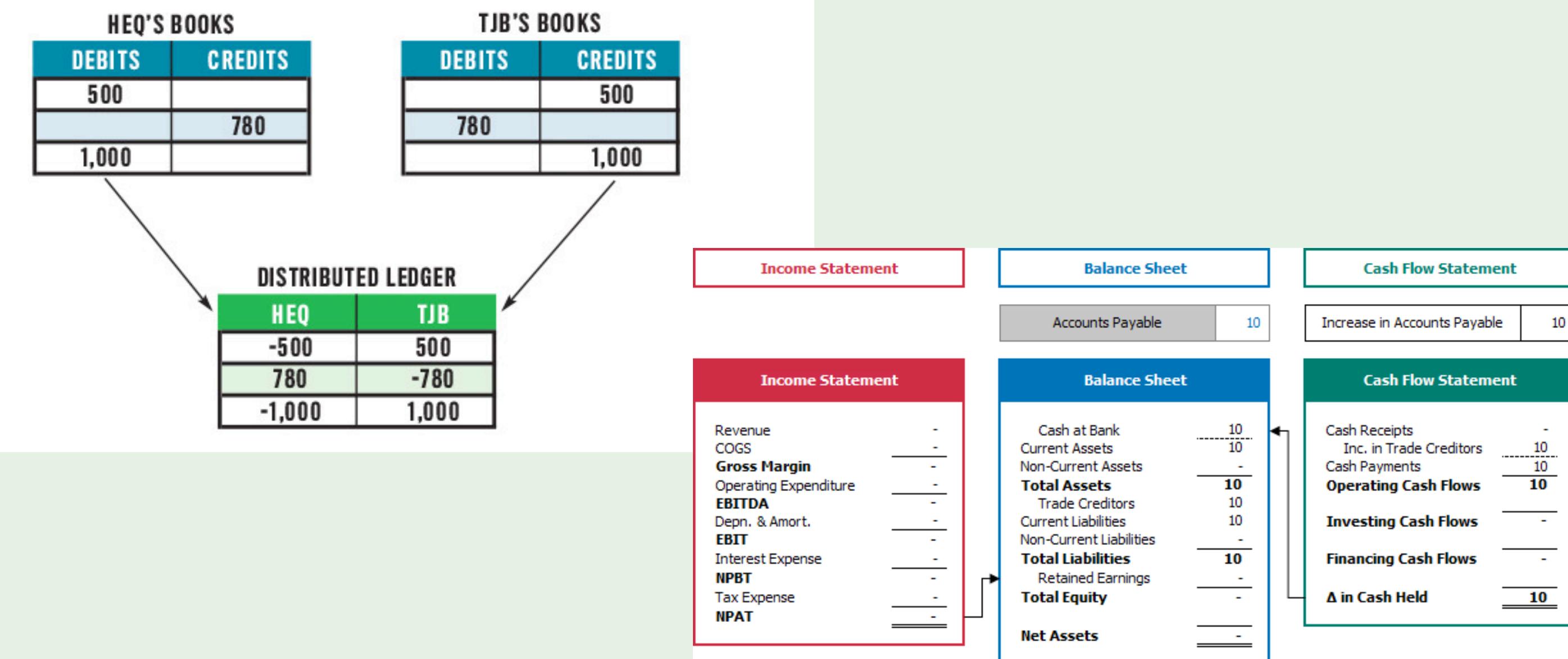


FIGURE 3: THE TRIPLE ENTRY



# Putting Sand Hill On-Chain

A huge issue in web3 is the lack of traditional forms of economic alignment. VC has solutions for these: waterfalls, drag-along, lockup, vesting, etc. Can we put these on-chain?

[carta.com/blog/the-life-of-a-cap-table](https://carta.com/blog/the-life-of-a-cap-table)  
[balajis.com/mirrortables](https://balajis.com/mirrortables)

### A Simple Financing

**Cap Table**

|             |     |   |
|-------------|-----|---|
| Bob         | 50% | ? |
| Mary        | 50% | ? |
| Option Pool | 0%  |   |

**Financing**

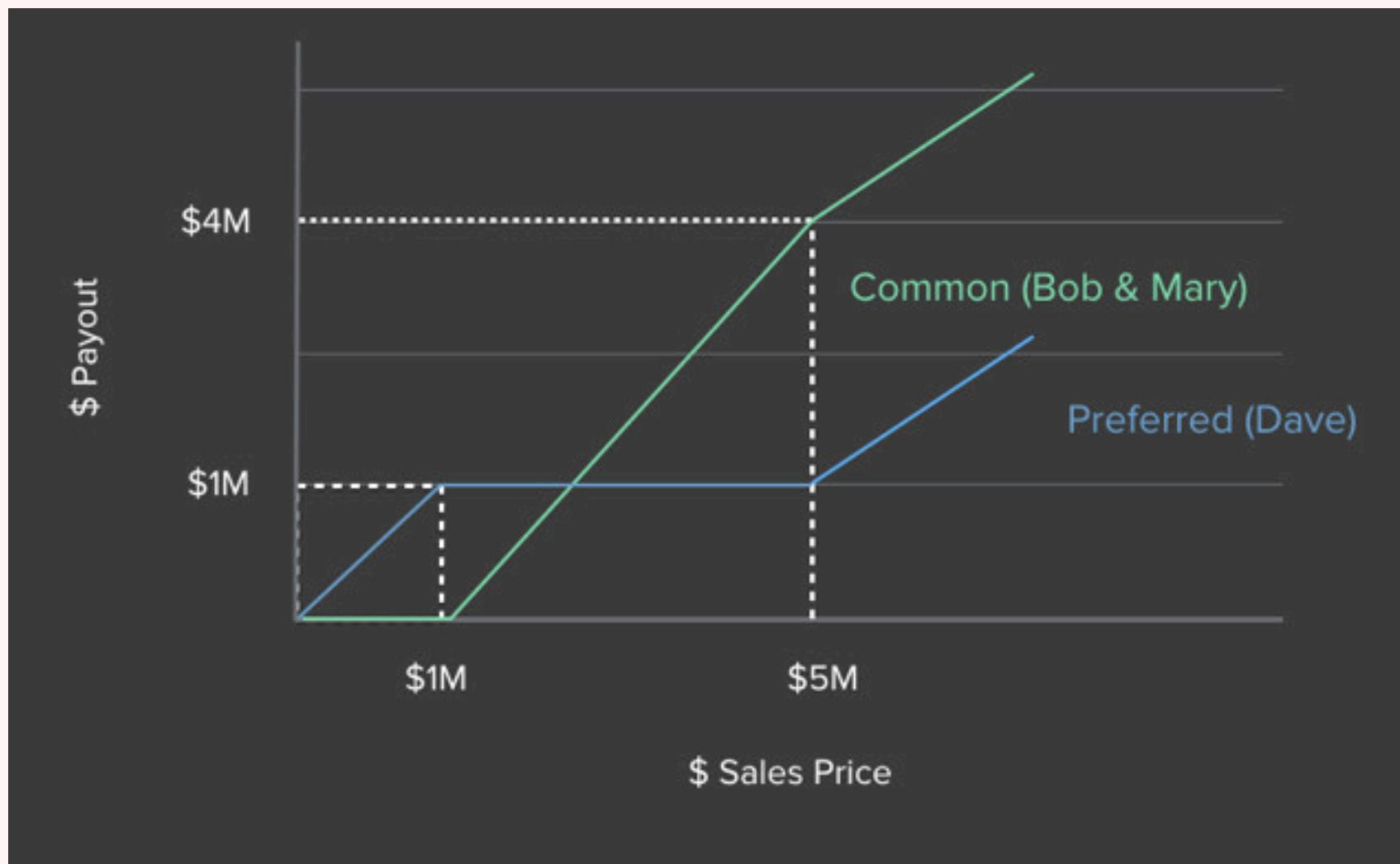
|                        |    |             |
|------------------------|----|-------------|
| Pre Money Valuation    |    | \$4,000,000 |
| Post Money Option Pool | 0% |             |

**New Investors**

|      |   |             |
|------|---|-------------|
| Dave | ? | \$1,000,000 |
|------|---|-------------|

What will this be?

eShares

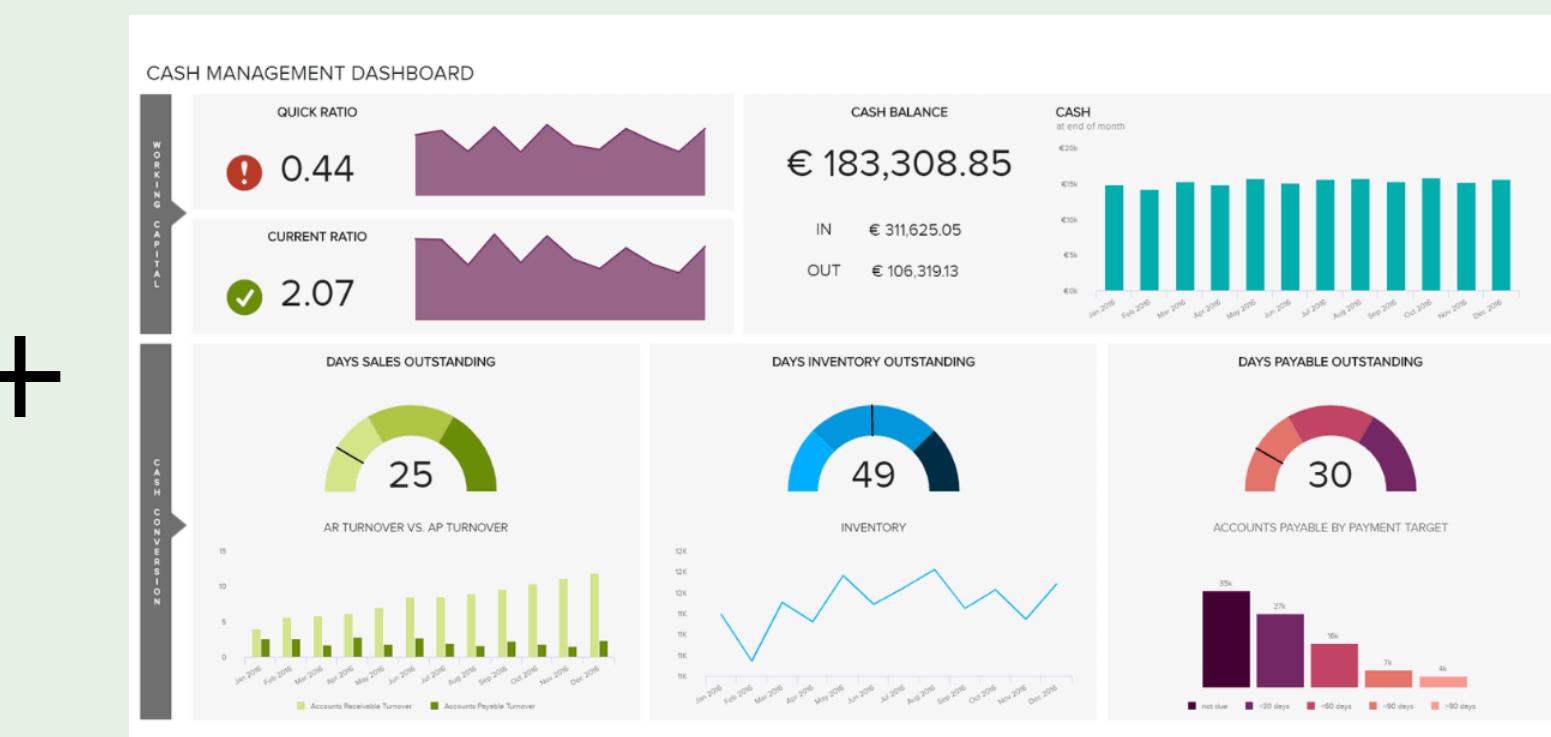
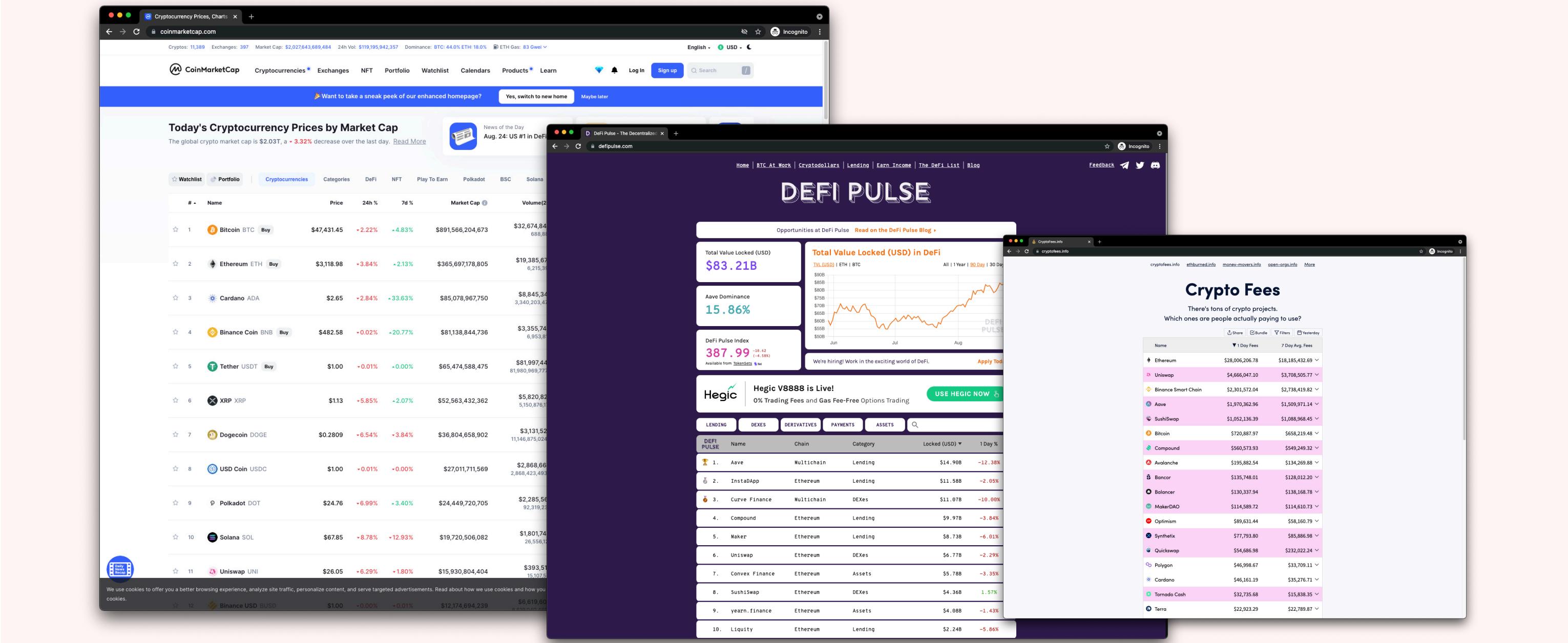


# A Pluggable Dashboard of Dashboards

There are many dashboards out there.

Can you create a Yahoo-style index of all of them, indexed by coin, open-sourcedness, and other variables?

duneanalytics.com has done really well here



# User-Aligned Metrics

The internet allowed measurement of individual pageviews, which turned traditional media into clickbait.

The blockchain enables *user-aligned* metrics. What does Men's Health look like in the time of FitBit? Does Bloomberg 2.0 boost your portfolio?

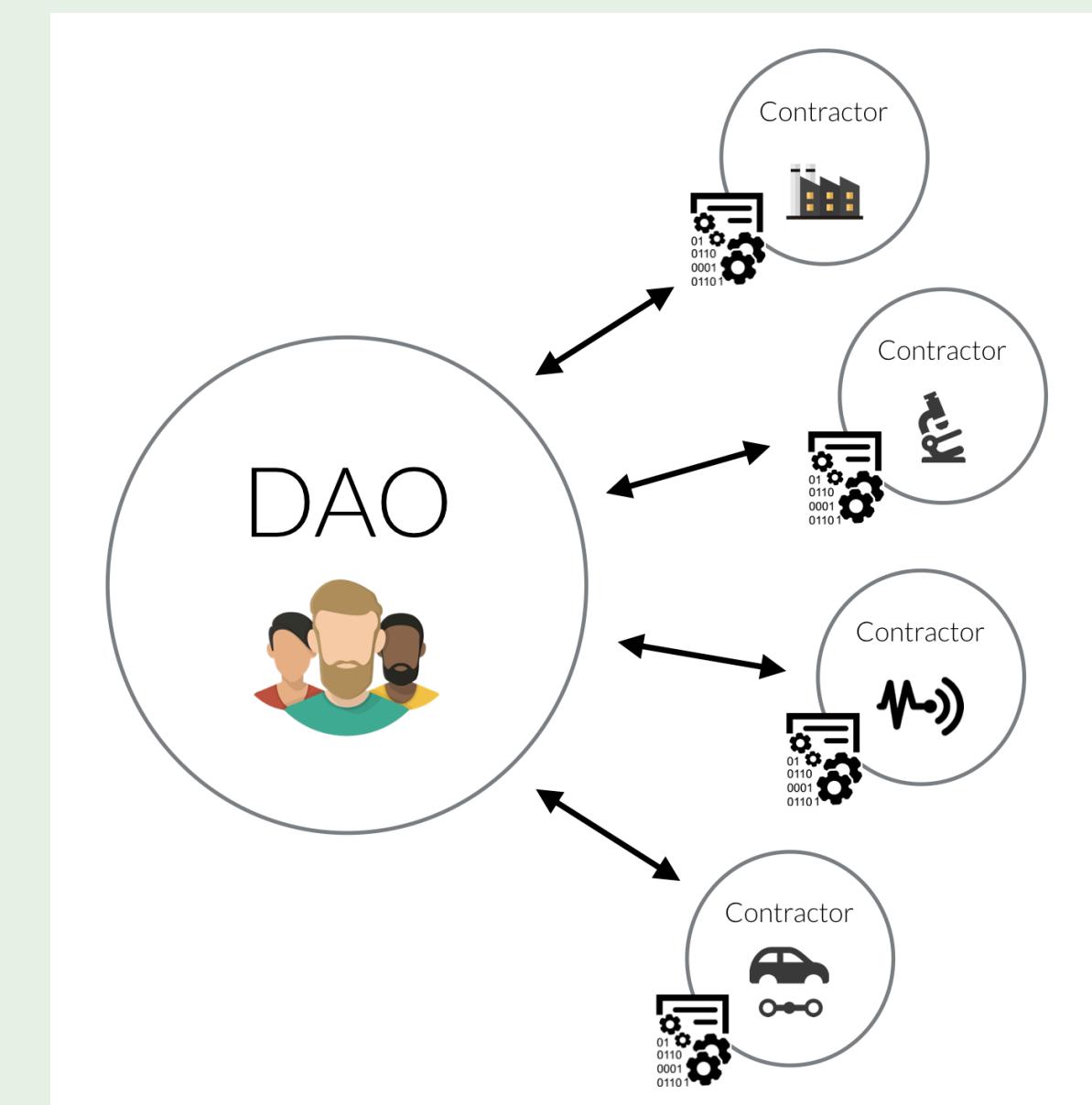
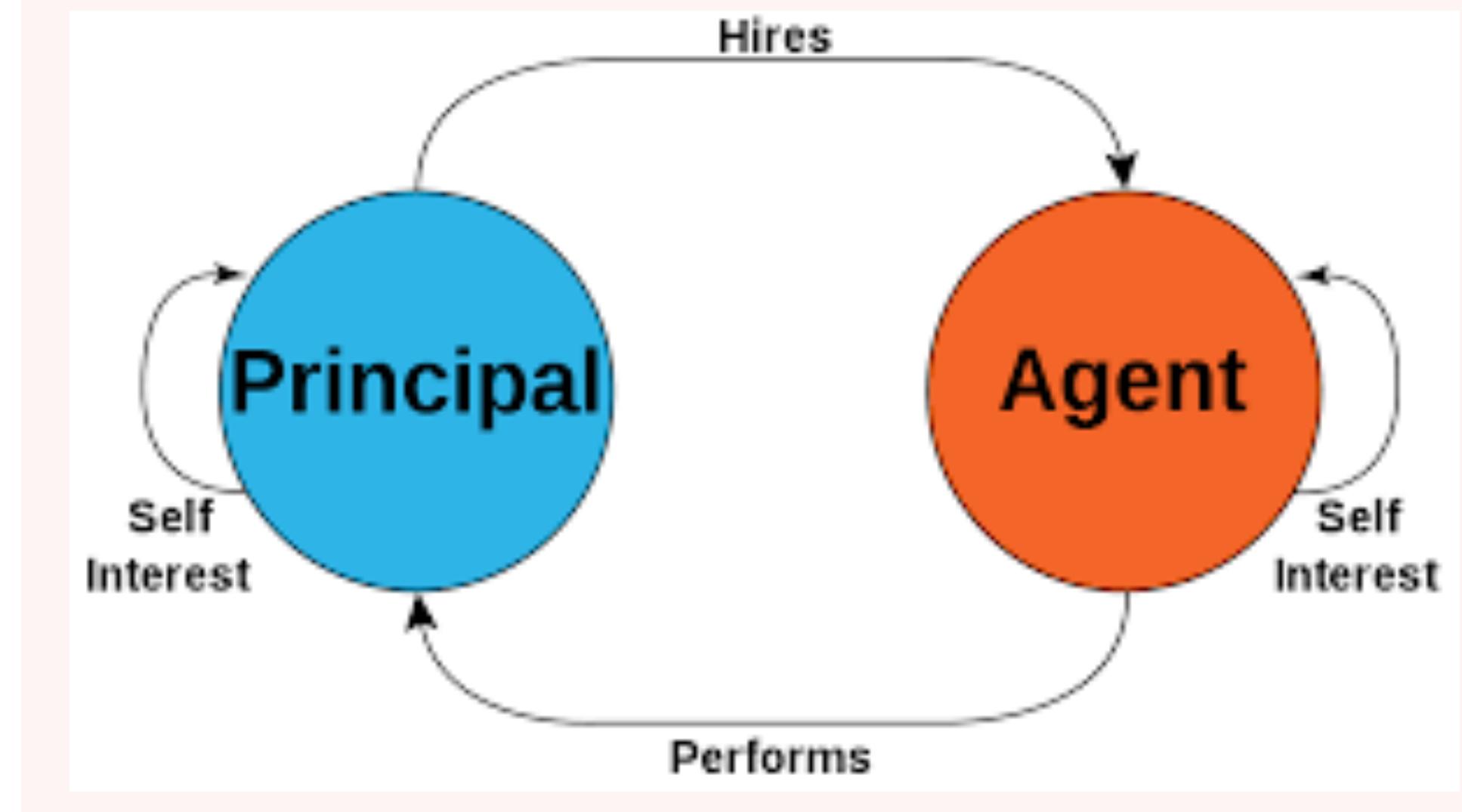


# Principal Agent - Delegation/ACL for DAOs

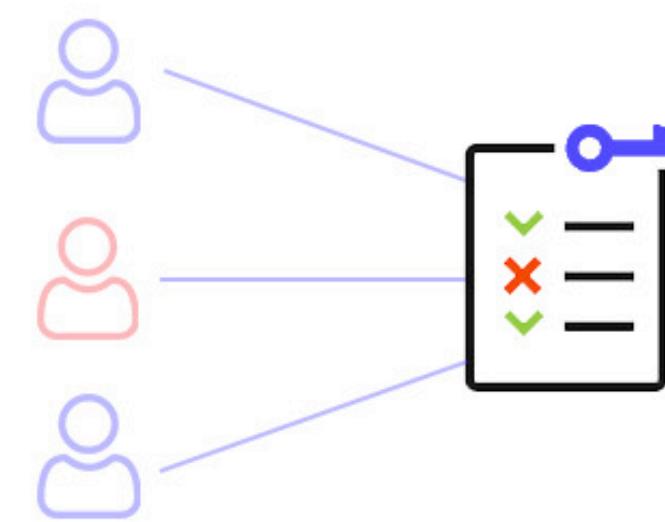
The principal/agent problem is about the divergence between any two parties in an orgchart.

Autonomy solves this: no person, no problem.

What's in between?



## Access Control List



# Pure CPA for web3 commerce

Google and Facebook don't do pure CPA ads because there is no third party who can testify to the validity of the transaction.

What if you did, for merchants accepting crypto?



FIGURE 3: THE TRIPLE ENTRY

| HEQ'S BOOKS |         |
|-------------|---------|
| DEBITS      | CREDITS |
| 500         |         |
|             | 780     |
| 1,000       |         |

| TJB'S BOOKS |         |
|-------------|---------|
| DEBITS      | CREDITS |
|             | 500     |
| 780         |         |
|             | 1,000   |

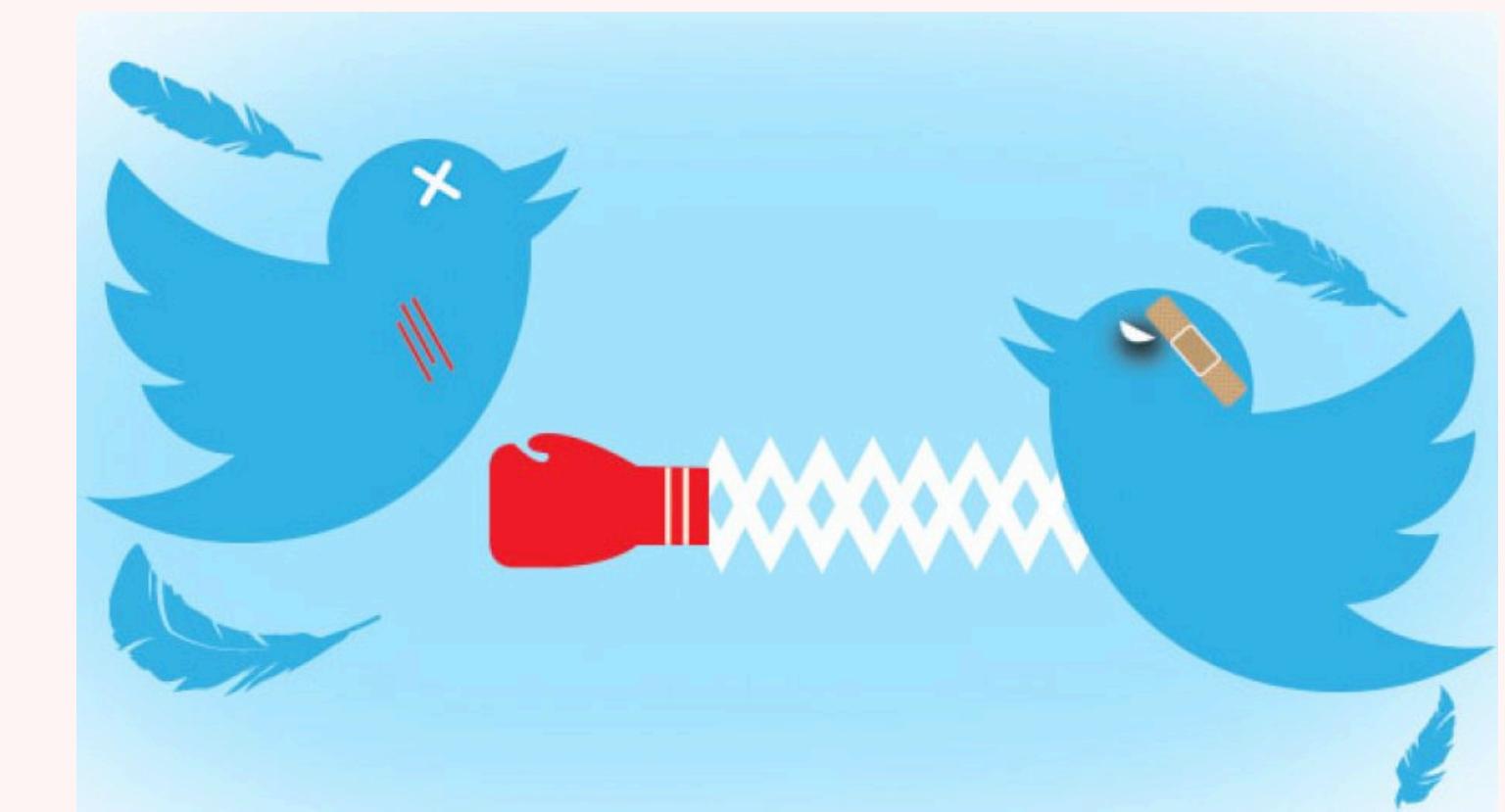
| DISTRIBUTED LEDGER |       |
|--------------------|-------|
| HEQ                | TJB   |
| -500               | 500   |
| 780                | -780  |
| -1,000             | 1,000 |



# Blockchain / L2 Performance Shootout

Like the programming languages benchmark game.

Have a set of open source benchmark programs to measure download time, throughput, etc. Anyone should be able to run and make pull requests.



## The Computer Language Benchmarks Game

“Which programming language is fastest?”

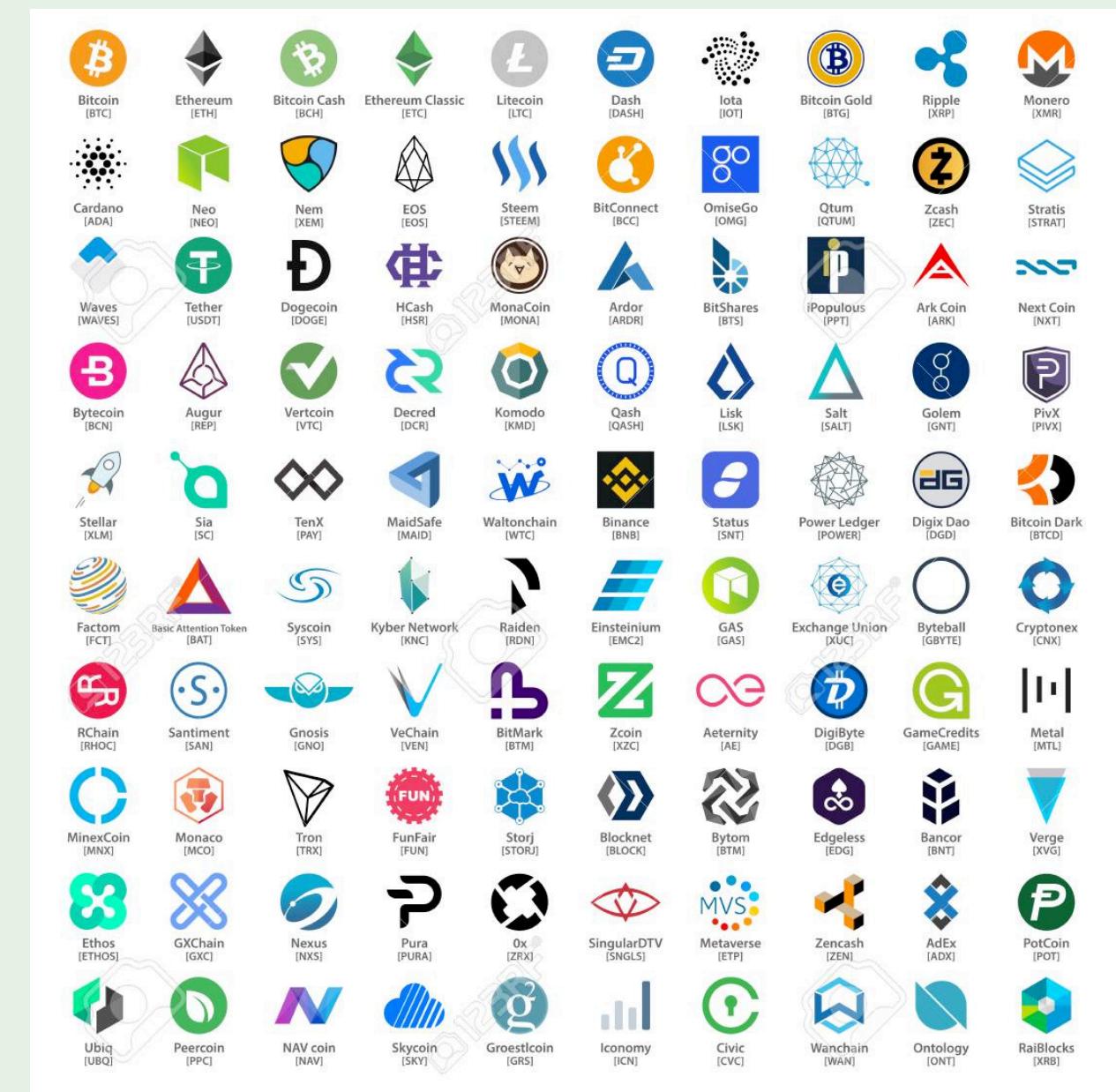
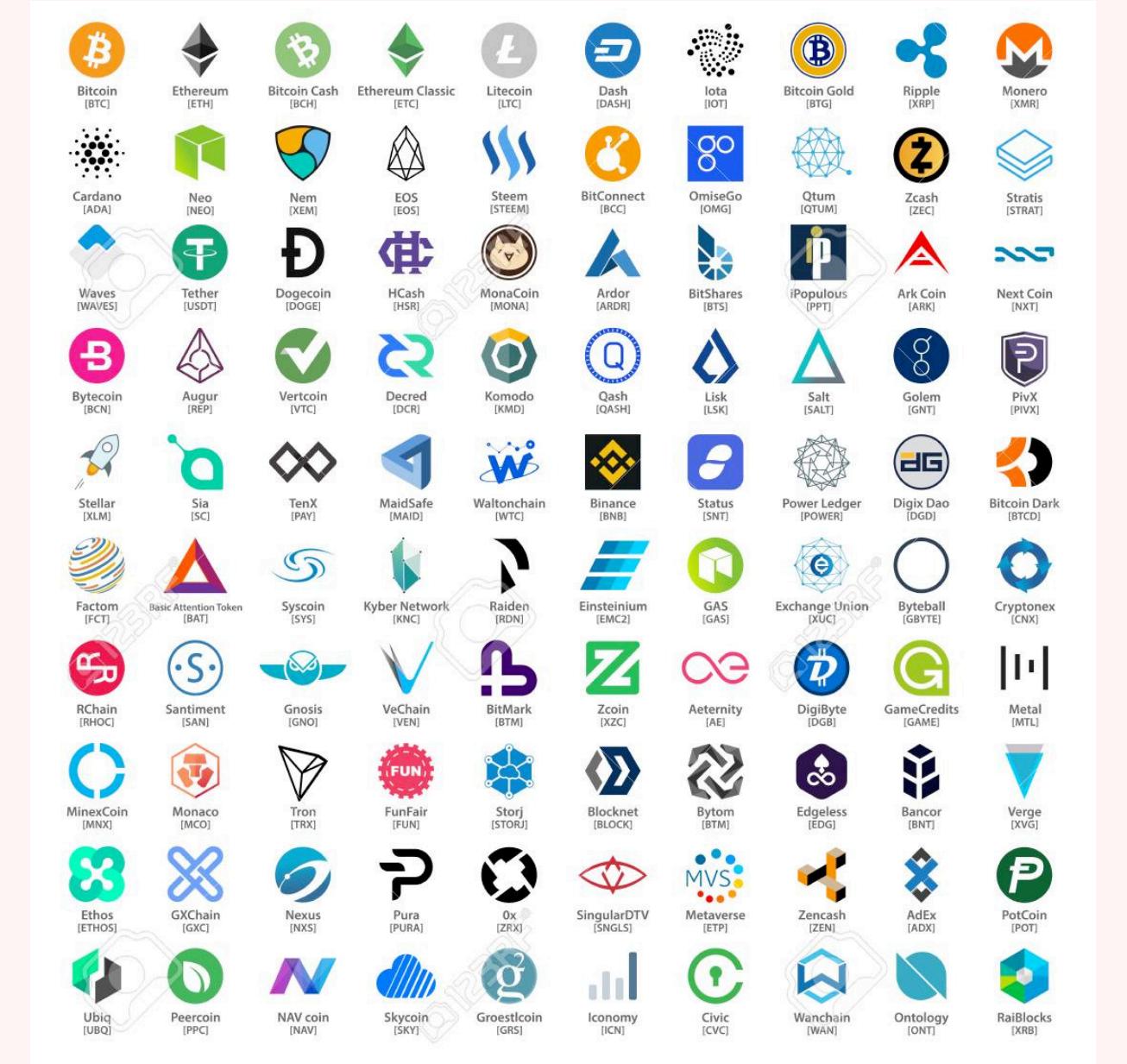
### Which programs are fastest?

“Our results show that real web applications behave very differently from the benchmarks...”

Too hard, let's go measure ... benchmark programs !

{ Which are fastest? } fannkuch-redux  
n-body    spectral-norm    mandelbrot

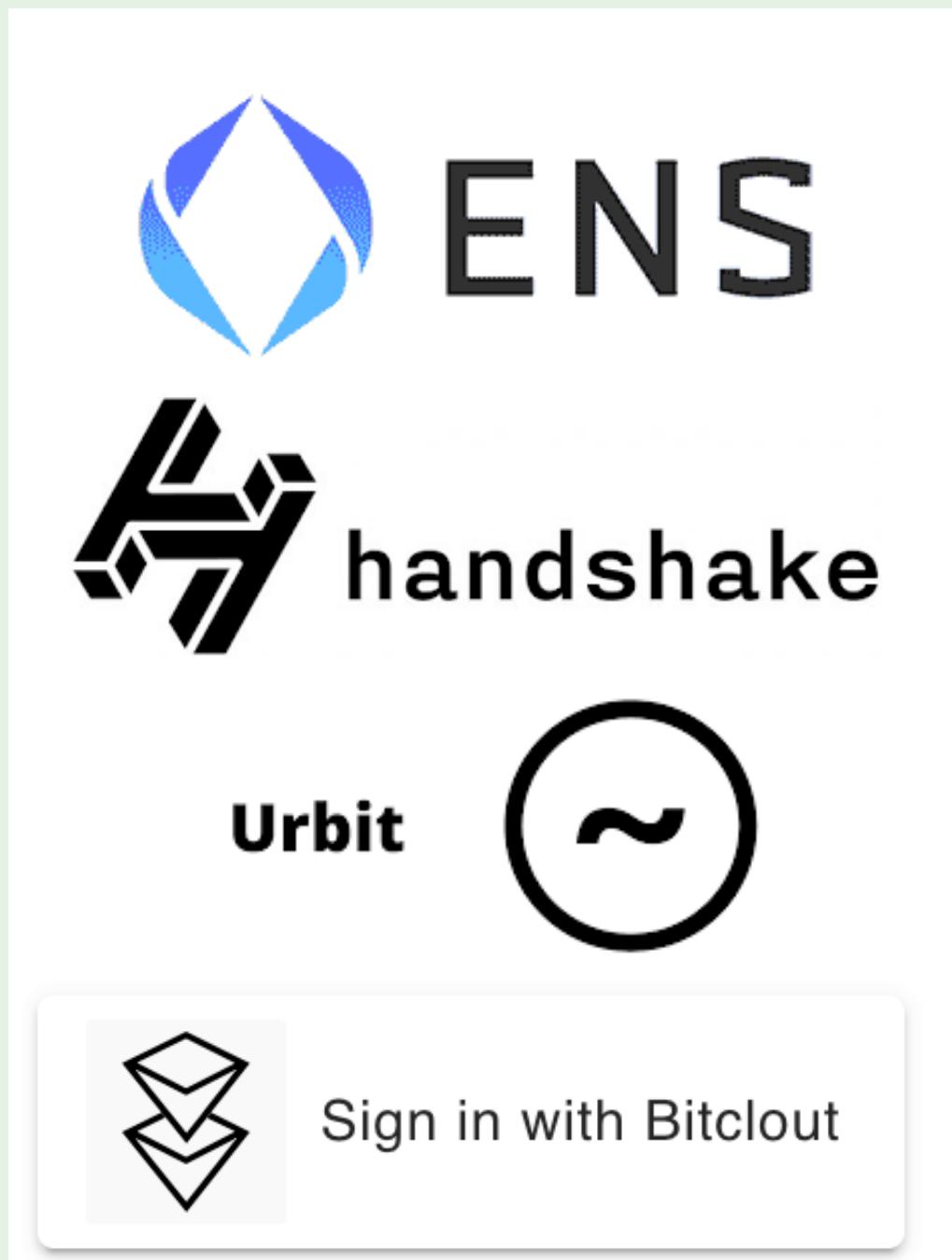
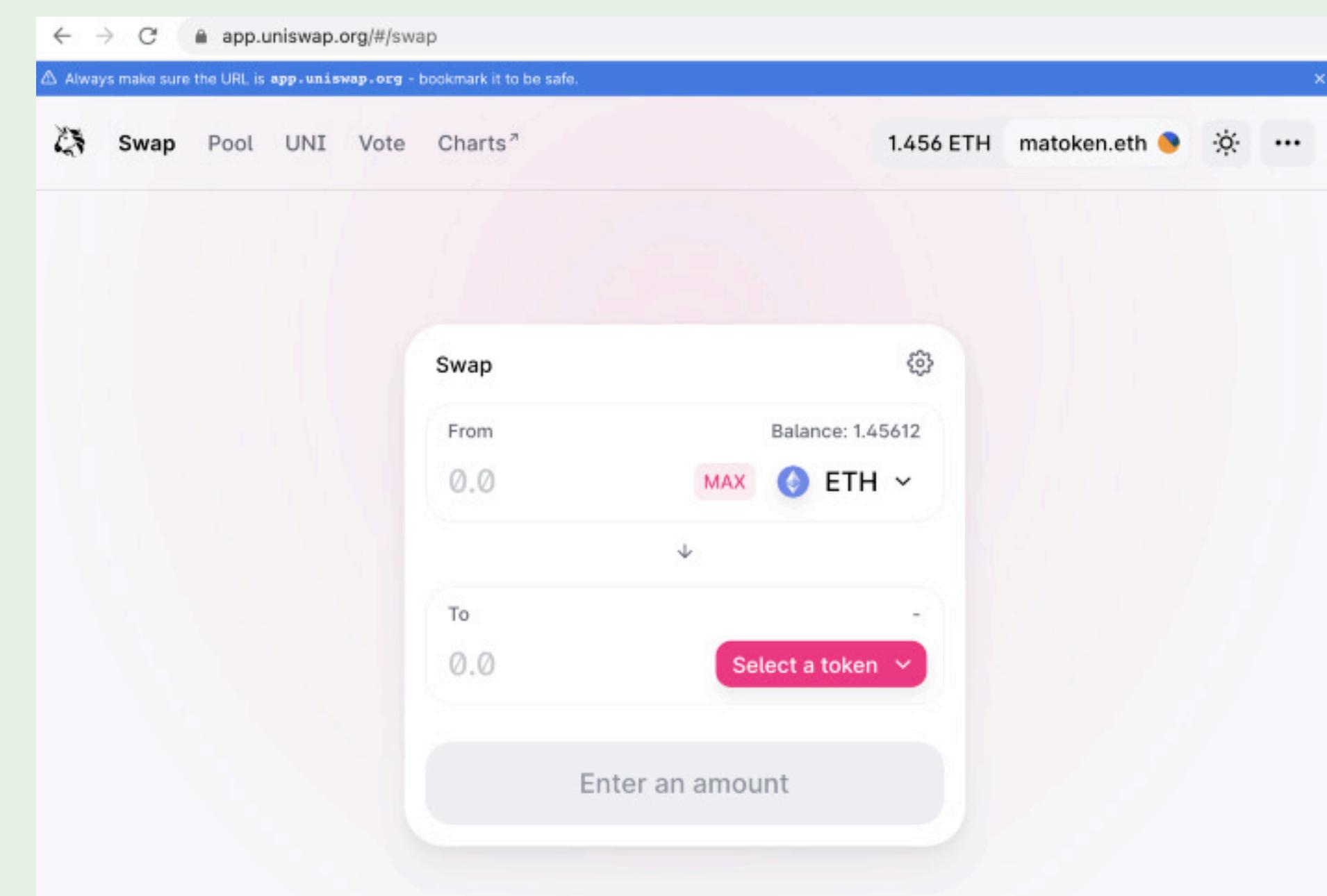
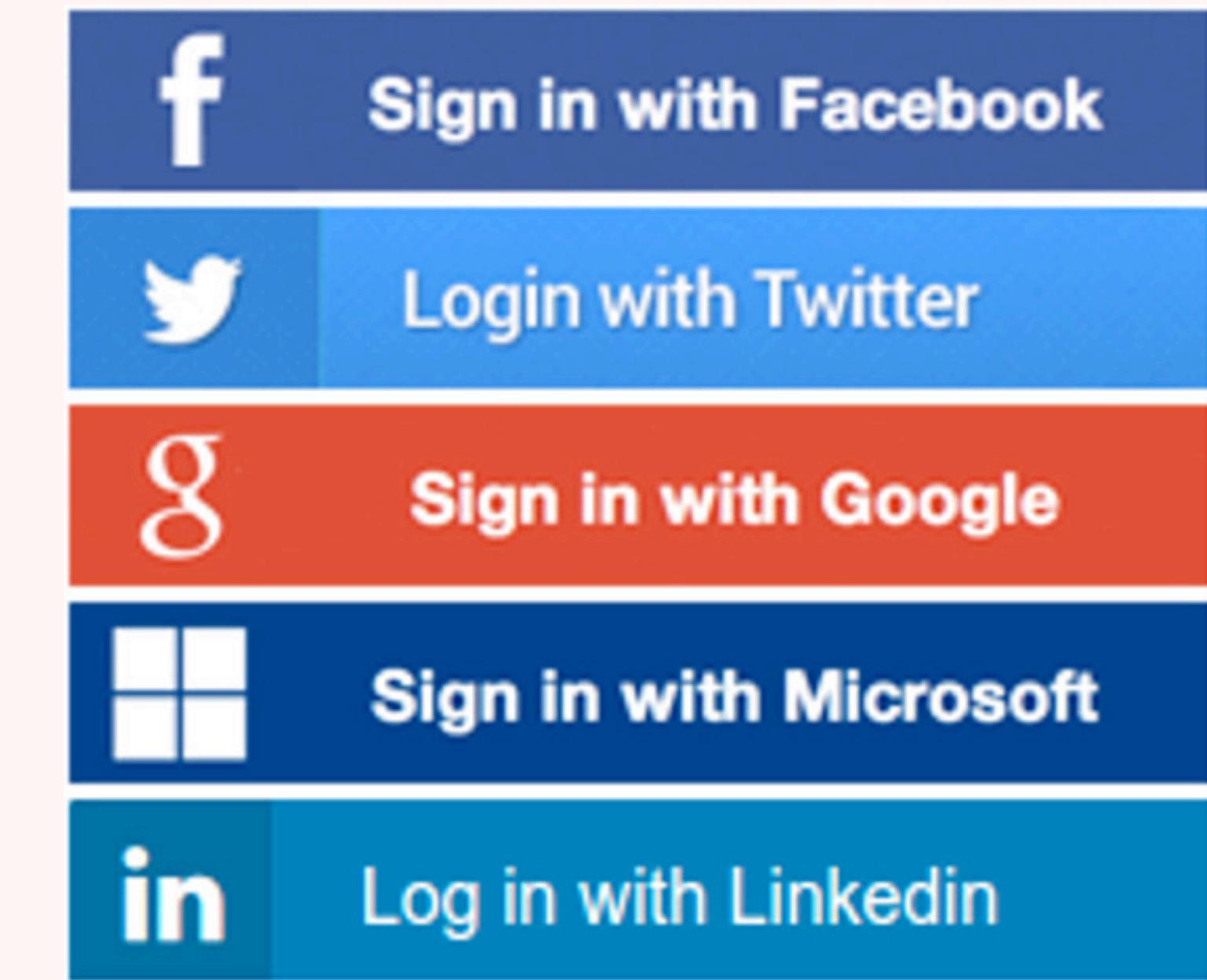
for



# Decentralized Login Widget: ENS, Urbit, Bitclout

We're gradually moving from  
passwords to private keys.

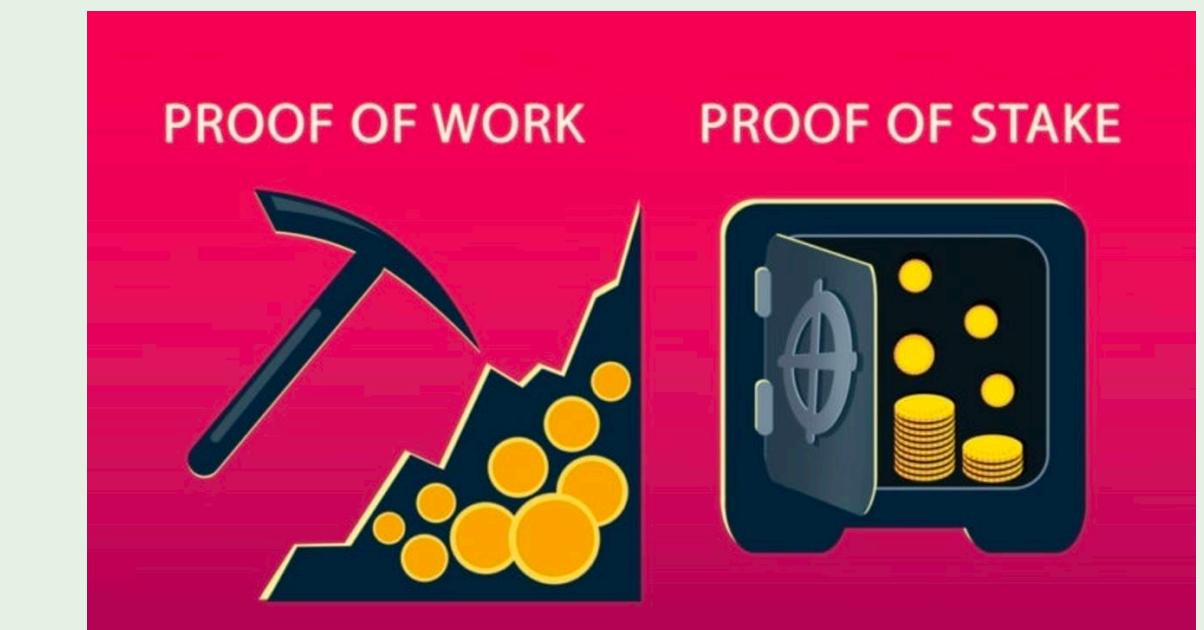
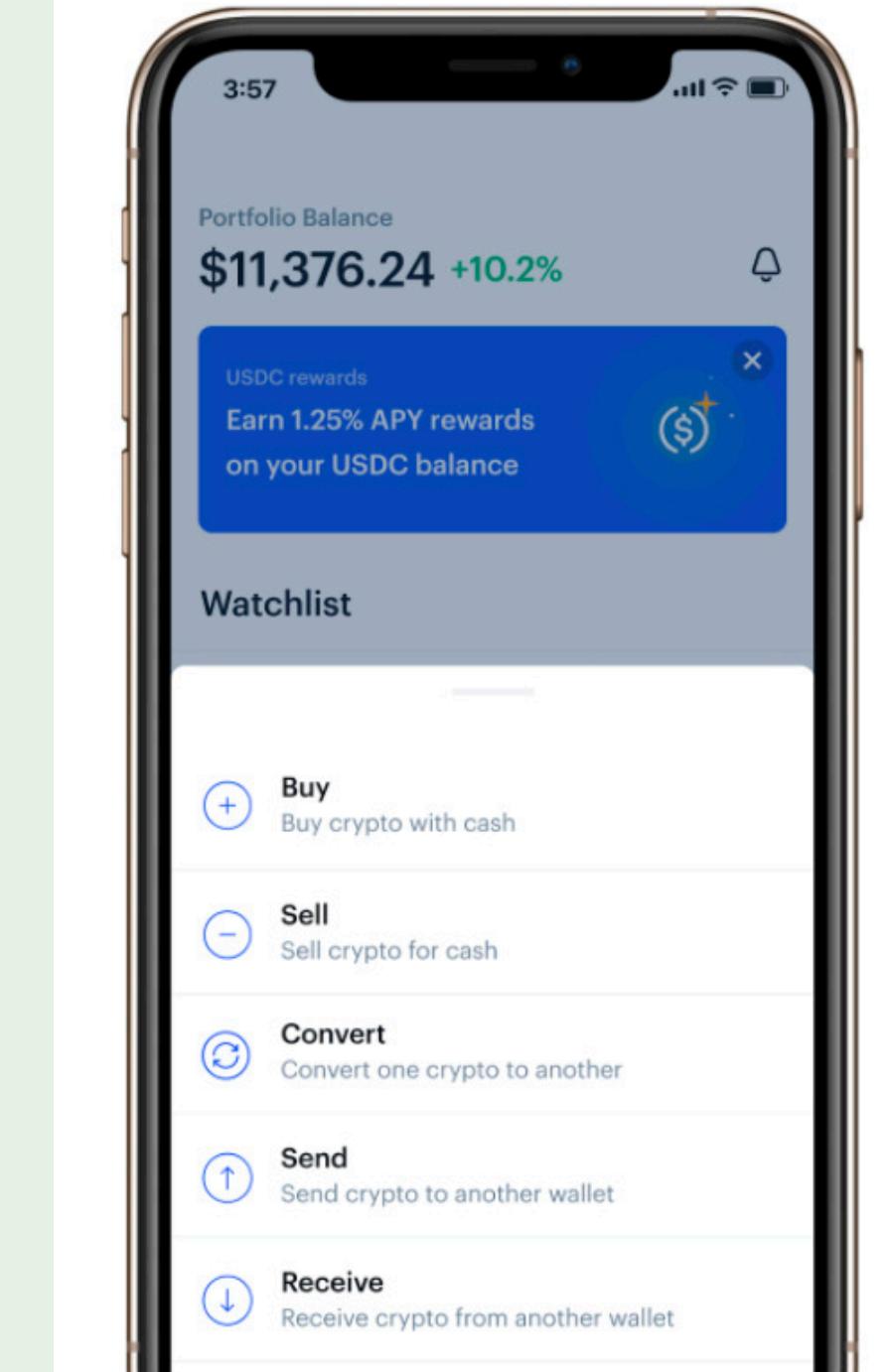
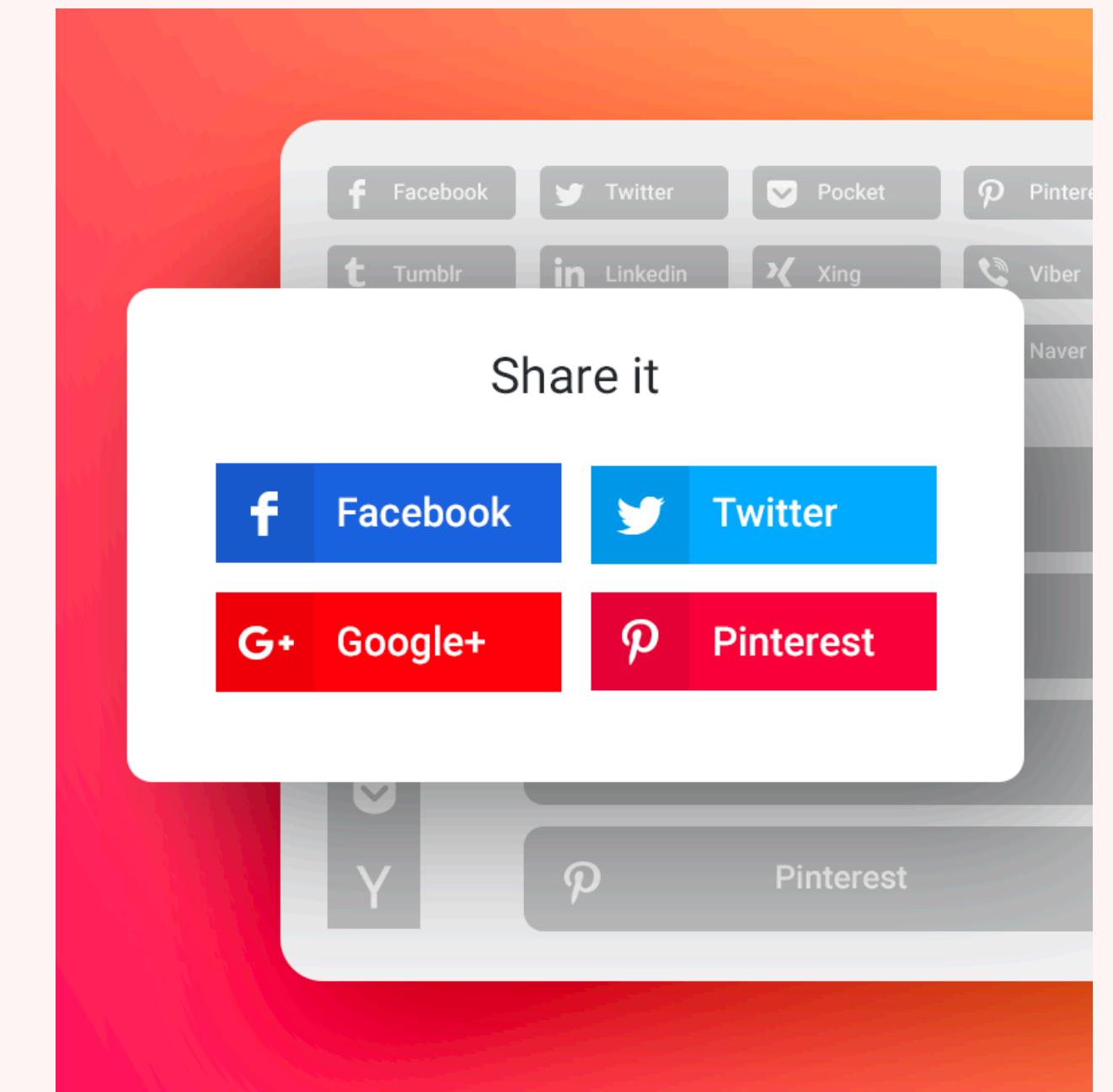
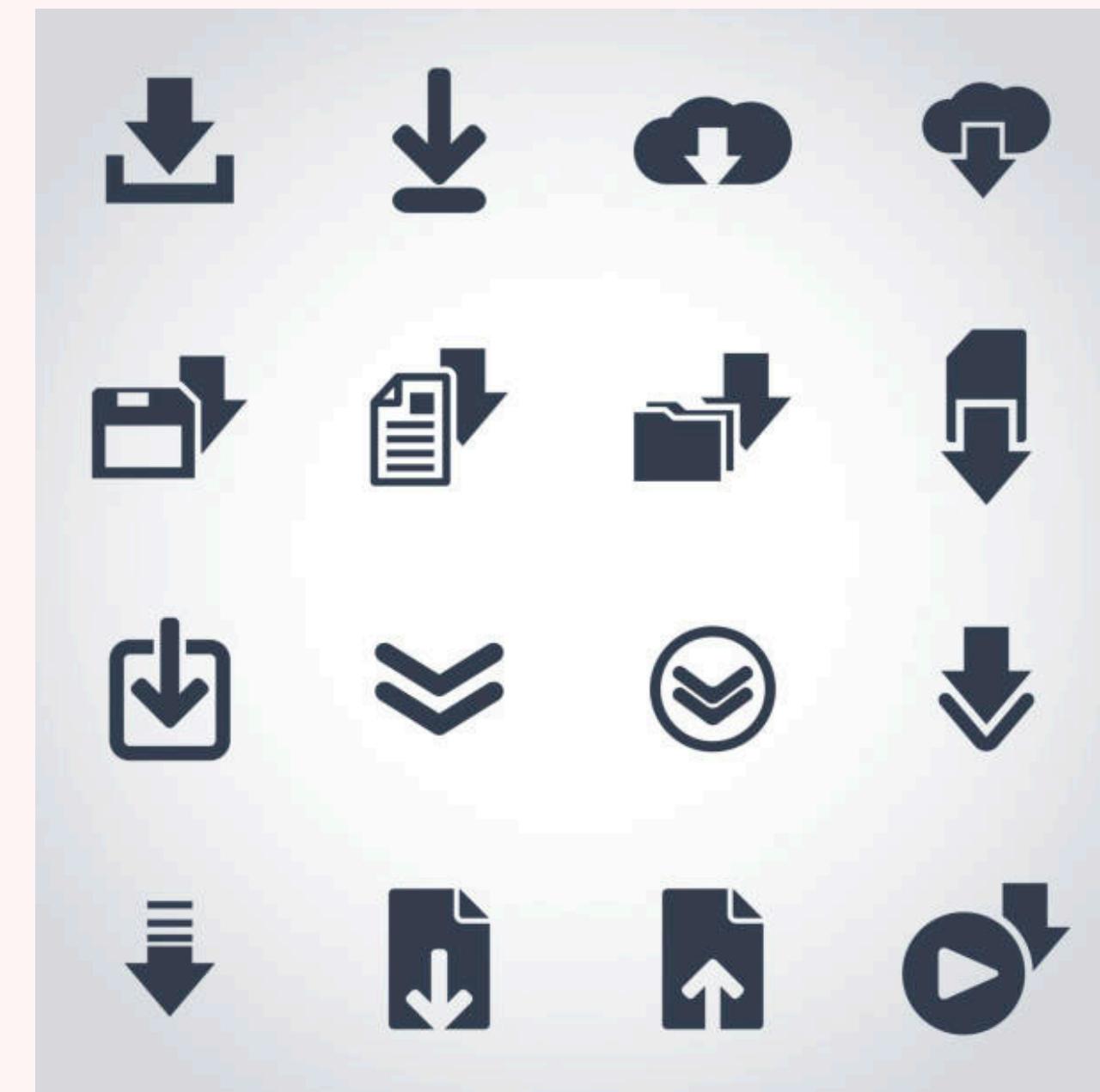
Can we go from the old school login  
widget to a simple new cross-  
service decentralized login widget?



# Enumerating the Nouns and the Verbs

In 2018 I gave an internal talk at Coinbase on the nouns (holders, miners, devs) and the verbs (buy, sell, send, receive) of the cryptoeconomy.

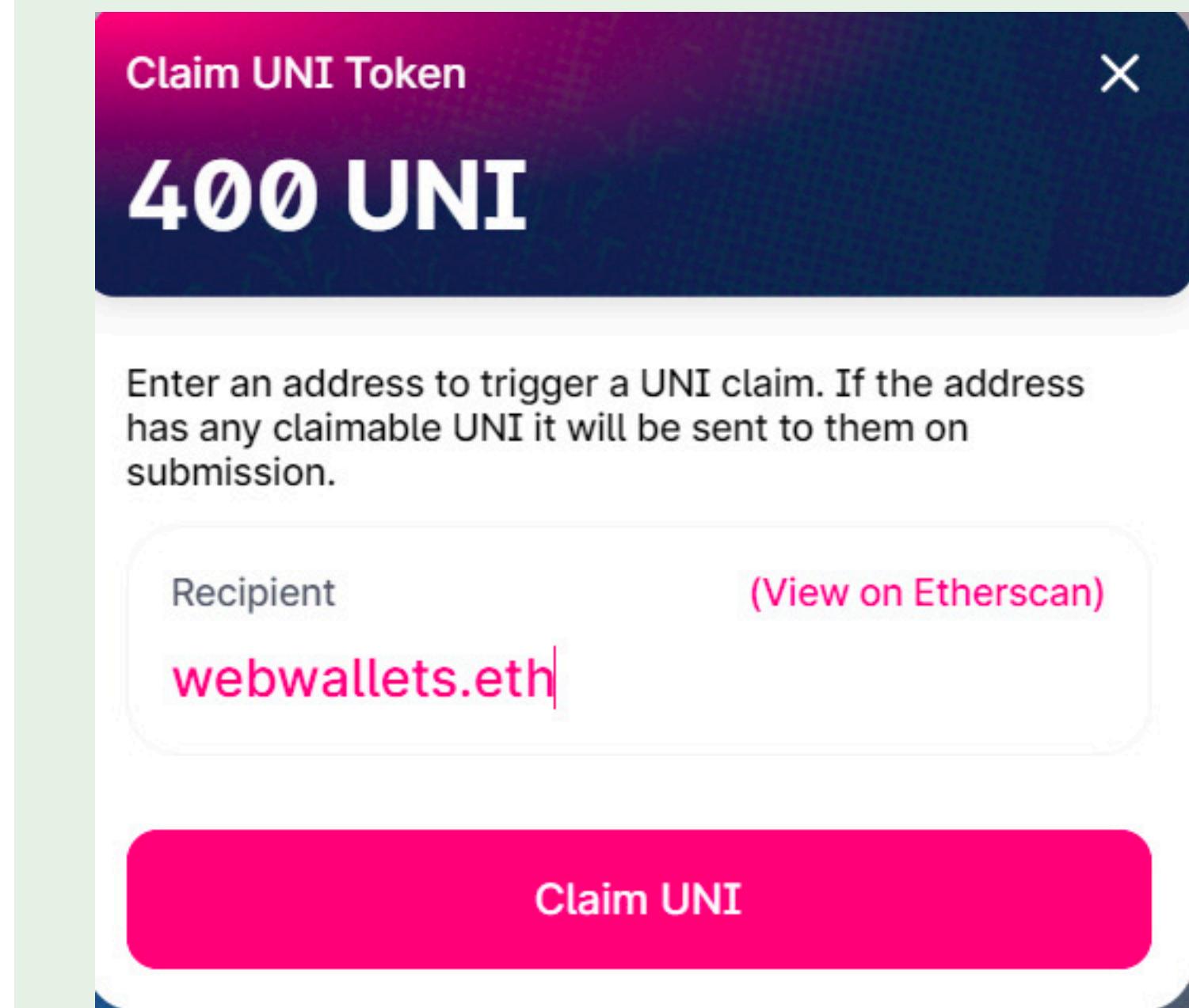
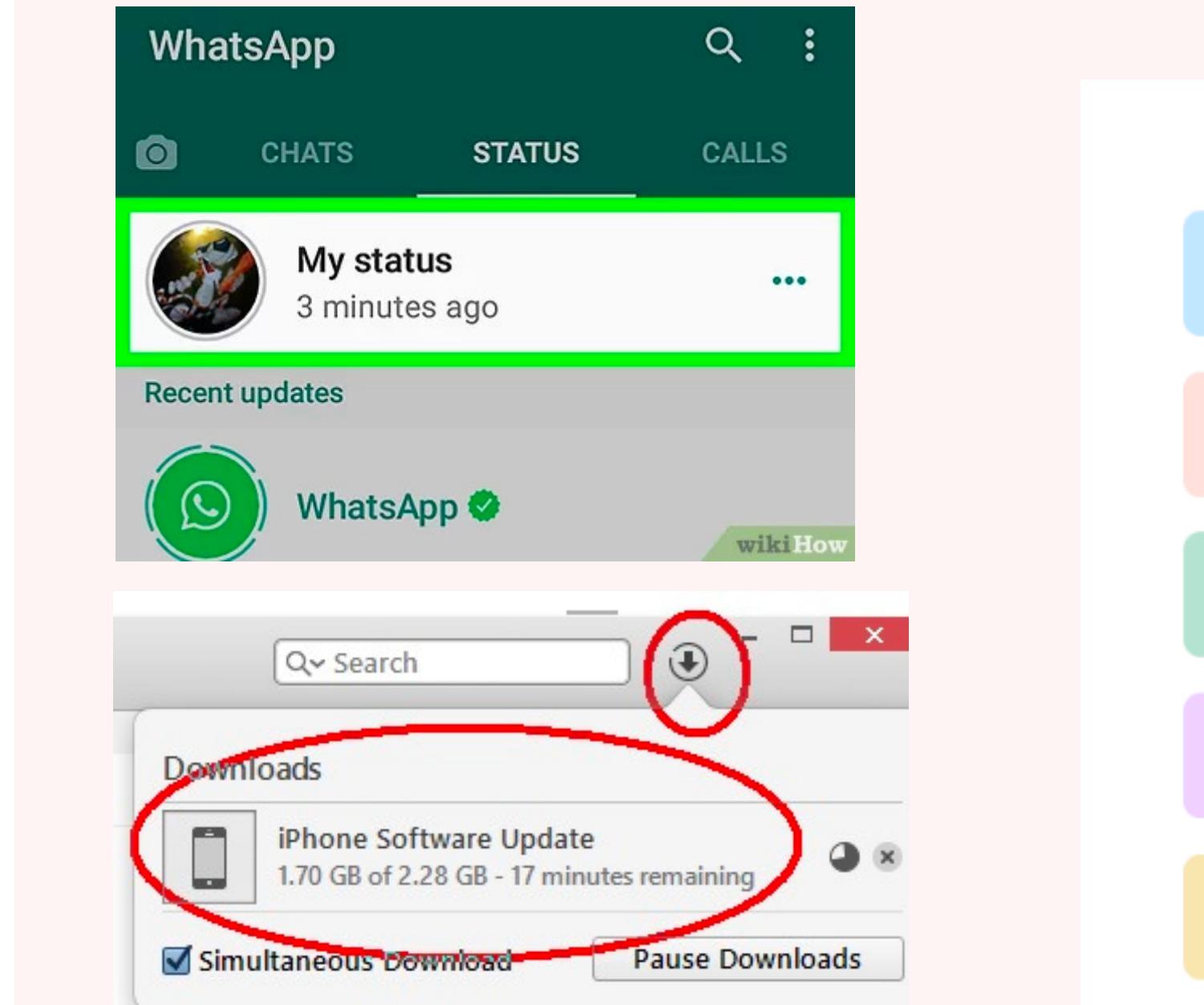
Can we enumerate all nouns and verbs, and how they connect?



# A web3 status dashboard

As simple as it sounds. For each coin, is it pre-launch, testnet, post-launch, etc?

Do we need to pick up our coins, or migrate them, or do something?



1729

**[support@1729.com](mailto:support@1729.com)**

If you build any of these, email us and we may fund them :)

# Next Steps

Please fill out the feedback form!

<https://airtable.com/shrcd0go4YeNQZdKS>