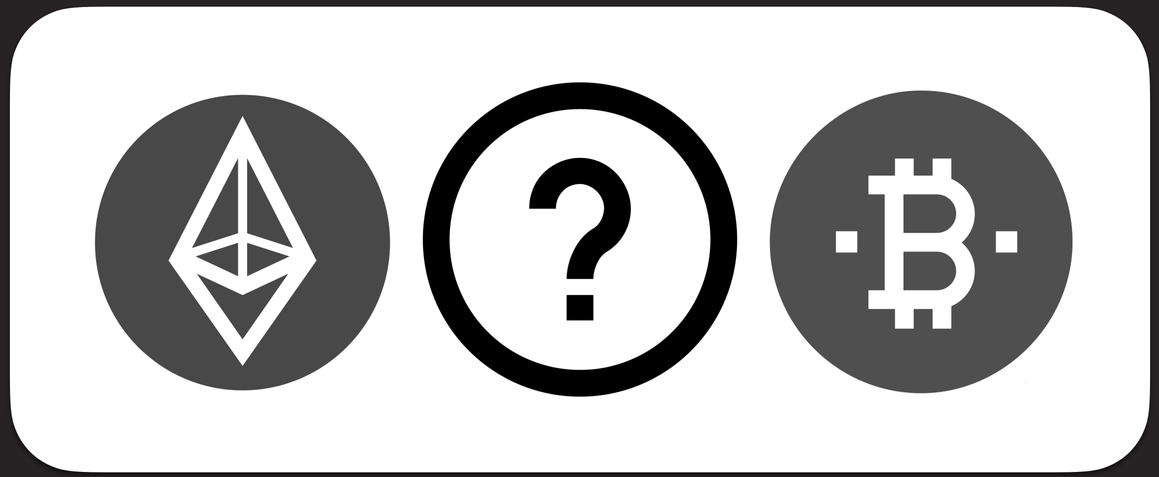
1729

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

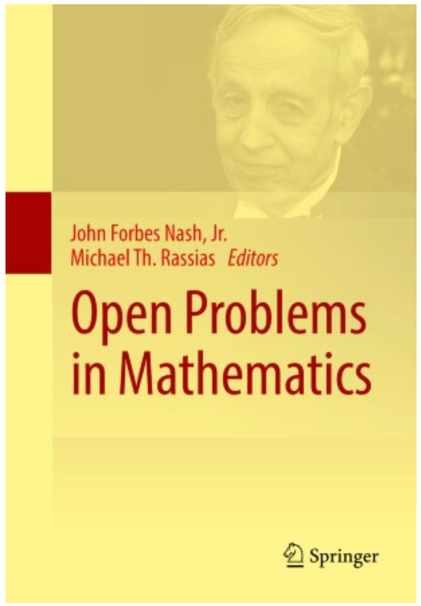
Open Problems

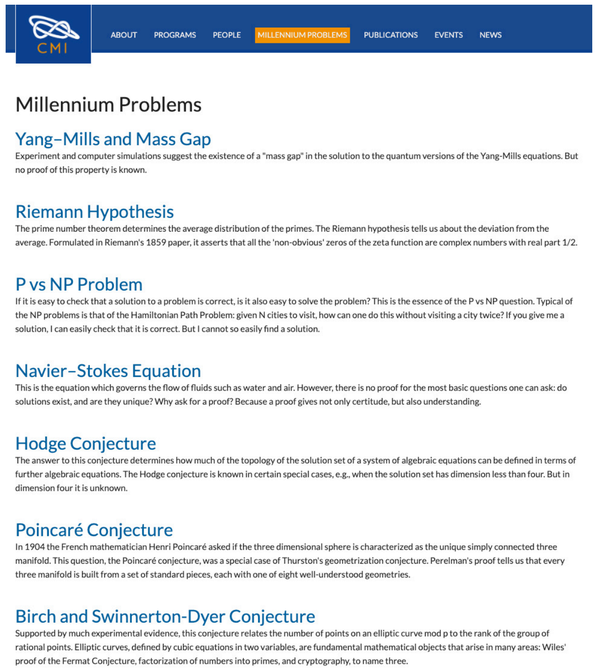
Motivation

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

Example: prize competition at 1729.com/inflation

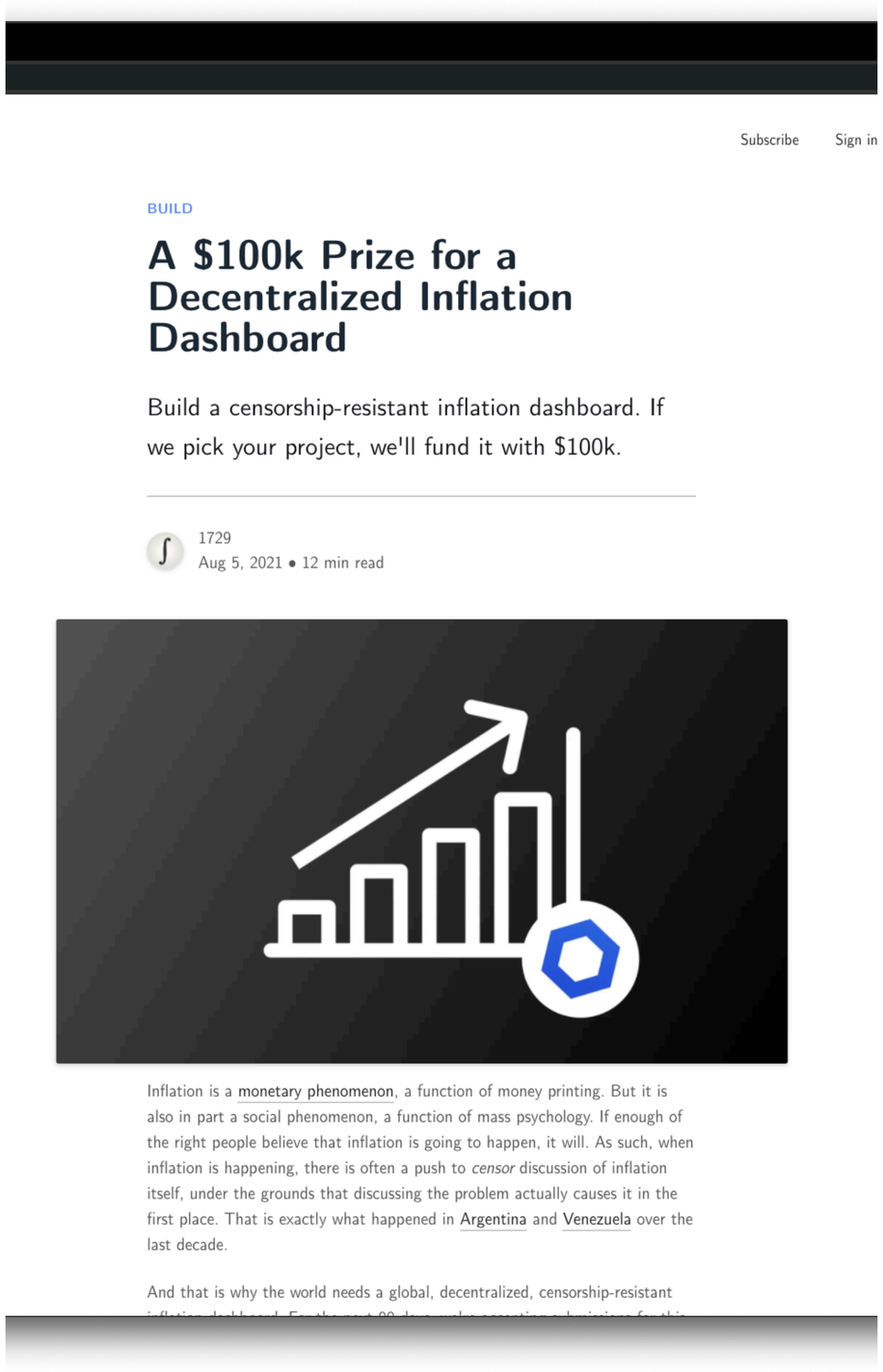
Today's talk is on a series of such (unsexy) problems, where funding is available if you solve them





Example: A Decentralized Inflation Dashboard

This one is written up completely at 1729.com/inflation



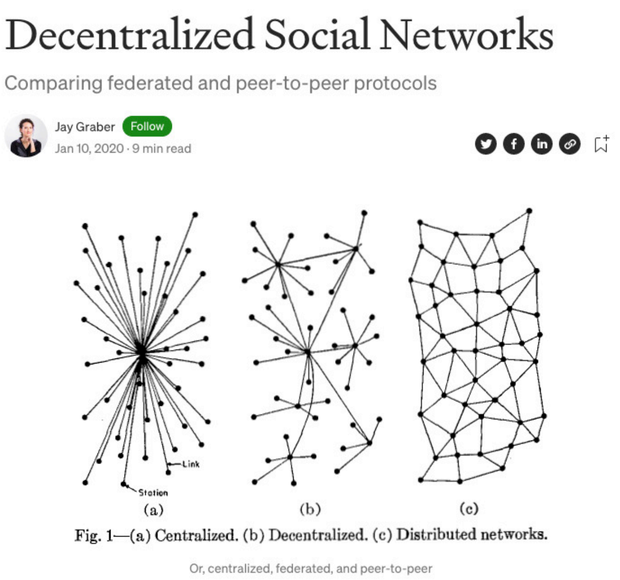
Do a Review, a GitHub, a Microsite, *then* Startup

A startup is a multiyear commitment.

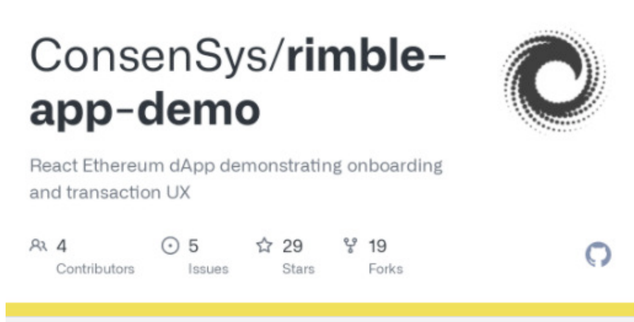
You can start with a technical review, a simple blog post on the area. Then set up a GitHub that you start poking at. Then deploy a microsite. Finally, if the initial traction works, do a startup.

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

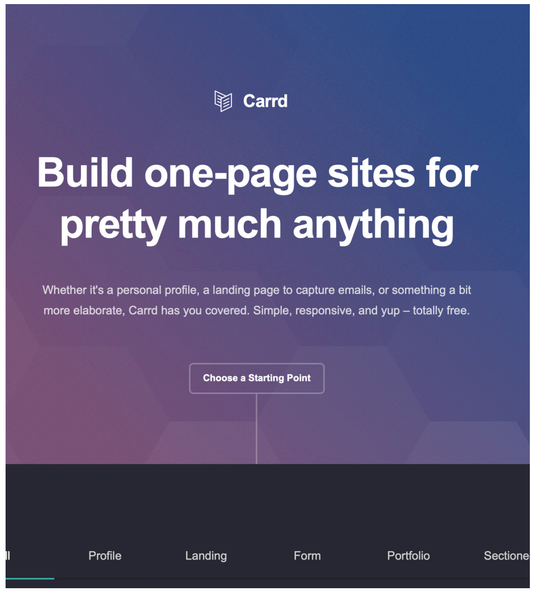
1



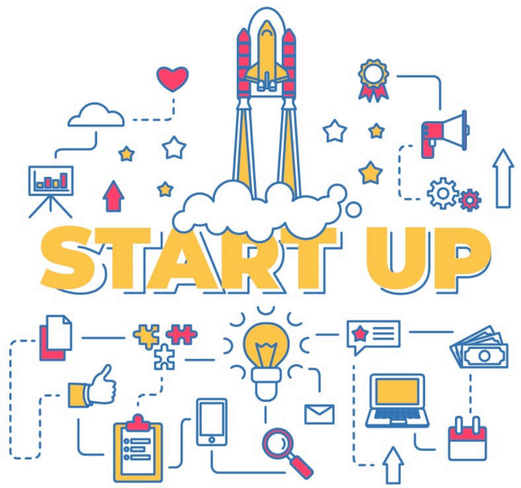
2



3



4



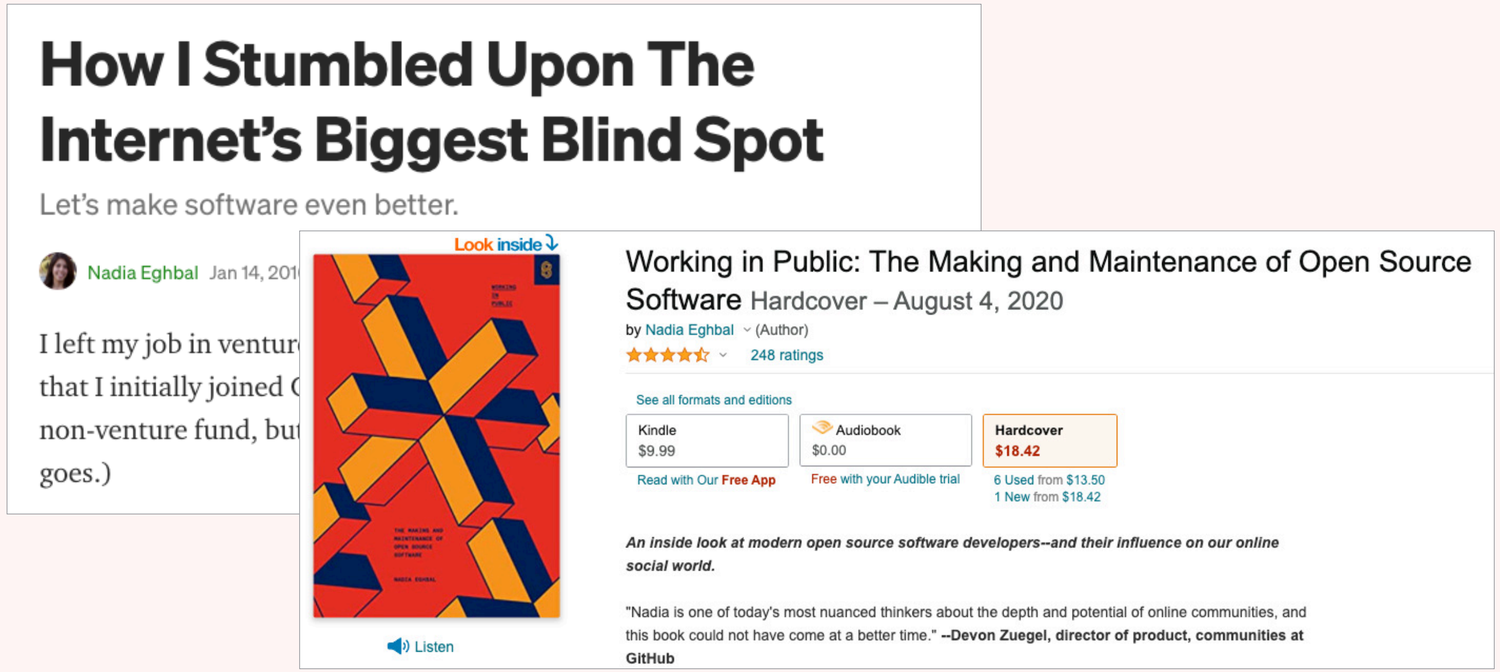
Overview: Blog, GitHub, Microsite, Startup

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



How I Stumbled Upon The Internet's Biggest Blind Spot

Let's make software even better.

Nadia Eghbal Jan 14, 201

I left my job in ventur
that I initially joined
non-venture fund, but
goes.)

Look inside

Listen

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 — Read with Our Free App

Audiobook $0.00 — Free with your Audible trial

Hardcover $18.42 — 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

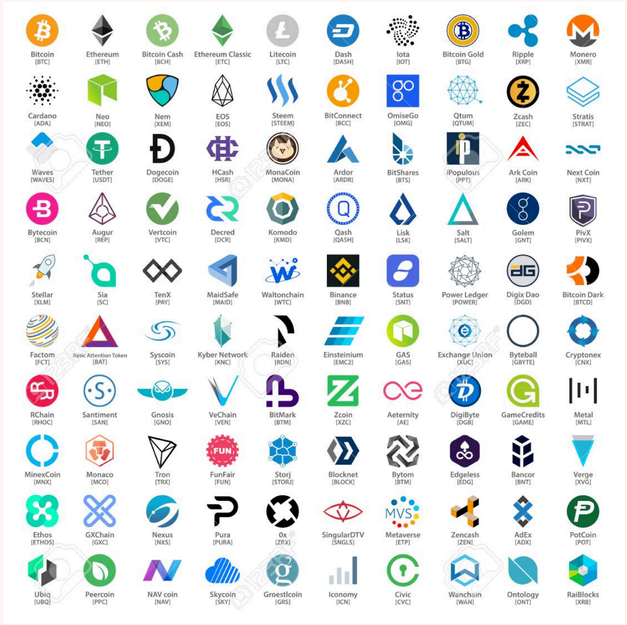
337 Retweets **128** Quote Tweets **2,251** Likes

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
bit.ly/2ULcimi
bit.ly/3mBbn3l

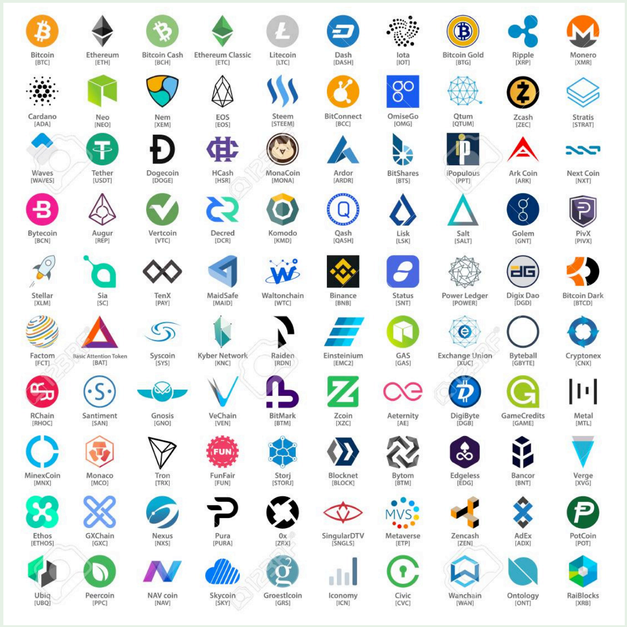
PostgreSQL



PostGIS
Spatial PostgreSQL

for

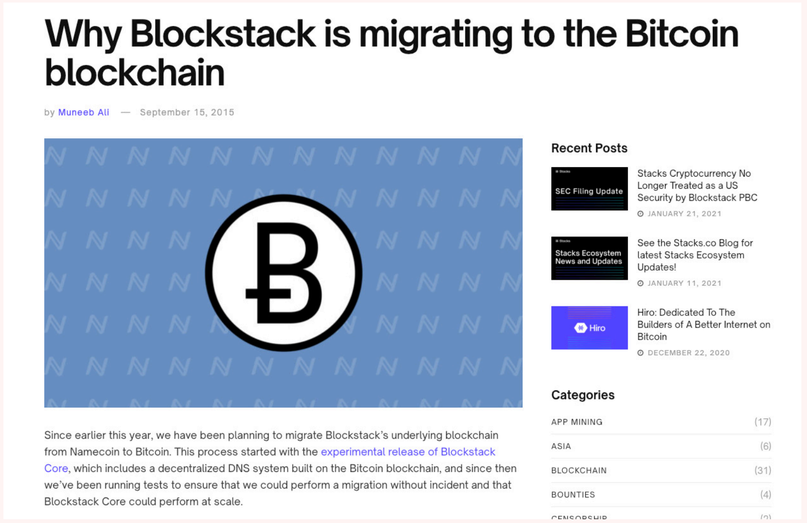
Rosetta

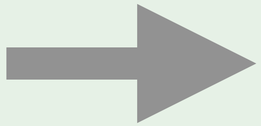


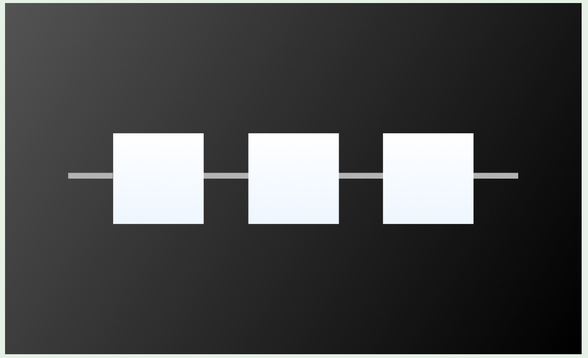
Chain Migration and Interoperation

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?





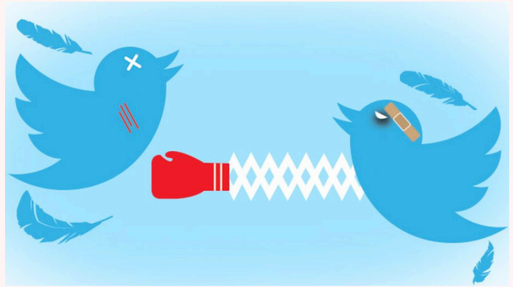


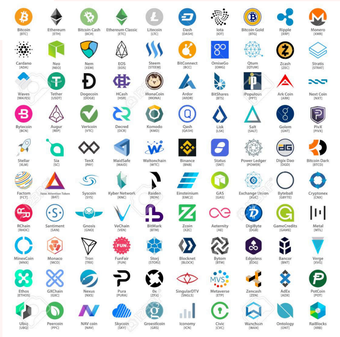
Quantifying & Optimizing Decentralization

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

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 $p_1 > \ldots > p_K$ 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:

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

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:

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

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:

$$g_j(x) \geq 0, \ j = 1, ..., J;$$

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

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

Anatoly Yakovenko @aeyakovenko · Aug 21

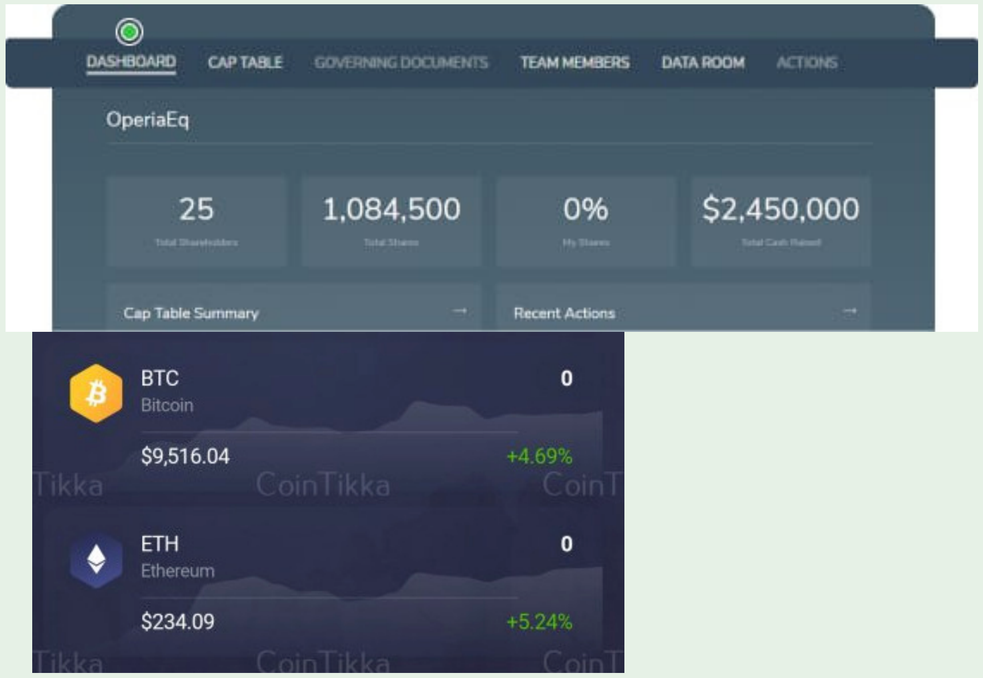
how is solana trading decentralization? the key facet we are focusing on is the **Nakamoto Coefficient**, aka the min set of nodes that add up to 33%. Eth2 is not focusing on that facet, instead on minimizing the cost of the honest majority to detect fraud proofs.

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



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

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

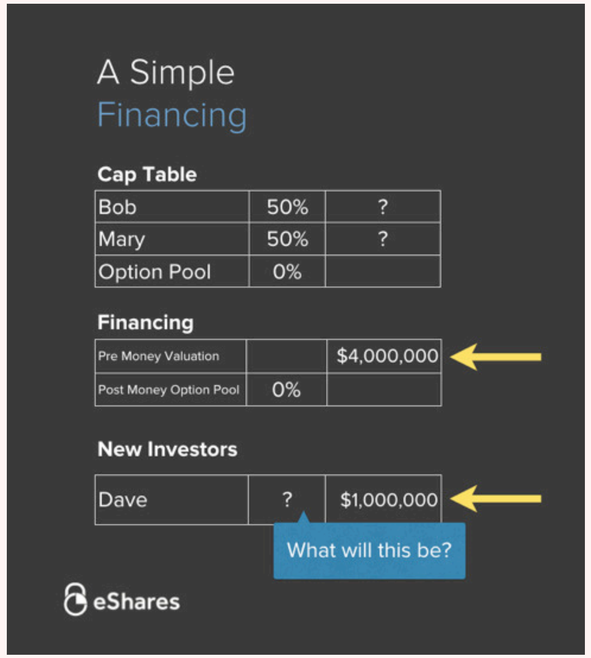
Income Statement	Balance Sheet	Cash Flow Statement
	Accounts Payable 10	Increase in Accounts Payable 10

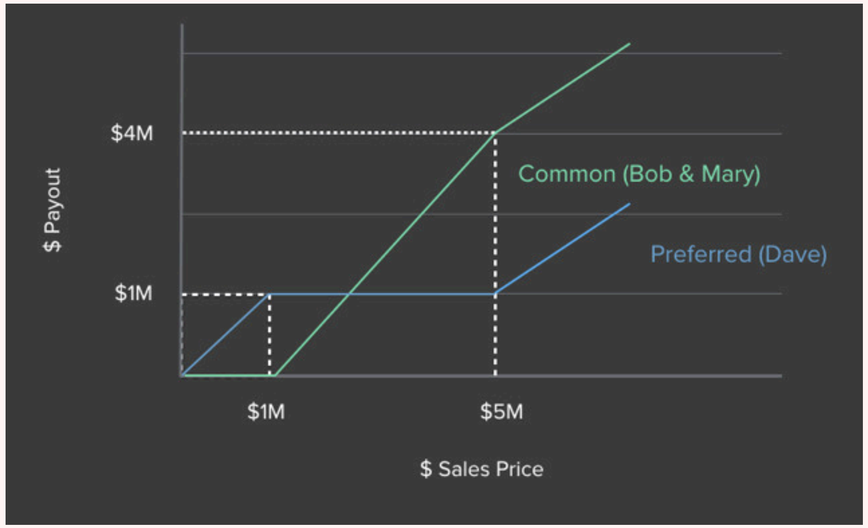
Income Statement		Balance Sheet		Cash Flow Statement	
Revenue	-	Cash at Bank	10	Cash Receipts	-
COGS	-	Current Assets	10	Inc. in Trade Creditors	10
Gross Margin	-	Non-Current Assets	-	Cash Payments	10
Operating Expenditure	-	**Total Assets**	**10**	**Operating Cash Flows**	**10**
EBITDA	-	Trade Creditors	10	**Investing Cash Flows**	-
Depn. & Amort.	-	Current Liabilities	10	**Financing Cash Flows**	-
EBIT	-	Non-Current Liabilities	-	**Δ in Cash Held**	**10**
Interest Expense	-	**Total Liabilities**	**10**		
NPBT	-	Retained Earnings	-		
Tax Expense	-	**Total Equity**	-		
NPAT	-	**Net Assets**	-		

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
balajis.com/mirrortables



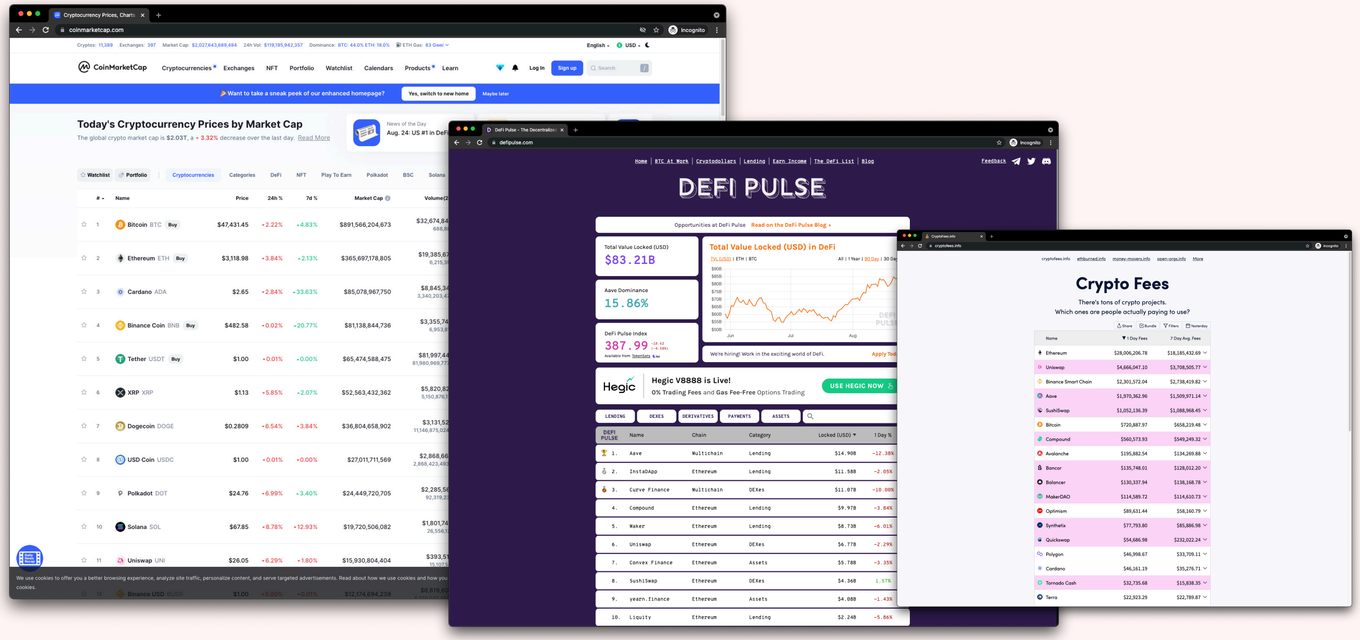


A Pluggable Dashboard of Dashboards

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

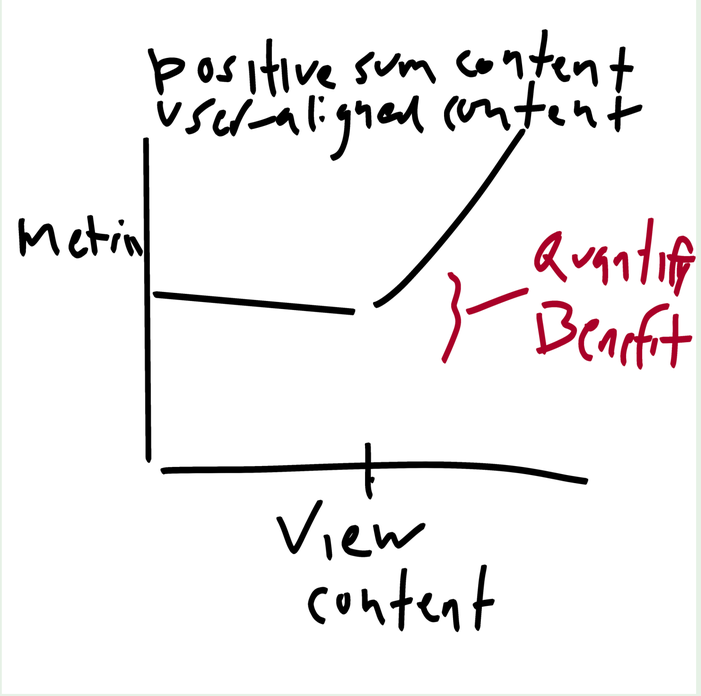


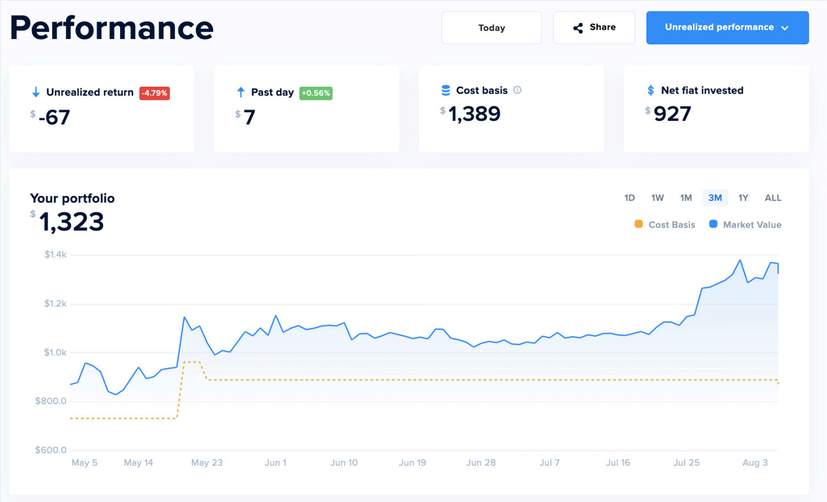
+

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?



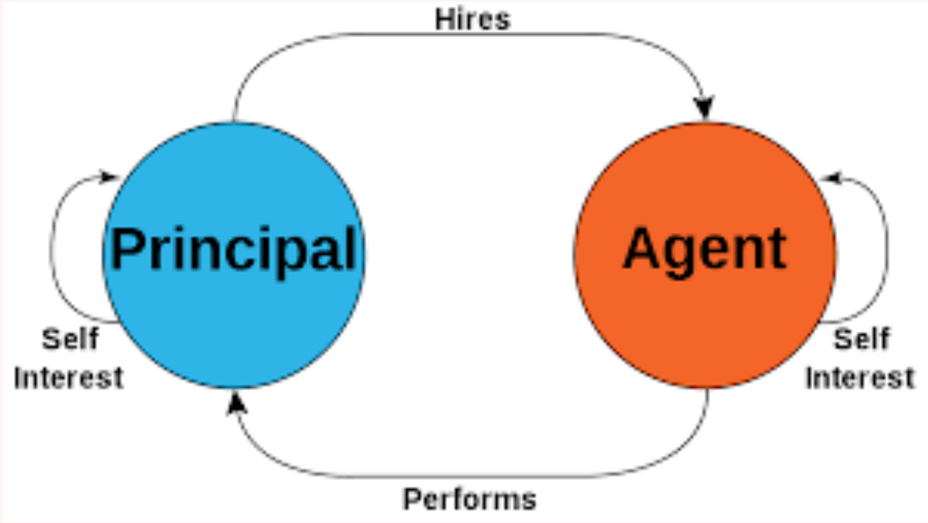


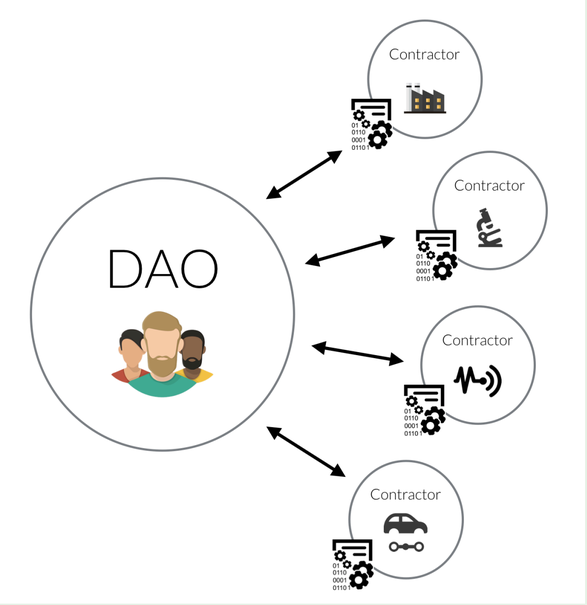
Principal Agent - Delegation/ACL for DAOs

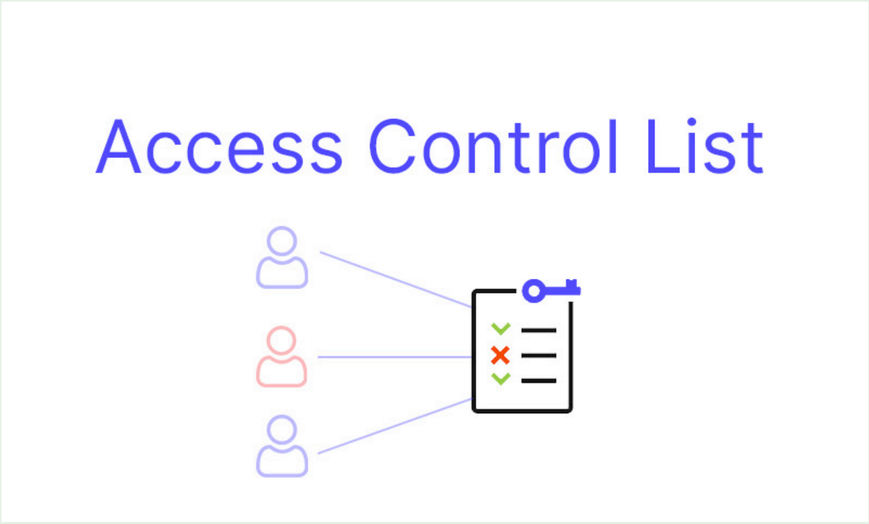
The principal/agent problem is about the divergence between any two parties in an orgchart.

Autonomy solves this: no person, no problem.

What's in between?



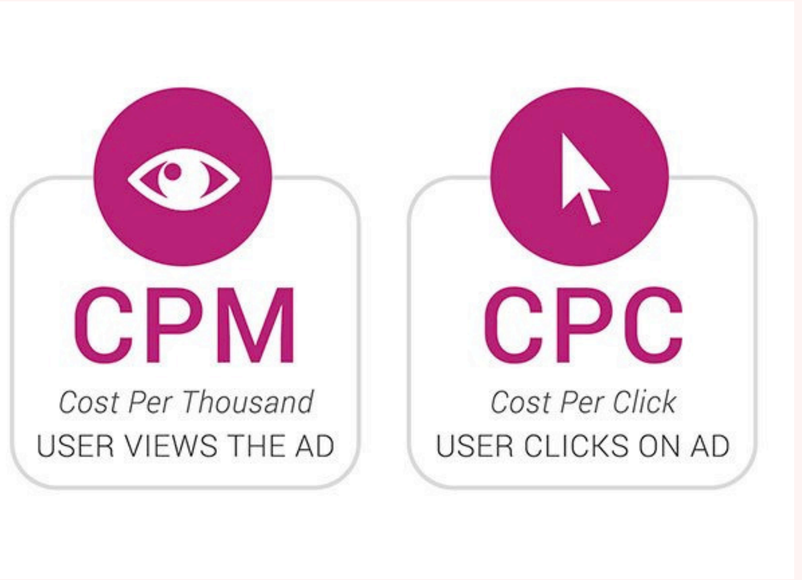


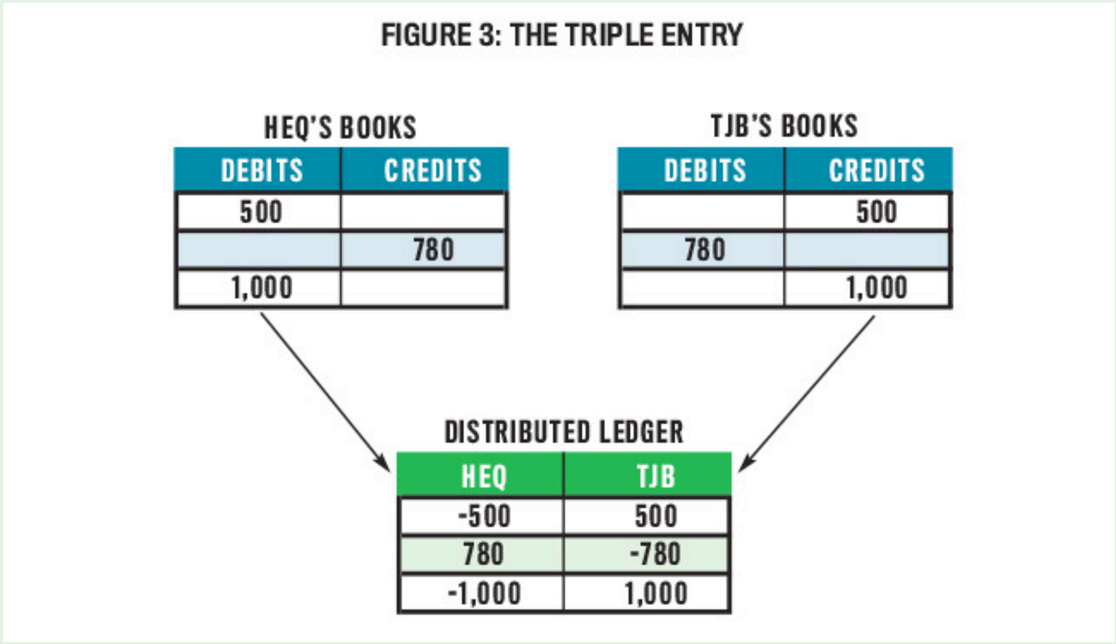


Pure CPA for web3 commerce

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?

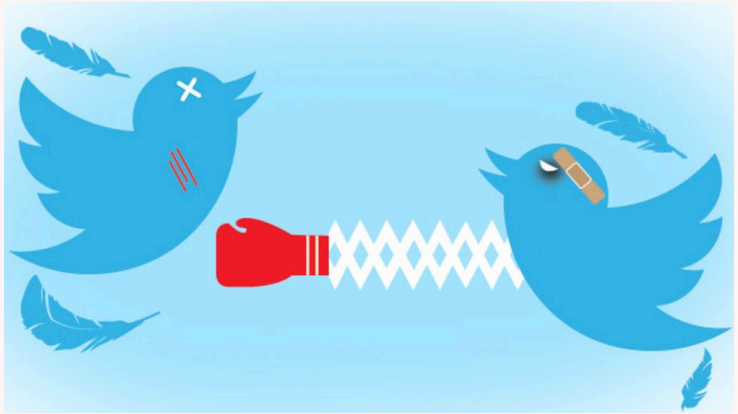


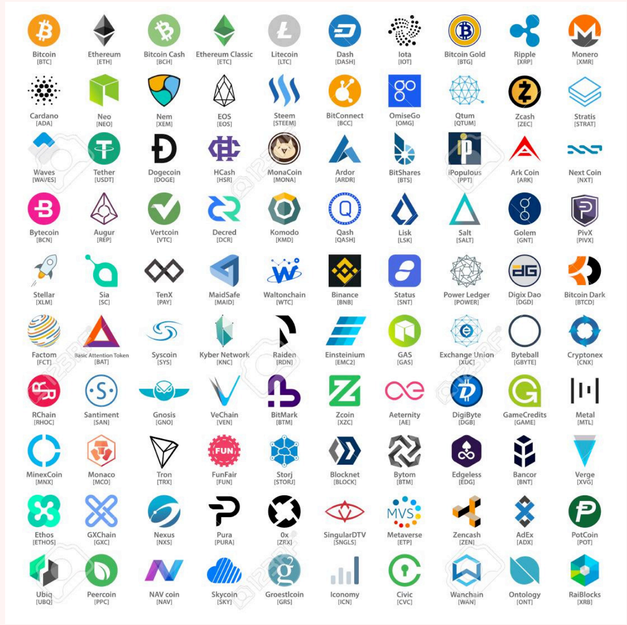


Blockchain / L2 Performance Shootout

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?

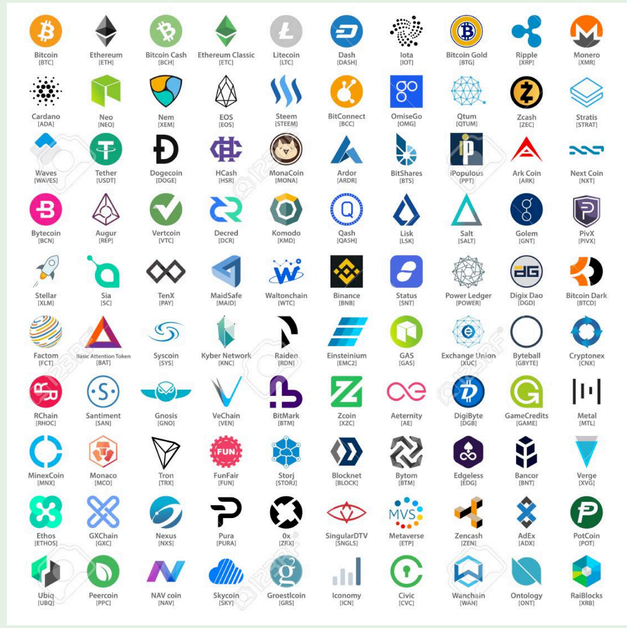
"Our results show that real web applications behave very differently from the benchmarks..."

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

{ Which are fastest? } fannkuch-redux

n-body spectral-norm mandelbrot

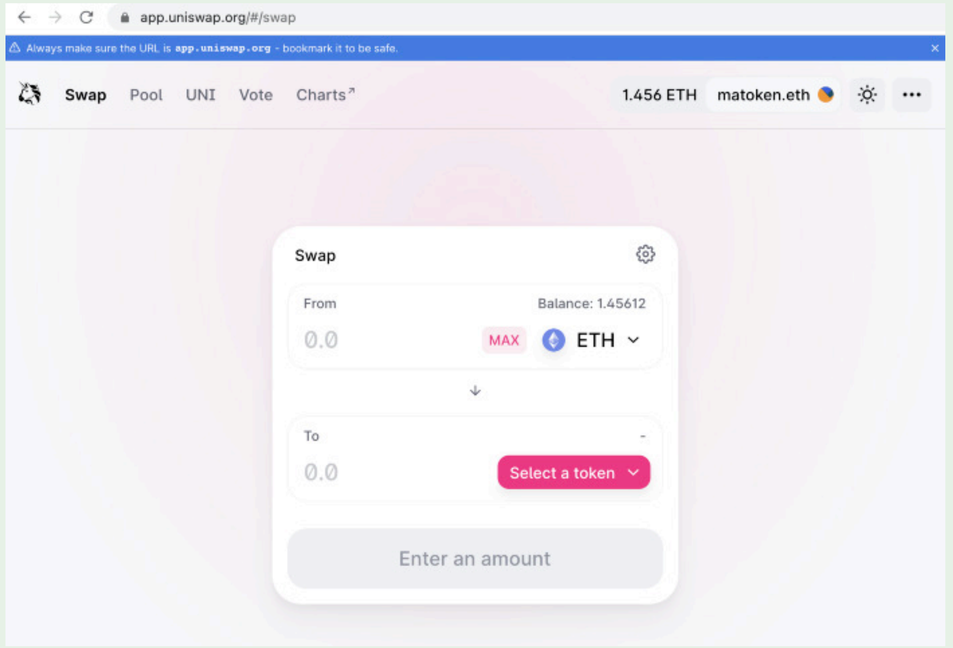
for

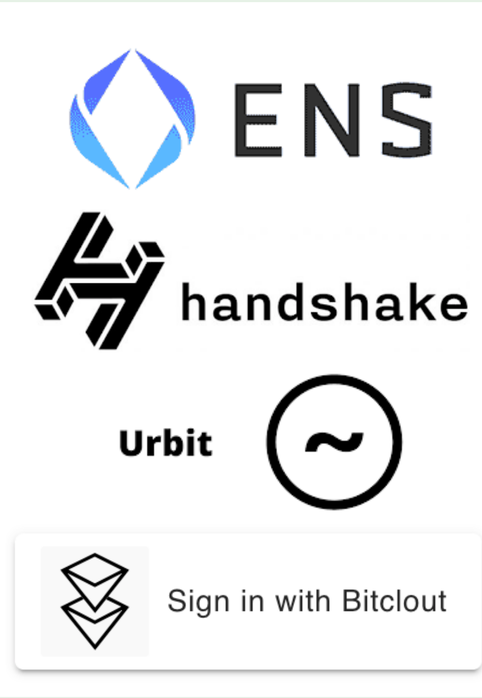


Decentralized Login Widget: ENS, Urbit, Bitclout

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?

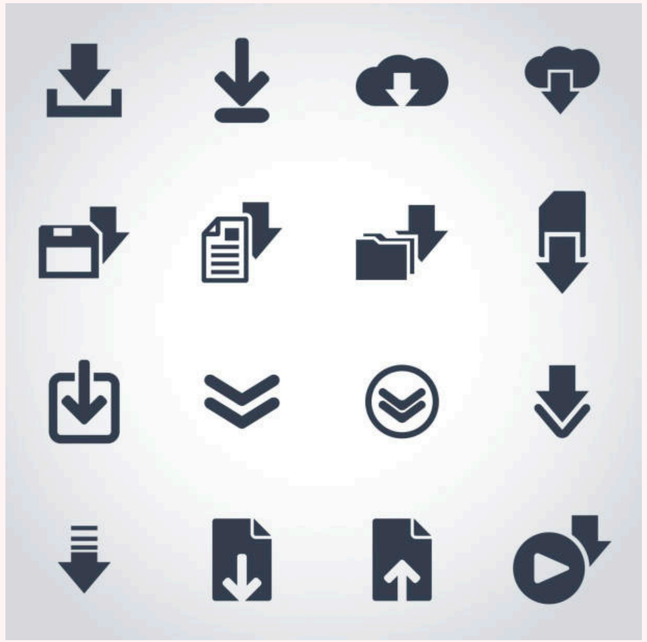


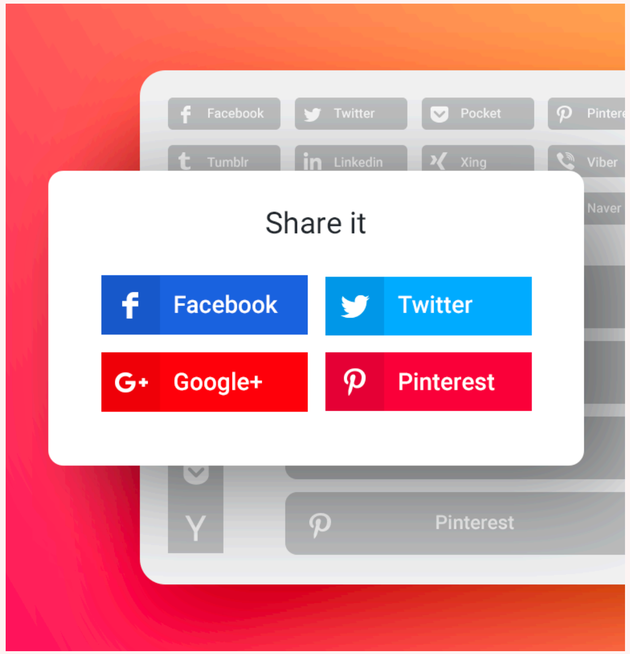


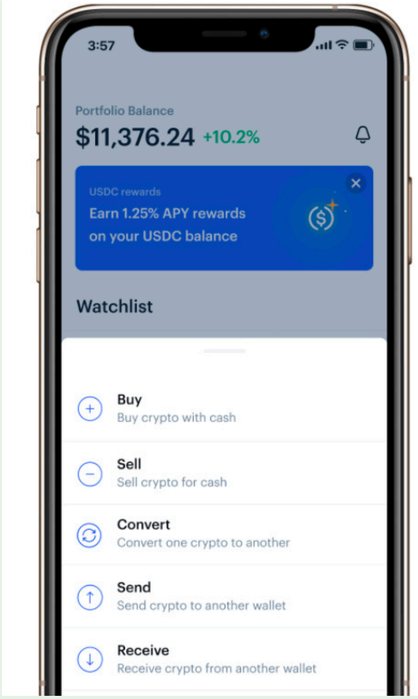
Enumerating the Nouns and the Verbs

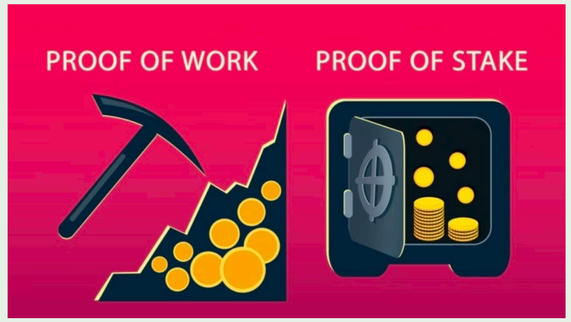
In 2018 I gave an internal talk at Coinbase on the nouns (holders, miners, devs) and the verbs (buy, sell, send, receive) of the cryptoeconomy.

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





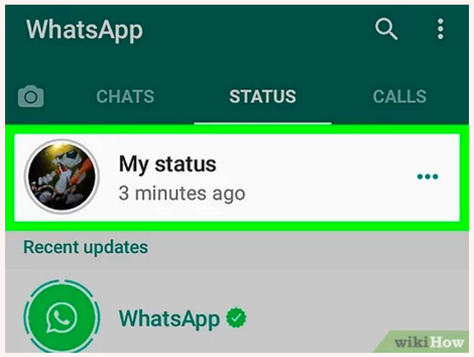


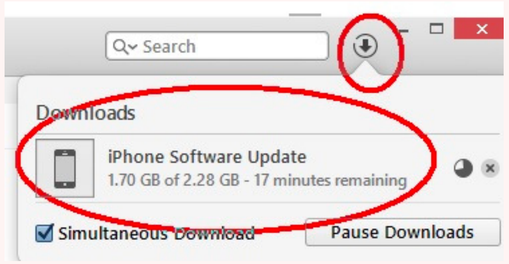


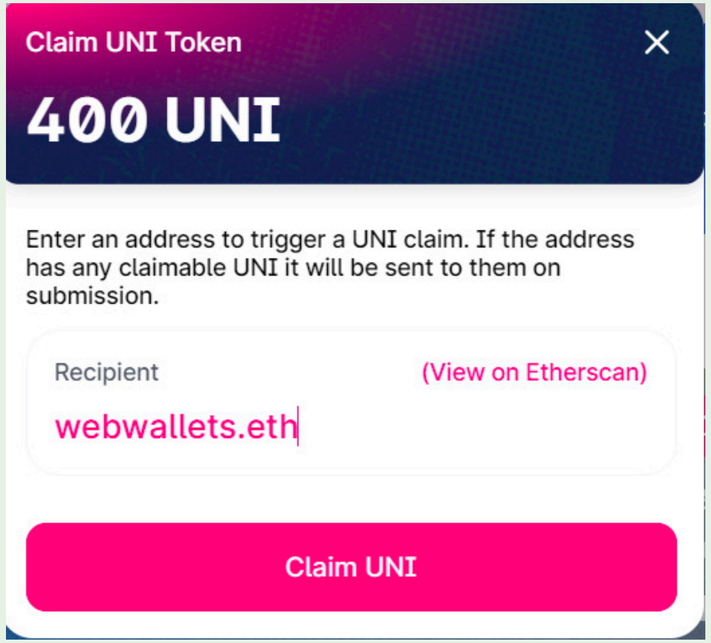
A web3 status dashboard

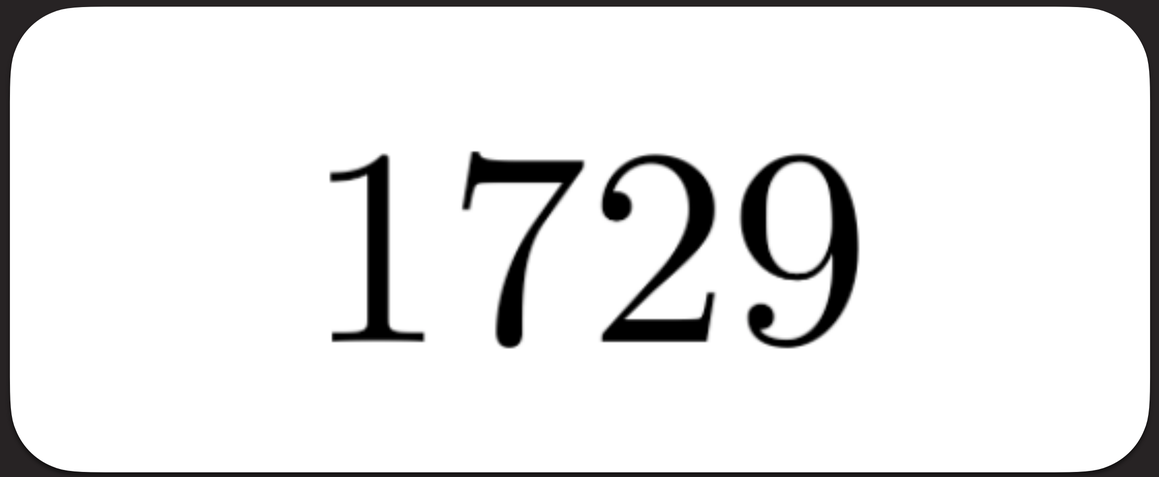
As simple as it sounds. For each coin, is it pre-launch, testnet, post-launch, etc?

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









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