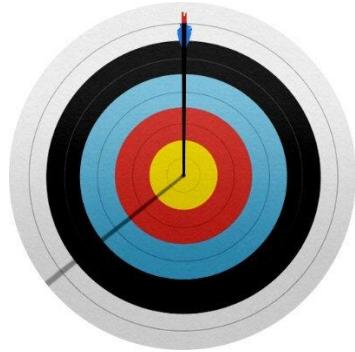


Making Sense of the Ethereum Foundation

Oct 11, 2022 - Devcon VI - Bogota



Josh Stark

I work for Ethereum at the EF

PROLOGUE













ethereum
foundation



ethereum
foundation



**ethereum
foundation**



**ethereum
foundation**



1. What is Ethereum?

what kind of *environment* is it for organizations?

2. What is the EF?

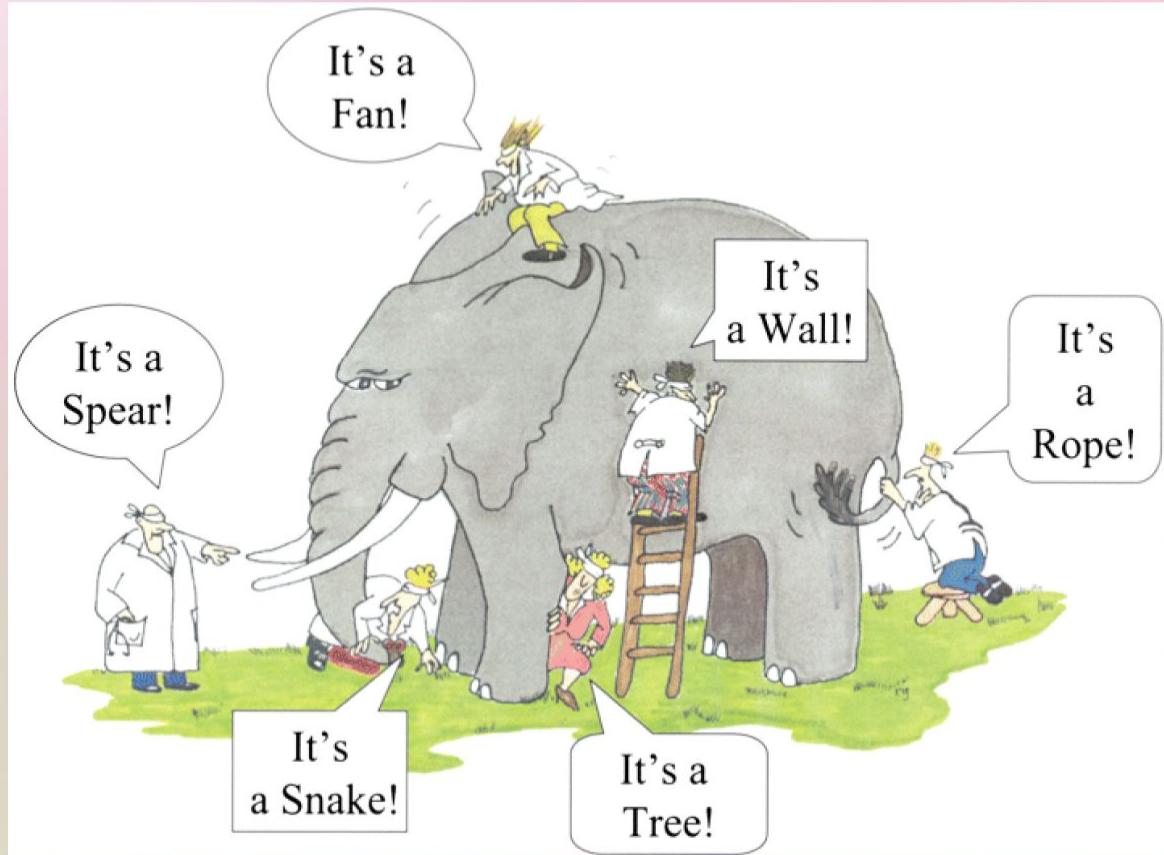
how did the EF evolve *for* that environment?

3. What else might we build together?

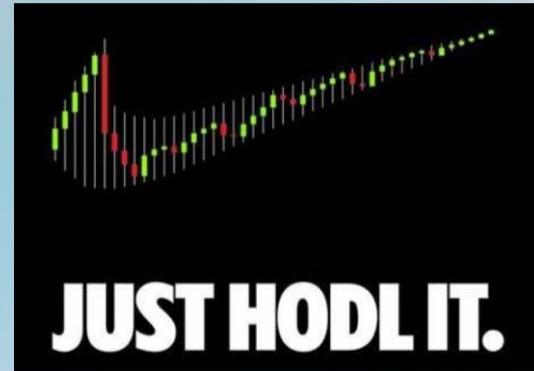
what is the space of possible ethereum organizations?

I. What is Ethereum?

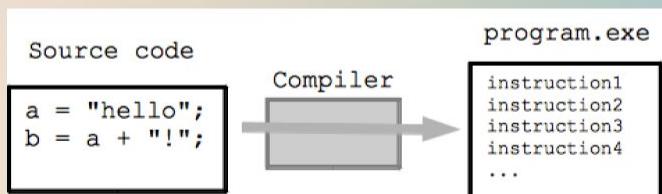
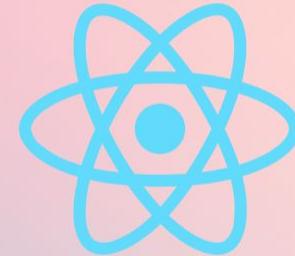
Ethereum is...



...a new financial system



...a developer platform



```
R RR RR
R RRRRRRRR R   R
R RRR R   RRRRRRRRRRRRR R   RRR R
RRR RR   RRRRRRRRRRRRRRRRR RRRR R
RRRR R   RRRRRRRRRRRRRRRRR RRRR R
RRRRR RRRRRRRRRRRRRRRRR RRRR R
RRRRRR RRRRRRRRRRRRRRRRR RRRR R
RRRRRRR RRRRRRRRRRRRRRR RRRR R
RRRRRRRR RRRRRRRRRRRRRRR RRRR R
RRRRRRRRR= RR = RRRRRRRRRR
RRRRRRRRRRR= RR = RRRRRRRRRR
RRRRRRRRRRR RR R RRRRRRRRRR
RR=RRRRRRRRRRRRRRRRRR=RR
RR = ==RRRRRRR RRRRRR= = RR
RR = ===== = RR
RR R R
R R
R

o2sh ~ git version 2.30.2
-----
Project: rust (11 branches, 92 tags)
HEAD: 98d4245 (master, origin/master)
Pending: 3+
Version: 1.53.0
Created: 11 years ago
Languages: Rust (97.4 %) Python (0.5 %)
          JavaScript (0.4 %) CSS (0.3 %)
          C++ (0.3 %) Markdown (0.3 %)
          Other (0.7 %)
Authors: 5% Brian Anderson 5259
        4% Niko Matsakis 4874
        3% Alex Crichton 3616
Last change: a day ago
Contributors: 4525
Repo: https://github.com/rust-lang/rust
Commits: 108408
Lines of code: 1001429
Size: 63.53 MiB (29704 files)
License: Apache-2.0, MIT

```

...an area of cutting edge research



research

Log In

all categories ► all tags ► Latest Categories Top

Topic Replies Views Activity

* Read this before posting

Administrivia

This is a semi-public forum for participating in Ethereum's research efforts, including but not limited to: Casper Sharding EVM improvements Low-level protocol improvements Economics protocol economics Resource pricing... read more

Introducing Arcology, a parallel L1 with EVM compatibility

Unbundling PBS: Towards protocol-enforced proposer commitments (PEPC)

Arithmetic hash based alternatives to KZG for proto-danksharding (EIP-4844)

MEV minimization using randomness

Scalable, transparent, and post-quantum secure computational integrity

Eli Ben-Sasson* Iddo Bentov† Yinon Horesh* Michael Riabzev*

March 6, 2018

Abstract

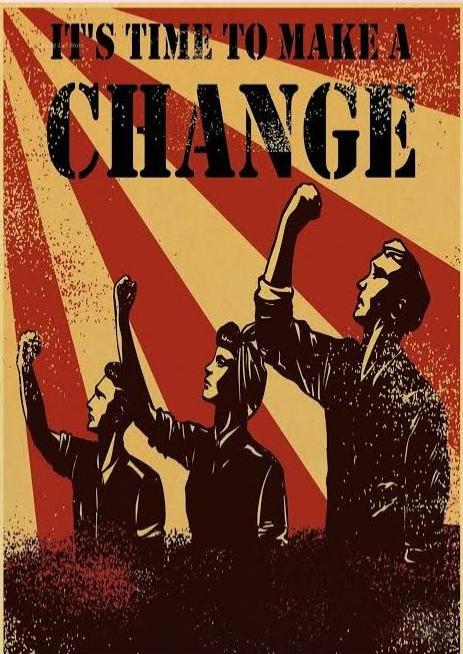
Human dignity demands that personal information, like medical and forensic data, be hidden from the public. But veils of secrecy designed to preserve privacy may also be abused to cover up lies and deceit by institutions entrusted with Data, unjustly harming citizens and eroding trust in central institutions.

Zero knowledge (ZK) proof systems are an ingenious cryptographic solution to this tension between the ideals of personal *privacy* and institutional *integrity*, enforcing the latter in a way that does not compromise the former. Public trust demands *transparency* from ZK systems, meaning they be set up with no reliance on a trusted party that can have its trapdoors that could be exploited by powerful parties to bear false witness. For ZK systems to be used with Big Data, it is imperative that public verification process scale sublinearly in data size. Transparent ZK proofs that can be verified exponentially faster than data size were first described in the 1990s but early constructions were impractical, and no ZK system realized thus far in code (including that used by crypto-currencies like Zcash™) has achieved both transparency and exponential verification speedup, simultaneously, for general computations.

Here we report the first realization of a transparent ZK system (ZK-STARK) in which verification scales exponentially faster than database size, and moreover, this exponential speedup in verification is observed concretely for meaningful and sequential computations, described next. Our system uses several recent advances on interactive oracle proofs (IOP), such as a "fast" (linear time) IOP system for error correcting codes.

Our proof-of-concept system allows the Police to prove to the public that the DNA profile of a Presidential Candidate does not appear in the forensic DNA profile database maintained by the Police. The proof, which is generated by the Police, relies on no external trusted party, and reveals no further information about the contents of the database, nor about the candidate's profile. In particular, no DNA information is disclosed to any party outside the Police. The proof is shorter than the size of the DNA database, and verified faster than the time needed to examine that database naively.

...a political movement(s)



THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5
More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billion may be needed as lending squeeze tightens

Allister Darling has been forced to consider a second bailout for banks after the collapse of Northern Rock last month. He will be asked to take out another £10 billion in March to cover the cost of bailing out the UK's biggest building society, TSB. Options include cash injections, nationalisation or a full-scale takeover by the state. The Treasury has found

that, despite intensive pressure, the banking system has not yet returned to normal levels of lending and other areas tighter regulation are needed. The Chancellor would be asked to propose that the Bank of England impose a new limit on the amount of lending that can be done by the banking system.

99p

Giant Killing? Guide to the FA Cup Third Round

Salmon Rushdie I Won't Marry Again

Detox in style The best spas on the planet

Working mums So that's how she does it

Michael Sheen Frost, Nixon and me

Start collecting books today! Pollard Inside

Max SC, min 5C

At least 400 Palestinians were killed in a week of strikes. See page 1

Pub chain sets the record straight over £2.4m to 2009 losses

on state-backed guarantees to encourage lending. The Chancellor has a range of options available to him, perhaps bypassing them if he believes they will not be effective. But he is expected to take out another £10 billion in March to cover the cost of bailing out the UK's biggest building society, TSB. Options include cash injections, nationalisation or a full-scale takeover by the state. The Treasury has found

that, despite intensive pressure, the banking system has not yet returned to normal levels of lending and other areas tighter regulation are needed. The Chancellor would be asked to propose that the Bank of England impose a new limit on the amount of lending that can be done by the banking system.

99p

Giant Killing? Guide to the FA Cup Third Round

Salmon Rushdie I Won't Marry Again

Detox in style The best spas on the planet

Working mums So that's how she does it

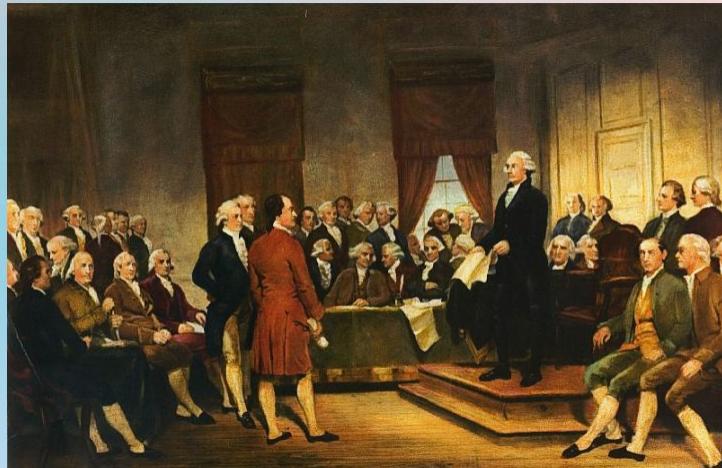
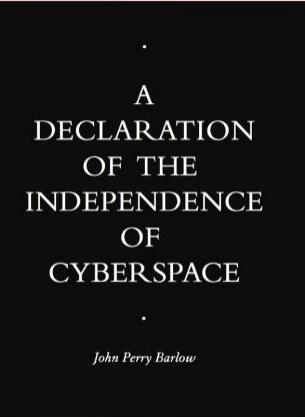
Michael Sheen Frost, Nixon and me

Start collecting books today! Pollard Inside

Max SC, min 5C

At least 400 Palestinians were killed in a week of strikes. See page 1

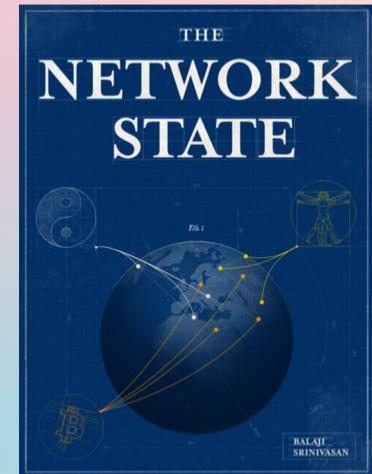
Pub chain sets the record straight over £2.4m to 2009 losses



...a new kind of state or jurisdiction



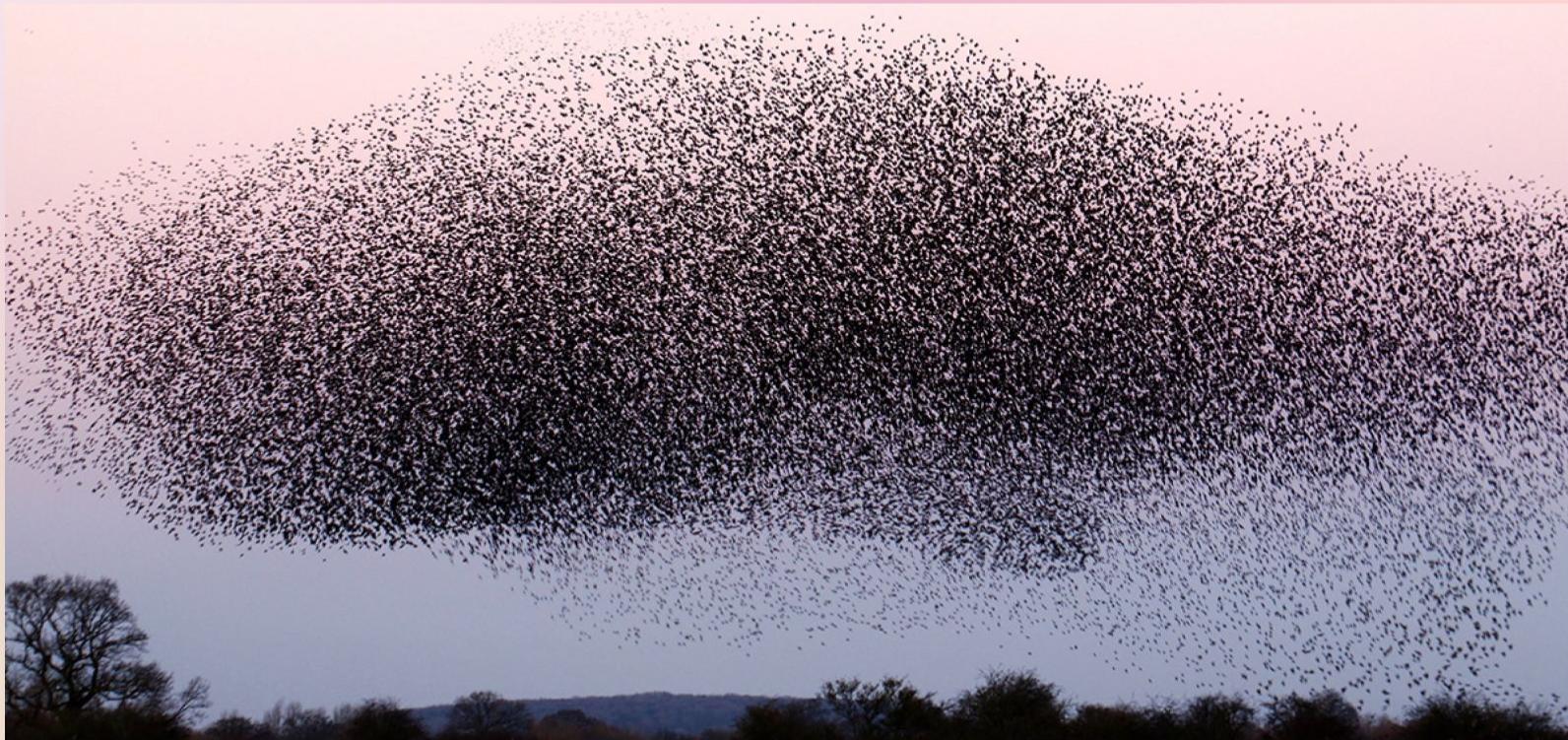
THE LAW
OF THE SEA



...a global project



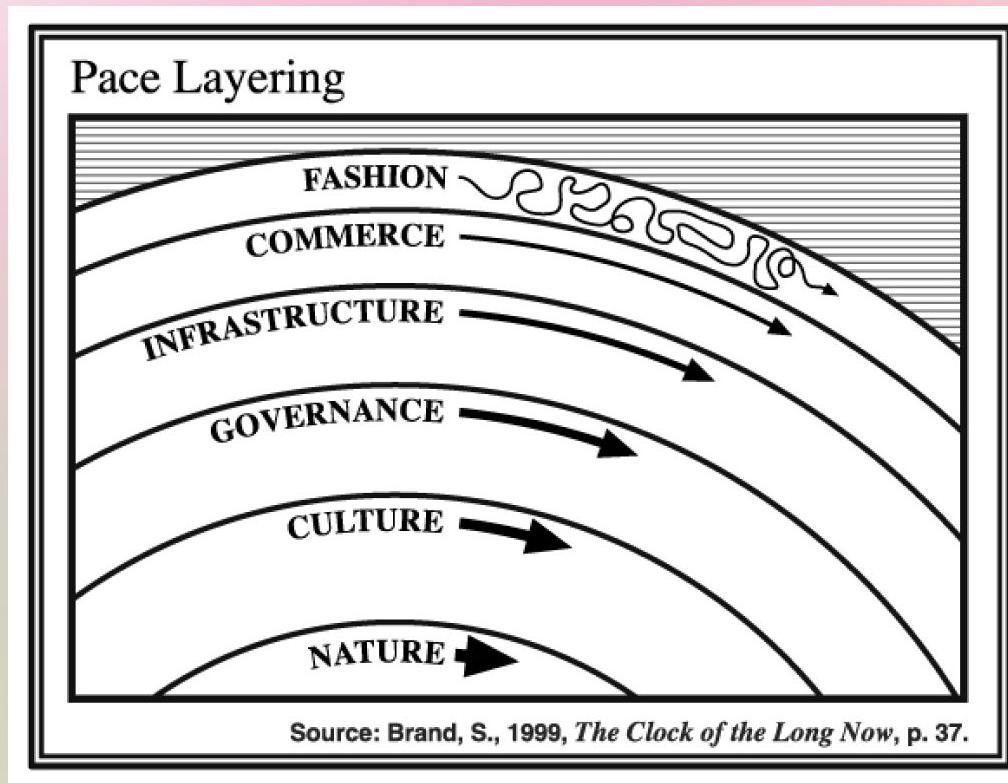
...a decentralized project.



...uncertain, changing, and evolving.



... a long term project.





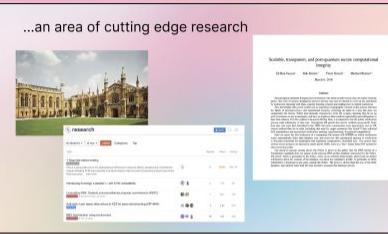
...a new financial system



...a developer platform



...an area of cutting edge research



...a global project



...a decentralized project.



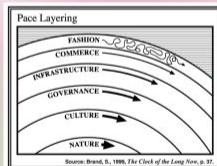
...a political movement(s)



...a new kind of state or jurisdiction



... a long term project.



...uncertain, changing, and evolving.



Who will do the maintenance?

Who will fund public goods?

Who will push our political
movement(s) forward?

Who will react to new problems
or opportunities we can't
anticipate now?

How should orgs working in a
decentralized ecosystem be
different?

The Space of Possible Ethereum Organizations



contribution to / role in ecosystem



ethereum
foundation

2. What is the EF?

EF basics

- Non-profit
- Community of teams
- Provides grants & funding to external orgs



<https://ethereum.foundation/report-2022-04.pdf>

The EF has evolved alongside the Ethereum ecosystem.



Over time, we have developed our own answers to some of the questions we talked about in the last section.

Question 1:

The Ethereum ecosystem is *decentralized* and inherently concerned with centralized power.

How should an organization operate in that environment?

THE TIMES

Max SC, min -SC

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50



Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout Inside

Israel prepares to send tanks and troops into Gaza



Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott, Deputy Editor
Giles Duley, Economics Correspondent

Alastair Darling has been forced to consider another rescue package for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to intervene again in the economy this spring—six months after the £75 billion part-nationalisation last July of the three biggest UK clearing banks. Options include cash injections, offering banks cheaper state guarantees to encourage them to lend again, or buying “toxic assets.” The Times has learnt.

The Bank of England revealed yester-

day that, despite intense pressure, the financial system had not yet recovered from last year and plus even tighter restrictions will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting its key interest rate to a record level of 2 per cent. Doing so would reduce the cost of borrowing, but have little impact on the lending squeeze.

Whitehall sources said that ministers planned to “keep the banks on life support” until the economy recovers, giving more help to restore lending levels. Finally, the Treasury plans to focus

on state-backed guarantees to encourage banks to lend again. It could also consider freezing, for a number of months, the interest rates charged by banks, perhaps swapping them for government bonds. The basic assets, such as houses and cars, held by the banking system, would be parked in a state vehicle or “bad bank” that would manage them. The Treasury would then sell them while “detoxifying” the main banking system.

Whitehall sources say they favour the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 8, col 1
Leading article, page 2



Michael Sheen
Frost, Nixon
and me
Magazine



Working mums
So that's how
she does it
Body & Soul



Detox in style
The best spas
on the planet
Travel



Salmon Rushdie
I Won't Marry
Again
Pages 22, 23

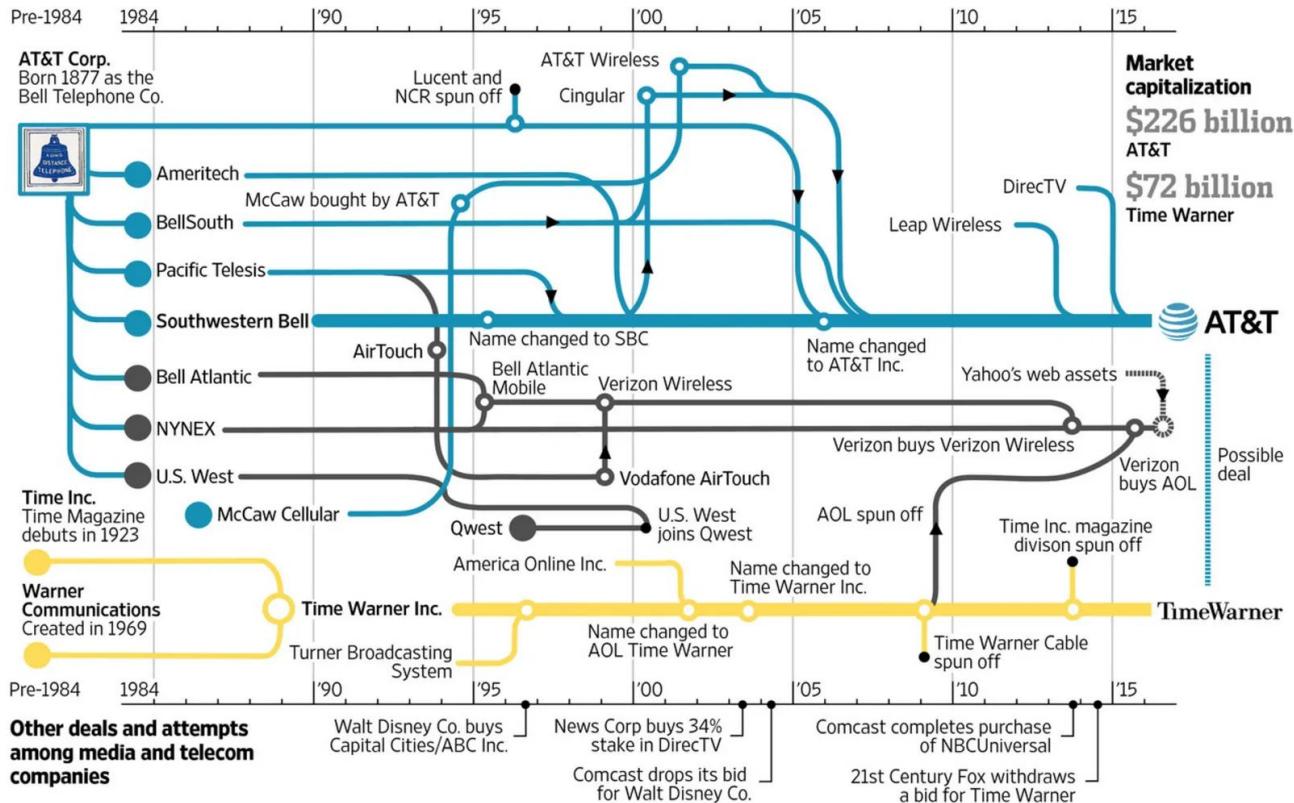


Giant Killing?
Guide to the FA
Cup Third Round
Sport



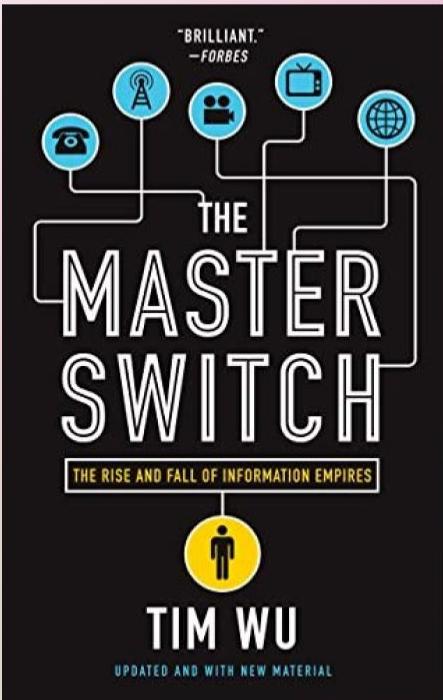
Converging Destinies

AT&T and Time Warner have reached an agreement to merge after decades of consolidation and deals in the telecommunication and media industries.



Source: staff and news reports

THE WALL STREET JOURNAL.



Who will control crypto?

0x44FB | August 22nd, 2022

19 Collected

By Saffron Huang & Josh Stark

The rise of statechains

Imagine that Ethereum succeeds. Blockchains become widely used for global commerce and coordination. Anyone with an internet connection and a phone can plug directly into a global network for money, value and identity. Every day, billions interact with an ecosystem of L2 chains secured by Ethereum. Security practices have improved at every level of the stack and major hacks are essentially nonexistent. It is commonplace for businesses and individuals to create crypto-tokens, and nations issue their fiat currency onto these networks.

The legal, social and economic codes of society have been completely reconfigured by the new organizations, interaction patterns and digital objects (NFTs, and more) that are now commonplace; the global economy adopts the "API" of blockchains as default.

saffron.mirror.xyz

- “I have good intentions, if I just had more power, I could do more good...”
- “To achieve our mission, we need to hire all the best people away from other orgs...”
- “If everyone loves and respects us, we can accomplish more...”



EF's answer:

Adopt a philosophy that pushes *back* against these dynamics.

Subtraction.



EF: a philosophy of subtraction

ADDITION MINDSET

Capture opportunities

Pull in-house

Unhappy when
others create value

Increase prestige

Matter **more**

SUBTRACTION MINDSET

Distribute opportunities

Push out to distribute

VS

Thrilled when
others create value

Decrease prestige

Matter **less**

- We don't try and attract attention to ourselves
→ *decrease prestige*
- We help create new independent orgs
→ *matter less*
- “Layered” allocation strategy involving community
→ *distribute opportunities*



but I don't wanna live in a world where someone else makes the world a better place better than we do.

Question 2:

There's a lot to be done.

Maintenance, research, fund public goods, advocacy,
etc.

Who will do it?

It can't be just the EF.

→ One org couldn't possibly do all of that...

→ Even if they could, it would introduce a centralization risk!

EF's answer:

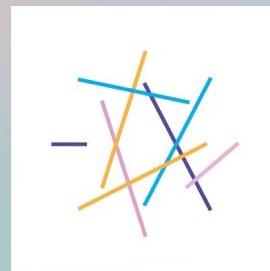
There must be *an ecosystem outside of us* that is capable of meeting these challenges, and adapting to new ones.

How can the EF help?

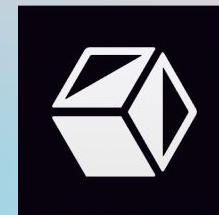
Help the people founding *new* organizations.



DAO Research
Collective.



0xPARC



Nomic
Foundation

Decide *not* to do certain things.

Example:

No EF internal Consensus-Layer (“Eth2”) client.

Question 3:

How do you create an org that can react to a rapidly changing ecosystem?

- Ecosystem is **rapidly** changing
- Future is uncertain
- Ecosystem taking on more responsibilities
 - because of the above, we need to adjust around that growth

Create an org with many independent decision-makers.

- Community of teams
- Layered allocation strategy

Flexible internal structure

- Titles are rare
- Organic transitions between teams

There are tradeoffs here!

- More organic flexibility → Less legibility
- Operational complexity
- Not a fit for everyone

Will other orgs face our same challenges?

Our ecosystem will contain ecosystems!

Should your org adopt subtraction?

3. What else might we
build?



@herdaolatam

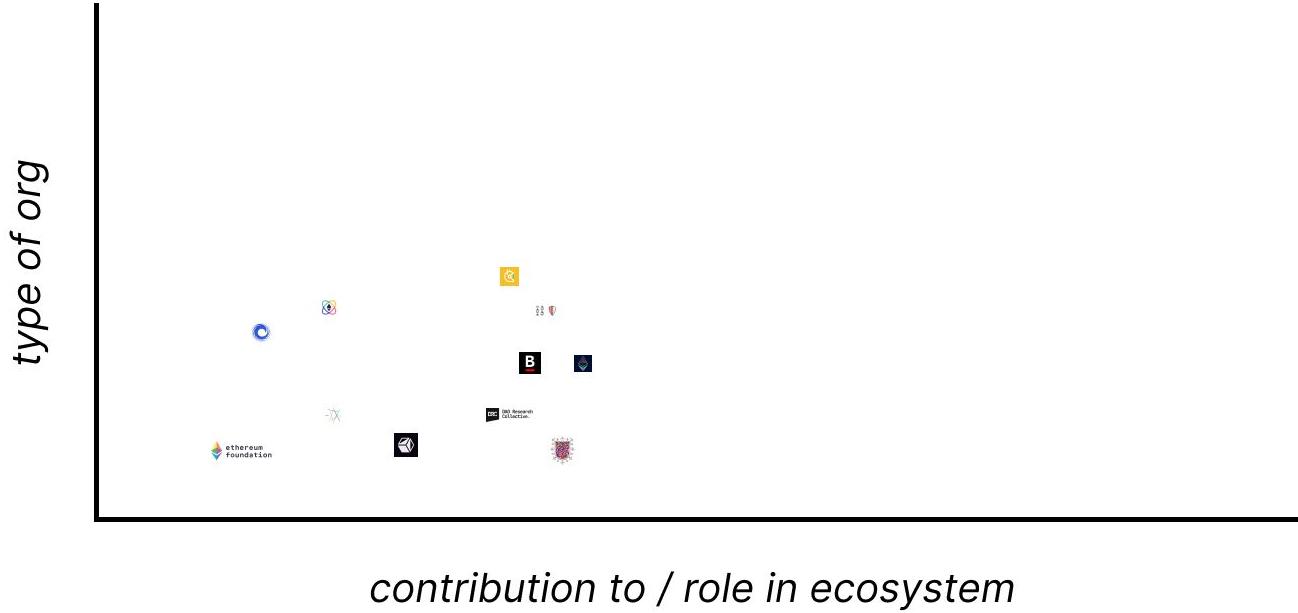
Blockchains are weird.

it can take a while to figure out
what to build with them.

Our preconceived notions
about what Ethereum *is* limits
what we can create.

Maybe that's also true about
our community?

The Space of Possible Ethereum Organizations



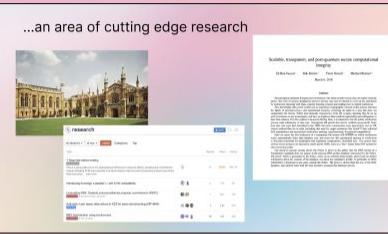
...a new financial system



...a developer platform



...an area of cutting edge research



...a global project



...a decentralized project.



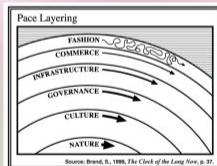
...a political movement(s)



...a new kind of state or jurisdiction



... a long term project.



...uncertain, changing, and evolving.



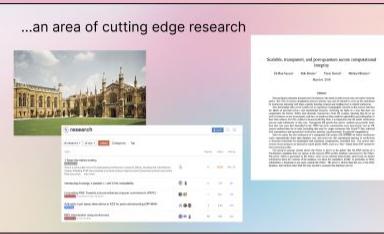
...a new financial system



...a developer platform



...an area of cutting edge research



...a global project



...a decentralized project.



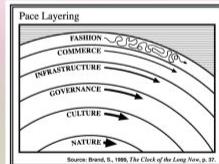
...a political movement(s)



...a new kind of state or jurisdiction



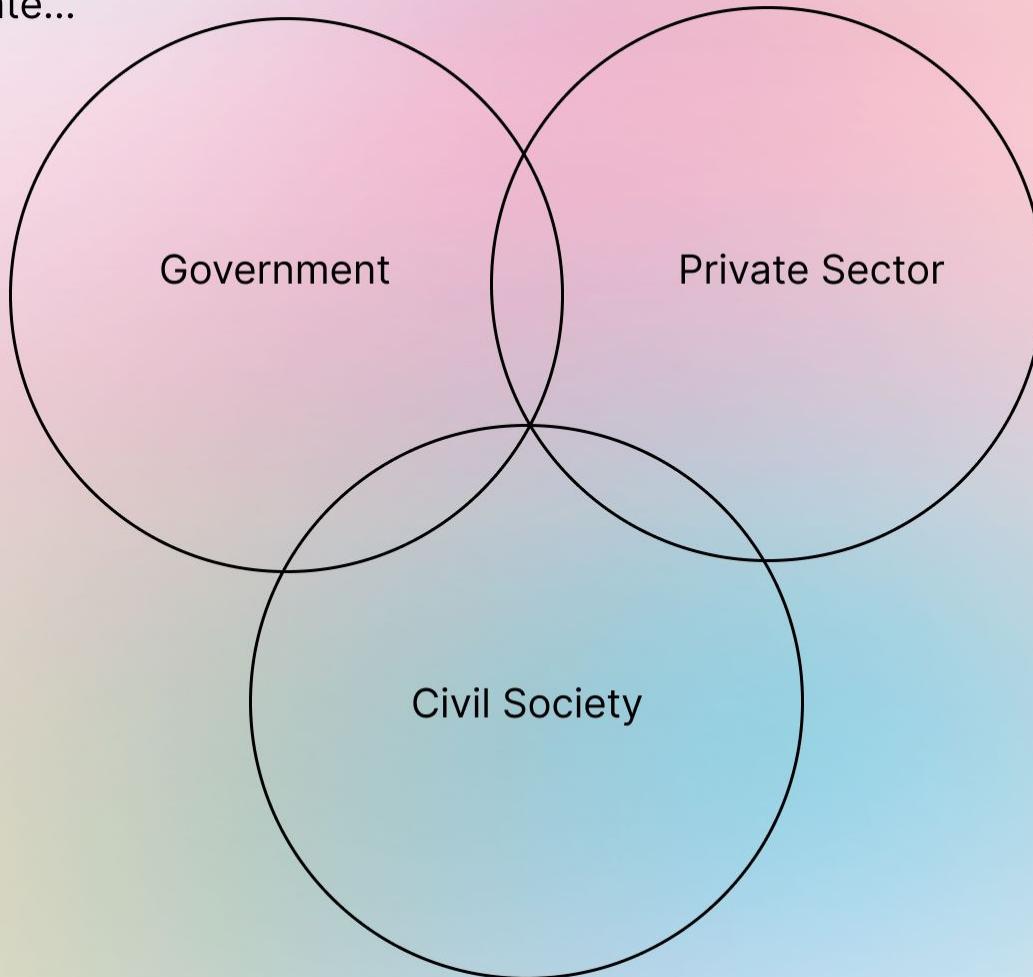
... a long term project.



...uncertain, changing, and evolving.



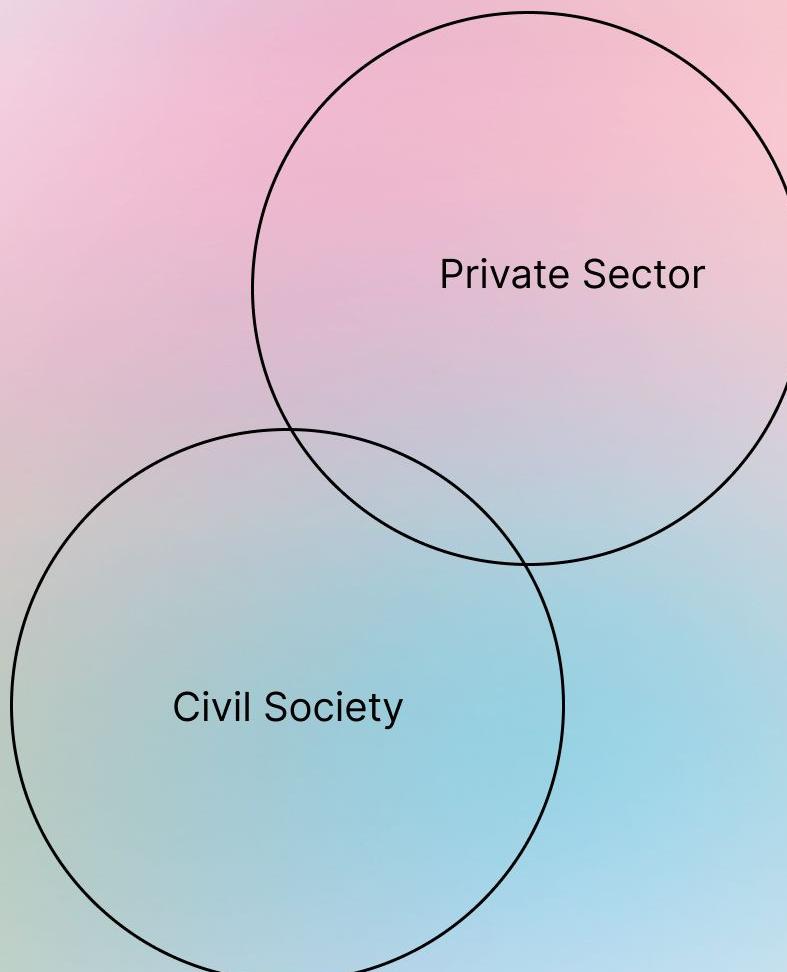
In a “traditional” state...



In a “traditional” state...

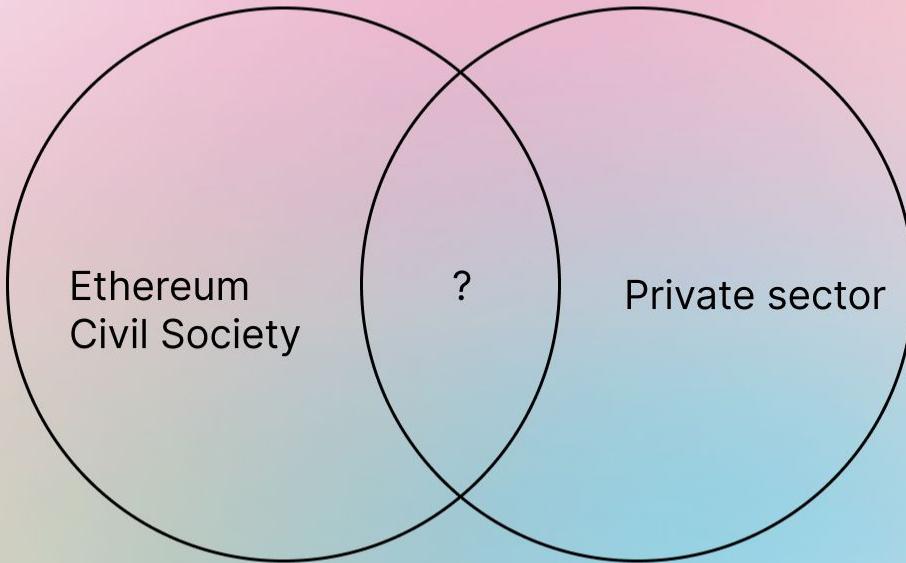
Civil Society

- Non profits
- Guilds
- Advocacy groups
- Educational institutions
- Religious organizations
- Charities
- Trade unions
- Clubs
- Political organizations
- Co-operatives
- Professional Associations
- +++



Private Sector

Civil Society



Ethereum Civil Society?

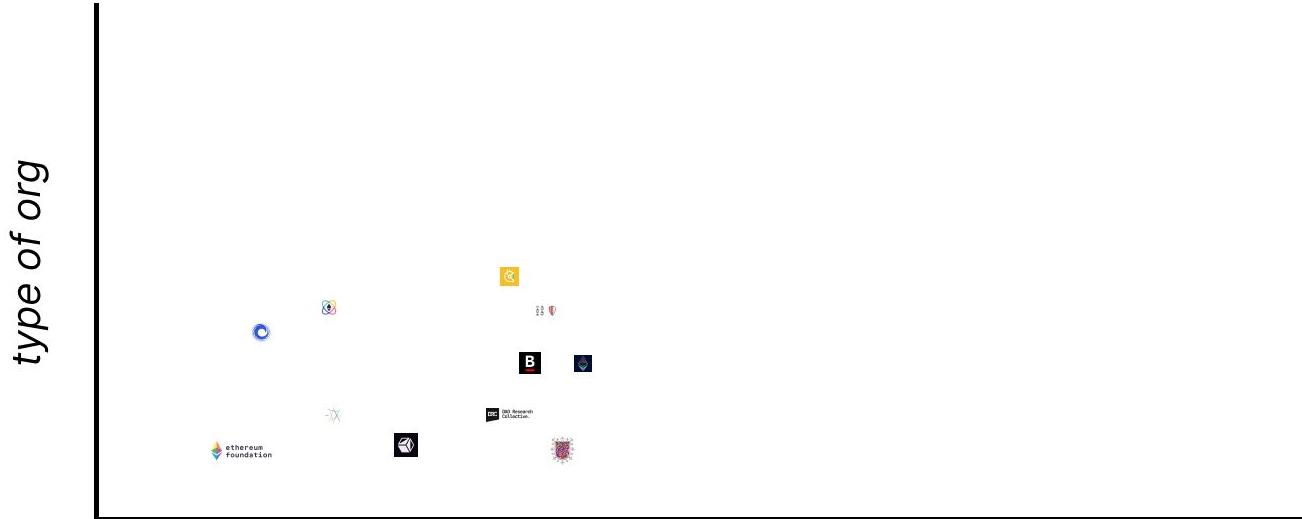


...and many others.

*Even a billion dollars of capital
cannot compete with a project
having a soul.*

- Some guy

The Space of Possible Ethereum Organizations



contribution to / role in ecosystem

thanks!

Josh Stark
Ethereum Foundation



@0xstark