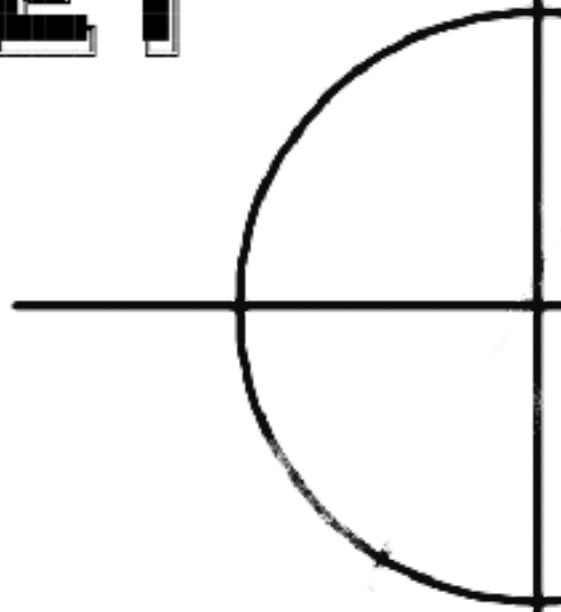
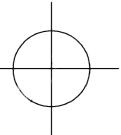


PRIVACY MARKET OUTLOOK IN WEB3





INTRO

MARKET OVERVIEW

KEY NEWS

- Tornado Cash
- Advocacy
- Privacy policies
- Privacy coins ban
- Zero-knowledge hype

FINANCIAL STREAMS

- Investments
- Cryptocurrencies
- Traction
- Other funding options

BUIDLers

- Use-cases
- Trusted setups
- Github stats
- Ecosystems
- R&D
- Hackathons
- Governance

RISKS

- Political Polarisation
- Anonymity
- Self-security
- Configurable privacy vs Consent

OPPORTUNITY

- Security
- Biases
- Network states
- Legal defence

CONCLUSION

END NOTES

There is also the important broader philosophical case for cryptocurrency as private money: the transition to a "cashless society" is being taken advantage of by many governments as an opportunity to introduce levels of financial surveillance that would be unimaginable 100 years ago.

Cryptocurrency is the only thing currently being developed that can realistically combine the benefits of digitalization with cash-like respect for personal privacy.

– Vitalik Buterin, Ethereum co-founder

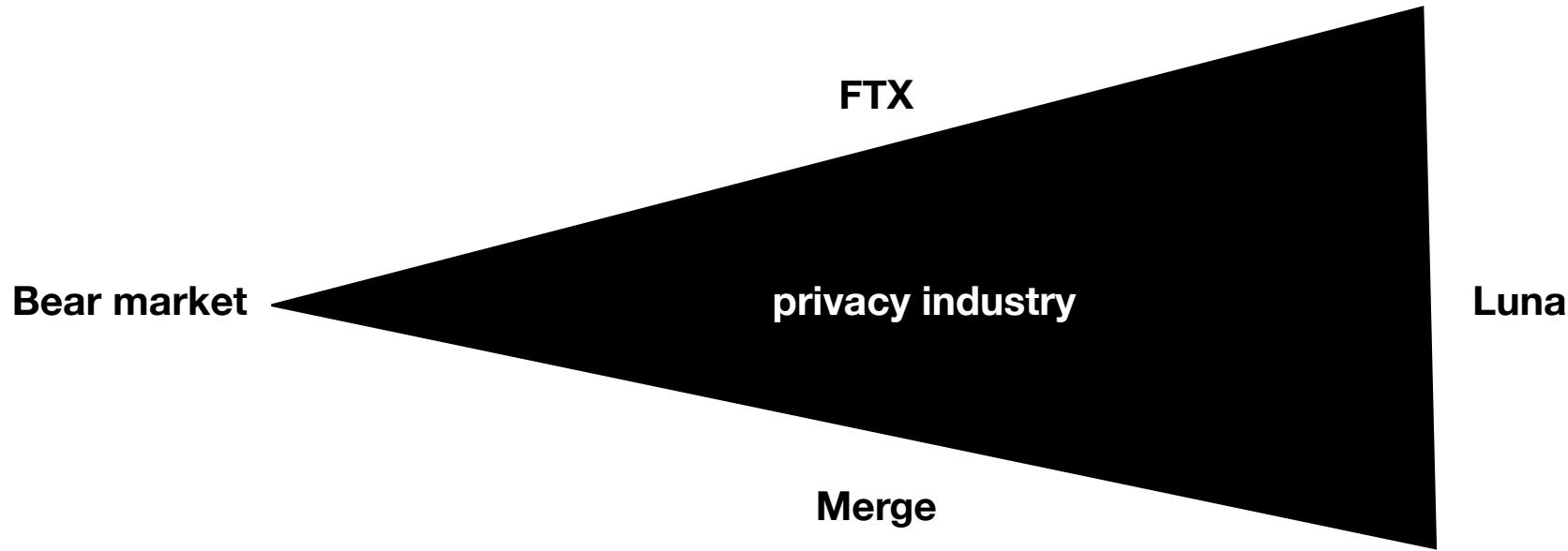
Introduction

This report's initial idea was the desire to structure the overall picture of the web3-privacy market. Explore hundreds of independent companies and their connections – present as an ecosystem with the potential for unity and collaboration.

Why is it important now? Regulators actively centralise the market. Moreover, while multiple agents are watching you, exchanges and wallets give you a sense of freedom of choice (“to KYC or not to KYC”). Analytics companies own & use your data without permission. Leaked news about the regulation of private cryptocurrencies and the Tornado Cash sanctions are a clear examples of why privacy needs advocacy.

Today, 300+ companies developing private solutions worldwide have a unique chance to unite and take responsibility for the original blockchain decentralisation ethos.

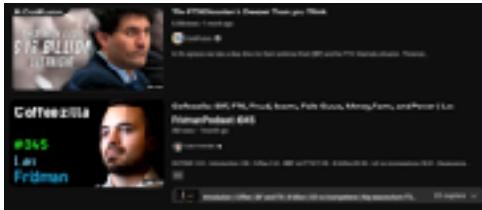
Privacy has been overshadowed by the hacks, scandals & financial crashes that happened last year.



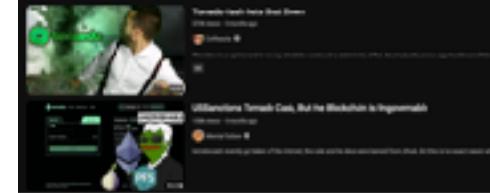
Exception: the OFAC sanctions against Tornado Cash. Even then, newsbreak did not last long in the media and social networks.

Media analysis shows that privacy is a niche topic within an industry.

SBF saga has dozens of millions of views on YouTube

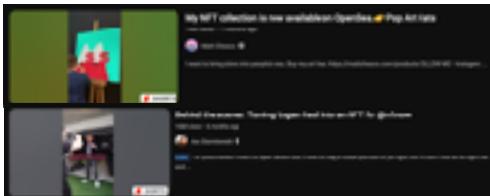


The biggest privacy-related case has ~1,5M views



X

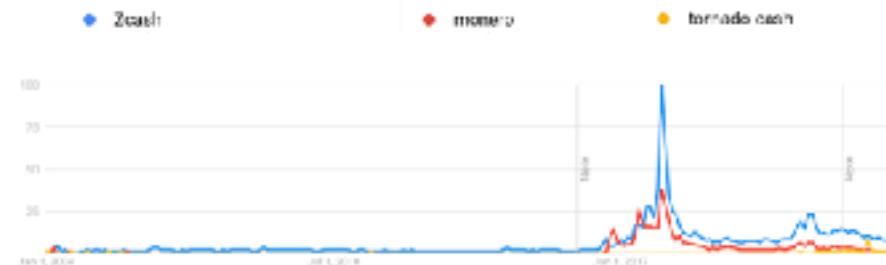
NFT has hundreds of millions of views



Privacy coins have the highest views because influencers promote them as investments



**Privacy
attention
peak was 5
years ago.**



Rare ecosystem bet on privacy

	Cosmos	Near	Polkadot	Avalanche	Polygon	Solana
Total amount of projects	266	998	550	304	1703	1500
Privacy projects	18	28	13	5	14	7
%	6.7	2.8	2.3	1.6	0.8	0.4

MARKET OVERVIEW

300+ projects are building privacy solutions

\$1B+ funding committed in 2022 to projects & ecosystems

110M+ times privacy apps were downloaded from Google Play

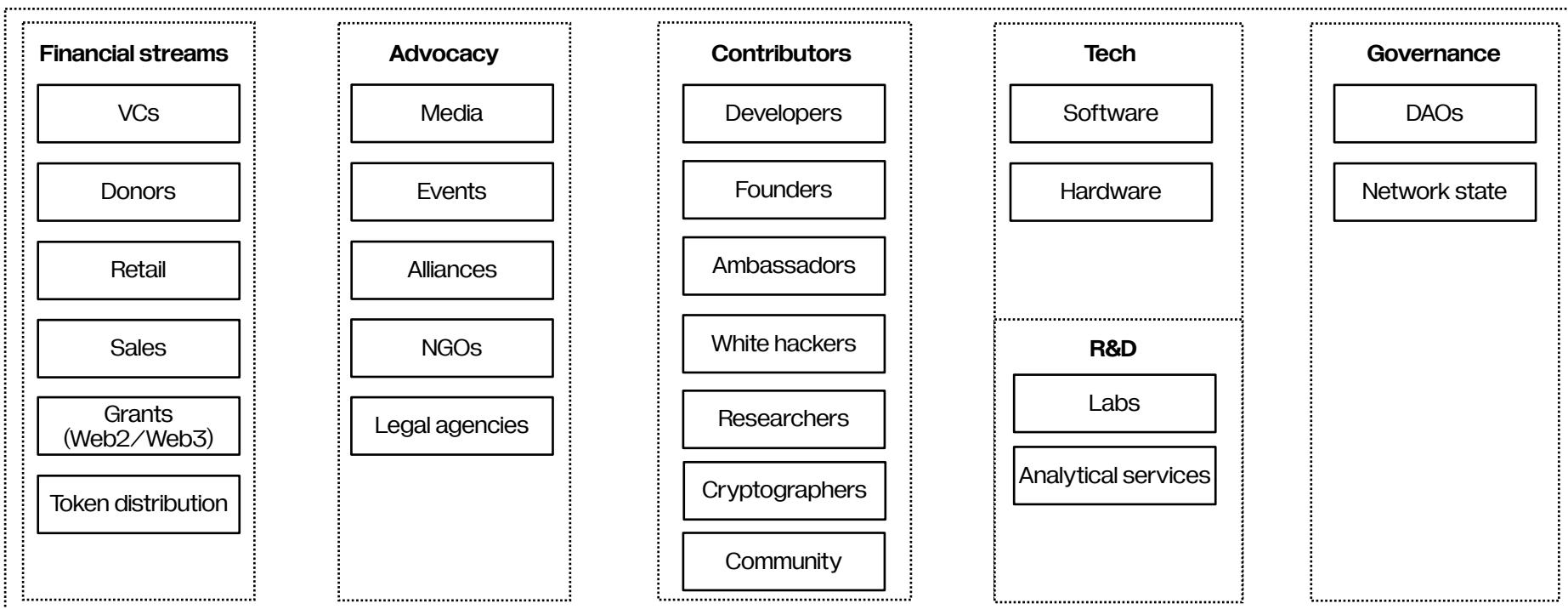
300+ vacancies exist in the market

727,681 Zcash total addresses

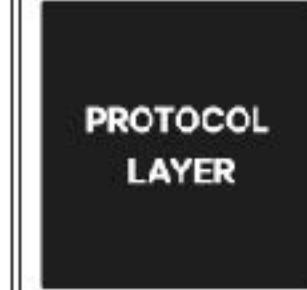
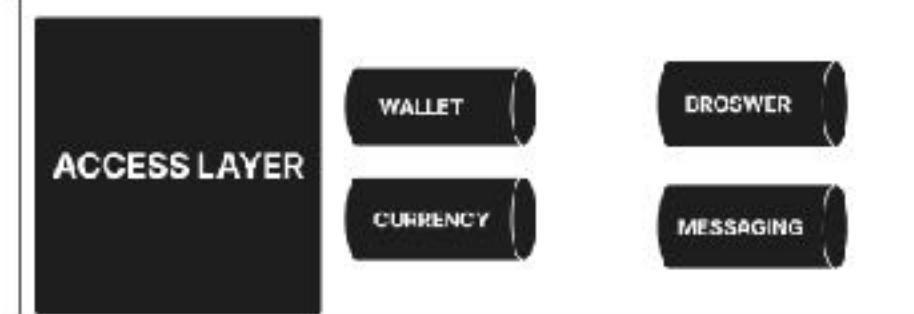
4,300 contributions across 177 countries participated in Manta Network's Trusted Setup

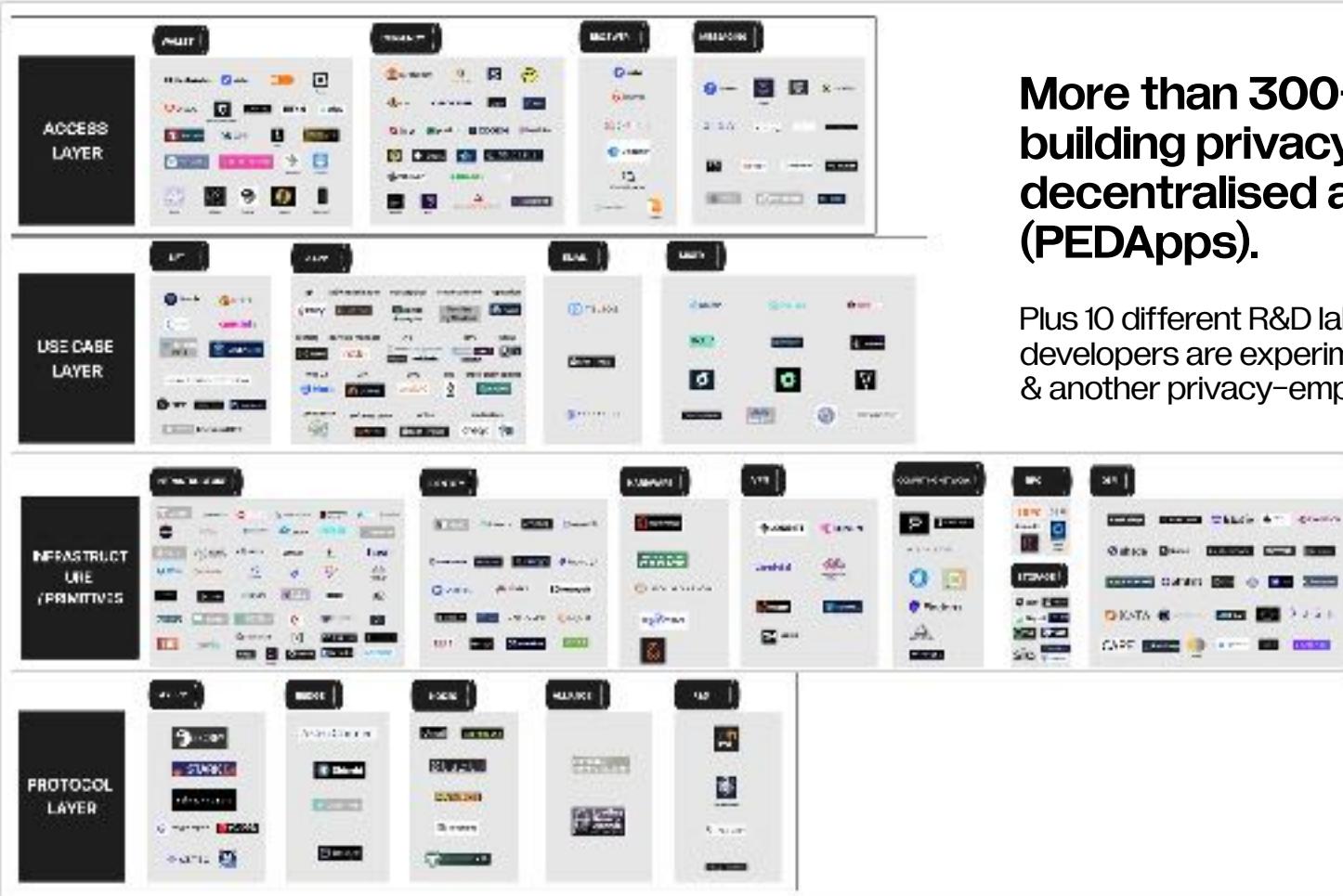
**The privacy market is fragmented.
Monero or Zcash holders are attacking
everyone else & pro-compliance projects
devalue anonymous activities.**

**In the meantime,
it's an ecosystem!**



The market is moving towards a full-privacy stack from network level privacy to selective identity disclosure.



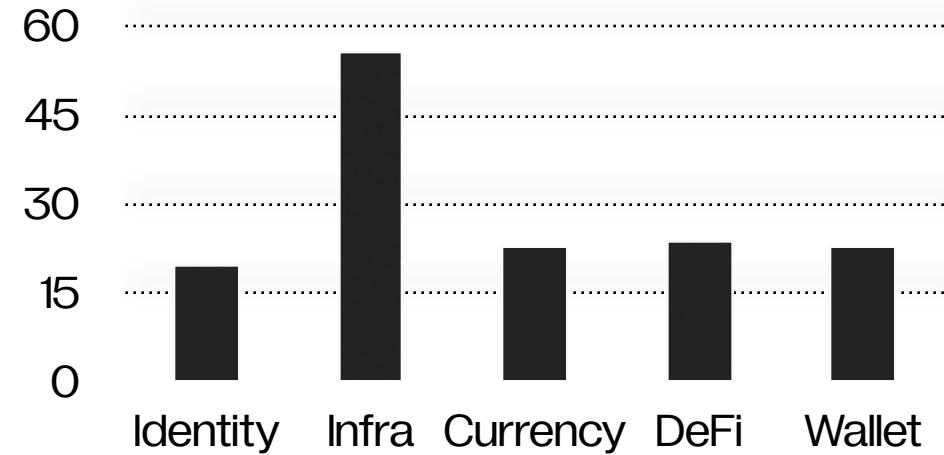


More than 300+ teams are building privacy-enhancing decentralised applications (PEDApps).

Plus 10 different R&D labs and hundreds of free developers are experimenting with ZK, FHE, MPC & another privacy-empowering tech.

Developers are focused on building

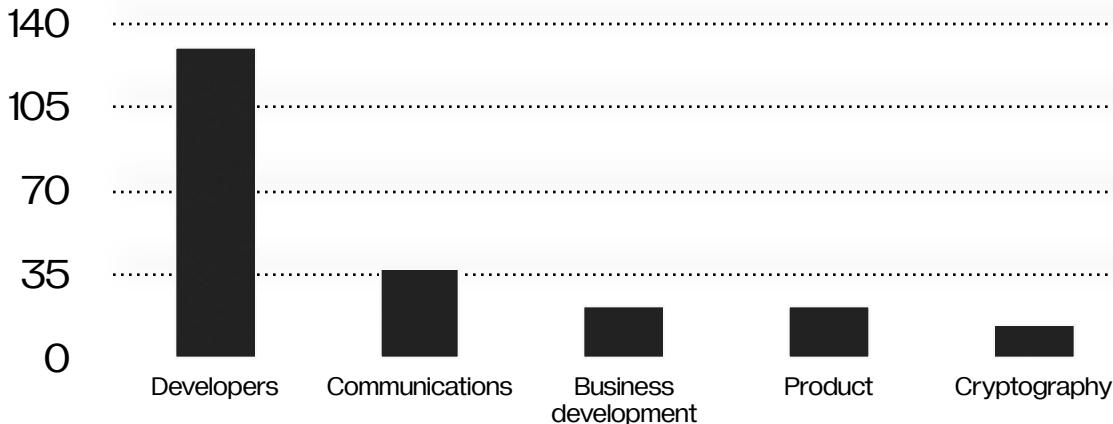
infrastructure,
DeFi solutions,
Decentralised identity.



Note: web3-identity is private by default. But it doesn't mean that developers share privacy-centric values.

Time to build!

300+ open vacancies exist in the market.



Hiring

- **52.8%** vacancies – developers
- **22%** vacancies – senior roles
- **3x** times more jobs for devs than marketing & PR

Also

- Product managers & UX/UI designers demand customer-centric approach
- Cryptographers's signals about ZK growth

Note: some companies decentralise teams via community engagement, builders programs & grants (Mina, NYM, Secret Network etc)



KEYNEWS

regulation

Tornado cash

x

OFAC

legal

Alliances

surveillance

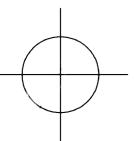
Metamask & Uniswap
sensitive data
aggregation backlash

regulation

Private currencies
potential regulation

R&D

ZK advancement



TORNADO CASH

Tornado cash sanctions & industry censorship had a chilling effect on the industry



vitalik.eth  @VitalikButerin

Replying to @beamercycle

I'll out myself as someone who has used TC to donate to this exact cause.

10:49 AM · Aug 9, 2022

Roman Semenov   @semenov_roman · Aug 8, 2022

My [GitHub](#) account was just suspended 

Is writing an open source code illegal now?

11 477 2,030 5,724



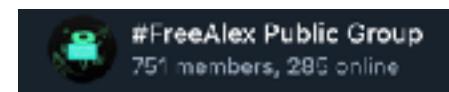
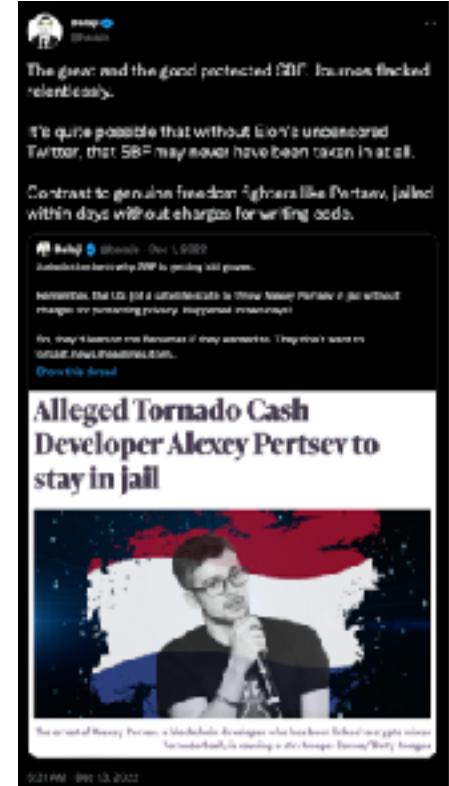
Network censorship showed high dependence on US regulations.

Both market players & service providers like GitHub took actions to protect themselves from sanctions. Moreover, some privacy solutions executives became “red-flagged”

Censored-centric services: Github. Infura. Oasis. Alchemy Platform. Circle.



Open-source development advocacy consolidated unexpected players from the Russian-dev community & crypto lawyers to Balaji



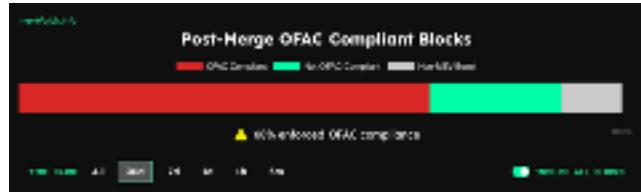
Tornado Cash brought greater issue

centralisation
(regulation,
compliance)

vs

de-regulation &
de-centralisation

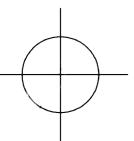
In other words: **how could decentralisation be accomplished within active censorship?**



1,000 Solana validators go offline
as Hetzner blocks server access
by Osato Araga-Nomaya



The Block | Solana



ADVOCACY

2 privacy-centric alliances were launched at Devcon Bogota

Universal Privacy Alliance



<https://privacyalliance.com>

Leading Privacy Alliance



www.leadingprivacy.com

Members

UPA (10): Nym, Manta Network, Secret network, Orchid, Electric Coin. Co, Status, Oasis Foundation, Railgun__, Aleo, Aztec

LPA (5): Blockwallet, Dusk Network, HOPR, Omnia, Panther protocol

Alliances commit to market advocacy

- Legal Fund
- Joint public statements
- Foster R&D
- Invest in education

Next events

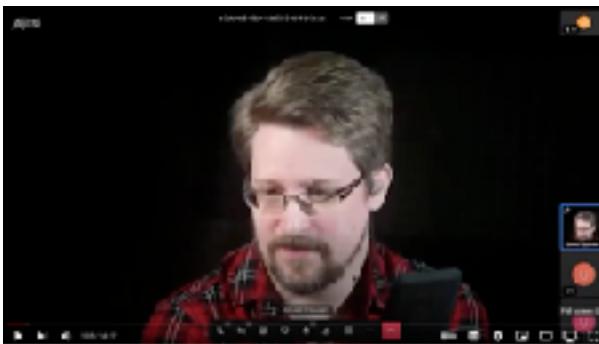
UPA Feb 24th to March 5th at ETH Denver
LPA

- Feb 28 ETH Denver
- 27-30 April ETH #Privacy Hackathon Istanbul
- 13-14 September Token 2049



Whistleblowers & long-term privacy advocates are already supporting the industry.

Edward Snowden participated in Universal Privacy Alliance & NYM launches



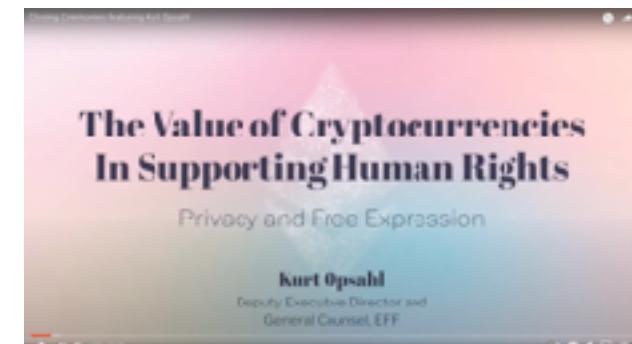
https://www.youtube.com/watch?v=i4oklUPOb_c

Chelsea Manning joined the NYM team

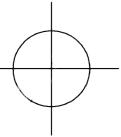


<https://www.politico.eu/article/chelsea-manning-crypto-token-nym-technologies-privacy>

Kurt Opsahl from EEF closed Devcon & contributed to ETH Brno



<https://www.youtube.com/watch?v=zZybrj8vTNc>



PRIVACY POLICIES

The community supported by Edward Snowden sent a signal to everyone trying to collect personal data – it's against decentralisation ethos.



Edward Snowden @snowden · Nov 5 · 2022

I'm told by Metamask that they're working on a response to the question below. (Note: IP records should never be retained for sharing.)

I've deleted my initial tweet, which contained an error (infuse was in fact acquired by ConsenSys, which also owns Metamask). Hope to hear more.



BRIANNE LINDNER

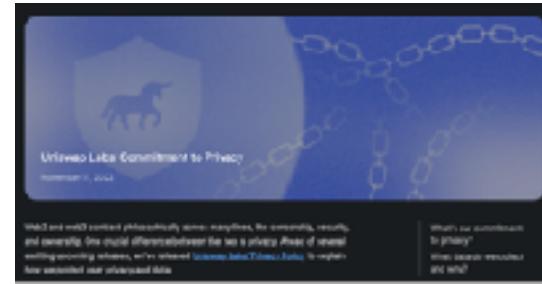
Nov 21 · 2022

Uniswap's new privacy policy sees backlash from decentralization buffs

Uniswap's newly released privacy policy comes in light of the FTX crisis, an event that has shined a spotlight on the need for transparency.



Collective action forced companies to listen to the community.



we do not collect and store personal data, such as first name, last name, street address, date of birth, email address, or IP address.

<https://uniswap.org/blog/commitment-to-privacy>

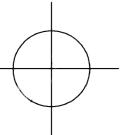
Business

ConsenSys to Update MetaMask Crypto Wallet in Response to Privacy Backlash

The firm clarified its data-sharing practices and said it will rebuild its wallet's settings page to address user concerns.

<https://consensys.net/blog/news/consensys-data-retention-update/>

Note: Uniswap & ConsenSys made PR statements but not direct actions.



PRIVACY COINS BAN

“The European Union could ban banks and crypto providers from dealing in privacy-enhancing coins such as zcash, monero, and dash under a leaked draft of a money laundering bill”
- Coindesk

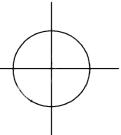
U.S. to announce international cryptocurrency action -statement

Reuters

Not the first time privacy coins could be sanctioned & banned from the leading exchanges, compliant services & the media.

But this time ban could become more thoughtful from a regulatory perspective.





ZERO-KNOWLEDGE ADVANCEMENT

Zero-knowledge cryptography became a “silver bullet” for almost every privacy case imagined

Carlos Guzman

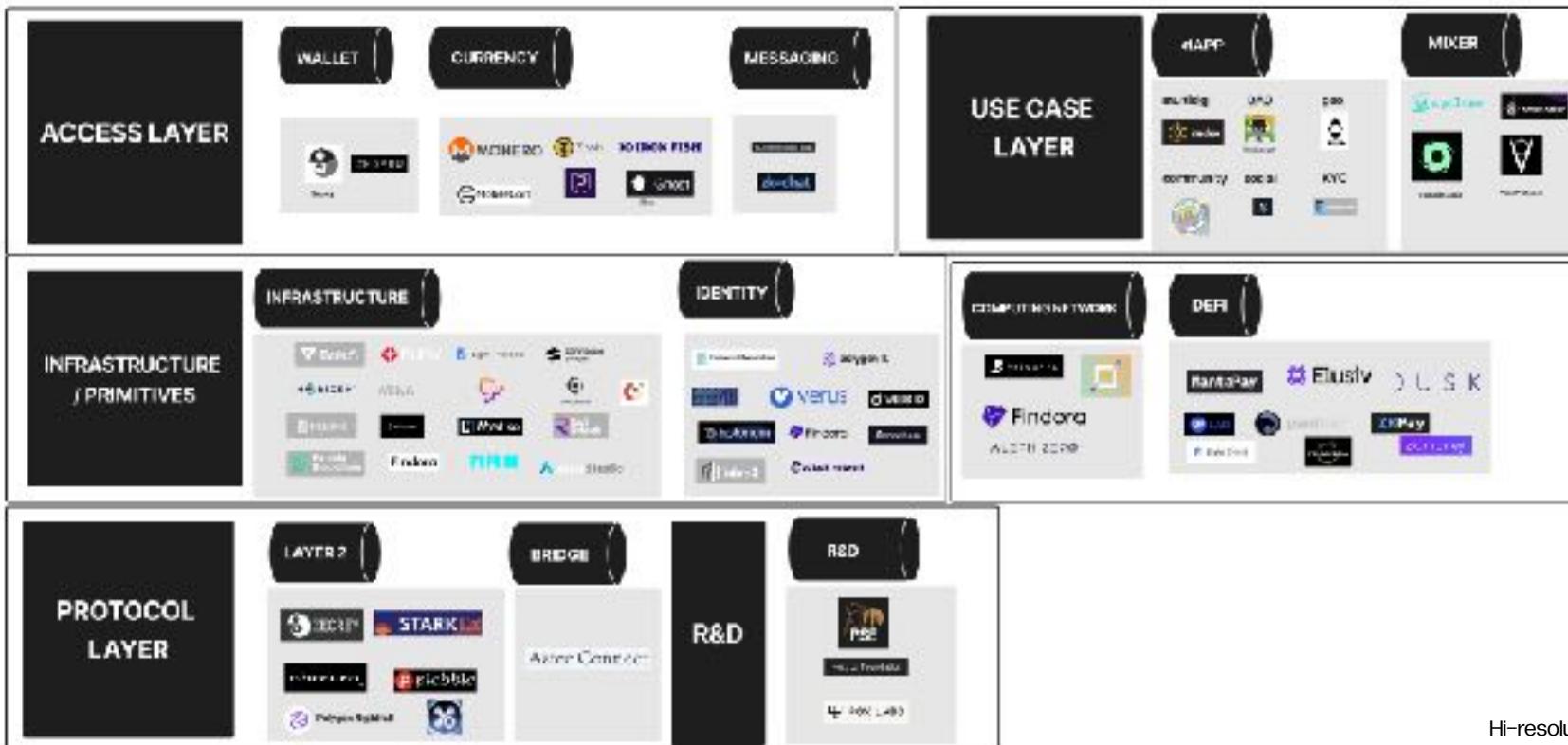
2023 will mark the beginning of a Cambrian explosion of zk-related apps across privacy, identity and bridging, among other things. There will be a large industry focus on developing credible forms of zk-compliance as privacy-related applications draw regulatory scrutiny.

I believe we will look back upon the industrialization of ZKPs* as a key milestone in the wide enterprise migration from private to public blockchains.

—Paul Brady
EY Global
Blockchain Leader

<https://minaproocol.com/blog/zkreport-2022>

20% of all privacy-enhancing solutions use ZK



Hi-resolution is available [here](#)

A research approach to ZK leads to imagining the whole ZK stack.

ZK social stack

There are many parallel efforts to reimagine and rearchitect online social systems to be more decentralized, permissionless, and censorship-resistant. Though different in their approaches, all these initiatives are creating basic building blocks for identity and reputation, then playing with different ways to stack the structure.

This helps to broaden ZK implications & approach them from a helicopter view (interconnected ecosystem).



The majority of ZK solutions are working on scalability, putting privacy aside.

Examples: privacy is a secondary effort for Polygon or StarkNet.

StarkNet is picturing L3 & L4-enabled privacy.



L3s and Fractal Layering

Multiple L3s will ride on top of an L2. Moreover, additional layers (L4, etc.) may be built upon L3 for fractal layering solutions.

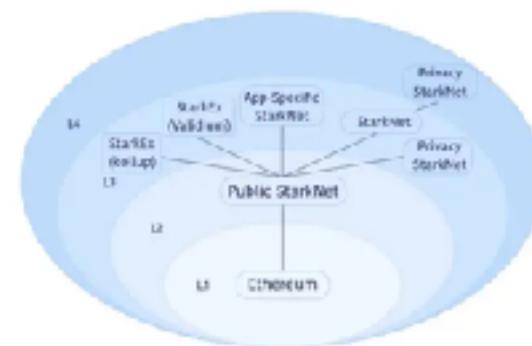


Diagram: A layer3 ecosystem



FINANCIAL STREAMS

There are multiple sources of income for privacy projects.

Investment track

VCs

Grants

Community

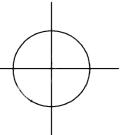
Donations

TGE

Trading

Commercial

B2B / B2C Sales



INVESTMENTS

VCs are interested in privacy.

Aleo raised \$270M total this year, and projects like Aztec or Espresso Systems closed their new rounds amid the bear market

Aleo Raises \$200M in Series B to Expand Private-by-Default, Blockchain Platform



Business

Espresso Systems Raises \$32M to Bring Scaling and Privacy to Web 3

“Privacy loves company”

Last year NYM & Secret Network announced partners' commitments to support builders.

Savvy investors know: the stronger the ecosystem – the higher interest within retail investors & people using utility tokens.

Business

Privacy Focused Blockchain Secret Network Announces \$400M in Funding

The project includes a \$225 million ecosystem fund and \$175 million accelerator pool.

Nym Technologies raises \$300M to advance internet privacy, sending token price up

The NYM Innovation fund will support research on markets and privacy-enhancing technologies.

1.3B both VC & retail investors supported the development of the privacy tech

Web3 privacy funding				Ecosystem fund	
\$298M	series B		Aleo	\$400M	
\$273M	series D		STARKWARE	\$300M	
\$136.7M	retail		Mina	\$160M	
\$119.1M	series B		Aztec	\$100M	
\$107.4M	series B		MobileCoin		
\$100M	retail		Status		
\$58M	retail		Secret Network (ex-Entangle)		
\$55.8M	retail		NYM		
\$46M	retail		Mask		
\$47.8M	retail		Orchid Labo		
\$35.4M	seed		Manta Network		

Still Privacy-centric investments play relevantly small role within whole Web3 investment landscape - around 4-5%.

Q4 2022

1	Web3/NFT/DAO/Metaverse/Gaming	31%
2	Trading/Exchange/Investing/Lending	13%
3	Infrastructure	7%
4	Payments/Rewards	7%
5	Tokenisation	7%
6	DeFi	6%
7	Privacy + security	4%

Q3 2022

1	Web3/NFT/DAO/Metaverse/Gaming	41%
2	Trading/Exchange/Investing/Lending	10%
3	Enterprise Blockchain	8%
4	DeFi	7%
5	Infrastructure	6%
6	Privacy + security	5%

Funds diversify their privacy-portfolios investing in different projects at the same time.

Polychain is an absolute champion – 13 privacy projects.

Fenbushi + gf.network – 9 projects.



Aleo, Anoma network, Manta Network, NYM, NuCypher, Oasis Labs, 0(1) Labs, Webb, Disco, Thesis, Foundation, =nil;, Light Protocol



Secret, Manta, Automata, Lit, Zcash, Sia, NuCypher, Status,



Aztec, Keep Network, Starkware, Mina



Mina, Oasis, Starkware, Zcash



post-ICO/IDO/TGE landscape

Retail fundraising is a common practice in the market. Projects from Status to Secret (earlier – Enigma) managed to deliver post-ICO products & scale decentralised tech.

ICO rush 2017-2018

Status



\$100M+

dock



\$20M+

Enigma (now-Secret)



\$45M+

TGE 2020-2021



Oasis Labs



\$45M+

Findora



\$21M+

TGE 2022



NYM



\$53M+

ChainPort



\$12M+

Interesting fact: NYM hit 1M registration within Coinlist in 2022.

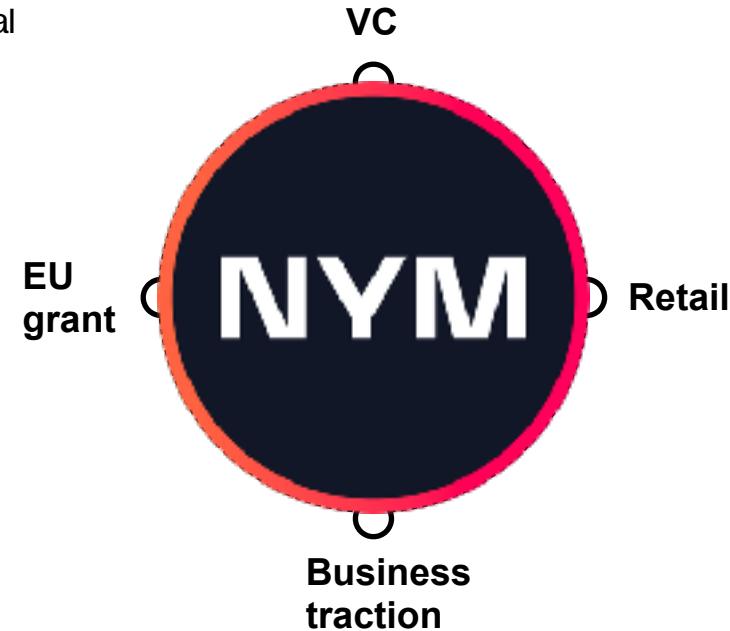


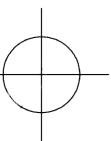
Privacy services diversify funding

Privacy builders know it's a "red flag" industry where communal funding isn't enough to sustain long-term growth.

NYM example

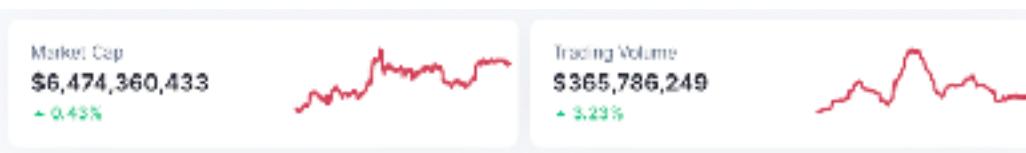
- receive initial money from the EU
- attract VCs
- outreach retail investors
- experiment with the token business utility
- empower ecosystem growth with the token supply





CRYPTOCURRENCIES

The bear market hit privacy coins trading volume & capitalisation.



#	Name	Price	24h %	24h \$	24h %	Market Cap	Volume (24h)	Outstanding Supply
55	Monero XMR	\$102.57	+0.50%	+0.50%	+0.50%	\$3,163,936,150	\$76,280,422 103,062 XMR	18,228,969 XMR
56	Zcash ZEC	\$65.01	+0.31%	+0.31%	+0.31%	\$2,275,581,293	\$74,924,728 1,662,829 ZEC	16,381,982 ZEC
57	Dash DASH	\$48.54	+0.50%	+0.50%	+0.50%	\$540,680,475	\$61,921,523 1,613,120 DASH	11,705,140 DASH
101	Decred DCR	\$2161	+0.64%	+0.64%	+0.64%	\$321,346,087	\$8,445,634 65,200 DCR	14,661,112 DCR
102	OpenBazaar OBZ	\$0.54,795	+0.21%	+0.21%	+0.21%	\$272,006,523	\$88,768,828 823,681,307 OBZ	5,725,710,503 OBZ
103	Horizen ZEN	\$10.57	+0.51%	+0.51%	+0.51%	\$149,242,619	\$17,769,488 1,079,812 ZEN	13,270,192 ZEN
104	Boxcar BXC	\$1.66	+0.28%	+0.28%	+0.28%	\$126,238,824	\$18,039,467 11,924,452 BXC	30,100,706 BXC

18 jan 2023

Economy shed more than 54% against the U.S. dollar as it dropped from \$11.7B in Jan. 2022 to the current \$6.4B.

NFT category Market Cap, for example, is \$16,34B





Monero still is the largest privacy coin by market cap.

Jan. 2022

XMR's price was around \$202.97 per unit and it had a market valuation of around \$3.66 billion on Jan. 19, 2022.

Today, XMR is exchanging hands for around \$174.05 per coin and it has an overall market capitalization of around \$3.17B.

**Comparing
Monero's Market cap
with other privacy
currencies**

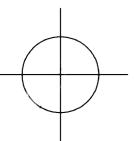


Zcash

holds the second-largest privacy coin market valuation this year and in January it was around \$1.53 billion.

Today, ZEC is exchanging hands for around \$45.23 per coin and it has an overall market capitalization of around \$731M.

Monero	\$3.17B
Zcash (ZEC)	23%
Decreed (DCR)	10%
Oasis Network (ROSE)	8.5



TRACTION

1.3% - privacy projects' DeFi market share

Category	Ranking (by TVL)	Protocols	TVL
Dexes	1	674	\$17.72b
Privacy	16	9	\$235.21m

Privacy projects ranking by categories

	Chains	1d Change	7d Change	1m Change	TVL
Bridges	9  ChainPort	   	+4.53%	-3.03%	+5.02%
Services	28  Sutenuzu	 	-0.25%	+4.70%	+11.26%
Yield	76  Cyclone	   	+0.38%	+11.32%	+10.38%

Tornado cash & Aztec are DeFi privacy champions

Privacy TVL Rankings

Name	Chains	1d Change	7d Change	1m Change	TVL
1 Tornado Cash	10	+0.04%	+10.07%	+25.00%	\$212,12m
2 Aztec	4	-1.01%	+11.29%	+30.07%	\$10,42m
3 Sienna Network	3	+0.18%	+14.45%	+23.13%	\$3,828,393
4 Raigun	5	+0.05%	-4.19%	-5.56%	\$3,014,692
5 zkBob	2	-0.89%	-6.54%	+2.30%	\$325,086
6 ShadeCash	1	+2.48%	+36.64%	+62.63%	\$46,697
7 Sherpa Cash	1	+1.96%	+37.19%	+45.55%	\$28,515
8 Typhoon Cash	1	+1.36%	+18.65%	+30.61%	\$26,935
9 Garble Money	1	-0.10%	0%		\$11,201

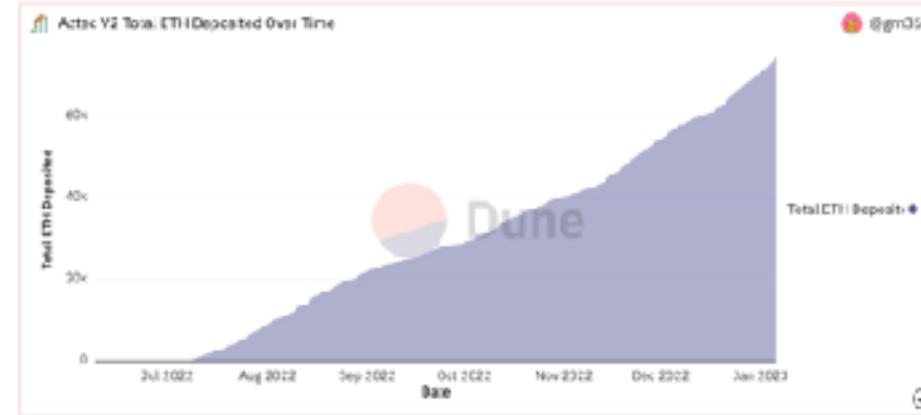
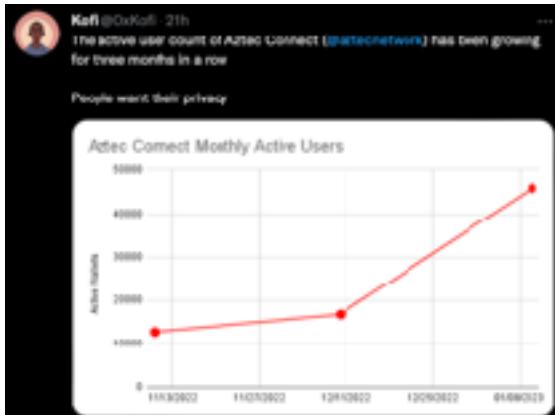
Project spotlight



Layer 2 network brings scalability and privacy to Ethereum.
Aztec uses zkSNARK proofs to provide privacy and scaling via our zkRollup service.

\$16.28M TVL

1M network transactions since launch (Aztec Connect)



**Casual dApps like
browsers &
messengers are
driving privacy literacy
& direct sales.**

Wallets

Edge	500K+
Samourai Wallet	100K+
Green: Bitcoin Wallet	100K+
Beldex Wallet	10K+

Browsers

Brave	100M+
Carbon	5M+
Status	1M+
Opera Crypto Browser	1M+
Puma Browser	500K+

Messengers

Session Messenger	1M+
Status	1M+
BChat - Web3 Secure Messenger	100K+
xx messenger	10K+

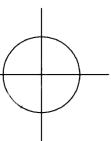
VPN

Mysterium VPN	500K+
Orchid: VPN, Secure Networking	100K+
BelNet: A decentralized VPN	10K+

“Office” alternative suite

Skiff Mail	100K+
Skiff Pages	5K+
Skiff Calendar	100

Important note: downloads aren't equal recurrent or paying users



OTHER FUNDING OPTIONS

Independent developers & researchers have access to various funding streams from communities to ecosystems.



Rotki - The portfolio tracker and accounting tool that protects your privacy

Estimated lifetime funding received ~\$456,000

[Gitcoin](#)



<https://ccs.getmonero.org>



<https://aztec.network/grants>

~5% of the market players have grant programs

Usually, they are ecosystem-centric players like [Mina](#) or [Oasis Foundation](#).

Grants are norms for community engagement within the privacy currencies

- [Zcash](#)
- [Monero](#)
- [MobileCoin](#)

Oasis Grants Program

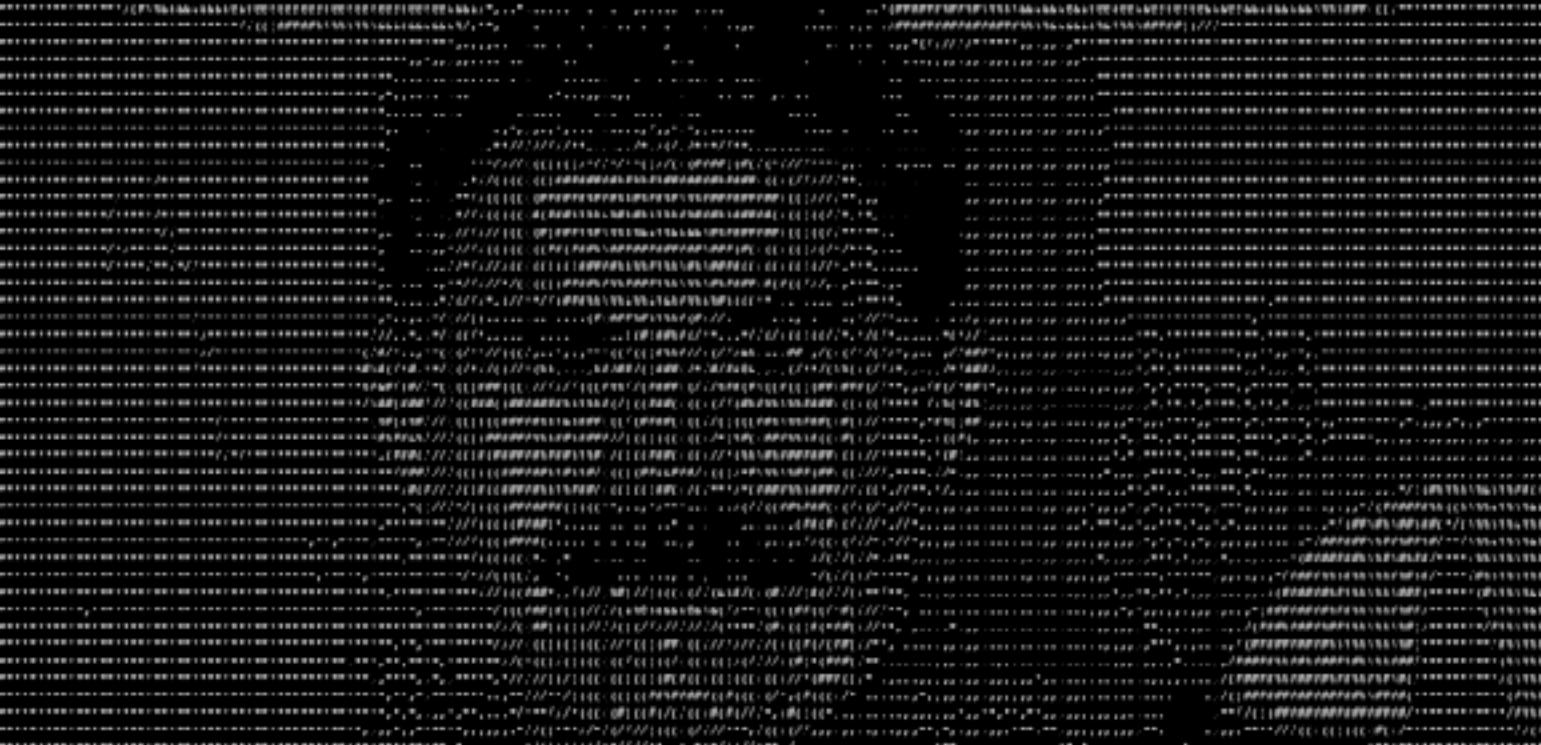
The Oasis Bloom Program helps developers kickstart their projects.

[Apply Now >](#)

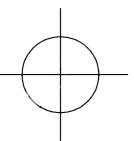


Interesting examples: DID ([Dock](#)), Storage ([Sia](#)) or post-quantum solutions ([xx](#))





BUILDING



USE-CASES

Developers explored 500+ different private use-cases. And it's just the beginning of potential privacy implications.

multisig	2FA	KYC	reputation	Verifying Supply Chains
gated community access	OS	cross-chain comms	Malicious actors blocklist	Proof of GitHub Contributions
portfolio manager	DAO voting	social	Private NFT	RPC
MEV minimisation	geo	credentials	Viewing Keys	Unique in-gaming items
api	notes	Age verification	Private galleries	Order history (marketplace)
Sensitive doc sharing	Anon bids	E-mail	VPN	Storage

R&D plays a crucial role in privacy landscape creation (beyond just financial use-cases) & argumentation against privacy sceptics.



Private NFTs played insignificant role in the Global NFT sales (\$21,9bn in 2022)

Reference:

[Stashh](#) marketplace trading volume ~ **\$7M** (last 12 months)

Major players like [OpenSea](#) don't promote privacy, more - anti-scam [safety](#).



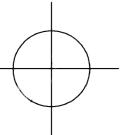
We received a lot of great bids on the first NFT in the collection, but Anon took the prize.

The 2nd auction, 'Pumpkin and Honey Bunny' is now live on [torantinonfts.com](#)



11:35PM · Jan 24, 2023

Read this as a necessity for the [Privacy-Web3 Market-Fit](#)

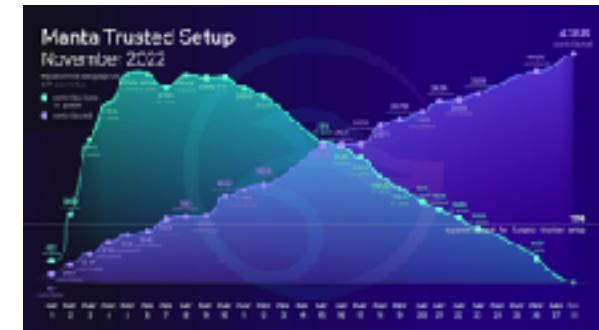


TRUSTED SETUPS

A multi-party computation ceremony turned into creative community-activation.

Manta Network breaks a world record with 4,300 contributions.

4,300 contributions across 177 countries



<https://twitter.com/MantaNetwork/status/1600322208898981889>

2,510 contributions

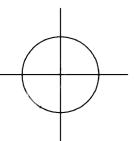


<https://blog.namada.net/completion-of-the-namada-trusted-setup/>

Namada

"Remarkable sources of randomness ranged from more to less appetising delicacies, environmental noise recording [by Palo Verde Generation Station](#) or [Oregonian nature combined with winter rain sounds](#), spotty friends or [little half-human and half-ET's frenetic typing](#)".

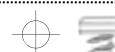




GITHUB STATS

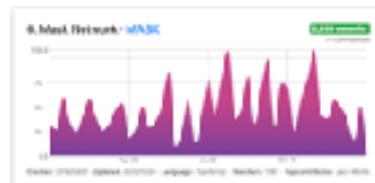
Privacy solutions developers extensively contribute to the general blockchain codebase.

- **43000+ commits** were generated by the top10 privacy projects
- **2 privacy services in top10 GitHub commits** at Cryptomiso tracker: Mina & Mask Network
- **2nd the most popular** – Mina





<https://github.com/MinaProtocol>



<https://github.com/DimensionDev/Maskbook>



<https://github.com/particl>



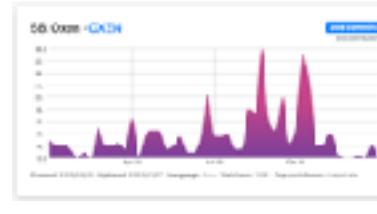
<https://github.com/zcash>



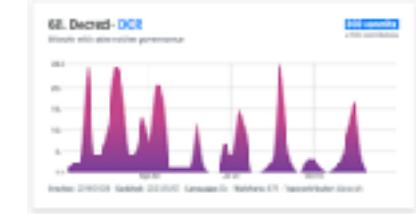
<https://github.com/status-im>



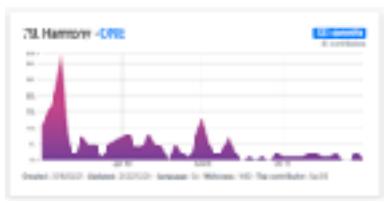
<https://github.com/mysteriumnetwork>



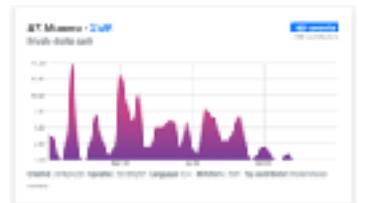
<https://github.com/oxen-io>



<https://github.com/decred>



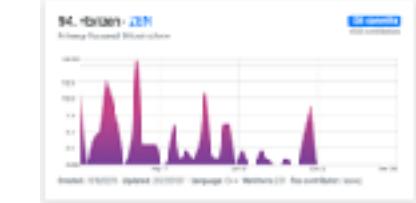
<https://github.com/harmony-one>



<https://github.com/monero-ecosystem>



<https://github.com/PirateNetwork>



<https://github.com/horizenofficial>

Other notable GitHub repositories

- <https://github.com/AztecProtocol>
- <https://github.com/darkrenaissance/darkfi>
- <https://github.com/Manta-Network>
- <https://github.com/scritlabs/SecretNetwork>
- <https://github.com/nymtech>

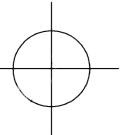
<https://github.com/hyle-team/zano>

100 contributors in the Main GitHub repo - example of active collaboration within privacy projects

General analysis showed high developer activity & contribution within privacy solutions.

Zcash	100
Particl	100
Status	100
Mina	76
Mask	74
Secret Network	50
Mysterium	38
NYM	35
DarkFi	27
Aztec	22

This is a reference table, not ranking



ECOSYSTEMS

The Privacy category is frequently missing from the protocol ecosystems

Ethereum

Payments	
 Tornado cash	Send anonymous transactions on Ethereum.

Browsers	
 Brave	Earn tokens for browsing and support your favorite creators with them.

Portfolios	
 Felt	Over 100+ portfolio tracks, earnings, spending and so much more that fits into your inbox.

Polygon

DeFi	662
Utility	275
NFT	501
Staking	392
DEX	80
DAO	101
DApps	211
BBB	92
Social	83
Taxis	65

Selected teams managed to develop extensive ecosystems like Secret.

DAPPS + ECOSYSTEM

Secret 28 dapps

<https://scrt.network/ecosystem/dapps>

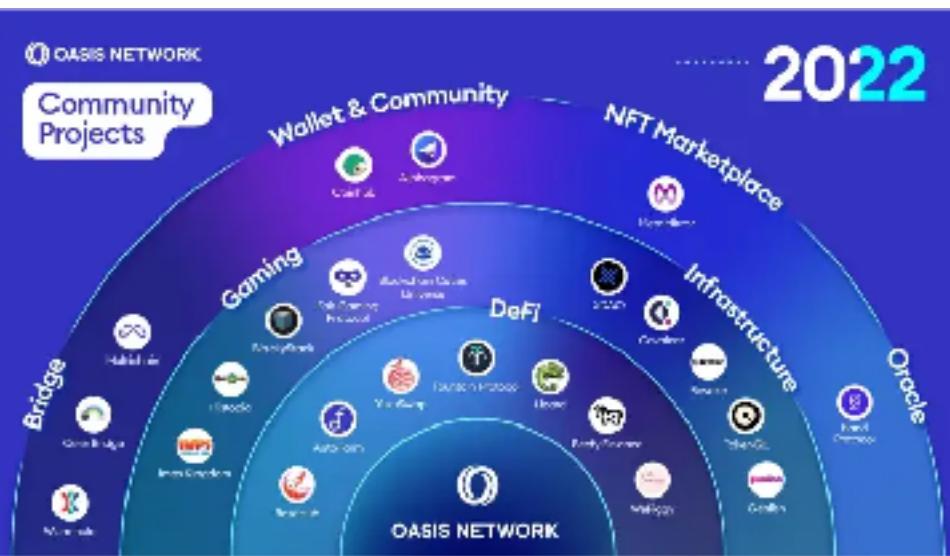
Tooling + eco

<https://scrt.network/ecosystem/tools>

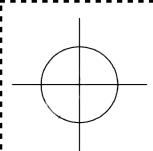
Note: the amount of ecosystem players usually doesn't match traction (both applicability & TVL)



2022 was the year of ecosystem funding commitments. Oasis, NYM, Secret announced hundreds of millions dedicated to internal & external developers.



"Our ecosystem fund grew from \$160 million to \$235 million with support from new partners", – Oasis Labs.



R&D

10+ labs are scaling privacy implementation

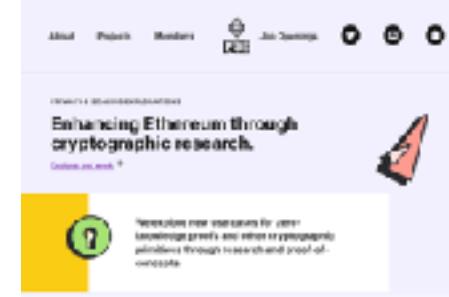
maturing cryptography, building use-cases, delivering services for ecosystems.



www.pOxeidon.xyz



<https://o1labs.org>



<https://appliedzkp.org>



R&D labs is a typical entity responsible for the tech delivery behind protocols & solutions.

Some labs research new technologies beyond locked-in ecosystems like Polkadot or Cosmos, & even act as a governing body before foundation.

Lab approach

Internal research

- Dev as a service
- Core protocol features dev
- Critical ecosystem features dev



External research

- Grants
- Hackathons
- Partnerships

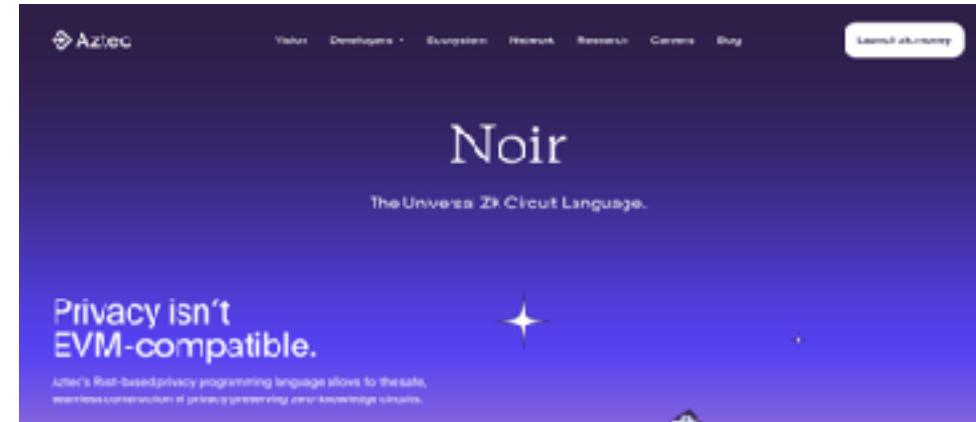
Lab evolution



Extensive R&D contribution lead to 2 separate ZK language development.

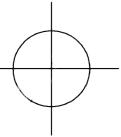


<https://leo-lang.org>



https://developer.aleo.org/getting_started/

Privacy companies' codebase legacy would be beyond just privacy but accelerate general ZK-applications development & experimentation.



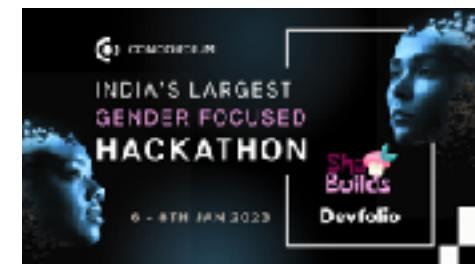
HACKATHONS

2022 was the year of privacy-centric hackathons.

Both privacy projects & event organisers put efforts into making privacy a cornerstone of the crypto market.

To name a few:

[ETH Berlin](#) or [ETH Brno](#).



Winners' examples

[rsociety](#)



LET'S HACK ETHBERLIN. We redistribute the 10k DAI from the Open Track to all the hackers, claimable from our smart contract.

[Lunar Wallet](#)



Is the first privacy native Ethereum wallet based on a built-in integration of TOR. This architecture enables users' IP addresses to be isolated from third parties.

Important mention: 1st [Monerokon](#) in 3 years happened in Lisbon

NYM collaborated with Filecoin to foster innovation within KYIV Tech Summit.

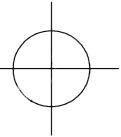
The Ukrainian–Russian war is a catalyst for privacy–centric projects, especially when your sensitive data could lead to unprecedented threats.

The “Citizen5” winner follows the general NYM’s trajectory for supporting freedom of speech via Anon data storing & sharing. Julian Assange, Edward Snowden & many other activists leaking sensitive data are applicable here.



<https://blog.nymtech.net/be-brave-as-ukraine-build-anondrop-at-the-kyiv-tech-summit-hackathon-4959ea99cfb8>



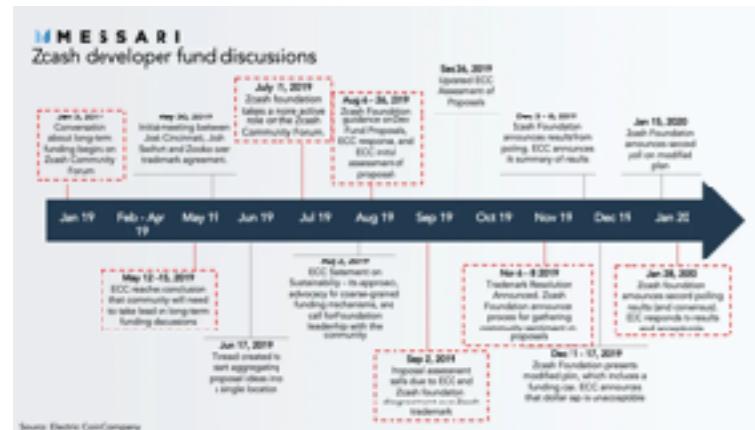


GOVERNANCE

Decentralised governance is more mature within key privacy coins Zcash & Monero.

Zcash highlights

- Transparency reports
 - Foundation + Electric Coin. Co
 - GitHub-centric ZIPs
 - Public incorporation & financial docs
 - active & public R&D



<https://messari.io/report/decentralizing-zcash>

2 vs 100+

Improvement Proposals comparison Mina vs Zcash



<https://github.com/MinaProtocol/MIPs>

<https://github.com/zcash/zips>

Privacy companies don't rush to decentralise their efforts when “everyone is making DAO around”.

Phala, Mina & Status are the ones to follow for active DAO transformation

deepdao.io stats

rank	organization	treasury	last 24hrs	top treasury tokens	main treasury chains	tokens holders	lifetime participants	proposals	votes
21	Phala	\$74.7M	0.9%	11	6	2.5k	0	24	27
68	Tornado Cash	49M	49.1%	6	5	8.0k	179	31	429
159	AssangeDAO	\$308.9k	0.1%	6	5	0.3k	11k	12	36k
238	Status	\$3.7k	0.1%	10	4	2	2	23	17

Note that the Tornado Cash case affected DAOs that went on hiatus.
Sacred Finance example

- [DAO announcement](#)
- [Discord silence](#)



The next big step for privacy companies – make financials transparent & accountable

Q3 ZF FINANCIAL SNAPSHOT

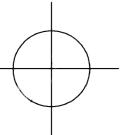
LIQUID ASSETS	UNRESTRICTED FUNDS		RESTRICTED FUNDS - ZCG	
	COIN BALANCE	USD VALUE	COIN BALANCE	USD VALUE
USD	5,531,529.72	\$5,532,530	2,441,889.45	\$2,441,893
USDC	0+	0+	0	0
ZEC	177,263.44	\$0,865,027	142,790.52	\$7,045,051
BTC	63.4	\$1,208,183	-	\$-
ETH	11.89	\$16,814	-	\$-
		\$16,822,453		\$2,447,944
LIABILITIES				
GRANT COMMITMENTS		\$102,580		\$2,739,918
ACCRUED EXPENSES & PAYROLL LIABILITIES		\$170,068		
		\$273,618		\$2,739,918
NET LIQUID ASSETS		\$16,548,841		\$2,738,026
USD VALUE (as of Sept. 30): \$22,600 USD/ZEC \$16,443.77 USD/USDC \$1,329.51 USD/ETH		Note: This simplified balance sheet does not include intangibles or illiquid assets and liabilities that would appear on ZF's full balance sheet (e.g. trademark, etc.).		



The big future challenge for this ecosystem is privacy. The status quo involves putting large amounts of information on-chain, which is something that is "fine until it's not", and eventually will become unpalatable if not outright risky to more and more people. There are ways to solve this problem by combining on-chain and off-chain information and making [heavy use of ZK-SNARKs](#), but this is something that will actually need to be worked on; projects like [Sismo](#) and [HeyAnon](#) are an early start. Scaling is also a challenge, but scaling can be solved generically with rollups and perhaps validiums. Privacy cannot, and must be worked on intentionally for each application.

- **Vitalik Buterin, Ethereum co-founder**

books



POLITICAL POLARISATION

Blockchain neutrality dilemma:

how the network could be positive for humanity
if it's censored (incl. self-censorship)?

Enterprise + state-ready decentralisation

- 100% Compliant
- Approved by Governments + Corporations
- Approved by business consultancies like EY + Gartner

Point of collision

- KYC
- Privacy policies (data aggregation)
- Capitalistic extraction practices
- Relations between corporations & state

Decentralisation

- 100% control over the privacy
- Selective disclosure
- Anonymity to non-democratic governments

Lots of corporations can't join public protocols feared of transparency, hacks & sensitive data leakage.

But privacy solutions from Polygon to Oasis Labs are fostering corporate-blockchain fit.

COMPANIES • BLOCKCHAIN

Equifax and Oasis partnering to build 'privacy first' on-chain KYC solution

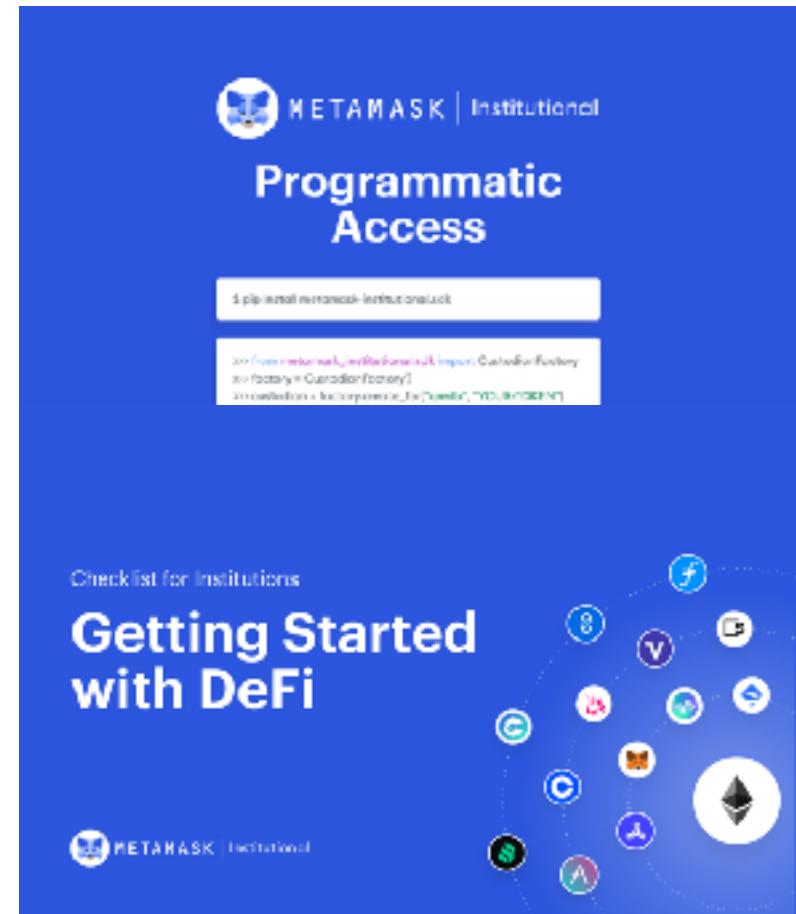


Privacy market has a completely opposite attitude to corporations

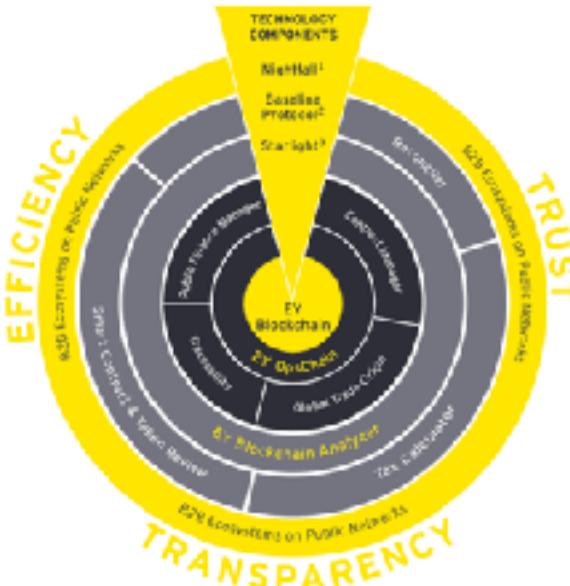
- one camp wants to abolish corporations
- other wants to transform them (ConsenSys, Oasis Labs)

Privacy Policies outrage shows that corporate &/or complaint practices are a centralised rudiment. So it **would be hard for these companies to sit on 2 chairs:**

1. Enterprise-friendliness
2. Community-driven.



Market actors should analyse corporate solutions to check if they match the initial Bitcoin, Ethereum ethos.



Ernst & Young Principal and Global Innovation Leader Paul Brody is bullish on the outlook of Ethereum going into 2023. He predicts a shift towards industrial, instead of purely financial applications.

EY blockchain solutions

EY OpsChain Contract Manager: Engage in a procurement workflow by issuing request for quotes, contracts, purchase orders and invoices across a network of trusted business partners.

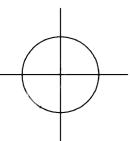
EY Blockchain Analyzer: Smart Contract & Token Review — Review the underlying code of smart contracts to increase confidence in blockchain-enabled transactions.

EY Blockchain Analyzer: Tax calculator — Upload transactions to download a Form 8949, which is used to calculate capital gains for US tax returns.

EY OpsChain Traceability: Improve traceability and transparency across the supply chain through the use of notarization and tokenization.

EY OpsChain Public Finance Manager: Provides governments and public sector organizations the solutions and tools for the effective management of public finances, while producing near-real-time performance reporting and advanced analytics.

EY Blockchain Analyzer: Reconciler — Bulk-reconcile on-chain and off-chain data to identify matches and mismatches of transactions.



ANONYMITY

“We are opposed to the state”

– Amir Taaki



**DarkFi challenges compliant privacy
& state dominance
over the web.**



Privacy (or even anonymity) is integral to DarkFi's political agenda. “Decentralisation” is a political notion, but selected few privacy leaders to go anti-state in their communication.

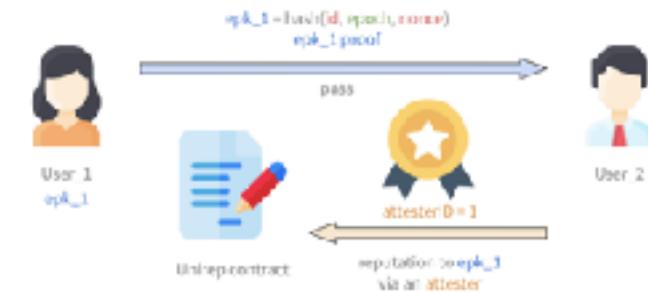
**PSE is trying to apply reputation to anonymity.
Basically, creating a scoring for everyone.**



Universal Reputation

The UniRep protocol evolved from an [ethresearch proposal by Barry WhiteHat](#) for a system where users could be banned or have their reputation destroyed even if they are anonymous.

The proposal outlined a mechanism for giving positive and negative reputation in a way that the user must accept while maintaining privacy.



Open question: how not to replicate negative policing practices from around the world on-chain.

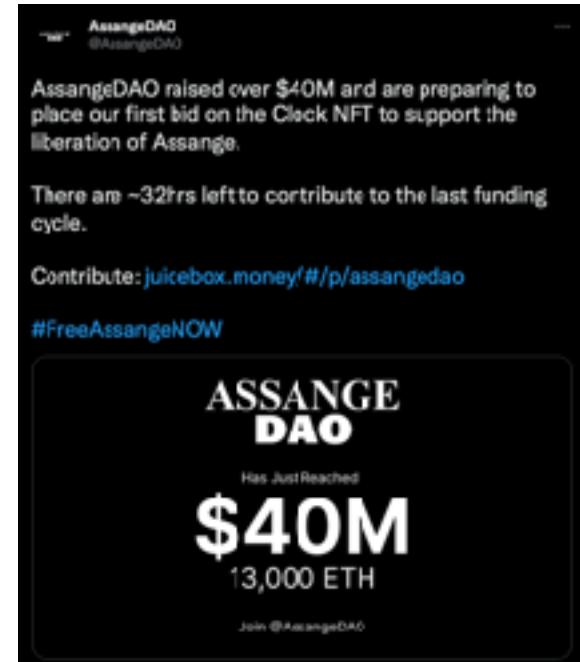


Political polarisation goes beyond so-called CeFi & DeFi markets. It raises questions about the community's values.

"Ethereum was not invented to make you rich, Ethereum was invented to make you **free**."

[@owocki](#)

Privacy helps to imagine a world where whistleblowers could work for humans without risk.



<https://assangedao.org>

How do trust projects if their team is fully anonymous?

They should attract a broader audience to scale.
How could anyone trust them if founders stay anon?

There are several exploration trajectories

1. Powerful storytelling behind the project.
2. One non-anon central figure (“martyr”).
3. Appealing product (non-anon NFTs made by Banksy).
4. Non-anon partner: NGO like EEF or Whistleblower.
5. Great cause (“War on the big tech”).

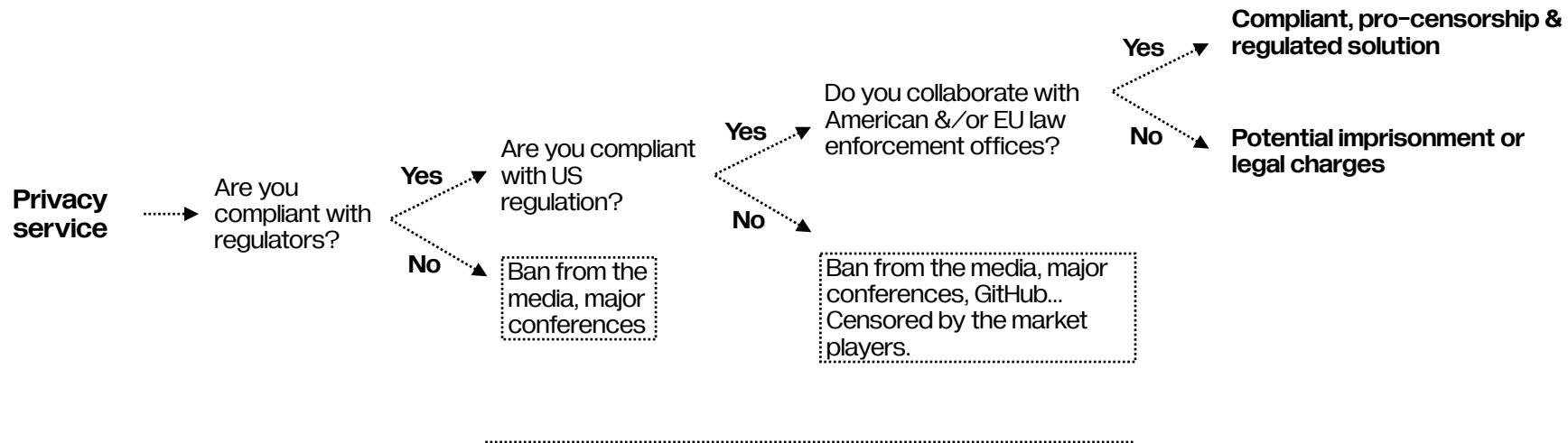


A potential investor asked why he should buy genesis tokens from anons of LunarDAO?

<https://lunardao.net>

The Future of the privacy-as-an-ideology is under attack.

You can get imprisoned if you don't play by the USA rules.



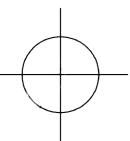
Market underground

Parallel economy

Community funded

Micro-communities

Niche media



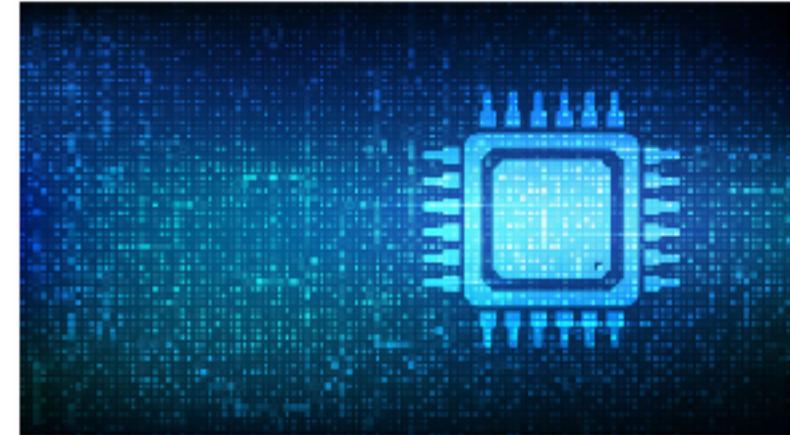
SELF-SECURITY

Privacy solutions are even more sensitive to hacks than non-privacy. Hacked funds and exposure of sensitive information damage market image.

Secret Network Crypto Transactions Not So Secret After All

Secret Network was supposed to keep transactions private, but researchers warn there's no telling how many people have decrypted them.

BY JEFFREY BROWN FOR REUTERSSec 10 DEC 2018



Case: <https://twitter.com/socrates1024/status/1597637285058863104>
SGX.fail website: <https://sgx.fail>

Only security audits, white hackers & community could prove that solution is private.

Privacy companies are experimenting with bug bounties, white hackers relations, security auditing to find a well-balanced approach to self-security.

Sienna's partners

Certik



Halborn



AUDIT REPORTS

vSIENNA →

SIENNA →

Rewards V3 →

SiennaSwap V1 →

SiennaSwap V2 →

SiennaLend →

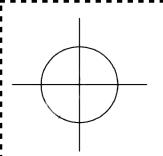
SiennaLend Updated Code →

Launched ICO →

Lending and Launched Updated Code →

Rewards Bonding Update →

<https://sienna.network/audits/>



CONFIGURABLE PRIVACY VS CONSENT

An open question to configurable privacy is how to avoid “dark patterns” like altering consent & giving agency over decision-making to a human?

Example:

- companies after GDPR found a way to trick humans: gather their data & surveil
- the web3 UX/UI should deliver true power over not just data, but the consequences of its leakages

Imagine this as a humanistic alert protecting the user from fast actions from **“Do you want to share your data with actor X?”** to **“We don’t recommend sharing this data if ...”**.

Explore more

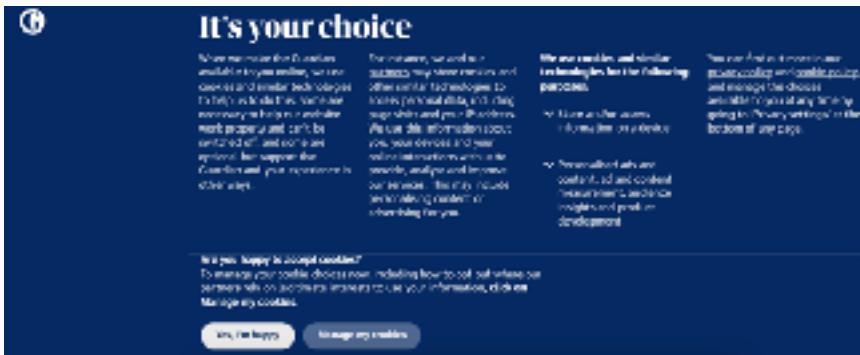
- [Aztec](#)
- [Espresso Systems](#)
- [Ruby](#)
- [Cerebrum](#)
- [Manta Network](#)

[cryptofireside.com](#)
privacy & transparency form

[Continue with Recommended Cookies](#)

The image shows a screenshot of the cryptofireside.com privacy & transparency form. It displays four separate sections, each with a label and a checkbox for 'Legitimate Interest' and 'Consent'. The sections are: 'Select: basic ads', 'Select: personalised ads', 'Select: personalised content', and 'Measure content performance'. Each section also includes a 'Cookie' checkbox and a '+' icon. The 'Consent' checkboxes are currently unchecked.

Web2 is lying to you



guardian.co.uk example

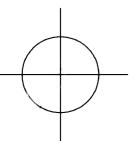
Web3 is confusing you

ZKP-enabled asset tracing for auditability

Yellow Submarine's sidechain supports auditable privacy-preserving assets using SNARK-friendly hybrid encryption and advanced Zero-knowledge Proof technologies such as Matrix sigma and binary-checking-friendly TurboPlonk.

<https://ys.finance/>

OPPORTUNITIES



SECURITY

Privacy could become a forefront of security. But instead privacy market delegate security advocacy to companies like Chainalysis.

Private wallets, for example, secure funds from hacking by default. But if you visit the product's website, they will say "We live in an Orwellian surveillance society where your information is being used to typecast and manipulate you". Meaning the state, but not hackers, scammers & other bad actors.

Radical on-chain security example.

Decentralized Security Incentivized for Everyone



<https://www.interlock.network/>

Opportunity: broaden audience range of privacy protection & became the mainstream toolbox for newcomers to "shield" themselves from cybercriminals.

Companies like Chainalysis or TRM would work with law enforcement units worldwide following the transactions.

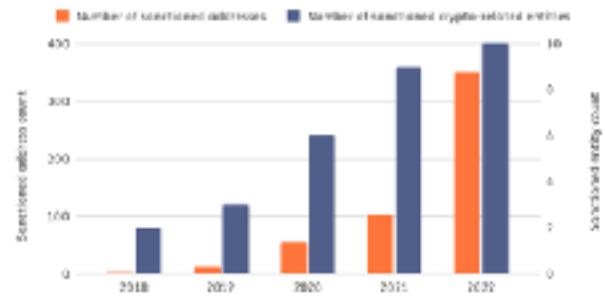
Privacy actors could actively add additional narration to general communication

- how could solutions be used to enhance security?
- what are the ethics of dev teams?

Denying that the market is full of scammers opens the door to cyber forensics to come & dominate the security agenda.



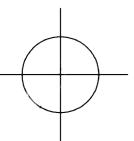
Sanctioned crypto-related entities and number of sanctions-related addresses by year added, 2018 - 2022



@Chainalysis

[How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime](#)





BIASES

Market is full of biases that stop founders to join their forces.

Privacy is for criminals

Why do you want to be anon if you have nothing to hide?

People don't want privacy

Privacy is norm

Privacy is a human right

Privacy is normal.

Privacy is for good guys. It's for moms and bike messengers and foodies.

Privacy is for business meetings and voting booths. It's why we have shower curtains. It's why we have that little padlock icon in our browser bar.

Privacy protects you from discrimination and from identity theft, and it keeps your food-delivery history under wraps. It can also shield you from those creepy somebody-has-definitely-been-listening-to-my-thoughts ads on social media apps.

Privacy isn't about shutting out everyone and everything. Instead, privacy gives you the power to choose what and with whom you'll share. It provides safety, control and the right to grant access.

Privacy gives you the ability to express yourself, to be creative, to spend your time and your money in whatever manner you like, without the scrutiny of others. It protects our intimate moments, our most embarrassing ambitions, our radical ideas and the ability to be our true selves.

Privacy is freedom, consent, dignity and security.

Privacy is normal.



NGOs like The Electronic Frontier Foundation have defended civil liberties for years.

That's why their level of augmentation against biases is more mature than the industrial players.

Collaboration with such NGOs would help to prepare mature ambassadors of both free speech & privacy (beyond legal officers).

Open question: how to make communities participate in privacy-as-a-movement? Creating an army of privacy guardians all over the world.

Code is Speech is a Core Principle

For decades, U.S. courts have recognized that code is speech. This has been a core part of EFF's advocacy for the computer science and technical community, since we established the precedent over 25 years ago in *Barnette v. U.S. Dep't of State*. As the Tornado Cash situation develops, we want to be certain that those critical constitutional safeguards aren't skirted or diluted. Below, we explain what those protections mean for regulation of software code.

<https://www.eff.org/deeplinks/2022/08/code-speech-and-tornado-cash-mixer>

US Treasury announcement: ECC's engagement on policy for economic freedom

Rebecca Greenbaum | August 8, 2022



<https://electriccoin.co/blog/us-treasury-announcement-eccs-engagement-on-policy-for-economic-freedom/>

Privacy companies could use comms to empower biased people.

But they conflict with each other at the moment.

**Automate &
Free the Web**

We can
reclaim the
internet
together

**Building a world
where your life
belongs to you.**

Privacy first.
Privacy second.

Live online without a trace.

Next generation
privacy for web3

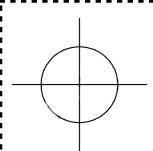
**More Privacy
Limitless Possibilities**

Discover a world of complete
privacy with Sahara

Welcome to the world of
encrypted DeFi ✨

Unchain the value of sensitive data. At scale.

Next Privacy Finance Ecology Protocol



Parallel economies evolute into Network states.

The Status team is launching Logos - a “grassroots movement” to provide trust-minimized, corruption-resistant governing services and social institutions to underserved citizens.

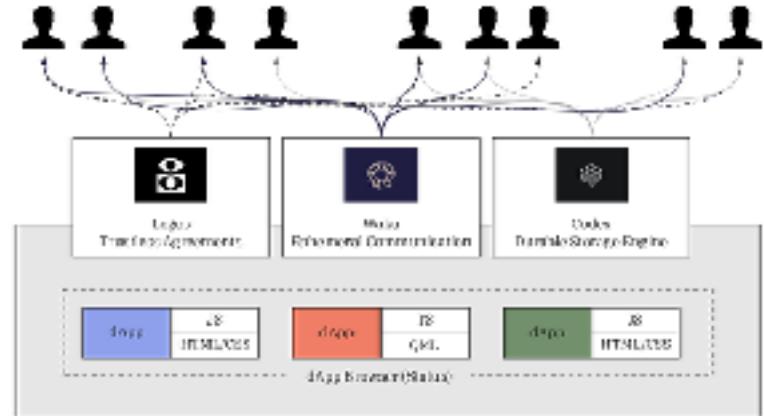


Logos.co

The main difference between Balaji's Network state & Logos is a non-capitalistic approach to the parallel economy from the latter.

The network state is an example of parallel economy executed within the Status' tech stack: Browser, Messenger, Storage plus DAO.

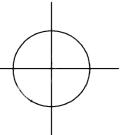
These services are highly synchronised with Ethereum ethos, decentralisation & Sovereignty.



Jarrad Hope, Status CEO

ETH Barcelona: [From Crypto-Currencies to Crypto-States](#)
Paralelni Polis: [Cypherpunk Suprajurisdictions against the Nation-State](#)





LEGAL DEFENCE

2023 will be a year of privacy's legal defence. Alliances, private currencies teams, non-profits like EEF or Coincentral would advocate for “privacy as a human right”.

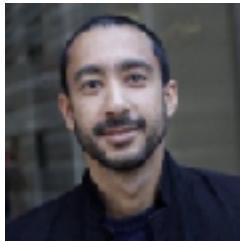


Blockchain Association
Benri Corporation
Betapersei
Caribbean Blockchain Alliance
CyberStorm
The Crypto Freedom Lab
DeFi Education Fund
Desert Blockchain
Edge
Electric Coin Co
Espers
Filecoin Foundation
Free Software Foundation
FrogCoin
LearningProof
Ledger
Manta Network
Mobilecoin
MotaCoin
Mysterium Network
Nighthawk Wallet for Zcash
Nillion Network
Nym Technologies
Protocol Labs
Proton
Quiet
Radiant Commons
RedditCoin
Reneum
SealVault
Secure Internet Voting
The Tor Project
Tutanota
WCOIN
Web 3.0 Technologies Foundation
Web3 Working Group
[WebQ.org](https://www.webq.org)
Zcash Foundation



Legal experts & policy makers are already part of privacy-centric projects.

[@ghappour](#)



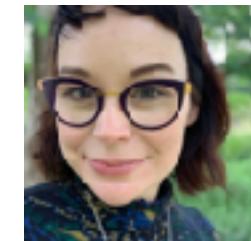
Prof [@BU_Law](#) & General Counsel [@nymproject](#)
Formerly: trial attorney, Guantanamo habeas counsel.

[@paulbrigner](#)



Head of U.S. Policy and Strategic Advocacy
[@ElectricCoinCo](#)

[@silkenoa](#)



crypto lawyer & mathematician - blockchain
aficionada & feminist - previously CLO/GC at
[@gnosisDAO](#) - [@LSEMaths](#) & [@StanfordLaw](#) alu



CONCLUSION

Analytical companies collect & analyse personal data right now.

Law enforcement agencies surveil the network. If there will be no community pressure – people won't even know about it.



Market actors have different views on privacy.

It's a "default lifestyle" for Monero followers, protection from prosecutions for Iran citizens, and the barrier to mass surveillance for law enforcement agencies.

Human rights

New business model

100% compliance

Do you
really own
your data?

How humanistic
is consent?

What if this government
is China or Syria?

Sovereignty

**Privacy
for enterprises**

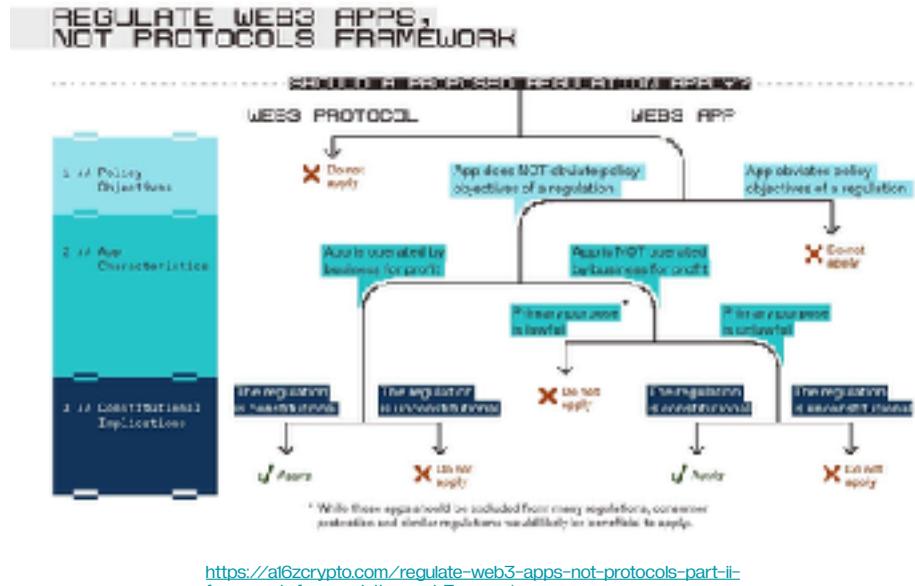
**Privacy
for governments**



Privacy market players are aware that extensive regulation could lead to

- open-source developers being imprisoned
- DAO voter's prosecution
- DAO-as-an entity sanctioning
- solutions banning, censoring, removing
- financial sources sanctioning

If this happens, privacy would have a “red flag” among investors, devs, media, and mass audiences.



Blender.io, Tornado Cash, Bitzlato cases showed that regulators would stress out all projects related to third-party money laundering or drug trafficking.

Dynamics

Market



Law enforcement & Chainalysis

1. Develop.
2. Test.
3. Scale.

1. Try to crack.
2. a) Positive – aggregate data & surveil.
b) Negative – put legal pressure.



ZK magic won't solve all privacy-related issues. Tornado Cash has ZK, for example.

Zk-Rollups will remain centralized. All rollups live on Ethereum rely on a centralized party known as a sequencer to order transactions.

Sequencers learn all your transactions and can profit from MEV at your expense.

2023 will be a year of ZK R&D, hacks & extensive testing. Think of it as an experiment to be proved – you won't be disappointed with its breaches.

FHE (fully homomorphic encryption), MPC (Multi-Party Computation) are other secure approaches to look up to in 2023.

Further read: <https://scrt.network/blog/beyond-zk-guide-to-web3-privacy-part-2>



Programmers were degraded to
robots by their bosses
- Ivan Jelincic, DarkFi

The tension between regulators & community would lead to the new developers class (or return to the roots of “free developers”).

Cypherpunks, Lunarpunks rhetorics help to unify various people around code self-sovereignty. So developers could capture value in projects & become owners of their societal roles.



<https://www.youtube.com/watch?v=QA3YZVDUN5s>

The general privacy use-cases are just on the horizon.

2023 will be a year of general privacy applicability from gated access to DAOs to private NFT collections.

Give Feedback On Proposals Anonymously

Anoun allows noun-holders to give feedback on proposals while maintaining their privacy using zero-knowledge proofs.

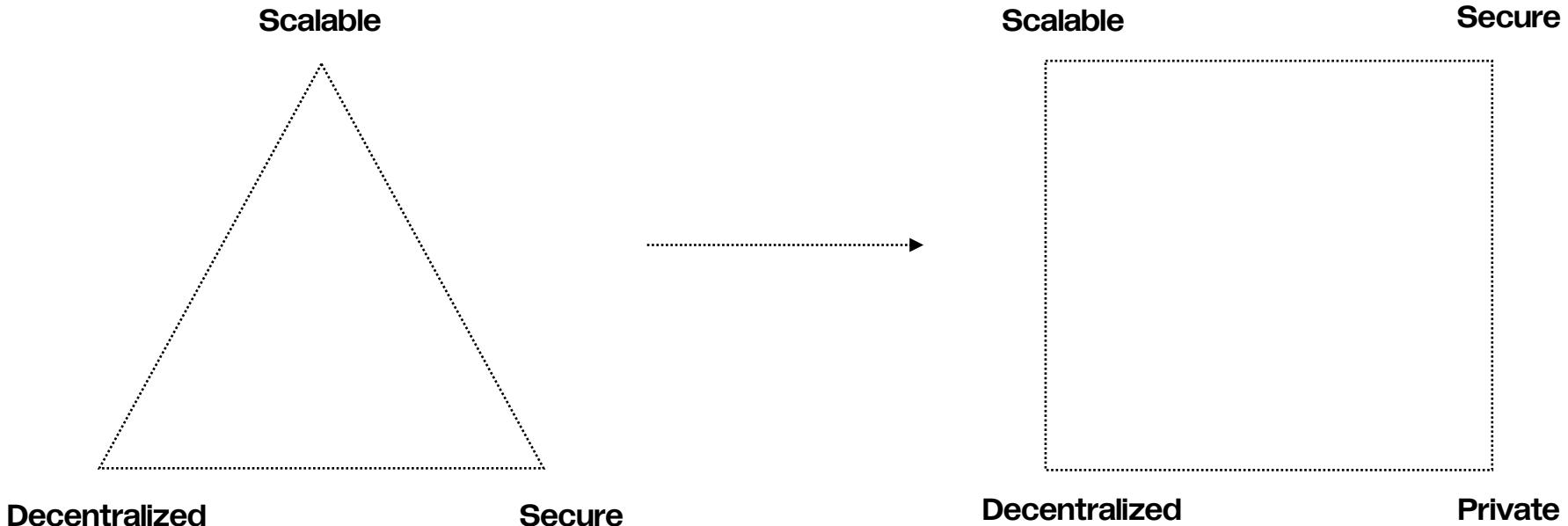


[AnonDAO](#)
[AnonNFT](#)
Anon ???



Blockchain quadrilemma is already here:

should we give away privacy in exchange for security or scale extensively (rollups) with privacy-as-a-secondary need & what would happen with privacy if the network becomes more centralised?



Privacy is significant in Big tech's public policy.

It diverts attention from Surveillance capitalism, market monopolisation & locked ecosystems. Web3 actors should ask themselves about the differences between them & champions of centralisation?



Privacy is a fundamental human right. It's also one of our core values. Which is why we design our products and services to protect it. That's the kind of innovation we believe in.

www.apple.com/privacy/



Your privacy is our priority. With end-to-end encryption, you can be sure that your personal messages stay between you and who you send them to.

www.whatsapp.com/privacy



At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organisations can control their data and have meaningful choices in how it is used. We empower and defend the privacy choices of every person who uses our products and services.

<https://privacy.microsoft.com/en-GB/>

Vision is the necessity for privacy-enhancing services.

It's rare for a privacy product company to have a long-term roadmap.

Example #1: the Manta network's roadmap ended last year (it was updated within the newsletter – generalised take for 2023).

Example #2: Electric Coin Co. – they published a 30-year vision. Here, the vision should be taken as a public commitment to popularising private cryptocurrencies. This entails the need for a comprehensive strategy and people with strategic thinking.



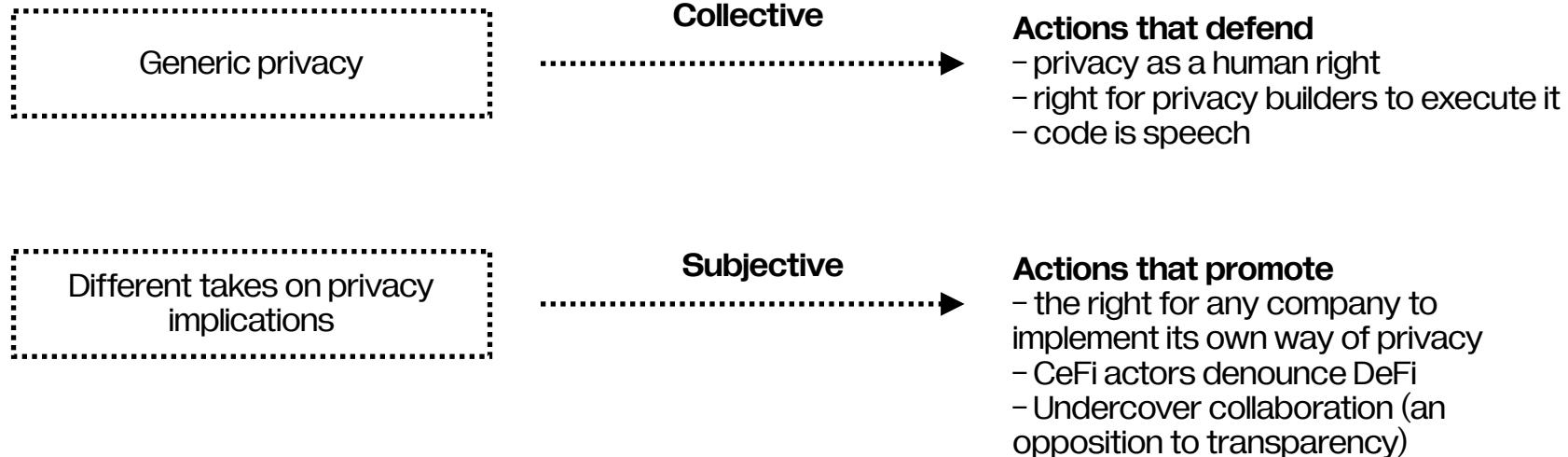
NYM

2018-2020	> Inception
2021	> Mainnet Launch
2022	> Token Launch
2023	> End-User Adoption
2024	> Institution Adoption <ul style="list-style-type: none"> Support enterprise use cases and institutional adoption - partnering with providers like R3, Signal, Google and IBM Cryptocurrency integration with finance, medical and personal data sectors API for integration into browsers and operating systems + standardise API's Create hardware wallets and secure dark wallets Scale to millions of users

Year end reports is a nice source of further research helping to understand how projects approach their commitments, roadmaps & future plans.

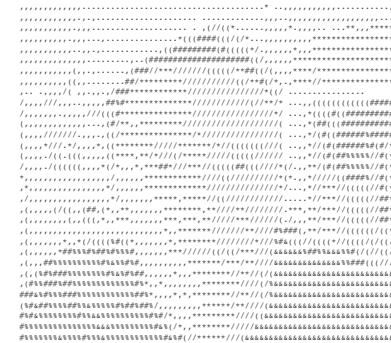
<u>Iron Fish</u>	<u>Lit</u>	<u>Partisia Blockchain</u>
<u>Oasis Protocol</u>	<u>Particl</u>	<u>Ruby Protocol</u>
<u>Findora</u>	<u>Manta Network</u>	<u>BlockWallet</u>
<u>Aleph Zero</u>	<u>Sia</u>	<u>Phala Network</u>
<u>Aleo</u>	<u>Horizen</u>	<u>Skiff</u>
<u>Suterusu</u>	<u>NYM</u>	<u>Oasis Protocol</u>

Market players should find out ways to distinguish between different takes on privacy (Monero Vs Zcash) & collective action that protects both users & builders.



You don't need to live in a distant future to access full-stack privacy.

While network-level privacy is around the corner (1 year+) - casual dApps from wallets to messenger are available today.



If web3 means ownership over data
Then it should be private

Data ownership

==

Privacy

You
Data

P
r
i
v
a
c
y

Big tech
Governments
Analytical companies
Data brokers
Marketing agencies
Hackers



To rephrase a famous quote

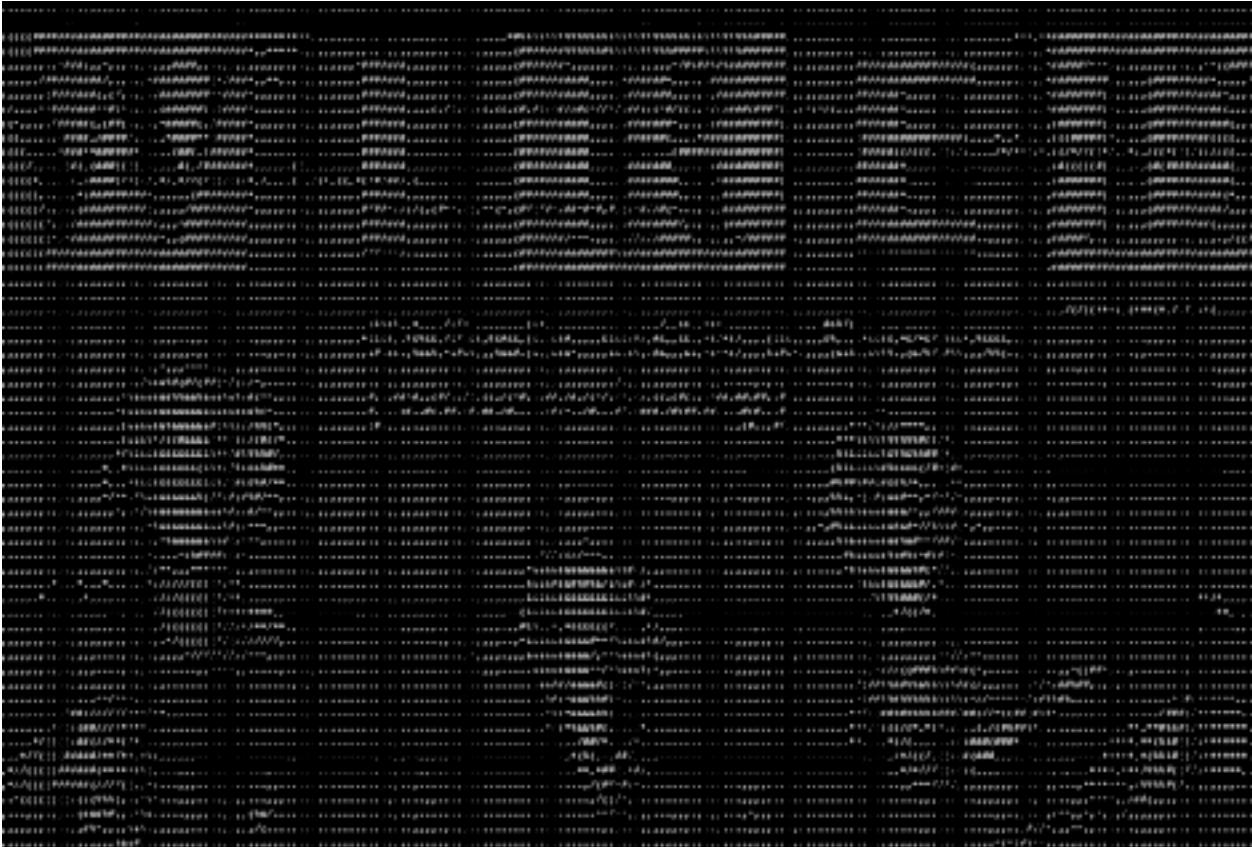
First they came for **Monero**,
and I did not speak out – because I was not a Monero person.

Then they came for **Tornado cash**,
and I did not speak out – because I was not using Tornado cash.

Then they came for **NYM**,
and I did not speak out – because I was not using mixnets.

Then they came for me — and there was no one left to speak for me.





END NOTES

Let's organize!



web3
privacy
now

Mykola
Siusko, 2023

Contribute
Connect

 [Web3privacy now](#)
 [@nicksvyaznoy](#)