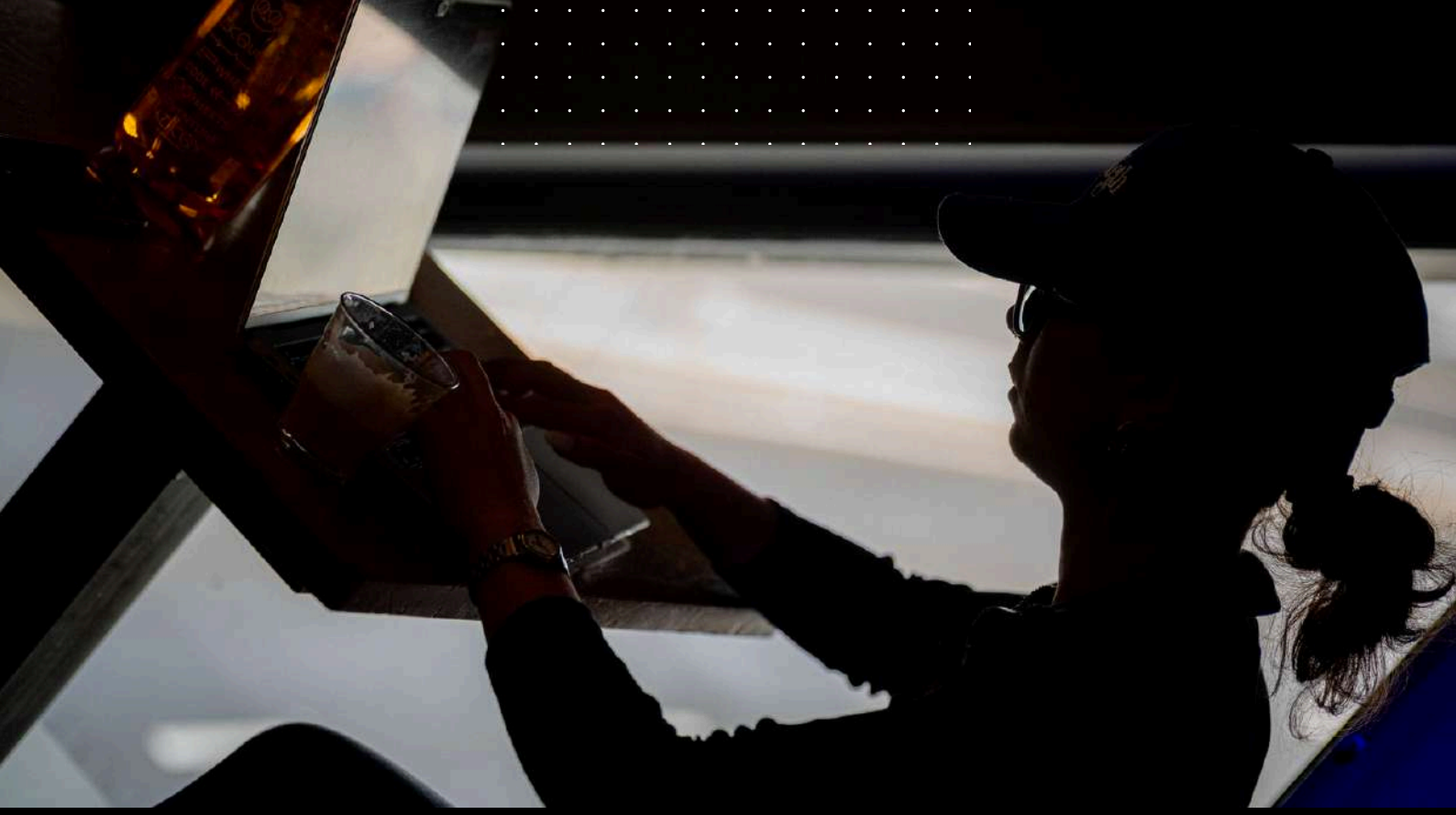


PRIVACY IS NORMAL

An overview of ETHDam 2024
A platform for Privacy and Freedom

TABLE OF CONTENTS

Introduction 2

ETHDam 2024 Overview 3

Normalize Privacy: Why we Organise ETHDam 6

Privacy at core 9

Challenging the best privacy solutions 11

Biggest Takeaways from ETHDam 12

- We need more liquidity, but where? 13
- Too much friction 15
- Regulators aren't playing nice 17

Tips on How to Be More Secure and Private 21

- Get audited 21
- Use existing tools for privacy, security and crypto 23
- Build better tools 24

Hackathon and Quadratic Funding 27

- Best Privacy 27
- Best Security 27

Looking Forward 31

Voices of ETHDam 36

Partners of ETHDam 39

INTRODUCTION

Buying crypto is a political statement.

This was our original tagline when I founded CryptoCanal in 2019. What started as Crypto 101 classes and monthly meetups has quickly evolved into an annual conference highlighting privacy and security, and the importance of financial sovereignty.

There are numerous conferences and events around crypto and financial freedom, but few that focus so heavily on privacy.

We cannot shy away from hard conversations. It is morally responsible that we challenge ideas and technologies that promise us said freedom. In an industry rife with scams and misinformation, it is imperative that we question the intent and incentives of everyone building a better future.

The message remains....

WE ARE NOT AFRAID TO BE POLITICAL.

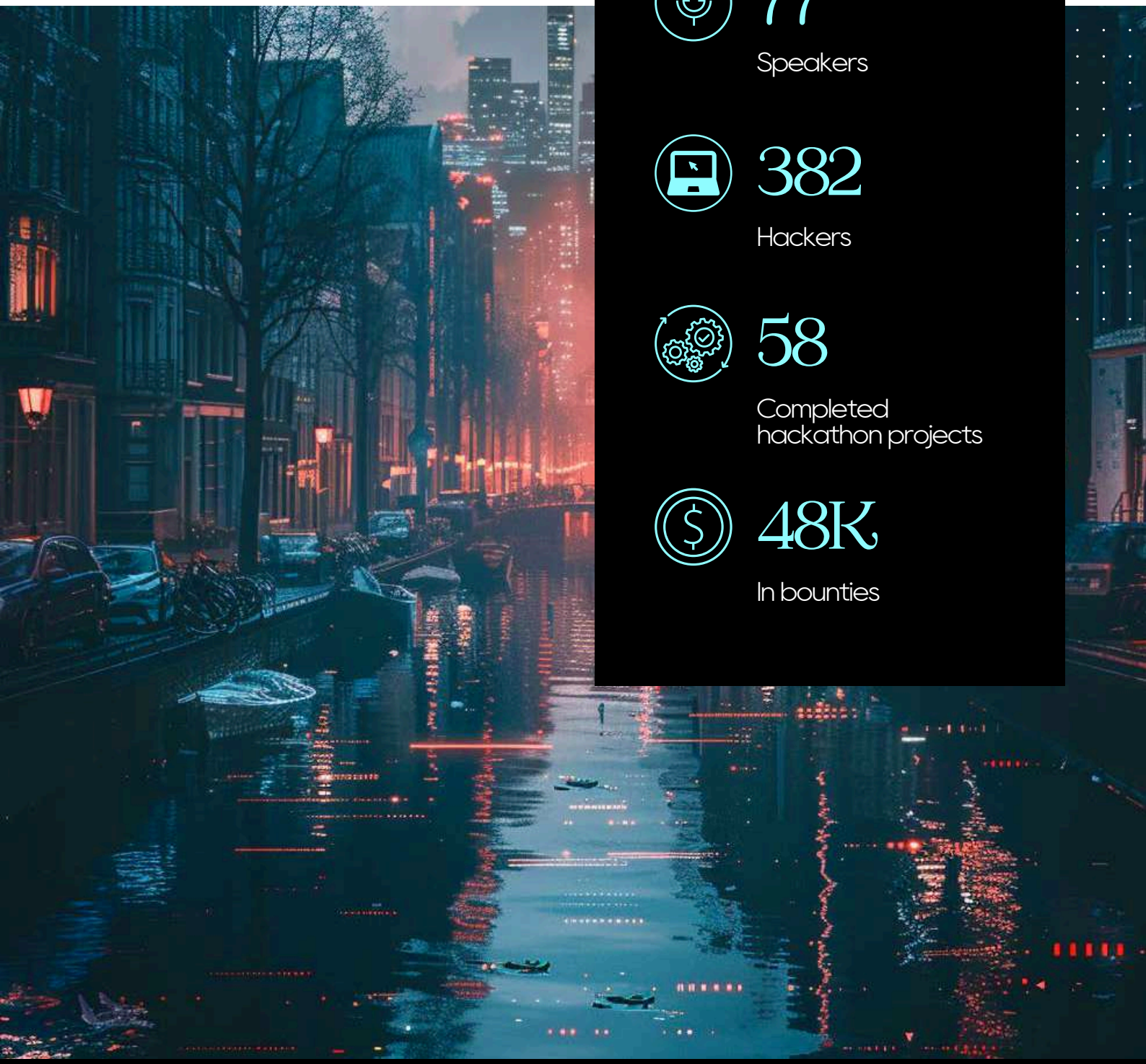
ETHDAM 2024 OVERVIEW

77
Speakers

382
Hackers

58
Completed hackathon projects

48K
In bounties



ETHDam

A PLATFORM FOR PRIVACY AND FREEDOM

"The important aspect of whatever fits the name 'privacy' is that it empowers individuals to operate with enhanced autonomy, and yet be able to influence the direction of society."

DAVID CHAUM, FOUNDER OF XX NETWORK


CULTUREEL
CENTRUM
ZAALVERH
CAFÉ
RESTAU
TornadoCash


web3privacy
now


NEW!
NEW!

NORMALIZE PRIVACY: WHY WE ORGANIZE ETHDAM

After Alexey Pertsev was arrested in August 2022 and held without charges for 260 days, it became clear that financial sovereignty wasn't the only technology under attack—governments have made a clear statement that privacy is not a right, and developers will be held responsible for how people use their solutions.

Yet crypto is the only industry where that seems to apply. Gun manufacturers are not arrested for how criminals use their products. Bank CEOs and their IT departments are not tried and convicted for the money laundering their customers commit. Governments rarely punish companies for mishandling private data, but will revoke a citizen's passport for exposing unethical surveillance practices.

At ETHDam, we want to counter the chilling effect the Dutch court ruling has created in the Netherlands. We want to encourage people to make privacy-conscious choices, and to understand the threats to a world without it. We want to educate builders and non-builders alike about how to build better systems. We also want lawyers and regulators to be part of the conversation so that they can better understand what is being built and why.

It may seem counterintuitive to work with legislative bodies and actors in order to be compliant with their privacy regulation (after all, what are we building these tools for, if not to protect ourselves from government overreach?).

However, we recognize that implementation matters.

We invite visionaries to come share their stories and visions, and to debate the future of privacy and organization. We also host builders, lawyers and regulation specialists to shed light on the reality of building privacy tools.

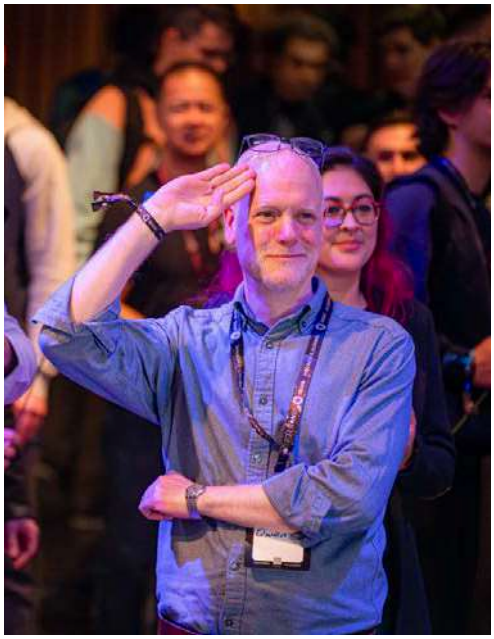
We believe that conversations among all involved parties are necessary in order to build not just the best, but also the most resilient privacy tools.

We put a lot of thought into who is on stage, who our partners are, and what technology is featured. We need dreamers and builders to work together to achieve the privacy-first future we want. What happens at ETHDam furthers the privacy space, and will hopefully lead to a better system than the legacy financial system we have now.

PRIVACY IS IMPORTANT EVERYWHERE

"We stand on the precipice of a declining US global power and we're seeing the rise of a multi-polar world. We need to stop thinking of the regulation and compliance and we have to look to our own future and chart our own path...Privacy allows us to expand the territory of freedom."

AMIR TAAKI, DEVELOPER FOR DARKFI




Hacker Speed Dating
Facilitated by:
ZAMA
zkSync
OASIS

PRIVACY AT CORE

It is only natural that CryptoCanal, a Dutch entity, hosts this privacy conference in our home town of Amsterdam, though we recognize the privilege of holding this conference in a stable democracy.

We live in a land where people trust the green checkmarks next to their Tikkie transactions and bank transfers. A place where modern people cannot begin to fathom being locked out of their bank accounts. However, barely a century ago, this same country required thousands of Jewish people to register themselves, only to be deported to their deaths.

We sit in the cozy comfort of Pakhuis de Zwijger having lofty conversations about protecting ourselves from government oversight and transacting without fear. But for some attendees, this fear is a reality.

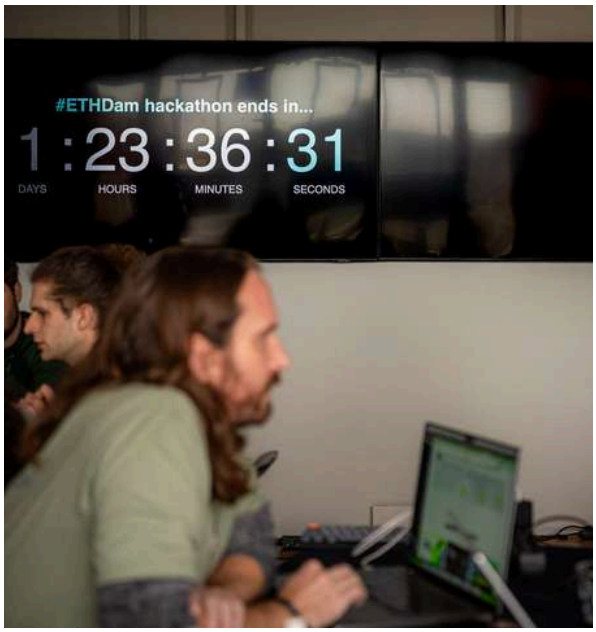
We must take action to defend everyone's right to privacy everywhere, Because when the threat does become tangible, it will likely be too late to take meaningful action.

"The Nazis in World War II were thrilled to discover how great the Dutch KYC was because it helped them figure out where all the Jews were. And that's why the Netherlands had the highest rate of Jews massacred out of any of the other European countries."

AMEEN SOLEIMANI, ADVISOR OF 0XBOW


OH NO... WHAT I DONE?!


NO PHOTO
PRIVACY IS NORMAL


#ETHDam hackathon ends in...
1 DAYS
23 HOURS
36 MINUTES
31 SECONDS

CHALLENGING THE BEST PRIVACY SOLUTIONS

ETHDam is a particularly niche conference in the greater Ethereum space because we are specifically focused on privacy and security, from panel discussions to hackathon bounties. We also invite non-EVM projects and chains in order to foster diverse discussions around best privacy and security practices. Next year, we anticipate hosting more conversations about the inevitable role of AI.

Blockchain has been celebrated as a transparent ledger, ideally deterring corruption and bad actors. However, its transparency has also made potential crypto adopters wary of broadcasting their activity. Despite this, bad actors have still successfully committed crimes with blockchain tools, much to the detriment of crypto's adoption.

As Railgun DAO Contributor Kieran Mesquita stated during the Lunarpunk vs. Solarpunk panel: "You can't assume that no one will ever try to attack or exploit your tech, let alone use it for bad causes. They need to be resilient to attack." Luckily, numerous builders in the space—including many of our partners—are working on usable, scalable privacy solutions.

ETHDam lead sponsor Oasis and partner Secret network implement trusted execution environments (TEEs), whereby the data, code or both is isolated in an enclave within a hardware system.

In contrast, ETHDam hackathon partner Zama implements fully homomorphic encryption (FHE), which allows blockchains to perform operations with encrypted data without giving third parties access to the data. Multiple can encrypt, and multiple can compute on it, and multiple people can decrypt.

Zero knowledge (ZK) proofs are another popular method of preserving privacy, implemented by ETHDam partners Firn Protocol and Panther Protocol. ZK encrypts transactions using elliptical-curve based cryptography.

Each method has its own trade-offs. For example, FHE is costly in terms of time and resources. TEE systems have been vulnerable to attacks in the past. ZK isn't suitable for multi-party communication and transactions.

Some partners such as Privacy and Scaling Explorations are using a combination of the technologies to train programmers interested in privacy technology.

As these methods are continuously put to the test, we look forward to seeing how they each evolve and overlap to ultimately make a secure, private toolkit for everyday living.

BIGGEST TAKEAWAYS FROM ETHDAM

For most people in attendance, it is agreed that crypto will play a role in preserving said sovereignty. However, the obstacles identified and solutions proposed to normalizing privacy and crypto varied among speakers.

"At some point this stuff needs to make the human race better off or it is fucking pointless."

JOEL VALENZUELA, BUSINESS DEVELOPMENT AND MARKETING AT DASH

TAKEAWAY #1

WE NEED MORE LIQUIDITY...BUT WHERE?

Adoption, usage and activity are key for any blockchain to succeed. For privacy-focused technology, it's imperative. Without liquidity, transactions are practically just as identifiable as transactions on Ethereum or Bitcoin.

But which chains are most likely to attract more users (and thus more liquidity): privacy-centered L1s or L2s?

Privacy-centered L1s exist, but there simply isn't enough liquidity. ZCash, for example, has tried, but because there's not enough activity, "99% of transactions could be traceable," cited Paul Puey, founder of Edge. As he pointed out in his talk "Driving Adoption of Privacy", when comparing stronger privacy tech (ZCash) to greater adoption (Monero), the crypto with greater adoption proved to preserve privacy better.

"The weaker technology but with a very high level of adoption actually equated to a higher level of privacy. So adoption is key in that sense, not just because we want people using it, but for the people that care about privacy, getting more people adopted into our pool helps give [us privacy] as well."

PAUL PUEY, CEO AND CO-FOUNDER OF EDGE

So it seems that, while the technology itself plays a role in preserving privacy—at least in regards to transactions—liquidity and adoption are the true necessities to preserve privacy.

But will people choose L1s over L2s for the sake of privacy? If a non-privacy focused L1 has a significant amount of liquidity, wouldn't building a privacy-focused L2 be an optimal choice?

In both "Current State and Future of Second Layer Networks" and "Ethereum Is Dying without L1 Scaling", speakers argued that L2s are not just a horrible user experience, but that they prevent L1s like Ethereum from scaling. During the "Monolithic vs. Modular Scaling" debate, Cyber Capital Founder Justin Bons said, "I don't actually consider Abritrum users to be Ethereum users. I think they're Arbitrum users. And in that case, a lot of these Layer 2 ecosystems are competing with the Layer 1 over fees and over usage."

Having multiple L2s on a single L1 creates confusion, and ultimately may hurt retention in the long run. However, as valid as those critiques may be, no other blockchain has quite the transaction volume that Ethereum has (though Solana seems to be catching up as of Q2 2024).

Some speakers, including Toghrul Maharramov from Scroll and Victor Sizaret from Starkware, acknowledge that L2s are a work in progress, but they are still optimistic about their purpose in the crypto ecosystem.

It seems that privacy-focused L2s (though few and far between) on popular blockchains like Ethereum may at least be a first step anyone can take today towards more successful adoption of privacy tools and crypto.

"People are focusing on making their existing codebase mature enough and optimized. Once that's done, then we can have a more serious chat about privacy."

TOGHRUL MAHARRAMOV, ROLLUP SORCERER OF SCROLL

TAKEAWAY #2

TOO MUCH FRICTION

"You have to deliberately go out of your way to do all of this."

HARRY ROBERTS, TECHNICAL PRODUCT MANAGER OF OASIS NETWORK

Privacy tools simply can't compete today with legacy tools. Even for ETHDam 2024, we heavily relied on Google forms because of how easy and accessible they are for collaboration. We paid our vendors in fiat with business bank accounts because it was one less point of friction in planning a three-day conference.

Privacy is not by default, but it should be. During the "Securing Secrets: Inside the Privacy Infrastructural Realm" talk, Secret Network CEO Alex Zaidelson claimed that the lack of privacy is what prevents greater adoption of crypto: "To make privacy available and easy, we need to make blockchain available and easy." Nowadays, the most common crypto transactions are from retail consumers buying and selling relatively small amounts of crypto—transactions that most users don't care if they're public. It's even considered a flex to have blue chip NFTs linked to a publicly known address.

However, as institutional interest increases and people take larger positions, they want some degree of privacy in their transactions and holdings. And if we want to see regular usage with crypto increase with other common transactions such as payroll, banking, and gaming, privacy will be imperative for even the everyday crypto user.

But as of now, the majority of crypto holders or users have less than half of their net worth on the blockchain. It could be due to lack of privacy, or lack of faith in security.

According to DASH's Joel Valenzuela, however, privacy is not the primary deterrent—it's because no one wants to use the tools that currently exist. Many people are building tools and platforms that attract investment, but not necessarily add value or solve problems for today's users.

Furthermore, he identifies another problem: the unspoken rule of not competing with Bitcoin, and of not collaborating with each other. Everyone is so concerned with having enough users and daily transaction volume that they aren't willing to collaborate with other ecosystem builders in order to grow the whole market—not just their own.

In classic founder mentality, Harry Roberts of Oasis Network proclaimed "You don't have to overthink things—just build the damn thing."

As much as we appreciate a "most fast and build things" mindset, we've seen where that can lead.

"The demand is there. The users are there. It's on us to build stuff they want to use."

CAPTAIN, FOUNDER OF FIRN PROTOCOL

TAKEAWAY #3

REGULATORS AREN'T PLAYING FAIR (OR AT LEAST AREN'T BEING FRIENDLY)

"If you want to make the simplest private wallet ever, you don't need to record any history. If you add history, that's another feature you have to develop, and then you have to decide how you will sync the history, and do you have to KYC your users...it turns it from a really simple application into something that you're having existential, moral dilemmas about."

HARRY ROBERTS, TECHNICAL PRODUCT MANAGER OF OASIS NETWORK

Soon after Pertsev's hearing, hackers and founders reached out to CryptoCanal to ask about whether they were building the next Tornado Cash, or if they would be safe. While we appreciate that we are a trusted resource for our community, it's clear that privacy builders need to provide more clarity on what will and will not be considered such a threat.

If financial institutions such as HSBC are (repeatedly) found guilty of laundering money, the precedent is simply to receive a fine—no bank CEO, CFO, CTO, engineer, or board member has ever been convicted of money laundering.

But in light of Pertsev's conviction and Roman Storm's pending case in the U.S., it seems that regulators are not interested in working with us. As 0xbox Advisor Ameen Soleimani pointed out in his talk "The Fight for Privacy", Dutch prosecutors were essentially being willfully ignorant of how Tornado Cash works (e.g. couldn't implement KYC for anyone interacting with the blockchain).

As of now, builders simply have to build in the regulatory dark, and once regulators catch wind of it, they find a way to determine that the technology is not compliant. As a result of unclear (or non-existent) feedback from regulators, some builders in the privacy crypto space have turned to their compatriots to pinpoint what exactly makes tools like Tornado Cash noncompliant—and build something that fits those unstated regulations.

"Using Tornado Cash isn't even illegal in the Netherlands...the regulators in the Netherlands are actually the only entity who could limit the use of Tornado Cash (at least in this country), and they have not used their power to do so. They prefer instead to try and imprison Alexey for writing unstoppable code."

AMEEN SOLEIMANI, ADVISOR OF 0XBOW

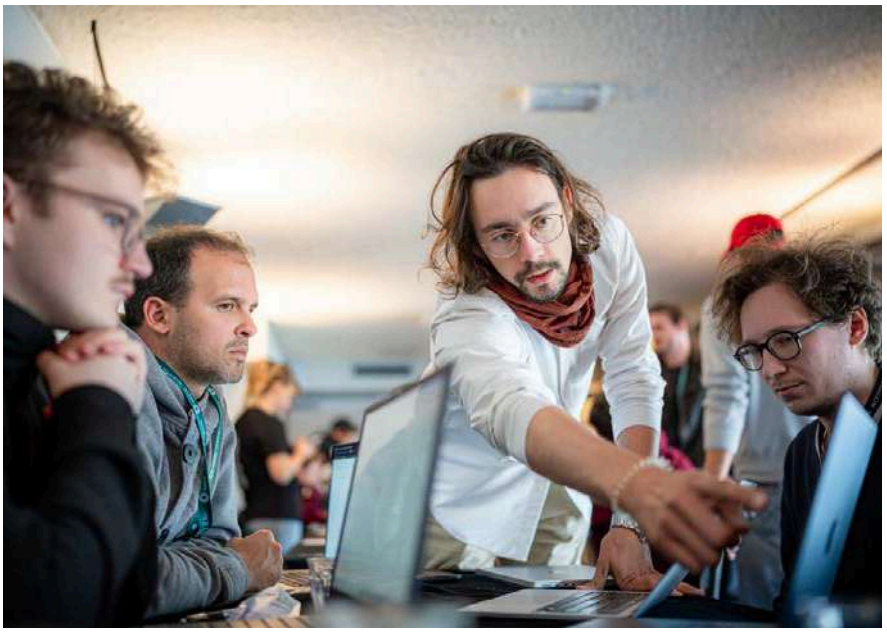
It's worth noting that legislation in the U.S. has a very clear impact on how much of the world approaches crypto (e.g. Pertsev was arrested by Dutch authorities just days after the U.S. sanctioned Tornado Cash).

So even if businesses—crypto or not—are in compliance with their own jurisdiction, U.S. regulation often has rippling effects. Many privacy and crypto enthusiasts look at Switzerland as an example of a state that respects privacy in the banking sector.

However, as Anoma legal advisor Fatemeh Fannizadeh explained through her own personal experience, Swiss banks will act in accordance with U.S. policies when it's in their best interests.

It remains to be seen whether and how regulators are willing to work with us, let alone try to understand what is being built.

> "Switzerland is literally colonized through its banks by the US. Why do private entities in Switzerland, far from the US, have to change their business models in order to comply with some future hypothetical risks? And then people who are legitimately in Switzerland—working and living there—why are they impacted by these potential future US politics?"
>
> **FATEMEH FANNIZADEH, LAWYER AND LEGAL AT ANOMA**



TIPS ON HOW TO BE MORE SECURE AND PRIVATE

We did not solve the question of privacy and adoption by any means. Many attendees and speakers, however, offered great tips and insights into how we can take meaningful action.

TIP #1: GET AUDITED

"The ambition is always to have very low risk in the code, but the risk is never zero."

OLIVER HOERR, FOUNDER OF HATS FINANCE

Third party audits have been a widely respected and accepted security measure. A fresh, diverse perspective on code can identify vulnerabilities that an in-house team may overlook.

From small independent auditors to crowd audits to white glove service auditors, there is a range of options to fit nearly any budget. Founder of Hats Finance Oliver Hoerr recommends getting multiple audits if possible. "No auditor should be so confident to say 'Do one audit with us and you'll be secure'" he advised during our Auditors & Bounty Hunters panel.

For anyone looking to have their product audited, the experience varies depending on what you need. Hats Finance, for example, gives recommendations on what to audit, and clients only pay for the vulnerabilities found by the community. As Trail of Bits Founder Josselin Feist explained, one of their engineers essentially shadows the dev team for a few weeks to thoroughly understand the codebase architecture and provide recommendations on all aspects of security, including aspects like integrations, testing, response plans and monitoring

APPROACHING AUDITS

There is no perfect, one-size-fits-all approach for auditing—but no auditor worth their weight will guarantee 100% security as a result of their work. "We can do an estimate on how much time we need, but there will be a lot of back and forth on the code that will give you more insight into what the next steps are," explains Feist. It can be especially difficult if the project approaches the auditor with a time crunch (e.g. a date to deploy).

It's also important to note that audits can only provide feedback on the code that exists at that moment. As the product continues to improve and evolve, that audit may no longer apply.

TIP #2: USE EXISTING TOOLS FOR PRIVACY, SECURITY AND CRYPTO

"The market decides what solutions get created and succeed. Who's the market? Is the market in this room? Yes! YOU are the market!"

JOEL VALENZUELA, BUSINESS DEVELOPMENT AND MARKETING AT DASH

For both individuals and companies, it's imperative to choose tools and software that prioritizes privacy as part of the service. As Puey pointed out during his talk, true privacy cannot be properly achieved without mass participation and adoption.

Luckily, he and others shared some of their favorite tools during the conference. Both Puey and Mesquita applauded Signal for private messaging. Mesquita also shared a number of privacy-focused tools in his talk The Boring Side of Privacy, from web browsers to email providers, business tools to note-taking apps. He even shared links to his tutorials on setting up a private DNS.

When it comes to private transactions, Puey highlighted Monero as one of the best options. Valenzuela also shared a number of tools for people to use for crypto payments (though not necessarily privacy-oriented). He explained how he lives entirely with crypto every day, including how he books travel, invoices clients, pays people and buys coffee.

All of these options are available to use now, and one of the best things we can do is to use them, break them, share them, and provide feedback so that not only these tools improve, but other people can start building what they may lack.

TIP #3: BUILD BETTER TOOLS

"We see this mental trap today when we look at the cypherpunk products that are on the market. They all have messaging like 'You don't want the state to spy on you!' and it's a very negative emotion that they're tapping into, and we end up responding to that. Cypherpunk is part of our legacy, but it's also a mixed legacy." –

AMIR TAAKI, DEVELOPER FOR DARKFI

In the grand scheme of things, most people may not consider privacy a noteworthy feature because they assume companies protect user information by default. And when they do see a product prominently advertising its privacy features, people assume it's a product for bad actors.

Many who attended ETHDam believe that privacy needs to be default in any product. Puey suggested that it needs to be hidden: "Hide privacy from the users. Don't make them go through any extra effort to get it. Otherwise you'll only get the illicit actors and the people who care."

Oftentimes, however, privacy comes into conflict with regulation (according to regulators, at least). Soleimani and his colleagues identified the "freedom of dissociation" as a key factor for people to keep themselves compliant. With their new project privacytools.com, users can publicly dissociate from a pool of funds while keeping their transactions private. In other words, users can prove their transactions are not criminal without disclosing with whom or for what amount they are transacting.

While many in attendance wanted privacy-oriented tools in all aspects of life, not all solutions are equally robust or functional. As Firn Protocol's Founder Captain McAteer shared during the "Frontiers in Privacy and Usability" panel, it may be worth perfecting privacy in crypto payments before addressing privacy in other areas of our lives: "Payment is just one use case for privacy, though it is possibly the biggest. We should start small (with payments) and do it really well. I want to build something that's a joy to use and will convert users, and I think payments is a perfectly good place to start."

Although we did not find any perfect solutions for building the next best privacy and security tools, the building spirit was alive and well throughout the conference, as evident during the ETHDam Hackathon.

HACKATHON AND QUADRATIC FUNDING

FOR PRIVACY AND SECURITY PROJECTS

After grinding away for 48 hours, the ETHDam Hackathon had a total of 58 projects submitted, all of which addressed varying challenges regarding privacy and security. Although there were fewer bounties offered compared to 2023, mentor Daniel de Witte noticed there were more hackers participating than the previous year—proving that bounties may not be the only factor attracting talent.

Hackathon partners offered bounties for their own challenges, and of the top 10 projects chosen by the ETHDam judges:

BEST PRIVACY

Best Privacy went to ZK Loyalty, a GDPR compliant, anonymous loyalty program that any small business can implement to reward repeat customers.

BEST SECURITY

Best Security went to OASISGUARD, an onchain password manager using hardware-level security with passkeys (Webauthn).

But the awards didn't stop there. Two days after the conference, we launched the ETHDam Quadratic Funding round. When hackathons are a separate part of an event, attendees don't always have the chance to see and appreciate all the hard work that hackers put into their projects.

Conference attendees received ETHDAM tokens to contribute to any of the registered projects. Over the course of 10 days, attendees contributed as many of their allotted tokens to as many projects as they wanted.

We choose to implement a QF round because the final amount of funds distributed to each project is based on the number of votes they receive, rather than the weight of each vote.

For example, 5 people might vote for Project A and contribute 2 ETH each, whereas 45 people might vote for Project B and contribute 0.1 ETH each. Project B may have received the majority of the votes, but Project A received more funding. If these projects had participated in a QF voting round, Project B would have received more funding because it received more votes.

We also used Minimum Anti-Collusion Infrastructure (MACI) to deter bribery or coercion. One of the wonderful yet fatal features of blockchain is that activity is public. With MACI, participation in a vote and correct vote tabulation are publicly verifiable, but specific voting information is not public. As a result, bad actors cannot confirm whether bribery efforts can work.

We did, however, encounter some issues during the voting process.

In short, the zk-SNARK circuit failed to generate a proof because of an error in the code. A single invalid message had been submitted, which meant the QF round was unable to finalize. Luckily, that message was an honest error and not a malicious vote or attack.

The ETHDam hackathon team worked closely with clr.fund to identify the problem, as well as come up with an appropriate solution. To resolve the issue without requiring every voter to re-submit their votes, clr.fund wrote a script that resubmitted the votes to new contracts (less the single invalid message). When we shared this information with the hackers, it was met with patience and understanding.

After all, what's a hackathon without a few bugs along the way?

The clr.fund team explains the issue in more detail on their website. As challenging as this process was, we also accept that mistakes happen with new technologies. Without people testing them, we can't improve them.


OtterTrack Finalists
1. Paygrid
2. Armitage
3. DeFiPy
4. Bermuda Pay
5. Slider
6. Fluidpay
7. Fidesium
8. LottoPGF
Got questions? -> slido.com -> #ETHDam


BEST SECURITY


Best Privacy
ZK Loyalty


OASISGUARD
Onchain Password Manager , Hardware-Level
Security with Passkeys (Webauthn)


OASIS
near
TRAIL OF BITS
privacy + scaling explorations
Waku
dRPC
THRESHOLD
AVALANCHE
LIDO
PANTHER
0xbow
FIRN
MAVEN11
CHAINSECURITY
CYBER CAPITAL
diva
secret
zkSync
Beefy
OBSCURA
ZAMA
bitvavo
ecosystem support program

LOOKING FORWARD

One topic the conference did not touch on was artificial intelligence, though it did find its way into many conversations off stage. As AI continues to captivate users and investors worldwide, attendees asked each other: what role will AI play in privacy?

According to xx network Founder David Chaum, AI has the potential to make crypto easier to use. It certainly helped hackers build their projects during the hackathon, which helped everyone deliver incredible projects. There are also a number of AI-powered solutions available for investors and traders. By the time ETHDam 2025 kicks off, we plan to introduce an AI hackathon track.

The possibilities for better privacy and security are truly endless, though as Valenzuela pointed out, we need to build tools that people can and want to use today. ETHDam was a great space for builders to share ideas and debate technological integrity, and we hope to see those conversations lead to fruitful products between then and the next conference.

ETHDam

LOOKING FORWARD

"Instead of privacy being something that's aspirational, or an on-going battle we may not win, now it's transitioned because of artificial intelligence breakthroughs. There's now an opportunity to prevail in a competitive business environment with systems that have tremendous disruptive capabilities."

DAVID CHAUM, FOUNDER OF XX NETWORK

SEE YOU IN MAY 2025!

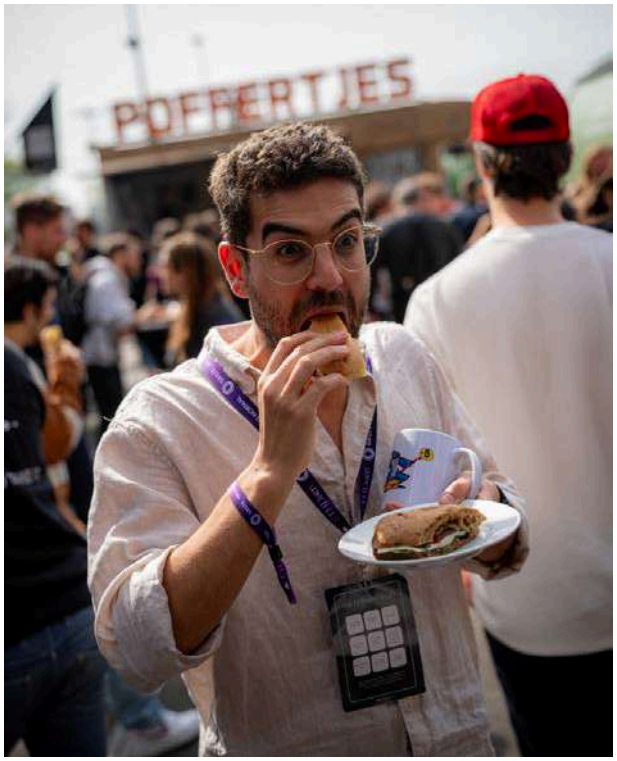
As an event curator, I want to platform the the harder conversations, that can be misconstrued or hard to have online.

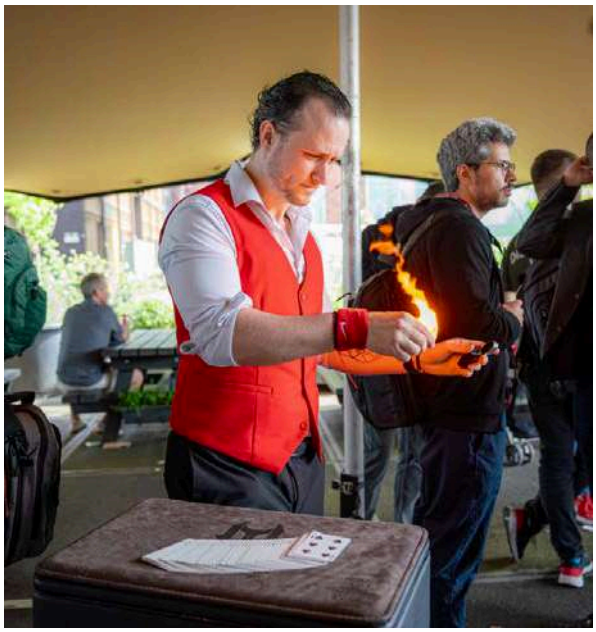
In the face of rising authoritarianism, more than ever, it is our duty, as hackers and builders to use and create resilient tools to enable true censorship resistance and privacy.

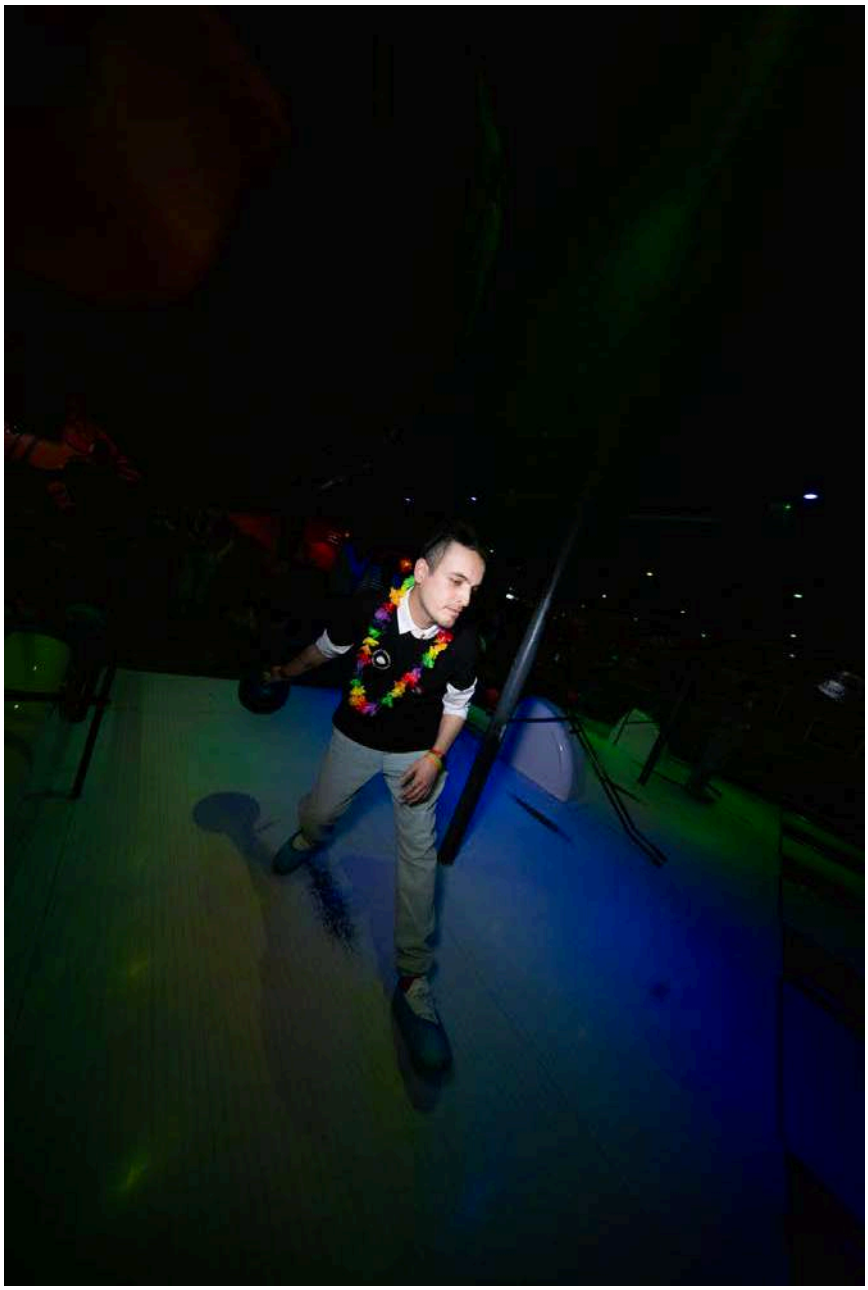
I will continue to uphold the cypherpunk values, dear to our ethos and I look forward to welcoming you in May 2025.

ELEONORE BLANC, CRYPTOCANAL FOUNDER

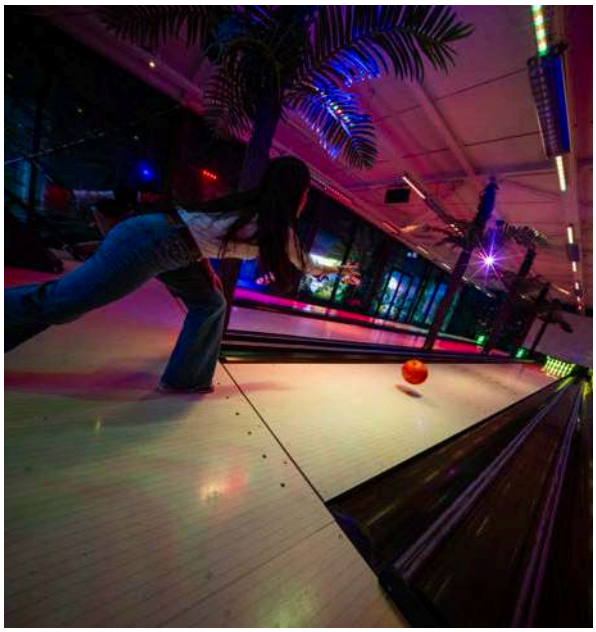

ETHDam
Dr. HAOYU HE
IEXEC
FRANCE
ETHDam
Joy ZHANG
French and chinese
Association
of Blockchain


POFFERTJES






ETHDam
AfterParty
with Bitvavo



VOICES OF ETHDAM

Welcome to ETHDam
Eleonore Blanc – CryptoCanal

Frontiers in Privacy and Usability
Harry Roberts – Oasis, Captain McAteer – Firn, Mihai Scarlat – Ocean

The Fight for Privacy
Ameen Soleimani – OxBow, Privacy Pools

Privacy: Past, Present and the Post Quantum World
Dr. David Chaum – xx network

Securing Secrets: Inside the Privacy Infrastructural Realm
Guru T – Waku , Alex Zaidelson – Secret Network, Haischel Dabian – Obscura, Oliver Gale – Panther Protocol

Confidential EVM: next-generation contracts
Harry Roberts – Oasis

The Boring side of Privacy
Kieran Mesquita – Railgun

Ethereum Foundation, the Privacy Scaling Exploration
Vivian Plasencia – PSE, Bandada, Tyler AtHeartEngineer – MACI, Sam Privacy Scaling Exploration, Ethereum Foundation | MACI Team Lead

Lunarpunk VS Solarpunk
serinko – Nym, LunarDao, Kieran Mesquita – Railgun, Ameen Soleimani – OxBow, Privacy Pools

How to build on a confidential EVM
Matevz Jekovec – Oasis

Why We're Not Using Crypto, and How to Fix It
Joel Valenzuela – Dash

Slither: introduction to custom analysis
Josselin Feist – Trail of Bits

Privacy preserving web3 communications at scale with Waku
Guru T – Waku

Send secure cross-chain transactions with NEAR
Owen – NEAR

Web3's Day-One-Decentralized Access
James – Threshold

Bandada: Managing Privacy-Preserving Groups
Vivian Plasencia – Privacy Scaling Exploration, Bandada

Own your data with TLSNotary
Hendrik Eeckhaut – Privacy Scaling Exploration, TLSNotary

Private on-chain voting: technical Introduction to MACI
Sam Richards – Privacy Scaling Exploration, MACI

Reentrancy in Cancun hardfork: the curious case of EIP1153 (transient storage)
Matthias Egli – ChainSecurity

Deciphering DAOs: Insights from Off-Chain Dynamics
David Truong – x23.ai

Hold the gate a little: designing the reliable dynamic timelock with Dual Governance
Kadmil – Lido

VOICES OF ETHDAM

Auditors & Bounty Hunters: who should secure your bags?
Oliver Horr – hats.finance, Goncalo Magalhaes – Immunefi, Erik Arfvidson Euler Finance, Josselin Feist – Trail of Bits & Matthias Egli – ChainSecurity

Staking, DVT and node operators: who will run Ethereum tomorrow?
Raul Calvo -Diva, Glenn Brown -Kiln, Ben Thalman -Figment & Emily Raffo – ChainSecurity

Manifesto for a Dark Renaissance: Anonymity as Hard Offensive Power
Amir Taaki – DarkFi

Critical changes to privacy protocols for mass adaption
Paul Puey – Edge Wallet

In Crypto we don't trust: how protocols approach security
Jack Sanford – Sherlock, CvH – Polygon, Kadmil – Lido

Aggregating DeFi: yield, ponzinomics, and building lasting value
Weso – Beefy, Anton Bukov – 1inch.io, Frank Brinkkemper – Summer.fi

Current State and Future of Second-Layer Networks
Victor Sizaret-Starkware, Toghrul Maharramov-Scroll, Emil Luta-ZKSync

DeFi Value Flows
Anton Bukov – 1inch.io

Ilium: Zero Knowledge Blockchain
Chris Pacia – illium

The future of Wallets
Paul Puey – Edge, Sami Waittinen – Trust, Emile Dubie – xDEFi

Cypherpunks unite
Joel Valenzuela – Dash, Kieran Mesquita – Railgun, Amir Taaki – DarkFi

Leveraging MPC to securely transact on all chains
Owen – NEAR

The future of web3 data layer is centralized?
Viacheslav Shebanov – dRPC

Ethereum is dying without L1 scaling
Justin Bons – Cyber Capital

Don't design a DVT protocol with a blockchain mindset
Jorge Cuartero – Diva Staking

Zama's fhEVM: Enabling Blockchain Privacy
Tore Frederiksen – Zama.ai

Novel application design space at the intersection of TEE&DeFi
Orest Tarasiuk – zkWarsaw

Network Privacy Matters
serinko – Nym, LunarDao

Privacy by Design: secure leaderboards with zk proofs on Aleo
Ramiro Ramirez – Obscura

Social media protocols
limone.eth – urbe.eth | ETHRome

VOICES OF ETHDAM

Unleashing the Power of the Internet: From Genesis to the Battle for Data Sovereignty with Nym VPN
Ade Molajo – Nym

Effective Product Security: Lessons from bug bounties and audits
CvH – Polygon

How does Starknet scale Ethereum
Victor Sizaret – Starkware

Alpha protection through privacy-web3 privacy primitive for DeFi
Oliver Gale – Panther Protocol

Unlimit your tech with Account Abstraction
Andrii Bondar – ZKSync

Relational Governance for the Lunarpunk Ethos
Sterlin Lujan – Logos

Hold the gate a little: designing the reliable dynamic timelock with Dual Governance
Kadmil – Lido

Ask a Lawyer! Web3 Privacy Workshop
Oliver Smith – GOV.DAO

Activating 100M people in privacy
Mykola Siusko – Web3PrivacyNow

The Future of zk-VM: Pioneering Optimization Techniques and Challenges
Ventali Tan

Enabling Privacy and Compliance with specialized Blockchains in the Avalanche Network
Martin Eckardt – Avalanche Labs

Zero Knowledge Proof of Reserves
Hodlon – Privacy Scaling Exploration

Rethinking Public Goods
Vee – Privacy Scaling Exploration

Ignorance is bliss – compliance vs privacy
Fatemeh Fannizadeh – Anoma

Crypto Scams, keeping people safe & alpha with onchain data!
Remy – Bitvavo, Frank – Whale Alert, Marina Khaustova – Crystal

See (no) evil: privacy and compliance on-chain
Philip Gradwell – Chainalysis

Fostering innovation amidst regulatory hurdles
Alexander Werkheim – Cyber Capital, Philip Gradwell – Chainalysis, Elke Karskens – Coinbase

Funding the Future through Founders
Aron van Ammers – Outlier Ventures, Pim – Maven11, Rene Darmos – Moonhill Capital

Monolithic Vs Modular scaling Debate
Justin Bons – Cyber Capital vs Toghrul Maharramov – Scroll

Security: from idea to $10m TVL
Evert Kors – Sherlock

THANK YOU


OASIS


near


TRAIL OF BITS


diva


CHAINSECURITY


FIRN


Waku


0xbow


THRESHOLD


AVALANCHE


LIDO


dRPC


CYBER CAPITAL


PRIVACY + SCALING
EXPLORATIONS


Beefy


OBSCURA


PANTHER


MAVEN11


secret


bitvavo


ecosystem
support
program

THANK YOU FOR YOUR ATTENTION.

ETHDam

A PLATFORM FOR PRIVACY AND FREEDOM

WRITTEN BY

Sterling Schuyler
Added Value Agency

ETHDAM POWERED BY CRYPTOCANAL