Program

Protocol BERG v2

The decentralized protocol and infrastructure conference.
June 12-13, 2025, Berlin

A Department of Decentralization event.

Abstract

Protocol Berg v2 is a conference focusing on protocol research, decentralized infrastructure, and core-developer experience. The two-day event with multiple stages, opportunities for technical workshops, and protocol community gatherings brings together protocol researchers and other stakeholders from different decentralized protocols.

This program outlines the content and speakers of the 89 sessions of the second Protocol Berg, held on June 12-13, 2025, in Prenzl'berg, Berlin. For this edition of the event, sessions are distributed over three stages and a workshop room.

The program is ordered chronologically and grouped by conference days.

Contents

1 Day 1

12. June 2025

1.1 François Garillot – Modern Multi-proposer consensus implementations

12.06.25 10:30 CEST
Workshop - Cinema 9
Consensus

Multi-proposer consensus protocols let multiple validators propose blocks in parallel, breaking the single-leader throughput bottleneck of classic designs. Yet the modern multi-proposer consensus implementation has grown a lot since HotStuff. THisworkshop will explore the implementation details of recent advances – DAG-based approaches like Narwhal and Sui's Mysticeti – and reveal how implementation details translate to real-world performance gains. We focus on the nitty-gritty: how network communication patterns and data handling affect throughput and latency. New techniques such as Turbine-like block propagation (inspired by Solana's erasure-coded broadcast) and lazy push gossip broadcasting dramatically cut communication overhead. These optimizations aren't just theoretical – they enable modern blockchains to process over 100,000 transactions per second with finality in mere milliseconds redefining what is possible in decentralized systems.

1.2 Georgy – Blockchain Ethics: Pure Reason or Pure Madness?

12.06.25 10:30 CEST
Side Stage - Cinema 7
Philosophy

This a work in progress attempting to answer seemingly simple and not very contradictory question. "Why can we not have ethics of blockchain applications?" We seem to have a burgeoning field of AI ethics, and even with a reasonable criticism against it, AI ethics does flourish both in industry and as research in academia. Contrast it with blockchain ethics which is hardly a mature subfield, but more of a painful (and emotional) topic. Are there good reasons to care about it? This is an empirical, philosophical, and normative question. And I argue that on all these accounts we have good reasons to care. First, I argue against radically skeptical position that blockchain ethics are impossible (even though it may seem like that). Then I explain how blockchain ethics is a distinctive area of enquiry that warrants distinctively different methodologies (so simply copying AI ethics not going to work). Finally, I identify key obstacles to blockchain ethics, namely: lack of consensus on conceptual frameworks, information asymmetries, and crowding out of morals.

1.3 Diogo Ribeiro – Designing Decentralized Storage: Without Better UX, Decentralization Remains an Underutilized Alternative

12.06.25 10:30 CEST
Main Stage - Cinema 10
Storage

Decentralized storage promises data permanence, censorship resistance, and trustless access—but poor UX is holding it back. While protocols like IPFS, Arweave, and Filecoin provide the technical backbone for decentralized file storage, users and developers struggle with complex retrieval, unclear incentives, and unreliable access.

1.4 Frederik Luehrs – Runtime Assertions: A New Paradigm for Customized Smart Contract Security

12.06.25 10:30 CEST
Side Stage - Cinema 6
Infrastructure

We propose a novel approach to blockchain security through concurrent runtime assertions - a modified EVM that enables real-time customized transaction validation alongside execution. By introducing an extended runtime environment applied to the current network's state, this system allows developers to define invariants about their protocols. These invariants are continuously verified, running in parallel to transaction execution, enabling immediate detection and prevention of security violations. Allowing for embedded security is a paradigm shift which fundamentally changes the way we approach blockchain safety, while maintaining transaction throughput through parallel validation.

1.5 Alexander Herrmann – Synchronized Priority Auctions

12.06.25 10:45 CEST
Side Stage - Cinema 6
Infrastructure

This talk will present a new paper of a novel 'Synchronized Priority Auctions' (SPA) framework designed to increase the efficiency of priority auctions by allowing multiple auc- tions to settle simultaneously in a single transaction. Building on the "Priority is All You Need" concept, our three-round mechanism (baseline bids, multi--app bids, and fallback execution) enables different applications—such as UniswapX and AMMs—to synchronize their priority auctions and eliminate the trading risks associated with sequential transactions. As a result, this new framework is ex- pected to enhance a variety of trading activities that rely on priority auctions, including improving MEV capture for liquidity providers, optimizing trade exe- cution for trading intents, and enabling more efficient liquidations.

1.6 Mf – the new Cypherpunk generation

12.06.25 11:00 CEST
Side Stage - Cinema 7
Philosophy

What's being a cypherpunk in the 2020s? Is our old manifesto from the early 1990s still relevant 30 years later? Our socio-economic environment has changed; where before computers were for a select few, we have now embraced digitalisation on masse.

How can you play a part in today's environment? A talk for builders, not limited to coders.

1.7 Shawn Tabrizi – PolkaVM: A fast and secure RISC-V based virtual machine

12.06.25 11:00 CEST
Side Stage - Cinema 6
Infrastructure

PolkaVM is a new general purpose user-level RISC-V based virtual machine, with modern features and functionality.

1.8 VIKTOR TRON – Non-local redundancy: Erasure coding and dispersed replicas for robust retrieval in the Swarm peer-to-peer network

12.06.25 11:00 CEST
Main Stage - Cinema 10
Storage

In this presentation, we describe in detail how non-local redundancy is implemented in the Swarm peer-to-peer network. Among other things, we show how to apply classic Reed-Solomon erasure codes to files in Swarm, discuss security levels of data availability and derive their respective parameterisations, describe a construct that enables cross-neighbourhood redundancy for singleton chunks to complete erasure coding, and explore alternative retrieval strategies applicable to erasure-coded files and their impact on latency as well as price of retrieval.

1.9 Thomas Pani – 25-Minute Solidity Fuzzer: Fuzzing Smarter, Not Harder

12.06.25 11:15 CEST
Workshop - Cinema 9
Cryptography

Fuzzing and Formal Methods are often seen as competing approaches to smart contract security. In this **hands-on workshop**, we combine insights from both, allowing participants to build a **minimal EVM/Solidity smart contract fuzzer in Python within 25 minutes**. We also explore critical questions such as:

- **How can we measure the success** of our fuzzing campaign?
- Is **the number of runs** a reliable coverage metric?
- **What alternative metrics** could provide deeper insights?
- Why is naive input generation insufficient for smart contracts?
- How can we **improve input generation** to achieve better coverage?

Participants will gain practical experience building a fuzzer while learning key concepts in **smart contract fuzzing**, guided by a **Formal Methods-informed approach**.

1.10 Lisa Akselrod – Anatomy of on-chain privacy

12.06.25 11:30 CEST
Main Stage - Cinema 10
Cryptography

How private blockchain differs from transparent blockchain: core components: - Blended private and public state - Client-side proof generation - zero-knowledge property (not just a snark) - Anatomy of a private smart contract - Private composability

What does it all mean for developers? What is the right mental model to approach building private dapps?

1.11 Andreas Erwig, Luis Bezzenberger, Marc Harvey-Hill – The Holy Trinity of Censorship Resistance in Ethereum

12.06.25 11:30 CEST
Side Stage - Cinema 7
Philosophy

Censorship resistance and decentralization have long been core principles of public blockchains, yet Ethereum faces increasing threats from real-time transaction censorship, particularly impacting DeFi users. The current Proposer-Builder Separation (PBS) supply chain has led to severe centralization, with two builders controlling over 80% of blocks and half of all relays censoring transactions. A promising approach to address this is the "Holy Trinity of Censorship Resistance", a combination of enshrined PBS (ePBS), FOCIL (Fork-Choice enforced Inclusion Lists), and encrypted mempools. This approach can even be extended by using Smart Accounts which give users more control over the transaction inclusion process. While this proposal has the potential to restore Ethereum's fairness and neutrality, challenges remain, particularly around the encrypted mempool design. Those challenges include designing a generalized encryption interface that supports multiple encryption mechanisms, ensuring that encrypted transactions remain decryptable despite changing encryption parameters, and guaranteeing a timely decryption of transactions.

In this talk we will discuss how these 3 pillars can work together and how they can be extended by Smart Accounts. Additionally, we will show a (Gnosis Chain) mainnet demo of the encrypted mempool in action from an end user perspective.

1.12 Konrad Urban – When Help Hurts: Why a Friendly Government is a Threat to Crypto

12.06.25 12:00 CEST
Side Stage - Cinema 7
Philosophy

A "friendly" government may seem beneficial for crypto, but it ultimately threatens decentralization. Just as the open internet was co-opted by corporations and regulators in the '90s and '00s, government-friendly crypto policies lead to surveillance and centralized control. While regulatory clarity invites mainstream adoption, it also empowers large players, marginalizing permissionless innovation. Crypto's strength lies in its resistance to control—once governments integrate it into traditional finance, its revolutionary potential fades. A hostile government forces decentralization; a friendly one lulls us into compliance, repeating the internet's fate.

1.13 Axel Eckerbom – SVM Protocol Design

12.06.25 12:00 CEST
Side Stage - Cinema 6
Infrastructure

The SVM is a powerful engine that enables low-cost, high-speed, high-performance, and high-throughput capabilities through parallelism. A scaling-with-hardware strategy allows performance enhancements to be captured within a monolithic design. However, the key challenge is designing the protocol to ensure decentralization scales in tandem with performance.

1.14 Esad Yusuf Atik – How to Build Rollups on Bitcoin

12.06.25 12:30 CEST
Side Stage - Cinema 6
Infrastructure

Ethereum has a bunch of rollups as part of the scaling roadmap. What about... Bitcoin?

This talk will focus on the extreme challenges of using Bitcoin as the data availability layer, the properties of BitVM-based bridges, and various trade-offs. You will be surprised to see what is possible (and what is not).

1.15 Robert Habermeier – Scaling Blockchain with SSDs is Smart (and Scaling with RAM is Stupid)

12.06.25 12:30 CEST
Main Stage - Cinema 10
Storage

Blockchain nodes are primarily bottlenecked by their access to disk for account and smart contract data. Scaling with RAM is a shortcut. Scaling by effectively utilizing Solid State Drives (SSDs) is robust and cheap.

1.16 Teresa Carballo, Zimt – Not your vote, not your lawyer: Delegation and the Legal Challenges

12.06.25 12:45 CEST
Workshop - Cinema 9
Philosophy

We will explore the dynamic intersection of delegation and DAOs, concepts driving the future of decentralized governance. Delegation enables more efficient decision-making and distribution of power within DAOs but comes with its risks and challenges both from the delegate and delegator sides.

We will dive into how delegation structures work in DAOs and the challenges they pose to traditional hierarchical models from a legal perspective, examining possible legal risks in governance delegation and how to mitigate them.

We'll look at real-world examples of successful DAOs and how they leverage delegation to foster innovation, transparency, and collaboration in the decentralized ecosystem, analyzing the particular role of delegates in these ecosystems, and legal measures taken by those ecosystems.

1.17 ERIN – Building Testnet Infrastructure (from the ground up)

12.06.25 13:00 CEST
Side Stage - Cinema 6
Infrastructure

When building scalable testnets which reflect real-world environments, there are many factors to take into account: ease of use for developers, performance, observability, maintenance, and cost. This workshop is meant to be an interactive session with a presentation for people to better understand how to build such systems starting "from scratch".

1.18 Fatemeh Fannizadeh – the economics of freedom

12.06.25 13:15 CEST
Side Stage - Cinema 6
Philosophy

Decentralisation is non negitiable. Is this a platitude or a controversial statement? Are you outraged to hear that crypto is meaningless if it is permissioned?

Well, worry not, there is no right or wrong answer, there is only disagreement. Censorship resistance, decentralisation, and permissionlessness have always been questionned. In this talk, you will hear about the economics of blockchain freedom, looking beyond the surface disagreements into what equilibriums they imply and command.

1.19 COSTANZA GALLO, ANN AND COSTANZA – Goodbye Cypherpunk values? Adapting to the new world order

12.06.25 13:30 CEST
Side Stage - Cinema 7
Philosophy

This talk would explore the original cypherpunk ethos from an Anthropological lens discuss how it can evolve to stay relevant by considering the evolving global scenarios: to remain relevant, cypherpunk principles must expand beyond technical resistance alone and engage with broader societal concerns from a social science lens. It will argue for reframing privacy and censorship resistance as essential to collective safety and freedom, and for cypherpunk values to break from web3 discourse and gain a central place in the broad mainstream discourse.

1.20 Christopher Goes – What would it really mean to build a world computer?

12.06.25 14:00 CEST
Main Stage - Cinema 10
Philosophy

The original vision of Ethereum was — at least nominally — to build a "world computer". Before debating whether Ethereum has succeeded or failed in doing so, or even whether the attempt itself is worthy, we must ask ourselves the question: what is a world computer, and what would it really mean to build one?

In this talk, I will approach this question from first principles: who is this world, what do they really want from a "world computer", and what kinds of logical unity ("one world computer') are both desirable and possible? Considered seriously, these questions imply substantially different design directions than those which the Ethereum ecosystem has taken, including a heterogeneous trust permissions system, a interoperability-first virtual machine, and a system architecture which understands itself as more of an operating system and less of a "blockchain". I will detail these directions, outline how they differ from the current technical Overton window, and conclude the talk by briefly sketching a possible path forwards for the Ethereum ecosystem.

1.21 Sergei Tikhomirov – Waku Service Marketplace: Decentralized Infrastructure for dApps

12.06.25 14:00 CEST
Side Stage - Cinema 7
Networking

Waku is a generalized peer-to-peer (P2P) communication protocol stack built on libp2p. It provides secure, decentralized messaging and is used by projects like Status, Railgun, and The Graph. An emerging idea is a Waku-based service marketplace, where developers can pay independent providers to deliver infrastructure services, such as querying historic messages, directly to their users off-chain. Using a marketplace instead of running their own nodes reduces complexity for dapp developers, avoids single points of failure, and improves decentralization. Additionally, users could interact with the marketplace directly, choosing providers without relying on the dApp developer. Marketplace consumers would maintain a reputation system to filter out providers with poor service. The marketplace concept is still in early stages. This talk presents the idea, outlines key challenges, and invites technical feedback.

1.22 Warren Winter – Mapping and Funding Our Dependencies in Open Knowledge

12.06.25 14:15 CEST
Side Stage - Cinema 7
Networking

Open knowledge has diverse forms — including open-source software, scientific research, and collaborative data commons — that are all built upon intricate webs of dependencies. As vividly demonstrated in cascading OSS failures caused by overlooked maintenance of dependencies (e.g., the npm left-pad incident), sustainable open knowledge production requires ongoing care and investment in its foundational contributions. This talk explores "knowledge dependency graphs" as a conceptual tool, generalizing from software dependency graphs, to better understand public goods coordination problems across diverse open knowledge domains. By examining how decentralized dependency funding protocols have met these challenges within software ecosystems, we explore their potential, and limitations, as part of an iterative approach toward sustainably supporting critical dependencies throughout the broader landscape of open knowledge.

1.23 Tino Breddin – Fast-track workshop: Running a HOPR node and using the GnosisVPN PoC

12.06.25 14:15 CEST
Workshop - Cinema 9
Cryptography

The GnosisVPN PoC allows technically savvy users to use Gnosis ecosystem websites and dapps anonymously over a VPN connection backed by the HOPR mixnet. This workshop will guide participants through the process of setting up a HOPR node, connecting to the GnosisVPN PoC, and using it. After completing the workshop, participants will be able to use GnosisVPN for their ongoing interactions in the Gnosis ecosystem, and their nodes will continue to contribute to decentralized anonymous communication infrastructure.

GnosisVPN will receive many more product improvements as outlined in GIP-122. The goal is to turn GnosisVPN into a general purpose VPN service to end users which leverages mixnet and web3 technologies to provide unique advantages over traditional VPNs.

Requirements:

- Participants must bring a laptop with Linux or macOS to run the GnosisVPN client.
- Participants must have a basic understanding of how to use the command line and SSH.
- Participants must have access to a Dappnode or VPS which can run a HOPR node.

References:
https://github.com/gnosis/gnosis_vpn-client/.

1.24 Savio – Welcome to Noirland

12.06.25 14:30 CEST
Side Stage - Cinema 7
Cryptography

A brief overview of what Noir the ZK language is, followed by a curated glimpse into cutting edge explorations, researches, and applications using Noir.

Previewing the future of privacy, right here at Protocol Berg.

1.25 BASTI – Golden Raspberry Awards Of Ethereum Scaling 2025

12.06.25 14:30 CEST
Main Stage - Cinema 10
Philosophy

Ethereum scaling is for everyone. It is for Layer 2s with EOA upgraders, unavailable data, backdoored proof systems, built-in censorship, straight-to-treasury bridges, ruggable gas tokens and 'proof systems'. I will honour the worst offenders against the unwritten values of Ethereum Alignment (tm). This practical context will allow us to find out what these unwritten values might be and each gilded raspberry shall be given with honest technical feedback on how to improve. Another nice takeaway is hopefully an abstracted technical intuition of the state of Ethereum scaling.

1.26 Tess Rinearson – Building for Core Devs: How OP Labs Accelerates Protocol Engineering

12.06.25 14:30 CEST
Side Stage - Cinema 6
Infrastructure

What happens when you start treating your core devs as customers, and build out specialized tooling, platforms and processes to make their work easier and their lives better?

In this talk, I'll share how the Platforms engineering team at OP Labs identified the pain points that Protocol devs face when working with the OP Stack (especially around testing and releases) and built dedicated devnets tooling, new E2E testing frameworks, and updated release pipelines to speed up our release cadence and improve our confidence in OP Stack releases and hardforks.

1.27 Ekaterina Riazantseva – Standardizing Ethereum metrics: PeerDAS and FOCIL retrospective

12.06.25 14:45 CEST
Side Stage - Cinema 6
Infrastructure

As the Ethereum ecosystem evolves, so do the challenges of monitoring and comparing protocol implementations. While Ethereum's Consensus and Execution specifications serve as a foundation, each client independently defines its own metrics. This divergence complicates everything from DevOps monitoring to core development comparisons and research simulations. In this talk, we will explore the efforts behind PeerDAS and FOCIL metrics standardization, showcasing real-world examples of how unified metrics can streamline feature delivery, improve cross-client validation, and empower researchers to run consistent simulations. By highlighting the successes and pitfalls encountered while building these metrics, we will demonstrate why standardized metrics are essential to maintaining Ethereum's robust and innovative environment.

1.28 Wassim Alsindi – The Chain Mail Gaze

12.06.25 15:00 CEST
Main Stage - Cinema 10
Philosophy

With their dreams of new 'Network State' empires, resource extraction, and colonial domination, today's tech overlords are the descendants of Europe's mediaeval Crusaders: well-financed, zealous fanatics remaking the world in the name of their greater good. Through a psycho-political reading of scarcity, chauvinism, and colonialism, The Chain Mail Gaze connects Crusader ideologues' desire for blood, land, and booty, to emerging 'frontiers' mediated by contemporary technologies.

1.29 Bastian Köcher – CorePlay - An actor-like framework for blockchains

12.06.25 15:00 CEST
Side Stage - Cinema 7
Consensus

We are building CorePlay, an actor-like framework on top of JAM. JAM is a next-generation blockchain architecture that allows smart-contract-like services to extend the base functionality of the chain. Each service inherits the security of the JAM validator set, and there can be a total of 341 service instances running in parallel per block. By using JAM, we gain access to continuations, deterministic gas metering, and synchronous composability. We think that these actors are the next evolution after smart contracts and writing bare blockchains. Actors will provide a similar level of logic encapsulation as smart contracts while gaining access to the same level of performance and blockspace as blockchains. Right now, we are seeing a push in the direction of vertical and horizontal scaling of blockchains. Vertical scaling only works up to a certain point but enables state locality and thus, synchronous interactions across the whole state. On the other hand, horizontal scaling increases the potential scaling horizon by sharding the execution and/or the data. JAM also scales horizontally by having execution and data sharding. However, it still allows synchronous interactions between the shards to make these shards operate as one instance.

This talk will give a high-level overview of the architecture of an actor and how the inherited properties of JAM enable developers to write simple and secure code. Also, it will go into detail on how actors will interact with each other synchronously.
Lastly, it will shed some light on the required orchestration infrastructure for scheduling and driving these actors.

1.30 Norbert Vadas – Economic security behind ZK proof generation

12.06.25 15:00 CEST
Side Stage - Cinema 6
Infrastructure

The economic security behind zero-knowledge proof generation is quite an under-explored topic. Several prover networks and marketplaces have emerged in the past 12 months, most of them relying on a slashable financial bond, but more sophisticated design mechanisms ensuring security, accessibility and decentralization are yet to be seen.

I'll dive into economic security in the context of ZK proof generation from different angles, covering 1. the nature of ZK proving as a hybrid task (it requires intense hardware resources but redundancy/wasted compute should be minimized), 2. the parallels between PoW mining and proof mining, 3. economic security through staking and restaking, and 3. viable alternatives such as reputation systems, Proof of Capacity and Availability for node operators, reputation-based reward mechanisms and more.

1.31 DistributedDoge – Datadex Pattern: Collect and share protocol-level metrics

12.06.25 15:15 CEST
Side Stage - Cinema 6
Storage

Collecting and sharing protocol-level metrics often occurs inside walled gardens of commercial providers, such as Google BigQuery or Dune, that offer great convenience but little control over data collection process.

Developers and analysts seeking flexibility in metric collection are often left wanting. This talk introduces Datadex, an architectural pattern relying on open-source tools for building public Data Portals that gather and publish metrics in a manner that is transparent, customizable, easily tailored to specific needs and free of access barriers. We'll share practical experiences of implementing Datadex pattern for Gitcoin (Allo Protocol), Filecoin, and real-world data sources,.

1.32 Victor Grishchenko – Can we do better than git's Merkle DAG?

12.06.25 15:30 CEST
Side Stage - Cinema 6
Networking

Git is 20 years old and git's Merkle DAG model is an established standard for decentralized systems. BitCoin and blockchains more or less follow in the footsteps. Same applies to the most of decentralized technology. The Replicated Data eXchange format aimed to overcome a number of pain points in that model, such as: accumulation of cryptographic sediment, coarse-grained-ness of data units, various inherent impedance mismatches and so on. So, how is the progress?

1.33 Paul Dylan-Ennis – No friends but the hash function: Descent into the Social Layer

12.06.25 15:30 CEST
Main Stage - Cinema 10
Philosophy

This talk is about the fringes of my Ethereum Social Layer research project. Despite six months research, the central question remains unclear to me: just what is the Social Layer? Rather than present a safe definition - in order to appear competent and professional - I will instead bring you on a tour of the competing definitions swirling around in my mind. We will descend, iceberg theory style, from the surface level or seemingly superficial definitions – the Social Layer is the community or Crypto Twitter – and then fall further into stranger, more esoteric answers, such as the Polycentric Ethereum, transglobal agorist fraternity and, of course, Technopolic cult of the hash function.

1.34 Samuel JJ Gosling – Quad-linear Voting (QLV)

12.06.25 15:30 CEST
Side Stage - Cinema 7
Consensus

Quad-linear voting (QLV) is a progressive plutoratic voting model, that aims align the interests of an organisation with its participants and make power dynamics explicit, rather than opaque, to complement a more strategic and nuanced governance process.

1.35 José Pedro Sousa – Learn Noir in an Afternoon (Or Your Money Back)

12.06.25 15:45 CEST
Workshop - Cinema 9
Cryptography

Noir is a Domain Specific Language for SNARK proving systems. It has been designed to use any ACIR compatible proving system. Its design choices are influenced heavily by Rust and focuses on a simple, familiar syntax. In this workshop, we will be learning the basics of Noir by writing a simple and fun example and deploying a verifier on an EVM chain.

1.36 Ellie Davidson – DA Layers vs. Confirmation Layers vs. Settlement Layers - Have we all just built the same thing?

12.06.25 16:00 CEST
Side Stage - Cinema 7
Consensus

This talk explores the similarities and distinctions between data availability (DA), confirmation, and settlement layers. While these layers are often discussed as separate components, they frequently function as variations of a consensus protocol.

We'll dive deep into the technical properties each layer requires and the consensus optimizations each one prioritizes. Using real-world examples—including CometBFT, HotShot, EigenDA, Gasper, and Ethereum 3-Slot Finality—we'll evaluate whether these layers are truly distinct or simply different approaches to the same underlying concept.

1.37 Phil Ngo, nflaig – How client diversity saved Holesky: Lessons for the future

12.06.25 16:00 CEST
Side Stage - Cinema 6
Infrastructure

Holesky, the largest Ethereum public testnet experienced one of the best, unplanned events for chaos testing as it hard-forked to Pectra. With an invalid block, consistent forking and a non-finality period spanning a duration of three weeks, client and infrastructure teams were pushed to Ethereum's limitations to discover edge cases that led to many fixes and lessons learned for the future. Join Nico and Phil of the Lodestar team as they detail their experiences and how the minority TypeScript consensus client Lodestar contributed to the recovery of the testnet.

1.38 Jaya Klara Brekke – Liberating the self from calculation: entropy in privacy enhancing technologies

12.06.25 16:00 CEST
Main Stage - Cinema 10
Philosophy

Entropy is a measure of randomness in information theory. This talk will discuss the role of entropy in privacy enhancing technologies from cryptography to noise generating networks and argue that the incalculable is essential for preserving the integrity and freedom of one's sense of self. The talk will draw on works by psychoanalyst Nuar Alsadir and philosophers Byung-Chul Han and Paolo Virno to articulate one of the profound 'accidents' that has accompanied the internet: the loss of cognitive integrity.

1.39 Masih Derkani – From Hours to Minutes: The Journey of Fast Finality on Filecoin

12.06.25 16:30 CEST
Side Stage - Cinema 7
Consensus

Embark on a behind-the-scenes tour of transitioning Filecoin's consensus mechanism from taking 7.5 hours to reaching finality, down to just a few minutes, with the adoption of Fast Finality (F3). This talk is all about our experiences and the lessons learned while changing consensus protocols on a live decentralized network. I'll dive into the real-world challenges we faced, from passively testing new protocols across a large-scale system to gracefully implementing these changes without disrupting the existing setup. I'll discuss the trial-and-error process of selecting the best network parameters through experiments and the balance we struck between speed and robustness, including maintaining strong censorship resistance. Join me as I share the technical insights and decision-making processes that guided us through this substantial upgrade, reflecting on the complexities and triumphs encountered along the way.

1.40 Marius, lightclient – Geth AMA

12.06.25 16:30 CEST
Side Stage - Cinema 6
Infrastructure

In this talk, we will answer all your questions regarding go-ethereum, how we view ourselves, how we think about the protocol, how to maintain criticial infrastructure, future ideas we're excited for and more. Come and bring your hardest questions!

1.41 Trent – Long term capture risks in Ethereum

12.06.25 16:30 CEST
Main Stage - Cinema 10
Philosophy

Software commons systems produce shared resources, which are at risk of capture from internal or external entities. This talk will explore long term capture in Ethereum: precedent case studies (Linux, Chromium), the landscape, risks, safeguards.

1.42 Nick Almond – F**k Off!: What if we forked crypto?

12.06.25 17:00 CEST
Main Stage - Cinema 10
Philosophy

The basic core primitive of blockchain governance is the fork. This talk will challenge us with a thought experiment, "what if we forked crypto?"

The crypto industry has fallen prey to capture, mindless speculation and nihilistic triviality straying far from its cypherpunk origins — we have hit a dead end. It's time to fork the entire industry.

We will utilise a Values based framework for analysing the state of the industry now and we will compare "what crypto is", with "what crypto should be" and then dig into possible practical ways in which we can execute an 'ontological fork' effectively recapturing crypto to its true direction.

This will involve coordinating both an attack and defence, building common pooled resources, darkDAOs and DAO activism, high coherence social consensus, forking as cultural practice, leveraging subsidiarity, expanding culture and dominating the social layer. Can we do it? Or more worryingly, what happens if we don't?

1.43 Nina Barbakadze – ZK: Accelerating DA Interop

12.06.25 17:00 CEST
Side Stage - Cinema 6
Infrastructure

In this presentation, I'll walk you through the Lazybridging protocol, a solution designed by engineers at Celestia Labs to natively support bridging across EVM rollups through Zero-Knowledge proofs.

1.44 Lukas – BitVM Engineering Tales

12.06.25 17:15 CEST
Workshop - Cinema 9
Consensus

Crafting BitVM required navigating numerous technical challenges and design decisions. In this talk, I'll share the research and engineering journey behind the BitVM protocol. I'll reveal abandoned approaches, implementation failures, and how these setbacks shaped the latest version of BitVM. Join me for practical insights from the R&D trenches.

2 Day 2

13. June 2025

2.1 Boris Godlin – Integrating Blockchain Data into AI Agents

13.06.25 10:00 CEST
Workshop - Cinema 9
Infrastructure

AI agents are transforming how we interact with data, but their effectiveness depends on real-time, reliable information. In this workshop, we will explore how to integrate blockchain data into AI agents using a SubQuery Indexer SDK. Participants will learn how to query on-chain data from different networks, process it efficiently, and use it to enhance AI-driven decision-making.

2.2 Madvi – Coordination as Intelligence: Envisioning Open Learning

13.06.25 10:00 CEST
Side Stage - Cinema 6
Philosophy

Coordination is the foundation of intelligence—both human and artificial. As we move toward an agent-centric internet, we must rethink how governance, trust, and open-source collaboration shape our digital ecosystems. This session explores philosophical and technical frameworks, from AGTP, to active inference and coordination theory, that enable self-governed, intelligence coordination networks.

2.3 Johannes Kühlewindt – Moderation is not a bad word: Towards Decentralised Content Moderation in P2P-Networks

13.06.25 10:00 CEST
Side Stage - Cinema 7
Networking

Moderation in peer-to-peer networks is often seen as incompatible with decentralization. Healthy, resilient distributed systems need tools to reduce spam and harmful behavior - without central authorities.

Starting from an overview of existing approaches, we move into specific considerations for for peer-to-peer code collaboration tool radicle. How can cryptographic identities and social trust graphs enable collaborative moderation, reputation management, and abuse mitigation, all while preserving permissionless participation?

None of this can be discussed without exploring the philosophical tension between openness and governance in decentralized content networks.

2.4 Sergey Fedorov – New insights into distributed and concurrent programming

13.06.25 10:15 CEST
Main Stage - Cinema 10
Consensus

Designing, verifying, correctly implementing and later improving core distributed protocols like consensus, which are critical for safety and reliability of decentralized systems, is notoriously difficult and error-prone. One of the biggest challenges here is dealing with the inherently concurrent nature of decentralized systems. But it's too important, and we can't really afford to get it wrong, so we need to take it seriously and do a much better job here. But how?

In order to make a breakthrough in this area, we would benefit from revisiting the fundamentals and trying to rethink distributed and concurrent programming from the first principles. How should we approach concurrency in distributed algorithms in a natural way and with confidence? How can we avoid excessive synchronization, prevent deadlocks and resource leakage? How can we make distributed and concurrent systems more simple, flexible, and reliable? In this talk, I will share with you some insights into the fundamentals of distributed and concurrent programming that could help us to overcome these difficulties and make a breakthrough for the future of decentralized computing!

2.5 Pavel Bautista – Monitoring Ethereum's Beacon Chain: A DEFCON Alert System for Safety and Liveness

13.06.25 10:15 CEST
Side Stage - Cinema 6
Consensus

We introduce a new tool that analyzes safety and liveness properties of the Beacon chain, designed to alert when the chain enters periods of low reliability. We present the different critical periods identified from Genesis to Today, and classified by our Defense Readiness Condition (DEFCON) Alert Systems that we propose.

2.6 Ori Shimony – DeCom - Building the Infrastructure for Decentralized Commerce

13.06.25 10:30 CEST
Side Stage - Cinema 6
Philosophy

The cypherpunk dream wasn't just permissionless finance—it was freedom to conduct peer-to-peer commerce without gatekeepers. Silk Road offered the first glimpse of this world before its collapse shut down that vision along with the marketplace. Meanwhile, Web2 platforms built trillion-dollar empires by intermediating commerce, extracting 20-30% while controlling who can participate. My research fellowship at the Ethereum Foundation examines why blockchain has revolutionized finance but failed to disrupt commerce. I'll present how recent advances in programmable cryptography, attestation frameworks, and AI agents now make it possible to realize the original cypherpunk vision of trustless commerce—not just for contraband, but for the trillion-dollar markets of goods and services that power our economy.

2.7 ODYSSEAS – Contract-based soft forks: Coining a term in search of hack prevention

13.06.25 10:30 CEST
Main Stage - Cinema 10
Consensus

In this talk, we talk about a novel mechanism we call the Credible Layer, which is designed as an overlay mechanism that enables a Blockchain network (L2 or L1) to enable contract-based soft forking. Developers can associate EVM bytecode with contract addresses which adds additional transaction rules to transactions that interact with these contracts. We will explore how such a mechanism effectively upgrades the STF of the network, and how it can either be enshrined to the underlying network or enforced by network validators, without making the underlying protocol aware of it. We will also explore the overarching theme of introducing user-space protocol upgrades (e.g Lido, EigenLayer, Credible Layer), ahead of enshrining such schemes onto the base layer.

2.8 Mikel Cortes – The eternal research of broadcasting messages, the limits of GossipSub

13.06.25 10:30 CEST
Side Stage - Cinema 7
Networking

Just when we thought the biggest bottleneck in P2P networking was reaching complex consensus mechanisms or generating efficient proofs, we realized that the fundamental networking protocol stack itself is one of them. Join this session to explore the latest open proposals for optimizing GossipSub in libp2p.

2.9 Vijay Krishnavanshi – Multi agentic architecture on top of p2p infra

13.06.25 10:45 CEST
Workshop - Cinema 9
Infrastructure

This workshop builds on the concept of shared memory enabled by Ethereum. It lays down the conceptual and practical benefits of having a shared memory layer for dApps but also AI agents and contrasts them with those of centralized cloud-based platforms. By going back to the roots of Ethereum's vision to be a platform for decentralized applications, this workshop will also provide an overview of the p2p storage networks (IPFS, SWARM, Codex) that was originally envisioning to support Ethereum's shared memory layer. The workshop will conclude with a practical demonstration of how networks of open AI agents can tap into Ethereum's shared memory and account abstraction to allow for a free flow of verifiable information between agents. The workshop is open to all knowledge archivists, developers looking to create self-sovereign AI agents or networks of public agents, and haters of big tech.

2.10 Leo BG – At the Intersection of Data Availability Sampling and Sharded Mempools

13.06.25 11:00 CEST
Side Stage - Cinema 7
Networking

A new design that mixes a sharded mempool with data availability sampling to achieve higher rollup throughput and high scalability for Ethereum. We present the results of our research in the P2P network for efficient blob dissemination and bandwidth reduction.

2.11 Barnabé Monnot – What we want from our nodes

13.06.25 11:00 CEST
Main Stage - Cinema 10
Consensus

Without clear goals for what our network should provide, we end up optimising for our means rather than for our ends. In this talk, I'll discuss the goals of our network — scale, hardness, verifiability and censorship-resistance — and how some of the means ("local building", "solo staking") should be re-evaluated in light of their contributions to these goals, given advances in protocol research.

2.12 Lefteris Kokoris Kogias – Walrus: An Efficient Decentralized Storage Network

13.06.25 11:00 CEST
Side Stage - Cinema 6
Storage

Decentralized storage systems face a fundamental trade-off between replication overhead, recovery efficiency, and security guarantees. Current approaches either rely on full replication, incurring sub- stantial storage costs, or employ trivial erasure coding schemes that struggle with efficient recovery especially under high storage- node churn. We present Walrus, a novel decentralized blob storage system that addresses these limitations through multiple technical innovations.

At the core of Walrus is Red Stuff, a two-dimensional erasure coding protocol that achieves high security with only 4.5x repli- cation factor, while enabling self-healing recovery that requires bandwidth proportional to only the lost data ((||/) versus (||) in traditional systems). Crucially, Red Stuff is the first protocol to support storage challenges in asynchronous networks, preventing adversaries from exploiting network delays to pass ver- ification without actually storing data.

Walrus also introduces a novel multi-stage epoch change proto- col that efficiently handles storage node churn while maintaining uninterrupted availability during committee transitions. Our sys- tem incorporates authenticated data structures to defend against malicious clients and ensures data consistency throughout stor- age and retrieval processes.

2.13 Alejandro Ranchal-Pedrosa – Rebased Rollups: Achieving Credibly Neutral Synchronous Composability with Low Latency and Cost

13.06.25 11:30 CEST
Side Stage - Cinema 7
Consensus

Rebased rollups introduce a novel paradigm blending the advantages of based and non-based rollups to provide synchronous composability, credible neutrality, and reduced latency without incurring the full cost and latency penalties associated with Ethereum-based rollups. By becoming "based on-demand" for durations shorter than a full Ethereum slot, rebased rollups efficiently utilize Ethereum's existing proposer set to facilitate faster transaction confirmations and increased throughput.

This presentation explores the technical challenges posed by current Layer 2 (L2) rollups, particularly fragmentation and loss of synchronous composability, and analyzes existing solutions including mesh and hub-based approaches, highlighting their limitations concerning credible neutrality and economic security. We present rebased rollups as a practical solution, detailing their architecture, security trade-offs, and mechanisms such as preconfirmations and dynamic attestation tracking.

We conclude by outlining how rebased rollups horizontally scale economic security and transaction throughput, providing Ethereum-aligned synchronous composability with latency comparable to centralized sequencers, ultimately balancing decentralization, neutrality, performance, and cost-effectiveness for the broader Ethereum ecosystem.

2.14 Tim Beiko – How Ethereum Governance (Actually) Works

13.06.25 11:30 CEST
Main Stage - Cinema 10
Philosophy

This talk will detail Ethereum's governance processes around facilitating network upgrades, and provide an overview of what protocol upgrades are being planned.

2.15 Lukas Rajnoha, Michal Převrátil – The Art of Manually Guided Fuzzing

13.06.25 11:30 CEST
Workshop - Cinema 9
Infrastructure

Manually Guided Fuzzing represents a paradigm shift in smart contract security testing, combining the precision of white-box approaches with the efficiency of targeted test flows. Unlike traditional fuzzing techniques that rely on randomness or predefined properties, this innovative approach empowers developers and auditors to direct the fuzzing process toward potential vulnerabilities with surgical precision, drastically improving both testing efficiency and vulnerability detection in complex DeFi systems.

2.16 Aata Hokoridani – StorageBeat: An Evaluation Framework for Storage Services

13.06.25 11:30 CEST
Side Stage - Cinema 6
Storage

Storage ecosystems provide wildly different types of services to again wildly different segments of the addressable storage consumer market. This talk will quickly survey the decentralised and centralised storage landscape before moving along to work done motivated by a long standing goal of our research team: How to analyse multiple storage providers along with their disparate guarantees, retrieval methods, SLAs, etc., on the same "playing field."

In the course of this work, we went through the motions of building an evaluation framework which rightly could be called a "StorageBeat," in blatant analogy with L2Beat. An important component of the talk is explanation of the pitfalls of and methods for constructing insightful metrics. e.g., state-rentals, availabilities, cryptographically ensured durabilities, incentives guarantees, etc., for storage ecosystems.

As a take away, attendees will be on firm footing for making rational decisions to choose best the ecosystem for, e.g, their own projects & dApps. In practice we have run into enormous amounts of confusion regarding storage services and how/what they provide. If anything this talk will uncloud this cloudy scenario.

2.17 Guillaume Ballet – Building zig program for zkvms: a case study with zeam

13.06.25 12:00 CEST
Side Stage - Cinema 7
Consensus

Most of zkvms SDKs only offer rust as a programming language. This talk will go over what is needed to implement other language frontends for zkvms, using zeam, the zig beam chain client, as a supporting example.

2.18 Lefteris Karapetsas – Privacy ist mir Wurst. I Got Nothing to Hide.

13.06.25 12:00 CEST
Main Stage - Cinema 10
Cryptography

This is a talk about "having nothing to hide." A talk about oversharing in the age of TikTok and Instagram, about doxing in the era of public blockchains, and about data sovereignty in a world dominated by centralized repositories. Why is privacy so often dismissed, and what does it really mean to give it up?

2.19 Andrew Macpherson – Reward and resource sharing mechanisms in decentralised storage

13.06.25 12:00 CEST
Side Stage - Cinema 6
Storage

Most data storage systems have a way to automatically decide the physical location that data will be stored. (That's why, for example, you don't have to calculate something about sectors and tracks when you save a file on your computer.)

If you do automatic allocation in decentralised storage, then you also need to automate the system that distributes payments to the service providers — Filecoin-style manual peer to peer negotiation is not possible. What is needed is a *mechanism* in the sense of microeconomic theory. This mechanism needs to have good properties if it is to foster a healthy service provider population and deliver good service and efficient prices to users.

I'll give an introduction to this subject in the context of the EthSwarm Protocol. In EthSwarm, as well as providing a fixed amount of capacity, service providers must buy revenue shares from a contract at a fixed price in a kind of Tullock contest. Perhaps surprisingly, even though this allocation system has nothing to do with the amount or quality of service provided, under good conditions it results in revenue share flowing to more efficient operators, resulting in more competitive pricing.

Target Audience: people researching and building decentralised services.

2.20 Aron Soos – How to Decentralize Any Front-End

13.06.25 12:15 CEST
Workshop - Cinema 9
Storage

This workshop is about decentralized storage, one of the key components to realize the World Computer. We'll use the time to run a storage node (Swarm), upload a website to the decentralized network, and set up ENS to make the site accessible also on web2 via eth.limo.

As we go through this demonstration, we'll also discuss challenges and solutions in decentralized storage, such as data availability, DDoS and censorship resistance, erasure coding, incentive systems, mutable vs. immutable data, and more.

For the practical segments, the session will use a terminal in a UNIX-like environment. It is encouraged to follow along, the only pre-requisite is a recent Node.js version installed on your machine.

2.21 Vasco Santos – Off-the-shelf Trustless HTTP Server for Content-Addressable Data

13.06.25 12:30 CEST
Side Stage - Cinema 6
Storage

A Minimal Blueprint for Trustless, Efficient Content Delivery - a technical proof of concept to rethink content-addressable serving.

2.22 Hudson Jameson – Are You Vitalik or Are You My Mom? An In Depth Analysis of Wallet Security Set-ups

13.06.25 12:30 CEST
Main Stage - Cinema 10
Cryptography

An often overlooked element of securing your digital assets is determining how paranoid you should be. Many times users go down rabbit holes of complicated schemes to backup and protect their wallets which ultimately causes complications when they need to access them. However, there are situations where you may be in a position of power or public identification that you need to go deeper. Do you need to secure your assets like Vitalik does or like my Mom does?

2.23 Raluca Diugan – Mechanisms for Unlocking Idle Blobspace

13.06.25 13:00 CEST
Side Stage - Cinema 6
Storage

EIP-4844 introduced cheaper, although temporary storage on Ethereum, allowing rollups to publish data cost-efficiently. With new and old rollups alike opting for such storage, blob count limits are set to increase with future network upgrades in the hope they meet demand. Another emerging approach to supplement blobspace consists of efforts for more efficient utilization, in essence by preventing (in aggregate) wasting valuable bytes to zero padding. In this talk, we explore proposed mechanisms, highlighting their suitability for different types of rollup architectures, as well as the challenges posed to research and development teams on both layers. Our goal is to consolidate a research direction towards more efficient utilization of blobspace, complementing the Danksharding roadmap.

2.24 Jaya Klara Brekke – The Forest That Protects the Public Good: Nym for Libp2p privacy (part2)

13.06.25 13:15 CEST
Workshop - Cinema 9
Networking

The public and private are not opposites, they are complementary: privacy is needed to sustain the security and integrity of people as well as infrastructure that serve the public good. This workshop will demo working code for running Libp2p traffic through Nym, built with the Nym Rust SDK.

2.25 Arik Galansky – MPC at internet scale

13.06.25 13:30 CEST
Side Stage - Cinema 7
Cryptography

Recent advancements in MPC allow it to be used to power internet scale applications and protecting end-users from some of the risks of wide blockchain adoption. MPC had a lot of challenges - many rounds of communication, intensive compute requirement, large communication overhead, inability to scale horizontally and more. We are not on the verge of solving the critical issues and bringing MPC to the general public. We will explore the problems and solutions (new and old) that make this happen.

2.26 Michelle Lee – IPFS: A Decade in Browsers

13.06.25 14:00 CEST
Main Stage - Cinema 10
Networking

Over the past decade, the IPFS public network has grown into millions of documents providing an alternative, resilient, and self-certifying web.

But what is web without browsers? This talk will covers our efforts getting ipfs:// handler support directly into browsers and the challenges we've faced. Looking into the future, we'll also preview our upcoming plans to reduce reliance on centralized HTTP <> IPFS gateways, including Helia's verified fetch, AutoTLS for libp2p, and how we think browsers and p2p will evolve in the coming years.

2.27 Leo Alt – Compiler-based optimizations for zkVMs

13.06.25 14:00 CEST
Side Stage - Cinema 7
Cryptography

General purpose zkVMs provide excellent developer experience in an ecosystem known for complex tooling. However, they currently require clusters of GPUs to generate proofs in acceptable time, and are still far away from providing client-side proofs to the masses, which is required by privacy use cases, for example.

While several optimizations focus on the prover software, compiler-based optimizations on the VM, ISA and guest program are still underdeveloped.

In this talk we will present our work on these techniques, including automatic synthesis of ZK precompiles and ZK-friendly program optimization. Our experiments integrating these optimizers in powdrVM and other zkVMs show that the techniques are framework- and prover-agnostic, and have the potential to improve proof generation performance by one order of magnitude and more.

2.28 Thomas Hsueh – Coordination-Avoidance: Rethinking Decentralized Networks Beyond Global Consensus

13.06.25 14:30 CEST
Side Stage - Cinema 6
Networking

Blockchains today are decentralized networks of fat servers. Rollups also operate on fat servers for sequencing and proving. The vast majority of users of these systems run thin clients that always interact through these servers, an architecture that (1) fails to leverage the local compute capability (2) rely on (decentralised) middlemen for interaction, necessitating transaction fees for middlemen incentivisation.

This talk introduces coordination-avoidance as a paradigm shift in decentralized computing. Instead of enforcing global consensus, coordination-avoidance enables direct P2P execution among users that operate local-first clients. This paradigm unlocks a new design space for applications that benefit from decentralization, high responsiveness, and safety at the same time.

I will discuss how DRP (Distributed Real-time Programs), a new Internet protocol, constructs a new kind of BFT state from consensus-free P2P networks. This approach enables applications with novel economic models that are impractical for any existing client-server architectures, regardless if the servers are decentralised.

2.29 Daniel Norman – Don't Trust, Verify: IPFS for (D)App Distribution on the Web in 2025

13.06.25 14:30 CEST
Main Stage - Cinema 10
Networking

The Bybit hack earlier this year, where attackers compromised the AWS-hosted Safe frontend and tricked Bybit into signing malicious transaction resulting in the loss of $1.4 billion, highlighted a longstanding problem: the web—and by extension, (d)apps—is fundamentally built trust rather than verification.

This talk will examine how IPFS can be used to distribute web applications in a way that reduces these risks. By using content addressing and local verification, developers can ensure users load exactly the code that was published, minimizing reliance on trust-based distribution.

We'll cover best practices for deploying dapps to IPFS, focusing on recent advancements to enable native IPFS support in browsers by leaning on HTTP as the foundation for interoperability.

2.30 Pedro Gomes – Two flavors of Smart Sessions: Session Keys vs SubAccounts

13.06.25 14:30 CEST
Side Stage - Cinema 7
Cryptography

Describing two different approaches to Smart Sessions to improve wallet-app interoperability. Each approach has its pros and cons but share the same philosophy of empowering apps with smart contracts with delegated signing and improved user experience.

2.31 Casey Carr – Swarming by the STIX: Exploring decentralized Traffic Light Protocol (TLP) and Semaphore for Spyware Honeytrapper indicator-sharing in highly-surveilled environments

13.06.25 14:45 CEST
Side Stage - Cinema 7
Philosophy

Journalists in politically-isolating environments face increasing threats from commodity spyware, often relying on NGOs for digital security support, not without bottlenecks and privacy risks. Recent abuses of mobile forensics tools, such as Cellebrite, highlight the dangers of centralized mobile security falling into the wrong hands. This proposal introduces a distributed Cyber Threat Intelligence (CTI) network integrating Traffic Light Protocol (TLP) and zero-knowledge proofs (Semaphore) to enable privacy-preserving, trustless indicator sharing. By leveraging honeypot-driven threat indicators and decentralized pub/sub mechanisms, at-risk users can safely contribute to and benefit from a broader CTI ecosystem without exposing personal metadata.

2.32 Andrej Berlin, Beth McCarthy – Designing Protocols for a New Social Fabric

13.06.25 14:45 CEST
Workshop - Cinema 9
Philosophy

How might we design protocols that shape behaviors and address real-world challenges? In this workshop, we will individually map behavioral patterns, prioritize key challenges, and merge our ideas to develop protocol concepts that encourage positive interactions. Borrowing from design principles used by companies like Google and Apple, this session will provide hands-on experience in structuring sociotechnical rules - without much discussion. No technical background is required—just curiosity and a willingness to be creative.

2.33 Misha Komarov – Bitcoin PIPEs: ZK-Proofs and Covenants on Bitcoin L1 without Softfork

13.06.25 15:00 CEST
Side Stage - Cinema 7
Cryptography

Bitcoin PIPEs (Polynomial Inner Product Encryption) is a new cryptographic primitive designed using special-purpose functional encryption and zero-knowledge proofs to enable both covenants and ZKPs on Bitcoin, without the need for altering the core protocol. The method proposed involves generating unique keys and signatures that are conditionally valid based on the satisfaction of proof conditions. This approach not only overcomes the current limitations of Bitcoin Script, but also opens up new possibilities for implementing new kinds of applications on the Bitcoin L1 (via application-specific Bitcoin PIPEs covenants) alongside true Bitcoin zkRollups, new token standards, and novel staking protocols.

White paper:
https://www.allocin.it/uploads/placeholder-bitcoin.pdf.

2.34 Nadiem Sissouno, Alexander Mueller – Rethinking Competition Models in Solver-Based Protocols

13.06.25 15:00 CEST
Side Stage - Cinema 6
Networking

Many solver-based decentralized protocols rely on competition models to incentivize actors like validators, solvers, and liquidity providers. While competition can drive efficiency, it also has a well-documented tendency to lead to centralization. As competitive dynamics favor the most resourceful players, smaller participants get squeezed out, ultimately reducing diversity and increasing reliance on a few dominant actors.

Interestingly, societies avoid competition models for roles deemed crucial to service quality, such as airport security or medical services, to prevent deterioration due to cost-cutting. However, in financial services, competition remains the norm, even when it may negatively impact system integrity.

This session explores alternative incentive models that prioritize resilience and decentralization over a pure race-to-the-bottom approach.

2.35 Edmund Edgar – Bluesky, atproto, how to hack on it and why it matters

13.06.25 15:00 CEST
Main Stage - Cinema 10
Networking

In 2019 Twitter asked a team of crypto and p2p devs to design a protocol for the next generation of permissionless social media. The protocol escaped Twitter and now drives Bluesky, the fast-growing social media site. It can do a lot more.

This talk will cover: - The principles underlying the design of atproto - Why those principles matter - Bluesky and the unbundling of feeds, blocklists, curation and tagging - How the protocol works (Dag-cbor, Merkle Search Trees, DID:PLC) - How to make bots to make stuff happen on-chain.

2.36 Dennis Trautwein – The surprising challenges of counting nodes

13.06.25 15:30 CEST
Side Stage - Cinema 6
Networking

How many nodes are in given network? A seemingly simple question with a more elusive answer than it seems. Different methodologies yield different results with implications for protocol design. Let's explore the hidden complexities.

2.37 Manu Alzuru – Redesigning Governance: Trust Networks, Decentralization, and the Dichotomy of Extremes in Politics

13.06.25 15:30 CEST
Main Stage - Cinema 10
Philosophy

In a world increasingly divided by extremes, the traditional structures of governance and political ideology no longer seem to offer the solutions we need. This talk will explore the potential of decentralized systems and cryptography to create new models for governance that break away from conventional dichotomies. Drawing from my experiences with pop-up cities, experiments in trust networks, and the growing need for decentralized approaches to communication and coordination, I will explore how peer-to-peer networks, zero-knowledge technologies, and open-source principles can build more transparent, resilient, and inclusive societies. We'll discuss the philosophical implications of decentralized governance, and how these systems can transcend the binary conflict between the extreme left and right by focusing on common values of trust, security, and privacy.

2.38 Nitya Subramanian – Key Management Mechanisms and their UX Properties

13.06.25 16:00 CEST
Side Stage - Cinema 7
Cryptography

ERC-4337, MPC, EOAs, Shamir Secret Sharing. Passkeys, Passwords, Phone Numbers, Enclaves, EIP-7702: the list goes on. WTF!?

In this talk, we'll go over not only what each of these are (and why we're still talking about key management in 2025), but the unique UX properties of each of these tools- and how we can put together the right stack to get the best UX for different use cases.

2.39 Ira Nezhynska – How to turn strangers into early adopters when they don't understand your tech

13.06.25 16:15 CEST
Workshop - Cinema 9
Philosophy

This design workshop is for developers-turned-founders who are launching their product to market and want to set it up for successful early adoption among non-technical users.

After a few exercises and a bit of theory, you'll leave home fully equipped with tactics and knowledge to: - communicate your hyper-complex product with clarity to those who don't (and don't need to) understand your tech in order to start using it daily and refer it to their friends - differentiate your product not with the features (aka, tech race) but through user aspirations and what matters in their lives - use symbols and styles to trigger a wider range of emotional and sensorial responses from the first interaction moment.

This workshop is a blend of product reputation reverse-engineering, user research, storytelling and visual communication.

Please, note, that this workshop is NOT for those who: - are deep in the lab/experimentation mode and are not emotionally ready to turn their tech innovation into a product on the market. - are developing dev tools.

2.40 Gavin Wood – Beyond the Ledger: JAM and the Future of Scalable Decentralized Computing

13.06.25 16:30 CEST
Main Stage - Cinema 10
Infrastructure

Blockchain tech can be more than just a ledger: it can be a scalable global computing network, moving away from transaction-centric blockchain design into a decentralised computer one, changing usage patterns, development patterns and tooling. The Join-Accumulate Machine (JAM) is a new protocol aiming to make the usage of blockchain core radically un-opinionated, and to enhance the scalability and efficiency of blockchain networks. By enabling parallel data processing and reducing redundancy, JAM enables seamless collaboration between different applications, storing all application states in a shared environment. This approach facilitates more efficient data accumulation and consensus mechanisms, leading to improved performance and resource utilization. The adoption of JAM represents a significant advancement in blockchain technology: offering a pathway toward more scalable and robust decentralized systems. It is a forward-looking discussion on the future of Web3: showing blockchains can go beyond transactions, enabling decentralized computing with continuous execution flow.

Gavin will provide an update on the latest developments on JAM, including achieved milestones by teams working around the JAM Implementer's Prize, the JAM toaster and JAM tart, an exciting onchain Execution of DOOM which showcases JAM's potential, and how to apply *any application* onchain: even those that don't resemble a blockchain/L2.

2.41 Jim Posen – A Functional VM for Verifiable Computing over Binary Fields

13.06.25 16:30 CEST
Side Stage - Cinema 7
Cryptography

This talk presents a new system for verifiable computing using the Binius proof library. Binius implements a hash-based SNARK built on towers of binary fields, which unlocks huge gains in computational efficiency compared with traditional SNARKs, particularly when using specialized hardware. Programs are written in a simple, statically-typed functional language similar to Standard ML, which compiles directly to a custom virtual machine optimized for cryptographic proofs. By co-designing the VM's instruction set and compiler with the Binius cryptographic library, we enable practical use cases like compressing Merkle tree proofs, aggregating hash-based signatures, and recursive SNARK proofs.

A Department of Decentralization event.
https://dod.ngo

This booklet was generated programmatically and is valid without signature. All content was provided as-is by the respective speakers.