Program

Protocol BERG

The decentralized protocol and infrastructure conference.
September 15, 2023, Berlin

A Department of Decentralization event.

Abstract

Protocol Berg is a one-day technical conference for protocol, system, and network engineers, decentralized-infrastructure administrators, researchers, and other curious minds from different ecosystems.

This program outlines the content and speakers of the 52 sessions of the first Protocol Berg, held on September 15, 2023, in Kreuzberg, Berlin. For this edition of the event, sessions are distributed over two stages and two workshop rooms.

The program is ordered chronologically.

Contents

1 Opening Ceremony

Magazin - Main Stage, 09:00 CEST, General

The Department of Decentralization welcomes you to Protocol Berg!

We briefly run you through the concept of the event and the program highlights of the day. Furthermore, we share logistical and operational tips on how to navigate the venue, information on food and drinks, and more.

2 Asynchronous Phil – Measuring Decentralization Across L2 Networks

Magazin - Main Stage, 09:30 CEST, Governance & Society

Many studies and analyses have been performed on Layer-1 protocols that measure decentralization to the point where we have an accepted set of standards. Such standards include, but are not limited to, nakamoto coefficient, validator distribution, and full node counts. This talk explores the challenges in measuring decentralization across layer-2s on Ethereum, Polkadot and Cosmos where the technology varies and creates new avenues of centralization more obscured from the view of users.

3 Thomas Jay Rush, Dawid Szlachta – Indexing Ethereum Mainnet for Near-Zero Cost

Atelier - Side Stage, 10:00 CEST, Infrastructure

A discussion about EVM client software, why it can't deliver accurate transactional histories (hint: it's missing an index), and what it would be like if it could.

In this talk, we describe the Unchained Index: a system for creating a naturally-sharded, immutable index for any EVM-based blockchain including L2s.

Using only the node software as its data source, the Unchained Index visits every binary corner of the chain's history, searching for address appearances (which is way more complicated than one might think). The algorithm is well-documented and open source. This ensures that the process is permissionlessly reproducible. The result of this indexing is stored as a collection of chunks.

By building chunks ("a time-ordered log of an index of a time-ordered log"), fronting the chunks with Bloom filters, and maintaining a manifest of all chunks and Blooms, we create an off-chain index that lives naturally on content-address stores such as IPFS. We publish the hashes of all parts of the index to a smart contract.

End users (by querying the Bloom filters via the smart contract) may download only that portion of the index that they are interested in (i.e., their own histories). This ensures that the system works on small machines. Using "Pin by Default" the system realizes the massive benefit of enlisting end users in the distribution of the chunks. Heavy users acquire, pin, and distribute a (...)

4 Aliasgar Merchant – CometBFT: The Shooting Star of Blockchain Consensus Protocols

Loft - Workshop 0, 10:00 CEST, Consensus

Ali will introduce CometBFT and discuss the unique features that set it apart from other blockchain protocols. You will find out why CometBFT is quickly becoming the preferred choice for decentralized applications and how it is addressing the scalability challenges in blockchain technology.

During the presentation, Ali will take a deep dive into the technical details of CometBFT. You will learn about its code and architecture, and explore the cryptographic primitives that keep it secure. This part of the presentation will be especially interesting for developers and blockchain enthusiasts who want to understand the inner workings of CometBFT.

Furthermore, Ali will discuss how CometBFT is contributing to the realization of decentralization in the blockchain industry. You will find out how CometBFT is enabling decentralized applications to thrive and empowering individuals to take control of their data and assets.

Finally, Ali will also introduce ABCI++, its features, and its potential impact on the blockchain industry. This presentation is a must-attend for anyone interested in the latest advancements in blockchain technology.

5 Jenny Pollack – idk what x is and at this point i'm afraid to ask

Magazin - Main Stage, 10:00 CEST, Governance & Society

together we will speed run the definitions of the terms that you've heard but would hate for someone to ask you to define on a podcast.

we'll go as fast as we can giving up to date working definitions and possibly examples of things like: AA, intents, MEV, suave, appchain, rollup, data availability, zk circuit, stark, snark, modular, monolith, 4337, proxy, custodian, mesh security, shared sequencers this talk will contain technical topics but should be suitable for all curious audiences.

6 Guillaume Ballet, Tanishq Jasoria – Verkle sync : bring a node up in minutes

Magazin - Main Stage, 10:30 CEST, Networking

A high-level introduction to verkle sync, a synchronization algorithm made possible by the use of verkle trees and stateless Ethereum.

This presentation covers the internal of verkle sync from the point of view of the attester and/or hobbyist, and proposes a separation between attesters and block proposers. It details why running a node will become much easier, for some purposes, once verkle trees are in use.

7 Jonas Seiferth – Retroactive Public Goods Funding: 2 Rounds in

Atelier - Side Stage, 10:30 CEST, Governance & Society

In this talk I want to share about Retroactive Public Goods Funding, what we learned in running 2 rounds of RetroPGF at Optimism, and what's next on our journey to summon Ether's Phoenix.

Cyberspace today suffers from a monumental market failure because its economic ruleset was built for the physical world. Public Goods are core to the growth of cyberspace but our current markets are unable to nurture that growth. Web3 presents an opportunity for cyberspace to only be occupied but governed by its citizens and reinvent how we organize and fund public goods in this digital age.

Optimism is experimenting with a new economic mechanism called Retroactive Public Goods Funding, in which citizens reward the creation and maintenance of public goods proportional to how much impact these public goods provide to the collective.

In March '23, we concluded our second RetroPGF experiment, where 69 Badgeholders allocated 10M OP among 195 Projects. We learned a bunch. We're on to the next experiment with exciting new improvements. One step closer to Ethers Phoenix.

8 Erik Kundt, Sebastian Martinez – Peer-to-peer code collaboration with Radicle

Loft - Workshop 0, 10:45 CEST, Networking

In this hands-on workshop, we'll learn how to use the Radicle stack to collaborate on a code project. We'll run our own nodes, connect to peers, and grow a virtual garden together.

Radicle is a local-first, peer-to-peer network for code collaboration, built on top of Git. It enables users to run their own nodes, ensuring censorship-resistant code collaboration and fostering a resilient network without reliance on third-parties.

Radicle functions as a protocol where each user on the network runs identical software, known as the Radicle Stack. This stack primarily consists of a command line interface and a networked service called the Radicle Node.

Users can also opt to run the Radicle Web client and HTTP daemon, providing a familiar web-based experience for enhanced accessibility and convenience.

In this workshop we will explore Radicle's code collaboration workflow by:

- running our own Radicle Node
- using the Radicle Web client & Radicle CLI
- connecting to a community seed node

Requirements:

- Device running Linux or MacOS (...)

9 Steffen Kux – Real web3 messaging must be encrypted, decentralized, and interoperable! Utilizing dm3 protocol as layer 0 of messaging.

Atelier - Workshop 1, 11:00 CEST, Infrastructure

The dm3 protocol is the web3 messaging protocol focusing on encryption, decentralization, scalability, and in particular interoperability. It utilizes the essential features for a lean messaging base protocol: a registry for public keys and decentralized delivery service nodes.

Email, SMS, and messengers such as WhatsApp, Signal, Telegram, and others are known and used by almost everyone today. The lack of comprehensive end-to-end encryption for e-mail and closed data silos for central messenger services are currently common. Cross-application communication is not possible. User profiles are under the control of large corporations.

With web3 we have new possibilities like key-based identities, decentralized registries on the blockchain, and end-to-end encryption, ... In the last month, several web3-based messaging solutions were introduced. While encryption, security, and privacy are consistently implemented, interoperability is still not yet solved but is needed even more.

With **dm3** , there exists a lean web3-based protocol for peer-2-peer messaging, which makes it possible to easily integrate secure communication into DApps. Interoperability with other protocols or services can be accomplished with little effort and without compromising on security. Protocol extensions for advanced privacy, group chats, (...)

10 Trent Van Epps – Protocol Guild: Funding & Incentivising Core Protocol Work

Atelier - Side Stage, 11:00 CEST, Governance & Society

The Protocol Guild aims to secure the future of Ethereum, by enabling a highly efficient way for its ecosystem and community to sustainably fund core protocol development, while rebalancing incentives for core protocol contributors.

The Protocol Guild itself is a collective of Ethereum's active core protocol contributors, which is today comprised of 130 individuals from +20 different ecosystem teams. These individuals are focused not only on maintaining Ethereum and the EVM as it exists today, but also on researching and implementing cutting-edge advancements which will help onboard the next wave of global users seeking the benefits of decentralized and censorship-resistant protocols. In short, the work done by this collective is of extreme importance to the long-term security of Ethereum.

Nevertheless, funding for core protocol work has historically come from a select number of entities, which only provides a fraction of the financial incentives compared to other available work (apps, L2s etc.), on a risk-adjusted basis. The Guild was created to serve as a counterbalance to this (and at worst, a funder of last resort), while providing core protocol contributors with a way to indirectly participate in the success of the broader ecosystem, and incentivize continued contributions over the long term.

In this presentation, I'll detail the different attributes and assurances that make Protocol Guild (...)

11 Christian Reitwiessner – powdr - a modular stack for zkVMs

Magazin - Main Stage, 11:00 CEST, Cryptography

In the recent months, there has been a surge in the popularity of zkVM implementations. Many of these use specialized solutions and code, sometimes even all the way down to the cryptography, which makes these zkVMs very monolithic and non-interoperable.

Powdr takes a modular approach to designing and constructing zkVMs, employing multiple compilation and optimization stages to arrive at the final prover and verifier. Users can define custom instruction sets for a VM, specify how those compile to constraints, generate sub-machines and declare how to connect them. Moreover, the flexibility of powdr enables users to select from a variety of proving backends when generating the prover and verifier components.

To validate this concept, we have successfully developed a fully functional verifier that compiles (no-std) Rust code into eSTARK and Halo2 proofs via the RISC-V architecture. Additionally, we are currently working on adapting this verifier to wasm and Valida, VMs that take very different architectural approaches than RISC-V.

12 Constanza Gallo – Will your crypto project be censored? Philosophy and practice of censorship

Magazin - Main Stage, 11:30 CEST, Governance & Society

Will your crypto project be censored? Censorship is spreading, from Infura blocking IP addresses, to Github taking the Tornado Cash repo down. This talk will provide a legal anthropological analysis of the elements that might put a project at risk, so that you can take the necessary steps to protect your efforts.

In this talk we want to examine the human and legal elements behind censorship at infrastructure level in order to know how to prevent your project being shut down by governments and/or infrastructure players.

13 Sacha – Emerging interfaces for building web3 applications

Loft - Workshop 0, 11:30 CEST, Infrastructure

New programable interfaces are emerging from the block space created by web3 — being either on-chain, off-chain and cross-chain or a combination of the three.

By breaking down what these interfaces are, this workshop will look into examples of these interfaces, with a focus on cross-chain programmability and the available technologies to choose from.

14 ELIZABETH – Decentralized and Shared Sequencer Architecture

Atelier - Side Stage, 11:30 CEST, Consensus

In this presentation, I'll go over the state of decentralized and shared sequencers for rollups, as well as existing and potential architectures for them. Decentralizing sequencers is needed for rollups to have true decentralization and censorship resistance, and sharing sequencers between rollups opens up the possibility of cross-rollup composability.

15 Parithosh, Barnabas Busa – Testnet or Not, Here We Come: A deep dive into running test networks

Atelier - Workshop 1, 11:45 CEST, Infrastructure

Post-Merge testnets are a beast to run, this workshop would give you an overview into all the tooling that exists to make this job easier. We would also setup a small testnet during this workshop to help familiarize with the tools.

Testnets are useful for more than Ethereum upgrades or dapps, they can be invaluable in prototyping EIPs and hunting for security issues. This workshop will deep dive into the extensive tooling we have for single host and multi host testnets, aiming to showcase our preferred options for various usecases.

16 ESKIMOR – Parachain Consensus from the Ground Up

Magazin - Main Stage, 12:00 CEST, Consensus

We will start with a problem statement and build up together how Parachain Consensus works. If time permits, we can also cover current work like asynchronous backing and time disputes.

17 Will Scott – Metadata-private data transfer

Atelier - Side Stage, 12:00 CEST, Networking

Metadata privacy is critical for personal and private data access. Today, mixnet-like systems are still the only privacy option for low latency data transfer that have been proven at scale. Other techniques are not far behind though, and can allow us to get similar or stronger privacy guarantees without sacrificing latency. I've advised a funding program over the last year aimed at supporting the transition to practice of private retrieval. This talk will survey currently available systems, and our current guesses for what methods can scale to widespread adoption.

Last year, Protocol Labs launched a funding program for metadata-private data transfer. This program is rooted in the belief that a combination of cryptographic and systems techniques should be able to offer low latency private data transfer at scale.

We have worked with groups investigating paths by which PIR, Private set intersection, Multiparty Computation, trusted hardware, and homomorphic encryption can be applied to this problem. This talk will describe the state of the art, overhead costs, and promise of these various techniques.

We'll also look at ways in which the the problem can be relaxed. Traditionally, data transfer has focused on a web2 model of a single authoritative origin. Using content addressed data means both that integrity (...)

18 AUSTINGRIFFITH – Developer Tooling, Education, and Funding

Loft - Workshop 0, 12:15 CEST, Infrastructure

Modern decentralized app stack, ethereum dev eduction, and streaming developer UBI.

Scaffold-eth-2 is a modern dapp stack and I'll demo how to get started shipping. SpeedRunEthereum.com is an educational journey for developers learning web3. BuidlGuidl DAO is streaming ETH to developers as UBI using special cohort streams.

19 TOMAKA – Creating a browser-embedded light client: a post-mortem

Magazin - Main Stage, 12:30 CEST, Networking

Smoldot is a JavaScript package containing a light client for the Polkadot network, that can run from within a web page. Its development, which started nearly 4 years ago, was no easy feat. This talk is a post-modern that will go over the challenges that have been encountered and how we solved them.

Creating a light client that can run from within a web browser presents a lot of engineering challenges, ranging from connectivity to maintaining a low CPU profile. This talk will present all these challenges, explain all the technological choices that we made, and why we had to write a brand new client from scratch.

20 Garrett MacDonald – Permanent Decentralized Storage: The use case of verifiably backing up external chain state

Atelier - Side Stage, 12:30 CEST, Databases

"If a file isn't backed up, it isn't your file" preceded "Not your keys, not your crypto", but it's important to look back to the Web1 figure of speech as it applies to Web3. If you have a multi-billion dollar protocol, it's a good idea to back it up.

I will briefly introduce Arweave as the permanent data storage layer of choice for many networks, and dive into the use case of Kyve.network, and how it is useful and prudent to store any other network's chainstate history in this way - particularly if a subject network discards data (as Ethereum is considering) this becomes important for historical and even accounting purposes.

21 Susannah Evans, Charleen Fei – Crossing Chains with Confidence: Unlocking Smart Contract Users through IBC Actor Callbacks

Magazin - Main Stage, 13:00 CEST, Networking

In this talk, we will explore the significance of actor callbacks, a critical extension to the Inter-Blockchain Communication (IBC) protocol. Actor callbacks provide a standardized interface that allows smart contracts to confirm the occurrence of a cross-chain actions. We will delve into the practical implications of this extension, showcasing how it enhances the workflows of inter-chain transactions. With actor callbacks, it is possible to transfer tokens and perform an action with the tokens combining the utility of transfer and general message passing across chains.

22 PROTOLAMBDA – Evolution of Optimistic Rollup proofs

Atelier - Side Stage, 13:00 CEST, Consensus

L2 Rollups are a core component of the Ethereum scaling strategy, and the security landscape is actively changing. This talk compares the different optimistic rollup proving methods, how EIP-4844 data-availability affects a proof, and how the proof itself can be designed with the latest L2 tech.

This talk is about proving methods, EIP-4844 proof support, and the latest R&D that includes a new bisection-game, pre-image oracle and proof VM (MIPS + experimental RISC-V). All open-source, open specs, and with future-compatibility for a multi-proof security approach: enabling L2 security improvements through the same principles as L1 client-diversity.

23 Laurence Kirk – Essential Maths for Zero Knowledge Proofs

Loft - Workshop 0, 13:30 CEST, Cryptography

A workshop explaining the essential maths needed to understand zero knowledge proofs.

his interactive workshop will go through the maths needed for zero knowledge proof creation and verification. It will cover

- Background cryptography / number theory
- Polynomial theory
- Commitment Schemes
- A run through of the zkSNARK and zkSTARK process
- Optimisation techniques used in popular protocols.

24 Federico Kunze Küllmer – Dynamic IBC: the new wave of dApp composability

Magazin - Main Stage, 13:30 CEST, Infrastructure

Until now, interoperable applications using IBC could only be built by launching your own chain on Cosmos. The new Dynamic IBC (dIBC) creates new possibilities for smart contracts to create their own data packets and compose with other dApps and appchains to unlock a new battery of use cases in web3.

25 Igor Mandrigin – Blockchain node DB designs: from Geth to Erigon

Atelier - Side Stage, 13:30 CEST, Databases

One of the definite feature of Erigon is how it stores blockchain state and state history in its own database. In this talk I will talk about the details, the database choices and the path the Erigon team took to go from the Geth data model into its own.

26 Max Inden – libp2p Workshop - Building a Peer-to-Peer Chat Application in Rust

Atelier - Workshop 1, 13:45 CEST, Networking

libp2p is a peer-to-peer networking library. We will build a chat app using the Rust implementation of libp2p. Our application will allow anyone with internet access across the globe to communicate. The workshop will give hands-on experience on how to build peer-to-peer vs. client-to-server.

27 Viet – Testing large scale networks with Testground

Atelier - Side Stage, 14:00 CEST, Infrastructure

We will explore the features and benefits of Testground, and demonstrate how it can be used to test distributed systems in a controlled and reproducible environment at scale.

In addition, we will cover test planning and strategies that worked for Celestia team that other protocol teams can take home as good point to start fresh.

In this presentation, we will introduce Testground and its key features, including its modular architecture, flexible testing parameters, and support for multiple languages and testing frameworks. We will also demonstrate how Testground can be used to test and optimize large-scale distributed systems, such as peer-to-peer networks, mempool, consensus algorithms.

Finally, we will discuss best practices for using Testground, including how to design effective test plans, how to interpret test results, and how to integrate Testground into existing testing workflows.Whether working on a client implementation or studying performance of the chain, Testground can help you test and validate systems at scale with different known telemetry/collection techniques and technologies.

28 Lefteris Karapetsas, Yabir Garcia, Konstantinos Paparas – The problem of historical data availability in EVM chains

Loft - Workshop 0, 14:15 CEST, Infrastructure

This presentation will try to explain what the problem of historical data availability is in EVM chains, why it exists and how we can try to tackle it.

Given an ethereum address, get all transactions involving it. Such a simple and fundamental thing to ask, though all EVM chains and other EVM inspired chains clients simply can't answer this easily.

The way the node client is built it's unable to provide this answer which has given raise to a host of problems as new protocols and indexing services arise to fill in the gap. As ethereum protocol development enters its 10th year the problem seems to be ignored and sweeped under the rug, such as with the removal of archive nodes.

All the above leads to a very unfortunate centralization of what was supposed to be a decentralized protocol. In the talk we will try to analyze the problem, some existing solutions and approaches and how we can do better so that ethereum can go into the next 100 years and have historical data available.

29 TINA – A Future to Protocol Upgradability

Atelier - Side Stage, 14:30 CEST, Governance & Society

Discussing our current protocol upgradability governance practices (pausability, timelocks, emergency operational procedures) and how we can move towards more sustainable on-chain consensus-driven governance as a path to decentralized protocol governance.

30 Gavin Wood – Agile Coretime: A Periodic, Sale-based Method for Assigning Polkadot Coretime

Magazin - Main Stage, 14:30 CEST, Consensus

The "Polkadot Ubiquitous Computer" (or just Polkadot UC), represents the public service provided by the Polkadot Network: it is a trust-free, WebAssembly-based, multicore, internet-native omnipresent virtual machine which is highly resilient to interference and corruption. The present system of allocating resources of the Polkadot Ubiquitous Computer (parachain slot auctions) is based on a model of one-core-per-parachain: this is a legacy interpretation of the Polkadot platform and is not a reflection of its present capabilities. With Polkadot's capability to adapt to its users'need, a new paradign for allocating coretime is being implemented by ecosystem teams. Coretime on the Polkadot UC is envisioned to be sold by the Polkadot System in two separate formats: Bulk Coretime and Instantaneous Coretime. When a Polkadot Core is utilized, we say it is dedicated to a "Task" rather than a "parachain". The Task to which a Core is dedicated may change at every Relay-chain block and while one predominant type of Task is to secure a Cumulus-based blockchain (i.e. a parachain), other types of Tasks are envisioned. Bulk Coretime is sold periodically on a specialised system chain known as the "Coretime-chain" and allocated in advance of its usage, whereas Instantaneous Coretime is sold on the Relay-chain immediately prior to usage on a block-by-block basis.

This talk aims to explain this paradigm change (...)

31 D. – The Anoma Protocol and its Design Process

Atelier - Side Stage, 15:00 CEST, Networking

This talk will give an introduction to the Anoma protocol architecture and its design process, to share what we learned and elicit feedback on how we could improve both.

Anoma is a distributed operating system for intent-centric counterparty discovery and privacy-preserving computation on linear and non-linear resources with heterogenous trust assumptions.

The protocol architecture has the following (non-exhaustive) goals and design process behind it:

Goal: Identify good component boundaries, to unbundle features and improve modularity.
Process:

- Analyze the outcomes of protocols that came before us, learn from their successes and problems.
- Example components: Consensus Algorithms, Network Transport, Programming Environment, State Machines

Goal: Maximize composability of components.
Process:

- Try to bridge the gap between real world systems and models from Programming Language Theory, Automata Theory and Category Theory.
- Come up with implementation agnostic interfaces using above theory.

Goal: Maximize flexibility of the protocol stack, since changes in a deployed system are costly, proportional to the significance of the change. (...)

32 Mario Havel – Ephemery: Disposable public testnet

Loft - Workshop 0, 15:00 CEST, Infrastructure

Introduction to Ephemery, a novel approach to testnets which enables a single testing infrastructure consisting of ephemeral networks with deterministic parameters.

Ephemery is an automatically reset testnet with each network iteration is created by a specified function which deterministically generates new genesis states. This kind of testnet can provide an alternative environment for short-term testing of applications, validators and also breaking changes in client implementations. It avoids issues of long running testnets which suffer from state bloat, lack of testnet funds or consensus issues. Periodically resetting the network back to genesis cleans the validator set, returns funds back to faucets while keeping the network reasonably small for easy bootstraping.

Test your applications, validators, client implementations or contribute to the testnet at ephemery.dev.

33 Anirudha Bose – Roll your own crypto

Atelier - Workshop 1, 15:15 CEST, Cryptography

Elliptic curve cryptography underpins the trillion dollar economy of cryptocurrencies. But it's often seen as some sort of sorcery, meant only for experts. While it's true that cryptography is a minefield, and therefore you should *never roll your own crypto* , it's still a useful method to build an understanding of cryptocurrencies from first principles.

In this workshop, we'll cover basic algebra necessary to get a theoretical understanding of elliptic curves, and learn how they are used for signing and verifying transactions. We'll then put this theory to practice by rolling our own toy implementation of the elliptic curve used in Ethereum and Bitcoin.

We'll cover the following topics during the workshop, although not in the same order. Please note that this programme may be subject to minor changes.

Foundational stuff

- Introduction to elliptic curves
- Field and group theory
- Elliptic curves under the hood
- Signature and verification (ECDSA)

Practical stuff

- Representing elliptic curves in code
- Implementing primitives for elliptic curve operations
- Implementing ECDSA (...)

34 Philipp Kant – Recursive SNARKs for Efficiency, Scalability, and Privacy

Atelier - Side Stage, 15:30 CEST, Cryptography

Blockchains, with their primary focus on decentralization, open participation, and resilience, inherently lack efficiency, scalability, and privacy. Similar to parallel computing algorithms, the scalability of a blockchain-based system depends on the extent to which computational tasks can be moved off-chain. Zero knowledge techniques, such as recursive SNARKs, offer an effective means of shifting computation off-chain, requiring only proof verification as part of the consensus process. Mina demonstrates the use of these techniques in its consensus algorithm Ouroboros Samasika and zkApps. Privacy poses a challenge in blockchain systems due to their open public ledgers. However, zero knowledge proofs enable reduced data exposure on the public ledger and allow fine-tuning of the level of disclosure. Etonec's payment system serves as an exemplary application showcasing enhanced privacy in blockchains.

35 Molly Mackinlay – Inter-Planetary Consensus: Scaling the open data economy

Magazin - Main Stage, 15:30 CEST, Consensus

Consensus poses a major scalability bottleneck in blockchain networks - hampering web-scale applications like Twitch, Twitter, Tiktok, or web3 alternatives to scale within web3. Interplanetary Consensus (IPC) is a new framework to enable on-demand horizontal scalability of Filecoin to meet web-scale application demands - unlocking an open data economy of composable subnets for scalable computation, fast data retrievals, application-specific gaming networks, and more on the Filecoin network.

IPC unlocks deploying subnets (self-governing chains) that spawn their own state, validate messages in parallel, and seamlessly interact with any network in the hierarchy, as well as with the Filecoin root network. Subnets can run different consensus algorithms, depending on application requirements.

IPC builds upon the Filecoin Virtual Machine launched in March 2023 - providing a framework to further program the Filecoin network, accommodating a variety of use cases while overcoming potential consensus bottlenecks, to load balance decentralised applications by spawning new blockchain substrates on-demand, and to tailor the system to better fit application needs. If you're interested in bringing IPC+FVM to your network - get in touch!

36 Afri Schoedon, Parithosh, Barnabas Busa – The Holešky Testnet Launch Hangout

Loft - Workshop 0, 15:45 CEST, Infrastructure

Coincidentally, the Holešky testnet is scheduled to launch during the Protocol Berg conference. Let's put it on screen and chat about testnet infrastructure.

The first long-standing, merged-from-genesis, public Ethereum testnet. Holešky will replace Goerli as a staking, infrastructure and protocol-developer testnet in 2023.

https://github.com/eth-clients/holesky

37 DAPPLION – Whisk: returning privacy to Ethereum proposers

Atelier - Side Stage, 16:00 CEST, Consensus

Proposal for Whisk: a privacy-preserving protocol for electing block proposers on the Ethereum beacon chain designed by George Kadianakis.

The beacon chain currently elects the next 32 block proposers at the beginning of each epoch. The results of this election are public and everyone gets to learn the identity of those future block proposers. This information leak enables attackers to launch DoS attacks against each proposer sequentially in an attempt to disable Ethereum. To fix this issue a SSLE strategy is proposed. Whisk is a privacy-preserving protocol for electing block proposers on the Ethereum beacon chain designed by George Kadianakis.

38 Barnabé Monnot, Sam Hart, Jannik, Robert Habermeier, Christopher Goes – The Blockspace Expo

Magazin - Main Stage, 16:30 CEST, Consensus

Protocol researchers and developers from distant ecosystems gather to talk about their blockspace.

We present a workshop centred around blockspace and its provision in four different ecosystems. Blockspace is the key resource supplied by blockchains, which allows users to transact. Considerable infrastructure has now seen the light of day towards refining blockspace and delivering more value across the stack, from users to the protocol. But blockspace is not an homogenous resource, being deeply tied with both the consensus protocols which supply it and the infrastructure which refines it. Comparing notes between ecosystems will allow us to uncover best practices and opportunities to learn from one another.

Our workshop will feature researchers and developers from four different ecosystems, represented by: Robert Habermeier (Polkadot), Sam Hart (Skip Protocol), Jannik Luhn (Shutter Network), and Barnabé Monnot (Robust Incentives Group @ Ethereum Foundation).

Each speaker will present key facts about their blockspace, its design and its philosophy (4x 8mins each). After these opening remarks, we feature a panel moderated by Christopher Goes (Heliax) to dive into the deep questions (~40 mins). Expect resource pricing, MEV, base-layer encryption, composability and many other themes to be discussed!

39 Dennis Trautwein – The Best of Both Worlds: Exploring the Role of Centralization in IPFS

Atelier - Side Stage, 16:30 CEST, Infrastructure

Web centralization and consolidation have created potential single points of failure, e.g., in areas such as content hosting, name resolution, and certification. The "Decentralized Web," led by open-source software implementations, attempts to build decentralized alternatives. The InterPlanetary File System (IPFS) is part of this effort and provides a fully decentralized object storage and retrieval layer. This comes with challenges, though: Decentralization can increase complexity and overhead, as well as compromise performance, scalability, and system stability. As the lead developers of IPFS, we have therefore begun to explore more hybrid approaches. In this talk, we will discuss the trade-offs, and our implemented and proposed solutions, as well as give an outlook.

40 RENE, NashQ – Running rollups on light nodes

Loft - Workshop 0, 16:30 CEST, Infrastructure

Learn how to run rollup software on a data availability sampling light node.

41 Tim Daubenschütz – p2p set reconciliation as storage-heavy dapp infrastructure 2.0

Atelier - Workshop 1, 16:45 CEST, Networking

With a set reconciliation algorithm built on js-libp2p-gossipsub and using Patricia Merkle Tries Farcaster (and Kiwi News) are pioneering a new type of credible neutral architecture for social+decentralized apps. In this talk, @timdaub will go through the architectural basics of what makes Kiwi News's replication algorithm work and how it uses the Ethereum mainnet for name space management and as a public key registry.

42 Masih Derkani – Indexing the Planet For Good

Atelier - Side Stage, 17:00 CEST, Networking

Immutable and verifiable content plays a key role in shaping the future of knowledge sharing for the good of all. At the same time, content represented in such a way amplifies the importance of routing; hashes are hard to remember, content keeps increasing, data moves and so do peers. This begs the question: how would we find "stuff" fast, efficiently and reliably without enabling centralised snooping? Find out what the InterPlanetary Network Indexer is addressing this issue for IPFS and FileCoin network.

While the benefits of immutable content are undeniable, a key challenge lies in efficient and reliable routing. With content increasing exponentially and data constantly in motion, the need for fast and secure discovery becomes crucial. But how can we achieve this without compromising privacy and falling into centralized surveillance?

In this talk, we will explore IPNI (InterPlanetary Network Indexer) as a solution to address these challenges head-on. We will begin by understanding the role of immutability in shaping the future of the web and why it is crucial for the integrity of content. Recognizing the need to reduce barriers for adoption, we will delve into the strategies employed by IPNI to simplify the process without compromising privacy or enabling centralized snooping akin to analytics platforms of today.

We will discuss cid.contact as one of the largest IPNI (...)

43 Jaya Klara Brekke, Max Hampshire – The Forest That Protects the Public Good: Nym mixnet for Libp2p privacy

Loft - Workshop 0, 17:15 CEST, 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 the Nym mixnet, built with the Nym Rust SDK.

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 presents the cypherpunk principle for understanding the public and private, namely "transparency for the powerful, privacy for the rest of us" - showing how to operationalise this in the context of decentralised infrastructures. The workshop presents the Nym mixnet as a privacy commons for libp2p, a core module for decentralised networking, used by Ethereum consensus clients and beyond. Recently, Chainsafe built a proof of concept integration of Nym for Lighthouse. This workshop will demo working code for running Libp2p traffic through the Nym mixnet, built with the Nym Rust SDK.

Distributed infrastructures suffer from a common vulnerability: that traffic is exposed, can reveal IP addresses and be used to deanonymise operators. This puts both operator as well as nodes at risk of DDoS attacks as well as censorship. Mixnets function like a forest surrounding and sustaining the public goods of such core (...)

44 Yajin (Andy) Zhou – Operation-level Concurrent Transaction Execution for Ethereum

Atelier - Side Stage, 17:30 CEST, Infrastructure

Despite the success in various scenarios, blockchain systems, especially EVM-compatible ones that serially execute transactions, still face the significant challenge of limited throughput. Concurrent transaction execution is a promising technique to accelerate transaction processing and increase the overall throughput. Existing concurrency control algorithms, however, fail to obtain enough speedups in real-world blockchains due to the high-contention workloads.

In this talk, I will propose a novel operation-level concurrency control algorithm designed for blockchains. The core idea behind our algorithm is that only operations depending on conflicts should be executed serially, while all other conflict-free operations can be executed concurrently. Therefore, in contrast to the traditional approaches, which block or abort the entire transaction when encountering conflicts, our algorithm introduces a redo phase to resolve conflicts at the operation level by re-executing conflicting operations only. We also develop a set of data dependency tracking mechanisms to achieve precise identification and speedy re-execution for conflicting operations. We implement a prototype named ParallelEVM based on Go Ethereum and evaluate ParallelEVM using real-world Ethereum blocks. The evaluation results show that ParallelEVM achieves an average speedup of 4.28×. If combined with state prefetching techniques, Parallel (...)

45 Federico Kunze Küllmer, Daniel Burckhardt – Crossing the Interoperability Bridge: A Deep Dive into Building Interoperable dApps with IBC

Atelier - Workshop 1, 17:30 CEST, Infrastructure

This workshop will be led by Federico Kunze Küllmer, who was part of the core team that developed the Inter Blockchain Communication Protocol (IBC). Federico is also the co-founder of Evmos, an EVM compatible blockchain that supports interoperable dApps via IBC. Federico will dive deep into the technical aspects of the IBC protocol, exploring how it enables cross-chain communication and discussing how Evmos simplifies the development of interoperable dApps. Attendees will have the opportunity to learn from the speaker's firsthand experience in implementing the IBC protocol and gain valuable insights into developing successful interoperable dApps using Solidity.

Join us for a comprehensive workshop on writing interoperable decentralized applications using the Ethereum Virtual Machine (EVM) and the Inter Blockchain Communication Protocol (IBC). This deep dive session will explore the key architectural components that enable interoperability between dApps, including a detailed deep dive of the EVM and IBC. The workshop will conclude with a hands-on demo, giving participants the opportunity to develop their own interoperable dApps using Solidity. This is an ideal opportunity for engineers looking to advance their dApp development skills and gain practical experience in the emerging field of blockchain interoperability.

46 Sebastian Buergel – beyond indexers: trustless application data snapshots

Atelier - Side Stage, 18:00 CEST, Infrastructure

I will present a trustless application data snapshot architecture based on on-chain hashed lists. I will also demonstrate an implementation of that architecture that is used by HOPR mix nodes to sync data much faster and with very few on-chain reads. The proposed mechanism is an orders of magnitude improvement in indexing speed at the cost of one on-chain hash + read + write of a single storage slot. Our open source base contract can be easily integrated into other smart contracts and combined with various frontend libraries.

47 Richard Meissner – How to unleash the power of Account Abstraction

Magazin - Main Stage, 18:00 CEST, Infrastructure

EIP-4337 gave some guidelines and visibility for Account Abstraction, but this is only the start. To fully unfold the power of smart contract based accounts it requires careful considerations and good standards. In this talk we want to give an overview on the current state of modular smart contract accounts and how to fully take advantage of the flexibility that comes with them.

Standards allow developers to group behind a common cause and push initiatives forward in a coordinated manner. For Smart Contract based accounts there are very few such standard in use up to this point, notably only ERC-1271 and ERC-4337. There are quite some initiatives around this topic by different teams which are worth taking a look at. In this session we will give an overview of the current state in this area and also outline how the Safe project is designing a protocol for this.

The following topics will be covered in this presentation:

- Recap of current state of Account Abstraction: ERC-1271 and ERC-4337
- The importance of standards for Account Abstraction
- Unleash the power of Account Abstraction: Safe Protocol and ERC-6900

48 Grigoris, Salim Virani – Rawsciousness

Loft - Workshop 0, 18:00 CEST, General

Exploring the Meaning of Existence in a Futuristic Crypto Epoch.

A and B two fictional characters who transcend to a parallel crypto space. After reflecting on each others existence and how they've been communicating, only then are able to reveal the true essence of a decentralised world.

A Short Film (A Non-Dual Media Production) Starring Alice and Bob Sci-Fi 15 min (FSK 12) 4k Language English.

49 Wassim Z. Alsindi – (mis)adventures in governance

Magazin - Main Stage, 18:30 CEST, Governance & Society

Eyewitness Reports from a Decade-Long Unaligned Bystander.

In this presentation, I will draw upon ten years of interdisciplinary research into the social formations around protocol networks.

50 Remco Bloemen – Worldcoin: Maximally private digital identity.

Atelier - Side Stage, 18:30 CEST, Cryptography

With over 2M members Worldcoin has the largest anonymity set for its zero knowledge proof of personhood protocol.

The talk will be about ZK Magic and technical aspects. ZKP was first used by ZCash to create transactional privacy (something we still don't have in Ethereum). Then we got distracted by the scaling problem and started developing ZKRollups. We now even have ZKEVMs. All of these require massive proving servers, and that has been the focus of ZKP development.

But we still need privacy, and for that we need small fast provers that users can run themselves. And it needs to run in the wallets. i.e. in the browser and on their phones. This creates a set of challenges very different from the ones you find in ZKRollups. There are a number of developments, tricks, and research areas that can help devs bring privacy to the users and I will be talking about those.

51 Toby Shorin, Laura Lotti, Sam Hart – The Nature of the Protocol

Magazin - Main Stage, 19:00 CEST, Governance & Society

Since 2019, we've been studying the novel dynamics unlocked by crypto protocols, articulating new mentals model for understanding them, such as "headless brands" and "squad wealth." Since our work on public goods and with our experience as researchers and builders, our thinking has taken a more deeply political turn as we consider the long-term impact of crypto protocols as institutional bodies.

Institutional legitimacy and accountability of actors are problems which recur time and again as critical themes in protocol development and operations. Attempts to solve these problems are very wide-ranging, drawing from notions of the state (DAO constitutionalism) to corporations (coin-voting shareholder governance). As a result, protocol work has become a byzantine maze of narratives and mismatched mental models which are often a poor fit for the technical affordances of blockchains.

In this keynote talk, we will share insights from 5 years of techno-cultural analysis in the crypto space. We'll then present several frameworks that reveal how accountability and legitimacy arise—or don't—in crypto protocols. Drawing from legal and political theory (featuring pirates), we'll share a political philosophy of crypto institutions that will help protocol stewards and core developers understand power, behavioral regulation, and even violence in the nature of the protocol.

52 Afri Schoedon, Franziska Heintel – Closing Ceremony

Magazin - Main Stage, 19:30 CEST, General

In this session, we invite you to grab a closing drink and wrap up the day with us! Learn more about the motivation behind Protocol Berg: What led us to organize this event and why did we decide to set it up as a donation-backed, sponsorless, non-profit event that is free to attend?

We will share our thoughts on event content curation, sponsors, and ecosystem collaboration. We will create transparency over our expenditures and how this event was financed.

We will also touch on the hardships and experiences of organizing a donation-only event, purely brought to you by a group of volunteers, always keeping in mind our goal: putting the attendee experience and content quality first.

A Department of Decentralization event.
https://protocol.berlin/decentralization

This booklet was generated programmatically and is valid without signature. All content was provided as-is by the respective speakers and is truncated to 1423 characters.