
ZCON 1 PROGRAM

NOTES ABOUT THE PROGRAM

Each day will have one track of presentations, all located in Grand Dalmacija.

Workshop locations are to be determined based on demand.

Time is written in 24-hour format.

WiFi Network: Zcon1
Password: Zcon1

PROGRAM KEY

✅ **Registration**
🍽️ **Meal**
🎤 **Presentation**
✍️ **Workshop**

WORKSHOP KNOWLEDGE LEVELS

LEVEL 1
New to cryptocurrency/looking to get started learning

LEVEL 2
Understand basic level concepts of
blockchain and/or encryption

LEVEL 3
Understand intermediate level concepts in Zcash
(ex. how shielded addresses work vs transparent
addresses, understand differences between upgrades)

LEVEL 4
Understand most components of zk-SNARKs
and other advanced cryptography

JUNE 21

16:00-18:30 Hotel Lobby
✅ **Preregistration**

DAY 1 - JUNE 22

08:00-08:50 Jims Foyer
✅ **Registration**

09:00-09:25 Grand Dalmacija
🎤 **Opening Keynote**
Andrew Miller @socrates1024
Zcash Foundation

09:25-09:50 Grand Dalmacija
🎤 **Envisioning Zcash at Global Scale**
Nathan Wilcox @least_nathan
Electric Coin Company

The year is 2030. What do money and cryptocurrency look like in that world? How do we envision Zcash in that world?

09:50-10:15 Grand Dalmacija
🎤 **Scalable Privacy**
Daira Hopwood @feministPLT
Electric Coin Company & Jacaranda Software

An exploration of the design space for scaling Zcash using recursive validation. Previous efforts along these lines, such as Coda, do not hide the transaction graph. I will go into detail about the obstacles to making this approach work in Zcash, and give a strawman design for full transaction validation in SNARK circuits, with preliminary performance estimates.

10:15-10:40 Grand Dalmacija
🎤 **Zcash For Every(One|Where): Creating Shielded Transactions on All The Things!**
Jack Grigg @str4d
Electric Coin Company

One of the many milestones along the path to widespread adoption of Zcash is the ability for everyone — and everything — to easily create shielded transactions. The deployment of Sapling was a huge step in the right direction, but we aren't there yet. In this presentation I will take a look at how far we've come, demonstrate where we are today, and discuss the work that remains to make this our reality.

10:40-11:05 Grand Dalmacija

🎤 **Making Zcash Shine with Rust**

Deirdre Connolly @durumcrustulum & Anna Kaplan @kaplannie
Zcash Foundation

The consensus-compatible Zcash node in Rust is here! The Zcash Foundation and Parity partnered to build a Zcash client in Rust. Building an alternative client for Zcash next to the Electronic Coin Company's zcashd is helpful to decentralize power structures in the Zcash ecosystem and prevent implementation-specific bugs in one client. We will present the development process and show the status of the Rust Zcash client.

11:05-11:20 Jims Foyer

🍽 **Coffee Break**

11:20-11:45 Grand Dalmacija

🎤 **Current State of Zcash Wallets**

Linda Lee @ProbablyLinda
Electric Coin Company

Last year, I said that I'd update the audience on what Zcash wallets looked like in a year. I'm following through! I looked at and evaluated 12+ wallets in the Zcash ecosystem, including the 12 wallets recommended on z.cash. I'll talk about common trends, new features, and my opinions about who the leaders are in the space.

11:45-12:10 Grand Dalmacija

🎤 **ZLiTE: Lightweight Clients for Shielded Zcash Transactions Using Trusted Execution**

Karl Wüst @fldpi
ETH Zurich

To receive shielded transactions in Zcash, the recipient must scan the blockchain, testing for each transaction if it is destined for them, which is not practical for bandwidth-constrained devices. In this talk, we present ZLiTE, a system that allows serving shielded transactions to lightweight clients in a privacy-preserving manner using a Trusted Execution Environment. ZLiTE protects against side-channel leakage and provides a bandwidth-efficient mechanism for the client to keep an up-to-date version of the witness needed to spend the funds they previously received.

DAY 1 - JUNE 22

12:10-12:35 Grand Dalmacija

🎤 **Transaction Linkability in Zcash: Portrait of a Miner in a Landscape**

Daniel Feher
University of Luxembourg

In this talk we first investigate the generic mining landscape and hierarchy of miners in Zcash, as well as the transition from GPUs to ASICs in 2018. We have developed ways to detect hidden ASIC mining, and have studied the centralizing effects of ASICs. Secondly, we explore interactions of mining with the shielded pool of transactions. Finally, we describe how an attacker might use public blockchain information to infer the mining hardware and mining rewards of individual miners, thus affecting the privacy of miners.

12:35-13:00 Grand Dalmacija

🎤 **The State of Privacy in Cryptocurrencies**

Ian Miers @secparam
Zcash Foundation

[redacted]

13:00-14:00 Restaurant Spalatum (third floor)

🍽 **Lunch**

14:00-14:25 Grand Dalmacija

🎤 **Flyclient: Super-Light Clients for Cryptocurrencies**

Benedikt Bünz @benediktbuenz
Stanford University

Flyclients are super light SPV clients that only require nodes to download a polylogarithmic number of block headers. The Flyclient protocol utilizes a novel block sampling approach to ensure that a chain contains sufficient PoW.

14:25-14:50 Grand Dalmacija

🎤 **Sonic — Nearly Trustless SNARK Setups**

Sean Bowe @ebfull
Electric Coin Company

In this talk, Sean Bowe will explain a new zk-SNARK scheme, Sonic, which boasts fast verification and small proof size while maintaining a robust and secure parameter setup process.

14:50-15:15 Grand Dalmacija

🎤 **A Selection of Pairing Based zk-SNARKs**

Mary Maller

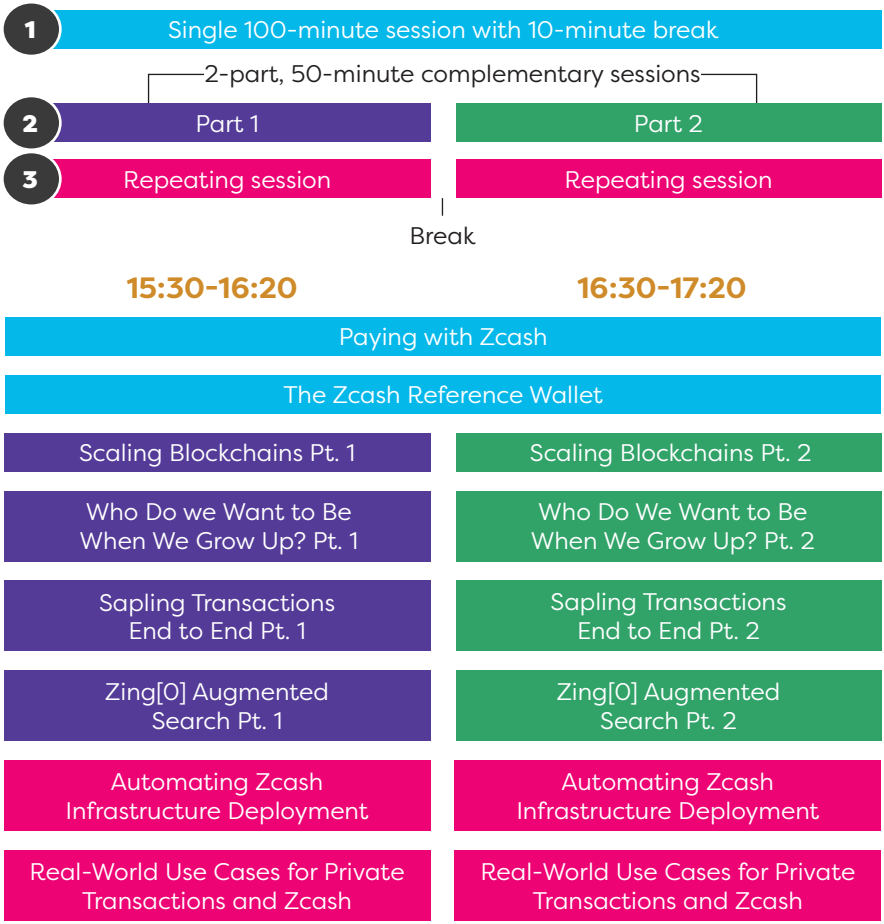
University College London

The applications of zk-SNARKs are becoming ever more prevalent, but different applications have different requirements from the protocols underlying them. In this talk we aim to give a brief overview of the different tradeoffs between a number of pairing based zk-SNARKs in the literature.

15:15-15:30 Jims Foyer

Break to find workshops

How do the workshops work? There are three kinds:



Find workshop details on the following pages.

DAY 1 - JUNE 22

15:30-17:20 SINGLE WORKSHOPS

The following workshops are a single 100-minute session with a 10-minute break. Locations to be determined based on demand.

LEVEL 1

✍️ **Paying with Zcash**

Eric Vaughn @paywithzcash
PayWithZ.cash

This workshop will examine the current trends in cybercoin spending use cases among Zcash and other popular coins, with the objective to learn where Zcash spending is at now and where it can go.

LEVEL 1

✍️ **The Zcash Reference Wallet: Hands-on with the Android SDK**

Joseph Van Geffen @geffenz & Kevin Gorham @anothergmale
Electric Coin Company

Learn how to edit the code and build your own customized personal wallet for Android mobile phones. Both the lead developer and designer from the Reference Wallet team will be on hand to help you customize the code and create an app with your own look and feel. This is a working session, so bring your devices (and have Android Studio installed and updated to save time)!

15:30-16:20 COMPLEMENTARY WORKSHOPS PART 1

The following workshops are part one of two complementary 50-minute sessions. Locations to be determined based on demand.

LEVEL 2-3

✍️ **Scaling Blockchains — Part 1**

Daira Hopwood @feministPLT
Nathan Wilcox @least_nathan
Electric Coin Company

The first session will be about high-level scalability architecture. Ideal participants will have some familiarity with Zcash, Bitcoin, and blockchains, layer 1 scalability, and/or distributed systems. This session will be technical, yet also high-level.

LEVEL 1

✍ **Who Do We Want to Be When We Grow Up? Conscious Community-Building**

Amber Baldet @AmberBaldet
Zcash Foundation

Look at where the Foundation is doing a good job of living up to our goals and where we have a big delta. Brainstorm specific things we could do to close gaps.

LEVEL 2

✍ **Sapling Transactions End to End — Basics of Cryptography**

Elena Nadolinski @leanthebean
Beanstalk

Have you ever wondered how Sapling works? This workshop will go over all the steps of creating a Sapling shielded transaction. Topics include address generation, components of a transaction, note encryption and decryption, view keys and more. All levels of cryptographic knowledge are welcome; everyone will walk away with a better understanding of how Sapling works end to end.

LEVEL 1

✍ **Zing[0] Augmented Search Without Loss of Privacy — Part 1**

Za Wilcox
Zing[0] Labs

Zing[0] leverages the unique privacy properties of Zcash to provide enhanced search results without nonconsensual use of the searcher's data.

15:30-16:20 REPEATING WORKSHOPS

The following workshops will be 50-minute sessions repeated after the break. Locations to be determined based on demand.

LEVEL 3

✍ **Automating Zcash Infrastructure Deployment**

Ian Munoz @IanAMunoz
Independent

A brief overview and guide to using container orchestration to deploy various components of the Zcash ecosystem.

DAY 1 - JUNE 22

LEVEL 1

✍ **Real-World Use Cases for Private Transactions and Zcash**

Ruben Galindo Steckel @rubengsp
ZEC fan, promoter, and partner

Anywhere crypto is a threat to local monetary policy (i.e. anywhere there are currency or capital controls), there will be restrictions on the exchange of local money for crypto. In Venezuela, Airtm was targeted by the Maduro government as a terrorist organization for making it easy for Venezuelans suffering the ravages of hyperinflation to preserve their wealth in digital dollars via a peer-to-peer exchange made possible by cryptocurrency. Any entrepreneur thinking about implementing a privacy technology can speak to Ruben about usability and value by the people living in places where basic human rights are not respected. He will gladly connect you with real-world users to demo your technology or help you come up with a go-to-market strategy.

16:20-16:30 Jims Foyer
Break to switch workshops

16:30-17:20 COMPLEMENTARY WORKSHOPS PART 2

The following workshops are part two of two complementary 50-minute sessions. Locations to be determined based on demand.

LEVEL 4

✍ **Scaling Blockchains — Part 2**

Daira Hopwood @feministPLT
Nathan Wilcox @least_nathan
Electric Coin Company

The second session will be explicitly about using zk-SNARKs as a building block for scalability designs. This will be highly technical and assume some familiarity with zk-SNARKs.

LEVEL 1

✍ **Who Do We Want to Be When We Grow Up? Foundation Activities and Governance**

Amber Baldet @AmberBaldet
Zcash Foundation

Review what the Foundation has done this year and why, share plans for next year, and take suggestions.

LEVEL 3-4

✍️ **Sapling Transactions End to End — Advanced**

Elena Nadolinski @leanthebean
Beanstalk

Have you ever wondered how Sapling works? This workshop will go over all the steps of creating a Sapling shielded transaction. Topics include address generation, components of a transaction, note encryption and decryption, view keys and more. All levels of cryptographic knowledge are welcome; everyone will walk away with a better understanding of how Sapling works end to end. This session will be more introductory, going over the basics of cryptography, what shielded/transparent transactions are, and how the wallets are different etc and then diving into specifics. The second session a bit more advanced skimming over the basics from the previous one and focusing more on the advanced topics.

LEVEL 3

✍️ **Zing[0] Augmented Search Without Loss of Privacy — Part 2**

Za Wilcox
Zing[0] Labs

Zing[0] leverages the unique privacy properties of Zcash to provide enhanced search results without nonconsensual use of the searcher's data.

18:00-19:00 Grand Dalmacija Terrace

🍽️ **Welcome Reception**

DAY 2 - JUNE 23

09:00-09:05 Grand Dalmacija Terrace

🎤 **Day 2 Opening Remarks**

Josh Cincinnati @acityinohio
Zcash Foundation

09:05-09:30 Grand Dalmacija

🎤 **Agoric, Smart Contracts, and Confidentiality**

Dean Tribble @DeanTribble
Agoric

Agoric status update and live demo.

DAY 2 - JUNE 23

09:30-09:55 Grand Dalmacija

🎤 **The State of the STARK**

Eli Ben-Sasson @EliBenSasson
Zcash & StarkWare

This talk will survey the latest progress, applications, and challenges along the road to adopting zk-STARKs in blockchains. First on Layer 2 (StarkDEX and StarkPay) and later (hopefully) as the Layer 1 solution for privacy at scale.

09:55-10:20 Grand Dalmacija

🎤 **Constructing a Fast Prime-Order Group**

Henry de Valence @hdevalence
Zcash Foundation

Decaf and Ristretto provide a construction of a prime-order group with a canonical, non-malleable encoding and other desirable properties, while retaining all of the speed and safety advantages of non-prime-order Edwards curves. In this talk, we will review the construction of Decaf and Ristretto, with a particular focus on the construction of the ristretto255 group, and consider how to apply these techniques to the arithmetic circuit context, where it turns out Decaf provides even greater advantages than in the software context.

10:20-10:45 Grand Dalmacija

🎤 **ZEXE: Enabling Decentralized Private Computation**

Pratyush Mishra @zkproofs
UC Berkeley

In this talk, I will introduce ZEXE, a system for conducting privacy-preserving decentralized computations using zero-knowledge proofs. I will focus on how one can use the strong privacy, expressivity, and efficiency guarantees of ZEXE to realize privacy-preserving analogues of popular applications, such as private user-defined assets, regulation-friendly private stablecoins, and private decentralized exchanges that allow users to trade these while providing front-running resistance.

10:45-11:00 Jims Foyer

🍽 **Coffee Break**

11:00-11:25 Grand Dalmacija

🎤 **The Mobile Wallet Tarpit**

Justin Smith @rusticbison
XMR Systems LLC

Few smartphone wallet apps are delivering the financial sovereignty and privacy benefits that their users imagine they are receiving. Why is it so difficult to extend financial privacy and sovereignty to mobile wallet app users, and what are the practical limitations to delivering these benefits in a smartphone app format? Where might smartphone wallet app development which focuses on financial privacy and sovereignty be headed? We will look at real-world examples to explore the answers to these questions.

11:25-11:50 Grand Dalmacija

🎤 **Tips and Tricks for Improved User Experience with ZKPs**

Bryant Eisenbach @fubuloubu
GunClear

At GunClear, we designed a privacy protocol using multiple separate ZK proof designs that allow ownership records for a firearm to be securely and privately transferred, ensuring both parties in the transaction have the necessary authorizations to participate without leaking identity. We will walk through the design process of our proof system and show how we composed these separate proofs together to ensure a rigorous and strong guarantee at the time of transaction while maintaining an adequate user experience during proof generation.

11:50-12:15 Grand Dalmacija

🎤 **ZKVM: Fast, Confidential Smart Contracts**

Cathie Yun @cathieyun & Oleg Andreev @oleganza
Interstellar

In our talk, we present ZkVM — an experimental multi-asset blockchain architecture for scalable and confidential smart contracts. ZkVM transactions contain programmable constraints over encrypted data and assets. ZkVM protects privacy of accounts and balances, has flexibility for building realistic higher-level protocols, and verifies transactions in milliseconds.

12:15-12:40 Grand Dalmacija

🎤 **ZK for the Enterprise — Quod Erit Demonstrandum (What Will Need to Be Proven)**

Jonathan Rouach @jonrouach
QEDIT

Challenges for deploying zero-knowledge in enterprise networks, or how can we assure that this new technology can be trusted, properly set up, and maintained.

DAY 2 - JUNE 23

12:40-13:40 Restaurant Spalatum (third floor)
🍽 **Lunch**

13:40-14:05 Grand Dalmacija
🎤 **Semaphore Roadmap for Ethereum**
Barry Whitehat @barrywhitehat
Ethereum Foundation

We will discuss: 1) How we can get reasonable privacy in Ethereum when there are a lot of different tokens. 2) Privacy for things other than money like votes, signals, and DAOs. 3) How we can use the same circuit for both — just change the smart contract. 4) And more!

14:05-14:30 Grand Dalmacija
🎤 **A Framework for Post-Quantum Succinct Arguments**
Alessandro Chiesa
UC Berkeley

In this talk, I will describe how one can combine cryptographic hash functions and probabilistic proofs to obtain efficient constructions of zk-SNARKs that are plausibly post-quantum.

14:40-15:30	15:40-16:30
Remittances — Design Sprint	
Toward Cross-Chain Interoperability with Zcash	
Evolving Beyond the Privacy Narrative	
ZKProof Standards Discussion Pt. 1	ZKProof Standards Discussion Pt. 2
Introduction to Programming zk-SNARKs with ZoKrates	ZoKrates Applications: zk-SNARKs in the Context of dApps
End-to-End Privacy for Cryptocurrency Subscription Payments Pt. 1	End-to-End Privacy for Cryptocurrency Subscription Payments Pt. 2
Lessons Learned from Benchmarking SONICs	Lessons Learned from Benchmarking SONICs
Mix Network Workshop Discussion	Mix Network Workshop Discussion

Find workshop details on the following pages.

14:30-14:40 Jims Foyer
Break to find workshops

14:40-16:30 SINGLE WORKSHOPS

The following workshops are a single 100-minute session with a 10-minute break. Locations to be determined based on demand.

LEVEL 1

✍️ **Remittances — Design Sprint**
Elena Giralt @elenita_tweets
Independent

Remittances have been an oft-cited use case for blockchain and cryptocurrencies. In this workshop, we will go over the remittance market, identify user needs, build empathy, and sketch out prototype ideas based on a design sprint format.

LEVEL 3

✍️ **Toward Cross-Chain Interoperability with Zcash**
Matt Luongo @mhluongo & James Prestwich @_prestwich
Thesis.co

Discussing cross-chain interopability efforts with Bitcoin and other "easier" chains. What do we need to do to make these efforts compatible with Zcash?

LEVEL 1

✍️ **Evolving Beyond the Privacy Narrative**
Josh Swihart @jswihart
Electric Coin Company

Depending on your language and home country, Zcash is recognized as a "privacy coin," "anonymous coin," or even a "dark coin." Based upon persona work and recent conversations that include businesses in the EU and regulators in Asia, we'll work through language, positioning, and engagement that we can collectively pursue with digital currency users, businesses, and regulators to reframe the narrative so that privacy becomes an expectation of digital currencies, rather than an edge case.

DAY 2 - JUNE 23

14:40-15:30 COMPLEMENTARY WORKSHOPS PART 1

The following workshops are part one of two complementary 50-minute sessions. Locations to be determined based on demand.

LEVEL 2

✍️ **ZKProof Standards Discussion — zkInterface: A Standard Interoperability Tool**

Daniel Benarroch @BenarrochDaniel & Eran Tromer @EranTromer
QEDIT and Zcash Foundation

We will use the time to follow up on discussions that took place at the 2nd ZKProof Workshop, about interoperability, domain-specific languages, and other topics, as prefered by the audience. We will take the opportunity to improve the existing proposals or to add content to the ZKProof Community Reference document. Join the workshop if you want to contribute to standardizing zero-knowledge proofs.

LEVEL 2

✍️ **Introduction to Programming zk-SNARKs with ZoKrates**

Stefan Deml @stefandeml
& Jacob Eberhardt @Jacob_Eberhardt
Ethereum Foundation

In this workshop, we provide a hands-on overview of ideas, building blocks, design considerations, and challenges when programming zk-SNARKs with ZoKrates. We give an overview of ZoKrates as a DSL and toolbox for zk-SNARKs on Ethereum, and introduce implementations of reusable cryptographic primitives. Furthermore, we explain how in-circuit and off-circuit logic interacts and which pitfalls to avoid when using zk-SNARKs in decentralized applications.

LEVEL 3

✍️ **End-to-End Privacy for Cryptocurrency Subscription Payments: Improving P4 (Private Periodic Payments Protocol) — Current Questions and Challenges**

Liz Steininger @liz315
Least Authority

I'll do a quick overview of current questions and challenges (with slides), then jump into the workshop part of solving these problems (use of Zcash shielded transactions, use of the Zcash encrypted memo field, use of other privacy coins and solutions).

14:40-15:30 REPEATING WORKSHOPS

The following workshops will be 50-minute sessions repeated after the break. Locations to be determined based on demand.

LEVEL 4

✍ **Lessons Learned from Benchmarking SONICs**

Alexander Vlasov @shamatar
Matter Labs

Universal CRS or linear size is an amazing achievement of the SONIC proof system. Both Sonics and proofs systems like Groth16 or GM17 (that are mostly used now) start with R1CS for circuit description, but differ completely under the hood. In this workshop those differences will be highlighted, along the corresponding performance tradeoffs and various operation modes.

LEVEL 1

✍ **Mix Network Workshop Discussion**

David Stainton @david415
Panoramix

Let's have an open discussion about privacy considerations, especially network-level privacy. We will discuss various desired traffic analysis resistance properties and how we can design communications systems to achieve them, with particular focus on solving these design problems with mix networks. My workshop isn't about cryptocurrency, it's about mix networks which are broadly applicable to not only cryptocurrencies but many other applications where users will benefit from reducing the amount of metadata leaked onto the network.

15:30-15:40 Jims Foyer
Break to switch workshops

DAY 2 - JUNE 23

15:40-16:30 COMPLEMENTARY WORKSHOPS PART 2

The following workshops are part two of two complementary 50-minute sessions. Locations to be determined based on demand.

LEVEL 3

✍️ **ZKProof Standards Discussion — Commit and Prove Functionality**

Daniel Benarroch @BenarrochDaniel & Eran Tromer @EranTromer
QEDIT & Zcash Foundation

We will use the time to follow up on discussions that took place at the 2nd ZKProof Workshop, about interoperability, domain-specific languages, and other topics, as prefered by the audience. We will take the opportunity to improve the existing proposals or to add content to the ZKProof Community Reference document. Join the workshop if you want to contribute to standardizing zero-knowledge proofs.

LEVEL 3

✍️ **ZoKrates Applications: zk-SNARKs in the Context of dApps**

Stefan Deml @stefandeml
& Jacob Eberhardt @Jacob_Eberhardt
Provable

In this workshop, we provide a hands-on overview of ideas, building blocks, design considerations and challenges when programming zk-SNARKs with ZoKrates. We give an overview of ZoKrates as a DSL and toolbox for zk-SNARKs on Ethereum and introduce implementations of reusable cryptographic primitives. Furthermore, we explain how in-circuit and off-circuit logic interacts and which pitfalls to avoid when using zk-SNARKs in decentralized applications.

LEVEL 2

✍️ **End-to-End Privacy for Cryptocurrency Subscription Payments: Improving P4 (Private Periodic Payments Protocol) — P4 Overview**

Liz Steininger @liz315
Least Authority

I'll do a quick P4 overview (with slides), then workshop about other business and broader applications of P4, beyond our initial use case with P4.

16:30-17:00

Break — gala begins immediately after the next panel

17:00-18:30 Grand Dalmacija

Privacy Panel with Monero Kon
Amber Baldet (moderating) @AmberBaldet, Zcash Foundation
Jack Gavigan @JackGavigan, Electric Coin Company
Peter Van Valkenburgh @valkenburgh, Zcash Foundation

In conjunction with Monero Kon, this panel will discuss the regulatory and advocacy environment for privacy-preserving cryptocurrencies.

19:00-20:00 Grand Dalmacija Terrace
🍽 **Cocktail Hour**

20:00-21:30 Pool Area
🍽 **Gala Dinner**

DAY 3 - JUNE 24

09:00-09:05 Grand Dalmacija
🎤 **Day 3 Opening Remarks**
Josh Cincinnati @acityinohio
Zcash Foundation

09:05-09:30 Grand Dalmacija
🎤 **Responsible Disclosure in Cryptocurrencies**
Benjamin Winston @industrybambam
Electric Coin Company

Cryptocurrency projects aren't normalized against "standard" information security practice. Much is made of the significant security opportunities that open source presents, but little is said about the pitfalls of trying to apply infosec to distributed OSS, particularly those implementing novel cryptographic protocols with neighboring projects sharing code and implementing the same protocol. In this talk, I describe the current state of security practice in cryptocurrency and the dilemmas Zcash has faced, along with what our answers have been so far. I make calls to action to improve security practice including disclosing to and coordinating with neighboring projects and eventually distributing hitherto centralized security functions.

DAY 3 - JUNE 24

09:30-09:55 Grand Dalmacija

🎤 **ZK Rollup: Ethereum Scalability with ZKPs**

Alex Gluchowski @gluk64
Ethereum Foundation, Matter Labs

Blockchain adoption in the real world is impossible without solving the scalability problem while preserving security and decentralization properties. Zero-knowledge proofs (ZKPs) offer promising new scaling methods. In this talk we will present ZK Rollup, a layer-2 SNARK-based scalability approach.

09:55-10:20 Grand Dalmacija

🎤 **The Next 700 ZKP Programming Languages**

Izaak Meckler @izmeckler
Coda/O(1) Labs

As a community, we have developed acceptably good ways of structuring SNARK programs. However, our understanding of the total design space of programming languages and architectures is pretty limited, and a systematic investigation has not been carried out. The task becomes particularly urgent in the face of the rapidly changing landscape of zero-knowledge proof systems with different computational models and efficiency characteristics. In this talk we highlight what we see as the major parameters in the design space of ZKP programming languages and what the coming years are likely to bring.

10:20-10:45 Grand Dalmacija

🎤 **Governance and Security Concerns**

Ryan Lackey @octal
Tezos Foundation

There is an eternal conflict: Protocols need to evolve over time, but users need certainty about necessary functionality. With blockchains and self-governance, these concerns are even more explicit. We will discuss some concerns and mechanisms for keeping blockchain protocols flexible while still maintaining trust with users. (Basically, showing certain properties to be inviolable or have much higher thresholds to change than others, either built-in mechanisms or via voting blocs.)

10:45-11:00 Jims Foyer

🍽 **Coffee Break**

11:00-11:25 Grand Dalmacija

🎤 **The GDPR and Privacy Impact of Using Zcash Shielded Transactions for SaaS**

Silvan Jongerius @silvanjongerius
TechGDPR

Last year, TechGDPR wrote a report about the GDPR and privacy challenges of using Zcash shielded transactions for recurring payments of a SaaS service. The analysis, commissioned by the Zerocoin Electric Coin Company, looked at the specification of Least Authority's Private Periodic Payment Protocol (P4) to analyze the impact. The lead author of the report will address the findings, challenges, and opportunities during this talk.

11:25-11:50 Grand Dalmacija

🎤 **Money at the Edge: How People Stay Afloat in Venezuela**

Alejandro Machado @alegw
Open Money Initiative

The Open Money Initiative has gone into the field to understand how Venezuelans survive in the midst of heavy capital controls, criminalization of free markets, and hyperinflation. We'll share stories from places like Cúcuta, where worthless bills are used as art and home decor, and Caracas, where individuals are saving in Bitcoin, trading it for local currency only at times of essential purchases. Together, we'll brainstorm how cryptocurrency products and services can be used in places where regimes have a tight grip on society.

11:50-12:40 Grand Dalmacija

🎤 **Governance: How To Lose Friends and Alienate People**

Anna Rose (moderating) @AnnaRRose, Zero Knowledge Summit
Adrian Brink @adrian_brink, Cryptium Labs
Lane Rettig @lrettig, Ethereum
Fredrik Harrysson @fredhrson, Parity

We'll discuss the latest issues facing cryptocurrency governance today, with perspectives from projects on the bleeding edge of both on- and off-chain governance.

12:40-13:40 Restaurant Spalatum (third floor)

🍽 **Lunch**

DAY 3 - JUNE 24

13:40-14:05 Grand Dalmacija
🎤 **Guide to Asia Go-to-Market and Blockchain Community Formation**
Joyce Yang @JoyceInNYC
Global Coin Research

14:05-14:30 Grand Dalmacija
🎤 **State of Electric Coin Company**
Zooko Wilcox @zooko
Electric Coin Company

The Electric Coin Company (ECC) invented Zcash and continues to evolve the protocol, drive adoption, and support the digital currency with world-class cryptographic research, engineering, awareness, regulatory advocacy and community engagement. In this session, ECC CEO Zooko Wilcox will provide an overview of recent ECC efforts, results, and its financial position. He will also outline a potential vision for the future and possible next steps as the company's funding comes to an end late next year.

14:30-14:55 Grand Dalmacija
🎤 **Scaling Zcash Governance**
Josh Cincinnati @acityinohio
Zcash Foundation

A worthy intellectual successor to Locke, Rousseau, Mill, and Rawls, Josh Cincinnati presents a breakthrough form of governance that will revolutionize everything we do. (The veracity of these claims have not be verified by the organizers of Zcon1, a group that confusingly includes Josh Cincinnati himself.)

15:00-16:30
✍️ **Freeform Workshops**

PLEASE FILL OUT THIS FEEDBACK FORM (FRONT AND BACK). RIP PAGE OFF WHEN YOU'RE DONE. TURN COMPLETED FORM AT THE REGISTRATION TABLE AND RECEIVE A THANK-YOU GIFT.

FEEDBACK

Thank you so much for attending Zcon1! We look forward to receiving your feedback.

Overall, how was your experience at Zcon1?

Awful ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Best conference EVER
1 2 3 4 5 6 7 8 9 10

Feel free to comment on your overall experience:

_____

_____

_____

How were the hotel and conference space at Zcon1?
Please include food judgements here as well.

Awful ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Best hotel, conference space, and food EVER
1 2 3 4 5 6 7 8 9 10

Feel free to comment on hotel, conference space, and food here:

_____

_____

_____

How was the presentation content at Zcon1?

Awful ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Best presentation content EVER
1 2 3 4 5 6 7 8 9 10

Feel free to comment on presentation content here:

_____

_____

_____

FEEDBACK (CONT'D)

How was the workshop logistics at Zcon1?

Awful ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 Best workshop logistics EVER

Feel free to comment on workshop logistics here:

_____

_____

_____

How was the logistics and organization at Zcon1?

Awful ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 Best logistics and organization EVER

Feel free to comment on logistics and organization here:

_____

_____

_____

How would you identify yourself?

- ○ Practitioner (engineer, coder, etc)
- ○ Academic researcher
- ○ Community/Governance member
- ○ Business person/Investor
- ○ Media
- ○ Miner
- ○ Student
- ○ Other: _____

Where are you from? (This is to help us understand visa needs.)

- ○ Canada
- ○ United States
- ○ Member state of the EU
- ○ European country not apart of the EU
- ○ Latin America: _____
- ○ Asia: _____
- ○ Oceana (Australia, New Zealand, etc)
- ○ Other: _____