ZCON 3

Presented by the Zcash Foundation

PROGRAM

WIFI network: Palms Meeting
Password: ZCON2022

Masks Required:
Masks are required for all attendees in all sessions and common areas. Masks will not be required during meals including, breakfast, lunch, the welcome dinner, and cocktail receptions. However, they WILL be required when moving around in common areas (like a buffet line). To-go containers will be provided for all meals.

Code of Conduct:
Zcon3 is a safe, harassment-free, and inclusive space and we expect everyone to adhere to our Code of Conduct: 1) Be respectful 2) Assume good faith 3) Be collaborative 4) Try to be concise 5) Transparency 6) Inclusivity. Please find someone with a blue lanyard or go to the info desk to report violations. More details: https://forum.zcashcommunity.com/faq

Discord
To reduce the risk of spreading COVID via mics, both virtual and in-person attendees are to use Discord to ask speakers questions while their session is live and async. Each channel has a session-specific channel - use the "thumbs up" emoji to bump up questions that other attendees ask. You can also converse with the speakers and other attendees on the session topic on the days that surround the talk.

- #lobby: This is where you'll enter the conference and is a great place to introduce yourself.
- #in-person: Private group for only in-person attendees; we will use this channel for announcements & in-person attendee questions about the conference.
- #jobs: For those looking for work or have employment opportunities.
- #technical-off-the-stage: Discuss topics that are not covered in the conference sessions.
- #non-technical-banter: Zebras just want to have fun!
- #help: General conference-related questions.
- To report a Code of Conduct violation tag @Moderator

Included Meals
Conference registration covers your breakfast and lunch each day, a Welcome Reception and dinner on Sunday, August 7th, and a cocktail reception on Monday, August 8th. Coffee and snacks will be provided between sessions.

DAY 1 SUMMARY:

Registration and Breakfast in Grand Ballroom Foyer, 2nd-floor Fantasy tower 8-9 AM. Please also note that there will be a 10-minute break between each session.

TRACK 1: GRAND BALLROOMS

9-9:30 AM
Opening Address
Jack Gavigan

9:40-10:40 AM
Protecting Civil Liberties With Privacy-Enhancing Technology
Kurt Opsahl

10:50-11:20 AM
State of Legislation, Regulation and Policy
Paul Brigner, Kurt Opsahl, Peter Van Valkenburgh, Jack Gavigan

11:30-12 PM
Zebra Update
Teor

12:10-12:40 PM
FROST Research Updates
Chelsea Komlo & Elizabeth Crites

12:40 - 1:40 PM
Lunch Break
Grand Ballrooms Foyer

1:40-2:30 PM
ZCG: Past, Present & Future

2:40-3:40 PM
Orchard Shielded Assets
Daniel Benarroch, Pablo Kogan

3:50-4:35 PM
Zondax HW wallet support: from 0 to Hero
Francesco Dainese & Ida Tucker

4:45-5:30 PM
Advancing Human Rights With Tor
Isabella Fernandes

TRACK 2: HARPER ROOMS

1:40-2:10 PM
FROST Engineering Updates
Deirdre Connolly & Conrado Gouvêa

2:40-3:10 PM
Marketing ZEC
Chris Tomeo

3:50-4:35 PM
Gemini: elastic SNARKs for diverse environments
Michele Orrù

After completing sessions on both tracks, we will take a break then move to Moon Nightclub (accessed via Casino Floor) where we will indulge in a Cocktail Reception (6-7:30 PM) and Welcome Dinner (7:30-9:30)

DAY 2 SUMMARY:

Breakfast will be served at the Grand Ballroom Foyer, 2nd-floor Fantasy tower 8-9 AM. Please also note that there will be a 10-minute break between each session.

TRACK 1: GRAND BALLROOMS

9:00-9:45 AM
Taiga: a dark forest of zero-knowledge programmability
Christopher Goes

9:55-10:40 AM
Tooling for building zkEVM: PIL and Circom
Jordi Baylina

10:50-11:50 AM
The Future of Decentralized Applications on Zcash, a Shared Community Roadmap (workshop)
Daniel Benarroch, Pablo Kogan, Aurel Nicolas

TRACK 2: HARPER ROOM

9:00-9:45 AM
Understanding the Moon Math of ZK Snarks (workshop)
Anna Kaplan & Liz Steininger

9:55-10:25 AM
Building a World Class UX for ZEC
Josh Swihart

10:50-11:50 AM
The Once and Future ECC Wallet (Dev and UX)
Pacu Gindre & Joseph Van Geffen

11:50 - 1:00 PM
Lunch Break: Grand Ballrooms Foyer

Track 1: Grand Ballrooms

1:00-1:30 PM
Proof Carrying Data
Pratyush Mishra

1:40-2:10 PM
Motivations of Proof of Stake
Zooko Wilcox

2:20-3:20 PM
ECC Proof of Stake
Nate Wilcox

3:30-4:30 PM
The Future of Zcash (panel)
Zaki Manian, Daniel Benarroch, Nathan Wilcox, Matthew Green, Jack Gavigan

Track 2: Harper Room

1:00-1:30 PM
Our Oldest Technology
David Boyer & Natasha Mynhier

4:30 - 5:30 PM
60 Minute Break

5:30 - 7:00 PM
Cocktail Reception: Ghost Bar (Accessed via Casino Floor)

DAY 3 SUMMARY:

Breakfast will be served at the Grand Ballroom Foyer, 2nd-floor Fantasy tower 8-9 AM. Please also note that there will be a 10-minute break between each session.

TRACK 1: GRAND BALLROOMS

9:00-9:45 AM
Halo 2 Community Showcase
Ying Tong

9:55-10:40 AM
Securely Scaling Decentralized Governance
Michael Lewellen

10:50-11:35 AM
Governance Panel

11:45-1 PM
Town Hall
Bootstrap and Zcash Foundation Boards

TRACK 2: HARPER ROOM

9-10 AM
A Forest of Levers: The Performance of Orchard
Jack Grigg (Str4d)

10:10-11:10 AM
Explaining the Security of Zcash
Daira Hopwood

TRACK 3: KENNEDY

9:00-9:30 AM
Bridging Sapling: Private Cross-Chain Transfers
Aleixo Sánchez

10:50-11:20 AM
Agoric: Scaling Web3 with JavaScript Smart Contracts
Dean Tribble

1:00-2:00 PM
Lunch Break
Grand Ballroom Foyer

Track 1

2-3 PM
Pool Retirement
Nate Wilcox

3:10-3:55 PM
Free2z: Peer-to-Peer Giving
Skylar Saveland & Jonathan Bird

Track 2

2-2:30 PM
New to Zcash? z2z & learn! (workshop)
Aditya

Once Zcon3 concludes, attendees are welcome to stick around to utilize the space for co-working and socializing

AUGUST 6

4:00 - 7:00PM
Pre-registration
2nd floor Fantasy Tower, Foyer

DAY 1 - AUGUST 7

8:00 - 9:00 AM
Registration
2nd floor Fantasy Tower, Foyer

9 - 9:30 AM
Opening Address
Grand Ballrooms

Jack Gavigan
Zcash Foundation

9:40-10:40AM
Grand Ballrooms

Protecting Civil Liberties With Privacy-Enhancing Technology

Kurt Opsahl
Electronic Frontier Foundation

The importance of protecting and preserving civil liberties through technologies, and the "why" behind financial privacy-the fundamental rights at issue, including avoiding financial censorship and the keeping the power of existing centralized hubs in check. He'll discuss the broader civil liberties context, not just privacy, but free expression (code is speech), due process for government inquiries, and the value of anonymity in effectuating those rights. He'll also talk about how the Zcash community can help protect these rights, with lessons from his work in digital rights advocacy, by learning the issues, building grassroots support and having their voices heard.

10:50-11:20 AM

Grand Ballrooms

State of Legislation, Regulation and Policy (panel)

Paul Brigner, Kurt Opsahl, Peter Van Valkenburgh

Chaired by: Jack Gavigan

A panel discussion on the state of legislation, regulation and policy affecting Zcash, and what role the Zcash community can play in influencing decision-makers to support Zcash's goals.

11:30-12 PM

Grand Ballrooms

Zebra Update

Teor

Zcash Foundation

Zebra is the Zcash Foundation's independent node implementation, currently under development in Rust. Teor will be providing an update on the progress we've made over the past year, as we continue to add more functionality, bringing Zebra closer to parity with zcashd.

12:10-12:40PM

Grand Ballrooms

FROST Research Updates

Chelsea Komlo & Elizabeth Crites

Zcash Foundation

In this talk, Chelsea and Elizabeth will review new research on FROST and variants of FROST, and how this research translates into practice. Finally, they will talk about what is next on the roadmap for multi-party signatures in the Zcash ecosystem and more generally.

12:40-1:40 PM

Lunch break

1:40-2:30 PM

Grand Ballrooms

Zcash Community Grants: Past, Present and Future

Aditya, Brian (aka Wobbzz), Cody Burns, Jason McGee

Chaired by: Hudson Jameson

The Zcash Community Grants (ZCG) Committee will be live in Vegas for Zcon3 to discuss the grants program. Topics include a 2022 grant retrospective, increased outreach efforts to attract high-quality grant applicants, and the Global Ambassador Program. The committee will also explain their new Request for Proposal/Input (RFP/RFI) initiative, which relies heavily on community feedback and seeks to bring in talent and developers to help grow the adoption and usability of Zcash. Current projects include the development of a plug-and-play full node and a coin-weighted polling mechanism. The panel will provide a behind-the-scenes look at the work the committee does that's not always evident from forum posts or meeting minutes, and will be followed by a Q&A session.

1:40-2:10 PM

Harper Room

FROST Engineering Updates

Deirdre Connolly & Conrado Gouvêa

Zcash Foundation

In this talk, Deirdre and Conrado will review the current status of FROST implementations, including our fully-generic library frost-core. They will talk about upcoming work such as integrating FROST into the Zcash protocol and future features, such as distributed key generation.

2:40-3:40 PM

Grand Ballrooms

Orchard Shielded Assets

Daniel Benarroch, Pablo Kogan

QEDIT

Daniel & Pablo will speak about the latest work in Zcash Shielded Assets (Grant), explain the details of the protocol QEDIT designed (and by then) will have implemented, as well as discuss what are the consequences and potential applications that this protocol enables. One of the main goals of this proposal is to enable more dApps and functionality on the Zcash chain to push for adoption. This is the first of many steps in that direction and QEDIT believes all the community should be aware of the specifics and the potential of the Orchard Shielded Assets protocol and applications.

2:40-3:10 PM

Harper Room

Marketing ZEC

Chris Tomeo

Electric Coin Co.

ECC's marketing, research and PR approach, plus planning for growth across different segments.

3:50-4:35 PM

Grand Ballrooms

Zondax HW wallet support: from 0 to Hero

Francesco Dainese & Ida Tucker

Zondax Wallet

After a multi-year effort with lots of hurdles, the Zondax team finally demo the complete Ledger support for shielded transactions in Zecwallet. Francesco and Ida are going to summarize the process, the challenges and the solutions that lead to their success in the final demo.

3:50-4:35

Harper Room

Gemini: elastic SNARKs for diverse environments

Michele Orrù

UC Berkeley

Elastic SNARKs allow the prover to allocate different resources (such as memory and time) depending on the execution environment and the size of the instance. It is this possible to set a memory budget to prove arbitrarily large R1CS instances, and the resulting output is independent of the prover's configuration.

He will present Gemini, an elastic SNARK. He will dive into the streaming algorithms that lead to space-efficient provers, and the implementation challenges we run into while developing space-efficient SNARKs in arkworks.

Joint work with Jonathan Bootle (IBM Research) and Alessandro Chiesa (EPFL).

4:45-5:30 PM

Grand Ballrooms

Advancing Human Rights With Tor

Isabela Fernandes

The Tor Project

The Tor Project is a non-profit that builds Tor, a technology that allows people to be anonymous online, protects their privacy and helps them bypass internet censorship. However, sometimes we think more about the technology and not as much about the people using it. There are many reasons why someone would use Tor, it can be simply because a father is worried about how much the 'internet' will learn about his kids. All the way to a campesino who needs protection while talking with lawyers about crimes committed by the local government. This talk will share some of these stories to help uplift the Tor Project mission, which is to help advance human rights.

5:30-6:00 PM

30-minute break before cocktail reception

6:00-7:30 PM

Moon Nightclub

Cocktail Reception

(Accessed via the Casino Floor using your Zcon3 Name badge as your "ticket")

7:30-9:30 PM

Moon Nightclub

Welcome Dinner

(Accessed via the Casino Floor using your Zcon3 Name badge as your "ticket". To-go boxes provided.)

DAY 2 - AUGUST 8

9:00-9:45 AM

Grand Ballrooms

Taiga: a dark forest of zero-knowledge programmability

Christopher Goes

The Anoma Project

Taiga is a private execution environment designed for fully programmable private transactions, architected around the concept of "validity predicates", boolean functions (instantiated as circuits) given access to state changes which enforce a relation over state transitions. Taiga draws substantial inspiration from Sapling, Orchard, and Zexe, but is written from the ground up to provide full programmable generality for both users and applications. In this talk Christopher Goes will outline the design history, structure, and scope of Taiga, and touch upon their discoveries of design space boundaries faced when architecting programmable privacy using zero-knowledge proofs.

9:00-9:45 AM

Harper Room

Understanding the Moon Math of ZK Snarks (workshop)

Anna Kaplan & Liz Steininger

Least Authority

Are you fascinated by zk-SNARKs and want to learn more about their inner workings? During this interactive workshop, Anna and Liz will focus on the mathematical and cryptographic foundations of zk-SNARKs by focusing on a pen-and-paper approach through every development step of the Groth16 zk-SNARK. Participants should note that learnings from these mathematical basics can be applied not only for understanding zk-SNARKs but also to being able to discuss modern cryptography more generally.

More information, exercises and background material can be found in the MoonMath Manual – to be released by Least Authority in mid-2022.

9:55-10:40 AM

Grand Ballrooms

Tooling for building zkEVM: PIL and Circom

Jordi Baylina

Polygon Hermex

Jordi Baylina is one of the most outstanding members of Ethereum community and part of the White Hat Group. He is the co-founder of iden3 and the main contributor to circom and snarkjs. Currently Jordi is the technical lead at Polygon Hermez building a zkEVM. Jordi will introduce how Polygonis building a zkEVM presenting PIL (Polynomial identity Language) and circom.

9:55-10:25 AM

Harper Room

Building a world class UX for ZEC

Josh Swihart

Electric Coin Company

To date, ECC has discovered and engineered some of the most important cryptographic technology ever built. They birthed the era of zero-knowledge cryptography with Zcash, optimized it with the Sapling upgrade and recently ushered in the next generation of zero-knowledge with Halo on NU5. But groundbreaking tech is not enough. It needs adoption. ECC has recently pivoted its strategy to focus on delivering a world-class UX for ZEC in support of the adoption of the ZEC token for peer-to-peer and Web 3 payments. In this session, Josh will provide an overview of the implications of this strategy shift and the progress ECC's made so far.

10:50-11:50 AM

Grand Ballrooms

The Future of Decentralized Applications on Zcash, a Shared Community Roadmap (workshop)

Daniel Benarroch, Pablo Kogan, Aurel Nicolas

QEDIT

The ZSA proposal project is opening the doors for the Zcash ecosystem to be much more functional and enable all kinds of (privacy) applications on chain. From DeFi, to private governance for DAOs, there are plenty of specific directions that the community can and should take toward that goal.
In this workshop, QEDIT will engage the community in a discussion to try to generate a shared roadmap for which applications are of most importance to all, and what is the path to achieving these. The goal is to have at least one or two teams come out of the workshop with the will to submit a joint grant to work on two or more applications (research, design and implementation).

10:50-11:50 AM

Harper Room

The Once and Future ECC Wallet (Dev and UX)

Pacu Gindre & Joseph Van Geffen

Electric Coin Company

On the eve of the Zcash Mobile Reference wallet's second birthday, join the ECC Wallet Team as they discuss the past and future of the mobile wallet. They will focus on the experience of building the app from scratch, the lessons they learned, and where they plan to go next. They will dig into how NU5 evolved the mobile app and how user feedback in real situations has helped. Additionally, they will expound on future features and known hurdles.

11:50-1 PM

Lunch break

1-1:30 PM

Grand Ballrooms

Proof Carrying Data

Pratyush Mishra

Aleo

Proof-carrying data (PCD) is a powerful cryptographic primitive that enables mutually distrustful parties to perform distributed computations that run indefinitely. However, most existing approaches to constructing PCD that rely on heavy cryptographic machinery such as succinct non-interactive arguments of knowledge (SNARKs) that have a succinct verifier. In this talk, Pratyush will introduce a new paradigm for PCD constructions that relies on much simpler ingredients while simultaneously improving asymptotic and concrete efficiency. This is joint work with Benedikt Bünz, Alessandro Chiesa, William Lin and Nick Spooner. The accompanying papers can be found at ia.cr/2020/499 and ia.cr/2020/1618.

1-1:30PM

Harper Room

Our Oldest Technology

David Boyer, Natasha Mynhier

37 LAINES

Natasha & David will present on their efforts and plans to bring more awareness to Zcash through our Zcash Community Grants funded short documentary. In particular, they will discuss why we believe education about Zcash and financial privacy is one of the most critical areas that needs improving in Zcash. Finally, they will examine their roadmap to create sustainable and entertaining educational content going forward.

1:40-2:10 PM

Grand Ballrooms

Motivations of Proof of Stake

Zooko

Electric Coin Co.

Should the Zcash community move to Proof-of-Stake? Here are the reasons that, in Electric Coin Co's opinion, we should

2:20-3:20 PM

Grand Ballrooms

ECC Proof of Stake

Nate Wilcox

Electric Coin Company

ECC has shared its interest in moving Zcash from a proof-of-work consensus mechanism to proof-of-stake. They started the initial research phase in the Fall with the goal of producing a concrete transition proposal to the Zcash community. This session will provide an overview of their research areas, the preferences they've developed for each, the rationale behind those preferences, and their latest focus and thoughts on proof-of-stake research.

3:30-4:30 PM

Grand Ballrooms

The Future of Zcash (panel)

Zaki Manian, Daniel Benarroch, Nathan Wilcox, Matthew Green
Chaired by Jack Gavigan,

Following the activation of NU5 at the end of May, it's time to consider "What's next?". There is broad support across the Zcash community for moving away from proof of work, and ECC have expressed support for a move to proof of stake. Meanwhile, the QEDIT team are hard at work on adding support for zk-assets to the Zcash protocol. This panel will bring technical leaders from across the Zcash ecosystem together to discuss what major enhancements and changes might be candidates for inclusion in the next few network upgrades.

4:30-5:30 PM

60-minute break before cocktail reception

5:30-7 PM

Ghostbar

Cocktail Reception

(Accessed via the Casino Floor using your Zcon3 Name badge as your "ticket")

DAY 3 - AUGUST 9

9:00-9:45 AM

Grand Ballrooms

Halo 2 Community Showcase

Ying Tong

Electric Coin Company

Since its deployment, the halo2 library has been adopted in projects like the zkEVM (community edition), Orbis, DarkFi, and Filecoin. Ying Tong will highlight a few examples from across the stack, showcasing how the library has been used, modified, and improved by community contributions. She will then discuss active areas of development, upcoming features on their roadmap, and a vision for a community-influenced halo2 ecosystem

9-10 AM

Harper Room

A Forest of Levers: The Performance of Orchard

Jack Grigg (Str4d)

Electric Coin Company

After a brief overview of the Orchard protocol (to provide some context), the first half of the talk will provide a medium-level introduction to Halo 2. Jack will look at how protocols are encoded into PLONK-style circuits, the ways in which they differ from Zcash's previous R1CS circuits, and how the Halo 2 protocol turns circuits into proofs.

9-9:30 AM

Kennedy Rooms

Bridging Sapling: Private Cross-Chain Transfers

Aleixo Sánchez
Web3 Foundation

ZCLAIM is a framework for trustless cross-chain asset migration, achieving wrapped shielded Zcash without revealing the transferred amount to any third party.

9:55-10:40 AM

Grand Ballrooms

Securely Scaling Decentralized Governance

Michael Lewellen
OpenZeppelin

Building governance systems for protocols to handle increasing levels of complex decision-making and security while remaining decentralized at their core is a daunting task. How do you ensure protocol upgrades are secure without gate-keeping? How should proposals be developed, accepted and passed without cumbersome bureaucracy? In this session, Michael will look at how different blockchain protocols and DAOs have approached these problems and what can be learned from them.

10:10-11:10 AM

Harper Room

Explaining the Security of Zcash

Daira Hopwood
Electric Coin Company

This talk is a deep dive into the security properties of the Zcash protocol and the cryptographic assumptions they depend on, in both classical and post-quantum settings. It aims to give an intuitive but detailed explanation of why Zcash is private, maintains balance, and enforces spend authorization.

10:50-11:35 AM

Grand Ballrooms

Governance Panel

Members of the Zcash Foundation and Bootstrap Project boards of directors will be joined by Hudson Jameson to discuss the state of Zcash governance, and how it might evolve in the future.

10:50-11:20 AM

Kennedy Rooms

Agoric: Scaling Web3 with JavaScript Smart Contracts

Dean Tribble
Agoric

An update on Agoric and next steps for interoperation with ZEC

11:45-1 PM

Grand Ballrooms

Town Hall

Chaired by: Peter Van Valkenburgh

Members of the Zcash Foundation and Bootstrap Project boards of directors will answer questions submitted in advance by the Zcash community.

1-2 PM

Lunch break

2-3 PM

Grand Ballrooms

Pool Retirement

Nate Wilcox
Electric Coin Company

A large part of the effort for the latter stages of NU5 development was integrating newer NU5 features with older pre-NU5 technologies. They've already initiated a policy for Sprout that limits transfers into the Sprout pool, but they need a more general set of guidelines for how they might retire older pools and technologies so that they can move faster with engineering efforts and reduce protocol complexity. This session will present some of their thoughts on how this could be accomplished, including a discussion of the social aspects of pool retirement.

2-2:30 PM

Harper Room

New to Zcash? z2z & learn! (workshop)

Aditya
Nighthawk Wallet

Workshop on using Zcash on mobile wallets for newbies or showcase Zcash Wallets and discuss UI/UX & Feedback.

3:10-3:55 PM

Grand Ballrooms

Free2z: Peer-to-Peer Giving

Skylar Saveland & Jonathan Bird

Aspects of integrating Zcash into a traditional website for payments and automation and why it's so easy if you make a few key decisions.

ZCON3

Presented by the Zcash Foundation

Participate in Zcon3 on Discord!