Zcash Foundation Q2 2021 Report

A review of Q2 development, expenses and approved grants.

Q2 REPORT

A WORD FROM OUR EXECUTIVE DIRECTOR

This is our second quarterly report for 2021, coming hot on the heels of our Q1 report. Our goal with these reports is to provide a summary of the Foundation's activities, and an overview of our finances, including a detailed breakdown of our spending. We welcome feedback, so if you have any questions or suggestions, please post them to the **Zcash Community forums!**

The second quarter of 2021 was a period of consolidation and growth for the Foundation. On the engineering front, we welcomed Janito and Conrado, which increased the size of the engineering team to six people. At the leadership level, we hired Alex as the Foundation's chief operating officer. With 25 years experience in the government and non-profit sectors, Alex fills a key gap, in terms of his expertise and experience of running 501(c)(3) organizations.

Having begun approving grants during Q1, the **Zcash Open Major Grants committee (ZOMG)** was very active during Q2, approving sizable grants for ZecWallet, Nighthawk wallet, and Arti, a Rust implementation of the Tor protocol, which will make it easier to integrate Tor into the Zcashd and Zebra node implementations. In total, ZOMG distributed over $625,000 during Q2.

In 2020, plans to hold Zcon (the Foundation's annual conference) in Lima, Peru were scuppered by the pandemic. With ongoing travel restrictions, we decided to make Zcon2 a virtual conference, streamed on YouTube, with audience participation and discussion taking place on Discord. **Zcon2 Lite** duly took place on June 8th and 9th, and all the presentations and panel discussions were recorded and can be watched on **YouTube.** Audience feedback after the event was very positive.

The engineering team's productivity was mildly impacted during Q2 as new team members were onboarded. Work continued on adding support for NU5 validation to Zebra. We also reviewed the roadmap for Zebra, and set a target of late October for the beta release of an "MVP" (minimum viable product) version of Zebra with a functionality scope limited to validating the blockchain, maintaining a mempool, and relaying transactions and blocks (i.e. no mining, wallet or transaction creation functionality yet).

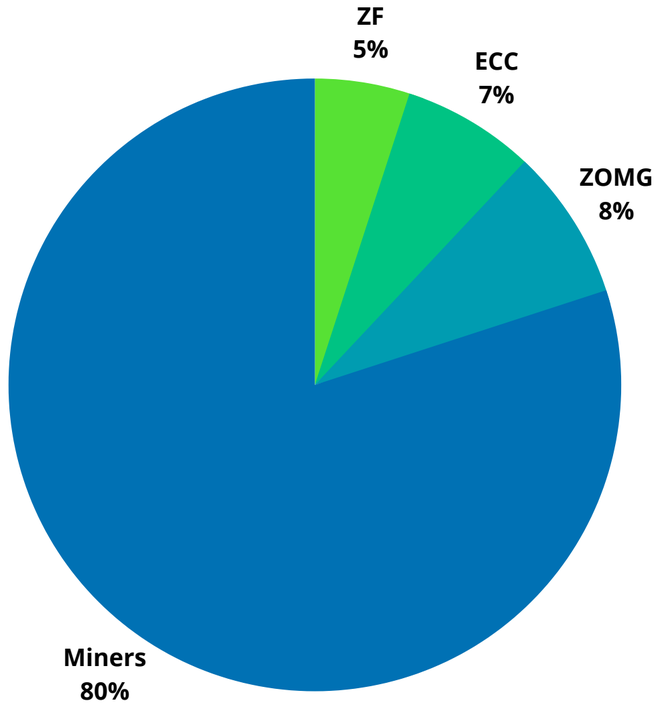
During Q2, the scope of NU5 expanded to include unified address, and the target date for NU5 mainnet activation changed from August 1st to late October, raising the possibility that Zebra may well be active on the Zcash network by the time NU5 activates!

As Q2 ended, the engineering team was looking forward to completing the NU5 validation work, and moving on to building Zebra's mempool functionality. Meanwhile, at the leadership level, it had become apparent that we needed to offer more and better support to ZOMG, and that was our primary focus as we began Q3.

Jack Gavigan - Executive Director

ISSUANCE OF THE ZCASH DEV FUND

- Zcash uses a Proof-of-Work consensus mechanism to produce blocks.
- From the launch of Zcash in October 2016 until November 2020, miners received 80% of the block reward (plus transaction fees). The remaining 20% was allocated to the "Founders Reward", which was distributed to various parties by the Electric Coin Company (ECC).
- **The Founders Reward expired in November 2020 at the first Zcash halving, which occurs every four years.** At that time, block rewards were halved to 3.125 and **a new development fund, as proposed and approved by the community in ZIP 1014, was implemented.**



The new structure stipulates that 80 percent of Zcash issuance continues to be distributed to miners, while 20 percent is devoted to Zcash development funding. **Of this 20%, 5% is allocated to support the work of the Zcash Foundation.** Another 8% of the total block reward (or about 40 percent of the new dev fund) goes towards ZOMG (which is received and administered as a restricted donation by ZF), and the ECC receives 7% of the total rewards.

Q2 '21 - ZF FINANCIAL TAKEAWAYS:

The USD value of funds received and held by ZF during Q2 was calculated using the following Messari closing prices for June 31st:

- **$130.93 USD/ZEC**
- **$35,048.58 USD/BTC**
- **$2,275.72 USD/ETH**

ZF Funds received:

- ZF received **16,285 ZEC ($2,132,154 USD)** from its slice of the Dev Fund during Q2, an average of average of 5,428 ZEC ($710,718 USD) a month.
- ZF realized approximately **$169,556 USD** per month in operating expenses.

Total held at end of Q2:

- ZF held $6,000,090 USD, 130,145 ZEC, 53.46 BTC, and 13 ETH for a total value of **$24,942,991 USD.**

Q2 '21 - ZOMG FINANCIAL TAKEAWAYS:

zomg

ZOMG Funds ZF received in Q2 at USD value were based on the following March 31 Messari closing prices:

- **$130.93 USD/ZEC**

ZOMG restricted funds that ZF received:

- ZF received **26,056 ZEC ($3,411,447 USD)**
- This was at an average of a 8,685 ZEC ($1,137,149 USD) a month of ZOMG restricted funds.
- ZF distributed **2,208 ZEC (valued at $445,029 USD** at the time of payment) and **$181,764 USD in Q2** - of ZOMG restricted funds for grants approved by the ZOMG committee.

Total held at end of Q2:

- ZF held custody of 52,220 ZEC (valued at $6,837,210 USD) and $519,663 USD for a total value of **$7,356,874 USD** restricted for use in funding major grants, as selected by ZOMG.

Q2 REPORT

Q2 (SPRINT 7-8) ENGINEERING OVERVIEW

Sprint 7 →

For our first sprint of the quarter, **Sprint 7,** the team worked on **validation of pre-NU5 consensus rules** as well as continuing to work on **NU5/Orchard updates.** The team also continued to identify and fix security and protocol correctness issues. Additionally, the team published a **Code of Conduct** for the Zebra project.

Sprint 8 →

During our **eighth sprint,** we put aside pre-NU5 work to fully concentrate on **NU5/Orchard,** and fix more security and protocol correctness issues. We also made some **usability improvements to allow Zebra to log to systemd-journald.** Finally, we were also happy to report **best-effort support for Apple M1 builds in Zebra.**

Q2 REPORT

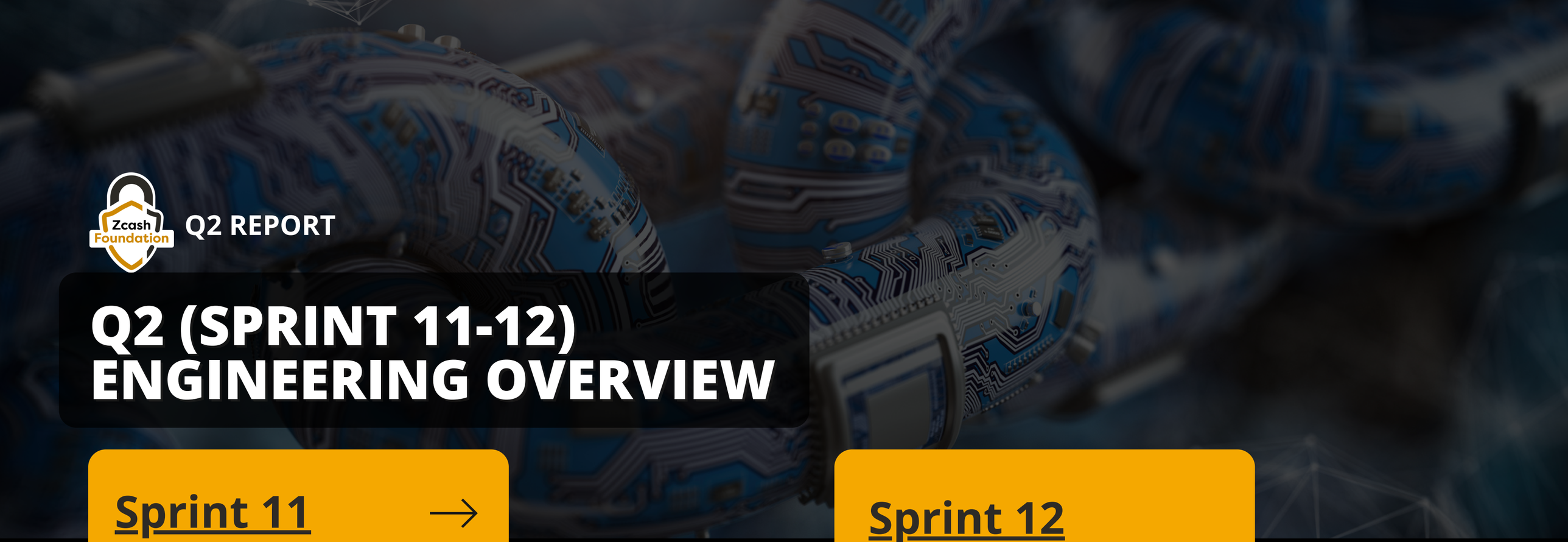
Q2 (SPRINT 9-10) ENGINEERING OVERVIEW

Sprint 9

In **Sprint 9** the team **continued to work on NU5** with the implementation of the necessary data structures to support **Orchard in Zebra**. We also worked on **implementing the RedPallas signature scheme** and continued to work on Transaction V5 implementation.

Sprint 10

For **Sprint 10**, we **implemented support to serialize and deserialize Orchard shielded data in Zebra** and implemented some methods to work on **Orchard Actions in Zebra.** We also continued to make **security fixes,** some of which were reported by the ***Equilibrium team***, recipients of a ZOMG grant to work on ***Ziggurat***, a new network stability framework for Zcash.



Q2 REPORT

Q2 (SPRINT 11-12) ENGINEERING OVERVIEW

Sprint 11 →

Sprint 11 coincided with Zcon2 Lite and as such, was a smaller sprint than usual - due to the engineering team's focus on Zcon2 Lite for half of the Sprint. In spite of this, the team continued to make progress on **NU5 and Transaction V5 support in Zebra.** We also made some additional **security fixes in the interaction between Zebra and other Zcash network nodes.**

Sprint 12

For our final sprint of Q2, Sprint 12, the engineering team made some more progress on **NU5 support in Zebra.** We started **working on ZIP-221** by integrating some existing code from **librustzcash** and made some further security fixes to ensure that Zebra acts as a well behaved node in the Zcash network.

MORE ON Q2...

The Engineering team devoted some time to focus on FROST and implemented some recommendations from the **audit**. Additionally, we were invited to submit a sponsored **post** to the ZKProofs Conference for which we wrote about how zero-knowledge proofs are used in Zcash and how Zebra does batch verification for zero-knowledge proofs. The Engineering Team continued working towards full validation of all the Zcash consensus rules in Zebra - with a focus on the new NU5 consensus rules and **ZIPs,** including work to support the Orchard shielded pool and the new Transaction V5 format. The team was also focused on fixing critical security issues related to Zebra's interaction with other nodes on the Zcash network, ready to be a well behaving node on the Zcash network in time for NU5 mainnet activation and Beta release.

The engineering team has also been collaborating with ECC engineers on the NU5 specification and ZIPs and have contributed some spec updates, in particular we identified a potential bug in the Zcash NU5 specification updates that would have allowed duplicate v5 coinbase transaction IDs. This was fixed by requiring that, from NU5 activation, the **expiry height field of a coinbase transaction is set to the block height.**

** NU5 is set to bring the first application of the **Halo 2 zero-knowledge proving system** - invented and developed at Electric Coin Co. (ECC). It eliminates the *trusted setup*, reducing the attack surface of the Zcash protocol and improving assurance about ZEC supply integrity. It also enables future circuit upgrades without the need for setup ceremonies, making the Zcash shielded protocol more agile for future improvements (such as *supporting additional assets*) and paves the way for proof aggregation and blockchain succinctness, two *scalability improvements* that enable the Zcash protocol to stay abreast of adoption.

ZCON2 Lite

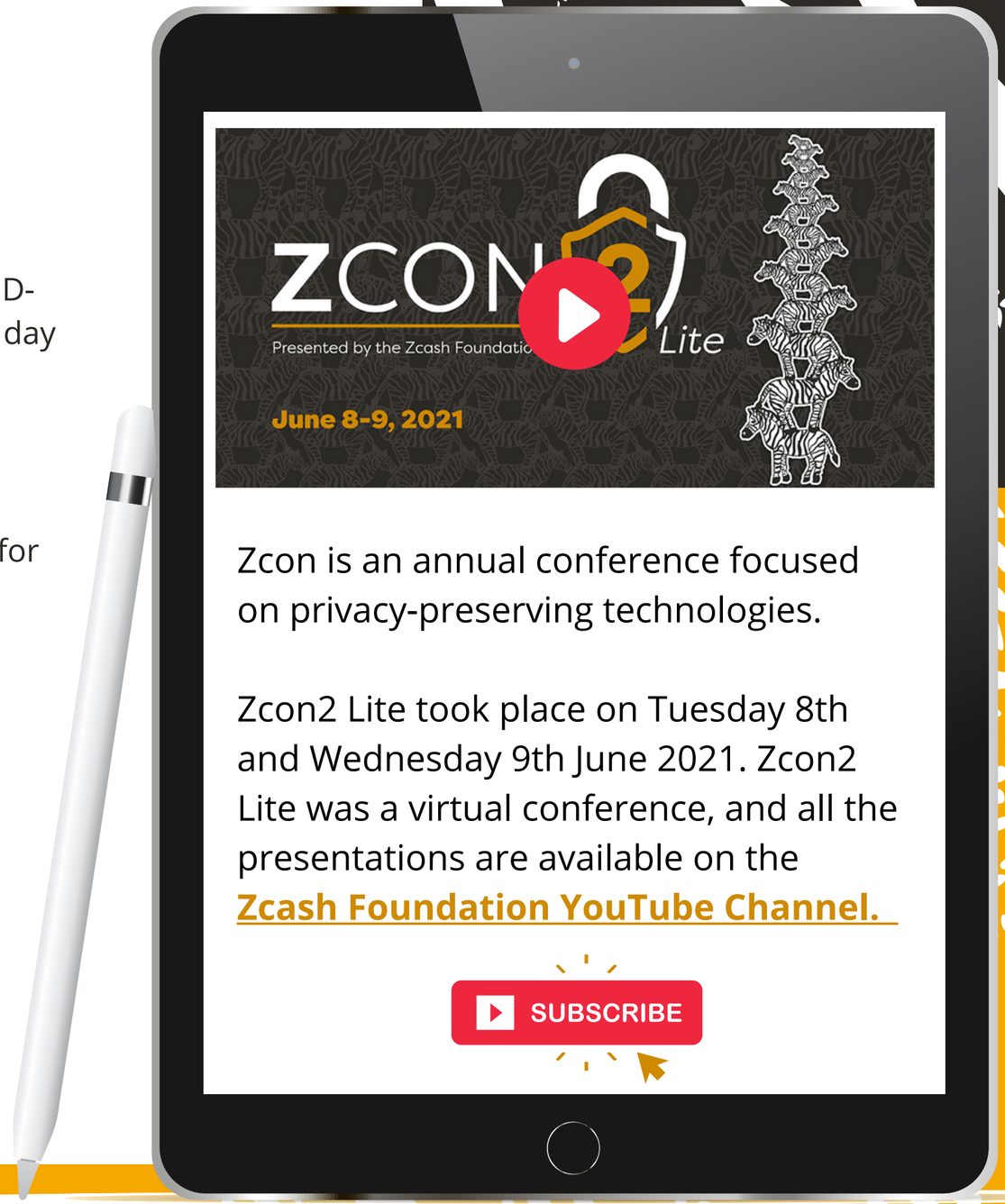
Presented by the Zcash Foundation

This year, ZF organized a virtual Zcon due to restrictions arising from COVID-19. The theme of this year's Zcon was "Privacy all the way down." The first day of Zcon2 Lite focused on Zcash and its ecosystem, while the second day looked at broader privacy themes, including new research into zero-knowledge proofs, interoperability, network privacy, and privacy metrics.

The entire ZF team and several from ECC contributed to the preparations for Zcon2 Lite. Involvement included, but was not limited to: program design, logistics, session moderation, engagement with attendees on Discord, conference publicity, panel participation, and delivering presentations.

We'd like to thank all of our speakers and panelists and the ECC for participating in the conference. We'd also like to give due credit for the tremendous work that happened behind the scenes to make Zcon2 Lite happen. Thank you especially to Danika, Ryan and Paige who were instrumental in making Zcon2 Lite a success.

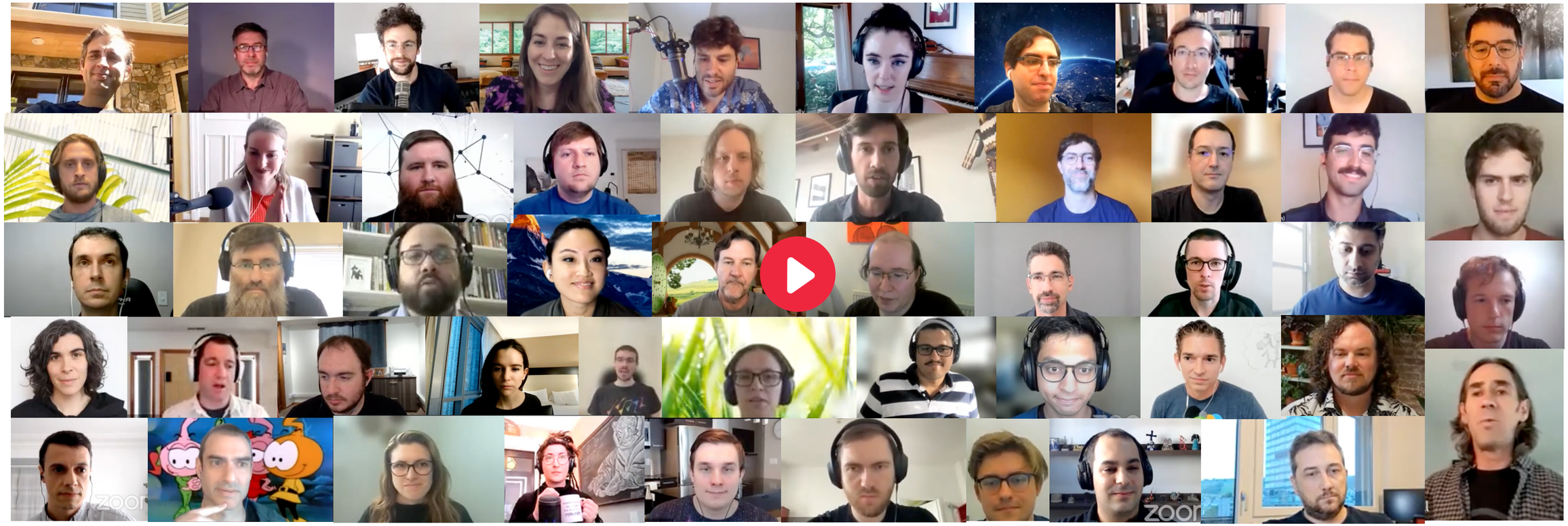
Catch up on the Zcon2 Lite conference discussions **here** and watch all sessions **here.**



ZCON 2 Lite

Presented by the Zcash Foundation

Thank you to all panelists and speakers!



482K impressions

402 Discord attendees

~6,000 playlist views

9/10 Attendee rating

ZCON 2 Lite

Presented by the Zcash Foundation

What attendees had to say:

Everything smooth, very interesting sessions. All very interesting content, there was a lot of technical but also privacy, adoption, integration with other chains, etc talks and panels. Was a great conference, more than I was expecting.

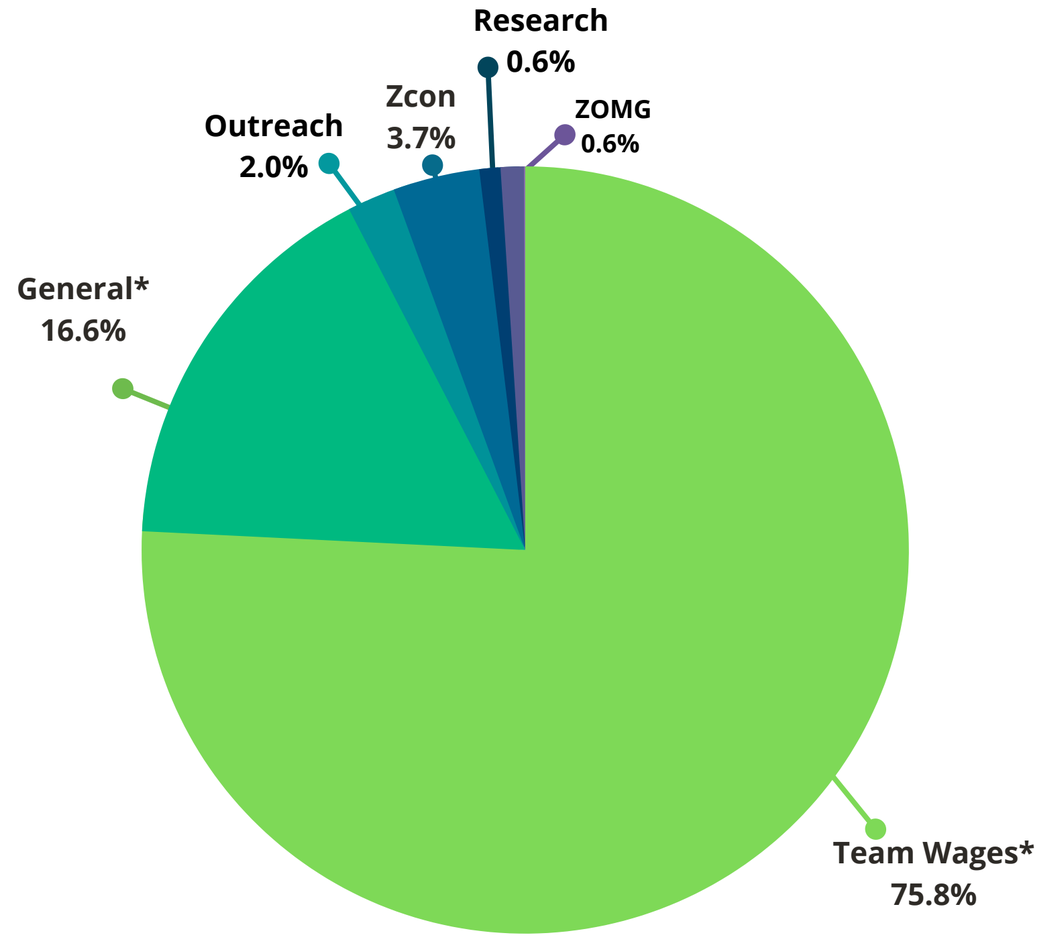
Great talks. Felt authentic. I like the discord channels, and the possibility of asking questions and interacting with other attendees. The content was both accessible and technically captivating.

I appreciate being educated on the technology and learning more about what's coming to the zcash network. It would be better in person, that's my only comment here. Very well organized.

Q2 USE OF FUNDS:

During Q2 2021, ZF's operating expenses averaged approximately **$169,556** USD per month. The breakdown of resource allocation is illustrated in the following graph:

Team compensation	**$385,476 USD**
General overhead expenses	**$84,565 USD**
Outreach, events expenses	**$10,318 USD**
Zcon	**$18,571 USD**
ZOMG member compensation	**$4,500 USD**
Research expense	**$5,000 USD**
Meals and entertainment	**$238 USD**
TOTAL	**$508,668 USD**



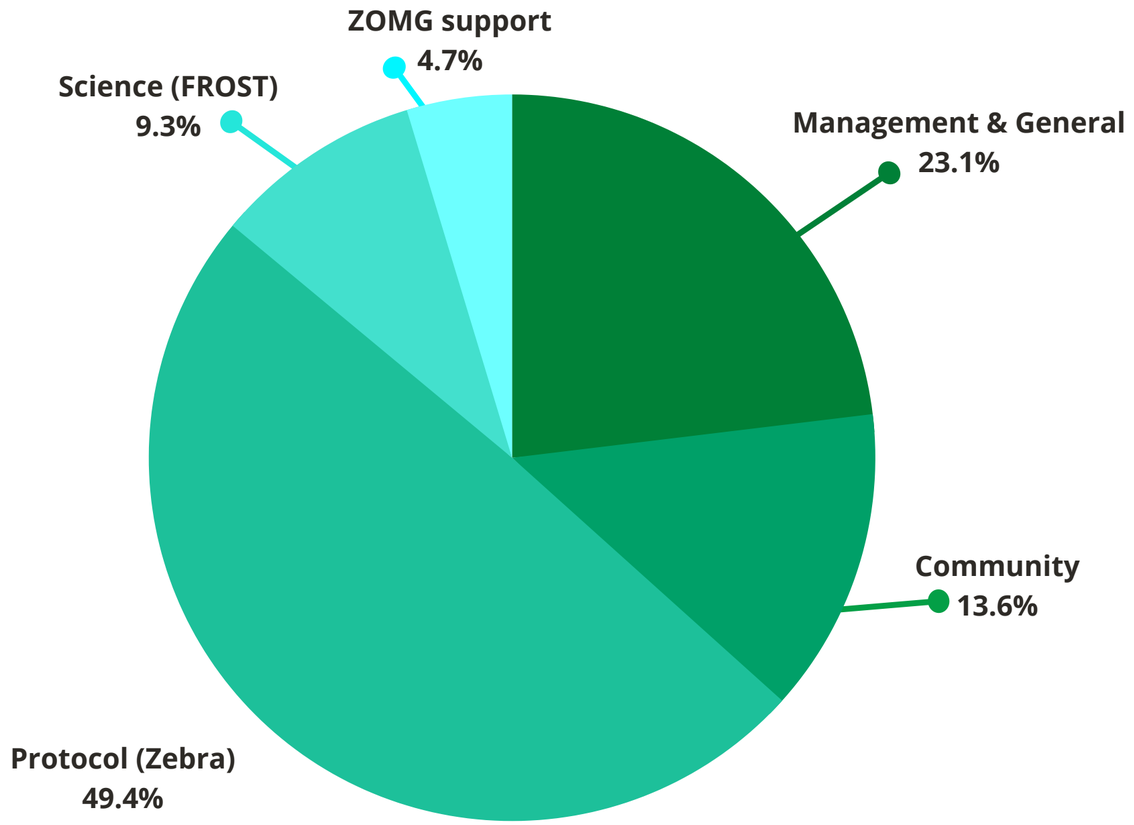
*** Team wages** encompasses all compensation and benefits paid to ZF staff and contractors. ZF does not operate any form of retention bonus or deferred compensation scheme.

***General expenses** refer to costs not related to labour. These include accounting, HR account fees, custodial service and banking fees, grant platform maintenance, insurance, legal fees as well as trademark enforcement.

Q2 PROGRAMS:

The following chart explains what type of programs the Foundation invested in during Q2. Please note, each team member's compensation and benefits are allocated to the program(s) they contribute to.

Management & General	$117,412 USD
Community	$69,042 USD
Protocol (Zebra)	$251,154 USD
Science (FROST)	$47,257 USD
ZOMG support	$23,803 USD
TOTAL	$508,668 USD



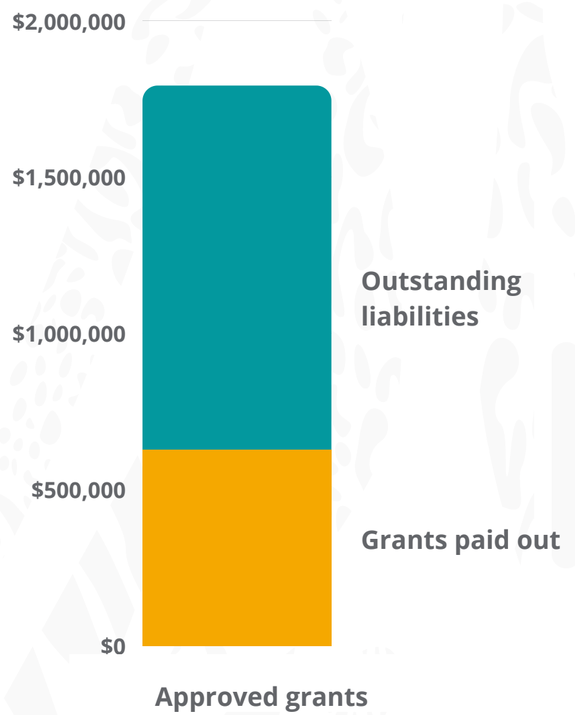
zomg

Q2 GRANTS:

The ZOMG Grants Program deploys substantial resources toward privacy-focused blockchain technology projects that meet the needs of a rapidly-accelerating Zcash ecosystem. Some key areas include: core infrastructure, social impact, improved developer tooling and UX, security, and access to education, integrations, research and more. **ZOMG approved 9 grants totalling $1,791,810 USD.**

- **Of those newly approved grants, ZOMG paid out $581,741 USD for completed milestones.**
- **ZOMG also paid out $45,052 USD for completed milestones for grants approved in Q1.**
- **At the end of Q2, ZOMG had an outstanding liability of $1,301,271 USD for approved grants that were in progress.**

The next pages highlight how the Grant program works as well as Q2's grant recipients.



zomg

HOW THE PROGRAM WORKS:

Individuals and teams **submit proposals** for projects that they believe will benefit the Zcash ecosystem. The Zcash Open Major Grants (ZOMG) committee has indicated the following areas of interest for funding: wallets, core and security, interoperability, apps, ongoing services, integration and education.

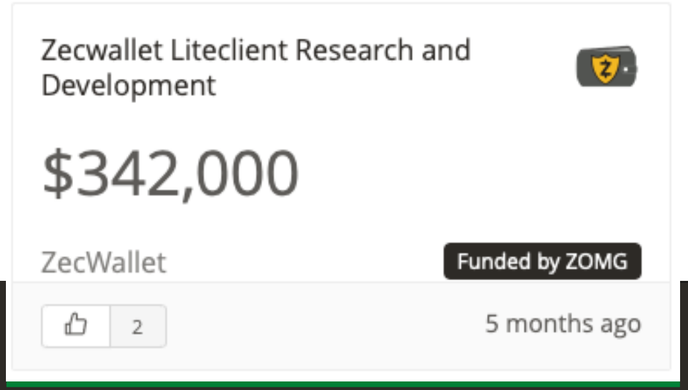
When an individual or team submits a proposal, they simultaneously **post the proposal on the Zcash Community Forums.** This will allow the community to share feedback on their project proposal, ask questions, and offer them suggestions**.**

ZOMG reviews the proposal, taking into consideration the community's feedback. ZOMG then approves or rejects the proposal, posting their decision on the forums and marking the proposal as either approved or refused on the Grants website..

For approved proposals, the requestor **posts regular updates on the forums, requesting milestone payments** as deliverables are completed (if applicable). The full grant cycle is public from initial request through project completion.

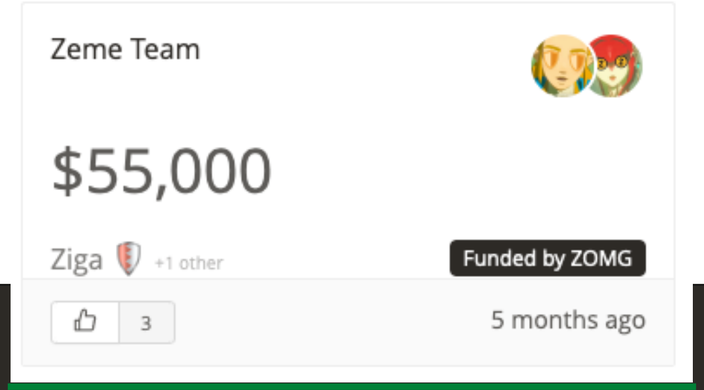
zomg

Q2 GRANT RECIPIENTS (1-3):



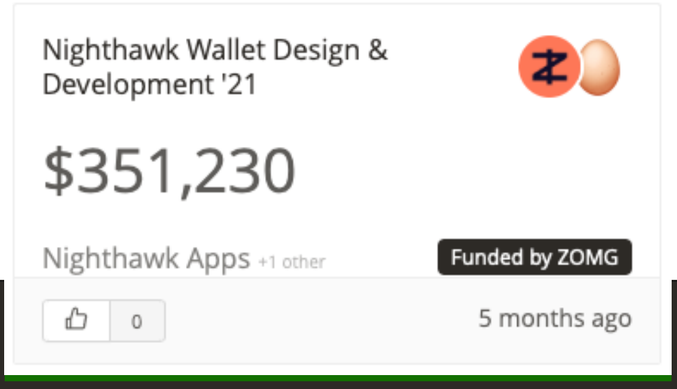
Zecwallet Lite, the light client mobile and desktop apps for Zcash have found some success within the Zcash community. The mobile and desktop apps are used by approximately ~7500 people today, but there is immense potential think to do even better.

Read more



Ziga and Zipha combined have 15+ years experience designing, coding and working at early stage venture backed companies. They are professional designers and have worked on numerous high budget crypto and non-crypto projects.

Read more

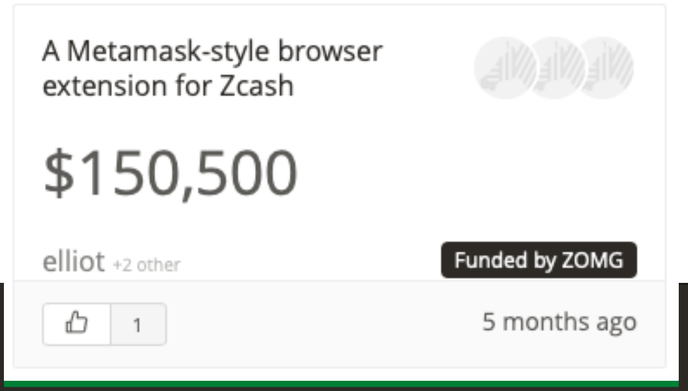


Nighthawk Wallet maintains the native apps for Android & iOS platforms along with bug-fixes, user support and security patches. They plan to expand the team & strengthen the underlying ECC codebase, ship regular updates and improve usability via UX design & app tutorial/FAQs.

Read more

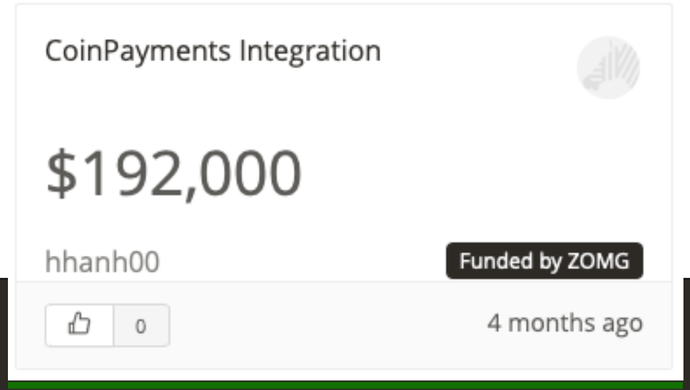
zomg

Q2 GRANT RECIPIENTS (4-6):



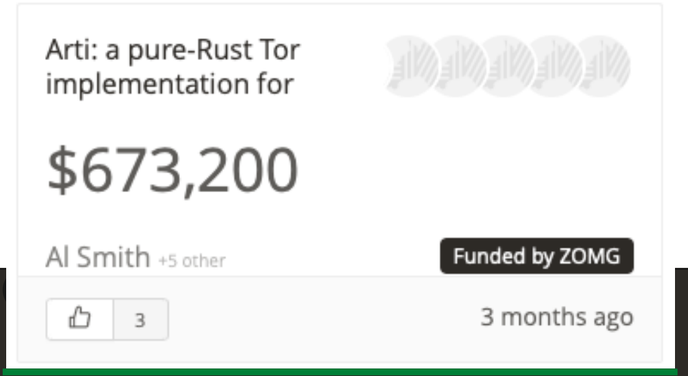
Fireice is a freelance C++ developer. He has experience writing miners for Monero and other cryptonote coins, as well as implementing a webwallet for Ryo currency. In Zcash he is helping out with running Telegram and Reddit communities.

Read more



CoinPayments (CP) is upgrading their platform. This is the opportunity to add support for ZEC both as transparent and shielded.

Read more

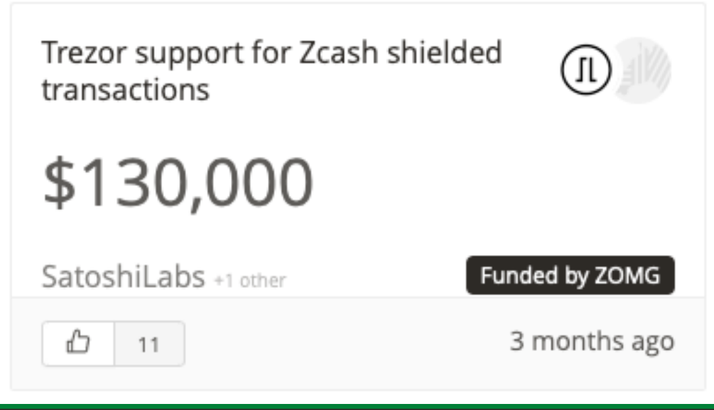


This proposal was submitted by the Tor Project: They've been developing the Tor since 2002. They've grown Tor to anonymize millions of users over thousands of volunteer-operated relays. Nick Mathewson, Tor cofounder and original developer of Arti, will direct this work.

Read more

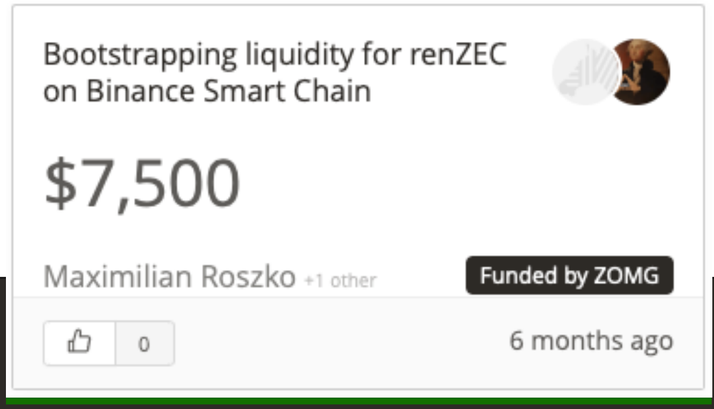
zomg

Q2 GRANT RECIPIENTS (7-9):



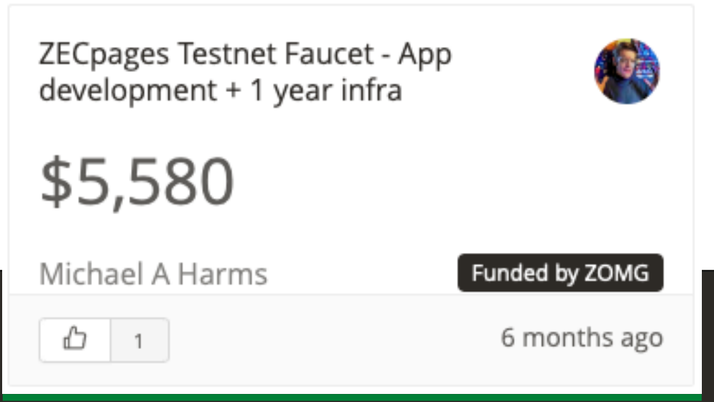
Subject of this grant is Trezor full support for Zcash Orchard (ZIP-224) shielded transactions. This includes necessary additions to Trezor firmware, Trezor Suite app and Trezor Connect API, which facilitates further integration with third-party wallets.

Read more



The Ren team has built RenVM, an open network providing access to inter-blockchain liquidity for decentralized applications. Currently, they have served about $3.3 billion in total and $4.7 million in Zcash volume going to and fro Ethereum to date. Zcash is one of the first assets they supported at launch and is one of the main assets they are trying to bootstrap liquidity and get integrations for.

Read more



Michael Harms is a full stack web developer. He first built ZECpages.com a year ago. He made zecmailer.com before that, as a way to streamline anonymous publishing. According to Michael, they are and will always be open source.

Read more

WE WELCOMED JANITO - OUR NEW CORE ENGINEER - IN MAY

Janito Filho
Core Engineer

Janito Vaqueiro Ferreira Filho has been a professional software developer for the last ten years. He is passionate about using the Rust programming language. This passion started three years ago while he was writing test software in Rust at the Brazilian Synchrotron Light Laboratory. He subsequently worked at Mullvad VPN, helping develop the client application so that more people can strive to have privacy as a universal right. He is now eager to dive into Zcash to learn more about zero-knowledge cryptography.

Janito would not have been able to get where he is today without the help of open source software and open access to information. That is why he is happy to continue working on open-source software, so that there is more source code available for people to learn from.

WE WELCOMED CONRADO - OUR NEW CRYPTOGRAPHY ENGINEER - IN MAY

Conrado Gouvêa
Cryptography Engineer

Conrado Gouvêa is a cryptography engineer who carried out research into the efficient software implementation of cryptographic algorithms such as elliptic curves, pairings, and authenticated encryption during his Masters and PhD studies at the University of Campinas.

Since then, he has been working for eight years in industry, developing software for cryptographic devices such as tokens and hardware security modules (HSMs), and has been involved in the development of a new HSM from the start. He has also participated in projects involving secure communications, writing and tailoring cryptographic libraries.

WE WELCOMED ALEX - OUR NEW CHIEF OPERATING OFFICER - IN MAY

Alex Bornstein
Chief Operating Officer

Alex Bornstein has enjoyed a colorful 25 year career in the governmental and non-profit sectors, beginning with a domestic operations and supply chain focus and then progressing to international non-profit leadership. Alex has managed operations for a large fire district in Oregon, created a supply chain division for an international humanitarian aid organization active in over sixty countries, led operations for an innovative foodbank with a state-wide footprint, and grown a youth focused non-profit into an impactful and well-regarded international organization.

Alex looks forward to utilizing his deep knowledge of non-profit operations to support the ZF's mission of building and supporting privacy infrastructure for the public good while upholding and advancing the Foundation's three values: transparency, inclusivity, and humility.

THANK YOU ZF BOARD

ZF would like to thank its board members for their continued contributions. Board service at ZF is voluntary - without compensation - and yet each year, our board members come together, dedicating their time and expertise to shape the future of the Zcash Foundation. ZF team acknowledges your efforts and ZF team appreciates each of you:

- **Jack Gavigan:** Executive Director of Zcash Foundation.
- **Andrew Miller (chair and treasurer):** Assistant professor in the electrical and computer engineering department at the University of Illinois at Urbana-Champaign, and an associate director of the Initiative for Cryptocurrencies and Contracts.
- **Peter Van Valkenburgh:** Director of research at Coin Center, a nonprofit organization focused on research, education, and advocacy on the intersection of policy and cryptocurrencies.
- **Matthew Green:** Associate professor of Computer Science at Johns Hopkins University, and one of the co-creators of Zcash.
- **Amber Baldet:** CEO of Clovyr, former J.P. Morgan blockchain program lead, and co-creator of a zero-knowledge settlement layer for enterprise Ethereum.
- **Ian Miers:** Assistant Professor of Computer Science at the University of Maryland and one of the co-creators of Zcash.

The Zcash Foundation is active on *Twitter.*

Join the conversation today!

Our goal at ZF is to create tools that help sustain open networks, enabling anyone and everyone to protect their own privacy on their own terms. **The essence of privacy itself is being able to choose what is or isn't shared with others. Privacy comprises both autonomy and consent; it is essential to human dignity and the healthy continuation of civil society.**

zfnd.org