Zcash Foundation Q1 2021 Report

A review of Q1 activities, finances and approved grants.

PRIVACY IS A FUNDAMENTAL RIGHT TO HUMAN DIGNITY

The Zcash Foundation is a public charity that builds and supports privacy infrastructure for the public good. We work on strengthening financial privacy with technology, focused on the Zcash protocol and blockchain.

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.**

Zcash Foundation

Q1 REPORT

Q1 REPORT

A WORD FROM ZF EXECUTIVE DIRECTOR

Welcome to our first quarterly report of 2021. We're resetting our approach to quarterly reporting, and introducing a new look, as part of our commitment to openness and transparency. In this report, we aim to provide a summary of the Foundation's activities during Q1, and an overview of our finances, including a detailed breakdown of our spending.

The first three months of 2021 were a period of change for the Zcash Foundation. On the engineering team, we welcomed Alfredo and Marek, and bade farewell to Henry and Jane. At the leadership level, I joined as executive director, taking over from Antonie Hodge, who had acted as interim executive director since Josh Cincinnati's departure last summer. Having helped the Foundation through its infancy, Antonie departed at the end of February to help establish another new cryptocurrency non-profit - Brink.

After its establishment late last year, the Zcash Open Major Grants committee (ZOMG) began approving grants in January. Also in January, one of the committee's founding members, Sarah Jamie Lewis, left the committee, with Michelle Lai replacing her.

During this quarter, the scope of the Foundation's research and engineering efforts were narrowed to focus on two key projects: Zebra, our independent Zcash node implementation, and FROST, a threshold signature scheme designed to bring multisig-style functionality to shielded Zcash.

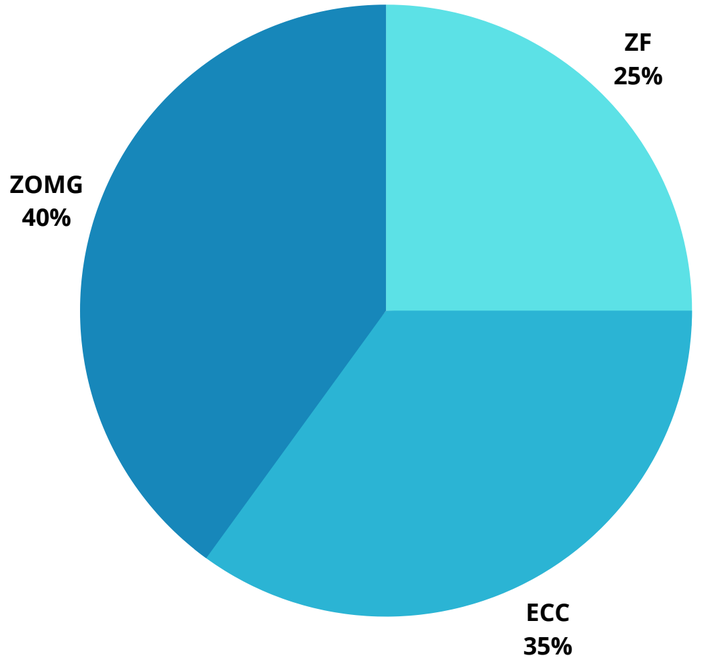
During Q1, the Electric Coin Company (ECC) announced plans to deploy Halo 2 (a new zero-knowledge proving system) in the next network upgrade (NU5), with an aggressive timeline, targeting mainnet activation on August 1st. As a result, in March the Foundation's engineering team began working to add support for validation of NU5 transactions to Zebra.

As Q1 ended, the Foundation was focused on recruiting more staff, planning Zcon 2 (which had been postponed from last year due to the pandemic), delivering on our engineering goals, and working collaboratively with ECC to support the deployment of Halo 2.

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 late 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.



Q1 '21 - ZF FINANCIAL TAKEAWAYS

The USD value of funds received and held by ZF during Q1 was calculated using the following Messari closing prices for March 31st:

- $158.28 USD/ZEC
- $58,847.79 USD/BTC
- $1,920.27 USD/ETH

ZF Funds received:

- ZF received a total of 16,105 ZEC ($2,549,099 USD) from its slice of the Dev Fund during Q1, an average of 5,368 ZEC ($849,699 USD) per month.
- ZF realized approximately $205,252 USD per month in operating expenses.

Total held at end of Q1:

- ZF held $5,479,111 USD, 119,217 ZEC, 52 BTC, and 13 ETH for a total value of $27,439,857 USD.

Q1 '21 - ZOMG FINANCIAL TAKEAWAYS

zomg

The USD value of funds received and held by ZOMG during Q1 was calculated using the following Messari closing price for March 31st:

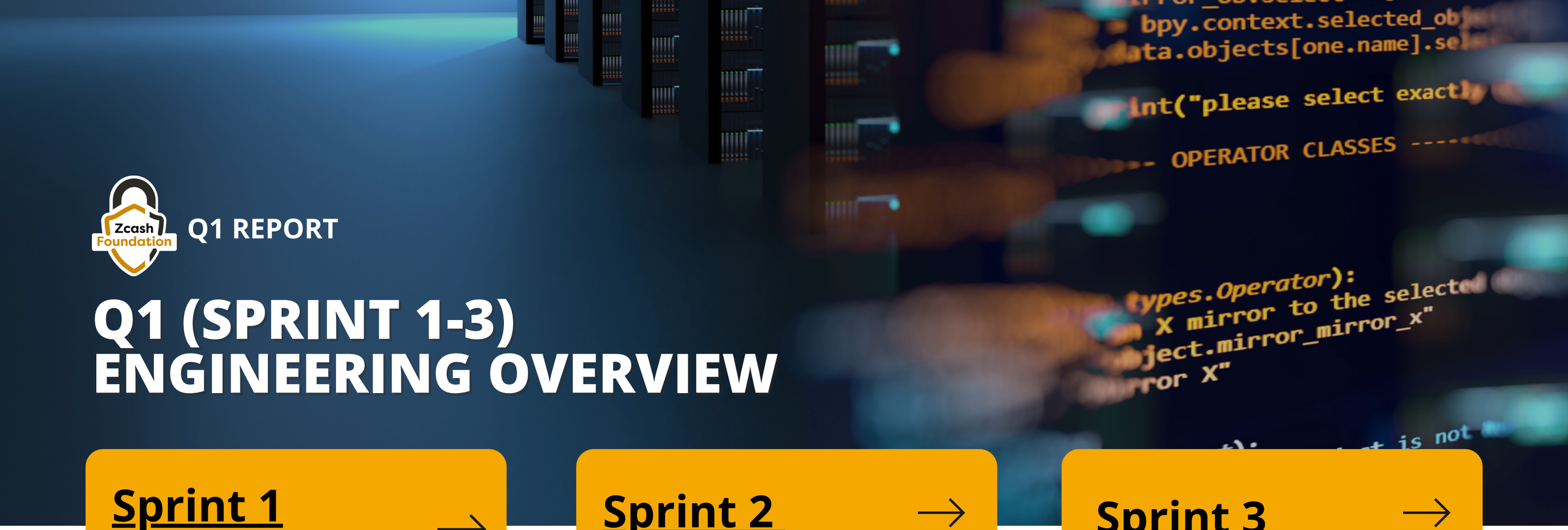
- $158.28 USD/ZEC

ZOMG restricted funds that ZF received:

- ZF received 25,768 ZEC ($4,078,689 USD) as a restricted donation from the ZOMG slice of the Dev Fund during Q1, an average of 8,589 ZEC ($135,9530 USD) per month.
- ZF distributed 954 ZEC (valued at $127,412 USD at the time of each milestone payment) for ZOMG grants during Q1.

Total held at end of Q1:

- ZF held custody of 37,051 ZEC (valued at $5,864,395 USD) restricted for use in funding major grants, as approved by ZOMG



Q1 REPORT

Q1 (SPRINT 1-3) ENGINEERING OVERVIEW

Sprint 1

The **first sprint** of 2021 culminated in our **first Alpha release for Zebra** which enabled: participating in the Zcash network, replicating the Zcash chain state, implementing the Zcash proof-of-work consensus rules, and syncing on main-net under excellent network conditions.

Sprint 2

For our **second sprint**, we made **further reliability and stability improvements** for long-running syncs as well as **resolving a number of software panics** during syncing, and reducing the number of hangs during syncing.

Sprint 3

During our **third sprint**, we continued our work on reliability and stability of the zebra node, this time with **improvements to node startup, node shutdown,** and further improvements to long-running syncs.

Q1 REPORT

Q1 (SPRINT 4-6) ENGINEERING OVERVIEW

Sprint 4 →

During our **fourth sprint,** Zebra's reliability and stability continued to improve and the team also improved some of its testing processes by making improvements to automated testing and continuous integration processes. We also **helped the ZOMG committee** to evaluate the Arti proposal and its potential use in Zebra.

Sprint 5 →

During our **fifth sprint,** we **started to work on the next Zcash network upgrade: NU5** and started fixing a number of security issues related to how Zebra interacts with other nodes on the Zcash network.

Sprint 6

On our **sixth sprint,** we **updated Zebra's mandatory checkpoint from Sapling activation to Canopy activation** and continued to work on making Zebra NU5 ready and fixing security issues. We also attracted some interest from Bitcoin developers looking to implement a bitcoin client in Rust.

MORE ON Q1...

During the first quarter of 2021, the Engineering team also worked on implementing FROST as a library to create multi-party threshold signatures. We then sent it off for audit.

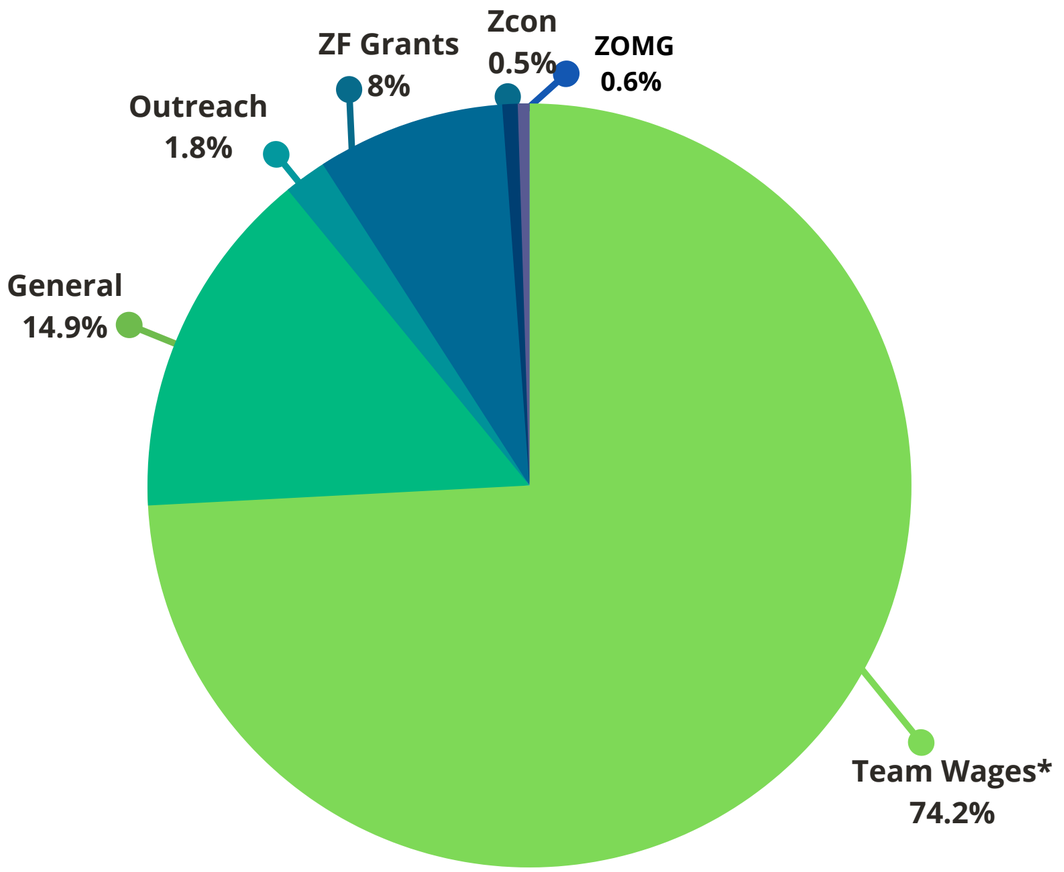
Another important contribution to the Zcash ecosystem that we would like to highlight is the addition of Groth16 batch math for proof verification that ZF engineer Deirdre Connolly contributed to the bellman crate. Bellman is a Rust library for building zk-SNARK circuits and is one of the libraries which are maintained by the **Zero-knowledge Cryptography in Rust group.**

We have also been reviewing the **Halo 2 book** and suggesting some **minor improvements.**

Q1 USE OF FUNDS:

During Q1 2021, ZF's operating expenses were **$615,152** an average of approximately **$205,250** USD per month. The breakdown of how that money was spent is illustrated here:

Team compensation	**$456,665 USD**
General overhead expenses	**$91,922 USD**
Outreach, events expenses	**$11,121 USD**
Zcon	**$3,020 USD**
ZF Grants	**$49,024 USD**
ZOMG member compensation	**$4,000 USD**
TOTAL	**$615,752 USD**



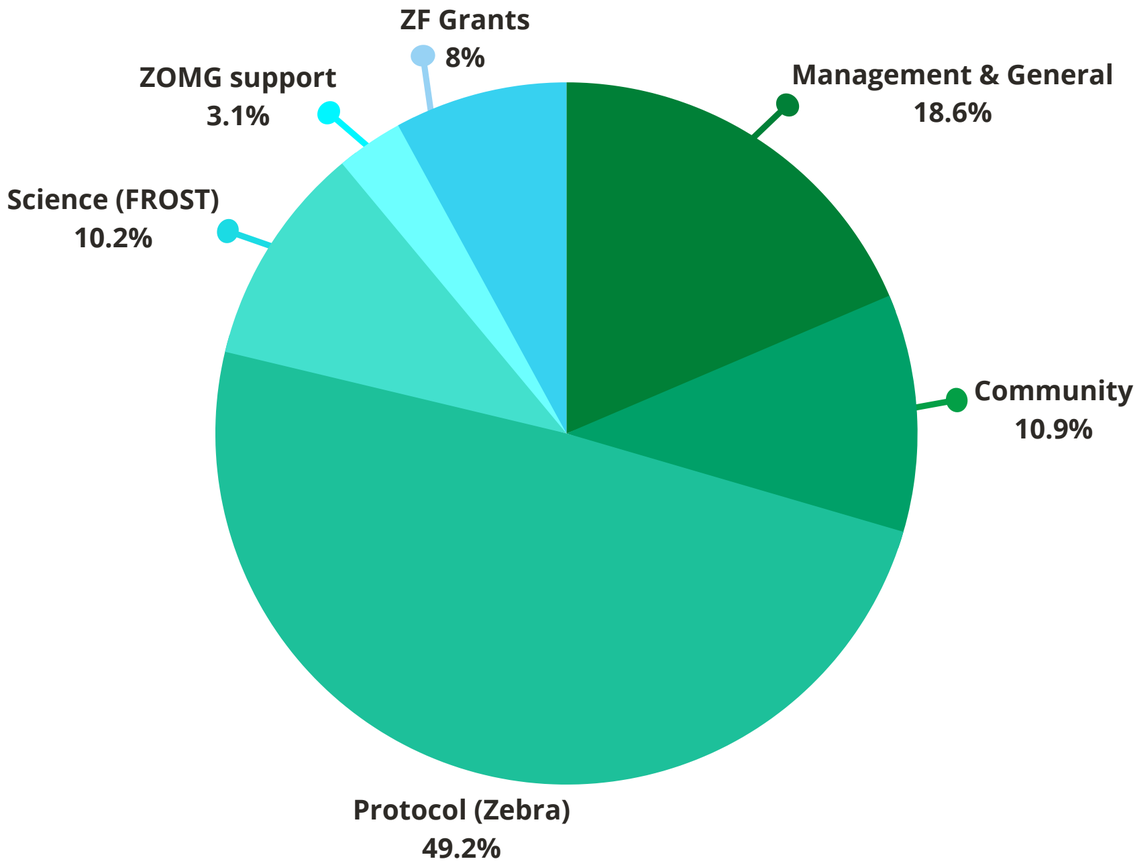
*** Team wages** encompasses all compensation and benefits paid to ZF staff and contractors. ZF does not operate any form of retention bonus or deferred compensation scheme.

***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.

Q1 PROGRAMS:

This chart shows how ZF's expenses were allocated across its various programs during Q1. Please note, each team member's compensation and benefits are allocated to the program(s) they contribute to.

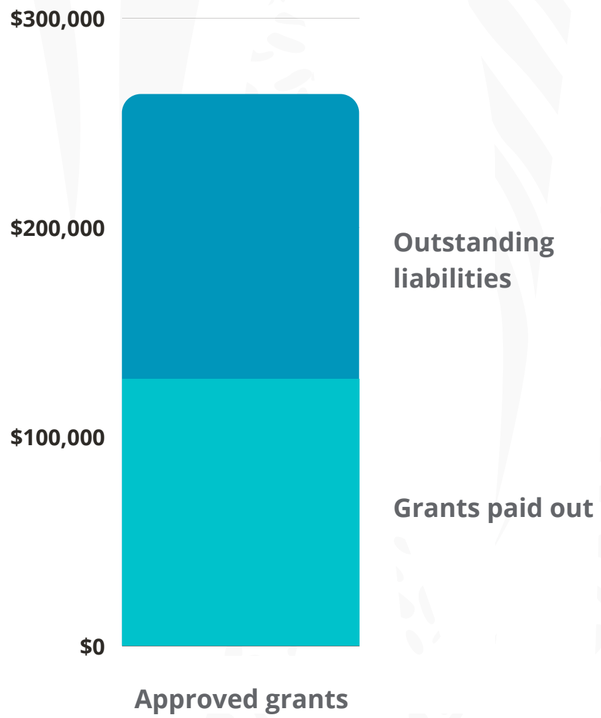
Management & General	$114,418 USD
Community	$67,365 USD
Protocol (Zebra)	$303,044 USD
Science (FROST)	$62,953 USD
ZF Grants	$49,025 USD
ZOMG support	$18,947 USD
TOTAL	$615,752 USD



zomg

Q1 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. **During Q1 2021, ZOMG approved 9 grants worth $263,666 USD and paid out $127,412 USD.** The next pages highlight how the Grant program works as well as Q1'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.

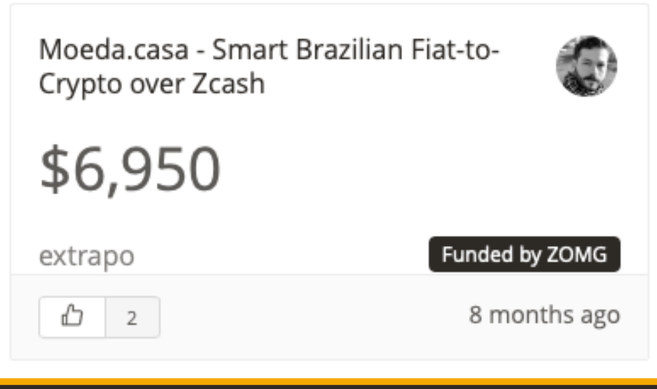
When an individual or team submits a proposal, they simultaneously **post the proposal on the Zcash Community Forums.** This will allow the community to share feedback on their project proposal, ask questions, and offer them suggestions.

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.

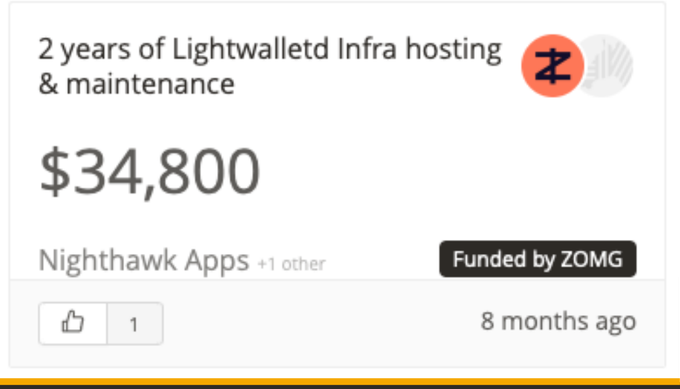
zomg

Q1 GRANT RECIPIENTS (1-3):



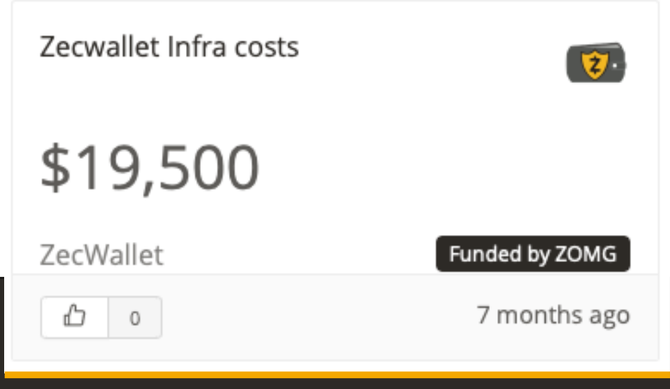
Rafael Polo was the chosen public name for this proposal, a Msc. Computer Scientist who had been developing dozens of tools and full stack software for more than two decades. From opening Computer Labs in Athens, to speculating with basic income in Lisbon.

Read more



Nighthawk Wallet Team has 20+ years of combined experience, with dev-ops led by Vamsi who has 10+ years experience in building & deploying scalable software with experience in handling peak demands, load balancing and triaging real time issues.

Read more

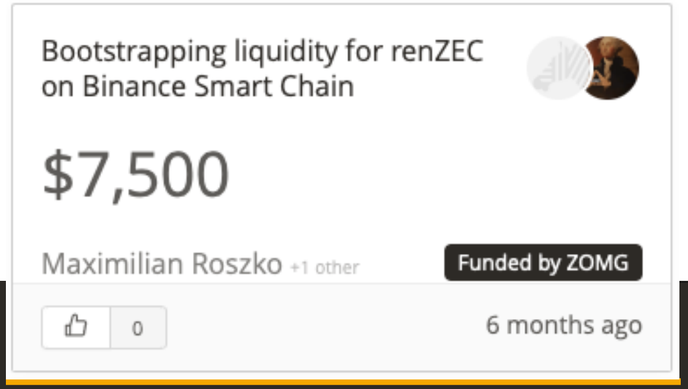


Zecwallet is a desktop and mobile Zcash wallet with full support for shielded and transparent transactions. Over the last month or so, traffic to the Zecwallet's LightwalletD servers has increased ~4x as old and new users refresh their wallets.

Read more

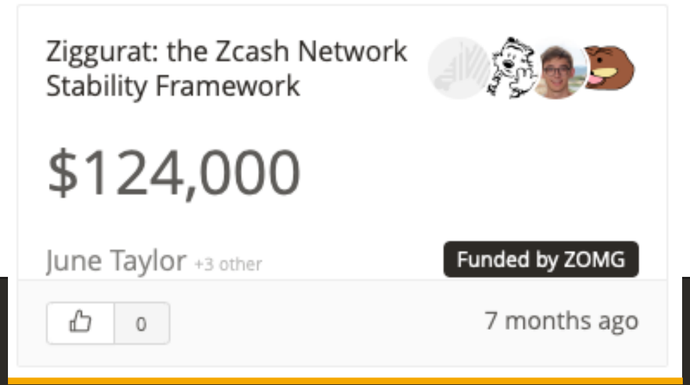
zomg

Q1 GRANT RECIPIENTS (4-6):



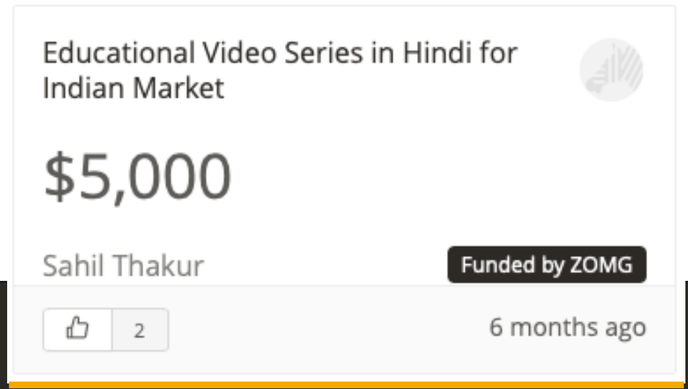
The Ren team has built RenVM, an open network providing access to inter-blockchain liquidity for decentralized applications. Currently, they have served about $3.3 billion in total and $4.7 million in Zcash volume going to and fro Ethereum to date. Zcash is one of the first assets they supported at launch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

Read more



Equilibrium is a software consultancy with a mission to further privacy and decentralization. Our clients include Aleo, Protocol Labs, and the Web3 Foundation. In addition to engineering talent, they also employ economists and expert cryptographers to deliver results beyond the bounds of software development.

Read more

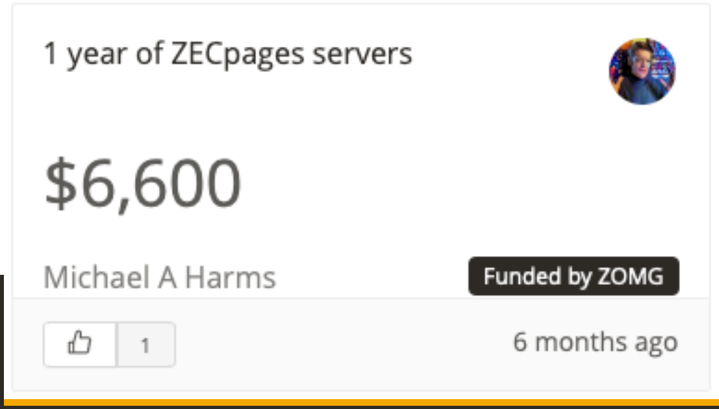


Finstreet is India's First Crypto Education Institute. Their platform acts as an easily accessible medium for people to learn about the importance of cryptocurrencies and the different asset classes associated with them.

Read more

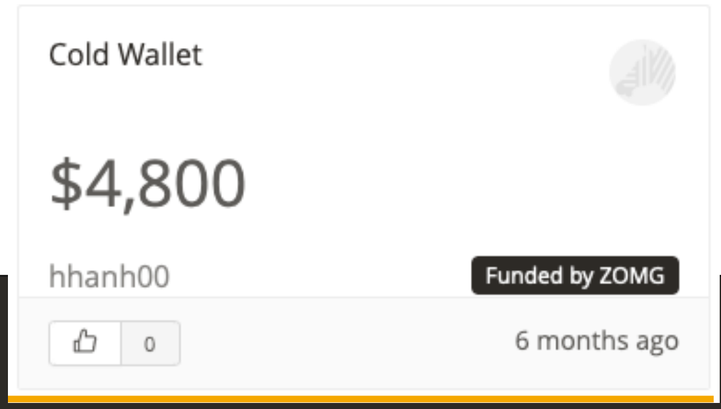
zomg

Q1 GRANT RECIPIENTS (7-9):



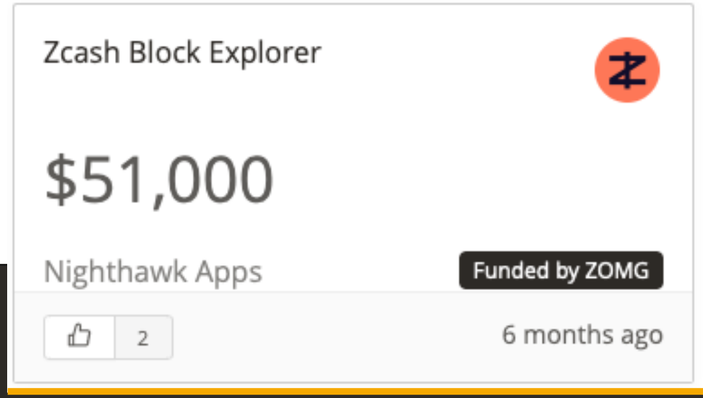
ZECpages is an example of what Balaji Srinivasan has called "Blockchain MVC", a full stack app built on a global data store. For ZECpages, this means a set of encrypted memos associated with one view key. This makes the data that powers ZECpages durable, auditable, and open.

Read more



Hanh has worked on system development for 25 years +. They worked in the SQL Server Engine, Windows CE and .NET framework. They also implemented a full node bitcoin in F# and Scala.

Read more



Nighthawk Wallet Team has 20+ years of combined experience in software development. With this grant, they want to build a block explorer that supports Zcash specific features requested by the community. Additionally, they plan to host the block explorer for both testnet and mainnet with support for tor v3 access.

Read more

WE WELCOMED ALFREDO - OUR NEW CORE ENGINEER - IN JANUARY

Alfredo Garcia
Core engineer

Alfredo is a self-taught developer who has worked in the blockchain industry for the last 5 years, as an active defender and contributor to the open source community. He started working for the Zcash protocol one year ago as a grant recipient from the Zcash Foundation.

As an outside contributor, Alfredo first worked on zcashd development and eventually focused on Zebra. While working on Zebra, he worked side by side with the Zebra team forming a productive relationship, which led to the Foundation offering him a role as a core engineer. Alfredo's main role within the Foundation is to help with the design and development of Zebra, the Foundation's Zcash protocol implementation.

WE WELCOMED JACK - OUR NEW EXECUTIVE DIRECTOR - IN FEBRUARY

Jack Gavigan
Executive Director

With over ten years of experience in finance, and four years at the Electric Coin Company (ECC), Jack's deep knowledge of Zcash, and his alignment with the Foundation's values makes him the ideal person to guide the Zcash Foundation into its preschool years.

Jack has a background in financial technology. He spent over a decade working on trading systems at major financial institutions such as Deutsche Bank, Credit Suisse, and Morgan Stanley (where he also spent a year as a trader). He became an advisor to ECC in early 2016, and joined the company as COO shortly before the launch of Zcash in October 2016. He relinquished the role of COO in 2018, and his recent focus at the time he left ECC was on regulatory relations.

WE WELCOMED MAREK - OUR NEW CRYPTOGRAPHY ENGINEER - IN MARCH

Marek Bielik
Cryptography engineer

Marek is an advocate of information privacy, FOSS and open-source hardware. In June, he graduated with a Masters in Computer Science from the Czech Technical University, where he also was a mentor in cryptography classes. His research includes work on algebraic cryptanalysis. During his interviewing, he found a bug in Zebra's implementation of the Zcash spec that we were able to fix.

During his undergraduate studies, he was a software engineer at the research and incubation center at TU Dublin. He has been closely watching the development of Bitcoin and other cryptocurrencies, and sees great potential in this technology while recognising that it is still, in many ways, immature. Marek is a passionate programmer with a particular interest in cryptography, and is thrilled to help with the development of Zcash.

THANK YOU TO THE 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.

zfnd.org