Zcash Foundation
Q4 2021 Report

A review of Q4 2021 development, expenses and approved grants.

A WORD FROM OUR EXECUTIVE DIRECTOR

This is our final quarterly report for 2021. Our goal in publishing these reports is to provide transparency regarding the Foundation's activities and finances, including a detailed breakdown of our spending, and a summary of our financial position. We welcome constructive feedback, so if you have any questions, suggestions or ideas for how we can improve these reports, please post them to the Zcash Community forums!

The Foundation Engineering team hit their objective of releasing an "MVP" (minimum viable product) version of Zebra in late October (v1.0.0-beta.0), which maintains a mempool and can actively contribute to the Zcash network by validating the blockchain, and relaying blocks and transactions. Following this release, the Engineering team continued working towards our objective of having Zebra capable of acting as a fully-validating node on the Zcash network by the time NU5 activates on mainnet. However, in December, ECC announced that the target date for mainnet activation was being pushed back from January to April 2022. As result, we adopted a new objective of preparing a Zebra stable release candidate that is production quality, ready to be audited, and can serve as a foundation for us - and others in the Zcash ecosystem - to build upon. We aim to have that stable release candidate ready by March 2022, after which we intend to begin adding the necessary functionality to Zebra to support light wallets.

During Q4, the ZOMG Committee approved 8 grants, totalling $895,960, and distributed $647,224 for completed grant milestones.

Towards the end of Q3, we paused the ZOMG elections process to seek advice on some conflict of interest questions. In November, having obtained advice from legal counsel, we were able to provide clarity regarding the conflict of interest policy that will apply to the ZOMG Committee going forward, and announced a revised schedule for the ZOMG Committee election. Seven candidates stood for election, and the successful candidates were:

- Aditya (aiyadt on the forums)
- Brian (Wobbzz on the forums)
- Hudson Jameson (Souptacular on the forums)
- Jason McGee (aquietinvestor on the forums)
- Michael Harms (Brunchtime on the forums)

Alongside the ZOMG Committee election, we polled the Zcash Community Advisory Panel (ZCAP) on a proposal from community member and ZOMG candidate Jason McGee, to amend ZIP 1014 to provide the ZOMG Committee with a discretionary budget. The ZCAP voted in favor of the amendment, recommending an annual budget of 3% of the Major Grants slice of the Dev Fund (approximately 3,156 ZEC), with a floor of $250,000 and a cap of $1,000,000.

We'd like to express our appreciation to the outgoing ZOMG Committee for their service to Zcash and its community. A top priority for the Foundation in Q1 2022 will be to help the new committee hit the ground running, and rejuvenate the major grants program.

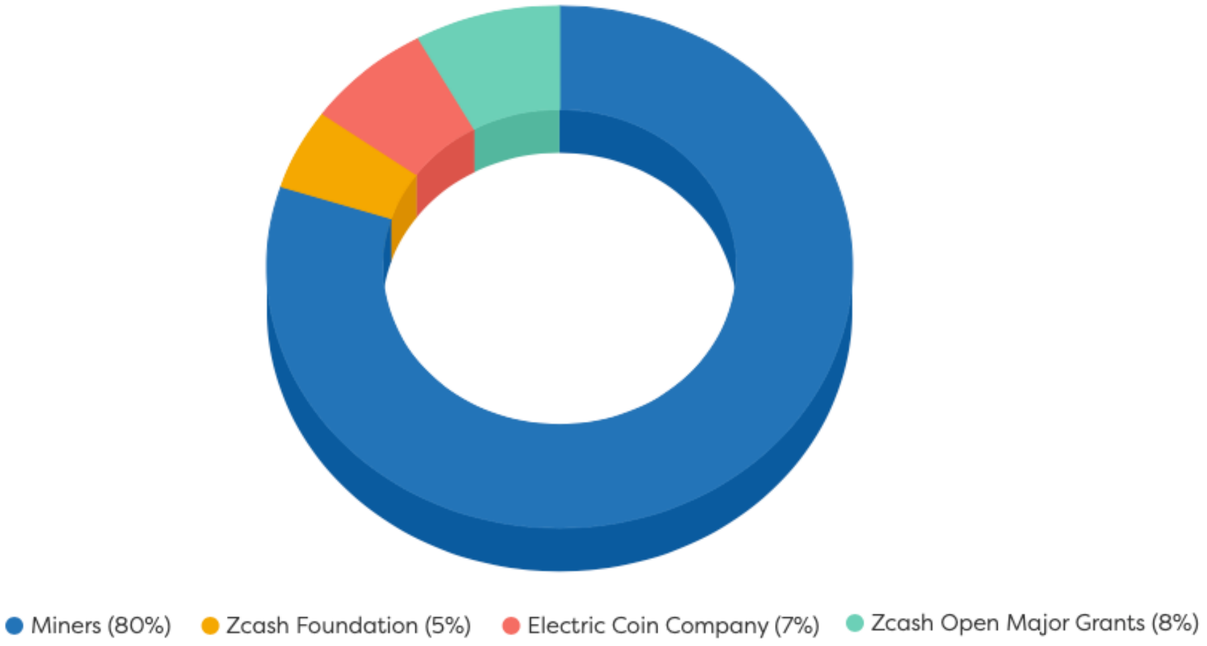
Jack Gavigan - Executive Director

ZCASH FOUNDATION SOURCE OF FUNDS:

The Zcash Community created the Dev Fund in late 2020 as a means of funding ongoing development of the Zcash protocol by the Zcash Foundation, the Electric Coin Company (ECC), and the Zcash Open Major Grants program (ZOMG).

Annually, the Zcash Foundation receives approximately 65,745 ZEC from the Dev Fund. In addition, the Foundation annually receives 105,192 ZEC as a restricted donation which may only be disbursed as major grants.

We release quarterly reports that describe our income and expenditure, with a detailed breakdown of our expenses, and a snapshot of the Foundation's financial position, in terms of liquid assets and liabilities that must be met using those assets.



Q4 '21 - ZF KEY FINANCIAL POINTS:

The USD value of funds received and held by ZF during Q4 was calculated using the following Messari closing prices for December 31:

- $146.47 USD/ZEC
- $46,209.11 USD/BTC
- $3,676.70 USD/ETH

ZF funds received:

- ZF received 16,480 ZEC ($2,413,826 USD) from its slice of the Dev Fund during Q3, at an average of average of 5,493 ZEC ($804,560 USD) a month.
- ZF incurred approximately $245,393 USD per month in operating expenses.

Total held at end of Q3:

- ZF held $6,510,605 USD, 150,262 ZEC, 56 BTC, and 13 ETH for a total value of $31,166,129 USD.

zomg

Q4 '21 - ZOMG KEY FINANCIAL POINTS:

ZOMG Funds ZF received in Q4 at USD value were based on the following December 31 Messari closing prices:

- $146.47 USD/ZEC

ZOMG restricted funds that ZF received:

- ZF received 26,084 ZEC ($3,820,523 USD) from the Dev fund, and 60,000 USDC from an external donor restricted for the Zcash Thorchain Integration grant.
- This was at an average of 8,695 ZEC ($1,273,557 USD) a month of ZOMG restricted funds.
- The Foundation distributed 3,191 ZEC and $175,032 USD (total value of $644,470 USD based on ZEC value at time of payments) in Quarter 4 of ZOMG restricted funds for grants approved by the ZOMG committee

Total held at end of Q4:

- ZF held custody of 94,066 ZEC (valued at $13,777,847 USD), $60,000 USDC, and $1,497,434 USD for a total value of $15,275,281 USD restricted for use in funding major grants, as selected by ZOMG

WORK ON ZEBRA

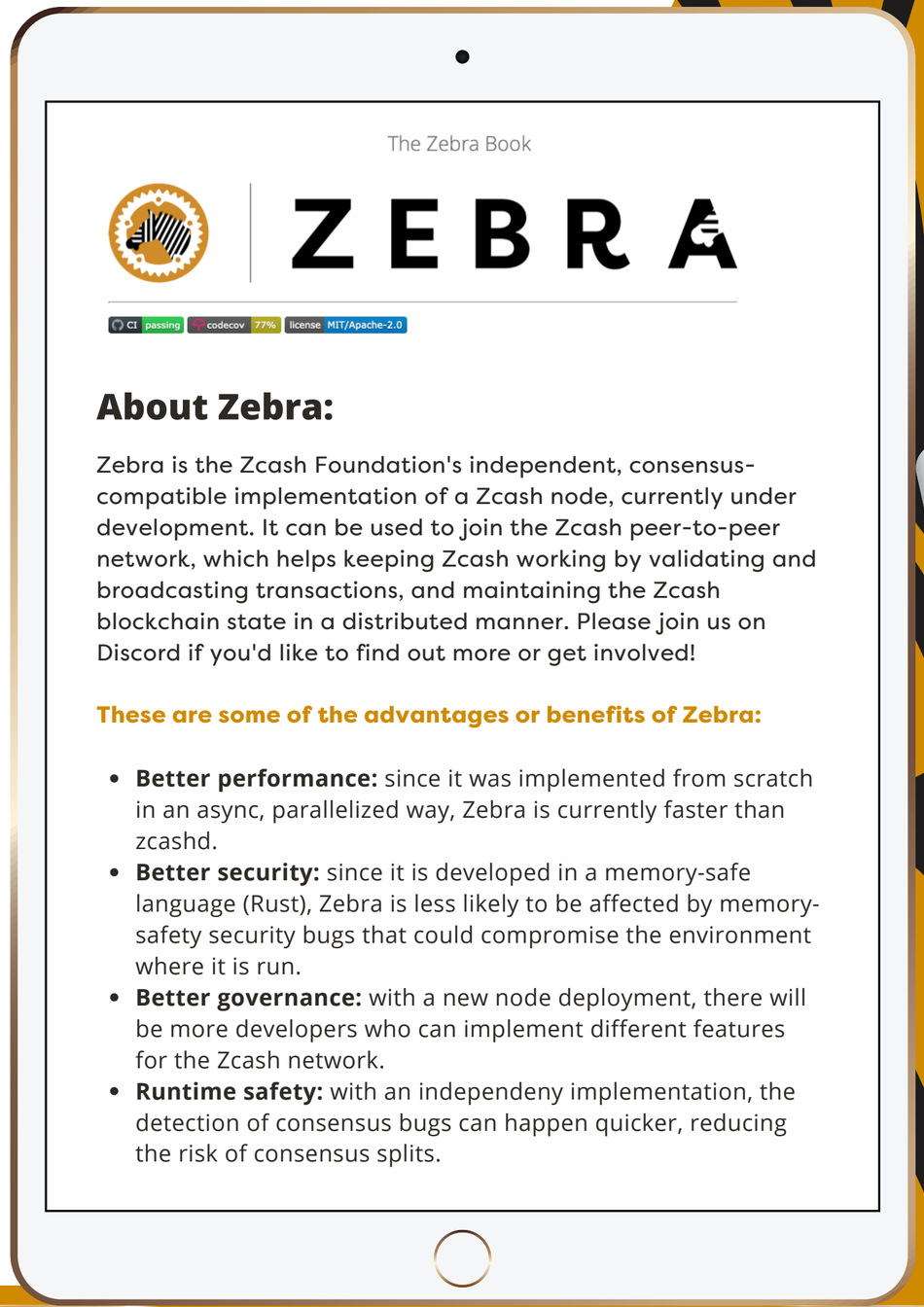
Zebra Gears up for NU5:

During the final quarter of 2021, the team worked on finishing off all the remaining work necessary for Zebra to act as a fully validating node, implementing all of the consensus rules up to and including Network Upgrade 5 and stabilising Zebra by fixing the security issues which could have had an adverse impact on the Zcash network.

About Zebra →

Join our Discord

Zcash Foundation Q4 REPORT

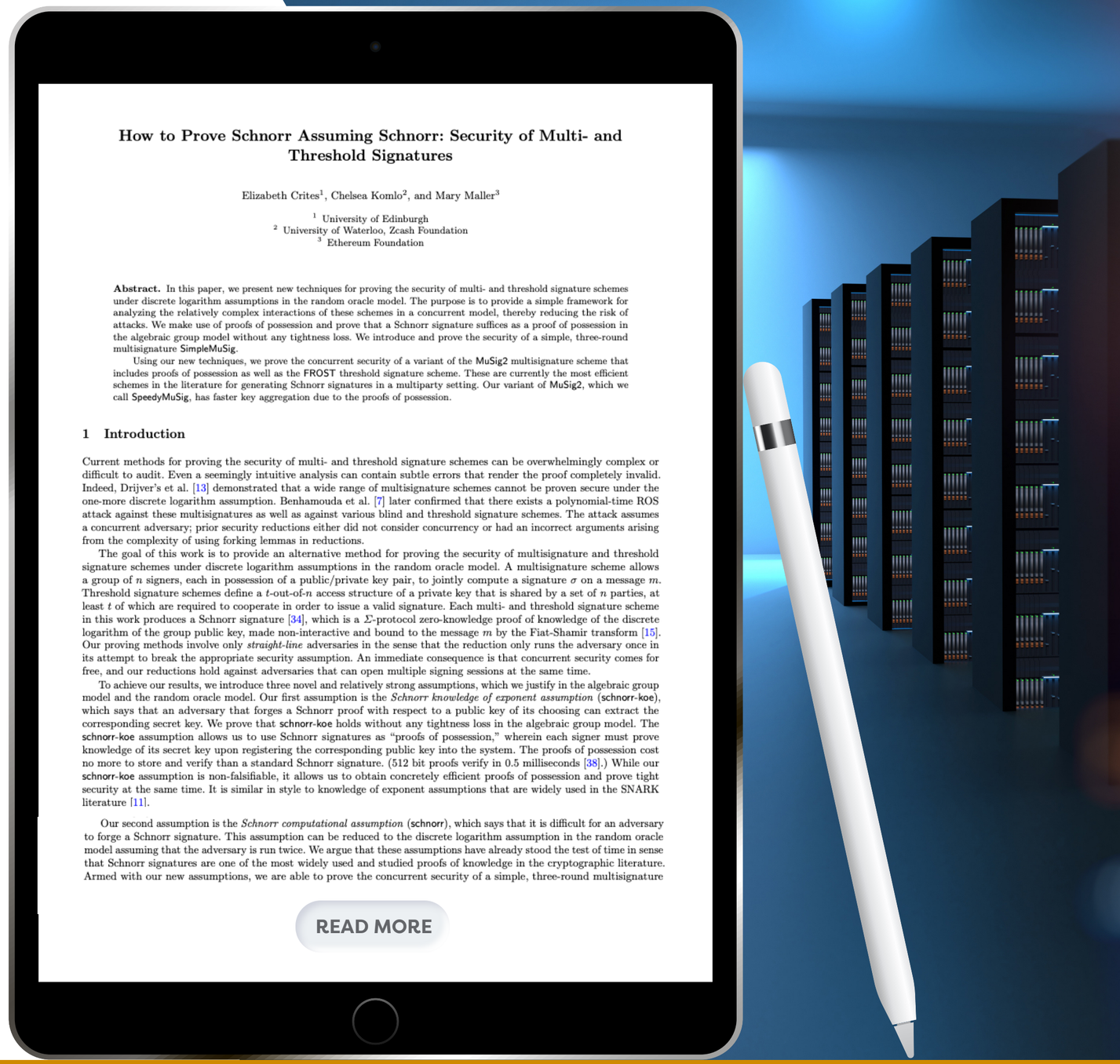


WORK ON FROST:

FROST spec draft

Work on FROST continued with monthly meetings to work on the spec draft as well as planning out the next steps on the Zcash Foundation's reference implementation of FROST on the Ristretto curve. During this time, we also split off the FROST library into its own Github repository.

About FROST →



Q4 ENGINEERING OVERVIEW:

SPRINT 20:

During Sprint 20, the team finished off the remaining work necessary to ensure that Zebra has a working mempool which can verify and relay gossiped blocks and transactions to other nodes on the network. We also worked on updating some cryptographic dependencies and improving our mempool metrics.

SPRINT 21:

For Sprint 21, we prepared and released our first Beta release, which included the fully finished mempool and implemented ZIP-401 compatible rules to address mempool Denial-of-Service. We also took this opportunity to fix a number of security issues which could adversely affect the Zcash network and we continued to investigate the reason for zebra nodes not being reachable by some DNS Seeders and block explorers. Additionally, we improved our user facing documentation and increased our test coverage. And finally, we took the opportunity to upgrade to the latest version of tokio, which was released with our second beta release.

Q4 ENGINEERING OVERVIEW:

SPRINT 22:

In Sprint 22 we continued to work towards our goal of having Zebra act as a fully participating and validating node by the time NU5 activates in early 2022. This included the calculation of block subsidies and support for parsing addrv2 messages as per ZIP-155. We implemented validation of Orchard proofs and note commitment trees and continued to work towards validation of Orchard anchors and validation of Sprout and Sapling note commitment trees and anchors. Finally, we also fixed a number of security issues that could pose a DDoS risk or otherwise negatively impact other nodes on the network.

SPRINT 23:

During Sprint 23 we continued to work on achieving full validation of Orchard, Sapling and Sprout proofs, note commitment trees & anchors. We finished implementing transaction header, transaction amount, and Zebra-specific NU5 validation. The team also worked on implementing automatic download and caching of the Sprout and Sapling Groth16 circuit parameters in Zebra. We fixed a number of security issues that could pose a local denial of service risk, or make it easier for an attacker to make a node follow a false chain.

Q4 ENGINEERING OVERVIEW:

SPRINT 24:

For Sprint 24 our aim was to finish all remaining Zcash network consensus rules up to and including NU5. We achieved this by implementing validation of JoinSplit Groth16 proofs used by Sprout transactions, which was the final missing piece. We also added security and network improvements to limit memory and CPU usage. In order to help diagnose networking issues in future, we also worked on measuring some additional metrics in Zebra.

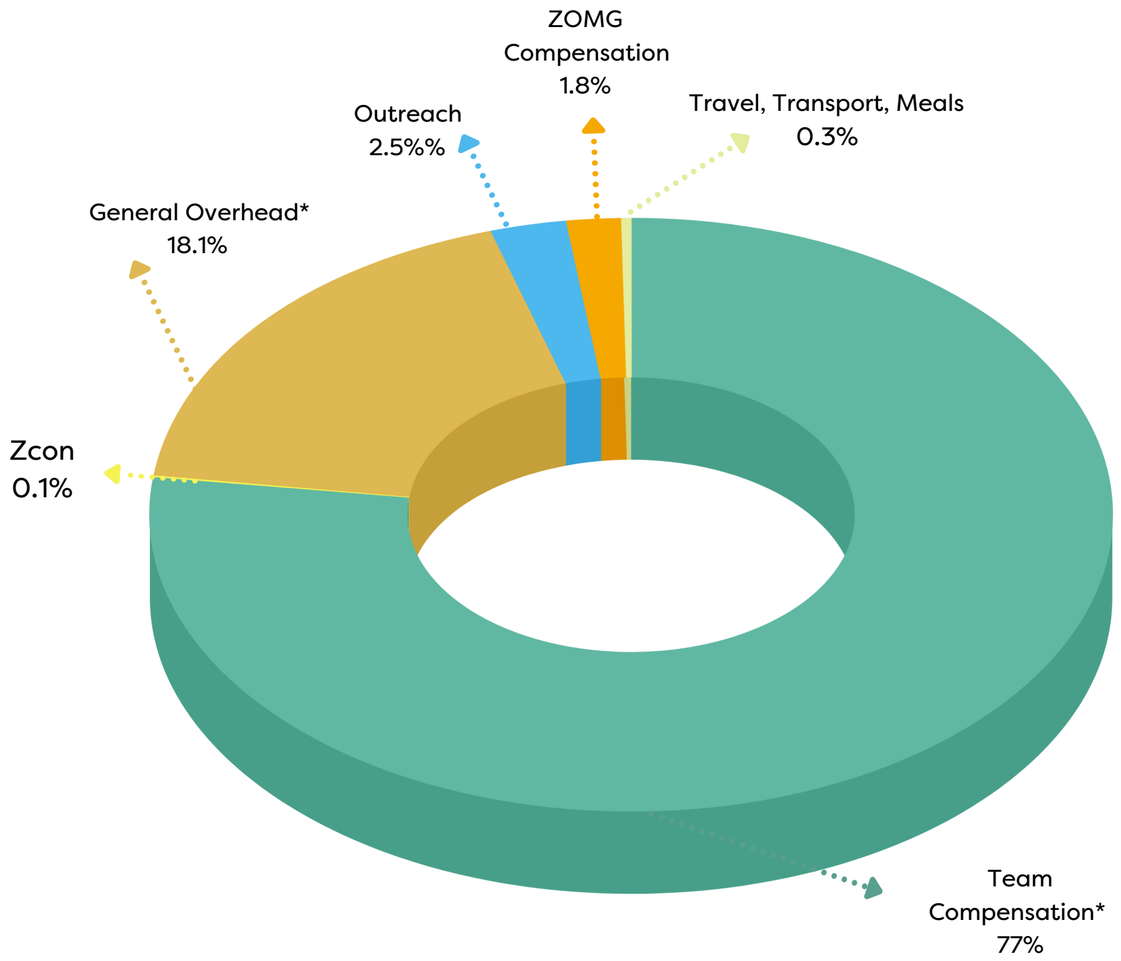
SPRINT 25:

Sprint 25, our last sprint for 2021, was dedicated to stabilising Zebra and working towards a stable release candidate version for audit by concentrating on any performance or security issues that could have an adverse effect on the Zcash network as a whole or on other nodes. During this last sprint we also took the opportunity to take some time to play with the Arti 0.0.2 release and provide some feedback to the project's grantees.

Q4 USE OF FUNDS:

During Q4 2021, ZF's operating expenses averaged approximately $245,393 USD per month. The breakdown of resource allocation is illustrated in the table below:

Team compensation*	$567,327
General Overhead Expenses*	$133,698
Outreach	$18,737
Zcon	$630
Travels, Meals, Transportation Expenses	$2,287
ZOMG Member Compensation	$13,500
Total	**$736,180 USD**



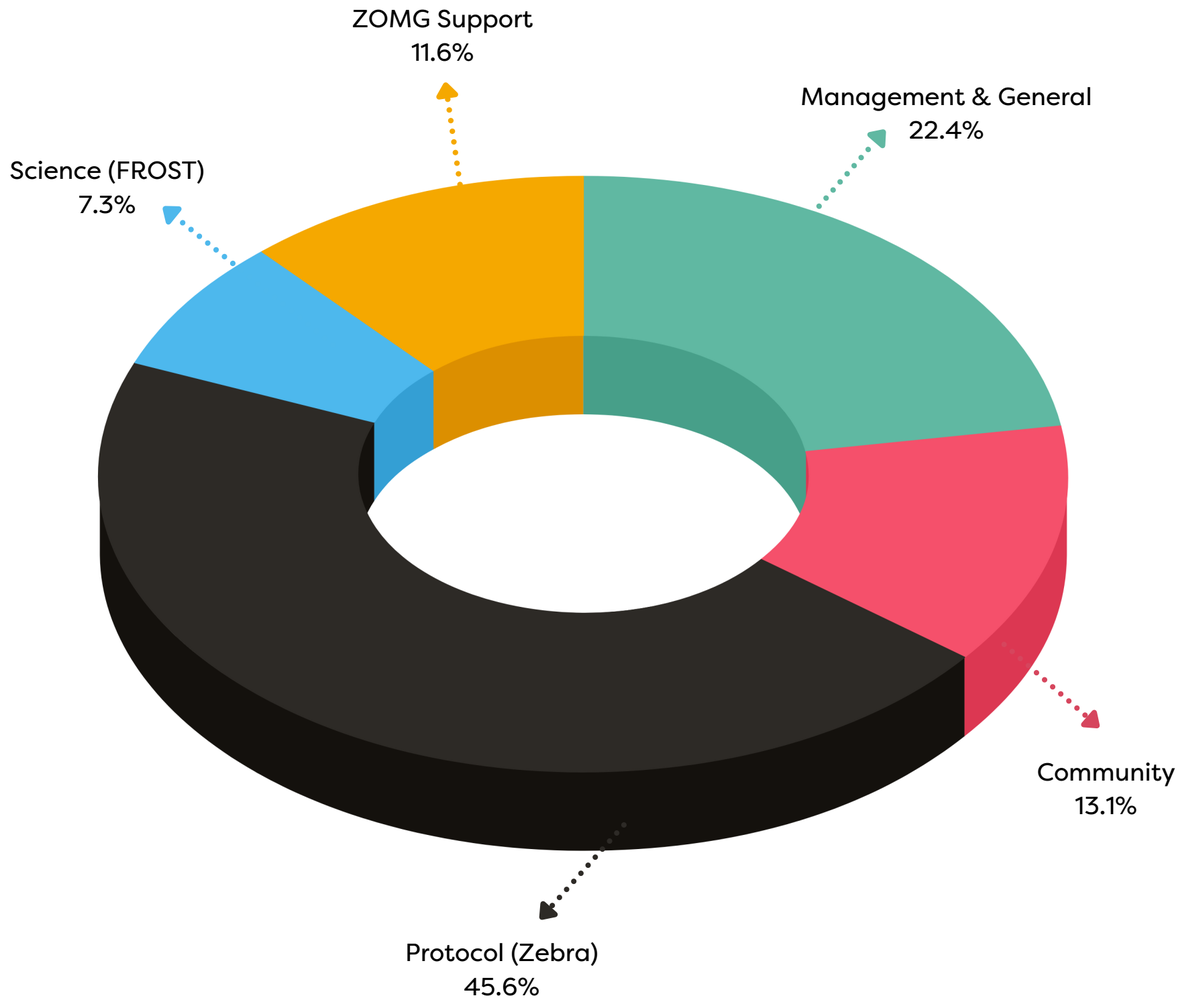
* Team compensation encompasses all compensation and benefits paid to ZF staff and contractors. ZF does not operate any form of retention bonus or deferred compensation scheme.

*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.

Q4 PROGRAMS:

The following chart explains what type of programs the Foundation invested in during Q4. Please note, each team member's compensation and benefits are allocated to the program(s) they contribute to.

Management & General	$163,157
Community	$95,594
Protocol (Zebra)	$331,682
Science (FROST)	$53,306
ZOMG Support	$84,179
Total	**$727,918 USD**



Q4 FINANCIAL SNAPSHOT:

	UNRESTRICTED FUNDS		FUNDS RESTRICTED FOR ZOMG	
LIQUID ASSETS:	**COIN BALANCE**	**USD VALUE**	**COIN BALANCE**	**USD VALUE**
USD		$6,510,605		$1,437,433.68
USDC			$60,000	$60,000
ZEC	150,261.66	$22,008,825.29	94,066.31	$13,777,893
BTC	56.251	$2,599,294.784		
ETH	12.894	$ 47,404		
		$ 31,166,129		***$ 15,275,326***
LIABILITIES:				
Grant commitments		$11067.9		$1,498,710
Accrued Expenses & Payroll Liabilities		$60,179.14		
NU5 Audit Contribution		$72,000		
		$143,247		***$1,498,710***
NET LIQUID ASSETS: (Liquid assets less liabilities)		***$31,022,882***		***$13,776,616***

CLOSING PRICES: DECEMBER 31, 2021

(Used to calculate USD value of coins)

- **$146.47 USD/ZEC**
- **$46,209.11 USD/BTC**
- **$3,676.70 USD/ETH**

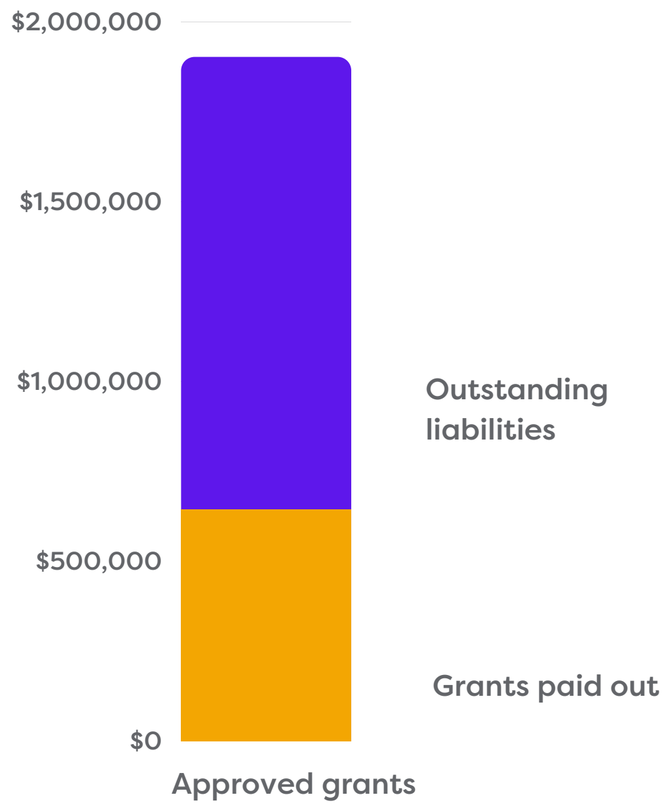
NB: This simplified financial snapshot does not include intangible or illiquid assets and liabilities that would appear on the Foundation's full balance sheet (e.g. the Zcash trademark, prepaid expenses, etc.).

Q4 ZCASH OPEN MAJOR GRANTS:

Zcash Foundation Q4 REPORT

The Zcash Open Major Grants Program (ZOMG) gives individuals and teams access to funding so that they can contribute to the growth of a rapidly-accelerating Zcash ecosystem. Some key areas include: core infrastructure, wallets, interoperability, apps, ongoing services, integrations, research and community. During Q4, ZOMG approved 8 grants totalling $895,960 USD.

- Of those newly approved grants, ZOMG paid out $168,485 USD for completed milestones.
- ZOMG also paid out $478,739 USD for grants approved in previous quarters.
- At the end of Q4, ZOMG had an outstanding liability of $1,498,710 USD for approved grants that were in progress.



ZCASH COMMUNITY GRANTS STEPS:

Please note that the Zcash Open Major Grants (ZOMG), rebranded to Zcash Community Grants in January 2022, as explained here.

1

Submit Proposal

Explaining how you can benefit the **Zcash ecosystem.**

2

Zcash Forums

Simultaneously post your proposal on the Zcash Community Forums for the community to provide their feedback on it.

3

Proposal Review

The reviewing Committee reviews the proposal, taking into consideration the community's feedback.

4

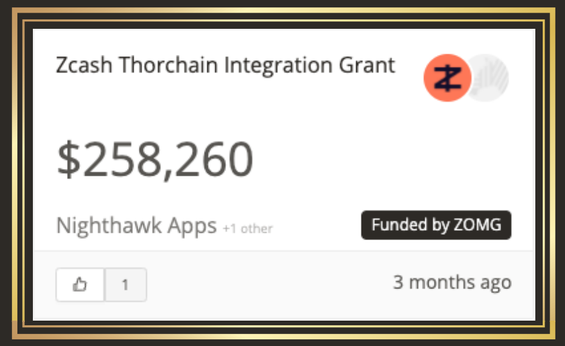
If Approved...

The requestor posts regular updates on the forums, requesting milestone payments as deliverables are completed.

Q4 APPROVED ZCASH OPEN MAJOR GRANTS:

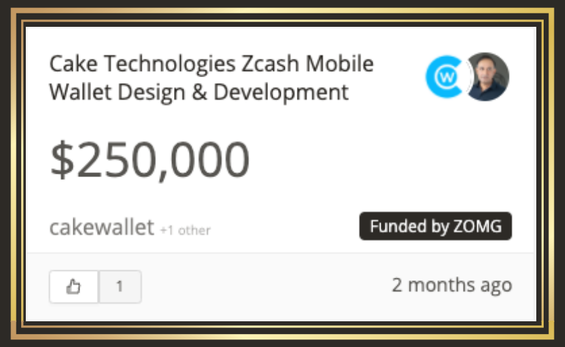
Zcash Foundation Q4 REPORT

About the recipients:



THORchain enables decentralized native ZEC swaps with popular cryptocurrencies, ERC20 tokens and stablecoins. THORchain will enable decentralized native ZEC swaps with popular currencies. Being the digital money focussed on privacy; adding support for Zcash on a DEX instead of wrapping the ZEC with a custodian opens up tremendous opportunity for existing and new Zcash users to acquire ZEC via simplified UX. The Foundation would like to thank the THORchain team and Erik Voorhees for their external pledges of support for this grant proposal.

Read more

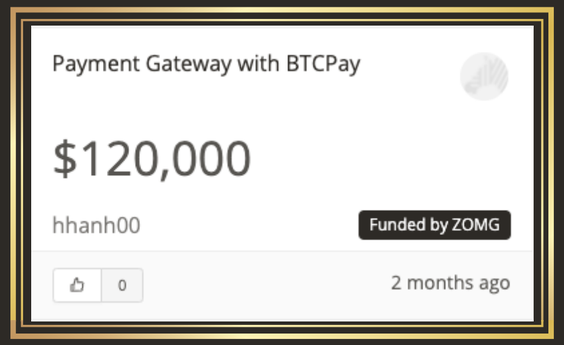


Cake Technologies, LLC is the company behind Cake Wallet, a noncustodial, open-source wallet for Bitcoin, Litecoin, and Monero. Cake Wallet has close to 200,000 users and has been around since January 2018. Cake Wallet is available on iOS and Android. With this grant, Cake Technologies would like to build a Zcash wallet that is compatible with NU5 and Halo Arc, heavily prioritizes using shielded addresses and fully shielded transactions, uses a simple interface similar to the existing Cake Wallet UI and is available for both iOS and android

Read more

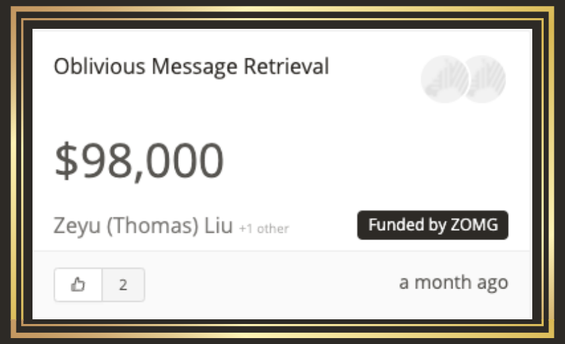
Q4 APPROVED ZCASH OPEN MAJOR GRANTS:

About the recipients:



Hanh is a software engineer who has worked for several major projects including: Windows (OS kernel), .NET framework (compiler and code generation) and SQL Server (Engine / query execution). He was also the CTO of startups and listed companies. He developed a payment gateway for Zcash and through this grant, aims to integrate it with the BTCPay payment framework.

Read more



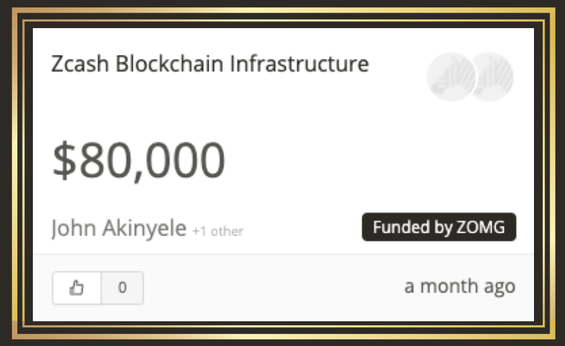
The main proposer is Zeyu (Thomas) Liu, a masters' student and Graduate Research Assistant at Columbia University. Thomas' research interests broadly lie in the field of cryptography, including lattice-based cryptography and blockchain-based protocols, as exemplified by his recent works on fully homomorphic encryption schemes and their applications. The proposal is submitted jointly with Eran Tromer, who will collaborate with Thomas on the academic research and will advise on execution and integration. Eran is an Associate Research Scientist at Columbia University, a coauthor of the Zerocash paper, a founding scientist of the Electric Coin Company and formerly an advisor to the Zcash Foundation.

Read more

Q4 APPROVED ZCASH OPEN MAJOR GRANTS:

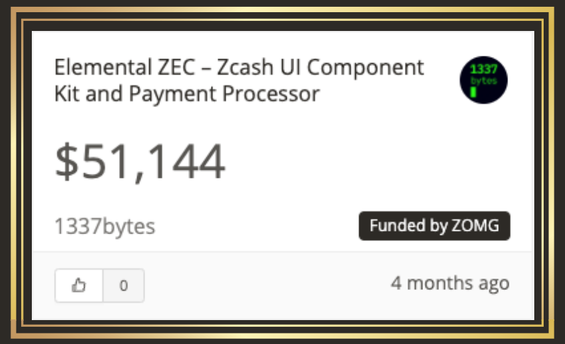
Zcash Foundation Q4 REPORT

About the recipients:



Alphega solutions is a consulting firm established by John Akinyele, an AWS Certified Solutions Architect Professional. The firm provides clients with solutions for migrating and implementing cloud-based production workloads. Alphega Solutions has been collaborating with Bolt Labs, Inc and Electric Coin Company since 2018 to implement a highly available Zcash full node and lightwalletd endpoint leveraging cloud-based containerized technologies.

Read more



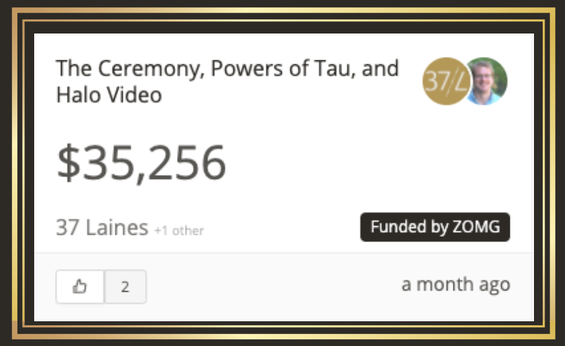
The applicant is a Software Engineer with experience working in web and app development, extensive expertise in building full-stack apps, design systems and server management; experience with JavaScript and Java. The goal of the proposal is to develop a set of open-source modular components and libraries for Zcash apps to use, including a minimal payment processor, compatible with BTCPayServer/BitPay API.The main users initially will be developers of existing and new Zcash apps. There will also be some example apps which can be used by ZEC holders, such as a Zcash donation app with a confirmation message or action, together with a demo Point of Sale app.

Read more

Q4 APPROVED ZCASH OPEN MAJOR GRANTS:

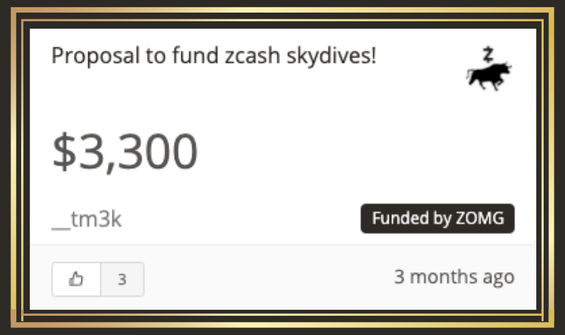
Zcash Foundation Q4 REPORT

About the recipients:



37 Laines is an award winning film production company run by Natasha Mynhier and Jeff Hammerton. In Q3 2021, they received a grant to produce a documentary about Zcash. This grant will fund production of an additional video to inform the world of the achievement of Halo.

Read more



_tm3k is a USPA B-licensed skydiver with 250+ jumps, located in California. He is also an outspoken and respected Zcash community member. The goal of his proposal is to create skydiving videos with a Zcash-branded parachute with the goal to bring awareness to Zcash in general. You can read more on his proposal by clicking on the button below:

Read more

COMMUNITY UPDATES: ZCAP EXPANSION

Zcash Foundation Q4 REPORT

The Zcash Community Advisory Panel is administered by the Zcash Foundation, and we are committed to making it more representative and independent. Following consultation with the Zcash community, the Foundation added new avenues for Zcash community members who make a meaningful contribution to the Zcash eco-system to join the ZCAP. These included:

Anyone who fulfilled all three of the following criteria:

- was a ZCAP member before June 2021, and
- did not invite another person to join ZCAP during the May/June expansion window, and
- was not removed from the ZCAP because they failed to vote in the most recent poll.

Zcash community members who had been active in the community since March 2020 also had the opportunity to volunteer to join the ZCAP.

In addition to this, the Zcash Foundation invited community members who met the following criteria to volunteer to serve on ZCAP:

- Grant recipients who had successfully completed more than 50% of their grant
- Community contributors who had:
  - made a meaningful contribution to one of the Zcash node projects on Github (zcashd and zebra),
  - authored or co-authored a ZIP (including ZIPs 1001-1013), or
  - led development of a significant Zcash software application, library, tool or similar.

The updated list of ZCAP members can be found here.

WE POLLED THE ZCAP ON ZOMG ELECTIONS AND ZIP 1014 AMENDMENT

The first Major Grants committee was elected in September 2020, and adopted the name Zcash Open Major Grants or ZOMG. In December 2021, the Zcash Foundation opened polling for the election of the next ZOMG Committee. The poll consisted of two questions:

- Which candidates should be elected to the next ZOMG Committee, and
- Whether ZIP 1014 should be amended to provide the ZOMG Committee with a discretionary budget.

Prior to the poll, the Foundation hosted a community call where the candidates introduced themselves and answered questions from the community. You can watch the call below, and the poll results can be found here.

THE ZCASH FOUNDATION WELCOMED A NEW CI/CD & DEVOPS ENGINEER

Zcash Foundation Q4 REPORT

Gustavo Valverde
DevOps Engineer

Gustavo has over ten years in information technology with experience in various fields, including information security, internal audit, business continuity, cloud architecture, DevOps, and product management. He has developed business continuity and disaster recovery plans development for financial institutions, built a DevOps culture at several startups, developed automated CI/CD workflows on complex teams, and supported critical infrastructures for SaaS solutions requiring high availability.

Gustavo loves continuous improvement and automation, and is eager to help with the automation of our development process and other DevOps-related subjects. He brings his hands-on experience using diverse technologies for platform management to help ZF build a DevOps culture.

Gustavo will support the rest of the engineering team with our testing infrastructure as we continue our work on zebra and help us with ongoing maintenance of our engineering infrastructure.

THANK YOU ZF BOARD

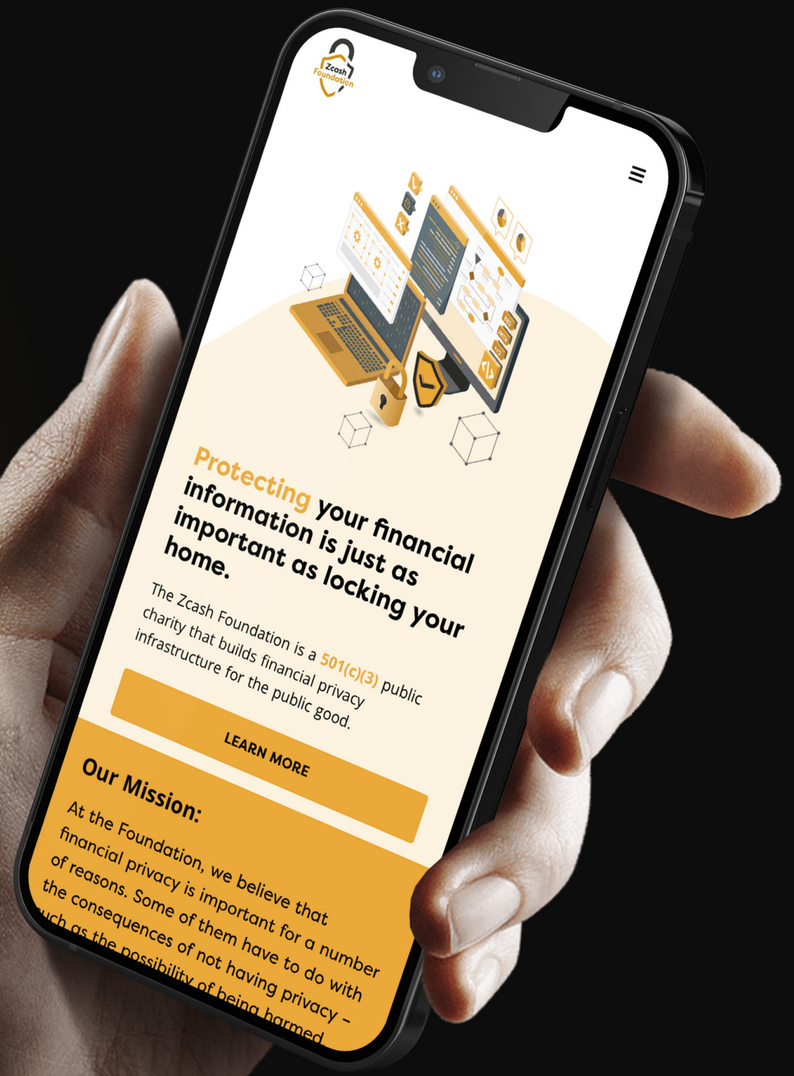
ZF would like to thank its board members for their continued contributions. Board service at ZF is voluntary - without compensation - and yet each year, our board members come together, dedicating their time and expertise to shape the future of the Zcash Foundation. ZF team acknowledges your efforts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

WE'RE REVAMPING OUR WEBSITE!

To better support our goal of improving the way we communicate with the Zcash community and the world at large, the Zcash Foundation is redesigning its website.

ETA: Q1 2022.



zfnd.org