Zcash Foundation
Q3 2021 Report

A review of Q3 development, expenses and approved grants.

A WORD FROM OUR EXECUTIVE DIRECTOR

This is our third 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 by category, 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!**

This quarter was a productive one for the Foundation Engineering team, as the new team members got up to speed, and they made progress towards our objective of releasing an "MVP" (minimum viable product) version of Zebra in late October.

The NU5 timeline continued to evolve, with the target date for mainnet activation being pushed back from late October to late November, and then to early 2022. As a result, we set ourselves a target of having Zebra capable of acting as a fully-validating node on the Zcash network by the time NU5 activates on mainnet.

In August, we consulted the Zcash Community Advisory Panel (ZCAP) regarding the reappointment of Andrew Miller, Matthew Green and Peter Van Valkenburgh to the Zcash Foundation's board, and sought the ZCAP's views on what the short- and long-term priorities for Zcash should be. The **results** have generated plenty of food for thought, and a lot of discussion on the Community forums.

In September, we recruited **Winfred as the Foundation's new Head of Communications**, filling a sorely felt need for better communications and transparency. Winfred began to have an immediate impact, reinvigorating the Foundation's social media presence, and overseeing the publication of our first quarterly report for 2021.

In Q3, the ZOMG Committee approved two grants, worth $278,014, and distributed over $320,000 for completed grant milestones. During Q2, it had become apparent that the Foundation needed to offer more and better support for ZOMG, in order to help attract more and better grant applications. To that end, we recruited Dan as the Foundation's Ecosystem Relations Manager. **Dan is a long-standing member of the Zcash community.** He will start full-time in his new role on October 1st, working with ZOMG and acting as a single point of contact for grant applicants. Winfred will also be providing support to ZOMG on the communications front, helping promote its activities and successes, and growing awareness of the availability of major grants.

During this quarter, we began preparing for the next round of elections to the ZOMG Committee. However, some **conflict of interest questions** emerged regarding whether it would be possible for a serving ZOMG Committee member to receive a ZOMG grant. To ensure clarity for candidates, we put the election timeline on hold so we can consult with current and prospective ZOMG Committee members, and obtain clear legal advice on this question. Resolving this issue and restarting the ZOMG election process is a key priority as we enter Q4.

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.
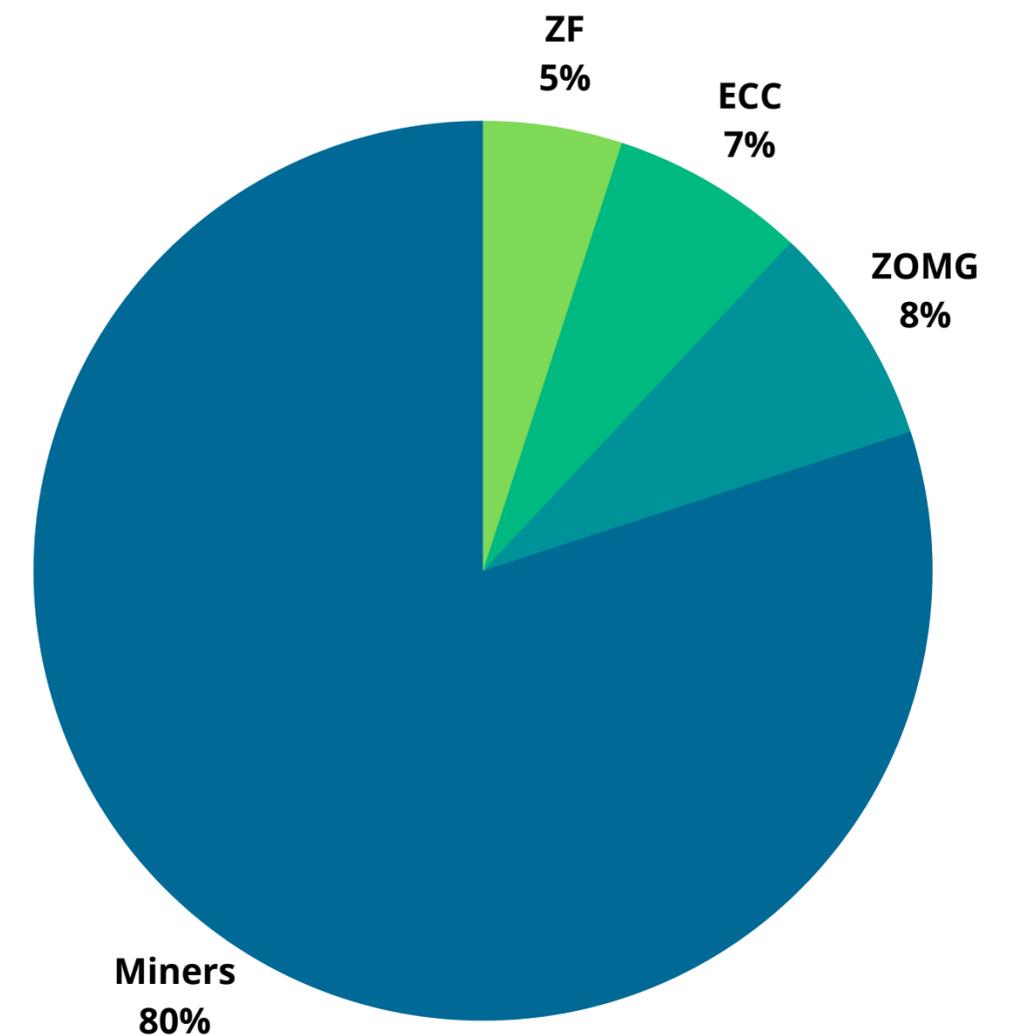
The existing structure stipulates that 80 percent of Zcash issuance continues to be distributed to miners, while 20 percent is devoted to Zcash development funding. **Of this 20%, 5% is allocated to support the work of the Zcash Foundation.** Another 8% of the total block reward (or about 40 percent 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.

ZF 5%
ECC 7%
ZOMG 8%
Miners 80%

Q3 '21 - ZF KEY FINANCIAL POINTS:

The USD value of funds received and held by ZF during Q3 was calculated using the following Messari closing prices for September 30:

- **$107.11 USD/ZEC**
- **$43,825.76 USD/BTC**
- **$3,000.82 USD/ETH**

ZF funds received:

- ZF received **16,467 ZEC ($1,763,780 USD)** from its slice of the Dev Fund during Q3, at an average of average of 5,489 ZEC ($587,927 USD) a month.
- ZF incurred approximately **$166,085 USD** per month in operating expenses.

Total held at end of Q3:

- ZF held $6,213,487 USD, 140,698 ZEC, 55 BTC, and 13 ETH for a total value of **$23,739,072 USD.**

Q3 '21 - ZOMG KEY FINANCIAL POINTS:

ZOMG Funds ZF received in Q3 at USD value were based on the following September 30 Messari closing prices:	**$107.11 USD/ZEC**
ZOMG restricted funds that ZF received:	- ZF received **26,377 ZEC ($2,825,240 USD)** - This was at an average of 8,792 ZEC ($941,711 USD) a month of ZOMG restricted funds. - ZF distributed **2,787 ZEC (valued at $321,049 USD** at the time of payment) of ZOMG restricted funds for grants approved by the ZOMG committee.
Total held at end of Q3:	ZF held custody of 71,750 ZEC (valued at $7,685,143 USD) and $1,453,297 USD for a total value of **$9,138,447 USD** restricted for use in funding major grants, as selected by ZOMG.

Q3 Summary:

Zebra Preparation for NU5 Testnet Activation

During Q3 2021, the engineering team focused on ensuring Zebra was ready to validate as many of the new NU5 consensus rules as possible, before NU5 activated on testnet.

We worked on the Orchard rules, and then we implemented related rules for Sapling, Sprout, and transparent transactions. We also started working on the implementation of Zebra's mempool, and added metrics dashboards that show Zebra's network communication and verification progress.

Q3 REPORT

The Zebra Book

Z E B R A

CI passing | codecov 77% | license MIT/Apache-2.0

About Zebra:

Zebra is the Zcash Foundation's independent, consensus-compatible implementation of a Zcash node, currently under development. It can be used to join the Zcash peer-to-peer network, which helps keeping Zcash working by validating and broadcasting transactions, and maintaining the Zcash blockchain state in a distributed manner. Please join us on Discord if you'd like to find out more or get involved!

These are some of the advantages or benefits of Zebra:

- **Better performance:** since it was implemented from scratch in an async, parallelized way, Zebra is currently faster than zcashd.
- **Better security:** since it is developed in a memory-safe language (Rust), Zebra is less likely to be affected by memory-safety and correctness security bugs that could compromise the environment where it is run.
- **Better governance:** with a new node deployment, there will be more developers who can implement different features for the Zcash network.
- **Runtime safety:** with an independeny implementation, the detection of consensus bugs can happen quicker, reducing the risk of consensus splits.

Sprint 13 →

For **Sprint 13**, the team continued to work on NU5, including Orchard and Transaction V5. We implemented new validation rules for transactions to:
- prevent double spends in the Sprout pool,
- check Sapling spends in V5 transactions, and
- validate parts of Orchard transactions.

Sprint 14 →

The Zcash Foundation's virtual team retreat took place during **Sprint 14**. This slowed down our delivery of new functionality during this sprint. However, we still managed to progress towards NU5 activation - with our **Zebra 1.0.0-alpha.14 release** which continued our work on Orchard and transaction v5.

Sprint 15 →

Sprint 15 was the last sprint where the team was fully focused on validating all of the NU5 consensus rules, before temporarily putting that aside to start implementing a mempool in zebra. During this sprint, the team finished the implementation of ZIP-244 in Zebra and partially implemented both ZIP-221 and ZIP-209. During this sprint, a majority of the team also attended a Rust training delivered by **Ferrous Systems** to ensure that we levelled up our Rust knowledge.

Q3 (SPRINT 16-18) ENGINEERING OVERVIEW

Sprint 16 →

For **Sprint 16**, we were excited to start working on implementing a mempool in zebra, which would move us closer to our goal of having a node that could fully participate in the Zcash network. During this sprint, we implemented the mempool component and storage. We also implemented a crawler to request transactions from peers to populate the mempool. In addition to this, we worked on ZIP-239 to implement transaction v5 data structures and network messages in the mempool. Finally, we finished the implementation of ZIP-209 and ZIP-221.

Sprint 17 →

During **Sprint 17** the team continued to focus solely on mempool work, implementing mechanisms to enable and disable the mempool - depending on chain synchronization state. Additionally, we started implementing the functionality needed to reply to requests for mempool data. We also implemented functionality needed for the downloading and verification of gossiped transactions from peers.

Sprint 18 →

For **Sprint 18,** we continued our work on the mempool, with a focus on testing. There was no release made at the end of this sprint since we were awaiting the NU5 testnet activation height. As this was subsequently changed, the team decided it was best to wait for the next sprint to tag a release containing this activation height.

Sprint 19 coincided with the activation of NU5 on testnet. As such, the team's attention was partially diverted from the mempool work onto the preparations to allow zebra nodes to participate in the NU5 activation on testnet by updating the required dependencies and consensus parameters. Our mempool work for this sprint was mainly focused on implementing mempool features which are exercised during network upgrade activation. Additionally, the team worked on updating the Zcash Foundation run DNS seeders with the NU5 testnet network protocol version.

Outside of Zebra land, the team continued working on FROST, with a number of team members engaged in helping out with an IETF draft. We started looking for potential FROST users and reaching out to exchanges to assess their interest in integrating FROST. At the end of August, *the FROST library* was submitted to and included in *Awesome Rust Cryptography,* a showcase of notable cryptography libraries developed in Rust - which is maintained by the *Rust Cryptography Interest Group's (RCIG).* At this time, the *ed25519-zebra* library was also included in the listing.

The Zcash Foundation also contributed to the next version of *the FROST CFRG draft,* moving it to a -01 status. Updates to the draft include specification of algorithms, serialization requirements, and additional discussion of security requirements and threat model.

During Q3, the Engineering team also helped the ZOMG by providing feedback when requested to help them with evaluation of grants. We also kept an eye on existing ZOMG grants, such as the *Arti* grant, ready to provide feedback and testing when required.

Q3 USE OF FUNDS:

During Q3 2021, ZF's operating expenses averaged approximately **$166,085** USD per month. The breakdown of resource allocation is illustrated in the table below:

Team compensation	**$394,224 USD**
General overhead expenses	**$83,180 USD**
Outreach, events expenses	**$13,275 USD**
Meals and entertainment	**$77 USD**
ZOMG member compensation	**$7,500 USD**
TOTAL	**$498,256 USD**

Outreach 2.7%
ZOMG 1.5%
General* 16.7%
Team Wages* 79.1%
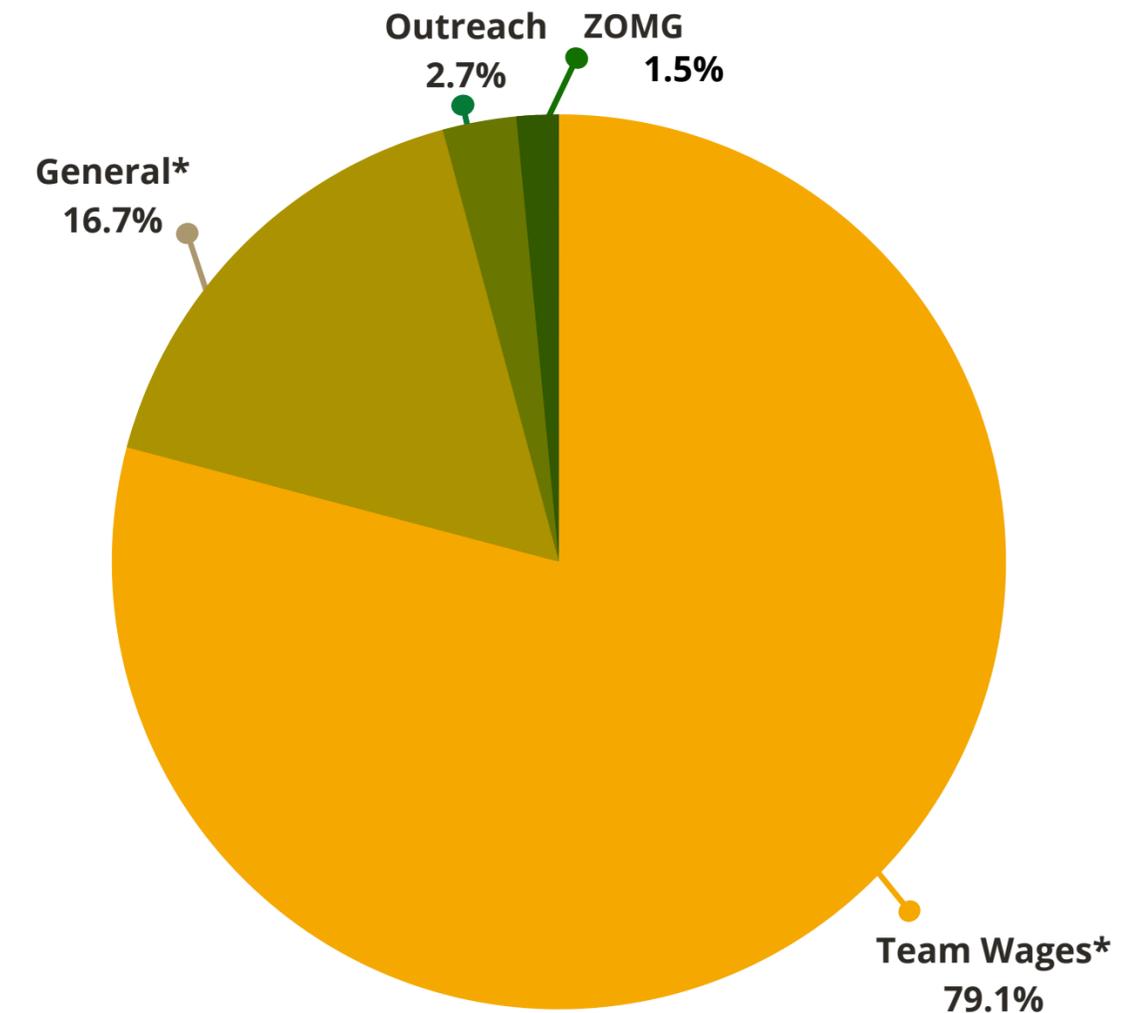
* Team wages encompasses all compensation and benefits paid to ZF staff and contractors. ZF does not operate any form of retention bonus or deferred compensation scheme.

*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.

Q3 PROGRAMS:

The following chart explains what type of programs the Foundation invested in during Q3. Please note, each team member's compensation and benefits are allocated to the program(s) they contribute to.

Management & General	**$119,815 USD**
Community	**$29,580 USD**
Protocol (Zebra)	**$311,693 USD**
Science (FROST)	**$4,348 USD**
ZOMG support	**$32,820 USD**
TOTAL	**$498,256 USD**

Zcash Foundation

ZOMG support 6.6%

Science (FROST) 1%

Management & General 24%

Community 5.9%

Protocol (Zebra) 62.6%
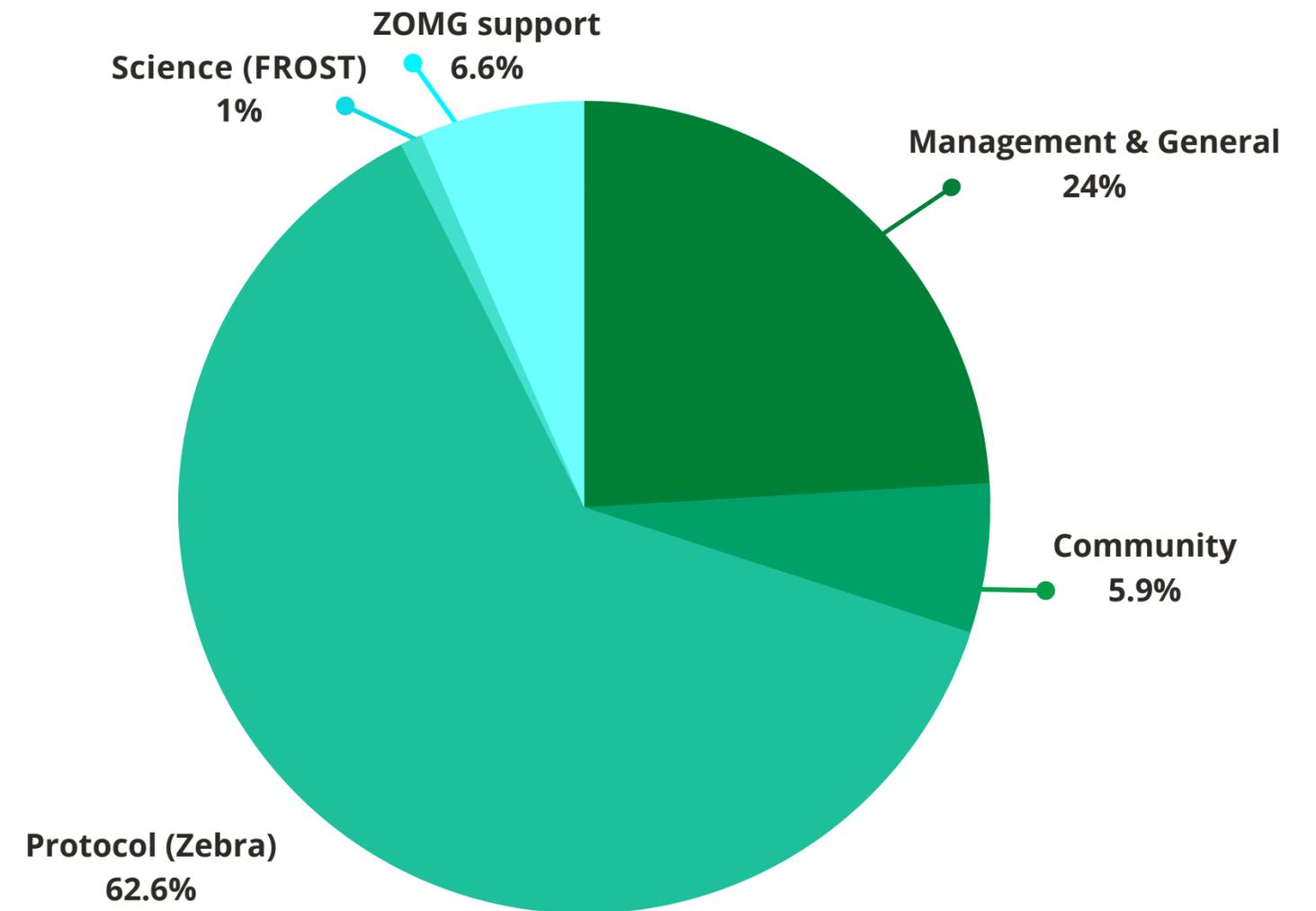
Q3 FINANCIAL SNAPSHOT:

LIQUID ASSETS:	UNRESTRICTED FUNDS		FUNDS RESTRICTED FOR ZOMG	
	COIN BALANCE	USD VALUE	COIN BALANCE	USD VALUE
USD		$6,213,487		$1,453,297
ZEC	140,698.35	$15,070,200	71,750.08	$7,685,151
BTC	55.14	$2,416,701		
ETH	12.89	$38,694		
		$23,739,082		**$9,138,447**
LIABILITIES:				
Grant commitments		$26,889		$1,258,236
Accrued Expenses & Payroll Liabilities		$124,987		
		$151,876		**$1,258,236**
NET LIQUID ASSETS: (Liquid assets less liabilities)		**$23,587,206**		**$7,880,211**

CLOSING PRICES: SEPTEMBER 30,2021
(Used to calculate USD value of coins)
- $107.11 USD/ZEC
- $43,825.76 USD/BTC
- $3,000.82 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.).

Q3 ZCASH GRANTS SUMMARY:

The Zcash Open Major Grants Program 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, interoperability, apps, ongoing services, integrations, research and community. During Q3, **ZOMG approved 2 grants totalling $278,014 USD.**

- Of those newly approved grants, ZOMG paid out **$4,168 USD** for completed milestones.

- ZOMG also paid out **$40,920 USD** for completed milestones for grants approved in Q1 and **$275,969 USD** for completed milestones for grants approved in Q2.

- At the end of Q3, ZOMG had an outstanding liability of **$1,258,236 USD** for approved grants that were in progress.

$2,000,000

$1,500,000

$1,000,000

$500,000

$0

Outstanding liabilities

Grants paid out
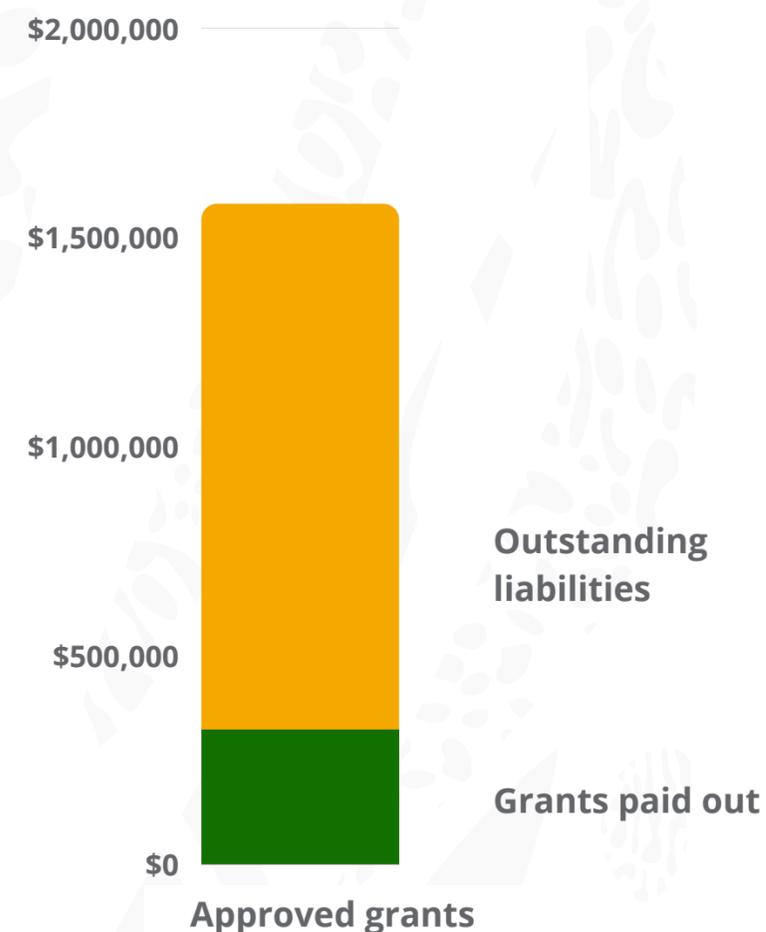
Approved grants

Q3 APPROVED ZCASH GRANTS:

About the recipients:
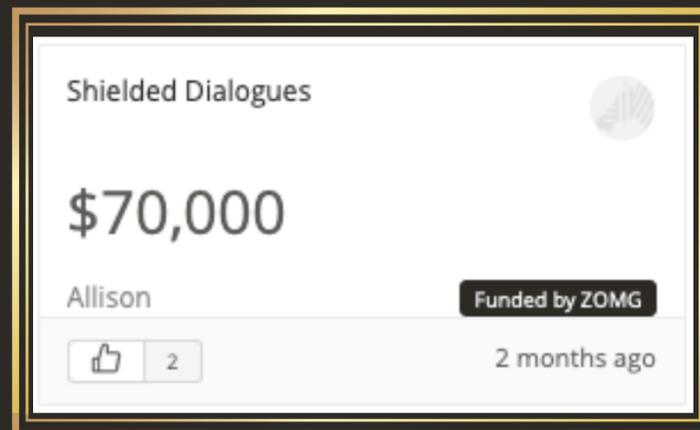
Shielded Dialogues

$70,000

Allison | Funded by ZOMG

👍 2 | 2 months ago

The grant applicant, Allison, runs a science and tech non-profit that has a monthly keynote podcast series with ~10k technology-oriented subscribers on Youtube, up to 80k views per video, and a strong existing network with the proposed interviewees for this grant. The Shielded Dialogues work is slated to begin in the beginning of 2022.

Read more
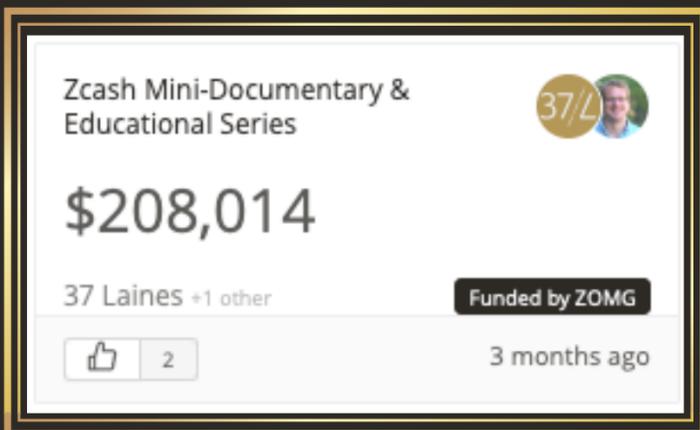
Zcash Mini-Documentary & Educational Series

$208,014

37 Laines +1 other | Funded by ZOMG

👍 2 | 3 months ago

37 Laines is an award winning film production company run by Natasha Mynhier and Jeff Hammerton. Out of their offices in Santa Monica and Denver, 37 Laines produces high quality creative work for clients across the US, including branded content, commercials, short films, music videos, digital content, web-series, live events, and documentaries. The Zcash Documentary & Educational Series project is a collaboration between 37 Laines, the Zcash Foundation, Electric Coin Company and the Zcash Open Major Grants.

Read more

ZCASH GRANT APPLICATION STEPS:

1 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.

2 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.

3 **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.

4 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.

Q3 UPDATE: ZOMG COMMITTEE SUPPORT

Early in September, the Zcash Foundation increased its support for the ZOMG committee by increasing the committee members' estimated time commitment from five hours per month, to fifteen hours per month. This resulted in an **increase in the nominal compensation for each member from $500 to $1,500 per month.** (The nominal compensation amount is at a rate of $100 per hour - a rate which is based on the average salary of a CEO of a non-profit with an annual budget of between $3.5 million and $13.4 million USD.)

The Foundation also **recruited more staff** in Q3 - who will work with the ZOMG Committee to promote and publicize the availability of major grants. These staff members will help ZOMG build a pipeline of grant applications, relieving them of the time-consuming communications and liaison responsibilities that have been demanding their time and attention.

Since November last year, the Zcash Foundation has also has provided support to ZOMG in the form of **minute-taking during ZOMG meetings, undertaking KYC and OFAC compliance checks for grant recipients, payment processing, and record keeping**. The Foundation took these activities on so as to enable the committee to better focus on their decision-making strengths. The Zcash Foundation is also **facilitating the coordination of community calls** aimed at bettering the operation of the ZOMG program.

ZF is earnest in its efforts to support the ZOMG and will be looking into additional ways that it can do so - without interfering with the committee's ability to make independent grant decisions.

WE WELCOMED WINFRED - OUR HEAD OF COMMS - IN SEPTEMBER

Winfred K. Mandela
Head of Comms

In this role, Winfred leads all Foundation communications activities. Over the past five years, Winfred has remained dedicated to blockchain projects, linking their innovations to customer-focused operations to build brands, create customer awareness and to drive customer preference for blockchain as a beneficially disruptive technology. Winfred has also been an active advocate for blockchain, presenting blockchain use-cases at high level events including those organized by the United Nations. During her time in the space, Winfred has had success on business development fronts, helping blockchain projects identify and secure grants from governing bodies and financial institutions.

A true blockchain enthusiast, Winfred's entry into the space was in fact as a trader. For several years now, she has been active on various financial markets and enjoys spending a lot of her free time analyzing trends for opportunity. In her role at the Foundation, Winfred is excited to tackle all things communications, and has already expressed determination to bring the Foundation's communicative practices to greater heights.

WE WELCOMED DAN - OUR ECOSYSTEM RELATIONS MANAGER - IN SEPTEMBER

In this role, Dan will take over some of the administrative tasks that the ZOMG is currently responsible for. Dan, known to the Zcash community as @decentralistdan on Twitter and on the forum, has been in the cryptocurrency space since 2017. He has been an active community member of both the Ethereum and Bitcoin ecosystems, and over the last three years he has focused almost exclusively on the Zcash ecosystem and its community, where:

- He started ZcashZeal, a Zcash community-focused Twitter account and blog.
- Zcash community members also voted for him to become one of the first forum moderators.
- He ran for the inaugural ZOMG committee last year.
- He is a Zcash Community Advisory Panel member.

Prior to joining ZF, Dan's work experience has been in the broadcasting industry - where he has spent the last decade working in Network television doing audio visual production. In addition, he has four years governance experience as an elected official to the Board of Trustees for his local 501c3 union.

Dan will work towards fostering stronger community relations by engaging with the Zcash community on the different ZF platforms, engaging frequently with members of the ZCAP, as well as with other Zcash ecosystem stakeholders.

Dan
Ecosystem Relations Manager

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.

Zcash Foundation

zfnd.org