ZOMG Whitepaper: Version 1.0

Last updated 6 June 2021

Table of Contents

A Story from the Future...

The year is 2030. Crypto is ubiquitous across our financial system. People are paying for their utilities and their daily coffee with stablecoins and cryptocurrencies. Retail investors have access to investment choices previously only available to people in certain countries, of certain wealth levels, and with privileged networks. Many are even earning their salaries in cryptocurrencies.

Against this backdrop of financial options, privacy-focused cryptocurrencies and privacy-protecting applications help individuals protect their safety and freedom. Their utility provider (nor any rogue employee) doesn't have knowledge of their crypto net worth. Criminal hackers do not gain access to information that could be financially devastating to victims, even if they succeed in compromising a database (which they often do). People are able to maintain lifestyles of their choice in private, without fearing that information on where they spend their money makes them vulnerable to punitive behavior from people with power over them. Individuals are able to advocate for their beliefs, without fearing that governments or large corporations can cut them off entirely from the financial system.

Today, in 2021, the social and political winds of change in the world are evolving rapidly. They have been since the Global Financial Crisis in 2008. Vast inequalities in the world and growing tension between superpowers with much to lose have led to dangerous confrontations, both domestic and international. Political polarization and the friction of changing social norms have led to people who are both angry and scared. Ubiquitous surveillance programs facilitated by rapidly advancing technology can be abused or misused, leaving you vulnerable to victimization. Cybersecurity breaches continue to threaten our financial and physical well-being. *It is clear that the world around us is destabilizing, and we cannot take our safety for granted.*

Zcash isn't a panacea for all these problems, but it is a tool with which we can protect the people and communities we care about.

Private finances are how we keep ourselves, our families, our communities, and our nations safe and free in the world. Without the ability to live freely, we can only live according to someone else's preferences, often in fear and with regret. In contrast, when we are able to live freely, we can build the world that we want.

The time to take back our freedom is now.

Introduction

Zcash provides individuals with the ability to preserve their freedom through financial privacy. The ZOMG was forged from the Zcash community in 2020, with the support of everyday heroes who wanted to see Zcash serve more people around the world. Together with the Zcash Foundation and the Electric Coin Company, we aspire to provide the means for individuals, wherever they are, to live free from unwanted scrutiny and unfair control.

80% of each Zcash block reward goes to miners. Of the remaining 20%, 40% goes to the ZOMG, from November 2020 to November 2024. ZOMG's responsibility is to allocate the funds towards grants that will help Zcash succeed. As an independent decision-making body from the ECC or ZF, ZOMG receives the largest slice of the block-reward of any non-mining entity. **ZOMG's mission is to make Zcash ubiquitous: wherever someone wants to use ZEC, they are able to use ZEC - easily and safely.**

The purpose of this paper is to lay out how we think we can achieve our mission. Version 1.0, first published as a working draft in June 2021, is co-written by (in alphabetical order): Chris Burniske (forum handle: @cburniske), Hudson Jameson (@Souptacular), Michelle Lai (lead author, @ml_sudo), Shawn (@minezcash) and Holmes Wilson (@holmesworcester).

Note: The paper is a living document. As the environment and players around us evolve, we expect to adapt parts of this document.

What Success Looks Like

When Zcash is ubiquitous, we believe this is what the world will look like:

From a technical angle

1. There is widespread adoption of ZEC across major financial applications such as DeFi, payments, tools for traders/investors, and other future innovations.

2. There is an active and substantial ecosystem of useful applications built on top of Zcash, including NFTs, stablecoins, means to earn salary in ZEC, and other future innovations.

3. There is strong infrastructure to support the building of financial and other useful applications. This includes block producers, scaling solutions, and other tools to track the health of the Zcash ecosystem.

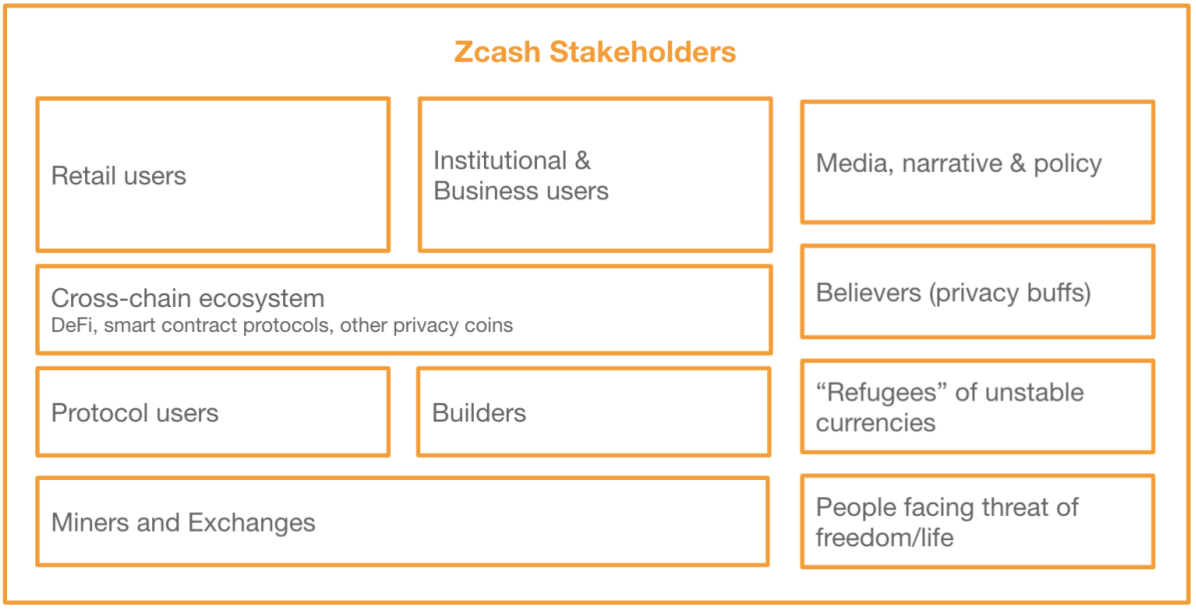
From a social angle

1. Zcash retains leadership in privacy features, with #1 mindshare. In the same way Ledger and Trezor are synonymous with self-custody today, when individuals or organizations think about privacy in this future state, they think about Zcash.

2. Arguments for privacy in on-chain transactions are widely-accepted. The belief that "privacy is only needed for nefarious action” is gone.

How to Succeed: Make ZEC Ubiquitous

Here is the market map of how we see the Zcash ecosystem. For Zcash to be ubiquitous, each stakeholder segment needs to have easy and safe ways to interact with ZEC.



Retail users		
Priority High	**Definition** Individuals who hold and use ZEC, reasons including investment and interest in private economic action.	**Actions taken with ZEC** Learn about Zcash/ZEC. Acquire and trade ZEC. Earn yield on DeFi platforms. Hold wealth (hodlers). Spend wealth. Keep assets safe from external factors including inflation and theft.
	Tools Available Today ● Informational: https://z.cash/, https://zfnd.org, https://electriccoin.co/ ● Community: https://forum.zcashcommunity.com/, Telegram, Discord, YouTube, zecpages.com ● Wallets with shielded support: ZECwallet Lite, Nighthawk, Unstoppable (multi-asset). Wallets with transparent support: many ● Payments: paywithz.cash ● DeFi wrappers: renZEC available via Ren Protocol	
	Where Work is Happening ● Secure and convenient ways of storing large amounts of ZEC e.g. hardware wallet support: Ledger support by Zondax (funded by ZOMG); offline wallets: cold wallet (funded by ZOMG) ● ZEC listing on more exchanges globally, with support for shielded where possible (ECC priority) ● Improving UX in wallets such as Zecwallet and Nighthawk (funded by ZOMG)	
	Gaps and Needs (some ideas) ● Browser extension wallet for ZEC (like Metamask) ● Shielded transaction support on popular multi-asset wallets ● Payment URIs. Easy one-click shielded payments. ZEC support on BTCPay, the	

	leading decentralized crypto payments service ● Ongoing support for Zecwallet Lite and Nighthawk wallet, including security review ● Additional features in Unstoppable wallet, especially for ZEC-swaps and DeFi features ● Updated docs for using Zcash on Tails, Qubes, and Whonix, which are privacy-focused OSs ● Better built-in network layer privacy (ZOMG is funding work on Tor integration) ● Marketing campaign to encourage ZEC holders to move ZEC from transparent to shielded addresses (potentially with matched funds) ● Convenient ways to spend ZEC in daily life with a wide variety of merchants

Institutional & Business users		
Priority Medium	**Definition** Institutions who add ZEC to their investment portfolio. Enterprises who use Zcash technology to conduct or secure their businesses, or to collect payments.	**Actions taken with ZEC** Acquire and trade ZEC. Accept ZEC as payment for goods and services. Use ZEC for transactions that they don't want known to competitors or other actors.
	Tools Available Today ● ZECFUND, Grayscale's Zcash Trust ($50mn AUM) ● Wrapped Zcash (ERC-20) by Anchorage, available for institutions	
	Where Work is Happening ● Business development efforts led by Electric Coin Company (ECC)	
	Gaps and Needs (some ideas) ● Greater AUM for ZECFUND ● ZEC ETF ● Assistance to fund managers to maintain compliance with regulatory and administrative requirements (FAQs, regulator conversations, etc) ● Support for ZEC by crypto payments processors e.g. Bitpay (centralized), BTCPay (decentralized) ● Zcash custody solutions for institutional Zcash holders	

Cross-chain ecosystem		
Priority Medium	**Definition** DeFi platforms. Smart contract protocols (e.g. Other privacy coins and solutions (e.g. Decred, Tornado Cash, Keep Network, Agoric).	**Actions taken with ZEC** Incorporate ZEC or wrapped ZEC into AMMs, lending protocols, etc. Build bridges between Zcash blockchain and other blockchains e.g. Cosmos, Polkadot, Binance Smart Chain. Bring wrapped assets (ETH, ZEC) to ZEC.
	Tools Available Today ● renZEC, by Ren Protocol	
	Where Work is Happening ● Creating renZEC liquidity on AMMs built on Binance Smart Chain (funded by ZOMG) ● Preliminary work on User Defined Assets (UDAs) to allow minting arbitrary tokens on Zcash (called ZSA's, or Zcash Shielded Assets, at the ECC). ECC is also conducting economic analyses on the potential impact of ZSA's on ZEC	

	Gaps and Needs (some ideas) ● Stablecoins on Zcash e.g. ZUSD, zCUSD, zDAI, zUSDC ● Support for ZEC on Decred's new DEX ● Establish liquidity in new cross-chain AMMs e.g. Thorchain ● Establish liquidity for Zcash on Ethereum (e.g. renZEC on Bancor) ● Build ZEC availability on cross-chain efforts built on Cosmos, Polkadot, etc. ● Complete technical work on UDAs, and bring popular assets to Zcash through cross-chain exchanges ● Generally, greater variety and liquidity in wrapped ZEC on a variety of smart contract platforms, including support on decentralized exchanges, and further integration in DeFi sectors such as lending, borrowing, and asset management

Protocol users		
Priority Medium	**Definition** Individuals and teams that interact with Zcash the technology as a network, as a set protocols, or as open source tools. Users of zk-snark technology.	**Actions taken with ZEC** Contributing to the evolution of the Zcash protocol. Analyzing Zcash's security properties. Contributing to Zcash implementations like zcashd or Zebra. Adding features to Zcash.
	Tools Available Today ● Specification, source code	
	Where Work is Happening ● The Arborist Calls	
	Gaps and Needs (some ideas) ● Alternative implementations of the Zcash client Solutions to network layer privacy ● Layer one scaling improvements ● Layer two scaling: ZK rollups for Zcash, state channels ● Smart contracts / general purpose programmability ● Formal verification ● Easy multi-sig tools for Z-addresses (e.g. an implementation of FROST in user-facing wallets) ● Light client servers / infrastructure ● In-protocol economic incentives for infrastructure operators	

Builders		
Priority High	**Definition** Devs at the ECC or ZF, and teams who build on top of Zcash, creating value for the entire Zcash community.	**Actions taken with ZEC** Reading from and writing to the Zcash blockchain. Contributing to the underlying clients (zcashd, zebrad).
	Tools Available Today ● Android SDK for mobile wallets ● iOS SDK for mobile wallets ● lightwalletd, a backend service providing an interface to the Zcash blockchain ● Testnet faucet (funded by ZOMG)	
	Where Work is Happening ● Tor support for Zcash (under consideration by ZOMG) ● Blockchain explorer, with support for viewing keys and other Zcash features	

	(funded by ZOMG) ● Stability testing (funded by ZOMG) ● libzebra
	Gaps and Needs (some ideas) For devs at the ECC or ZF ● Performance improvements to core code, protocols, and popular libraries ● Security auditing for popular libraries, and wallets ● Tools to measure the health of the Zcash network/ecosystem, e.g. a high quality network explorer, network security tooling (e.g. Observatory proposal) ● Identify parts of the Zcash codebase that are security-critical and conducive to formal methods for proving correctness of code ● Use start-of-the-art formal verification tools to construct computer-checkable proofs of their correctness, with respect to suitable security specifications ● Ideas for such components: Sapling circuits (or parts thereof), Bellman cryptographic code (or parts thereof), consensus rules For app builders ● An easy way to get on-ramped into the Zcash ecosystem and learn how to use Zcash securely (docs, forums, website, videos, SDKs) ● "Mastering Zcash" book ● An improved "Zcash Protocol Spec" for developers ● Performance improvements to SDKs and libraries ● React Native SDK and libraries ● Network layer privacy solutions for SDKs and libraries

Miners and Exchanges		
Priority Acceptable state	**Definition** Miners are teams or individuals that produce blocks and earn ZEC block rewards. Exchanges are centralized and decentralized exchanges where ZEC can be traded.	**Actions taken with ZEC** Miners: Processing transactions, receiving ZEC block rewards, liquidating ZEC. Exchanges: Keeping a treasury and ledger of ZEC assets (where applicable), maintaining an order book or liquidity pools (AMMs), settling with counterparties.
	Tools Available Today ● zcashd (ECC) ● Mining guide	
	Where Work is Happening ● zebrad (ZF)	
	Gaps and Needs (some ideas) ● DIY mining kits, like Casa for bitcoin ● DevOps tooling for Zcashd+Lightwalletd, to encourage community members to deploy and maintain Zcash infrastructure ●	

Media, narrative, and policy advocacy		
Priority High	**Definition** News, blogs, and other material that contribute towards creating the right narrative for Zcash. The goal is to increase interest and adoption of	**Actions taken with ZEC** n.a.

	ZEC, and in particular shielded transactions.	
	Tools Available Today ● None	
	Where Work is Happening ● Blogs and YouTube channels of electriccoin.co, zfnd.org ● Crypto enthusiasts around the internet with no official affiliation to Zcash who create YouTube videos, podcasts, blog pieces, etc	
	Gaps and Needs (some ideas) ● Fiction and nonfiction writing highlighting the need for privacy, especially written for people who are on the fence ● Weekly Zcash newsletter, that helps interested individuals and teams stay up-to-date on what's happening with Zcash (without needing to spend hours on the forums/blogs/youtube) ● Market and user study: who are our current and potential users? ● Regulator-friendly 101 pieces on the pros, cons, and selective-privacy features of Zcash ● Joint publications with personal data protection privacy watchdogs (governmental or non-governmental) ● Informational campaigns for areas of the world where privacy is necessary to protect certain individuals from political, religious or social persecution ● Partnerships with humanitarian organizations to bring financial freedom and privacy to their beneficiaries ● Rapid response public mobilization campaigns to specific regulatory threats to Zcash, privacy-focused cryptocurrencies, self-hosted wallets, etc	

Unfinished categories [Work In Progress. Suggestions and comments welcome]:

1. Believers (privacy buffs).
2. "Refugees" of unstable currencies.
3. People facing the threat of freedom/life.

Notes on Strategy

Areas of focus

We'd like to spread ZOMG funds in a way that narrows the gap in as many stakeholder territories as possible. Retail Users, Builders and Media are some of the most important stakeholder categories where we have urgent gaps to close. Therefore, our focus will be on categories that are marked as Red or Orange. We believe that when we achieve "green" (Acceptable State) in all the major stakeholder categories, anyone who wants to engage with the Zcash ecosystem will be able to do so easily and effectively.

Soliciting applications

We expect that the vast majority of grants will be proposed independently by teams and individuals who want to see more privacy tech in the world. However, if we see an unmet

gap in any certain category, we will actively solicit applications from capable teams, in the form of bounties.

Profile of grantees

We'd like to provide grants to teams of all sizes, from the individual hobbyist to specialist teams. Hobbyists and small teams have been the lifeblood of the Zcash ecosystem since our launch in 2016, alongside the ECC and the Zcash Foundation. We'd also like to reach out to large organizations who may not be actively looking to apply to grant programs nor focused on ZEC, such as exchanges and widely adopted wallet providers. This will allow us to tap into their network of users and infrastructure, and ultimately accelerate our impact. We believe that this mix of small and large teams will allow us to spread more quickly and effectively across the sea of potential ZEC users.

Impact timeline

We distinguish "hair on fire" projects from "moonshot" projects based on how quickly they need to be solved and how quickly value is likely to be realized. An example of a "hair on fire" projects with urgent gaps to fill are the Zecwallet and Nighthawk mobile wallets, which are mainstays of ZEC usability today. An example of a "moonshot" project is support for Tor's Arti implementation, which has secondary benefits for Zcash in the form of metadata privacy when Zcash nodes and wallets are used.
As stewards of the funds allocated to the ZOMG, most of the projects we approve will need to have clear and immediate benefits for the Zcash community. These projects can take the form of months-long development projects, or weeks-long experiments with DeFi projects. On the other hand, we believe some projects are going to require significant time and investment to realize outsized benefits over the long term, and we are willing to make opportunistic investments with such impact profiles.

Pace of allocation

We're not in a rush to deploy ZEC. Over the 4-year life of the ZOMG, our funds are limited by design. We intend to maximize their runway and impact by only awarding funds to projects that we believe have the greatest mileage. We will have an emphasis on strategic value, and on quality. Furthermore, with ZEC's supply halving every 4-years, and uncertain ZOMG funding past 2024, we hope for other ZOMG committees to prudently manage funds such that ZOMG can accrue a sizable treasury to fund grants well into the future.

Shielded vs transparent transactions

We have a bias towards projects that support shielded transactions by default, as we believe that helps us achieve our mission of helping people live free lives more quickly. However, there are technical and regulatory barriers that make shielded transactions harder to support in some cases. We believe that transparent transactions are sufficient in the majority of

transactions as long as a shielded transaction is occasionally employed. Therefore, we will not hold back support for projects that predominantly support transparent transactions.

Coordination with ZF and ECC

We believe that for maximum impact, the ZOMG needs to actively collaborate with the Zcash Foundation and the ECC. While we make funding decisions independently of both organizations (and in particular the Zcash Foundation, which is the legal entity that disburses ZOMG funds), it is important to us that the funds we allocate achieve synergies with the work that both organizations are doing.

Success Metrics

We would consider our efforts to be successful when Zcash is commonly referred to and used as the private version of Bitcoin by people usually outside of the Zcash community. Perhaps one day Zcash may even overtake Bitcoin in dominance. See the above section “What Success Looks Like” for more qualitative measures of success.

Quantitative metrics are tricky with Zcash due to the inherently privacy-preserving nature of z-transactions and the apps that find a natural fit with Zcash (e.g. p2p wallets with anonymity promises).

Nonetheless, here are some metrics that we could document over time.

Note: This is a work in progress, and needs to be finalized together with the ZF and the ECC, who possess the expertise and the ability to measure these figures on an ongoing basis.

Transaction volumes (t and z)

- Overall
- On exchanges
- In DeFi
- In Payments

Shielded transactions

- Number of transactions Z2Z, Z2T, T2Z (+ as % of shielded transactions)
- Volume of shielded transactions Z2T, T2Z
- Value in the shielded pools

Number of users

- Zebra and ZcashD
- Wallets
- Nodes running

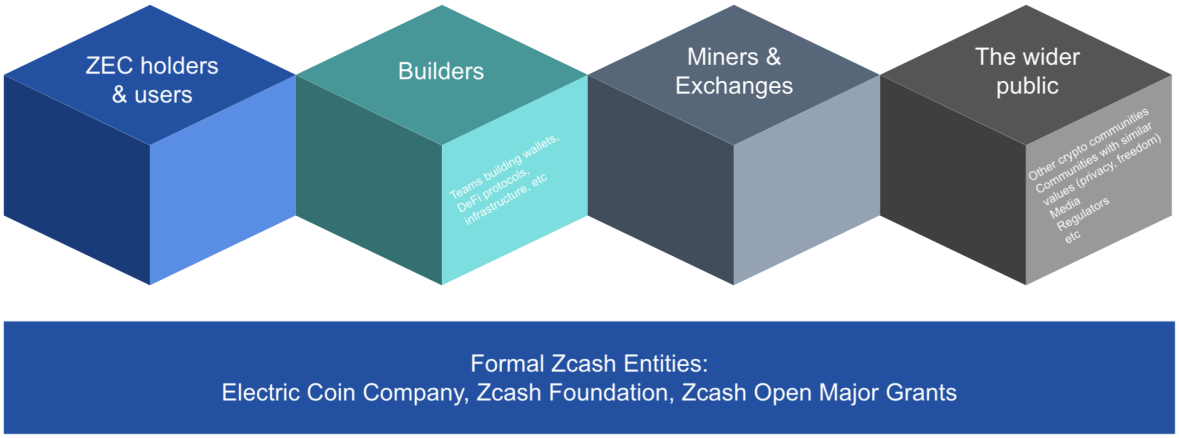
Others

- ZEC or wrapped ZEC ranking within the top 30 most used applications (?)
- The "payments" metric as measured by Messari seeks to measure on chain economic activity and seems to be a reasonable proxy for overall project health and interest

Basic Assumptions

Who comprises the Community?

When interacting in Zcash forums (such as on our website zcashomg.com, on zcashcommunity.com, on Discord, or on Telegram), we use the "Community" to loosely refer to several major groups of individuals and teams (see diagram below). This is a lower-resolution definition of "Stakeholders" which we defined earlier in this paper.



How is the ZOMG different from ZF and ECC?

The Electric Coin Company (ECC) invented Zcash and is responsible for engineering much of the Zcash related software that exists today. The mission of the ECC is to **empower people through economic freedom**. They support Zcash through research and development, engineering, partnerships and regulatory efforts.

The Zcash Foundation (ZF) is a 501(c)(3) public charity that builds **financial privacy infrastructure for the public good**, primarily serving the users of the Zcash protocol and blockchain. The Foundation also supports other applications of zero-knowledge cryptography, as well as other approaches to private cryptocurrency.

ZOMG (Zcash Open Major Grants) exists to fund projects that advance the usability, security, privacy, and adoption of Zcash. Legally speaking, ZOMG is a technology advisory board that constitutes a committee of the Zcash Foundation, under its bylaws. Grants are

chosen by a committee of five members who were chosen by the Zcash Community Advisory Panel in an open election. ZOMG is one of the major funding pillars of Zcash, alongside the ECC and ZF. Although ZOMG is not directly affiliated with the ECC, we work closely with the ECC and other groups to help our mission to distribute our grant funds in the most efficient and effective ways possible.