Zen White Paper

Robert Viglione, Rolf Versluis, and Jane Lippencott *

May 2017

Abstract

Zen is an end-to-end-encrypted system with zero-knowledge technology over which communications, data, or value can be securely transmitted and stored. It is an integration of revolutionary technologies that create a system over which innovation can accelerate by combining three functions that are traditionally done separately: 1) transactions 2) communication, and 3) competitive governance. This is done in a secure and anonymous manner, using a worldwide distributed blockchain and computing infrastructure. The system integrates multiple best-in-class technologies to form an open platform for permissionless innovation that can evolve with user preferences.

*The authors can be reached at rob@zensystem.io, rolf@zensystem.io, and jane@zensystem.io, respectively. We would also like to thank Jake Tarren for comments and suggestions, as well as the broader Zclassic and Zen communities for helping us develop these ideas and make this movement possible.

Contents

1 Purpose

"Critique by creating." -Michelangelo Buonarroti

We live in a hyper-regulated and surveilled world where billions of individuals are deprived of basic human rights, such as property ownership, privacy, free association, and access to information. The technology now exists to solve some of these problems, and Zen's early implementation will do exactly that.

Zen is a collection of products, services, and businesses built around an enabling technology stack employing zero-knowledge proofs and a core set of beliefs. As a distributed blockchain system leveraging the latest censorship-evading techniques, fully encrypted communications, and a social and governance model designed for long term viability, Zen will contribute to the human right to privacy and provide the necessary networking infrastructure for people to securely collaborate and build value within a borderless ecosystem. Our mission is to integrate the latest technologies available post-Satoshi with a decentralized, voluntary, and peaceful set of social structures to improve life for anyone who wants to participate. We believe that this is an idea whose time has come.

Zen's framework is a secure, privacy-oriented infrastructure with a governance system structured to enable participants to collaboratively extend functionality in many dimensions. Opportunities include hosting of individual identification data, selective proof of title for property, decentralized banking services, privacy-preserving p2p/b2b asset exchange, mutual aid societies, p2p insurance, decentralized humanitarian aid mechanisms, or use purely as an anonymous token of value.

These functions can be utilized to serve disenfranchised populations currently excluded from vital services such as banking and healthcare due to lack of identification, capital, and secure channels. They can also be leveraged by individuals who desire to take ownership over and monetize their private data, or, for example, by enterprising communities that wish to develop a competitive bidding system on internally generated solar energy. The unique implementations are unbounded, the common link being the belief that decentralization is the engine of moral progress, and that voluntary solutions are the most creative and enduring.

2 History

Zen builds on the heritage of the best cryptocurrencies, network architecture, and distributed file sharing systems in existence by incorporating both existing as well as new features to yield a solid foundation designed for long term viability. Just as important as our technology stack, we're building on the latest ideas in distributed consensus and competitive governance. Some of the foundations of our project come from Bitcoin, Dash, Decred, and Seasteading.

Zcash extended Bitcoin with fully anonymous shielded transactions, so that users could choose between normal Bitcoin-like addresses (t-addresses) or shielded addresses resistant to traffic correlation analysis (z-addresses). Then we created Zclassic, a Zcash clone that changed some key parameters our community felt were important: we removed both the 20% Founders' Reward for the first four years (10% lifecycle equivalent) and the slow start to the money supply. Since launching Zclassic, we've formed a vibrant open-source community eager to move the technology forward in a unique direction. Some early accomplishments include developing an open source mining pool application for both Zcash and Zclassic, as well as Windows and Mac wallets.

Our team realized that Zclassic could be further extended as a fully encrypted network with an innovative economic and governance model that better aligns with Satoshi's original vision for a decentralized global community. We view Zclassic as a fundamentally pure open-source, all-volunteer cryptocurrency project, while Zen extends into a platform with internal funding to facilitate a broader set of communications, file-sharing, and economic activities.

3 Specifications at Launch

Zen is the overarching system over which ZenCash tokens disseminate, similar to projects like Ethereum that has its Ether token. ZenCash is designed as a fork from Zclassic, and will be extended with the following additional features.

1. Release date: 8PM EDT, 23rd May 2017 as a fork from Zclassic (0:00 UTC).
2. Equihash hashing algorithm, which is a memory-hard, proof-of-work mining algorithm based on the generalized Birthday Problem and Wagner's algorithm for it. Equihash was created by Alex Biryukov and Dmitry Khovratovich of the University of Luxembourg.
3. Block reward: 12.5 ZenCash.
4. Block generation: 2.5 minutes.
5. Block size: 2 MB.
6. Difficulty adjustment algorithm: Digishield V3, tweaked to use the following trailing-average difficulty window:

$$\text{next difficulty} \;=\; \text{last difficulty} \;\times \sqrt{\frac{150 \text{ seconds}}{\text{last solve time}}}$$

7. Division of each PoW block reward and transaction fees between miners and other stakeholders:
   (a) 88% to miners.
   (b) 5% to one or more DAOs.
   (c) 3.5% to Secure Node Operators.
   (d) 3.5% to the Core Team.

8. Total eventual coin supply: 21 million.
9. Reward halving every ≈ 4 years, per Bitcoin.
10. Shielded Transactions obscure sender, receiver, and amount from blockchain.
11. Transparent transactions publish sender, receiver, and amount on blockchain.
12. Secure message field in z_transaction with 1024 bytes of characters:
    (a) Secure publishing to GNUnet and / or IPFS locations.
    (b) Short messages between users.
    (c) Publish to channels viewable by anyone with channel capable wallet.
13. Secure Nodes perform infrastructure functions:
    (a) Ensure all network communications are encrypted between nodes.
    (b) Maintain full ZenCash blockchain.
    (c) Provide certificate-based encryption connections for ZenCash wallet applications.
14. Secure Nodes meeting requirements receive coinbase rewards.
15. Domain Fronting service for z_transactions using a commercial CDN.
16. Governance by one or more DAOs. (see Governance section).
17. Zen DAOs responsible for the operations and continued improvement of the system. They will build and operate:
    (a) Zen information distribution (Web, wiki, blog, media).
    (b) Proposal System and Voting System.
    (c) Reporting and monitoring systems.
18. Core Team:
    (a) Includes founders of Zen.
    (b) Mission is to guide launch and early growth and development.
    (c) Fund expenses important to development and maintenance.
    (d) Operate at the interface of Zen and traditional systems.

4 Roadmap

"Trial and error is freedom." (Taleb, 2012)

Zen is launching as an integration of revolutionary technologies to create a system upon which innovation can accelerate. We're structuring optimal decentralization and persistent competition so the system constantly evolves and never hits a comfort plateau. The initial Roadmap covers a 12- to 18-month development window to get the system functioning autonomously. The key to this is establishing the core set of integrations with our own secure node network, a distributed data storage system like GNUnet, and the broader ecosystem of exchanges, mining pools, and user communities. ZenCash needs to be fully operational,

easily available, and useful to a diverse variety of stakeholders. Our Roadmap reflects the emphasis on ZenCash as our first and most important initial product in the Zen portfolio.

1. Develop improved wallets.
   (a) Windows for t and z transactions, messaging, GNUnet publishing.
   (b) Linux for t and z transactions, messaging, GNUnet publishing.
   (c) Mac for t and z transactions, messaging, GNUnet publishing.
   (d) Mobile (Android and iOS) for t and z transactions.
   (e) Hardware for t and z transactions, messaging, GNUnet publishing.
   (f) Web wallet for t and z transactions, messaging, and GNUnet publishing.
2. Domain Fronting service for z_transactions using a commercial CDN.
3. Zen systems servers in resilient multi-data center configuration.
4. Infrastructure resiliency testing, results, and improvements.
5. Implement Segregated Witness.
6. Governance R&D deliverables, including fully tested operational system (see Governance section):
   (a) Research report.
   (b) Constitution.
   (c) Tested and implemented voting system.
   (d) First election standing up at least one DAO, transitioning Core Team.

5 Functional Elements

Zen brings together many different elements to form a working whole. Instead of regular nodes, Zen requires Secure Nodes, which ensures the nodes maintain a basic standard of security and performance to ensure the system remains distributed, resilient, and secure. By enforcing encrypted communication between nodes, and between nodes and wallets, Zen protects against eavesdropping and man-in-the-middle attacks.

Zen also addresses a metadata weakness of other cryptocurrencies. For instance, by communicating in a potentially compromised fashion and then sending Bitcoin, the participants in a Bitcoin transaction are potentially exposed to identification by transaction correlators. ZenCash will incorporate secure messaging within shielded transactions, so users can agree on the transaction, send it, and then verify receipt. These functional elements will manifest into the following systems:

- ZenTalk – A new type of secure communications network that allows for one-to-many communication using the blockchain to store messages permanently.
- ZenPub – An anonymous document publishing platform using GNUnet or IPFS.
- ZenHide – The ability to circumnavigate crypto-commerce blocking using domain fronting.

5.1 T_transactions

T_transactions are the traditional blockchain-recorded transactions controlled by a private key in a wallet. These are derived from Bitcoin, and enable rapid compatibility with exchanges, wallets, and other Bitcoin-derived ecosystem applications.

5.2 Z_transactions

These are transactions sent to shielded addresses, as inherited from Zcash and Zclassic. Balances in shielded addresses are private. If spending to one or more shielded addresses, the value stays private but any transparent addresses on the receiving end will deshield the token and reveal the value received on the blockchain. The input shielded addresses and whether the value was sent from one or two of these remains confidential when deshielded. The Zcash protocol describes this process in detail:

> Value in Zcash is either transparent or shielded. Transfers of transparent value work essentially as in Bitcoin and have the same privacy properties. Shielded value is carried by notes, which specify an amount and a paying key. The paying key is part of a payment address, which is a destination to which notes can be sent. As in Bitcoin, this is associated with a private key that can be used to spend notes sent to the address; in Zcash this is called a spending key.
>
> To each note there is cryptographically associated a note commitment, and a nullifier 1(so that there is a 1:1:1 relation between notes, note commitments, and nullifiers). Computing the nullifier requires the associated private spending key. It is infeasible to correlate the note commitment with the corresponding nullifier without knowledge of at least this spending key. An unspent valid note, at a given point on the block chain, is one for which the note commitment has been publicly revealed on the block chain prior to that point, but the nullifier has not.
>
> A transaction can contain transparent inputs, outputs, and scripts, which all work as in Bitcoin [Bitcoin-Protocol]. It also contains a sequence of zero or more JoinSplit descriptions. Each of these describes a JoinSplit transfer which takes in a transparent value and up to two input notes, and produces a transparent value and up to two output notes. The nullifiers of the input notes are revealed (preventing them from being spent again) and the commitments of the output notes are revealed (allowing them to be spent in future). Each JoinSplit description also includes a computationally sound zk-SNARK proof, which proves that all of the following hold except with negligible probability:
>
> - The input and output values balance (individually for each JoinSplit transfer).

- For each input note of non-zero value, some revealed note commitment exists for that note.
- The prover knew the private spending keys of the input notes.
- The nullifiers and note commitments are computed correctly.
- The private spending keys of the input notes are cryptographically linked to a signature over the whole transaction, in such a way that the transaction cannot be modified by a party who did not know these private keys.
- Each output note is generated in such a way that it is infeasible to cause its nullifier to collide with the nullifier of any other note.

Outside the zk-SNARK, it is also checked that the nullifiers for the input notes had not already been revealed (i.e. they had not already been spent).

A payment address includes two public keys: a paying key matching that of notes sent to the address, and a transmission key for a key-private asymmetric encryption scheme. "Key-private" means that ciphertexts do not reveal information about which key they were encrypted to, except to a holder of the corresponding private key, which in this context is called the viewing key. This facility is used to communicate encrypted output notes on the blockchain to their intended recipient, who can use the viewing key to scan the blockchain for notes addressed to them and then decrypt those notes.

The basis of the privacy properties of Zcash is that when a note is spent, the spender only proves that some commitment for it had been revealed, without revealing which one. This implies that a spent note cannot be linked to the transaction in which it was created. That is, from an adversary's point of view the set of possibilities for a given note input to a transaction, its note traceability set, includes all previous notes that the adversary does not control or know to have been spent. This contrasts with other proposals for private payment systems, such as CoinJoin or CryptoNote, that are based on mixing of a limited number of transactions and that therefore have smaller note traceability sets.

The nullifiers are necessary to prevent double-spending: each note only has one valid nullifier, and so attempting to spend a note twice would reveal the nullifier twice, which would cause the second transaction to be rejected.

5.3 ZenTalk

The Z_transactions in ZenCash have the ability to incorporate text-based messages, which are encrypted and included in the blockchain. There is a 1024 character limit for these messages, and they enhance the ability for users to conduct secure commerce. Instead of

discussing the transaction in other less-secure channels that may not have the same level of privacy enhancements as Zen, users can communicate via the ZenTalk messages with the other party or parties before and after the shielded transfer takes place with very small z_transaction spends. These messages can be sent directly from one z_address to another, and they can also be sent to a channel. By generating a z_address from the hash of a channel name, users can subscribe to the channel and read anything published by anyone to the channel.

For example, the channel #ZenCash_announcements would hash to zXXXXXXXXXXXX, allowing any user to send an anonymous message to the channel. Each message would cost a finite amount of ZenCash to send, since it is contained in a z_transactions, therefore reducing the amount of non-useful messages on common channels. Official announcements would be signed by private key and would only be displayed if deemed valid. Furthermore, essentially private group messages can be published using z_transactions by first creating a complex channel name,and then encrypting the contents of the message with keys only the desired recipients have. ZenTalk messages would be encrypted with algorithms such as AES-256 with Perfect Forward Secrecy (PFS), matching current standards of encryption for secure communication.

5.4 ZenPub

Zen has the ability to publish documents to the IPFS or GNUnet. This is done by publishing a IPFS or GNUnet address in the text field of a z_address. The preferred document publishing system at this time is GNUnet, because it provides the required infrastructure for anonymous publishing and maintains an active database of documents. The system is similarly extensible to IPFS or any other future distributing archival system. By creating an anonymous messaging layer in conjunction with an anonymous publishing layer, ZenPub allows for the creation of truly anonymous publications which can be rapidly distributed to interested readers.

5.5 ZenHide

It is possible for regulators in countries hostile to crypto-commerce to block traditional crypto-currencies like Bitcoin and even Zcash. Zen uses Domain Fronting to extend the ability to complete transactions in adversarial network environments, as explained in Blocking-resistant communication through domain fronting abstract:

> We describe “domain fronting,” a versatile censorship circumvention technique that hides the remote endpoint of a communication. Domain fronting works at the application layer, using HTTPS, to communicate with a forbidden host while appearing to communicate with some other host, permitted by the censor.
>
> The key idea is the use of different domain names at different layers of communication. One domain appears on the “outside” of an HTTPS request–in the

> DNS request and TLS Server Name Indication, while another domain appears on the "inside"–in the HTTP Host header, invisible to the censor under HTTPS encryption.
>
> A censor, unable to distinguish fronted and non-fronted traffic to a domain, must choose between allowing circumvention traffic and blocking the domain entirely, which results in expensive collateral damage.
>
> Domain fronting is easy to deploy and use and does not require special cooperation by network intermediaries. We identify a number of hard-to-block web services, such as content delivery networks, that support domain-fronted connections and are useful for censorship circumvention.

The specific implementation of Domain Fronting used by Zen at launch is with a Commercial Content Distribution Network, but as with every aspect of our architecture, flexibility is designed in from the start and the system can extend in many directions as the technology evolves.

5.6 Zen Secure Nodes

The nodes are the key systems that maintain the Blockchain, accept transactions from wallets, validate miner solutions, and act as the decentralized computing and communications system for cryptocurrencies. In Zen, all information transmitted to and from the Secure Nodes is encrypted with valid certificates using TLS version 1.3 and further protected with Perfect Forward Secrecy (PFS). As part of the Secure Node capability, the ZenCash application improves functionality by:

- Extending RPC to enable AES encrypted data to reside in shielded transactions.
- Extending RPC to enable perfect forward secrecy handshakes between public keys.

Secure nodes that meet all requirements will be rewarded the Secure Node portion of the mining in a queued manner. Secure nodes need to monitor the #secure node channel. The Secure Node payment system is intended to be operated in an auditable manner with clear standards to maximize operability and minimize issues.

1. Basic infrastructure functions performed by Secure Nodes:
   (a) Ensure all network communications are encrypted between nodes.
   (b) Maintain full Zen blockchain.
   (c) Provide certificate-based encryption connections for ZenCash wallet applications.
2. Secure Nodes meeting the requirements outlined below receive 3.5% of block coinbase reward in a way that rewards uptime at full functionality:
   (a) Operate node software on a capable system as specified by infrastructure requirements.

- Recommended memory is more than 4 GB.

(b) Maintain entire ZenCash blockchain on the system.
(c) Provide a valid SSL certificate to the ZenCash Node software to use for communicating with other nodes and wallets.
(d) Keep at least 42 ZenCash on the server in a t_address for staking.
(e) Monitor the SecureNode channel for challenge messages from SecureNodeHQ approximately every 10 minutes (in a z_transaction message field).
(f) Respond to challenge with identifying information of the Secure Node.
(g) Challenge response will be a combination of two things:
    i. Send a shielded message to SecureNodeHQ containing public t_address and GNUnet document location in message field.
    ii. Publish a document to GNUnet signed with private t_address including:
        A. Public t_address of staking Zen, which will also be used for reward payment.
        B. SSL certificate and IP address.
        C. Block header from blockchain.
        D. Other information that may be necessary to make sure it is a unique server.
(h) Each Zen Secure Node must also be a peer on the GNUnet systems to publish the challenge response anonymously and support the anonymous publications from other elements of the system.
(i) Other potential requirements that may come up in future to allow ZenCash system to use the Secure Nodes for consensus and computing power.

3. Zen Secure Node Payment System (Z-SNPS):
    (a) Z-SNPS operated by a Zen DAO.
    (b) Z-SNPS will track challenge responses from each Secure Node.
    (c) Secure Nodes will be tracked and published by their t_addresses.
    (d) Mined block will pay the 3.5% reward to the ZC-SNPS system, which will periodically distribute the ZenCash to Secure Nodes based on their uptime in the defined time-period.

Because Zen will have this distributed computing network in the form of compensated Secure Nodes, these nodes may be required to provide other computing services for the network depending on the evolution of community consensus.

5.7 Zen Standard Nodes

The ZenCash application can be operated on any linux server, Mac, or PC. The client acts as both a node and a wallet. Although it does not have the full encryption capability a Secure Node does, all nodes help the system to run function efficiently and remain resilient

to attack.

5.8 ZenCash Wallet Software

The ZenCash software can be operated as a wallet. The command line wallet is the basic form, but Graphical User Interface (GUI)-based versions already exist for desktop. Mobile, Web, Raspberry Pi, and other hardware wallets are high priority to immediately develop to enhance the user experience and security for ZenCash tokens. Wallets can be configured to use any available ZenCash node for communication, or can be set up to only connect to Secure Nodes in order to maintain high standards of information security.

5.9 Applications

Zen is what we consider to be an optimally decentralized open source project, and so we expect applications to be built and contributed to the ecosystem by many parties. Many of these contributions will likely come in voluntary open source fashion, but we expect a robust business community to grow around the platform as well. Additionally, the Core Team has a full application development plan that's already in-process. This includes, but is not limited to:

- Node Application
- Equihash Open Source Mining Pools
- Governance Applications
- Monitoring and Reporting Systems
- Wallets of every type
- Secure Node Monitoring System
- Secure Node Payment System

6 Governance

"Thus do ideologies fall: not by violence but by examples showing a better way." -Joe Quirk, Seasteading Institute

Zen is designed with a decentralized governance model incorporating multi-stakeholder empowerment and the flexibility to evolve to optimally suit our community. Fundamentally, our philosophy on governance is that we do not know a priori the best approach, but we have some ideas for how to initialize the system and enable it to evolve with the needs of the community. We believe in governance as a service (GaaS) and aim to efficiently provide value to our direct stakeholders, the broader community, and the world.

"*Any industry that delivers poor service for a high price deserves to be disrupted*" (Quirk, 2017), governance being a consummate example. In solidarity with other projects

and ideas taking root around the world, we reject forced centralization and embrace voluntaryism. Rather than entrusting a minority of the people with power, we believe that all people have the right to be trusted with freedom.

The core philosophy of our governance model is that decentralization of power maximizes inclusion and creativity. Practical implementations must recognize that pooling resources and effort provides synergies that should be optimally balanced against full decentralization; optimal points being state and time-varying, best determined through voluntary participation and secession.

Importantly, we are implementing a system where competing DAOs can emerge to share resources or even completely subsume less efficient or unpopular versions. There should be no one-size-fits-all structure invariant across environment, function, culture, or time; rather, structures should be fluid, suited to specific problems, and flexible to scale when working and fade when failing relative to alternatives. Such a system of systems would dynamically evolve in such a way that it is antifragile to competitive feedback.

Our objective governance state will balance decentralization, implementation efficiency, separation of powers, broad stakeholder empowerment, and evolutionary flexibility. This initial state will be the result of at least a 12- to 18-month R&D effort into game theoretic, political science, and economics research into optimal voting mechanisms coupled with feedback from multiple testnet implementations. The project will be one of our first funded efforts with final deliverables including a comprehensive research report and operational code integrated into the Zen network. Within 6 months of governance implementation we expect to have leadership teams in operation from our first full and open election.

6.1 Optimal Decentralization

"A specter is haunting the modern world, the specter of crypto anarchy." -Crypto Anarchist Manifesto

By decentralization we mean that everyone has an equal opportunity to participate, that we are fully inclusive, and that decision-making authority is maximally diffuse such that the system is resistant to capture. Theoretical maximum decentralization means that every individual retains authority to equally influence decision-making; this is difficult to implement in practice when pooling resources to collaborate on a common system. Even if implemented in such a pure fashion, individual decisions naturally pool for collaboration efficiency and resources accumulate to certain stakeholders at unequal rates.

We cannot stop these natural forces, nor is there reason to categorically deem them harmful in every instance. What we can do is to design the system such that all participation is voluntary, that decision-making power over resource allocation is balanced across a broad cross-section of stakeholder types, and that a credible mechanism exists to evolve with feedback. A structure infused with flexibility is more important than initially designing the best system to suit all circumstances, especially since we are creating a movement

so expansive that predicting all developments is essentially impossible.

Implementation efficiency is also a big concern for decentralized organizations. Pure decentralization could suffer decision-making paralysis, voter apathy, or delusions of the herd at the extrema. This is why we initially shy away from a system of pure democracy for all decision-making, and are taking the time to research competing models and test them under varying conditions of stress. Our proposed system of free and open competition for DAOs is designed to encourage groups of high-performing functional area experts and professionals to propose their leadership in specialized domains so that our system-wide efficiency in converting resources to higher-value end products or services is continually evolving to suit user needs and demands.

6.2 Checks & Balances

A key lesson learned from human history is that powers are best separated and competing power clusters should provide some equilibrium state of checks and balances. The balancing should be resilient to unchecked growth in any single power cluster such that the entire system succumbs to capture. To initially prevent this condition, Zen is launching with a Core Team in control of 3.5% of block reward funding, and an initial DAO comprised of industry leaders controlling 5% of resources. In addition, our objective state to be implemented after the 12- to 18-month R&D and test phase will include a hybrid type of multi-stakeholder voting so that a wide cross-section of the community retains power to influence decisions and resource allocations. Every aspect of our governance structure will ultimately be subject to competitive feedback and change. We are taking an evolutionary approach that starts with a simple model that will grow with the community.

7 DAO: Infrastructure, Proposals, and Voting

The Zen system will have at least one DAO funded by a portion of the mining rewards, and governed by a voting system that brings stakeholders together. This system of governance helps ensure that implementation of changes, improvements, and integrations minimizes contention and reduces the chance that a disagreement leads to a fork in the project. As we unroll our broader governance plan derived from rigorous R&D and testing, the goal is to open the governance landscape to full competition; this means that we could see multiple competing DAOs emerge with different teams working on different problems. Each DAO would emerge with its own proposed structure, processes, and goals, which ensures these attributes are evolving through competition and the wrong initial organizational decisions do not perpetuate.

Our DAOs will be responsible for building, maintaining, and improving the infrastructure that keeps the system going. It is also responsible for implementing changes to the Zen software applications, and is flexible enough to accommodate other community priorities,such as community outreach, marketing, training, etc.

As the Zen system grows in popularity, the support structures for users, miners, Secure Node operators, and ecosystem partners will need to grow and scale as well. The DAO structures will have funds, allocated through projects and proposals, with which to assist in the growth and support.

The community is encouraged to participate in contributing to Zen in all different ways. The DAOs are responsible for coordinating the community contributions, and have funds to assist in offsetting expenses incurred by the community. One of the purposes of proposals is to repay community members for their expenses in supporting the system.

At launch, Zen will have one DAO staffed with respected professionals that span relevant industries. When the governance plan is ready for implementation, this DAO will be one proposed grouping subject to market competition for others who might wish to stand up their own governance structures; the broad community will make that decision.

7.1 Zen Infrastructure Operated by DAO

The DAO system will maintain application servers and services, including:

- Secure Node validation server(s).
- Forum server(s).
- Slack moderation.
- Websites.
- Blogs.
- Proposal system.
- Voting system.
- Binary repositories.

The DAOs are responsible for the following support:

- Help people use ZenCash or other system features.
- Help Secure Node operators.
- Troubleshoot node reward problems.
- Troubleshoot voting system problems.
- Provide support escalation.
- Provide rapid and final issue adjudication.

DAO distributes ZenCash to proposal owners after a successful vote and expiration of the veto period.

There will initially be 3-5 DAO officers, but this will ultimately be unbounded. Officers can be anonymous, but that is not a requirement. In fact, openly declaring identity comes with the advantage that prior professional achievements and character strength are naturally inherited into the Zen system.

There will be disputes and so resolution mechanisms need to be developed to adjudicate these efficiently and fairly. One idea that will be explored in the Governance R&D project will be to establish a judiciary and jury system.

7.2 Proposal Submission and Voting

Each DAO will have its own structure, processes, and priorities, but one consistent mechanism will be a system of free and open proposal submissions for work and an evaluation and award process. There is no reason to specify how this happens, only that it should happen. This is an open community to all of humanity, so there should be no barriers to participation. One proposed method for our initial DAO is as follows:

1. Vote every two months. Proposal submission deadline two weeks before voting. Voting dates: Jan 31, Mar 31, May 31, July31, Sept 31, Nov 31.
2. Proposal submission opens day after vote.
3. Veto – core team may veto a proposal within 7 days of a vote with a unanimous core team veto (this should almost never be done).
4. Proposals can be funded in the ZenCash equivalent of the local fiat currency on the date of the vote (prevent Dash issue of rapid rise leading to project rejection).
5. Voting done with tokens. 1440 voting tokens distributed 1 month before vote.
6. Most decisions done by majority vote $>$ 720 token holders voting yes.
7. Some decisions by supermajority vote $>$ 1080 token holders voting yes.

7.3 Voting Process

Token Distribution Plan – done for every voting period, 1440 tokens altogether:

1. 360 tokens for sale – allows users and ZenCash holders to buy votes.
   (a) 1-30: 1 ZenCash
   (b) 31-60: 2 ZenCash
   (c) 61-90: 3 ZenCash
   (d) etc. up to 12 ZenCash per token for last group of 30
2. 240 – ZenCash project developers.
   - Awarded by commits, pull requests, or other reasonable measure of contribution.
   - Goal is to empower software and system developers.
3. 60 – Exchanges that carry ZenCash.
   (a) Top 6 by volume get 10 each.
4. 60 – Mining pool owners.
   (a) 1 awarded every 480 blocks to pool finding the block.
5. 360 – Secure Nodes.

   (a) 1 awarded every 40 blocks until all 360 are awarded.
6. 120 – DAO officers, equally divided amongst officers.
7. 240 – Core Team, equally divided amongst core team members.

8 Zen Core: Foundation and Leadership

The Core Team initially consists of the three early founders for the project, Joshua Yabut, Rob Viglione, and Rolf Versluis. Each founder is a leader within his respective professional domain and has a strong track record of performance and cryptocurrency expertise.

Josh is an experienced red teamer and exploit developer who previously served the aerospace industry. He has a passion for developing adversary-resistant networks and for redefining the status quo. He holds an Offensive Security Certified Expert (OSCE) certification, a Masters degree from DePaul University in IT Project Management, and has extensive knowledge in exploiting government and corporate networks. Josh has extensive cryptocurrency development experience leading the core team for Zclassic, developing the z-nomp mining pool protocol, supporting the ZCash development community, and consistently delivering quality software.

Rob is a former physicist, mercenary mathematician, and military officer with experience in satellite radar, space launch vehicles, and combat support intelligence. Contributions within the crypto space include being part of Zclassic's core team, support to the Bitshares project, heading up BlockPay's U.S. & Canada Ambassador program,and consulting for Bitgate. He's currently a PhD Candidate in finance @UofSC researching cryptofinance and teaching "Bitcoin & Blockchain Applications in Finance." Rob holds an MBA in Finance & Marketing and the PMP certification. He is a passionate libertarian who advocates peace, freedom, and respect for individual life.

Rolf is an experienced business owner in the IT industry and owns a mid-size Bitcoin and Zclassic (ZenCash) mining operation in Alpharetta, Georgia. With prior experience at Cisco systems, the semiconductor industry, and as a nuclear trained officer in the US Submarine force, Rolf brings leadership, management, and technical operational expertise to the ZenCash organization.

The motivation for forming a Core Team entity with decision-making authority and an independent budget was to rapidly deploy the system and efficiently execute a wide range of early development tasks that will culminate in a fully operational network outlined in our Roadmap; the ultimate result will be a transition to the broader governance structure resulting from R&D and testing. Our goal is to work ourselves out of our jobs after delivering on the initial Roadmap and standing up our first elected DAO per the governance plan. At that point we'll run for office within the existing DAO, or consider launching our own to add to the competitive dynamics of the system.

9 Zen Community: Strong and Vibrant

Zen is evolving symbiotically with the Zclassic project, with our combined community numbering around 1,000 forum members, developers, miners, traders, long-horizon investors, partner organizations, exchanges, bloggers, etc. As a fully open and inclusive project, all kinds of contributions and support have flowed in to Zen from around the world, and this impromptu yet consistent collective is one of our defining features as a system. Our community already has an enduring history not only of positive relationships and friendly interactions but also of spontaneous support and engagement emerging to prevent or solve disparate problems.

9.1 The Ethics of Open Source

Open source projects can take on an evolving and fluid set of ethics, however the founders of this one hope to keep the community centered on the principles of zen, hence our name. We are developing a system we hope will be used for peaceful collaboration, permissionless innovation, and maximum inclusion. We hope our legacy will be a massively positive surplus to society, and we personally reject working with anyone intent on harm, either physical or through fraud.

9.2 Zen Support

Zen Support refers to a community of Zen Developers and other distributed IT professionals committed to advancing the technology and offering basic assistance to users. This network will be funded by the DAO, and will serve to make Zen's technology the most intuitive, easy to engage with in the ecosystem. Zen Support will also consist of a network of contributors from various industries who are committed to serving as ambassadors, mentors, and support for Zen Contributors. See more in subsequent Zen Community sections. Zen Support is a commitment that Zen is structurally designed to foster inclusiveness, collaboration, and collective aid, and that the executive officers, Zen Ambassadors, Verified Zen Entrepreneurs, or any representative of the Zen Community will be a resource for contributors to depend on and collaborate with.

9.3 Zen Outreach

Our Roadmap includes exciting, unprecedented outreach programs that will serve to strengthen our collective and facilitate engagement with people of all walks of life. In short, Zen does not have a singular "target market"; how could we, when the practical use cases and implementations of our technology are vast and diverse? We do not intend to confine utilization of Zen to the personal visions of our Core Team members, so alternatively we will launch programs upon inception designed to maximize engagement with Zen and allow community members to adapt our mission and initiatives as Zen evolves. Our initial DAO is

reserving resources to fund experimental programs and to reward active contributions to our community. Some of these proposed program ideas are explained below.

Once again, Zen is *inclusive* and *agnostic*, and our global presence will mirror these core values. We will include interest groups such as entrepreneurs, activists, developers, universities, corporations, and uninformed but curious individuals, all boasting varying track-records of engagement with the cryptocurrency space.

Through our **Zen Ambassador Program**, experienced users, thought leaders, and passionate community members will be granted opportunities to represent Zen, propagating our vision to people in corners of the world without access to the resources, capital, and technology necessary to discover and join our community out of individual initiative. Leaders in this program can serve many purposes, from advising Zen startups to mentoring Zen Chapters to representing Zen in the press.

By participating in our **Zen Youth Program**, global minors will be offered intensive coding and business development education, and unique opportunities for engagement with the Zen collective. This initiative will be multifaceted, with offerings ranging from global youth competitions for DAO-funded startups built on the Zen platform to lotteries allocating resources to cover education expenses of Zen Youths. These young pioneers will also be mobilized to recruit their peers and engage their communities.

Entrepreneurs managing DAO-funded projects will be **Zen Verified Entrepreneurs** and gain access to relevant startup-accelerator-style perks, such as access to successful business mentors, marketing and user acquisition channels, open sourced developer engagement, direct channels to investors and venture capital firms, and events, partnerships, and seminars designed to collaboratively resolve issues and foster innovation.

Individual contributors will gain access to plug and play content fashioned to assist in spawning grassroots movements in the form of **Zen Chapters** proselytizing Zen technology, ethics, and/or governance and developing projects around the world. These Zen Chapters will be localizable and customizable, with fluid emphasis depending on region and community needs. Zen will offer a foundational online platform of material resources, ranging from:

- Marketing and educational content detailing the origins, specifics, differentiations, and goals of Zen.
- Templates and ideas for groups that wish to create Zen-sponsored promotional or educational events, conferences, and competitions.
- Modules, discussions, and webinars on Zen principles and relevant subjects for Chapters to participate in and contribute to, such as Coding, Entrepreneurship, Ethics of Decentralization, Foundations of Blockchain, etc.
- Database of business plans, legal documents, revenue models, user acquisition tactics, etc. to further the aims of Chapters undertaking a business development initiative or community improvement endeavor.

- Access to Zen contributors and developers for support, advice, guidance, and assistance via Zen channels.

For example, a Zen Chapter in the Philippines, where only around 30% of the population has access to financial services, could engage virtually with the international collective to develop a FinTech project catering to the particular needs of Filipinos and specifications of the country's culture and infrastructure. Such scalable engagement could drastically reduce the friction that has historically inhibited communities from autonomously stimulating their own small-scale economies and augmenting their capacity to compete.

Virtual interaction and communication is an invaluable development of the 21st century, and will be the core channel for connecting people thousands of kilometers away to cooperatively foster Zen innovation and development. That being said, we at Zen recognize that there is something sensational about face-to-face interaction with those equally dedicated to and mobilized around a set of principles and common vision. **Zen University** will take place annually to reward and engage Zen's most active and value-adding contributors, up-and-coming youth, and stand-out entrepreneurs. There will also be a lottery distributing tickets at random to especially compliant and secure Zen nodes. The theme, content, and intent of this event will vary based on preferences of the Zen Community.

Our resources are meant for our Zen Community, which encompasses many more categories of participants and initiatives, and offers much more value than the traditional stakeholders of a cryptocurrency project. We hope to be as much of a social movement as we are a technology project, the pure end goal to assist in making life more free and more fulfilling for as many people as we can.

10 Competitive Landscape

"We've long believed that over time companies tend to get comfortable doing the same thing, just making incremental changes. But in the technology industry, where revolutionary ideas drive the next big growth areas, you need to be a bit uncomfortable to stay relevant." -Larry Page, Alphabet

Competition is infused into Zen at its very core; by its nature, it is a necessity of optimal decentralization and a principle we believe enables beneficial evolution. This process also includes competition in the broader cryptocurrency landscape for ZenCash, and for our system in the ecosystem of blockchain platforms.

ZenCash directly competes with ZCash, Zclassic, Dash, Monero, ZCoin, Bytecoin, ShadowCash, Boolberry, and other privacy-augmented cryptocurrencies. Competition ranges across multiple dimensions, but from a technology perspective, we directly compete with the other zero-knowledge currencies using zk-SNARKs. ZCash was the pioneer

in this domain, and our technology directly benefits from their ground breaking contributions. Privacy as a feature also means that ZenCash competes with other implementations, such as the Zerocoin protocol, CryptoNote, RingCT, and simpler mixers. All of these coins serve a particular privacy-oriented niche on the cryptocurrency demand curve.

Our value proposition is that we incorporate elements that we consider to be best-in-class, which starts with inheriting ZCash's implementation of zero-knowledge shielding via zk-SNARKs, but we take this a crucial step further and obfuscate our entire network with end-to-end encryption and enable messaging within the most secure infrastructure in the space. Importantly, we do not intend to be displaced, because we are structurally prepared to not only update and rejuvenate our systems as the underlying technology advances, but to ourselves be the space's innovators.

Zen is building a system architecture with ZenCash as its token of value, or transaction fuel. As such, we also compete with broader platform-type projects, such as Ethereum, Ethereum Classic, NEM, Lisk, and Synereo over which decentralized applications (dApps) can be built. In this domain, Zen's simple scripting language inherited from Bitcoin and ZCash retains high security and resilience from a broad array of attack vectors, but also limits the degrees of freedom useful for complex code executions possible for platforms with enhanced Turing-complete scripting, similar to Ethereum and Ethereum Classic. Our advantage in this competitive arena is that dApps can be built on top of the world's most secure cryptocurrency network, and that we are flexible enough to operate across chains in strategic partnerships.

Our unique innovation to the cryptocurrency community is our fully competitive and evolutionary governance model to empower a broad cross-section of stakeholders in an environment of optimal decentralization. Bitcoin created the original breakthrough in distributed consensus, but other projects have since taken that further with various voting mechanisms. These projects range from Dash with its simple proposal submission and community voting model all the way to Decred with its embedded community governance; each has contributed positively to the evolution of decentralized consensus, but Zen takes this to the next level by relaxing additional constraints such that our system is set to evolve over time through perpetual competition between providers of governance services within the ecosystem. We are implementing an autonomous system that will change with feedback and trial-and-error innovations in how decentralized systems organize to solve specific problems. In this sense, we believe Zen is groundbreaking in social technology, pioneering a system that has never been attempted at scale.

From a broader perspective, Zen competes with incumbent currencies and banking systems, as well as emergent FinTech startups with particular advantage in providing services to the disenfranchised. We choose to make our contribution to this innovative, social welfare oriented space by providing enhanced privacy and security. As a secure messaging and distributed data archival system, we compete with other services, such as Signal, Telegram, and the Tor Project. There are also an infinite number of potential projects that can be built on the Zen platform, increasing our competitiveness exponentially.

We view competition as an enabler of healthy processes of growth and therefore welcome maximum competition. We'd rather live in a world with fierce competitors forcing us to accelerate our own innovations than a static world devoid of progress. We hope that Zen adds positively to human welfare by integrating great technologies and communities, morphing governance into a competitive service, and enabling anyone in the world to participate in our system of permissionless, collaborative, and decentralized innovation. We also view incumbents and future startups in this space as potential partners and allies instead of winner-takes-all competitors.

11 The Future of Zen

Forecasting is a challenging exercise, but we see a bright future for Zen and the peaceful and productive ecosystem we're building. We believe that the decentralized, fully inclusive, voluntary, and flexible organization we're creating will be seen as obviously superior in the future compared to the static, centralized, one-size-fits all versions perpetuated in the 20th century. The advent of cryptography, voluntaryist philosophy, and blockchain technology make such a thing possible, and we believe many people already do, and will, share our vision for a better world; especially when they see how we can accelerate innovation and improve human welfare by empowering everyone to express their values.

The next one to two years will see this vision come to fruition in our early organization by executing our Roadmap. There will certainly be challenges along the way, but flexibility and peaceful cooperation consistently overcomes seemingly insurmountable issues.

We are fortunate to live in an age of incredible innovation in both technology and ideas. We are building on top of the shoulders of the proverbial giants, some of them listed below, but many others go unnamed only because they are so numerous and the contributions so foundational.

References

[1] Juan Benet. (2014) IPFS - Content Addressed,Versioned, P2P File System.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin.

[3] Evan Duffield, Kyle Hagan. (2014) Darkcoin: Peer-to-Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System.

[4] David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. (2015) Blocking-resistant communication through domainfronting.

[5] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Zcash Protocol Specification Version 2017.0-beta-2.5.

[6] May, T. (1992). The cryptoanarchist manifesto. High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace.

[7] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.

[8] Quirk, Joe, and Patri Friedman. (2017) Seasteading: How Floating Nations Will Restore the Environment, Enrich the Poor, Cure the Sick, and Liberate Humanity from Politicians. Free Press.

[9] Taleb, N. N. (2012). Antifragile: Things that gain from disorder (Vol. 3). Random House.