ENTWURF

Diese Übersetzung ist eine Entwurfsversion. Wenn Sie Fehler sehen und gerne beitragen möchten, wenden Sie sich bitte an unser Team mit einer aktualisierten Version!

Zen White Paper

Robert Viglione,
Rolf Versluis,
und Jane Lippencott.

Mai 2017

ABSTRACT

Zen ist ein end-to-end verschlüsseltes System mit einer zero-knowledge Technologie, mit deren Hilfe Kommunikation, Daten oder Werte sicher übertragen und gespeichert werden können. Es stellt eine Integration von revolutionären Technologien dar die ein System bilden, das Innovation durch die Kombination dreier Funktionen beschleunigt, die traditionell getrennt voneinander durchgeführt wurden:

1) Transaktionen 2) Kommunikation und 3) Konkurrierende Governance. Das Ganze wird in einer sicheren und anonymen Form aufgesetzt, indem eine weltweit verbreitete Blockchain und Computerinfrastruktur genutzt wird. Das System integriert zahlreiche best-in-class Technologien, um eine offene Plattform für unbeschränkte Innovation bereitzustellen, die sich anhand der User Präferenzen entwickeln kann.

Die Autoren können unter rob@zensystem.io, rolf@zensystem.io, and jane@zensystem.io, kontaktiert werden.
Wir möchten Jake Tarren unseren Dank für Kommentare, Anmerkungen und Vorschläge aussprechen, sowie den ZClassic und Zen communities, die uns bei der Entwicklung dieser Ideen geholfen und diese Bewegung ermöglicht haben.

INHALTSVERZEICHNIS

Ziel

“Kritik durch Erschaffen.” - Michelangelo Buonarroti

Wir leben in einer extrem regulierten und überwachten Welt, in der Milliarden von Individuen ihrer grundlegenden Menschenrechte, wie dem Recht auf Grundbesitz, Datenschutz, freie Vereinigung und dem Zugang zu Informationen beraubt werden. Doch die Technologie, um einige dieser Probleme zu lösen, existiert bereits und Zen’s frühe Implementierung wird genau das erreichen.

Zen ist eine Sammlung aus Produkten, Dienstleistungen und Unternehmen das um eine ermöglichende Technologieplattform herumgebaut wird, die zero-knowledge Proofs und eine Kernmenge an Werten nutzt. Als ein verteiltes Blockchain System aufbauend auf den neuesten Techniken, um Zensur zu entgehen, vollständig verschlüsselter Kommunikation und einem auf langfristige Umsetzbarkeit konzipiertem Sozial- und Governancemodell, wird Zen zum Menschenrecht auf Datenschutz beitragen und die benötigte Netzwerkinfrastruktur für Menschen bereitstellen, um sicher zusammenzuarbeiten und Werte in einem grenzenlosen Ökosystem zu schaffen. Unsere Mission sehen wir in der Integration der neuesten post-Satoshi Technologien mit einer dezentralisierten, freiwilligen und friedlichen Menge an sozialen Strukturen, um das Leben aller Beteiligten zu verbessern. Wir glauben, dass es die richtige Zeit für unsere Idee ist.

Die Rahmenbedingungen für Zen sind eine sichere, und Datenschutz-orientierte Infrastruktur mit einem Governancemodell so strukturiert, dass es den Beteiligten ermöglicht wird, in Zusammenarbeit die Funktionalität in weitere Dimensionen zu erweitern. Zu den Möglichkeiten, die Zen bietet, gehören das Hosting von persönlichen Identifikationsdaten, ausgewählte Nachweise von Eigentumstiteln, dezentralisierte Bankdienstleistungen, p2p/b2b Austausch von Vermögenswerten bei Wahrung des Datenschutzes, Gesellschaften zur gegenseitigen Hilfeleistung, p2p Versicherungen, dezentralisierte Mechanismen zur humanitären Hilfe oder um es lediglich als anonymisierten Wertgegenstand zu nutzen.

Diese Funktionen können genutzt werden, um entrechteten Bevölkerungsgruppen zu helfen, die derzeit von notwendigen Dienstleistungen wie dem Banken- und Gesundheitswesen aufgrund fehlender Identifikation, fehlendem Kapital oder fehlender sicheren Verbindungen ausgeschlossen sind. Die Funktionen können ebenfalls eingesetzt werden, um Eigentum zu übertragen oder private Daten zu monetarisieren, oder zum Beispiel von innovativen Communities, um ein kompetitives Auktionssystem für eigens erzeugten Solarstrom zu entwickeln. Die einzigartigen Implementierungen sind unbegrenzt, die gemeinsame Verbindung ist die Überzeugung, dass Dezentralisierung der Motor des moralischen Fortschritts ist und dass freiwillige Lösungen die Kreativsten und Beständigsten sind.

Geschichte

Zen baut auf der Tradition der besten existierenden Kryptowährungen, Netzwerkarchitekturen und vebreiteten Filesharingsystemen auf, indem sowohl existierende, als auch neue Features integriert werden, welches eine solide Basis ergibt, um eine langfristige Funktionsfähigkeit zu erbringen. Genauso wichtig wie unsere Technologieplattform ist unsere Tätigkeit bezüglich der neuesten Ideen rund um verbreiteten Konsens und kompetitive Governance. Einige der Grundlagen unseres Projektes kommen von Bitcoin, Dash, Decred and Seasteading.

ZCash hat Bitcoin um vollständig anonymisiert geschütze Transaktionen erweitert, sodass User zwischen normalen Bitcoin-ähnlichen Adressen (t-addresses) und geschützen Adressen, die gegen Traffic Korrelationsanalysen (z-adresses) abgesichert sind, wählen können. Daraufhin haben wir ZClassic entwickelt, einen ZCash Klon, der einige Schlüsselparameter verändert hat, die von unserer Community als wichtig eingeschätzt wurden: Wir haben sowohl den 20%igen Gründerbonus für die ersten vier Jahre (entspricht 10% während des Lebenszyklus) eliminert, als auch den langsamen Start der Geldversorgung. Seit dem ZClassic Launch haben wir eine lebhafte open-source Community geschaffen, die die Technologie begierig in eine einzigartige Richtung bewegen wird. Einige frühe Errungenschaften beinhalten die Entwicklung einer open-source Miningpool Applikation für ZCash und ZClassic, und Windows und Mac Wallets.

Unser Team hat realisiert, dass ZClassic zu einem vollständig verschlüsselten Netzwerk mit einem innovativem Ökonomie- und Governancemodell erweitert werden könnte, das besser zu Satoshi's ursprünglicher Vision einer dezentralisierten und globalen Community passt. Wir verstehen Zclassis als ein fundamental reines, open-source Kryptowährungsprojekt auf freiwilliger Basis, während Zen in eine Plattform mit interner Aufbringung von Mitteln er-

Spezifikationen beim Launch

Zen ist das übergreifende System über das ZenCash Token verbreitet werden, ähnlich Projekten wie Ethereum, das wiederum Ether Token besitzt. ZenCash ist als eine Fork von ZClassic konzipiert und wird um folgende, zusätzliche Features erweitert.

1. Release Datum: 20 Uhr EDT, 30.05.2017 als eine Fork von ZClassic (0:00 UTC).

2. Equihash Hashing Algorithmus ist ein memory-hard, proof-of-work Mining Algorithmus der auf dem allgemeinen Birthday Problem und Wagner's Algorithmus dafür basiert. Equihash wurde von Alex Biryukov und Dmitry Khovratovich an der Universität Luxemburg erzeugt.

3. Blockvergütung: 12.5 ZenCash.

4. Blockerzeugung: 2.5 minutes.

5. Blockgröße: 2 MB.

6. Difficulty adjustment Algorithmus: Digishield V3, optimiert um die folgendes trailing-average Schwierigkeitsfenster zu nutzen:

   $$\text{Next difficulty} = \text{last difficulty} \times \sqrt{(150 \text{ secondes} / \text{last solve time})}$$

7. Verteilung jeder PoW Blockvergütung und der Transaktionsgebühren zwischen den Minern und anderen Stakeholdern:

(a) 88% Miner.

(b) 5% für einen oder mehrere DAOs.

(c) 3,5% für Secure Node Betreiber.

(d) 3,5% für das Kernteam.

8. Gesamtsumme des Münzangebots: 21 Millionen.

9. Halbierung der Vergütung ~ 4 Jahre, ähnlich Bitcoin.

10. Geschützte Transaktionen verbergen Sender, Empfänger und Betrag in der Blockchain.

11. Transparente Transaktionen veröffentlichen Sender, Empfänger und Betrag in der Blockchain.

12. Sichere Nachrichtenfenster in z_Transaktionen mit 1024 bytes Zeichen:

(a) Sicheres Veröffentlichen im GNUnet und/oder IPFS Standorte.

(b) Kurznachrichten zwischen Nutzern.

(c) Veröffentlichen in Channels, sichtbar für alle mit kompatiblen Wallets.

13. Secure Nodes übernehmen Infrastrukturfunktionen:

(a) Gewährleisten, dass die komplette Kommunikation zwische nodes verschlüsselt ist.

(b) Erhalten die komplette ZenCash Blockchain aufrecht.

(c) Bieten zertifizierte verschlüsselte Verbindungen für ZenCash Wallet Applikationen.

14. Secure Nodes, die den Ansprüchen gerecht werden, werden auf Münzbasis belohnt.

15. Domain Fronting Services für z Transaktionen benutzen eine kommerzielle CDN.

16. Governance durch einen oder mehrere DAOs (siehe Governance).

17. Zen DAOs zeichnen verantwortlich für den Betrieb und die kontinuierlichen Verbesserungen im System. Sie werden folgendes aufbauen und steuern:

(a) Verbreitung von Informationen über Zen (Web, Wiki, Blog, Medien).
(b) Vorschlags- und Abstimmungssystem.
(c) Berichts- und Kontrollsysteme.

18. Kernteam:

(a) Umfasst die Gründer von Zen.
(b) Mission ist es den Launch und das frühe Wachstum und Entwicklung zu lenken.
(c) Ausgaben der Geldmittel sind von Bedeutung für die Entwicklung und die Instandhaltung.
(d) Steuerung am Schnittpunkt zwischen Zen und den traditionellen Systemen.

Roadmap

“Ausprobieren bedeutet Freiheit.” (Taleb, 2012)

Zen wird als eine Integration von revolutionären Technologien gestartet, um ein System zu schaffen, auf dessen Grundlage Innovation beschleunigt werden kann. Wir werden optimale Dezentralisierung und fortwährenden Wettbewerb konstruieren, damit sich das System beständig weiterentwickelt und niemals ein Komfortlevel erreicht. Die anfängliche Roadmap deckt ein 12- 18-monatiges Entwicklungsfenster ab, um das System autonom funktionsfähig zu gestalten. Der Schlüssel hierfür ist die Entwicklung eines Kernsatzes an Integrationen mit unserem eigenen, Secure Node-Netzwerk, einem verbreiteten Datenspeichersystem wie GNUnet und einem größeren Ökosystem des Austauschs, der Miningpools und der Usercommunities. ZenCash muss vollständig funktionsfähig, leicht verfügbar und nützlich für eine breite Masse von Stakeholdern sein.

Unsere Roadmap spiegelt die Bedeutung von ZenCash als unserem ersten und wichtigsten anfänglichen Produkt im Zen Portfolio dar.

1. Verbesserte Wallets entwickeln.

   (a) Windows für t und z Transaktionen, Nachrichtenaustausch, GNUnet Veröffentlichungen.

   (b) Linux für t und z Transaktionen, Nachrichtenaustausch, GNUnet Veröffentlichungen.

   (c) Mac für t und z Transaktionen, Nachrichtenaustausch, GNUnet Veröffentlichungen.

(d) Mobil (Android und iOS) für t und z Transaktionen.

(e) Hardware für t und z Transaktionen, Nachrichtenaustausch, GNUnet Veröffentlichungen.

(f) Web Wallet für t und z Transaktionen, Nachrichtenaustausch, GNUnet Veröffentlichungen.

2. Domain Fronting Services für z Transaktionen durch die Nutzung von kommerziellen CDN.

3. Zen System Server in belastbarer Multi-Daten Center Konfiguration.

4. Widerstandsfähigkeit der Infrastruktur testen, auswerten und verbessern.

5. Segregated Witness implementieren.

6. Governance R&D Leistungen, inklusive vollständig getesteter Betriebssysteme (siehe Governance):

(a) Forschungsbericht.

(b) Verfassung.

(c) Getestetes und implementiertes Abstimmungssystem.

(d) Erste Wahl die Implementierung wenigstens eines DAO, Übergang des Kernteams.

Funktionale Elemente

Zen bringt eine Vielzahl verschiedener Elemente zusammen und formt eine funktionale Einheit daraus. Anstelle regulärer Nodes erfordert Zen Secure Nodes, was einen grundsätzlichen Standard in Punkto Sicherheit und Leistung gewährleistet und wiederum dafür sorgt, dass das System verteilt, belastbar und sicher bleibt. Durch die Durchsetzung verschlüsselter Kommunikation zwischen den Nodes, und zwischen Nodes und Wallets schützt Zen vor Abhöraktionen und Man-in-the-Middle Angriffen.

Zen begegnet zudem einer Schwachstelle in den Metadaten anderer Kryptowährungen. Wenn beispielsweise die Kommunikation in einer potentiell kompromittierten Art und Weise stattfindet und anschließend Bitcoins gesendet werden, sind die Teilnehmer der Transaktion eventuell durch die Transaktionskorrelatoren identifizierbar. ZenCash wird deshalb sichere Nachrichtenübermittlung innerhalb geschützter Transaktionen beinhalten, damit User sich auf eine Transaktion einigen, sie durchführen und den Erhalt bestätigen können. Diese funktionalen Elemente werden durch folgende Systeme sichtbar:

ZenTalk – Ein neuer Typ eines sicheren Kommunikationsnetzwerks, das eine one-to-many Kommunikation durch das dauerhafte Speichern von Nachrichten in der Blockchain ermöglicht.

ZenPub – Eine anonymisierte Plattform zur Veröffentlichung von Dokumenten durch die Nutzung von GNUnet oder IPFS.

ZenHide – Die Möglichkeit, das Blockieren von Kryptohandel durch die Nutzung von Domain Fronting zu umgehen.

5.1 T Transaktionen

T_Transaktionen sind die herkömmlichen, in einer Blockchain protokollierten Transaktionen, die durch einen privaten Schlüssel in einer Wallet kontrolliert werden. Diese werden von Bitcoin hergeleitet und ermöglichen zügige Kompatibilität mit Währungen, Wallets und anderen von Bitcoin hergeleiteten Ökosystemapplikationen.

5.2 Z Transaktionen

Hierbei handelt es sich um Transaktionen, die an geschützte, von ZCash und ZClassic übernommene, Adressen gesendet werden. Kontostände in geschützten Adressen sind privat. Wenn an eine oder mehrere geschützte Adressen Geld geschickt wird, bleibt der Wert privat, aber jede transparente Empfängeradresse wird den Token entschlüsseln und den erhaltenen Wert in der Blockchain offenlegen. Die geschützten Senderaddressen und ob der Wert von einer oder mehrerer dieser Adressen geschickt wurde, bleibt vertraulich, auch nachdem der Wert übermittelt wurde. Das ZCash Protokoll beschreibt diesen Prozess detailliert:

> Werte in ZCash sind entweder transparent oder geschützt. Transfers von transparenten Werten werden grundsätzlich wie in Bitcoin gehandhabt und haben die gleichen Merkmale von Datenschutz. Geschützte Werte werden durch Notes ausgeführt, die den Betrag und den zahlenden Schlüssel bestimmen. Der zahlende Schlüssel ist Teil einer Zahlungsadresse, die ein Ziel darstellt, an welches die Notes geschickt werden können. Genau wie in Bitcoin ist das mit einem privaten Schlüssel verbunden, der zum Ausgeben dieser Notes genutzt werden kann, die an diese Adresse geschickt wurden; in ZCash heißt es “Spending Key”.
>
> Mit jeder Note ist eine Note Commitment kryptographisch verbunden, sowie ein Nullifier 1 (damit es eine 1:1:1 Beziehung zwinschen Notes, Note Commitments und Nullifiern gibt). Um den Nullifier zu berechnen

benötigt man den verbundenen privaten Spending Key. Note Commitment und den dazugehörigen Nullifier zu nutzen ist ohne den dazugehörigen privaten Spending Key nicht möglich. Eine unverbrauchte, gültige Note, an einer Stelle in der Blockchain, ist eine, für die das Note Commitment öffentlich vor der Stelle in der Blockchain offenbart wurde, aber nicht der Nullfier.

Eine Transaktion kann aus transparenten Inputs, Outputs und Skripten bestehen, die alle wie in Bitcoin funktionieren [Bitcoin Protokoll]. Es beinhaltet ebenfalls eine Sequenz aus keinen oder mehreren JoinSplit Beschreibungen. Jeweils wird ein JoinSplit Transfer beschrieben, der einen transparenten Wert und bis zu zwei Input Notes aufnimmt und einen transparenten Wert und bis zu zwei Output Notes erzeugt. Die Nullifier der Input Notes werden gezeigt (damit sie in der Zukunft nicht nochmal genutzt werden können) und die Output Notes Commitments werden gezeigt (damit sie in der Zukunft genutzt werden können). Jede JoinSplit Beschreibung umfasst zudem einen berechnet fundierten SNARK Proof, der belegt, dass folgendes mit an Sicherheit grenzender Wahrscheinlichkeit korrekt ist:

Die Input und Output Kontostände (individuell für jeden JoinSplit Transfer)

Für jeden nicht-null Input Note existieren einige, offenen Note Commitments

Der Prover kannte die privaten Spending Keys der Input Notes.

Die Nullifier und Note Commitments sind korrekt berechnet worden. Die

privaten Spending Keys der Input Notes sind während der kompletten Transaktion kryptographisch mit einer Signatur verbunden, sodass die Transaktion nicht durch eine Seite, die die privaten Schlüssel nicht kannte, modifiziert werden kann.

Jeder Output Note wird solchermaßen erzeugt, dass es nicht möglich ist den Nullifier mit dem Nullifier einer anderen Note kollidieren zu lassen

Außerhalb des zk-SNARK wird des Weiteren überprüft, dass die Nullifier für die Input Notes nicht schon vorher offengelegt wurden (z.B. dass sie nicht schon genutzt wurden).

Eine Zahlungsadresse beinhaltet zwei öffentliche Keys: einen Paying Key, der mit den an die Adresse geschickten Notes übereinstimmt und einem Transmission Key für ein key-privates, asymmetrisches Verschlüsselungsschema. "Key-privat" bedeutet, dass Geheimtexte nicht offenlegen, für welchen Key sie verschlüsselt wurden, außer für den Besitzer des dazugehörigen privaten Keys, der in diesem Kontext Viewing Key genannt wird. Diese Funktion wird zur Kommunikation durch verschlüsselte Output Notes mit dem beabsichtigten Empfänger in der Blockchain genutzt, der den Viewing Key verwenden kann um die Blockchain nach Notes zu durchsuchen, die an ihn adressiert sind und sie anschließend zu entschlüsseln.

Die Grundlage der Datenschutzmerkmale von ZCash ist, wenn eine Note benutzt wird, der Nutzer lediglich belegt, das seine Form des Commitments für ihn offengelegt wurde, ohne zu veröffentlichen, welches Commitment genau. Das impliziert, dass eine genutzte Note nicht an die Transaktion gebunden werden kann, in welcher sie erzeugt wurde. Das ist, aus dem Blickwinkel eines Widerparts die Menge an Möglichkeiten für eine gegebene Note, die in die Transaktion eingebracht wurde, seine Menge an Rückverfolgbarkeit der Note, welche alle vorherigen Notes beinhaltet, die nicht vom Widerpart kontrolliert oder dessen Nutzung dem Widerpart bekannt sind. Das kontrastiert mit anderen Vorschlägen für private Zahlungssysteme, wie CoinJoin oder CryptoNote, die auf der Vermischung von einer begrenzten Anzahl an Transaktionen basieren und daher kleinere Mengen an Rückverfolgbarkeit der Notes haben.

Die Nullifier sind notwendig um doppelte Nutzung zu verhindern: Jede Note hat lediglich einen gültigen Nullifier, wodurch der Versuch eine Note zweimal zu nutzen den Nullifier zweimal offenlegen würde, was zur Ablehnung der zweiten Transaktion führen würde.

5.3 ZenTalk

Die Z_Transaktionen in ZenCash sind fähig, textbasierte Nachrichten zu integrieren, die verschlüsselt sind und zur Blockchain hinzugefügt werden. Es gibt eine Begrenzung von 1024 Zeichen für diese Nachrichten, und sie verbessern die Fähigkeit der User sicheren Handel zu betreiben. Statt die Transaktionen in anderen, weniger sicheren Channels, die nicht das gleiche Niveau an Datenschutz wie Zen bieten, zu besprechen, können die User via ZenTalk Nachrichten mit der oder den anderen Parteien kommunizieren. Die Möglichkeit besteht sowohl bevor als auch nachdem der geschützte Transfer stattgefunden hat und benötigt lediglich einen kleinen Aufwand an Z_Transaktionen. Diese Nachrichten können direkt von einer Z_Adresse zu einer anderen geschickt werden und sie können in einem Kanal geschickt werden. Durch die Erzeugung einer z_Adresse vom Hash eines Kanalnamens, können User den Kanal abonnieren und alles Veröffentlichte in diesem Kanal lesen.

Zum Beispiel würden Ankündigungen des Channels #ZenCash an zXXXXXXXX geschickt und es allen Usern erlauben, anonyme Nachrichten an den Channel zu schicken. Jede Nachricht würde eine begrenzte Menge an ZenCash kosten, da sie in einer z_Transaktion enthalten ist, und damit die Menge an wenig nützlichen Nachrichten in populären Channels reduzieren. Offizielle Ankündigungen würden durch Private Keys gezeichnet sein und lediglich gezeigt werden, wenn sie als fundiert erachtet wurden. Zudem können im Wesentlichen private Gruppennachrichten durch die Nutzung von z_Transaktionen erscheinen indem zunächst ein komplexer Channelname erzeugt wird und dann der Inhalt der Nachrichten mit Keys verschlüsselt wird, die lediglich die gewünschten Empfänger besitzen. ZenTalk Nachrichten würden durch

Algorithmen wie AES-256 mit Perfect Forward Secrecy (PFS) verschlüsselt, die den derzeitigen Verschlüsselungsstandards für sichere Kommunikation entsprechen.

5.4 ZenPub

Zen hat die Fähigkeit, Dokumente in IFPS oder GNUnet zu veröffentlichen. Das erreicht man durch das hinzufügen einer IFPS oder GNUnet Adresse im Textfeld einer z_Adresse. Das derzeit bevorzugte System zur Veröffentlichung von Dokumenten ist GNUnet, weil es die benötigte Infrastruktur für anonymes Veröffentlichen bereitstellt und eine aktive Datenbank an Dokumenten pflegt. Das System ist auf ähnliche Art erweiterungsfähig mit Bezug auf IFPS oder irgendwelche anderen, zukünftigen Archivsysteme. Durch die Einführung einer Nachrichtenebene in Verbindung mit einer anonymen Veröffentlichungsebene, ermöglicht ZenPub die Erzeugung tatsächlich anonymer Veröffentlichungen, die schnell an interessierte Leser verteilt werden können.

5.5 ZenHide

Es ist Regulierungsbehörden aus Krypto-Handel feindlichen Ländern möglich, traditionelle Krypto-Währungen wie Bitcoin und selbst ZCash zu blockieren. Zen nutzt Domain Fronting um die Möglichkeit auszuweiten, Transaktionen in feindlichen Netzwerkumgebungen auszuführen. So auch erklärt im "Blocking-resistant communication through domain fronting" Auszug:

> Wir beschreiben "Domain Fronting", eine vielseitig anwendbare Technik zur Umgehung von Zensur, welche den entfernten Endpunkt der Kommunikation verbirgt. Domain Fronting funktioniert in der Anwendungsebene durch die Nutzung HTTPS' um mit einem verbotenen Host zu kommunizieren, während es den Anschein hat, mit einem anderen Host in Verbindung zu stehen, der vom Zensor erlaubt ist.
>
> Der Kerngedanke ist die Nutzung von verschiedenen Domainnamen in

verschiedenen Ebenen der Kommunikation. Eine Domain erscheint in einer HTTPS Anfrage, der DNS Anfrage und der TLS Servernamen Angabe nach „außen“, während eine andere Domain „innen“ erscheint, im HTTP Host header, der durch die HTTPS Verschlüsselung für den Zensor unsichtbar ist.

Ein Zensor, der nicht in der Lage ist zwischen fronted und non-fronted Traffic einer Domain zu unterscheiden, muss ich entscheiden ob er Umgehungstraffic zulässt oder die Domain komplett blockiert, was zu teurem Kollateralschäden führt.

Domain Fronting ist einfach in der Anwendung und Nutzung und benötigt keine speziellen Kooperationen von Netzwerkmittlern. Wir identifizieren eine Anzahl an schwer zu blockierenden Webservices, so wie Content-Auslieferungsnetzwerken, die domain-fronted Verbindungen unterstützen und nützlich für die Umgehung von Zensur sind.

Die spezifische Implementierung von Domain Fronting, wie sie von Zen beim Launch genutzt wird, erfolgt mit einem Content Distribution Netzwerk, aber so wie bei jeder Komponente unserer Architektur ist sie von Beginn an auf Flexibilität angelegt und das System kann im Zuge der technologischen Entwicklungen in zahlreiche Richtungen erweitert werden.

5.6 Zen Secure Nodes

Die Nodes sind die Kernsysteme, die die Blockchain aufrechterhalten, Transaktionen von Wallets anerkennen, Miner Lösungen validieren und als dezentrales Rechnungs- und Kommunkationssystem für Kryptowährungen agieren. In Zen werden alle übermittelten Information zu und von den Secure Nodes mit wirksamen Zertifikaten unter der Nutzung von TLS Version 1.3 verschlüsselt und darüber hinaus mit Perfect Forward Secrecy (PFS) geschützt. Als Teil der Secure Node Fähigkeiten verbessert sich die Funktionsfähigkeit der ZenCash-Applikation durch:

Erweiterung RPC, um es AES verschlüsselten Daten zu ermöglichen, geschützten Transaktion innezuwohnen.

Erweiterung RPC, um perfect secrecy handshakes zwischen öffentlichen Keys zu ermöglichen.

Secure Nodes, die alle Anforderungen erüllen, warden mit dem Secure Node Anteil des Minings durch eine Rangfolgemethode belohnt. Secure Nodes müssen den #secure node Kanal verfolgen. Das Secure Node Bezahlsystem soll in einer nachvollziehbaren Art und Weise mit eindeutigen Standards bezüglich der Maximierung der Betriebsfähigkeit und der Minimierung von Problemen operieren.

1. Grundlegende Infrastrukturfunktionen, die durch Secure Nodes geleistet werden:

   (a) Sicherstellen, dass jedwede Netzwerkkommunikation zwischen den Nodes verschlüsselt ist.
   (b) Komplette Zen Blockchain bereitstellen.
   (c) Zertifizierte Verschlüsselungsverbindung für ZenCash Wallet Applikationen.

2. Secure Nodes, die die beschriebenen Anforderungen erfüllen, erhalten 3.5% der Blockmünzbasisvergütung in einer Weise die Betriebszeit in voller Funktionalität belohnt:

   (a) Node Software in einem fähigen System operieren, wie es von den Infrastrukturanforderungen erfordert wird. Empfohlene Memory sind mehr als 4 GB.

(b) Beibehaltung der kompletten ZenCash Blockchain im System.

(c) Ein valides SSL Zertifikat zur ZenCash Node Software bereitstellen zur Kommunikation mit anderen Nodes und Wallets.

(d) Wenigstens 42 ZenCash auf dem Server in einer t_Adresse für die Beteiligung belassen.

(e) Den SecureNode Kanal für Challenge-Nachrichten alle zehn Minuten vom SecureNodeHQ überwachen (in einem z_Transaktionsnachrichtenfeld)

(f) Challenges mit dem Identifizieren von Informationen des Secure Nodes beantworten.

(g) Die Antwort auf die Challenge wird eine Kombination zweier Dinge sein:

i. Eine geschützte Nachricht an das SecureNodeHQ schicken, die die öffentliche t_Adresse und den GNUnet-Dokumentenspeicherort im Nachrichtenfeld beinhaltet.

ii. Ein Dokument im GNUnet veröffentlichen, das mit privater t_Adresse gezeichnet ist und folgendes beinhaltet:

A. Öffentliche t_Adresse des Zenanteils, der ebenfalls für Zahlung der Belohnung genutzt wird.

B. SSL Zertifikat und IP Adresse.

C. Block Header der Blockchain.

D. Andere Informationen, die eventuell nötig sind um sicherzugehen, dass es sich um einen spezifischen Server handelt.

(h) Jeder Zen Secure Node muss ebenfalls ein Peer im GNUnet System sein um die Challenge-Antwort anonym veröffentlichen zu

können und anonyme Publikationen von anderen Elementen des Systems unterstützen zu können.

(i) Andere mögliche Anforderungen, die in der Zukunft auftauchen könnten um dem ZenCash-System zu erlauben, die Secure Nodes für Konsens und Rechenkraft zu nutzen.

3. Zen Secure Node Payment System (Z-SNPS):

(a) Z-SNPS wird durch einen Zen DAO operiert.

(b) Z-SNPS wird die Challenge-Antworten von allen Secure Nodes nachverfolgen.

(c) Secure Nodes werden durch ihre t_Adressen nachverfolgt und veröffentlicht.

(d) Mined Blöcke werden die 3.5% Belohnung an das ZC-SNPS System zahlen, welches ZenCash regelmäßig an die Secure Nodes verteilt, basierend auf deren Betriebszeit in dem definierten Zeitraum.

Da Zen dieses verteilte Rechennetzwerk in der Form von vergüteten Secure Nodes haben wird, wird es für diese Nodes eventuell erforderlich sein, je nach Weiterentwicklung des Communityverständnisses, andere Rechenleistungen für das Netzwerk zu leisten.

5.7 Zen Standard Nodes

Die ZenCash Applikation kann auf jedem Linuxserver, Mac oder PC operiert werden. Der Client funktioniert als Node und Wallet. Obwohl er nicht die volle Verschlüsselungsfähigkeit wie ein Secure Node hat, helfen alle Nodes dem System, Funktionen effizient zu betreiben und gegen Attacken widerstandsfähig zu sein.

5.8 ZenCash Wallet Software

Die ZenCash Software kann als Wallet operiert werden. Die Command Line Wallet ist die grundsätzliche Form, aber Graphical User Interface (GUI-) basierte Versionen existieren schon für Desktops. Mobil, Web, Rasperry Pi und andere Hardware Wallets sind eine Topppriorität, die es so schnell wie möglich zu entwickeln gilt, um die Erfahrung der User und die Sicherheit von ZenCash Token zu steigern. Wallets können so konfiguriert werden, dass sie jeden verfügbaren ZenCash Node zur Kommunikation nutzen können, oder können so aufgesetzt werden, dass sie sich nur mit Secure Nodes verbinden um einen hohen Standard an Informationssicherheit zu gewährleisten.

5.9 Applikationen

Wir betrachten Zen als ein optimal dezentralisiertes open-source Projekt und deshalb erwarten wir, dass Applikationen von vielen Parteien konstruiert und zum Ökosystem beigetragen werden. Viele dieser Beiträge werden wahrscheinlich aufgrund einer freiwilligen open-source Stimmung erfolgen, aber wir erwarten ebenfalls, dass eine starke, unternehmerische Community um die Plattform herum wachsen wird. Zusätzlich hat das Kernteam einen vollständigen Entwicklungsplan für Applikationen, der bereits in Arbeit ist. Das beinhaltet, ohne darauf begrenzt zu sein:

Node Applikationen
Equihash open-source Mining Pools
Governance Applikationen
Kontroll- und Berichtssysteme
Alle Arten von Wallets
Secure Node Kontrollsystem
Secure Node Zahlungssystem

Governance

“Deshalb scheitern Ideologien: Nicht durch Gewalt, sondern durch Beispiele wie es besser geht.” -Joe Quirk, Seasteading Institute

Zen ist im Sinne eines dezentralisierten Governance-Modells erdacht, das die Befähigung vieler Stakeholder und die Flexibilität, sich optimal der Community anzupassen, beinhaltet. Grundsätzlich sieht unsere Philosophie vor, dass wir a priori die beste Herangehensweise nicht kennen, aber dass wir einige Ideen haben, wie wir das System initialisieren und es gestalten, damit es sich mit den Ansprüchen der Community entwickeln kann. Wir glauben in Steuerung als ein Service (GaaS) und beabsichtigen unseren direkten Interessenvertretern, der erweiterten Community und der Welt Nutzen effizient bereit zu stellen.

„Jede Industrie, die schlechten Service zu hohen Preisen bietet, verdient es erschüttert zu werden” (Quirk, 2017), Governance als ein vollendetes Beispiel. In Solidarität mit anderen Projekten und Ideen, die überall auf der Welt existieren, lehnen wir erzwungene Zentralisierung ab und unterstützen Voluntarismus. Anstatt einer Minderheit der Menschen mit Macht zu vertrauen, glauben wir, dass alle Menschen das Recht haben, mit Freiheit betraut zu werden.

Die Kernphilosophie unseres Governancesystems ist, dass Dezentralisierung von Macht Inklusion und Kreativität maximiert. Praktische Implementierungen müssen erkennen, dass das Zusammenführen von Ressourcen und Bemühungen Synergien bietet, die optimal gegen vollständige Dezentralisierung abgewogen werden müssen; optimale Punkte sind Zustands- und Zeitvaria-

bel und werden am besten durch freiwillige Teilnahme und Loslösung bestimmt.

Es ist bedeutend, dass wir ein System aufsetzen, in dem konkurrierende DAOs entstehen können um Ressourcen zu teilen oder sogar weniger effiziente oder unbeliebte Versionen zu überlagern. Es sollte keine one-size-fits-all Struktur geben, die gegenüber der Umwelt, Funktionen, Kulturen oder der Zeit unveränderlich ist; stattdessen sollten Strukturen beweglich sein, angepasst an spezifische Probleme und flexibel zu wachsen, wenn nützlich und zu verschwinden, wenn im Begriff zu scheitern verglichen mit Alternativen. Solch ein System der Systeme würde sich dynamisch entwickeln, sodass es antifragil im Angesicht kompetitiven Feedbacks ist.

Unser gegenständlicher Zustand der Steuerung wird Dezentralisierung, Implementierung von Effizienz, Trennung von Macht, Ermächtigung weiter Teile der Stakeholder und evolutionäre Flexibilität austarieren. Dieser anfängliche Zustand wird das Ergebnis von wenigstens 12- 18-monatigen Bemühungen in Forschung und Entwicklung in Spieltheorie, Politikwissenschaft und ökonomischer Forschung bezüglich optimaler Abstimmungsmechanismen in Verbindung mit der Rückmeldung von zahlreichen Testnet Implementierungen sein. Das Projekt wird eine unserer ersten finanzierten Bemühungen mit finalen Ergebnissen sein, was einen ausführlichen Forschungsbericht und einen operativen Code, der in das Zen Netzwerk integriert wird, beinhaltet. Innerhalb von sechs Monaten der Governanceimplementierung erwarten wir Führungsteams im Einsatz zu haben, nachdem unsere ersten vollständigen und offenen Wahlen stattgefunden haben.

6.1 Optimale Dezentralisierung

“Ein Schreckgespenst sucht die moderne Welt heim, das Schreckgespenst der Kryptoanarchie.” -Crypto Anarchist- Manifesto

Mit Dezentralisierung meinen wir, dass jeder die gleiche Möglichkeit hat, zu

partizipieren, dass wir vollkommen inklusiv agieren und dass die Entscheidungsfindung größtmöglich diffundiert, sodass das System widerstandsfähig gegenüber Übernahmen ist. Theoretisch bedeutet maximale Dezentralisierung, dass jeder Einzelne legitimiert ist, Entscheidungsfindungen in gleichem Maße beeinflussen zu können; dieser Zustand ist schwierig in der praktischen Implementierung, wenn man Ressourcen bündelt um in einem gemeinsamen System zusammenzuarbeiten. Selbst wenn es so implementiert wäre, einzelne Entscheidungen vereinigen sich auf natürliche Weise zur Effizienz in der Zusammenarbeit und Ressourcen sammeln sich bei bestimmten Stakeholdern in einem ungleichen Verhältnis.

Wir können diese natürlichen Kräfte nicht stoppen, noch gibt es einen Grund dafür, sie ausnahmslos als schädigend zu erachten. Wir können jedoch ein System gestalten, sodass jede Teilnahme freiwillig ist, Macht zur Entscheidungsfindung bezüglich der Allokation von Ressourcen über einen großen Querschnitt an Stakeholdern verteilt ist und ein zuverlässiger Mechanismus zur Weiterentwicklung mittels Feedbacks existiert. Eine Struktur, die mit Flexibilität durchzogen ist, ist wichtiger, als von Beginn an das beste System aufzusetzen, das sich an alle Umstände anpasst, speziell da wir eine Bewegung gründen, die so expansiv ist, dass es unmöglich erscheint, alle Entwicklungen vorherzusagen.

Die Effizienz bezüglich der Implementierung ist ebenfalls ein wichtiges Bedenken bei dezentralisierten Organisationen. Reine Dezentralisierung könnte zu einer Lähmung in der Entscheidungsfindung führen, zu geringer Wahlbeteiligung oder zu einem Irrglauben der Gruppe im Extremfall. Deshalb scheuen wir uns zu Beginn ein System reiner Demokratie für jede Entscheidung zu gründen und nehmen uns die Zeit konkurrierende Modelle zu untersuchen

und sie unter wechselnden Stressbedingungen zu testen. Unser vorgeschlagenes System der freien und offenen Konkurrenz für DAOs ist geschaffen um Gruppen von high-performing Experten und Profis funktionaler Gebiete zu ermutigen, ihre Führerschaft in spezialisierten Bereichen vorzuschlagen, sodass sich unsere systemweite Effizienz der Umwandlung von Ressourcen in höherwertige Endprodukte oder -services kontinuierlich weiterentwickelt, und sich den Bedürfnissen und den Anforderungen unserer User anpasst.

6.2 Checks & Balances

Eine wichtige Lektion der Menschheitsgeschichte ist, dass Macht am besten getrennt wird und konkurrierende Cluster von Macht einen Zustand des Gleichgewichts von gegenseitiger Kontrolle herbeiführen sollten. Die Balance sollte unkontrolliertem Wachstum in einem einzelnen Cluster gegenüber widerstandsfähig sein, wodurch das ganzheitlich System einer Übernahme erliegen könnte. Um diesen Zustand von Beginn an zu verhindern, wird Zen mit einem Kernteam starten, das 3.5% der Finanzierung der Block-Belohnung kontrolliert und einem anfänglichen DAO, der Industrieführer enthält, die 5% der Ressourcen kontrollieren. Zusätzlich wird unser objektiver Zustand, der nach der 12- 18-monatigen Forschungs- und Entwicklungsphase und anschließendem Testen implementiert wird, einen hybriden Typ des Multi-Stakeholder Abstimmens beinhalten, sodass ein großer Querschnitt der Community die Macht behält, Entscheidungen zu beeinflussen und Ressourcen zuzuteilen. Jede Komponente unser Governancestruktur wird letztlich kompetitivem Feedback und Veränderung unterliegen. Wir bedienen uns hier einer evolutionären Herangehensweise, die mit einem einfachen Model beginnt und mit der Community wachsen wird.

DAO: Infrastruktur, Vorschläge und Abstimmungen

Das Zen-System wird wenigstens einen DAO haben, der durch einen Teil der Miningbelohnung finanziert ist und durch ein Abstimmungsverfahren gesteuert wird, das Stakeholder zusammenbringt. Dieses System der Steuerung soll helfen zu gewährleisten, dass die Umsetzung von Veränderungen, Verbesserungen und Integration die Wahrscheinlichkeit von Streitigkeiten begrenzt und die Aussicht auf eine Fork des Projekts aufgrund von Uneinigkeit reduziert. Wenn wir unseren erweiterten Governanceplan, nach intensiver Forschungs- und Entwicklungsarbeit implementieren, ist das Ziel, die Governancelandschaft dem Wettbewerb zu öffnen; das bedeutet, wir könnten in der Zukunft mehrere, konkurrierende DAOs mit unterschiedlichen Teams, die an unterschiedlichen Problemen arbeiten, entstehen sehen. Jede DAO würde mit einer eigen vorgeschlagenen Struktur, Prozessen und Zielen geschaffen werden, was garantiert, dass sich diese Eigenschaften durch Wettbewerb entwickeln und die falschen organisatorischen Entscheidungen zu Beginn nicht weitergeführt werden.

Unsere DAOs werden für den Aufbau, die Wartung und die Verbesserung der Infrastruktur, die das System am Laufen halt, verantwortlich sein. Sie sind außerdem für die Umsetzung von Veränderungen der Zen Software-Applikationen verantwortlich und flexibel genug, sich den Prioritäten der Community, wie Reichweite, Marketing und Training anzupassen.

Sobald das Zen System an Bekanntheit gewinnt, werden ebenso die unterstützenden Strukturen für User, Miner, Secure Node Betreiber und Ökosys-

tempartner wachsen und sich anpassen müssen. Die DAO Strukturen werden Mittel haben, die durch Projekte und Vorschläge verteilt werden und mit denen das Wachstum und die Unterstützung gefördert wird.

Die Community soll ermutigt werden, zu Zen auf unterschiedlichste Art und Weise beizutragen. Die DAOs sind für das Koordinieren der Communitybeiträge verantwortlich und haben die Mittel Ausgaben der Community zu begleichen. Eines der Ziele von Vorschlägen ist es, die Communitymitglieder für ihre Ausgaben, die durch die Unterstützung des Systems anfallen, zu entschädigen.

Zum Launch wird Zen einen DAO mit bekannten Fachleuten verschiedener Branchen haben. Sobald der Governance Plan bereit für die Umsetzung ist, wird dieser DAO einer der vorgeschlagenen Gruppen sein, die dem Wettbewerb mit anderen Ideen zur Governance Struktur unterliegen; die breite Masse der Community wird die Entscheidung treffen.

7.1 Zen Infrastructure Operated by DAO

Das DAO System wird Applikationsserver und -services pflegen:

- Secure Node Server zur Validierung.
- Forum Server.
- Moderation von Slack.
- Websites.
- Blogs.
- Vorschlagssystem.
- Abstimmungssystem
- Binäre Quellen.

Die DAOs sind für folgenden Support zuständig:

Menschen helfen, ZenCash oder andere Systemfunktionen znuzen.
Secure Node Betreibern helfen.
Fehler des Belohnungssystems beheben.
Fehler des Abstimmungssystems beheben.
Für die Ausweitung des Supports sorgen.
Rasche und definitive Entscheidung bezüglich Fragen und Problemen bieten.

DAO verteilt nach einer erfolgreichen Abstimmung und dem Ende der Vetophase ZenCash an die Ideengeber des Vorschlags.

Es wird zu Beginn 3-5 DAO Verantwortliche geben, was aber letztlich offen sein wird. Verantwortliche können anonym bleiben, aber das ist keine Voraussetzung. Tatsächlich bringen offen geführte Identitäten den Vorteil, dass frühere, fachmännische Erfolge und Charakterstärken auf natürliche Art in das Zensystem aufgenommen werden.

Es wird Auseinandersetzungen geben, weshalb Mechanismen zur Lösung entwickelt werden müssen, um diese effizient und fair zu entscheiden. Eine Idee, die im Forschungs- und Enwicklungsprojekt zum Thema Governance geprüft wird, ist die Etablierung eines Gerichtswesens und eines Jurysystems.

7.2 Proposal Submission and Voting

Jedes DAO wird eine eigene Struktur, Prozesse und Prioritäten haben, aber ein gleicher Mechanismus wird ein offenes und freies System zur Einhändigung von Vorschlägen zur Arbeit sein, sowie ein Entwicklungs- und Vergabeprozess. Es gibt keinen Grund anzugeben, wie es passiert, nur, dass es passieren sollte. Es ist eine für die gesamte Menschheit offene Community, weshalb es keine Hürden für die Teilnahme geben sollte. Eine vorgeschlagene Methode

für unseren DAO zu Beginn lautet wie folgt:

1. Abstimmung alle zwei Monate. Deadline zur Abgabe von Vorschlägen zwei Wochen vor der Abstimmung. Abstimmungsdaten: 31. Jan, 31. März, 31. Mai, 31 Jul, 31 Sep, 31 Nov.

2. Abgabe von Vorschlägen ist einen Tag nach der Abstimmung möglich.

3. Veto – das Kernteam kann einem Vorschlag innerhalb von 7 Tagen nach einer Abstimmung mit einem einstimmigen Kernteam-Veto widersprechen (Das sollte eigentlich nie passieren).

4. Vorschläge können im ZenCash Equivalent des Einheimischen in der Währung am Tag der Abstimmung finanziert werden (Um dem Problem des raschen Anstiegs wie bei Dash vorzubeugen, der zur Ablehnung des Projektes führt)

5. Abstimmung mit Token. 1440 Abstimmungstoken werden einen Monat vor der Abstimmung verteilt.

6. Der Großteil der Entscheidungen wird durch einfache Mehrheit getroffen > 720 Besitzer von Token wählen "Ja"

7. Einige Entscheidungen durch qualifizierte Mehrheit > 1080 Tokenbesitzer wählen "Ja"

7.3 Abstimmungsprozess

Verteilungsplan für Token, für jede Abstimmungsphase wiederholt, 1440 Token insgesamt:

1. 360 Token stehen zum Verkauf – erlaubt den Usern und ZenCash Besitzern Stimmen zu kaufen.

   (a) 1-30: 1 ZenCash

   (b) 31-60: 2 ZenCash

   (c) 61-90: 3 ZenCash

   (d) etc. bis zu 12 ZenCash per Token für mindestens eine Gruppe von 30

2. 240 - ZenCash Projetkentwickler.

   Vergeben aufgrund von Engagement, Pull-Requests oder anderen begründeten Bewertungen ihrer Beiträge.
   Das Ziel ist Software und Systementwickler zu befähigen.

3. 60 – Börsen, die ZenCash führen.

   (a) Top 6 gemessen am Volumen bekommen 10 jeder.

4. 60 -- Eigentümer von Mining Pools

   (a) wird alle 480 Blocks verteilt, um das Gründen des Blocks bündeln.

5. 360 – Secure Nodes.

   (a) 1 wird alle 40 Blocks verteilt bis alle 360 verteilt sind.

Zen Community: Stark und Lebendig

Zen wird sich symbiotisch mit dem ZClassic Projekt entwickeln, mit unserer kombinierten Community die rund 2.000 Forum Mitglieder, Entwickler, Miner, Händler, langfristige Investoren, Partnerorganisationen, Börsen, Bloggern etc. zählt. Als ein komplett offenes und inklusives Projekt sind alle möglichen Beiträge und Hilfestellungen von überall auf der Welt in Zen eingeflossen und dieses improvisierte und gleichzeitig beständige Kollektiv ist eines unser entscheidenden Merkmale als ein System. Unsere Community hat bereits eine andauernde Geschichte nicht nur positiver Beziehungen und freundlicher Interaktionen sondern auch spontanen Supports und Engagements, das hervortritt um verschiedene Probleme zu verhindern oder zu lösen.

8.1 Open Source Ethos

Open-source Projekte können ein sich entwickelndes und fließendes Set an ethischen Grundsätzen annehmen, allerdings hoffen die Gründer dieses Projektes die Community auf die Prinzipien von Zen fokussiert zu halten, sprich unserem Namen. Wir entwickeln ein System, bei dem wir hoffen, dass es für friedliche Zusammenarbeit, erlaubnisfreie Innovationen und maximale Inklusion genutzt wird. Wir hoffen, dass unser Vermächtnis ein enormer, positiver Überschuss für die Gesellschaft sein wird und wir persönlich weigern uns mit irgendjemandem zu arbeiten, der Schaden, egal ob physisch oder durch Betrug, beabsichtigt.

8.2 Zen Support

Zen Support bezieht sich auf eine Community von Zen Entwicklern und anderen verteilten IT Fachleuten, die sich dem Thema widmen, Technologie weiterzubringen und Usern grundlegende Hilfe anzubieten. Dieses Netzwerk

wird durch die DAO finanziert und wird dafür sorgen, die Zen Technologie zur intuitivsten und am einfachsten einzusetzenden innerhalb des Ökosystems zu machen. Zen Support wird zudem aus einem Netzwerk aus Mitwirkenden verschiedenster Industrien bestehen, die sich dazu verpflichten, als Botschafter, Mentoren und Unterstützer für Zen Mitwirkende zu helfen. Mehr darüber in nachfolgenden Zen Community Abschnitten. Zen Support ist eine Verpflichtung, dass Zen strukturell dafür entworfen ist, Inklusion, Zusammenarbeit und kollektive Hilfe zu fördern und dass die ausführenden Verantwortlichen, Zen Botschafter, verifizierte Zen Unternehmer oder jegliche Vertreter der Zen Community eine Ressource darstellen, auf die sich Mitwirkende verlassen und mit denen sie zusammenarbeiten können.

8.3 Zen Outreach

Unsere Roadmap enthält aufregende, beispiellose Outreach-Programme die dazu dienen werden, unser kollektives und förderndes Engagement mit Menschen aller Gesellschaftsschichten zu stärken. Kurzum Zen hat keinen einzelnen Zielmarkt; wie könnten wir auch, wenn der praktische Anwendungsfall und die Umsetzung unserer Technologie breit und vielseitig sind? Wir haben nicht vor die Nutzbarkeit von Zen auf die persönlichen Vorstellungen unserer Kernteammitglieder zu beschränken, alternativ werden wir daher Programme launchen, die von Beginn an dafür entworfen sind, dass Engagement mit Zen zu maximieren und den Communitymitgliedern zu erlauben, unser Mission und Initiative anzupassen, wenn Zen sich weitereinwickelt. Unser anfängliches DAO stellt Ressourcen zurück um experimentelle Programme zu fördern und aktive Beiträge zu unserer Community zu belohnen. Einige dieser vorgeschlagenen Programmideen sind unten erklärt.

Einmal mehr, Zen ist integrativ und agnostisch und unsere weltweite Präsenz wird diese Kernwerte wiederspiegeln. Wir werden Interessengruppen wie Unternehmer, Aktivisten, Entwickler, Universitäten, Firmen und uninformierte

aber neugierige Einzelpersonen, die sich alle mit variierenden Erfolgsbilanzen von Engagement im Bereich Kryptowährungen schmücken, integrieren.

Durch unser Zen Ambassador Program werden erfahrenen Usern, Vordenkern und leidenschaftlichen Community Mitgliedern Möglichkeiten gegeben, Zen zu repräsentieren und unsere Vision an Menschen in Ecken der Welt heranzutragen, die ohne Zugang zu Ressourcen, Kapital und Technologie sind, die nötig wären um unserer Community durch Eigeninitiative beizutreten. Führungspersonen in diesem Programm können mehreren Zielen dienen, von der Beratung von Zen Startups bis zum Mentoring von Zen Chaptern um Zen in der Presse zu repräsentieren.

Durch die Teilnahme an unserem Zen Youth Program werden globalen Minern intensives Coding und Schulungen mit Bezug auf Geschäftsentwicklung angeboten und einzigartige Möglichkeiten für das Engagement mit der Zen Kollektive. Diese Initiative wird facettenreich sein mit Angeboten die von weltweiten Wettbewerben unter Jugendlichen für DAO-finanzierte Startups, die auf der Zen Plattform basieren, bis zu Lotterien reichen, die Ressourcen verteilen um Ausgaben für die Ausbildung der Zen Youth zu decken. Diese jungen Pioniere werde auch dazu mobilisiert, Gleichaltrige zu rekrutieren und sich in ihren Communities zu engagieren.

Unternehmer, die DAO-finanzierte Projekte managen werden Zen Verified Entrepreneurs und bekommen Zugang zu relevanten startup-accelerator-style Vorteilen, wie Zugang zu erfolgreichen Business Mentoren, Marketing- und Nutzerakquise-Channels, open-source Einsatz der Entwickler, direkte Channels zu Investoren und Venture Capital Firmen und Events, Partnerschaften und Seminaren, die dazu entworfen sind, gemeinsam Probleme zu lösen und Innovationen voranzutreiben.

Einzelne Mitgestalter werden Zugang zu Plug und Play Inhalten erhalten, gestaltet um in der Verbreitung der Bewegung durch Zen Chapter zu helfen,

die die Zen Technologie, ethische Grundsätze und/oder Governance- und Entwicklungsprojekte rund um die Welt erklären. Diese Zen Chapter werden lokalisierbar und konfigurierbar sein, mit flexiblem Schwerpunkt je nach Region und Bedürfnissen der Community. Zen wird über eine grundlegende Online-Plattform materieller Ressourcen verfügen, die wie folgt aussehen:

Marketing und bildende Inhalte, die die Ursprünge, Einzelheiten, Differenzierungen und Ziele von Zen beschreiben.

Vorlagen und Ideen für Gruppen, die Zen gesponserte Werbe- oder Bildungsevents, Konferenzen und Wettbewerbe abhalten möchten.

Module, Diskussionen und Webinare bezüglich Zen Prinzipien und wichtigen Themen für Chapters um teilzunehmen und beizutragen, mit beispielsweise Coding, Unternehmertum, ethischen Grundsätzen von Dezentralisierung, Grundlagen der Blockchain, etc.

Datenbanken von Business Angels, juristischen Dokumenten, Umsatzmodellen, Taktiken zur Userakquise etc. um Chapter dem Ziel näher zu bringen, eine Initiative zur Geschäftsentwicklung unternehmen oder sich um eine Verbesserung der Community bemühen.

Zugang zu Zen Mitwirkenden und Entwicklern zur Unterstützung, Rat, Anleitung und Hilfestellungen via Zen Channels.

Zum Beispiel könnte ein Zen Chapter auf den Philippinen, wo lediglich 30% der Bevölkerung Zugang zu finanziellen Dienstleistungen haben, virtuell mit der internationalen Gemeinschaft zusammenarbeiten, um ein FinTech Projekt zu entwickeln, das die speziellen Bedarfe der Phillippinos und Besonderheiten der Kultur und Infrastruktur berücksichtigt. Solch ein skalierbares Engagement könnte die Reibereien reduzieren, die diese Gesellschaften in der Vergangenheit von autonomer Stimulierung ihrer eigenen kleinen Wirtschaften

abgehalten haben und ihre Fähigkeit zu konkurrieren verbessern.

Virtuelle Interaktion und Kommunikation ist eine unschätzbare Entwicklung des 21. Jahrhunderts und wird der Kern-Channel sein, um Menschen tausende Kilometer entfernt voneinander zu verbinden um in Zusammenarbeit Zen Innovation und Entwicklung zu fördern. Abgesehen davon erkennen wir bei Zen, dass es etwas Großartiges ist, mit denjenigen persönlich zu interagieren, die sich auf gleiche Weise den gleichen Prinzipien und einer gemeinsamen Vision widmen. Zen University wird jährlich stattfinden, um Zen's aktivste und wertschaffendste Mitwirkende, aufstrebende Jugendliche und herausstechende Unternehmer zu ehren und zu motivieren. Es wird außerdem eine Lotterie geben, die Tickets nach dem Zufallsprinzip an besonders konforme und sichere Zen Nodes verteilt. Das Thema, der Inhalt und das Ziel dieses Events werden den Präferenzen der Community folgend variieren.

Unsere Mittel sind für unsere Zen Community gedacht, was viele weitere Kategorien von Teilnehmern und Initiativen umfasst und viel mehr Wert als die herkömmlichen Interessengruppen eines Kryptowährungsprojekts bietet. Wir hoffen genauso eine soziale Bewegung wie ein technologisches Projekt zu sein, mit dem unverfälschten Endziel dabei zu helfen, Leben freier und für so viele Menschen wie möglich erfüllender zu machen.

Wettbewerbslandschaft

“Wir haben lange geglaubt, dass Firmen mit der Zeit dazu tendieren, bequem zu werden während sie dieselben Dinge machen, nur inkrementelle Veränderungen vornehmen. Aber in der technologischen Industrie, wo revolutionäre Ideen die nächsten großen Wachstumsgebiete vorantreiben, muss man ein bisschen unbequem sein um relevant zu bleiben.» -Larry Page, Alphabet

Wettbewerb durchdringt Zen bis zu dessen Kern; auf natürliche Art und Weise ist es eine Notwendigkeit von optimaler Dezentralisierung und ein Grundsatz, von dem wir glauben, dass er positive Entwicklungen ermöglicht. Dieser Prozess beinhaltet auch Wettbewerb in einer größeren Kryptowährungslandschaft für ZenCash und für unser System im Ökosystem von Blockchain Plattformen.

ZenCash konkurriert direkt mit ZCash, ZClassic, Dash, Monero, ZCoin, Bytecoin, ShadowCash, Boolberry und anderen Datenschutz-umfassenden Kryptowährungen. Der Wettbewerb bewegt sich zwischen einer Zahl an Dimensionen, aber von einer technologischen Perspektive aus konkurrieren wir direkt mit den anderen zero-knowledge Währungen die zk_SNARKs benutzen. ZCash war der Pionier in diesem Bereich und unsere Technologie profitiert unmittelbar von deren bahnbrechenden Beiträgen. Datenschutz als Funktion bedeutet ebenfalls, dass ZenCash mit anderen Implikationen konkurriert, sowie Zerocoin Protokoll, CryptoNote, RingCT und einfachere Mixers. All diese Coins dienen einer speziellen Nische auf der Nachfragekurve für Kryptowährungen.

Unser Leistungsversprechen lautet, dass wir Elemente integrieren, die wir als best-in-class betrachten. Das beginnt mit der Übernahme von ZCash's Umsetzung des zero-knowledge Schützens via zk-SNARKs, aber wir gehen noch einen bedeutenden Schritt weiter und verschleiern unser komplettes Netzwerk mit end-to-end Verschlüsselung und ermöglichen Nachrichtenübermittlung mit der sichersten Infrastruktur der Branche. Wichtig ist, dass wir nicht beabsichtigen verdrängt zu werden, weil wir strukturell vorbereitet sind unsere Systeme nicht nur upzudaten und zu verjüngen, sobald die zugrundeliegende Technologie voranschreitet, sondern selbst die Innovatoren in der Industrie zu sein.

Zen baut eine Systemarchitektur mit ZenCash als seinem Wert-Token, oder Treibstoff für Transaktion. Als solcher konkurrieren wir ebenfalls mit Projekten größerer Plattform-Typen wie Ethereum, Ethereum Classic, NEM, Lisk und Synereo über die dezentralisierte Applikationen (dApps) gebaut werden können. Auf diesem Gebiet behält Zen's einfache Scriptingsprache, die von Bitcoin und ZCash übernommen wurde, eine hohe Sicherheit und einen großen Widerstand gegen eine breite Palette von Angriffvektoren, aber begrenzt gleichzeitig die Grade an Freiheit, die nützlich für komplexe Codeausführungen möglich für Plattformen mit erweiterter Turing-complete Scripting sind, ähnlich zu Ethereum und Ethereum Classic. Unser Vorteil in dieser kompetitiven Arena ist, dass dApps zusätzlich zu dem weltweit sicherstem Kryptowährungsnetzwerk gebaut werden können und dass wir flexibel genug sind, über Chains strategischer Partnerschaften zu operieren.

Unsere einzigartige Innovation in der Kryptowährungscommunity ist unser vollständig konkurrierendes und evolutionäres Governance Modell, einen breiten Querschnitt an Stakeholdern in einer Umgebung optimaler Dezentralisierung zu bevollmächtigen. Bitcoin hat den ursprünglichen Durchbruch in verteilter Einigkeit geschaffen, aber andere Projekte haben es seitdem mit diversen Abstimmungsmechanismen weiterentwickelt. Diese Projekte bewegen sich zwischen Dash mit seinem einfach Vorschlagsabgabe- und Communityabstimmungsmodell bis hin zu Decred mit seiner verankerten Com-

munity-Governance; jede hat positiv zur Entwicklung der dezentralisierten Einigkeit beigetragen, aber Zen hebt es durch zusätzliche Beschränkungen auf ein neues Niveau, wie das unser System darauf ausgerichtet ist, sich mit der Zeit durch andauernden Wettbewerb zwischen Anbietern von Governance Services innerhalb des Ökosystems weiterzuentwickeln. Wir implementieren ein autonomes System, das sich mit Feedback und trial-and-error Innovationen wie sich dezentralisierte Systeme organisieren, verändern wird um spezifische Probleme zu lösen. In diesem Sinn glauben wir, dass Zen eine bahnbrechende Neuerung in sozialer Technologie ist, ein System als erster aufzusetzen, das niemals in diesem Maße versucht wurde.

Aus allgemeiner Sicht konkurriert Zen mit aktuellen Währungen und Banksystemen, genauso wie mit aufstrebenden FinTech Startups mit besonderem Vorteil, den Entmündigten Services bereitzustellen. Wir haben uns dazu entschlossen, unseren Beitrag zu diesem innovativen, an Sozialleistungen orientiertem Bereich zu leisten, indem wir gesteigerten Datenschutz und Sicherheit bieten. Als ein sicheres Nachrichtenübermittlungs- und ein verbreitetes Datenarchivierungssystem konkurrieren wir mit anderen Services, wie Signal, Telegram und dem Tor Projekt. Es gibt zudem eine unendliche Anzahl potentieller Projekte, die auf unserer Zen Plattform gebaut werden können und unsere Wettbewerbsfähigkeit exponentiell erhöhen.

Wir sehen Wettbewerb als einen Wegbereiter für gesunde Prozesse des Wachstums und begrüßen maximalen Wettbewerb daher. Wir würden lieber in einer Welt mit erbitterten Konkurrenten leben, die uns zwingen, unsere Innovationen zu beschleunigen, als in einer statischen Welt frei von Fortschritt. Wir hoffen, dass Zen positiv zum menschlichen Wohlergehen beiträgt, indem es großartige Technologien und Communities integriert, Governance in einen konkurrierenden Service verwandelt und es jedem auf der Welt ermöglicht, an unserem System der unverbotenen, zusammenwirkenden und dezentralisierten Innovation teilzuhaben. Wir sehen Etablierte und zukünftige Startups in diesem Bereich als potentielle Partner und Alliierte und nicht als Winner-takes-all Konkurrenten.

Die Zukunft Zen's

Prognostizieren ist eine herausfordernde Aufgabe, aber wir sehen eine glänzende Zukunft für Zen und das friedliche und produktive Ökosystem, das wir aufbauen. Wir glauben, dass die dezentralisierten, vollkommen integrativen, freiwilligen und flexiblen Organisationen, die wir erschaffen, in der Zukunft überlegen sein werden verglichen mit den statischen, zentralisierten, one-size-fits-all Versionen, die im 20. Jahrhundert aufrechterhalten wurden. Die Einführung von Kryptographie, freiwilliger Philosophie und Blockchain Technologie machen so etwas möglich und wir glauben, viele Menschen teilen unsere Vision einer besseren Zukunft bereits jetzt und werden sie zukünftig teilen; besonders, wenn sie sehen, wie wir Innovationen beschleunigen können und das menschliche Wohlbefinden verbessern können, indem wir jedem die Befähigung geben, seine Werte auszudrücken.

Die nächsten ein oder zwei Jahre werden zeigen, wie diese Vision in unserer anfänglichen Organisation verwirklicht werden wird, indem wir unsere Roadmap realisieren. Auf dem Weg wird es sicherlich Herausforderungen geben, aber Flexibilität und friedliche Zusammenarbeit überkommen stets schier unüberwindbare Probleme.

Wir haben das Glück in einem Zeitalter unglaublicher Innovation, sowohl der Technologie als auch der Ideen, zu leben. Wir bauen auf den Schultern der sprichwörtlichen Riesen, einige davon sind unten aufgelistet, aber andere bleiben ungenannt und zwar nur, weil es so viele von ihnen gibt und die Beiträge so grundlegend sind.

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 Du eld, Kyle Hagan. (2014) Darkcoin: Peer-to-Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System.

[4] David Fi eld, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. (2015) Blocking-resistant communication through domain-fronting.

[5] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) ZCash Protocol Speci cation 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 Re-store the Environment, Enrich the Poor, Cure the Sick, and Liberate Humanity from Politicians. Free Press.

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