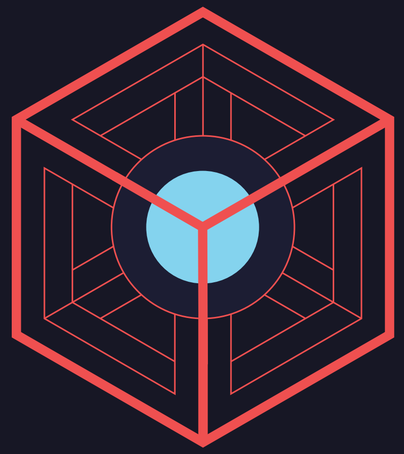


Z E N

[Ein Dezentralisiertes Finanzsystem]

ABSTRAKTES

Ein Mechanismus, welcher alleinig auf einem Peer-to-Peer System basiert, würde es sich gegenseitig misstrauenden Parteien erlauben, Verträge ohne Bezug auf das existierende Rechtssystem zu entwickeln. Diese Vereinbarungen, auch Smart Contracts genannt, können in Code niedergefasst werden, wobei im Streitfall dieser auf einem öffentlichen, dezentralisiertem Netzwerk ausgeführt wird.

Aktuellen Plattformen fehlt die Sicherheit und Zuverlässigkeit um finanzielle Verträge auszuführen. Zen ist eine neue Plattform, welche die Erstellung, Vereinfachung und Einhaltung von Verträgen ermöglicht. Wir benutzen die ZF* Sprache, wobei sie auf dem BTC Paradigma (UTXO) basiert. Damit können wir formelle Verifikation und den Ausdruck von beweisen und deren Verifikation garantieren. Alle Zen Token werden gleich behandelt, wobei auch das BTC Netzwerk beobachtet wird, um Interoperabilität zu gewährleisten.

MOTIVATION

Der Kern des Zen Teams, arbeitet schon seit 2014 in der Blockchainszene zusammen. Nach jahrerlanger Forschung, fingen sie im Juni 2016 an das Zen Protocol zu entwickeln.

Wir glauben, dass Menschen das Recht haben, Ihre eigenen Finanz-Assets zu kontrollieren. Wir fühlen uns verantwortlich, die Menschen mit den dafür benötigten Mitteln auszustatten.

Benutzen Sie Crypthograpy um Utensilien und Assets auf einem dezentralisiertem Netzwerk zu erstellen, zu handeln und zu lagern.

PROBLEM

Konventionelle Finanzen

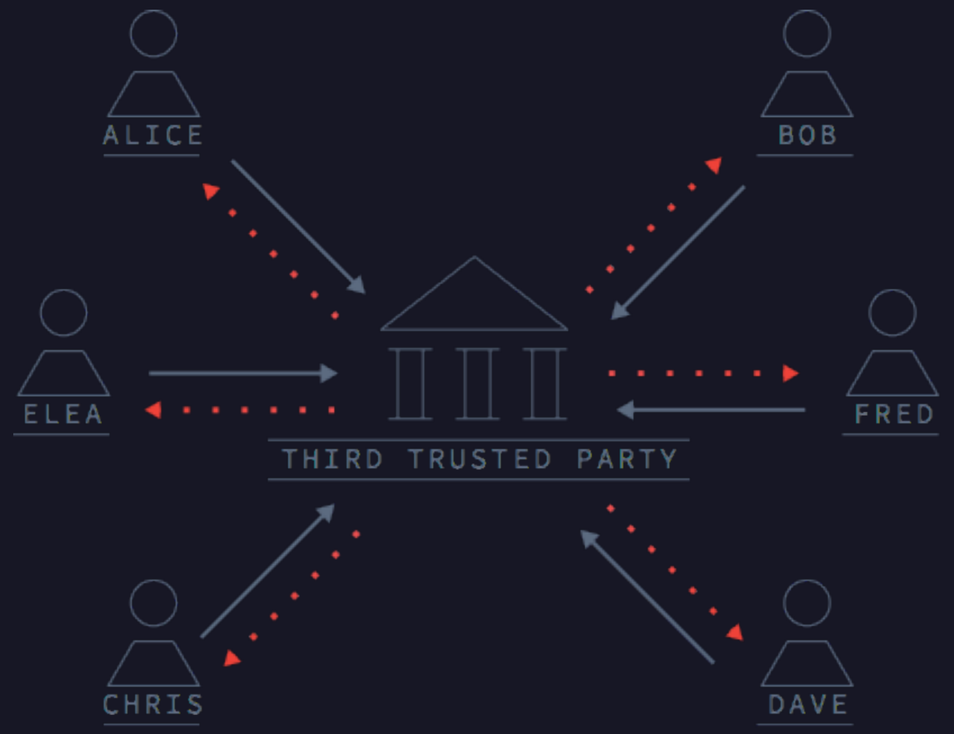
Anstatt uns den Risiken der anderen Partei auszusetzen, benutzen wir vertrauenswürdige Finanzinstitutionen um dieses zu umgehen. Diese Institutionen vereinfachen die Mehrzahl unser Transaktionen. Diese Institutionen begrenzen unsere Freiheit :

- Limitierter Zugang

  Finanzinstitutionen beschränken, *wer* das Finanzsystem nutzen kann und für *was* er es nutzen kann.

- **Limitierte Kontrolle**

Bis zu einem Gewissen Grad besitzen wir unsere Assets nicht, sondern erhalten eine Obligation der Bank. Die Bank kann z.B. durch Insolvenz oder Konfiszierung daran scheitern, die Vreeinbarung einzuhalten.



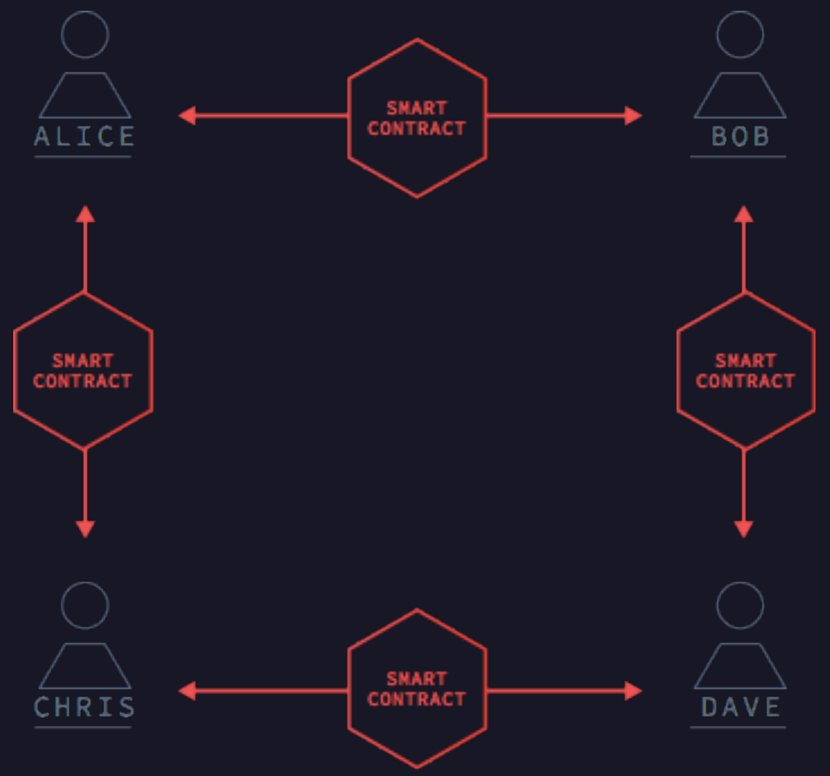
LÖSUNG

Ein Dezentralisiertes Finanzsystem

Wenn wir unsere Abhängigkeit von Dritten beseitigen könnte, könnten wir wieder den Besitz unserer Assets proklamieren. Dies würde effizientere Märkte mit weniger Limits und Gebühren ermöglichen.

Indem wir die BTC Technologie benutzen, können wir ein dezentralisiertes Finanzsystem entwickeln.

Eine neue Blockchain, welche in Finanzen spezialisiert ist, erlaubt es uns die Assets zu kryptographieren und unterstützt den Cash Flow in Form von Smart Contracts.



LÖSUNG

Eine neue, maßgeschneiderte Blockchain

Der Raum ist voll mit zentralisierten Finanz Blockchains und dezentralisierten Blockchains, welche jedoch nicht auf den Finanzsektor abzielen. Wir sehen das Potenzial der Blockchain Technolgie in Verbindung mit dezentralisierten Finanzen. Zen versucht diese Nische zu füllen

Brauchen wir wirklich noch eine Blockchain?

	DECENTRALIZED	CENTRALIZED
FINANCIAL	**Bitcoin, Zen**	Bank chains, R3CEV, digital assets, holdings, etc…
NON FINANCIAL	Ethereum, Appcoins	Supply chain, blockchains IBM, Skuchain

BITCOIN

Bitcoin ist dezentraliiertes Geld

Wir glauben, dass **Bitcoin die ultimative Währung ist.** Satoshi entschied sich, Bitcoins Features zu begrenzen, um sich auf dessen Role als Zahlungsmittel zu konzentrieren. Satoshi beteuerte, dass es nicht skalieren würde, jeden Proof of Work im System zu speichern.

Bitcoin misst die Funktionalität, die die Finanzwelt benötigt.

Wir brauchen eine neue Blockchain für dezentrale Finanzen, eine Blockchain, welche mehrere Assets und komplexe Besitzesverhältnisse unterstützt.

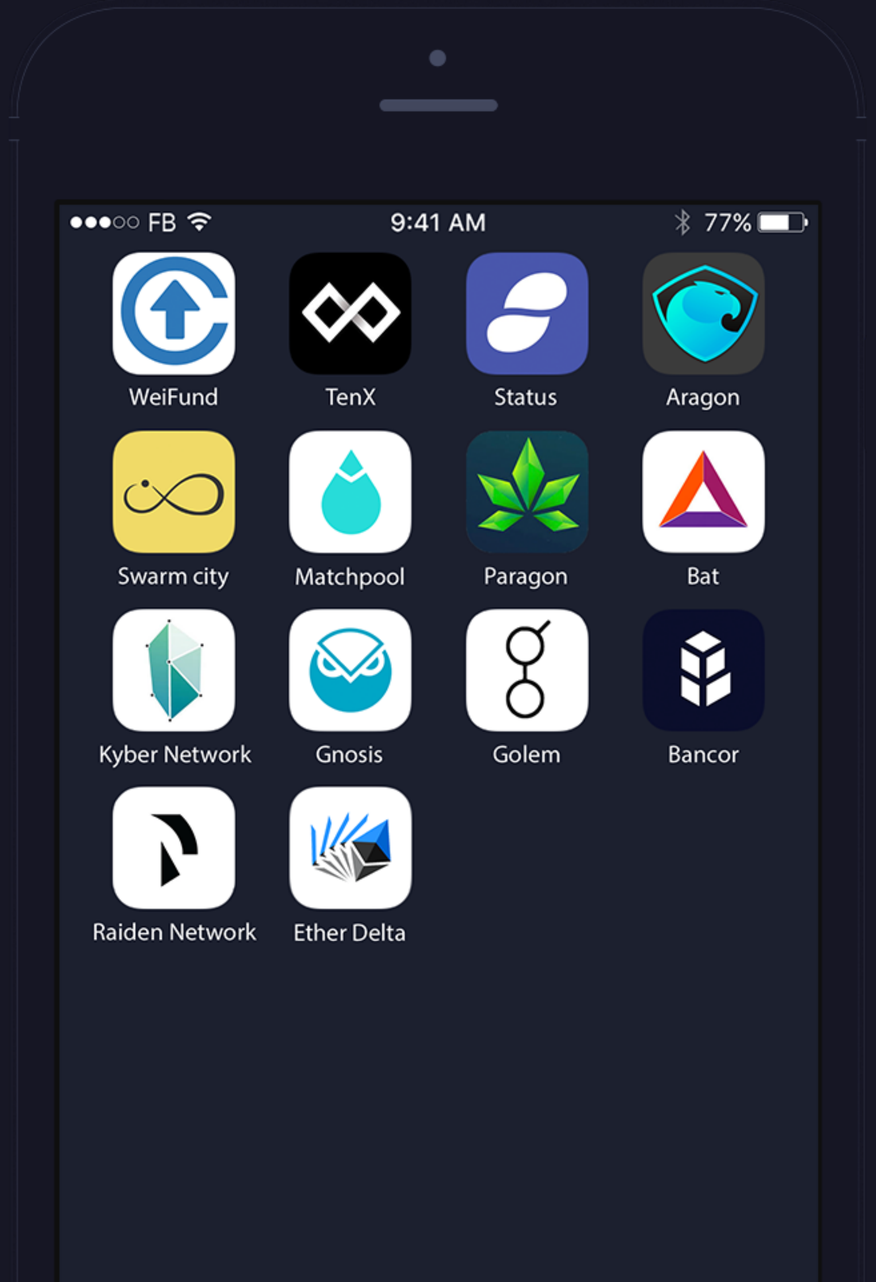
THERE ARE AN ESTIMATED 21M BRICKS (400 OZ PER BRICK) OF GOLD IN THE WORLD

ETHEREUM

Ethereum ist dezentralisierte „Berechnung“

Ethereums Ziel ist es, eine Plattform für die Entwicklung von dezentralisierten Applikationen, wie z.B. Facebook oder Uber ohne zentralen Server, zu sein. Ethereum ist primär eine Entwicklerplattform und bietet Programmiersprachen (Solidity) and Application Binary Interfaces (ABI).

Um diese Funktionalität zu erlauben, stellt Ethereum die Ethereum Virtual Machine (EVM) zur Verfügung, wo Berechnungszyklen gezählt und das „gas“ System verwendet wird.



ZEN

Zen ist „dezentralisierte Finanzen“

Zen ist eine neue Plattform, welche auf dezentralisierte Finanzinstrumente fokussiert ist. Zen erlaubt Peer-to-Peer Zugang zu neuen und konventionellen Assets.

Genauso wie Bitcoin die Notwendigkeit von Banken für den Geldtransfer eliminierte, wird Zen unsere Abhängigkeit von Banken aus dem Finanzökosystem loswerden.

TOKEN

Assets werden kryptographisch in einem wallet gehalten.

ACS

Zens “Ausführungs Umgebung”, vergleichbar mit Bitcoins Stack oder Ethereums EVM.

BITCOIN INTEGRATION

Zen läuft parallel und komplementär zu Bitcoin.

CONTRACTS

Ersetzen Mittelmänner mit dezentralisierten Escrow Mechanismen.

ORACLES

Können von Ereignissen in der echten Welt abhängen, wie z.B. der Börse.

MULTI HASH MINING

Token Besitzer stimmen darüber ab, welche Algorithmen den Mining Preis erhalten, um einen Interessensausgleich zwischen Minern und Token Besitzern zu garantieren.

ARCHITECTURE

Token

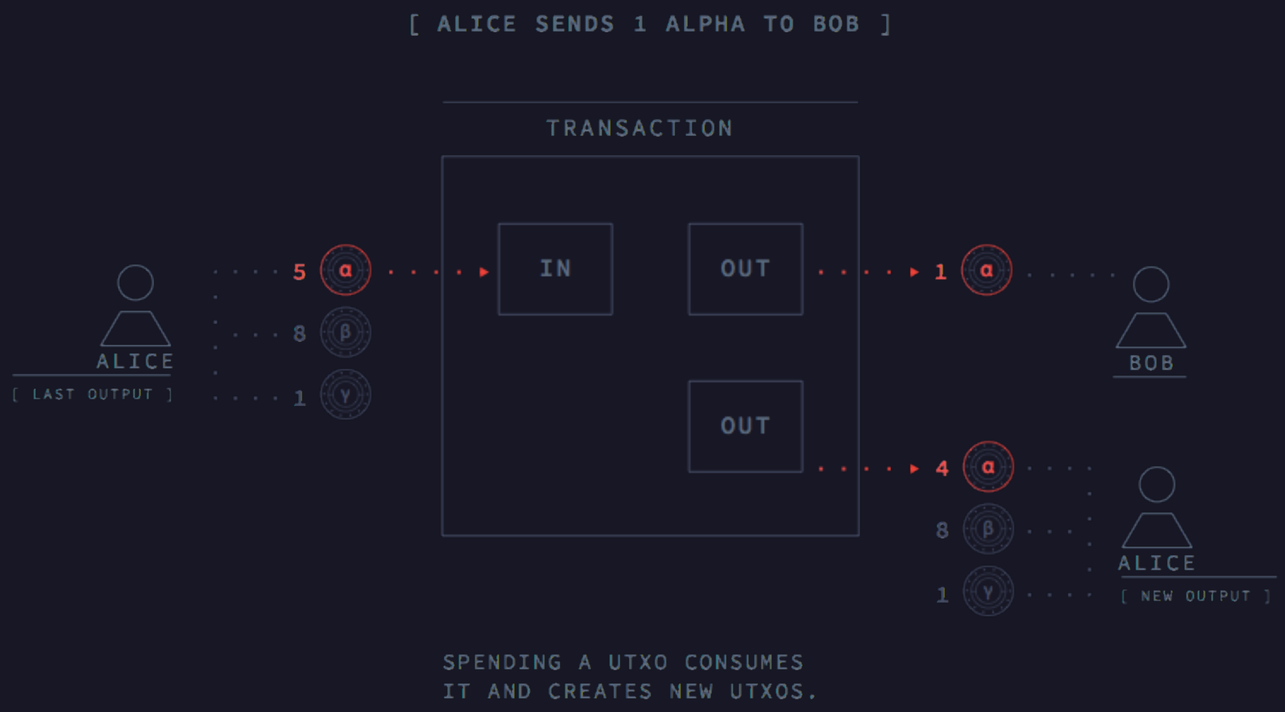
Im Gegensatz zu Bitcoin, welches nur BTC unterstützt oder Ethereum, welches ERC20 unterstützt, hat Zen Multi Token schon in seinem Protokoll eingebaut.

Das heißt, das jeder Token in Zen einen ähnlichen Status zum nativen Zen Token besitzt. Deswegen kann der native Zen Token jeden anderen Token managen und andere Token können zur Bezahlung von Miner Gebühren benutzt werden.

Dies ist von regem Interesse, da finanzielle Verträge in „normale“ Währungen wie USD oder EUR denominiert werden können. Tokens werden in Transaction Outputs gespeichert, so wie Bitcoin, und könne mit den richtigen Rechten wieder aktiviert werden.

Token haben generell einen Wert, weil:

- Leute glauben, dass sie einen Wert besitzen
- Sie werden von Contracts unterstützt, welche Sicherheit besitzen



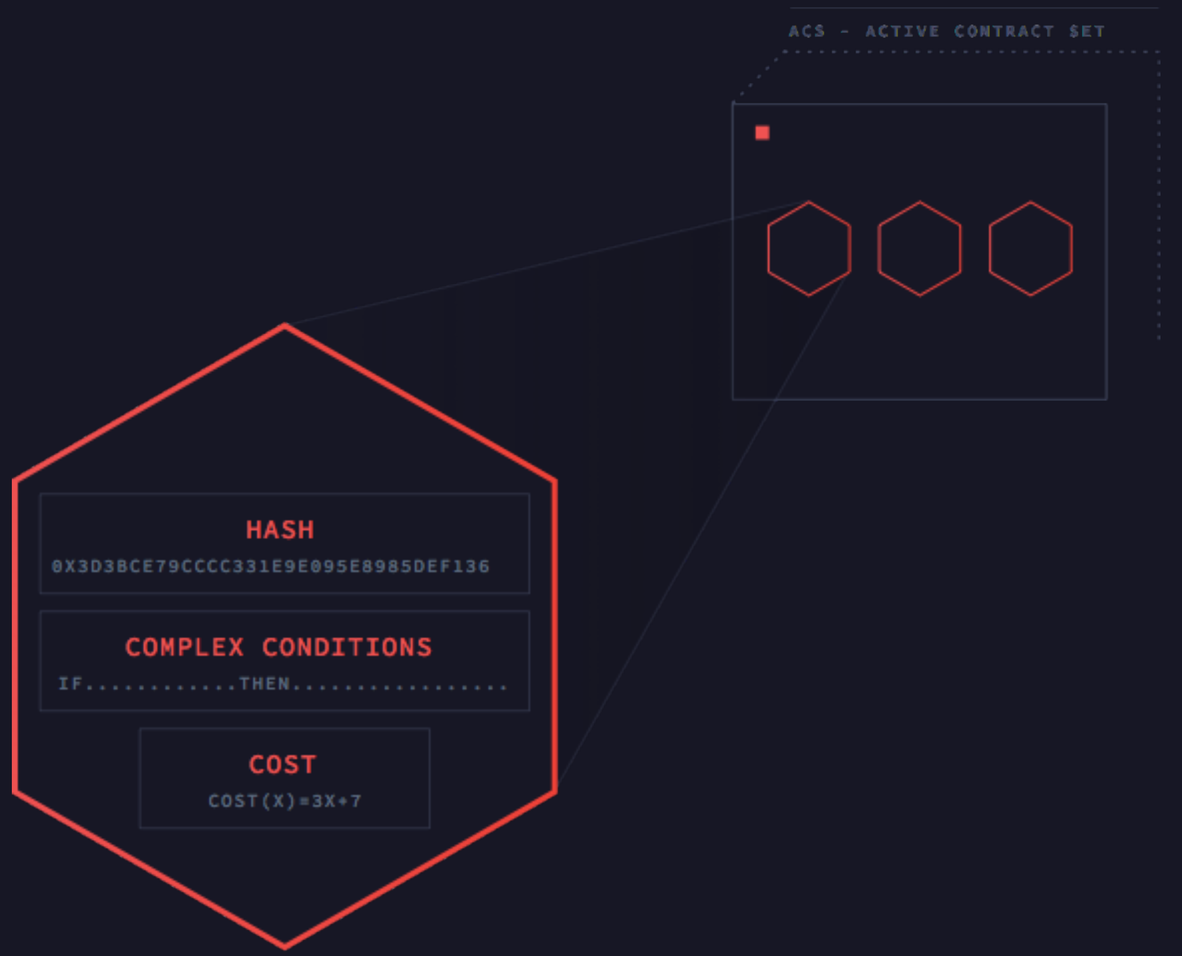
ARCHITECTURE

Contracts

Contracts sind in F* geschrieben – eine funktionelle, formell verifizierte Sprache. Formelle Verifikation, gepaart mit einem Kostenmodell, ermöglichen es Zen Protocol zu wissen, wie lange jeder Contract zur Ausführung braucht, bevor sie die Blockchain betreten.

Contracts sind Unveränderbar – (Ihr Code verändert sich nie). Deswegen, hat jeder Contract einen einzigartigen mathematischen Erkennungscode (seinen Hash). Indem man diesen Hash benutzt, kann man einem Token sehr einfach einen PoC zuschreiben.

Jeder Contract ist vom Rest der Blockchain isoliert–
Ein Conract kann die Blockchain nur verändern oder mit anderen Contracts kommunizieren, wenn eine Transaktiok kreiert wird. Contracts machen nichts unabhängig. Sie fungieren eher als Validierungsdaten, welche Nodes helfen soll, zu entscheiden, ob eine Transaktion akzeptiert wird.



[EACH CONTRACT IS IDENTIFIED BY ITS HASH]
[CONTRACTS ARE WRITTEN IN OUR DIALECT OF ZF*]
[CONTRACTS ARE ISOLATED FROM EACH OTHER]

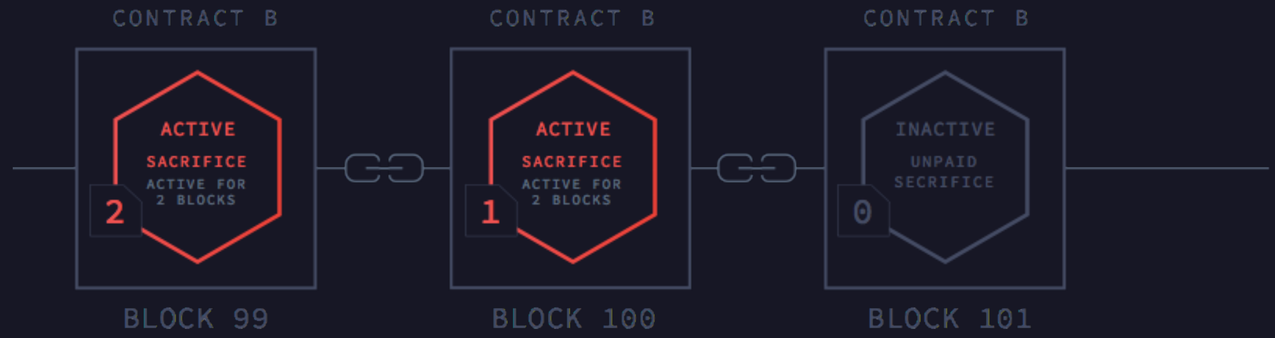
ARCHITECTURE

Active Contract Set

- Wenn aktiviert, werden Contracts von F* in Machine Code umgewandelt.
- Die kompilierten Contracts werden im RAM der Node gespeichert.
- Contracts müssen aktiv sein, um Transaktionen zu erstellen.
- Jeder kann einen contract aktiveiren oder verlängern, wenn er einen sog. Contract Sacrifice benutzt.

Der Contract Sacrifice

- Der Contract Sacrifice kompensiert die Miner, welche den Contract aktiv halten müssen. Der Sacrifice wir zwischen den Minern verteilt, welche Blöcke während der aktiven Periode finden.
- Obwohl Transaktionsgebühren mit jedem Token beglichen werden können, muss der Contract Sacrifice in Zen bezahlt werden.



ANWENDUNGSBEISPIEL - AAPL CFD

An diesem Beispiel kann man sehen, wie Token, und die Active Contracts zusammenarbeiten, um Peer-to-Peer Finanzverträge zu erstellen.

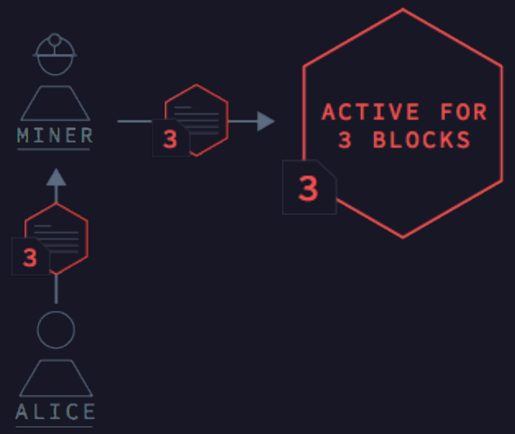
1

- **Alice verfasst einen Contract for Difference (CFD) auf AAPL for 30 days.**
- **Alice macht Geld, wenn AAPL sinkt.**
- **Ihre Gegenpartei macht Geld, wenn AAPL steigt.**

USE CASE - AAPL CFD

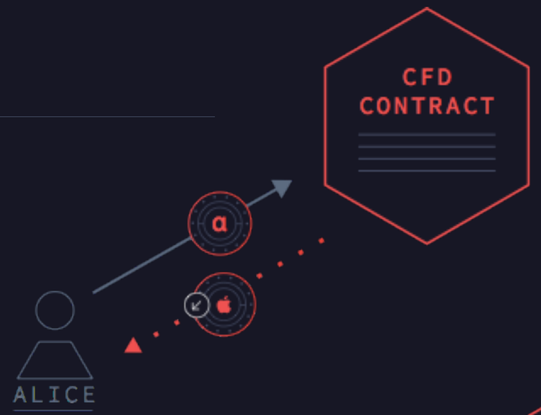
2

- Alice aktiviert den Contract für 3 Blöcke.



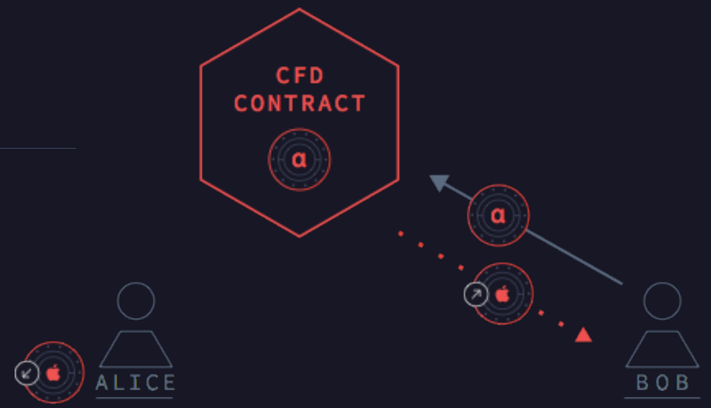
3

- Alice besichert den Active Contract und geht damit einen Short ein.



4

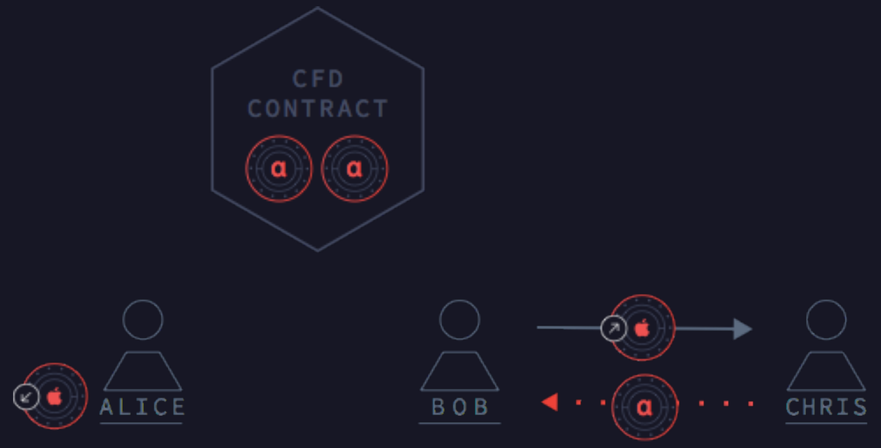
- Bob sieht den besicherten Contract und erfüllt seinen Teil der Vereinbarung, indem er die Token sendet.



USE CASE - AAPL CFD

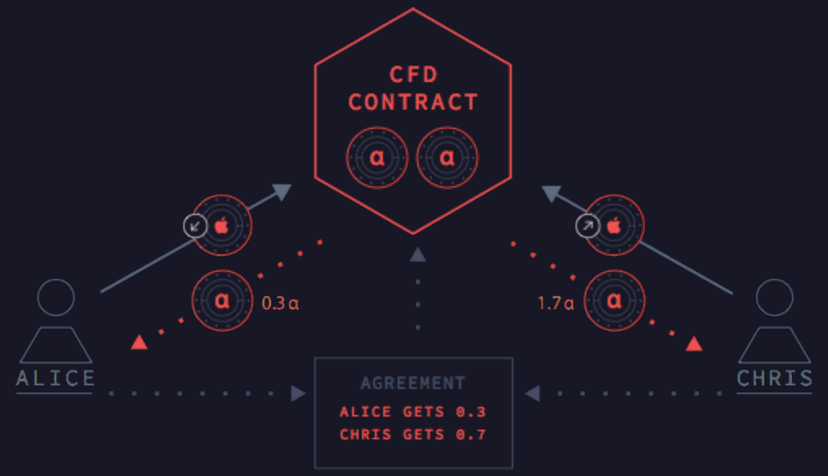
5

- Der Contract wird inaktiv
- Bob kann seine Position immer noch loswerden, indem er seine Token an jemand anderen Verkauft.



6

- Nach 30 Tagen, muss der Account reaktiviert werden, um die Escrow Gelder freizuschalten.
- Wenn Alice und Chris sich einig werden, dass AAPL um 70% gestiegen ist, unterzeichnen sie eine Transaktion, in der Alice 0.3 α und Chris 1.7α erhalten.



ABER WAS, WENN ALICE NICHT KOOPERIERT?

INTRODUCING ORACLES

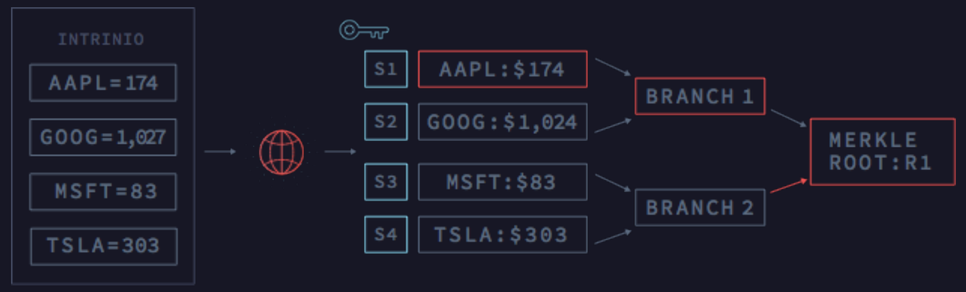
Oralce erlaubt es Contracts, auf Basis von Echtweltinformationen zu agieren

Contracts geben im Vorraus bekannt, von welchen Oracles sie Daten benötigen.

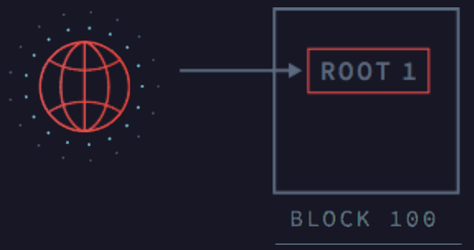
Legale Verträge verwenden Richter und werden bei Gericht geschlichtet. Smart Contracts verwenden Oracles und werden in der Blockchain geschlichtet.

Wie Oracles funktionieren:

1 **Oracles ziehen Daten aus den APIs und sortieren diese in ein einen Merkle Tree; Jedes Blatt ist mit einem secret/ nonce ausgestattet.**

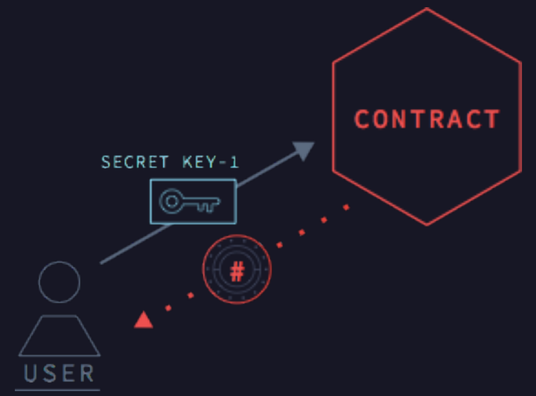


1 **Das Oracle fügt die Merkle Tree Wurzel in die Blockchain ein.**



2 **Wenn ein Benutzer einen Contract mit einer bestimmten Information, z.B. zur Konfliktlösung, versorgen muss, so bezahlt der Benutzer das Oracle, welches ihm in Gegenzug die gewünschte Information liefert.**

3 **Mithilfe der Nonce, kann der Nutzer dem Vertrag den Preis beweisen und somit die Mittel beziehen.**

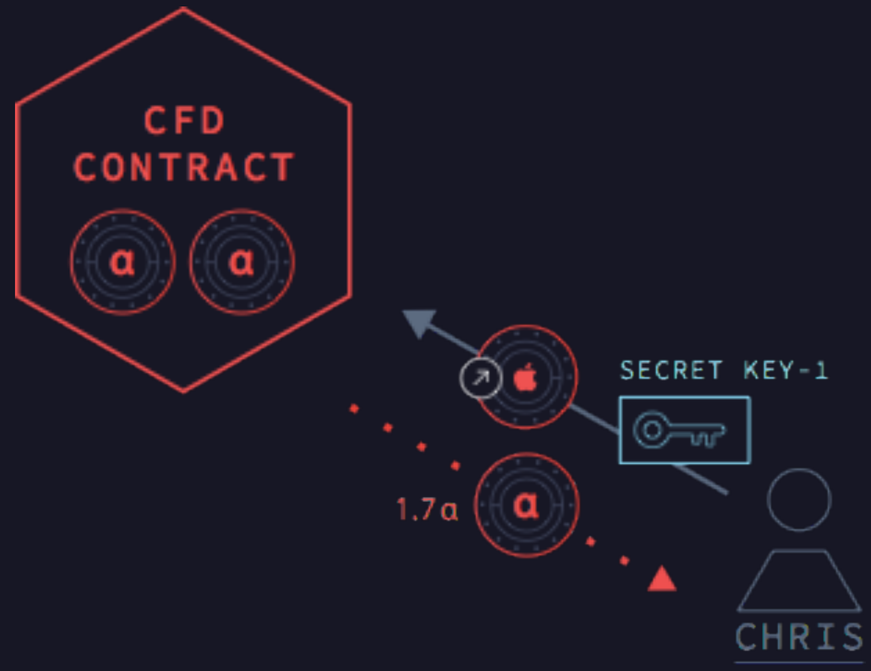


USE CASE - AAPL CFD CONTINUED

Streitschlichtung

Für den Fall, dass Alice und Chris sich nicht einig werden, kann Chris das Oracle für die Information bezahlen(S1).

- Dann sendet Chris die Infos an den Vertrag, welcher ihm 1.7alpha asuzahlt.



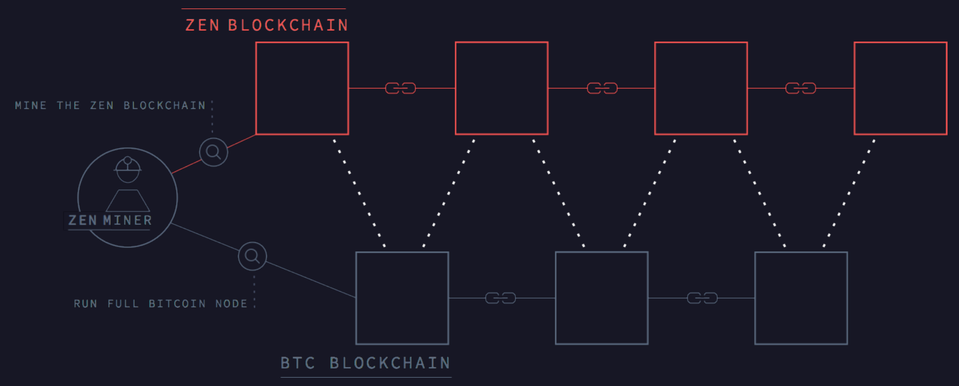
BITCOIN INTEGRATION

Vorherige Bemühungen, die Komplexität der Blockchain zu erhöhen, hatten folgende Strategien:

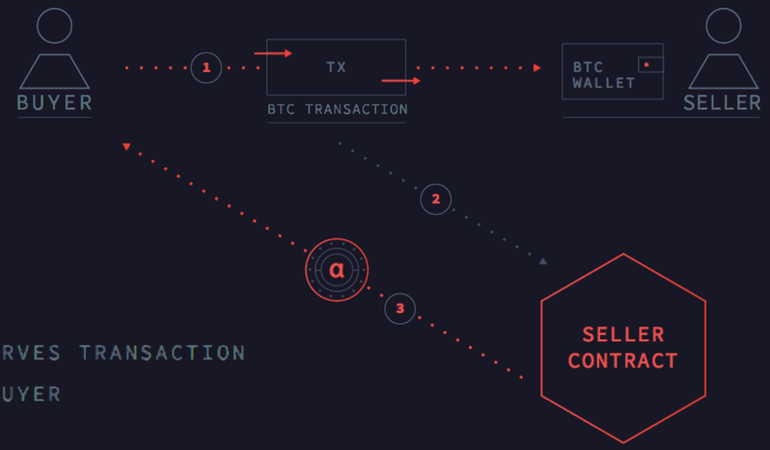
1. Eine alternative Blockchain kreieren, welche die Nutzung eines AltCoins erforderlich macht.
2. Ein supplementäres Protokoll entwickeln, z.B. eine Side-Chain, welche jedoch keinen proprietären Token hat und folglich unterschiedliche Sicherheits- und Belohnungsmechanismen wie Bitcoin hat.

Zenverfolgt einen neuen Ansatz, eine separate Blcokchain mit ihrem eigenen Token, welche parallel zum Bitcoin Netzwerk läuft.

Merged Consensus – Zen Miner minen die Zen Blcokchain und beobachten die Bitcoin Blockchain, was cross-chain Funktionalität ermöglicht.



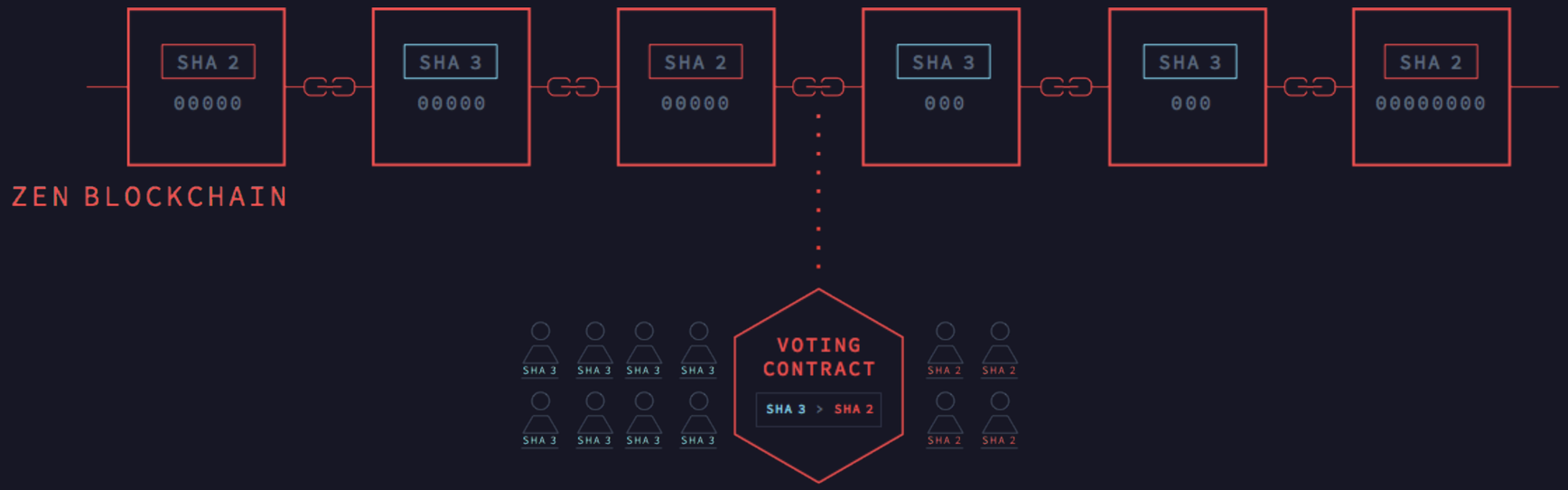
Cross-Chain Contract – Versicsherungen, die in der Zen Chain gespeichertsind, deren Premium aber an eine BTC Adresse bezahlt wird..



ZEN

Multi-Hash Mining – Token Besitzer Representation

- Verschiedene Hash Funktionen können zum Minen eines Blocks genutzt werden.
- Jede Hash Funktion hat einen verschiedenen Schwierigkeitsgrad
- Target Ratio jedes Blockes und jeder Hash Funktion, wird durch die Token Besitzer bestimmt.



ROADMAP


Idee ist formalisiert
Q3 2016
Q4 2016
Die zu verwendenden Technologien werden gewählt
Kostenmodell ist vervollständigt
Q1 2017
Q2 2017
Smart Contracts und Oracle in C#
Refaktorisierung von Entwicklungsverträgen
Q3 2017
Q4 2017
Alpha
Release Kandidat
Q1 2018
Q2 2018
Genesis Block
Aufbau des Ökosystems
Q3 2018

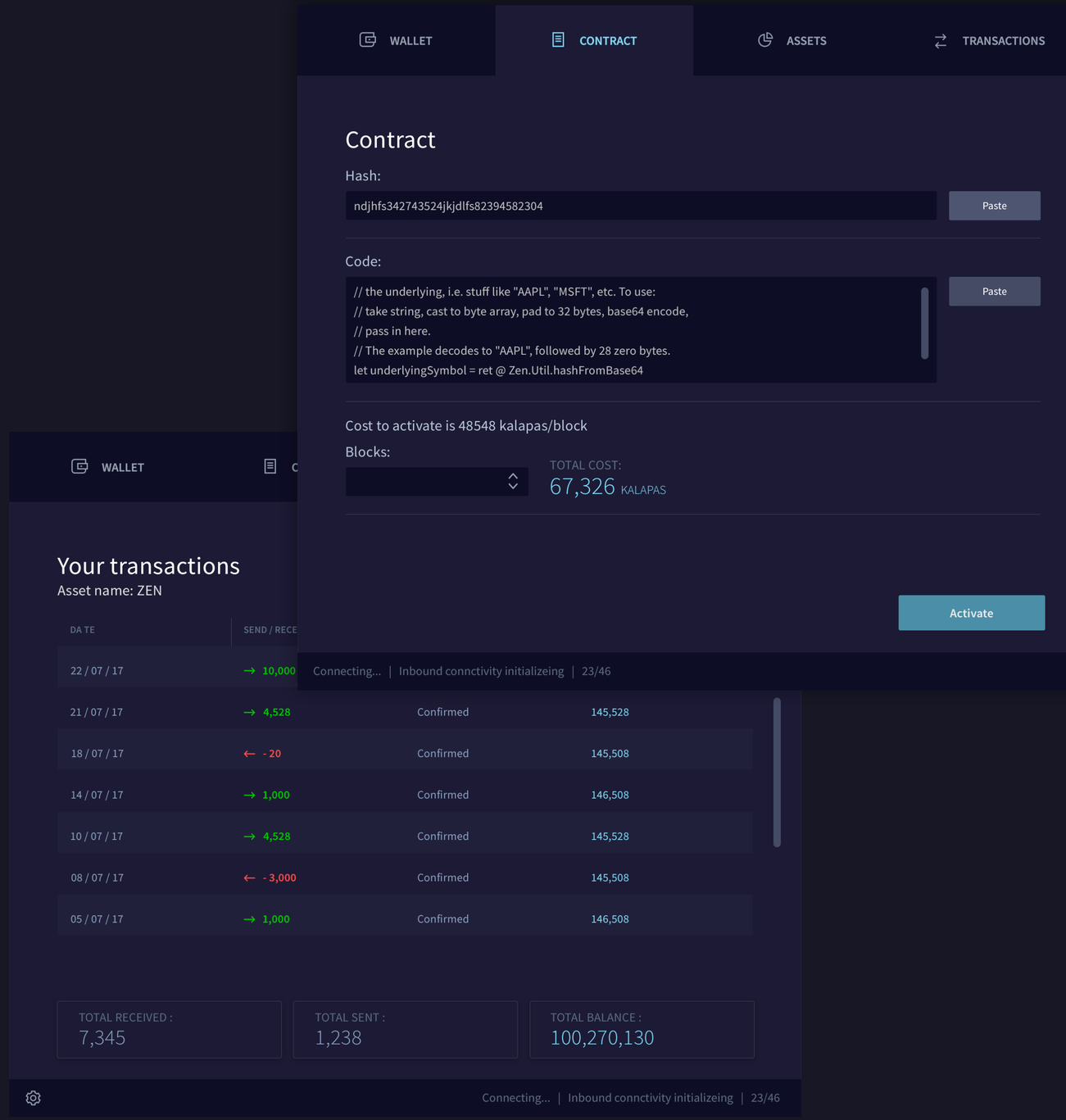
ZEN

Alpha

Momentan besitzen wir eine von Grund auf entwickelte Alpha, welche ACS implementiert, die F* Smart Contracts beinhaltet und die Aktienpreise von intrinio.com abruft.

Zen Alpha

DOWNLOAD



ZEN TEAM

We're a small team building a very big product.

Adam Perlow

CEO

Adam is ein Absolvent der Ökonomie an der IDC, ein Israelischer Armeereservist, und ein Bitcoin Pionier. Er wusste schon über Bitcoins große Zukunft bescheid, als er zum ersten Mal im Jahre 2011 davon hörte.

Nathan Cook

CTO

Nathan ist ein Cambridge Mathematik Absolvent. Wenn er heutzutage seinen Job beschrieben müsste, dann würde er Kapital helfen, seine Existenz zu finden. Er liest viel.”

Sharon Urban

Führender Entwickler

Sharon ist eine höchst erfahrener und begabter System-Ingineur, welcher gerne mit den guten Typen arbeitet

Asher Manning

Entwickler, Formale Methoden

Ash hat Mathematik, Physik und Informatik an der McGill University studiert, wo er Forschung an der "Homotopy Type" Theorie betrieb. Zuvor arbeitete er bei Skybox Security und HSBC.
Ash ist einer der Entwickler von F* Sprachеund benutzt dieses zusammen mit neuster Forschung um Zen zu programmieren und ihm fortschrittliche Sicherheitsfunktion und Ressourcengrenzen.

ZEN TEAM

We're a small team building a very big product.

Doron Somech

Vizepräsident Forschung und Entwicklung

Doron, war Mitgründer und CTO von leverate.com

Elan Perach

Head of Product

Elan hat schon mehrere Startups aus dem Boden gezogen, und agiert schon seit 2011 in der Krypto Szene. Er startete die erste Webseite zum Verkauf von Bitcoins in Israel.

Eleanor Milstein

Art Director

Eli ist unsere Produktdesign-Guru und bringt 6 Jahre Erfahrung aus verschiedenen Startups mit, in welchen sie als Designerin oder Mitgründerin tätig war.

Isaac Rodgin

Community Manager

Dank seines Ökonomie und Informatik Abschlusses an der IDC, bringt Isaac einen starken Background in die Mannschaft. Die letzten 5 Jahre, hat er in verschiedenen Startups in einer VIelzahl von Tätigkeitsfeldern gearbeitet.

ADVISORY

Pamir Gelenbe

Pamir ist Managing Partner bei Libertus Capital, wo er sich auf dezentralisierte Systeme, Enterprise Blockchain und Digitale Währungen spezialisiert hat. Er ist ein Investor bei Kraken, Ledger Wallet, Shapeshift, Crypto Facilities und in zahlreiche dezentralisierte Protokolle. Zuvor arbeitete er als Partner bei Humingbirds Ventures, Morgan Stanley und D.E. Shaw. Er graduierte von der Duke und Columbia University mit einem Bachelor in Elektrotechnik und einem Master in Unternehmensforschung..

Ran Nussbaum

Ran Nussbaum ist Managing Partner und Mitgründer von The Pontifax Group. Der Fund besitzt ins seinem Portfolio mehr als 50 globale Unternehmen. Bevor er Ponitfax beitrat, war er ein Partner bei Israels größter Business Intelligence und Strategie Beratungsfirma.

Ron Gross

Ron hat Technion mit einem Master in Informatik absolviert. Er hat bei vielen Firmen gearbeitet, sowohl bei kleinen Startups als auch bei Google. Ron besitzt weitreichende Erfahrung in den Bereichen Web Architektur, Sicherheit und Algorithmen.

Ron ist seit 2011 stetig in Bitcoin involviert gewesen und hat dabei die Werbetrommel für seine Liebe zu Bitcoin geschlagen. Er ist ein Befürworter von open source, Transparenz und der Dezentralisierung von Macht und Technologie. Er is Mitbegründer der Israelische Bitcoin Stiftung und Bitcoin Gesellschaft und war und war Exekutivdirektor der Mastercoin Stiftung (erster Token Verkauf der Welt).