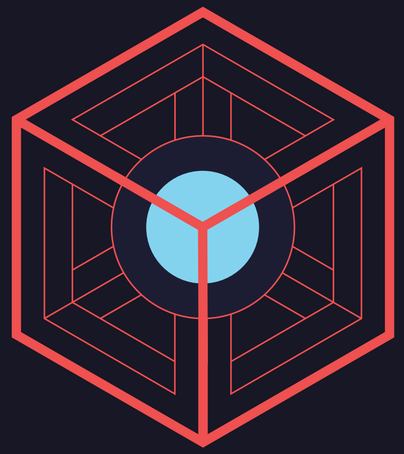


# ZEN

[ GEDECENTRALISEERD FINANCIEEL SYSTEEM ]

# ABSTRACT

Een peer-to-peer mechanisme voor het beheer van afspraken en relaties geeft partijen het vertrouwen om te kunnen handelen zonder dat er sprake is van een juridisch systeem of een geschillencommissie. Deze techniek noemen we tegenwoordig 'smart-contracts'. Door het peer-to-peer karakter is niemand te baas en blijft het in beheer van het gedecentraliseerde netwerk. Het probleem met de huidige platformen is dat deze niet eenvoudig schalen en dat de beveiliging nog onvoldoende is voor betrouwbare handel.

Zen is een nieuw platform welke smart-contracts implementeert dat op basis van het UTXO principe (wat ook door Bitcoin gebruikt wordt) werkt. Het Zen protocol combineert dit met de ZF* programmeer taal welke de mogelijkheid biedt voor 'format verification'. Deze combinatie van technieken zorgt ervoor dat de contracten snel en eenvoudig op te zetten zijn en bovendien erg schaalbaar. Zen heeft daarnaast de eigenschap om de Bitcoin blockchain bij te houden om Zen en Bitcoin assets eenvoudig uit te wisselen.

# MOTIVATIE

Het core-team is in 2014 begonnen met het onderzoek naar de blockchain technologie. In juni 2016, na jaren onderzoek, is begonnen met de ontwikkeling van het Zen Protocol.

**Het idee is ontstaan om mensen echt het gevoel te geven dat zij de controle hebben over hun eigen assets. Sindsdien voelt het team van Zen zich verantwoordelijk voor het creeren op opzetten van deze tools.**

Gebruikt cryptography voor het maken, handelen en opslaan van reguliere assets, contracten en andere middelen op een gedecentraliseerd netwerk.

# HUIDIG PROBLEEM

## Conventionele handel

Om zo min mogelijk risico te lopen maken de meeste mensen gebruik van tussenpersonen bij het drijven van handel. Deze tussenpersonen zijn daarom verantwoordelijk voor bijna alle handel die er plaatsvindt.

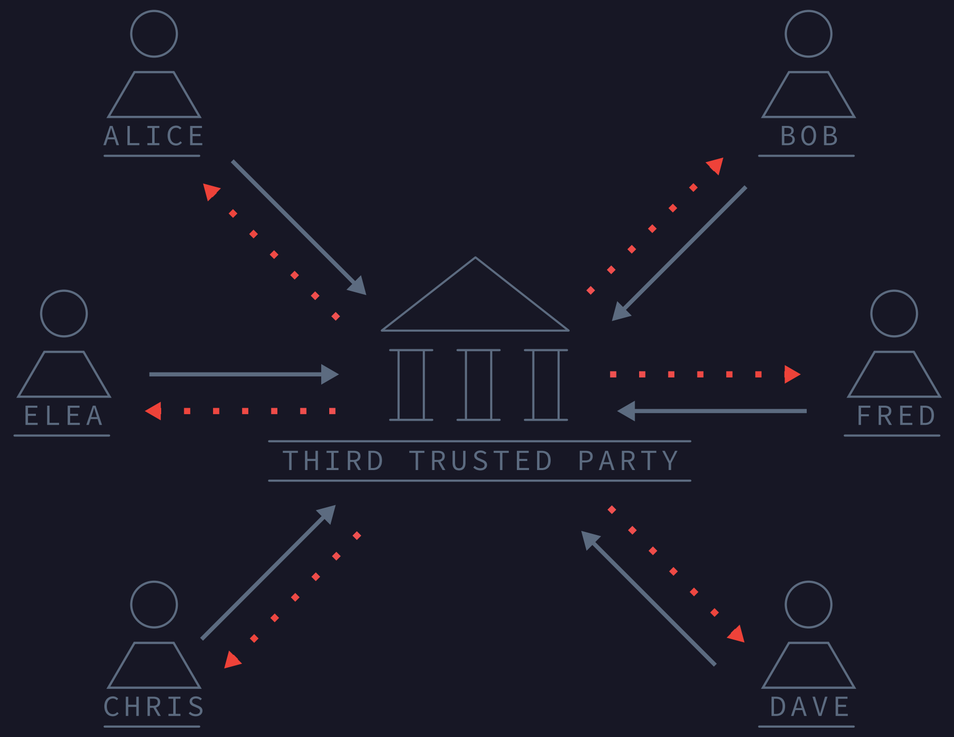
**Ze hebben echter allemaal een beperking:**

- **Geen volledige controle**

  De partijen bepalen de toegang tot de assets. En bepalen in welke mate dit wordt verhandeld.

- **Beperkt eigenaar**

  Tot op zekere hoogte heb je niet de volledige controle over jou assets. De bank speelt er een belangrijke rol in en kan de asset niet vrijgeven of zelfs wegnemen van de persoon.



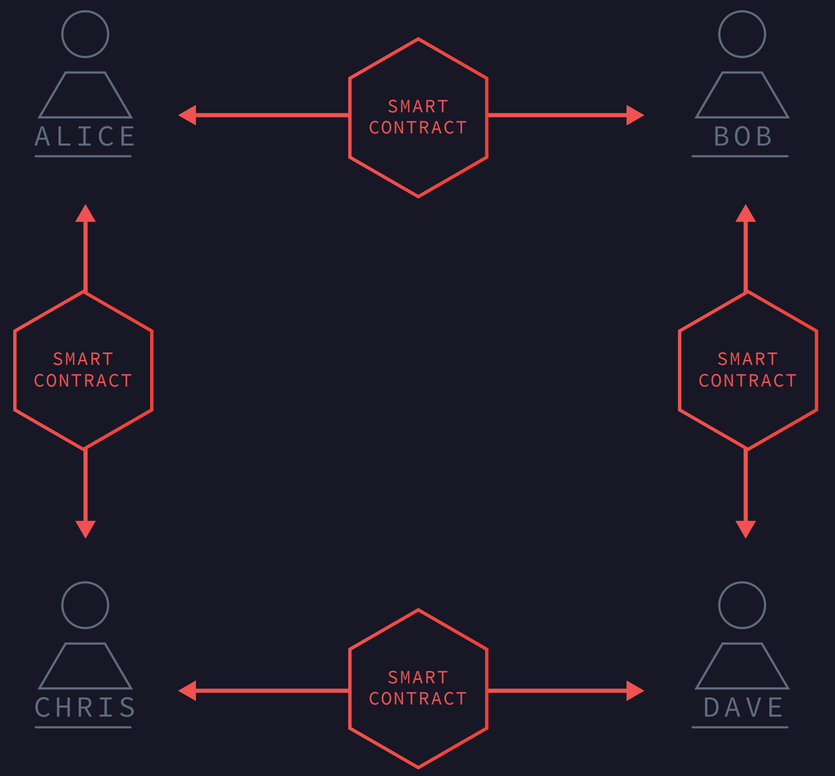
# DE OPLOSSING

## Een gedecentraliseerd handelsplatform

Als we ons onafhankelijk maken van deze banken en third-parties kunnen de volledige controle krijgen over onze assets en geld. Wij geloven dat dit een veel efficiëntere manier van handelen is en geeft de vrijheid terug aan de personen zelf.

**Met gebruik van de Bitcoin technologie is het mogelijk om een gedecentraliseerd handelsplatform te creëren.**

Een nieuwe blockchain technologie gespecialiseerd in het handelen van assets wat geregeld wordt door nieuwe ontwikkelingen in smart-contracts.



# DE OPLOSSING

## Een nieuwe custom-build blockchain

De markt is nu gevuld met gecentraliseerde blockchains welke gericht zijn op financiën. Gedecentraliseerde oplossingen zijn vooral gefocust op niet financiële blockchains. Zen heeft als hoger doel om deze niche markt te vullen.

**Hebben we daar echt een Blockchain voor nodig?**

| | GEDECENTRALISEERD | GECENTRALISEERD |
|---|---|---|
| FINANCIAL | **Bitcoin, Zen** | Bank chains, R3CEV, digitale assets, holdings, etc.. |
| NON FINANCIAL | Ethereum, Appcoins | Supply chain, blockchains IBM, Skuchain |

# BITCOIN

## Bitcoin is een vorm van gedecentraliseerd geld.

Wij geloven dat de **Bitcoin een ultieme vorm van geld is.** Sathosi heeft ervoor gekozen om de functies van de Bitcoin te beperken en zich te concentreren op een valuta. Sathosi verklaarde het volgende: "Een Proof-of-Work systeem met een dataset, is heel moeilijk te schalen".

Bitcoin mist juist deze functionaliteit voor het beheren van financiën.

We hebben een nieuwe blockchain nodig voor een gedecentraliseerd systeem. Een blockchain die ondersteuning biedt voor meerdere assets en complexere shares.

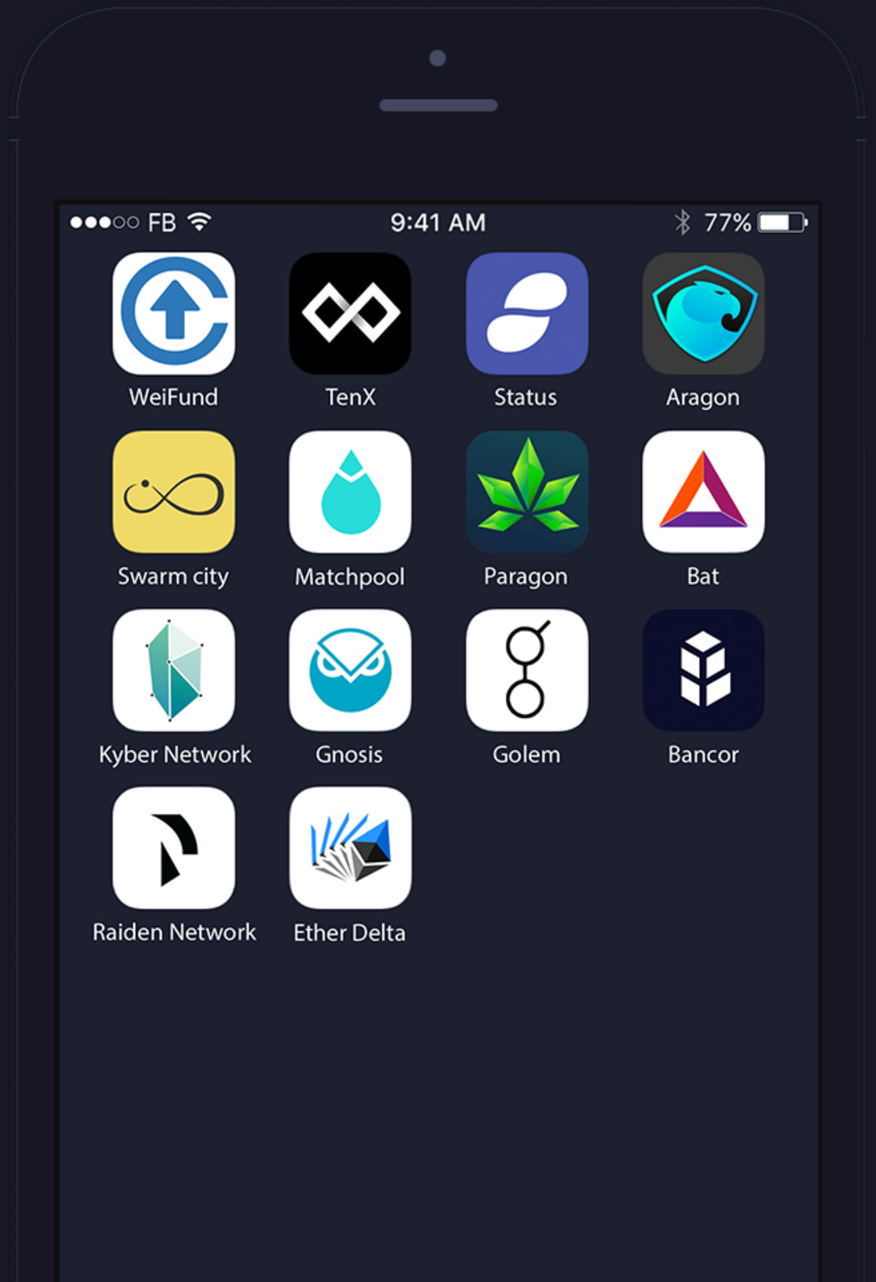

THERE ARE AN ESTIMATED 21M BRICKS (400 OZ PER BRICK) OF GOLD IN THE WORLD

# ETHEREUM

## Ethereum is een vorm van gedecentraliseerde computations

Het doel van Ethereum is om een platform te zijn welke gedecentraliseerde applicaties aanbiedt. Denk hierbij aan Facebook of Uber zonder een centrale server. Ethereum focust zich op de ontwikkelaars en biedt handige programmeertalen zoals Solidity en Application Binary Interfaces (ABI).

**Om deze functionaliteit mogelijk te maken biedt Ethereum de Ethereum Virtual Machine, waarbij de reken cyclus wordt geteld in het gassysteem.**



ZEN

# Zen is een gedecentraliseerd platform voor het beheer van financiën

Zen is een nieuw platform voor gedecentraliseerde assets. Zen biedt de mogelijkheid voor peer-to-peer toegang voor zowel nieuwe als nieuwe meer conventionele assets.

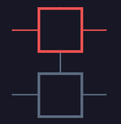
**Net zoals de Bitcoin ervoor gezorgd heb dat we niet meer afhankelijk zijn van de banken, zorgt Zen ervoor dat we ook financiering kunnen krijgen.**

## TOKENS

Assets worden cryptografisch opgeslagen in je eigen wallet

## ACS

Zen's "execution environment", vergelijkbaar met de Bitcoin's stack of de Ethereum's EVM.



## BITCOIN INTEGRATIE

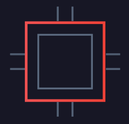
Zen loopt parallel met de Bitcoin en werkt als aanvulling.

## CONTRACTEN

Vervang tussenpersonen door gedecentraliseerde escrow functionaliteiten

## ORACLES

Contracten kunnen afhankelijk zijn van events in de echte wereld. Bijvoorbeeld de schommeling van prijzen op de markt.



## MULTI HASH MINING

De stakeholders kunnen stemmen over de hash-configuratie waarbij de miners een evenwicht houden tussen het belang van de miners en token-houders.

# ARCHITECTUUR

## Tokens

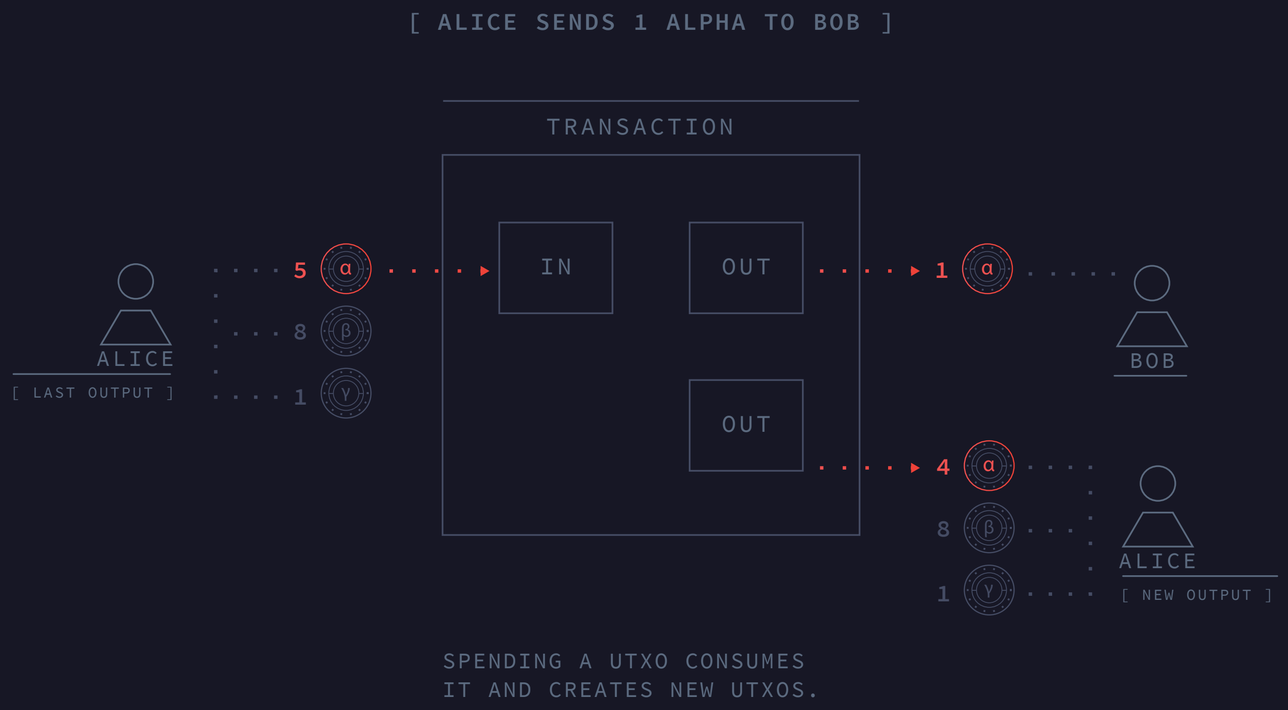
**In tegenstelling tot de Bitcoin die alleen ondersteuning biedt voor BTC of Ethereum met ERC-20 contracten. Zen heeft ook ondersteuning voor meerdere tokens welke zijn ingebouwd op protocolniveau.**

Dat betekent dat elke token in het Zen protocol een vergelijkbare status heeft als de standaard Zen-token. Daarom kan elk contract in Zen een andere token bevatten en beheren.

Dit is van belang omdat hiermee financiële contracten kunnen worden uitgedrukt in "normale" valuta zoals dollar of euro. Tokens worden opgeslagen in transacties net als bij de Bitcoin en kunnen ontgrendeld worden met de juiste rechten.

Tokens krijgen waarde doordat:

- Mensen geloven in de waarde
- Ze worden ondersteund door contracten die onderpand hebben



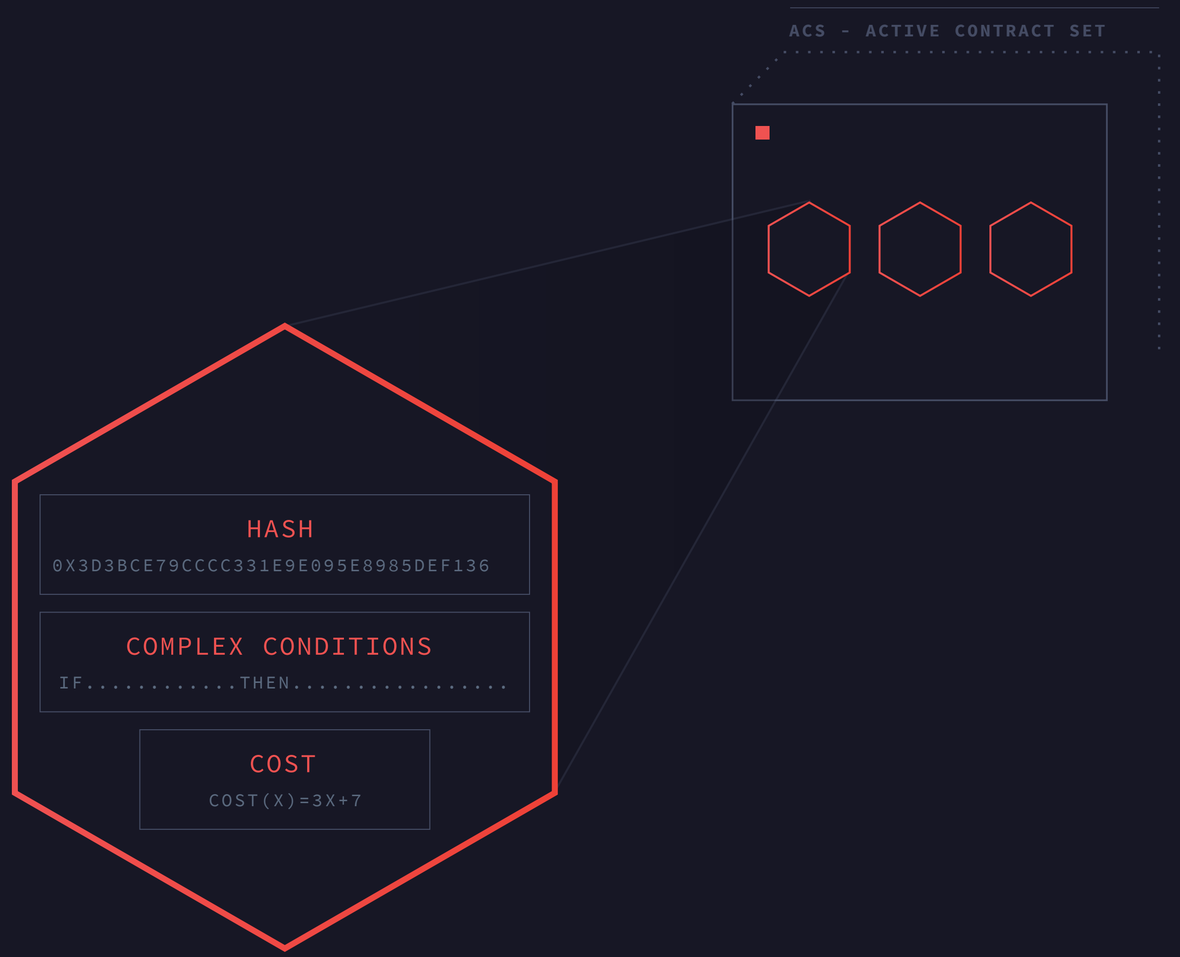
# ARCHITECTUUR

## Contracten

**De contracten zijn geschreven in F*** - een functionele, high-level en formeel geverifieerde taal. Formele verificatie gekoppeld aan een model zorgt ervoor dat de contracten in het Zen-protocol **vooraf bewijzen hoe lang het duurt voordat ze opgenomen worden in de blockchain.**

**Contracten zijn onveranderlijk** - (de code verandert nooit). Daarom kan elk contract een unieke cryptografische functie (hash) bevatten. Met behulp van deze hash is het eenvoudig aan te tonen dat de hash klopt met het betreffende contract.

**Elke contract is geisoleerd van de rest van de blockchain** – de status van een contract kan alleen gewijzigd worden indien er een transactie gemaakt wordt. De contracten doen dus niet zomaar iets. In plaats daarvan fungeren ze als validatie, die gebruikt worden om nodes te helpen voor het bepalen van het accepteren van transacties.




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

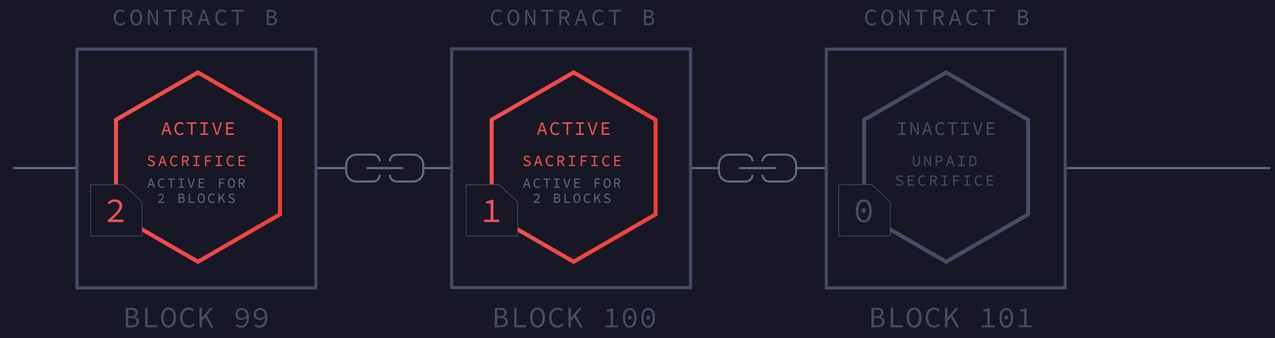
# ARCHITECTUUR

## Active Contract Set

- Bij het activeren worden de contracten geconverteerd van F* naar machine code.
- Vervolgens wordt het contract gecompileerd en opgeslagen in het RAM van de nodes.
- Contracten moeten actief zijn om een transactie te creëren voor bijvoorbeeld het versturen van tokens.
- Iedereen kan het contract activeren of verlengen met een 'contract sacrifice'.


## The ‘Contract Sacrifice’.

- Het 'contract sacrifice' compenseert de miners die het contract onderhouden. De 'sacrifice' is verdeeld over de miners die de blocks succesvol vinden.
- Hoewel de transacties fees betaald kunnen worden in elke token moet de sacrifice betaald worden in Zen.



# USE CASE - AAPL CFD

Laten we nu bekijken hoe tokens, contracten en actieve contracten samenwerking om een peer-to-peer handelsplatform te vormen.

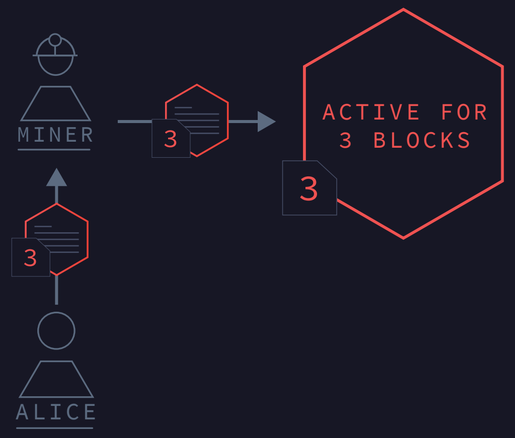
1

- **Alice maakt een CFD contract op de AAPL aandelen voor 30 dagen.**
- **Alice verdient dus als de koers van AAPL omlaag gaat.**
- **De tegenpartij verdient geld als de koers van AAPL omhoog gaat.**


# USE CASE - AAPL CFD

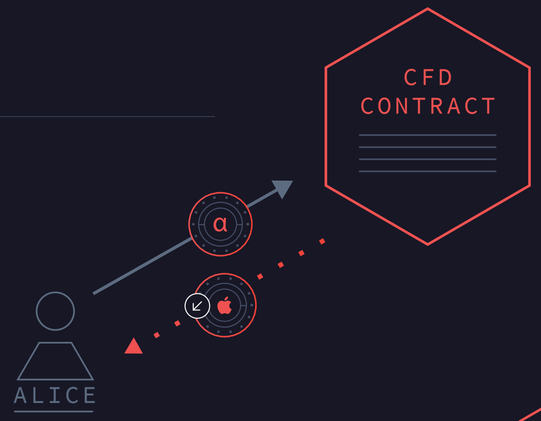
2

- Alice activeert het contract voor 3 blocks.



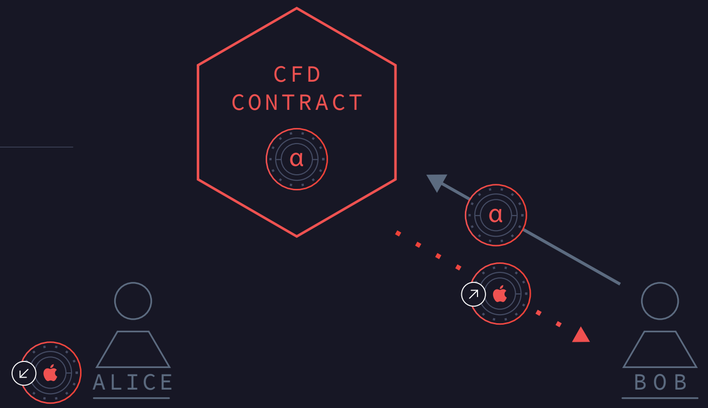

3

- Alice maakt hierbij het contract als onderpand door short te gaan.




4

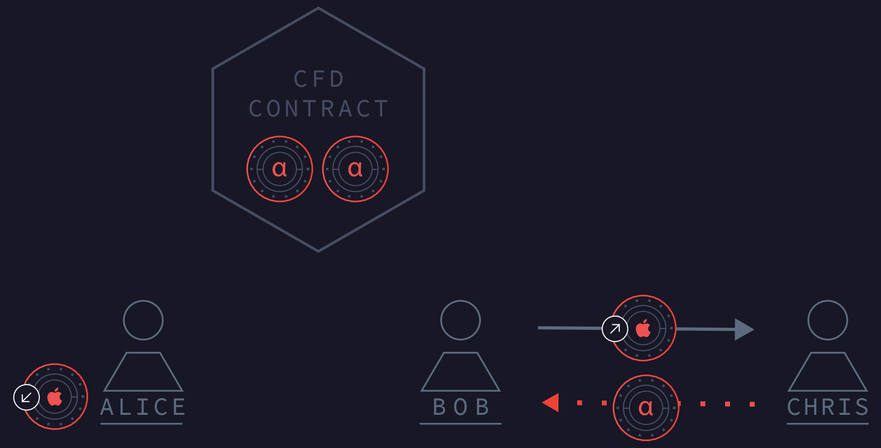
- Bob ziet het contract en eist de tokens van de andere kant.



# USE CASE - AAPL CFD

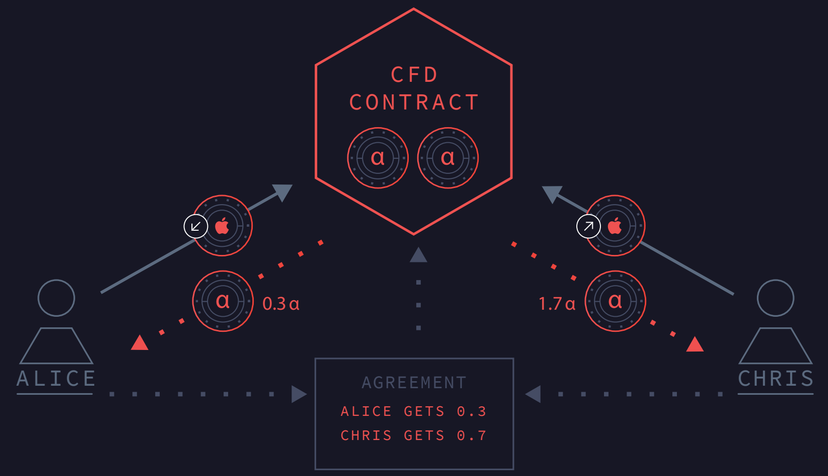
5

- Het contract wordt inactief.
- Bob kan de positie toch verlaten door zijn contract aan iemand anders te verkopen.




6

- Na 30 dagen moet het contract opnieuw geactiveerd worden om het vastgehouden geld op te nemen.
- Als Alice en Chris het over eens zijn dat AAPL 70% is gegroeid, tekenen ze beide de transactie. Alive krijgt vervolg 0.3α en Chris 1.7α.




MAAR WAT ALS ALICE NIET MEEWERKT?

# DE INTRODUCTIE VAN ORACLES

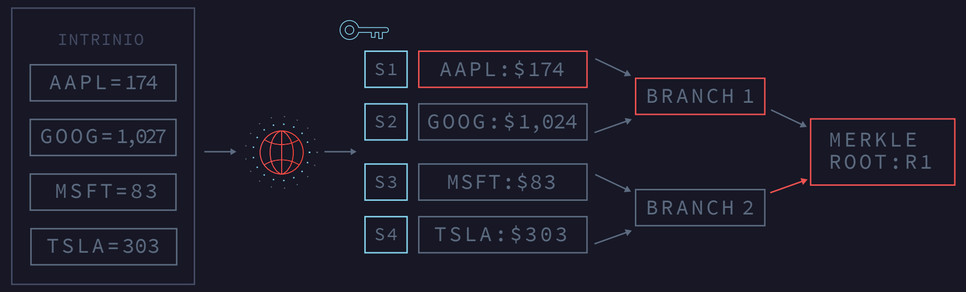
## De Oracles zorgen voor de verbinding naar de echte wereld

Contracten vermelden van tevoren welk Oracle vertrouwd worden om gegevens te verstrekken.

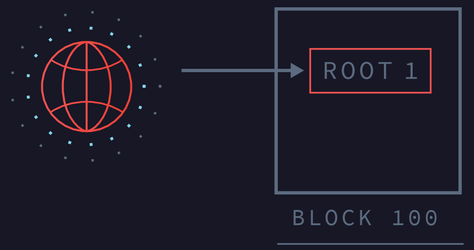
Juridische contracten kunnen rechters gebruiken mocht het misgaan. De smart-contracts gebruiken de oracles en worden weergegeven op de blockchain.

## Hoe werken de Oracles:

1 **De Oracles halen gegevens uit de Web-API's en sorteert deze in een Merkle Tree. Elke tak is salted en voorzien van een secret/nonce.**

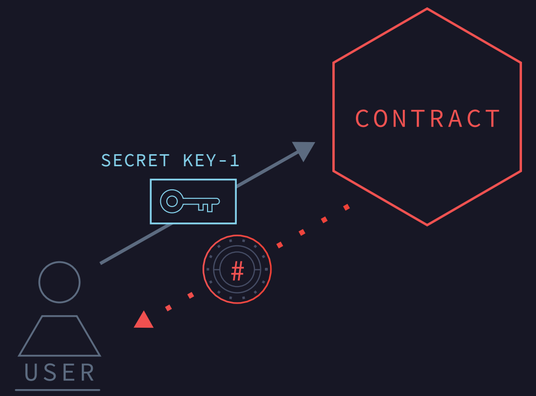



1 **Het Oracle voegt de Merkle Tree toe aan de blockchain.**




2 **Wanneer een gebruiker het contract voorziet van een specifieke stuk data, betaald de gebruiker het Oracle waarop deze het secret of de nonce onthult.**


3 **Met gebruik van de nonce kan de gebruiker bewijzen dat het contract uitgegeven is en zijn assets vervolgens innen.**

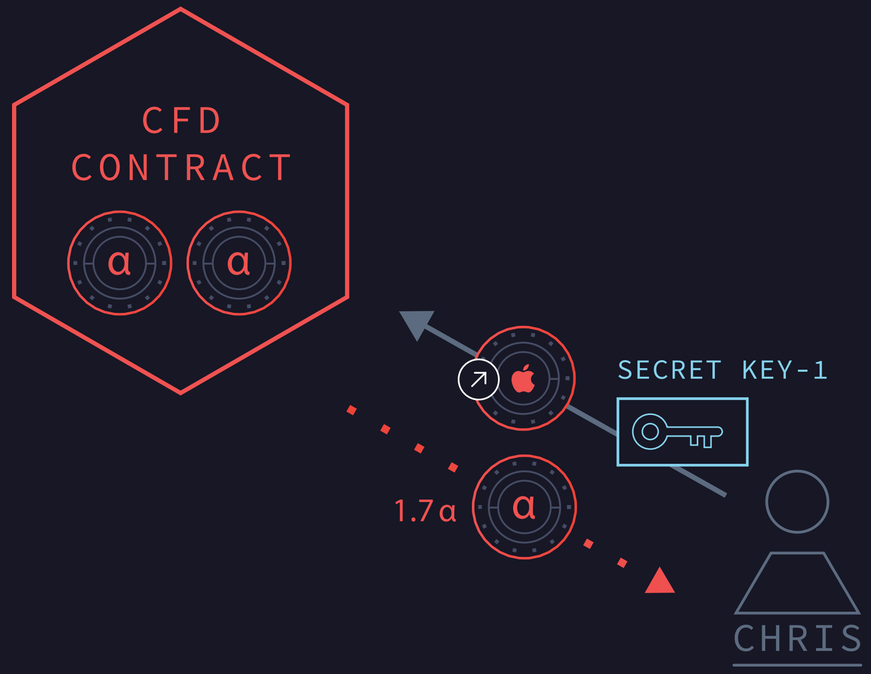


# USE CASE - AAPL CFD VERVOLG

## Oplossen van geschillen

**Dus in het geval dat Alice en Chris het niet eens worden betaald Chris het Oracle om de secret (S1) prijs te geven.**

- Chris stuurt vervolgens het geheim met de 'call-optie' naar het contract en het contract betaald Chris 1.7α.



# BITCOIN INTEGRATIE

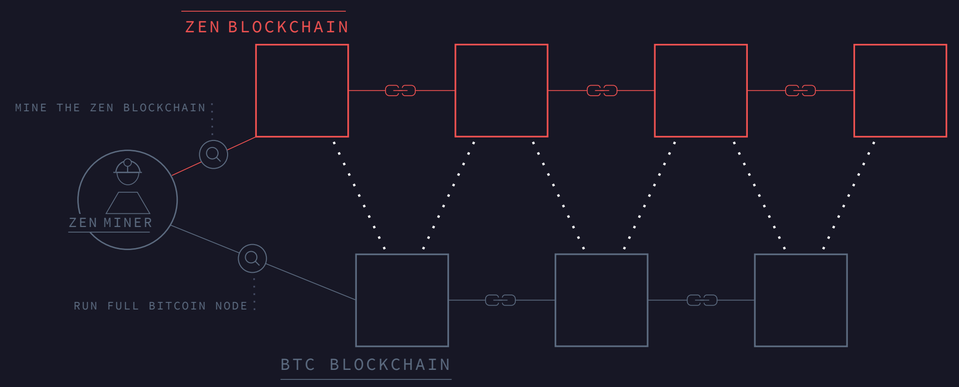
Eerdere inspanning om de complexiteit van de 'Blockchain' te vergroten hebben twee invalshoeken:

1 **Het opzetten van een alternatieve blockchain die het gebruik van Alt-coins noodzakelijk maakt.**

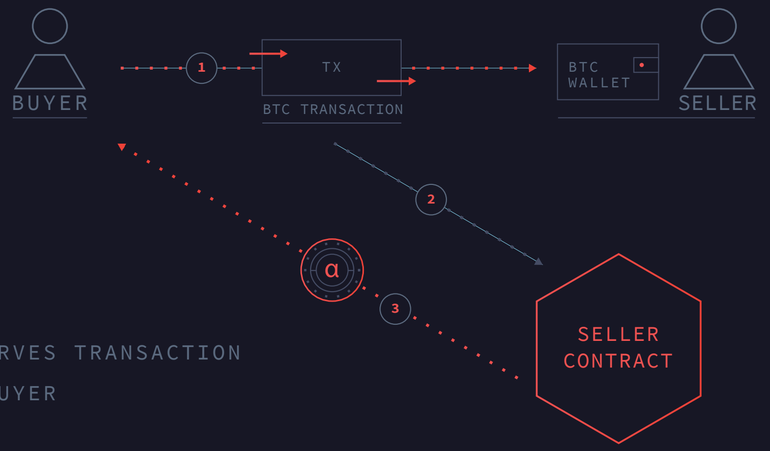
2 **Het opzetten van een aanvullend protocol, bijvoorbeeld een side-chain welke niet dezelfde functionaliteiten bezit op gebied van veiligheid als de Bitcoin.**

Zen heeft gekozen voor een compleet nieuwe benadering. Een aparte blockchain met een eigen tokens die parallel loopt met het Bitcoin-netwerk.

**Consensus** – Zen gebruikers minen de Zen blockchain en houden tegelijkertijd de Bitcoin blockchain continue in de gaten. Dit zorgt voor cross-chain functionaliteiten.




**Cross-Chain Contracten** – Het contract wordt behouden in de Zen blockchain, maar de fee's worden betaald aan Bitcoin adressen.

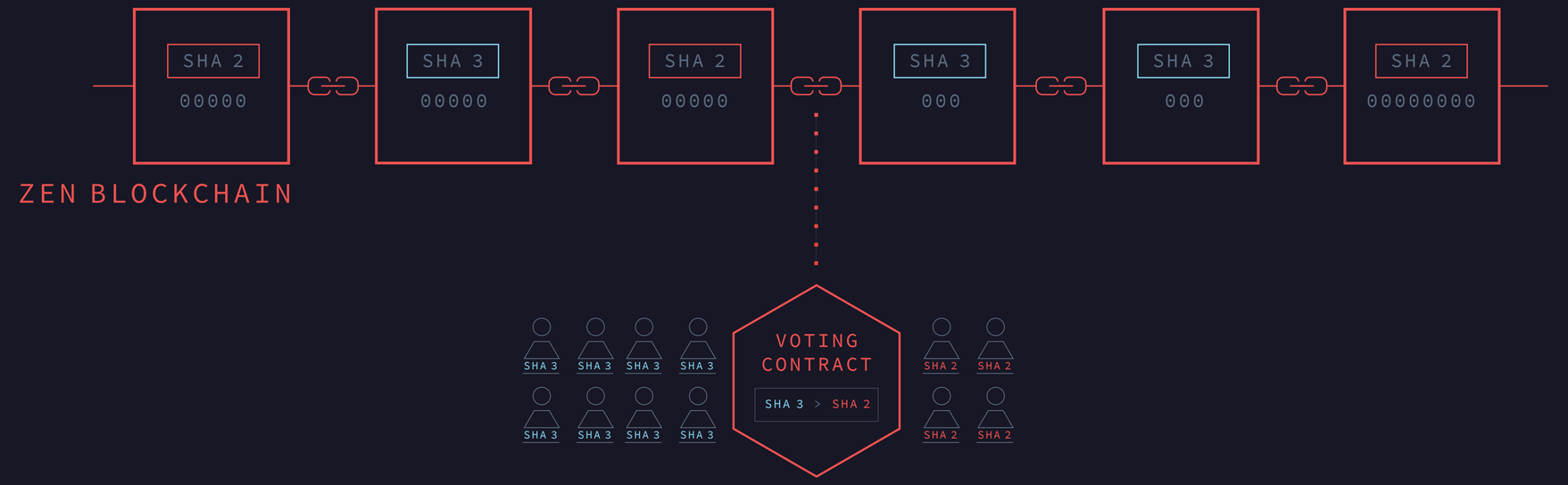



1. BUYER SENDS BTC TO SELLER
2. SELLER'S ZEN CONTRACT OBSERVES TRANSACTION
3. CONTRACT SENDS TOKENS TO BUYER

ZEN

# Multi-Hash Mining – De token houders bepalen

- Verschillende hash-functies worden gebruikt om een block te vinden.
- Elke hash-functie heeft een verschillende moeilijkheidsgraad.
- De target-ratio gegenereerd bij iedere hash-functie wordt vastgesteld door de houders van Zen token.



# ROADMAP


Idea is opgezet
Q3 2016
Q4 2016
De technologie-stack is gekozen
Kostenmodel afgerond
Q1 2017
Q2 2017
Smart-contracts en Oracle in C#
Refactoring van development contracten
Q3 2017
Q4 2017
Alpha
Kandidaten gepresenteerd
Q1 2018
Q2 2018
Genesis block
Bouw van het ecosysteem
Q3 2018

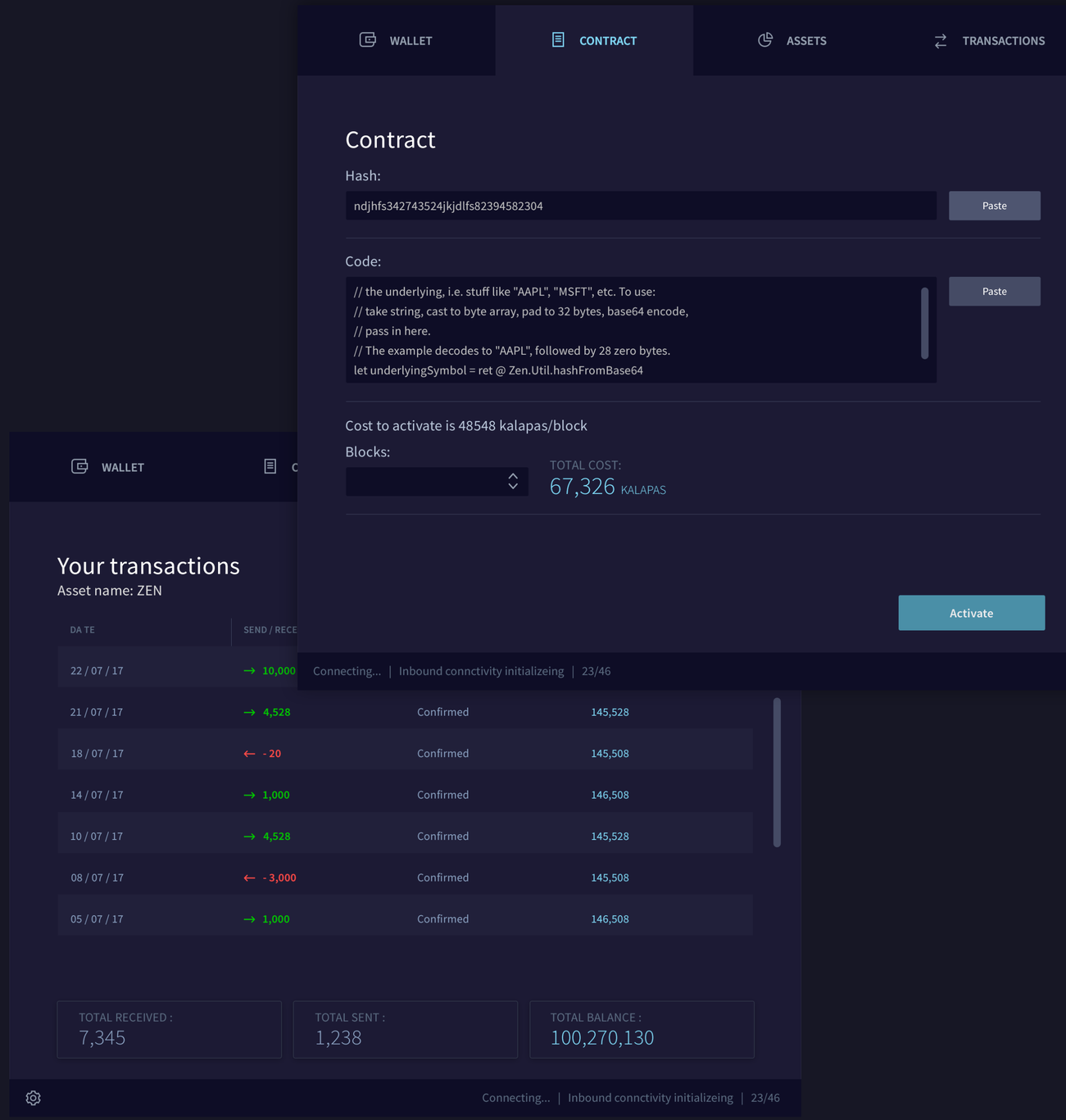
ZEN

# Alpha

Momenteel hebben we een werkende Alpha versie met gebruik van een geheel nieuwe blockchain. Er is een implementatie van het ACS, de smart-contracts in F* en Oracles welke zijn data krijgt van intrinio.com

**Zen Alpha**

DOWNLOAD



# ZEN TEAM

Wij zijn een klein team met een groots product

## Adam Perlow

*CEO*

Adam is een economie student van de IDC, reservist van het Israëlische leger en wel bekend met de Bitcoin. Sinds het begin van de Bitcoin medio 2011, heeft Adam er altijd geloof in gehad.

## Nathan Cook

*CTO*

Nathan is een voormalig wiskunde postgraduaat van de Universiteit in Cambridge. Als hij zijn werk zou moeten omschrijven, zou hij zeggen "deelnemen aan een kapitaal dat zichzelf tot leven wekt".

## Sharon Urban

*Hoofd-ontwikkelaar*

Sharon is een zeer bekwame en ervaren systeembeheerder welke het cool vindt om met de goede en skilled gasten te werken!

## Asher Manning

*Ontwikkelaar, Formal methods*

Ash heeft wiskunde, natuurkunde en computer science gestudeerd aan de universiteit van McGill. Ook heeft hij meegewerkt aan het onderzoek naar de Homotopy Type Theory.

# ZEN TEAM

Wij zijn een klein team met een groots product

## Doron Somech

*VP R&D*

Doron was de mede-oprichter en CTO van leverate.com

## Elan Perach

*Head of Product*

Elan heeft al meerdere startups gestart waard onder NFX.com en is in de crypto industrie sinds 2011. Elan heeft tevens de eerste website gebouwd welke Bitcoins verhandelde in Israel.

## Eleanor Milstein

*Art Director*

Eli is onze design guru. Met ruim 6 jaar ervaring van verschillende startups heeft zij ervaring als product designer en het zijn van een mede-oprichter.

## Isaac Rodgin

*Community Manager*

Afgestudeerd aan de IDC Herzliya met zowel een business als computer science diploma. Daarnaast ook ruim 5 jaar ervaring in community management en verkoop.

# ADVISEURS

## Pamir Gelenbe

Pamir is patner bij libertuscapital.com waar hij zich focust op decentralisatie, enterprise blockchains en digitale valuta. Hij is een investeerder in onder andere; Kraken, Legder Wallet, Shapeshift, Crypto Facilities en tal van gedecentraliseerde protocollen. In het verleden heeft hij gewerkt voor Morgan Stanley en D.E. Shaw. Pamir is gepromoveerd aan de Duke Universiteit en de Columbia Universiteit. Pamir heeft daar zijn BSc behaald in Electrical Engineering en zijn Master in Operations Research.

## Ran Nussbaum

Ran Nussbaum is partner en mede-oprichter van pontifax.com. Hij investeert in ruim 50 verschillende bedrijven overal ter wereld. Voordat Ran Pontifax joinde was hij partner met Israel's grootste business intelligence & consulting bedrijf.

## Ron Gross

Ron is afgestudeerd aan de Technion met een Master in Computer Science. Hij heeft al bij verschillende bedrijven gewerkt variërend van kleine startups tot grote corporates zoals Google. Ron heeft veel ervaring in de webarchitectuur, alsmede in beveiliging en algoritmen. Ron is sinds 2011 betrokken bij de Bitcoin en verspreid sindsdien het woord, de kennis en liefde hiervoor. Hij is een groot voorstander van open source, transparantie en de decentralisatie van macht en technologie. Ron was mede-oprichter van de Israëlische Bitcoin gemeenschap en Executive Director van de Mastercoin Foundation (de eerste token sale ooit).