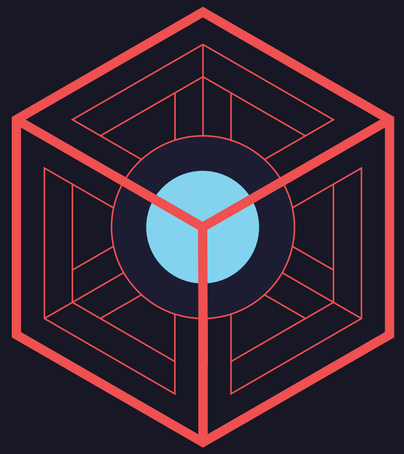


ZEN

[UN SISTEMA FINANZIARIO DECENTRALIZZATO]

ASTRATTO

Un meccanismo puramente peer-to-peer per strutturare le relazioni contrattuali consentirebbe parti reciprocamente diffidenti di redigere contratti senza fare affidamento sul sistema legale per risolvere un’eventuale disputa. Questi accordi, noti anche come Smart Contracts o "Contratti intelligenti", possono essere sottoscritti impegnandosi in un contratto digitale descritto in codice e le controversie possono essere risolte eseguendo tale codice su una rete pubblica decentralizzata.

Le piattaforme attuali non dispongono delle funzionalità o della sicurezza necessarie per eseguire in modo affidabile i contratti finanziari. Zen è una nuova piattaforma di contratto intelligente che consente la creazione, la facilitazione e risoluzione, degli obblighi contrattuali. Basato sul paradigma Bitcoin (verifica UTXO), facciamo uso di ZF *, un linguaggio funzionale utilizzato per la verifica formale, per esprimere e verificare le prove dei limiti sul consumo delle risorse contrattuali. Nello Zen, tutti i token sono "i cittadini di prima classe ", sono supportati più asset e si osserva la rete Bitcoin per facilitare l'interoperabilità.

MOTIVAZIONE

Il team del protocollo Zen ha iniziato a collaborare nel 2014 nell'ambito della blockchain e in seguito a diversi anni di ricerca hanno iniziato lo sviluppo del Protocollo Zen a Giugno 2016.

La motivazione che ha generato la visione dello Zen è che crediamo che le persone abbiano il diritto di possedere le proprie risorse finanziarie e sentiamo la responsabilità di fornire alle persone gli strumenti necessari per averne il completo controllo.

Utilizzare la crittografia per creare, scambiare e archiviare attività finanziarie convenzionali, contratti e strumenti su una rete decentralizzata.

PROBLEMA

Finanza convenzionale

Piuttosto che essere esposti al rischio della controparte, utilizziamo le istituzioni finanziarie come intermediari fidati. Queste istituzioni finanziarie facilitano la maggior parte delle transazioni economiche.

Queste istituzioni limitano le nostre libertà:

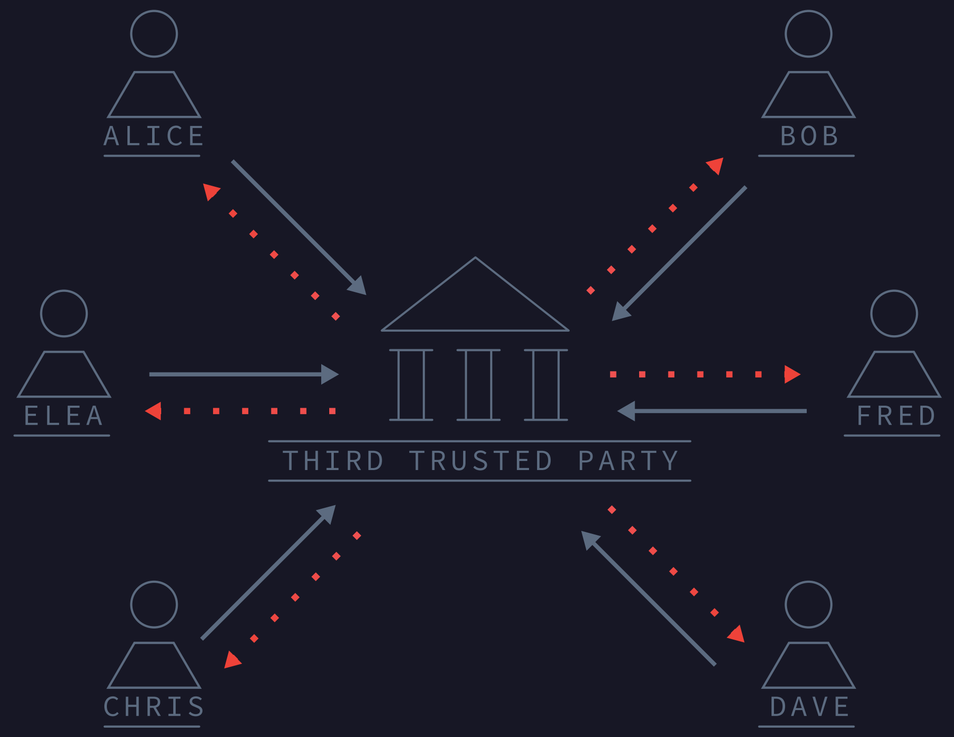
- **Accesso limitato**

  Le istituzioni finanziarie limitano ***chi*** può accedere al sistema finanziario e ***cosa*** possono fare nel sistema finanziario.

- **Proprietà / controllo limitati**

  T In una certa misura, non possediamo o controlliamo completamente i nostri beni, più che altro abbiamo un obbligo da parte della banca.

  La banca potrebbe non adempiere a questo obbligo, a causa di insolvenza o confisca.



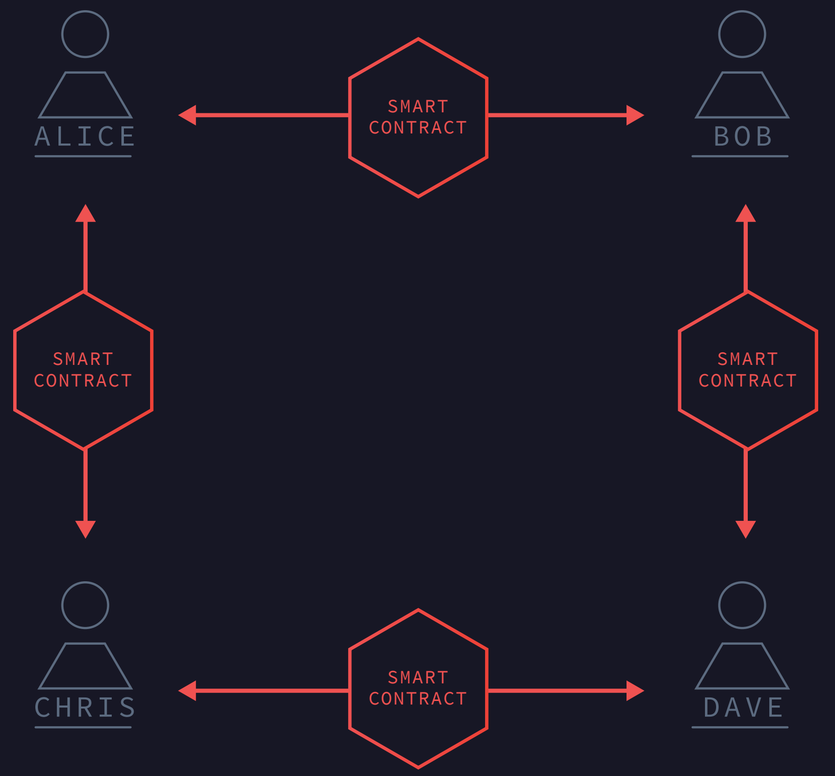
SOLUZIONE

Un Sistema Finanziario Decentralizzato

Se togliamo la nostra dipendenza da terze parti, potremmo rivendicare la proprietà dei nostri beni e delle nostre libertà. Crediamo che avremmo mercati più efficienti, con meno burocrazia e tasse.

Usando la tecnologia Bitcoin, possiamo creare un sistema finanziario decentralizzato.

Una nuova blockchain, specializzata per la finanza, ci consente di possedere le nostre risorse crittograficamente e applica i flussi di denaro che provengono da tali beni usando i contratti intelligenti.



SOLUZIONE

Una nuova blockchain costruita su misura

Questo ambiente è pieno di blockchain centralizzate focalizzate sulla finanza e di blockchains decentralizzate focalizzate su casi d'uso non finanziari. Noi vediamo il potenziale della tecnologia blockchain: finanza decentralizzata. Il progetto Zen tenta di riempire quella nicchia nel mercato.

Abbiamo davvero bisogno di un'altra Blockchain?

	DECENTRALIZZATO	CENTRALIZZATO
FINANZIARIO	**Bitcoin, Zen**	Catene di banche, R3CEV, asset digitali, partecipazioni, ecc ...
NON FINANZIARIO	Ethereum, Appcoins	Supply chain, blockchains, IBM, Skuchain

BITCOIN

Il Bitcoin è denaro decentralizzato

Crediamo che Bitcoin sia la forma di denaro definitiva. Satoshi ha scelto di limitare le funzionalità di Bitcoin con lo scopo di concentrarsi sul far interpretare a Bitcoin il ruolo di soldi. Satoshi ha affermato "Ammucchiare tutti i sistemi di quorum di proof-of-work nel mondo in un dataset non scala “.

Bitcoin manca della funzionalità richiesta per la finanza.

Abbiamo bisogno di una nuova blockchain per la finanza decentralizzata, una blockchain che supporta molteplici asset e costrutti di proprietà complessi.

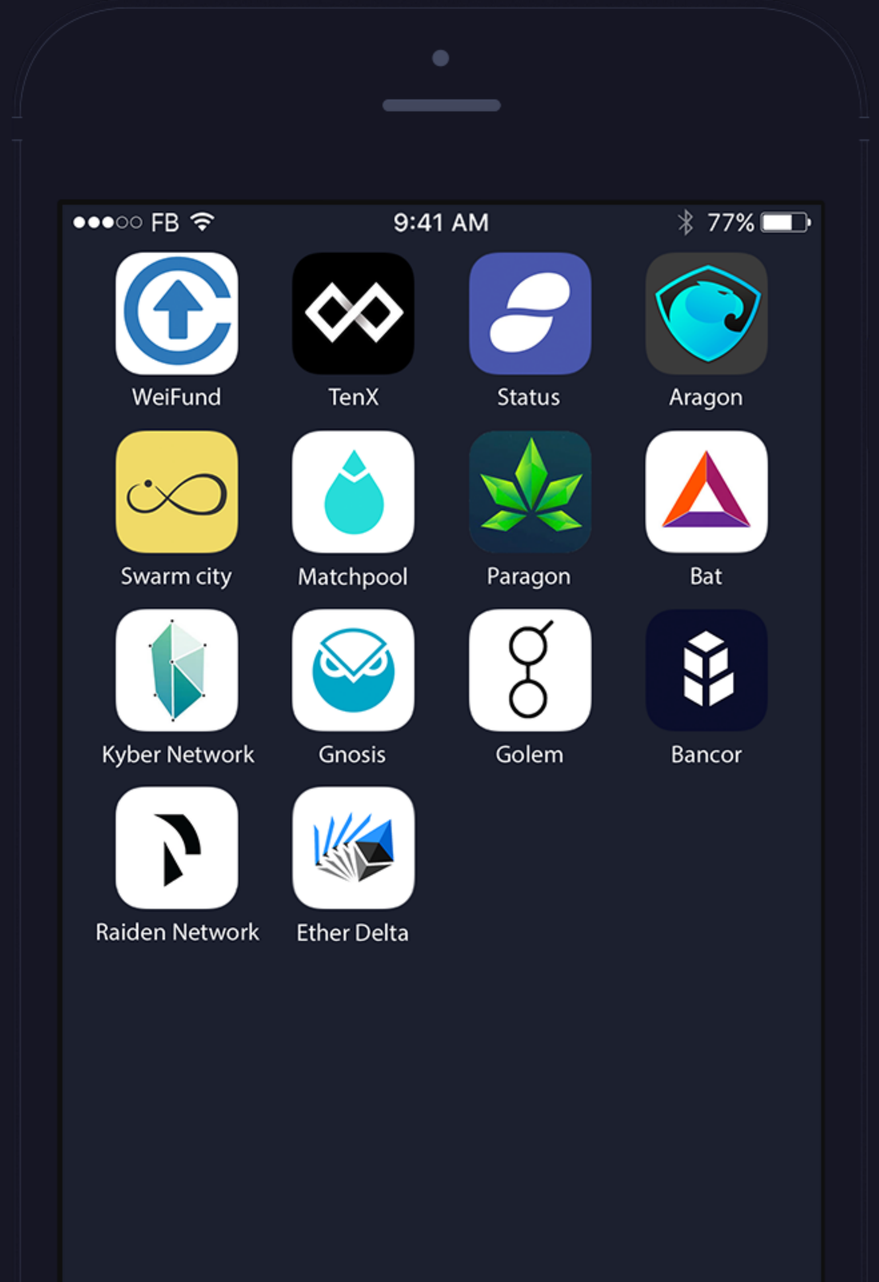
THERE ARE AN ESTIMATED 21M BRICKS (400 OZ PER BRICK) OF GOLD IN THE WORLD

ETHEREUM

Ethereum è computazione decentralizzata

L'obiettivo di Ethereum è di essere una piattaforma per lo sviluppo di applicazioni decentralizzate, per esempio Facebook o Uber senza un server centrale. Ethereum è una piattaforma focalizzata sugli sviluppatori e fornisce lingue di programmazione conveniente (Solidity) e Application Binary Interfaces (ABI).

Al fine di abilitare questa funzionalità, Ethereum fornisce l'Ethereum Virtual Machine (EVM), dove vengono contati i cicli di calcolo del sistema di gas in uso.



ZEN

Zen è finanza decentralizzata

Lo Zen è una nuova piattaforma focalizzata su strumenti finanziari decentralizzati. Zen consente l'accesso peer-to-peer contemporaneamente a asset nuove e convenzionali.

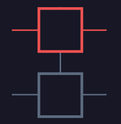
Allo stesso modo in cui Bitcoin ha rimosso il nostro affidamento alle banche per il trasferimento di denaro, Zen intende rimuovere il nostro affidamento alle banche per impegnarsi nella finanza.

TOKENS

Vengono tenuti crittograficamente in un portafoglio.

ACS

"Ambiente di esecuzione" dello Zen, equivalente allo stack di Bitcoin o all'EVM di Ethereum.



INTEGRAZIONE ALLA BITCOIN

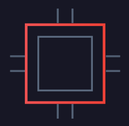
Lo Zen corre in parallelo e agisce in maniera complementare a Bitcoin.

CONTRACTS

Sostituisci gli intermediari con meccanismi di depositi a garanzia decentralizzati

ORACLES

I contratti possono dipendere dagli eventi del mondo reale come il movimento dei prezzi nel mercato degli stock.



MULTI HASH MINING

Gli stakeholder votano su quali algoritmi di hash faranno ricevere la ricompensa del mining, stabilendo un equilibrio tra gli interessi dei minatori e dei titolari di token.

ARCHITETTURA

Tokens

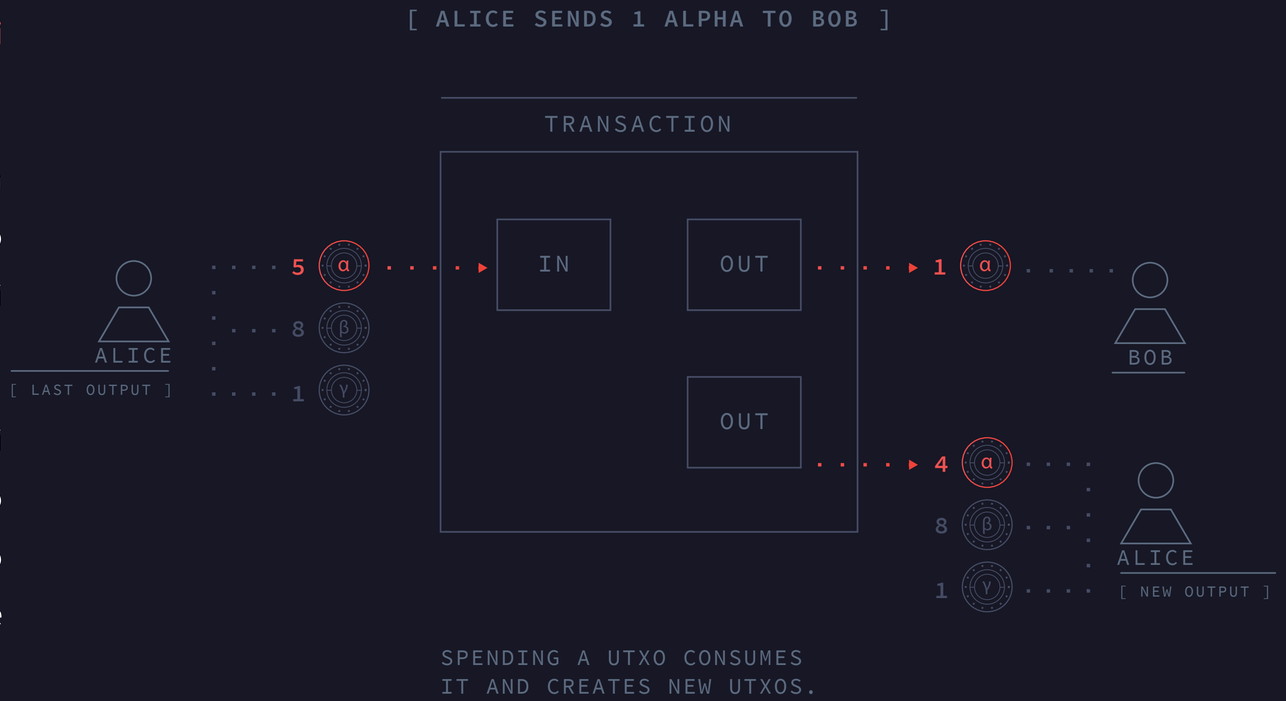
A differenza di Bitcoin che supporta solo BTC o di Ethereum che ha contratti ERC-20, lo Zen ha diversi token integrati a livello di protocollo.

Ciò significa che ogni tipo di token in Zen ha uno status simile allo Zen token nativo. Pertanto ogni contratto in Zen può contenere e gestire qualsiasi altro token e qualsiasi token può essere utilizzato per pagare le commissioni di transazione ai minatori.

Questo è di particolare interesse in quanto consente ai contratti finanziari di essere denominati in valute "normali" come il dollaro o l'euro. I token sono memorizzato nella produzione delle transazioni, proprio come in Bitcoin, e può essere sbloccato con le autorizzazioni giuste, quindi bloccate di nuovo in nuove uscite.

I token generalmente hanno valore perché:

- Le persone credono di avere un valore
- Sono supportati da contratti che contengono garanzie



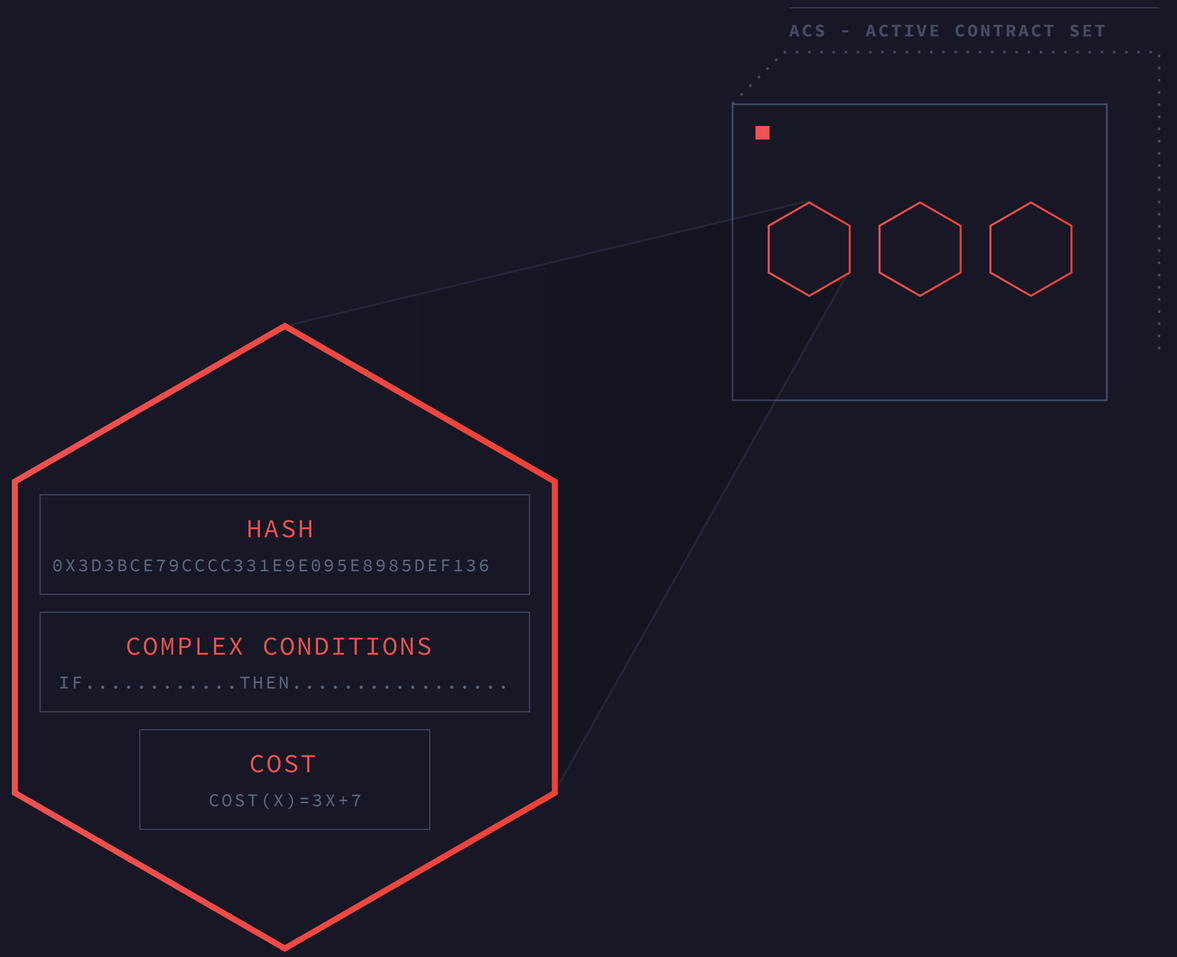
ARCHITETTURA

Contratti

I contratti sono scritti in F * – un linguaggio formalmente verificato funzionale, scritto in maniera dipendente e di alto livello. Verifica formale, unita a un modello di costo, consente a tutti i contratti del protocollo Zen di **dimostrare per quanto tempo impiegano ad eseguirsi prima che entrino nella blockchain..**

I contratti sono immutabili– (il loro codice non cambia mai). Pertanto ciascun contratto può avere un identificatore matematico univoco (il suo hash). Usando questo hash, è facile associare token e prove con un contratto.

Ogni contratto vive in isolamento dal resto della blockchain –
Un contratto può solo cambiare lo stato della blockchain e comunicare con altri contratti creando una transazione. I contratti non fanno nulla in maniera indipendente. Piuttosto, agiscono come dati di convalida, che sono utilizzati per aiutare i nodi a determinare se accettare o meno una transazione.



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

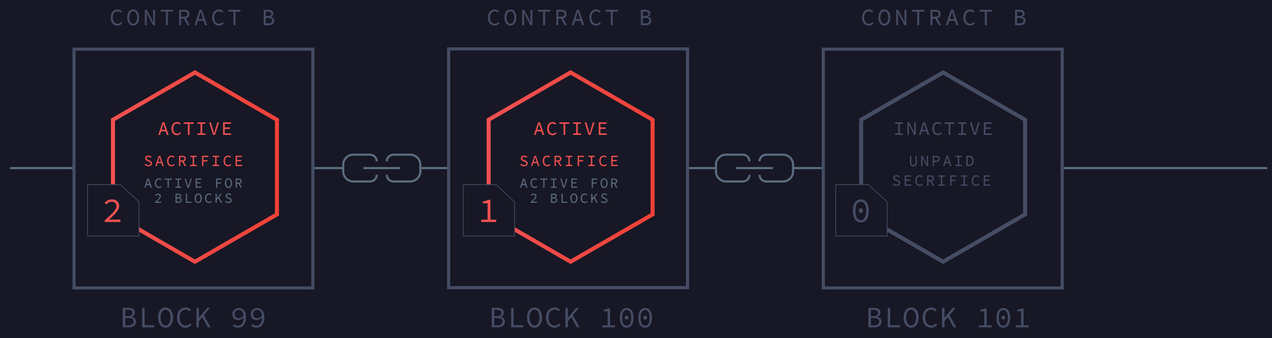
ARCHITECTURE

Set di Contratti Attivi

- All'attivazione, i contratti vengono convertiti da F * a codice macchina.
- I contratti compilati sono memorizzati nella RAM del nodo.
- I contratti devono essere attivi per creare transazioni, come l'invio o emissione di token.
- Chiunque può attivare o estendere un contratto con un contratto di sacrificio.

Il sacrificio nel contratto

- Il sacrificio contrattuale compensa i minatori che devono mantenere il contratto. Il sacrificio è diviso tra i minatori che trovano blocchi durante il periodo attivo.
- Mentre le commissioni di transazione possono essere pagate in qualsiasi token, il sacrificio nel contratto deve essere pagato in Zen.



CASI D’USO - AAPL CFD

Diamo un'occhiata a come funzionano i token, i contratti e il set di contratti attivi insieme per creare un contratto finanziario peer-to-peer.

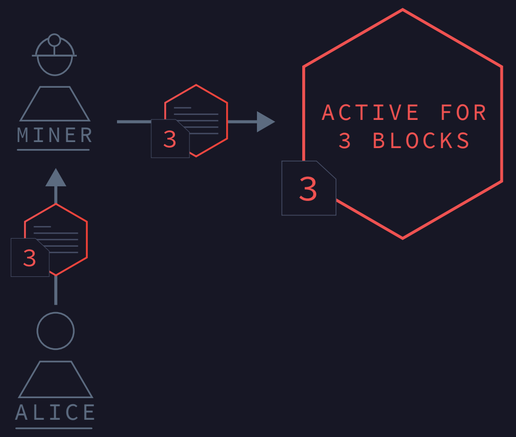
1

- **Alice scrive un contratto per differenza (CFD) su AAPL per 30 giorni.**
- **Alice guadagna se AAPL va giù.**
- **La sua controparte guadagna se AAPL sale**

CASI D’USO - AAPL CFD

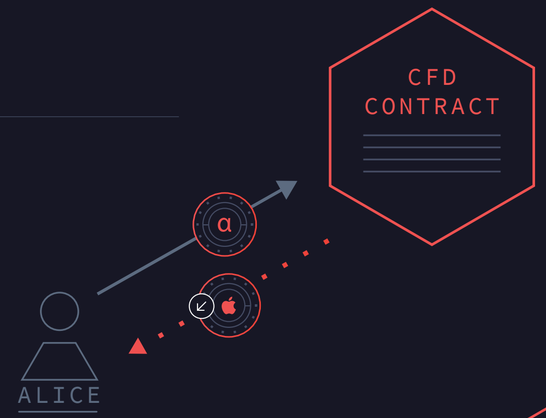
2

- Alice attiva il contratto per 3 blocchi.



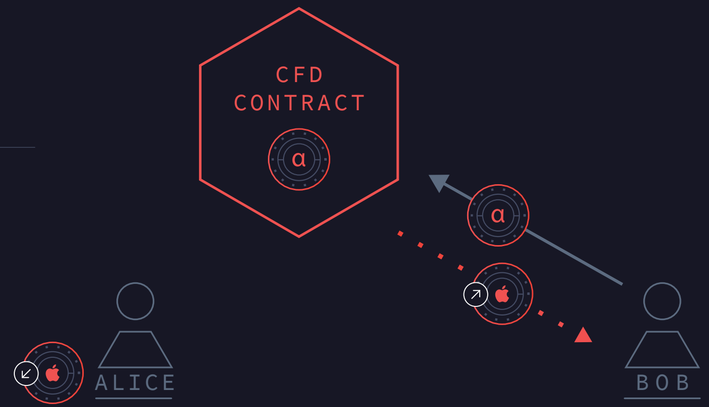
3

- Alice garantisce il contratto attivo, inserendo una posizione corta (short position).



4

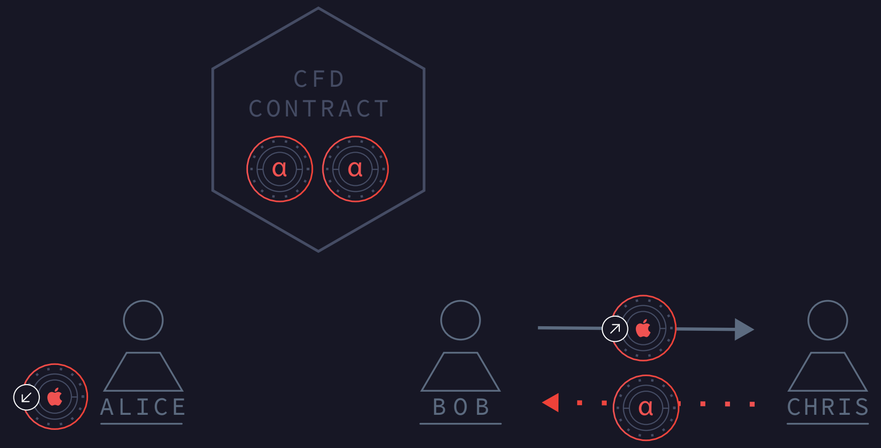
- Bob vede il contratto collateralizzato e si posiziona dall'altra parte inviando token.



USE CASE - AAPL CFD

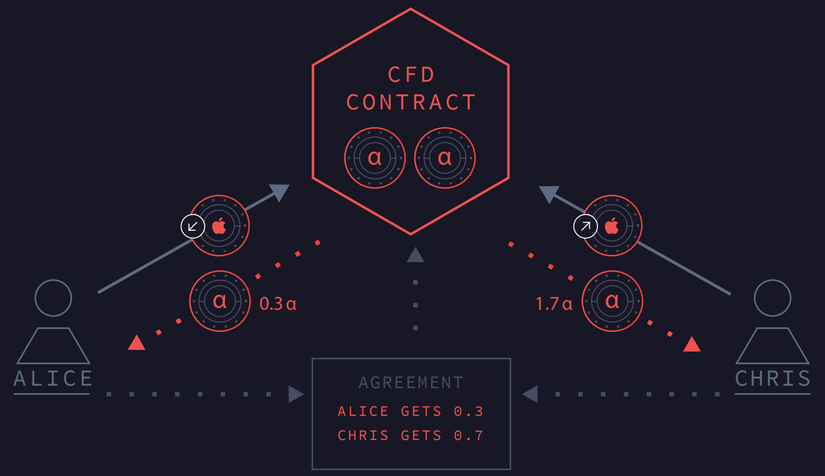
5

- Il contratto diventa inattivo
- Bob può ancora uscire dalla sua posizione vendendo il suo Contratto token a qualcun altro.



6

- Dopo 30 giorni, il contratto deve essere riattivato per ritirare i fondi in garanzia.
- Se Alice e Chris sono d'accordo che AAPL è aumentato del 70%, firmano una transazione in cui Alice ottiene 0,3 α e Chris ottiene 1,7 α.



MA COSA SUCCEDE SE ALICE NON SI DIMOSTRA COOPERATIVA?

VI PRESENTIAMO ORACLE

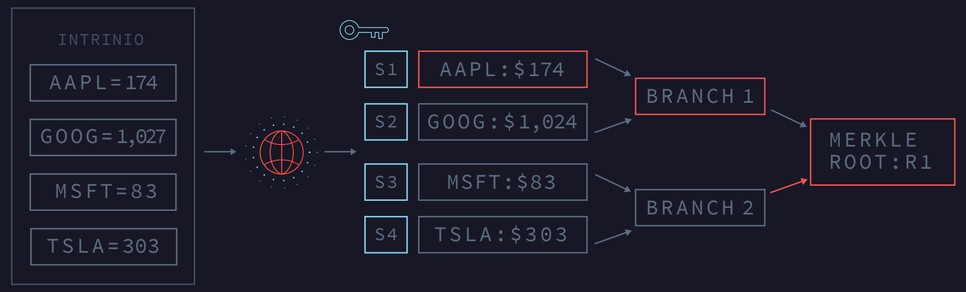
Gli oracoli consentono ai contratti di operare su dati del mondo reale

I contratti indicano in anticipo a quali oracle si farà riferimento nel fornire dati al contratto.

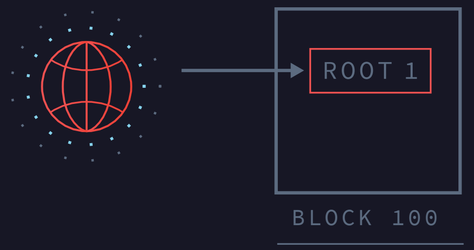
I contratti legali usano i giudici e sono arbitrati in tribunale, gli smart contract utilizzano oracoli e sono arbitrati sulla blockchain.

Come funzionano gli oracoli:

1 **Oracles estrae i dati dalle API Web e li ordina in un Merkle Tree; Ogni foglia è saldata con un segreto / nonce.**

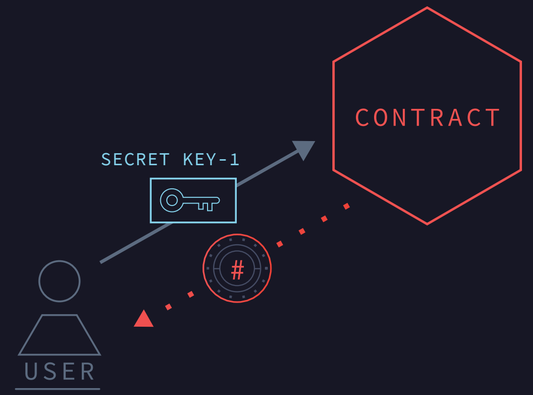


2 **L'Oracolo inserisce una radice di Merkle sulla blockchain**



3 **Quando un utente deve fornire al contratto una foglia / un pezzo di dati specifici (ad esempio per risolvere a disputa), l'utente paga l'oracolo e l'oracolo rivela il nonce.**

4 **Usando il nonce, l'utente può provare al contratto quale è il prezzo impegnato e prelevare i fondi.**

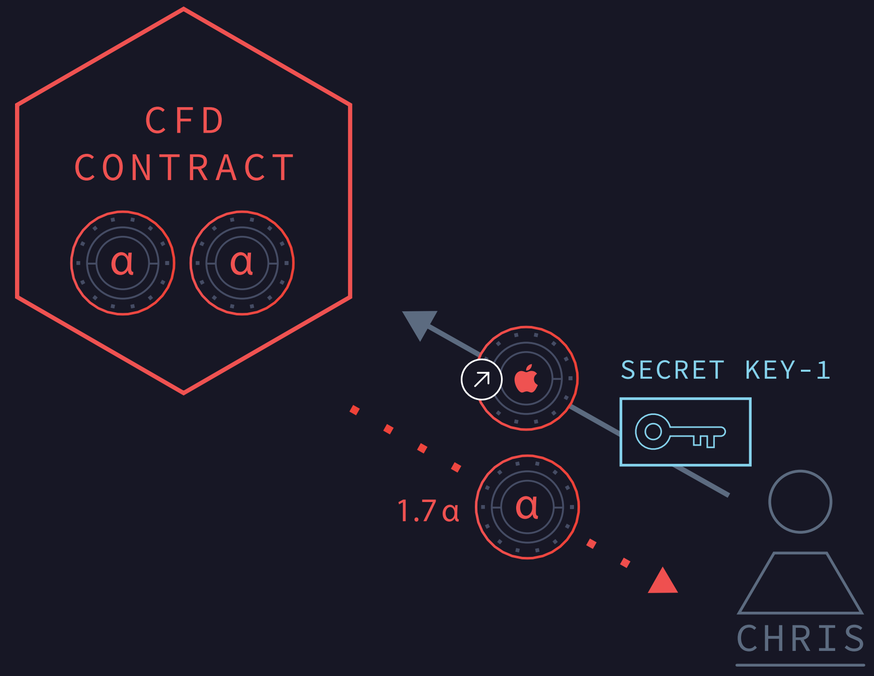


CONTINUAZIONE DEI CASI D’USO - AAPL CFD

Risoluzione della disputa

Quindi, nel caso in cui Alice e Chris non possano essere d'accordo, Chris pagherà l'oracolo per fornirgli il segreto (S1).

- Chris invia quindi il segreto e l’opzione chiamata al contratto, e il contratto paga chris 1.7alpha.



INTEGRAZIONE BITCOIN

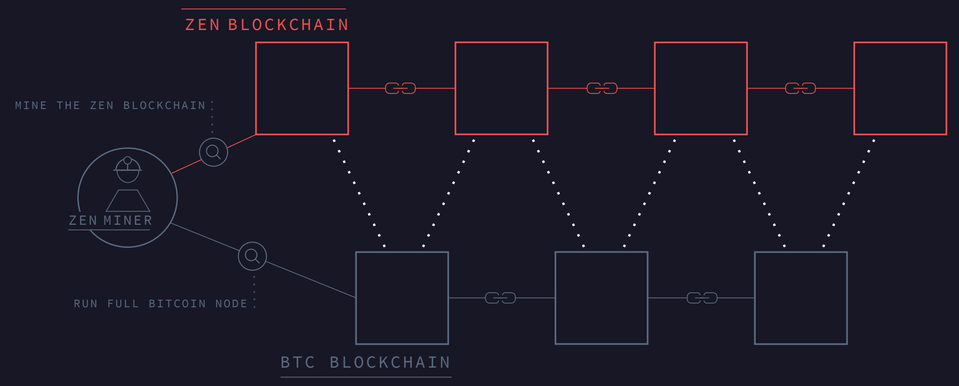
Gli sforzi passati per aumentare la complessità nei sistemi "blockchain" hanno adottato due strategie:

1 **Creare una blockchain alternativa che richiede l'uso di un AltCoin.**

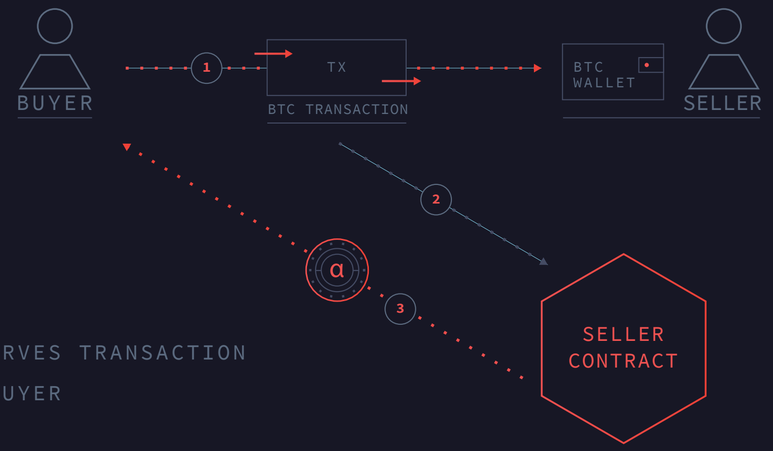
2 **Creare un protocollo supplementare, ad es. una catena laterale, che manca di un token proprietario e quindi differisce dai meccanismi di incentivazione / sicurezza di Bitcoin.**

Lo Zen ha un nuovo approccio, una blockchain separata con il suo proprio token, che viene eseguito in parallelo alla rete Bitcoin.

Consenso unito – I minatori Zen minano la Blockchain di Zen e osservano la Blockchain di Bitcoin. Questo permette funzionalità intra-chain.



Contratto intra-chain – Il collaterale è detenuto nella catena Zen, ma il premio è pagato ad un indirizzo Bitcoin.

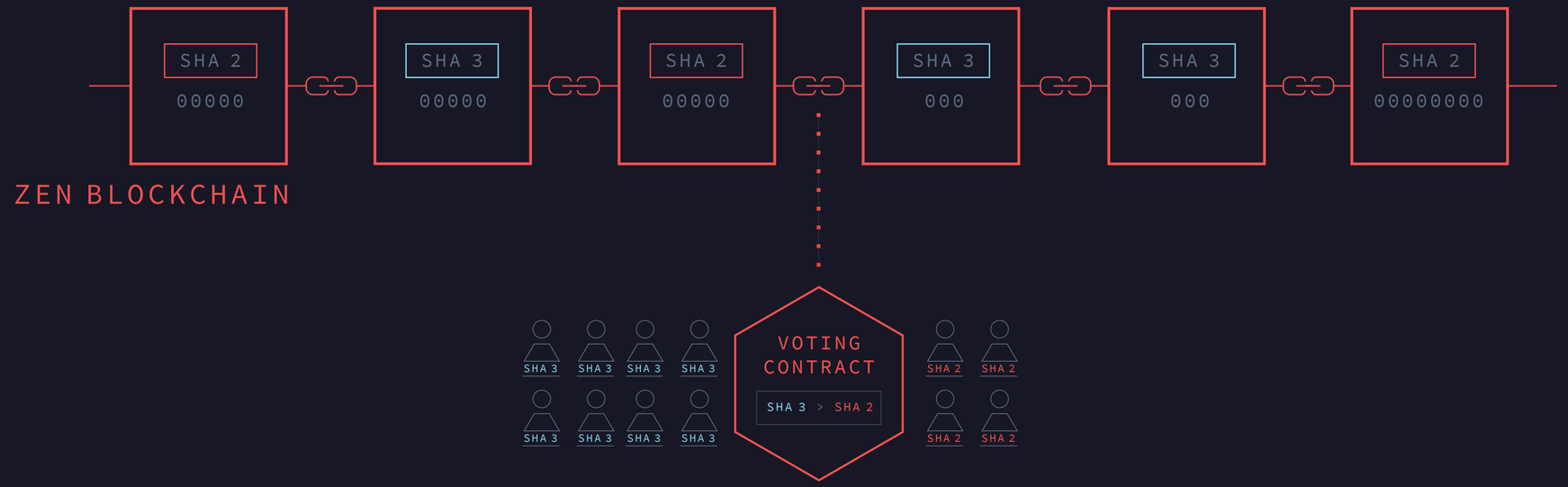


1. BUYER SENDS BTC TO SELLER
2. SELLER'S ZEN CONTRACT OBSERVES TRANSACTION
3. CONTRACT SENDS TOKENS TO BUYER

ZEN

Multi-Hash Mining – schema di token holder

- È possibile utilizzare diverse funzioni hash per trovare un blocco.
- Ogni funzione di hash ha un diverso requisito di difficoltà.
- Il rapporto di destinazione dei blocchi generati da ciascuna funzione di hash è stabilito dai possessori di token Zen.



ROADMAP


L’idea viene formalizzata
Q3 2016
Q4 2016
Il tipo di tecnologia è deciso
Il modello di costo viene completato
Q1 2017
Q2 2017
Gli smart contracts e oracles sono in C#
Ricostituzione e sviluppo dei contratti
Q3 2017
Q4 2017
Alpha
Rilascio del candidato
Q1 2018
Q2 2018
Blocco genesis
Costruzione dell’ecosistema
Q3 2018

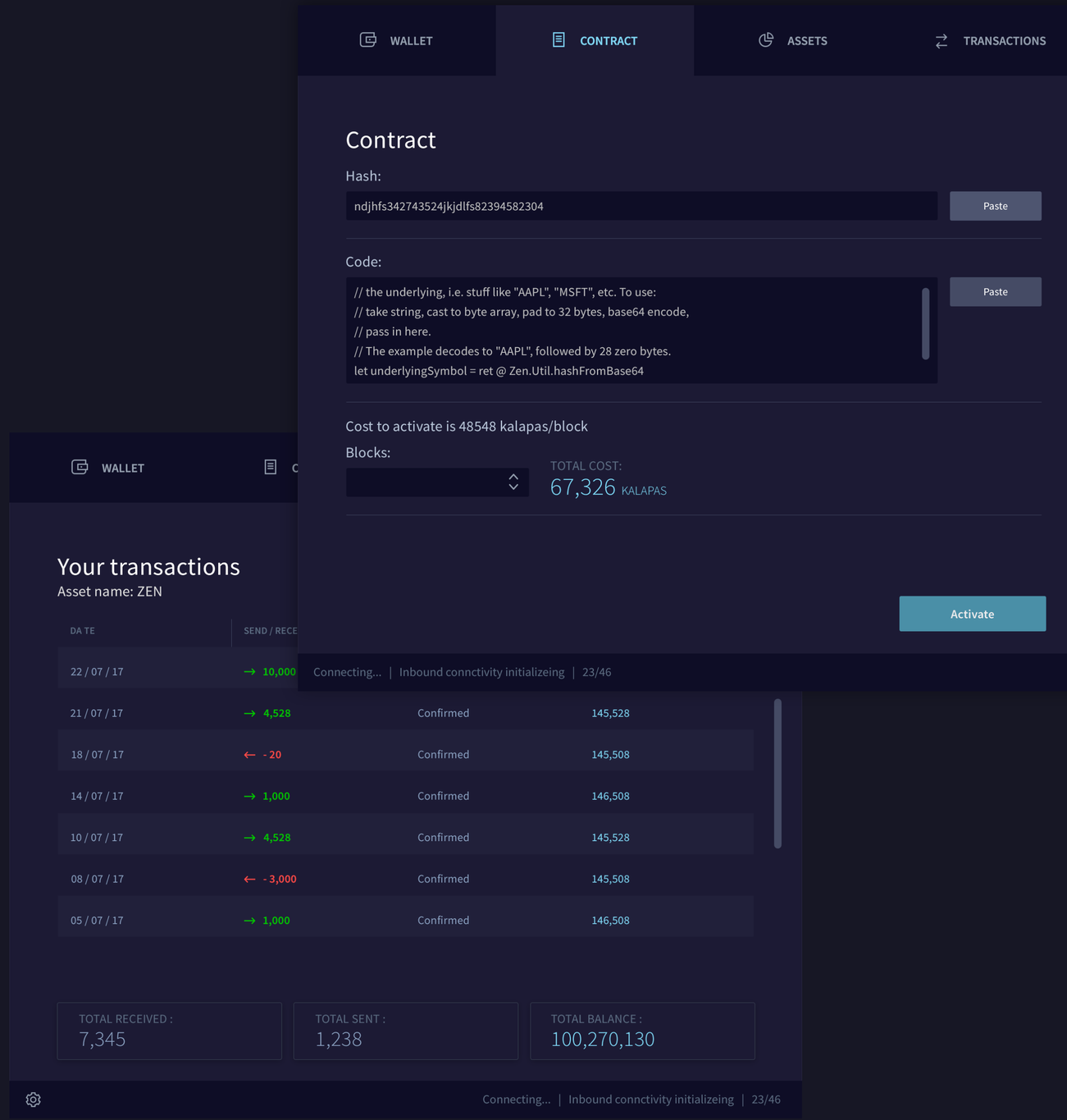
ZEN

Alpha

Al l momento abbiamo un alpha funzionante con una blockchain costruita da zero, implementazione dell'ACS, contratti intelligenti scritti in F * che dimostrano il loro costo e gli oracoli che recuperano i prezzi delle azioni da intrinio.com

Zen Alpha

DOWNLOAD



ZEN TEAM

Siamo una piccola squadra che costruisce un grande prodotto.

Adam Perlow

Amministratore delegato

Adam è un laureato in finanza dell'IDC, un riservista dell'esercito israeliano, e una vecchia leva dentro Bitcoin. Era risaputo che sarebbe andando alle stelle dal giorno in cui ne ha sentito parlare per la prima volta nel lontano 2011.

Nathan Cook

CTO

Un dottorato in matematica a Cambride University. Descrive il suo lavoro così: "prendendo parte al capitale lo si porta ad esistere"

Sharon Urban

Sviluppatore principale

Sharon è altamente qualificato ed un esperto ingegnere informatico che ama lavorare con i bravi ragazzi!

Asher Manning

Sviluppatore, Metodi Formali

Ash studia matematica, fisica e CS a McGill University e ha lavorato alla ricerca nella teoria dei tipi di omotopia.

ZEN TEAM

Siamo una piccola squadra che costruisce un grande prodotto.

Doron Somech

VP R&D

Doron, è stato il co-fondatore e CTO di leverate.com

Elan Perach

Responsabile del prodotto

Elan ha avviato più startup, un Alumni di NFX.com, è nell'ambiente cripto dal 2011, ed ha creato il primo sito web per vendere Bitcoin in Israele.

Eleanor Milstein

Direttore artistico

Eli è il nostro guru del design di prodotto, che porta 6 anni di esperienza da diverse startup sia come product designer che come cofondatrice.

Isaac Rodgin

Direttore della comunità

Laureato da IDC Herzliya, con entrambe le Lauree in Economia e Informatica. Con oltre 5 anni in Community Management e vendite.

CONSULENTI

Pamir Gelenbe

Pamir è un Managing Partner di Libertus Capital, dove si è concentro su sistemi decentralizzati, blockchain d'impresa e valuta digitale. È un investitore in Kraken, LedgerWallet, Shapeshift e Crypto Facilities e diversi protocolli decentralizzati. In precedenza, ha fatto da Partner presso Hummingbird Ventures, e ha anche lavorato da Morgan Stanley e D.E. Shaw. Pamir si è laureato alla Duke University e Columbia University con un BSc. In Ingegneria elettrica e un MSc. in ricerca operativa.

Ran Nussbaum

Ran Nussbaum è un socio amministratore e co-fondatore di The Pontifax Group. Il fondo ha più di 50 società di portafoglio in tutto il mondo. Prima di unirsi a Pontifax, era un socio della più grande impresa israeliana nonchè società di consulenza strategica e intelligence.

Ron Gross

Ron si è laureato al Technion con un MSc in Computer Science. Ha lavorato in diverse aziende, da piccole startup a Google e ha una vasta esperienza nell'architettura web, sicurezza e algoritmi. Ron è stato continuamente coinvolto con Bitcoin da marzo 2011, diffondendo la voce, conoscenza e amore per Bitcoin. È un convinto sostenitore dell'open source, trasparenza e decentralizzazione del potere e della tecnologia. Ron cofondò la comunità israeliana di Bitcoin e Foundation e fu il Direttore esecutivo della Mastercoin Foundation (prima ICO al mondo).