Z E N

[UM SISTEMA FINANCEIRO DESCENTRALIZADO]

RESUMO

Um mecanismo completamente ponto-a-ponto para estruturar relações contratuais permitiria que partes mutualmente desconhecidas possam elaborar contratos sem a dependência de um sistema de mediação de disputas. Esses acordos, também conhecidos como "Contratos Inteligentes", podem ser submetidos como um contrato digital baseado em código e as suas disputas resolvidas executando o código em uma rede pública descentralizada.

As plataformas atuais não possuem a funcionalidade ou a segurança necessária para executar com segurança contratos financeiros. O Zen é uma nova plataforma de contratos inteligentes que permite a criação, facilitação e execução de obrigações contratuais. Com base no paradigma de Bitcoin (verificação UTXO), usamos o ZF*, uma linguagem funcional usado para verificação formal, para representar e verificar provas de trabalho no uso dos recursos contratuais. No Zen, todos os tokens são como “autoridades" que oferecem suporte a múltiplos recursos e observam a rede Bitcoin para facilitar a sua interoperabilidade.

MOTIVAÇÃO

A equipe central do protocolo Zen começou conjuntamente a trabalhar na blockchain em 2014, depois de anos de pesquisa começou o desenvolvimento do Protocolo Zen em Junho de 2016.

A motivação que gerou a visão do Zen é que acreditamos que as pessoas têm o direito de possuir seus ativos financeiros, e nós sentimos a responsabilidade de fornecer às pessoas as ferramentas necessárias para que realizem.

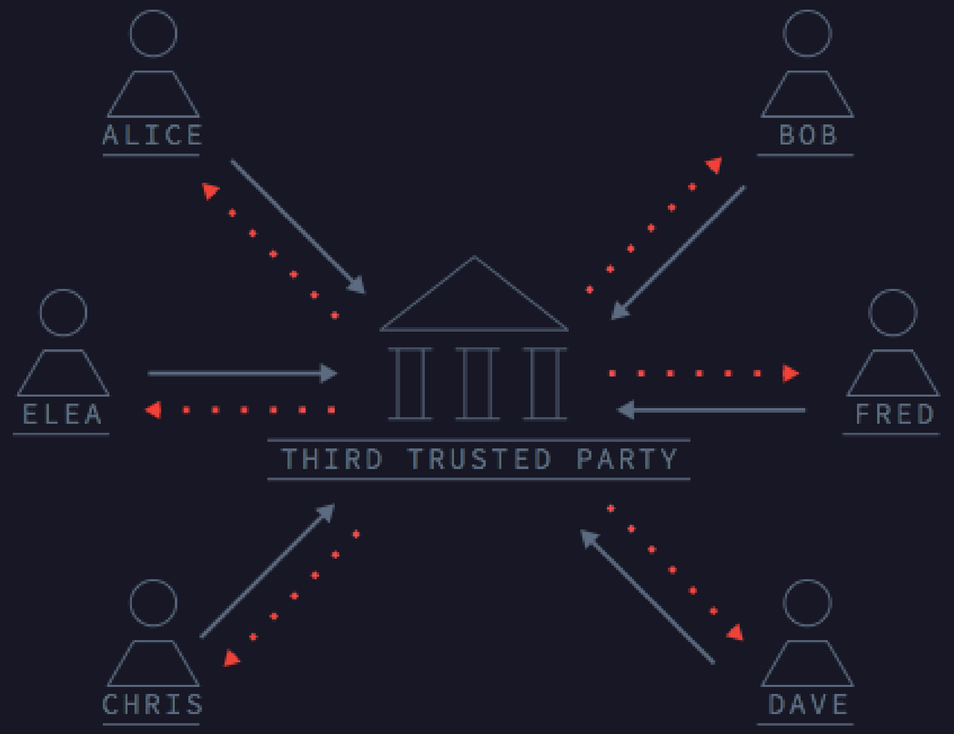
O Zen permite que as pessoas tenham um "canivete suíço" no bolso. Use a criptografia para criar, negociar e armazenar ativos financeiros convencionais, como ações, títulos e derivados, em uma rede descentralizada.

PROBLEMA

Sistema Financeiro Convencional

Para não sermos expostos ao risco do contraparte, usamos instituições financeiras como intermediários confiáveis. Essas instituições financeiras facilitam a maioria das transações econômicas. **Essas instituições limitam nossas liberdades:**

- **Acesso Limitado**
  As instituições financeiras restringem quem tem acesso e o que podem fazer no sistema financeiro.
- **Propriedade Limitada**
  Nós não possuímos nossos ativos de fato, mas sim uma obrigação bancária. O banco pode não cumprir esta obrigação, seja por insolvência ou por confisco.



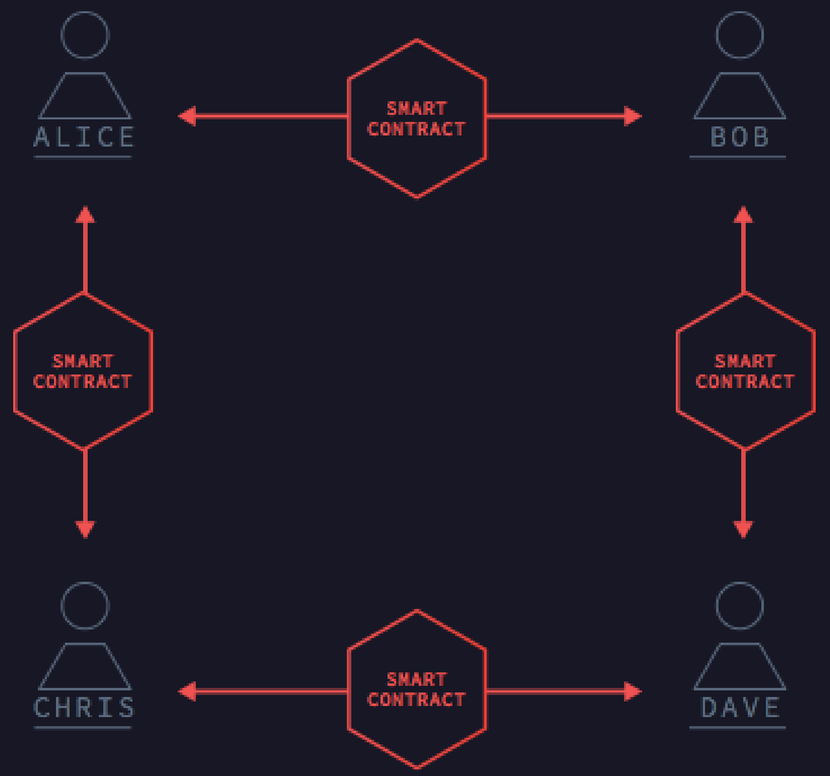
SOLUÇÃO

Um Sistema Financeiro Descentralizado

Se removêssemos a terceira parte de confiança, poderíamos reivindicar a propriedade de nossos ativos e a liberdade de fazer com eles o que quisermos. Teríamos mercados mais interessantes, com menos burocracia e taxas.

Usando a tecnologia Bitcoin, podemos criar um sistema financeiro descentralizado.

Uma nova blockchain, especializada em finanças, nos permitiria possuir nossos ativos de forma criptográfica, reforçando a movimentação de caixa que parte desses ativos , tudo isso usando contratos inteligentes.



SOLUÇÃO

Nós construímos uma nova Blockchain para esse propósito

O cenário atual é preenchido com blockchains centralizadas focadas em finanças e blockchains descentralizadas focadas em casos de uso não financeiros. Não há quem não perceba o potencial da tecnologia blockchain - financiamento descentralizado. Zen tenta preencher esse nicho no mercado.

Precisamos realmente de outra Blockchain?

	DESCENTRALIZADO	CENTRALIZADO
FINANCEIRO	**Bitcoin, Zen**	Rede bancária, R3CEV, ativos digitais, participações, etc…
NÃO FINANCEIRO	Ethereum, Appcoins	Cadeias de abastecimento,, blockchains IBM, Skuchain

BITCOIN

Bitcoin é dinheiro descentralizado

Acreditamos que **Bitcoin é a última forma de dinheiro**. Satoshi escolheu limitar os recursos do Bitcoin de forma a concentrá-lo para servir como dinheiro em papel. Satoshi argumentava que "empilhar qualquer sistema de prova de trabalho do mundo em um conjunto de dados não é escalável".

Bitcoin não possui a funcionalidade necessária para o financiamento.

Precisamos de uma nova blockchain para finanças descentralizada, uma blockchain que tenha suporte para **múltiplos ativos e construções de propriedade complexas**.

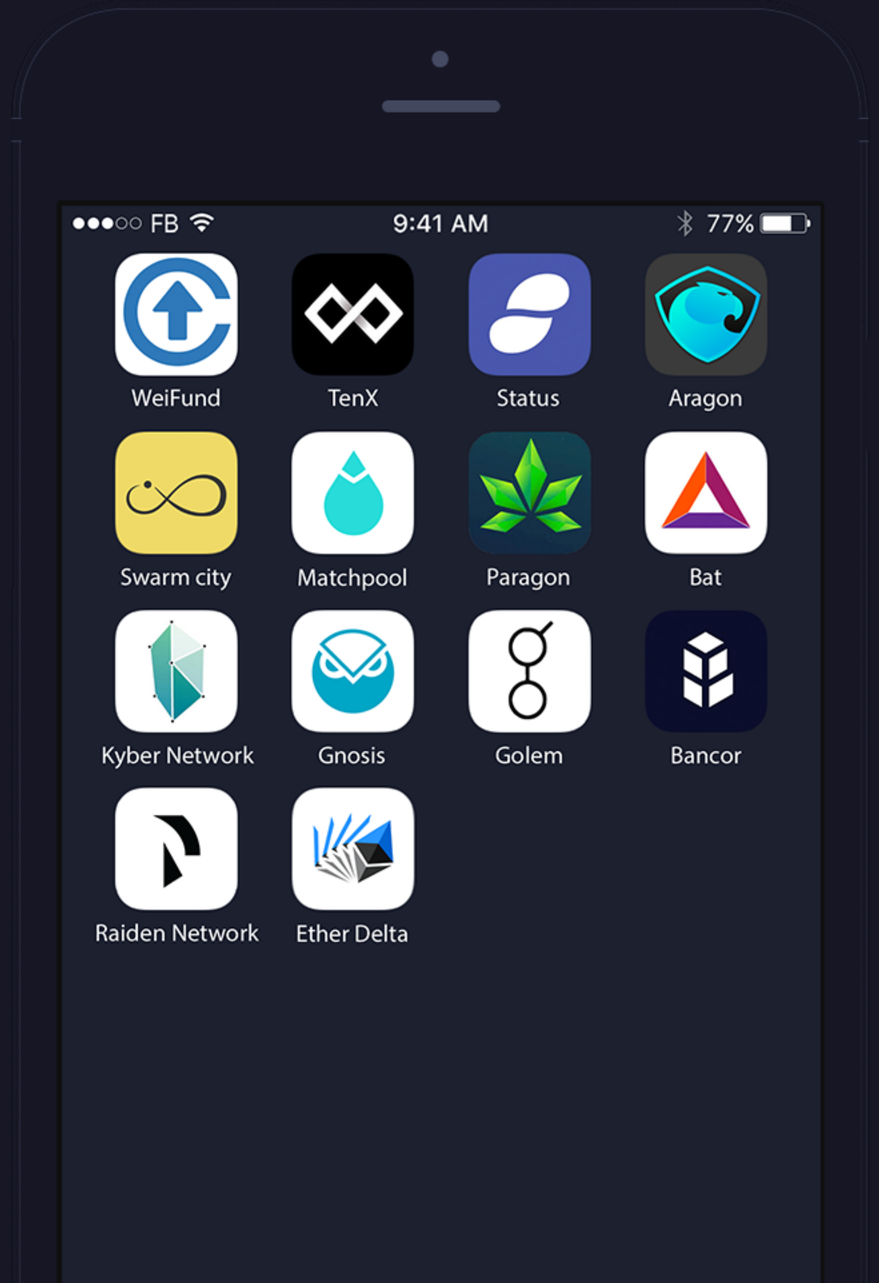
ESTIMA-SE QUE HAJA 21M TIJOLOS (400 OZ CADA) DE OURO NO MUNDO

ETHEREUM

Ethereum é uma computação descentralizada

O objetivo da Ethereum é ser uma plataforma para o desenvolvimento de aplicativos descentralizados, por exemplo, o Facebook ou Uber sem um servidor central. Ethereum é uma plataforma focada no desenvolvolvimento e fornece linguagens de programação (Solidity) e interfaces (ABIs) convenientes.

Para habilitar esta funcionalidade, Ethereum fornece a Máquina Virtual Ethereum (EVM), onde os ciclos computacionais são contados e usam o sistema de gás.



ZEN

Zen é um sistema financeiro descentralizado

O Zen é uma nova plataforma focada em instrumentos financeiros descentralizados. O Zen permite o acesso seguro a novos ativos (derivações diferentes) e ativos convencionais (como ações e títulos).

Assim como o Bitcoin retirou nossa dependência dos bancos para transferir dinheiro, o Zen remove nossa dependência dos bancos no envolvimento de finanças.

TOKENS

Os ativos são mantidos criptograficamente em uma carteira

ACS

O "ambiente de execução" do Zen, equivalente à stack de Bitcoin ou ao EVM da Ethereum.

INTEGRAÇÃO BITCOIN

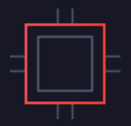
O Zen roda e atua em paralelo com o Bitcoin, como um complemento.

CONTRATOS

Substitua intermediários por mecanismos descentralizados de custódia

ORÁCULOS

Os contratos podem depender de eventos do mundo real, como o movimento dos preços no mercado de ações.



MINERAÇÃO MULTI HASH

As partes interessadas votam em quais algoritmos de hash receberão a recompensa da mineração, estabelecendo um equilíbrio entre os interesses dos mineradores e dos detentores de token.

ARQUITETURA

Tokens

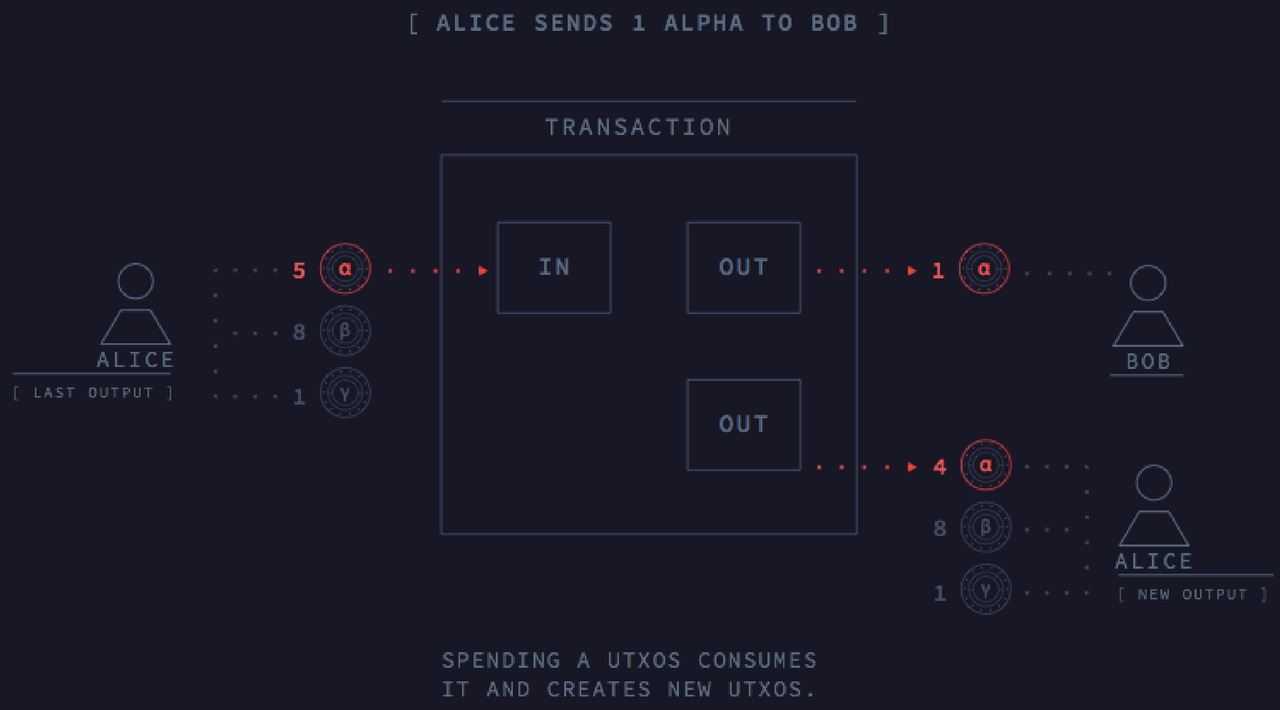
Ao contrário do Bitcoin que só tem suporte para BTC, ou Ethereum que possui contratos ERC 20, o Zen tem tokens múltiplos incorporados no nível do protocolo.

Isso significa que todo tipo de token no Zen tem um status semelhante ao seu token nativo, portanto, todos os contratos no Zen podem conter e gerenciar qualquer outro token, assim como qualquer token pode ser usado para pagar taxas de transação.

Isso é particularmente interessante porque permite que os contratos financeiros sejam denominados como moedas "normais" como o real, dólar ou euro. Os tokens são armazenados nas saídas da transação, assim como no Bitcoin, e podem ser desbloqueados com as permissões corretas e depois bloqueados novamente em novas saídas.

Tokens geralmente têm valor porque:

- As pessoas acreditam que tem valor;
- Eles são apoiados por contratos que tem garantias.



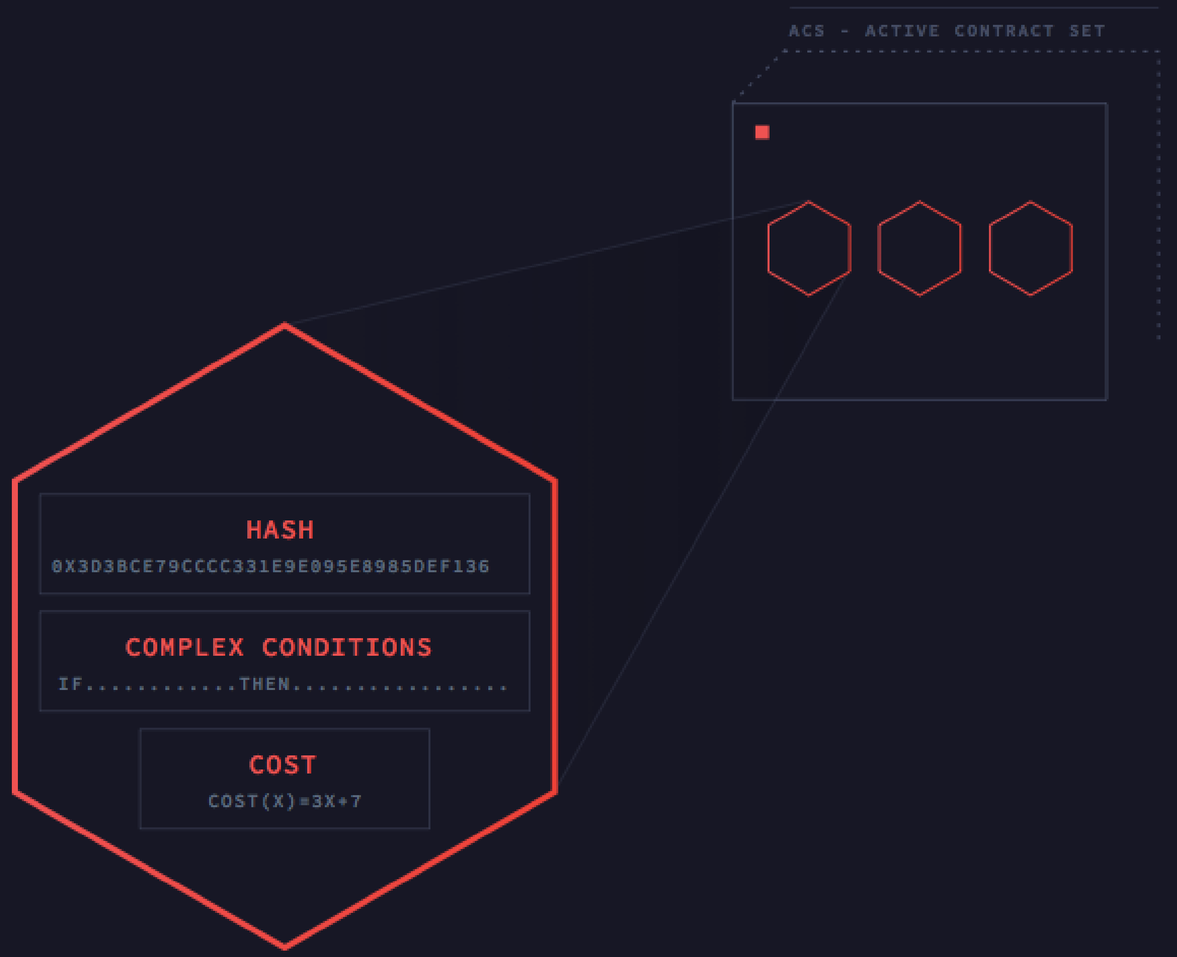
ARQUITETURA

Contratos

Os contratos são escritos em F* - Uma linguagem funcional tipada, de alto nível e formalmente verificada. A verificação formal, em conjunto com um modelo de custo, permite que todos os contratos no Protocolo Zen **especifiquem quanto tempo vão levar para seren executado santes de entrar na blockchain**.

Contratos são imutáveis (seu código nunca muda), portanto, cada contrato deve ter um único identificador matemático (um hash). Usando este hash é fácil associar tokens e verificações com um contrato.

Cada contrato fica separado do restante da blockchain. Um contrato só pode alterar seu estado da blockchain e/ou se comunicar com outros contratos, criando um UTXO (transação). Os contratos não fazem nada de forma independente, ao contrário, eles atuam com validação de dados, que é usado para auxiliar os mineradores a determinar se uma transação deve ou não ser incluída em um bloco.



[CADA CONTRATO É IDENTIFICADO PELO SEU HASH]
[CONTRATOS SÃO ESCRITOS NO NOSSO DIALETO ZF*]
[CONTRATOS SÃO ISOLADOS UNS DOS OUTROS]

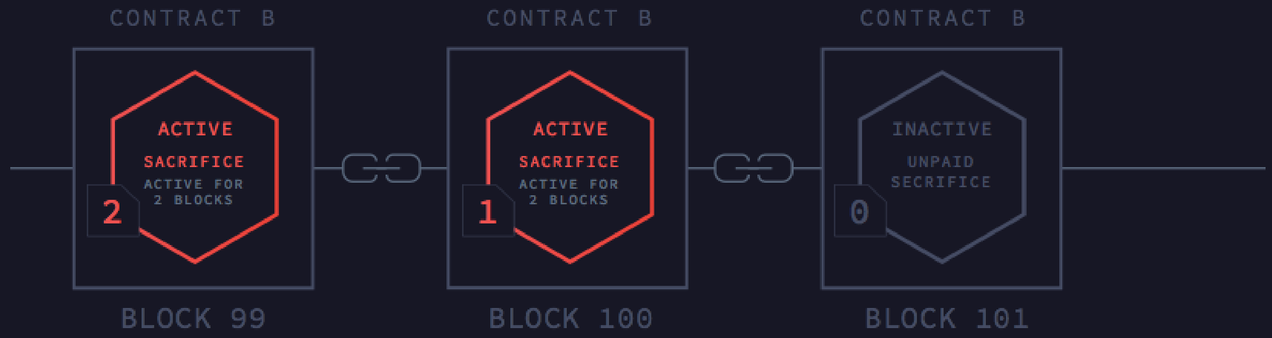
ARQUITETURA

Conjunto de Contrato Ativo

- Os contratos compilados são armazenados na RAM dos mineradores.
- Os contratos devem estar ativos para criar transações, como enviar e/ou emitir tokens.
- Qualquer pessoa pode ativar ou extender um contrato com uma oferta de contrato.

A Oferta de Contrato

- A oferta de contrato compensa os mineradores a mantê-lo. A sua taxa é dividida entre os mineradores que encontrarem blocos durante o período ativo. Oferta = Tamanho do contrato x Blocos ativos.
- Enquanto as taxas de transações podem ser pagas em qualquer token, a oferta de contrato deve ser paga em Zen.



CASO DE USO - AAPL CFD

Veja como são Tokens, Contratos e Ativos

Contratos trabalham em conjunto para facilitar o ponto-a-ponto do contrato financeiro .

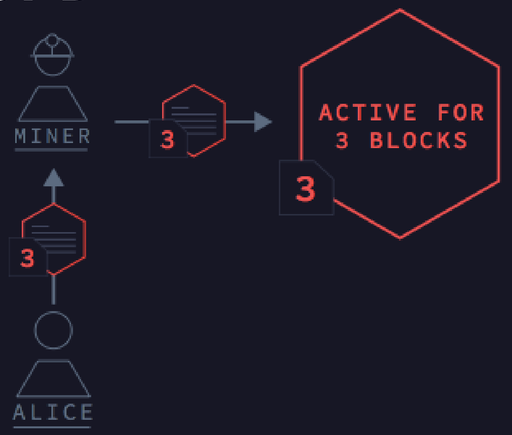
1

- **Alice escreve um contrato (CFD) na AAPL por 30 dias.**
- **Alice ganha dinheiro se a AAPL cair.**
- **Sua contraparte ganha dinheiro se AAPL subir.**

CASO DE USO - AAPL CFD

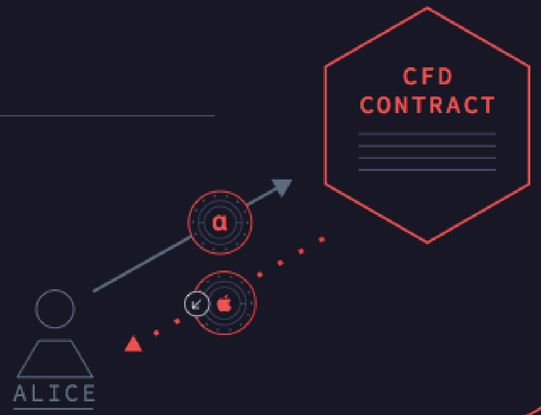
2

- Alice ativa o contrato por 3 blocos.



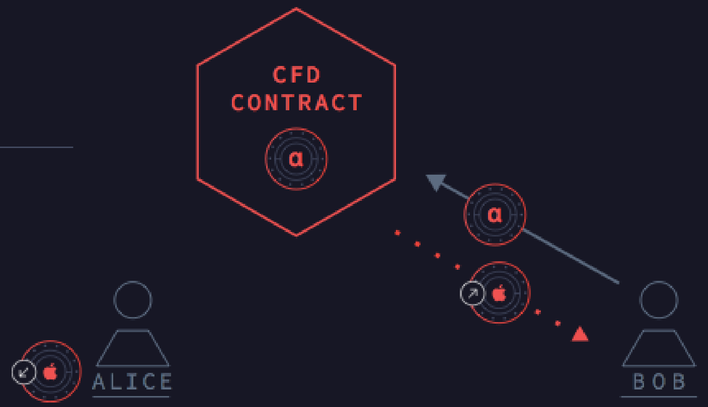
3

- Alice “colateraliza” um contrato ativo, entrando em “short position”.



4

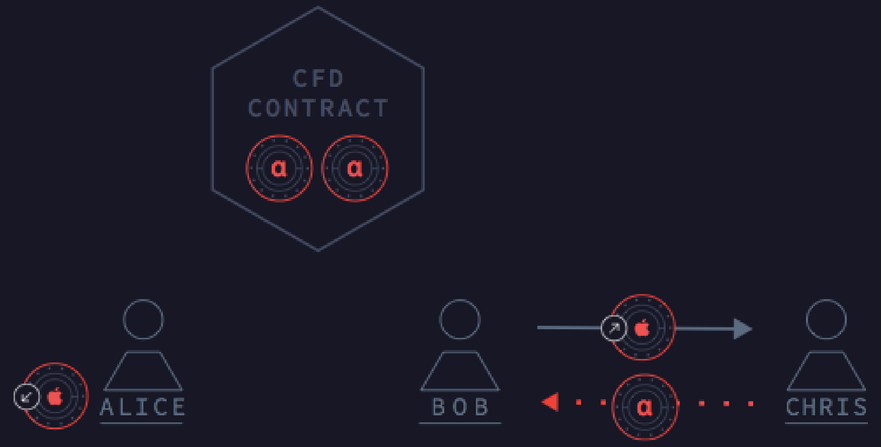
- Bob vê o contrato colateralizado e leva para a outra parte, enviando tokens.



CASO DE USO - AAPL CFD

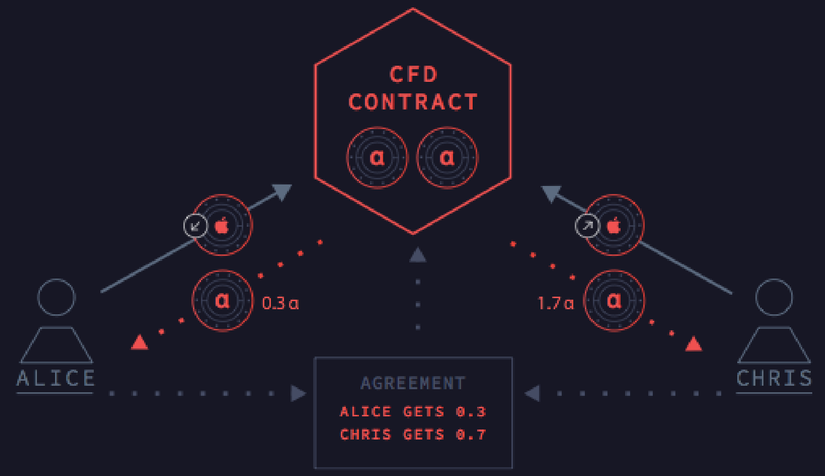
5

- O contrato fica inativo
- Bob ainda pode sair de sua posição vendendo seus tokens para outra pessoa.



6

- Após 30 dias, o contrato precisa ser reativado para retirar os fundos de garantia.
- Se Alice e Chris concordarem com a AAPL acima de 70%, eles assinam uma transação onde Alice obtém 0,3α e Chris recebe 1,7 α



MAS E SE ALICE NÃO CONCORDAR?

INTRODUZINDO ORÁCULOS

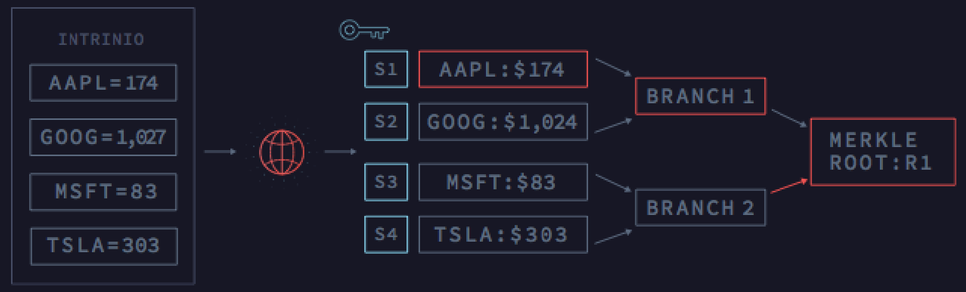
Oráculos permite operar contratos no mundo real

Os contratos indicam antecipadamente qual(is) oráculo(s) será(ão) invocado(s) para fornecer dados ao contrato.

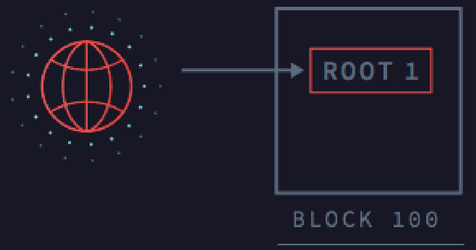
Contratos legais usam cartórios para serem arbitrados, contratos inteligentes usam oráculos e são arbitrados na blockchain.

Como os oráculos trabalham:

1 **Os oráculos puxam dados das APIs da web e classificam-nas em uma árvore de Merkel, em cada folha é incluído um segredo/nonce.**

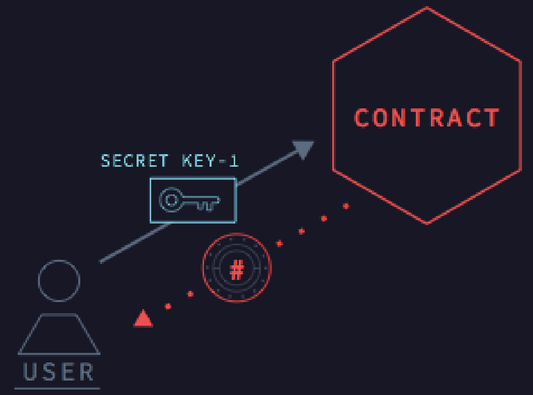


1 **O Oráculo insere a raíz de Merkel na Blockchain**



2 **Quando um usuário precisa fornecer o contrato com uma folha específica / peça de dados (ex.: resolver uma disputa), o usuário paga o oráculo e o oráculo revela o nonce.**

3 **Usando o nonce, o usuário pode provar ao contrato o preço comprometido e retirar seus fundos.**

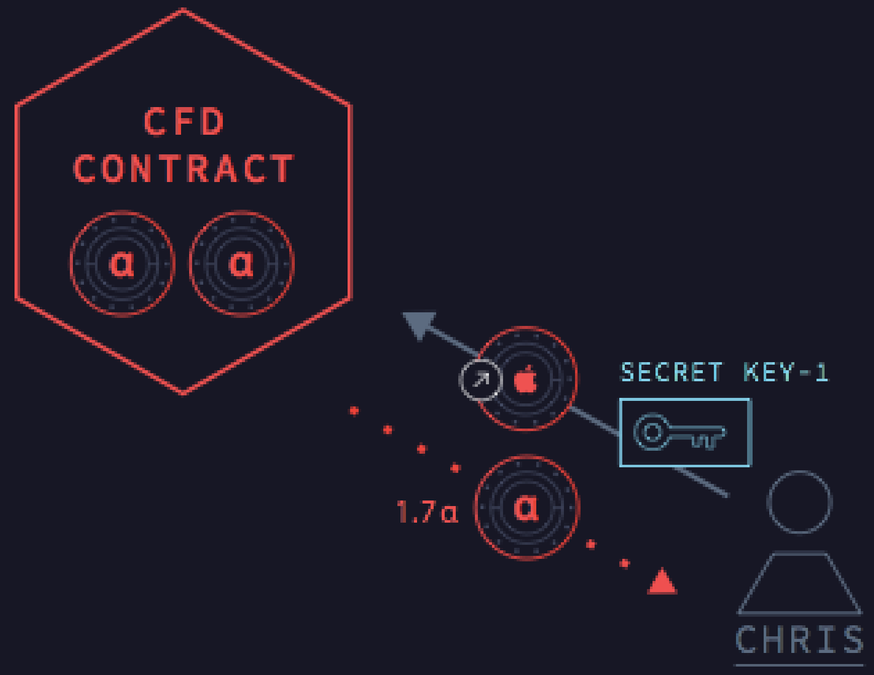


CONTINUAÇÃO DO CASO DE USO - AAPL CFD

Resolução de disputa

Então, no caso de Alice e Chris não concordarem, Chris irá pagar o oráculo para lhe fornecer o segredo (S1).

- Chris então envia o segredo e a opção de compra do contrato , o contrato paga à Chris 1.7 alpha.



INTEGRAÇÃO BITCOIN

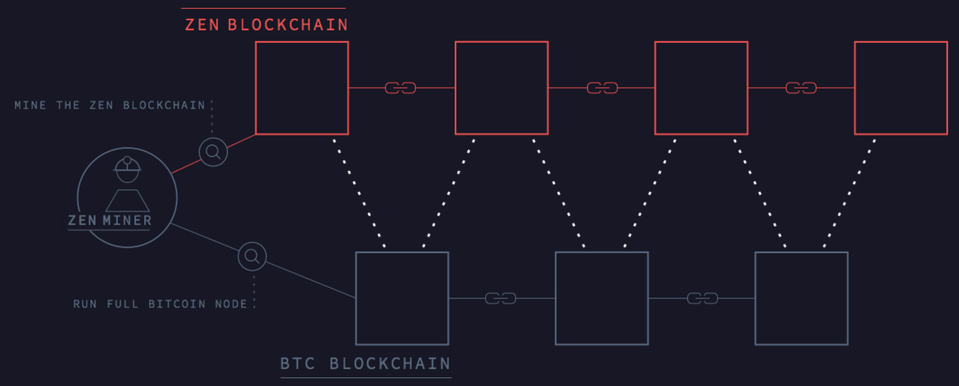
Os últimos esforços para aumentar a complexidade nos sistemas 'blockchain' seguiramduas estratégias:

1 **Criar uma cadeia de blocos alternativa com o uso de uma AltCoin**

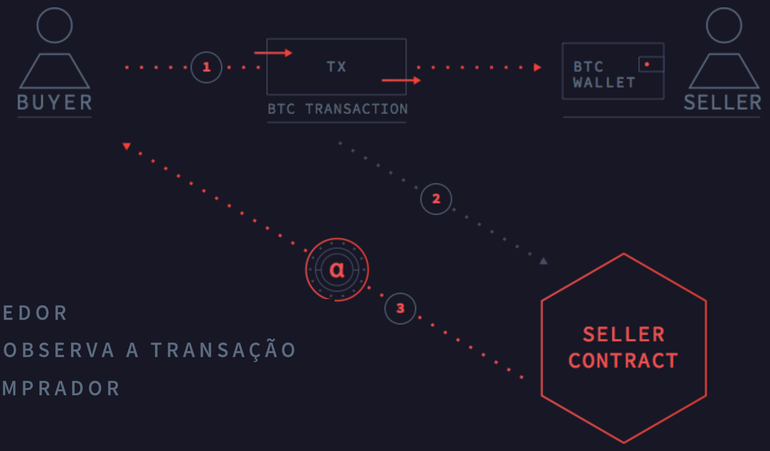
2 **Criar um protocolo suplementar que não possui um token proprietário e, portanto, diferente dos mecanismos de incentivo/segurança do Bitcoin.**

O Zen adota uma nova abordagem, uma cadeia de blocos separada com seu próprio token, que é executado em paralelo à rede Bitcoin.

Consenso mesclado - Mineradores Zen mineram a Blockchain do Zen e observam a Blockchain do Bitcoin. Isso permite a funcionalidade de uma cadeia cruzada.



Cadeia de contrato cruzado - A garantia é realizada na cadeia Zen, mas a recompensa é paga a um endereço de Bitcoin.

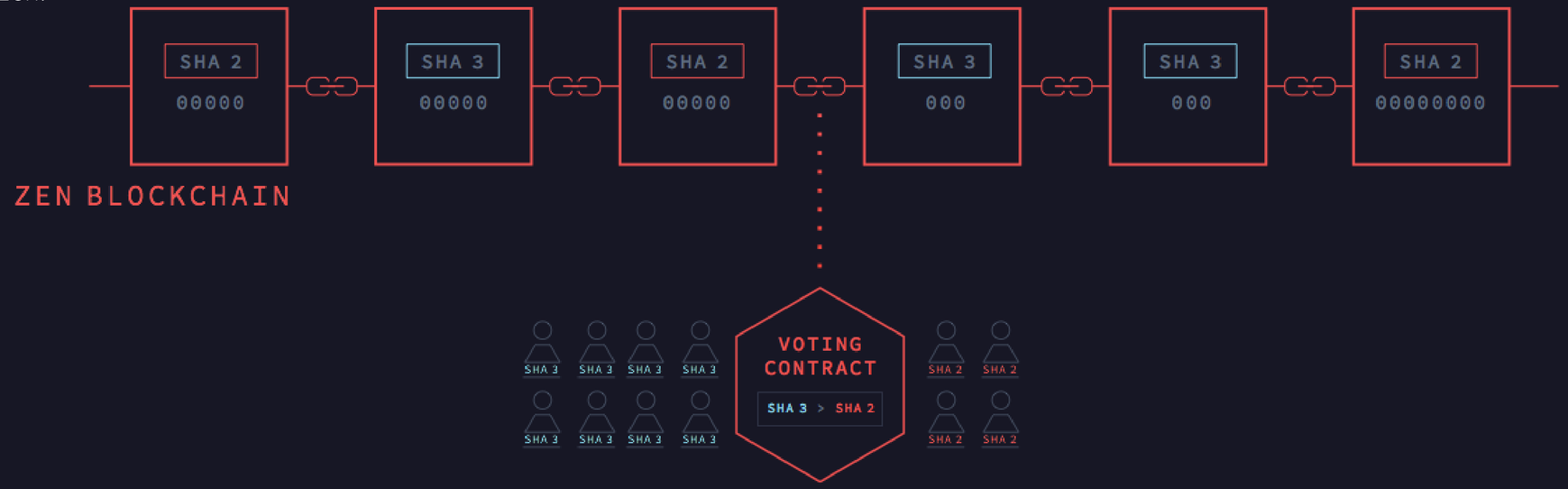


1. COMPRADOR ENVIA BTC AO VENDEDOR
2. O VENDEDOR DO CONTRATO ZEN OBSERVA A TRANSAÇÃO
3. CONTRATO ENVIA TOKENS AO COMPRADOR

ZEN

Mineração Multi Hash – democracia representativa

- Diferentes funções de hash podem ser usadas para encontrar um bloco.
- Cada função de hash tem um requisito de dificuldade diferente.
- O tamanho dos blocos gerados em cada função de hash é estabelecida pelos proprietários de token Zen.



ROTEIRO


Ideia formalizada
3º Trimestre de 2016
4º Trimestre de 2016
A tecnologia é escolhida
Modelo de custo completo
1º Trimestre de 2017
2º Trimestre de 2017
Contratos inteligentes e oráculos em C#
Refatoração de contratos de desenvolvimento
3º Trimestre de 2017
4º Trimestre 2017
Alfa
Lançamento do produto
1º Trimestre de 2018
2º Trimestre de 2018
Bloco Genesis
Construção do ecosistema
3º Trimestre de 2018

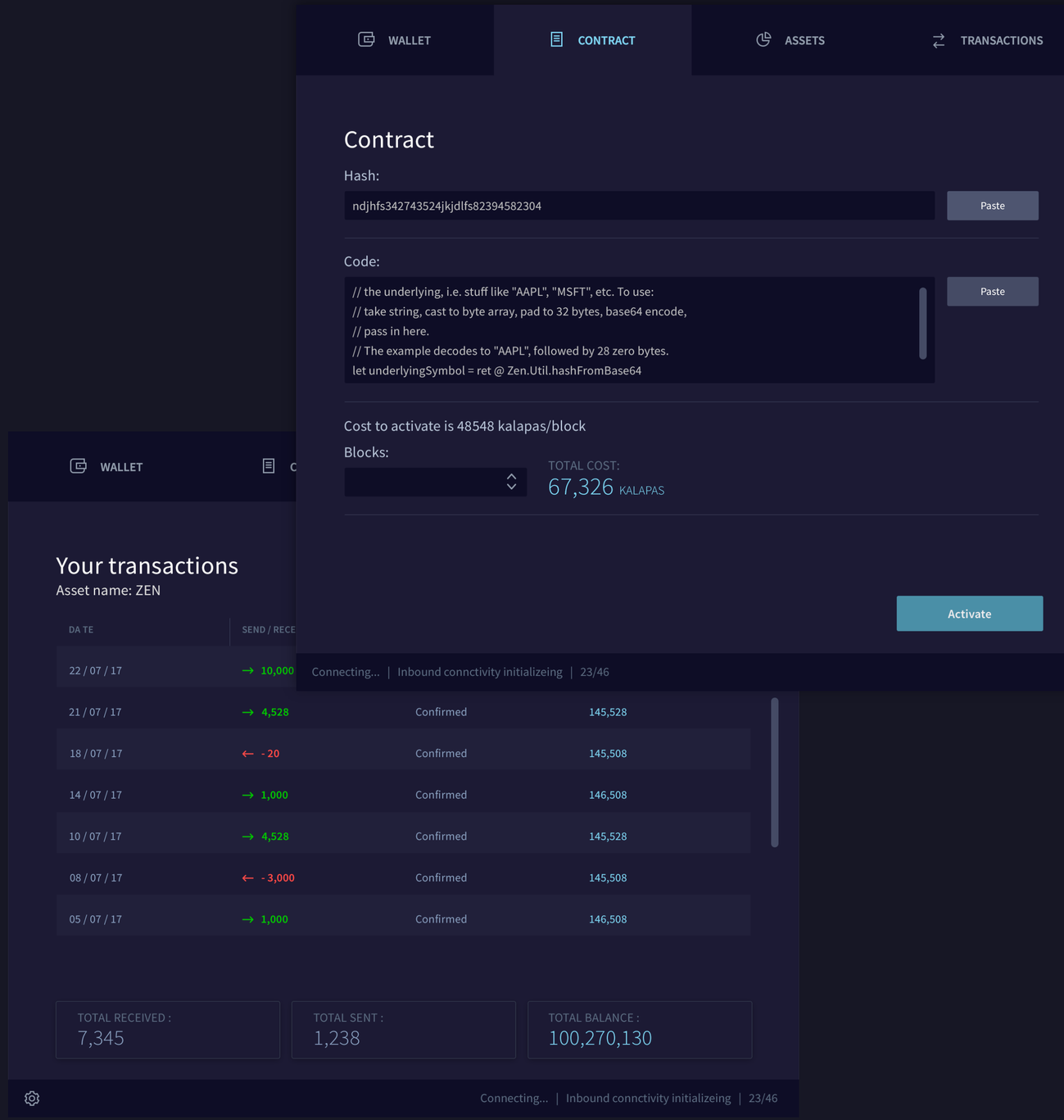
ZEN

Alfa

Atualmente, temos um alfa funcional com uma blockchain construída a partir do zero, implementação de ACS, contratos inteligentes escritos em F* que comprovam seu custo e oráculos buscando preços de ações da intrinio.com

Zen Alfa

DOWNLOAD



EQUIPE ZEN

Nós somos uma equipe pequena construindo um grande roduto

Adam Perlow

CEO

Adam é graduado em finanças na IDC, reservista do exército israelense e um velho holder de Bitcoin. Ele sabia o que estava acontecendo desde o dia em que ouviu falar sobre isso, lá atrás em 2011.

Nathan Cook

CTO

Pós-graduadoo em matemática pela Universidade de Cambridge. Ele descreve seu trabalho: “Participar ao máximo, com toda a sua existência.”

Sharon Urban

Desenvolvedor Chefe

Sharon é um engenheiro de sistemas altamente qualificado e experiente que adora trabalhar com boas pessoas!

Asher Manning

Desenvolvedor, Métodos formais

Ash estudou Matemática, Física e CS na Universidade McGill e trabalhou pesquisando "Homotopy Type Theory".

EQUIPE ZEN

Nós somos uma equipe pequena construindo um grande roduto

Doron Somech

VP R&D

Doron é co-funddador e CTO da leverate.com

Elan Perach

Líder de Produto

Elan iniciou várias startups, ex-aluno da NFX.com, está na área de criptografia desde 2011 e construiu o primeiro site para vender bitcoin em Israel.

Eleanor Milstein

Diretora de Arte

Eli é a nossa guru no design de produtos, trazendo 6 anos de experiência de várias startups tanto como designer de produto quanto como co-fundador.

Isaac Rodgin

Gerente de Comunidade

Graduado em IDC Herzliya, com licenciatura em negócios e Ciência da Computação. Com mais de 5 anos em Gestão de comunidades e Vendas.

CONSULTORES

Pamir Gelenbe

Pamir é sócio-gerente da Libertus Capital, onde se concentra em sistemas descentralizados, blockchains empresariais e moeda digital. Ele é investidor nas instalações Kraken, Ledger Wallet, Shapeshift e Crypto Facilities e vários protocolos descentralizados. Anteriormente, ele atuou como parceiro da Hummingbird Ventures e também trabalhou na Morgan Stanley e D.E. Shaw. Pamir se formou na Universidade Duke e na Universidade de Columbia como Bacharel em Engenharia Elétrica e Mestrado em Pesquisa de Operações.

Ran Nussbaum

Ran Nussbaum é sócio-gerente e co-fundador do The Pontifax Group. O fundo funciona com mais de 50 empresas de portfólio em todo o mundo. Antes de se juntar a Pontifax, ele era parceiro da maior empresa de consultoria estratégica e de inteligência de negócios de Israel.

Ron Gross

Ron se formou no Technion como Mestre em Ciência da Computação. Trabalhou em várias empresas, desde pequenas startups até o Google, possui uma vasta experiência em arquitetura web, segurança e algoritmos. Ron esteve envolvido continuamente com o Bitcoin desde março de 2011, divulgando a palavra, o conhecimento e o amor pelo Bitcoin. Ele é um firme defensor de código aberto, transparência e descentralização do poder e da tecnologia. Ron é co-fundador da comunidade Israelita de Bitcoin além de Fundar e ter sido Diretor Executivo da Fundação Mastercoin (a primeira ICO do mundo).