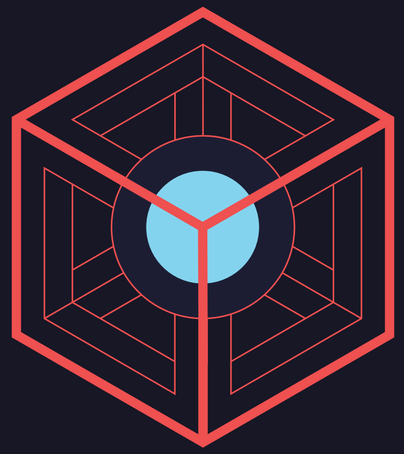


ZEN

ZEN 一个去中心化的金融系统

摘要

一个纯粹的点对点机制，用于构建契约关系，允许相互不信任的参与者制定合约，而不依赖法律系统进行纠纷调解。这些协定被称为“智能合约”，通过代码形式提交数字合约，通过在公共去中心化的网络执行上述的代码来解决纠纷。

现有的平台缺少可靠地执行金融合约的功能或者安全性。Zen是一个新的智能合约平台，能够创建、促进和决议合同义务。基于比特币范式（UTXO验证），我们通过使用一种用于形式验证的函数式语言ZF*，来表述和验证合约资源消耗的边界证明。在Zen系统，所有的代币都是“一等公民”，支持多重资产，并通过观测比特币网络来促进互操作性

动力

从2014年开始，Zen协议的核心团队就开始从事区块链领域的工作，经过多年的研究之后，在2016年六月开始Zen协议的开发。

促使Zen愿景产生的动力是，我们相信人们有权拥有他们自己的金融资产，并且我们有责任提供给大家必要的工具使之成为可能。

Zen提供给人们一个口袋里的“瑞士银行”。使用密码学在去中心化的网络中创建、交易和存储常见的金融资产，如股票、债权和衍生资产。

问题

传统金融

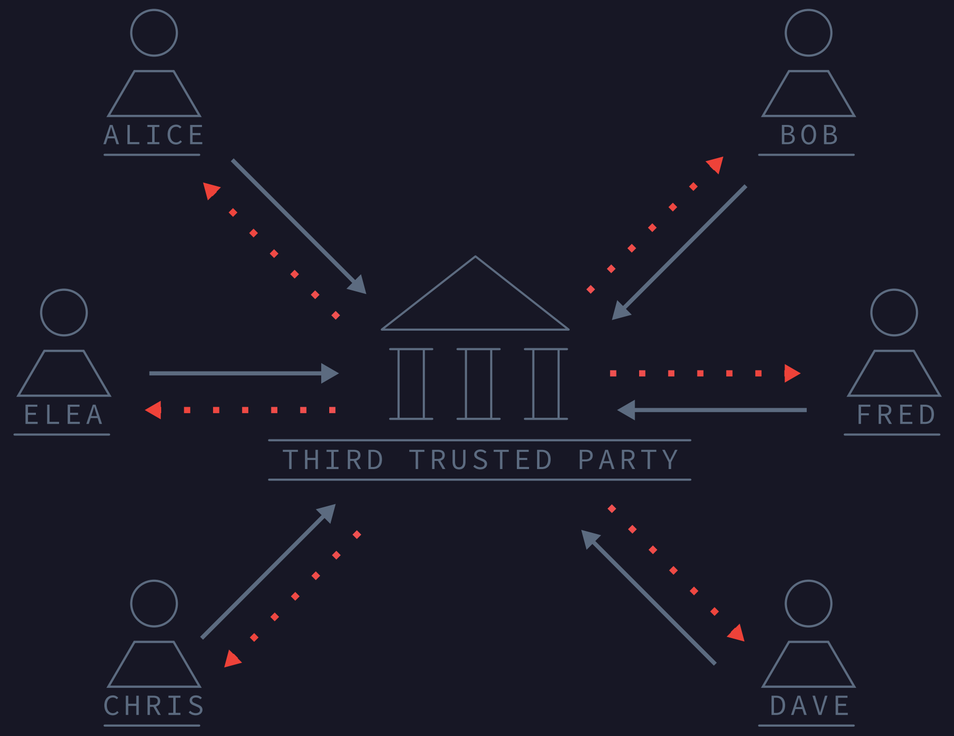
我们将金融机构视为受信任的中介机构，而不是为了暴露交易风险。这些金融机构促进了大多数的经济交易，却限制了我们的自由:

- **访问限制**

  访问限制金融机构限制了谁可以访问金融系统，并且他们在金融系统中可以做什么。

- **所有权限制**

  我们并不真正拥有我们的资产，而是拥有来自银行的债务。由于破产或征用，银行可能不履行债务。



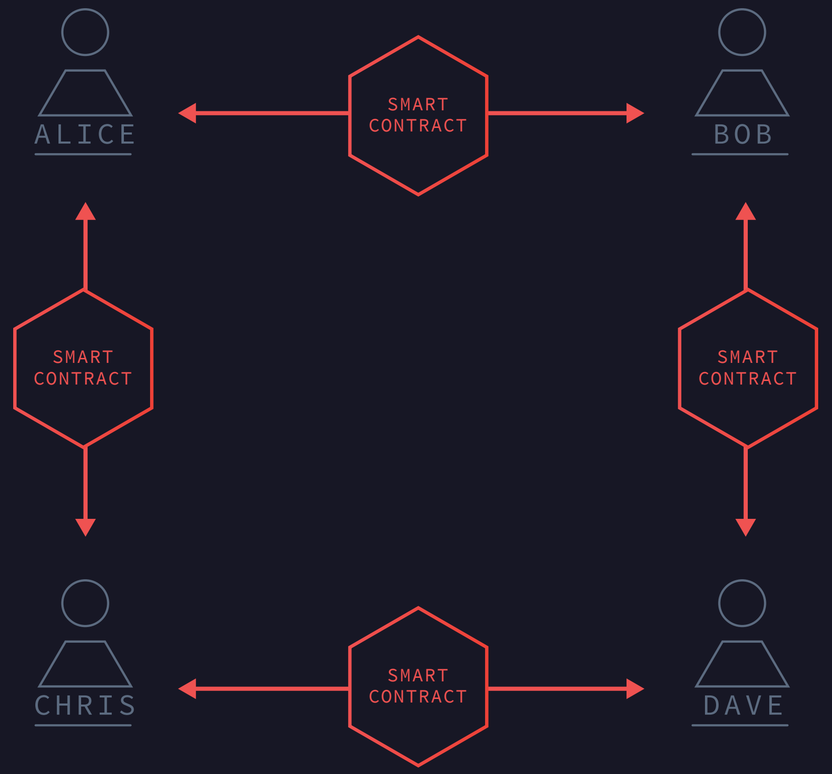
解决方案

去中心化的金融系统

如果我们消除对第三方的依赖，我们就可以收回资产的所有权和自由，从而根据自己的意愿参与金融活动。我们将会拥有更多高效率的市场，伴随的是更少的繁文缛节和费用。

使用比特币技术，我们可以创建一个去中心化的金融系统

一个专门用于金融的新的区块链，使得我们能够拥有加密过的资产，使用智能合约将这些资产产生的资金流强制执行。



解决方案

为此目的，我们创建了一个新的区块链

目前市场上充斥着各种各样中心化的金融服务和去中心化的非金融区块链应用。目前还没有人意识到区块链技术应用于去中心化金融服务中的潜力。Zen试图填补这一市场空白。

我们真的需要另外一个区块链吗?

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

比特币

比特币是去中心化的货币

我们相信比特币是货币的终极形式。Satoshi选择限制比特币的功能，从而更好地服务于货币这一角色。Satoshi认为，“将世界上所有的工作量证明的仲裁系统堆成一个数据集不易于扩展。”

比特币缺少金融服务所需的功能

我们需要一个新的去中心化金融区块链，能够支持多重资产和复杂所有权构建。

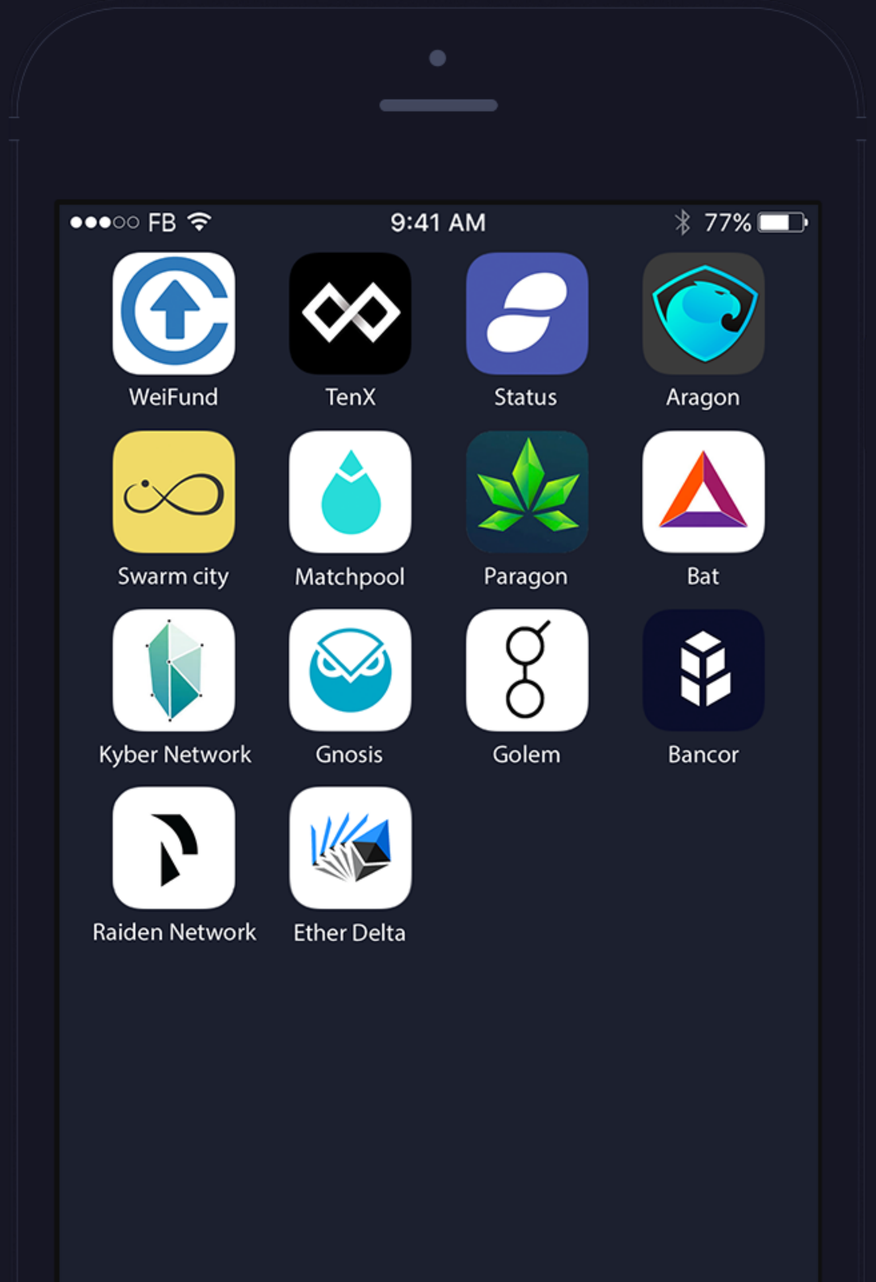
THERE ARE AN ESTIMATED 21M BRICKS (400 OZ PER BRICK) OF GOLD IN THE WORLD

以太坊

以太坊是一个去中心化计算平台

Ethereum的目标是成为一个开发去中心化应用的平台，例如没有中央服务器的Facebook或Uber。Ethereum是一个专注于开发者的平台，提供了方便的编程语言(Solidity)和接口(ABIs)。

为了实现这一功能，Ethereum提供了以太虚拟机(EVM)，进行周期数的计算，使用“瓦斯”系统。



ZEN

Zen是一个去中心化的金融平台

Zen是一个专注于去中心化金融工具的平台。Zen能够使人们无需许可就可以访问新式资产（如复杂衍生物）或者传统资产（如股票和债券）。

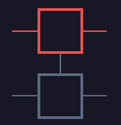
比特币不依赖于银行实现价值的转移，于此类似，Zen也不依赖于银行参与到金融服务之中。

代币

资产被加密存储在钱包中。

Zen的“执行环

境”，等同于比特币的协议栈或者以太坊的EVM。



比特币集成

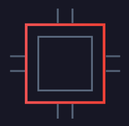
Zen并行运行，且向比特币网络致意

合约

通过去中心化担保机制取代中介机构。

预言机

合约可以依赖于真实世界的事件，如股票市场价格的波动。



多哈希挖矿

利益相关者投票决定使用哪种哈希算法来获取挖矿奖励，从而平衡矿工和代币持有者的利益。

架构

代币

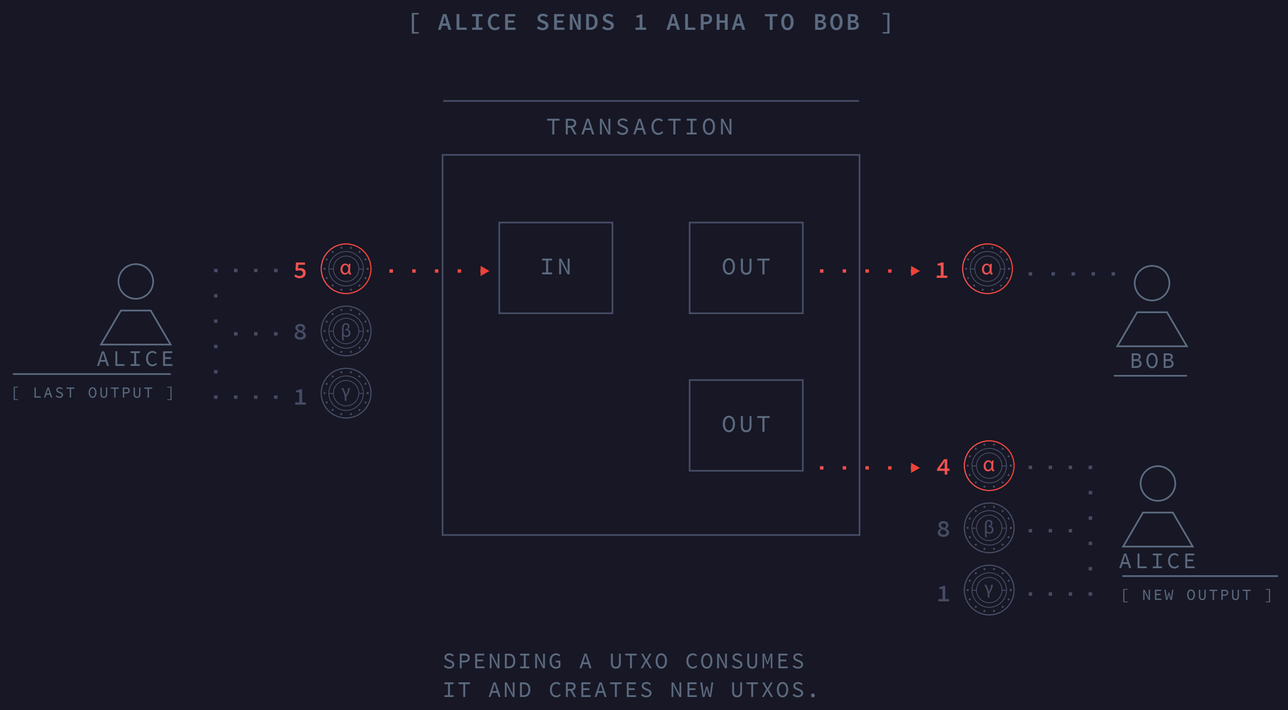
不同于比特币仅支持BTC，以太坊拥有ERC 20 合约，Zen在协议层就支持构建多重代币。

也就是说，Zen网络中每一种代币和Zen的原生代币拥有相同的状态，因此Zen中所有的合约都能够承载和管理任何其他代币，并且任何代币都可以用来支付交易费用。

这是非常有趣的，因为它允许以“正常”货币(如美元或欧元)计价的金融合约。代币存储在交易输出中，和比特币一样，通过使用正确的权限进行解锁，然后锁定在新的交易输出中。

代币通常保有价值，因为：

- 人们相信它们拥有价值
- 代币由持有抵押物的合约背书



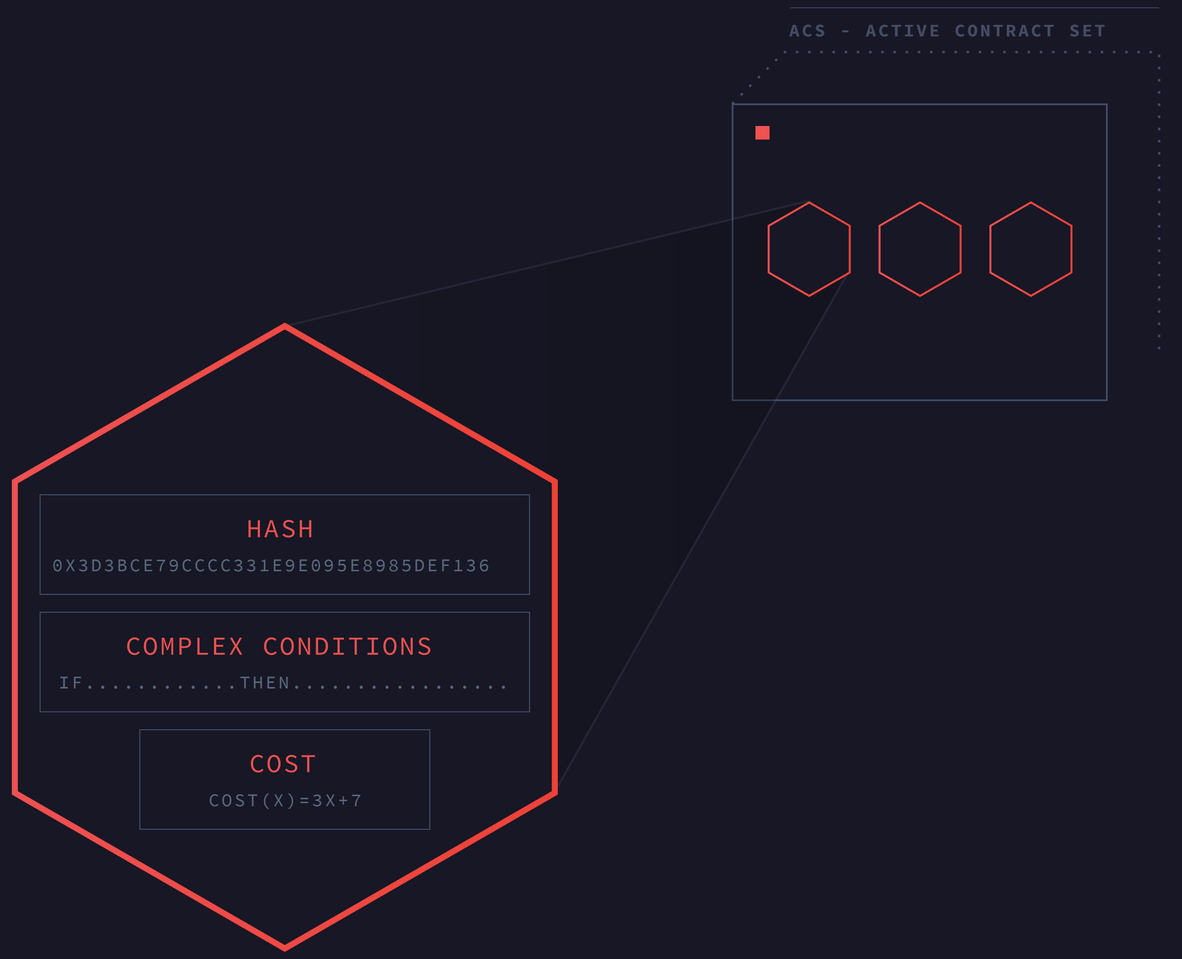
架构

合约

合约由F*语言编写，它是一种函数式、强类型、高级别、形式验证过的语言。形式验证，再加上成本模型，使Zen协议中的合约在进入区块链之前就这能证明将会运行多长时间。

合约是不可改变的(合约代码从不更改)，因此每个合约都有一个惟一的数学标识符(哈希值)。使用这一哈希，很容易将代币和证明与契约联系起来。

合约存在于和区块链的其余部分相隔离的区域。合约只能改变区块链的状态，或者通过创建一个UTXO(交易)与其他合约进行通信。合约不独立做任何事情，而是作为验证数据，用于帮助矿工确定是否应该将某一交易包含在区块中。



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

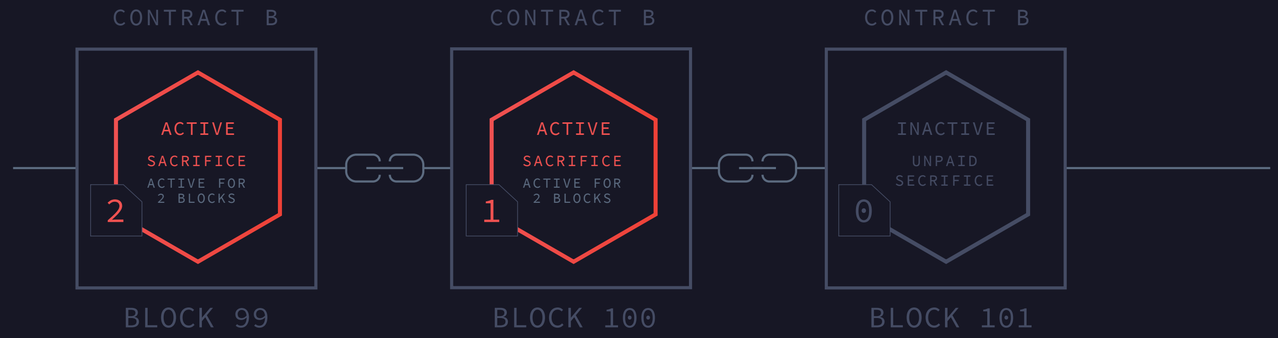
架构

有效合约集

- 激活合约从F*代码转换为机器码。
- 编译后的合约存储在矿工的RAM中。
- 有效合约才能创建交易，如发送和发行代币。
- 任何人都可以通过合约牺牲激活或者扩展一个合约。

合约牺牲

- 合约牺牲补偿了维持合同运行的矿工。这些牺牲的代币被分给那些在合同有效期找到区块的矿工们。
  牺牲数额 = 合约大小 X 有效区块
- 虽然交易费用可以以任何代币进行支付，但合约牺牲必须用Zen支付。



使用案例 - AAPL CFD

让我们看一下代币、合约和有效合约集如何合作促进点对点金融合约。

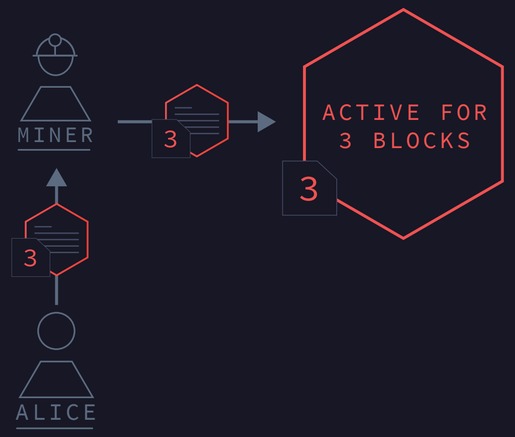
1

- Alice 编写了一个为期30天的AAPL差价合约（CFD）
- 如果AAPL价格下跌，那么Alice将会获利如果AAPL价格上涨，那么合约对手方将会获利

使用案例 - AAPL CFD

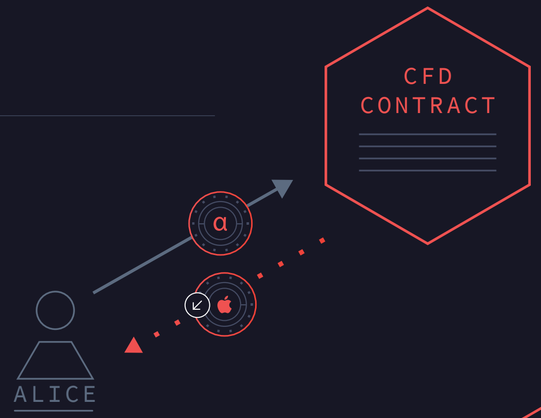
2

- Alice选择在3个区块内激活合约



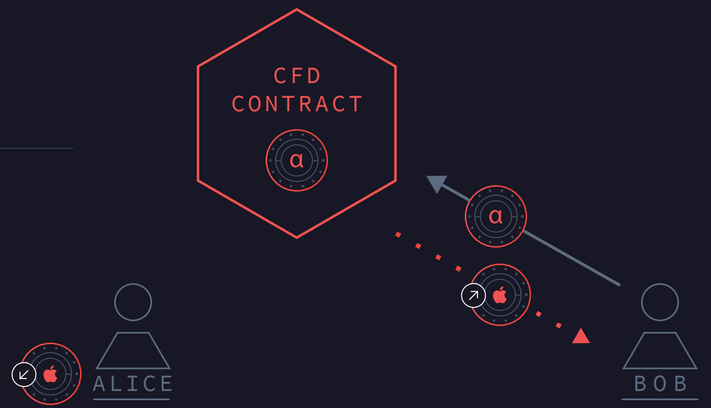
3

- Alice“抵押”有效合约，进入空头。



4

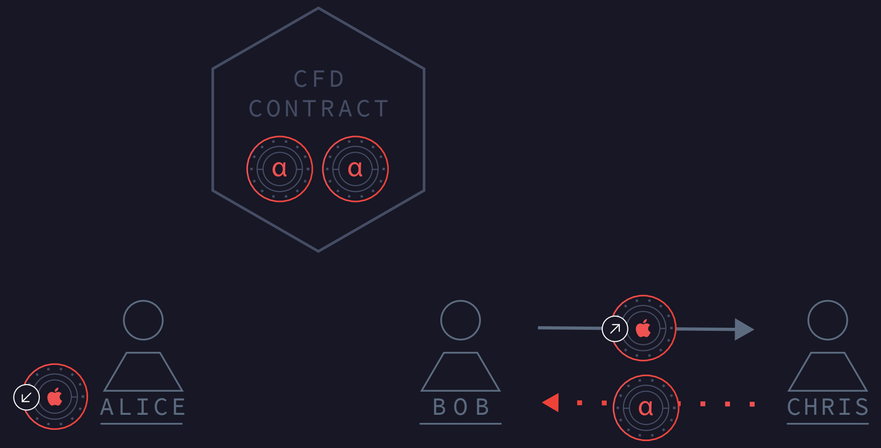
- Bob看到抵押过的合约，通过发送代币选择多头。



使用案例 - AAPL CFD

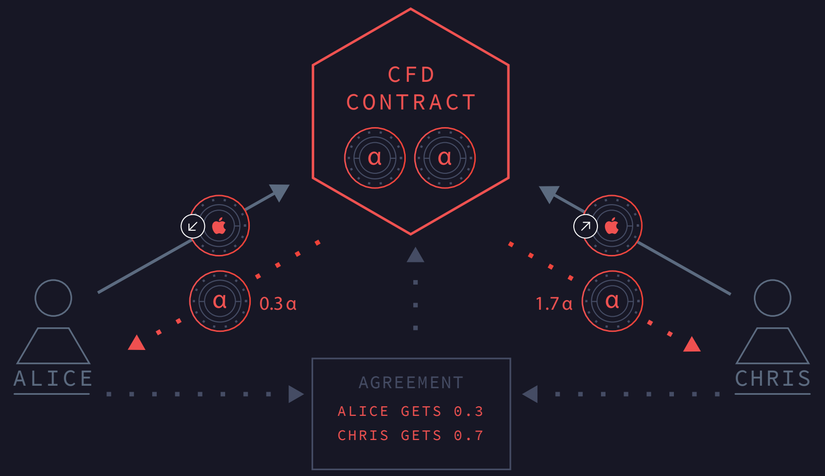
5

- 合约变为无效
- Bob仍然可以通过出售他的代币给他人，退出他所在的位置。



6

- 30天后，合约需要被重新激活，从而收回托管的资金。
- 如果Alice和Chris达成一致AAPL上涨 70%，那么他们签署一项交易，Alice获得0.3倍和Chris得到1.7倍。



但是，如果Alice不合作呢？

预言机介绍

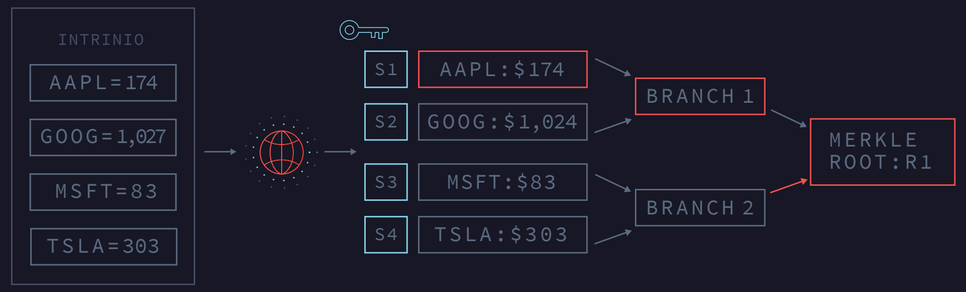
预言机允许合约基于真实世界的数据运转。

合同状态将依赖预言机为合同提供数据。

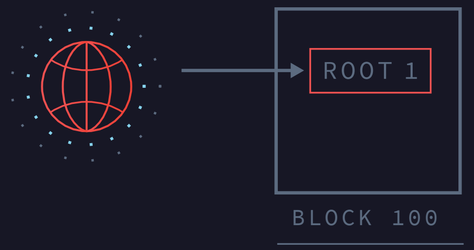
法律合约通过法官，在法庭上进行仲裁，智能合同使用预言机，并在区块链上面进行仲裁。

预言机如何工作：

1 预言机从web API提取数据，并将其排序为Merkel Tree，每个叶子节点都由一个秘钥或者随机数进行盐化。

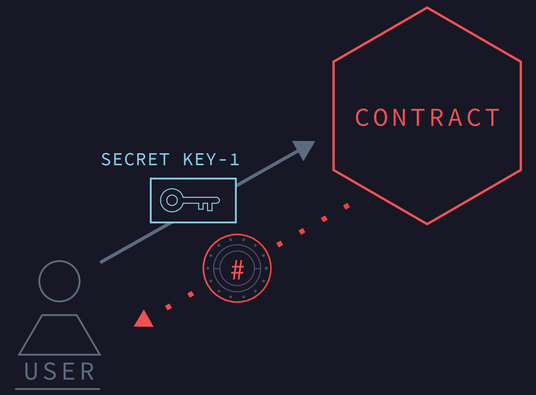


1 The Oracle inserts the Merkle Root to the blockchain.



2 当用户需要用特定的叶节点或数据（如用于解决争端）时，用户需要向预言机支付费用，预言机才会显示随机数。

3 用户可以使用这一随机数向合约证明承诺的价格是什么，并取出资金。

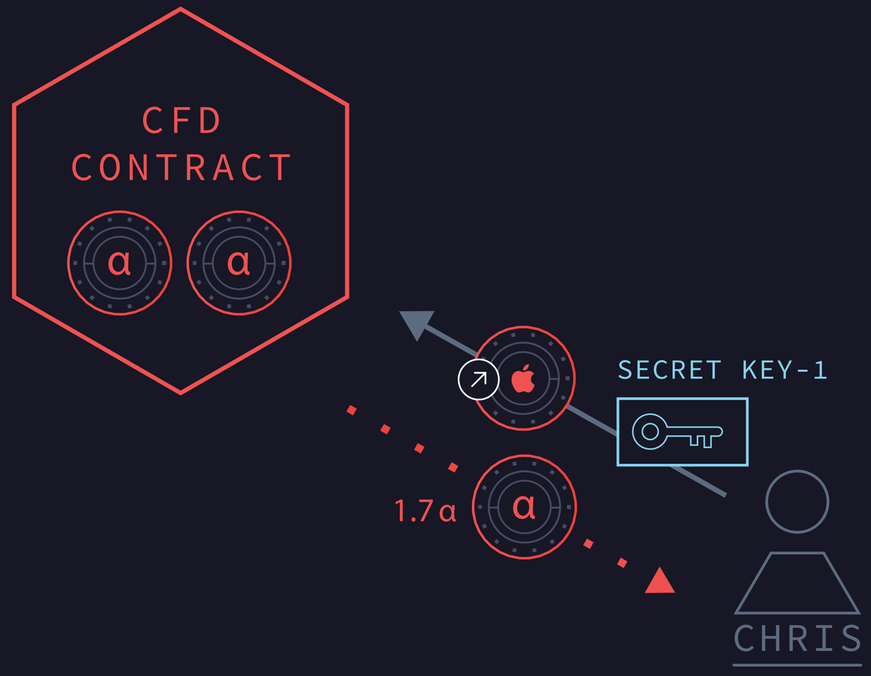


使用案例-AAPL CFD延伸

争议解决

因此，在Alice和Chris无法达成一致的情况下，Chris将通过向预言机支付费用，从而获取预言机提供的秘钥(S1)。

- 之后Chris向合约发送秘钥和看涨期权，合约支付给Chris 1.7倍率投资资金。



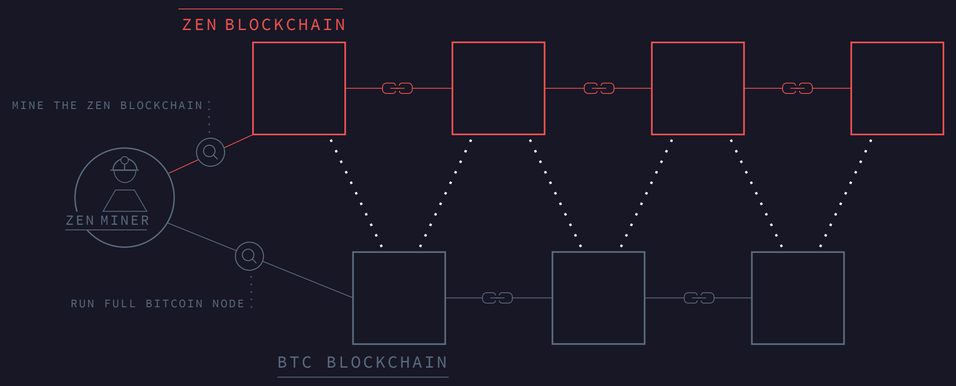
比特币集成

过去为了在区块链系统中增加复杂性的，采取了以下两种策略:

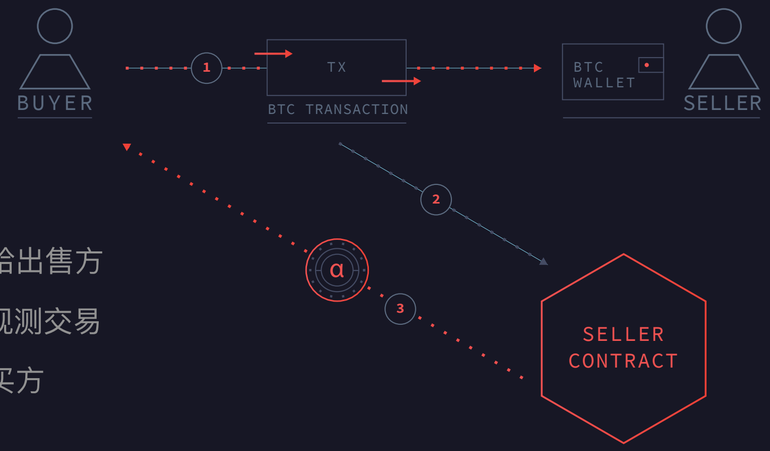
1. 创建一个必须使用其它代币的替代区块链。
2. 创建一个补充协议如侧链，缺乏一个专有的代币，因此不同于比特币的激励/安全机制。

Zen采用了一种新的方法，即一个拥有自己代币的独立区块链，并与比特币网络并行运行。

融合共识 - Zen矿工生产Zen的区块链，并观测比特币区块链，从而允许了跨链功能。



跨链合约 - 抵押品包含在Zen区块链中，但它的溢价支付给比特币地址。

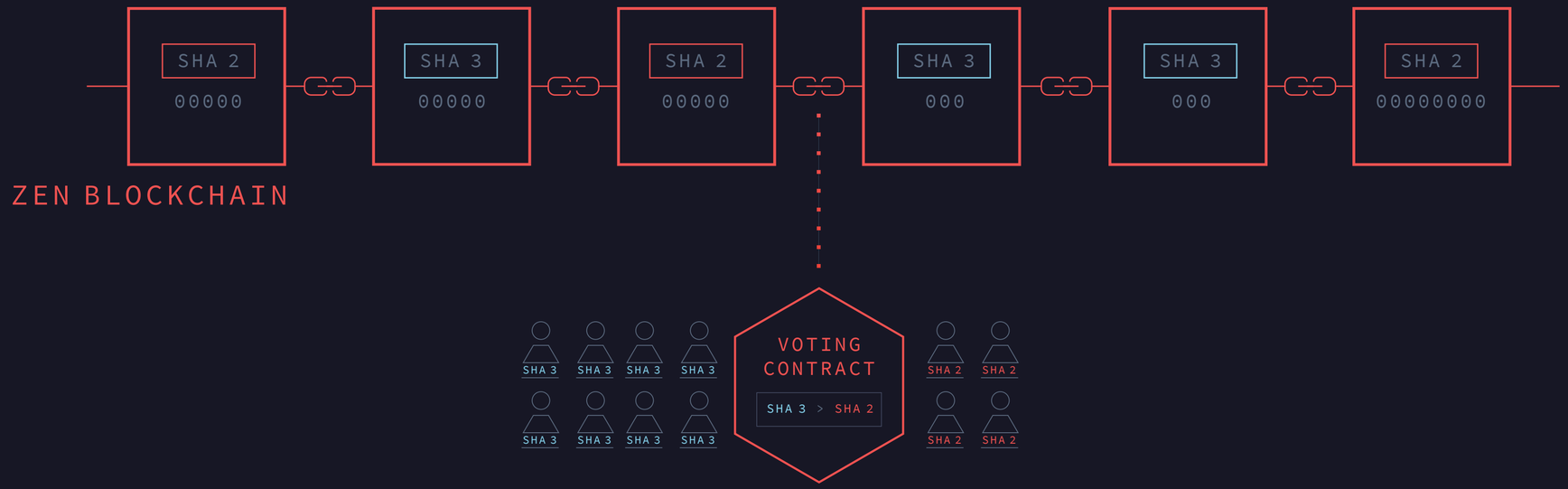


1. 购买方发送比特币给出售方
2. 出售方的ZEN合约观测交易
3. 合约发送代币给购买方

比特币集成

多哈希挖矿 - 代议制民主

- 可以使用不同的哈希函数生产区块
- 每个哈希函数都有不同的难度要求。
- 每个哈希函数生成区块的目标比率是由Zen代币持有人投票决定的。



ROADMAP


想法正式形成
Q3 2016
Q4 2016
技术栈选择完成
成本模型完成
Q1 2017
Q2 2017
用C#编写智能合约和预言机
重构、开发合约
Q3 2017
Q4 2017
Alpha
发布候选版本
Q1 2018
Q2 2018
起源区块
建立生态系统
Q3 2018

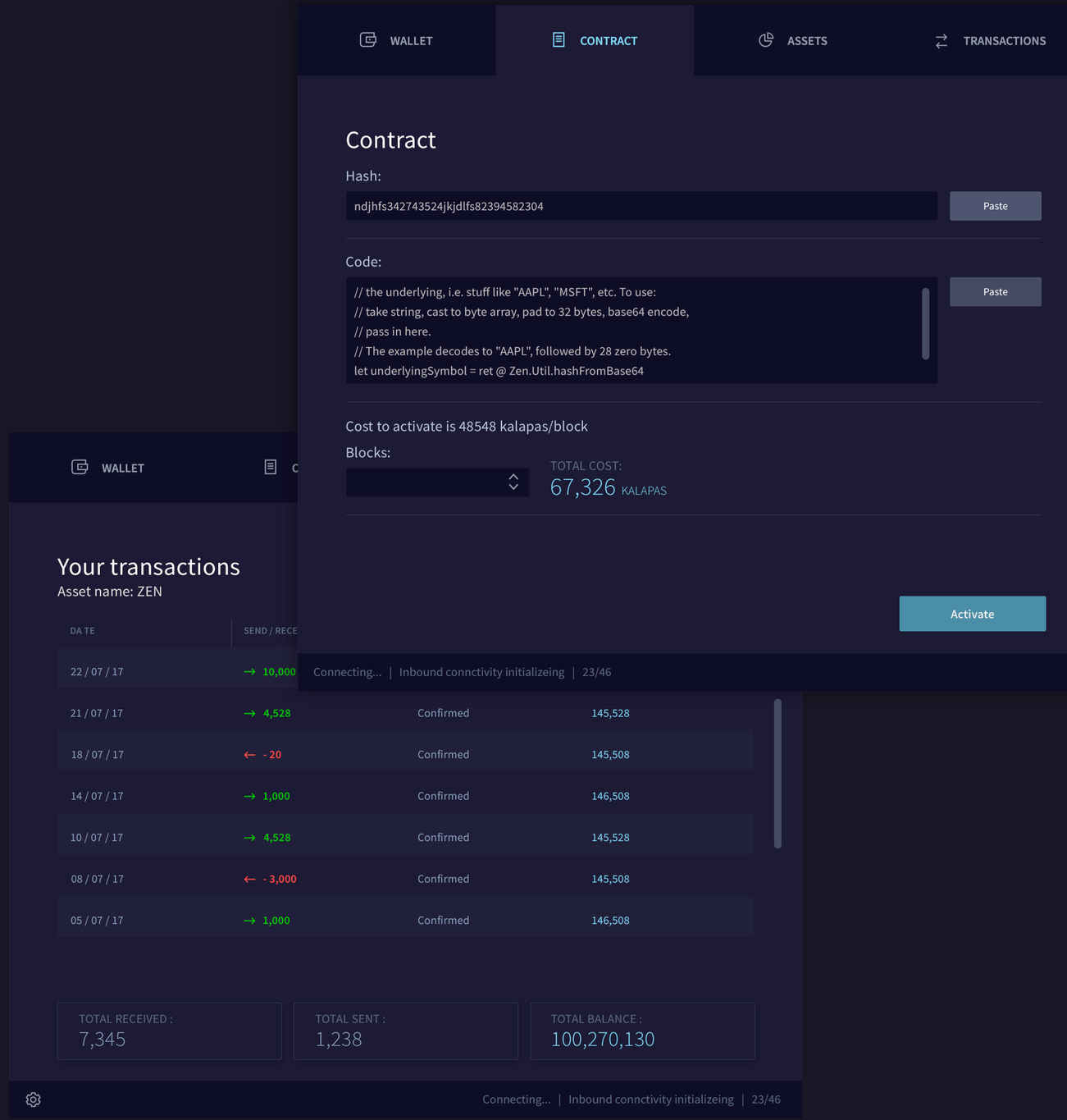
ZEN

我们现在有

一个运行的alpha版本，它是一个从头开始构建的区块链，实现了ACS，使用能够完成成本证明的F*语言编写智能合约，以及从intrinio.com获取股票价格的预言机。

Zen Alpha

DOWNLOAD



ZEN TEAM

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

Adam Perlow

CEO

Adam is a finance grad from the IDC, an Israeli army reservist, and an old hand in Bitcoin. He’s known it was going places since the day he first heard about it, way back in 2011.

Nathan Cook

CTO

A former maths postgrad from Cambride University. He describes his job: “taking part in capital bringing itself into existence”

Sharon Urban

Lead Developer

Sharon is a highly skilled and experienced systems engineer who loves working with the good guys!

Asher Manning

Developer, Formal methods

Ash studied Maths, Physics & CS at McGill University and worked on research in Homotopy Type Theory.

ZEN TEAM

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

Doron Somech

VP R&D

Doron, was the co-founder and CTO of leverate.com

Elan Perach

Head of Product

Elan has started multiple startups, an NFX.com alumni, has been in the crypto space since 2011, and built the first website to sell bitcoin in Israel.

Eleanor Milstein

Art Director

Eli is our product design guru, bringing 6 years of experience from several startups both as a product designer and as a co-founder.

Isaac Rodgin

Community Manager

Graduated from IDC Herzliya, with both Business and Computer Science degree. With over 5 years in Community Management and sales.

ADVISORY

Pamir Gelenbe

Pamir is a Managing Partner at Libertus Capital where he focuses on decentralised systems, enterprise blockchain, and digital currency. He is an investor in Kraken, Ledger Wallet, Shapeshift, and Crypto Facilities, and several decentralized protocols. Previously, he served as a Partner at Hummingbird Ventures, and also worked at Morgan Stanley and D.E. Shaw. Pamir graduated from Duke University and Columbia University with a BSc. in Electrical Engineering and MSc. in Operations Research.

Ran Nussbaum

Ran Nussbaum is a managing partner and co-founder of The Pontifax Group. The fund runs more than 50 portfolio companies all around the globe. Prior to joining Pontifax, he was a partner at Israel's largest business intelligence and strategic consulting firm.

Ron Gross

Ron has graduated from the Technion with an M. Sc in Computer Science. He has worked at several companies, ranging from small startups to Google, and has an extensive experience in web architecture, security, and algorithms. Ron has been continuously involved with Bitcoin since March 2011, spreading the word, knowledge, and love of Bitcoin. He is a firm advocate of open source, transparency and decentralization of power and technology. Ron co-founded the Israeli Bitcoin community and Foundation and was the Executive Director of the Mastercoin Foundation (the world's first ICO).