ZEN

[A DECENTRALIZED FINANCIAL SYSTEM]

ABSTRACT

A purely peer-to-peer mechanism to structure contractual relationships would allow mutually distrusting parties to draft contracts without reliance on the legal system for dispute resolution. These agreements, also known as ‘Smart Contracts’, can be entered by committing to a digital contract drafted in code, and disputes can be resolved by executing such code on a public decentralized network.

Current platforms lack the functionality or security required to reliably execute financial contracts. Zen is a new smart contract platform that enables the creation, facilitation, and resolution, of contractual obligations. Based on the Bitcoin paradigm (UTXO verification), we make use of ZF*, a functional language used for formal verification, to express and verify proofs of bounds on contract resource consumption. In Zen, all tokens are “first class citizens”,multiple assets are supported, and the Bitcoin network is observed to facilitate interoperability.

MOTIVATION

The core team at Zen protocol started working together in 2014 in the blockchain space and after years of research began development of the Zen Protocol in June 2016.

The motivation which spawned the vision of Zen is that we believe that people have a right to own their financial assets, and we feel a responsibility to provide people with the necessary tools to empower themselves.

FINANCE

Use cryptography to create, trade, and store conventional financial assets, contracts, and instruments over a decentralized network.

PROBLEM

Conventional Finance

Rather than be exposed to counterparty risk, we use financial institutions as trusted intermediaries. These financial institutions facilitate the majority of economic transactions. **These institutions limit our freedoms:**

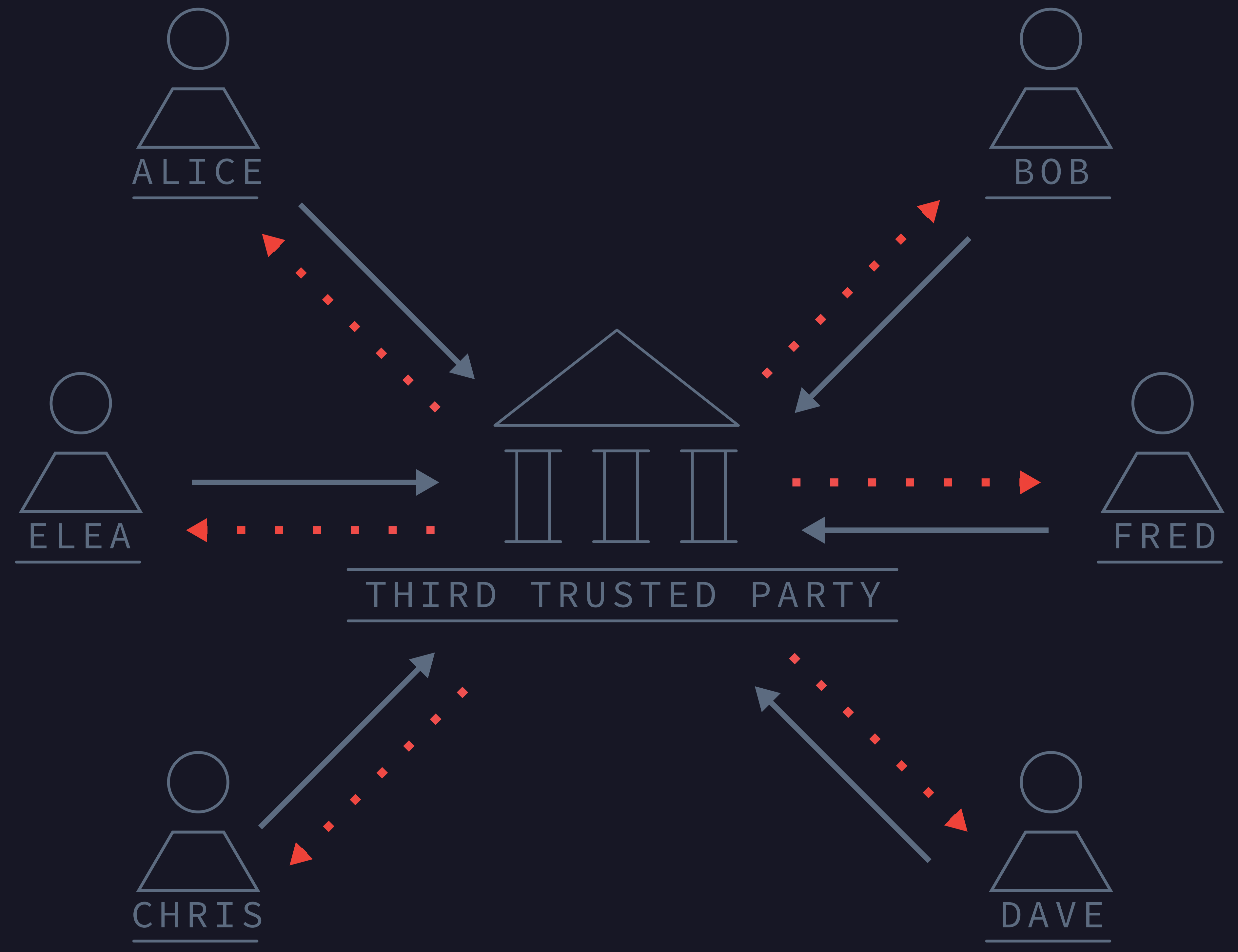
- **Limited Access**

  Financial institutions restrict ***who*** can access the financial system, and ***what*** they can do in the financial system.

- **Limited ownership/control**

  To a certain extent we do not fully own or control our assets, rather we have an obligation from the bank.

  The bank can fail to fulfill this obligation, due to insolvency or confiscation.



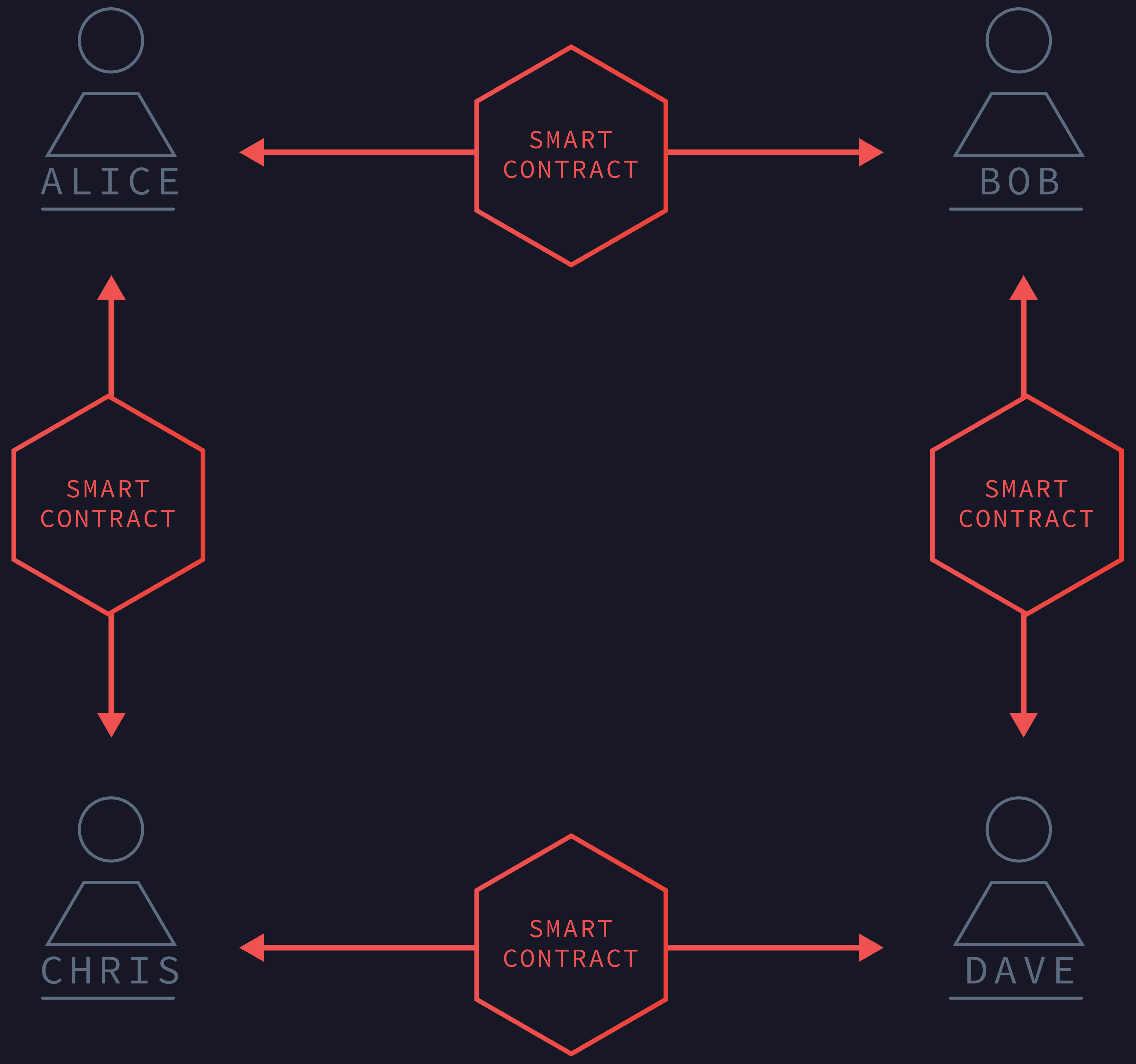
SOLUTION

A Decentralized Financial System

If we removed our dependence on third parties, we could reclaim ownership of our assets and our liberties. We believe we would have more efficient markets, with less red tape and fees.

Using Bitcoin technology, we can create a decentralized financial system.

A new blockchain, specialized for finance, allows us to own our assets cryptographically, and enforces the cash flows which emanate from those assets using smart contracts.



SOLUTION

A new custom-built blockchain

The space is filled with centralized blockchains focused on finance, and decentralized blockchains focused on non financial use cases. We see the potential of blockchain technology - decentralized finance. Zen attempts to fill that niche in the market.

Do we really need another Blockchain?

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

BITCOIN

Bitcoin is decentralized money

We believe **Bitcoin is the ultimate form of money.** Satoshi chose to limit Bitcoin’s features in order to focus on Bitcoin serving the role of money. Satoshi argued “Piling every proof-of-work quorum system in the world into one dataset doesn't scale.”

Bitcoin lacks the functionality required for finance.

We need a new blockchain for decentralized finance, a blockchain which has support for **multiple assets** and **complex ownership constructs.**

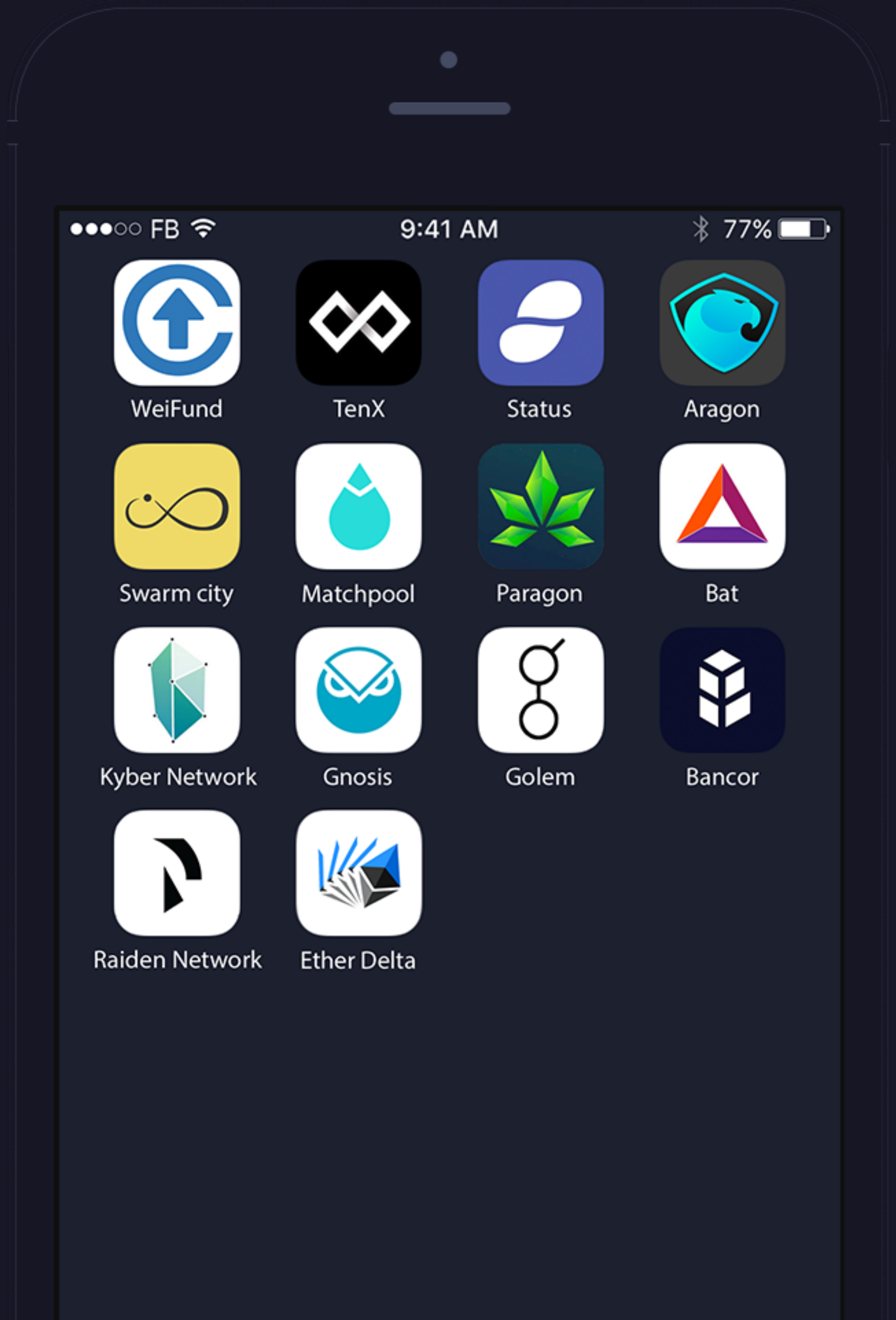
THERE ARE AN
ESTIMATED 21M BRICKS
(400 OZ PER BRICK) OF
GOLD IN THE WORLD

ETHEREUM

Ethereum is decentralized computation

Ethereum’s goal is to be a platform for developing decentralized applications, for example Facebook or Uber without a central server. Ethereum is a developer focused platform and provides convenient programming languages (Solidity) and Application Binary Interfaces (ABI).

In order to enable this functionality, Ethereum provides the Ethereum Virtual Machine (EVM), where computational cycles are countedthe gas system is used.



ZEN

Zen is decentralized finance

Zen is a new platform focused on decentralized financial instruments. Zen enables peer to peer access to both new and conventional assets .

Just as Bitcoin removed our reliance on banks to transfer money, Zen removes our reliance on banks to engage in finance.

TOKENS

Assets are held cryptographically in a wallet.

ACS

Zen's "execution environment", equivalent to Bitcoin's stack or Ethereum's EVM.

BITCOIN INTEGRATION

Zen runs in parallel, and acts as a complement to Bitcoin.

CONTRACTS

Replace intermediaries with decentralized escrow mechanisms

ORACLES

Contracts can depend on real world events such as the movement of prices in the stock market.

MULTI HASH MINING

Stakeholders vote on which hash algorithms will receive the mining reward, striking a balance between the interests of miners and token holders.

ARCHITECTURE

Tokens

Unlike Bitcoin which only has support for BTC, or Ethereum which has ERC 20 contracts, Zen has multi tokens built in at the protocol level.

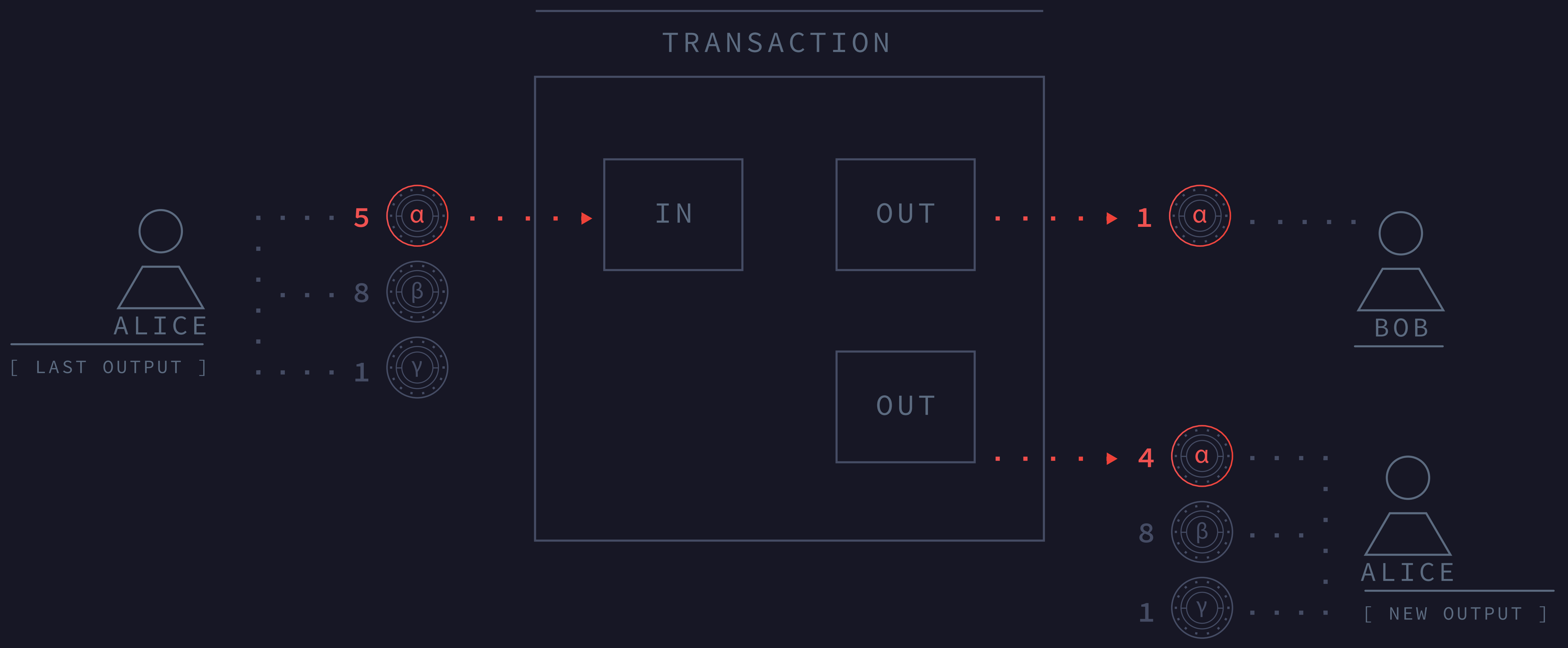
That means that every sort of token in Zen has a similar status to the Zen native token. Therefore every contract in Zen can hold and manage any other token, and any token can be used to pay transaction fees to miners.

This is of particular interest as it allows financial contracts to be denominated in “normal” currencies such as the dollar or euro. Tokens are stored in transaction outputs, just as in Bitcoin, and can be unlocked with the right permissions, then locked again in new outputs.

Tokens generally have value because:

- People believe they have value
- They are backed by contracts which hold collateral

[ALICE SENDS 1 ALPHA TO BOB]



SPENDING A UTXO CONSUMES IT AND CREATES NEW UTXOS.

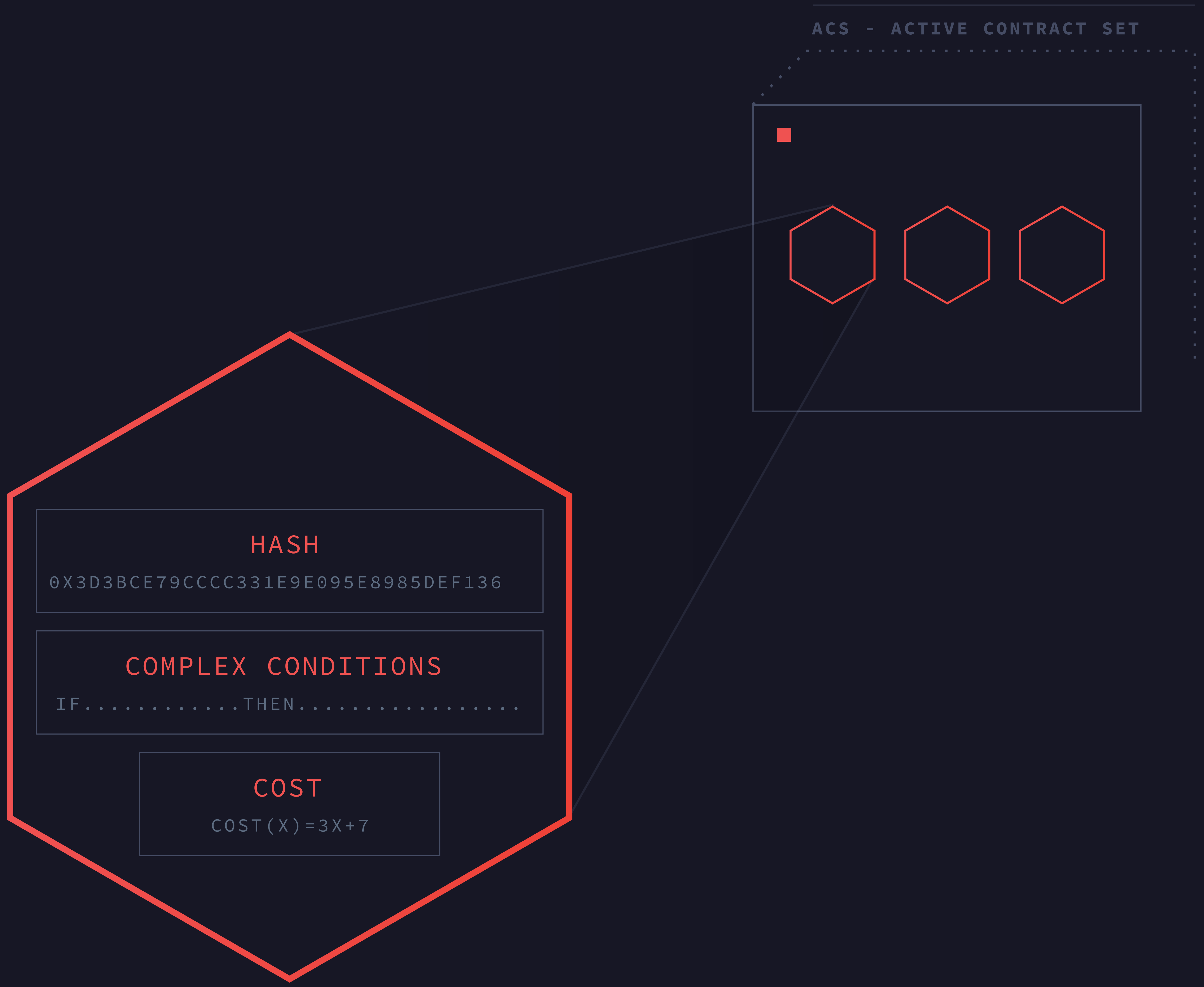
ARCHITECTURE

Contracts

Contracts are written in F* – a functional, dependently typed, high level, formally verified language. Formal verification, coupled with a cost model, enables all contracts in the Zen Protocol to **prove how long they take to run before they ever enter the blockchain.**

Contracts are immutable – (Their code never changes). Therefore each contract can have a unique mathematical identifier (its hash). Using this hash, it is easy to associate tokens and proofs with a contract.

Each contract lives in isolation from the rest of the blockchain – A contract can only change the state of the blockchain and communicate with other contracts by creating a transaction. Contracts do not do anything independently. Rather, they act as validation data, which is used to help nodes determine whether or not to accept a transaction.



ACS - ACTIVE CONTRACT SET

HASH

0X3D3BCE79CCCC331E9E095E8985DEF136

COMPLEX CONDITIONS

IF............THEN.................

COST

COST(X)=3X+7

[EACH CONTRACT IS IDENTIFIED BY ITS HASH]

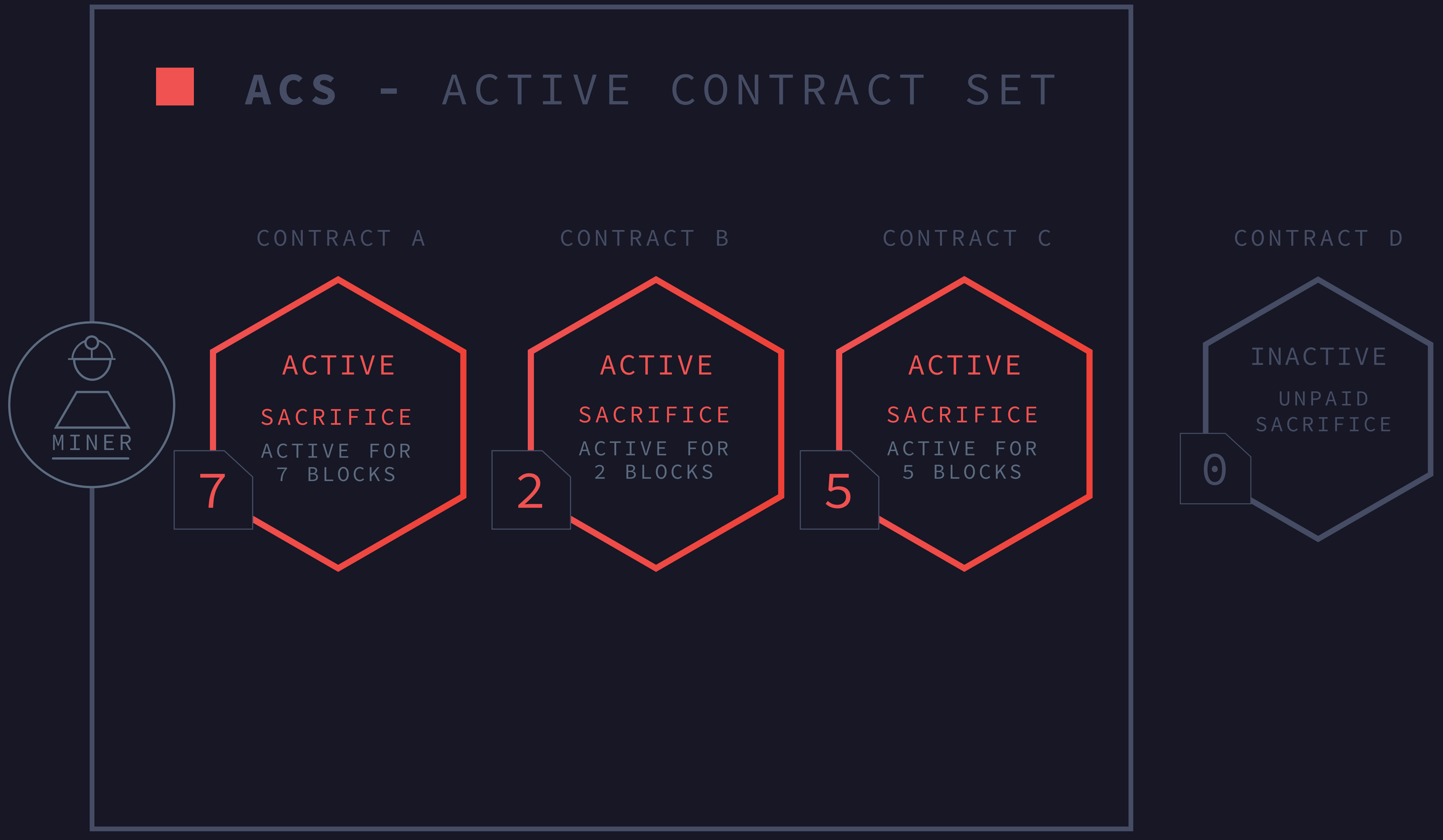
[CONTRACTS ARE WRITTEN IN OUR DIALECT OF ZF*]

[CONTRACTS ARE ISOLATED FROM EACH OTHER]

ARCHITECTURE

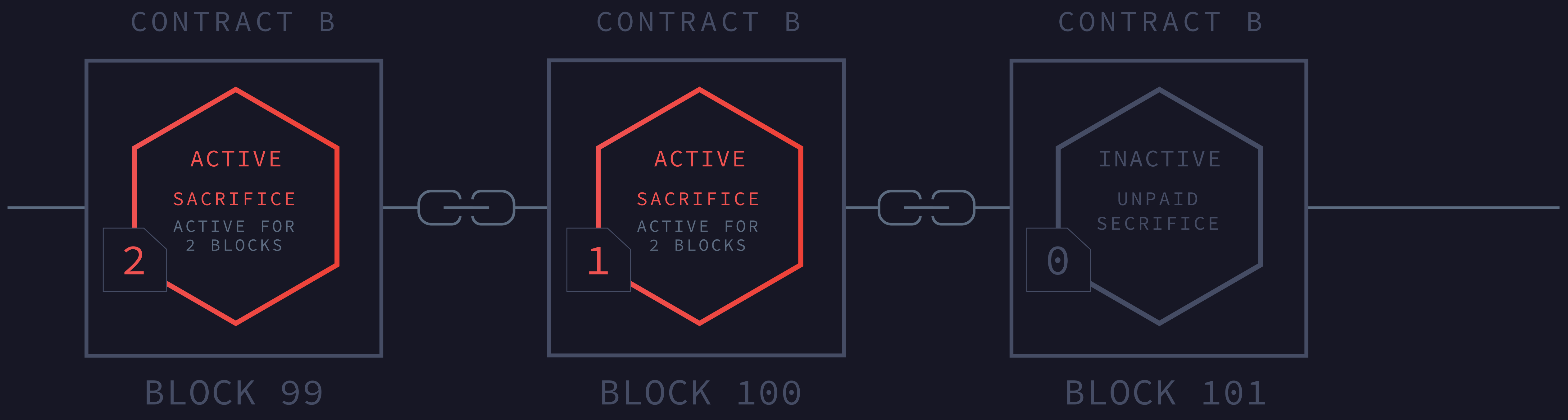
Active Contract Set

- Upon activation, contracts are converted from F* to machine code.
- The compiled contracts are stored in the node’s RAM.
- Contracts must be active to create transactions, such as sending or issuing tokens.
- Anyone can activate or extend a contract with a contract sacrifice.



The Contract Sacrifice.

- The contract sacrifice compensates the miners who must maintain the contract. The sacrifice is divided among the miners who find blocks during the active period.
- While transaction fees can be paid in any token, the contract sacrifice must be paid in Zen.

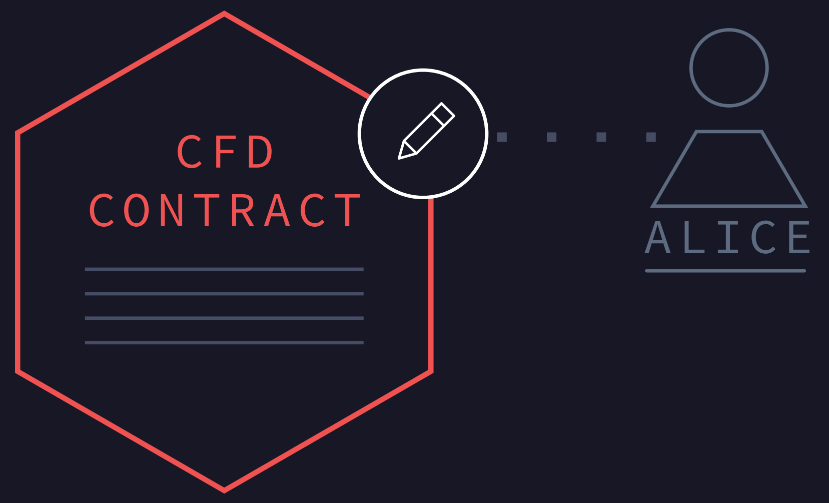


USE CASE - AAPL CFD

Let’s look at how Tokens, Contracts, and the Active Contract Set work together to create a peer to peer financial contract.

1

- Alice writes a contract for difference (CFD) on AAPL for 30 days.
- Alice makes money if AAPL goes down.
- Her counterparty makes money if AAPL goes up.



CFD CONTRACT

ALICE

ZEN TOKEN

ANY TOKEN

AAPLE CFD

LONG AAPL TOKEN

SHORT AAPL TOKEN

ACTIVE CONTRACT

INACTIVE CONTRACT

ALICE

BOB

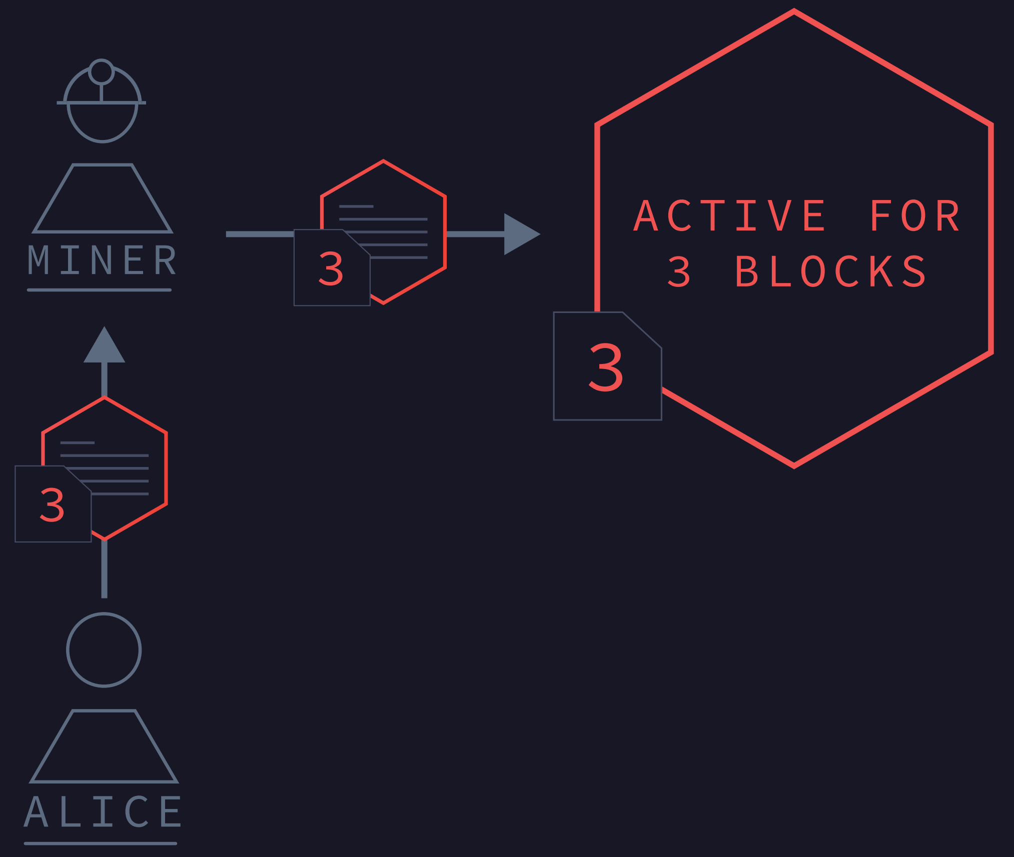
CHRIS

MINER

USE CASE - AAPL CFD

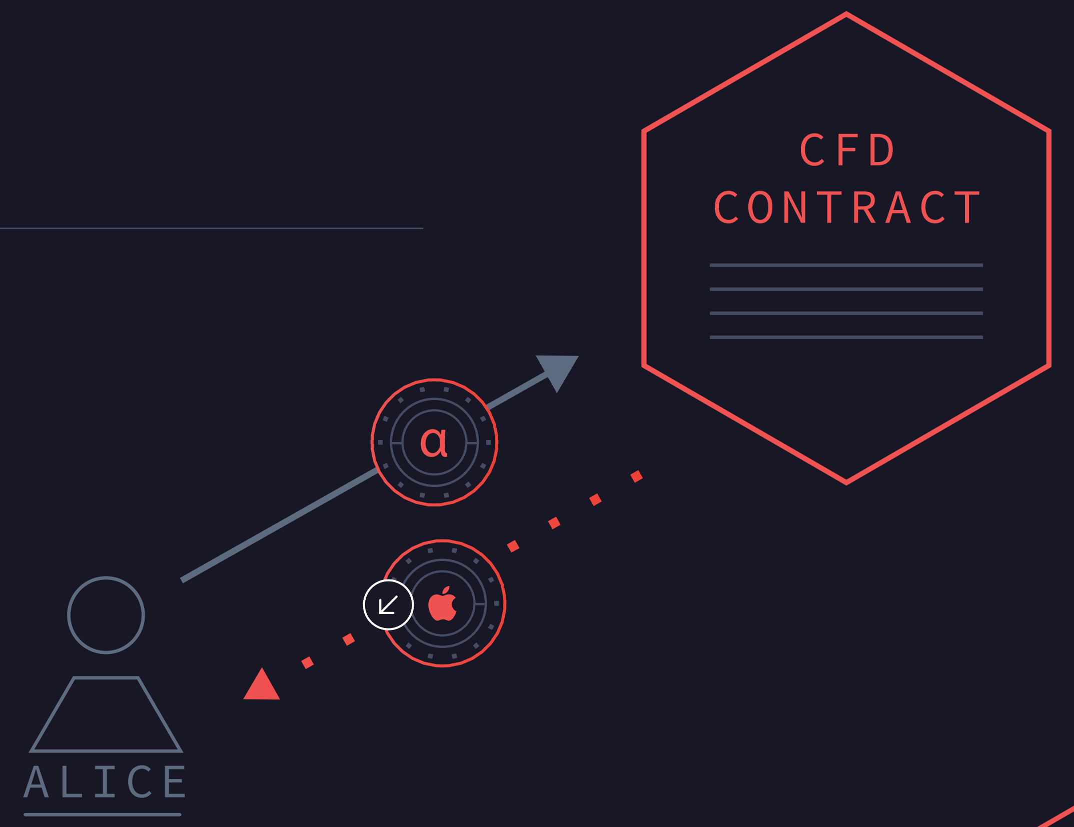
2

- Alice activates the contract for 3 blocks.



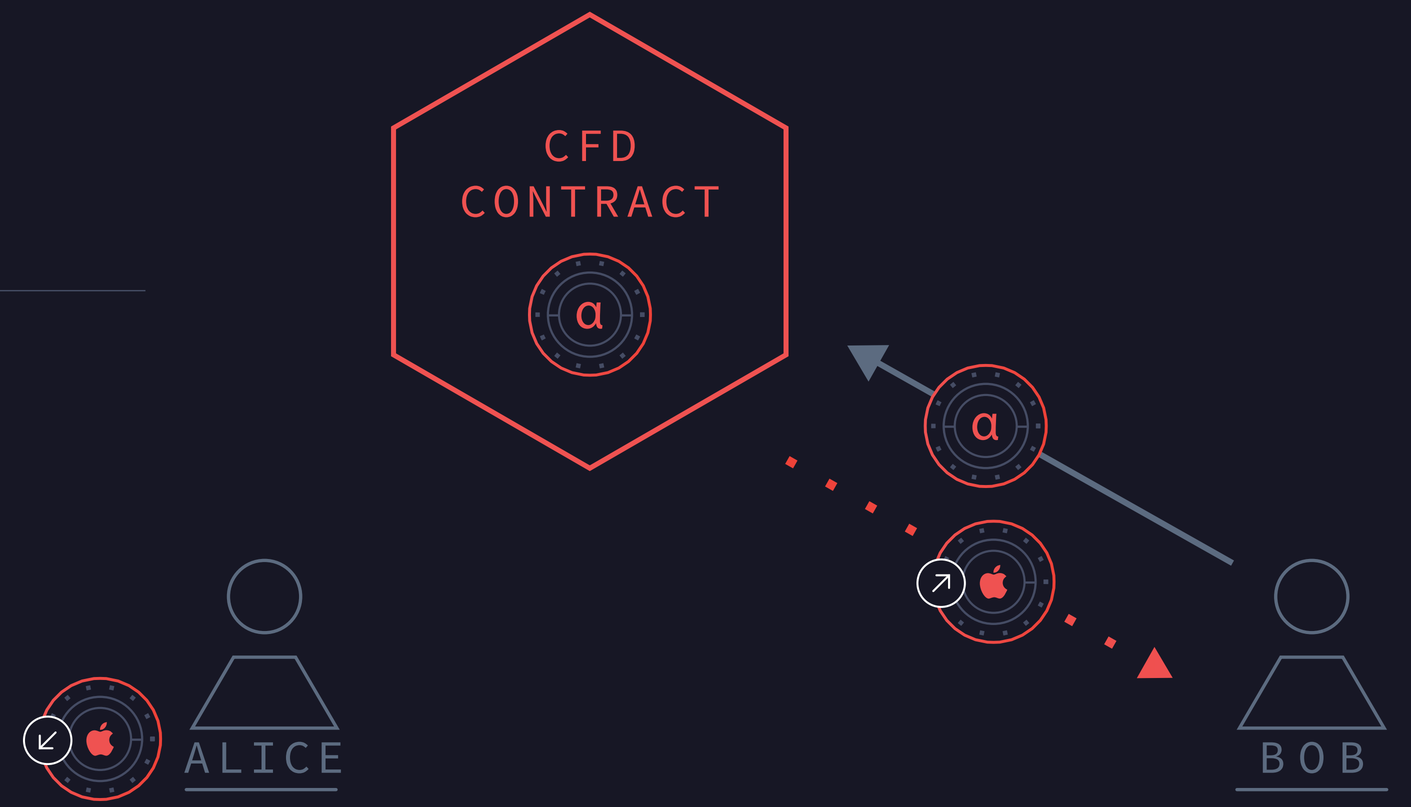
3

- Alice collateralizes the active contract, entering a short position.



4

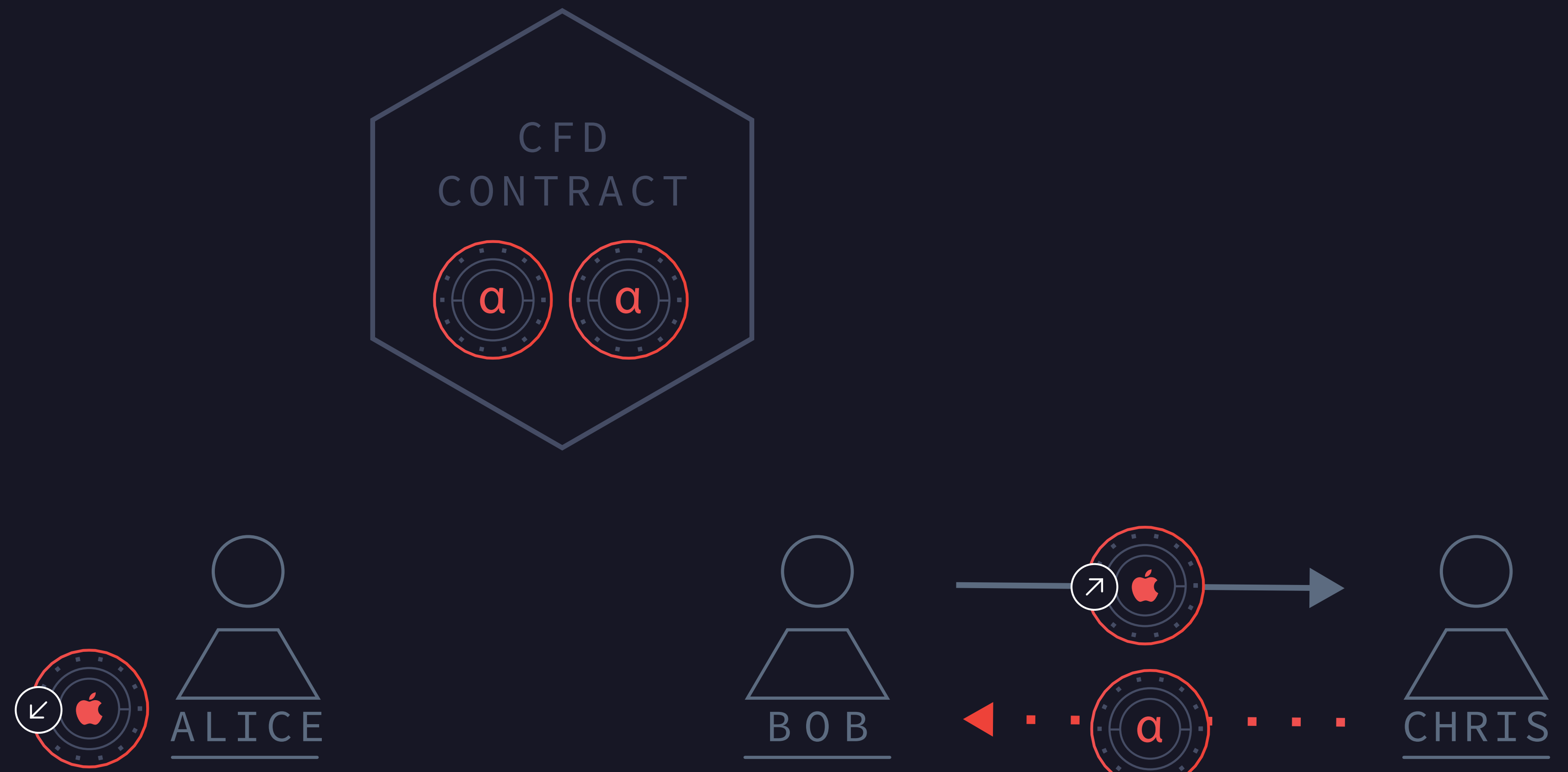
- Bob sees the collateralized contract and takes the other side by sending tokens.



USE CASE - AAPL CFD

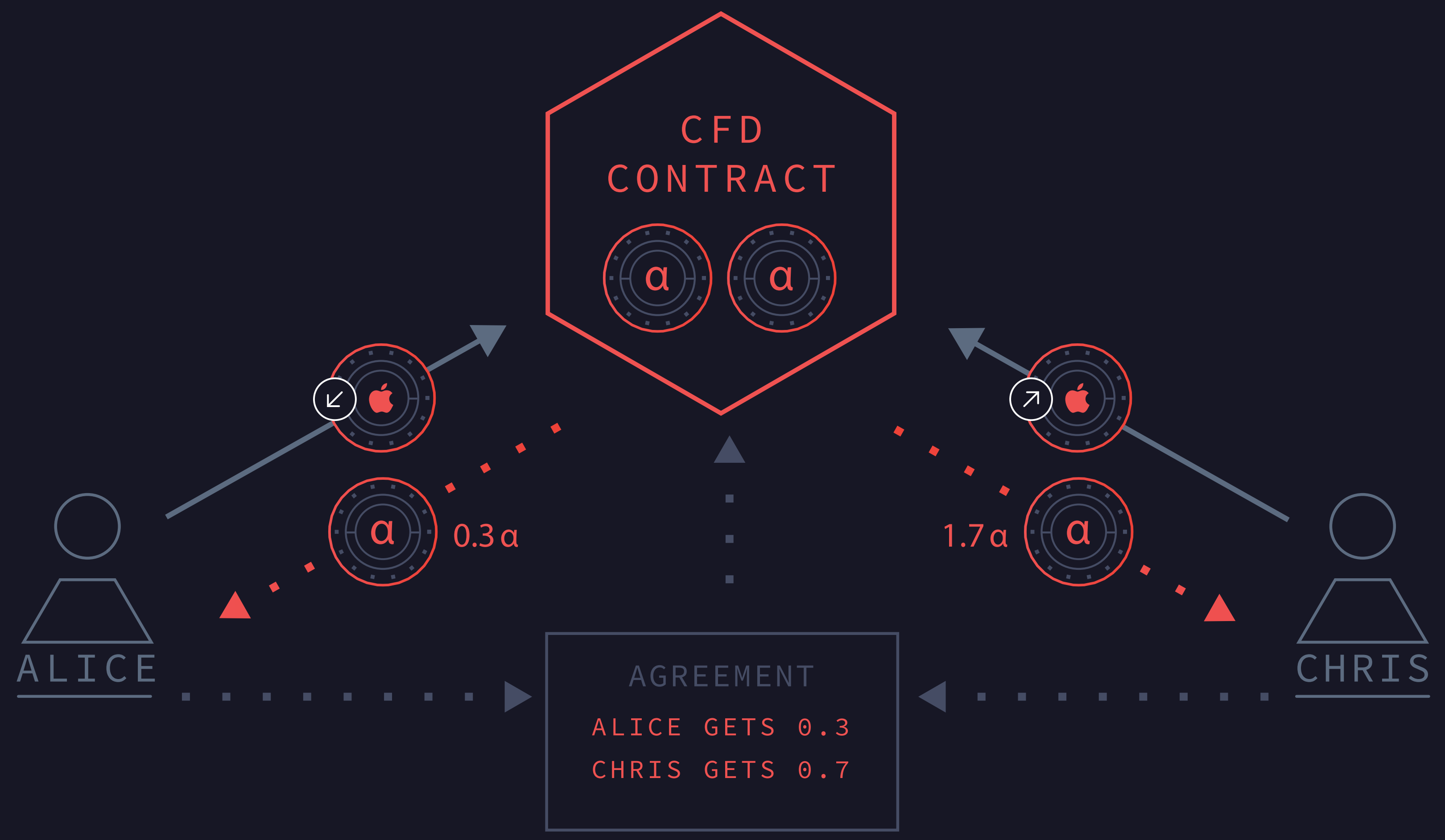
5

- The contract becomes inactive
- Bob can still exit his position by selling his Contract Token to someone else.



6

- After 30 days the contract needs to be reactivated to withdraw the escrowed funds.
- If Alice and Chris agree that AAPL is up 70% they sign a transaction where Alice gets 0.3 α and Chris gets 1.7α.



BUT WHAT IF ALICE IS NOT COOPERATIVE?

INTRODUCING ORACLES

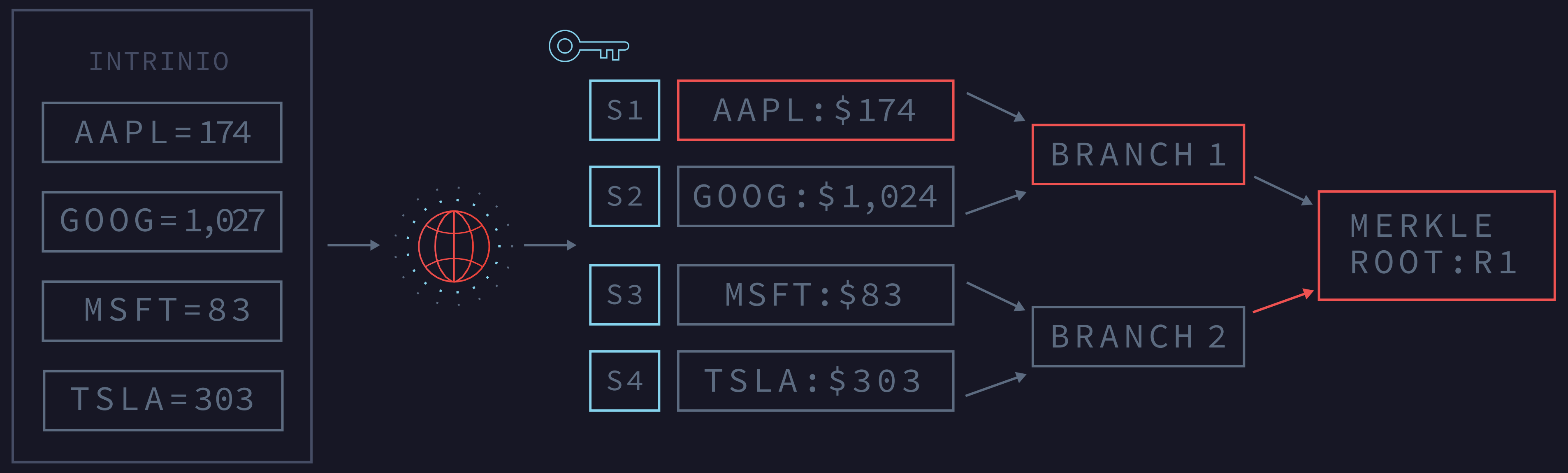
Oracles allow contracts to operate on real world data

Contracts state in advance which oracle(s) will be relied on to provide data to the contract.

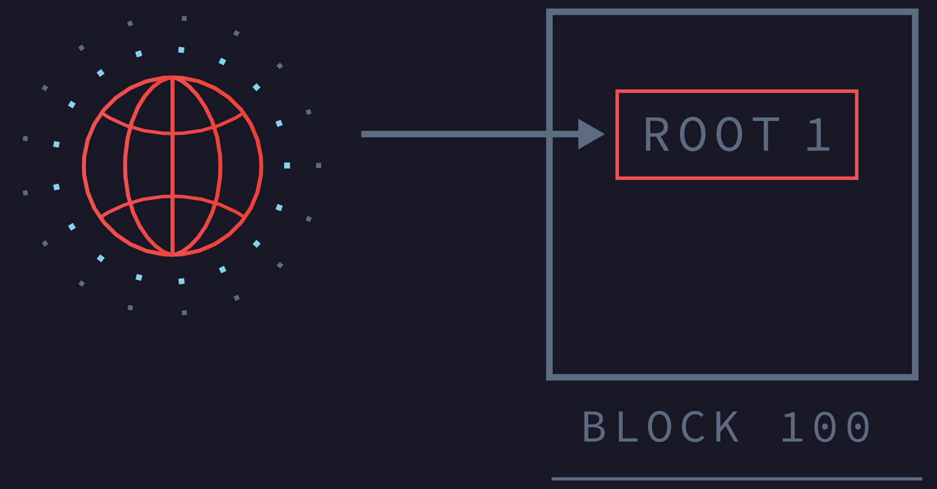
Legal contracts use judges and are arbitrated in court, smart contracts use oracles and are arbitrated on the blockchain.

How oracles work:

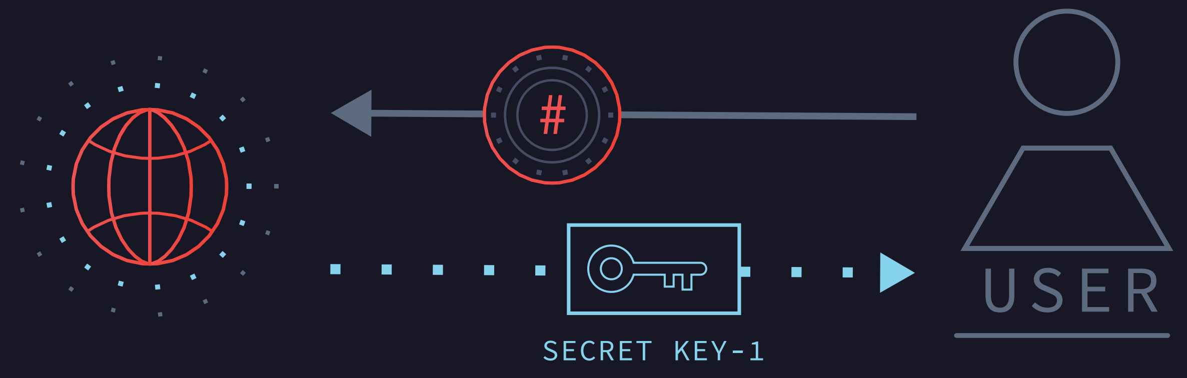
1 Oracles pull data from web APIs and sort them into a Merkle Tree; Each leaf is salted with a secret/nonce.



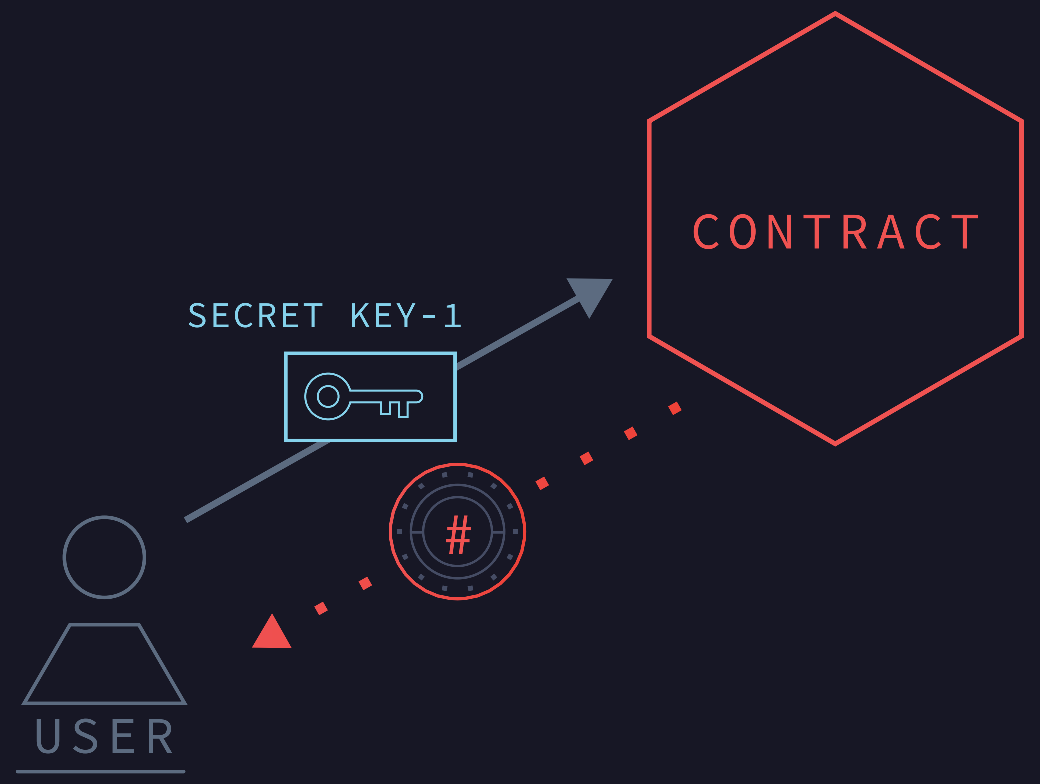
1 The Oracle inserts the Merkle Root to the blockchain.



2 When a user needs to provide the contract with a specific leaf/piece of data (i.e. to resolve a dispute), the user pays the oracle and the oracle reveals the nonce.



3 Using the nonce, the user can prove to the contract what the committed price is and withdraw funds.

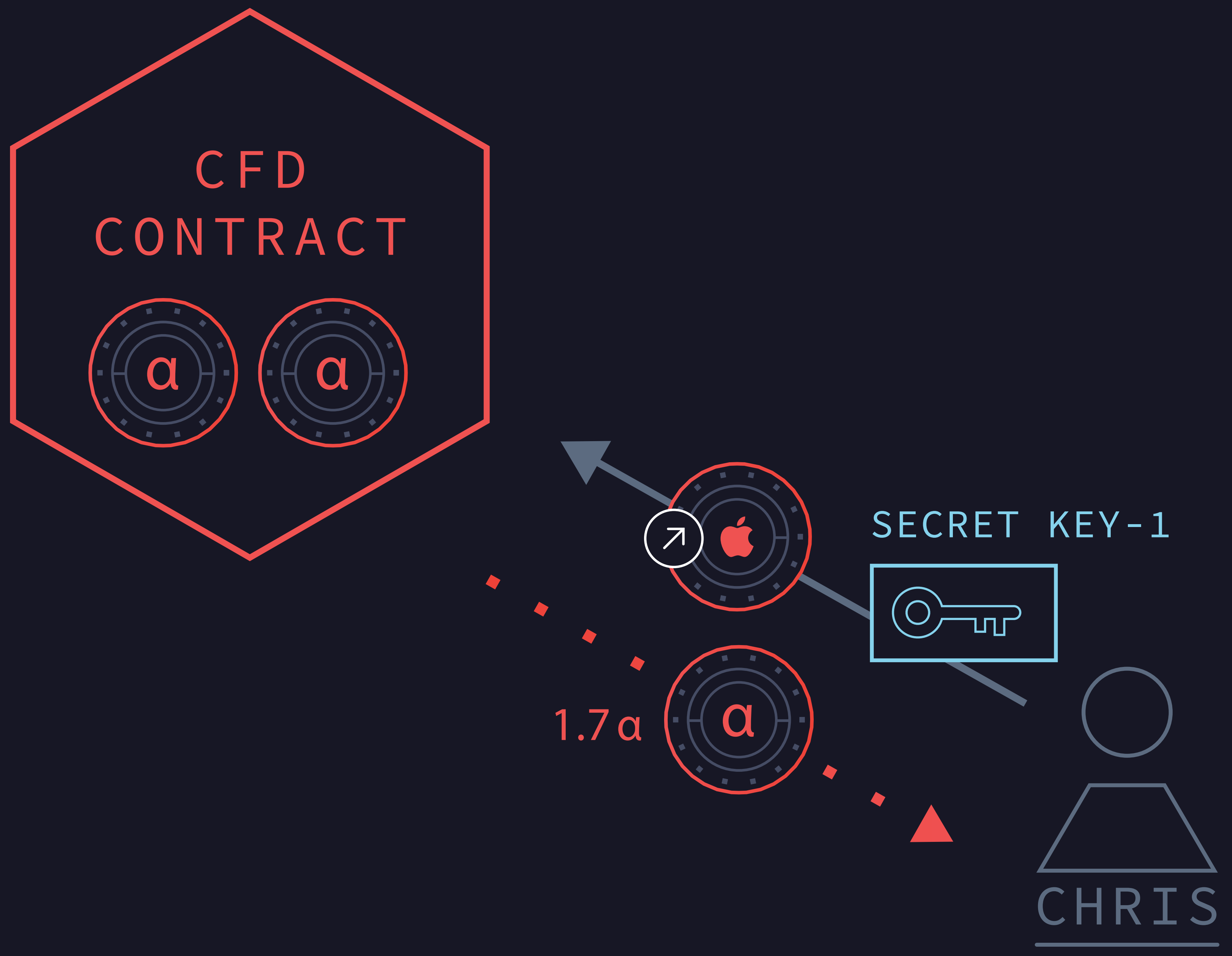


USE CASE - AAPL CFD CONTINUED

Dispute resolution

So in the event that Alice and Chris cannot agree then Chris will pay the oracle to provide him with the secret (S1).

- Chris then sends the secret and the call option to the contract, and the contract pays chris 1.7alpha.



BITCOIN INTEGRATION

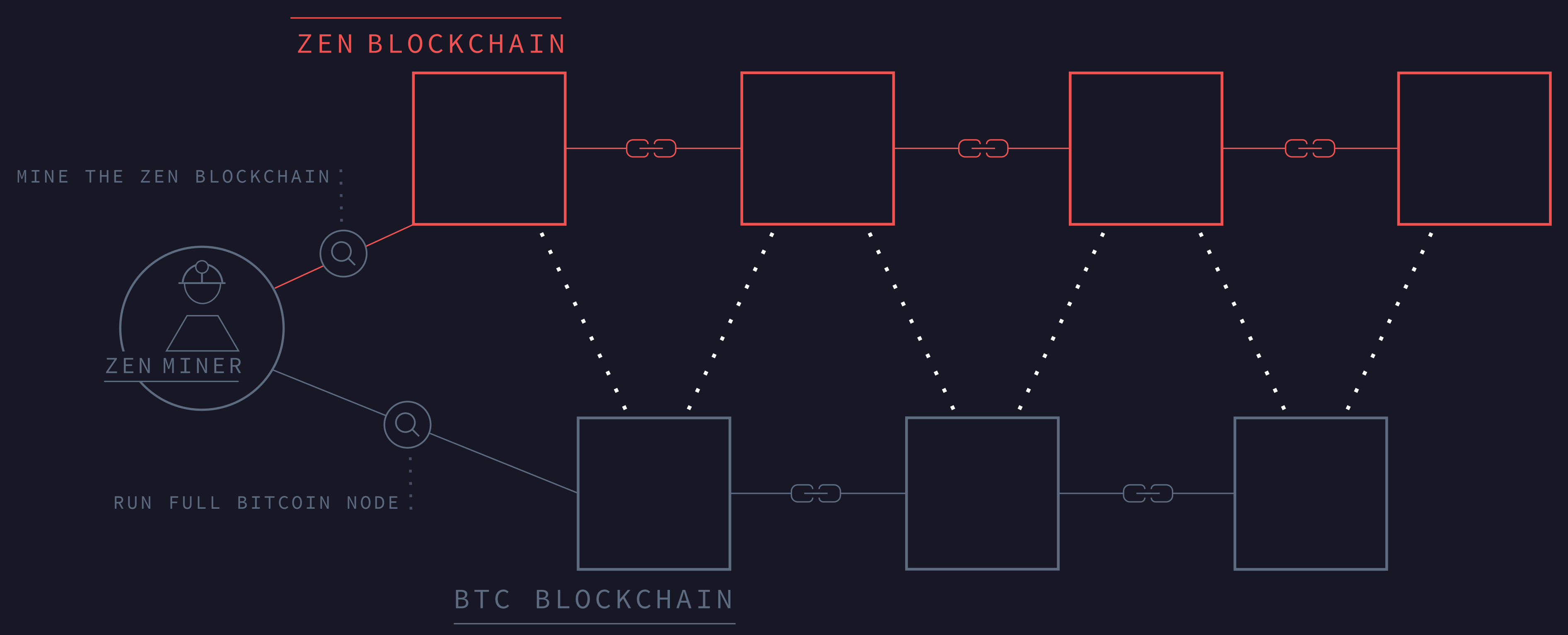
Past efforts to increase complexity in ’blockchain’ systems have taken two strategies:

1 **Create an alternative blockchain which necessitates the use of an AltCoin.**

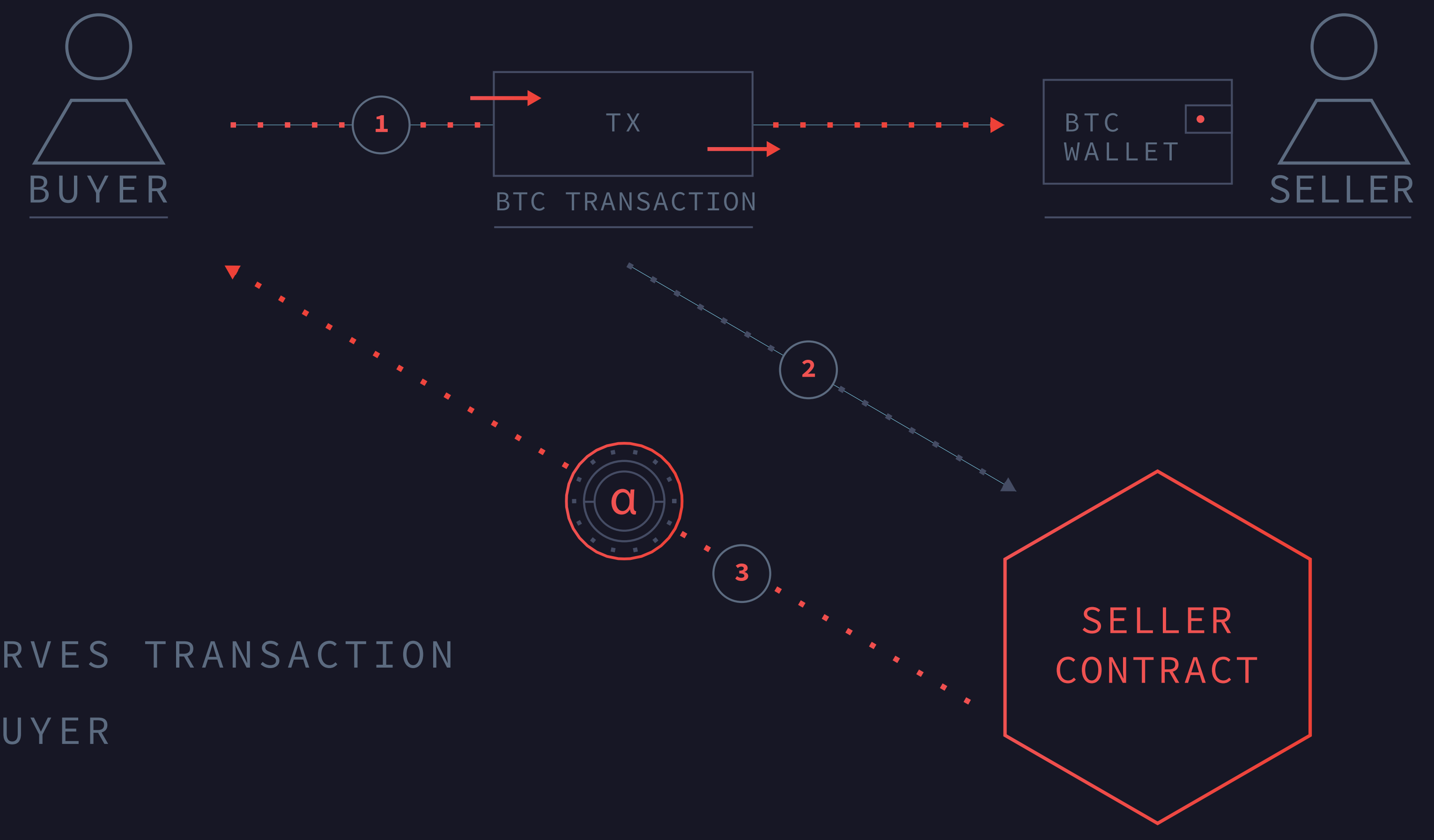
2 **Create a supplementary protocol, e.g. a side-chain, which lacks a proprietary token and thus differs from Bitcoin’s incentive/security mechanisms.**

Zen takes a new approach, a separate blockchain with its own token, which runs in parallel to the Bitcoin network.

Merged Consensus – Zen miners mine the Zen Blockchain and observe the Bitcoin Blockchain. This allows cross-chain functionality.



Cross-Chain Contract – Collateral is held in the Zen chain, but the premium is paid to a Bitcoin address.

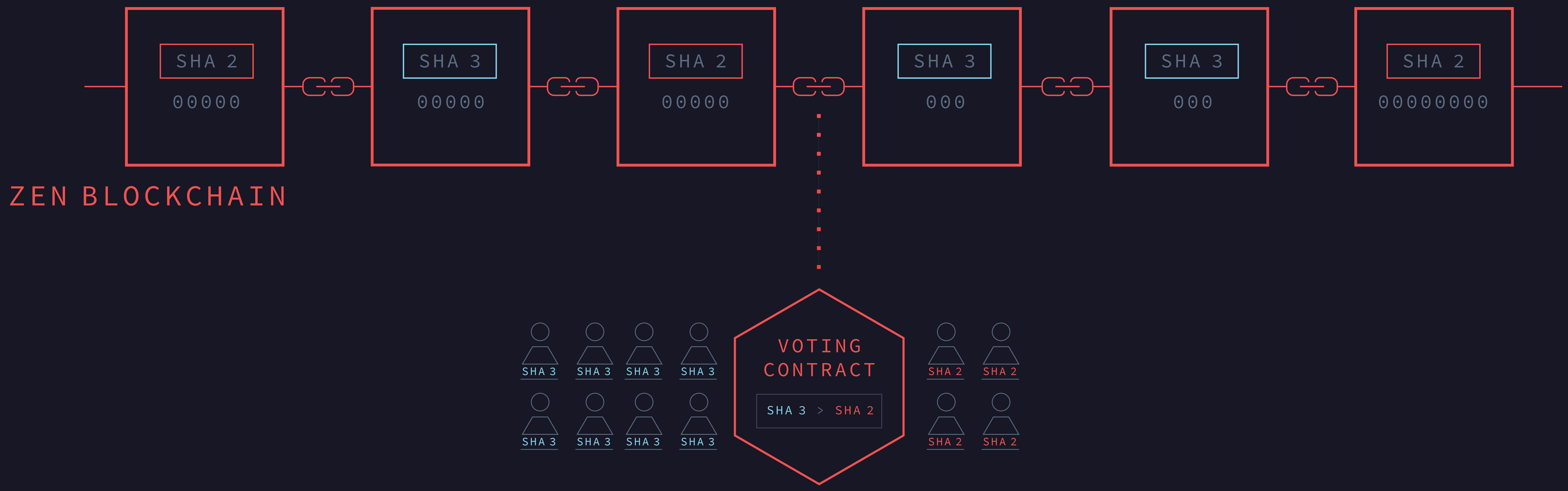


1. BUYER SENDS BTC TO SELLER
2. SELLER’S ZEN CONTRACT OBSERVES TRANSACTION
3. CONTRACT SENDS TOKENS TO BUYER

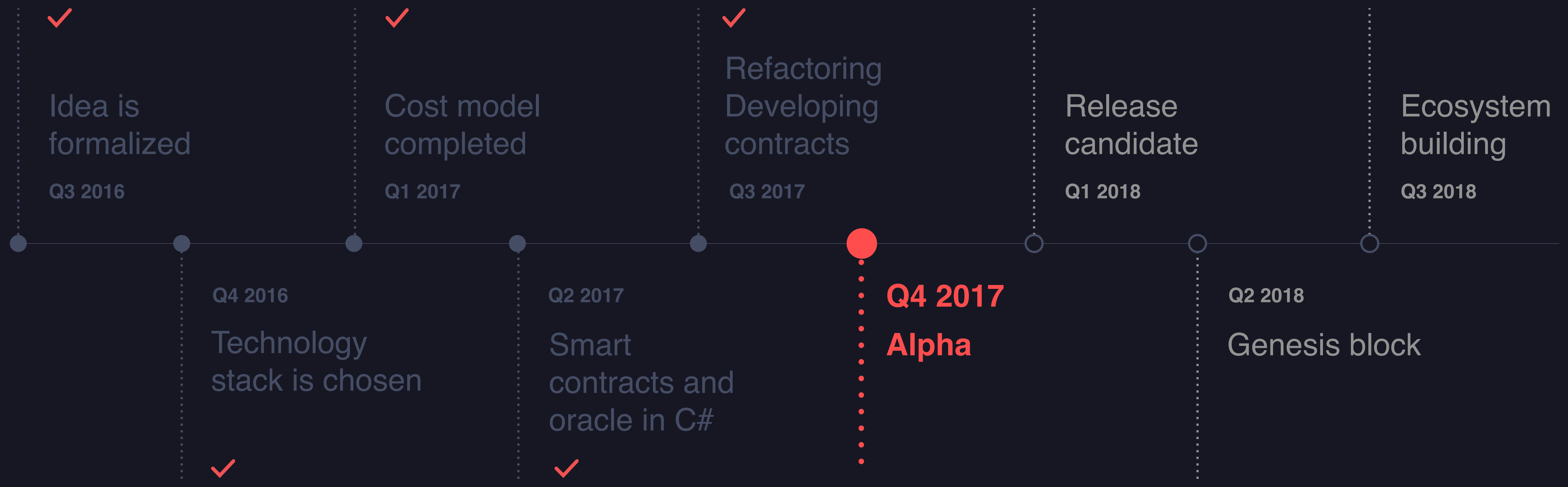
ZEN

Multi-Hash Mining – token holder representation

- Different hash functions can be used to find a block.
- Each hash function has a different difficulty requirement.
- Target ratio of blocks generated by each hash function is established by Zen token holders.



ROADMAP



✓ Idea is formalized

Q3 2016

Q4 2016

Technology stack is chosen ✓

✓ Cost model completed

Q1 2017

Q2 2017

Smart contracts and oracle in C# ✓

✓ Refactoring Developing contracts

Q3 2017

Q4 2017

Alpha

Release candidate

Q1 2018

Q2 2018

Genesis block

Ecosystem building

Q3 2018

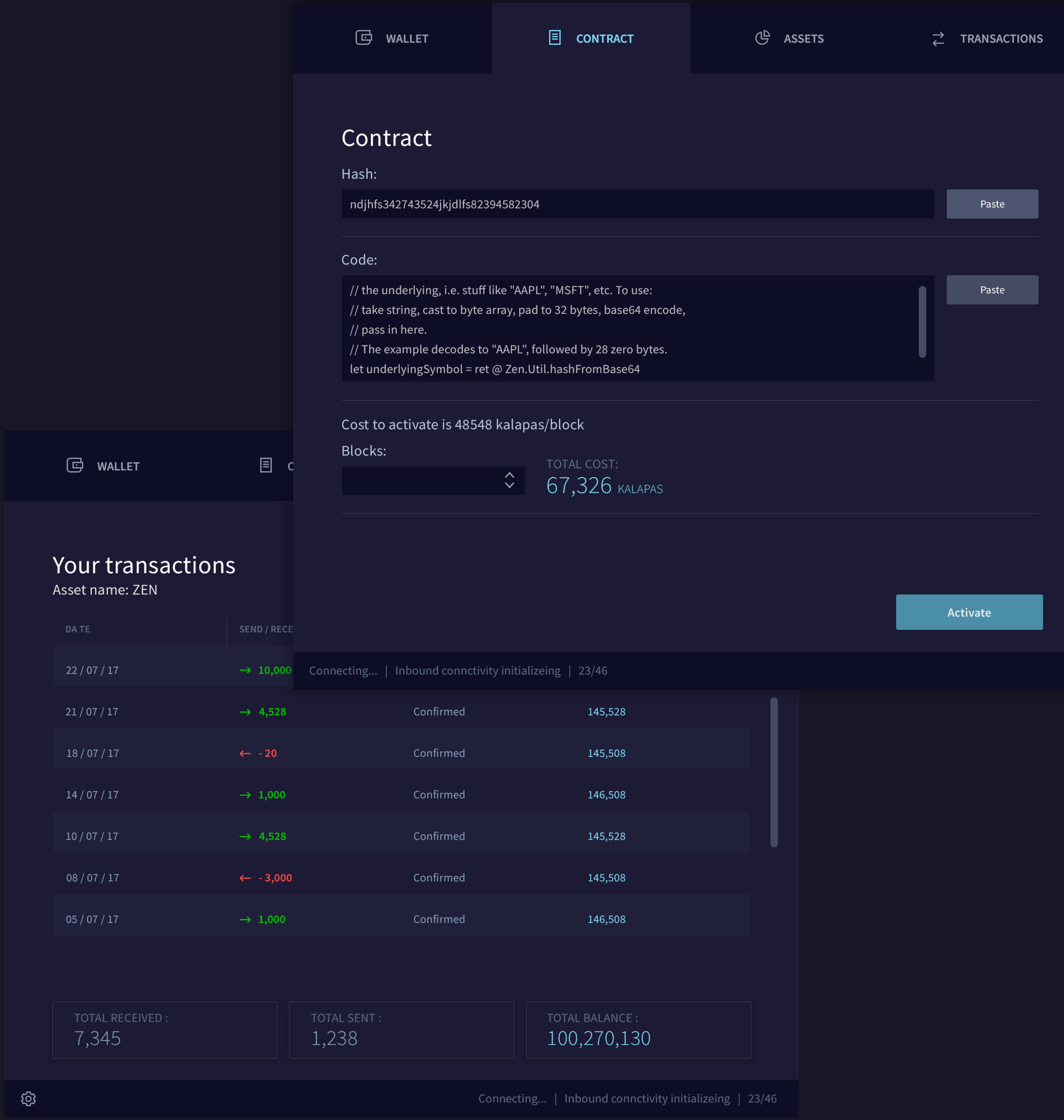
ZEN

Alpha

We currently have a working alpha with a blockchain built from scratch, implementation of the ACS, smart contracts written in F* that prove their cost, and oracles fetching stock prices from intrinio.com

Zen Alpha

DOWNLOAD



Contract

Hash:

ndjhfs342743524jkjdlfs82394582304

Code:

```
// the underlying, i.e. stuff like "AAPL", "MSFT", etc. To use:
// take string, cast to byte array, pad to 32 bytes, base64 encode,
// pass in here.
// The example decodes to "AAPL", followed by 28 zero bytes.
let underlyingSymbol = ret @ Zen.Util.hashFromBase64
```

Cost to activate is 48548 kalapas/block

Blocks:

TOTAL COST:
67,326 KALAPAS

Connecting... | Inbound connctivity initializeing | 23/46

Your transactions

Asset name: ZEN

DA TE	SEND / RECE		
22 / 07 / 17	→ 10,000		
21 / 07 / 17	→ 4,528	Confirmed	145,528
18 / 07 / 17	← - 20	Confirmed	145,508
14 / 07 / 17	→ 1,000	Confirmed	146,508
10 / 07 / 17	→ 4,528	Confirmed	145,528
08 / 07 / 17	← - 3,000	Confirmed	145,508
05 / 07 / 17	→ 1,000	Confirmed	146,508

TOTAL RECEIVED :
7,345

TOTAL SENT :
1,238

TOTAL BALANCE :
100,270,130

Connecting... | Inbound connctivity initializeing | 23/46

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!

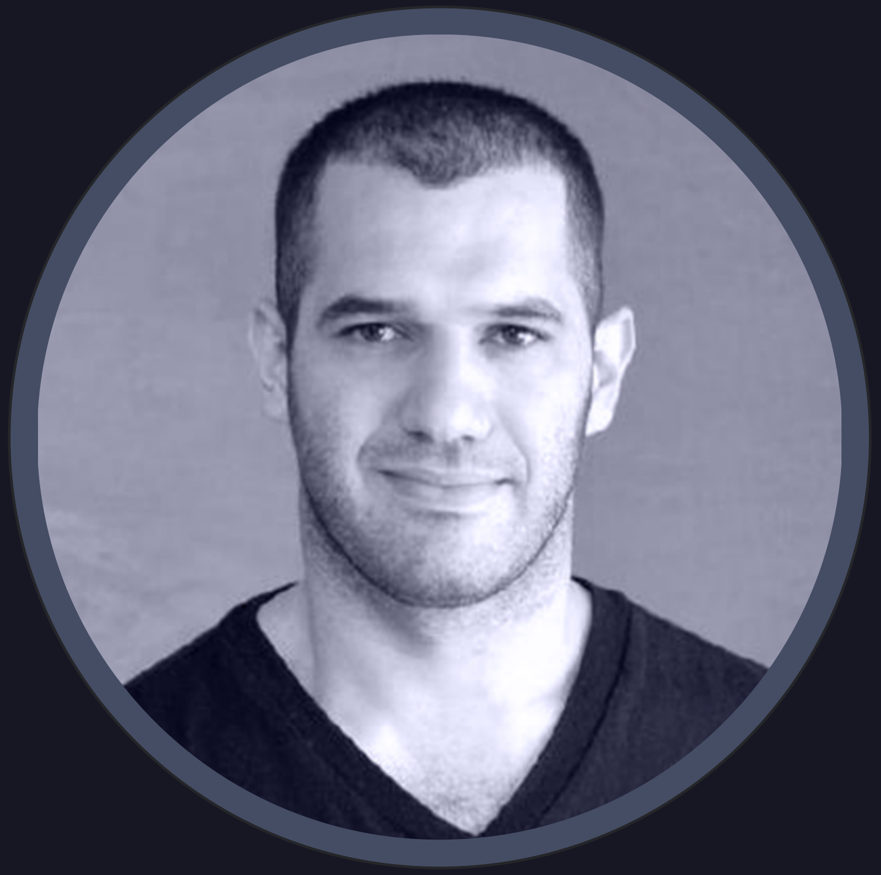
Asher Manning

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).