

**Z E N**

[ ДЕЦЕНТРАЛИЗОВАННАЯ ФИНАНСОВАЯ СИСТЕМА ]



## АННОТАЦИЯ

Истинно одноранговый механизм выстраивания договорных взаимоотношений позволил бы взаимно недоверяющим сторонам составлять проекты контрактов, не полагаясь на законодательство для урегулирования споров. Данные соглашения, также известные как «смарт-контракты», могут быть заключены путём осуществления цифрового контракта, составленного по коду, и споры могут быть решены путём выполнения такого кода в открытой децентрализованной сети.

Существующие платформы испытывают недостаток функциональности или безопасности, необходимой для надёжного выполнения финансовых контрактов. Zen - это новая платформа смарт-контрактов, которая предоставляет возможность создания, упрощения и решения контрактных обязательств. Основываясь на парадигме Bitcoin (верификации UTXO), мы используем ZF\* - язык функционального программирования, используемый для формальной верификации, выражения и проверки предельных доказательств потребления контрактных ресурсов. В Zen все токены являются "полноправными жителями", поддерживается несколько активов, а сеть Bitcoin находится под наблюдением, чтобы способствовать совместимости.





В блокчейн пространстве основная команда протокола Zen начала работать вместе еще в 2014 году и после многолетних исследований начали разработку протокола Zen в июне 2016 года.

**Мотив, который породил видение Zen - это наши убеждения в том, что люди имеют право владеть своими финансовыми активами и мы ответственны за предоставление людям необходимых инструментов для расширения своих возможностей.**

Используйте криптографию для создания, торговли и хранения традиционных финансовых активов, контрактов и инструментов на основе децентрализованной сети..

Ф И Н А Н С Ы

# ПРОБЛЕМА

## Традиционная финансовая сфера

Вместо того, чтобы подвергаться партнерскому риску, мы используем финансовые институты в качестве доверенных посредников. Эти финансовые институты облегчают большинство экономических операций. **Эти институты ограничивают наши свободы:**

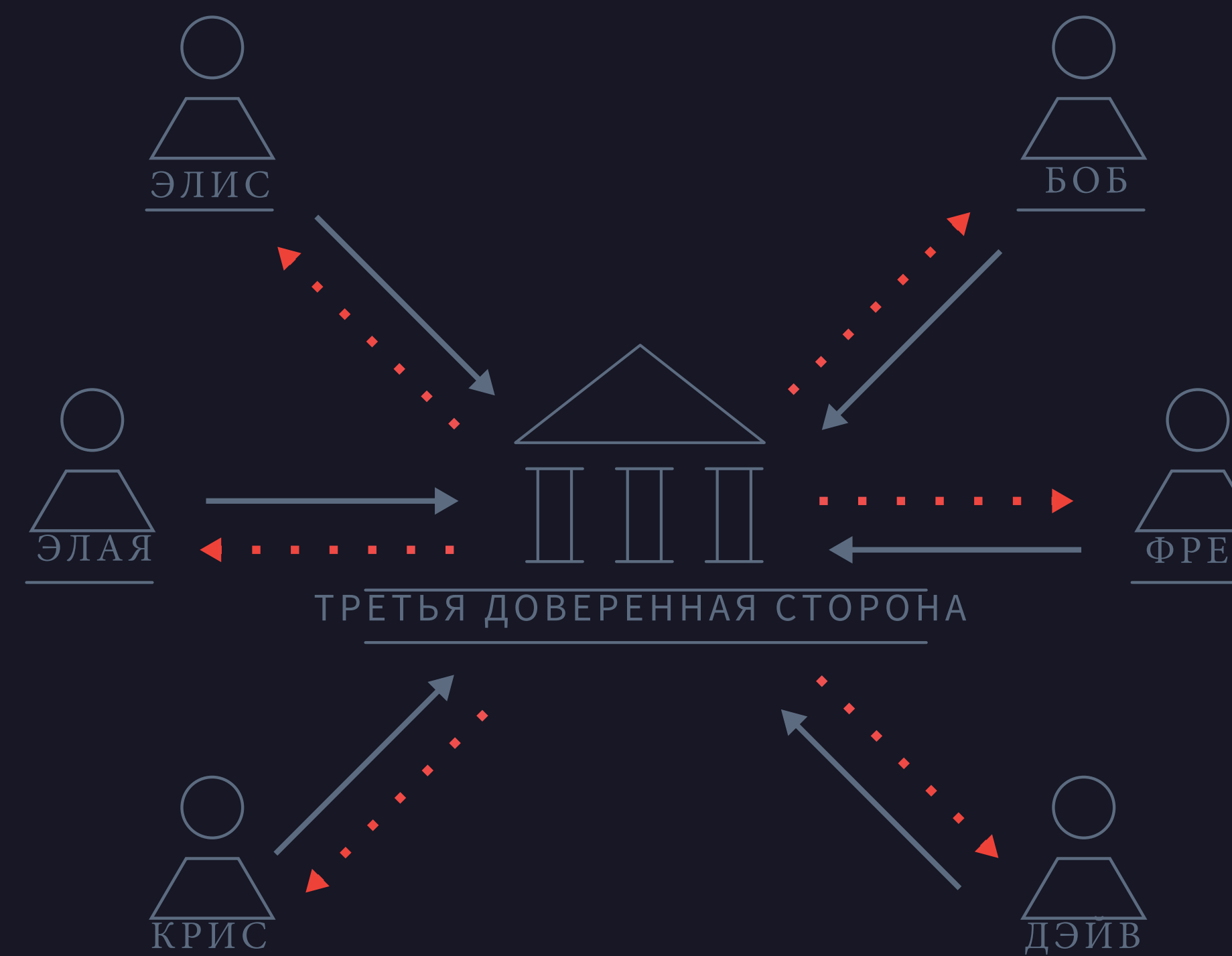
- **Ограниченный доступ**

Финансовые институты ограничивают тех, кто имеет доступ к финансовой системе и то, что они могут делать в финансовой системе.

- **Ограниченное владение/контроль**

В некоторой степени, мы не полностью владеем или контролируем наши активы, а имеем обязательства перед банком.

Банк может не выполнить данное обязательство в связи с неплатежеспособностью или конфискацией.



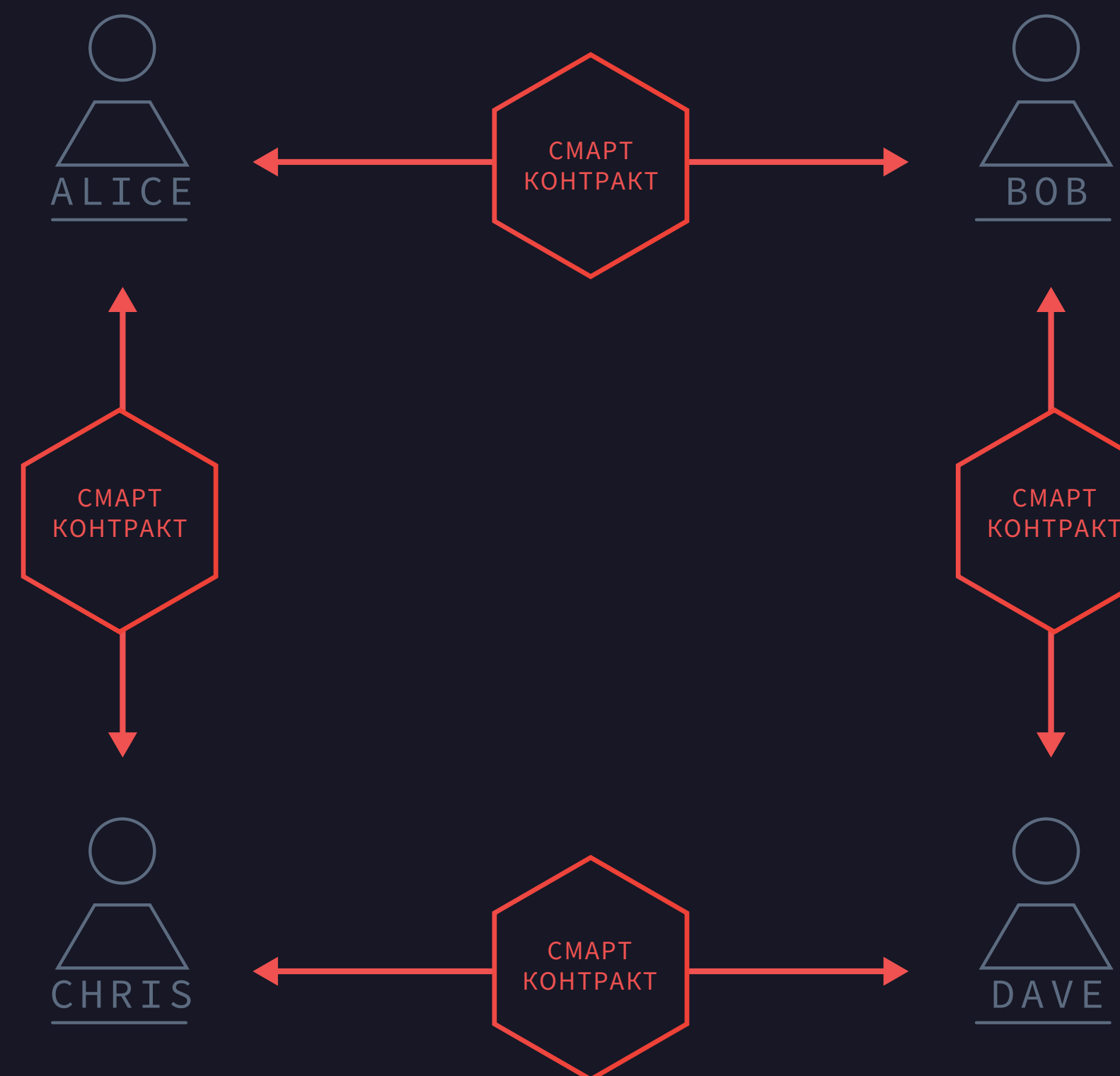


## Децентрализованная финансовая система

Если бы мы устранили нашу зависимость от сторонних организаций, то могли бы вернуть право собственности на наши активы и наше право выбора. Мы верим, что создадим более эффективные рынки с меньшим количеством бюрократии и комиссионных.

**Используя технологию Bitcoin, мы можем создать децентрализованную финансовую систему.**

Новый блокчейн, специально созданный для финансовой деятельности, позволяет нам владеть нашими активами криптографическим способом и обеспечивает денежные потоки, которые исходят из этих активов с помощью смарт-контрактов.





## Новый блокчейн специального назначения

Вселенная заполнена централизованными блокчейнами, ориентированные на финансы, и децентрализованными блокчейнами, ориентированные на нефинансовые пользовательские сценарии. Мы видим потенциал технологии распределённой базы данных в децентрализованных финансах. Zen попытается занять эту нишу на рынке.

**Неужели вам нужен новый блокчейн?**

	ДЕЦЕНТРАЛИЗОВАННЫЕ	ЦЕНТРАЛИЗОВАННЫЕ
ФИНАНСОВЫЕ	<b>Bitcoin, Zen</b>	Банковские цепочки, R3CEV, цифровые активы, вклады, прочее...
НЕФИНАНСОВЫЕ	Ethereum, Appcoins	Цепочки поставок, блокчейны IBM, Skuchain



## Bitcoin - это децентрализованные деньги

Мы верим в то, что **Bitcoin является высшей формой денег**. Сатоши решил ограничить возможности Bitcoin, потому что хотел сосредоточиться на использовании Bitcoin в качестве денег. Сатоши утверждал: «Наложение каждой системы кворума доказательства выполнения работы в мире в один пакет данных не масштабируется».

Bitcoin не хватает функциональности, необходимой для финансовой сферы деятельности.

Нам нужен новый блокчейн для децентрализованных финансов. Блокчейн, который поддерживает множественные активы и сложные конструкции владения.



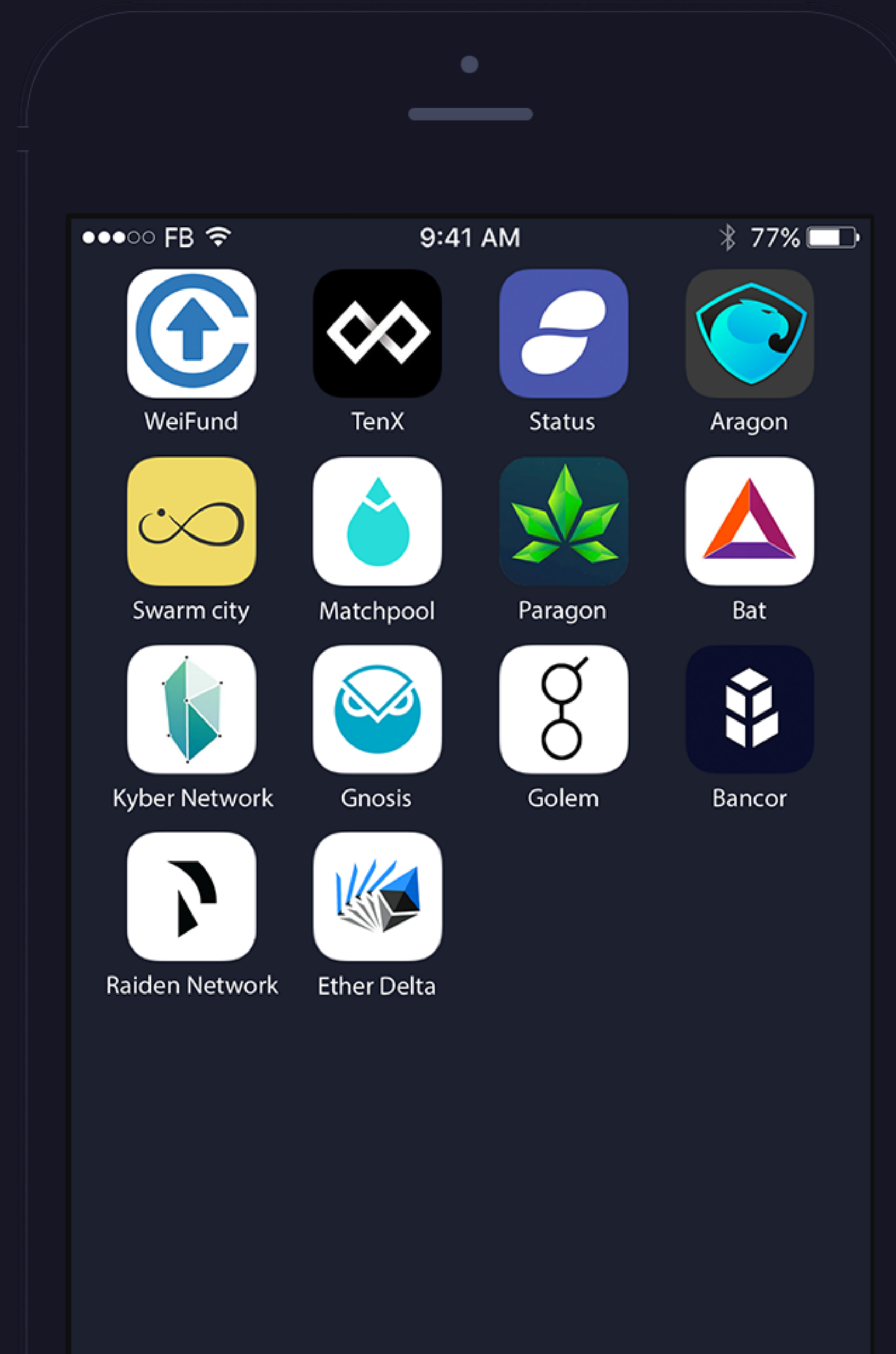
В мире существует  
примерно 21м слитков  
(400 унций каждый)  
золота в мире



## Ethereum - это децентрализованный вычислительный процесс

Цель Ethereum заключается в том, чтобы стать платформой для разработки децентрализованных приложений, например, Facebook или Uber без центрального сервера. Ethereum - это платформа, ориентированная на разработчиков. Она предоставляет удобный язык программирования (Solidity) и двоичный интерфейс прикладного программирования (ABI).

**Чтобы обеспечить данную функциональность, Ethereum предоставляет виртуальную вычислительную машину Ethereum (EVM), где подсчитываются вычислительные циклы и используется газовая система.**



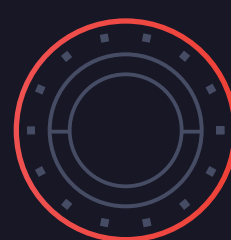




# Zen - это децентрализованные финансы

Zen - это новая платформа, ориентированная на децентрализованные финансовые инструменты. Zen позволяет использовать одноранговый доступ как к новым, так и традиционным активам.

Так же, как Биткойн устранил нашу зависимость перевода денег с банков, Zen устраняет нашу зависимость в финансах с банков.



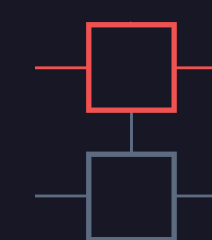
## ТОКЕНЫ

Активы хранятся в криптографическом кошельке.



## НАБОР АКТИВНЫХ КОНТРАКТОВ

“Среда выполнения” Zen эквивалентна Bitcoin stack или EVM Ethereum.



## ИНТЕГРАЦИЯ BITCOIN

Zen работает параллельно, и действует как дополнение к Bitcoin.



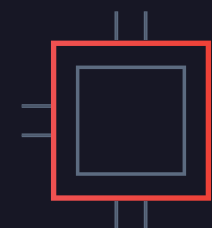
## КОНТРАКТЫ

Заменяют посредников децентрализованными механизмами депонирования



## ОРАКУЛЫ

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



## МУЛЬТИ-ХЕШ МАЙНИНГ

Стейкхолдеры голосуют, по каким хеш-алгоритмам будут получать вознаграждения за майнинг, соблюдая баланс между интересами майнеров и владельцев токенов.

## Токены

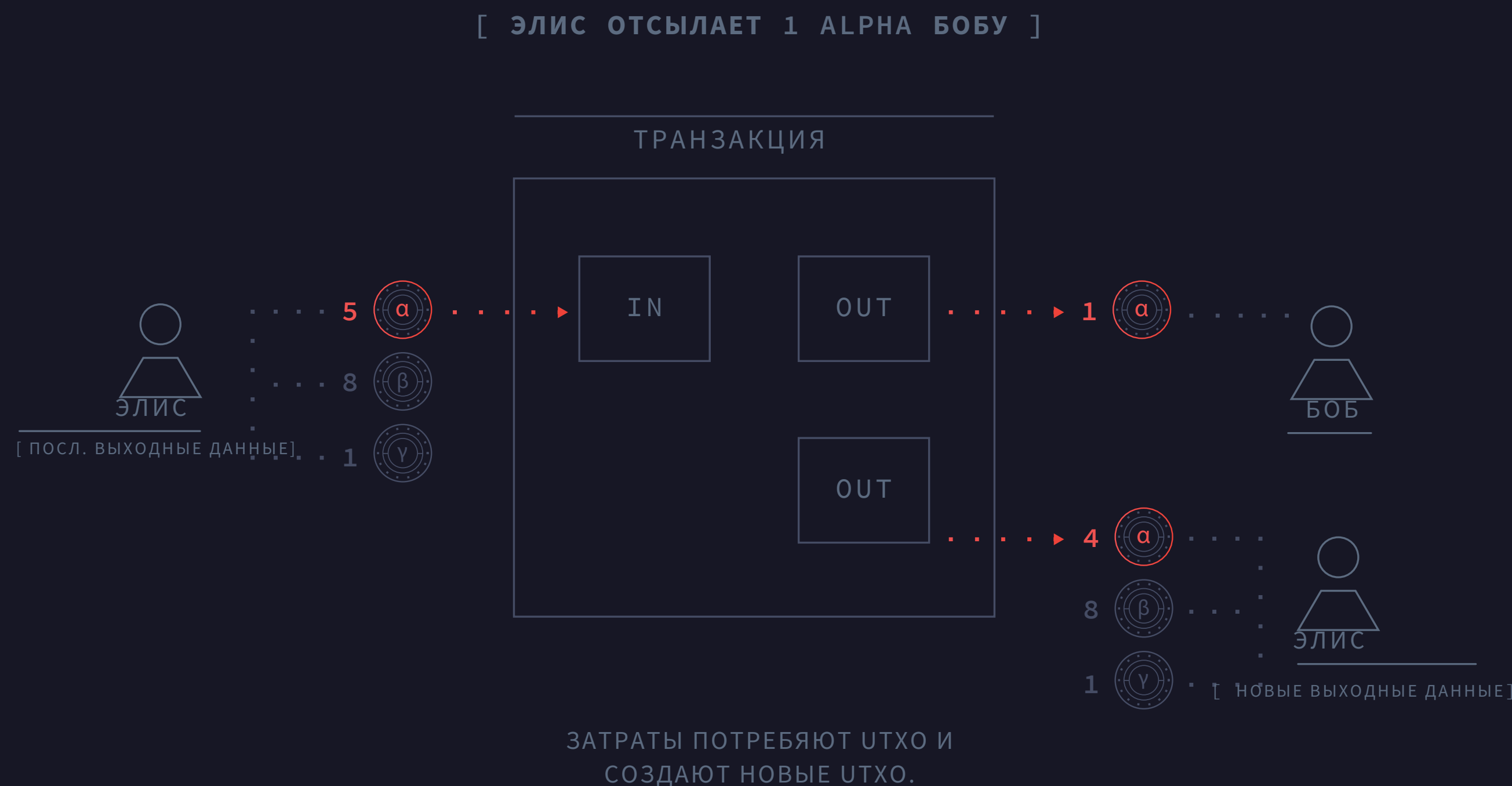
**В отличие от Bitcoin, который поддерживает только BTC, или Ethereum, у которого есть контракты ERC20, у Zen есть различные токены, встроенные на уровне протокола.**

Это означает, что каждый тип токена в Zen имеет схожий статус с нативным токеном Zen. Поэтому, каждый контракт в Zen может содержать и управлять любым другим токеном, и любой токен может использоваться для оплаты комиссий за транзакции майнерам.

Это представляет особый интерес, поскольку позволяет деноминировать финансовые контракты в “обычных” валютах, таких как доллар или евро. Токены хранятся в выходных данных транзакций, как и в Bitcoin, и могут быть разблокированы необходимыми разрешениями, а затем снова заблокированы в новых выходных данных.

Обычно, токены имеют ценность, поскольку:

- Люди верят в то, что они имеют ценность
- Они обеспечены контрактами, в которых содержится залог



## Контракты

**Контракты написаны на F\*** – функциональном, с зависимыми типами, высокоуровневом, формально верифицированном языке программирования. Формальное верифицирование в сочетании с моделью стоимости позволяет всем контрактам в протоколе Zen **доказать, сколько времени требуется для выполнения, прежде чем они когда-либо войдут в распределенную базу данных.**

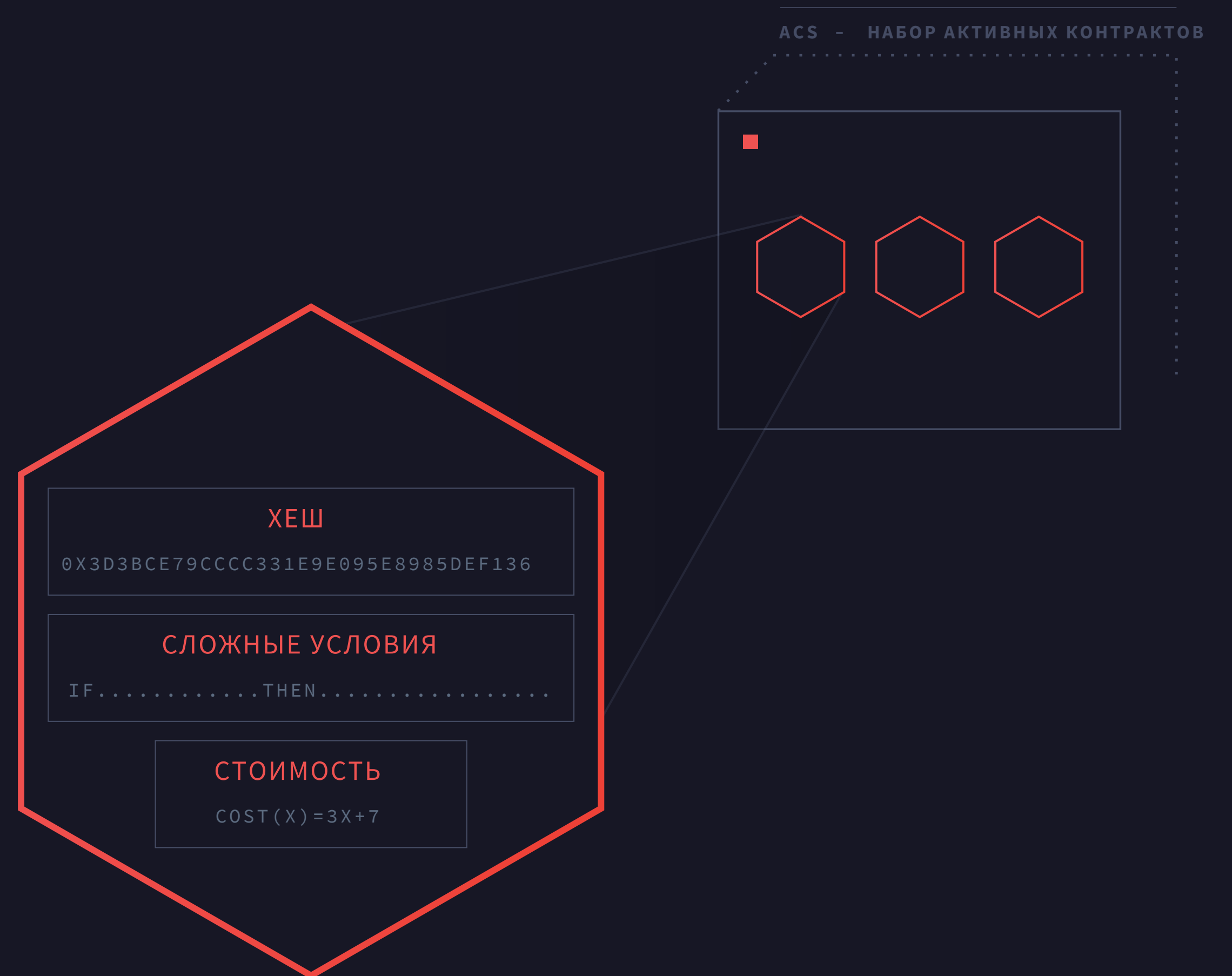
**Контракты неизменяемы** – (Их код никогда не меняется). Поэтому каждый контракт может иметь уникальный математический идентификатор (его хеш). Используя этот хеш, легко сопоставить токены и доказательства с контрактом.

### **Каждый контракт существует в изоляции от остальных контрактов**

**блокчейна** – Контракт может изменить состояние блокчейна и

взаимодействовать с другими контрактами только путём создания транзакции.

Контракты ничего не делают самостоятельно. Наоборот, они действуют как контрольные данные, которые используются, чтобы помочь узлам определять, принимать транзакцию или нет.



- [ КАЖДЫЙ КОНТРАКТ ИДЕНТИФИЦИРОВАН СВОИМ ХЭШЕМ ]
- [ КОНТРАКТЫ НАПИСАНЫ НА НАШЕМ ЯЗЫКЕ ZF\* ]
- [ КОНТРАКТЫ ИЗОЛИРОВАНЫ ДРУГ ОТ ДРУГАС ]

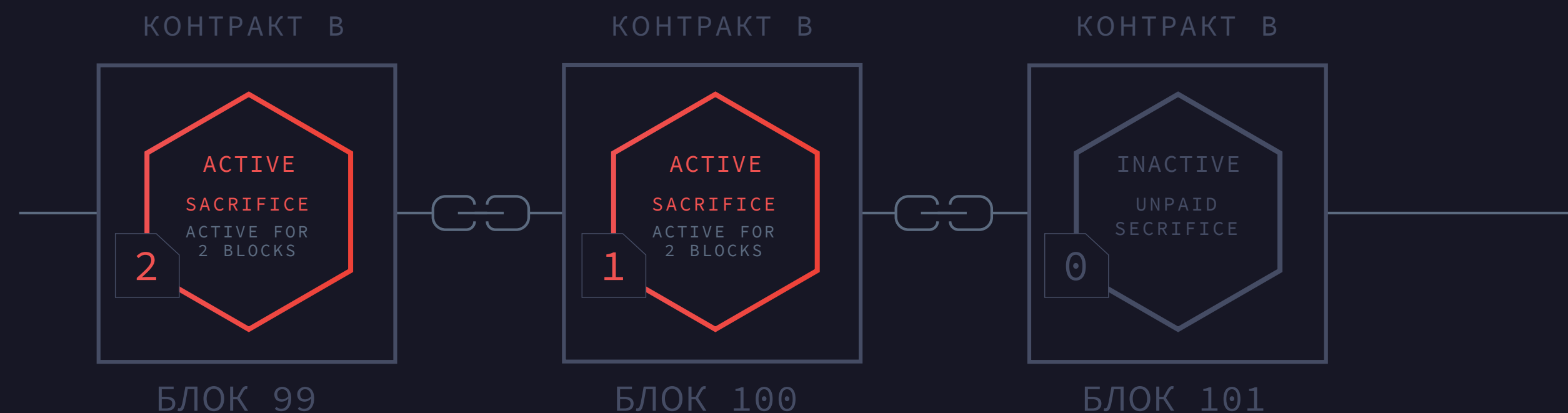
## НАБОР АКТИВНЫХ КОНТРАКТОВ

- При активации контракты преобразуются из F\* в машинный код.
- Скомпилированные контракты хранятся в оперативной памяти узла
- Контракты должны быть активны для создания сделок, таких как отправка или выдача токенов.
- Любой человек может активировать или продлить контракт применив жертвование контракта.



## Пожертвования контракта

- Пожертвования контракта компенсирует майнеров, которые должны обслуживать контракт. Пожертвование делится между майнерами, которые находят блоки в течение активного периода.
- В то время как комиссии за транзакции могут быть оплачены в любом токене, контракт жертвования должен быть оплачен в Zen.





# ПОЛЬЗОВАТЕЛЬСКИЙ СЦЕНАРИЙ - КОНТРАКТ НА РАЗНИЦУ AAPL

Давайте рассмотрим на то, как токены, контракты и набор активных контрактов работают вместе для создания однорангового финансового контракта.

1

- Элис пишет контракт на разницу (CFD) AAPL на 30 дней.
- Элис зарабатывает, если AAPL снижается.
- Её контрагенты зарабатывают, если AAPL повышается





# ПОЛЬЗОВАТЕЛЬСКИЙ СЦЕНАРИЙ - КОНТРАКТ НА РАЗНИЦУ AAPL

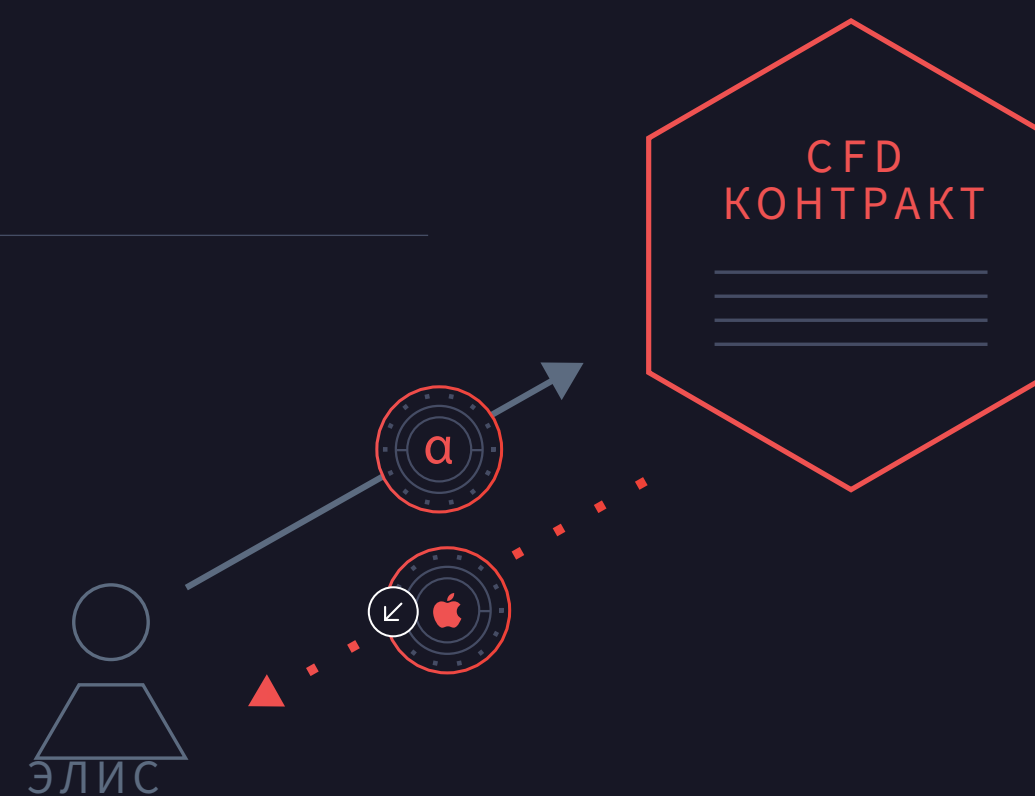
2

- Элис активирует контракт на 3 блока



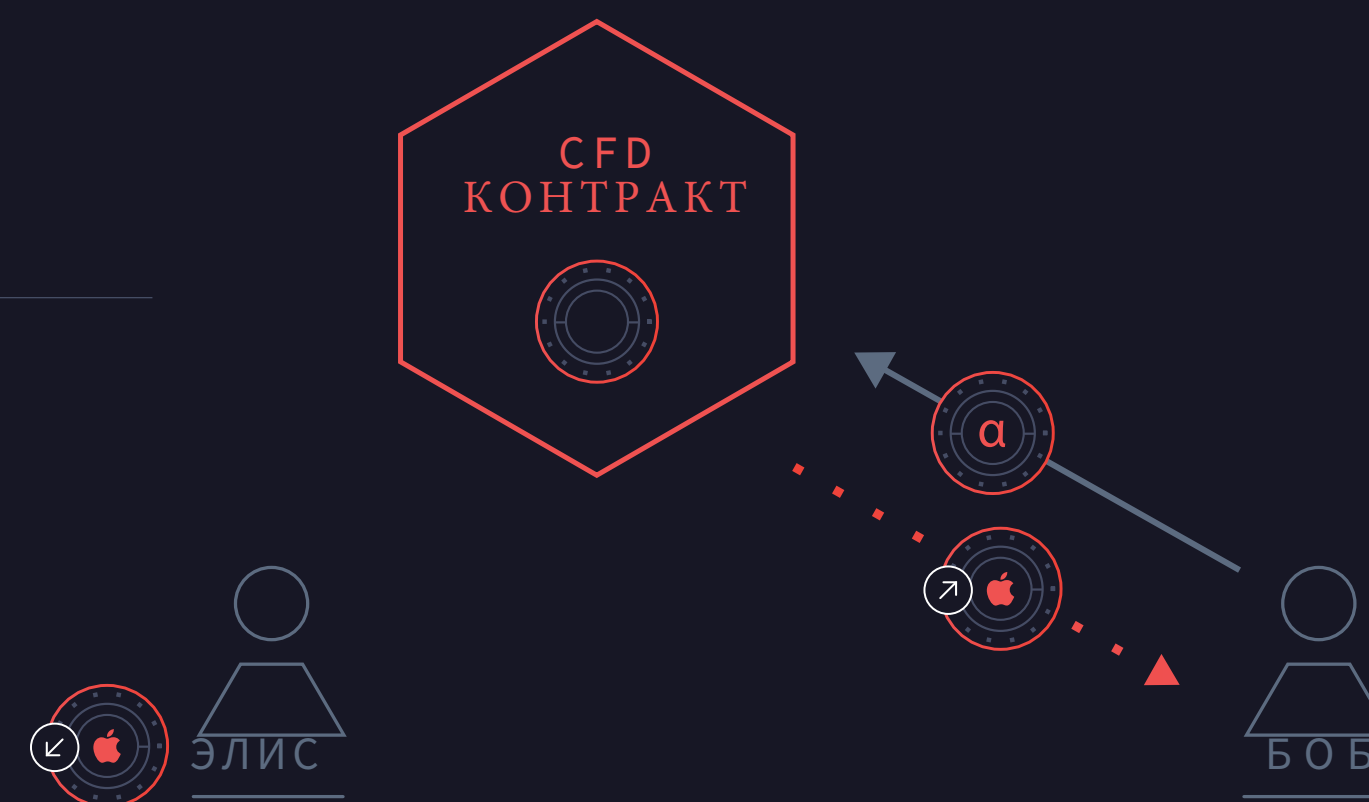
3

- Элис обеспечивает залог активного контракта, вводя короткую позицию.



4

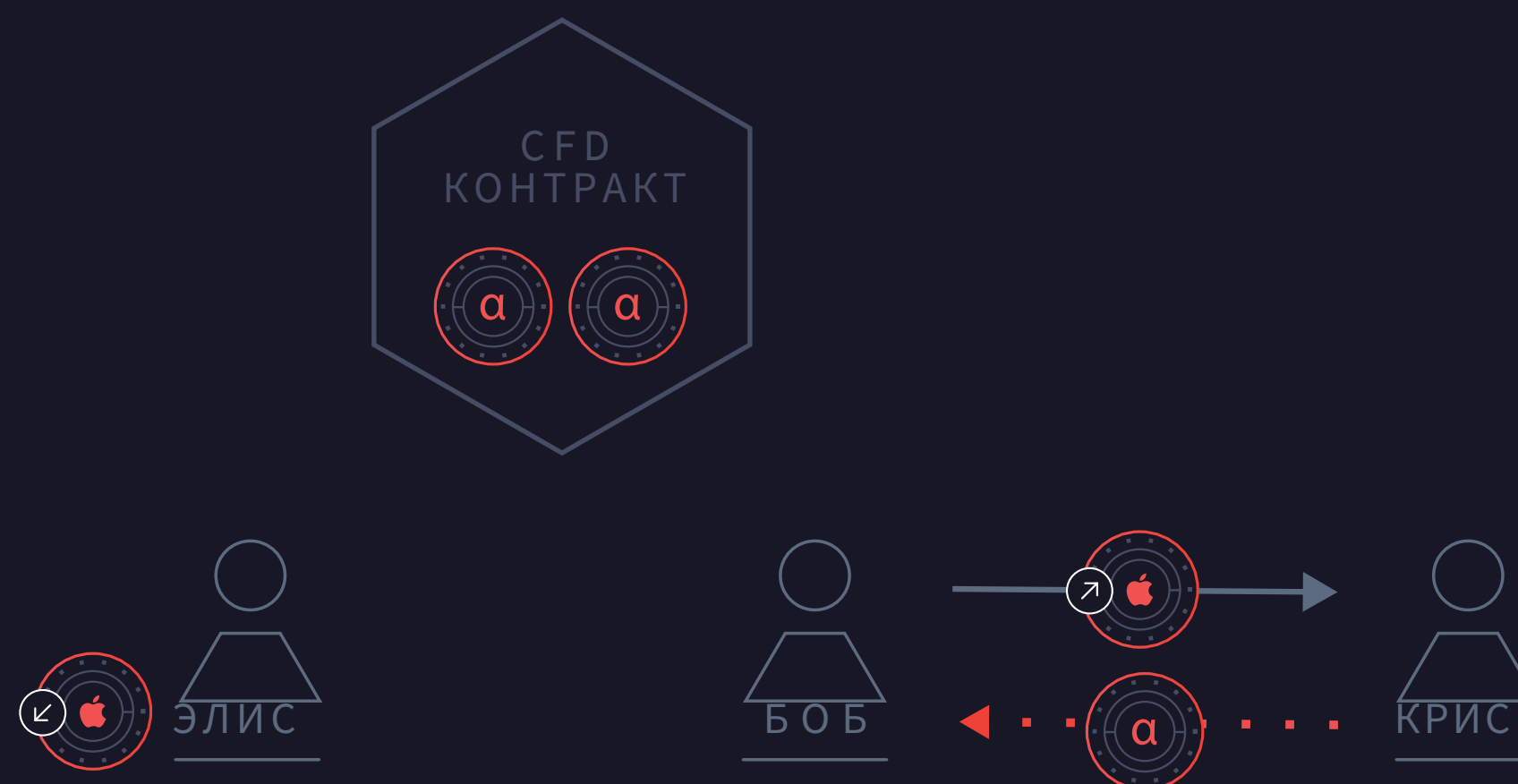
- Боб видит обеспеченный контракт и становится на другую сторону, отправляя токены.



# ПОЛЬЗОВАТЕЛЬСКИЙ СЦЕНАРИЙ - КОНТРАКТ НА РАЗНИЦУ AAPL

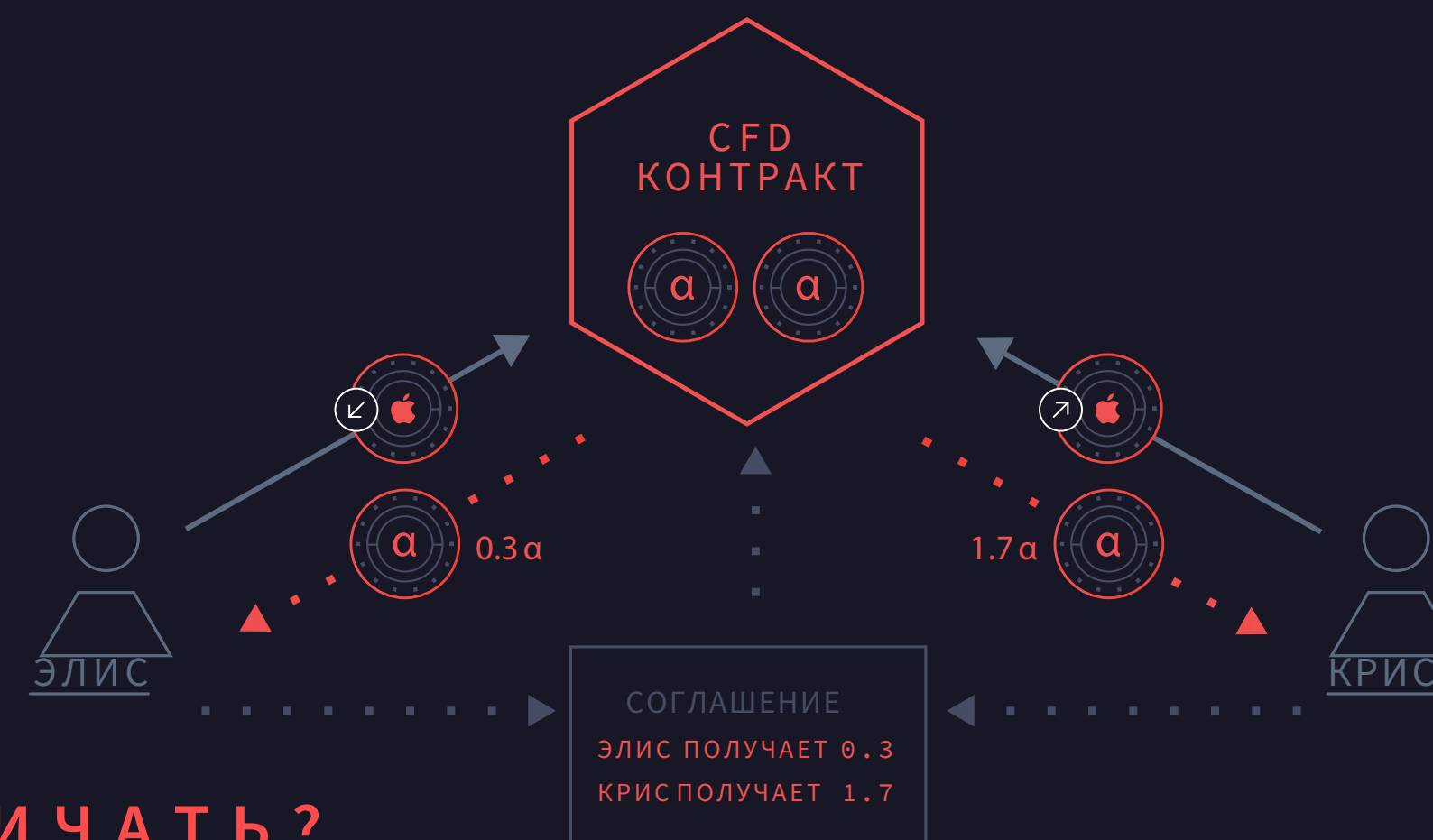
5

- **Контракт становится неактивным**
- **Боб все еще может выйти из своей позиции, продав свой контрактный токен кому-то другому.**



6

- **Спустя 30 дней контракт необходимо возобновить, чтобы вывести депозитные средства.**
- **Если Элис и Крис соглашаются что AAPL повысился на 70% они подписывают сделку, где Элис получает 0.3 а, а Крис получает 1.7 а.**



**НО ЧТО ДЕЛАТЬ, ЕСЛИ АЛИСА НЕ ХОЧЕТ СОТРУДНИЧАТЬ?**

# ПРЕДСТАВЛЯЕМ ОРАКУЛЫ

## Оракулы контракты позволяют работать с реальными данными

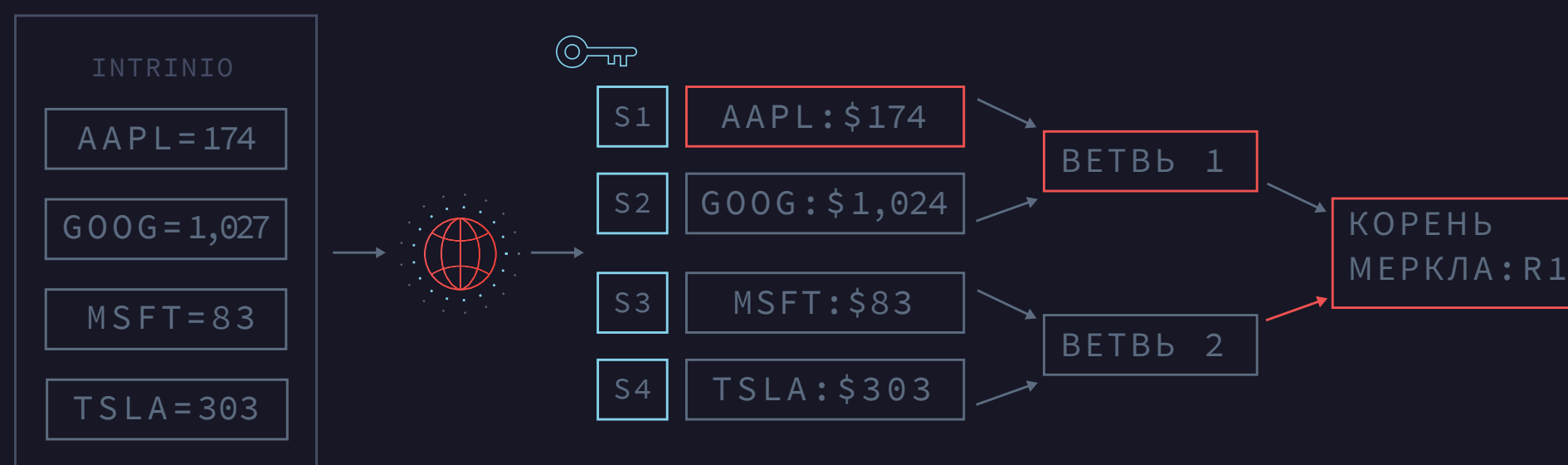
Контракты заблаговременно утверждают, на какие оракул(ы) будут полагаться, чтобы предоставить данные контракту.

Юридические контракты используют судей и рассматриваются в суде, а умные контракты используют оракулы и решаются в арбитражном порядке на блокчейне.

## Как работают оракулы:

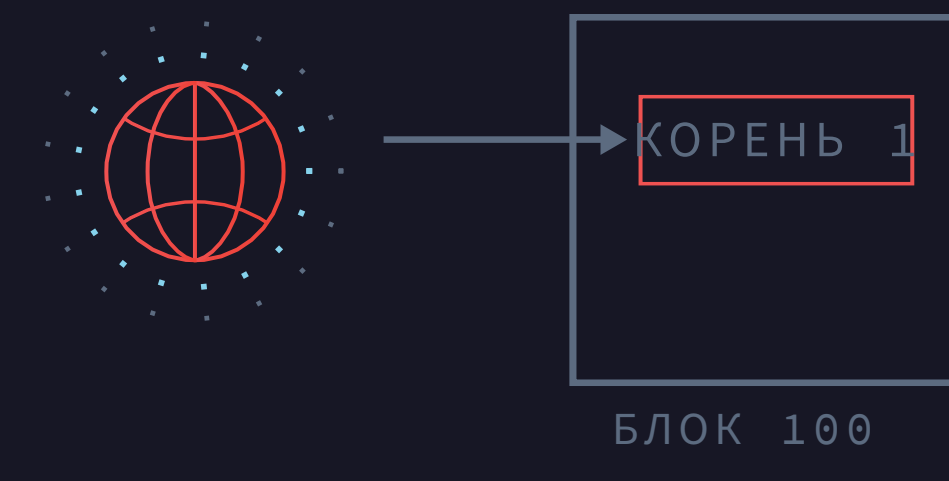
1

Оракулы извлекают данные из сетевых программных интерфейсов и сортируют их в дерево Меркл; Каждый лист консервируется секретным ключом/случайным кодом.



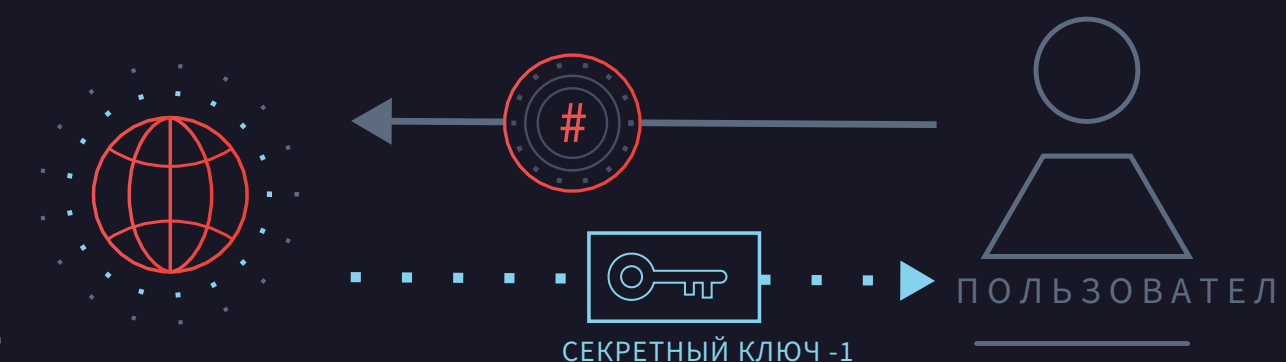
1

Оракул вставляет корень Меркла в блокчейн.



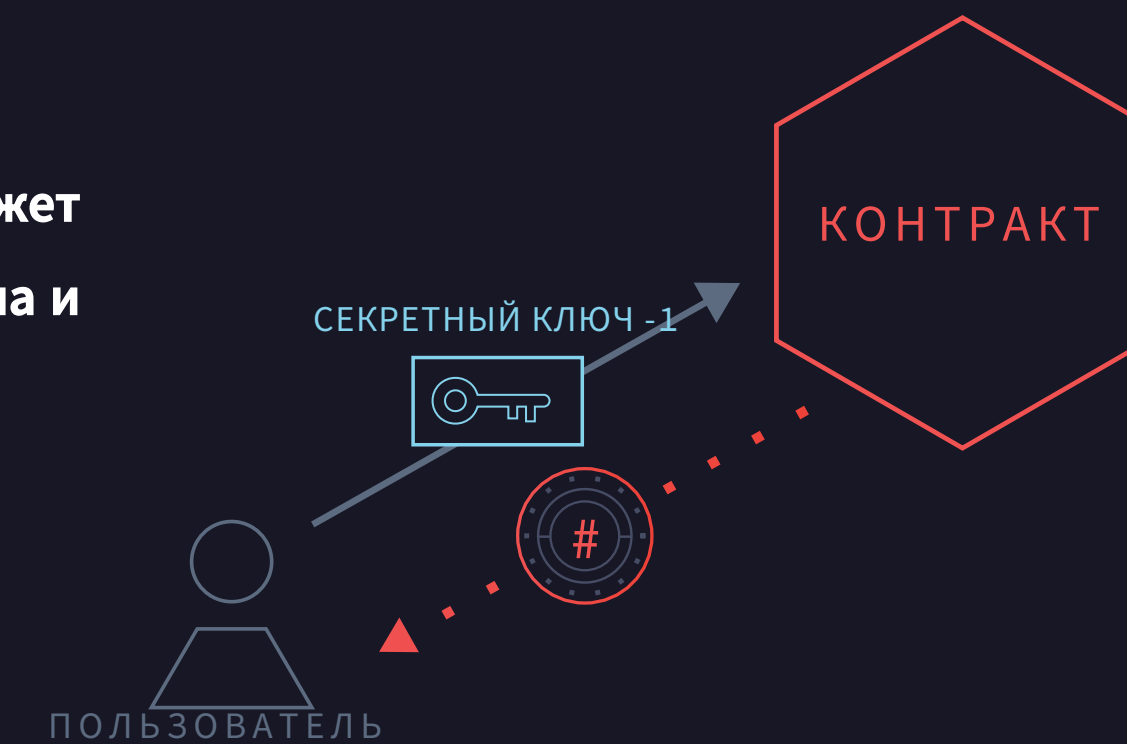
2

Когда пользователю необходимо предоставить контракт с определенным листом/фрагментом данных (т. е. для решения спора), пользователь оплачивает Оракул, а Оракул раскрывает случайный код.



3

Используя случайный код, пользователь может доказать контракту, какова совершаемая цена и вывести средства.



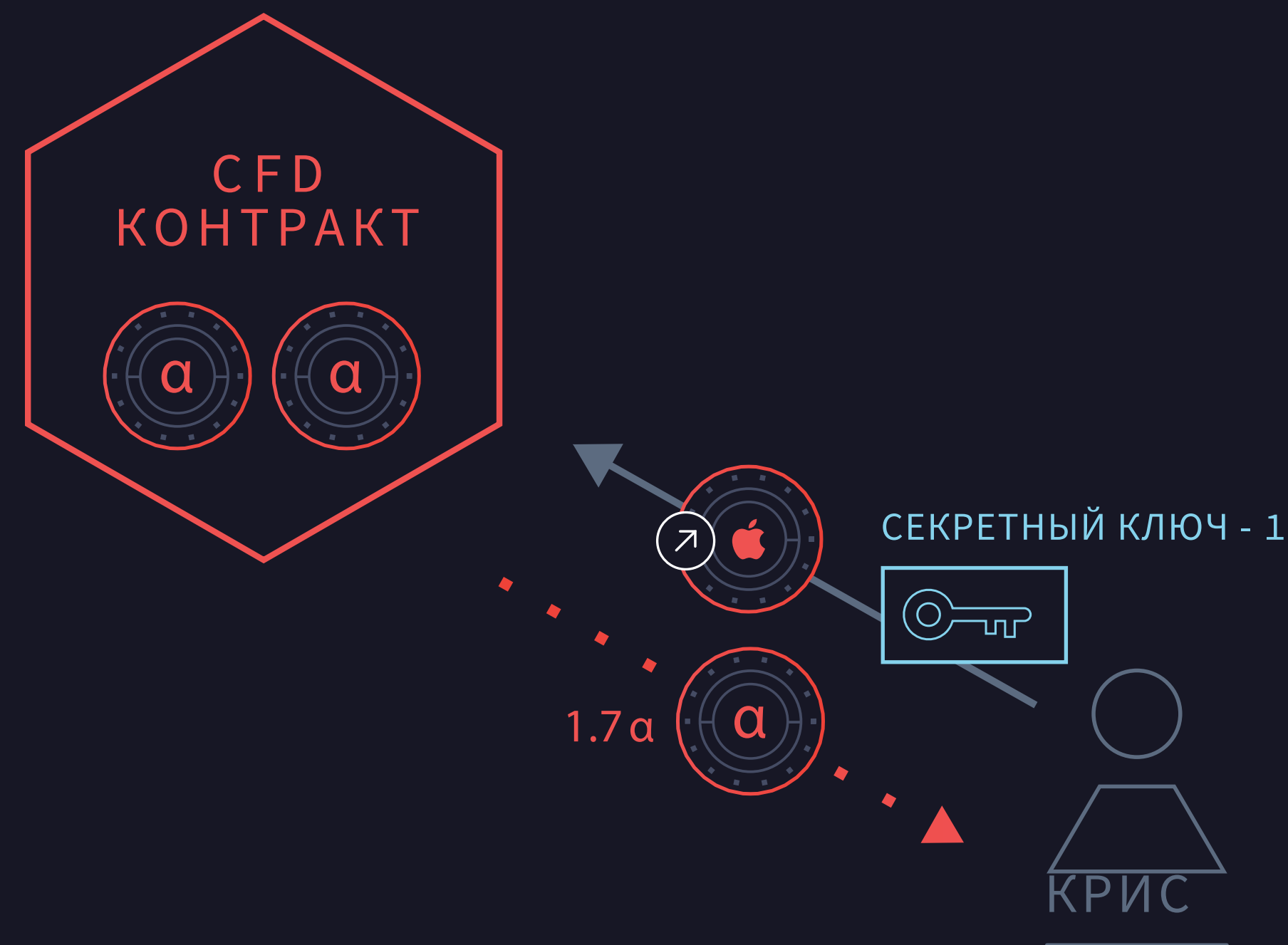


# ПОЛЬЗОВАТЕЛЬСКИЙ СЦЕНАРИЙ - ПРОДОЛЖАЕТСЯ КОНТРАКТ НА РАЗНИЦУ AAPL

## Разрешение споров

Поэтому в случае, если Элис и Крис не могут договориться, Крис заплатит оракулу, чтобы он предоставил ему секретный ключ (S1).

- Затем Крис отправляет секретный ключ и колл-опцион в контракт, а контракт оплачивает Крис 1.7 alpha.



# ИНТЕГРАЦИЯ С BITCOIN

Прошлые попытки увеличения сложности в блокчейн системах приняли две стратегии:

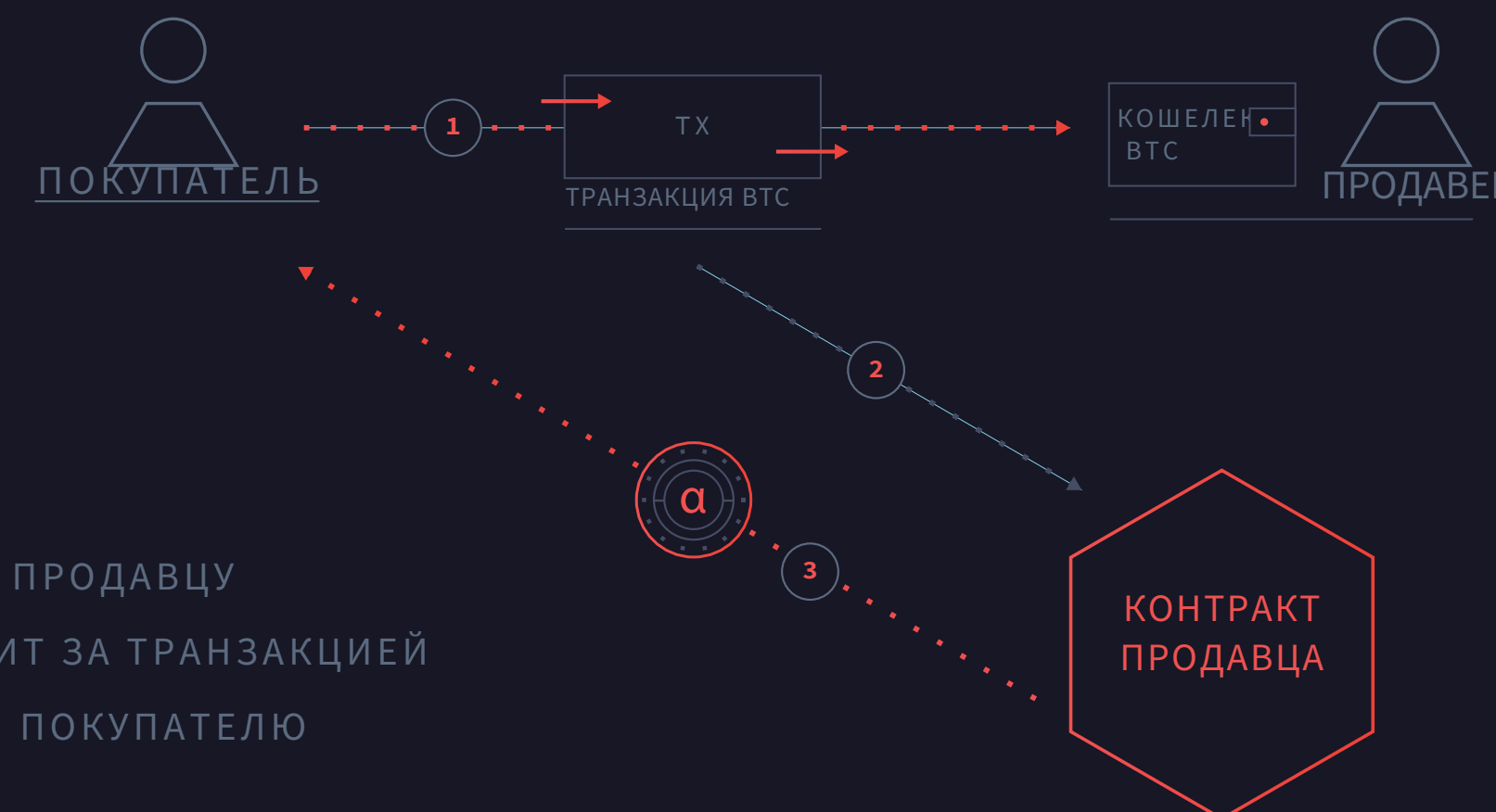
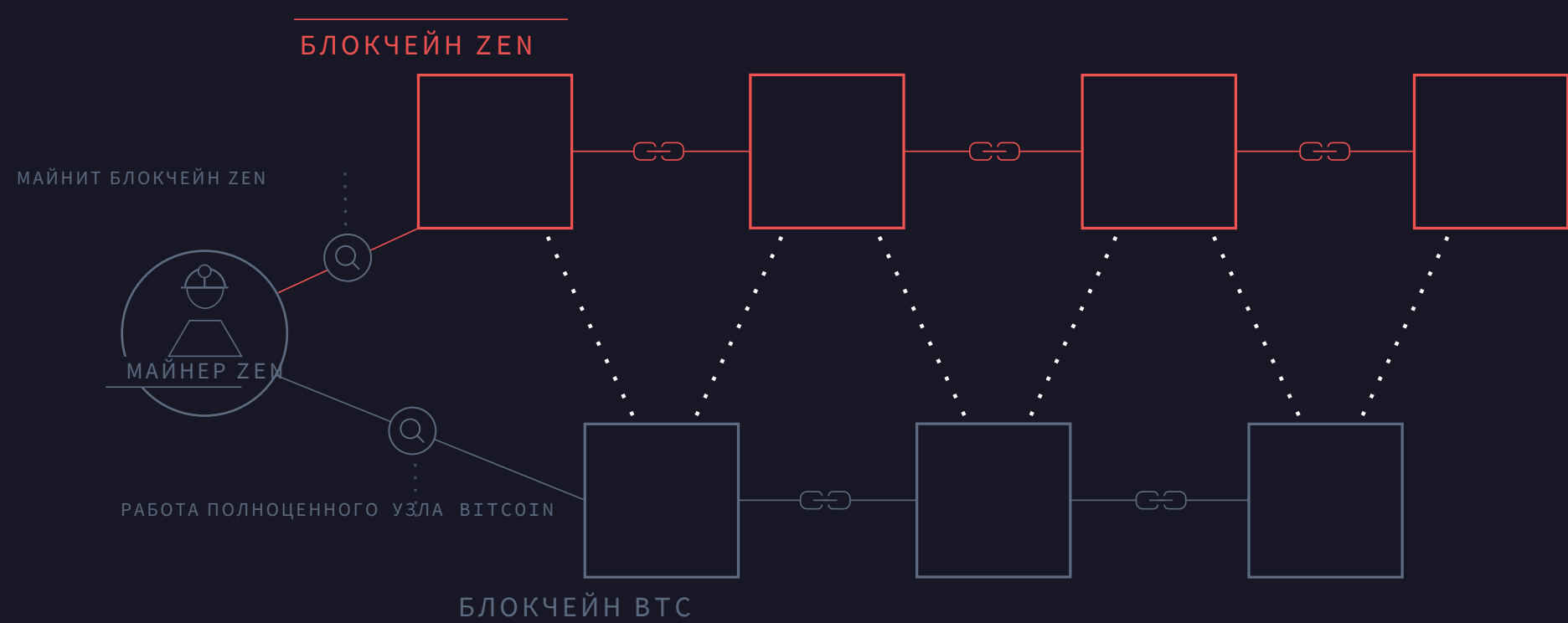
1 | Создать альтернативный блокчейн, который требует использования Альткоина.

2 | Создать дополнительный протокол, например сайд-чейн, который не имеет фирменного токена и тем самым отличается от механизмов стимулирования/безопасности Bitcoin.

Zen использует новый подход, самостоятельный блокчейн с собственным токеном, который работает параллельно с сетью Bitcoin.

**Объединенный консенсус** – Майнеры Zen добывают на блокчейне Zen и следят за блокчейном Bitcoin. Это позволяет использовать функциональность кросс-чейн.

**Кросс-чейн контракт** – Залог удерживается в цепочке Zen, но награда выплачивается на Bitcoin адрес.



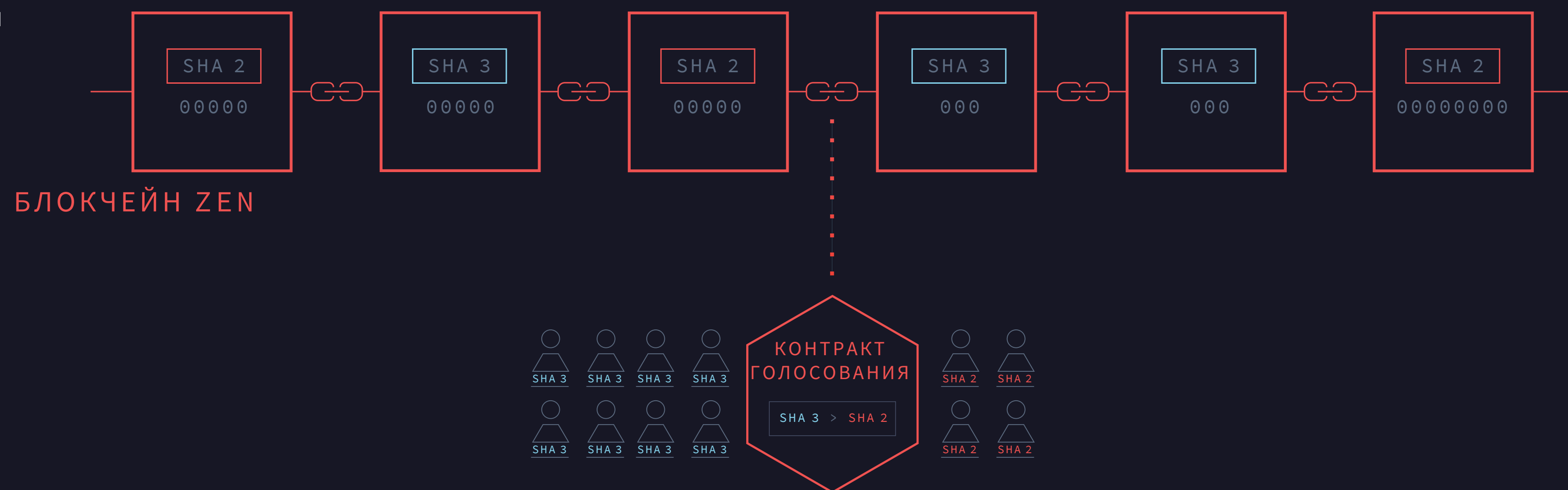
1. ПОКУПАТЕЛЬ ОТПРАВЛЯЕТ BTC ПРОДАВЦУ
2. ZEN КОНТРАКТ ПОДАВЦА СЛЕДИТ ЗА ТРАНЗАКЦИЕЙ
3. КОНТРАКТ ОТПРАВЛЯЕТ ТОКЕНЫ ПОКУПАТЕЛЮ



# Мульти-хеш майнинг – представление для владельцев

## токена

- Для поиска блока можно использовать различные хеш-функции.
- Каждая хеш-функция имеет различное требование к сложности.
- Целевое соотношение блоков, генерируемых каждой хеш-функцией, устанавливается держателями токенов Zen.



# ПЛАН РАЗВИТИЯ







# Альфа

В настоящее время у нас есть действующая альфа с распределенной базой данных, построенной с нуля, реализация ACS, смарт-контрактов, написанных на языке F\*, которые доказывают их стоимость, и оракулы, получающие цены на акции от [intrinsic.com](http://intrinsic.com)

Zen Альфа

СКАЧАТЬ

The screenshot displays the Zen Alpha wallet interface. At the top, there are navigation tabs: WALLET, CONTRACT, ASSETS, and TRANSACTIONS. The 'CONTRACT' tab is active, showing a 'Contract' section with a 'Hash' field containing 'ndjhfs342743524jkdlfs82394582304' and a 'Code' field with a sample script. Below this, it states 'Cost to activate is 48548 kalapas/block' and shows 'Blocks: 67,326 KALAPAS' with a 'TOTAL COST: 67,326 KALAPAS' label. An 'Activate' button is visible on the right.

The 'Your transactions' section shows a list of transactions for the asset 'ZEN'. The table below summarizes these transactions:

DATE	SEND / RECEIVE	STATUS	BALANCE
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

Summary statistics at the bottom:

- TOTAL RECEIVED : 7,345
- TOTAL SENT : 1,238
- TOTAL BALANCE : 100,270,130

At the bottom right, there is a status bar: 'Connecting... | Inbound connectivity initializeing | 23/46'.



# КОМАНДА ZEN

Мы создаем очень большой продукт при помощи маленькой команды



**Adam Perlow**

*ГЕНДИРЕКТОР*

Адам является выпускником университета IDC в области финансов, военнообязанным израильской армии и бывалым знатоком биткойна. Он знал, что биткойн добьётся успеха с первых дней как он впервые услышал о нем ещё в 2011 году.



**Nathan Cook**

*РУКОВОДИТЕЛЬ ТЕХНИЧЕСКОГО ОТДЕЛА*

Nathan является бывшим аспирантом математических наук Кембриджского университета. Если бы ему пришлось описывать свою работу в наши дни, то это было бы "участие в создании капитала". Он много читает.



**Sharon Urban**

*ВЕДУЩИЙ РАЗРАБОТЧИК*

Sharon - высококвалифицированный и опытный специалист по системам управления, который любит работать с хорошими парнями!



**Asher Manning**

*РАЗРАБОТЧИК, ФОРМАЛЬНЫЕ МЕТОДЫ*

Ash изучал математику, физику и вычислительную технику в университете McGill и работал над исследованиями в гомотопической теории типов.





# ZEN TEAM

Мы создаем очень большой продукт при помощи маленькой команды



**Doron Somech**

*ВИЦЕ-ПРЕЗИДЕНТ ПО  
ИССЛЕДОВАНИЯМ И РАЗРАБОТКАМ*

Doron, в прошлом был соучредителем и техническим руководителем в leverate.com



**Elan Perach**

*РУКОВОДИТЕЛЬ ПРОДУКТА*

Бывший сотрудник организации NFX.com, Elan запустил несколько стартапов, в крипто пространстве с 2011 года, а также он построил первый веб сайт по продаже биткоина в Израиле.



**Eleanor Milstein**

*АРТ-ДИРЕКТОР*

Eli - это наша гуру по дизайну продукта, обладает 6-летним опытом работы в нескольких стартапах как дизайнером продукта, так и соучредителем.



**Isaac Rodgin**

*МЕНЕДЖЕР ПО СВЯЗЯМ С  
ОБЩЕСТВЕННОСТЬЮ*

Успешно окончил университет IDC, получив степень в области бизнеса и компьютерных наук. Имеет более чем 5 летний опыт работы в продажах и управлении сообществом.



## Pamir Gelenbe

---

Pamir является управляющим партнёром в Libertus Capital, где он фокусируется на децентрализованных системах, корпоративном блокчейне, и цифровой валюте. Он является инвестором в Kraken, Ledger Wallet, Shapeshift и Crypto Facilities, а также в несколько децентрализованных протоколов. Ранее он служил в качестве партнёра в Hummingbird Ventures, а также работал в Morgan Stanley и D.E. Shaw. Pamir окончил Университет Duke и Колумбийский университет со степенью бакалавра естественных наук по электротехнике и магистра естественных наук в области операционных исследований.



## Ran Nussbaum

---

Ran Nussbaum - управляющий партнёр и соучредитель The Pontifax Group. Фонд управляет более чем 50 портфелями компаний по всему миру. До прихода в Pontifax он был партнёром крупнейшей израильской компании бизнес-аналитики и стратегического консалтинга.



## Ron Gross

---

Ron окончил Technion со степенью магистра в области компьютерных наук. Он работал в нескольких компаниях, начиная от небольших стартапов и заканчивая Google, и имеет большой опыт в области веб-архитектуры, безопасности и алгоритмов.

Ron непрерывно, с марта 2011 года, увлечён биткойном, распространяя информацию, знания и любовь к биткойну. Он является решительным сторонником источников с открытым исходным кодом, прозрачности и децентрализации власти и технологии. Ron являлся сооснователем израильской организации и биткойн-сообщества, а также исполнительным директором Mastercoin Foundation (первой мировой продажи токенов).