



Децентрализованный кросс-чейн протокол передачи ликвидности и данных



Содержание

1. Вступление.....	3
2. Вызовы.....	4
3. Обзор кросс-чейн рынка.....	6
4. Резюме проекта.....	9
5. Видение.....	10
6. Миссия.....	11
7. Обзор конкурентов	11
8. Решение: протоколы EYWA.....	14
9. Функции и преимущества.....	18
10. Принцип работы.....	21
11. Токеномика проекта.....	35
12. Команда.....	41
13. Юридическая информация.....	43
14. Источники.....	49

1. Вступление

Считается, что технология блокчейн имеет три основных ограничения, которые образуют трилемму блокчейна: масштабируемость, децентрализация и безопасность. Создателем Ethereum Виталиком Бутериным[1] было высказано предположение, что улучшение любого из трех основных аспектов блокчейна может быть достигнуто только в результате принесения в жертву двух других. Например, повышение безопасности возможно только путем принесения в жертву децентрализации и масштабируемости, в то время как масштабируемость требует жертв в виде децентрализации и безопасности. Такое положение дел и неотъемлемые ограничения технологии обуславливают сложности в распространении децентрализованных сетей, их проблемы с безопасностью и растущей централизацией, что проявляется в сегментации крипторынка на многочисленные блокчейны, биржи и протоколы.

Однако, помимо трех столпов постулата, существует четвертый важный фактор, который препятствует принятию и распространению блокчейна как технологии среди пользователей на рынке в целом и как жизнеспособной системы международных платежей в глобальном масштабе. Отсутствие надлежащих связей и взаимодействия между различными существующими блокчейнами превращает децентрализованную среду в большой архипелаг сегрегированных систем, которые конкурируют между собой и часто настолько самофокусированы, что векторы их развития противоречат друг другу.

Распространение феномена криптовалюты на традиционные рынки в виде нового класса активов привлекает все большее внимание к децентрализованной экономике в целом. Такую динамику и движения институциональных и розничных инвесторов лучше всего наблюдать в рамках децентрализованного финансового рынка, или DeFi, который привлек интерес не только обычных пользователей, но и целых корпораций, желающих извлечь выгоду из блокчейн технологий как новой силе в мире финансов.

Сектор DeFi стремительно растет, порождая гонку экосистем. На этом рынке регулярно появляются новые игроки. По прогнозам аналитиков, капитализация рынка DeFi должна была достичь 100 миллиардов долларов к концу 2021 года. Но по данным coingeko, на конец первого квартала эта отметка была уже достигнута при ежедневном объеме торгов в диапазоне 12-14 миллиардов долларов. Вероятно, капитализация DeFi может вырасти на порядки в течение нескольких лет, учитывая интерес институциональных инвесторов.

Лидером рынка DeFi является Ethereum, за ним следуют Binance Smart Chain, Polygon (Matic), Huobi Ecochain, стремительно набирающие объемы ликвидности, также есть и другие экосистемы, такие как Polkadot, Avalanche, Tron, Neo, Solana, Near, Terra и другие.

Каждая экосистема разрабатывает и продвигает свои блокчейны и протоколы на их основе, и у каждого блокчейна в DeFi есть свои слабые места: у одних слишком дорогие транзакции (например, Ethereum), у других – высокая централизация (как у Binance Smart Chain), у третьих недостаточно ликвидности. В конечном итоге все накладные расходы и сложности ложатся на пользователей. Им требуется заводить

разные кошельки и держать в них нативные монеты для оплаты транзакций в каждом из блокчейнов, и это очень далеко от комфортного пользовательского опыта.

Крупнейшие DeFi-протоколы, такие как AAVE, Uniswap, Curve, Sushi Swap, Cream постепенно увеличивают количество поддерживаемых блокчейнов, стремясь уйти от огромных комиссий Ethereum, отдавая предпочтение решениям, позволяющим масштабировать их бизнес, – Polygon, Fantom, Arbitrum, Optimism и многим другим. Все крупные блокчейн-экосистемы создают мосты между собой – Polkadot (Kusama), Ethereum, Solana, Cosmos, Terra, Avalanche – и стремятся выйти за границы своего блокчейна.

Эти факты говорят о том, что будущее DeFi – стать интернетом блокчейнов или, как еще его называют, – Web-3.0.

Поэтому мы считаем, что траектория развития DeFi направлена в сторону усиления и унификации взаимодействия между множеством блокчейнов, имеющих различные свойства и предназначение.

2. Вызовы

Большая часть протоколов DeFi происходит из Ethereum, те протоколы, которые находятся внутри Ethereum, испытывают сложности от его недостатков – низкой пропускной способности и высоких транзакционных комиссий.

Есть множество попыток решить эти проблемы. Запускаются альтернативные решения, наследующие логику работы Ethereum, например Tronchain, Binance Smart Chain, Huobi EcoChain. Они решают проблему пользователей и разработчиков DeFi-протоколов в части стоимости транзакций и скорости работы, но при этом приносят в жертву децентрализацию.

Существует множество протоколов второго уровня – сайдчейны, роллапы, использующие криптографию нулевого разглашения для решений задач масштабирования и анонимизации, такие как ZK-Sync, Aztec Network, Dusk network, Starknet и многие другие.

Есть блокчейны, которые имеют достаточно высокую децентрализацию и совместимы с Ethereum, такие как Matic (Polygon), Avalanche, Celo и Near. Есть блокчейны, которые идут своим путем: Solana, Polkadot, Cosmos, FreeTON, Cardano.

У подобных экосистем иные проблемы – привлечение новых пользователей, обучение разработчиков новым языкам программирования и подходам к разработке, привлечение ликвидности. Иными словами, им не хватает комьюнити во всех смыслах этого слова.

Мы с интересом наблюдаем за происходящими процессами и понимаем, насколько большую работу необходимо проделать всему глобальному сообществу разработчиков DeFi, чтобы создать решения для массового рынка. Мы искренне восхищаемся талантливыми и умными людьми, которые делают это, их видением будущего.

Поэтому наш вызов состоит в том, чтобы создать экосистему, которая будет удобным инструментом в руках разработчиков DeFi-экосистем и протоколов. Инструментом, который позволит DeFi-проектам работать в синергии, используя преимущества и возможности всех лучших DeFi-экосистем и протоколов. EYWA дает возможность разным блокчейн-экосистемам взаимно обогащать друг друга в части ликвидности, комьюнити, технической интеграции разных DeFi-проектов.

Кроме того, мы стремимся решать проблемы конечных пользователей здесь и сейчас, создавая прикладной функционал, призванный упростить пользовательский опыт и открыть доступ к новым возможностям для заработка.

Итак, перечислим актуальные проблемы DeFi:

1. Плохой пользовательский опыт.
2. Фрагментация ликвидности между множеством пулов и блокчейнов.
3. Множество разных стеков технологий, плохо совместимых между собой.
4. Высокие комиссии.
5. Комиссии во множественных активах при кроссчейн-взаимодействии.
6. Низкая пропускная способность блокчейнов.
7. Отсутствие готовых инструментов и стандартизированного подхода к взаимодействию блокчейнов.

Нередко перемещаемые между блокчейнами активы являются неликвидными и не интегрированы в существующие протоколы DeFi. И это большая проблема как для разработчиков, так и для пользователей, потому что для полноценной работы им потребуется взаимодействие сразу с несколькими протоколами.

Как правило, люди перемещают активы между разными блокчейнами для вполне конкретных целей: трейдинг, участие в IDO, кредитование, участие в выгодном фарминге/стейкинге и при этом они хотят сэкономить на стоимости транзакций.

Иными словами, для конечных пользователей необходимо комплексное решение уровня приложения. Необходимо иметь мгновенную кроссчейн-ликвидность при обмене и доходном фермерстве, предоставлять пользователю информацию в удобном для него виде и минимизировать количество операций. И все это ради того, чтобы комфортно перемещать капитал между разными блокчейнами в рамках своей стратегии инвестирования или иных задач. По нашему мнению, с точки зрения разработчиков DeFi, использующих имеющиеся DeFi-протоколы как элементы финансового LEGO, назрела необходимость в новом инструменте – универсальном протоколе кроссчейн-взаимодействия, поддерживающем разнородные блокчейны. Это необходимо, чтобы масштабировать существующие и создавать новые децентрализованные приложения, сосредоточиваясь на разработке их уникальной бизнес-логики, а не на решении проблем взаимодействия между блокчейнами.

Такой инструмент добавит новое измерение в финансовое LEGO – представьте себе, раньше вы играли в обычный 2D Tetris, и в какой-то момент он стал трехмерным и фигуры приобрели объем. Такая игра будет намного увлекательнее!

3. Обзор кросс-чейн рынка

В общем случае задача интероперабельности между блокчейнами сводится к передаче абстрактных данных – не активов, а именно данных. Иными словами, требуется передать хеш транзакции tx и ее содержимое $source\ data$ из блокчейна А в блокчейн В и выполнить в блокчейне В формальное доказательство существования именно этой транзакции с ее данными в исходном блокчейне А. Содержимым транзакции может быть закодированный вызов «удаленного» смарт-контракта. Кроме этого, нас интересует, чтобы соединяемые блокчейны могли быть гетерогенными, то есть имеющими разную финальность.

Примером интероперабельного решения в рамках гомогенных блокчейнов с конечной финальностью могут служить проекты Cosmos и Polkadot, которые по сути являются изолированными экосистемами. Какие подходы существуют для решения такой задачи?

Большинство проектов решают проблему в частном случае – рассматривая передачу данных между блокчейнами как задачу по передаче активов (REN, ChainSwap, ThorChain, Anyswap, Binance Bridge). В качестве исключения можно привести проекты Axelar Network и Poly network, которые, как и мы, предусматривают возможность осуществления кроссчейн-вызовов между блокчейнами, не ограничиваясь работой только с активами.

Для переноса ценности между блокчейнами многие проекты, включая наш, используют синтетические активы, также их называют обернутыми (wrapped) или привязанными (pegged).

В этом случае определенная сумма актива $X(A)$ блокируется в смарт-контракте или кошельке в блокчейне А как обеспечение (Anyswap, ChainSwap, Poly network) либо в промежуточной сети (ThorChain, REN). Далее данные об этом передаются в блокчейн В, где осуществляется выпуск синтетического актива $sX(A)$ на такую же сумму либо отправка аналогичного токена $X(B)$ из кошелька/смарт-контракта.

Уязвимость этого метода состоит в проблеме «доверенного оракула». Для того чтобы передать данные из блокчейна А в блокчейн В, необходимо использовать внешнюю по отношению к этим блокчейнам сущность – децентрализованную сеть оракулов (или блокчейн, являющийся сетью оракулов). Это важно, потому что вредоносный оракул может провести атаку *man-in-the-middle*, прислав недостоверные данные.

Для решения проблемы доверенного оракула применяют следующие подходы:

- централизованная защищенная сеть, контролируемая одним владельцем – Binance Bridge;
- построение промежуточного блокчейна с BFT-консенсусом (Byzantine Fault Tolerance), используя MPC (Multi Party Computation), основываясь на принципах Proof-of-Stake (PoS) либо Proof-of-Authority (PoA) – Poly network, Axelar network, ThorChain, ChainSwap;
- гибридный подход, сочетающий в себе MPC и PoS, но без создания собственного промежуточного блокчейна, использующий для осуществления логики работы PoS смарт-контракты в публичном блокчейне – REN.

Дальнейшую классификацию решений можно провести по способу хранения и источнику происхождения ликвидности. Ликвидность в системе может быть кастодиальной – в этом случае ее контролирует один агент или группа агентов; и некастодиальной – когда ликвидность предоставляется и контролируется множеством независимых друг от друга игроков. Рассмотрим конкретные случаи:

Централизация + кастодиальная ликвидность

Создание централизованного доверенного сервиса-оракула либо сети оракулов, которые полностью контролируются разработчиками системы, и использование централизованной кастодиальной ликвидности. Очевидно для децентрализованной системы не подходит, хотя вполне успешно применяется на практике для решения частных задач отдельных проектов и имеет большую гибкость[2].

PoS/PoA MPC блокчейн + кастодиальная ликвидность

Создание промежуточного блокчейна-моста С для пересылки активов между блокчейнами А и В (ThorChain[3], Anyswap[4], Axelar network[5]).

Блокчейн С строится на основе входящих транзакций от подключенных блокчейнов. Там хранится информация о передаваемых данных и консенсусе узлов или оракулов, каждый из которых является узлом сети С. В целевом блокчейне В, как правило, производится merkle-доказательство существования транзакции в исходном блокчейне А (подобно Near Rainbow Bridge[6]) либо доказательство существования записи об этой транзакции в цепочке С.

Зачастую все передаваемые между блокчейнами А и В средства распределенно хранятся на специальных пороговых кошельках (используется схема пороговой подписи – TSS[7]), которые сгенерированы участниками сети С, то есть они подконтрольны им (ThorChain, Axelar network, Anyswap v2).

В блокчейне С в качестве консенсуса используется BFT-консенсус совместно с Proof-of-Stake (PoS) либо Proof-of-Authority (PoA) и TSS.

Этот метод по своей сути схож с первым (централизацией), он более децентрализован, но менее надежен, в силу того применяется PoA либо PoS – высоким залогом и малым (менее сотни) числом узлов. Таким путем не достичь высокой децентрализации и безопасности системы, но при этом система становится менее гибкой и масштабируемой, нежели backend. Самый главный недостаток подобных блокчейнов, по нашему мнению, состоит в том, что вместо того, чтобы работать как транспортный уровень, они становятся распределенным кастодиальным хранилищем средств, управляемых относительно небольшой группой лиц.

РоА MPC блокчейн + некастодиальная ликвидность

Poly network[8] – на основе блоков из разных блокчейнов строится полицепь – сайдчейн, включающая в себя все входящие кроссчейн-транзакции. Цепочка строится на принципах BFT и использует MPC – схему пороговой подписи. На основе этой цепочки производятся доказательства для целевых блокчейнов.

Основным минусом данного подхода мы считаем непрозрачность членства в этом блокчейне – для участия необходимо получить разрешение от двух третей участников сети путем их голосования. Хотя цель разработчиков блокчейна как раз и состояла в том, чтобы построить доверенную сеть, управляемую уважаемыми организациями.

К преимуществам можно отнести некастодиальную ликвидность, которая не контролируется участниками сети, а размещается в конечных блокчейнах любыми разработчиками DeFi, которые хотят построить свое решение на основе этого протокола, а также иметь возможность совершения кроссчейн-вызовов между блокчейнами.

РоА/PoS MPC без промежуточного блокчейна + кастодиальная ликвидность

REN[9] – проект использует REN VM, finite state machine, производя MPC, – многосторонние вычисления с нулевым знанием (zero knowledge) по нахождению публичного и приватного адреса для депозита криптовалют различных блокчейнов, в том числе не имеющих смарт-контрактов (BTC, LTC, ZEC, FIL). При этом никто из участников не может узнать ни одного приватного ключа.

Когда пользователь производит депозит на указанный адрес, в одной из сетей назначения создается привязанный актив, например в Solana это может быть renBTC. REN играет важную роль в экосистеме DeFi, токенизируя несовместимые активы.

Вычисления в сети REN производят так называемые Darknodes[10], сама сеть не является блокчейном, а стремится к достижению консенсуса PoS со слешингом (штрафами), используя смарт-контракты, размещенные в публичном блокчейне Ethereum. Для запуска ноды необходимо разместить в смарт-контракте залог в 100 000 REN. Разработчики REN в настоящий момент полностью контролируют сеть, поэтапно переходя к полной децентрализации[11].

Примечательно, что при этом сеть Darknodes насчитывает уже свыше 1700 узлов[12], что говорит о высоком потенциале децентрализации и надежности системы. К минусам можно отнести кастодиальное хранение ликвидности внутри сети, хотя надо отдать должное: это, вероятно, единственный способ работы с блокчейнами, не имеющими смарт-контрактов. Главные минусы – закрытый исходный код узла, потому что разработчики предоставили только часть кода и два аудита закрытых репозиторий, а также частично централизованное управление на данный момент.

Roll-DPoS MPC сайдчейн + некастодиальная ликвидность

EYWA Cross-chain Data Protocol (CDP) – протокол передачи данных между гетерогенными блокчейнами, включающий в себя сеть оракулов EYWA Relayer Network, владельцы которых вносят залоги и несут материальную ответственность за передаваемые данные. Держатели узлов получают награды по принципу DPoS и выполняют MPC-вычисления, формируя единую пороговую BLS подпись, которой подписываются передаваемые данные. Каждый узел сети является нодой блокчейна, цепочка блоков которого хранит текущее состояние сети и информацию о входящих кросс-чейн транзакциях.

Алгоритм Roll-DPoS позволяет решить проблему масштабирования классического DPoS за счет применения принципа лотереи и равных возможностей всех участников, что делает сеть бесконечно масштабируемой. Более подробно об этом алгоритме и о структуре EYWA Relayer Network мы расскажем в технической части документа.

На основе EYWA Cross-chain Data Protocol построен EYWA Cross-chain Bridge, необходимый для передачи токенов между блокчейнами. Он блокирует активы в исходном блокчейне и выпускает привязанные «е»-токены в целевом блокчейне, подобно тому, как это делает REN, но ликвидность при этом хранится в смарт-контрактах. Более подробно об этом написано в разделе номер 8. Важно отметить, что ликвидность в мосте не контролируется держателями узлов EYWA Relayer Network, в отличие от REN.

EYWA Cross-chain Liquidity Protocol (CLP) – децентрализованная кроссчейн-биржа, распределенная в различных блокчейнах. Она позволяет конечным пользователям работать с нативными и синтетическими активами, не используя промежуточные сущности (в отличие от ThorChain), выполняя обмены, добавляя или удаляя активы в пулах ликвидности.

Это дает возможность упростить пользовательский опыт за счет автоматизации работы с выпуском и сжиганием синтетических токенов при кроссчейн-операциях. Поскольку мы используем такие же подходы, как и любой AMM DEX, ликвидность в системе является не кастодиальной.

4. Резюме проекта

Проект EYWA – это комплексная система, которая позволяет различным экосистемам блокчейнов обогащать друг друга с точки зрения ликвидности, сообщества и технической интеграции различных протоколов DeFi. EYWA – это базовое решение для создания кросс-чейн протоколов DeFi следующего поколения.

Экосистема, которую создает проект EYWA, поддерживает инициативы по сближению различных блокчейнов и протоколов, увеличивая синергию и привлекая новых людей и новый капитал в сектор DeFi. Мы надеемся, что многие новые протоко-

лы DeFi будут построены с использованием технологий EYWA, поскольку основная философия проекта EYWA – это интеграция, коммуникация и сотрудничество между многочисленными командами, которые трудятся над разработкой протоколов DeFi и ускоряют массовое принятие блокчейна и криптовалют.

5. Видение

DeFi – это будущее мировых финансовых институтов, и мы находимся в самом начале стремительного роста этого сектора. На это указывает интерес к этой сфере крупных венчурных фондов и институциональных инвесторов, таких как Andreessen Horowitz, Polychain Capital, Alameda Research и других.

Значительные инвестиции в разработку и развитие умных блокчейнов и DeFi-протоколов порождают гонку технологий. Мы считаем, что конкуренция DeFi-экосистем в конечном итоге приведет к созданию простых финансовых продуктов для массового рынка. Продуктов, которые будут доступны в каждом мобильном устройстве и не потребуют от вас понимания, как работают блокчейны, в каких активах платить комиссии, в каких кошельках хранить эти активы, где покупать их и тому подобное.

С этой точки зрения EYWA является базовым решением для создания кроссчейн-DeFi-протоколов нового поколения. Мы искренне считаем, что на рынке уже создано достаточное количество блокчейнов с хорошими технологиями и большими перспективами, поэтому в данный момент нужно налаживать кооперацию между этими гигантами, а не множить сущности*.

Именно поэтому наш подход – блокчейн-агностик, мы не отдаем предпочтения какому-либо одному блокчейну. Мы применяем технологию блокчейн исключительно для валидации и безопасной передачи кроссчейн-данных, чтобы оставаться на уровне надсистемы**.

Используя нашу технологию, игроки рынка смогут работать не только внутри разнородных DeFi-экосистем, как это было раньше, но и между ними, что создает множество новых рынков и перспективных кейсов. Например, таких как одновременный доступ к ликвидности из многих блокчейнов, кроссчейн-фарминг, распределенные мультичейн DAO, кроссчейн-протоколы займов, кроссчейн-биржи, стейблкоины, обеспеченные криптовалютами разных блокчейнов и многое другое.

Экосистема, которую мы строим, поддерживает инициативы по сближению различных блокчейнов и протоколов, увеличивая синергию и привлекая новых людей и новые капиталы в сектор DeFi.

На базе EYWA будет построено множество других DeFi-протоколов, философия EYWA предполагает интеграцию, конкуренцию и сотрудничество между множеством команд, создающих DeFi.

* Здесь имеется в виду «Бритва Оккама», философское понятие, призывающее не множить сущности при логических построениях, если в этом нет необходимости.

** О надсистемах рассказывает ТРИЗ – Теория Решения Изобретательских Задач, автор которой, Генрих Альтшуллер, изучил более сорока тысяч патентов и сформулировал на основании этого анализа свою теорию.

6. Миссия

Наша миссия – объединить DeFi, способствовать выходу этой индустрии на новый уровень зрелости, адаптировать DeFi для массового пользователя.

Мы намерены сделать DeFi инструментом, который позволит улучшить свое материальное положение множеству людей в мире. Мы стремимся сделать децентрализованные финансы легкими, удобными и понятными даже для новичков. Для этого необходимо максимально упростить пользовательский опыт при взаимодействии с DeFi, и поэтому мы создаем экосистему, которая объединит все лучшее, что было создано в DeFi.

Мы идем в это будущее, решая проблему взаимодействия между блокчейнами и, как следствие, фрагментации ликвидности между ними. Первый шаг на этом пути – наши протоколы кроссчейн-передачи данных и ликвидности.

7. Обзор конкурентов

Поскольку проблема фрагментации ликвидности очевидна, над ее решением работает множество различных команд по всему миру, и мы внимательно изучили их решения. Отдельно выделим протоколы, позволяющие совершать произвольные кросс-чейн вызовы:

Name	Cross-chain calls between heterogeneous DeFi blockchains	Consensus	Decentralization	Status	Security
Poly network	+	PoA MPC chain	< 50 nodes	production	hacked
Axelar network	+	DPoS MPC chain	< 100 nodes	in development	N/A
Connext	only EVM-supported blockchains	Basic consensus EVM-chains	interactive atomic swaps	in production	audited
Cosmos HUB+IBC	only tendermint-based homogeneous blockchains	PoS blockchain	< 300 nodes	in development	audited
ChainBridge	+	PoA MPC blockchain agnostic	< 30 nodes	in development	N/A
Chainlink Cross-Chain Interoperability Protocol (CCIP)	+	PoA MPC blockchain agnostic	~400 nodes	in development	N/A
EYWA	+	Roll-DPoS MPC sidechain	infinity scalable	in development	N/A

Большинство команд сосредоточены на создании мостов к своим собственным блокчейнам либо решению задачи интероперабельности в частных случаях; и лишь немногие (включая EYWA) решают задачу в общем виде.

В основной массе команды сосредоточены на создании мостов для ликвидности между блокчейнами, позволяющие обменивать одинаковые активы.

Мы же смотрим на эту задачу шире – создаем комплексное решение, включающее в себя как транспортный, так и прикладной уровень.

EYWA предоставляет гибкую инфраструктуру для разработчиков интероперабельных приложений и децентрализованную кроссчейн-биржу для конечных пользователей.

Blockchain agnostic подход позволяет нам иметь большую гибкость в развитии и управлении токеномикой проекта.

Приведем сравнительную таблицу по 16 кросс-чейн проектам:

Name	Cross-chain bridge	Pay tx fees in any asset	Cross-chain swap any x:y tokens	Instant add Cross-chain pools	Liquidity	Consensus	Speed 2-way bridge	Interoperability between heterogeneous DeFi lockchains	Security audit
Poly network	+	-	+ (O3swap)	-	Non-custodial	PoA MPC chain < 50 nodes	medium	Any	hacked
ThorChain	+	-	+	Need use Rune	Custodial	DPoS chain < 80 nodes	fast	Any	hacked
Connext	+	-	+	-	Non-custodial	Basic consensus EVM-chains	slow	only EVM supported chain	audited
Near Rainbow bridge	+	-	-	-	Custodial	Basic consensus (Ethereum - PoW, Near - PoS)	slow	only Ethereum, Near	audited
REN	+	-	-	-	Custodial	PoA MPC blockchain agnostic > 1500 nodes	fast	Any	audited, no open source
Cosmos HUB+IBC	+	-	+	-	Non-custodial	PoS chain < 300 nodes	fast	tendermint-based homogeneous blockchains	audited
Polygon	+	-	-	-	Custodial	PoS chain ~100 nodes	slow	only EVM supported chain, L2	audited
Anyswap v2+v3	+	-	+	-	V2: Custodial V3: Non-custodial	PoA MPC blockchain agnostic (DCRM) 30 nodes	fast	Any	hacked
Multichain	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic (DCRM) 30 nodes	fast	Any	audited
Chainswap	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic < 30 nodes	fast	Any smarcontract chains	hacked
DFYN	-	-	-	-	Non-custodial	none	none	only EVM supported chain	n/a
Binance Bridge	+	-	-	-	Custodial	centralized service	fast	Any	audited, trusted
ChainBridge	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic	fast	Any	n/a
Axelar network	+	-	-	-	Custodial	DPoS MPC chain < 100 nodes	n/a	Any smarcontract chains	n/a
Chainlink (CCIP)	+	-	-	-	Non-custodial	PoA MPC blockchain agnostic ~400 nodes	n/a	Any	n/a
EYWA	+	+	+	+	Non-custodial	Roll DPoS MPC sidechain infinity scalable	fast	Any smarcontract chains	n/a

Информация о данных приведенных в таблице: [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33]

Нас пугает явная тенденция к централизации кроссчейн-решений: многие проекты выбирают архитектуру, которая заведомо не может иметь высокой степени децентрализации. Мы считаем, что некоторая степень централизации может быть уместна на ранних стадиях, но архитектура должна учитывать масштабирование консенсуса до приемлемой степени децентрализации (более 1000 участников).

Второй по популярности проблемой является кастодиальная ликвидность, когда решение транспортного уровня превращается в распределенное кастодиальное хранилище ликвидности, управляемое малой группой лиц.

Третья проблема – отсутствие стандартизированного подхода к передаче вызовов и ликвидности между блокчейнами и, как следствие, потенциально высокая сложность интеграции имеющихся кроссчейн-протоколов и их узкий, ограниченный функционал, неудобный для конечного пользователя.

Необходимо отметить, что рынок передачи кроссчейн-вызовов еще не сформирован и находится на очень ранней стадии, крупные игроки постепенно начинают входить в него.

Мы ставим перед собой задачу стать одними из лидеров этого рынка, понимая всю его специфику и глубину.

8. Решение: протоколы EYWA

EYWA – это инфраструктурное решение, состоящее из ряда компонентов.

EYWA Cross-chain Liquidity Protocol (CLP).

Как практики, мы создаем протокол прикладного уровня, который дает пользователям новые возможности для работы с DeFi.

Мы решаем проблему «последней мили» – разрабатываем удобную децентрализованную кроссчейн-биржу для пользователей, у которых есть задача перемещать активы между блокчейнами в рамках своей стратегии заработка в DeFi.

Если рассматривать наш подход с точки зрения приведенной в разделе 3 классификации, EYWA можно отнести к следующему типу: Roll-DPoS MPC sidechain + некастодиальная ликвидность.

Что такое EYWA Cross-chain Liquidity Protocol? - Это система децентрализованных АММ-бирж, расположенных в разных блокчейнах, объединенная в одном интерфейсе.

- Мы предполагаем поддержку различных моделей АММ, наиболее подходящих для разных типов активов: стабильные пулы (Curve[34]), классические пулы Uniswap v2[35], v3 и Balancer v2[36]. Мы будем стремиться создавать пулы, наиболее удобные как для целей разработчиков, так и для конечных пользователей и провайдеров ликвидности. Этот подход обеспечит некастодиальную ликвидность в системе, которая будет предоставляться поставщиками ликвидности. Они будут зарабатывать на этом, благодаря yield farming, получая награды в токене EYWA.
- EYWA Cross-chain Bridge - составная часть нашего протокола ликвидности. Для

переноса ценности (токенов) между блокчейнами мы используем обеспеченные синтетические активы - “е”-токены, создаваемые и конвертируемые по принципу mint-burn. Мы называем эти операции *synthesis* и *unsynthesis*. Для передачи произвольной информации между блокчейнами используется EYWA Cross-chain Data Protocol. Блокируя оригинальный актив в одном блокчейне, мы создаем его синтетический аналог в другом блокчейне. При обратной операции синтетический актив сжигается, а оригинальный - возвращается. Наличие таких активов позволяет осуществлять быстрое создание кросс-чейн-пулов и мостов ликвидности, физически находящихся в одном блокчейне и обеспечивающих быстрое двустороннее перемещение активов. Таким образом, ликвидность будет свободно распространяться между блокчейнами, концентрируясь там, где это наиболее выгодно и перспективно. Мы будем активно следить за развитием индустрии и своевременно предлагать новые возможности пользователям. Данная система является открытой и поэтому любой DeFi проект сможет создать свой кросс-чейн пул ликвидности, используя нашу систему.

- Синтетические активы как кросс-чейн мост. Для разработчиков DeFi мы предлагаем удобный и быстрый способ перемещать свои токены в интересующие их блокчейны. Существует два подхода при построении кросс-чейн моста:

- блокировать свои токены в исходном блокчейне и получать их синтетическую репрезентацию в целевом блокчейне, в этом случае у вас будет один источник эмиссии и единая токеномика проекта.

- создать в каждом блокчейне свой токен и обменивать эти токены через мост, в этом случае мост выступает хранилищем, особенность этого подхода в том, что в каждом из блокчейнов у вас будет отдельная токеномика, но при этом вы будете владельцем контракта токена.

Мы придерживаемся первого подхода, поскольку он наиболее гибкий и простой, с точки зрения обслуживания моста.

- Некастодиальная ликвидность в кросс-чейн мостах. Ликвидность, хранимая в смартконтрактах в качестве обеспечения синтетических активов может быть извлечена либо владельцами, либо общим решением большинства голосов DAO EYWA.

EYWA Cross-chain Data Protocol (CDP)

Открытый децентрализованный протокол кросс-чейн передачи данных, способный работать между гетерогенными блокчейнами, и мы намерены дать этот инструмент всем разработчикам DeFi. Это транспортный уровень решения, он состоит из набора смарт-контрактов в разных блокчейнах и собственной децентрализованной сети оракулов.

Это позволит командам сосредоточиться на разработке бизнес-логики своих DAPPS, не отвлекаясь на решение задач интероперабельности. Наш протокол позволит связать любые два смарт-контракта, находящиеся в разных блокчейнах, реализуя удаленные вызовы между ними.

Многие проекты создают свои мосты для ликвидности между блокчейнами, для нас же мосты - это всего лишь частный случай использования транспортного уровня - протокола кросс-чейн передачи данных.

EYWA Cross-chain Data Protocol состоит из децентрализованной сети оракулов EYWA Relayer Network и набора смартконтрактов в разных блокчейнах.

EYWA Relayer Network

Идеология этой сети вдохновлена проектами Chainlink, Ren и Horizen[37].

Сеть оракулов является сайдчейном, который может иметь связь с любыми блокчейнами, поддерживающими смарт-контракты. Эта сеть публикует данные о своем состоянии и управляется с помощью смартконтрактов, расположенных в любом подходящем (быстром, децентрализованном, дешевом) публичном блокчейне. Сеть оракулов имеет распределенный консенсус. Голосуя, они подтверждают факт проведения транзакции в исходном блокчейне.

Когда достигается кворум, сеть записывает проверенные данные о транзакциях и криптографические доказательства в управляющий блокчейн и затем дальнейшая передача этих транзакций в целевые блокчейны осуществляется при помощи любых заинтересованных сторон. Абсолютно любой человек может передавать эти кроссчейн-транзакции и быть владельцем узла этой EYWA Relayer Network.

Участники зарабатывают благодаря системе стимулов, заложенной в токеномику проекта. Также необходимо заметить, что держателям узлов для участия в консенсусе необходимо быть держателями залога – определенной суммы governance токенов этого проекта, которые размещаются в специальный смарт-контракт. Он начисляет вознаграждения держателям узлов.

С точки зрения безопасности консенсуса оракулов мы используем современный и экологичный подход к децентрализации, применяемый в таких проектах, как Tezos, Polkadot, FreeTon, IoTeX, Algorand и Ethereum 2.0 – proof of stake с механизмом слешинга.

Иными словами, держатели узлов EYWA несут материальную ответственность за передаваемые ими данные. В случае, если EYWA Relayer Network фиксирует искажение передаваемых данных, все участники, которые принимали в этом участие, штрафуются.

EYWA Multichain Gasless

Подсистема, которая отвечает за оплату транзакций протокола во множестве блокчейнов. Мы делегируем ей исполнение транзакций пользователей и исполнение транзакций между блокчейнами от имени оракулов EYWA Relayer Network.

Это позволяет снять с пользователей необходимость оплачивать комиссии во многих активах и позволяет им выбирать, в каком активе платить комиссию. Так-

же gasless дает возможность компенсировать транзакционные расходы некоторым группам пользователей.

Основная суть этой подсистемы состоит в том, что у вызывающего существует возможность отправить транзакцию в блокчейн за счет получателя. В этом случае вместо отправки транзакции в блокчейн формируется и подписывается offchain-метатранзакция, которая затем передается ретранслирующим узлам; ее содержимое и структура верифицируется смарт-контрактами и затем выполняется.

В своем коде мы используем разработки таких проектов как OpenGSN[38] и Gnosis Safe[39], опираясь на стандарт EIP-712[40].

EYWA Cross-chain DAO [41][42]

Для управления смарт-контрактами системы, распределенной во множестве блокчейнов, мы сделаем систему принятия решений распределенной и управляемой держателями governance токена проекта. Для связывания различных частей системы мы будем использовать EYWA Cross-chain Data Protocol.

9. Функции и преимущества

Для поставщиков ликвидности:

Кроссчейн-доходное фермерство или кроссчейн-фарминг: поставщик ликвидности может предоставлять ликвидность в кроссчейн-пулы и получать награду за это. По сути, для этого ему потребуется создать обеспеченные синтетические активы родом из различных блокчейнов и добавить их в пул ликвидности.

Кросс-чейн пулы без непостоянных потерь с ограниченной ликвидностью и повышенной доходностью: для эффективной работы кроссчейн-пулов не требуется неограниченная ликвидность, поэтому предложение для поставщиков ликвидности будет ограниченным и имеющим привлекательную доходность.

Отсутствие непостоянных потерь достигается за счет структуры пулов: они будут состоять из различных репрезентаций и аналогов одинаковых активов, например curve пул в блокчейне Matic вида:

eUSDC(ETH)+eUSDC(BSC)+eUSDC(HECO)+USDC(Matic)

ещё один пример, curve пул в Binance Smart Chain:

eETH(ETH)+eETH(Matic)+eETH(Solana)+ETH(bep20)

Либо аналогичный пул Uniswap v2 в Binance Smart Chain:

eWBTC(ETH)+BTCB(bep20)

«е»-токены – это синтетические активы EYWA, выпускаемые мостом EYWA, обеспеченные заблокированным залогом в смарт-контракте исходного блокчейна.

Название bep20 токена в Binance Smart Chain вида eUSDC(ETH) обозначает, что это синтетический актив, обеспеченный erc20 токеном USDC в блокчейне Ethereum. Это обеспечение хранится в специальном контракте (мы называем его Portal) и может быть извлечено путем вызова моста EYWA – при этом токен bep20 eUSDC(ETH) будет сожжен, а пользователь, который вызвал эту операцию, получит на свой кошелек в блокчейне Ethereum erc20 токен USDC.

Для конечных пользователей EYWA DEX (трейдеров):

Кросс-чейн обмены - пользователи могут беспрепятственно обменивать один нативный токен на другой нативный токен в другой цепи, например, ETH на BNB или USDT(BSC) на USDC(ETH) используя при обмене два или даже три блокчейна.

Это может достигаться как за счет использования собственных пулов ликвидности протокола EYWA, так и за счет агрегации пулов ликвидности существующих крупных децентрализованных бирж в различных блокчейнах.

Возможность совершать дешевые транзакции, обменивая активы “дорогих” блокчейнов, например обменивать ERC20 токены Ethereum, используя дешевый промежуточный блокчейн - loopback swap.

Например обмен вида:

```
Ethereum: USDT(ERC20) => synthesis (mint) in Polygon: eUSDT(ETH) =>
=>swap in Polygon: eUSDT(ETH)/eETH(ETH) => get eETH(ETH) =>
=>unsynthesis (burn) in Polygon: eETH(ETH) => Ethereum: ETH
```

Возможность совершать кросс-чейн транзакции между двумя блокчейнами, используя дешевый и быстрый промежуточный блокчейн. Например рассмотрим следующий обмен:

Пользователь обменивает USDC между блокчейнами Ethereum и Binance Smart Chain, используя кросс-чейн curve-пул в Polygon:

```
Ethereum: USDC(ERC20) => synthesis (mint) in Polygon: eUSDC(ETH) =>
=>swap in Polygon: eUSDC(ETH)/eUSDC(BSC)/eUSDC(HECO)/USDC(Polygon)=>
=>get eUSDC(BSC) => unsynthesis (burn) in Polygon: eUSDC(BSC) => BSC: USDC(BEP20)
```

Важно отметить, что в двух предыдущих кейсах пользователь имеет возможность совершить эту цепочку операций автоматически, при этом заплатив комиссию в имеющемся у него активе в исходном блокчейне, опытный же пользователь может вручную контролировать этот процесс и оплачивать комиссии в базовых активах сетей

Скорость кросс-чейн обменов: быстрый двухсторонний обмен между различными блокчейнами. В отличие от многих мостов (Polygon PoS bridge, Near Rainbow Bridge, Plasma, Connex), наша технология даёт возможность совершать операции с практически одинаковой скоростью, вне зависимости от направления обмена.

Компенсация транзакционных издержек некоторым группам пользователей из прибыли протокола. Например такой группой пользователей могут быть трейдеры, совершающие сделки на небольшие суммы и имеющие скромный торговый оборот.

Возможность получать комиссионные, приглашая поставщиков ликвидности и трейдеров.

Улучшенный UX для конечных пользователей благодаря безгазовым транзакциям: пользователь сможет оплачивать комиссии в тех активах, которые он меняет, или выбрать удобный актив для оплаты комиссий. Прогрессивная шкала комиссий для трейдеров, в зависимости от их торговых объемов. Чем больше объем - тем ниже комиссия.

Возможность выгодного обмена: Это обеспечит интеллектуальная маршрутизация между пулами ликвидности в разных цепочках, осуществляющая поиск оптимального пути для кросс-чейн обмена.

Для разработчиков DeFi проектов:

Возможность быстрой кросс-чейн интеграции своего протокола, используя технологию EYWA Cross-chain Data Protocol (CDP).

Разработчики смогут обеспечить взаимосвязь между своими смарт-контрактами, развернутыми в разных блокчейнах.

В том числе они смогут создавать собственные мосты для ликвидности, кросс-чейн кредитование, кросс-чейн фарминг и другие приложения.

Быстрая кросс-чейн ликвидность - разработчики смогут перемещать токены своих проектов между блокчейнами, используя EYWA Bridge и создавать собственные кросс-чейн пулы ликвидности используя Cross-chain Liquidity Protocol.

Возможность присоединиться к сообществу разработчиков EYWA, принимать участие в хакатонах, получать гранты от EYWA DAO и вместе с нами строить будущее DeFi.

Для стейкеров и держателей узлов децентрализованных сетей:

Возможность поддерживать работу EYWA Relay Network, быть владельцем её узлов либо стейкером и зарабатывать на этом.

Для держателей токена EYWA - быть частью DAO EYWA:

Возможность принимать участие в управлении протоколом путем подачи предложений и участия в голосованиях.

Определять ключевые решения по развитию экосистемы EYWA.

Получать прибыль от стейкинга и поощрения за принятие участие в голосованиях.

10. Принцип работы

В этом разделе более подробно рассмотрим техническую часть и внутреннее устройство компонентов EYWA.

EYWA Cross-chain Data Protocol and Relay Network

В этом разделе более подробно рассмотрим техническую часть и внутреннее устройство компонентов EYWA.

EYWA Cross-chain Data Protocol and Relay Network

Протокол состоит из децентрализованной сети оракулов EYWA Relay Network и набора смартконтрактов, расположенных в публичных блокчейнах. Он является транспортным уровнем и обеспечивает интероперабельность с выполнением требований:

- Децентрализованная работа протокола с большим количеством участников, защищенного от компрометации сговором узкого круга лиц.
- Низкая стоимость входа в консенсус при высокой стоимости компрометации.
- Возможность объединять сети с различными технологическими решениями и правилами валидации/формирования блоков.
- Передающая сеть не должна хранить передаваемые активы — не кастодиальное решение.

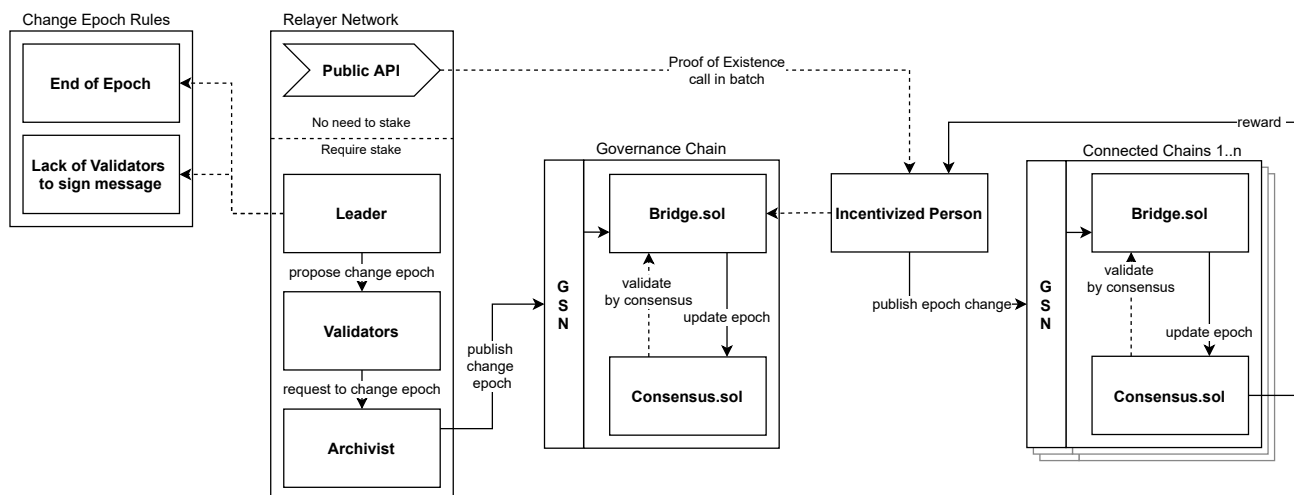
Повышение стоимости компрометации достигается путем увеличения количества участников консенсуса — тысячи узлов против десятков в PoA, DPoS решениях и разделением обязанностей между участниками путем ввода ролей:

- **Лидеры** – участники консенсуса, которые собирают из новых запросов на передачу данных между гетерогенными блокчейнам пакеты и передают валидаторам на проверку.
- **Валидаторы** – производят проверку пакетов, поступающих от Лидеров. Работая в рамках BFT-консенсуса – Tendermint[43] приходят к единому мнению о валидности пакета и подтверждают его генерацией коллективной (MPC) подписи основанной на криптографической системе BLS[44].
- **Архивариусы** – публикуют обработанные пакеты в публичную, независимую сеть для фиксации результата работы протокола и обеспечения доступности информации.
- **Резервные валидаторы** – необходимы для защиты консенсуса от потенциальной атаки для предотвращения функционирования протокола.

Честность выбранных на роль участников достигается экономической выгодой, построенной на дилемме заключённого[45] из теории игр – каждому участнику выгодно предать злоумышленника (даже при наличии предварительного сговора) и получить за это награду, чем присоединиться к нему и понести наказание.

Роли распределяются случайным образом между участниками сети и закрепляются за ними до конца эпохи.

Эпохи и сменяемость участников



Эпоха – это промежуток работы протокола, ограниченный по времени или максимальному количеству пакетов.

Использование алгоритма Roll-DPoS гарантирует постоянную сменяемость участников, выполняющих роли консенсуса. Roll-DPoS - это алгоритм масштабирования, устраняющий перечисленные выше проблемы. Основанный на честной лотерее (построенной на проверяемой случайной функции – VRF) выбор случайных участников сети для выполнения работы устраняет риск сговора для влияния на сеть узким кругом злоумышленников, так как прогнозировать результаты лотереи математически невозможно.

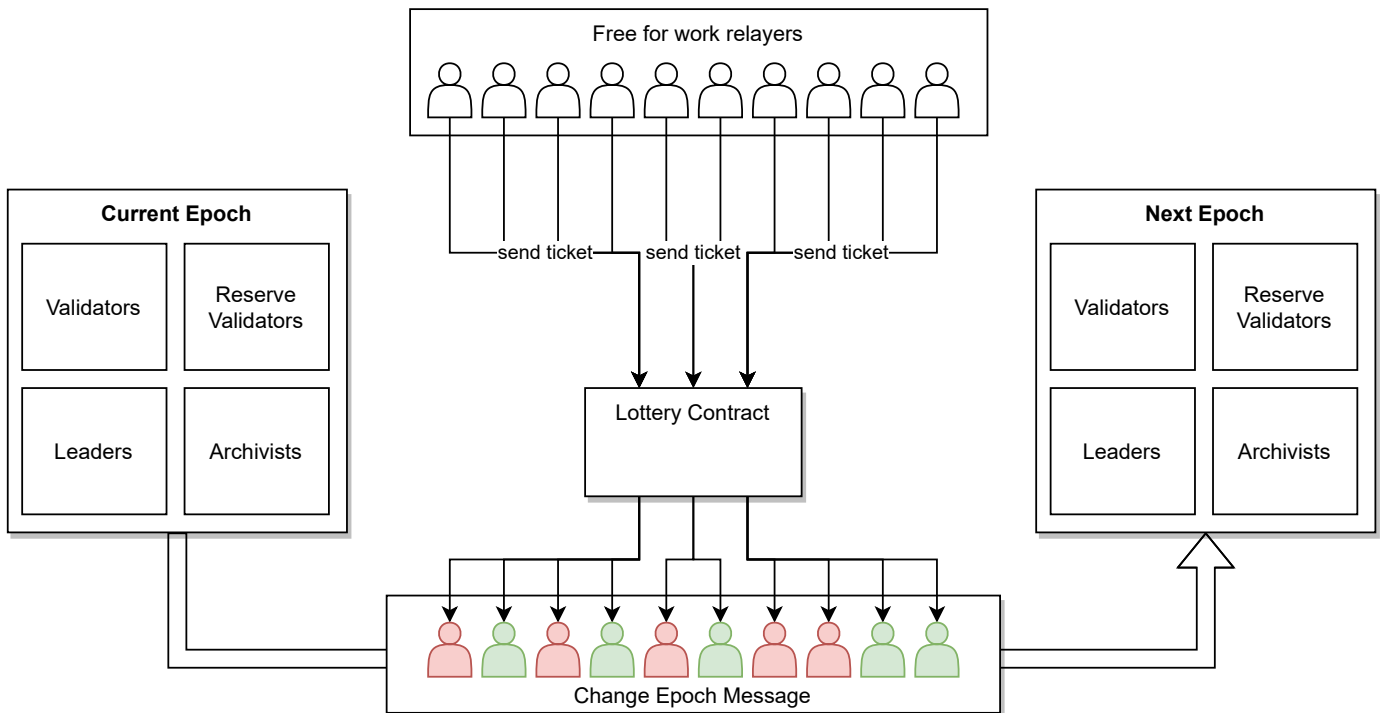
Данный алгоритм используется в блокчейне IoTeX[46], специализирующемся на объединении интернета вещей (IoT) в единый блокчейн, где они используют Roll-DPoS для бесконечного масштабирования сети.

Алгоритм смены эпохи аналогичен алгоритму обработки кросс-чейн запроса на передачу данных, но в качестве источника запроса выступает сам протокол, а получателем являются все сети, подключенные к протоколу.

EYWA Cross-chain Data Protocol ведет учет и выбор участников эпохи в смарт-контракте, выполняемом в независимом публичном блокчейне, гарантирующем, что у участников протокола нет возможности повлиять на ход выполнения.

При нормальной работе протокола формированием запроса на смену эпохи, валидацией и исполнением занимаются лидер, валидаторы и архивариус, но для устранения возможности заблокировать смену эпохи валидаторами, необходима роль резервных валидаторов, работа которых заключается в принудительной смене эпохи.

Лотерея ролей



Для организации честной лотереи используется верифицируемая случайная функция (сокращенно VRF) и стартовая точка (сид).

VRF[47] – криптографический примитив, который может отображать входные данные в проверяемый псевдослучайный выход. В 1999 году Микали (основатель Algorand), Рабин и Вадхан создали VRF. В настоящее время алгоритм VRF используется в различных схемах шифрования, протоколах и системах.

Сид (Seed) – это число, точка, с которой начинается последовательность псевдослучайных чисел. Незначительное изменение стартовой точке ведет к непрогнозируемой смене результата генерации псевдослучайных чисел.

Лотерея ролей для эпохи E_N проходит в 3 этапа:

Фиксация размера обеспечения потенциальных участников лотереи. При смене эпохи E_{N-3} фиксируется состояние сети в корне дерева меркла, включающее в себя все суммы обеспечения участников на данный момент.

$Balance_i = (key, value)$ – кортеж из публичного ключа кошелька и его баланса токенов EYWA.

$$CirculationSupply = \bigcup_{i=0}^I Balance_i$$

$CirculationSupply$ – множество всех не заблокированных балансов $Balance_i$, I пользователей протокола,

$stake(Balance_i.key, Balance_i.value, S) = Stake_j$ – функция заморозки части S баланса пользователя $Balance_i.value$ и получения им стейка $Stake_j$.

$$Stake_j = (Balance_i.key, S), S \leq Balance_i.value$$

$TotalStake = \bigcup_j Stake_j$, $Stake_j \in TotalStake$ – множество всех стейков $Stake_j$ из J участников консенсуса.

$TotalStake \cap CirculationSupply = \emptyset$ – все заблокированные в стейкинге токены не участвуют в общей циркуляции.

$Collateral = 100\,000\ EYWA$ – размер минимального стейка, гарантирующий честную работу пользователя, может быть изменен общим решением DAO EYWA.

$RelayersStake = \bigcup_{k=0}^K Stake_k$, $\forall Stake_k \in RelayersStake$

$Stake_k.value \geq Collateral$, $RelayersStake \subseteq TotalStake$

$RelayersStake$ – подмножество $TotalStake$, состоящее из K стейков участников $Stake_k$, value которых больше или равно размеру минимального обеспечения $Collateral$, имеющих шанс победы и право участия в лотерее.

В ходе эпохи E_{N-2} любой участник ($Participant_i$), желающий принять участие в эпохе, публикует лотерейный билет $draw(Stake_k)$ в сеть управления. С публикацией лотерейного билета, участник фиксирует размер своего обеспечения и блокирует изменение его до завершения эпохи.

$draw(Stake_k) = Participant_i$

$LotteryStake = \bigcup_{i=0}^L Participant_i$

$\forall Participant_i \in LotteryStake$, $Participant_i \notin RelayersStake$,

$RelayersStake \cap LotteryStake = \emptyset$

В момент смены эпохи E_{N-1} публикуется результат VRF сгенерированный участниками эпохи и используется как стартовая точка (*Seed*) для лотерейных билетов. Разнесение во времени раскрытие стартовой точки, фиксации размеров обеспечения и публикации лотерейных билетов, необходимо для усиления консенсуса путем устранения возможности манипуляции для получения преимущества в лотерее.

$Seed \in N$ — псевдослучайное число, результат проверяемой функции генерации случайных чисел.

В момент смены эпохи E_{N-1} прием билетов на участие в эпохе E_N завершается и список участников определен. Участники формируют коллективные ключи и передают их участникам текущей эпохи для начала работы. Список участников лотереи, получивших право на участие в эпохе определяется весовой функцией с приоритетом участникам получившим наивысший результат в ходе лотереи. Вес лотерейного билета определяется как: отношение хеша от пары ключа владельца билета и сида лотереи по модулю обеспечения владельца билета к сумме всех обеспечений участников.

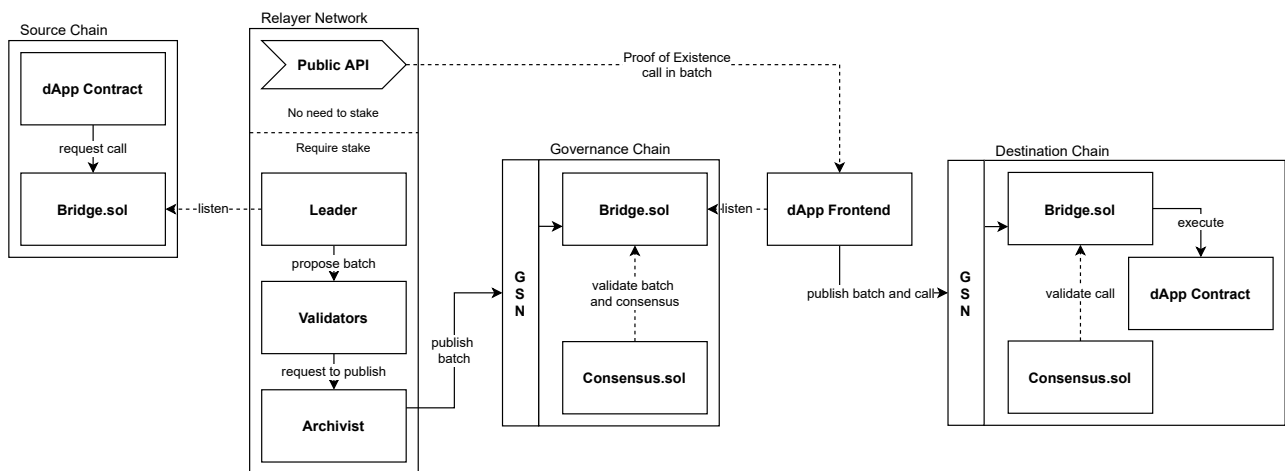
$$weight(Participant_p) = \frac{HASH(Participant_p.Key, Seed)(mod Participant_p.Value)}{\sum_{i=0}^L Participant_i.Value}$$

$$0 < weight(Participant_p) \cdot Participant_p.Value \leq \sum_{i=0}^L Participant_i.Value$$

Следовательно, чем выше залог участника, тем выше его шансы выиграть в лотерею и попасть в эпоху. Билеты сортируются по их результату и роли распределяются от наивысшего к наименьшему в порядке значимости роли: валидаторы, резервные валидаторы, лидеры, архивариусы. Количество участников каждой роли определяется настройками протокола.

Дизайн EYWA Cross-chain Data Protocol

Основная задача протокола - передать запрос произвольного приложения X из сети A в сеть B. Приложение X реализует в сети A смарт-контракт для формирования и отправки запроса в Bridge смарт-контракт протокола в сети A.



Лидер эпохи выполняет свои обязательства добавлением нового запроса в пакет (batch) для последующей проверки Валидаторами и публикации Архивариусом.

После финализации блока сетью управления с пакетом, содержащим запрос, работа сети оракулов EYWA Relay Network завершена. Сеть управления - это любой EVM-совместимый блокчейн, отвечающий требованиям децентрализации, скорости и низкой стоимости транзакций, в настоящее время существует немало таких блокчейнов, мы изучаем и тестируем их, выбирая наиболее подходящий, возможные кандидаты: Harmony One, IoTeX, Avalanche, Celo, Polygon.

Выполнение запроса в сети B может совершить любая заинтересованная сторона: клиент-приложение X, специализированный сервис или пользователь.

Для минимизации технологической сложности, связанной с хранением и управлением различной криптовалютой, необходимой для покрытия транзакционных издержек в блокчейнах назначения, протокол EYWA предоставляет сервис EYWA Multichain Gasless.

Алгоритм выполнения запроса

Пошаговый алгоритм выполнения кросс-чейн вызова выглядит так:

1. Контракт стороннего разработчика вызывает метод `transmitRequestV2` в контракте `Bridge.sol` в сети источнике вызова и передает идентификатор сети назначения, адрес/идентификатор контракта получателя, средства для оплаты работы (не менее суммы, выставленной как минимальная оплата в настройках протокола), и данные для вызова.
2. Контракт `Bridge` создает событие `OracleRequest` с полученной информацией от контракта стороннего разработчика.
3. Лидеры эпохи отслеживают события из сетей источников и сохраняют локально информацию о вызове, ожидающем валидации.
4. Выбранный лидер пакета (определяется `round-robin` алгоритмом из списка всех лидеров эпохи), определяет момент необходимости формирования пакета и формирует пакет подписанный личным ключом. И предлагает валидаторам эпохи для проверки
5. Валидаторы принимают пакет если:
 - a. Включены все ожидающие проверки запросы и действия требуемые протоколом (или достигнут лимит пакета, определенный общими настройками протокола),
 - b. Все включенные действия валидны: существует соответствующий запрос в источнике или действие ожидаемо в соответствии с правилами протокола, например, начисление вознаграждения, изъятие средств для компенсации работы и т.д.
 - c. Пакет предложен лидером в отведенный для него временной промежуток,
 - d. Назначен ожидаемый архивариус,
 - e. Выставлен ожидаемый порядковый номер пакета,
6. Валидаторы генерируют общую подпись и передают пакет архивариусу для публикации.
7. Архивариус проверяет пакет:
 - a. Пакет указывает на текущую эпоху,
 - b. Порядковый номер пакета соответствует ожидаемому (следующий от известного),
 - c. Все включенные действия валидны: существует соответствующий запрос в источнике или действие ожидаемо в соответствии с правилами протокола, например, начисление вознаграждения, изъятие средств для компенсации работы и т.д.
 - d. Выбранные лидер и архивариус пакета соответствуют ожидаемым (`round-robin` от порядкового номера пакета и списка лидеров и архивариусов текущей эпохи),
 - e. Подпись лидера сгенерирована от ключа выбранного лидера,
 - f. Верифицирует подпись и проверяет, что для ее генерации требовалось более, чем $\frac{2}{3}$ всех валидаторов.
8. Если пакет не соответствует правилам, архивариус игнорирует пакет и ждет следующий. Если пакет прошел проверку, архивариус подписывает своим личным ключом и вместе с подписью публикует в сеть управления протоколом.

9. Контракт в сети управления проверяет полученный пакет на соответствие правилам (аналогично архивариусу, но в рамках смарт-контракта).
10. Контракт в сети управления проверяет подпись архивариуса.
11. Контракт в сети управления добавляет в реестр пакет и создает событие Batch, содержащее данные пакета и подпись архивариуса.
12. Заинтересованные в исполнении действий пользователи (отправители первоначальных запросов или другие лица), ожидают возникновения события в сети управления и отправляют в финальные вызовы в сети назначения транзакцией, содержащей: массив недостающих пакетов, включающий текущий пакет и вызов (для выполнения).
13. Контракт принимающей стороны валидирует пакет по аналогии с контрактами в сети управления. Недостающие пакеты в проверке не нуждаются, так как наличие более актуального пакета подтверждает валидность предыдущих.
14. Контракт исполняет вызов и возвращает успех или ошибку.
15. В случае ошибки, контракт принимающей сети автоматически создает событие RequestRevertAction, работающее по аналогии с RequestAction, но в обратном направлении для оповещения сети источника об ошибке.

Типы вызовов и команд в пакете

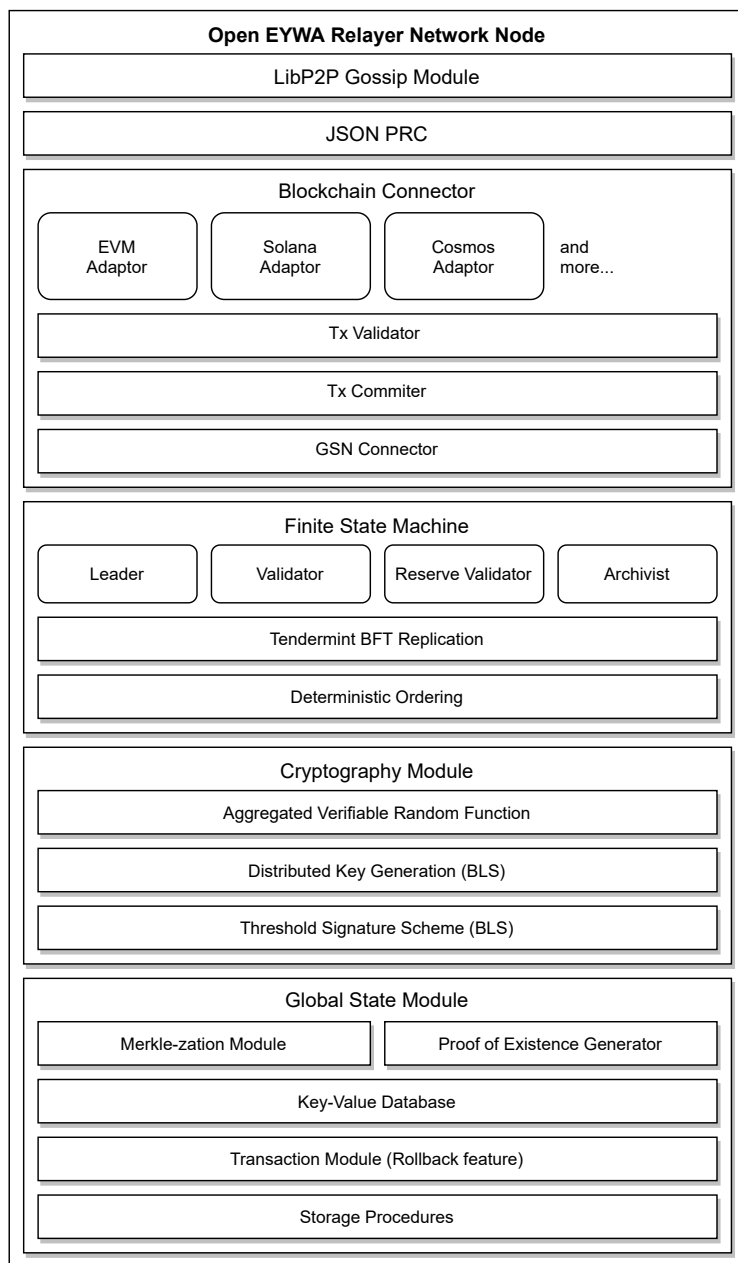
Для реализации всего спектра взаимодействий, протокол вводит всего пять типов запросов:

1. От сети А в сеть В.
2. От сети А в сеть оракулов.
3. От сети оракулов в сеть А.
4. От сети оракулов во все сети.
5. От сети оракулов в сеть оракулов (внутренняя команда)

Алгоритм смены эпохи аналогичен обработке кросс-чейн вызова, но требует проверки соответствия участников состоянию в сети управления протоколом, а не наличия исходного запроса на действие. При нормальной работе протокола формированием запроса на смену эпохи, валидацией и применением занимаются лидер, валидаторы и архивариус, но для устранения возможности заблокировать смену эпохи валидаторами, необходим пул резервных валидаторов, работа которых заключается в принудительной смене эпохи.

Архитектура узла EYWA Relayer Network

Сеть протокола представляет из себя пиринговую сеть оракулов – EYWA Relayer Network. Программное обеспечение оракулов имеет модульную архитектуру, модули которой опционально могут быть отключены в зависимости от назначения узла.



LibP2P Gossip – организации p2p сети и обмен сообщениями через интернет.

JSON RPC – внешнее API.

Blockchain Connector – взаимодействие с блокчейн сетями.

FSM – организация сценариев и правил работы.

Cryptography – реализация криптографических методов

Global State – хранение и менеджмент состояния сети: балансов, обеспечения, вознаграждение и т.д.

LibP2P Gossip

Эффективно обмениваться сообщениями критически важно для построения большой пиринговой сети. Пиринговая сеть EYWA Relay Network основана на открытой библиотеке libP2P, используемой в проектах IPFS, Substrate. Из коробки библиотека позволяет строить распределённые хэш-таблицы для поиска ближайших соседей и организовывать протокол сплетен с криптографическими доказательствами консистентности сообщений.

JSON RPC

Привычный для централизованной инфраструктуры способ удаленного взаимодействия с узлом. Позволяет удобно реализовать возможность вызова удаленных процедур и получения данных.

Внешний программный интерфейс необходим для:

1. Управления собственным узлом
2. Получения данных:
 - Доказательств включения,
 - Состояния сети: балансы, обеспечения, эпоха и т.д.
 - Информации об обработанных и ожидающих запросах.
3. Отправки запросов без сети источника (от сети оракулов к сети получателю)

Blockchain Connector

Модуль, унифицирующий взаимодействия с гомогенными сетями. Необходимость поддержки большой выборки сетей, требует абстрагировать бизнес-логику от специфики взаимодействия с конкретной сетью. Для каждой сети (или типа сетей, например, Ethereum-like) создается уникальный адаптер, позволяющий:

- Проверить запрос
- Проверить транзакцию
- Отправить транзакцию
- (Опционально) Отправить транзакцию без средств для оплаты работы сети (GSN)

Deterministic Finite State Machine

Конечный автомат (FSM) — способ описания правил и сценариев выполнения бизнес-логики. Для работы децентрализованного протокола от конечного автомата требуется удовлетворение требований:

- Детерминированное выполнение сценариев вне зависимости от окружения
- Детерминированная сортировка команд

- Репликация устойчивая к византийскому поведению
- Для выполнения всех требований EYWA Relay Network реализует practical BFT консенсус.

Cryptography Module

Консенсус протокола зависит от реализации трех криптографических процедур:

- Distributed Key Generation
- Threshold Signature Scheme
- Verifiable Random Function
- Global State Module

Глобальное состояние сети хранится в базе ключ-значение, без требований к структуре значений и типу ключей. Для оперирования с состоянием в конечных блокчейн сетях без необходимости репликации всего состояния, используются доказательства на деревьях Меркла. Деревья Меркла базовый подход для доказательства честности и включения части данных в общие данные без необходимости предоставления общих данных. Доказательства Меркла широко используются во всех децентрализованных сетях, от упрощенного доказательства платежа в Bitcoin до доказательств состояния виртуальной машины Ethereum.

Потенциальные векторы атаки

Препятствование функционированию протокола через невыполнение обязательств лидера по формированию пакетов

Так как интернет не дает гарантий доставки сообщений и избранный лидер может испытывать проблемы с подключением без заведомо злого умысла, мерой наказания является отсутствие награды за предложенный пакет. Поэтому единственный способ компенсировать затраты на лотерею участнику получившему роль лидера — это исправно формировать правильные пакеты.

Препятствование функционированию протокола через невыполнение обязательств архивариуса по публикации и подписи пакетов для сети управления

От надлежащей работы архивариусов зависит пользовательский опыт и поэтому в протоколе предусмотрено наказание за их некорректную работу. Если пакет был сформирован и подготовлен к публикации, но за отведенный для этого срок данного действия не последовало, то все запросы и вознаграждения переносятся в следующий пакет, а также добавляется специальное действие, штрафующее архивариуса на сумму, установленную настройками протокола.

Формирование пакетов с действиями, не проходящими проверку

Если валидаторы получили пакет от лидера, содержащий действия, идущие враз-

рез с общими правилами (несанкционированное получение вознаграждения, запросы без источника или любые другие изменения, не проходящие проверку), лидер признается злоумышленником и в следующем пакете штрафуются на сумму, установленную протоколом. Данный штраф должен быть отражен в следующем пакете, иначе последующий лидер будет признан сообщником и тоже понесет наказание.

Препятствование функционированию протокола через невыполнение обязательств валидаторов

От надлежащей работы валидаторов зависит пользовательский опыт и протокол вводит ряд наказаний если пакет был предложен, но за отведенный для срок для валидации и подписи данных действий не последовало.

Валидация и подпись зависит от стабильной работы $\frac{2}{3}$ всех валидаторов для формирования коллективной подписи. Принимая во внимание проблемы интернета описанные выше, есть вероятность, что у большинства валидаторов может физически не быть возможности сформировать подпись, не имея злого умысла.

Поэтому если валидаторы испытывали временные трудности и смогли до завершения эпохи вернуться к работе, они теряют лишь вознаграждение за пропущенные пакеты.

Если валидаторы до конца эпохи не смогли вернуться к работе, происходит смена эпохи по инициативе резервных валидаторов и текущий круг валидаторов понесет наказание в размере суммы, установленной настройками протокола.

EYWA Cross-chain Bridge

Для перемещения ценности между блокчейнами мы используем синтетические активы – EYWA tokens, или e-tokens. Е-токены создаются всякий раз, когда кому-то требуется переместить актив между двумя блокчейнами.

Рассмотрим пример:

Боб перемещает токен x_A из блокчейна А в блокчейн В.

Мы используем следующий подход:

Боб посылает транзакцию в EYWA Cross-chain Bridge, оригинальный токен x_A блокируется в смартконтракте Portal в блокчейне А, его транзакция вызывает событие в смартконтракте Bridge. Это событие отслеживается и обрабатывается сетью оракулов EYWA Relayer Network.

Они верифицируют входящие транзакции и совершают кросс-чейн вызовы смартконтрактов в блокчейнах назначения. В нашем примере транзакция Боба вызовет смартконтракт Synthesis в блокчейне В, который выпустит в блокчейне В синтетический токен ex_A , обеспеченный заблокированным в блокчейне А токеном x_A .

При этом Боб в любой момент может выполнить обратное преобразование и забрать оригинальный актив x_A .

Таким образом, EYWA Cross-chain Bridge выполняет кросс-чейн преобразования вида:

$s(x_A, A, B) = ex_A$ - synthesis (mint) function for transfer from chain A to chain B

$u(ex_A, B, A) = x_A$ - unsynthesis (burn) function for transfer from chain B to chain A

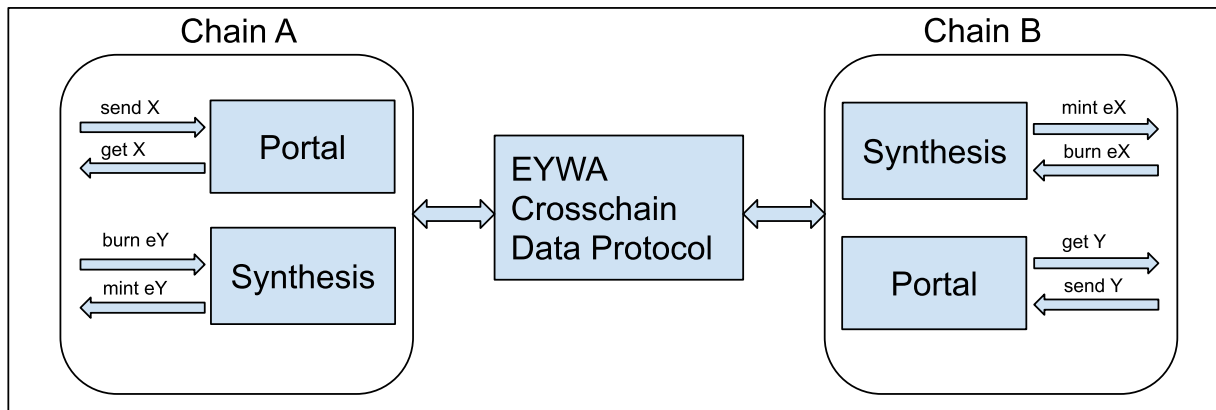
$s(y_B, B, A) = ey_B$

$u(ey_B, A, B) = y_B$

$\forall x_A, ey_B \in A \forall y_B, ex_A, \forall A, B \in S$

Где A, B - блокчейны из S - множества блокчейнов, имеющих смартконтракты

EYWA Cross-chain Bridge состоит из смартконтрактов Portal и Synthesis, расположенных в каждом из блокчейнов A, B и использует EYWA Cross-chain Data Protocol (CDP) для передачи кросс-чейн вызовов между ними.



EYWA Cross-chain Liquidity Protocol

Протокол ликвидности EYWA включает себя смартконтракты кросс-чейн мостов EYWA Cross-chain Bridge, развернутые во множестве блокчейнов и контракты AMM бирж, развернутые в каждом из подключенных блокчейнов. Это необходимо для того, чтобы обеспечить ликвидность для синтетических активов EYWA. Поскольку пользователь ожидает получить ликвидный актив при перемещении между блокчейнами, мы обеспечиваем это, создавая пулы ликвидности с синтетическими активами.

Например: пользователь перемещает 100 USDT (erc20) из Ethereum в Binance Smart Chain и ожидает получить 100 USDT (ber20), для того, чтобы обеспечить такой обмен, мы выполним следующую цепочку действий:

1. 100 USDT (erc20) блокируется в смартконтракте Portal в Ethereum, создается событие в контракте Bridge, которое начинают обрабатывать узлы EYWA Relayer Network.
2. EYWA Relayer Network вызывает смартконтракт Bridge в Binance Smart Chain, посылая туда информацию для вызова смартконтракта Synthesis.
3. Synthesis выполняет вызов и синтезирует 100 токенов eUSDT(ETH) и отправляет их пользователю.

4. Выполняется обмен 100 eUSDT(ETH) на 100 USDT в пуле ликвидности eUSDT(ETH)/USDT (Uniswap v2 like pool), где USDT - это нативный bep20 токен в Binance Smart Chain.

Точно такой же механизм позволит обменивать между собой произвольные активы из различных блокчейнов. Мы предполагаем внедрять поддержку различных моделей АММ, наиболее подходящих для разных типов активов: стабильные пулы (Curve) для активов с одинаковой ценой, классические пулы Uniswap v2 для активов с разной ценой, пулы Uniswap v3 с возможностью контролировать ценовой диапазон, в котором предоставляется ликвидность и Balancer v2 для объединения активов разных типов в один пул.

Пользователь может добавить или удалить ликвидность (создать пул ликвидности) в активах x_A из блокчейна А и y_B из блокчейна В и получить свой LP токен в сети А или В, на выбор. В этом случае в целевом блокчейне (например В) создается пул ликвидности и происходят следующие преобразования:

$s(x_A, A, B) = ex_A$ - перемещение x_A из цепи А в цепь В,

$ex_A + y_B \Rightarrow Lp_B(ex_A, y_B)$ - добавление ликвидности в блокчейне В,

$x_A, ey_B \in A; y_B, ex_A, Lp_B \in B, \forall A, B \in S$

$\forall x_A \exists ex_A \Rightarrow \exists Lp_B(ex_A, y_B) \forall y_B, ex_A$

где ex_A - синтетический актив, выпущенный на блокчейне В посредством блокировки оригинального актива x_A в исходном блокчейне А.

Lp_B - токен кросс-чейн пула ликвидности в блокчейне В, состоящий из синтетического актива ex_A и нативного y_B .

При удалении ликвидности происходит обратный процесс с возможностью получить ликвидность либо в оригинальных активах и сетях, либо получить оригинальный актив плюс синтетический актив.

$removeLp_B(ex_A, y_B) \Rightarrow ex_A + y_B$ - удаление ликвидности из пула в блокчейне В,

$u(ex_A, B, A) = x_A$ - перемещение x_A из блокчейна В обратно в А, через сжигание ex_A .

Пользователь может производить любые обменные операции между нативными и/или синтетическими активами в рамках пулов имеющих на каждом из блокчейнов.

Пользователь может добавить ликвидность/создать пул ликвидности в любом из поддерживаемых блокчейнов, используя как любые синтетические активы, уже выпущенные в этом блокчейне с использованием нашей платформы, так и нативные активы этого блокчейна.

Это порождает большое множество возможных комбинаций, например рассмотрим вариант использования АММ пулов типа Uniswap v2:

$x_A + y_A \Rightarrow Lp_A(x_A, y_A)$ - классический пул Uniswap v2 в блокчейне А.

$s(x_A, A, C) = ex_A$ - перемещение x_A из блокчейна А в блокчейн С,

$s(y_B, B, C) = ey_B$ - перемещение y_B из блокчейна В в блокчейн С,

$ex_A + ey_B \Rightarrow Lp_C(ex_A, ey_B)$ - кроссчейн пул в блокчейне C, связывающий активы x_A и y_B из блокчейнов A и B.

$$\forall x_A \in A, y_B \in B, ex_A, ey_B \in C \Rightarrow \exists Lp_C(ex_A, ey_B) \in C.$$

$s(x_A, A, B) = ex_A$ - перемещение x_A из блокчейна A в блокчейн B,

$s(y_A, A, B) = ey_A$ - перемещение y_A из блокчейна A в блокчейн B,

$ex_A + ey_A \Rightarrow Lp_B(ex_A, ey_A)$ - пул-петля, обменивающий активы из блокчейна A внутри блокчейна B, что актуально для Ethereum.

$$\forall x_A, y_A \in A; \exists ex_A, ey_A, Lp_B(ex_A, ey_A) \in B$$

$s(x_A, A, B) = ex_A$ - перемещение x_A из блокчейна A в блокчейн B,

$ex_A + y_B \Rightarrow Lp_B(ex_A, y_B)$ - кроссчейн пул в блокчейне B, связывающий активы x_A и y_B из блокчейнов A и B.

$$\forall x_A \in A \exists ex_A \in B, y_B \in B \exists Lp_B(ex_A, y_B) \in B$$

Иными словами, пользователь может создавать любые пулы ликвидности (как кроссчейн, так и классические), работая в пределах одного, двух и даже трёх блокчейнов в случае с Uniswap пулами.

Если рассмотреть Curve-пулы, то число блокчейнов в кроссчейн пуле может достигать шести-восьми, а в случае с Balancer - более десяти, если этого потребует бизнес-логика.

11. Токеномика проекта

Общее предложение токена EYWA составит 1 миллиард с возможностью дополнительного выпуска общим решением комьюнити.

	EYWA tokens	%, total supply	Vesting time	Unlock
Private round	120,000,000	12%	18 months	10% 6 months after TGE, weekly unlock after
Public sale	20,000,000	2%	TBA	TBA
Airdrop for early adopters	10,000,000	1%	none	100% after mainnet
DigiU.Ventures seed investor	50,000,000	5%	20 months	10% 9 months after TGE, weekly unlock after
Founders and team	170,000,000	17%	20 months	10% 12 months after TGE, weekly unlock after
Advisers (up to 5%)	50,000,000	5%	20 months	10% 12 months after TGE, weekly unlock after
DAO treasury: yield farming, staking rewards, grants, marketing, governance incentivise, strategic investors allocation.	580,000,000	58%		
Total:	1,000,000,000	100%		

Вестинг и заморозка активов

Все токены, реализованные в ходе приватных раундов финансирования, токены команды и эдвайзеров будут заморожены с постепенной разблокировкой согласно плану вестинга, который приведен в таблице выше.

Все замороженные токены смогут принять участие в защите сети сразу после запуска EYWA Relay Network в mainnet. Замороженные токены могут быть делегированы в governance-контракты на протяжении всего срока вестинга. Полученные за этот период награды также будут заморожены и будут разблокироваться постепенно согласно расписания, которое мы опубликуем после запуска сети в майннет.

Этот механизм позволит защитить ранних розничных инвесторов, развивать проект поэтапно, постепенно наращивать объем передаваемой ценности и иметь значительную защищенность и децентрализацию уже на раннем этапе.

Airdrops

Мы предусматриваем вознаграждение для ранних пользователей, тестирующих и DeFi энтузиастов в размере 1% от эмиссии.

Тестирование будет многоэтапным.

1. Тестирование интерфейсов для основных кроссчейн-механик.
2. Тестирование EYWA Relayer Network.
3. Bug bounty для профессиональных разработчиков на поиск ошибок в коде.

Альфа-тестирование пройдет в формате игры, участники будут выполнять различные задания и зарабатывать баллы. Согласно накопленным баллам по окончании тестирования мы создадим коллекцию уникальных NFT, чем больше очков – тем более редкий NFT смогут получить участники. На каждый NFT пропорционально будут начислены токены EYWA, в зависимости от его уникальности. Мы считаем этот подход максимально открытым и честным.

Награды за стейкинг Roll-DPoS

Для того чтобы стать держателем узла EYWA Relayer Network, необходимо будет внести в смарт-контракт минимальный залог в размере 100 000 EYWA.

На первой фазе запуска сети держатели узлов EYWA Relayer Network будут получать в токенах EYWA фиксированную годовую доходность на свой залог.

Дополнительная возможность для заработка – персональные стейкинг-пулы, которые автоматически создаются для каждого узла, имеющего минимальный залог. Владелец узла может устанавливать комиссию в своем пуле, в каждый пул можно будет делегировать сумму, в пять раз превышающую стейк владельца пула.

Со временем, помимо фиксированной доходности, узлы начнут получать дополнительное вознаграждение – процент от оплаты за передаваемые сетью кроссчейн-вызовы.

Помимо кроссчейн-вызовов, со временем мы планируем добавить функциональность DeFi-оракулов – сеть сможет оказывать услуги по поставке price feeds и VRF, а также gasless-транзакции для различных DeFi-приложений во множестве блокчейнов.

Процент годовой инфляции, расходуемой на EYWA Relayer Network, будет изменяться путем голосования в DAO EYWA.

DAO EYWA

Наш путь к полной децентрализации – это построение кроссчейн-DAO как системы смарт-контрактов, управляющих всеми параметрами протокола EYWA:

- скорость эмиссии в EYWA Relay Network;
- размер комиссии за кроссчейн-вызовы;
- размер комиссии за работу с синтетическими активами;
- размер комиссии за обменные операции;
- процент вознаграждения разработчиков;
- процент, расходуемый на выкуп токенов EYWA с рынка;
- доходность пулов ликвидности;
- управление лимитами в пулах ликвидности;
- управление контрактами, хранящими ликвидность, обеспечивающую синтетические e-токены;
- решения о выдаче грантов;
- предложения по новому функционалу и многое другое.

Поскольку EYWA будет включать в себя огромное количество смарт-контрактов, распределенных во множестве блокчейнов, управление ими будет осуществляться из одного блокчейна, в котором будет располагаться главный Governance-контракт, посылающий сообщения timelock-контрактам в других блокчейнах, используя EYWA Cross-chain Data Protocol.

Владельцем контрактов на раннем этапе будет multisig кошелек разработчиков, а затем – timelock-контракты, подчиняющиеся главному Governance-контракту.

Держатели токенов, заблокированных в EYWA Relay Network, будут иметь возможность участия в голосованиях DAO EYWA.

Награды за кросс-чейн фарминг

Основной принцип токеномики EYWA – бережливость и разумное расходование токенов. Следуя этому принципу, мы дадим провайдерам ликвидности уникальное предложение: стабильно получать высокую доходность без риска непостоянных потерь.

Как мы этого достигнем?

1. Поскольку основная часть доходов от предоставления ликвидности в DeFi – это доход в токенах проектов, в которые предоставляется ликвидность, мы приняли решение сделать это главным видом их дохода.

Чтобы обеспечить доходность выше рынка, для каждого пула мы ограничим максимально возможное количество ликвидности, на которое будут выплачиваться вознаграждения токенами EYWA. Остальная часть ликвидности будет получать прибыль только от обменных операций. Это условие связано с тем, чтобы эффективно расходовать токены проекта.

Для того, что получать повышенные вознаграждения за предоставление ликвидности в токенах EYWA, необходимо будет заблокировать некоторое их количество в стейкинге EYWA Relay Network на определенный срок. Это количество будет зависеть от желаемого объема капитала. После блокировки требуемого числа токенов провайдер ликвидности будет получать повышенную доходность. Заблокированные в стейкинге средства будут давать вам голоса в DAO. Этот подход применяется в проекте Curve и он нам близок. <https://dao.curve.fi/minter/calc>

Каждый кроссчейн-пул по своей сути является мостом для нативных токенов между двумя и более блокчейнами. И для того чтобы этот пул был эффективен для его пользователей с точки зрения величины ценового проскальзывания, в нем должно быть вполне конкретное количество ликвидности, что является расчетной величиной, в зависимости от типа пула (Uniswap v2, Curve, etc). Наша задача – максимизировать количество кроссчейн-пулов для различных активов и направлений, поэтому их будет много и мы будем стремиться балансировать ликвидность между ними равномерно.

Кроме того, доходность лимитированного пула ликвидности является более прогнозируемой – при его максимальном наполнении провайдер ликвидности может выполнить пессимистичный расчет доходности, имея только одну неизвестную – цену токена EYWA. В обычных пулах доходность провайдеров ликвидности снижается за счет конкуренции – неконтролируемого притока нового капитала в размерах, порой избыточных для выполнения основной функции пула ликвидности – выгодного обмена. Мы сможем гибко управлять доходностью и емкостью пулов, меняя следующие параметры:

- разрешенный максимальный объем LP токенов кроссчейн-пула, который может быть размещен в смарт-контракте фарминга токена EYWA;
 - количество токенов EYWA, выделяемых на каждую тысячу долларов ликвидности в пуле.
2. Мы устанавливаем низкую комиссию за обменные операции на EYWA DEX в диапазоне от 0.04% до 0,2%, в зависимости от типа пула, что будет привлекательно для трейдеров и часть этой комиссии будет распределяться на оплату текущих нужд проекта. Более подробно это описано в разделе комиссии EYWA. За счет ограниченных пулов ликвидности мы будем стремиться держать доходность выше рынка, несмотря на то, что не планируем отдавать часть комиссий трейдерам. Они получают эти деньги в виде токенов EYWA, ценность которых будет поддерживаться за счет регулярного обратного выкупа и множества различных способов применения токена, описанных в разделе Token Utility.
 3. Блокировка вознаграждений.
По умолчанию получаемые за предоставление ликвидности награды будут заморожены.
Вы сможете разморозить награды, полученные при фарминге, предоставив на некоторое время ликвидность в пуле с токеном EYWA. Это будет способствовать высокому уровню ликвидности токена EYWA.

Utility token

1. Токен EYWA используется для обеспечения безопасности и децентрализации передачи информации между блокчейнами, поскольку в выбранной нами модели консенсуса протокол передачи данных удастся скомпрометировать, только имея не менее чем 50-65% от общего заблокированного стека. Держатели узлов EYWA Relayer Network являются холдерами токена EYWA и получают в нем вознаграждения. Они заинтересованы в исправной работе протокола и намерены защищать свои инвестиции.
2. Для рядовых инвесторов, не имеющих достаточных знаний, чтобы запустить собственную ноду, существует возможность делегировать свои токены в лю-

бой из доступных стейкинг-пулов работающих узлов, не доверяя ему свои средства, и принимать участие в стейкинге.

3. Токен EYWA будет служить платежным средством для расчета за осуществление кроссчейн-вызовов и являться аналогом Gas-токена в Ethereum, то есть мы планируем осуществлять приоритезацию кроссчейн-вызовов согласно размеру комиссий, выплачиваемых за эти вызовы.
4. Токен EYWA используется в качестве вознаграждения для провайдеров ликвидности, предоставляющих активы в кроссчейн-пулы.
5. Токен EYWA является governance-токеном и позволяет принимать участие в управлении протоколом через голосование. Один токен дает один голос.

Комиссии EYWA

1. Комиссия EYWA Cross-chain Bridge – 0-0,1% за выпуск и уничтожение «е»-токенов. По сути это комиссия за перемещение активов между блокчейнами.
2. Комиссия за обменные операции в EYWA DEX – от 0.04% до 0,2%, в зависимости от типа пула, в любом из поддерживаемых блокчейнов.
3. Комиссия за кроссчейн-вызовы – плата, взимаемая в токенах EYWA за валидацию кроссчейн-вызовов, является динамической величиной и зависит от загруженности сети EYWA и стоимости транзакций, в задействованных в вызове блокчейнах.
4. Комиссия за совершение gasless-вызовов – помимо основной стоимости вызова самой транзакции или цепочки транзакций, мы закладываем небольшую премию, чтобы гарантировано компенсировать свои затраты.
5. Комиссия за вызов DeFi-оракулов (в будущем) – плата за пользование price feeds, VRF.

Все комиссии, которые зарабатывает протокол EYWA, могут быть направлены на финансирование следующих видов целевой деятельности:

- a. выкуп токенов EYWA с рынка и пополнение казны DAO. В зависимости от ситуации может быть принято решение сжигать часть этих токенов, хотя мы предполагаем, что это не потребуется;
- b. покупка и пополнение нативными криптовалютами gasless-смарт-контрактов, обеспечивающих работу EYWA Relay Network. Эти контракты поддерживают работу системных процессов – смену эпох, запись информации о новых пакетах транзакций, передачу информации об эпохах и пакетах между всеми блокчейнами;
- c. вознаграждение узлам EYWA Relay Network;
- d. субсидирование транзакционных издержек некоторым группам пользователей, имеющих небольшой оборот и совершающих небольшие сделки;
- e. поддержка и расширение команды разработки, расходы на маркетинг и пиар проекта;
- f. Выделение грантов, проведение хакатонов, баг баунти.

Поскольку невозможно знать будущее, мы закладываем максимальную гибкость в токеномику, чтобы иметь возможность управлять стимулами. Со временем некоторые процессы, вероятно, будут автоматизированы, такие как автоматический выкуп токена EYWA.

Гранты и хакатоны

Мы намерены активно привлекать разработчиков DeFi-протоколов и стимулировать их использовать EYWA Cross-chain Data Protocol для построения собственных кроссчейн-приложений.

Эта функция будет доступна, начиная со стадии альфа-тестирования – уже в тестнетах разработчики смогут отлаживать кроссчейн-взаимодействие своих смарт-контрактов, используя нашу технологию. Мы будем поддерживать команды и проекты, интегрирующие наши технологии. Для этого DAO EYWA будет выделять ресурсы на гранты, организацию и проведение собственных хакатонов, быть спонсором на крупных хакатонах, таких как EthGlobal. Мы планируем использовать такие площадки, как Gitcoin и ImmuneFi, для размещения грантов, проведения онлайн-хакатонов и bug bounty. Открытые тестирования кода позволят нам непрерывно повышать безопасность и устойчивость протокола.

12. Команда:



Boris Povar
Chief Executive
Officer, founder
Linkedin



**Alexander
Denisov**
Chief Technical
Officer
Linkedin



Alexander I
Chief Strategic
Officer, founder
Linkedin



Sergey Zinenko
Chief Financial
Officer, founder
Linkedin



Anatoliy Gugel
Chief Marketing
Officer
Linkedin



Denis Glotov
Head of Tech
Linkedin



**Bogdan
Sivochkin**
Blockchain Lead
Linkedin



**Dmitriy
Christianov**
Golang
Developer
Linkedin



Vadim Gukasov
Solidity
Developer,
Teamlead
Linkedin



Vladimir Smelov
Solidity
Developer
Linkedin

Команда:



Dmitriy Gogolev
Solidity
Developer
[LinkedIn](#)



Robert Sayahov
Frontend
Developer
[LinkedIn](#)



Alexey Nagorniy
Frontend
Developer,
Teamlead
[LinkedIn](#)



**Stanislav
Kardash**
Frontend
Developer
[LinkedIn](#)



Andrey Starkov
Frontend
Developer



**Dmitriy
Gromadsky**
Chief Product
Designer
[LinkedIn](#)



**Roman
Fedoskin**
Chief Product
Officer
[LinkedIn](#)

13. Юридическая информация:

IMPORTANT NOTICE

PLEASE READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED “DISCLAIMER OF LIABILITY”, “NO REPRESENTATIONS AND WARRANTIES”, “REPRESENTATIONS AND WARRANTIES BY YOU”, “CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS”, “MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS”, “NO ADVICE”, “NO FURTHER INFORMATION OR UPDATE”, “RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION”, “NO OFFER OF SECURITIES OR REGISTRATION” AND “RISKS AND UNCERTAINTIES” CAREFULLY.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, PLEASE CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

EYWA Tokens are not intended to constitute securities in any jurisdiction. This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

This White Paper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by the distributor/vendor of EYWA Tokens (the “Distributor”) to purchase any EYWA Tokens, nor shall it or any part of it, nor the fact of its presentation form the basis of, or be relied upon in connection with any contract or investment decision.

The Distributor will be EYWA (“EYWA”), and will deploy all proceeds of sale of the EYWA Tokens to fund EYWA’s cryptocurrency project, businesses and operations.

No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the EYWA Tokens and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper.

Any agreement as between the Distributor and you as a purchaser, and in relation to any sale and purchase, of EYWA Tokens (as referred to in this White Paper) is to be governed by only a separate document setting out the terms and conditions (the “Terms and Conditions”) of such an agreement. In the event of any inconsistencies between the Terms and Conditions and this White Paper, the former shall prevail.

You are not eligible and you are not to purchase any EYWA Tokens in the EYWA Initial Token Sale (as referred to in this White Paper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

There are risks and uncertainties associated with EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in this White Paper).

This White Paper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this White Paper is prohibited or restricted.

No part of this White Paper is to be reproduced, distributed or disseminated without including this section and the following sections entitled “Disclaimer of Liability”, “No Representations and Warranties”, “Representations and Warranties By You”, “Cautionary Note On Forward-Looking Statements”, “Market and Industry Information and No Consent of Other Persons”, “Terms Used”, “No Advice”, “No Further Information or Update”, “Restrictions On Distribution and Dissemination”, “No Offer of Securities Or Registration” and “Risks and Uncertainties”.

DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, EYWA and/or the Distributor shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES

EYWA and/or the Distributor does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this White Paper.

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this White Paper or such part thereof (as the case may be), you represent and warrant to EYWA and/or the Distributor as follows:

(a) you agree and acknowledge that the EYWA Tokens do not constitute securities in any form in any jurisdiction;

(b) you agree and acknowledge that this White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities in any jurisdiction or a solicitation for investment in securities and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper;

(c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this White Paper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this White Paper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

(d) you agree and acknowledge that this White Paper, the undertaking and/or the completion of the EYWA Initial Token Sale, or future trading of the EYWA Tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the EYWA and/or the Distributor, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in this White Paper);

(e) the distribution or dissemination of this White Paper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to EYWA and/or the Distributor;

(f) you agree and acknowledge that in the case where you wish to purchase any EYWA Tokens, the EYWA Tokens are not to be construed, interpreted, classified or treated as:

- (i) any kind of currency other than cryptocurrency;
- (ii) debentures, stocks or shares issued by any person or entity (whether EYWA and/or the Distributor)
- (i) rights, options or derivatives in respect of such debentures, stocks or shares;
- (ii) rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;
- (iii) units in a collective investment scheme;
- (iv) units in a business trust;
- (v) derivatives of units in a business trust; or
- (vi) any other security or class of securities.

(g) you are fully aware of and understand that you are not eligible to purchase any EYWA Tokens if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore;

(h) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology;

(i) you are fully aware and understand that in the case where you wish to purchase any EYWA Tokens, there are risks associated with EYWA and the Distributor and their respective business and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper);

(j) you agree and acknowledge that neither EYWA nor the Distributor is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this White Paper or any part thereof by you; and

(k) all of the above representations and warranties are true, complete, accurate and non- misleading from the time of your access to and/or acceptance of possession this White Paper or such part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in this White Paper, statements made in press releases or in any place accessible by the public and oral statements that may be made by EYWA and/or the Distributor or their respective directors, executive officers or employees acting on behalf of EYWA or the Distributor (as the case may be), that are not statements of historical fact, constitute “forward- looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding EYWA’s and/or the Distributor’s financial position, business strategies, plans and prospects and the future prospects of the industry which EYWA and/or the Distributor is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to EYWA’s and/or the Distributor’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this White Paper regarding EYWA and/or the Distributor are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of EYWA and/or the Distributor to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

(a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which EYWA and/or the Distributor conducts its respective businesses and operations;

(b) the risk that EYWA and/or the Distributor may be unable or execute or implement their respective business strategies and future plans;

(c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;

(d) changes in the anticipated growth strategies and expected internal growth of EYWA and/or the Distributor;

(e) changes in the availability and fees payable to EYWA and/or the Distributor in connection with their respective businesses and operations;

(f) changes in the availability and salaries of employees who are required by EYWA and/or the Distributor to operate their respective businesses and operations;

- (g) changes in preferences of customers of EYWA and/or the Distributor;
- (h) changes in competitive conditions under which EYWA and/or the Distributor operate, and the ability of EYWA and/or the Distributor to compete under such conditions;
- (i) changes in the future capital needs of EYWA and/or the Distributor and the availability of financing and capital to fund such needs;
- (j) war or acts of international or domestic terrorism;
- (k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of EYWA and/or the Distributor;
- (l) other factors beyond the control of EYWA and/or the Distributor; and
- (m) any risk and uncertainties associated with EYWA and/or the Distributor and their businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper).

All forward-looking statements made by or attributable to EYWA and/or the Distributor or persons acting on behalf of EYWA and/or the Distributor are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of EYWA and/or the Distributor to be materially different from that expected, expressed or implied by the forward-looking statements in this White Paper, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this White Paper.

Neither EYWA, the Distributor nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of EYWA and/or the Distributor will be as discussed in those forward-looking statements. The actual results, performance or achievements of EYWA and/or the Distributor may differ materially from those anticipated in these forward-looking statements.

Nothing contained in this White Paper is or may be relied upon as a promise, representation or undertaking as to the future performance or policies of EYWA and/or the Distributor.

Further, EYWA and/or the Distributor disclaim any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

MARKET AND INDUSTRY INFORMATION AND NO CONSENT OF OTHER PERSONS

This White Paper includes market and industry information and forecasts that have been obtained from internal surveys, reports and studies, where appropriate, as well as market research, publicly available information and industry publications. Such surveys, reports, studies, market research, publicly available information and publications generally state that the information that they contain has been obtained from sources believed to be reliable, but there can be no assurance as to the accuracy or completeness of such included information.

Save for EYWA, the Distributor and their respective directors, executive officers and employees, no person has provided his or her consent to the inclusion of his or her name and/or other information attributed or perceived to be attributed to such person in connection therewith in this White Paper and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information by such person and such persons shall not be obliged to provide any updates.

While EYWA and/or the Distributor have taken reasonable actions to ensure that the information is extracted accurately and in its proper context, EYWA and/or the Distributor have not conducted any independent review of the information extracted from third party sources, verified the accuracy or completeness of such information or ascertained the underlying economic assumptions relied upon therein. Consequently, neither EYWA, the Distributor, nor their respective directors, executive officers and employees acting on their behalf makes any representation or warranty as to the accuracy or completeness of such information and shall not be obliged to provide any updates on the same.

TERMS USED

To facilitate a better understanding of the EYWA Tokens being offered for purchase by the Distributor, and the businesses and operations of EYWA and/or the Distributor, certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in this White Paper. These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and vice versa and words importing the masculine gender shall, where applicable, include the feminine and neuter genders and vice versa. References to persons shall include corporations.

NO ADVICE

No information in this White Paper should be considered to be business, legal, financial or tax advice regarding EYWA, the Distributor, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper). You should consult your own legal, financial, tax or other professional adviser regarding EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper). You should be aware that you may be required to bear the financial risk of any purchase of EYWA Tokens for an indefinite period of time.

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorised to give any information or representation not contained in this White Paper in connection with EYWA and/or the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper) and, if given, such information or representation must not be relied upon as having been authorised by or on behalf of EYWA and/or the Distributor. The EYWA Initial Token Sale (as referred to in the White Paper) shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of EYWA and/or the Distributor or in any statement of fact or information contained in this White Paper since the date hereof.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this White Paper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this White Paper or such part thereof (as the case may be) at your own expense and without liability to EYWA and/or the Distributor.

Persons to whom a copy of this White Paper has been distributed or disseminated, provided access to or who otherwise have the White Paper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this White Paper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF SECURITIES OR REGISTRATION

This White Paper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this White Paper. Any agreement in relation to any sale and purchase of EYWA Tokens (as referred to in this White Paper) is to be governed by only the Terms and Conditions of such agreement and no other document. In the event of any inconsistencies between the Terms and Conditions and this White Paper, the former shall prevail.

You are not eligible to purchase any EYWA Tokens in the EYWA Initial Token Sale (as referred to in this White Paper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a citizen or resident of the Republic of Singapore.

No regulatory authority has examined or approved of any of the information set out in this White Paper. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this White Paper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective purchasers of EYWA Tokens (as referred to in this White Paper) should carefully consider and evaluate all risks and uncertainties associated with EYWA, the Distributor and their respective businesses and operations, the EYWA Tokens, the EYWA Initial Token Sale and the EYWA Wallet (each as referred to in the White Paper), all information set out in this White Paper and the Terms and Conditions prior to any purchase of EYWA Tokens. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of EYWA and/or the Distributor could be materially and adversely affected. In such cases, you may lose all or part of the value of the EYWA Tokens.

14. Источники

- [1] Виталик Бутерин о шардинге <https://vitalik.ca/general/2021/04/07/sharding.html> - [Страница 3]
- [2] Кросс-чейн мост Binance <https://www.binance.org/en/bridge> - [Страница 7]
- [3] Сеть кросс-чейн ликвидности ThorChain <https://www.thorchain.com/> - [Страница 7]
- [4] Anyswap DEX <https://anyswap.net/> - [Страница 7]
- [5] Протокол кросс-чейн интероперабельности Axelar Network <https://axelar.network/> - [Страница 7]
- [6] Совместимость блокчейна NEAR с Ethereum <https://near.org/blog/eth-near-rainbow-bridge/> - [Страница 7]
- [7] Основы пороговой криптосистемы https://en.wikipedia.org/wiki/Threshold_cryptosystem - [Страница 7]
- [8] Whitepaper PolyNetwork <https://www.poly.network/PolyNetwork-whitepaper.pdf> - [Страница 8]
- [9] Протокол кросс-чейн передачи ликвидности REN Project <https://renproject.io/> - [Страница 8]
- [10] Второй сайт REN Project <https://www.darknodes.io/> - [Страница 8]
- [11] Github REN Project <https://github.com/renproject/ren/wiki/Phases> - [Страница 8]
- [12] Релиз REN Project <https://medium.com/renproject/going-live-with-renvm-v0-4-941fb097e983> - [Страница 8]
- [13] Whitepaper PolyNetwork <https://www.poly.network/PolyNetwork-whitepaper.pdf> - [Страница 13]
- [14] Взлом PolyNetwork <https://medium.com/poly-network/honour-exploit-and-code-how-we-lost-610m-dollar-and-got-it-back-c4a7d0606267> - [Страница 13]
- [15] Cosmos Stargate IBC <https://stargate.cosmos.network/> - [Страница 13]
- [16] Fusion Yellowpaper <https://www.fusion.org/themes/fusion/assets/pdf/Fusion-Yellow-Paper.pdf> - [Страница 13]
- [17] FAQ Anyswap DEX <https://anyswap-faq.readthedocs.io/en/latest/index.html> - [Страница 13]
- [18] Github Anyswap DEX <https://fusiondev.gitbook.io/fusion/dapps/anyswap/> - [Страница 13]
- [19] Взлом Anyswap <https://anyswap.medium.com/anyswap-multichain-router-v3-exploit-statement-6833f1b7e6fb> - [Страница 13]
- [20] Github Antonell Multibridge <https://github.com/antonell/multibridge.xyz> - [Страница 13]
- [21] Кросс-чейн мост Anyswap <https://multichain.xyz/> - [Страница 13]
- [22] Приложение для кросс-чейн транзакций Chainswap <https://chainswap.com/> - [Страница 13]
- [23] Взлом Chainswap <https://chain-swap.medium.com/asap-token-important-update-67073aae925c> - [Страница 13]
- [24] Сеть кросс-чейн ликвидности ThorChain <https://thorchain.org/> - [Страница 13]
- [25] Взлом ThorChain <https://medium.com/breadcrumbsapp/thorchain-heist-an-analysis-of-the-fund-flow-7ca18a18d044> - [Страница 13]
- [26] Взлом ThorChain 2 <https://medium.com/breadcrumbsapp/thorchain-hack-2-analysis-of-the-fund-flow-bb53f07b0f46> - [Страница 13]
- [27] Whitepaper Polygon <https://polygon.technology/lightpaper-polygon.pdf> - [Страница 13]
- [28] Litepaper DFYN DEX <https://www.dfyn.network/assets/docs/Dfyn-Litepaper.pdf> - [Страница 13]
- [29] Кросс-чейн мост Binance <https://academy.binance.com/en/articles/an-introduction-to-binance-bridge> - [Страница 13]
- [30] Протокол кросс-чейн интероперабельности Chainlink <https://chain.link/solutions/cross-chain> - [Страница 13]
- [31] Протокол кросс-чейн интероперабельности Connexx <https://docs.connexx.network/> - [Страница 13]

-
- [32] Протокол кросс-чейн интероперабельности ChainBridge <https://chainbridge.chainsafe.io/> - [Страница 13]
 - [33] PR статья о ChainBridge <https://medium.com/chainsafe-systems/a-bridge-to-a-new-world-7627472eaf9d> - [Страница 13]
 - [34] Curve DEX <https://curve.fi/> - [Страница 14]
 - [35] Uniswap DEX <https://uniswap.org/> - [Страница 14]
 - [36] Balancer DEX <https://balancer.fi/> - [Страница 14]
 - [37] Проект Horizen <https://www.horizen.io/> - [Страница 16]
 - [38] Проект Ethereum Gas Station Network <https://opengsn.org/> - [Страница 17]
 - [39] Платформа управления криптоактивами Gnosis Safe <https://docs.gnosis.io/safe/> - [Страница 17]
 - [40] Стандарт подписей Ethereum EIP-712 <https://eips.ethereum.org/EIPS/eip-712#simple-summary> - [Страница 17]
 - [41] Основы DAO <https://coinmarketcap.com/alexandria/article/what-is-a-dao-> [Страница 17]
 - [42] Основы DAO <https://medium.com/smartz-blog/what-is-dao-and-how-it-works-d43ec5bc236f> - [Страница 17]
 - [43] Tendermint BFT <https://tendermint.com/core> - [Страница 21]
 - [44] Основы цифровых подписей BLS https://en.wikipedia.org/wiki/BLS_digital_signature - [Страница 21]
 - [45] Основы “Дилеммы заключенного” https://en.wikipedia.org/wiki/Prisoner%27s_dilemma - [Страница 21]
 - [46] Whitepaper IoTeX http://files.iotex.io/publications/IoTeX_Whitepaper_1.5_EN.pdf - [Страница 22]
 - [47] Whitepaper Algorand https://algorandcom.cdn.prismic.io/algorandcom%2Fa26acb80-b80c-46ff-a1ab-a8121f74f3a3_p51-gilad.pdf - [Страница 23]