ОБЗОР ПРОЕКТА

FANTOM

UBF

Краткое описание и история проекта

Fantom — это высокопроизводительная, масштабируемая, совместимая с EVM (Ethereum Virtual Machine, виртуальная машина Ethereum) и безопасная платформа смарт-контрактов, с направленным ациклическим графом (DAG).

Вместе со своим собственным токеном (FTM) Fantom стремится решить проблемы, связанные с платформами смарт-контрактов, в частности скорость транзакций, которую, по словам разработчиков, они сократили до двух секунд.

Fantom — это децентрализованная платформа смарт-контрактов с открытым исходным кодом для DApps (децентрализованных приложений) и цифровых активов, созданная в качестве альтернативы Ethereum. Fantom ставит перед собой цель преодолеть ограничения блокчейна предыдущего поколения и сбалансировать три компонента: масштабируемость, безопасность и децентрализацию. Проект предлагает набор инструментов для упрощения процесса интеграции существующих DApp, а также подробную систему вознаграждений за стейкинг и встроенные инструменты DeFi.

Одной из сильных сторон Fantom является его производительность и эффективная обработка транзакций, а именно тысячи транзакций в секунду, где расчеты по транзакциям занимают 1-2 секунды, а стоимость составляет доли цента за транзакцию. В результате Fantom обеспечивает более высокую масштабируемость при меньших затратах.

Экосистема основана на двух основных технологиях: протоколе Lachesis и Opera.

Протокол Lachesis — это основной уровень консенсуса, который защищает сеть Fantom, обеспечивая как скорость транзакций, так и безопасность.

Lachesis — это механизм консенсуса aBFT (Asynchronous Byzantine Fault Tolerant – Асинхронная Византийская Отказоустойчивость), это свойство

системы способное противостоять классу отказов, возникающих из-за Проблем Византийских Генералов), использующий алгоритм направленного ациклического графа (DAG). Как это работает: сетевые данные могут обрабатываться в разное время, и сеть фильтрует участников, пропуская только одну треть, которые выделены из-за ошибочного или злонамеренного поведения, без ущерба для сетевых процессов.

Механизм консенсуса aBFT Proof-of-Stake (PoS) поддерживает эффективность всей сети, его конструкция обеспечивает безопасность на максимальной скорости. Разработчики Fantom подчеркивают, что механизм PoS — явление безлидерное — нет лидеров блоков и участников, и любой может присоединиться (или выйти) из сети нод в удобный момент.

Ключевые качества Lachesis: асинхронность, отсутствие лидеров, византийская отказоустойчивость и почти мгновенная завершенность.

Что касается Opera - это система разработки приложений и платформа развертывания основной сети Fantom, а также хостинг DApp без разрешений и с открытым исходным кодом. Благодаря интеграции EVM и поддержке языка программирования Solidity Fantom обладает полным набором возможностей смарт-контрактов, что позволяет пользователям беспрепятственно взаимодействовать с платформами Ethereum, сохраняя при этом преимущество эффективности транзакций Fantom.

Fantom Foundation пришел к выводу, что удаление лидеров блоков повышает безопасность сети, поэтому Opera использует модель PoS и валидаторов без лидеров (валидаторы не определяют, какие блоки действительны).

В дополнение к тому, что это быстрая, безопасная и дешевая платежная платформа, которая позволяет совершать быстрые и безопасные платежи с минимальными затратами, Fantom также имеет управление по цепочке, когда

пользователи голосуют токенами FTM (один токен равен одному голосу). Из особенностей: пользователи имеют право выражать степень согласия/несогласия по шкале от 0 до 4.

Модульный Fantom

Модульность делает Fantom исключительно гибким. Разработчики могут перенести свои существующие dApp на основе Ethereum в основную сеть Fantom Opera за считанные минуты, существенно повысив производительность и снизив затраты.

Fantom безопасен и экологичен

Fantom защищен Proof-of-Stake. В отличие от Proof-of-Work, используемого Биткоином и Эфиром, Proof-of-Stake предотвращает централизацию и экономит электроэнергию.

Lachesis может обеспечить безопасность распределенных сетей корпоративного уровня. Fantom предлагает абсолютную завершенность, что означает, что транзакции никогда не могут быть отменены, как в сетях с вероятностной завершенностью.

Механизм консенсуса также может масштабироваться до сотен нод, повышая децентрализацию и, следовательно, безопасность.

Наконец, у Lachesis нет лидера. Устранив лидеров, безопасность не полагается на небольшой набор действующих лиц.

Fantom с открытым исходным кодом

Наши команды стремятся создавать строительные блоки, которые каждый может использовать и настраивать в соответствии со своими потребностями. Мы неуклонно стремимся к высокой прозрачности нашей работы. Основываясь на этих принципах, наш код имеет открытый исходный код и доступен на Github.

Fantom открыт для всех

Fantom не имеет системы разрешений. Любой может запустить ноду.

В Opera Chain от Fantom практически неограниченное количество нод-валидаторов может участвовать в защите сети, если они держат у себя как минимум 1 000 000 FTM.

Если у вас меньше токенов или вы не являетесь экспертом в управлении распределенными системами, вы все равно можете участвовать в защите сети.

Вы можете делегировать как минимум 1 FTM ноде валидатора и получать вознаграждение.

Стратегические партнеры

Chainlink

Band protocol

The Graph

Covalent

Ankr

API3

INDEPENDENT CAPITAL
BLOCKCHAIN FUND

Команда

“Мы создаем инфраструктуру для более связанного и эффективного будущего, в котором люди смогут воспользоваться технологическими прорывами для улучшения качества своей жизни.

Мы смиренно гордимся тем, что являемся частью цифровой революции, которая в конечном итоге охватит все аспекты нашей жизни, от платежей и полностью цифровой экономики до цифровой идентификации, медицинских карт и создания Интернета цифровых активов глобального масштаба.”

Фонд Fantom был основан южнокорейским ученым-компьютерщиком доктором Ан Бьюнг Иком (Dr. Ahn Byung Ik). В настоящее время генеральным директором платформы является Майкл Конг (Michael Kong).

Ahn Byung Ik

Founder

Michael Kong

CIO

Команда Fantom имеет большой опыт, прежде всего, в области разработки блокчейна с полным стеком, и стремилась создать платформу смарт-контрактов, которая обеспечивает масштабируемость, децентрализацию и безопасность.

Согласно официальному сайту, команда Fantom также состоит из инженеров-специалистов, ученых, исследователей, дизайнеров и предпринимателей. Сотрудники находятся по всему миру, что соответствует духу распределенной платформы.

Технологическая часть проекта

Что такое Lachesis (Лахезис)?

Lachesis — это aBFT алгоритм консенсуса. Проще говоря, механизм консенсуса — это двигатель, который приводит в действие блокчейн.

По сравнению с классическим консенсусом и консенсусом Накамото, Lachesis является более быстрым, более масштабируемым и более безопасным выбором.

Разработчики могут использовать Lachesis для создания одноранговых приложений без необходимости создавать собственный сетевой уровень.

Лахезис – это:

Асинхронный: участники могут обрабатывать команды в разное время.

Без лидера: ни один участник не играет «особую» роль.

Византийская Отказоустойчивость: поддерживает одну треть неисправных нод, включая злонамеренное поведение.

Финал: выход Lachesis можно использовать немедленно. Нет необходимости ждать подтверждения блока; транзакции подтверждаются за 1-2 секунды.

Почему Лахезис?

Мы создали Lachesis, чтобы преодолеть ограничения предыдущих алгоритмов консенсуса. На самом деле это идеальный вариант для приложений, которым требуется высокая пропускная способность, быстрая завершенность и безопасность банковского уровня.

В сегодняшнем быстро меняющемся мире все, что требует ожидания или задержки любого рода, просто не будет использоваться.

Lachesis устраняет барьер для создания быстрых децентрализованных приложений, которые может использовать каждый.

Создаете ли вы улучшенную версию существующих продуктов для таких секторов, как платежи, отслеживание цепочек поставок, хранение данных в здравоохранении и т. д., или для революционных изменений в многообещающей отрасли, такой как DeFi, Lachesis может все.

Что такое алгоритм консенсуса?

Механизм консенсуса является ядром распределенных технологий. В децентрализованной среде, где ни один центральный объект не проверяет транзакции, протокол консенсуса гарантирует, что все участники сети достигнут соглашения: сеть в целом проверяет транзакции полностью ненадежным способом.

Классический консенсус

Классические протоколы консенсуса были созданы задолго до блокчейна; они используются с 1980-х годов в распределенных базах данных.

Византийская отказоустойчивость (BFT)

Byzantine Fault Tolerance — это способность распределенной сети достигать консенсуса, следовательно, продолжать работу, несмотря на неверную информацию или злонамеренных участников внутри сети.

До Биткоина единственным способом поддерживать византийскую отказоустойчивость в распределенной сети было ограничение количества нод.

Практическая византийская отказоустойчивость (pBFT)

Практическая византийская отказоустойчивость — это модель для достижения консенсуса, позволяющая многим компьютерам вести себя как один, метод, известный как репликация конечного автомата (State Machine Replication (SMR)).

Ноды достигают консенсуса в отношении решения — такого как действительность блока — путем обмена сообщениями друг с другом о решении. В этой системе безопасность увеличивается с количеством честных нод. Честные ноды соглашаются с правильным решением и отвергают неправильное решение, предложенное злонамеренными нодами, если количество злонамеренных нод составляет менее одной трети от общего числа.

Системы pBFT энергоэффективны; им не нужны большие вычислительные ресурсы или много энергии для работы. Кроме того, pBFT может быстро достигать консенсуса, поскольку все ноды находятся в постоянной связи друг с другом, и нет необходимости в многочисленных подтверждениях. Транзакции завершаются, как только ноды соглашаются с решением.

Достижение консенсуса можно упростить, выполнив четыре шага:

1. pBFT использует механизм голосования для выбора ведущей ноды в циклическом формате
2. Лидер инициирует решение и передает его вторичным нодам
3. Все ноды, как ведущие, так и второстепенные ноды, отправляют ответ
4. Ответ считается действительным, когда ⅔ + 1 нода отправляют один и тот же ответ

Если лидер действует злонамеренно, он может быть удален большинством нод.

Однако постоянная связь также является ахиллесовой пятой pBFT: она правильно работает только в сетях с ограниченным количеством нод. Накладные расходы на связь увеличиваются в геометрической прогрессии с каждой новой нодой, которая присоединяется к сети, как и время, необходимое для ответа.

Сети pBFT также уязвимы для атак Sybil, когда один объект принимает несколько идентификаторов. Сети становятся более устойчивыми к таким атакам с большим количеством нод; однако при большем количестве нод производительность снижается, как показано выше.

Консенсус Накамото

Сатоши Накамото разработал механизм консенсуса, который решит проблемы масштабируемости классического консенсуса.

Консенсус Накамото — это модель BFT, созданная для работы в одноранговых сетях с тысячами нод, что способствует децентрализации и безопасности. Модель устраняет накладные расходы на связь, вводя Proof-of-Work.

Несмотря на улучшения, эта модель привносит другие проблемы.

- Proof-of-Work требует от всех нод решения сложных математических задач, которые потребляют огромное количество энергии.
- Он имеет очень высокое время до завершения и низкую пропускную способность. В случае Биткоина новый блок создается каждые 10 минут. Безопасно подождать 3–6 подтверждений блока — от 30 до 60 минут — прежде чем считать транзакцию завершенной. В классических системах консенсуса транзакция считается завершенной в течение нескольких секунд.

Асинхронная византийская отказоустойчивость (aBFT)

Асинхронная византийская отказоустойчивость — это наивысший стандарт алгоритмов консенсуса. Он решает трилемму масштабируемости блокчейна, согласно которой одновременно возможны только два из следующих трех компонентов:

- Децентрализация
- Безопасность

- Масштабируемость

Консенсусный протокол aBFT обеспечивает максимальную децентрализацию, высокую масштабируемость и безопасность банковского уровня.

В сети aBFT ноды могут достигать консенсуса независимо, передавая эту информацию, и им не нужно обмениваться окончательными блоками.

По этой причине механизмы консенсуса aBFT полностью лишены лидера, что повышает безопасность: нет циклического перебора и доказательства работы.

В отличие от pBFT, который основан на том факте, что все сообщения, которыми обмениваются ноды, в конечном итоге будут доставлены, aBFT допускает задержку или полную потерю сообщений. Помимо повышения устойчивости сетей к DDoS-атакам, aBFT также снижает задержку транзакций, в результате чего сеть становится быстрее.

Наконец, сети aBFT обеспечивают большую масштабируемость и децентрализацию, поскольку нет чрезмерной связи, ограничивающей количество участвующих нод.

Консенсус Lachesis

Lachesis — это алгоритм консенсуса aBFT на основе DAG, который предлагает ощутимые улучшения по сравнению как с классической моделью, так и с моделью Накамото.

Lachesis является асинхронным, безлидерным и окончательным, а также устойчивым к византийским отказам.

Lachesis предназначен для простого подключения к приложениям, написанным на любом языке программирования. Разработчики могут

сосредоточиться на построении логики приложения и интегрировать Lachesis для обработки аспекта репликации конечного автомата.

Lachesis подключается к другим нодам Lachesis и гарантирует, что все обрабатывают одни и те же команды в одном и том же порядке. Для этого он использует одноранговые сети и алгоритм консенсуса DAG aBFT.

Как действует Лахезис?

Каждая нода Лахезис хранит локальный ациклический ориентированный граф (DAG), состоящий из блоков событий, каждый из которых содержит транзакции. Группа обеспечения доступности баз данных, фиксирующая взаимосвязь между событиями «происходит до», используется для расчета точного конечного порядка событий и, следовательно, транзакций независимо на каждой ноде.

Блоки событий делятся на подтвержденные и неподтвержденные блоки событий. Новые блоки событий не подтверждаются, в то время как все блоки событий из последних 2-3+ кадров подтверждаются и впоследствии упорядочиваются честными нодами.

Результатом консенсуса являются пакеты подтвержденных блоков событий, где каждый пакет событий называется блоком. Завершенные блоки, образующие финальную цепочку, вычисляются из блоков событий независимо на каждой ноде.

В отличие от Proof-of-Work, циклического Proof-of-Stake, чеканки Proof-of-Stake и синхронизации BFT, ноды Lachesis этого не делают; отправлять блоки друг другу. Только события синхронизируются между нодами. Валидаторы не голосуют за конкретное состояние сети; вместо этого они периодически обмениваются наблюдаемыми транзакциями и событиями с одноранговыми

сетями.

В отличие от классического консенсуса, такого как pBFT, Lachesis не использует новые события на текущих выборах; вместо этого новые события используются для голосования за события на 2-3+ предыдущих виртуальных выборах одновременно. Это приводит к меньшему количеству созданных согласованных сообщений, поскольку одно и то же событие повторно используется в разных выборах.

Следовательно, Lachesis обеспечивает меньшее время до завершения и меньшие коммуникационные издержки по сравнению с синхронным BFT.

Что такое эпохи в Лахезисе?

Структура событий Лахезиса представляет собой DAG событий. Для оптимизации хранения и извлечения группа DAG разделена на подгруппы DAG, каждая из которых называется эпохой. Каждая эпоха состоит из множества завершенных блоков.

Каждая эпоха запечатывается, когда выполняется одно из следующих условий:

- Эпоха достигает определенного количества блоков
- Эпоха длится определенное время
- В этом блоке подтвержден хотя бы один читер (мошенник)
- Запечатывание эпохи запрашивается контрактом NodeDriver.

Когда эпоха запечатывается, ее внутренние индексы эпох обрезаются, а новые события запечатанных эпох игнорируются. Каждая эпоха формирует отдельную DAG, поэтому родительские группы из других эпох не допускаются.

Для проверки работоспособности каждое событие включает хэш предыдущей эпохи.

Для более подробного технического и подробного ознакомления с Lachesis вы можете посетить нашу GitHub проекта.

Что такое FTM?

FTM — это основной токен в сети Fantom. FTM используется для защиты сети посредством стейкинга, управления, платежей и комиссий.

Для чего используется FTM?

Защита сети

Основная полезность токена FTM заключается в защите сети с помощью системы Proof-of-Stake.

Для участия ноды валидатора должны иметь не менее 3 175 000 FTM, а стейкеры должны заблокировать свои FTM. В обмен на услугу как ноды, так и стейкеры получают вознаграждение и комиссионные за эпоху.

Помимо предотвращения централизации, система также является экологически чистой.

Платежи

Токен FTM идеально подходит для отправки и получения платежей благодаря высокой пропускной способности сети Fantom, быстрой финализации и низким комиссиям.

На Fantom денежные переводы занимают около 1 секунды и стоят около 0,0000001 доллара!!!

Ончейн управление

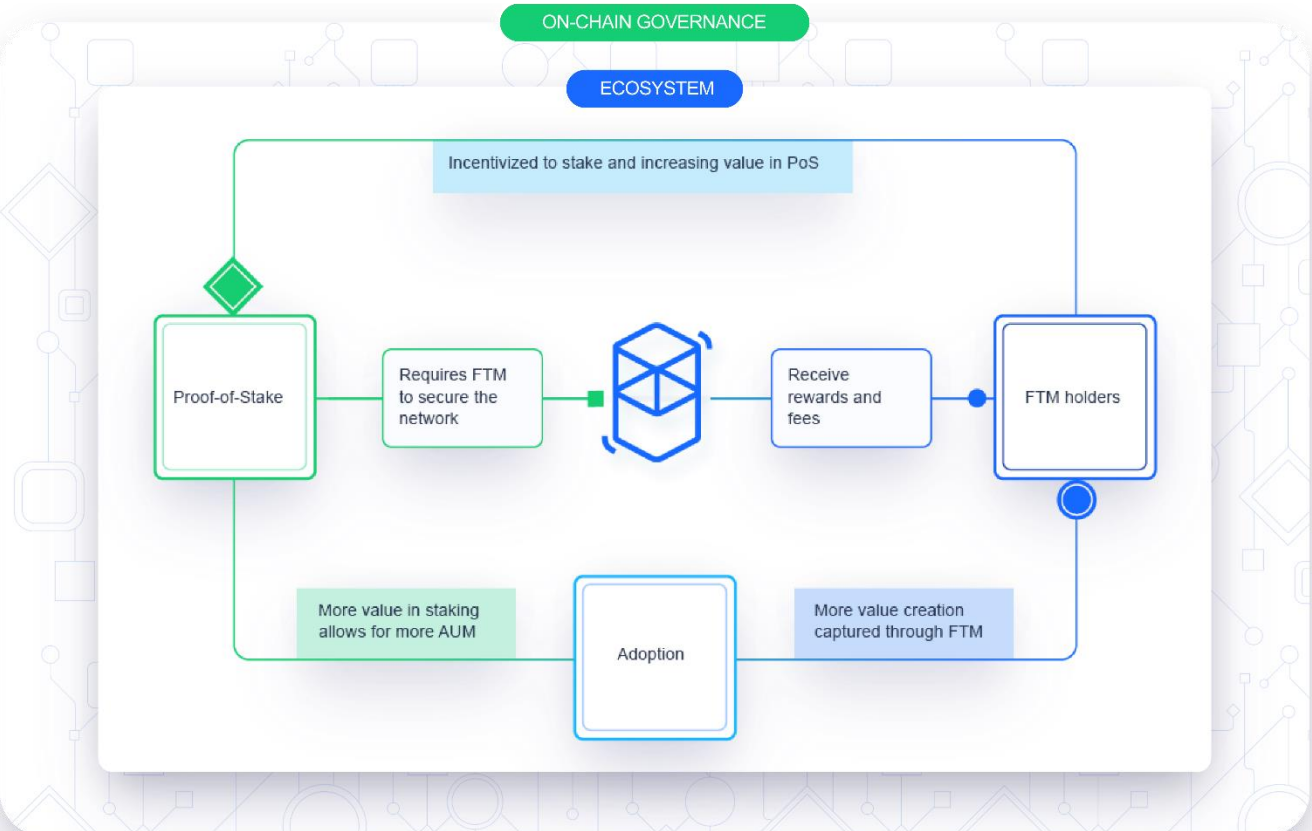
FTM необходим для управления цепочкой. Поскольку Fantom — это полностью децентрализованная экосистема без разрешений и без лидера, любое решение относительно сети осуществляется внутрисетевым управлением. Благодаря управлению заинтересованные стороны могут предлагать изменения и улучшения и голосовать за них. FTM — это токен управления, необходимый для участия в процессе голосования.

Комиссии сети

FTM используется для сетевых сборов, таких как сборы за транзакции и сборы за развертывание смарт-контрактов или создание новых сетей.

Без минимального барьера сеть станет легкой мишенью для спама, что в конечном итоге снизит производительность и заполнит реестр бесполезной информацией.

Плата за Fantom очень дешевая, но достаточная, чтобы злоумышленнику было чрезвычайно дорого провести атаку.



Обеспечение FTM

Общий объем поставок составляет 3,175 миллиарда FTM. В настоящее время в обращении находится 2,5 миллиарда монет, а остальные зарезервированы для вознаграждений за стекинг. Если вознаграждения останутся на текущем уровне (в зависимости от решений руководства), потребуется более двух лет, чтобы распределить все вознаграждения и достичь полного оборота всего предложения.

Общее предложение распределяется по разным стандартам токенов, чтобы упростить торговлю. Все токены, взятые вместе, никогда не превысят общую сумму в 3,175 миллиарда FTM.

На данный момент FTM доступен как собственный токен основной сети, как токен ERC-20, BEP-2, BEP-20. Также токен представлен в сетях Solana и Celo.