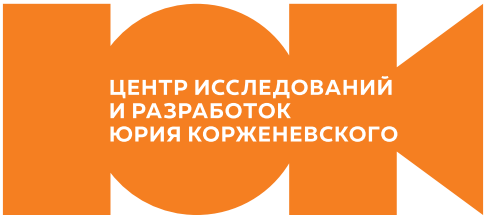

Перспективы развития Telegram Open Network

TON может стать самым большим криптовалютным сообществом в мире. Платформа даст рядовым разработчикам доступ к миллионной аудитории и возможность создавать приложения на базе криптотехнологий. Аналогичного масштаба прорыв совершил Amazon, когда дал обычным разработчикам доступ к безразмерным хранилищам файлов и облачным серверам.

О создании TON стало известно в 2017 году, но до сих пор в открытых источниках нет кода проекта и данных о тестах, зато есть техническое описание платформы на 130 страницах. Мы разобрали описание платформы и собрали в одной статье потенциально важные для бизнеса и криптосообщества моменты.

Инвестиционная привлекательность

– Тесная связь создателей с бизнес-ангелами.

– Сотрудничество с представителями легального блокчейн-сообщества (QIWI)

– Потенциальный доступ к глубокой аналитике интересов пользователей и созданию новых платформ в том виде, в котором они нужны пользователям.

– Привлечение к разработке проекта призеров спортивного программирования даёт возможность развивать проект максимально динамично — также проходила разработка Вконтакте и Telegram.

– Дистанцирование от серого и криминального капитала на этапе закрытого раунда инвестирования выводит проект в максимально легальную плоскость — это открывает возможность для масштабного партнерства с зарубежными финансовыми институтами.

– Нападки патентных троллей уже сами по себе дают положительную оценку проекту.

Прогноз развития платформы

Мы проанализировали техническое описание проекта и предыдущие работы команды, на основании этого делаем вывод:

– TON может запуститься в 2019 году.

– Команда сможет привлечь десятки миллионов пользователей в первые же месяцы работы.

– В течение года после запуска платформа станет самым большим криптовалютным сообществом в мире.

– Через два-три года после запуска появятся сопоставимые платформы с новыми идеями, но им не удастся переманить существенную часть пользователей TON.

Сильные стороны проекта

– Существующий прямой доступ более чем к 200 миллионам[1] активных пользователей.

– На разработку проекта и развертывание системы привлечена большая сумма инвестиций.

– Команда разработчиков уже создавала user-friendly global приложения.

– У проекта нет прямых конкурентов.

– Проекту помогают множество активных сторонних разработчиков приложений и ботов.

– В Telegram уже реализованы[2] функции приема платежей и сохранения адреса доставки.

– Согласно данным исследования globalwebindex[3], большая часть пользователей заинтересована в возможности пересылать деньги через мессенджер.

Слабые стороны проекта

– Высокая сложность системы сервисов платформы.

– Некоторые технические решения используются впервые и еще не протестированы на крупных проектах.

1 https://telegram.org/blog/200-million
2 https://telegram.org/blog/payments
3 https://blog.globalwebindex.com/chart-of-the-day/telegram-bbm-and-wechat-users-keenest-on-transferring-money/

Детали проекта

Распределение монет

На начальном этапе работы в распоряжении TON Foundation останется больше половины монет. Позже создатели проекта планируют сократить это число до 10%. Большое количество монет на начальном этапе поможет сгладить скачки курса и сделать экономику платформы более стабильной.

Самоизлечивающийся блокчейн

Подобное решение не использовалось в крупных проектах. Это новый подход, и он находится в одной из ключевых точек системы — исправлении ошибок в реестре.

Масштабируемость

Несмотря на заявленную в описании проекта «бесконечную шардируемость», вычислительные ресурсы системы ограничены — в алгоритме консенсуса участвует только определенное количество участников. Но часть нагрузки можно перенести на сторонних пользователей.

Бесконечная шардируемость — одна из основных отличительных особенностей TON, она позволяет непрерывно и без остановки разделять нагрузку на сервисы, каждый из которых обрабатывают отдельные участники сети.

Централизованность

Общее количество валидаторов программно ограничено сотней участников (в дальнейшем предполагается увеличение до тысячи). Валидаторами становятся претенденты, внесшие наибольший депозит, а для обработки транзакций требуется мощное оборудование. Все это увеличивает порог входа.

Разработчиками предложены способы объединения участников с необходимым депозитом и участников с необходимым оборудованием — вместе они смогут обрабатывать транзакции. В то же время в текущих крупнейших криптовалютах основная вычислительная мощность сосредоточена в руках пяти-шести майнинг пулов.

Закрытый код

Пока что код закрыт. Можно предположить, что некоторые части кода TON так и останутся закрытыми, а их безопасность будет «доказываться» конкурсами с предложением награды за попытку взломать систему снаружи без возможности анализа кода. Также работает Telegram — код клиентов и алгоритмы открыты и описаны, а код серверной части закрыт.

Общая сложность проекта

Некоторые проблемы проекта решены усложнением системы. Так, например, блоки шардчейнов должны получать подписи не только валидаторов своей группы, но и соседних — чтобы стимулировать работу межшардового роутинга сообщений.

С таким количеством сложных взаимодействующих подсистем больше шансов допустить ошибку или не учесть какой-то момент, чем при работе с относительно простой системой, как биткоин. Хотя и в биткойне есть проблемы, например с централизацией.

Шардчейн — это отдельная цепочка блоков с транзакциями определенной группы аккаунтов. Шардчейны могут делиться и объединяться, равномерно распределяя нагрузку на участников сети.

Валидатор — участник сети, который занимается проверкой транзакций пользователей и построением цепочки блоков.

Технический анализ

Проект представляет из себя набор решений для определенного круга задач. Круг задач был собран по текущим тенденциям рынка. То есть, вероятно, был планомерно составлен список проблем, которые проект должен решать, и для всех них было найдено решение.

Ключевые особенности проекта

– Масштабируемость.

– Тьюринг-полная стековая машина с возможностью создания высокоуровневых языков.

– Механизм расширения, дополнения и реконфигурации системы.

– Использование Martin-Lf dependent type theory в спецификации структур данных и сериализации сообщений.

– Широкие возможности изменения конфигурации через стандартный протокол системы.

– Широкая дополнительная инфраструктура из коробки (DNS, Storage, Micropayments, Anonymizer).

Блокчейн

Консенсус

Для обеспечения консенсуса выбран алгоритм Proof-of-Stake в группе предопределенных (системой в автоматическом режиме) валидаторов. Валидаторы общаются по BFT протоколу, он выдерживает до нечестных участников.

Масштабируемость

Для распределения нагрузки систему составили из множества разнородных блокчейнов. Динамическое масштабирование системы достигается так:

В главном единственном мастерчейне фиксируются изменения: хеши новых блоков, настраиваемые параметры системы, ввод новых функций, регистрация новых блокчейнов, доказательства недобросовестности валидаторов и другие. В обработке транзакций мастерчейна принимают участие все валидаторы.

Мастерчейн — главный блокчейн TON, в котором фиксируются хеши блоков всех остальных чейнов и сервисная информация.

Для остальных — несистемных — транзакций существует вплоть до воркчейнов. Каждый работает по своим правилам и может быть добавлен через специальную транзакцию в мастерчейн. Изначально в системе есть только один воркчейн.

Каждый воркчейн логически состоит из аккаунтчейнов — цепочек транзакций для каждого аккаунта. На практике несколько аккаунтчейнов объединяются в шардчейны, где объединены транзакции группы аккаунтов. Каждый шардчейн обрабатывается отдельно от остальных. Воркчейн может состоять из одного или вплоть до шардчейнов. Шардчейны могут динамически во время работы делиться и объединяться.

Воркчейн — блокчейн для пользовательских транзакций. Новый воркчейн со своими отдельными правилами и модулями может быть добавлен во время работы системы.

Взаимодействие блокчейнов

От существующих систем TON отличается «тесным взаимодействие блокчейнов». Аккаунты взаимодействуют с помощью сообщений. В отличие от других проектов — Cosmos, PolkaDot — эти сообщения не проходят через единую точку или единый блокчейн, а доставляются напрямую от аккаунта отправителя к аккаунту получателя.

Для доставки сообщений между шардчейнами одновременно применяется два подхода: быстрый и надежный.

– Быстрая доставка происходит по прямым сетевым каналам, но без гарантий доставки.

– Надежная доставка происходит через «роутинг по гиперкубу». Сообщение передается между соседними шардами с занесением в шардчейн. За недоставленное сообщение — штраф. Если быстрый подход сработал, то надежный, но медленный, останавливается.

Самоизлечивающийся блокчейн

В нормальной ситуации система не может принять и зафиксировать некорректную транзакцию, так как минимум валидаторов должны подписать блок. Однако система позволяет обнаруживать и исправлять некорректные блоки.

Некорректный блок исправляется, при этом все корректные операции остаются нетронутыми. Все последующие блоки, которые зависели от некорректного блока, также заменяются. При этом новые версии блоков ссылаются на старые через хеш, и старые версии остаются в системе.

Новые блоки в системе ссылаются на корректные версии исправленных.
Если обычно цепочка строится слева направо, то исправления достраиваются снизу, и дальнейший рост системы вправо происходит от исправленных блоков. Поэтому самоизлечивающийся блокчейн еще называют «2—блокчейн».

Сеть

Все взаимодействие между участниками происходит через собственную реализацию стека сетевых протоколов. На нижнем уровне используется свой протокол негарантированного обмена датаграммами (ADNL), построенного на UDP, с возможностью переключения на TCP/IP. В этом протоколе своя адресация, шифрование.

Насколько можно судить по пейперу TONa, UDP пакеты для большинства сообщений состоят из SHA512 хеша (адресата) и зашифрованного тела сообщения (публичным ключом адресата). Привязки к определенным портам UDP нет. Эти особенности усложняют блокировку, распознавание и определение трафика.

Поверх нижнего протокола обмена датаграммами существуют стриминговые протоколы, каналы, виртуальные подсети — публичные, приватные, скрытые.

TON DHT

Этот сервис — важная часть сети Telegram. С его помощью можно найти адрес нужного участника. Например, участника, который обрабатывает сообщения определенного аккаунта, чтобы передать ему транзакцию. Через этот же сервис ноды могут обновить таблицу соседей. Если один из участников использует прокси, он может записать его UDP адрес в специальный ключ DHT, чтобы остальные могли с ним связаться.

Смартконтракты

Исполнением смартконтрактов будет заниматься тьюринг-полная виртуальная машина. Разработка кода под эту машину будет надежной и простой благодаря строгой типизации, большому набору встроенных операций и встроенной проверке на переполнение типов. Позже для удобства могут быть реализованы компиляторы с высокоуровневыми языками наподобие Java, Haskell, ML.

Машина будет работать над универсальными ячейками памяти. Эти ячейки — универсальная структура, которая используется для представления, хранения и пересылки блоков и прочих структур системы.

Дополнительные сервисы

На основе блокчейна, смарт-контрактов и сетевого стека будут реализованы дополнительные сервисы: Storage, DNS, Micropayments Lightning Network — они упрощают взаимодействие с проектом для обычного пользователя, на основе этих сервисов можно быстро собрать функциональное приложение.

Интеграция в реальный мир

Продуманы детали интеграции проекта в реальный мир. Взаимодействие между внутренней сетью и внешним миром обеспечивается небольшим прокси, после пользователи смогут взаимодействовать с сервисами внутри сети TON, а сервисы TON могут получать информацию извне. Так может быть создано несколько вариантов приложений:

– On-chain: все данные и их обработка находятся в сети TON

– Off-chain: все данные и их обработка происходят на отдельных серверах, которые доступны в сети TON

– Mixed: часть данных и обработчиков выполняются on-chain, остальная часть off-chain

Конкуренты

Мы не нашли описания технологии, которая даже в теории масштабировалась бы также хорошо как TON. Есть проекты с множествами связанных блокчейнов. Там их взаимодействие происходит через единую точку, узкое место всей системы — PolkaDot, Cosmos. Есть проект с несколькими блокчейнами, широкими возможностями виртуальной машины, но без описания механизмов масштабирования — EOS.IO.

Капитализация

По данным Coinmarketcap, Биткоин по-прежнему остается самым дорогим проектом[4]. На втором месте Эфириум, остальные проекты далеко позади. Все новые проекты технически более совершенны, но набирают стоимость медленно, и с трудом отнимают долю у зарекомендовавших себя проектов. Telegram же смог собрать достаточно средств[5] чтобы оказаться в топ-10 криптовалют по капитализации в первом закрытом раунде.

Из всего этого можно сделать вывод, что Telegram Open Network еще до запуска оценивается очень высоко, а новые проекты не смогут отобрать существенную долю капитализации на старте.

4 https://coinmarketcap.com/charts/#dominance-percentage
5 https://www.bloomberg.com/news/articles/2018-03-30/telegram-raises-1-7-billion-in-coin-offering-may-seek-more

Старший аналитик — Никифор Серяков,
Редактор — Людмила Вожакова.