Волшебники из города Web-3 или как TON торгует «анонимностью» и «свободой»

Историческая отсылка. В 2009 году Сатоси Накамото представил программное обеспечение, в котором был организован протокол криптовалюты Bitcoin. В своей статье *The Cryptography Mailing list* от 31 октября он описал Bitcoin – полностью децентрализованную систему электронной наличности, не требующую доверия третьим сторонам.[1] Именно это событие ознаменовало появление феномена Web-3 – сети, отличной от предшествующих эпох Web-1 и Web-2 (их основные черты выходят за рамки данной статьи) и наполненной следующими уникальными особенностями:

- Высококачественными интеллектуальными алгоритмами – поиск ассоциативных правил и их применение к базе данных, содержащей большое количество транзакций.
- Открытостью – отсутствие KYC. В проверке нет необходимости, так как Web-3 – это отказ от двойных расходов при работе с финансовыми посредниками. (Монетный двор, банк).[2]
- Свободой – отмена цензуры. Роль модерации берет на себя сообщество.
- Децентрализацией – данные не хранятся на одном сервере, они распределены между пользователями.
- Вездесущностью – IoT-устройства как главные распространители интернета.

Со времен появления блокчейна Bitcoin, а также в процессе его становления и утверждения, рынок стал насыщенным. Произошел кардинальный перевес в сторону использования технологии блокчейна для распространения оплат цифровыми активами разных видов. Далее процесс и вовсе превратился в инструмент спекуляции ценой. Это и есть основной параметр привлечения аудитории для современных блокчейн проектов. «А будет ли памп[3], и каким образом?» **Именно The Open Network использует этот параметр наиболее зверским и циничным по отношению к людям, и недобросовестным к игрокам рынка методом. Этот тезис мы постараемся достаточно аргументировать в данной статье.**

Что объединяет быстро набирающие оборот блокчейны постбиткойновского появления? Вероятно, то, что сам Сатосси Накамото отметил в своем документе. А именно процесс достижения общего соглашения.

Консенсус – это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети.

Это неотъемлемый элемент работы блокчейна. Скажем так, если вы как будущий разработчик вашего блокчейна не озадачились решением проблемы византийских генералов, то блокчейн вы не создадите. В своем основном документе Сатосси Накамото четко связывает процесс достижения консенсуса (POW) с выгодой узла, поддерживающего работоспособность сети. В разделе «Incentive» он выражает следующую мысль: «Стимул может побудить узлы оставаться честными. Если жадный злоумышленник сможет собрать больше процессорной мощности, чем все честные узлы, ему придется выбирать: использовать ее для обмана людей, воруя обратно свои платежи, или использовать ее для генерации новых монет. Ему будет выгоднее играть по правилам, таким правилам, по которым он получит больше новых монет, чем все остальные вместе взятые, чем подрывать систему и обоснованность своего собственного богатства.»[4]

---

[1]Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf.
[2]Bitcoin P2P e-cash paper. The Mail archive [Сайт] URL: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.
[3]Pump – искусственное повышение цены криптовалют [Электронный ресурс] URL: https://telegra.ph/Slovar-Pure-Net-10-20.
[4]Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf.

Одним из способов управления механизмом был постепенный выпуск Биткойнов, не переполняя рынок всеми 21 миллионами Биткойнов сразу. Для этого код Биткойна был разработан таким образом, чтобы позволить добывать только фиксированное количество Биткойнов каждый год, пока не будет достигнут лимит в 21 миллион Биткойнов.

Новые Биткойны поступают в обращение, когда новый блок расшифровывается и добавляется в блокчейн. Майнинг Биткойна запрограммирован алгоритмом сложности, который помогает поддерживать стабильность всей системы.

Таким образом, достижение консенсуса Биткойна – это качественно просчитанный, выгодный для участников сети процесс работы.

Выгода участников или узлов сети, с момента появления Биткойна – основополагающий факт достижения консенсуса.

Тем не менее у консенсуса Биткойна есть уязвимые места. Общая критика включает в себя то, что он требует огромного количества вычислительной энергии, он плохо масштабируется (подтверждение транзакций занимает около 10-60 минут) и большая часть майнинга сосредоточена в тех регионах мира, где электроэнергия дешевая.

Весь этот пул проблем дал толчок развитию иным консенсусам, которым удавалось решить основные проблемы Биткойна, но не удалось избавиться от параметра «выгоды». Среди всех прочих стоит обратить внимание на консенсус POS (Proof of stake)[5], смысл которого и положен в ядро консенсуса блокчейна The Open Network. Но прежде, чем мы перейдем непосредственно к проекту, тезисно опишем данный консенсус.

В этом типе алгоритма консенсуса вместо того, чтобы инвестировать в дорогостоящее компьютерное оборудование в гонке за добычей блоков, валидатор инвестирует в монеты системы.

Обратите внимание на термин валидатор. Это связано с тем, что при доказательстве доли не происходит создания монет (майнинга). Вместо этого все монеты существуют с первого дня, а валидаторы (их также называют стейкхолдерами, поскольку они владеют долей в системе) оплачиваются строго в виде комиссии за транзакции.

В системе proof of stake ваш шанс быть выбранным для создания следующего блока зависит от доли монет в системе, которой вы владеете (или отложили для ставки).

Таким образом, валидаторы за поддержание работы сети вознаграждаются комиссией за транзакции, проходящие в данной сети.

Этого небольшого объема информации достаточно для понимания того, что проект The open network транслирует недостоверные данные.

Сооснователь Telegram Николай Дуров в 2020 году опубликовал документ[6], в котором излагаются детали консенсуса в блокчейне Telegram Open Network (TON)[7], который получил название Catchain. Алгоритм доказательства доли (PoS) на основе Byzantine Fault Tolerant (BFT) аналогичен механизмам, используемым блокчейнами NEO и Cosmos.

Одним словом, изобретенный Николаем Дуровым велосипед называется «Tendermint» с небольшим усовершенствованием некритичных вопросов в процессе голосования валидаторов по блокам.

Заимствование технологий у других субъектов рынка не являлось бы преступлением со стороны проекта TON, если бы его администрация так активно не «кидалась» на других игроков рынка по причине подобного же воровства. К примеру, авторы проекта TON в своей статье «Comparison of TON, Solana and Ethereum 2.0»[8] от 7 апреля 2022 года называют

---

[5]Proof of stake — криптовалютный механизм консенсуса для обработки транзакций и создания новых блоков в блокчейне [Электронный ресурс] URL: https://telegra.ph/Slovar-Pure-Net-10-20.

[6]Durov N. Catchain Consensus: An Outline [Электронный ресурс] URL: https://test.ton.org/catchain.pdf.

[7]Действительно, правильная расшифровка TON – Telegram Open Network. Высокоинтеллектуальный ход впользу переименования TON в The Open Network ознаменован надеждой на то, что в такого рода случае люди перестанут верить в причастность TON к Telegram.

[8]Comparison of TON, Solana and Ethereum 2.0 [Электронный ресурс] URL: https://ton.org/comparison_of_blockchains.pdf.

блокчейн Solana «альтернативным проектом третьего поколения», а TON (по их представлению) в отличие от Solana, «позволяет мгновенно развернуть смартконтракты любой сложности, обеспечивает более высокий уровень безопасности благодаря механизму консенсуса с более коротким временем завершения транзакций и блоков, и, возможно, самое главное – динамическое шардирование.» Апологетов проекта TON, которые выступают в качестве авторов данной статьи, мало интересовало, что благословляемый ими шардинг также придуман задолго до них.[9] Более того успешно был реализован в других проектах еще до создания TON.[10]

В труде «Comparison of TON, Solana and Ethereum 2.0» приведено множество беспочвенных сравнений, их перечисление не обосновано в рамках данной статьи. Мы намеревались показать читателю тривиальность доказательной базы в технических документах TON.

Так или иначе, мы не претендуем на то, что наши размышления по поводу даты или качества создания тех или иных инноваций в рамках технологии блокчейн истина в последней инстанции. В конце концов, это примерно также, как рассуждать на тему «кто же на самом деле первый изобрел телефон?»

В связи с чем, мы бы хотели обратить внимание читателя на отношение административного звена TON к комьюнити, которое следует за проектом.

Прежде всего, с точки зрения инвестора непонятно, как стартап, который заявлял о максимальной эмиссии в 5,000,000,000 монет во всех СМИ и в том числе в технических документах на момент написания статьи имеет общее предложение в:

- 5,072,191,961 – на официальном сайте[11]
- 5,057,362,773 – CoinGecko[12]
- 5,047,558,528 – CoinMarketCap[13]

Наиболее интересно то, как преподносит информацию CoinMarketCap. Где общее предложение уже превышает максимальное. Стоит отметить, что указанные данные противоречат не только информации ключевых СМИ, но и здравому смыслу.

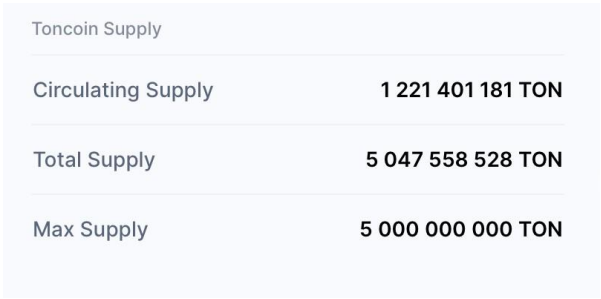

Рис.1 CoinMarketCap: обзор TON

Рис. 2 CoinGecko: обзор TON

[9]Впервые шардинг был использован в ролевой онлайн игре Ultima Online [Сайт] URL: https://uo.com.
[10]Что такое шардинг [Сайт] URL: https://forklog.com/cryptorium/chto-takoe-sharding.
[11]Toncoin: The future of currency [Электронный ресурс] URL: https://ton.org/toncoin.
[12]CoinGecko [Электронный ресурс] URL: https://www.coingecko.com/en/coins/the-open-network.
[13]CoinMarketCap [Электронный ресурс] URL: https://coinmarketcap.com/currencies/toncoin/.

Помимо того, что данные везде отличаются, также ситуация заставляет задуматься: а ограничена ли эмиссия вовсе?

К слову, CoinGecko информацию указал правильно. В его таблице наблюдается знак бесконечности.

Так или иначе, для прояснения вопроса об эмиссии давайте обратимся к первоисточнику, а именно к работе The open network[14] от 26 июля 2021 года. В этой статье автор поясняет: «необходимости в более крупных единицах не будет, поскольку первоначальный запас монет TON будет ограничен пятью миллиардами (5 - 109) монет TOH (т.е. 5 гигатонн).[15]

Таким образом, если верить этому первоисточнику эмиссия монеты ограничена 5,000,000,000, но в проекте TON существует инфляционный механизм. Интересно подчеркнуть, что в основном криптовалютные проекты борются с инфляцией, TON же ее, напротив, вводит, аргументируя это следующими словами:

«Этот запас будет увеличиваться очень медленно, по мере накопления вознаграждений валидаторам за добычу новых блоков мастерчейна и шардчейна. Эти вознаграждения составят примерно 20% (точное число может быть скорректировано в будущем) от ставки валидатора в год, при условии, что валидатор добросовестно выполняет свои обязанности, подписывает все блоки, никогда не выходит из игры и не подписывает недействительные блоки. Таким образом, у валидаторов будет достаточно средств, чтобы инвестировать в лучшее и быстрое оборудование, необходимое для обработки постоянно растущего количества транзакций пользователей.»[16]

Если мы прибавим инфляцию TON к инфляции фиатного доллара, а также учтем понимание о росте цен на «лучшее и быстрое оборудование» (в долларах США и особенно в российских рублях), то получим отрицательную мотивацию валидатора сети TON.

Также в документе прописано, что блокчейн не предусматривает сжигание монет.[17]Тема эмиссии и, как следствие, токеномики проекта TON – очень интересный и обширный вопрос, который целесообразно раскрыть в отдельной статье. На данный момент, мы хотим, чтобы у читателя сложилось четкое понимание отсутствия прозрачности в вопросе токеномики проекта.

Не менее занимательно обратить внимание на феномены «децентрализации» и «анонимности» в понимании проекта TON.

Напомним, в мае 2020 года Павел Дуров сообщил о закрытии проекта Telegram Open Network (TON) из-за судебного конфликта с Комиссией по ценным бумагам и биржам США и запрета на распределение монет.[18]

После этого события, необходимо было принять решение: отказаться от реализации проекта или же передать его в руки посредникам. Руководящие лица решили действовать по второму пути. Так появился The Open Network.

Сегодня мы имеем целый список сервисов сети TON, которые направлены на построение Web-3. С полным списком можно ознакомиться на официальном сайте проекта.[19]

Чтобы разобраться почему блокчейн TON – это не Web-3, стоит обратить внимание на проект Fragment.[20] Мы выбрали его, в связи с тем, что он был выпущен последним и имеет тесную связь с централизованным мессенджером Telegram. На момент написания

---

[14]The open network based on the work of DR. Nikolai Durov [Электронный ресурс] URL: https://ton.org/whitepaper.pdf.
[15]Там же. С. 125.
[16]Там же. С. 126.
[17]Там же. С. 126.
[18]Суд США запретил Telegram распределять Gram среди инвесторов из других стран [Сайт] URL: https://forklog.com/news/sud-ssha-zapretil-telegram-raspredelyat-gram-sredi-investorov-iz-drugih-stran.
[19]Welcome to The Open Network [сайт] URL: https://ton.org/.
[20]Fragment [сайт] URL: https://fragment.com.

данной статьи на площадке Fragment можно только купить, ранее отобранные у пользователей Telegram юзернеймы. Продать свои собственные пока не выйдет, так как данный функционал анонсирован, но еще не реализован.

Итак, как же можно приобрести юзернейм и попробовать заработать на нем? Для этого необходимо привязать свой аккаунт Telegram, то есть номер телефона, который ранее вы оформляли по паспорту страны, гражданином которой вы являетесь. И привязать к платформе Fragment ваш кошелек сети TON. Надеемся читатель уже озадачился вопросом анонимности в вышеописанном процессе.

На примере данного кейса давайте обратим внимание на феномен децентрализации в рамках проекта TON.

Если пользователь приобрел NFT (юзернейм) и, к примеру, его, банковские счета блокируются ввиду подозрения в преступлении в рамках законодательства страны. Будет ли обязан Telegram предоставить данные об этом пользователе? Непременно да.[21] Потому что Telegram – это централизованный мессенджер. А если пользователь является гражданином, к примеру, Белоруссии, где легализованы криптовалюты и блокчейн, то его ожидает конфискация активов.[22]

Также, стоит обратить внимание, что юзернеймы ранее были централизовано отобраны у пользователей во имя мнимой «децентрализации» от Telegram. И теперь продаются от лица Telegram назад комьюнити. Так что же мешает Telegram отобрать у вас вновь юзернейм, в случае, если он станет прибыльным NFT на платформе Fragment, при условии, что юзернеймы не хранятся в блокчейне TON. Они также лежат на серверах Telegram.

И последний аргумент в пользу отсутствия анонимности и децентрализации в проекте TON. Стоит держать в уме, что основным камнем преткновения в проекте TON является сам Telegram. Мессенджер может как развить (то есть привлечь людей), так и погубить его, что и произойдет, по причине отсутствия обещаемых ими возможностей, а именно анонимности и децентрализации. И подтвердить данный тезис можно следующими фактами. Дочерняя компания мессенджера Smart Glocal[23], создавшая Telegram pay и Donate bot требует обязательного ввода банковских реквизитов и прохождения полной процедуры верификации.

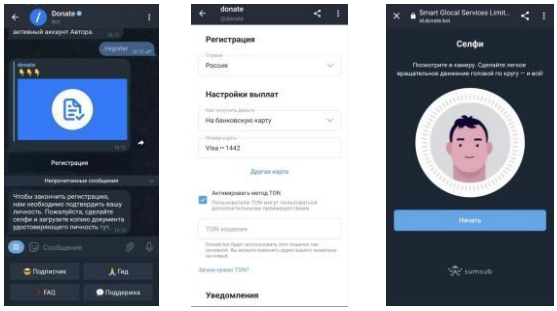

Рис.3. Процесс регистрации

Таким образом, даже если вы не привязывали адрес своего кошелька сети TON к сервисам компании Smart Glocal, но однажды воспользовались «децентрализованной» платформой Fragment, которая «не принадлежит Telegram», мессенджеру будет известен адрес вашего кошелька.

Подводя итог, следует отметить, что TON возможно и мог бы стать подобием децентрализованного проекта, если бы не заручился поддержкой Telegram. Но выбрав этот путь, увы оказался бы на обочине вместе с иными такими же тривиальными блокчейнами

[21]СМИ: Telegram передал пользовательские данные Германии. Что это значит? [сайт] URL: https://kod.ru/telegram-germany-usder-data.
[22]О реестре адресов (идентификаторов) виртуальных кошельков и особенностях оборота криптовалюты. [сайт] URL: https://president.gov.by/ru/documents/ukaz-no-48-ot-14-fevralya-2022-g.
[23]Smart Glocal [сайт] URL: https://smart-glocal.com/.

на Dpos. Конгломерат мессенджера Telegram и блокчейна TON – это ни что иное как деспотическая машина, которая действует не в направлении развития блокчейн технологий и отстаивания анонимности, свободы, децентрализации, а в направлении ущемления всего перечисленного.

Почему-то мир так устроен, что о свободе громче всех кричат надсмотрщики рабов.
Сэмюэл Джонсон

Балачевцева М.А.

Источники

1)Bitcoin P2P e-cash paper. The Mail archive. [Электронный ресурс] URL: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.
2)The open network based on the work of DR. Nikolai Durov [Электронный ресурс] URL: https://ton.org/whitepaper.pdf, 2021.
3)Comparison of TON, Solana and Ethereum 2.0 [Электронный ресурс] URL: https://ton.org/comparison_of_blockchains.pdf, 2022.
4)Durov N. Catchain Consensus: An Outline [Электронный ресурс] URL: https://test.ton.org/catchain.pdf, 2020.
5)S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system [Электронный ресурс] URL: https://bitcoin.org/bitcoin.pdf, 2008.