

Практическое управление BFT

Митя Горошевский

Второе издание

ПРОЕКТ V

«Все правительственные чиновники, — объяснил Мелит, — носят служебный значок, который содержит традиционное количество тессуума, взрывчатого вещества, о котором вы, возможно, слышали. Заряд управляется по радио из будки для граждан. Любой гражданин имеет доступ к стенду с целью выразить свое неодобрение правительству».

Мелит вздохнул. «Это навсегда останется черной меткой на послужном списке бедного Борга».

— Вы позволяете людям выражать свое неодобрение, взрывая чиновников? Гудман в ужасе прохрипел.

— Это единственный способ, который что-то значит, — сказал Мелит. — Сдергивай и балансируй. Как народ в наших руках, так и мы в руках народа».

— И именно поэтому он хотел, чтобы я сменил его срок. Почему мне никто не сказал?»

— Ты не спрашивал, — сказал Мелит с подозрительной улыбкой, — не смотри так испуганно.

Убийство всегда возможно, знаете ли, на любой планете, при любом правительстве. Мы пытаемся сделать это конструктивным. При этой системе люди никогда не теряют связи с правительством, а правительство никогда не пытается взять на себя диктаторские полномочия. И, поскольку все знают, что он может обратиться к будке для граждан, вы будете удивлены, насколько редко она используется. Конечно, всегда есть горячие головы...»

Гудман встал и направился к двери, не глядя на тело Борга.

«Разве вы все еще не хотите стать президентом?» — спросил Мелит.

"Нет!"

«Это так похоже на вас, землян», — грустно заметил Мелит. «Вы хотите ответственности, только если она не сопряжена с риском. Это неправильное отношение к управлению государством».

— Роберт Шекли. Билет в Транай

Абстрактный

Проблема управления децентрализованным сообществом — это проблема консенсуса. Поскольку целью любого управления сообществом является достижение консенсуса в отношении его решений, протокол должен быть предложен с некоторыми правилами консенсуса, с которыми соглашается сообщество, включая правила обновления протокола. Если каждая часть сообщества начнет создавать свои собственные правила для каждого решения, которое они хотят принять, консенсуса с другими сторонами не будет достигнуто во время конфликта.

Ниже я представляю неофициальные спецификации для протокола практического византийского отказоустойчивого управления для Free TON и некоторые обсуждения по этому поводу.

Управление

Давайте подумаем об управлении блокчейном как о социальном блокчейне более высокого уровня. Можно также думать об этом как о виртуальном осколке, блокчейн-рабочей цепи, для управления Free TON. Все принятие решений Участник должен иметь токен такой воркчейн. Поскольку полезность указанного токена будет зависеть от его права голоса, чем больше таких токенов у Участника, тем больше его право голоса.

Чтобы быть блокчейном, управляемым сообществом, решения о его децентрализованном управлении должны широко обсуждаться. Без такого обсуждения они теряют свой статус сообщества. После обсуждения каждый держатель токена должен провести прямое голосование за такое решение. Не должно быть делегирования голосов. Может быть использовано голосование с мягким большинством (SMV) ² для принятия решения, достигнутое в сообществе даже с небольшим оборотом или не достигнутое, если не существует консенсуса.

Существует множество типов предложений, за которые глобальное сообщество должно голосовать. Например, предложения о партнерстве, выделение средств субуправлениям, предложения по прекращению финансирования субуправлений, предложения по изменению самой системы путем корректировки ее параметров или введения новых системных смарт-контрактов. Давайте согласимся, что SMV должен быть основным механизмом принятия решений на уровне консенсуса нашей рабочей цепочки управления, когда все члены сообщества должны голосовать (голосование сообщества). К сожалению, это не всегда так.

Проблема государственного финансирования много раз подробно обсуждалась в пространстве блокчейна, но лучшее решение, которое пока пришло сообществу, — это проблема квадратичного финансирования ³. Те квадратичным финансированием, которое решает что-то неясное. Настоящая проблема заключается не в том, как принять решение о финансировании, а в том, как принять решение о результатах финансирования. У сообщества нет особых проблем с определением областей, где требуется решение, а с тем, как эффективно оценивать эти решения после их представления.

Давайте предположим, что нашему Блокчейну необходимо улучшить протокол, для чего необходимы глубокие знания технических аспектов нашего Блокчейна и набор математических навыков и навыков программирования. Поскольку эти навыки довольно редки, мы должны предположить, что немногие члены нашего сообщества обладают такими навыками. Понятно, что если мы будем использовать SMV для принятия этих решений, в лучшем случае никакие решения никогда не будут приняты, в худшем случае сообщество будет подвержено манипуляциям, искажению фактов или вообще мошенничеству. Поэтому нужен какой-то другой механизм принятия таких решений. К счастью, у Free TON уже есть часть ответа.

¹ Telegram Open Network, д-р Николай Дуров, <https://ton.org/ton.pdf>, стр.5 Как описано в

² Декларации о децентрализации Free TON

³ Квадратичные платежи: введение, Виталик Бутерин, <https://vitalik.ca/general/2019/12/07/quadratic.html>

Меритократическое распределение токенов

Одна из проблем сети дизайна POS, которую⁴ заключается в том, что он требует от валидаторов материальной заинтересованности в том, чтобы они боялись бы потерять. Это предположение обеспечивает основу для теории игр, лежащей в основе Proof of Stake. Участники заинтересованы в обеспечении правильности блокчейна возможностью потерять свои доли, если они этого не сделают.⁵

Обычно блокчейны POS начинаются с продажи своих токенов будущим валидаторам, чтобы создать отправную точку этой игры. В Free TON с самого начала всем было ясно, что мы не собираемся никому продавать токены. Головоломка, которую нам предстояло решить, — как распределить токены таким образом, чтобы это допускала теория игр Proof of Stake.

Free TON нашел решение этой проблемы в модели меритократического распределения токенов (MTD). Он начинается с того, что сообщество предлагает Конкурс, в котором могут участвовать все остальные члены сообщества. Конкурс обсуждается, и если сообщество соглашается с тем, что конечный результат этого Конкурса принесет пользу сообществу и сети в целом, бюджет этого конкурса голосуется через SMV. Теперь любой член сообщества может принять участие, представив свою работу на конкурсы. В конце жюри голосует за конкурсные работы, и победителям распределяются жетоны.

Подуправление

Следуя этой логике, у нас будет структура, в которой голосование сообщества будет выделять средства на все конкурсы. Это оказалось непрактичным. Если всем участникам нужно будет голосовать за каждый Конкурс, количество утвержденных конкурсов будет недостаточным. Чтобы исправить это, нам нужно ввести блокчейны с множественным управлением. Давайте думать об этом как о своего рода шардинге.

Для достижения большей масштабируемости MTD сообщество может формировать группы (также называемые субуправлениями), которые подают заявки на более широкий спектр конкурсов. В этом случае сообщество голосует не за один конкретный конкурс, а за бюджетную основу для серии конкурсов, проводимых Группой.

Для целей настоящего предложения субуправление – это группа участников, которым Сообщество выделяет некоторые государственные средства. Но подобно тому, как шардинг организован сегодня в мультисегментированном блокчейне и по тем же причинам, выбор жюри никогда не должен осуществляться субуправлением. Групповое жюри, подобно валидатору, установленному в блокчейне proof-of-stake, должно быть выбрано из более широкого сообщества, чтобы снизить риск мошенничества. Жюри также должно меняться от конкурса к конкурсу случайным образом, точно так же, как меняется набор валидаторов осколков.

⁴ <https://www.peercoin.net/whitepapers/peercoin-paper.pdf> <https://>

⁵ blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

Вместо государственного финансирования группа может получать частное финансирование. На самом деле, как только все токены сообщества Free TON будут исчерпаны, государственное финансирование должно быть естественным образом заменено частным. Тем не менее, выбор жюри для частного финансирования может остаться прежним. Таким образом, частный конкурс будет оцениваться тем же консенсусом общественного жюри, что повышает безопасность голосования субуправлений, помогая гарантировать инвестору справедливое распределение его средств, если, конечно, такое распределение желательно.

Подуправление представляет собой закрытую группу, в которой изменение статуса члена осуществляется голосованием SMV. У группы могут быть разные настройки для голосования SMV, например пороги супербольшинства для приглашения нового члена или отмены членства могут быть установлены голосованием субуправления.

Конкурсы являются единственным типом предложений, которые могут получать государственное финансирование от сообщества. Если финансирование предоставляется субуправлению, оно должно использоваться только для финансирования конкурсов и ни для какого другого вида распределения финансирования. Злоупотребление системой путем введения типов Конкурсов, для которых невозможна конкуренция (например, замаскированные «выплаты по контракту или заработной плате»), должно быть отклонено Жюри.

В любом случае теперь у нас есть еще один механизм в дополнение к SMV. Мы можем распределять токены на основе заслуг по решению всех участников, то есть сообщества, обеспечить финансирование Конкурса или набора Конкурсов в Группе, а затем Жюри выбрать победителей.

Жюри

С введением групп, которые могут создавать свои собственные соревнования, мы добавили дополнительный вектор атаки на нашу систему управления. Если присяжные выбираются из группы, это явно может привести к коррупции присяжных и групповому сговору. Теперь нам нужно решить, как мы будем выбирать присяжных и, самое главное, как мы будем обеспечивать их честность.

Эта проблема очень похожа на проблему выбора набора валидаторов в сегментированном блокчейне и уже рассматривалась в этом контексте.

Давайте представим конкурс как блок, заявку как транзакцию, а жюри как валидаторов. Совершенно очевидно, что для сохранения безопасности нам нужно, чтобы присяжные были в курсе игры (т.е.

⁶ Главный аргумент против других методов распределения токенов заключается в том, что они не соответствуют основной ценности Free TON — меритократическому распределению токенов. Таким образом, это должно быть вне сферы общественного финансирования. Второй аргумент заключается в том, что любое такое распределение вне метода Конкурса неизбежно приведет к увеличению бюрократии. Бюрократия не только неэффективна, не только разлагает общество, но и противоречит принципу децентрализации.

ставка), они должны чередоваться как можно быстрее между соревнованиями, и, наконец, рыбаки должны быть там, чтобы проверить правильность своего решения и наказать жюри, если они ошибутся.

В блокчейне может быть проверено доказательство правильности блока или, следовательно, вина за его некорректность. Когда мы оцениваем конкурс, результаты в большинстве случаев субъективны. Поэтому вероятно, потребуется несколько более сложный механизм, как описано ниже.

Чтобы добавить некоторую сложность, не все конкурсы имеют одинаковую область достоинств и, следовательно, не могут оцениваться одними и теми же членами жюри, поэтому нам необходимо ввести своего рода сегментирование управления. Подумайте о разных блочных структурах, требующих разных наборов валидаторов, но связанных одними и теми же правилами токена и консенсуса.

Это кажется логичным, если мы выберем жюри из других победителей конкурсов Free TON. Конечно, есть проблема курицы и яйца. Назовем это проблемой с нулевым состоянием. Поскольку у нас уже есть первый состав жюри и первые победители конкурса в сообществе Free TON, его можно использовать для создания такого нулевого состояния. Обобщая, для запуска такой системы управления, вероятно, потребуется провести серию специальных конкурсов с доверенным жюри, чтобы выбрать более квалифицированных членов жюри.

По окончании конкурса каждому победителю предлагается стать членом жюри. Если они соглашаются, часть их конкурсного приза автоматически переходит на счет их жюри в специальном управленческом DePool.

⁸ с прикрепленным тегом, указывающим на их область заслуг, взятую из домена конкурса.

Члены жюри имеют полное право на все вознаграждения, которые будет генерировать Управление DePool, но их доля жюри будет использоваться для гарантии правильности их суждения о конкурсах, которые они оценивают. Члены жюри всегда могут вывести свою долю из пула управления, если нет активных конкурсов, в которых они участвуют.

9

Жюри может увеличить свою ставку, отправив больше своих конкурсных призов в Governance DePool, но они не могут передавать какие-либо другие жетоны для увеличения ставки жюри.

Впоследствии доли в управлении DePool используются для выбора членов жюри для любого конкретного конкурса. Например, проводится конкурс с тегом «JavaScript». Все члены DePool управления чей кол присяжных находится в верхних 90 pct. всех ставок жюри, которые в настоящее время не участвуют ни в каких других решениях конкурса (порог жюри) и к которым прикреплен тег «JavaScript», участвуют в выборах жюри для случайного выбора¹⁰. Количество жюри

⁷ https://computersciencewiki.org/index.php/Merkle_proof <https://>

⁸ docs.ton.dev/86757ecb2/p/45d6eb-depool-specifications Должен быть предусмотрен

⁹ специальный механизм «запроса на отзыв» для членов жюри.

¹⁰ Случайная означает псевдослучайную функцию, доступную в виртуальной машине Free TON от F810 до F81F. Диапазон инструкций.

ставки NJS, выбранные случайным образом членами жюри до тех пор, пока общая доступная ставка жюри не достигнет общего приза.

Тег указывает на домен Конкурса. Он должен быть частью метаданных смарт-контракта конкурса. Конкурс может иметь несколько тегов, если требуется несколько областей знаний. В этом случае будет выбрана только группа жюри, у которой есть все перечисленные теги. Если имеющийся состав Жюри составляет менее 5 человек, конкурс не может быть вынесен на голосование. Поскольку жюри выбирается тегом, манипуляция тегом представляет собой потенциальную угрозу. Поэтому сообщество или суб-группа управления должны обсудить выбор тега для конкретного конкурса. Жюри может отклонить конкурс на основании выбранного тега, т. е. конкретный конкурс не вписывается в область компетенции конкретной группы жюри.

Жюри Голосование

Проходит голосование жюри, в ходе которого каждый член жюри имеет от 1 до 10 баллов, которые он может присвоить каждой работе.

Выбор жюри, а также голосование жюри являются псевдоанонимными с использованием любой подходящей схемы фиксации-раскрытия. В конце голосования жюри отправит открытое голосование в JMVC, которое сравнит хэши всех оценок и комментариев и отправит сообщение корневому жюри. Жюри Рут проверит, что JMVC является оригинальным, и примет голосование. Ключ жюри принимается только после окончания периода голосования.

Каждый член жюри должен предоставить письменное обоснование своей оценки. Обоснование не должно быть ограничено по размеру.

Время голосования жюри VT устанавливается автоматически на основе его призового фонда PP и количества полученных заявок NS \times . Минимальное время голосования жюри - 1 неделя для всех конкурсы и предложения.

Для оценки времени судейского процесса предположим, что нам нужно 33% от общей длительности конкурса CD для случая, если у нас есть только одна заявка, и 10% от общей продолжительности конкурса для каждой «бесконечной» заявки. Итак, мы предлагаем отношение

$$VT'(TS) = CD * F(PP) * TS * (10\% + 23\% * \exp((1-TS)/5))$$

$$VT(TS) = \max . [VT'(TS), 1 \text{ неделя}]$$

с коэффициентом нормализации PP0, установленным на 100 000 тонн $F(PP) = 3 - 7/3 * (6/7)^{(PP/PP0)}$, так что $F(0) = 66\%$, $F(PP0) = 1$, $F(\infty) = 3$.

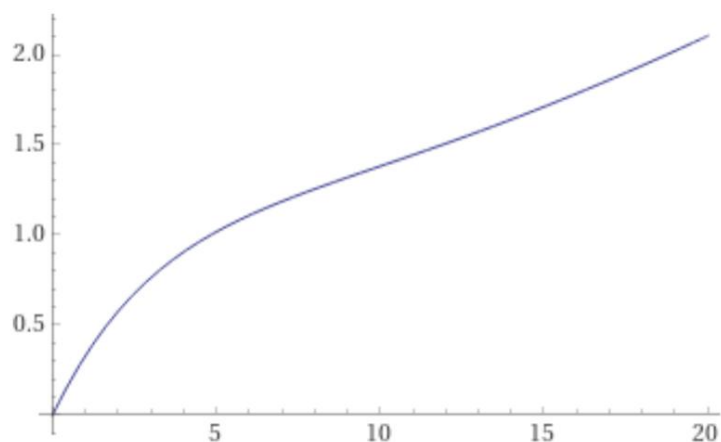


График $VT'(TS)$ с $PP = PP_0$ и $CD = 1$.

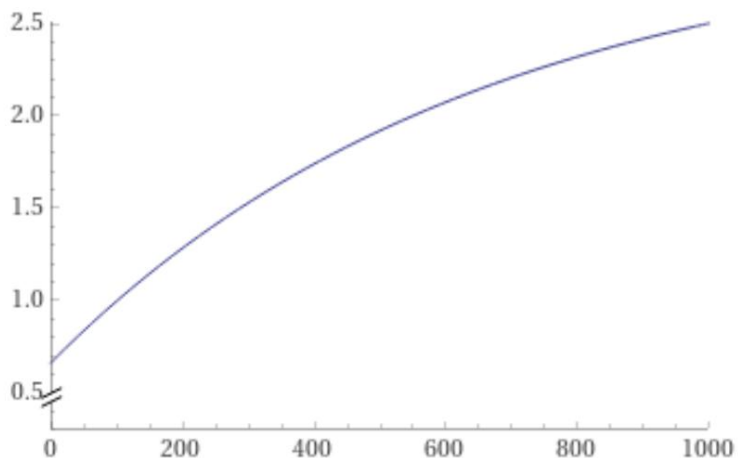


График $F(PP)$ с $PP_0 = 100$.

Ожидается, что жюри будет голосовать монотонно в течение периода голосования. Затем период голосования делится на количество заявок, и ожидается, что члены жюри проголосуют как минимум за одну заявку в каждый из этих периодов. Если члену жюри не хватает 33% своих мест, его вознаграждение уменьшается на 5% каждый раз, пока не достигнет 50% вознаграждения жюри, которое сокращается, если не все работы оцениваются пропорционально.

Жюри может отклонить конкурс, предложенный субуправлением, если общие правила управления, описанные в этом документе, нарушены. Если 66% ставок членов жюри отклонили конкурс, случайным образом из всех членов жюри формируется специальная комиссия. Такой отказ автоматически создаст Предложение SMV для голосования сообщества, чтобы заблокировать государственные средства в этом субуправлении.

После того, как жюри проголосовало за представленные работы, они получают право на часть призового фонда конкурса пропорционально их доле жюри.

Важно отметить, что отклонение заявки или конкурса не повлияет на общий призовой фонд для компенсации жюри. Даже если все заявки или конкурс будут отклонены, жюри должно получить свою часть призового фонда конкурса.

Член Жюри не может воздержаться от голосования по любой причине.

Суд присяжных и административная компенсация

Жюри должно хорошо оплачиваться за свою работу, так как мы должны ожидать качественного решения даже самых сложных конкурсов.

Вознаграждение жюри JS должно быть пропорцией времени голосования VT к общему призовому фонду PP конкурса:

$$JP = (VT/CD) * PP / F(PP)$$

Административная поддержка – это все, что связано с созданием, подготовкой, продвижением и обсуждением конкурса. Административная поддержка составляет до 2% и должна быть указана в конкурсной заявке с кошельками участников сообщества вместе с долей административной поддержки. Всякий раз, когда сообщество принимает Конкурс, оно автоматически принимает оплату административных сборов за него.

Рубка

Прежде чем жюри получит свою компенсацию, устанавливается период порицания, составляющий $\frac{1}{3}$ времени голосования жюри, в течение которого рыбаки имеют возможность просмотреть голосование жюри и их обоснования. Если никаких действий не происходит, ставка Рыбака возвращается Рыбаку за вычетом комиссионных.

Чтобы доказать вину присяжных, рыбакам необходимо использовать метод вины смарт-контракта конкурса, чтобы предъявить вину и прикрепить к ней несколько кристаллов TON. Как только значение общей суммы вины в ТОННАХ достигает общей стоимости присяжных по обвинению, необходимой для проведения расследования, плюс некоторая комиссия (скажем, 5%), вина принимается во внимание. Проходит второй тур выборов жюри. На этот раз новое жюри по обвинению выбирается случайным образом, в нем больше членов жюри, чем в первой попытке. Каждый раз количество членов Blame Jury увеличивается на 33%. Если в базе управления DePool под выбранным тегом больше нет членов жюри, выбор включает похожие теги, где сходство измеряется как близость к другим тегам, связанным с выбранным тегом.

избранный состав жюри. Если весь доступный пул жюри исчерпан, голосование SMV используется в последнем туре для определения результата.

Жюри Blame снова оценивает все конкурсные работы. Если вина подтверждается отличием новой оценки от первоначальной оценки с отклонением, описанным ниже, пересчитывается голосование жюри конкурса.

Мы предлагаем, чтобы каждая заявка имела справедливую оценку и определяла ее следующим образом.

Мы предполагаем, что определенная окрестность значения среднего балла соответствует честному суждению, а выбросы соответствуют неправильному (или злонамеренному) поведению присяжных. Интервал честности мы определяем как $[m - 33\% M, m + 33\% M]$, где m — расчетное среднее значение, а M — максимальный балл (в настоящее время 10). Так, например, если среднее значение равно 4, интервал честности равен $[1;7]$.

Злоумышленный ранг определяется следующим образом: $r' = r^*(1-a) + \text{константа}$, где r' - новый ранг, a - некоторый скорости $a \cdot r_c$, которая должна быть определена в дальнейшем на основе сходимости ранга с реальными сетевыми данными, r_c - текущий ранг обвинения, который задан по соотношению

$r_c = 0$, для v в интервале честности ; r_c

$= |v - m| / M$.

То есть r_c становится равным 1, например, когда $v = 0$ (заявка отклонена) для обвиняющего жюри, в то время как среднее значение установлено на M .

Тогда при текущем ранге r ставка жюри уменьшается на r как коэффициент. Каждое правильное жюри может повысить рейтинг благодаря заданному алгоритму.

Осужденный член жюри лишается своего присяжного вознаграждения, которое вместо него получает присяжное по обвинению. Осужденный член жюри зарезан. Рыбак получает урезанное значение.

«Неявка» — часть, эквивалентная получению $\frac{1}{3}$ текущего рейтинга жюри в качестве ставки жюри, сокращается, если член жюри не голосовал за конкурс, для которого он был выбран.

Приз

Еще одна проблема, связанная с MTD, с которой сталкивается наше сообщество, — это определение призового фонда конкурса. Было много предложений как-то сделать это определение алгоритмическим. Действительно, в то время как сообщество может судить о том, следует или не следует в целом направлять некоторые средства

где-то человеку, не обладающему конкретными экспертами, очень сложно судить, подходит ли тот или иной призовой фонд для той или иной области.

Давайте помнить, что основная цель Конкурса — побудить как можно больше людей внести свой вклад в Free TON в обмен на токены. Поэтому нам важно количество и качество представленных материалов. Проще говоря, мы могли бы создать механизм, с помощью которого призовой фонд будет зависеть от количества качественных заявок. Получить эти параметры достаточно просто. Количество, очевидно, является простым методом подсчета представлений смарт-контракта конкурса, а качество оценивается жюри, как описано выше.

Сообществу или суб-управлению в этом отношении нужно только предоставить приз за победившее решение (1-е место) и продолжительность конкурса. -> PP (для использования в предыдущих формулах) и призы за каждое выигрышное место

Для данного Конкурсного призового фонда PP стоимость баллов жюри рассчитывается как:

$$\text{знак равно } [h \cdot ((h \cdot 2/3/10)^2)] \times 10$$

где NS — любое количество представлений выше порога. Затем окончательный приз за каждую заявку рассчитывается как количество полученных баллов, умноженное на значение балла PV.

Обратите внимание, что ориентировочный бюджет, предоставленный субуправлением, в большинстве случаев не будет распределяться полностью.

К сожалению, вклад в один конкурс экономически не равен вкладу в другой с таким же баллом. Поэтому в будущем может быть разработан механизм, который будет определять приблизительную цифру экономической ценности конкурсного балла в зависимости от предмета конкурса.

В блокчейне у нас есть только один механизм, который определяет экономическую ценность системы. Такая система платит за газ. Поэтому довольно легко рассчитать экономическую ценность Конкурса. Для этого нам нужно взять хэш каждого контракта, который был произведен в этом конкурсе, и просуммировать весь газ всех существующих контрактов с этим хешем, оплаченным до определенной даты.

Конечно, для первых соревнований эту цифру должны угадать организаторы. Но со временем эта цифра будет автоматически корректироваться.

Теперь, зная значение, мы можем предсказать, какое примерное значение призового фонда могут иметь определенные теги.

Как насчет конкурсов, которые не создают смарт-контракты? Например, социальные конкурсы, конкурсы мемов, медиа- и PR-конкурсы и так далее. Я считаю, что все эти конкурсы должны иметь на выходе хотя бы один смарт-контракт. В противном случае они не вносят вклад в блокчейн.

Давайте рассмотрим конкурс на социальный мем. Если использование мема продвигает проект, это должно быть отражено где-то в цепочке. Если мы не можем отследить ончейн-эффект этого конкурса, мы можем не финансироваться из общественных фондов сообщества. Поэтому дизайнеры конкурса должны создать способ измерения результатов конкурса. Обратная ссылка на смарт-контракт, спрятанное «сокровище» внутри какого-то qr-кода кошелька и так далее. На эту тему можно написать книгу «Искусство конкурсного дизайна», но это выходит за рамки данной работы.

Любые выигрыши в конкурсах должны распределяться автоматически после окончания периода порицания.

11

Голосование

Давайте закончим вопросом, с которого, вероятно, следовало бы начать: кто может голосовать?

В современной демократии практически повсеместно используется принцип «один человек — один голос». Его снова и снова критиковали, но для реальной демократии, где жизнь каждого человека зависит от решений правительства его страны, это, вероятно, единственное решение. Главный аргумент по этому поводу в том, что человек не может добровольно (имеется в виду просто по доброй воле) уйти.

Мы можем критиковать эту часть сколько угодно. Реальность такова, что мы еще не живем в обществе, где человек сам выбирает место для жизни.

К счастью, Free TON — это цифровая реальность. Каждый может прийти или выйти в любое время. Никто никому не навязывает участие. Это само по себе является формой свободы, на которую опирается каждое управление блокчейном и консенсус.

Как обсуждалось выше, в Proof-of-Stake это доля собственных токенов блокчейна, которая гарантирует участнику его долю в протоколе. Поэтому очевидно, что участие в управлении таким протоколом должно быть напрямую связано с количеством токенов, которое ставит человек.

Но не создает ли это проблему олигархии? И да и нет.

¹¹ Чтобы быть полезными, решения, победившие в конкурсах, иногда требуют активной разработки и поддержки со стороны их авторов. Сейчас это делают всевозможные схемы вестинга, но вручную контролировать выплаты и необходимый уровень поддержки участников утомительно. По нашему мнению, следует избегать любых схем наделения правами, поскольку они добавляют чрезмерное количество бюрократии. Вместо этого следует рассмотреть децентрализованное решение Git, которое создает конкурсные предложения из проблем и запросов функций. В целом следует избегать крупных соревнований, а вместо этого следует отдавать предпочтение более мелким, целенаправленным соревнованиям.

«Предельная полезность денег — это величина, на которую увеличилась бы полезность индивидуума, если бы ему дали небольшое количество дополнительных денег, на единицу прироста. Дополнительные деньги могут увеличить полезность двумя способами. Во-первых, это прибавка к богатству, которое потребитель может выделить на потребление. Тогда предельная полезность денег определяется дополнительным потреблением, которое они финансируют. Во-вторых, некоторые модели спроса на деньги предполагают, что потребители извлекают полезность непосредственно из наличия денег. Тогда количество имеющихся денег становится аргументом функции полезности, а предельная полезность денег возникает в результате увеличения этого¹² аргумента».

Последнее в Free TON достигается за счет ставок. Первое является прямой функцией МПД. Если распределение токенов не будет меритократическим, оно должно быть чем-то другим — услугами, продуктами или другим эквивалентом ценности — чем-то, чего у нас нет в начале, чем-то, что в любом случае не должно подпадать под действие механизма распределения государственного финансирования.

После создания открытого рынка и свободной торговли токеном начинают появляться такие услуги и продукты, а предельная полезность токена начинает определяться его потребительской способностью. В то же время Дающие, которые усиливают МПД, естественным образом высыхают. Должны ли мы тогда заявить, что МПД закончился, и забыть о нем?

Если это так, то это уже не вопрос олигархии, а необходимость сетевого управления в целом. Затем должны быть созданы механизмы защиты, чтобы мирно распустить все управление и лишить сеть возможности что-либо изменить в режиме «бери или живи». Олигархический контроль над меритократической сетью возможен только в том случае, если меритократия не обеспечивает никакой предельной полезности. Для ясности это означает, что на данном этапе Free TON больше не предоставляет никаких технических или бизнес-инноваций на уровне протокола.

Подобно Биткойну, он просто хорош в том, что он делает.

Если это та сеть, которую мы хотим построить, нам не нужно начинать думать сейчас о том, как мы создадим устойчивое децентрализованное управление, а скорее о том, как мы мирно расформируем ее, не о том, как мы создадим основу для инноваций, а о том, как мы превратим сеть в стабильное состояние, ограничивающее любые дальнейшие изменения. Не то, как мы создаем динамичную платформу, привлекающую больше предпринимателей-разработчиков, а то, как мы приспосабливаемся к спекулянтам и биржам, которые могли бы использовать этот блокчейн для торговли.

Для меня этот сценарий представляет собой отход от всех ценностей Free TON, заявленных в Декларации о децентрализации. В нем указывается принцип мягкого большинства, как алгоритм принятия решения. Сеть, управляемая сообществом, просто подразумевает наличие устойчивого децентрализованного управления, управляемого сообществом. Только благодаря такому управлению мы можем создать децентрализованную платформу для массовых вариантов использования и, следовательно, предельной полезности ее токена.

¹² <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100133871>

Чтобы достичь этого, нам нужно не только подумать, как будут распределяться токены из первоначального предложения, но и как мы будем продолжать поддерживать MTD даже после того, как первоначальные дающие иссякнут. Именно с помощью таких механизмов мы можем гарантировать, что единственной созданной нами олигархией будет Олигархия заслуг. Такая олигархия никогда не станет проблемой до тех пор, пока распределение будет более или менее сбалансировано по многим областям заслуг.

Благодарности

Отдельное спасибо Андрею Ляшину за рецензию и важные дополнения к работе.

об авторе

Я Митя Горошевский, соучредитель и технический директор TON Labs. Я израильтянин, у меня более 25 лет опыта в создании ИТ-проектов, я был соучредителем и руководителем Delta Three Corporation, Internet Telecom, Popular Telephony; имеет патенты в распределенных вычислениях, разработал первую бессерверную концепцию еще в 2004 году, в том числе изобрел слово «бессерверный»; следит за биткойнами с 2009 года, запустил крипто-мессенджер на основе чата на основе Ripple, был архитектором нескольких проектов на блокчейне Ethereum, прежде чем присоединиться к TON Labs. Я являюсь автором первого проекта первоначальной декларации о децентрализации Free TON, я являюсь одним из авторов предложений по улучшению ключей Free TON, таких как лицензия на бесплатное программное обеспечение TON VM Opcode, архитектура распределенного токена, практическая византийская динамическая резка, децентрализованные пулы. (DePools), децентрализованных ботов (DeBots) и децентрализованной службы имен (DeNS), которые являются частью концепции сквозной децентрализации, которую я представил.

TON Labs является основным разработчиком Free TON. Мы реализуем протокол TON на компьютерном языке Rust уже 2,5 года, основываясь исключительно на доступных на тот момент спецификациях блокчейна. В общей сложности TON Labs вложила более 2 млн. строк кода свободного программного обеспечения к свободному Экосистема TON, которая легла в основу стека сетевого программного обеспечения Free TON, мы называем TON OS.

Когда Free TON был запущен, мы участвовали в разработке и реализации ключевых изменений протокола, что является довольно существенным отклонением от первоначального дизайна доктора Николая Дурова. Основными причинами этих изменений, помимо повышения безопасности и производительности протокола, являются аспекты децентрализации управления сетью.