О новом алгоритме достижения консенсуса для стабильных криптовалют

Э. Э. Гасанов[1], М. Б. Суюнбекова[2]

Криптовалюты, цена которых привязана к физическим активам, называют стабильными (стейблкоинами). В данной работе показано, что для стабильных криптовалют использование алгоритма достижения консенсуса типа Proof-Of-Work нецелесообразно, потому что за проделанную трудную работу для достижения консенсуса кто-то должен будет заплатить, и количество денег в системе будет уменьшаться. В данной работе предлагается новый алгоритм достижения консенсуса, основанный на принципе лотереи, который может быть использован для стабильных криптовалют и для цифровых валют центральных банков.

Ключевые слова: Криптовалюты, цифровые валюты центральных банков, алгоритмы достижения консенсуса.

Традиционно финансовые транзакции, т.е. передача денежных средств от одного лица другому, осуществляется через посредничество банков. Криптовалюта была введена для того, чтобы отказаться от услуг банков для осуществления финансовых транзакций. Фактически криптовалюта представляет собой распределенную базу данных транзакций, когда каждый пользователь хранит у себя весь список транзакций. Количество денег на счету пользователя может быть проверено с использованием данного списка. Чтобы не было разногласий важно, чтобы у каждого пользователя был один и тот же список транзакций. Этот список представляет собой цепь блоков — *блокчейн*, где каждый блок содержит некоторое множество транзакций. Каждый пользователь может сформировать свой блок транзакций, но добавление блоков в цепь осуществляется через некоторые фиксированные интервалы, и в каждый момент в цепь может быть добавлен только один блок. Алгоритм, который позволяет выбрать из всего множества сформированных блоков один блок, который будет добавлен в цепь, называется *алгоритмом достижения консенсуса.*

[1] *Гасанов Эльяр Эльдарович* — профессор каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: el_gasanov@mail.ru.

Gasanov Elyar Eldarovich — professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intelligent Systems.

[2] *Суюнбекова Манзурахон Батыржановна* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: artem.propazhin@mail.ru.

Suyunbekova Manzurakhon Batyrzhanovna — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intelligent Systems.

Первая в мире криптовалюта появилась в 2008 году и называется биткоином [1]. Алгоритм достижения консенсуса в биткоине состоит в следующем. Новый блок, добавляемый в блокчейн биткоина, содержит хеш предыдущего блока. В новом, ещё неподтверждённом блоке есть специальная область, которую можно менять — «nonce». По данным добавляемого блока вычисляется хеш. Если хеш не превышает установленного заранее фиксированного порога, то хеш считается правильным, и новый блок может быть добавлен в блокчейн. Иначе nonce меняется и пересчитывается хеш. Пользователи, которые пытаются добавить свой блок в блокчейн, подбирая nonce, называются *майнерами*. Майнер, который первым получил хеш, не превышающий установленный порог, считается выигравшим, и его блок добавляется в блокчейн. Порог подбирается таким образом, чтобы правильный хеш нельзя было получить быстрее определенного времени, задающего интервалы между добавляемыми блоками. За добавленный блок выигравший получает вознаграждение в виде биткоинов. Остальные майнеры начинают игру заново, пытаясь добавить свой блок в новый блокчейн. Такой процесс вычисления хеша и добавления новых блоков в блокчейн называется *майнингом*, а алгоритм достижения консенсуса, при котором выигравшим считается тот, кто первый посчитал правильный хеш, называется Proof-Of-Work.

Как правило выигрывает тот, у кого имеются серьезные вычислительные мощности для быстрого вычисления хеша. При майнинге тратится огромное количество энергии, причем все вычисления тратятся впустую в том плане, что ничего по факту не производится, но трудоёмкость подсчёта хэша в биткоинах гарантирует сохранение целостности цепочки, невозможность её подделки.

Главным недостатком биткоина является то, что эта криптовалюта ничем не обеспечена, и формирование ее цены носит спекулятивный характер. Поэтому возникает необходимость в криптовалютах, цена которых привязана к физическими активами (фиатные валюты, драгоценные камни, природные ресурсы, ценные бумаги и пр.). Такие криптовалюты называют *стейблкоинами* («stable» —- «стабильный») [2]. В числе стабильных криптовалют значатся Tether, Dai, а также цифровые валюты центральных банков — *ЦВЦБ*. Так, в октябре 2020 года Банк России представил доклад для общественных консультаций по созданию цифрового рубля [1], а в апреле 2021, после его широкого обсуждения, опубликовал концепцию цифрового рубля [2].

[1]Сайт Центрального Банка РФ. URL: `https://www.cbr.ru/analytics/d_ok/dig_ruble/`

[2]Сайт Центрального Банка РФ. URL: `https://www.cbr.ru/Content/Document/File/120075/concept_08042021.pdf`

В правильных стабильных криптовалютах нельзя использовать алгоритм Proof-Of-Work в качестве алгоритма достижения консенсуса, поскольку за потраченную на вычисления энергию надо платить, что приведет к вымыванию физических активов и снижению ценности криптовалюты. Этим объясняется актуальность разработки новых алгоритмов достижения консенсуса. Обзор по существующим алгоритмам достижения консенсуса можно найти в [3], [4], [5].

Аналогично созданию ЦВЦБ для регуляции денежных средств страны центральным банком в условиях цифрового мира, можно рассмотреть создание криптовалюты, а именно стейблкоина, для конкретной отрасли. Преимуществами создания и использования отраслевой криптовалюты можно считать рационализацию криптовалюты; мониторинг товара; свободную реализацию продажи продуктов компаний-участниц отрасли и выгоду от всех продаваемых товаров. Как следствие из вышеперечисленного можно получить оживление рынка отрасли, рост спроса на товар, а также свободное обращение капитала и поток инвестиций, что позволит компаниям-участницам отказаться от высокопроцентных кредитов у банков и других внешних вкладчиков.

В ходе рассмотрения отраслевой криптовалюты, подразумевается, что любой актив отрасли (каждая единица товара, фиатные деньги, ценные бумаги, здания, оборудование и т.д.) будет учитываться при эмиссии валюты. Каждая транзакция фиксирует куплю-продажу продукта отрасли, передачу средств. Таким образом с помощью блокчейна можно отследить историю каждого единичного товара, и через цепочку данных можно осуществлять мониторинг.

У криптовалют есть огромный потенциал, даже если учесть лишь блокчейн – децентрализованную систему хранения данных. Поэтому, добавив к уже существующей в криптовалютах высокой степени защиты и анонимности, её подкреплённость ощутимым, понятным для каждого пользователя сертифицированным товаром, а также исключив энергозатратный пересчёт nonce, можно было бы вывести термин «криптовалюта» на новый уровень.

В данной работе предлагается новый алгоритм достижения консенсуса, который не требует существенных затрат энергии, и он основывается на принципе лотереи.

Предлагаемый подход состоит из четырех стадий.

Первая стадия называется входом в игру. Игроки входят в игру по очереди. Первый входящий в игру объявляет свой «вклад» — некоторое натуральное число c_1. В результате он получает свой интервал $[l_1, r_1)$, где $l_1 = 0$, $r_1 = l_1 + c_1$. Предположим, что уже m игроков вступили в игру, m-й игрок получил интервал $[l_m, r_m)$. Вступая в игру, $(m+1)$-й игрок объявляет свой вклад c_{m+1} и получает свой интервал $[l_{m+1}, r_{m+1})$,

где $l_{m+1} = r_m$, $r_{m+1} = l_{m+1} + c_{m+1}$. Пусть в игру вступило n игроков и $L = \sum_{i=1}^{n} c_i$ — суммарный вклад всех игроков.

На второй стадии каждый из игроков вырабатывает некоторое достаточно большое случайное число a_i, $i = 1, \ldots, n$.

На третьей стадии игроки обмениваются случайными числами, и в результате обмена каждый игрок вычисляет полную сумму случайных чисел $S = \sum_{i=1}^{n} a_i$.

На четвертой стадии каждый игрок вычисляет число $R = S \mod L$. Выигравшим признается тот игрок i, для которого выполняется $R \in [l_i, r_i)$. Выигравший игрок забирает всю сумму S за вычетом заранее обговоренной комиссии, а также добавляет свой блок в блокчейн, высчитав хеш. Отметим, что в данном подходе необходимость в nonce пропадает.

Наиболее сложным является третья стадия, в которой должны обмениваться информацией игроки, не доверяющие друг другу.

Рассмотрим протокол, с помощью которого два игрока, не доверяющие друг другу, могут обменяться информацией.

Рассмотрим следующую игру двух игроков A и B. Игрок A вырабатывает случайное натуральное число a, а игрок B — случайное натуральное число b. Если $a+b$ нечётное число, то побеждает игрок A. Иначе победителем является игрок B.

Возникает вопрос: как игроку A передать своё число a игроку B, а тому в свою очередь предать своё число b игроку A так, чтобы никто из них не смог смошенничать. Например, если игрок A первым отправит своё число a, то игрок B сможет подобрать число b так, чтобы $a + b$ был чётным, и отправит A не случайное число, а подобранное.

Эту задачу можно решить с помощью протокола, подобного протоколу «Подбрасывание монеты по телефону» Мануэля Блума [6]. Осуществляется обмен с помощью однонаправленной функции $f(x)$ следующим образом. Игрок A передаёт игроку B число $f(a)$. Игрок B передаёт игроку A число $f(b)$. Игрок A передаёт игроку B число a. Игрок B передаёт игроку A число b. Игрок A вычисляет число $f(b)$ и убеждается, что оно совпадает с полученным числом $f(b)$, а игрок B вычисляет число $f(a)$ и убеждается, что оно совпадает с полученным числом $f(a)$. Игроки суммируют числа a и b, и у обоих получается число $a + b$.

Описанный выше протокол обмена между игроками A и B будем обозначать через O и представлять как $O_{A,B}(a, b)$.

Теперь рассмотрим протокол обмена данными между n игроками, не доверяющими друг другу.

Пусть имеется n игроков A_1, A_2, ... , A_n, которые вырабатывают случайные числа a_1, a_2, ... , a_n соответственно. Протокол обмена этими числами будем обозначать через P. В результате этого протокола у каждого игрока формируется число $a_1 + ... + a_n$, данный протокол будем представ-

лять как $P(a_1, ..., a_n)$. В качестве базовой операции используем протокол O. Описывать протокол будем индуктивно.

Обозначим: $O_{i,j}(x, y) := O_{A_i,A_j}(x, y)$.

Базис индукции. Протокол P для двух игроков с числами a_1 и a_2 — это $O_{1,2}(a_1, a_2)$. Протокол P для трёх игроков с числами a_1, a_2 и a_3 — это последовательность протоколов $O_{1,2}(a_1, a_2)$, $O_{1,3}(a_1 + a_2, a_3)$, $O_{2,3}(a_1 + a_2, a_3)$. При этом игрок A_3 добавляет число $a_1 + a_2$ в свою сумму только один раз, ведь протокол $O_{2,3}(a_1 + a_2, a_3)$ нужен по сути только игроку A_2 для получения числа a_3.

Индуктивный переход. Нам дано n натуральных чисел $a_1, \ldots, a_n$, и пусть по предположению индукции мы умеем применять протокол P к числу игроков, меньшему чем n.

Применим протокол P дважды, разделив игроков на два подмножества: $P(a_1, ..., a_k)$ и $P(a_{k+1}, ..., a_n)$, где $k =]\frac{n}{2}[$. В результате первые k игроков получат число $s_1 = a_1 + ... + a_k$, а следующие $n - k$ игроков получат число $s_2 = a_{k+1} + ... + a_n$. Теперь проведём обмен полученными числами между подмножествами так, чтобы первые k игроков получили число s_2, а следующие $n - k$ игроков число s_1 и данную операцию назовём *слиянием протоколов*.

Рассмотрим два случая.

1) $n = 2k$. Выполняем протоколы $O_{1,k+1}(s_1, s_2)$, ... , $O_{k,n}(s_1, s_2)$. Таким образом i–тый игрок обменивается числом с $(i + k)$–ым, $i = \overline{1, k}$. В результате все игроки получат число $s_1 + s_2$.

2) $n = 2k - 1$. Выполняем протоколы $O_{1,k+1}(s_1, s_2)$, ... , $O_{k-1,n}(s_1, s_2)$. Затем выполняем протокол $O_{k,k+1}(s_1, s_2)$, причём в последнем протоколе игрок A_{k+1} обменивается числом s_2, а не числом $s_1 + s_2$ и число s_1, которое он получил от двух игроков, он учитывает в своей сумме один раз. Таким образом при слиянии $P(a_1, ..., a_k)$ и $P(a_{k+1}, ..., a_n)$ игрок A_{k+1}, игрок с наименьшим индексом из второго подмножества игроков, участвует в обмене два раза, а все остальные по одному. В результате все игроки получают у себя число $s_1 + s_2$.

Обозначим через $Q(n, i)$ количество протоколов O, в которых участвует i-й игрок, при выполнении протокола P для n игроков.

Теорема 1. *Предложенный протокол P решает задачу достижения консенсуса, и для любого натурального n, $n > 1$, и для любого номера $i \in \{1, \ldots, n\}$ выполнены неравенства* $[\log_2 n] \leq Q(n, i) \leq]\log_2 n[+ 1$.

Таким образом каждый игрок во время игры совершает логарифмическое от общего количества игроков число элементарных обменов.

В дальнейшем планируется исследование устойчивости предложенного алгоритма к различным атакам.

Список литературы

[1] Nakamoto S., “Bitcoin: A Peer–to–Peer Electronic Cash System”, *Self-published Paper*, 2008, 9 pp.

[2] Еременко Ю.М., Козлова Н.Ш., “Стейблкоин как стабильная криптовалюта”, *Студент и наука*, **4(11)** (2019), 17–21

[3] Huanliang Xiong, Muxi Chen, Canghai Wu, Yingding Zhao, Wenlong Yi, “Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms”, *Future Internet*, **14**:2 (2022), 47, https://www.mdpi.com/1999-5903/14/2/47.

[4] Тороев А.С., Сизоненко А.Б., “Анализ эффективности алгоритмов достижения консенсуса в распределенных системах обработки данных на основе технологии блокчейн”, *Вестник компьютерных и информационных технологий*, **17**:11(197) (2020), 13–22.

[5] Бахвалова Е.А., Судаков В.А., “Исследование алгоритмов консенсуса для блокчейн-платформ”, *Препринты ИПМ им.М.В.Келдыша*, **26** (2021), 1–16.

[6] Blum M., “Coin Flipping by Telephone: A Protocol for Solving Impossible Problems”, *ACM SIGACT News*, **15**:1 (1981), 23–27.

On a new algorithm for reaching consensus for stablecoins
Gasanov E.E., Suyunbekova M.B.

Cryptocurrencies, the price of which is tied to physical assets, are called stablecoins. This paper shows that for stablecoins, the use of a Proof-Of-Work consensus-building algorithm is impractical, because someone will have to pay for the hard work done to reach a consensus, and the amount of money in the system will decrease. This paper proposes a new consensus-building algorithm based on the lottery principle that can be used for stablecoins and for digital currencies of central banks.

Keywords: Cryptocurrencies, digital currencies of central banks, consensus building algorithms.

References

[1] Nakamoto S., “Bitcoin: A Peer–to–Peer Electronic Cash System”, *Self-published Paper*, 2008, 9 pp.

[2] Eremenko Yu.M., Kozlova N.Sh., "Stablecoin as a stable cryptocurrency", *Student and Science*, **4(11)** (2019), 17–21 (In Russian)

[3] Huanliang Xiong, Muxi Chen, Canghai Wu, Yingding Zhao, Wenlong Yi, "Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms", *Future Internet*, **14**:2 (2022), 47, https://www.mdpi.com/1999-5903/14/2/47.

[4] Toroev A.S., Sizonenko A.B., "Analysis of The Effectiveness of Consensus-Building Algorithms in Distributed Data Processing Systems Based on Blockchain Technology", *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, **17**:11(197) (2020), 13–22 (In Russian).

[5] Bakhvalova E.A., Sudakov V.A., "Research of consensus algorithms for blockchain platforms", *Keldysh Institute Preprints*, **26** (2021), 1–16 (In Russian).

[6] Blum M., "Coin Flipping by Telephone: A Protocol for Solving Impossible Problems", *ACM SIGACT News*, **15**:1 (1981), 23–27.