УДК 681.3.06

Н.Е. ИВАНОВ, Р.В. ОЛЕЙНИКОВ, д-р техн. наук

ОЦЕНКА ПРОПУСКНОЙ СПОСОБНОСТИ ПЛАТФОРМЫ ETHEREUM НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СМАРТ-КОНТРАКТА

Введение

Децентрализованная платежная система (криптовалюта) Bitcoin стала первой платформой для учета виртуального актива, в которой клиенты и участники сети, не доверяя друг другу, способны приходить к единому консенсусу (согласованному состоянию балансов пользователей системы, истории транзакций и пр.). Для решения вопроса впервые была предложена технология блокчейн в качестве базы данных для узлов сети [1]. Успешное функционирование и возрастающая популярность платежной системы Bitcoin (капитализация Bitcoin составляет более 316 млрд долларов на 18.12.2017 [2]) увеличили интерес к используемым в ней решениям [1].

Новая технология блокчейн привнесла в распределенные системы доверие к данным, циркулирующим между узлами таких систем, и вызвала заметный интерес в финансовом секторе и других областях, непосредственно связанных с учетной деятельностью. Появление первой платформы, позволяющей разрабатывать полноценные программируемые смарт-контракты, Ethereum, открывает широкий потенциал в реальном создании и использовании децентрализованных приложений [3, 4].

Смарт-контракт – компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн. На платформе Ethereum смарт-контракт представляется в виде программного кода, корректное выполнение которого обеспечивается согласованием результатов его работы между узлами платформы [4].

Самым популярным смарт-контрактом в сети Ethereum является контракт начального размещения токенов (Initial Coin Offering, далее – ICO). Он служит для сбора средств в поддержку проектов финансирования стартапов и для эмиссии виртуальных активов – токенов [5]. Для понимания преимуществ, которые несет этот контракт, стоит обратить внимание на его типичные, но не обязательные, свойства и логику работы.

1) Пользователь отправляет на адрес контракта определенную сумму в виде криптовалюты Ethereum. В качестве вознаграждения ему отправляются виртуальные активы – токены. Таким образом обеспечивается распродажа токенов.

2) При сборе определенной суммы распродажа токенов прекращается.

3) При достижении определенной даты распродажа токенов прекращается.

4) Когда распродажа прекращается, если учредители не получили минимально необходимую сумму, то распродажа считается неудавшейся, и все пользователи, вложившие деньги, могут вернуть средства.

Компании, проводящие ICO для обеспечения интереса пользователей к инвестициям, могут наделить токены такими свойствами.

1) За токены можно приобрести продукт или услугу компании [5].

2) Владельцы токенов могут принимать участие в голосованиях внутри компании (digixDAO) [6].

3) Токены могут быть выведены на биржу (если соответствуют стандарту ERC20) и быть объектом торговли [7].

4) Владельцам токенов могут выплачивать дивиденды [8].

Для того чтобы быть более уверенными в успешном проведении ICO, компании прибегают к рекламным кампаниям. Иногда это приводит к чрезмерному количеству желающих участвовать в распродаже токенов. Количество транзакций, генерируемых ими, приводит к тому, что сети Ethereum приходится отклонять часть поступающих заявок [9]. В таком случае часть участников сети должны отправить свою транзакцию повторно и вновь ожидать подтверждения.

Анализ литературных данных и постановка проблемы

Главным недостатком блокчейн технологий является сложность их масштабирования и, соответственно, сравнительно низкая пропускная способность. Блокчейн технологии имеют ограничения по скорости обработки одной транзакции, а обрабатывающие узлы ограничены размером буфера транзакций. Оценка пропускной способности и вероятности отказа в обслуживании транзакций в платформе Ethereum позволит понять целесообразность использования смарт-контрактов. Теория систем массового обслуживания (СМО) предоставляет возможность произвести такие оценки и предоставить в итоге информацию о среднем времени ожидания операции в системе, вероятности отказа в обслуживании и зависимости этих величин от параметров системы: размера буфера ожидания, среднего времени обработки одной заявки [10].

Цель и задачи исследования

Целью работы является разработка математической модели для оценки пропускной способности платформы Ethereum, что позволит оценить, с каким уровнем нагрузки способна справиться платформа. Для достижения данной цели необходимо:

1) провести анализ условий, при которых функционирует глобальная платформа Ethereum;
2) определить параметры математической модели;
3) разработать математическую модель на основе СМО.

Анализ функционирования платформы ETHEREUM

На платформе Ethereum циркулируют множество транзакций, связанных с смарт-контрактами или же обычными криптовалютными переводами между пользователями. При разработке математической модели наличие этих транзакций не учитывается, поскольку они создают неравномерную и, в то же время, сравнительно незначительную нагрузку на сеть. Наибольшую же нагрузку сеть Ethereum испытывает во время проведения ICO распродаж. Транзакций, вызывающих код ICO контракта, в эти периоды подавляющее большинство, поскольку платформа Ethereum в первую очередь обрабатывает транзакции с более высокой комиссией, а остальные ставит в очередь или отбрасывает [4]. Для получения токенов раньше других участников распродажи, пользователи значительно увеличивают комиссию за транзакции, что приводит к тому, что некоторый промежуток времени большая часть подтверждаемых транзакций связана с эмиссией токенов [5]. Поэтому данное упрощение математической модели наиболее соответствует реальным процессам.

Разработка математической модели

Для согласования терминологий теории СМО и блокчейн, под транзакциями и заявками на обслуживания будем иметь в виду одно и то же.

Разработка математической модели СМО на основе платформы Ethereum включает в себя несколько допущений и упрощений.

1) Считается, что все транзакции, циркулирующие в системе, направлены на эмиссию новых токенов, ICO.

2) Принимается, что существует только один канал обслуживания. Несмотря на то, что сеть Ethereum – распределенная система, в итоговую базу данных блокчейн будет записан только один блок, от одного узла [4].

3) В математической модели не учитывается возникновение ветвлений (forks), так как различия будут в древовидной структуре блоков, а не в последовательностях транзакций.

4) Время генерации нового блока подчиняется экспоненциальному закону (коэффициент ковариации для этого закона – константа, равная единице) [4].

5) В блокчейн-платформе Ethereum нет максимально возможного размера блока и ограничения по количеству и размеру транзакции, однако существует ограничение на максималь-

ное количество газа (gas, комиссии за транзакцию), используемого в блоке. Эта величина может быть уменьшена или увеличена в следующем блоке на 20 процентов [4]. Это также позволяет в теории неограниченно увеличивать размер блока. При разработке математической модели принято, что максимальное количество транзакций в блоке будет равно 77. Это число взято из среднего количества транзакций в блоке реальной сети Ethereum [11], полученного по состоянию на ноябрь 2017 г.

6) Появление новых транзакций (другими словами, заявок) подчиняется простейшему закону распределения, а именно пуассоновскому.

В разрабатываемой математической модели считается, что поток входных заявок является простейшим, поскольку он соответствует свойствам стационарности, ординарности и отсутствию последействия в рассматриваемых условиях. Хотя ICO имеет различное количество заявок на протяжении всей распродажи на относительно небольших промежутках времени (1 – 10 минут), возникновение новой заявки будет стационарным. Каждая транзакция обрабатывается последовательно и имеет строгий порядок записи в децентрализованный блокчейн; благодаря этому обеспечивается ординарность потока заявок. При отказе сети Ethereum в обработке заявки пользователь повторно отправит транзакцию, однако в рассматриваемых нами коротких промежутках времени такого не произойдет, поскольку факт сбоя будет обнаружен пользователем не сразу, что позволяет представить повторный запрос как новую заявку, что обеспечивает свойство отсутствия последействия.

Рассмотрим формулу для подсчета среднего времени ожидания заявки [10]:

$$\omega = \frac{\lambda \times b^2 \times \left(1 + v^2\right)}{2 \times \left(1 - \lambda \times b\right)} \tag{1}$$

где λ – интенсивность потока заявок, b – среднее время обработки одной заявки, v – коэффициент вариации закона распределения среднего времени обработки одной заявки [10].

Знаменатель выражения показывает, что при $\lambda \times b$ больше или равным единице, среднее время ожидания выполнения одной заявки стремится к бесконечности. Действительно, если интенсивность слишком высока, то на бесконечном интервале заявка никогда не будет обработана [10].

Подсчитаны значения, соответствующие нашей блокчейн системе. Среднее время обработки одной заявки

$$b = \frac{\textit{среднее время нахождения блока}}{\textit{количество транзакций в блоке}} = \frac{15}{77} \approx 0{,}195\,\textit{сек}. \tag{2}$$

Среднее время нахождения блока и среднее количество транзакций блоке получено из среднестатистических характеристик реально работающей сети Ethereum на ноябрь 2017 года [11]. Коэффициент вариации для экспоненциального закона, определяющего время обработки одной заявки, равен единице. Таким образом, получим формулу среднего времени ожидания обработки одной заявки, зависящиго от интенсивности входного потока:

$$\omega = \frac{\lambda \times 0.038}{1 - \lambda \times 0.195} \tag{3}$$

Приведен график зависимости величины среднего времени ожидания одной заявки от интенсивности входных заявок (см.рис. 1).

Из графика следует, что при приближении интенсивности входного потока заявок к значению обратной величины среднего времени обработки b, среднее время ожидания заявки стремится к бесконечности. Однако для системы с наличием ограниченной очереди заявок такое значение интенсивности приведет к резкому увеличению вероятности в отказе обслуживания заявки.

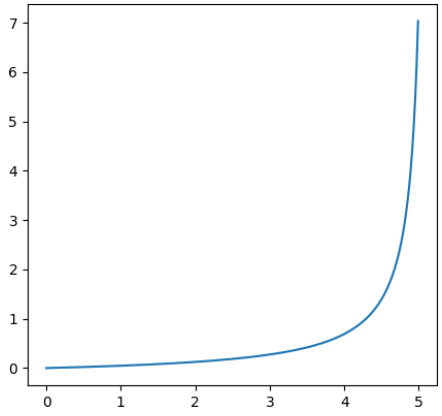

Рис. 1. График зависимости среднего времени ожидания обработки одной заявки к интенсивности входного потока заявок

Приведена формула вероятности того, что система с количеством каналов n, длиной очереди m будет заполнена на s заявок. Эта вероятность равна вероятности отказа заявке в обслуживании при наличии ограниченной очереди, когда s равно m [10]:

$$p_{n+s} = \frac{\frac{(\lambda \times b)^n}{n!} \times \left(\frac{\lambda \times b}{n}\right)^s}{\sum_{k=0}^{n} \frac{(\lambda \times b)^k}{k!} + \frac{(\lambda \times b)^n}{n!} \times \sum_{s=1}^{m} \left(\frac{\lambda \times b}{n}\right)^s} \quad (4)$$

Эта формула представляет собой обобщенный вид [10]. Для того чтобы получить вероятность отказа в обслуживании, необходимо подсчитать значения этой вероятности с предположением, что буфере размера m уже находится m заявок. Подставим значения для нашего случая: n=1, s=m, b=0.195:

$$p_{m+1} = \frac{(\lambda \times 0.195)^{m+1}}{1 + \lambda \times 0.195 + \sum_{s=1}^{m} (\lambda \times 0.195)^{s+1}} \quad (5)$$

Приведен график зависимости интенсивности поступающих заявок к вероятности отказа заявке в обслуживании при размере буфера, равном m=100 (рис. 2). Размер буфера выбран таким, поскольку, хотя размер буфера значительно больше у реальных узлов, его увеличение не повлияет на график существенным образом, однако осложнит вычисления, что будет показано в дальнейшем анализе.

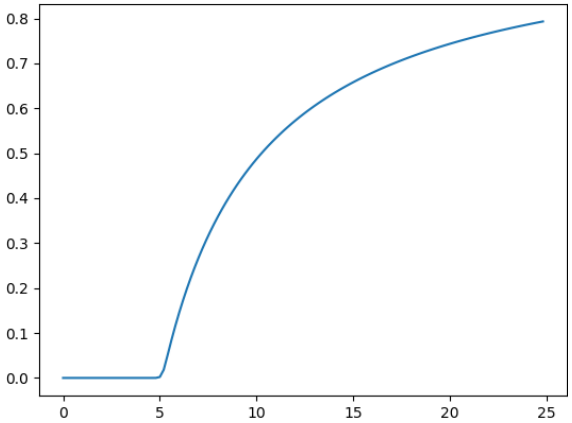

Рис. 2. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок

Обсуждение результатов исследования модели

Из приведенных формул и графиков можно выделить параметры, которые влияют на такие характеристики системы, как среднее время ожидания заявки на обработку и вероятность отказа в обслуживании заявки:

1) среднее время обработки одной заявки – *b*;
2) размер буфера заявок – *m*;
3) количество каналов обработки заявок – *n*;
4) интенсивность входного потока заявок – λ.

При этом интенсивность входного потока λ не является той величиной, которая может быть урегулирована разработчиками системы и является параметром среды, в котором функционирует система. Тогда улучшение характеристик системы может быть достигнуто тремя способами:

1) увеличением буфера заявок;
2) уменьшением среднего времени обработки одной заявки;
3) увеличением количества каналов параллельной обработки заявок.

Увеличение буфера заявок может быть достигнуто увеличением оперативной памяти вычислительных узлов сети. Уменьшение среднего времени обработки одной заявки и увеличение числа каналов требуют переработки самого протокола консенсуса блокчейн систем [3]. Проанализируем как изменение данных параметров влияет на вероятность отказа заявки в обслуживании.

Ниже приведена зависимость этой величины от размера буфера, равного 1, 3, 10, 100 и 1000 заявок с фиксированным значением среднего времени обработки одной заявки b=0.195 (рис. 3).

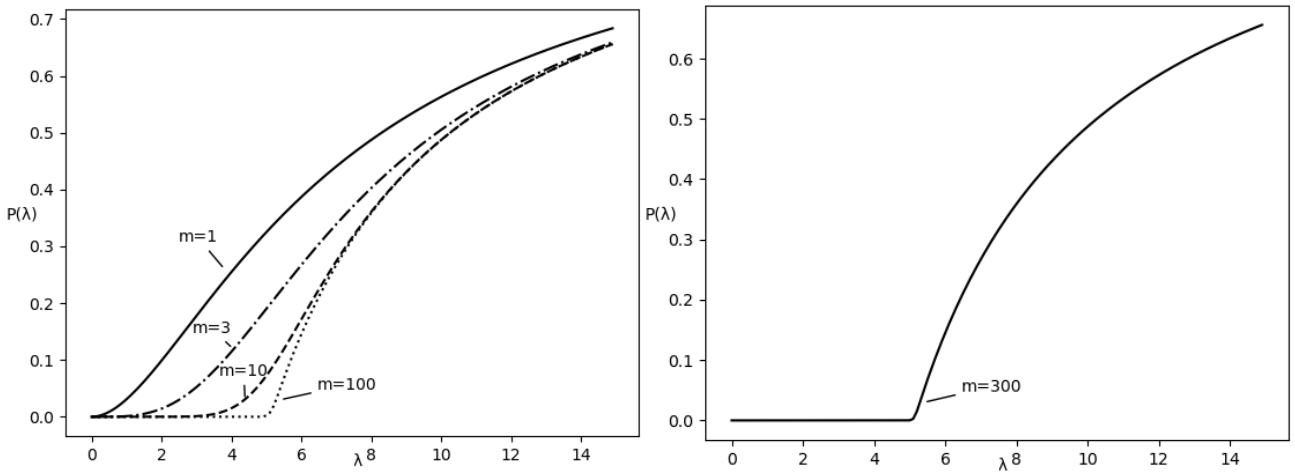

Рис. 3. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок при *m*=1,3,10,100,300

Из полученных графиков следует, что увеличение размера буфера ожидания заявок имеет свой предел по улучшению эффективности работы системы. На графиках с размером буфера *m*=1, 3, 10 заметен сдвиг и уменьшение сглаженности перехода к моменту резкого увеличения вероятности отказа заявки в обслуживании при больших значениях интенсивности входного потока заявок. Однако анализ графиков с размером буфера *m*=100, 300 свидетельствует, что они существенно не отличаются. Таким образом, размер буфера после определенного значения не повышает эффективность системы.

Стоит дополнительно отметить, что на практике больший размер буфера позволит системе преодолеть моменты неожиданного и резкого увеличения количества транзакций на некотором локальном промежутке времени. Время ожидания обработки транзакций будет

значительно больше, однако это позволит сохранить большее количество транзакций пользователей в системе без необходимости в их повторной отправке, что повышает надежность используемой системы.

Приведены графики вероятности отказа заявки в обслуживании с фиксированным размером буфера заявок m=100 и средним временем обработки одной заявки b=0.5, 0.1, 0.05 (см. рис. 4).

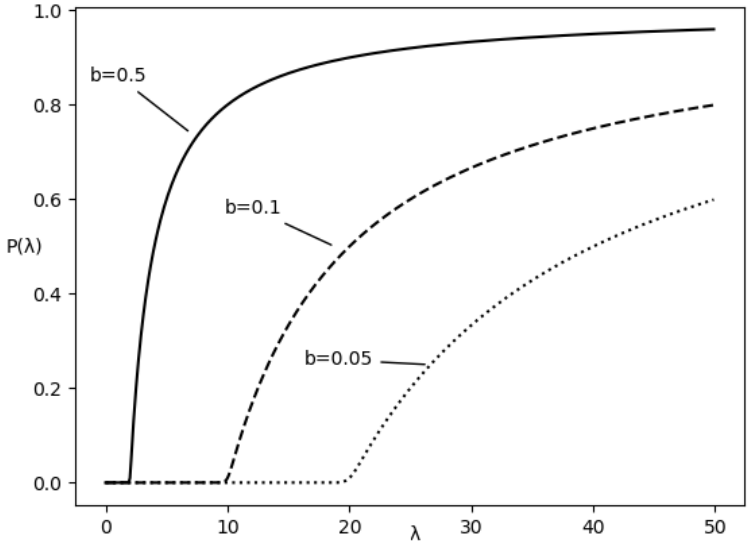

Рис. 4. График зависимости вероятности отказа в обслуживании заявки от интенсивности входного потока заявок при b = 0.5, 0.1, 0.05

На основе этих графиков можно сделать вывод, что уменьшение среднего времени обработки транзакции позволяет отодвинуть момент резкого повышения вероятности отказа системы в обслуживания до больших значений интенсивности входного потока заявок. Кроме того, зависимость этих величин обратно пропорциональна друг другу. Из этого следует, что от уменьшения среднего времени обработки транзакции в системе пропускная способность системы всегда будет увеличиваться. Однако добиться этого улучшения значительно сложнее, так как для улучшения этой характеристики необходимо усовершенствовать протокол нахождения консенсуса между узлами сети, что представляет из себя значительно более трудную задачу, требующую сложных теоретических исследований и тестирования прототипов.

Увеличение количества каналов обработки заявок улучшает параметры системы аналогично уменьшению среднего времени обслуживания одной заявки таким образом, что система с двумя каналами и средним временем обслуживания заявки b эквивалентна системе с одним каналом и средним временем обслуживания одной заявки $b/2$ (соответственно, графики для данного случая не приводятся). Команда разработчиков платформы Ethereum считает увеличение количества каналов блокчейн-технологий наиболее перспективным среди всех остальных и уже ведут разработки в этом направлении. Это улучшение называется Ethereum Plasma [12].

Выводы

Разработана математическая модель смарт-контракта ICO на основе платформы Ethereum, ориентированная на анализ проблемы низкой пропускной способности блокчейн-систем. Характеристики модели зависят от таких параметров как размер буфера транзакций, среднее время обработки одной транзакции и количество каналов обслуживания. Исходя из данных характеристик модель позволяет определить вероятность отказа транзакции в обслуживании в зависимости от интенсивности входящего потока заявок, на основании чего организаторы ICO могут прогнозировать максимально допустимую нагрузку на сеть.

Кроме того, на основе анализа зависимостей характеристик модели от параметров было установлено, что решение проблемы масштабируемости блокчейн-технологий возможно только благодаря уменьшению среднего времени обработки одной транзакции либо увеличению количества каналов, для чего необходима модернизации алгоритма консенсуса и применения технологий, подобных Lightning Network [13].

Список литературы: 1. *Why Bitcoin* Matters [Электронный ресурс]/ Marc Andreessen. – Режим доступа: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters – 15.11.2017 – Загл. с экрана. 2. *Cryptocurrency* Market Capitalizations [Электронный ресурс]/ Coinmarketcup team. – Режим доступа: https://coinmarketcap.com/ - 18.12.2017 – Загл. с экрана. 3. *Ether Sale*: A Statistical Overview [Электронный ресурс]/ Vitalik Buterin – Режим доступа: https://blog.ethereum.org/ether-sale-a-statistical-overview- 15.11.2017 – Загл. с экрана. 4. *Ethereum* white-paper [Электронный ресурс] /Ethereum Foundation – Режим доступа: https://bitcoil.co.il/Doublespend.pdf – 15.11.2017 – Загл. с экрана. 5. *Initial Coin* Offering (ICO) [Электронный ресурс]/ Investopedia team – Режим доступа: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp – 15.11.2017 – Загл. с экрана. 6. *Digix's* Whitepaper: The Gold Standard in Crypto-Assets [Электронный ресурс]/ Anthony C. Eufemio, Kai C. Chng, Shaun Djie – Режим доступа: https://digix.global/whitepaper.pdf – 15.11.2017 – Загл. с экрана. 7. *What is ERC-20* and What Does it Mean for Ethereum [Электронный ресурс]/ Nathan Reiff – Режим доступа: https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum – 15.11.2017 – Загл. с экрана. 8. *What are Polybius* tokens and why should they be in every crypto-investor's portfolio [Электронный ресурс]/ Polybius team – Режим доступа: https://blog.polybius.io/what-are-polybius-tokens-and-why-should-they-be-in-every-crypto-investors-portfolio-73a813c77429 – 15.11.2017 – Загл. с экрана. 9. *How the status* ico almost crashed the ethereum network [Электронный ресурс]/ Ashour Iesho – Режим доступа: http://bitcoinist.com/how-the-status-ico-almost-crashed-the-ethereum-network – 15.11.2017 – Загл. с экрана. 10. *Вентцель Е.С.* Теория Вероятностей. - М., 1969. 576 с. 11. *Ethereum* network statistic [Электронный ресурс] – Режим доступа: https://ethstats.net – 15.11.2017 – Загл. с экрана. 12. *Plasma:* Scalable Autonomous Smart Contracts [Электронный ресурс]/ Joseph Poon, Vitalik Buterin – Режим доступа: https://plasma.io/plasma.pdf – 15.11.2017 – Загл. с экрана. 13 *The Bitcoin* Lightning Network: Scalable Off-Chain Instant Payments [Электронный ресурс]/ Joseph Poon, Thaddeus Dryja – Режим доступа: https://lightning.network/lightning-network-paper.pdf – 15.11.2017 – Загл. с экрана.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 09.11.2017