ОСНОВНЫЕ СЕТЕВЫЕ ХАРАКТЕРИСТИКИ BLOCKCHAIN ТРАФИКА И ПОДХОДЫ К МОДЕЛИРОВАНИЮ

DOI: 10.36724/2072-8735-2020-14-4-39-45

Елагин Василий Сергеевич,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ***elagin.vas@gmail.com***

Спиркина Анастасия Валентиновна,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ***anastasia.4991@mail.ru***

Владыко Андрей Геннадьевич,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ***vladyko@sut.ru***

Иванов Евгений Игоревич,
Корпоративный центр ПАО "Ростелеком", г. Санкт-Петербург, Россия, ***e.ivanov@rt.ru***

Помогалова Альбина Владимировна,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ***a.l.b.i.n.a@bk.ruu***

Аптриева Елизавета Алексеевна,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ***lizok.5757@gmail.com***

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90050/19

Ключевые слова: *блокчейн, распределенный реестр, сети передачи данных, децентрализованные системы*

В связи с появлением передовых технологий и множества разнообразных приложений в настоящее время важным элементом на современных сетях связи становится технология Blockchain из-за её технических возможностей и особенностей. Рассматривается поведенческая модель сервисов Blockchain, на основе экспериментальных данных подтверждается её достоверность. Рассматриваются также определение Blockchain, достоинства и недостатки данной технологии и основные сетевые атаки, которым подвергаются сети с Blockchain узлами. Авторы обозначают основные технические характеристики и их особенности, связанные с передачей информации через сеть, определяют схему сети при работе с транзакциями Blockchain, а также зависимость характеристик сети от параметров приложений. Проводится анализ применения данной модели для обнаружения сервисов Blockchain и возможности дискредитации существующих механизмов безопасности данной технологии. Приводится описание ключевых результатов эксперимента, в рамках которого проводился анализ трафика. Авторы представили графики интенсивности обмена данными на разных этапах работы технологии Blockchain. Приводится зависимость распределения числа пакетов от их размера и зависимость плотности распределения временных интервалов между пакетами. Представленный эксперимент показал, что зависимость распределения числа пакетов от их размера и зависимость плотности распределения временных интервалов между пакетами являются близкими к логнормальному закону. В статье даны рекомендации по сокрытию профиля трафика Blockchain, что значительно усложнит его идентификацию на сети передачи данных.

Информация об авторах:
Елагин Василий Сергеевич*, к.т.н., доцент кафедры Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия*
Спиркина Анастасия Валентиновна*, аспирант, кафедра Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия*
Владыко Андрей Геннадьевич*, директор института, Научно-исследовательский институт "Технологии связи" Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия*
Иванов Евгений Игоревич*, руководитель направления лаборатории КЦ г. Санкт-Петербург Корпоративный центр ПАО "Ростелеком", г. Санкт-Петербург, Россия*
Помогалова Альбина Владимировна*, магистрант, ассистент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия*
Аптриева Елизавета Алексеевна*, студент, кафедра Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия*

Для цитирования:
Елагин В.С., Спиркина А.В., Владыко А.Г., Иванов Е.И., Помогалова А.В., Аптриева Е.А. Основные сетевые характеристики blockchain трафика и подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Том 14. №4. С. 39-45.

For citation:
Elagin V.S., Spirkina A.V., Vladyko A.G., Ivanov E.I., Pomogalova A.V., Aptrieva E.A. (2020) The main network characteristics of blockchain traffic and modeling approaches. *T-Comm*, vol. 14, no.4, pp. 39-45. (*in Russian*)

Введение

Blockchain – это распределенная база данных, которая состоит из постоянно растущего списка структурированных данных, а также у которой устройства хранения и обработки данных не подключены к общему серверу [1, 2].

Практичность Blockchain технологии легко оценить, когда предъявляются высокие требования к системе по хранению данных и подтверждению их подлинности.

Представим преимущества и недостатки данной технологии [1].

Преимущества:

– децентрализация;
– надежность и конфиденциальность;
– компромисс и консенсус;
– прозрачность транзакций и системы.

Недостатки:

– масштабируемость;
– мошенничество и необратимость операций при ошибках;
– скорость обработки транзакций ниже, чем в текущих системах;
– возможность проведения незаконных либо теневых операций.

Технические аспекты

В Blockchain технологии безопасность обеспечивается с помощью децентрализации. Формируется реестр данных, который управляется самостоятельно. Целостность транзакций организуются с помощью криптографических правил [3]. При синхронизации узлов сети Blockchain - все записи транзакций сохраняются и обновляются на устройствах. Узлом может быть любое устройство с доступом к сети Интернет. Как только узлы загружены, они выполняют одноранговое обнаружение, чтобы связаться с другими доступными узлами, используя TCP порт. Роль узла – поддерживать сеть, хранить и обновлять копию, обрабатывать транзакции.

Процедура обмена информацией в рамках Blockchain состоит из ряда сообщений, передающихся по определенным правилам. Пример сценария обмена информацией представлен на рис. 1.

Основные типы сообщения, использующиеся при обмене информацией [4]:

Version, veract, addr, getaddr, getblocks, inv, getdata, block.

Передача блоков по сети осуществляется по традиционному стеку TCP/IP. Блок представляет собой контейнер, объединяющий транзакции для включения в реестр. Блоки состоят из заголовков, и тел из списков транзакций.

Заголовок состоит из ссылки на предыдущий хеш, значения сложности, временной метки и случайного числа, корня дерева Меркла.

Алгоритм действий технологии Blockchain при работе с транзакциями представлен на рис. 2.

Технология Blockchain применяет криптографические алгоритмы для защиты данных пользователя и обеспечения надежности системы [4, 5].

Криптографические основы в технологии Blockchain делятся на две категории: первичные и вторичные. Первая категория применяется для обеспечения защиты от несанкционированного доступа, публичной проверки и достижения консенсуса (хеш и стандартные цифровые подписи). Вторая категория используется для повышения конфиденциальности и анонимности транзакций.

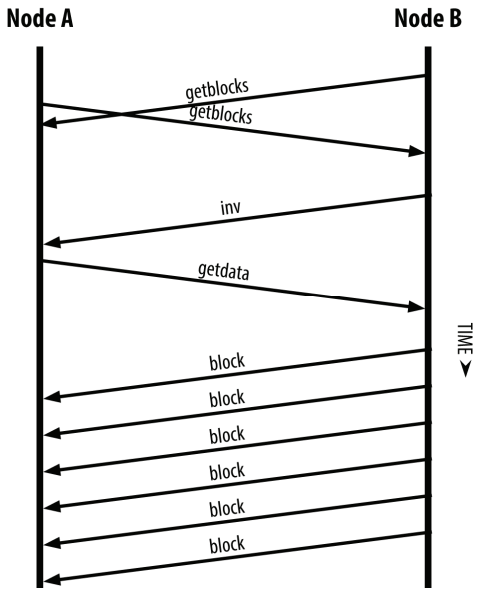

Рис. 1. Пример сценария обмена при синхронизации узлов

Хэширование. В технологии Blockchain хеширование используется для описания изменений процессов, произведенных с транзакциями, а также для защиты данных от изменения и определения их размера. Что повышает безопасность при работе с данными, так как при изменении определенного блока потребуется пересчет всех последующих, который потребует огромных вычислений и будет сложным в реализации.

С помощью электронной подписи в документ добавляется особая метка, которая позволяет подтвердить принадлежность подписи владельцу, а также установить отсутствие искажения данных с момента формирования документа.

Закрытые ключи используются пользователем для подписи транзакций, открытые применяются для проверки подлинности транзакций других пользователей. Безопасность технологии Blockchain обеспечивается за счет использования криптографических примитивов и децентрализации.

Сетевые атаки

В настоящих сетях из-за неполной защищенности или ошибок пользователей появляется возможность проводить различные сетевые атаки. При этом для Blockchain систем угрозы немного отличаются от атак для стандартных компьютерных сетей.

Ниже приведены примеры сетевых атак, которым подвержены Blockchain системы:

1. Атака 51%

При контроле нарушителем более половины узлов Blockchain-сети, злоумышленник может создать свою цепочку блоков, что позволит вставлять только свои данные. Такое может быть реализовано и при контроле менее половины узлов, однако при этом происходит значительное снижение вероятности проведения успешной атаки.

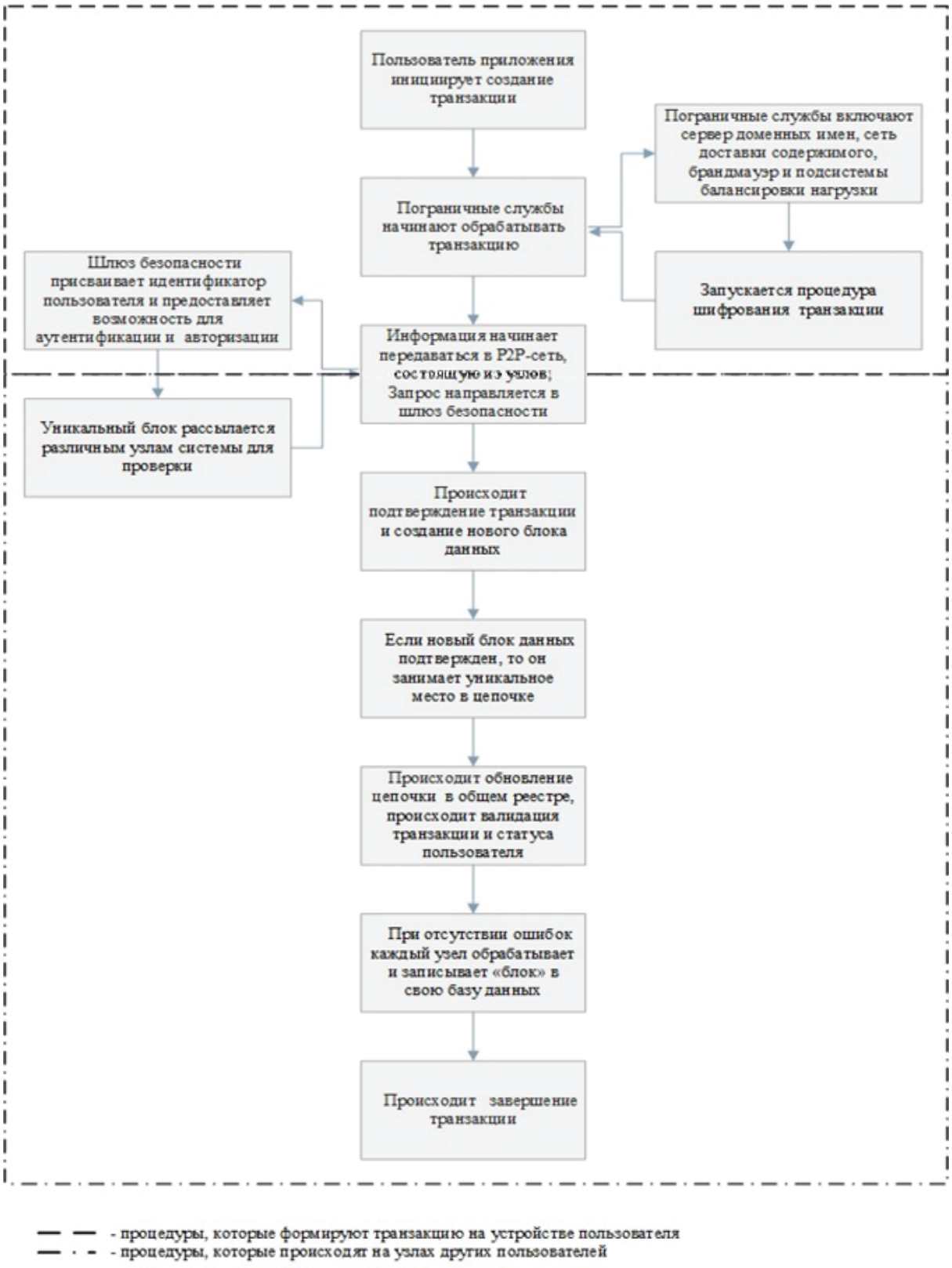

Рис. 2. Алгоритм действий Blockchain технологии при работе с транзакциями

На данный момент для проведения атаки такого типа в развитых сетях требуется значительная вычислительная мощность, получить которую в настоящее время затруднительно.

2. Атака Сибиллы

Для атаки Сибиллы характерно приобретение нескольких сущностей одним узлом.

Чаще всего данная атака используется для фальсификации голосований или накрутки рейтинга. Нарушитель может получить возможность видеть все транзакции, либо ограничить доступ пользователя ко всей сети. Для защиты применяются эвристические правила для исключения вредоносного трафика, обращение в доверенный сертификационный центр, либо введение ограничения действий пользователя в отведенный промежуток времени.

3. DDoS

При DDoS атаке происходит пересылка большого количества схожих пакетов для ограничения работоспособности узла или системы.

Во многих Blockchain системах для защиты от такой атаки типа применяются методы, основанные на ограничении размера блока, ограничении числа проверок подписи, блокировке подозрительных транзакций или поведения.

4. Взлом криптографии

Алгоритмы для вычисления хэш-функции технологии Blockchain невозможно взломать на оборудовании, которое доступно в настоящее время, однако при появлении квантовых компьютеров появится возможность взлома. В таком случае, алгоритмы шифрования систем необходимо будет заменить на более сложные.

Большинство Blockchain систем не взламывались, однако обнаруживаются проблемы с безопасностью у кошельков и аккаунтов на сторонних сервисах, так или иначе связанных с работой этой технологии.

Трафик Blockchain является шифрованным, однако анализ поведенческой модели позволит идентифицировать потоки данных с возможностью прогнозирования дальнейшего влияния на сервисы.

Сетевые характеристики технологии Blockchain

Необходимо определить сетевой процесс взаимодействия и технические характеристики трафика при использовании Blockchain технологии для анализа поведенческой модели. [4, 9] Также необходимо оценить влияние передачи большого количества транзакций, а также оценить объем служебных данных, который появляется при сокрытии трафика (рис. 3).

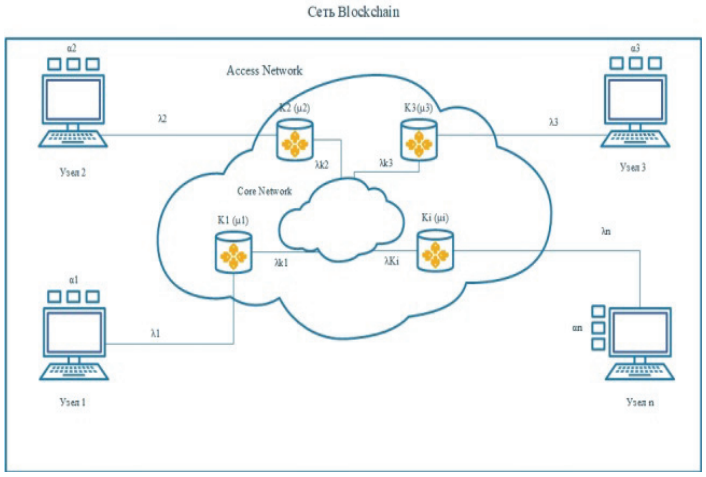

Рис. 3. Схема распределения потоков трафика blockchain

Загрузка сети (ρ) при этом будет зависеть от:

$$p\ F(n, \alpha_n, d, \lambda_n, \mu, k_i), \quad (1)$$

где:

n – количество узлов в Blockchain сети (единиц);

α_n – интенсивность формирования транзакций (транзакций в секунду);

k_i – количество задействованных маршрутизаторов (единиц);

μ – интенсивность обработки пакетов маршрутизаторами (пакетов в секунду);

λ_n – интенсивность формирования пакетов (пакетов в секунду);

d – размер блоков (байт).

При синхронизации узлов трафик Blockchain провоцирует лавинообразную загрузку сети.

Для Blockchain технологии характерна передача информации резким всплескам. Подобные всплески происходят в связи с синхронизацией узлов между собой при первичном подключении или после решения криптографической задачи.

Детальное исследование характеристик параметров, представленных в (1) зависимости позволит оценить влияние каждого узла на загрузку сети и определить это влияние на характеристики сети, которые необходимы для качественной работы приложений.

Если возможно описать модель и определить первичные зависимости трафика Blockchain от характеристик сети, то существует большая вероятность идентификации трафика на сети доступными средствами.

Таким образом, необходимо определить возможность выделения профиля трафика Blockchain на сети передачи данных.

Для анализа поведения трафика на сети, было создано пять виртуальных клиентов на базе Linux Ubuntu 18.04 LTS, связанных между собой и с внешней сетью, с ролями майнера и инициатора транзакций.

Обобщенная схема проведения эксперимента приведена на рис. 4.

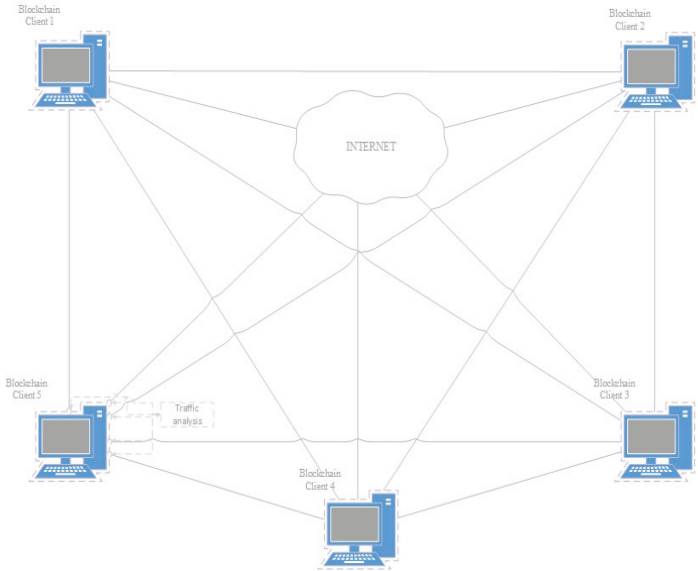

Рис. 4. Обобщенная схема проведения эксперимента

В ходе экспериментов, виртуальные клиенты отправляли транзакции аналогичному клиенту, с частотой 4 транзакции в секунду. Эксперименты проводились в разное время суток, с одинаковой последовательностью действий. Данные получены в рамках 50 испытаний, обработаны с помощью математического аппарата статистического анализа.

Результаты, представленные на графиках интенсивности обмена пакета при работе В (рис. 5, 6, 7), отражают, что вне зависимости от времени суток трафик передается по аналогичным распределениям, варьирующихся незначительно и представляет собой поток трафика с лавинообразными всплесками интенсивности.

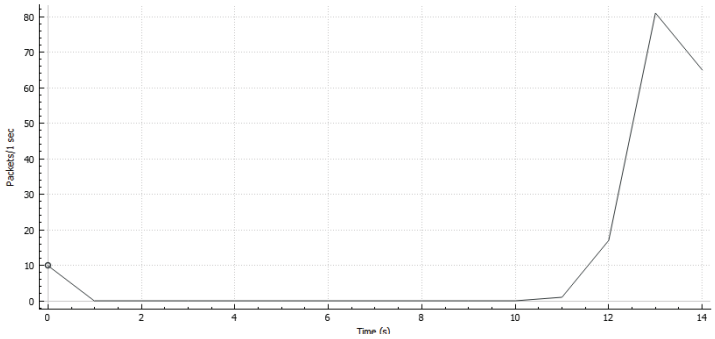

Рис. 5. Интенсивность обмена пакетами на узле при первоначальной синхронизации с сетью

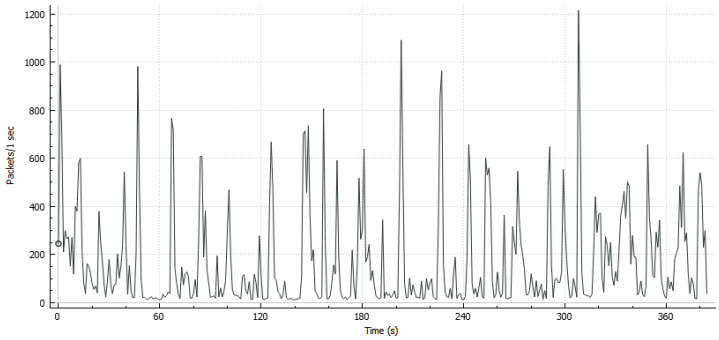

Рис. 6. Интенсивность обмена пакетами на узле при синхронизации узла с соседями и майнинг

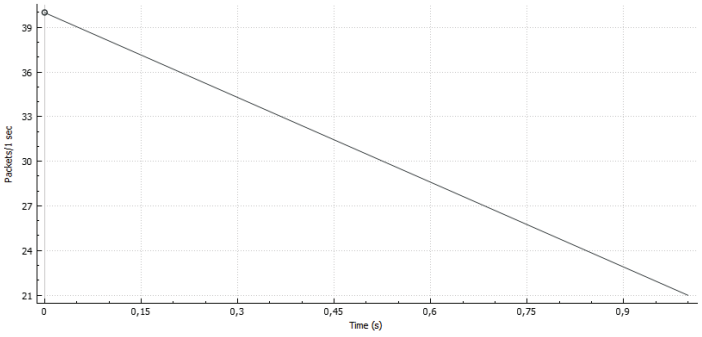

Рис. 7. Интенсивность обмена пакетами на узле после майнинга

Кроме того интерес вызывают графики зависимости распределения числа пакетов от их размера и плотности распределения временных интервалов между пакетами.

На графиках, определяющих распределения числа пакетов от их размера (рис. 8) видно, что большая часть пакетов (85%) представлена в интервале 65-250 байт и включает трафик, переданный при синхронизации данных между узлами. Так же можно заметить тип трафика (9%), передаваемый в рамках транзакций, который имеет длину свыше 1100 байт.

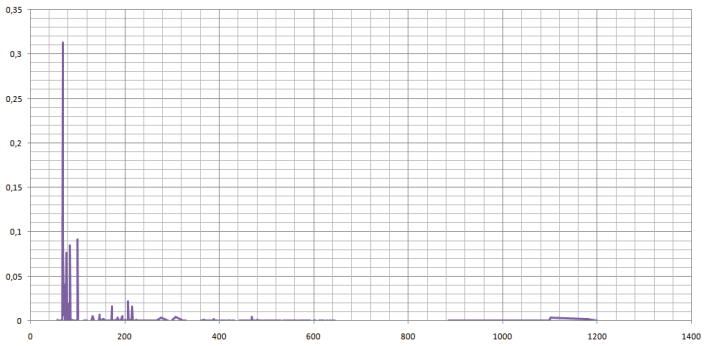

Рис. 8. Зависимость количества пакетов (в%) от длины пакета

При анализе плотности распределения временных интервалов между пакетами можно увидеть зависимость на рис. 9, в свою очередь во всех экспериментах задержка для большинства пакетов не превышала 0,2 мс.

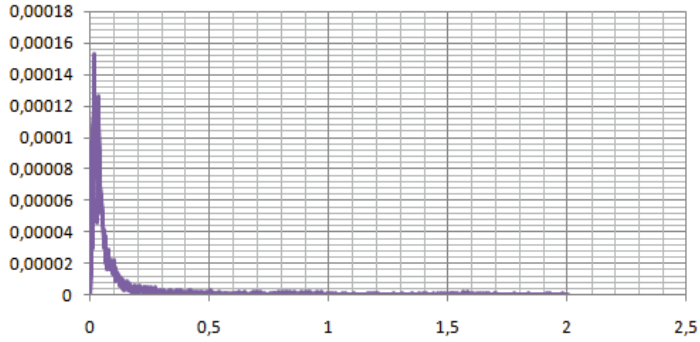

Рис. 9. Зависимость количества пакетов (в%) от времени между пакетами (мс)

В дальнейшем был проведен статистический анализ полученных данных.

Для обеих зависимостей, верно, что:

Поскольку коэффициент вариации больше 70%, то совокупность приближается к грани неоднородности.

Значения As и Ex мало отличаются от нуля. Таким образом, можно предположить близость данной выборки к логнормальному распределению.

Проверка гипотезы по критерию согласия Пирсона показала, что нет оснований отвергать гипотезу о логнормальном законе распределения.

Таким образом, данные зависимости можно представить в рамках математической модели логнормального распределения с различными весовыми коэффициентами, графики представлены на рис. 10, 11.

Статистический анализ показал, что отдельные характеристики трафика Blockchain могут быть смоделированы при помощи распределения близкого к нормальному, что позволяет использовать данные аналитической модели для идентификации Blockchain трафика и его прогнозирования.

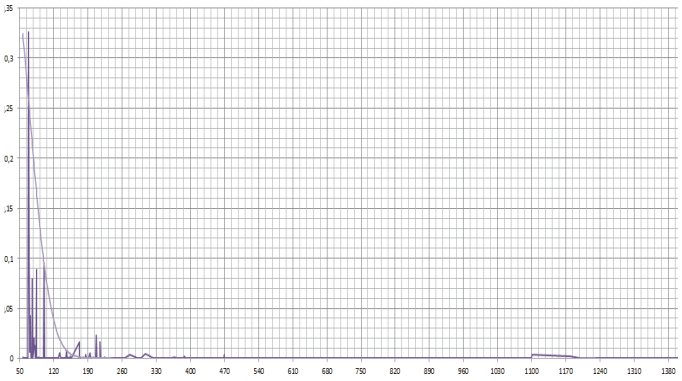

Рис. 10. Сравнение полученных результатов со значениями, полученными при логнормальном распределении

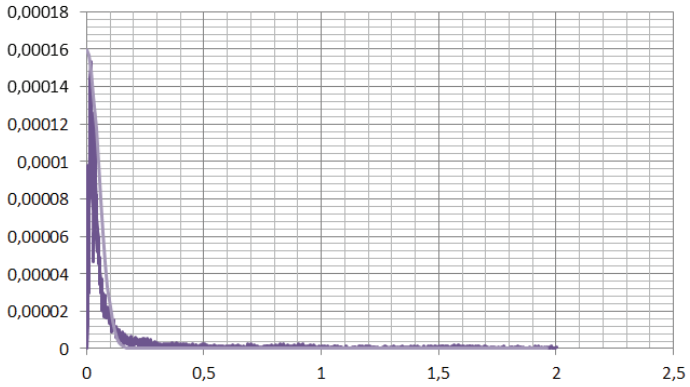

Рис. 11. Сравнение полученных результатов со значениями, полученными при логнормальном распределении

Таким образом, для сокрытия трафика нам необходимо динамически изменять характеристики, представленные в исследовании. Для изменения зависимости распределения числа пакетов от их размера можно искусственно варьировать длину блоков. Основными решениями для таких изменений являются программные утилиты, либо ручная настройка передачи данных с устройства. Для изменения зависимости плотности распределения временных интервалов между пакетами можно рассмотреть искусственное изменение времени между передачей пакетов, а так же изменение размера пакетов и алгоритма их передачи.

Выводы

Несмотря на шифрование технологии Blockchain, её можно идентифицировать в потоке с помощью решений глубокого анализа пакетов, которые включают поведенческий анализ, что в дальнейшем позволит дискредитировать и использовать в своих целях сервисы данной технологии.

В статье были проанализированы основные характеристики трафика Blockchain и представлены аналитические модели, которые позволяют прогнозировать загрузку сети. И в дальнейшем обеспечить качественный и безопасный обмен данными на данном участке сети.

В рассмотренном эксперименте проводился анализ трафика в рамках 3 минутных сессий, чего оказалось достаточно для выделения поведения трафика технологии Blockchain. Эксперимент показал, что зависимость распределения числа пакетов от их размера и зависимость плотности распределения временных интервалов между пакетами являются близкими к логнормальному.

Литература

1. *W. Mougayar*, The business blockchain, New Jersey: John Wiley & Sons Inc., Hoboken, 2016.
2. *Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao and M. A. Imran*, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," *in* IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5791-5802, June 2019.
3. *Елагин В.С., Онуфриенко А.В.* Как оператору заработать на OTT-сервисах и при чем тут SDN? // T-Comm: Телекоммуникации и транспорт, 2017. №1. С. 17-21.
4. *Antonopoulos A.M.* Mastering Bitcoin, O'Reilly Media Inc, 2017.
5. *Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г.* Сети связи, SPb.: BHV – St. Petersburg, 2014.
6. *M.V. Buinevich.* Problem issues and trends in is supply in the field of telecommunications // Protection of information. Insider, vol. 1 (73), pp. 49-55, 2017.
7. *M. Buinevich, A. Vladyko*. Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: an overview of cyber attacks // Information (Switzerland), vol. 10, no. 1, pp.1-27, 2019.
8. *Y. Guan and X. Ge*, "Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks // in IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 48-59, March 2018.
9. *A.B. Goldstein, A.A. Zarubin, A.V. Onufrienko, V.S. Elagin and I.A. Belozertsev*. Synchronization of delay for OTT services in LTE // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, 2018, pp. 1-4, July 04-05.
10. *A.B. Goldstein, N.A. Sokolov, V.S. Elagin, A.V. Onufrienko and I.A. Belozertsev.* Network Characteristics of Blockchain Technology of on Board Communication // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1-5, March 20-21.
11. *V.S. Elagin, I.A. Belozertsev, B.S. Goldshtein, A.V. Onufrienko and A.G. Vladyko*. Models of QOE ensuring for OTT services // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1-4, March 20-21.
12. *M. Makolkina, A. Koucheryavy, A. Paramonov*. Investigation of Traffic Pattern for the Augmented Reality Applications // Lecture notes in computer science, vol. 10372, 2017, pp. 233-246.
13. *T. Topór-Kamiński, B. Krupanek, J. Homa*. Delays models of measurement and control data transmission network // Studies in Computational Intelligence, vol. 440, 2013, pp. 257-278.
14. *Дао Ч.Н., Парамонов А.И.* Модели концентрации трафика M2M и оценка его влияния на QOS в сетях 5G // Телекоммуникации, ч. 4, 2018. С. 47-54.
15. *Парамонов А.И., Маколкина М.А., Киричек Р.В., Выборнова А.И., Богданова Е.Г.* Математические модели в сетях связи. СПбГУТ (Санкт-Петербург), ч. 1, 2018.

THE MAIN NETWORK CHARACTERISTICS OF BLOCKCHAIN TRAFFIC AND MODELING APPROACHES

Vasiliy S. Elagin, *SPbGUT, St. Petersburg, Russia,* ***elagin.vas@gmail.com***
Anastasia V. Spirkina, *SPbGUT, St. Petersburg, Russia,* ***anastasia.4991@mail.ru***
Andrei G. Vladyko, *SPbGUT, St. Petersburg, Russia,* ***vladyko@sut.ru***
Evgeniy I. Ivanov, *Corporate center of Rostelecom, St. Petersburg, Russia,* ***e.ivanov@rt.ru***
Albina V. Pomogalova, *SPbGUT, St. Petersburg, Russia,* ***a.l.b.i.n.a@bk.ru***
Elizaveta A. Aptrieva, *SPbGUT, St. Petersburg, Russia,* ***lizok.5757@gmail.com***

Abstract

Due to the emergence of advanced technologies and a variety of applications, Blockchain technology is now becoming an important element on modern communication networks due to its technical capabilities and features. The article considers the behavioral model of Blockchain services, and its reliability is confirmed on the basis of experimental data. The authors consider the definition of Blockchain, advantages and disadvantages of this technology. In this article, the authors consider the main network attacks that networks with Blockchain nodes are subjected to. The authors identify the main technical characteristics and their features related to the transmission of information through the network, determine the network scheme when working with Blockchain transactions, and the dependence of network characteristics on application parameters. The analysis of the use of this model for detecting Blockchain services and the possibility of discrediting the existing security mechanisms of this technology is carried out. The article describes the key results of the experiment in which traffic analysis was performed. The authors presented graphs of the intensity of data exchange at different stages of the Blockchain technology. Also in this article, the authors give the dependence of the distribution of the number of packages on their size and the dependence of the density of the distribution of time intervals between packages. The presented experiment showed that the dependence of the distribution of the number of packets on their size and the dependence of the density of the distribution of time intervals between packets are close to the lognormal law. In addition, the article provides recommendations for hiding The blockchain traffic profile, which will significantly complicate its identification on the data transmission network.

Keywords: *Blockchain, distributed registry, security, data protection, network, decentralized systems.*

References

1. W. Mougayar. (2016). *The business blockchain*, New Jersey: John Wiley & Sons Inc., Hoboken.
2. Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao and M. A. Imran. (2019). Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment. *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791-5802, June 2019.
3. V.S. Elagin, A.V. Onufrienko. (2017). How can an operator make money on OTT services and what does SDN have to do with it?. *T-Comm*, vol. 1, pp. 17-21.
4. A.M. Antonopoulos. (2017). *Mastering Bitcoin*, O'Reilly Media Inc.
5. B.S.Goldstein, N.A. Sokolov, G.G. Yanovsky. (2014). *Communication Networks*, SPb.: BHV – St. Petersburg.
6. M.V. Buinevich. (2017). Problem issues and trends in is supply in the field of telecommunications. *Protection of information. Insider*, vol. 1 (73), pp. 49-55.
7. M. Buinevich, A. Vladyko. (2019). Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: an overview of cyber attacks. *Information (Switzerland)*, vol. 10, no. 1, pp. 1-27.
8. Y. Guan and X. Ge. (2018). Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks. *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48-59, March 2018.
9. A.B. Goldstein, A. A. Zarubin, A.V. Onufrienko, V.S. Elagin and I.A. Belozertsev. (2018). Synchronization of delay for OTT services in LTE. *2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO),* Minsk, 2018, pp. 1-4, July 04-05.
10. A.B. Goldstein, N.A. Sokolov, V.S. Elagin, A.V. Onufrienko and I.A. Belozertsev. (2019). Network Characteristics of Blockchain Technology of on Board Communication. *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, 2019, pp. 1-5, March 20-21.
11. V.S. Elagin, I.A. Belozertsev, B.S. Goldshtein, A.V. Onufrienko and A.G. Vladyko. (2019). Models of QOE ensuring for OTT services. *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, 2019, pp. 1-4, March 20-21.
12. M. Makolkina, A. Koucheryavy, A. Paramonov. (2017). Investigation of Traffic Pattern for the Augmented Reality Applications. *Lecture notes in computer science*, vol. 10372. pp. 233-246.
13. T. Topir-Kamiiski, B. Krupanek, J. Homa. (2013). Delays models of measurement and control data transmission network. *Studies in Computational Intelligence*, vol. 440, pp. 257-278.
14. Ch.N. Tao, A.I. Paramonov. (2018). Models of traffic concentration M2M and assessment of its impact on QOS in 5G networks. *Telecommunications*, vol. 4, pp. 47-54.
15. A.I. Paramonov, M.A. Makolkina, R.V. Kirichyok, A.I. Vybornova, E.G. Bogdanova. (2018). *Mathematical models in communication networks*. St. Petersburg State University of Telecommunications prof. M.A. Bonch-Bruevich (St. Petersburg), vol. 1.

Information about authors:
Vasiliy S. Elagin, *associate Professor of the Department of Infocommunication systems of SPbGUT, St. Petersburg, Russia*
Anastasia V. Spirkina, *postgraduate student, Department of Infocommunication systems of SPbGUT, St. Petersburg, Russia*
Andrei G. Vladyko, *director R&D of SPbGUT, St. Petersburg, Russia*
Evgeniy I. Ivanov, *head of direction laboratory corporate center of Rostelecom, St. Petersburg, Russia*
Albina V. Pomogalova, *master student, Assistant of Department of Software Engineering and Computer Facilities of SPbGUT, St. Petersburg, Russia*
Elizaveta A. Aptrieva, *student, Department of Infocommunication systems of SPbGUT, St. Petersburg, Russia*