УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2020 Том 20 № 4 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2020 Vol. 20 No 4 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004 doi: 10.17586/2226-1494-2020-20-4-472-484

ТЕХНОЛОГИЯ БЛОКЧЕЙН В СЕТЯХ 5G

С.В. Беззатеев[a,b], И.Р. Федоров[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, 190000, Российская Федерация
Адрес для переписки: bsv@aanet.ru

Информация о статье

Поступила в редакцию 18.05.20, принята к печати 20.06.20
Язык статьи — русский

Ссылка для цитирования: Беззатеев С.В., Федоров И.Р. Технология блокчейн в сетях 5G // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 4. С. 472–484. doi: 10.17586/2226-1494-2020-20-4-472-484

Аннотация

В связи с бурным развитием мобильных сетей и ростом подключенных к ним устройств различного типа обеспечение целостности и конфиденциальности передаваемых данных становится первостепенной задачей. Появление криптовалюты повлекло за собой возобновление интереса к технологии блокчейн и возможности ее использования в различных областях. В статье рассмотрены существующие в настоящий момент способы применения технологии блокчейн в сетях 5G с целью решения проблем безопасности, сетевого взаимодействия и повышения производительности, а также для разработки новых направлений, расширяющих возможности сервисов и приложений в сетях пятого поколения. Представлен анализ современных исследовательских работ по интеграции технологии блокчейн и ключевых технологий, применяющихся в мобильных сетях пятого поколения. Особое внимание уделено вариантам применения технологии блокчейн в облачных и граничных вычислениях, программно-определяемых сетях, виртуализации сетевых функций, 5G-слайсинге и прямом взаимодействии устройств. Основываясь на материалах, представленных в обзоре, перечислены возможности, которые технология блокчейн может предоставить мобильным сетям и сервисам 5G за счет использования децентрализованной архитектуры и алгоритма умного контракта. Основное внимание в материалах предлагаемого обзора уделено трем основным аспектам: повышению безопасности передаваемой информации, повышению производительности системы и управлению ресурсами. Статья может быть полезна специалистам и научным сотрудникам, работающим в области информационной безопасности мобильных сетей пятого поколения, а также для экспертов в сфере технологии блокчейн в качестве актуального обзора различных вариантов применения технологии блокчейн в сетях пятого поколения.

Ключевые слова

блокчейн, мобильные сети, 5G, безопасность, децентрализация, облачные вычисления

doi: 10.17586/2226-1494-2020-20-4-472-484

BLOCKCHAIN TECHNOLOGY IN 5G NETWORKS

S.V. Bezzateev[a,b], I.R. Fedorov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
[b] Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation
Corresponding author: bsv@aanet.ru

Article info

Received 18.05.20, accepted 20.06.20
Article in Russian

For citation: Bezzateev S.V., Fedorov I.R. Blockchain technology in 5G networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2020, vol. 20, no. 4, pp. 472–484 (in Russian). doi: 10.17586/2226-1494-2020-20-4-472-484

Abstract

The rapid development of mobile networks and the growth of various types of devices connected to them has called forth the integrity and confidentiality ensuring of the transmitted data that now is a high-priority problem. The emergence of cryptocurrency was followed by renewal of interest in blockchain technology and the possibility of its use in various fields. The paper discusses currently existing methods of blockchain technology application in 5G networks in order to solve security problems, network connectivity and productivity improvement, as well as to develop new directions that expand the capabilities of services and applications in fifth-generation networks. The paper presents analysis of modern

research works on the blockchain technology integration and key technologies used in the fifth-generation mobile networks. Particular attention is paid to applications of blockchain technology in cloud computing, edge computing, software-defined networking, virtualization of network functions, 5G-slicing and device-to-device communication. Based on the materials presented in the review, the options are outlined that blockchain technology can provide to 5G mobile networks and services through the use of a decentralized architecture and a smart contract algorithm. The materials of the proposed review is focused on the three main aspects: enhancement of transmitted information security, system performance and resources management. The paper can be useful to specialists and researchers working in the field of information security of the fifth-generation mobile networks, as well as for experts in the field of blockchain technology as an up-to-date overview of various applications of blockchain technology in the fifth-generation networks.

Keywords
blockchain, mobile network, 5G, security, decentralization, cloud computing

Введение

Мобильные сети пятого поколения (5G) представляют собой следующий важнейший этап в развитии глобальных сетей и услуг электросвязи. Мобильные сети 5G обеспечивают более высокую пропускную способность по сравнению с сетями четвертого поколения (4G), что позволяет обеспечить большую доступность широкополосной мобильной связи. Более того, в сетях 5G поддерживаются массовые машинные коммуникации (mMTC) и обеспечивается высоконадежная связь со сверхнизкой задержкой [1]. Стоит отметить, что все вышеперечисленное открывает путь для новых бизнес-возможностей, соединяя между собой миллиарды устройств и обеспечивая быстрое развитие телекоммуникаций. Основное видение будущих услуг мобильных сетей 5G заключается в предоставлении персонализированной и ориентированной на пользователя ценности, позволяющей подключать практически все аспекты человеческой жизни к сетям связи [2]. Однако новые технологии и услуги в сетях 5G предъявляют и новые требования к безопасности и конфиденциальности данных, поэтому методов и средств информационной безопасности, использующихся в предыдущих поколениях мобильных сетей, будет недостаточно. Обеспечение безопасности в сетях 5G станет более сложной задачей из-за большого количества подключенных устройств различного типа. Актуальной проблемой является обеспечение открытой архитектуры данных и обеспечение их прозрачности и неизменности при совместном использовании и многопользовательском доступе. Среди существующих инновационных решений блокчейн является наиболее перспективной технологией для удовлетворения этих новых требований безопасности [3, 4].

В широких кругах блокчейн известен как технология, лежащая в основе криптовалюты Bitcoin [5]. Однако реальная история технологии блокчейн началась намного раньше (первая работа, посвященная этой технологии, была опубликована в 1991 г.) [6]. С технической точки зрения блокчейн представляет собой децентрализованную, неизменную и прозрачную базу данных. Концепция блокчейн основана на архитектуре одноранговой сети, в которой информация о транзакциях контролируется всеми участниками сети, а не каким-либо одним централизованным узлом. В настоящее время данная технология была исследована и применена в различных областях, таких как Интернет вещей (IoT) [7, 8], умный город [9], транспортные сети [10] и различные отрасли промышленности [11].

С появлением криптовалюты блокчейн вызвал огромный интерес в научных кругах, что повлекло за собой ряд обзоров, в которых рассматриваются многие аспекты технологии, такие как архитектура, концепция, техническая сторона и области применения. Мобильные сети 5G также привлекли внимание и повлекли за собой ряд исследовательских работ. Благодаря переходу с сетей 4G на 5G существенно изменились скорости и объемы передаваемой информации. В качестве примера можно привести компанию «Билайн», которая для проведения испытаний на территории угольного разреза «Черногорский» (УОГР Абаканский, г. Черногорск, Хакасия) развернула фрагмент сети беспроводной связи стандарта 5G протяженностью 1,5 км, покрывающей маршрут следования самосвалов-роботов. Покрытие обеспечено двумя распределенными двухсекторными базовыми станциями стандарта 5G (gNodeB), работающими в режиме non-standalone, используемая ширина канала 100 МГц[1]. Также сеть 5G развивается рекордными темпами в Китае (по данным Mediasat в стране к маю 2020 г. насчитывается более 50 млн пользователей мобильной связи 5G)[2].

Представители компании Huawei, которая является ведущим мировым поставщиком базовых станций 5G, заявили, что в настоящее время коммерческие сети развернуты в 34 странах и регионах мира, при этом сети нового поколения уже активно используются в медийной и обрабатывающей промышленностях[3].

По мере увеличения покрытия 5G и создания более интеллектуальных приложений, требующих больших скоростей обмена огромными объемами данных, существенно возросла опасность успешных атак на такие системы, и, соответственно, потребовались более быстрые и эффективные методы защиты целостности и достоверности передаваемых и обрабатываемых данных. Именно здесь блокчейн может оказать огромную помощь благодаря своей повышенной безопасности. Даррен Садана, генеральный директор Choice IoT, плат-

[1] Билайн [Электронный ресурс]. Режим доступа: https://spb.beeline.ru/about/press-center-new/press-releases/details/1541032/, свободный. Яз. рус. (дата обращения: 24.05.2020).

[2] Медиастат [Электронный ресурс]. Режим доступа: http://mediasat.info/2020/05/04/kitaj-5g-2/, свободный. Яз. рус. (дата обращения: 24.05.2020).

[3] IXBT [Электронный ресурс]. Режим доступа: https://www.ixbt.com/news/2020/03/09/5g-34-50.html, свободный. Яз. рус. (дата обращения: 24.05.2020).

формы управления IoT, отмечает, что блокчейн может предотвратить взлом, и предсказывает, что большинство компьютерных программ, задействованных в мире IoT вскоре также перейдут на блокчейн: «Даже если небольшая часть взломана, это не повлияет на всю программу. Фактически, большая часть кодирования переместится в блокчейн в ближайшем будущем, так как он более устойчив к взлому»[1]. По мнению директора лаборатории блокчейн и цифровой экономики China Telecom Group Ляна Вэя (Liang Wei), блокчейн поможет добиться более эффективного и безопасного распределения ресурсов 5G и отслеживания их использования: «Децентрализованный обмен протоколами и платежи могут осуществляться автоматически с помощью смарт-контрактов. Сочетание технологий 5G и блокчейн — это тенденция будущего. DLT (Distributed Ledger Technology) и 5G улучшают характеристики и дополняют друг друга. Подобные реализации на базе 5G могут предоставить неограниченные возможности для создания приложений Интернета вещей»[2].

Однако вопреки растущему интересу к этим двум технологиям в существующих обзорах уделяется достаточно мало внимания их интеграции. В данной статье представлен обзор именно по использованию блокчейн в сетях 5G для предоставления различных видов услуг, включая облачные вычисления, граничные вычисления, программно-определяемые сети, виртуализацию сетевых функций, 5G-слайсинг и прямое взаимодействие устройств (Device-to-device, D2D). На основании данного обзора выделены особенности использования блокчейн в основных концепциях мобильных сетей 5G, а также ряд проблем и нерешенных вопросов для дальнейшего исследования.

Определение блокчейн и хеш-функции

В настоящей статье под понятием «блокчейн» понимается цепочка блоков, содержащих информацию о транзакциях и последовательно связанных с помощью хешей. Хеш-функция H — это функция, которая принимает входные данные произвольного размера и преобразует их в битовую строку фиксированного размера. Криптографические хеш-функции имеют ряд дополнительных свойств:

1) стойкость к коллизиям — трудно найти два сообщения a и b, для которых будет верным $H(a) = H(b)$;
2) сопротивление поиску первого прообраза — для выходной строки h должно быть сложно найти a такое, что $H(a) = h$;
3) сопротивление поиску второго прообраза — для заданного сообщения a и строки $y = H(a)$ трудно найти второе сообщение b такое, что $H(b) = y$.

В блокчейн криптографические хеш-функции используются для: генерации открытых и закрытых ключей; в дайджестах сообщений в подписи; решения криптографических головоломок (Proof of work, POW в Bitcoin). Например, в Bitcoin хеш-функцией для сообщения x является SHA256d (SHA256 выполняется дважды).

$$\mathrm{SHA256d}(x) = \mathrm{SHA256}(\mathrm{SHA256}(x)).$$

Блокчейн и облачные вычисления

Облачные вычисления (Cloud computing) привлекли огромное внимание благодаря своей вычислительной мощности и объемам хранилища данных, в результате чего проведен ряд исследований, и произведена их интеграция в мобильные сети 5G [12, 13]. Однако в эпоху мобильных сетей 5G массовый трафик данных, переданный от устройств IoT в облако, приводит к ряду новых проблем безопасности, касающихся управления конфиденциальностью данных и обеспечения их целостности [14]. В настоящее время сервисы в облаке предоставляются и управляются централизованно. Тем не менее, такая конфигурация уязвима для одноточечных сбоев, которые создают угрозу для облачных сервисов с точки зрения доступа пользователей по требованию. Более того, стоит обратить внимание на проблемы, связанные с конфиденциальностью пользовательских данных, учитывая большой объем разнородных данных в мобильных сетях 5G, которые собираются, передаются, хранятся и используются в облачных сервисах. Фактически, пользователи IoT часто доверяют облачным провайдерам, которые управляют приложениями, и при этом очень мало знают о том, как передаются данные, и кто в настоящее время использует их информацию [15]. Отметим также, что даже в концепции распределенного облака с несколькими серверами данные распределяются не полностью, а хранятся в некоторых центрах обработки данных с высокой плотностью [16]. В этом случае может возникнуть утечка огромного количества разнородных данных и нарушение конфиденциальности пользователей в случае атаки на один из облачных серверов.

В традиционных облачных системах поставщики ресурсов имеют полный контроль над внешними сетевыми данными, тогда как пользователи не знают об этом и не имеют возможности отслеживать данные после выгрузки в облако. Это ставит перед пользователями задачу по проверке и мониторингу потоков или использования данных, особенно в сценариях мобильных сетей 5G, где среди участников сетей крайне необходима прозрачность. Для эффективного решения вышеуказанных проблем безопасности в облачных вычислениях мобильных сетей 5G можно интегрировать блокчейн. В некоторых работах уже рассматривалось использование блокчейн с целью повышения надежности и безопасности внешних сетей 5G в сценариях управления доступом [17]. Блокчейн необходим для построения платформы верификации между устройствами IoT, устройством BBU (Battery Backup Unit) и производителем, где информация о доступе

[1] Как технология 5G изменит мир [Электронный ресурс]. Режим доступа: https://bb.lv/statja/lifenews/2020/04/13/kak-tehnologiya-5g-izmenit-mir, свободный. Яз. рус. (дата обращения: 24.05.2020).

[2] China Telecom внедряет блокчейн в системы 5G [Электронный ресурс]. Режим доступа: https://bits.media/china-telecom-vnedryaet-blokcheyn-v-sistemy-5g/, свободный. Яз. рус. (дата обращения: 24.05.2020).

пользователя хранится в цепочке блоков неизменным образом, а умные контракты используются для выполнения автоматической аутентификации пользователя. В другом исследовании была предложена облачно-ориентированная среда IoT, включающая в себя умные контракты и блокчейн для безопасной проверки происхождения данных [18]. Объединение блокчейн с облачными вычислениями позволяет создать комплексную сеть безопасности, в которой метаданные (криптографический хеш) хранятся в блокчейн, а фактические данные — в облачном хранилище, что делает его легко масштабируемым и обеспечивает высокую достоверность данных.

Блокчейн и граничные вычисления

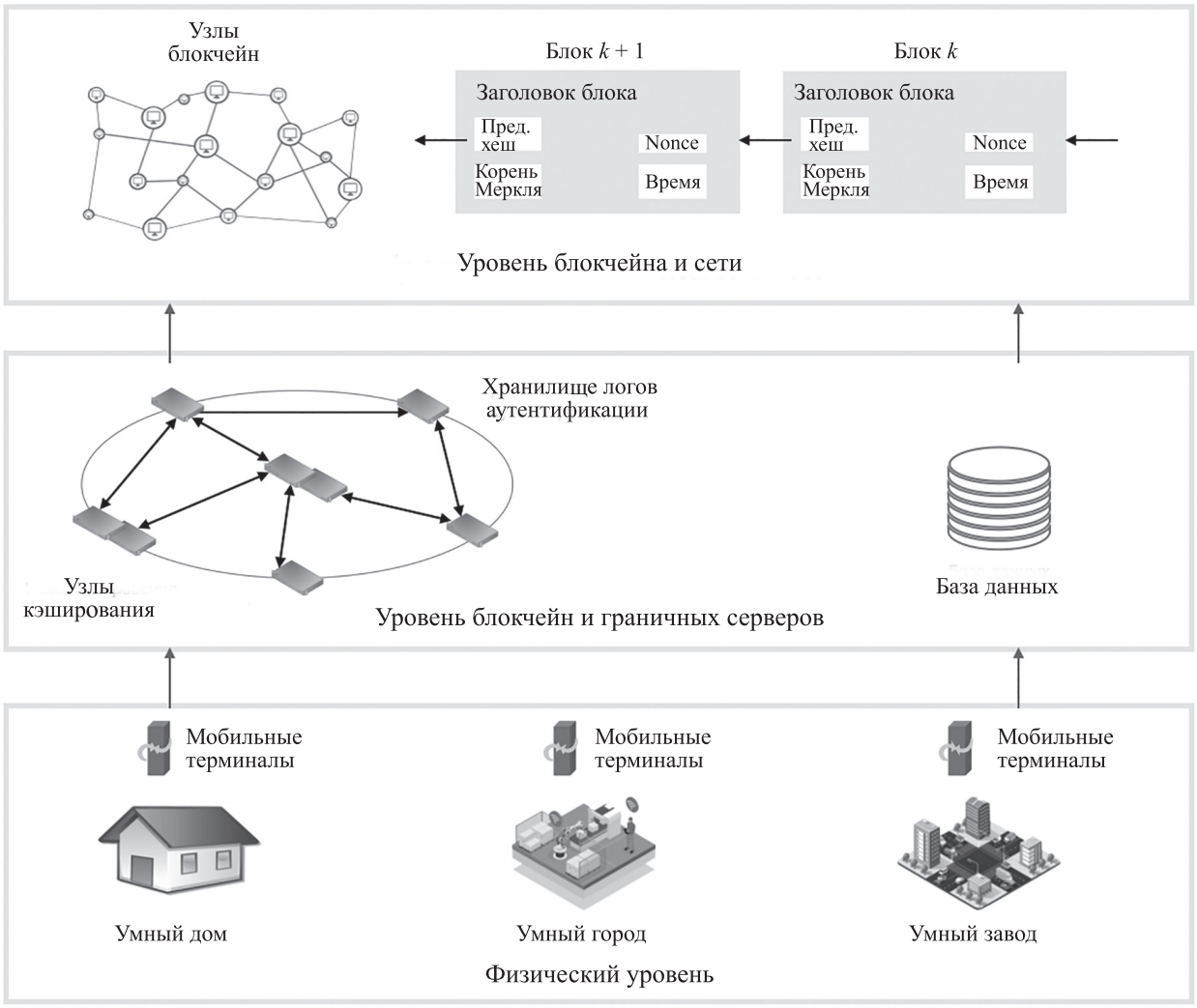
Граничные вычисления (Multi-access Edge Computing, MEC) стали перспективной технологией для расширения возможностей услуг 5G. Подобно концепции облачных вычислений, граничные вычисления могут предоставлять ряд сервисов с возможностью обработки и хранения данных, поддержки неоднородности и улучшения качества обслуживания. Несмотря на то, что фактически периферийные серверы менее мощны, чем удаленные облачные серверы, они расположены на границе сети в непосредственной близости от устройств IoT, что обеспечивает высокоэффективную обработку данных 5G с гораздо меньшей задержкой передачи по сравнению с удаленным облачным сервером [19]. Распределенная структура граничных вычислений потенциально приносит многочисленные преимущества, от повсеместных вычислительных сервисов, и улучшения масштабируемости до уменьшения сложности управления сетью, чтобы справиться с ростом количества устройств IoT и быстрым ростом требований к услугам мобильных сетей 5G [20]. Несмотря на это, безопасность данной технологии является серьезной проблемой, так как обработка данных в динамических граничных вычислительных средах может быть уязвимой для атак злоумышленников [21, 22]. Кроме того, информация о настройке и конфигурации, предоставляемая поставщиками услуг граничных вычислений, должна быть надежной и безопасной, но на самом деле эти факторы подвергаются сомнению из-за высокой динамичности и открытости системы. Предотвращение нарушений работы системы, вызванных атакой на граничный узел в многоканальных вычислениях, является первостепенной задачей для сетей граничных вычислений на основе 5G.

Блокчейн стал многообещающей технологией, позволяющей решить большинство проблем в области безопасности сетей, с которыми сталкиваются существующие архитектуры передовых вычислений. Одно и то же свойство как блокчейн, так и MEC, построенного на сетях, хранилищах, вычислениях и связи, делает их сочетание естественным. Результаты последних исследований показали, что блокчейн можно применять к граничным вычислительным системам для поддержки ряда служб безопасности и управления в граничных вычислениях [23]. Блокчейн может поддерживать услуги сетей 5G на основе граничных вычислений в трех основных аспектах: создание сетей, хранение данных и вычислительные процессы, как показано на рис. 1.

С помощью блокчейн можно оптимизировать сетевые возможности MEC. Блокчейн может использоваться для построения распределенной и надежной системы аутентификации с целью обеспечения аутентификации и обмена информацией между различными IoT-платформами на основе граничных вычислений [24]. Данные аутентификации и информация о доступе пользователей могут безопасно храниться в цепочке блоков, которая также способна автоматически отслеживать действия мобильных терминалов (устройств) без необходимости в централизованном сервере управления. В некоторых работах можно найти описание архитектуры системы на основе блокчейн для граничных вычислений с целью предотвращения утечки пользовательской информации при совместной работе за счет создания безопасного канала связи и постоянной регистрации транзакций [25, 26]. Функциональность блокчейн также может применяться для управления ресурсами и их распределения, что повышает производительность граничных вычислений, гарантируя при этом безопасность сети [27, 28]. Блокчейн также обеспечивает функции безопасности с целью эффективного хранения данных для граничных вычислительных систем за счет децентрализованного хранилища данных, обеспечиваемого объединенной емкостью сети одноранговых узлов для хранения и обмена контентом. В одном из исследований была предложена основанная на MEC система совместного использования ресурсов с использованием блокчейн и автономной структуры для хранения неизменяемых данных [29]. Наконец, блокчейн может поддерживать вычислительные процессы в сетях MEC и обеспечить возможность аутентификации для защиты систем на основе MEC. С помощью блокчейн можно создать уровень аутентификации между граничными серверами и устройствами IoT для защиты от внешних атак [30]. Таким образом, блокчейн может обеспечить прозрачность, конфиденциальность и безопасность данных в граничных вычислениях мобильных сетей 5G.

Блокчейн и программно-определяемые сети

Программно-определяемая сеть (Software-Defined Network, SDN) — это интеллектуальная сетевая архитектура, которая призвана улучшить управляемость и гибкость сетей. Основной концепцией SDN является разделение плоскости управления вне сетевых коммутаторов и обеспечение внешнего управления данными через логический программный контроллер, обеспечивающий взаимный доступ между различными частями гетерогенных сетей [31]. Эта архитектура проектирования не только предлагает ряд новых вариантов архитектуры, управления и эксплуатации, но также предоставляет возможность эффективной доставки пользовательских услуг при более эффективном использовании сетевых ресурсов. В контексте 5G SDN разработан для того, чтобы сделать услуги связи, предоставляемые сетями 5G, программируемыми, где потоками трафика можно динамически управлять



k — номер блока
Nonce — число, которое может быть использовано один раз

Рис. 1. Интеграция блокчейн и граничных вычислений для услуг 5G

для достижения максимальной производительности. Однако, несмотря на очевидные преимущества этой технологии, существует ряд нетривиальных проблем, а именно: безопасность, гибкость и масштабируемость. Одним из основных свойств архитектуры SDN является разбиение плоскости управления и плоскости данных, что, в свою очередь, также расширяет поверхность атаки сети и создает возможности атаки для прикладного уровня [32]. Кроме того, централизованная архитектура контроллера SDN также уязвима для атак на уровне управления, что может привести к злонамеренному изменению контроллеров, маршрутизаторов и коммутаторов, генерации и потере данных таблицы потоков [33].

В то же время существует ряд нерешенных вопросов, например, каким образом масштабировать сети SDN, чтобы позволить нескольким контроллерам SDN взаимодействовать друг с другом, при этом обеспечивая безопасный обмен информацией между ними? За счет распределенной сетевой архитектуры поставщики услуг SDN не только могут снизить затраты и повысить гибкость для расширения сети, но также развернуть новые сервисы для удовлетворения новых требований рынка [34]. Концепция централизованной архитектуры SDN уязвима к риску единичного отказа в том случае, когда сетевой объект подвергается атаке или скомпрометирован, что приводит к нарушению работы всей сети. Следовательно, разработка децентрализованной архитектуры SDN, которая может решить эту проблему и улучшить качество услуг, является жизненно необходимой. В средах с несколькими сетями SDN устройства могут быть несовместимыми и не иметь возможности обеспечивать взаимодействие и совместную работу из-за строгих требований к задержке от различных поставщиков услуг 5G. Для использования сетевых ресурсов требуется централизованное хранилище, поддерживаемое всеми сторонами для поставщика услуг, но сложно достичь взаимного доверия между поставщиками и справедливости в плане распределения ресурсов из-за потенциальных конфликтов интересов поставщиков услуг. Как добиться надежного и эффективного взаимодействия сетей с несколькими SDN и обеспечить надежное совместное использование ресурсов?

Многие исследования были посвящены исследованию блокчейн как децентрализованного решения обеспечения безопасности для SDN. Блокчейн можно использовать в качестве механизма аутентификации для сетей 5G на основе SDN с целью устранения ненужной повторной аутентификации при повторной передаче обслуживания между гетерогенными сотами [35]. Множество контроллеров SDN в этом предлагаемом подходе могут связываться друг с другом и взаимодействовать с блокчейн, который обеспечивает безопасный обмен информацией между ними. Транзакции и сообщения из блокчейн могут передаваться через выделенные ключи передачи контроллеру. Каждый контроллер SDN имеет выделенный ключ, полученный из цепочки блоков, и который применяется для передачи и получения информации. В свою очередь проблема масштабируемости может быть эффективно решена с помощью иерархической структуры на основе блокчейн. В случае, если какой-либо контроллер SDN выйдет из строя в ячейке, система будет управлять этой ячейкой, используя другой контроллер SDN в сети, где консенсус между кандидатами в контроллеры SDN может быть достигнут с помощью блокчейн. Таким образом, интеграция блокчейн в SDN позволяет удалить посредников для аутентификации, снизить операционные издержки и обеспечить глобальную доступность сервисов для всех пользователей.

Блокчейн и виртуализация сетевых функций

Виртуализация сетевых функций (NFV) — это концепция сетевой архитектуры, стандартизированная Европейским институтом телекоммуникационных стандартов (ETSI), в которой используется стандартное оборудование для размещения различных независимых сетевых программных компонентов [36]. Согласно спецификации, разработанной ETSI, структура NFV-домена представляет собой систему из компонентов трех типов: виртуализованных сетевых функций (Virtualised Network Function, VNF), NFV-инфраструктуры (Network Function Virtualisation Infrastructure, NFVI), средств управления NFV-системой и оркестрации команд (NFV Management and Orchestration, MANO) [37]. NFV фактически реализует сетевые функции (NF), отделяя аппаратные устройства (такие как брандмауэры, шлюзы) от функций, которые на них выполняются, чтобы предоставить виртуализированные шлюзы, виртуализированные брандмауэры и даже виртуализированные компоненты сети, обеспечивая гибкие сетевые функции. Таким образом, сетевые операторы могут значительно сэкономить на оборудовании и снизить накладные расходы, а также автоматизировать работу сети, не заботясь об установке оборудования. В частности, NFV содержит ряд преимуществ для мобильных сетей 5G, среди которых — повышение гибкости и масштабируемость соединений NF благодаря отделению программного обеспечения от аппаратного [38].

Однако NFV также сталкивается с новыми проблемами безопасности [39, 40]:

1) в случае участия нескольких облачных провайдеров в одной NFV-среде для предоставления услуг данные могут быть скомпрометированы и злоумышленниками, что приводит к утечке информации [41];
2) в случае использования арендаторами одной и той же облачной инфраструктуры возрастает вероятность атак внутри облака;
3) при использовании протоколов оркестрации для миграции виртуальных машин и распределения ресурсов требуется обеспечить безопасность связи между оркестратором и физическими машинами.

На самом деле данная архитектура очень чувствительна к атакам с разных горизонтов. Фактически злоумышленник может создать виртуальную машину для работы на сервере и использовать ее для внешних атак типа «отказ в обслуживании».

В таком контексте блокчейн стал эффективным инструментом для решения этих проблем [42, 43].

Во-первых, блокчейн может обеспечить безопасное управление операциями оркестрации цепочки сервисных функций в открытой платформе для виртуализации сетевых функций (OPNFV) [44]. Архитектура данного решения изображена на рис. 2 и состоит из трех основных модулей:

1) визуализации, который обеспечивает интерфейс между арендаторами, службами NFV и Service Function Chaining (SFC);
2) оркестрации, который выполняет инструкции, переданные арендаторами через модуль визуализации;
3) блокчейн, который проверяет и подтверждает транзакции перед выполнением модулем оркестрации.

За счет регистрации всех инструкций, которые управляют сервисными цепочками, предложенная схема может гарантировать подлинность, целостность и невозвратимость инструкций в многопользовательской и многодоменной среде NFV.

Во-вторых, на основе блокчейн можно предложить структуру виртуальной аутентификации виртуальных машин (VMOA) с целью защиты операций NFV для аутентификации команд оркестрации в жизненном цикле облачных сервисов [45]. Благодаря устранению требования третьих сторон в VMOA и безопасности блокчейн, предлагаемое решение потенциально достигает преимуществ, таких как целостность записей, отказоустойчивость и надежность сети, по сравнению с его централизованными аналогами.

В-третьих, за счет использования умных контрактов можно обеспечить безопасность управления сетевыми срезами и операциями по конфигурации VNF [46]. Таким образом, блокчейн представляет собой эффективный подход для создания уровня аутентификации для служб управления и оркестрации NFV (MANO) в административных доменах.

Блокчейн и 5G-слайсинг

С целью поддержки различных типов приложений IoT, мобильные сети 5G опираются на концепцию сетевого разделения (5G-слайсинг), которая заключается в разделении нескольких виртуальных сетей, работающих на одном физическом оборудовании [47]. Такой подход позволяет операторам связи разделять свои сети на конкретные услуги и приложения, такие как «умный

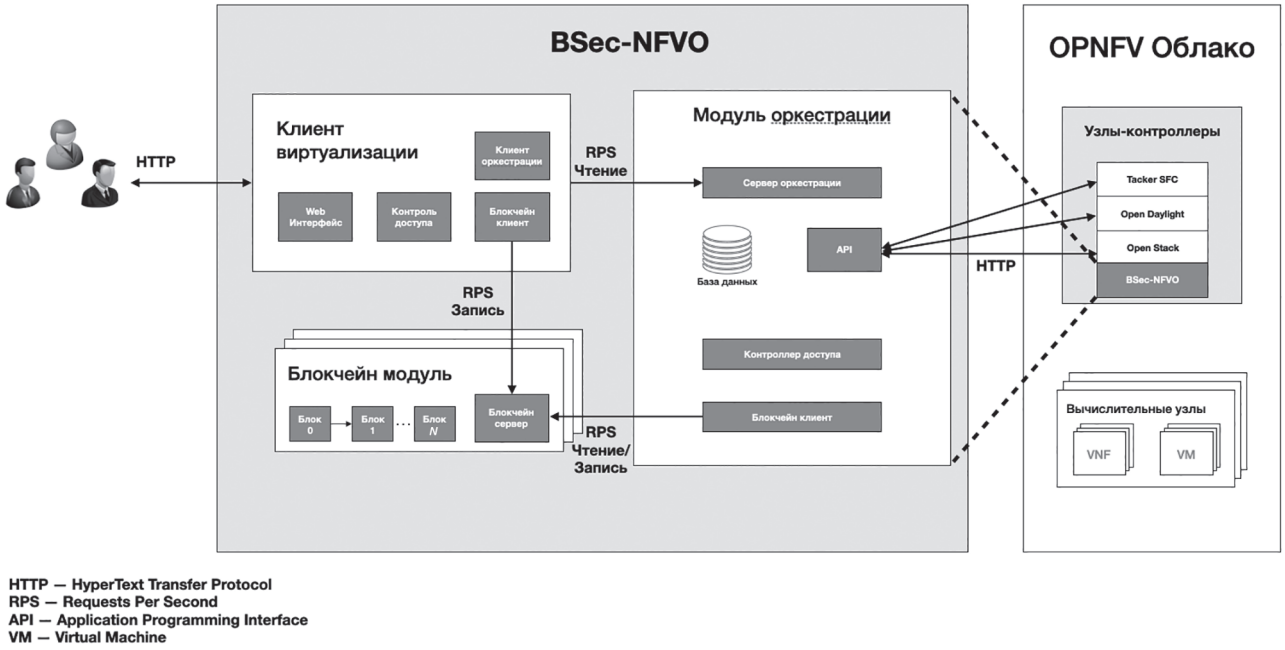


Рис. 2. Концепция архитектуры NFV на основе блокчейн

дом», «умный завод» и т. д., но в то же время добавляет угрозы безопасности между слоями (слайсами) и проблемы гармонизации ресурсов между сегментами доменов [48, 49]. Например, при совместном использовании экземпляров сетевого сегмента в открытых облачных архитектурах злоумышленники могут злоупотреблять эластичностью емкости одного слайса, чтобы использовать ресурсы другого целевого слайса, что делает его недоступным. Кроме того, поскольку множественные слайсы часто имеют общие функции плоскости управления, злоумышленники могут использовать эту слабость сети для компрометации данных целевого среза путем злонамеренного доступа к общим функциям из другого среза, что приводит к утечке данных и нарушению целостности системы [50].

Блокчейн может быть использован для создания надежных сквозных сетевых срезов (слайсов), что позволит их провайдерам управлять своими ресурсами. Для гарантии безопасных транзакций между провайдером сетевых срезов и поставщиком ресурсов для услуг 5G блокчейн используется для создания механизма посредничества в сетевой секции [51]. На рис. 3 показана схема торговли сетевыми срезами за счет использования блокчейн и умных контрактов [52–54]. Блокчейн поддерживает микропроцессы по конфигурации ресурса с использованием брокера срезов сети 5G в промышленной автоматизации и в интеллектуальных сетях. Производственное оборудование самостоятельно арендует сетевой сегмент, необходимый для операций по требованию, утверждает соглашение об уровне обслуживания (SLA) и оплачивает плату за обслуживание на основе фактического использования. В некоторых работах можно найти архитектуру беспроводной виртуализации на основе цепочки блоков, в которой беспроводные ресурсы, такие как радиочастотные каналы, делятся на несколько слайсов (n) для операторов мобильных виртуальных сетей (MVNO) [55]. Каждая транзакция в блокчейн для беспроводной виртуализации содержит информацию о распределении полосы пропускания, максимальной мощности канала и скорости передачи данных, которые используются MVNO при обслуживании своих пользователей. Таким образом, распределенная схема на основе цепочки блоков надежно создает новые MVNO, не раскрывая их приватную информацию широкой публике.

Блокчейн и прямое взаимодействие устройств

Прямое взаимодействие устройств (D2D) — технология, которая позволяет мобильным устройствам (таким как смартфон, планшет и т. д.) напрямую связываться друг с другом без участия точки доступа или базовой станции сотовой инфраструктуры. D2D использует преимущества близости устройства связи для эффективного использования доступных ресурсов, что позволяет повысить общую пропускную способность системы, уменьшить задержки связи, снизить потребление энергии и нагрузку на трафик [56]. Однако прямая связь между мобильными устройствами также создает новые нетривиальные проблемы для мобильных сетей 5G на основе D2D с точки зрения безопасности, управления и производительности. Важной задачей является обеспечение безопасности при обмене данными между устройствами с целью низкой задержки [57]. При отсутствии в сети механизма аутентификации устройства D2D могут получить незаконный доступ к ресурсам на облачных и граничных серверах. Кроме того, существующие архитектуры D2D полагаются на внешние полномочия для предоставления разрешения на данные и запроса аутентификации во время обмена данными D2D, что может привести к ненужной задержке связи и ухудшить общую производительность сети [58].

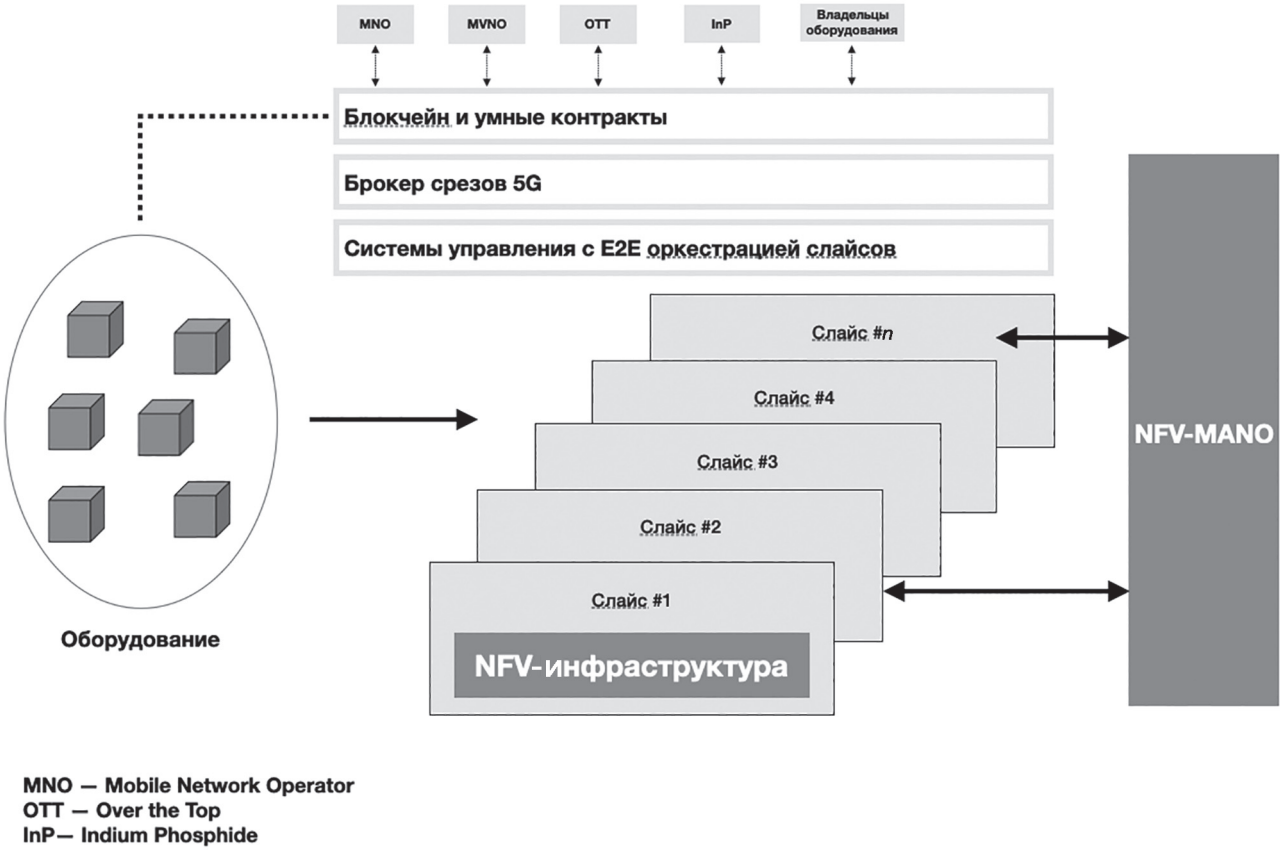


Рис. 3. Схема торговли сетевыми срезами на основе блокчейн

Блокчейн позволяет преодолеть вышеописанные трудности в мобильных сетях 5G. В качестве примера можно привести использование блокчейн для построения безопасной схемы обмена контентом среди мобильных устройств в режиме D2D [59]. Для снижения нагрузки на вычислительные устройства, граничные серверы с высокой вычислительной мощностью используются для запуска задач майнинга для блокчейн. В частности, блокчейн демонстрирует свою эффективность в предоставлении стимулирующего решения, которое поощряет пользователей с поддержкой кэширования хранить и обмениваться контентом с другими мобильными устройствами путем D2D-взаимодействия. Политика награждения, обеспечиваемая блокчейн, стимулирует процесс майнинга в устройствах D2D, повышая надежность и безопасность сети D2D. В частности, блокчейн и умные контракты можно использовать для разработки торгового приложения между продавцом и покупателем посредством D2D-взаимодействия [60]. Торговля может осуществляться автоматически путем запуска умного контракта, что обеспечивает прозрачный и надежный обмен данными между различными пользователями. Блокчейн также можно рассмотреть для построения распределенной защищенной системы мониторинга в сетях с использованием D2D-взаимодействия с целью обеспечения высокого уровня безопасности при сниженных накладных расходах [61]. В частности, защищенное управление доступом с использованием блокчейн также интегрировано для поддержки аутентификации личности.

Выводы (Резюме)

Интеграция блокчейн с мобильными сетями 5G — актуальная тема для исследований [62]. Проанализировав исследовательские работы, можно обнаружить, что блокчейн может хорошо поддерживать технологии 5G в трех ключевых аспектах: безопасность, производительность системы и управление ресурсами. Результат анализа приведен в таблице. Например, концепции облачных вычислений и MEC на основе блокчейн позволяют децентрализовать облачные/граничные сети 5G, что избавляет от централизованного управления в базовой сети и предлагает децентрализованное честное соглашение с блокчейн. Даже когда сущность скомпрометирована злонамеренными атаками или угрозами, общая работа задействованной сети все еще поддерживается посредством консенсуса по распределенным реестрам. В SDN использование блокчейн как повышает безопасность благодаря удалению посредников для аутентификации, так и снижает операционные издержки. Блокчейн также позволяет эффективно и безопасно управлять ресурсами при NFV и 5G-слайсинге за счет умных контрактов. Стоит отметить, что блокчейн также может помочь установить безопасную прямую связь между пользователями (в режиме D2D), используя вычислительную мощность всех участников для управления сетью вместо стороннего посредника. Это потенциально может уменьшить задержку соединения между устройствами и обеспечить глобальную доступность для всех пользователей.

Таблица. Возможность поддержки блокчейн технологиями 5G по трем ключевым аспектам

Технология	Безопасность	Производительность системы	Управление ресурсами
Облачные вычисления	+	–	–
Граничные вычисления (MEC)	+	–	–
Программно-определяемые сети (SDN)	+	+	–
Виртуализация сетевых функций (NFV)	+	–	+
5G-слайсинг	+	–	+
Прямое взаимодействие устройств (D2D)	+	+	–

(+) – поддержка технологии

Заключение

Всесторонний обзор исследовательских работ по интеграции блокчейн в мобильные сети 5G позволяет выявить много важных результатов, которые позволили бы в дальнейшем открыть многочисленные возможности для вновь возникающих сценариев 5G. В данной статье представлен обзор последних достижений в области применения блокчейн в мобильных сетях 5G. Подробно рассмотрена интеграция блокчейн в ключевые технологии сетей 5G, а именно: облачные вычисления, граничные вычисления, программно-определяемые сети, виртуализацию сетевых функций, 5G-слайсинг и прямое взаимодействие устройств. Благодаря своим многообещающим свойствам блокчейн позволяет предоставить новый набор инновационных решений для сетей и услуг 5G с целью повышения безопасности, конфиденциальности, децентрализации и преобразования архитектур управления сетью для улучшения качества обслуживания. Следовательно, в технологиях 5G нужно использовать преимущества блокчейн для обеспечения гибкости и безопасности при предоставлении услуг мобильной связи и повсеместного охвата.

Литература

1. Agiwal M., Roy A., Saxena N. Next generation 5G wireless networks: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2016. V. 18. N 3. P. 1617–1655. doi: 10.1109/COMST.2016.2532458
2. Panwar N., Sharma S., Singh A.K. A survey on 5G: The next generation of mobile communication // Physical Communication. 2016. V. 18. P. 64–84. doi: 10.1016/j.phycom.2015.10.006
3. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the internet of things // IEEE Access. 2016. V. 4. P. 2292–2303. doi: 10.1109/ACCESS.2016.2566339
4. Zheng Z., Xie S., Dai H., Chen X., Wang H. An overview of blockchain technology: Architecture, consensus, and future trends // Proc. 6th IEEE International Congress on Big Data (BigData Congress). 2017. P. 557–564.
5. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008.
6. Haber S., Stornetta W.S. How to time-stamp a digital document // Journal of Cryptology. 1991. V. 3. N 2. P. 99–111. doi: 10.1007/BF00196791
7. Wang X., Zha X., Ni W., Liu R.P., Guo Y.J., Niu X., Zheng K. Survey on blockchain for Internet of Things // Computer Communications. 2019. V. 136. P. 10–29. doi: 10.1016/j.comcom.2019.01.006
8. Ali M.S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M.H. Applications of blockchains in the Internet of Things: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2019. V. 21. N 2. P. 1676–1717. doi: 10.1109/COMST.2018.2886932
9. Xie J., Tang H., Huang T., Yu F.R., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges // IEEE Communications Surveys & Tutorials. 2019. V. 21. N 3. P. 2794–2830. doi: 10.1109/COMST.2019.2899617
10. Jiang T., Fang H., Wang H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis // IEEE Internet of Things Journal. 2019. V. 6. N 3. P. 4640–4649. doi: 10.1109/JIOT.2018.2874398
11. Rabah K. Overview of blockchain as the engine of the 4th industrial revolution // Mara Research Journal of Business & Management. 2017. V. 1. N 1. P. 125–135.
12. Wübben D., Rost P., Bartelt J., Lalam M., Savin V., Gorgoglione M., Dekorsy A., Fettweis G. Benefits and impact of cloud computing on 5G signal processing: Flexible centralization through cloud-RAN // IEEE Signal Processing Magazine. 2014. V. 31. N 6. P. 35–44. doi: 10.1109/MSP.2014.2334952

References

1. Agiwal M., Roy A., Saxena N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 3, pp. 1617–1655. doi: 10.1109/COMST.2016.2532458
2. Panwar N., Sharma S., Singh A.K. A survey on 5G: The next generation of mobile communication. *Physical Communication*, 2016, vol. 18, pp. 64–84. doi: 10.1016/j.phycom.2015.10.006
3. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the internet of things. *IEEE Access*, 2016, vol. 4, pp. 2292–2303. doi: 10.1109/ACCESS.2016.2566339
4. Zheng Z., Xie S., Dai H., Chen X., Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. *Proc. 6th IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.
5. Nakamoto S. Bitcoin: *A peer-to-peer electronic cash system*, 2008.
6. Haber S., Stornetta W.S. How to time-stamp a digital document. *Journal of Cryptology*, 1991, vol. 3, no. 2, pp. 99–111. doi: 10.1007/BF00196791
7. Wang X., Zha X., Ni W., Liu R.P., Guo Y.J., Niu X., Zheng K. Survey on blockchain for Internet of Things. *Computer Communications*, 2019, vol. 136, pp. 10–29. doi: 10.1016/j.comcom.2019.01.006
8. Ali M.S., Vecchio M., Pincheira M., Dolui K., Antonelli F., Rehmani M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, no. 2, pp. 1676–1717. doi: 10.1109/COMST.2018.2886932
9. Xie J., Tang H., Huang T., Yu F.R., Xie R., Liu J., Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, no. 3, pp. 2794–2830. doi: 10.1109/COMST.2019.2899617
10. Jiang T., Fang H., Wang H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet of Things Journal*, 2019, vol. 6, no. 3, pp. 4640–4649. doi: 10.1109/JIOT.2018.2874398
11. Rabah K. Overview of blockchain as the engine of the 4th industrial revolution. *Mara Research Journal of Business & Management*, 2017, vol. 1, no. 1, pp. 125–135.
12. Wübben D., Rost P., Bartelt J., Lalam M., Savin V., Gorgoglione M., Dekorsy A., Fettweis G. Benefits and impact of cloud computing on 5G signal processing: Flexible centralization through cloud-RAN. *IEEE Signal Processing Magazine*, 2014, vol. 31, no. 6, pp. 35–44. doi: 10.1109/MSP.2014.2334952

13. Chen M., Zhang Y., Li Y., Mao S., Leung V.C. EMC: Emotion-aware mobile cloud computing in 5G // IEEE Network. 2015. V. 29. N 2. P. 32–38. doi: 10.1109/MNET.2015.7064900
14. Zhou J., Cao Z., Dong X., Vasilakos A.V. Security and privacy for cloud-based IoT: Challenges // IEEE Communications Magazine. 2017. V. 55. N 1. P. 26–33. doi: 10.1109/MCOM.2017.1600363CM
15. Li J., Wu J., Chen L. Block-secure: Blockchain based scheme for secure P2P cloud storage // Information Sciences. 2018. V. 465. P. 219–231. doi: 10.1016/j.ins.2018.06.071
16. Yang M., Margheri A., Hu R., Sassone V. Differentially private data sharing in a cloud federation with blockchain // IEEE Cloud Computing. 2018. V. 5. N 6. P. 69–79. doi: 10.1109/MCC.2018.064181122
17. Yang H., Wu Y., Zhang J., Zheng H., Ji Y., Lee Y. BlockONet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul // Proc. Optical Fiber Communications Conference and Exposition (OFC 2018). 2018. P. 1–3. doi: 10.1364/ofc.2018.w2a.25
18. Ali S., Wang G., Bhuiyan M.Z.A., Jiang H. Secure data provenance in cloud-centric internet of things via blockchain smart contracts // Proc. 4th IEEE SmartWorld, 15th IEEE International Conference on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovations, SmartWorld/UIC/ATC/ScalCom/CBDCom/IoP/SCI. 2018. P. 991–998. doi: 10.1109/SmartWorld.2018.00175
19. Taleb T., Samdanis K., Mada B., Flinck H., Dutta S., Sabella D. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration // IEEE Communications Surveys & Tutorials. 2017. V. 19. N 3. P. 1657–1681. doi: 10.1109/COMST.2017.2705720
20. Pham Q.-V., Fang F., Ha V.N., Piran J., Le M., Le L.B., Hwang W.-J., Ding Z. A Survey of multi-access edge computing in 5G and beyond: fundamentals, technology integration, and state-of-the-art // IEEE Access. 2020. V. 8. P. 116974–117017. doi: 10.1109/ACCESS.2020.3001277
21. Mukherjee M., Matam R., Shu L., Maglaras L., Ferrag M.A., Choudhury N., Kumar V. Security and privacy in fog computing: Challenges // IEEE Access. 2017. V. 5. P. 19293–19304. doi: 10.1109/ACCESS.2017.2749422
22. Zhang J., Chen B., Zhao Y., Cheng X., Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues // IEEE Access. 2018. V. 6. P. 18209–18237. doi: 10.1109/ACCESS.2018.2820162
23. Stanciu A. Blockchain based distributed control system for edge computing // Proc. 21st International Conference on Control Systems and Computer Science (CSCS). 2017. P. 667–671. doi: 10.1109/CSCS.2017.102
24. Guo S., Hu X., Guo S., Qiu X., Qi F. Blockchain meets edge computing: A distributed and trusted authentication system // IEEE Transactions on Industrial Informatics. 2020. V. 16. N 3. P. 1972–1983. doi: 10.1109/TII.2019.2938001
25. Liu H., Zhang Y., Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing // IEEE Network. 2018. V. 32. N 3. P. 78–83. doi: 10.1109/MNET.2018.1700344
26. Li M., Zhu L., Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing // IEEE Internet of Things Journal. 2019. V. 6. N 3. P. 4573–4584. doi: 10.1109/JIOT.2018.2868076
27. Qiao G., Leng S., Chai H., Asadi A., Zhang Y. Blockchain empowered resource trading in mobile edge computing and networks // Proc. IEEE International Conference on Communications (ICC 2019). 2019. P. 8761664. doi: 10.1109/ICC.2019.8761664
28. Zheng X., Mukkamala R.R., Vatrapu R., Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage // Proc. 20th International Conference on e-Health Networking, Applications and Services (Healthcom). 2018. P. 1–6. doi: 10.1109/HealthCom.2018.8531125
29. Rahman M.A., Rashid M.M., Hossain M.S., Hassanain E., Alhamid M.F., Guizani M. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city // IEEE Access. 2019. V. 7. P. 18611–18621. doi: 10.1109/ACCESS.2019.2896065
30. Tang W., Zhao X., Rafique W., Dou W. A blockchain-based offloading approach in fog computing environment // Proc. 16th IEEE International Symposium on Parallel and Distributed Processing with Applications, 17th IEEE International Conference on Ubiquitous Computing and Communications, 8th IEEE International Conference on Big Data and Cloud Computing, 11th IEEE International Conference on Social Computing and Networking and 8th IEEE

13. Chen M., Zhang Y., Li Y., Mao S., Leung V.C. EMC: Emotion-aware mobile cloud computing in 5G. *IEEE Network*, 2015, vol. 29, no 2, pp. 32–38. doi: 10.1109/MNET.2015.7064900
14. Zhou J., Cao Z., Dong X., Vasilakos A.V. Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, 2017, vol. 55, no. 1, pp. 26–33. doi: 10.1109/MCOM.2017.1600363CM
15. Li J., Wu J., Chen L. Block-secure: Blockchain based scheme for secure P2P cloud storage. *Information Sciences*, 2018, vol. 465, pp. 219–231. doi: 10.1016/j.ins.2018.06.071
16. Yang M., Margheri A., Hu R., Sassone V. Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud Computing*, 2018, vol. 5, no. 6, pp. 69–79. doi: 10.1109/MCC.2018.064181122
17. Yang H., Wu Y., Zhang J., Zheng H., Ji Y., Lee Y. BlockONet: blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul. *Proc. Optical Fiber Communications Conference and Exposition (OFC 2018)*, 2018, pp. 1–3. doi: 10.1364/ofc.2018.w2a.25
18. Ali S., Wang G., Bhuiyan M.Z.A., Jiang H. Secure data provenance in cloud-centric internet of things via blockchain smart contracts. *Proc. 4th IEEE SmartWorld, 15th IEEE International Conference on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovations, SmartWorld/UIC/ATC/ScalCom/CBDCom/IoP/SCI*, 2018, pp. 991–998. doi: 10.1109/SmartWorld.2018.00175
19. Taleb T., Samdanis K., Mada B., Flinck H., Dutta S., Sabella D. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Communications Surveys & Tutorials*, 2017, vol. 19, no. 3, pp. 1657–1681. doi: 10.1109/COMST.2017.2705720
20. Pham Q.-V., Fang F., Ha V.N., Piran J., Le M., Le L.B., Hwang W.-J., Ding Z. A Survey of multi-access edge computing in 5G and beyond: fundamentals, technology integration, and state-of-the-art. *IEEE Access*, 2020, vol. 8, pp. 116974–117017. doi: 10.1109/ACCESS.2020.3001277
21. Mukherjee M., Matam R., Shu L., Maglaras L., Ferrag M.A., Choudhury N., Kumar V. Security and privacy in fog computing: Challenges. *IEEE Access*, 2017, vol. 5, pp. 19293–19304. doi: 10.1109/ACCESS.2017.2749422
22. Zhang J., Chen B., Zhao Y., Cheng X., Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access*, 2018, vol. 6, pp. 18209–18237. doi: 10.1109/ACCESS.2018.2820162
23. Stanciu A. Blockchain based distributed control system for edge computing. *Proc. 21st International Conference on Control Systems and Computer Science (CSCS)*, 2017, pp. 667–671. doi: 10.1109/CSCS.2017.102
24. Guo S., Hu X., Guo S., Qiu X., Qi F. Blockchain meets edge computing: A distributed and trusted authentication system. *IEEE Transactions on Industrial Informatics*, 2020, vol. 16, no. 3, pp. 1972–1983. doi: 10.1109/TII.2019.2938001
25. Liu H., Zhang Y., Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network*, 2018, vol. 32, no. 3, pp. 78–83. doi: 10.1109/MNET.2018.1700344
26. Li M., Zhu L., Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet of Things Journal*, 2019, vol. 6, no. 3, pp. 4573–4584. doi: 10.1109/JIOT.2018.2868076
27. Qiao G., Leng S., Chai H., Asadi A., Zhang Y. Blockchain empowered resource trading in mobile edge computing and networks. *Proc. IEEE International Conference on Communications (ICC 2019)*, 2019, pp. 8761664. doi: 10.1109/ICC.2019.8761664
28. Zheng X., Mukkamala R.R., Vatrapu R., Ordieres-Mere J. Blockchain-based personal health data sharing system using cloud storage. *Proc. 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1–6. doi: 10.1109/HealthCom.2018.8531125
29. Rahman M.A., Rashid M.M., Hossain M.S., Hassanain E., Alhamid M.F., Guizani M. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, 2019, vol. 7, pp. 18611–18621. doi: 10.1109/ACCESS.2019.2896065
30. Tang W., Zhao X., Rafique W., Dou W. A blockchain-based offloading approach in fog computing environment. *Proc. 16th IEEE International Symposium on Parallel and Distributed Processing with Applications, 17th IEEE International Conference on Ubiquitous Computing and Communications, 8th IEEE International Conference on Big Data and Cloud Computing, 11th IEEE International Conference on Social Computing and Networking and 8th IEEE*

International Conference on Sustainable Computing and Communications, ISPA/IUCC/BDCloud/SocialCom/SustainCom 2018. 2018. P. 308–315. doi: 10.1109/BDCloud.2018.00056
31. Zaidi Z., Friderikos V., Yousaf Z., Fletcher S., Dohler M., Aghvami H. Will SDN be part of 5G? // IEEE Communications Surveys & Tutorials. 2018. V. 20. N 4. P. 3220–3258. doi: 10.1109/COMST.2018.2836315
32. Bouras C., Kollia A., Papazois A. SDN & NFV in 5G: Advancements and challenges // Proc. 20th Conference on Innovations in Clouds, Internet and Networks (ICIN). 2017. P. 107–111. doi: 10.1109/ICIN.2017.7899398
33. Ahmad I., Namal S., Ylianttila M., Gurtov A. Security in software defined networks: A survey // IEEE Communications Surveys & Tutorials. 2015. V. 17. N 4. P. 2317–2346. doi: 10.1109/COMST.2015.2474118
34. Sharma P.K., Singh S., Jeong Y.-S., Park J.H. DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks // IEEE Communications Magazine. 2017. V. 55. N 9. P. 78–85. doi: 10.1109/MCOM.2017.1700041
35. Yazdinejad A., Parizi R.M., Dehghantanha A., Choo K.-K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks // IEEE Transactions on Network Science and Engineering. 2019. early access. doi: 10.1109/TNSE.2019.2937481
36. Yousaf F.Z., Bredel M., Schaller S., Schneider F. NFV and SDN-key technology enablers for 5G networks // IEEE Journal on Selected Areas in Communications. 2017. V. 35. N 11. P. 2468–2478. doi: 10.1109/JSAC.2017.2760418
37. Mijumbi R., Serrat J., Gorricho J.-L., Bouten N., De Turck F., Boutaba R. Network function virtualization: State-of-the-art and research challenges // IEEE Communications Surveys & Tutorials. 2016. V. 18. N 1. P. 236–262. doi: 10.1109/COMST.2015.2477041
38. Abdelwahab S., Hamdaoui B., Guizani M., Znati T. Network function virtualization in 5G // IEEE Communications Magazine. 2016. V. 54. N 4. P. 84–91. doi: 10.1109/MCOM.2016.7452271
39. Farris I., Taleb T., Khettab Y., Song J. A survey on emerging SDN and NFV security mechanisms for IoT systems // IEEE Communications Surveys & Tutorials. 2019. V. 21. N 1. P. 812–837. doi: 10.1109/COMST.2018.2862350
40. Alwakeel A.M., Alnaim A.K., Fernandez E.B. A survey of network function virtualization security // Proc. SoutheastCon 2018. 2018. P. 8479121. doi: 10.1109/SECON.2018.8479121
41. Reynaud F., Aguessy F.-X., Bettan O., Bouet M., Conan V. Attacks against network functions virtualization and software-defined networking: State-of-the-art // Proc. NetSoft Conference and Workshops. 2016. P. 471–476. doi: 10.1109/NETSOFT.2016.7502487
42. Ak E., Canberk B. BCDN: A proof of concept model for blockchain-aided CDN orchestration and routing // Computer Networks. 2019. V. 161. P. 162–171. doi: 10.1016/j.comnet.2019.06.018
43. Commonalities of Network Function Virtualization, Blockchains and Smart Contracts [Электронный ресурс]. URL: https://files.ifi.uzh.ch/CSG/teaching/FS18/ComSys/Talk9.pdf, свободный. Яз. англ. (дата обращения: 26.05.2020).
44. Rebello G.A.F., Alvarenga I.D., Sanz I.J., Duarte O.C.M. BSec-NFVO: A blockchain-based security for network function virtualization orchestration // Proc. IEEE International Conference on Communications (ICC 2019). 2019. P. 8761651. doi: 10.1109/ICC.2019.8761651
45. Bozic N., Pujolle G., Secci S. Securing virtual machine orchestration with blockchains // Proc. 1st Cyber Security in Networking Conference (CSNet). 2017. P. 1–8. doi: 10.1109/CSNET.2017.8242003
46. Rebello G.A.F., Camilo G.F., Silva L.G.C., Guimarães L.C.B., de Souza L.A.C., Alvarenga I.D., Duarte O.C.M. Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology // Proc. 20th International Conference on High Performance Switching and Routing (HPSR). 2019. P. 8808114. doi: 10.1109/HPSR.2019.8808114
47. Afolabi I., Taleb T., Samdanis K., Ksentini A., Flinck H. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions // IEEE Communications Surveys & Tutorials. 2018. V. 20. N 3. P. 2429–2453. doi: 10.1109/COMST.2018.2815638
48. Kaloxylos A. A survey and an analysis of network slicing in 5G networks // IEEE Communications Standards Magazine. 2018. V. 2. N 1. P. 60–65. doi: 10.1109/MCOMSTD.2018.1700072
49. Foukas X., Patounas G., Elmokashfi A., Marina M.K. Network slicing in 5G: Survey and challenges // IEEE Communications Magazine. 2017. V. 55. N 5. P. 94–100. doi: 10.1109/MCOM.2017.1600951

International Conference on Sustainable Computing and Communications, ISPA/IUCC/BDCloud/SocialCom/SustainCom 2018, 2018, pp. 308–315. doi: 10.1109/BDCloud.2018.00056
31. Zaidi Z., Friderikos V., Yousaf Z., Fletcher S., Dohler M., Aghvami H. Will SDN be part of 5G? . *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 4, pp. 3220–3258. doi: 10.1109/COMST.2018.2836315
32. Bouras C., Kollia A., Papazois A. SDN & NFV in 5G: Advancements and challenges. *Proc. 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, 2017, pp. 107–111. doi: 10.1109/ICIN.2017.7899398
33. Ahmad I., Namal S., Ylianttila M., Gurtov A. Security in software defined networks: A survey. *IEEE Communications Surveys & Tutorials*, 2015, vol. 17, no. 4, pp. 2317–2346. doi: 10.1109/COMST.2015.2474118
34. Sharma P.K., Singh S., Jeong Y.-S., Park J.H. DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Communications Magazine*, 2017, vol. 55, no. 9, pp. 78–85. doi: 10.1109/MCOM.2017.1700041
35. Yazdinejad A., Parizi R.M., Dehghantanha A., Choo K.-K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Transactions on Network Science and Engineering*, 2019, early access. doi: 10.1109/TNSE.2019.2937481
36. Yousaf F.Z., Bredel M., Schaller S., Schneider F. NFV and SDN-key technology enablers for 5G networks. *IEEE Journal on Selected Areas in Communications*, 2017, vol. 35, no. 11, pp. 2468–2478. doi: 10.1109/JSAC.2017.2760418
37. Mijumbi R., Serrat J., Gorricho J.-L., Bouten N., De Turck F., Boutaba R. Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 2016, vol. 18, no. 1, pp. 236–262. doi: 10.1109/COMST.2015.2477041
38. Abdelwahab S., Hamdaoui B., Guizani M., Znati T. Network function virtualization in 5G. *IEEE Communications Magazine*, 2016, vol. 54, no. 4, pp. 84–91. doi: 10.1109/MCOM.2016.7452271
39. Farris I., Taleb T., Khettab Y., Song J. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, no. 1, pp. 812–837. doi: 10.1109/COMST.2018.2862350
40. Alwakeel A.M., Alnaim A.K., Fernandez E.B. A survey of network function virtualization security. *Proc. SoutheastCon 2018*, 2018, pp. 8479121. doi: 10.1109/SECON.2018.8479121
41. Reynaud F., Aguessy F.-X., Bettan O., Bouet M., Conan V. Attacks against network functions virtualization and software-defined networking: State-of-the-art. *Proc. NetSoft Conference and Workshops*, 2016, pp. 471–476. doi: 10.1109/NETSOFT.2016.7502487
42. Ak E., Canberk B. BCDN: A proof of concept model for blockchain-aided CDN orchestration and routing. *Computer Networks*, 2019, vol. 161, pp. 162–171. doi: 10.1016/j.comnet.2019.06.018
43. *Commonalities of Network Function Virtualization, Blockchains and Smart Contracts*. Available at: https://files.ifi.uzh.ch/CSG/teaching/FS18/ComSys/Talk9.pdf (accessed: 26.05.2020).
44. Rebello G.A.F., Alvarenga I.D., Sanz I.J., Duarte O.C.M. BSec-NFVO: A blockchain-based security for network function virtualization orchestration. *Proc. IEEE International Conference on Communications (ICC 2019)*, 2019, pp. 8761651. doi: 10.1109/ICC.2019.8761651
45. Bozic N., Pujolle G., Secci S. Securing virtual machine orchestration with blockchains. *Proc. 1st Cyber Security in Networking Conference (CSNet)*, 2017, pp. 1–8. doi: 10.1109/CSNET.2017.8242003
46. Rebello G.A.F., Camilo G.F., Silva L.G.C., Guimarães L.C.B., de Souza L.A.C., Alvarenga I.D., Duarte O.C.M. Providing a sliced, secure, and isolated software infrastructure of virtual functions through blockchain technology. *Proc. 20th International Conference on High Performance Switching and Routing (HPSR)*, 2019, pp. 8808114. doi: 10.1109/HPSR.2019.8808114
47. Afolabi I., Taleb T., Samdanis K., Ksentini A., Flinck H. Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 3, pp. 2429–2453. doi: 10.1109/COMST.2018.2815638
48. Kaloxylos A. A survey and an analysis of network slicing in 5G networks. *IEEE Communications Standards Magazine*, 2018, vol. 2, no. 1, pp. 60–65. doi: 10.1109/MCOMSTD.2018.1700072
49. Foukas X., Patounas G., Elmokashfi A., Marina M.K. Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine*, 2017, vol. 55, no. 5, pp. 94–100. doi: 10.1109/MCOM.2017.1600951
50. Zhang S. An overview of network slicing for 5G. *IEEE Wireless Communications*, 2019, vol. 26, no. 3, pp. 111–117. doi: 10.1109/MWC.2019.1800234

50. Zhang S. An overview of network slicing for 5G // IEEE Wireless Communications. 2019. V. 26. N 3. P. 111–117. doi: 10.1109/MWC.2019.1800234
51. Nour B., Ksentini A., Herbaut N., Frangoudis N.P.A., Moungla H. A blockchain-based network slice broker for 5G services // IEEE Networking Letters. 2019. V. 1. N 3. P. 99–102. doi: 10.1109/LNET.2019.2915117
52. Backman J., Yrjölä S., Valtanen K., Mämmelä O. Blockchain network slice broker in 5G: Slice leasing in factory of the future use case // Proc. 2017 Internet of Things Business Models, Users, and Networks. 2017. P. 1–8. doi: 10.1109/CTTE.2017.8260929
53. Valtanen K., Backman J., Yrjölä S. Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case // Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW). 2018. P. 185–190. doi: 10.1109/WCNCW.2018.8368983
54. Valtanen K., Backman J., Yrjölä S. Blockchain-powered value creation in the 5G and smart grid use cases // IEEE Access. 2019. V. 7. P. 25690–25707. doi: 10.1109/ACCESS.2019.2900514
55. Rawat D.B., Alshaikhi A. Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints // Proc. 2018 International Conference on Computing, Networking and Communications (ICNC). 2018. P. 332–336. doi: 10.1109/ICCNC.2018.8390344
56. Ansari R.I., Chrysostomou C., Hassan S.A., Guizani M., Mumtaz S., Rodriguez J., Rodrigues J.J.P.C. 5G D2D networks: Techniques, challenges, and future prospects // IEEE Systems Journal. 2018. V. 12. N 4. P. 3970–3984. doi: 10.1109/JSYST.2017.2773633
57. Hamoud O.N., Kenaza T., Challal Y. Security in device-to-device communications: a survey // IET Networks. 2018. V. 7. N 1. P. 14–22. doi: 10.1049/iet-net.2017.0119
58. Wang M., Yan Z. Security in D2D communications: A review // Proc. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015). 2015. V. 1. P. 1199–1204. doi: 10.1109/Trustcom.2015.505
59. Cui H., Chen Z., Liu N., Xia B. Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks // Proc. 2019 IEEE International Conference on Communications Workshops (ICC Workshops). 2019. P. 8757177. doi: 10.1109/ICCW.2019.8757177
60. Niya S.R., Shüpfer F., Bocek T., Stiller B. Setting up flexible and light weight trading with enhanced user privacy using smart contracts // Proc. IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World (NOMS 2018). 2018. P. 1–2. doi: 10.1109/NOMS.2018.8406112
61. Yang G., Wu X., Wu Y., Chen C. A distributed secure monitoring system based on blockchain // International Journal of Performability Engineering. 2018. V. 14. N 10. P. 2393–2402. doi: 10.23940/ijpe.18.10.p15.23932402
62. Nguyen D.C., Pathirana P.N., Ding M., Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey // Journal of Network and Computer Applications. 2020. V. 166. P. 102693. doi: 10.1016/j.jnca.2020.102693

51. Nour B., Ksentini A., Herbaut N., Frangoudis N.P.A., Moungla H. A blockchain-based network slice broker for 5G services. *IEEE Networking Letters*, 2019, vol. 1, no. 3, pp. 99–102. doi: 10.1109/LNET.2019.2915117
52. Backman J., Yrjölä S., Valtanen K., Mämmelä O. Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. *Proc. 2017 Internet of Things Business Models, Users, and Networks*, 2017, pp. 1–8. doi: 10.1109/CTTE.2017.8260929
53. Valtanen K., Backman J., Yrjölä S. Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case. *Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2018, pp. 185–190. doi: 10.1109/WCNCW.2018.8368983
54. Valtanen K., Backman J., Yrjölä S. Blockchain-powered value creation in the 5G and smart grid use cases. *IEEE Access*, 2019, vol. 7, pp. 25690–25707. doi: 10.1109/ACCESS.2019.2900514
55. Rawat D.B., Alshaikhi A. Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints. *Proc. 2018 International Conference on Computing, Networking and Communications (ICNC)*, 2018, pp. 332–336. doi: 10.1109/ICCNC.2018.8390344
56. Ansari R.I., Chrysostomou C., Hassan S.A., Guizani M., Mumtaz S., Rodriguez J., Rodrigues J.J.P.C. 5G D2D networks: Techniques, challenges, and future prospects. *IEEE Systems Journal*, 2018, vol. 12, no. 4, pp. 3970–3984. doi: 10.1109/JSYST.2017.2773633
57. Hamoud O.N., Kenaza T., Challal Y. Security in device-to-device communications: a survey. *IET Networks*, 2018, vol. 7, no. 1, pp. 14–22. doi: 10.1049/iet-net.2017.0119
58. Wang M., Yan Z. Security in D2D communications: A review. *Proc. 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015)*, 2015, vol. 1, pp. 1199–1204. doi: 10.1109/Trustcom.2015.505
59. Cui H., Chen Z., Liu N., Xia B. Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks. *Proc. 2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019, pp. 8757177. doi: 10.1109/ICCW.2019.8757177
60. Niya S.R., Shüpfer F., Bocek T., Stiller B. Setting up flexible and light weight trading with enhanced user privacy using smart contracts. *Proc. IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World (NOMS 2018)*, 2018, pp. 1–2. doi: 10.1109/NOMS.2018.8406112
61. Yang G., Wu X., Wu Y., Chen C. A distributed secure monitoring system based on blockchain. *International Journal of Performability Engineering*, 2018, vol. 14, no. 10, pp. 2393–2402. doi: 10.23940/ijpe.18.10.p15.23932402
62. Nguyen D.C., Pathirana P.N., Ding M., Seneviratne A. Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications*, 2020, vol. 166, pp. 102693. doi: 10.1016/j.jnca.2020.102693

Авторы

Беззатеев Сергей Валентинович — доктор технических наук, доцент, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация; заведующий кафедрой, Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, 190000, Российская Федерация, Scopus ID: 6602425996, ORCID ID: 0000-0002-0924-6221, bsv@aanet.ru

Федоров Иван Романович — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0003-2422-4714, Ivanfedorov@itmo.ru

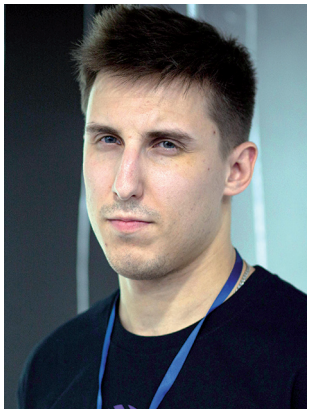
Authors

Sergey V. Bezzateev — D.Sc., Associate Professor, Professor of Practice, ITMO University, Saint Petersburg, 197101, Russian Federation; Head of Chair, Saint Petersburg State University of Aerospace Instrumentation (SUAI), Saint Petersburg, 190000, Russian Federation, Scopus ID: 6602425996, ORCID ID: 0000-0002-0924-6221, bsv@aanet.ru

Ivan R. Fedorov — Postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0003-2422-4714, Ivanfedorov@itmo.ru

Сергей Валентинович Беззатеев окончил Институт авиационного приборостроения по специальности «инженер-системотехник». В 1987 году получил степень кандидата наук по специальности «Системный анализ, управление и обработка информации». Работал в Институте аэрокосмического приборостроения научным сотрудником, доцентом. В 2004 году назначен руководителем проекта в совместной лаборатории Samsung-ГУАП по информационной безопасности в беспроводных сетях. С 2010 года – заведующий кафедрой технологий защиты информации в Санкт-Петербургском государственном университете аэрокосмического приборостроения. В 2011 году защитил диссертацию на соискание ученой степени доктора технических наук. Лауреат премии Правительства Санкт-Петербурга в области образования (2012 год). Руководитель работ и участник научных исследований по Гранту академической программы EC NordSecMobile (2013 год) с коллегами из Norwegian University of Science and Technology. С 2017 года профессор факультета безопасных информационных технологий Университета ИТМО. Основными областями научных интересов являются алгебраическая теория кодирования и криптографические методы защиты информации. Опубликовал более 100 научных работ, из них более 70 в ведущих международных изданиях, индексируемых в базе данных SCOPUS. Обладатель более 20 патентов, в том числе 15 международных.

Sergey V. Bezzateev graduated from Leningrad Aerospace Instrumentation Institute in 1980 witn the “System engineer” diploma. In 1987 he received his PhD degree in “System analysis, control and information processing” specialty. He was working as a Researcher and Associate Professor. From 2004 till 2007 he was a Project Leader in Samsung-SUAI Joint Laboratory for information security in wireless networks. From 2010 he was a Professor and Head of Chair of Information Security Technologies in Saint Petersburg State University of Aerospace Instrumentation (SUAI). In 2011 he received the Doctor of science degree in “Information theory”. In 2012 he was awarded the St. Petersburg Government Prize for education. In 2013 he won the grant from EC NordSecMobile Academic program and participated in the joint research with colleagues from Norwegian University of Science and Technology. From 2017 he is a Professor of Secure Information Technologies school in ITMO University. His main research interests are: algebraic coding theory and cryptographic methods of information protection. He is the author of more than 100 scientific papers, including more than 70 ones in the leading international editions indexed by the SCOPUS database. He has got more than 20 patents, including 15 international ones.



Федоров Иван Романович окончил с отличием Санкт-Петербургский государственный университет аэрокосмического приборостроения по направлению «Информатика и вычислительная техника» (программа бакалавриата). Подготовил и защитил магистерскую работу «Алгоритмы совместного многоядерного планирования реального времени со статическим методом назначения приоритетов задачам». С 2019 года аспирант в Университете ИТМО по направлению «Информационная безопасность». Автор одного патента и девяти научных статей.

Ivan R. Fedorov graduated with honors from Saint Petersburg State University of Aerospace Instrumentation (SUAP) with a bachelor’s degree in “Informatics and Computer Engineering” in 2016. He completed his master’s course in SUAI and defended his master’s thesis on “Algorithms for joint multi-core real-time planning with a static method for assigning priorities to tasks” in 2018. Since 2019 he is studying at the postgraduate school of ITMO University in the field of “Information Security”. He is the author of 1 patent and 9 scientific papers.