6. Castryck W., Decru T. An efficient key recovery attack on SIDH // In: C. Hazay, M. Stam (eds.) Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part V. – Lecture Notes in Computer Science. – Vol. 14008. – Berlin, Heidelberg: Springer-Verlag, 2023. – Pp. 423–447. – DOI: doi.org/10.1007/978-3-031-30589-4_15.

7. Basso A., Maino L., Pope G. FESTA: Fast Encryption from a Supersingular Torsion Attacks // In: J. Guo, R. Steinfeld (eds.) Advances in Cryptology – ASIACRYPT 2023. – Singapore: Springer Nature Singapore, 2023. – Pp. 98–126.

8. Nakagawa K., Onuki H. QFESTA: efficient algorithms and parameters for FESTA using quaternion algebras [Electronic resource] // IACR Cryptol. ePrint Arch. – 2023. – Paper 2023/1468. – URL: https://eprint.iacr.org/2023/1468 (access date: 31.05.2024).

9. Moriya T. IS-CUBE: an isogeny-based compact KEM using a boxed SIDH diagram [Electronic resource] // IACR Cryptol. ePrint Arch. – 2023. – Paper 2023/1506. – URL: https://eprint.iacr.org/2023/1506 (access date: 31.05.2024).

10. Fouque P., Hoffstein J., Kirchner P., Lyubashevsky V., Pornin T., Prest T., Ricosset T., Seiler G., Whyte W., Zhang Z. Falcon: fast-fourier lattice-based compact signatures over NTRU [Electronic resource]. – Specifications v1.0. – 2019. – URL: https://www.di.ens.fr/~prest/Publications/falcon.pdf (access date: 31.05.2024).

УДК 004.056
doi:10.18720/SPBPU/2/id24-510

Калинин Максим Олегович [1],
профессор, д-р техн. наук, профессор;
Крундышев Василий Михайлович [2],
доцент, канд. техн. наук;
Платонов Владимир Владимирович [3],
доцент, канд. техн. наук, доцент;
Супрун Александр Федорович [4],
доцент, канд. техн. наук, доцент

УСОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА БЛОКЧЕЙНА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ЦИФРОВОЙ СРЕДЫ УМНОГО МЕГАПОЛИСА

[1,2,3,4] Россия, Санкт-Петербург,
Санкт-Петербургский политехнический университет Петра Великого,
[1] max@ibks.spbstu.ru, [2] vmk@ibks.spbstu.ru, [3] plato@ibks.spbstu.ru,
[4] suprun@ibks.spbstu.ru

Аннотация. Проанализированы проблемы безопасности и устойчивости механизмов распределенного реестра в системах умного мегаполиса, в том числе защищенность алгоритмов распределенного консенсуса. Сформулированы требования к алгоритму распределенного консенсуса, создаваемому для усиления защищенности блокчейна и обеспечения киберустойчивости цифровой среды умного мегаполиса.

Представлен гибридный алгоритм распределенного консенсуса, сочетающий алгоритмы Tangle и Proof-of-Authority и защищенный с помощью технологий доверенных вычислений и удаленной аттестации. Решение устраняет недостатки, характерные для известных алгоритмов распределенного консенсуса классического блокчейна и сдерживающие его применение в крупномасштабных киберсредах.

Ключевые слова: алгоритм распределенного консенсуса, безопасность, блокчейн, гибридный алгоритм, распределенный реестр, умный мегаполис.

Maxim O. Kalinin [1],
Professor, Doctor of Technical Science;
Vasiliy M. Krundyshev [2],
Associated Professor, Candidate of Technical Science;
Vladimir V. Platonov [3],
Associated Professor, Candidate of Technical Science;
Aleksandr F. Suprun [4],
Associated Professor, Candidate of Technical Science

IMPROVING THE BLOCKCHAIN MECHANISM TO ENSURE CYBER SUSTAINABILITY OF THE SMART CITY DIGITAL ENVIRONMENT

[1,2,3,4] Peter the Great St.Petersburg Polytechnic University, St. Petersburg, Russia,
[1] max@ibks.spbstu.ru, [2] vmk@ibks.spbstu.ru, [3] plato@ibks.spbstu.ru,
[4] suprun@ibks.spbstu.ru

Abstract. The problems of cybersecurity and sustainability of the distributed registries in the use case of a smart city system are analyzed. The security problem of distributed consensus algorithms is reviewed. The requirements for the distributed consensus algorithm created to enhance the security of the blockchain and ensure the cyber sustainability of the digital environment of a smart city are formulated. A hybrid distributed consensus algorithm is proposed that combines the Tangle and Proof-of-Authority consensus algorithms and is protected using trusted computing and remote attestation technologies. The proposed solution eliminates the vulnerable features of known distributed consensus algorithms of the classic blockchain that hinder its use in large-scale cyber environments.

Keywords: distributed consensus algorithm, security, blockchain, hybrid algorithm, distributed registry, smart city.

Введение

Умный мегаполис (smart city) – современная технологическая концепция, направленная на решение проблем эффективного функционирования городской среды и обеспечения удобной жизни людей в городе [1, 2], в том числе задач логистики, транспортировки, работы городского и жилищного хозяйства, управления технической и социальной инфраструктурой, вовлеченности людей в муниципальное управление и хозяйственные процессы.

Важнейшая характеристика среды умного мегаполиса – устойчивость [3], достижение которой обеспечивается путем оптимизации

использования современных цифровых технологий, улучшения качества услуг, уменьшения расходов и поддержания защищенности [1, 2]. Проблемы на стыке задач обеспечения киберустойчивости и защищенности умного мегаполиса обусловлены рядом факторов [4]:

– крупным масштабом такой цифровой среды, разнообразием вовлеченных технологий и системных компонентов, включающих интернет вещей (Internet of Things, IoT), сенсорные сети (wireless sensor networks, WSN), технологии «Больших Данных» (BigData), машинное обучение [3];

– количеством и разнообразием источников данных и заинтересованных участников разного уровня полномочий и критичности;

– децентрализованным управлением и, как следствие, отсутствием постоянного всестороннего доверия и единой управляемости [4].

В ответ на данный вызов технология распределенного реестра, в частности, блокчейн, позволяет не доверяющим друг другу участникам взаимодействия работать без доверенного посредника [5]. При этом распределенный реестр обеспечивает прозрачность, доказуемость и безопасность взаимодействий между участниками. Используемые для решения задач киберустойчивости и защищенности распределенные реестры различаются базовыми моделями и принципами безопасности, но вместе с тем их объединяет то, что все они основаны на криптосистемах с открытым ключом, одноранговой (peer-to-peer) схеме работы и на механизме распределенного консенсуса [6].

В рамках проведенного исследования авторами проанализированы проблемы безопасности систем распределенного реестра умного мегаполиса. Рассмотрены недостатки блокчейна при применении в системах умного мегаполиса, связанные с недостатками базовых алгоритмов распределенного консенсуса. Представлен новый гибридный алгоритм распределенного консенсуса, устраняющий причины возникновения киберугроз со стороны механизма распределенного консенсуса и пригодный для работы в крупномасштабных киберсредах.

1. Анализ безопасности технологии распределенного реестра

Применение технологии распределенного реестра в целом является популярным подходом к обеспечению защищенности и устойчивости любых распределенных киберсред, в том числе интернета вещей умного мегаполиса, за счет устранения единственной точки отказа и достижения высокого доверия к процессам и данным средствами механизма распределенного консенсуса. Специфика применения блокчейна в цифровой среде умного мегаполиса определяется такими задачами, как обеспечение конфиденциальности данных, обработка чувствительных данных, энергоэффективность механизмов консенсуса, совместимость протоколов и моделей доверия, а также производительность [6–8].

Анализ современных исследований в области безопасности распределенных реестров умных мегаполисов показывает, что большая их часть посвящена использованию блокчейна в системах интернета вещей [9–13].

Ряд исследований направлен на решение задач масштабируемости блокчейна в интернете вещей умного мегаполиса (например, [11]). Отмечается, что алгоритмы распределенного консенсуса, используемые в блокчейне, подходят для информационных систем, обрабатывающих ограниченное количество транзакций. Киберсреда умного мегаполиса генерирует такой объем транзакций, которое современные блокчейн-системы обрабатывают с нарастающими, довольно большими, задержками [11]. В качестве решения в [11] предложено вместо последовательного упорядочивания транзакций (цепной связи блоков транзакций) использовать транзакции в виде направленного ориентированного графа (каждая новая транзакция «подтверждает» несколько предыдущих транзакций, обладающих наибольшей высотой). Такой подход позволяет выполнять параллельную обработку транзакций и обеспечивает устойчивость к разделению сети.

Рост числа обрабатываемых транзакций в крупномасштабной системе увеличивает объем данных, подлежащих хранению в блокчейне. Для решения этой проблемы авторами работы [14] предложено хранить данные во внешнем хранилище распределенной файловой системе IPFS. Непосредственно в блокчейне хранятся только хэш-образы данных.

Помимо рассмотренной проблемы масштабируемости, препятствующей внедрению блокчейна в умные мегаполисы, блокчейн является причиной возникновения новых специфических кибератак с использованием блокчейна [15]:

– *liveness attack*: нарушитель вносит значительные задержки в процесс обработки транзакций; для защиты от данной атаки применяется механизм распределенного консенсуса Conflux [16];

– *double spending*: нарушитель отменяет или изменяет успешно проведенную транзакцию; способы защиты представлены в работах [17, 18];

– «*атака большинства*» (majority attack, или атака 51 %): нарушитель, контролирующий более 50 % ресурсов блокчейна, может нарушить целостность данных, хранимых в нем; атака не может быть предотвращена, так как она определена природой блокчейна, однако ее реализация может быть значительно затруднена для нарушителя с помощью определенных защитных приемов: например, введения штрафов за обработку транзакций в тайне от остальных узлов, внедрения механизма контрольных точек [19];

– *компрометация закрытых ключей*: позволяет нарушителю проводить транзакции от имени других участников; защита обеспечивается схемами группового управления ключами [20];

– *утечка информации*: из-за прослеживаемости транзакций возможны утечки критичной информации о субъектах и объектах транзакций;

конфиденциальность данных в данном случае обеспечивается криптографическими средствами [21];

– *selfish mining*: нарушитель выполняет обработку транзакций втайне от остальных узлов блокчейна; в определенных случаях это позволяет отменить результаты обработки транзакций, полученные другими узлами; контрмеры для данного вида атак приведены в работе [22];

– *перенаправление сетевого трафика средствами BGP* (BGP hijacking): нарушитель может перехватывать сообщения, пересылаемые между узлами распределенного реестра, замедляя обработку транзакций; для защиты от данной атаки предложена схема BGPCoin [23];

– *Sybil attack*: использование нарушителем множества поддельных учетных записей для компрометации репутационной системы и проведения атак отказа в обслуживании; в работе [24] предлагается способ обнаружение аномалий в сообщениях, пересылаемых между узлами блокчейна.

В дополнение к точечным решениям отдельных проблем безопасности блокчейна умного мегаполиса, в современных исследованиях поднимаются вопросы построения принципиально новых архитектур блокчейн-систем умного мегаполиса с учетом проблем масштабируемости и безопасности. Например, авторами работы [13] предлагается двухуровневая архитектура блокчейн-системы, где первый уровень образован множеством закрытых распределенных реестров, оптимизированных для использования маломощными устройствами за счет отказа от асимметричных криптопримитивов в пользу симметричных, а также упрощенного алгоритма консенсуса. Второй уровень представлен блокчейном, обеспечивающим взаимодействие между реестрами первого уровня, а также доступ к облачным системам. Схожая технология кластеризации блокчейна представлена в исследовании [25].

В качестве альтернативных решений в области обеспечения безопасности и киберустойчивости блокчейна крупных систем выделяются предложения использовать постквантовую криптографию [11, 26], система SmartPrivChain, предназначенная для защищенного обмена данными между системами умного города на базе алгоритма распределенного консенсуса, реализующего многомерную модель доверия [27]; системы PrivySharing [28] с многоканальным блокчейном для обработки данных определенного типа (медицинских, транспортных и т. д.) с разграничением доступа к каналам.

Анализ существующих реализаций блокчейнов для защиты цифровых сред умного мегаполиса показал, что превалирующее число современных исследований в рассматриваемой области посвящено задаче интеграции и обеспечения совместной работы технологий блокчейна и интернета вещей. Сочетание указанных технологий дает значительные преимущества с точки зрения обеспечения киберустойчивости и защищенности умных

мегаполисов, но практическая реализуемость данного симбиоза остается весьма ограниченной до тех пор, пока не будет разрешены проблемы безопасности и масштабируемости рабочих механизмов самого блокчейна.

2. Анализ безопасности алгоритмов распределенного консенсуса в больших блокчейн-системах умного мегаполиса

В настоящее время в блокчейн-системах, рекомендуемых экспертным сообществом для защиты умного мегаполиса, применяется множество алгоритмов распределенного консенсуса: proof-of-work (PoW), proof-of-stake (PoS), proof-of-authority (PoA), PBFT, Tangle [4–6]. В крупномасштабных средах указанные алгоритмы становятся уязвимыми, позволяя нарушителям реализовать довольно чувствительные кибератаки, указанные выше. Рассмотрим примеры уязвимостей безопасности, характерных для различных семейств алгоритмов консенсуса.

Для алгоритмов консенсуса семейства PoW характерна «атака большинства» (majority attack, или атака 51 %) [19]. Особенность данной атаки – невозможность ее предотвратить. Однако ее реализация нарушителем может быть значительно затруднена с помощью ряда контртехник, например, введением механизма штрафов за обработку транзакций в тайне от остальных узлов, алгоритма распределенного консенсуса «delayed PoW», контрольных точек [19].

Алгоритмы консенсуса типа PoS и delegated PoS подвержены отказам в обслуживании, подмене реестра (long range attack) и атаке Сивиллы (Sybil Attack) [29].

Алгоритмам консенсуса PoA свойственна высокая централизация, что делает их уязвимыми к сговору сторон, контролирующих узлы блокчейна, которые отвечают за обработку транзакций [30]. Также алгоритмы PoA подвержены атаке клонирования [31].

Алгоритмы консенсуса PBFT реализуют синхронный обмен, что может привести к блокировке обработки транзакций [32].

Алгоритмам консенсуса Tangle, равно как и PoW-алгоритмам, свойственна уязвимость, приводящая к реализации «атаки большинства» [33].

Таким образом, все базовые алгоритмы распределенного консенсуса блокчейна уязвимы в крупномасштабных системах и позволяют через блокчейн реализовать специфические кибератаки в цифровой среде умного мегаполиса, вследствие чего технология блокчейна требует доработки в плане усиления базовой защищенности и устранения причин возникновения характерных киберугроз.

3. Усовершенствование механизма блокчейна с учетом проблем безопасности и масштабируемости

Умный мегаполис представляет собой уникальную сетевую информационную структуру, не имеющую единого центра управления. Такая среда

объединяет гетерогенные информационные системы, контролируемые разными участниками: физическими лицами, частными, муниципальными и государственными организациями. В системах умного мегаполиса могут применяться открытые и закрытые реестры, что определяет ограничения на множество допустимых алгоритмов распределенного консенсуса.

Большой размер цифровой среды умного мегаполиса и работа с огромным количеством данных (Bigdata) также ограничивают множество и возможности применяемых алгоритмов распределенного консенсуса. Для крупномасштабных сред с большим количеством участников, узлов и защищаемых данных необходимо использовать алгоритмы, которые обеспечиват высокую производительность при обработке большого числа транзакций. Таким возможностями из всего разнообразия алгоритмов распределенного консенсуса, применимых в открытых распределенных реестрах, обладают Tangle-алгоритмы [5]. Из множества алгоритмов, применимых в закрытых реестрах, сравнимую производительность демонстрируют алгоритмы консенсуса PoA [32].

Таким образом, для усиления защищенности блокчейна и обеспечения киберустойчивости цифровой среды умного мегаполиса алгоритм распределенного консенсуса должен удовлетворять следующим требованиям:

– *безопасность*: использование принципа работы, не подверженного известным уязвимостям алгоритмов распределенного консенсуса;

– *универсальность*: применимость для открытых и закрытых распределенных реестров;

– *высокая производительность и масштабируемость*: обеспечение высокой скорости обработки большого количества транзакций и применимость в крупномасштабных распределенных средах.

С учетом перечисленных требований авторами построена система защищенного блокчейна для цифровых сред умного мегаполиса, основанная на гибридном алгоритме распределенного консенсуса. Разработанный новый алгоритм распределенного консенсуса основан на агрегации алгоритмов Tangle и PoA, защищенной с помощью технологий доверенных вычислений [33] и удаленной аттестации [34] (см. рис. 1).

Распределенный реестр состоит из узлов двух типов: узлов, реализующих алгоритм распределенного консенсуса класса Tangle (на рис. 1 обозначены Tangle), и доверенных узлов, реализующих алгоритм распределенного консенсуса PoA, защищенный с помощью технологий доверенных вычислений и удаленной аттестации (на рис. 1 обозначены Proof-of-authority). Доверенные узлы имеют в своем составе TPM [33]. На доверенных узлах исполняется эталонное ПО, состав которого контролируется с помощью измеряемой загрузки [33].

Tangle-узлы получают данные (Data на рис. 1) от различных источников (источниками являются компоненты самих узлов, например,

встроенные сенсоры, исполняющиеся на узле процессы, и внешние источники, например, устройства интернета вещей умного мегаполиса, для которых узел является шлюзом). Узлы, реализующие Tangle-алгоритм, проверяют полученные данные, преобразуют их в транзакции (на рис. 1 – Transaction(Data)) и записывают транзакции в реестр, где они становятся доступны для остальных узлов.

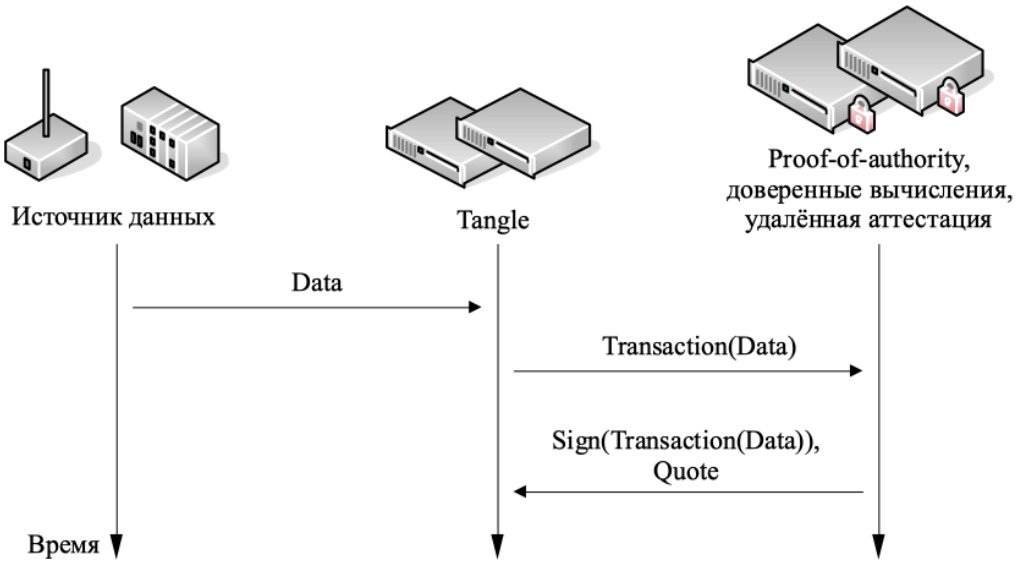

Рис. 1. Схема работы гибридного алгоритма распределенного консенсуса

Доверенные узлы, реализующие алгоритм PoA, подтверждают новые транзакции, опубликованные узлами, реализующими алгоритм Tangle. С момента подтверждения транзакция считается исполненной. Подтверждение транзакции выполняется в соответствии с используемым алгоритмом PoA: доверенный узел подписывает транзакцию (на рис. 1 – Sign(Transaction(Data))). В дополнение к цифровой подписи доверенный узел подтверждает целостность своего программного обеспечения с помощью результата выполнения команды удаленной аттестации TPM2_Quote [34]. Подтверждение целостности программного обеспечения подтверждает целостность реализации алгоритма PoA. Одноразовый код, подаваемый на вход команды TPM2_Quote и обеспечивающий защиту от атаки повторного воспроизведения, может быть получен из криптографического хэш-образа подтверждаемой транзакции.

Построенный алгоритм консенсуса отвечает всем выдвинутым требованиям и делает невозможной эксплуатацию уязвимостей исходных алгоритмов распределенного консенсуса.

При такой схеме консенсуса «атака большинства» становится принципиально нереализуемой, так как транзакции нарушителя не получат подтверждения доверенных узлов. Доверенные узлы не могут реализовывать произвольное подтверждение транзакций, потому что алгоритм подтверждения является доверенным вычислением, контролируемым с помощью удаленной аттестации. Доверенные узлы не обладают полномочиями

по проведению собственных транзакций, так как они только подтверждают уже существующие транзакции.

Разработанный алгоритм отвечает требованию универсальности. Для закрытого блокчейна узлы, реализующие алгоритм Tangle, являются необязательными. В этом случае преобразование данных в транзакции могут выполнять доверенные узлы, реализующие алгоритм PoA.

Алгоритм не снижает общую производительность системы, сохраняя уровень быстродействия базовых алгоритмов Tangle и PoA [5, 32] (увеличивается лишь задержка при обработке транзакций).

Заключение

Технология распределенного реестра в целом позволяет увеличить защищенность и устойчивость цифровой среды умного мегаполиса, а также обеспечивает доверие к информационным процессам, связанным с обеспечением цифровизации экономики и жизни городского населения.

Однако, для успешного внедрения и применения технологии распределенного реестра в крупномасштабной распределенной киберсреде, какой является умный мегаполис, необходима разработка новых механизмов, обеспечивающих высокую производительность при обработке большого числа транзакций, а также защищенность от специфических киберугроз, связанных с монополизацией нарушителем ресурсов блокчейна. Также необходимы решения, позволяющие интегрировать друг с другом разнотипные распределенные реестры.

Авторами предложено усовершенствование механизма блокчейна для цифровой среды умного мегаполиса, заключающееся в создании гибридного алгоритма распределенного консенсуса, основанного на совместном применении алгоритмов консенсуса Tangle и PoA и защищенного с помощью технологий доверенных вычислений и удаленной аттестации. Представленное решение уникально тем, что обеспечивает безопасность блокчейна, компенсируя изъяны базовых алгоритмов распределенного консенсуса; универсальность и высокую производительность при обработке большого числа транзакций.

Благодарности

Исследование выполнено за счет гранта Российского научного фонда № 24-11-20005, https://rscf.ru/project/24-11-20005/; грант Санкт-Петербургского научного фонда (договор № 24-11-20005 о предоставлении регионального гранта).

Список литературы

1. Winkowska J., Szpilko D., Pejić S. Smart city concept in the light of the literature review // Engineering Management in Production and Services. – 2019. – Vol. 11. – No. 2 – Pp. 70–86.

2. Kirimtat A., Krejcar O., Kertesz A., Tasgetiren M. F. Future trends and current state of smart city concepts: a survey // IEEE Access. – 2020. – Vol. 8. – Pp. 86448–86467.

3. Majdoubi D. E., El Bakkali H., Sadki S. Towards smart blockchain-based system for privacy and security in a smart city environment // 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), Marrakesh, Morocco. – 2020. – Pp. 1–7.

4. Li S. Application of blockchain technology in smart city infrastructure // IEEE International Conference on Smart Internet of things (SmartIoT), Xi'an, China. – 2018. – Pp. 276–2766.

5. El Ioini N., Pahl C. A review of distributed ledger technologies // On the Move to Meaningful Internet Systems. OTM 2018 Conferences. OTM 2018. LNCS. – Springer: 2018. – Vol. 11230. – Pp. 277–288.

6. Chinnasamy P., Vinothini C., Arun Kumar S., Allwyn Sundarraj A., Annlin Jeba S. V., Praveena V. Blockchain technology in smart-cities // Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library. – Cham: Springer, 2021. – Vol. 203.

7. Tekeoglu A., Ahmed N. TangoChain: a lightweight distributed ledger for Internet of things devices in smart cities // 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco. – 2019. – Pp. 18–21.

8. Hakak S., Khan W. Z. , Gilkar G. A., Imran M., Guizani N. Securing smart cities through blockchain technology: architecture, requirements, and challenges // IEEE Network. – 2020. – Vol. 34. – No. 1. – Pp. 8–14.

9. Moro P. E., Duke A. K. Distributed ledger technologies and the Internet of things: a devices attestation system for smart cities // The Journal of The British Blockchain Association. – 2020. – DOI:https://doi.org/10.31585/ jbba-3-1-(7)2020.

10. Alotaibi B. Utilizing blockchain to overcome cyber security concerns in the Internet of things: a review // IEEE Sensors Journal. – 2019. – Vol. 19. – No. 23. – Pp. 10953-10971.

11. Ahi A., Singh A. V. Role of distributed ledger technology (DLT) to enhance resiliency in Internet of things (IoT) ecosystem // 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates. – 2019. – Pp. 782–786.

12. Ali M., Karimipour H., Tariq M. Integration of blockchain and federated learning for Internet of things: Recent advances and future challenges // Computers & Security. – 2021. – Vol. 108. – Paper 102355. – DOI:10.1016/j.cose.2021.102355.

13. Paul R., Baidya P., Sau S., Maity K., Maity S., Mandal S. B. IoT based secure smart city architecture using blockchain // 2nd International Conference on Data Science and Business Analytics (ICDSBA), Changsha, China. – 2018. – Pp. 215–220.

14. Ali M. S., Dolui K., Antonelli F. IoT data privacy via blockchains and IPFS // Proceedings of the 7th International Conference on the Internet of Things. – ACM, 2017. – Art. 14. – Pp. 1–7.

15. Singh S., Hosen A. S. M. S., Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed IoT network // IEEE Access. – 2021. – Vol. 9. – Pp. 13938–13959. – DOI:10.1109/ACCESS.2021.3051602.

16. Chenxin L., Peilun L., Dong Z., Zhe Y., Ming W., Guang Y., Wei X., Fan L., Andrew C. Y. A decentralized blockchain with high throughput and fast confirmation // Proc. USENIX Annu. Tech. Conf. (USENIX ATC). – 2020. – Pp. 515–528.

17. Nicolas K., Wang Y. A novel double spending attack countermeasure in blockchain // Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON). – 2019. – Pp. 383–388.

18. Begum A., Tareq A. H., Sultana M., Sohel M. K., Rahman T., Sarwar A. H. Blockchain attacks, analysis and a model to solve double spending attack // International Journal of Machine Learning and Computing. – 2020. – Vol. 10. – No. 2. – Pp. 1–6.

19. Sayeed S., Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack // Applied Sciences. –2019. – Vol. 9. – No. 9. – Paper 1788. – DOI:https://doi.org/10.3390/app9091788.

20. Pal O., Alam B., Thakur V., Singh S. Key management for blockchain technology // ICT Express. – 2021. – Vol. 7. – Iss. 1. – Pp. 76–80.

21. Bhushan B., Sharma N. Transaction privacy preservations for blockchain technology // International Conference on Innovative Computing and Communications. Advances in Intelligent Systems and Computing. – Singapore: Springer, 2021. – Vol. 1166. – P. 377–393.

22. Nicolas K., Wang Y., Giakos G. C. Comprehensive overview of selfish mining and double spending attack countermeasures // IEEE 40th Sarnoff Symposium. – 2019. – Pp. 1–6. – DOI:https://doi.org/10.1109/Sarnoff47838.2019.9067821.

23. Xing Q., Wang B., Wang X. POSTER: BGPCoin: A trustworthy blockchain-based resource management solution for BGP security // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. – ACM, 2017. – Pp. 2591–2593. – DOI:https://doi.org/10.1145/3133956.3138828.

24. Swathi P., Modi C., Patel D. Preventing sybil attack in blockchain using distributed behavior monitoring of miners // 10th International Conference on Computing, Communication and Networking Technologies. – 2019. – Pp. 1–6.

25. Honar Pajooh H., Rashid M., Alam F., Demidenko S. Multi-layer blockchain-based security architecture for Internet of things // Sensors. – 2021. – Vol. 21. – Paper 772. – DOI:https://doi.org/10.3390/s21030772.

26. Shahid F., Khan A., Jeon G. Post-quantum distributed ledger for Internet of things // Computers and Electrical Engineering. – 2020. – Vol. 83. – Paper 106581.

27. Majdoubi D. E., El Bakkali H., Sadki S. Towards smart blockchain-based system for privacy and security in a smart city environment // 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications. – 2020. – P. 1–7.

28. Makhdoom I., Zhou I., Abolhasan M., Lipman J., Ni W. PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities // Computers & Security. – 2020. – Vol. 88. – Paper 101653.

29. Nair P. R., Dorai D. R. Evaluation of performance and security of proof of work and proof of stake using blockchain // Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks. – 2021. – Pp. 279–283.

30. Praveen G., Anand M., Singh P. K., Ranjan P. An overview of blockchain consensus and vulnerability // Information and Communication Technology for Intelligent Systems. ICTIS 2020. Smart Innovation, Systems and Technologies. – Singapor: Springer, 2021. – Vol. 195. – Pp. 459–468.

31. Ekparinya P., Gramoli V., Jourjon G. The attack of the clones against proof-of-authority // arXiv. – 2019. – DOI:https://doi.org/10.48550/arXiv.1902.10244.

32. De Angelis S., Aniello L., Lombardi F., Margheri A., Sassone V. PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain [Electronic resource] // Italian Conference on Cybersecurity. – 2018. – URL: https://ceur-ws.org/Vol-2058/paper-06.pdf (access date: 31.05.2024).

33. Shen C., Zhang H., Wang H., Wang J., Zhao B., Yan F., Yu F., Zhang L., Xu M. Research on trusted computing and its development // Science China Information Sciences. – 2010. – Vol. 53. – Pp. 405–433.

34. Remote Attestation [Electronic resource] // tpm2-software community. – 2019. – URL: https://tpm2-software.github.io/tpm2-tss/getting-started/2019/12/18/Remote-Attestation.html (access date: 31.05.2024).