ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

құралдар. Технологияның арқасында "ақылды қоғамдық кеңістік" жалпы тұрғындарының өмір сүру сапасын жақсартты және оның экологиялық тұрақтылығын нығайта түсті.

Көптеген компаниялар Интеллектуалды көлік жүйелері мен цифрландыру құралдарын жасауға тырысып келеді, өйткені бүгінгі таңда біздің күнделікті өмірімізге өздігінен жүретін көліктер кірсе ал Оңтүстік Кореяда 2022 жылдың қарашасында өздігінен жүретін автобустарды іске қосты.

Қазіргі таңда Ақылды технологиялар біздің өміріміздің ыңғайлы әрі қауіпсіз етуге жағдай жасауда.

Қолданылған әдебиеттер тізімі

1. https://russoft.org/news/kak-sozdayut-umnyj-transport-v-raznyh-stranah-mira/).
2. https://www.experfy.com/internet-of-things/intelligent-transportation
3. https://www.traffictechnologytoday.com/news/traffic-management/yunex-traffic-to-unveil-new-advanced-traffic-controller-at-its-world-congress.html
4. https://blogs.worldbank.org/sustainablecities/how-seoul-korea-transforming-smart-city
5. https://center2m.ru/intellektualnye-transportnye-sistemy

УДК 004.056

ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА В ВОЕННОЙ СФЕРЕ

Оспанов Руслан Маратович

ospanovrm@gmail.ru

докторант 1 курса (8D06306 – Системы информационной безопасности),

ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Д.Ж.Сатыбалдина

Бисембаев Ильнур Байзулаевич

Начальник Департамента защиты государственных секретов Генерального штаба ВС РК, Астана, Казахстан

Введение. Технологии распределенного реестра - это технологии, обеспечивающие работу и использование распределенных реестров, т.е. реестров, которые совместно используются множеством участников, образующих сеть, и синхронизируются между ними с использованием механизма консенсуса. Распределенные реестры разработаны таким образом, чтобы быть защищенными от несанкционированного доступа, предназначенными только для добавления, неизменными, содержащими подтвержденные и проверенные транзакции [1]. Одним из основных преимуществ технологий распределенного реестра является то, что они могут обеспечить высокий уровень безопасности, прозрачности и неизменности, что делает их хорошо подходящими для сценариев использования, связанных с передачей цифровых активов или записью цифровых транзакций. Наиболее известным и широко используемым примером технологии распределенного реестра является блокчейн, технология, лежащая в основе таких криптовалют, как Биткойн и Эфириум. Технологии распределенного реестра можно использовать в самых разных отраслях и приложениях, таких как финансовые услуги, управление цепочками поставок, цифровая идентификация, игровая индустрия и т.д. К преимуществам этих технологий относятся повышенная прозрачность, безопасность и эффективность, а также возможность создавать новые бизнес-модели и возможности. Некоторые из ключевых особенностей DLT включают в себя: децентрализация (транзакции записываются и проверяются через сеть компьютеров, а не центральным органом), неизменяемость (после того, как транзакция записана, ее нельзя изменить или удалить), прозрачность (все участники сети могут получить доступ и проверить транзакции), безопасность (используется криптография для защиты транзакций и обеспечения защиты реестра от несанкционированного доступа). Таким образом, технологии распределенного реестра могут предложить множество потенциальных преимуществ, особенно с точки зрения безопасности, прозрачности и децентрализации. Но у него также есть ограничения, такие как масштабируемость и стоимость. Технологии все еще находятся в активном процессе развития и совершенствования.

В целом, технологии распределенного реестра - это перспективные технологии, способные произвести революцию во многих отраслях и создать новые возможности для государства, бизнеса и частных лиц.

Применение в военной сфере. Технологии распределенного реестра, и, в частности, технология блокчейн, имеют несколько потенциальных применений в военных целях, некоторые из которых включают:

Безопасная связь: технологии распределенного реестра могут использоваться для защиты военной связи путем создания защищенной от несанкционированного доступа записи сообщений, доступной только уполномоченному персоналу. Это может помочь предотвратить несанкционированный доступ к конфиденциальной информации и снизить риск кибератак.

Управление цепочками поставок: военные в значительной степени полагаются на сложные цепочки поставок для закупки и распределения оборудования, оружия и других ресурсов. Технологии распределенного реестра могут использоваться для отслеживания движения товаров и обеспечения их своевременной доставки в нужное место. Это могло бы помочь уменьшить потери, мошенничество и злоупотребления в военной логистике.

Кибербезопасность: технологии распределенного реестра могут использоваться для защиты военных сетей и предотвращения кибератак. Создавая децентрализованную сеть, устойчивую к взлому, блокчейн может обеспечить более безопасную платформу для военных данных и коммуникаций.

Проверка личности: технологии распределенного реестра могут использоваться для проверки личности военнослужащих и предотвращения мошенничества с идентификацией. Создавая защищенную от несанкционированного доступа запись данных персонала, технологии распределенного реестра могут гарантировать, что только авторизованный персонал имеет доступ к конфиденциальной информации и ресурсам.

Смарт-контракты: технологии распределенного реестра могут использоваться для создания смарт-контрактов, которые могут автоматизировать определенные аспекты военных операций, такие как закупки, логистика и техническое обслуживание. Это может помочь сократить расходы и повысить эффективность военных операций.

В целом технологии распределенного реестра могут повысить безопасность, эффективность и прозрачность военных операций. Однако существуют также опасения по поводу безопасности и масштабируемости, а также возможности неправомерного использования злоумышленниками. Поэтому перед внедрением технологий распределенного реестра в военных приложениях требуется тщательное рассмотрение и планирование.

Военные, оборонные правительственные организации различных государств предпринимают конкретные практические шаги для внедрения перспективных технологий в военных, оборонных целях.

Так например, в апреле 2016 года Агентство перспективных оборонных исследовательских проектов (Defense Advanced Research Projects Agency (DARPA)) Министерства обороны США (US Department of Defense (DoD)) в рамках программы SBIR (Small Business Innovation Research) выпустило заявку на предложение под номером DoD SBIR 2016.2 SB162-004 [2] о создании безопасной платформы обмена сообщениями и транзакций, которая отделяет создание сообщения от передачи (транспорта) и приема сообщения с использованием децентрализованной магистрали обмена сообщениями, позволяющей кому угодно в любом месте отправлять безопасное сообщение или проводить другие транзакции через несколько каналов, прослеживаемых в децентрализованном реестре. В результате были профинансированы целый ряд блокчейн-проектов военного назначения [3].

В сентябре 2016 года Galois and Guardtime Federal объявили, что они совместно получили контракт на 1,8 миллиона долларов от Агентства перспективных оборонных исследовательских проектов (Defense Advanced Research Projects Agency (DARPA)) Министерства обороны США (US Department of Defense (DoD)) для проверки корректности инфраструктуры бесключевой подписи (Keyless Signature Infrastructure (KSI)) компании Guardtime Federal [4]. Контракт был нацелен на финансирование значительных усилий, направленных на продвижение состояния

инструментов формальной верификации и всех систем мониторинга целостности на основе блокчейна.

В апреле 2016 года Агентство НАТО по связи и информации (NATO Communications and Information Agency (NCI Agency)) объявило конкурс Defence Innovation Challenge, с целью ускорения преобразующих, современных технологических решений в поддержку требований НАТО C4ISR и кибернетического потенциала [5]. Одним из направлений конкурса был поиск инновационных решений в области военного применения технологии блокчейн, в частности, применение технологии блокчейн в военной логистике, применение технологии блокчейн к закупкам и финансированию, другие применения, представляющие интерес для военных.

В 2017 году в 14-ом номере журнала “European Defence Matters” (Вопросы Европейской Обороны) Европейского Оборонного Агенства (European Defence Agency (EDA)) в заглавной статье “A journey into the future” техническими экспертами Агенства был представлен анализ 10 прорывных технологических разработок, являющихся перепроектирование ландшафта обороноспособности [6]. В числе этих 10 направлений рассматривалась и технология блокчейн для обороны.

10 апреля 2019 года Администрация программы оборонных закупок Южной Кореи (Defense Acquisition Program Administration (DAPA)) сообщила в пресс-релизе о том, что они планируют повысить надежность данных в военной промышленности с помощью блокчейна [7]. Государственное агентство по закупкам вооружений заявило, что оно стремится использовать блокчейн-платформу для обеспечения безопасного обмена данными о проектах по военным закупкам между соответствующими правительственными организациями и устранения фальсификации данных. Согласно пресс-релизу, в новой инициативе было заявлено участие таких организаций, как Агентство по оборонному развитию (Agency for Defense Development) и Оборонное агентство по технологиям и качеству (Defense Agency for Technology and Quality). Помимо повышения доверия к оборонным проектам с помощью блокчейна, DAPA также намеревалась сократить документооборот, связанный с подачей заявок на проекты госзакупок, а также унифицировать свою документацию, отмечалось в пресс-релизе.

За последнее десятилетие было опубликовано множество аналитических и научно-исследовательских отчетов (например, [8], [9]) о возможностях и перспективах применения технологии блокчейн и в целом технологий распределенного реестра в военной сфере, а также множество соответствующих академических научных работ (например, [10], [11], [12]).

Пример применения. Рассмотрим в качестве примера применение блокчейна в отношении управления информацией в военной инфокоммуникационной среде: использование блокчейна в качестве механизма для реализации отдельных меток доверенной информации [11]. В данном случае больше всего интересует использование блокчейнов для хранения метаданных, описывающих информацию, которая имеет решающее значение для обеспечения эффективного и безопасного управления информацией в военной инфокоммуникационной среде.

Каждая военной организация имеет определенную политику информационной безопасности. Внедрение политики обеспечивает то, что только уполномоченные лица имеют доступ к информации и могут изменять, удалять или раскрывать информацию. Как правило, в не электронной информационной среде документы имеют пометку об уровне секретности, например “совершенно секретно”. При традиционном подходе данные связываются с этими метаданными (т. е. маркировкой) на бумаге. Существуют стандартные методы привязки в случае цифровых документов. В качестве альтернативного подхода можно предложить использовать технологию блокчейн для реализации доверенного решения для хранения и распространения не привязанных меток. Такие метки включают в себя метаданные, описывающие объекты данных, но не привязанные напрямую к объектам данных и не хранимые вместе с ними. Преимущество решения на базе блокчейна по сравнению с традиционной PKI для реализации профиля привязки отдельных меток заключается в том, что оно обеспечивает более простую интеграцию с потенциальными союзниками, не являющимися участниками инфокоммуникационной среды организации. В случае контролируемого блокчейна используется отдельный механизм аутентификации, чтобы гарантировать, что только избранные объекты имеют доступ к данным, тем самым улучшая

подотчетность. Кроме того, блокчейн-решение может гарантировать неизменность сохраненных метаданных. Можно создать два реестра, один для хранения только данных, а второй для хранения метаданных и связанных с ними криптографических артефактов. Это гарантирует, что метаданные могут быть доступны для группы объектов, отличной от той, у которой есть доступ к данным. Это также потенциально повысит безопасность за счет разделения метаданных и данных. С помощью технологии блокчейн можно развернуть все представленные подходы к связыванию.

Безопасная привязка представлена отношением между объектом данных и его метаданными. Привязка может включать криптографический артефакт. Криптографический артефакт создается с использованием стандартизированного криптографического метода, такого как цифровая подпись или код аутентификации. Существуют три способа выполнения привязки:

1) объект данных вместе с метаданными инкапсулируются внутри привязки и представляются новым составным объектом данных.

2) привязка встроена в объект данных, и привязка содержит ссылку на объект данных.

3) метаданные хранятся в отдельной структуре от объекта данных с двумя связанными по ссылке. Существует несколько возможностей для реализации такой доверенной привязки:

а) Привязка содержит метаданные, криптографический артефакт и ссылку на объект данных.

б) Привязка содержит объект данных, криптографический артефакт и ссылку на метаданные.

в) Привязка содержит только ссылки на все элементы или имеет один из них и ссылку на другие.

В контексте блокчейна нас особенно интересует третий вариант привязки, описанный выше. Хотя распределенный реестр в принципе можно использовать для любой реализации третьего варианта привязки, представляется наиболее выгодным включать в блокчейн метаданные и криптографический объект, а также ссылку на объект данных. Этот случай предлагает два важных преимущества: 1) он прозрачен с точки зрения обработки и хранения исходных данных, так как не нужно добавлять/сохранять дополнительную информацию вместе с самим объектом данных; и 2) распределенный реестр обеспечивает общий репозиторий для информации метаданных, к которому могут обращаться пользователи.

Чтобы добиться доверенной привязки, необходима структура данных, которая может неизменяемым образом связать метку безопасности с объектом данных. При разработке такого профиля привязки на основе блокчейна возникает пара вопросов [11].

Прежде всего, согласно политике, только составитель данных может наносить на документ маркировку безопасности. Следовательно, по очевидной причине необходимо использовать контролируемый блокчейн, т. е. третья сторона не может публиковать потенциально преднамеренно неверные метаданные безопасности для объекта данных, принадлежащего кому-то другому. Такие действия могут привести к утечке данных и, возможно, к эксфильтрации конфиденциальных данных злоумышленником.

Во-вторых, в большинстве случаев, чтобы уменьшить нагрузку на управление безопасностью, блокчейн должен быть общедоступным для чтения, чтобы любая сторона, требующая доступа к данным или получающая данные, могла проверить требования безопасности для обработки и защиты конкретных данных. объект. Более того, хотя в целом метаданные, описывающие содержимое объекта данных, должны быть неизменными, сама маркировка безопасности может меняться со временем. Это может произойти либо из-за рассекречивания информации по прошествии определенного периода времени, либо из-за изменения некоторых предостережений относительно выпуска, включенных в маркировку. Обычно этот тип изменений является монотонным, и поэтому не принято удалять предостережения относительно выпуска в отношении данных, которые уже были выпущены. Однако возможность выполнять такие изменения в маркировке безопасности должна быть зарезервирована только для уполномоченных сторон и зарегистрирована как транзакция по изменению маркировки в блокчейне. Наконец, тот же блокчейн можно также использовать для записи обязательств сторон, которым были переданы

объекты данных, для обработки данных в соответствии с политикой безопасности создателя, что обеспечивает повышенную подотчетность потока данных.

Заключение. Технологии распределенного реестра, как и любые другие технологии, предназначены для решения конкретных задач. Современные тренды развития технологий распределенного реестра показывают возросший интерес к их применению в различных отраслях. Технологии уже оказали глубокое влияние на экономику и отрасли промышленности по всему миру, и их влияние будет продолжать расти. Технологии распределенного реестра можно использовать в различных конкретных областях военной сферы, включая повышение кибербезопасности, сокращение единых точек отказа при принятии экстренных решений, повышение эффективности оборонной логистики и операций цепочки поставок, а также повышение прозрачности аудита закупок. В конечном счете, у технологии блокчейна есть огромный потенциал, и это привело к тому, что во всем мире усилия в области исследований и разработок направлены на создание успешных систем технологии блокчейн, которые увеличат влияние и мощь стран по всему миру. Рассмотренный выше пример демонстрирует лишь один из многих возможных сценариев применения блокчейна в военной сфере.

Список использованных источников

1. ISO 22739:2020 Blockchain and distributed ledger technologies - Vocabulary. 2020
2. Secure Messaging Platform.The SBIR and STTR Programs. SBIR.gov. https://www.sbir.gov/node/1144411
3. Award Data. The SBIR and STTR Programs. SBIR.gov. https://www.sbir.gov/sbirsearch/award/all?firm=&topic=SB162-004
4. Galois and Guardtime Federal Awarded $1.8 Million DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System. Galois, Inc. https://galois.com/news/galois-guardtime-formal-verification/
5. NCI Agency innovation challenge. NCI Agency. https://www.ncia.nato.int/about-us/newsroom/nci-agency-innovation-challenge.html
6. European Defence Matters. Issue 14. 2017. https://eda.europa.eu/docs/default-source/eda-magazine/edm-issue-14_web.pdf
7. Partz H. South Korea State Defense Arm DAPA to Build Blockchain Platform for Military Acquisition // Cointelegraph.com. April 10, 2019. https://cointelegraph.com/news/south-korea-state-defense-arm-dapa-to-build-blockchain-platform-for-military-acquisition
8. Potential uses of blockchain by the U.S. Department of Defense. Report. Value Technology Foundation. March 2020.
9. Willink T.J. On blockchain technology and its potential application in tactical networks // Defence Research and Development Canada. DRDC - Ottawa Research Centre. Scientific Report. DRDC-RDDC-2018-R033. April 2018
10. Sudhan A., Nene M.J. Employability of blockchain technology in defence applications // 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 2017, pp. 630-637, doi: 10.1109/ISS1.2017.8389247.
11. Wrona K., Jarosz M. Does NATO Need a Blockchain? // MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 2018, pp. 667-672, doi: 10.1109/MILCOM.2018.8599845.
12. Kavya K.R., Kavitha M. Military Message Passing using Consortium Blockchain Technology // 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 1273-1278, doi: 10.1109/ICCES48766.2020.9138014.
13. Babu A. S., Supriya M. Blockchain Based Fog Computation Model For Military Vehicular Application // 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-6, doi: 10.1109/GCAT55367.2022.9971868.