Всероссийский конкурс исследовательских и проектных работ
школьников «Высший пилотаж»

Применение технологии blockchain для построения орбитального сервера

Исследовательская работа

Направление «*Спутникостроение и геоинформационные технологии: Terra Notum*»

Автор: Андреева Мария Александровна
учащийся 9 класса,
МАОУ «Классический лицей №1»
г. Ростов-на-Дону

2024 г.

Оглавление

Введение

Президент России Владимир Путин на заседании наблюдательного совета АНО «Россия – страна возможностей» сообщил: «У нас большие планы и по ближнему космосу, и по дальнему космосу. Здесь есть над чем работать, чем заниматься» [1].

Рис. 1. Встреча автора проекта с Президентом РФ В.В. Путиным на космодроме Восточный [2]

Цель работы – разработать программную оболочку распределенного реестра данных на основе BlockChain для построения орбитального сервера, базирующегося на космическом аппарате стандарта CubeSat.

В процессе работы были поставлены и последовательно решены следующие задачи:

– определены параметры сверхмалого космического аппарата;

– исследованы существующие блокчейн-технологии;

– собран и запрограммирован прототип-демонстратор кубсата;

– предложены направления развития проекта.

Описание проблемы

Суть дата-центров заключается в обеспечении конфиденциальности и полной неприкосновенность контента.

Этот вопрос стал особо актуален в банковской сфере, особенно при международных транзакциях: необходимо обеспечить защищённый доступ к данным в любой точке планеты [3]. Более того с распространением криптовалют и подобных цифровых активов, обладающих высокой ликвидностью, способы защиты и анонимности вышли на принципиально новый уровень.

Поясним: любые дата-центры (сервера) могут быть атакованы как через сеть виртуально, так и физически:

- санкции, ограничения на транзакции – мир глобален, следовательно, при возникновении вопросов в какой-либо юрисдикции возможен вариант введения ограничений на финансовые потоки и тем самым наносится экономический ущерб конечному бенефициару таких ресурсов
- физические атаки на дата-центры – несанкционированный доступ с выемкой оборудования, либо форс-мажорные обстоятельства (воздействие факторов непреодолимой силы, которые нельзя предвидеть или избежать, включая объявленную или фактическую войну, гражданские волнения, эпидемии, блокаду, землетрясения, наводнения, пожары, техногенные катастрофы и другие стихийные бедствия)
- выход из строя дата-центра из-за сбоя в системах энергопитания, локальные или веерные отключения доступа в сеть Интернет
- проникновение через удалённый доступ, хакерские атаки и воздействие вредоносного программного обеспечения

Также существует особо ценные данные, которые необходимо передать от одного абонента к другому. Если использовать сеть интернет, то есть вероятность отслеживания такого контента. Передача через курьеров тоже не решает вопрос безопасности: существует вероятность перехвата.

Каждая отличительная особенность технологии BlockChain (блокчейн) позволяет получить определенное технологическое решение обозначенных ранее проблем. Рассмотрим шесть технологий, которые позволяет достичь BlockChain:

- Одноранговое устройство сети — повышение надежности сохранения информации.
- Прямая передача данных и постоянный онлайн — ускорение обменом информацией.
- Алгоритм консенсуса — избавление от посредников.
- Алгоритм создания блоков — повышение доверия в сети.

- Запись информации в блоки, защищенные хешами — наблюдение всей истории изменений.
- Ассиметричное шифрование — обеспечение одновременной работы множества участников.

Технология BlockChain в первую очередь ориентирована на обеспечение высокого уровня надёжности хранения и валидации данных среди множества участников, не доверяющих друг другу.

Достигается это за счёт децентрализации принятия решения о добавлении новых записей и хранением локальной копии истории множеством участников.

Реализации BlockChain поддерживают работу умных контрактов. Основная идея умных контрактов заключается в следующем: при наступлении определенных условий, автоматически выполняется алгоритм, заданный в контракте. Например: при появлении записи о переводе некоторой суммы денежных средств от пользователя А пользователю В, происходит запись о передаче права на владение некоторой собственности от пользователя В пользователю А.

Технологическое решение

Проект основан на новых коммуникационных технологиях (распределённый реестр передачи данных в виде последовательности BlockChain); то есть обеспечение защиты коммуникационных линий от хакерских атак. В итоге орбитальный сервер, построенный на основе BlockChain, функционирует таким образом, что пользователь мгновенно узнает о вторжении в канал связи. При этом сам сервер находится на орбите – нет физического доступа, то есть нельзя украсть «флешку»; а хранилище на базируется на сверхмалых космических аппаратах (рис.2).

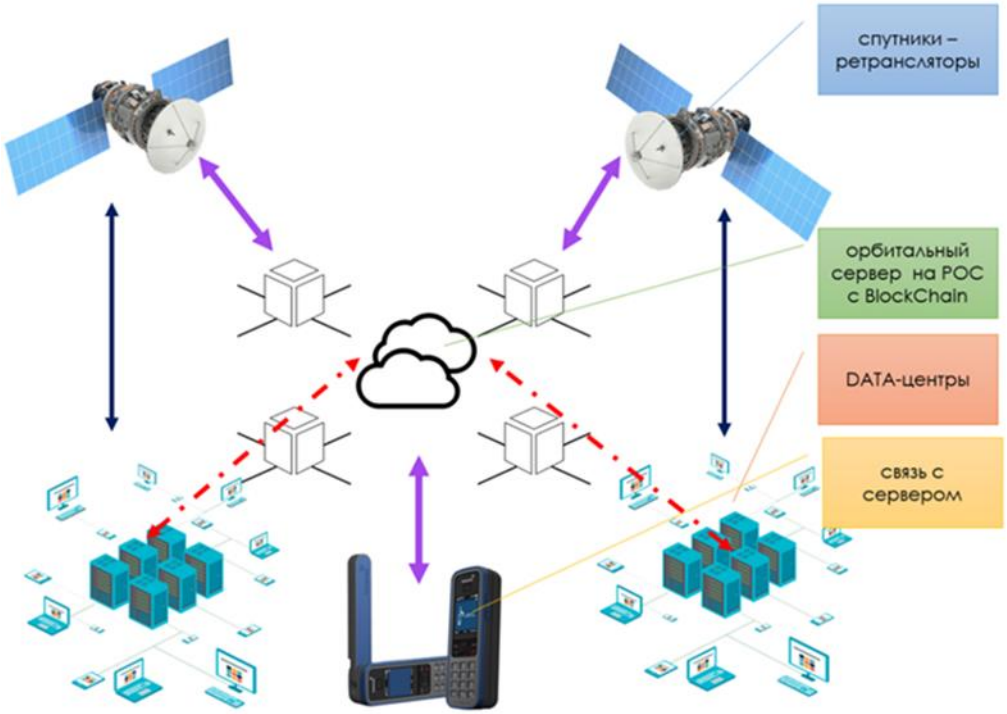

Рис. 2

Наноспутники

Сверхмалыми космическими аппаратами (наноспутники, СМКА) называются спутники, имеющие массу до 10 кг (рис. 3). Наиболее популярными являются наноспутники стандарта CubeSat (1U, 2U, 3U) [4]. Стандарт был разработан в 1999 году, первый CubeSat был запущен в 2003 г. К 2022 году зарегистрировано более 3500 проектов СМКА.

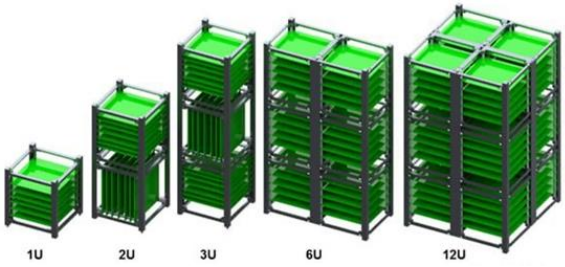

Рис. 3

В настоящее время наблюдается четвёртый этап развития наноспутников.

- Первый этап – доказательство возможности создания полноценного СМКА возникновение образовательных программ нового типа.
- Второй этап – отработка в космосе малоразмерных обеспечивающих систем, формирование рынка комплектующих.
- Третий этап – использование платформ CubeSat для отработки новых технологий и проведение экспериментов в космосе.
- Четвёртый этап – создание группировок СМКА, совместно решающие задачи, которые невозможно решать «большими КА».

Технологичность

- Современная электроника и материалы (COTS)
- Размеры 100х100х100 мм и малая масса (1 модуль до 1,5 кг)

Универсальность

- Обеспечение работы спектра полезных нагрузок
- Преемственность решений

Низкая стоимость

- Разработанные спецификации
- Запускается попутно

Блокчейн

Что такое Блокчейн? Блокче́йн (англ. blockchain — цепь из блоков) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хешсуммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы. При этом предыдущие блоки не затрагиваются. Если изменяемый блок последний в цепочке, то внесение изменений может не потребовать существенных усилий. Но если после изменяемого блока уже сформировано продолжение, то изменение может оказаться крайне трудоёмким процессом. Дело в том, что копии цепочек блоков хранятся на множестве разных кластерах независимо друг от друга [5].

Классификации и типы BlockChain (принято рассматривать три классификации):

- британская, предложенная Марком Уолпортом, главным научным консультантом правительства Великобритании, в отчете «Распределенная книга: за рамками блокчейна»;
- канадская, о которой рассказал создатель платформы Ethereum Виталий Бутерин во время доклада «О публичных и приватных блокчейнах»;
- российская, которую озвучила на конференции «блокчейн и открытые платформы» в 2016-м году зам. председателя Центробанка России Ольга Скоробогатова.

Компонентная база полезной нагрузки CubeSat

Бортовой вычислительный модуль (рис. 4) предназначен для управления спутником. Содержит устройства, такие как процессорный модуль Raspberry, контроллер системы ориентации, гироскоп и магнитометр, блок управления катушками, датчик температуры, таймер реального времени и система энергопитания. Плата весит 55 грамм и работает в диапазоне от -40 до +85ºC. Она имеет различные интерфейсы для подключения устройств и может быть программируема в ходе полета. Ее архитектура позволяет экономично использовать соответствующие микроконтроллеры для каждого режима работы. На ней мы планируем реализовывать систему хранения в виде RAID 1E.

Рис. 4

Базовая плата полезной нагрузки (рис.5) предназначена для разработки полезной нагрузки. Она содержит микроконтроллер с драйвером шины CAN, область для прототипирования и макетирования, а также электрическую принципиальную схему и программное обеспечение. Плата включает микроконтроллер, датчики температуры и питания, а также коммутаторы питания и датчики тока. Ее основные достоинства - проверенные решения с совместимостью с исходной архитектурой, возможность модификации исходного кода и обновление программного обеспечения во время полета. На ней будет происходить шифрование и обработка данных с использованием блокчейна.

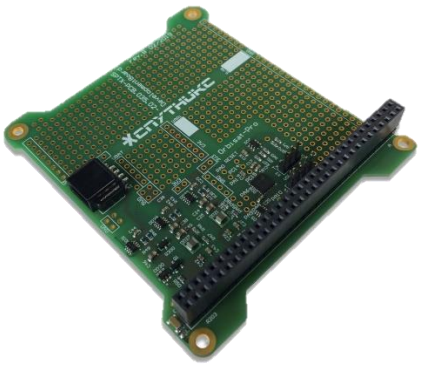

Рис. 5

Блокчейн представляет собой распределенную базу данных записей всех транзакций или цифровых событий, которые были выполнены и переданы участвующим сторонам. Чтобы понять, как работает блокчейн, очень важно детально разобраться в концепции хеширования. Любая сеть блокчейнов состоит из трех основных частей:

- Узел / блок: это основной строительный блок любой блокчейн. Он действует как база данных для хранения информации, относящейся ко всем транзакциям. Размер, период и событие запуска блоков различны для каждой блокчейн-цепочки. Каждый блок или узел содержит полную запись всех транзакций, которые когда-либо были записаны в этой блокчейн-цепочке.
- Сеть: Сеть состоит из «полных узлов».
- Хэш: он действует как цепочка, которая связывает один блок с другим, математически можно сказать, что он «связывает» все блоки вместе. Это одна из самых сложных для понимания концепций в блокчейне. Он склеивает блокчейны вместе и позволяет им создавать математическое доверие и поддерживать конфиденциальность, а также безопасность в сети. Хэш в блокчейне создается из данных, которые были в предыдущем блоке. Таким образом, хэш является отпечатком этих данных и блокирует блоки по порядку и времени.

Рис. 6

Материалы и методы исследования

Для выполнения проекта использовался ряд методов и оборудования. Ниже представлено описание использованных методов, экспериментального оборудования и средств обработки данных.

Блокчейн-технология использована для обеспечения безопасности и целостности данных, собираемых от кубсата и отправляемых на него. Благодаря распределенной и надежной структуре блокчейна, данные защищены от внешних воздействий и манипуляций.

В качестве системы для управления и мониторинга систем выл выбран микроконтроллер Arduino. Так же использовалась хеш-функция SHA 256. Этот алгоритм хеширования всегда выдает выходные данные фиксированной длины 256 бит или 32 байта, независимо от размера входной транзакции. Это означает, что если мы хэшируем два разных входных файла с использованием SHA-256 (рис. 7), скажем, один из них представляет собой фильм объемом 1 гигабайт, а другой – изображение объемом 5 килобайт, то в обоих случаях длина выходного хэша будет составлять 256 бит.

Рис. 7

Методы исследования:

1. Экспериментальный метод: Эксперименты были проведены с использованием 1U кубсата, чтобы собрать данные и информацию о его работе в космическом пространстве.

2. Технология блокчейн: Блокчейн-технология была использована для обеспечения безопасности и целостности данных, собираемых от кубсата. Благодаря распределенной и надежной структуре блокчейна, данные могли быть защищены от внешних воздействий и манипуляций.

3. Использование Arduino: Плата Arduino была выбрана для управления и мониторинга системы на кубсате. Это гибкая платформа для разработки и тестирования различных функций и сенсоров на кубсате.

Экспериментальное оборудование:

1. 1U кубсат: Кубсат размером 1U – это небольшой спутник, разработанный для выполнения определенных задач в космическом пространстве.

2. Arduino-плата: Для управления и мониторинга кубсата была использована плата Arduino. Она была связана с другими компонентами кубсата для выполнения задач, сбора данных и взаимодействия с блокчейн-технологией.

Средства обработки данных:

1. Программное обеспечение на Arduino: Было разработано программное обеспечение на языке программирования Arduino, которое позволило управлять и контролировать различные аспекты работы кубсата, необходимо для сбора и передачи данных с кубсата.

2. Система блокчейн: Для обеспечения безопасности данных, собранных с кубсата, была развернута система блокчейн. Данные, полученные от кубсата, были хешированы и записывались в блокчейн, что обеспечивало их надежность и невозможность вмешательства.

3. Средства анализа данных: Для анализа и интерпретации данных, собранных с кубсата, использовадись различные инструменты и программные средства, в зависимости от конкретных целей и задач исследования.

Также был использован RAID 1E (рис.8) для хранения данных. Он сочетает в себе превосходную скорость обработки данных с высоким уровнем надежности, не требуя при этом вычисления контрольных сумм. RAID 1E применяется для мощной графической станции.

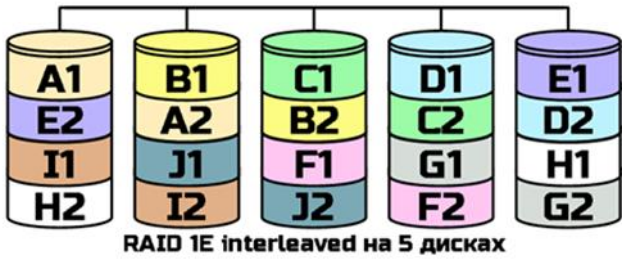

Рис. 8

В итоге, объединение технологии блокчейн и платформы Arduino в данном проекте позволило обеспечить безопасность и надежность данных, собранных с кубсата, и обеспечить управление и мониторинг его работы в космосе.

Анализ полученных результатов

Основные результаты и их ценность:

1. Зашифрованные данные:

Получение зашифрованных данных является важным достижением. Защита данных, собранных от кубсата, при помощи блокчейн-технологии гарантирует их

целостность и надежность. Это обеспечивает доверие к данным и предотвращает их манипуляцию.

2. Успешное проведение эксперимента:

Успешное выполнение эксперимента с 1U кубсатом свидетельствует о том, что планирование и реализация космической миссии были эффективными. Это подтверждает техническую компетентность и способность выполнения космических исследований.

Ценность результатов:

1. Научная ценность:

Получение зашифрованных данных и успешное проведение эксперимента могут представлять значимость в научных исследованиях. Эти данные могут быть использованы для изучения космической среды, выполнения научных экспериментов и расширения нашего знания о космосе.

2. Практическая ценность:

Результаты могут иметь практическое применение в области космических исследований и разработки космических технологий, например, для улучшения систем управления космическими аппаратами или разработки новых технологий связи и навигации в космосе.

В итоге, получение зашифрованных данных и успешное выполнение эксперимента с использованием технологии блокчейн и Arduino представляют важные шаги в космических исследованиях, способствуя научному и технологическому прогрессу и обеспечивая надежность и целостность данных из космоса [6].

Вывод

Эксперимент: Получение зашифрованных данных и успешное выполнение эксперимента с использованием технологии блокчейн и Arduino представляют важные шаги в космических исследованиях, способствуя научному и технологическому прогрессу и обеспечивая надежность и целостность данных из космоса.

Работа в космосе: Проект основан на новых коммуникационных технологиях (распределённый реестр передачи данных в виде последовательности BlockChain), обеспечивающих защиту коммуникационных линий от хакерских атак. В итоге, орбитальный сервер, построенный на основе BlockChain, функционирует таким образом, что пользователь мгновенно узнает о вторжении в канал связи. При этом сам сервер находится на орбите – нет физического доступа, то есть нельзя украсть «флешку»; а хранилище базируется на сверхмалых космических аппаратах. После успешного

эксперимента на кубсате, мы будем готовиться к установке дата-центра на Российской орбитальной станции (РОС).

Блокчейн является потенциальной технологией, которая может изменить наше привычное понимание компьютерных систем, и способна опередить классические централизованные системы в плане безопасности, отказоустойчивости и возможно в быстродействии. Но, к сожалению, он еще не получил достаточной популярности и доверия со стороны разработчиков. Блокчейну еще предстоит встать в первые ряды решений классических проблем компьютерных систем.

Распределенные реестры на основе наноспутников в отличие от существующих позволяют сформировать гибкую и независимую среду обмена анонимными данными с отсутствием физического доступа к системе.

Список источников

1. Путин сообщил, что у России большие планы по освоению и ближнего, и дальнего космоса. 19 июля 2023 г. URL: https://tass.ru/kosmos/18313585 (дата обращения 06.12.2023)

2. На космодроме «Восточный» Владимир Путин встретился с ученицей лицея из Ростова-на-Дону. URL: https://www.1tv.ru/news/2023-09-13/461179-na_kosmodrome_vostochnyy_vladimir_putin_vstretilsya_s_uchenitsey_litseya_iz_rostova_na_donu (дата обращения 06.12.2023)

3. Галанин И. И. Возможности применения технологии блокчейн в принятии решений // Материалы докладов XXIV Международной научно-технической конференции, посвященной 100-летию Нижегородской радиолаборатории «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ ИСТ-2018». — Нижний Новгород: Нижегородский государственный технический университет им. Р. Е. Алексеева, 2018. — с. 594–598. https://www.elibrary.ru/item.asp?id=42420867 (дата обращения 07.12.2023)

43. Макаров С. Б. Сверхмалые спутники готовы отправиться в космос / Высшая школа прикладной физики и космических технологий Института электроники и телекоммуникаций СПбПУ. 13.09.2022. URL: https://research.spbstu.ru/news/sverhmalye_sputniki_gotovy_otpravitsya_v_kosmos/ (дата обращения 06.12.2023)

5. Решение Федеральной службы по интеллектуальной собственности от 16 мая 2019 г. по заявке N 2016729454 Об оставлении в силе решения Роспатента в отношении «БЛОКЧЕЙН BLOCKCHAIN». URL: http://ivo.garant.ru/#/document/77984012 (дата обращения 07.12.2023)

6. Андреева, М. А. Применение технологии блокчейн для построения орбитального сервера / М. А. Андреева, О. А. Соколова. — Текст : непосредственный // Юный ученый. — 2023. — № 1 (64). — С. 31-33. — URL: https://moluch.ru/young/archive/64/3289/ (дата обращения: 15.01.2024).