УДК 004.56
doi:10.31799/1684-8853-2022-5-40-48
EDN: KJPXLT

Научные статьи
Articles

Построение архитектуры туманных вычислений с использованием технологии блокчейн

А. В. Пименов[а], *студент, orcid.org/0000-0002-9136-3514*
И. Р. Федоров[а], *аспирант, orcid.org/0000-0003-2422-4714*
С. В. Беззатеев[б], *доктор техн. наук, профессор, orcid.org/0000-0002-0924-6221, bezzateev_sergey@mail.ru*
[а]*Университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *по мере роста количества и многообразия устройств, подключенных к сети Интернет, растут требования как к производительности сети, так и к обеспечению безопасности хранения и передачи данных. Проблемы производительности решают, как правило, за счет облачных, туманных и граничных вычислений, а проблема безопасности хранения и передачи данных остается актуальной. Одним из эффективных путей ее решения является использование технологии блокчейн.* ***Цель:*** *проектирование архитектуры сети туманных вычислений на основе технологии блокчейн.* ***Результаты:*** *проведенные исследования в области туманных вычислений позволили определить требования к их архитектуре: автономность, масштабируемость, гибкость, иерархичность, безопасность, надежность, доступность, удобство обслуживания. Выделенные критерии построения архитектуры обусловили выбор в пользу частного блокчейна из-за его более высокой производительности по сравнению с открытым блокчейном. Проведен сравнительный анализ алгоритмов консенсуса, которые чаще других используются в частных блокчейнах, и выбран наиболее подходящий. В соответствии с установленными требованиями и результатами анализа спроектирована модель архитектуры туманных вычислений на основе частного блокчейна. Архитектура включает четыре элемента: конечные устройства, туманные узлы, узлы оркестрации и облачную инфраструктуру. В блокчейн входят туманные узлы и узлы оркестрации, за счет чего обеспечивается конфиденциальность, доступность и целостность данных в туманной сети.* ***Практическая значимость:*** *результаты исследования могут быть использованы при проектировании сетей туманных вычислений как по отдельности, так и в составе мобильных сетей 5G.*

Ключевые слова *— туманные вычисления, архитектура туманных вычислений, блокчейн, информационная безопасность, оркестрация, интернет вещей.*

Для цитирования: Пименов А. В., Федоров И. Р., Беззатеев С. В. Построение архитектуры туманных вычислений с использованием технологии блокчейн. *Информационно-управляющие системы*, 2022, № 5, с. 40–48. doi:10.31799/1684-8853-2022-5-40-48, EDN: KJPXLT

For citation: Pimenov A. V., Fedorov I. R., Bezzateev S. V. Designing fog computing architecture with the use of blockchain technology. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 5, pp. 40–48 (In Russian). doi:10.31799/1684-8853-2022-5-40-48, EDN: KJPXLT

Введение

В современном мире связь приобретает ключевое значение, и ее технологии быстро развиваются. На данный момент к сетям связи подключены миллиарды различных устройств, а к 2030 году даются прогнозы на десятки миллиардов подключенных устройств [1]. Существуют такие технологии, как интернет вещей (Internet of Things, IoT), которые предъявляют высокие требования к связи между устройствами. Общемировая цифровизация требует огромного количества используемых устройств, имеющих выход как минимум в локальную сеть, а зачастую и в облако [2].

С развитием технологии IoT во всех сферах возникают следующие проблемы: недостаток на устройствах вычислительных ресурсов и информационная безопасность (ИБ) данных, содержащихся в сети. Если проблему недостатка мощностей сегодня решают в основном за счет облачных, туманных и граничных вычислений, то проблема безопасности IoT-устройств стоит очень остро. Согласно данным ENISA (Агентство Европейского союза по сетям и информационной безопасности), инциденты с устройствами интернета вещей входят в тройку угроз с наибольшим финансовым ущербом для компаний.

На данный момент уже есть различные предложения по архитектуре туманных вычислений, однако они сталкиваются с определенными вопросами в области обеспечения ИБ данных и оптимизации потребления ресурсов у устройств, предоставляющих свои услуги для туманных вычислений. Эталонная архитектура OpenFog RA [3] предлагает решение проблем, однако не все варианты этих решений рассмотрены.

В 2018 году Национальный институт стандартов и технологий США сформулировал официальное определение термина туманные вычисления:

«Туманные вычисления — это многоуровневая модель, обеспечивающая повсеместный доступ к общей совокупности масштабируемых вычислительных ресурсов. Туманные узлы являются контекстно-зависимыми и поддерживают единую систему управления данными и организации связи. Туманные вычисления минимизируют время сетевого отклика поддерживаемых приложений, а также обеспечивают конечные устройства локальными вычислительными ресурсами и, при необходимости, сетевым подключением к централизованным сервисам».

В туманных вычислениях можно выделить следующие проблемы и угрозы ИБ [4–6].

1. Проблема аутентификации устройств. Чтобы получить доступ к службам сети тумана, устройство должно сначала стать частью сети, пройдя аутентификацию. Это представляет собой серьезную проблему, поскольку устройства ограничены различными параметрами.

2. Проблема безопасности беспроводной передачи данных. Обеспечение безопасности туманной сети затруднено из-за уязвимостей стандартных протоколов беспроводной передачи данных.

3. Проблема, связанная с доверием устройств внутри в сети. Устройства туманных вычислений часто разворачиваются без строгого контроля и защиты, поэтому они подвержены всем типам угроз безопасности.

4. Проблема конфиденциальности конечных пользователей. Узлы тумана находятся в непосредственной близости от конечных пользователей и могут собирать конфиденциальные данные.

5. Вредоносные атаки. Среда туманных вычислений может подвергаться многочисленным вредоносным атакам, и, таким образом, без удобных мер безопасности возможности сети могут быть серьезно подорваны.

Перечисленные проблемы не позволяют гарантировать конфиденциальность и целостность информации в туманных сетях. Это может привести к раскрытию конфиденциальных данных пользователей, сбою операций в сети, репутационным и материальным потерям корпораций. В данной работе мы рассматриваем возможность решения выявленных проблем с помощью технологии блокчейн.

Преимущества интеграции технологии блокчейн и туманных вычислений

Блокчейн — это технология хранения данных в цепочке последовательно связанных блоков. Каждый блок содержит уникальный код, называемый хешем. Блок также содержит хеш предыдущего блока в цепочке. После того как запись добавлена в цепочку, ее невозможно изменить. Несмотря на то, что блокчейн подвержен специфическим атакам, его широко используют при реализации различных проектов для решения актуальных проблем ИБ.

1. Защита от DDoS. Предполагается создание одноранговой сети доставки контента на основе неиспользуемой полосы пропускания участников сети. В проекте использовалась инфраструктура блокчейна Ethereum и предполагалась экономическая модель мотивации подключенных участников на основе собственного цифрового актива [7].

2. Безопасность конечных устройств интернета вещей. Регистрация устройства в доверенном распределенном реестре теоретически позволяет устранить различные уязвимости интернета вещей (обеспечение целостности прошивок устройств, проблемы с подключением и аутентификацией). Одним из базовых механизмов защиты устройств с помощью технологии блокчейн является хранение контрольной суммы метаданных ПО прошивки (версия, время обновления и т. п.) в блокчейне. Любое обновление сверяется с доверенным журналом-протоколом изменений, тем самым обеспечивается гарантия целостности устройства. На сегодня защита распределенных сетей является одним из наиболее перспективных прикладных применений технологии блокчейн в сфере ИБ. Стоит также отметить реализации распределенного реестра, нацеленные на защиту IoT (проект IOTA) [8].

3. Децентрализованная идентификация и аутентификация. Концепция децентрализованной идентификации с помощью блокчейна предполагает, что пользователи могут самостоятельно хранить свои персональные данные. Таким образом обеспечивается полный контроль над доступом к личной информации [9].

В целом можно выделить следующие основные преимущества от интеграции блокчейна и туманных вычислений.

1. Блокчейн позволяет обеспечивать целостность, доступность и конфиденциальность, т. е. ИБ данных в туманной сети.

2. Блокчейн решает проблему обеспечения аутентификации устройств в туманной сети.

3. Использование блокчейна повышает защиту сети от DoS, вредоносных и других атак, а также от помех и искажений самой сети. Конечно, блокчейн имеет свои уязвимости, однако использование частного блокчейна с нужным алгоритмом консенсуса позволяет нивелировать большинство из них.

4. Блокчейн позволяет обеспечивать постоянный мониторинг используемых и доступных ресурсов в каждом кластере сети или узле, т. е. повышается осведомленность внутри сети.

5. Участники туманных вычислений могут получать вознаграждение за счет предоставления своих ресурсов туманной сети, что создает мотивацию для участия в туманных вычислениях.

Проект модели туманных вычислений с использованием технологии блокчейн

Больше всего применений туманные вычисления находят в «умных» системах, которые требуют обработки информации в режиме реального времени: умные автомобили, дроны-доставщики, умные дома [10]. Все это можно объединить в рамки умного города, поэтому при проектировании модели будем отталкиваться от этого объекта.

Также надо иметь в виду уже выполненные исследования в области проектирования архитектуры туманных вычислений: OpenFog RA, NIST [11] и др. В ходе исследований мы использовали некоторые предложенные решения в построении архитектуры и придерживались принципов, определенных в OpenFog:

— автономность;
— масштабируемость;
— открытость;
— безопасность;
— RAS (надежность, доступность, удобство обслуживания);
— гибкость;
— иерархичность;
— программируемость.

Выделим основные употребляемые нами элементы.

1. Конечное устройство — основной клиент туманных служб. Может представлять собой умную машину, роутер, компьютер. Надо понимать, что в парадигме туманных вычислений датчики в туманной машине не обращаются напрямую в туман, а участвуют в граничных вычислениях, а сами граничные вычисления по необходимости могут обращаться в туман или облако. Одно конечное устройство могут обслуживать множество туманных узлов.

2. Туманный узел — основной элемент туманной сети. Он представляет собой физическое или виртуальное устройство, которое предоставляет вычислительные услуги туманной сети. Модели их развертывания такие же, как и у облачных вычислений.

3. Узел оркестрации — управляющий элемент в туманной сети. Он организует работу туманных узлов, ведет учет и мониторинг ресурсов, управляет событиями и имеет прочие организующие функции, необходимые для нормального функционирования туманной сети. Каждый узел управляет одним гибким сегментом туманной сети.

4. Облачная инфраструктура — туманные вычисления разрабатывались как дополнение к облаку, поэтому архитектура туманных вычислений должна учитывать связь с облачной инфраструктурой для различных «тяжелых» вычислений или хранения большого количества информации.

Модель открытого блокчейна не подходит по многим причинам. Во-первых, она не обеспечивает соблюдение всех аспектов ИБ данных, а именно конфиденциальности. В туманных вычислениях может содержаться множество конфиденциальной информации, к тому же она обрабатывается близко к конечным устройствам, что может позволить установить личность владельца. Во-вторых, открытый блокчейн требует много ресурсов на подтверждение транзакций, что критично для туманных вычислений, так как они должны поддерживать системы реального времени. В проведенном исследовании [12] производительности открытого блокчейна Ethereum и частного блокчейна Hyperledger Fabric доказано, что производительность частного блокчейна выше в несколько десятков раз и может быть выше даже в сотни раз. Еще у открытых блокчейнов существует проблема масштабируемости, что также критично для туманных вычислений. В-третьих, мы не можем полностью доверять туманным узлам, так как не можем контролировать их развертывание. Даже авторизованное устройство может использоваться злоумышленником для атаки на туманную сеть.

Это приводит к тому, что требуется рассматривать архитектуру частных или гибридных блокчейнов. Использование частного блокчейна по сравнению с открытым блокчейном несет следующие преимущества.

1. Конфиденциальность. Используя частный блокчейн, можно быть уверенным, что передаваемая и хранимая информация в туманных сетях будет иметь аспект конфиденциальности ИБ данных.

2. Низкое потребление ресурсов. Алгоритмы консенсуса у частного блокчейна требуют меньшего количества участия узлов, что приводит к снижению потребления пропускной способности у узлов и уменьшению накладных расходов.

3. Обеспечение доверия внутри сети. Главные узлы (узлы оркестрации) будут разворачиваться под контролем, что повышает уровень доверия внутри сети.

Использование гибридного блокчейна в рамках данной статьи не будем затрагивать, так как, несмотря на его преимущества с точки зрения распределения прав, он требует подробного изучения и анализа в качестве платформы для взаимодействия устройств в туманных вычислениях. Прежде чем приступать к его изучению, следует

рассмотреть варианты построения архитектуры с помощью частного блокчейна, и, уже зная ее недостатки, можно устранять их с помощью гибридного блокчейна.

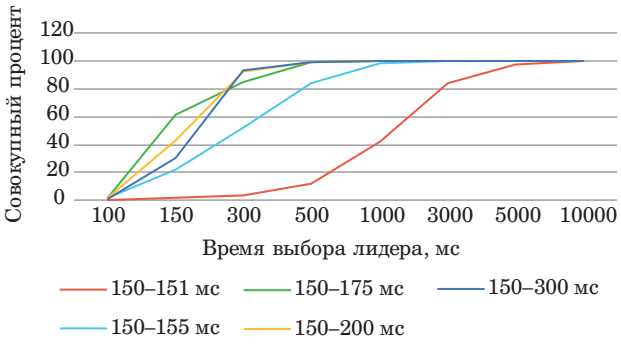
Второй немаловажной деталью является алгоритм консенсуса. На данный момент не существует специализированного алгоритма консенсуса для туманных вычислений. В настоящей работе рассмотрены следующие алгоритмы консенсуса: PBFT, PoAh, PoA и Raft. Выбор этих алгоритмов обусловлен их распространением в исследованиях, связанных с алгоритмами консенсусов частных блокчейнов и архитектур для IoT, граничных и туманных вычислений [13–17]. В рамках данного исследования не будем подробно останавливаться на принципах работы алгоритмов, а рассмотрим их специфику, производительность, преимущества и недостатки. Проведя сравнительный анализ, выберем алгоритм или предложим альтернативу на основе предложенных алгоритмов.

Алгоритм PBFT является одним из основных алгоритмов для частных блокчейнов. Популярная блокчейн-платформа Hyperledger Fabric использует этот алгоритм консенсуса, что дает высокую эффективность, устойчивость к сбоям и обеспечивает работу до участия трети неисправных узлов. Главным недостатком PBFT является низкая масштабируемость.

Алгоритм консенсуса PoA — довольно популярное решение среди различных предприятий и компаний. В нем каждый валидатор является абсолютно доверенным узлом за счет его разворачивания доверенным участником. Главным преимуществом алгоритма PoA является более высокая эффективность по сравнению с PoW, простота и масштабируемость [18, 19]. Из недостатков можно выделить слабую производительность по сравнению с более производительными алгоритмами и отсутствие мотивации для рядовых участников в блокчейне. Невозможность задать мотивацию является достаточно серьезным недостатком, который будет рассмотрен ниже.

Одним из алгоритмов, который тоже получил широкое распространение, является Raft. Его особенностью является то, что в блокчейне присутствует выборный лидер и его подписчики, которые синхронизируют свои узлы с ним. Это обеспечивает простоту, надежность, высокую эффективность (решения принимает один узел-лидер) и масштабируемость, однако требует дополнительных задержек и ресурсов на проведение выборов (рис. 1).

Кроме широко используемых алгоритмов консенсуса, рассмотрим алгоритм PoAh, который был предложен для применения в крупных сетях IoT. Этот алгоритм предназначен для решения проблемы высокого потребления ресурсов иными



■ ***Рис. 1.*** Анализ достижения выбора лидера при различных значениях тайм-аута

■ ***Fig. 1.*** Aanalysis of achieving leader election at different timeout values

алгоритмами консенсуса в маломощных устройствах IoT. Он содержит механизм аутентификации с цифровой подписью для доступа и проверки блока. В нем также вводятся уровни доверия, которые имеют базовое значение и меняются со временем в зависимости от качества работы узла. Соответственно, доверенные узлы, которые могут доказать свою идентичность, участвуют в консенсусе. Такой подход существенно снижает расходы за счет того, что современные асимметричные методы шифрования очень быстры. Несмотря на то, что применение PoAh больше подходит для граничных вычислений, где участвуют преимущественно маломощные устройства, идеи этого алгоритма консенсуса тоже можно использовать в туманных вычислениях.

Результаты исследований внесены в таблицу.

Как видно из таблицы, в исследованиях проводился анализ различных частей того или иного алгоритма консенсуса (в Raft исследуется скорость выбора лидера, а, например, в PoAh анализируется скорость аутентификации устройства и ответа от блокчейна). Кроме того, видны различия по характеристикам и архитектуре среды тестирования, что несколько усложняет сравнение различных алгоритмов, поэтому при выборе алгоритма консенсуса будем отталкиваться от потребностей нашей архитектуры.

Выделим основные требования, которые должны обеспечивать туманные вычисления в рамках умного города:

1) поддержка систем реального времени;

2) оказание услуг по обработке и хранению данных;

3) обеспечение высокого уровня ИБ данных в туманной сети;

4) мотивация рядовых участников для предоставления ресурсов туманным вычислениям;

5) реализация принципов гибкости, масштабируемости и иерархичности сети;

■ Результат анализа производительности алгоритмов консенсуса
■ The result of the consensus algorithms' performance analysis

Алгоритм консенсуса	Производительность консенсуса	Характеристики макета (виртуальной машины)	Комментарии
PBFT	Максимальное TPS: 45 Задержка для 50 транзакций: 1,5 с	Intel i7-7700k, ОЗУ 32 ГБ, жесткий диск 512 SSD. Построен в Hyperledger Fabric	Анализ производительности в исследованиях дал примерно одинаковый результат даже при различных характеристиках испытательного стенда, так как блокчейн не потребляет все ресурсы в ОС
	Максимальное TPS: 52 Задержка для 50 транзакций: 1,29 с	4 ядра Intel Cascade Lake, 8 Гб оперативной памяти, ОС Ubuntu 20 LTS, 20 Гб HDD. Построен в Hyperledger Fabric	
PoAh	Создание, заполнение транзакциями и интегрирование блока размером 35 байт за 3,34 с	Шесть одноплатных компьютеров Raspberry Pi	Для анализа производительности применялись маломощные устройства, симулирующие IoT
	Для различных услуг разное время выполнения: от 4 до 10 с	Dell Alienware Aurora R11 Core i7 Смоделировано 50 устройств	
PoA	TPS: 14 Задержка подтверждения транзакции: 5 мин	Нет информации	–
Raft	Для стандартного тайм-аута (150–300 мс) время определения лидера достигает 3 с	5 нод, подключенных через Ethernet-коммутатор 1 Гбит/с, со средним временем трансляции 15 мс	Основное беспокойство вызывает достижение состояния определения лидера, так как без него блокчейн-сеть не может выполнять свои функции. Производительность алгоритма при определенном лидере высока, так как транзакции выполняет только один узел, а остальные синхронизируются с ним

6) простота как для использования клиентами, так и для участия в качестве туманного узла;

7) поддержка автономности кластера в случае отказа узла оркестрации.

В соответствии с этими требованиями мы предлагаем архитектуру туманных вычислений с интеграцией частного блокчейна. Она также будет состоять из четырех элементов, но с некоторыми особенностями.

1. Конечное устройство (клиент). При необходимости оказания услуг клиент обращается к ближайшему туманному узлу. Кроме информации о требовании, предъявляемом к запрашиваемой услуге, клиент должен предоставить метаданные для определения приоритета выделения услуги по обработке данных (системы реального времени будут иметь приоритет выше, чем, например, системы коммунальных датчиков). Также клиент должен пройти регистрацию и получить секретный и открытый ключ. Открытый ключ имеется у всех узлов оркестрации в туманной сети.

2. Туманные узлы. В рамках данной архитектуры туманные узлы входят в некоторый кластер, который управляется одним из узлов оркестрации. Сами кластеры являются гибкими, и узлы могут как входить в них, так и выходить в зависимости от решения узла оркестрации. Узлы, кроме обработки и хранения данных, должны регулярно передавать в узел оркестрации данные о своем состоянии и информацию о своих ресурсах. Туманный узел собирает и отправляет в узел оркестрации запросы на услуги клиентов. Каждый туманный узел входит в блокчейн, однако не участвует в подтверждении транзакций из-за проблем доверия к ним и экономии ресурсов. Операции, которые назначаются узлом оркестрации, оформляются в виде смарт-контракта, который включает в себя контейнер с исполняемыми инструкциями и окружением или блоки для хранения, а также вознаграждение за оказываемую услугу. Это позволит мотивировать частные лица для участия в туманных вычислениях.

Для непосредственного участия в туманных вычислениях узел должен пройти аутентификацию и выбрать объем ресурсов и определенные условия для их представления (например, если заряд батареи на мобильном устройстве ниже 50 %).

3. Узлы оркестрации. Каждый узел выполняет свои обязанности в своем кластере. Кроме того, именно эти узлы участвуют в алгоритме консенсуса и, соответственно, ведут учет бухгалтерской книги и подтверждают транзакции. Также именно эти узлы имеют связь с облачной инфраструктурой.

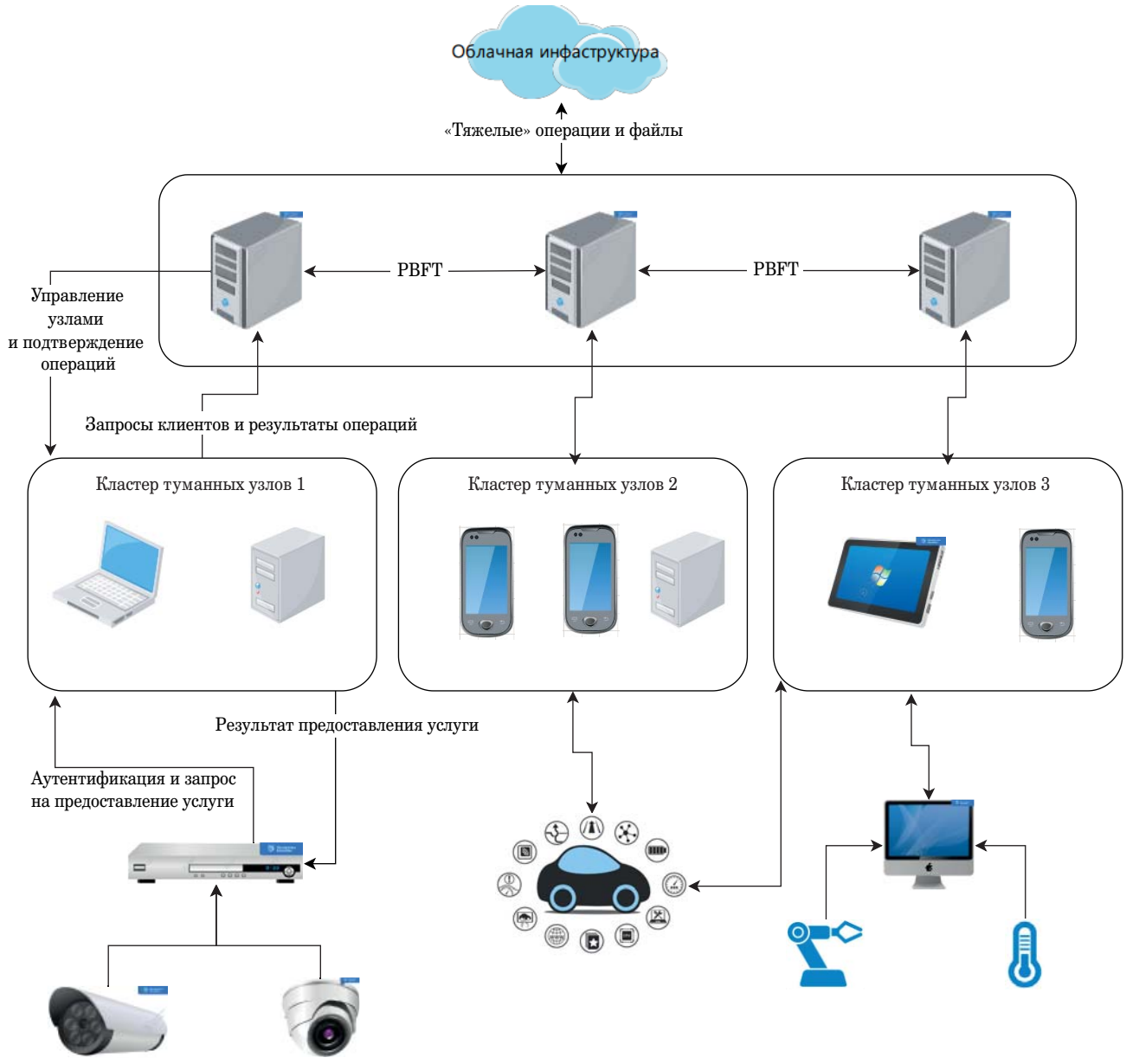
4. Облачная инфраструктура. Облако лежит за пределами туманных вычислений, поэтому архитектура на него не распространяется. Однако сообщение между блокчейном и облаком выглядит также перспективным направлением для исследований [20].

На основании описанных выше требований и архитектуры можно выделить следующие критерии, которым должен удовлетворять алгоритм консенсуса:

1) поддержка работы алгоритма частными блокчейн-платформами;

2) поддержка системы мотивации участников;

3) возможность масштабируемости при увеличении числа узлов в сети.



■ ***Рис. 2.*** Общий вид архитектуры туманных вычислений с использованием технологии блокчейн

■ ***Fig. 2.*** General view of fog computing architecture using blockchain technology

Также при выборе стоит обращать внимание на скорость подтверждения транзакций и накладные расходы в случае, если алгоритм требует выбора узла лидера.

В качестве алгоритма консенсуса для узлов оркестрации выберем PBFT, так как он в большей степени соответствует заявленным критериям, и в нашей архитектуре небольшое количество узлов, которые принимают участие в консенсусе.

Алгоритм Raft тоже годится для использования, однако он требует выбора узла лидера, что нам не подходит, так как во время выборов сервер становится недоступен для оказания услуг свыше 3 с, а при сетевых задержках это время может еще увеличиться, что делает этот алгоритм неподходящим для туманных вычислений. Кроме того, Raft не поддерживается всеми блокчейн-платформами, в отличие от PBFT, который является классическим алгоритмом для приватного блокчейна.

Алгоритм PoA не подходит из-за того, что в нем невозможно задать мотивацию для участия рядовых узлов, которая крайне важна для реализации действительно качественной и расширяемой архитектуры. Кроме того, у него низкая скорость подтверждения транзакций, что также делает его применение невозможным в туманных вычислениях.

Алгоритм PoAh выглядит перспективным для использования в гибридном блокчейне, однако мы не будем рассматривать данный класс блокчейна в этой работе вследствие ограниченности по тематике и объему.

Общий вид архитектуры представлен на рис. 2.

Из преимуществ данной архитектуры можно выделить следующие принципы, поддерживаемые ею:

— безопасность;
— масштабируемость;
— открытость;
— RAS (надежность, доступность, удобство обслуживания);
— гибкость;
— иерархичность.

Существуют проблемы с автономностью кластеров, так как они полностью зависимы от узла оркестрации, и отказ его работы может привести к краху существенной части туманной сети. В таком случае оставшиеся работоспособные узлы оркестрации должны временно взять на себя обязанности выбывшего узла, это также возможно за счет использования технологии блокчейн.

Одним из основных преимуществ использования блокчейна является обеспечение конфиденциальности, доступности и целостности данных в нем. Это достигается за счет использования криптографических средств, хранения хешей файлов и метаданных операций в блокчейне, а также шардирования хранимых файлов в туманной сети.

Заключение

В ходе анализа существующих предложений по архитектуре туманных вычислений выявлены проблемы, связанные с обеспечением ИБ данных, оркестрацией и неясным разделением туманных узлов, которые предоставляют услуги клиентам. Кроме того, установлено, что все разрабатываемые архитектуры не учитывают мотивацию участия частных лиц в туманной сети, что крайне важно для общественных туманных вычислений. Предлагаемая архитектура решает эти проблемы с помощью внедрения частного блокчейна, который благодаря своим свойствам позволяет безопасно пользоваться услугами туманных вычислений, а также дает мотивацию за счет вознаграждения участников туманных вычислений. Однако данная архитектура требует развертывания базовой части туманной сети и финансирования, при этом обеспечивает наибольшую жизнеспособность в рамках общественной работы и поддержания таких систем, как умная транспортная сеть и система доставки с помощью дронов.

Литература

1. **Галактионов М. А., Маколкина М. А., Киричек Р. В.** Обзор протоколов сетей связи шестого поколения и сетей 2030. *СПбНТОРЭС: тр. ежегодной НТК*, 2021, № 1, с. 183–186. https://conf-ntores.etu.ru/assets/files/2021/cp/papers/183-186.pdf (дата обращения: 21.06.2022).
2. **Плотников В. А.** Цифровизация производства: теоретическая сущность и перспективы развития в российской экономике. *Известия Санкт-Петербургского государственного экономического университета*, 2018, № 4, с. 16–24.
3. **Abdulkareem K. H., Mohammed M. A., Gunasekaran S. S., Almhiqani M. N., Mutlag A. A., Mostafa S. A., Ali N. S., Dheyaa A. I.** A Review of fog computing and machine learning: Concepts, applications, challenges, and open issues. *IEEE Global Communications Conf. (GLOBECOM)*, 2019, pp. 1–6, doi:10.1109/ACCESS.2019.2947542
4. **Khan S., Qin Y., Parkinson S.** Fog computing security: A review of current applications and security solutions. *Journal of Cloud Computing*, 2017, vol. 6, no. 19, pp. 1–22. doi:10.1186/s13677-017-0090-3
5. **Velasquez K., Abreu D., Assis M., Senna C., Aranha D., Bittencourt L., Laranjeiro N., Curado M., Viei-**

ra M., Monteiro E., Madeira E. Fog orchestration for the internet of everything: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 2019, no. 9, pp. 1–23. doi:10.1186/s13174-018-0086-3
6. **Khalid F.** Privacy and security problems in fog computing. *Communications on Applied Electronics*, 2016, no. 4, pp. 1–7. doi:10.5120/cae2016652088
7. **Ren S., Liu B., Yang F., Wei X., Yang X., Wang C.** BlockDNS: Enhancing domain name ownership and data authenticity with blockchain. *IEEE Global Communications Conf. (GLOBECOM)*, 2019, pp. 1–6. doi:10.1109/GLOBECOM38437.2019.9013817
8. **Conti M., Kumar G., Nerurkar P., Saha R., Vigneri L.** A survey on security challenges and solutions in the IOTA. *Journal of Network and Computer Applications*, 2022, vol. 203, pp. 1–27. doi:10.1016/j.jnca.2022.103383
9. **Тюкалова Н. М., Разувакин А. А.** Современная концепция цифровой идентификации авиапассажиров. *Научный Вестник МГТУ ГА*, 2018, т. 21, № 4, с. 39–47. doi:10.26467/2079-0619-2018-21-4-39-47
10. **Mahmood Z., Ramachandran M.** Fog computing: Concepts, principles and related paradigms. *Fog Computing: Concepts, Frameworks and Technologies*. Springer, 2018. Pp. 3–21. doi:10.1007/978-3-319-94890-4_1
11. **Iorga M., Feldman L., Barton R., Martin M., Goren N., Mahmoudi C.** *Fog Computing Conceptual Model*. Special Publication (NIST SP). National Institute of Standards and Technology, 2018. doi:10.6028/NIST.SP.500-325. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf (дата обращения: 21.06.2022).
12. **Федоров И. Р., Пименов А. В., Панин Г. А., Беззатеев С. В.** Технология блокчейн в сетях 5G: сравнение производительности приватных и публичных блокчейнов. *Проблемы информационной безопасности. Компьютерные системы*, 2021, № 3(47), с. 55–62.
13. **Pahlajani S., Kshirsagar A., Pachghare V.** Survey on private blockchain consensus algorithms. *1st Intern. Conf. on Innovations in Information and Communication Technology (ICIICT)*, 2019, pp. 1–6. doi:10.1109/ICIICT1.2019.8741353
14. **Puthal D., Mohanty S., Yanambaka V., Kougianos E.** PoAh: A novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks. *arXiv: CS – Cryptography and Security*, 2020, pp. 1–26. doi:10.48550/arXiv.2001.07297
15. **Dongyan H., Xiaoli M., Shengli Z.** Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020, vol. 50, iss. 1, pp. 172–181. doi:10.1109/TSMC.2019.2895471
16. **Saide Z., Zhipeng C., Huafu H., Yingshu L., Wei L.** zkCrowd: A hybrid blockchain-based crowdsourcing platform. *IEEE Transactions on Industrial Informatics*, 2020, vol. 16, iss. 6, pp. 4196–4205. doi:10.1109/TII.2019.2941735
17. **Latif S., Idrees Z., Ahmad J., Lirong Z., Zou Z.** A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, 2021, vol. 21. doi:10.1016/j.jii.2020.100190
18. **Kaur M., Khan M. Z., Gupta S., Noorwali A., Chakraborty C., and Pani S. K.** MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. *IEEE Access*, 2021, vol. 9, pp. 80931–80944. doi:10.1109/ACCESS.2021.3085187
19. **Schäffer M., Di Angelo M., Salzer G.** Performance and scalability of private ethereum blockchains. *Business Process Management: Blockchain and Central and Eastern Europe Forum. Lecture Notes in Business Information Processing*. Springer, 2019. No. 361. Pp. 103–118. doi:10.1007/978-3-030-30429-4_8
20. **Беззатеев С. В., Федоров И. Р.** Технология блокчейн в сетях 5G. *Научно-технический вестник информационных технологий, механики и оптики*, 2020, т. 20, № 4(128), с. 472–484. doi:10.17586/2226-1494-2020-20-4-472-484

UDC 004.56
doi:10.31799/1684-8853-2022-5-40-48
EDN: KJPXLT

Designing fog computing architecture with the use of blockchain technology

A. V. Pimenov[a], Student, orcid.org/0000-0002-9136-3514
I. R. Fedorov[a], Post-Graduate Student, orcid.org/0000-0003-2422-4714
S. V. Bezzateev[b], Dr. Sc., Tech, Professor, orcid.org/0000-0002-0924-6221, bezzateev_sergey@mail.ru
[a]ITMO University, 49, Kronverksky Pr., 197101, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Due to the growth in the number and variety of devices connected to the Internet, the requirements for network performance and data transmission security are increasing. Today, performance problems are usually solved through cloud, fog and

edge computing, while the problem of data storage and transmission security remains relevant. One of the effective ways to solve this problem is to use blockchain technology. **Purpose:** Designing the architecture of a fog computing network based on blockchain technology. **Results:** Based on the research in the field of fog computing, the requirements for the fog computing architecture were determined, such as: autonomy, scalability, flexibility, hierarchy, security, reliability, availability, serviceability. The selected criteria for building an architecture led to the choice in favor of a private blockchain due to its higher performance compared to a public blockchain A comparative analysis of the consensus algorithms that are most often used in private blockchains was carried out and the most suitable one was chosen. Based on the requirements put forward and the results of the analysis, a fog computing architecture model based on a private blockchain was designed. The architecture consists of four elements: end devices, fog nodes, orchestration nodes, and cloud infrastructure. The blockchain includes fog nodes and orchestration nodes, which ensures the confidentiality, availability and integrity of data in the fog network. **Practical relevance:** Paper results can be used in the design of fog computing networks both separately and as part of 5G mobile networks.

Keywords — fog computing, fog computing architecture, blockchain, information security, orchestration, Internet of Things.

For citation: Pimenov A. V., Fedorov I. R., Bezzateev S. V. Designing fog computing architecture with the use of blockchain technology. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 5, pp. 40–48 (In Russian). doi:10.31799/1684-8853-2022-5-40-48, EDN: KJPXLT

References

1. Galaktionov M. A., Makolkina M. A., Kirichek R. V. Overview of the protocols of the sixth generation communication networks and networks 2030. *SPbNTORES: tr. ezhegodnoj NTK* [Proc. 76th Scientific and Technical Conference of St. Petersburg NTO RES im. A. S. Popova, Dedicated to the Radio Day]. Saint-Petersburg, 2021, no. 1, pp. 183–186. Available at: https://conf-ntores.etu.ru/assets/files/2021/cp/papers/183-186.pdf (accessed 21 June 2022) (In Russian).
2. Plotnikov V. A. Digitalization of production: the theoretical essence and development prospects in the Russian economy. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta*, 2018, no. 4, pp. 16–24 (In Russian).
3. Abdulkareem K. H., Mohammed M. A., Gunasekaran S. S., Almhiqani M. N., Mutlag A. A., Mostafa S. A., Ali N. S., Dheyaa A. I. A review of fog computing and machine learning: Concepts, applications, challenges, and open issues. *IEEE Global Communications Conf. (GLOBECOM)*, 2019, pp. 1–6. doi:10.1109/ACCESS.2019.2947542
4. Khan S., Qin Y., Parkinson S. Fog computing security: A review of current applications and security solutions. *Journal of Cloud Computing*, 2017, vol. 6, no. 19, pp. 1–22. doi:10.1186/s13677-017-0090-3
5. Velasquez K., Abreu D., Assis M., Senna C., Aranha D., Bittencourt L., Laranjeiro N., Curado M., Vieira M., Monteiro E., Madeira E. Fog orchestration for the internet of everything: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 2019, no. 9, pp. 1–23. doi:10.1186/s13174-018-0086-3
6. Khalid F. Privacy and security problems in fog computing. *Communications on Applied Electronics*, 2016, no. 4, pp. 1–7. doi:10.5120/cae2016652088
7. Ren S., Liu B., Yang F., Wei X., Yang X., Wang C. BlockDNS: Enhancing domain name ownership and data authenticity with blockchain. *IEEE Global Communications Conf. (GLOBECOM)*, 2019, pp. 1–6. doi:10.1109/GLOBECOM38437.2019.9013817
8. Conti M., Kumar G., Nerurkar P., Saha R., Vigneri L. A survey on security challenges and solutions in the IOTA. *Journal of Network and Computer Applications*, 2022, vol. 203, pp. 1–27. doi:10.1016/j.jnca.2022.103383
9. Tyukalova N. M., Razuvakin A. A. Modern concept of digital identification of air passengers. *Civil Aviation High Technologies*, 2018, vol. 21, no. 4, pp. 39–47 (In Russian). doi:10.26467/2079-0619-2018-21-4-39-47
10. Mahmood Z., Ramachandran M. *Fog computing: Concepts, principles and related paradigms*. In: *Fog Computing: Concepts, Frameworks and Technologies*. Springer, 2018. Pp. 3–21. doi:10.1007/978-3-319-94890-4_1
11. Iorga M., Feldman L., Barton R., Martin M., Goren N., Mahmoudi C. *Fog Computing Conceptual Model*. Special Publication (NIST SP). National Institute of Standards and Technology, 2018. doi:10.6028/NIST.SP.500-325. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf (accessed 21 June 2022).
12. Fedorov I. R., Pimenov A. V., Pamim G. A., Bezzateev S. V. Blockchain in 5G networks: Perfomance comparison of private and public blockchain. *Information Security Problems. Computer Systems*, 2021, no. 3(47), pp. 55–62 (In Russian).
13. Pahlajani S., Kshirsagar A., Pachghare V. Survey on private blockchain consensus algorithms. *1st Intern. Conf. on Innovations in Information and Communication Technology (ICIICT)*, 2019, pp. 1–6. doi:10.1109/ICIICT1.2019.8741353
14. Puthal D., Mohanty S., Yanambaka V., Kougianos E. PoAh: A novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks. *arXiv: CS — Cryptography and Security*, 2020, pp. 1–26. doi:10.48550/arXiv.2001.07297
15. Dongyan H., Xiaoli M., Shengli Z. Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020, vol. 50, iss. 1, pp. 172–181. doi:10.1109/TSMC.2019.2895471
16. Saide Z., Zhipeng C., Huafu H., Yingshu L., Wei L. zkCrowd: A hybrid blockchain-based crowdsourcing platform. *IEEE Transactions on Industrial Informatics*, 2020, vol. 16, iss. 6, pp. 4196–4205. doi:10.1109/TII.2019.2941735
17. Latif S., Idrees Z., Ahmad J., Lirong Z., Zou Z. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, 2021, vol. 21. doi:10.1016/j.jii.2020.100190
18. Kaur M., Khan M. Z., Gupta S., Noorwali A., Chakraborty C., and Pani S. K. MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. *IEEE Access*, 2021, vol. 9, pp. 80931–80944. doi:10.1109/ACCESS.2021.3085187
19. Schäffer M., Di Angelo M., Salzer G. *Performance and scalability of private ethereum blockchains*. In: *Business Process Management: Blockchain and Central and Eastern Europe Forum. Lecture Notes in Business Information Processing*. Springer, 2019. Vol. 361. Pp. 103–118. doi:10.1007/978-3-030-30429-4_8
20. 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(128), pp. 472–484 (In Russian). doi:10.17586/2226-1494-2020-20-4-472-484