THE CURRENT STATE OF BLOCKCHAIN TECHNOLOGY: PROBLEMS AND DIRECTION OF DEVELOPMENT

Zaytsev V.,
Professor at the Department of Computational Mathematics and Programming
Moscow Aviation Institute (National Research University), Moscow, Russia
Horielyshev S.
Graduate student
Moscow Aviation Institute (National Research University), Moscow, Russia

СОВРЕМЕННОЕ СОСТОЯНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙНА: ПРОБЛЕМЫ И НАПРАВЛЕНИЕ РАЗВИТИЯ

Зайцев В. Е.
Професор кафедри «Вычислительная математика и программирование»
Московский авиационный институт (Национальный исследовательский университет), Москва, Россия
Горелышев С. С.
Аспирант
Московский авиационный институт (Национальный исследовательский университет), Москва, Россия
https://doi.org/10.5281/zenodo.11390817

Abstract

The article analyzes the most popular and productive blockchain technologies, which made it possible to identify and summarize their advantages and disadvantages from the point of view of technical implementation. Promising directions for improving blockchain technologies have been identified: the use of directed acyclic graphs, sharding technology, as well as improving the consensus algorithm.

Аннотация

В статье проведен анализ наиболее популярных и производительных блокчейн-технологий, который позволил выявить и обобщить их преимущества и недостатки с точки зрения технической реализации. Определены перспективные направления усовершенствования блокчейн-технологий: использование направленных ациклических графов, технологию шардинга, а также усовершенствование алгоритма консенсуса.

Keywords: blockchain technology, sharding, consensus algorithms, decentralization, security, scalability.

Ключевые слова: технология блокчейна, шардинг, алгоритм консенсуса, децентрализация, безопасность, масштабируемость.

Введение. Стремительная информатизация современного общества, изменение взглядов человечества на организацию экономических, политических и социальных процессов, а также развитие вычислительной техники приводит к значительному увеличение объема информации, которую необходимо обрабатывать и анализировать в реальном масштабе времени. Этот процесс требует от вычислительных средств высокого быстродействия, больших объемов как оперативной, так и дисковой памяти.

В современном мире все большее распространение получают распределенные системы вычисления, облачные технологии, децентрализованное хранение информации. Однако при всех их преимуществах связанных с повышением быстродействия возникают и новые проблемы. В основном они касаются угроз безопасности информации циркулирующей в распределенной сети, их целостности и конфиденциальности. Кроме того, в аспекте обработки данных возникают сложности с процессом масштабирования и реализации алгоритмов обработки повышенной сложности. Технологии распределенных вычислений и децентрализованного хранения информации были представлены еще в 90-х годах. Тем не менее понятие “блокчейн” стали использовать недавно, после того как Сатоши Накамото показал, как эти технологии могут быть использованы для устройства новой финансовой системы [1]. Так, в 2008 году появился биткоин, что положило начало истории развития блокчейна.

В настоящее время под терминами “технология блокчейн” (blockchain) или “технология распределенного реестра” (distributed ledger technology – DLT) понимают технологический протокол, который позволяет осуществлять обмен данными напрямую между различными договаривающимися сторонами внутри сети без необходимости в посредниках [2,3].

Анализ финансовых вложений в сферу информационных технологий за последнее время показал стремительный рост и особенно это касается разра-

боток, направленных на развитие блокчейн технологий. Рынок блокчейн технологий является относительно новым и растущим [4]. Так, согласно [5] за 2017 год, общие расходы разных стран на решения этих вопросов составили 945 млн. долл. США. В 2018 году объем рынка блокчейн увеличился до 1,5 млрд. долл. США. К 2024 году прогнозируется рост объемов рынка до 19 млрд. долл. США [5, 6]

Таким образом, анализ современного состояния развития технологии блокчейна и определения перспективных путей ее развития является актуальной задачей на современном этапе.

Постановка задачи. В настоящее время технология блокчейн развивается как обособленная технология, которая может применяться и за рамками систем криптовалют. Согласно отчету международной исследовательской и консалтинговой компании IDC, на начало 2021 года блокчейн находит широкое применение трансграничных платежах и расчетах (15,9%), отслеживании партий товаров (10,7%), финансировании торговых операций (10%), управлении активами (8,8%), управлении аутентификацией (7,6%) [5,6].

Применение данной технологии в различных областях цифровой экономике и бизнесе за рубежом становится все более перспективным. На развитии этих аспектов обращают пристальное внимание страны Европейского союза. Так Европейский совет подчеркивает, что развитие “цифровой” экономики является стратегическим направлением, определяющим конкурентоспособность стран на мировой арене [7, 8].

В рамках документов [9–11] были определены национальные приоритеты на долгосрочный период, а именно переход к цифровой экономике и внедрение новых форматов государственного управления. В [12] указывается, что своевременное создания условий для внедрения различных цифровых технологий является необходимым залогом дальнейшего развития государства. Это, прежде всего, формирование информационной инфраструктуры, информационной безопасности, нормативно-правовое регулирование, формирование исследовательских компетенций и технологических основ, подготовка кадров, образование.

Для цифровой экономики условно можно выделить следующие области применения блокчейн-технологий [13]:

– в области финансов: транзакции на основе криптовалют (например, внедрение цифровых платежей на основе эфира, биткоин);

– в области экономики, рынков и интернета вещей: смарт-контракты (например, применение технологии работы с акциями, облигациями, закладными, фьючерсами, правовыми титулами, активами и т.д.);

– в области управления: организация государственного управления, науки, образования, здравоохранения и др. (применение технологии вне рамок финансовых транзакций).

О перспективности технологии блокчейна существуют различные противоречивые мнения экспертов [14,15]. Несмотря на некоторые успешные попытки внедрения технологии блокчейна, она пока остается экспериментальной со всеми сопутствующими рисками, проблемами внедрения и эксплуатации [16]. Преимущества и недостатки технологии блокчейна приведены в многочисленных работах ряда авторов [2,4,8,17–20].

Однако, экспертное сообщество обращает внимание на недостаточную изученность таких аспектов применения блокчейн как информационная безопасность, достоверность данных, быстродействие, эффективность протокола взаимодействия узлов (выработка консенсуса) в сети блокчейн [21].

Таким образом, анализ работ в области применения блокчейна выявил необходимость проведения исследований направленных на устранения “белых пятен”, мешающих дальнейшему развитию технологии блокчейна с технической точки зрения.

Цель статьи – определение перспективных направлений развития и усовершенствования блокчейн-технологий путем анализа их технических возможностей по устранению существующих недостатков.

Для достижения цели были поставлены следующие задачи:

1. провести анализ существующих блокчейн-технологий, их преимуществ и недостатков с точки зрения технической реализации;

2. определение перспективных направлений усовершенствования блокчейн-технологий.

Анализ существующих блокчейн-технологий. Будем рассматривать блокчейн, именно как обособленную технологию с технической точки зрения, анализируя ее преимущества и недостатки.

Компанией Deloitte был составлен рейтинг городов по числу проектов, реализуемых на блокчейне [6]. Возглавляет список Сан-Франциско, где разрабатываются различные программные решения для организации работы бирж, интерфейсы для работы блокчейнов, платежные инструменты для криптовалют и др. Лондонские специалисты активно занимаются цифровой идентификацией и смарт-контрактами. Специалисты Нью-Йорка разрабатывают проекты, связанные с решением задач в финансовой сфере (сервисы финансовых услуг). Китайские проекты, которые разрабатываются в Пекине и Шанхае, связаны с криптовалютами и биржами криптовалют. Особый акцент делается на масштабируемость проектов и их производительность [22].

По мнению аналитиков международной консалтинговой компании McKinsey [23], реальный прогресс внедрения блокчейн-технологий в экономику незначителен и не оправдывает огромных вложений денежных средств, что обосновано возникшими техническими трудностями.

На сегодняшний день существует более 10 тыс различных блокчейнов, которые являются либо публичными (открытый код) либо частными. Рассмотрим некоторые характеристики существующих популярных и быстрых блокчейнов (табл.1):

1. Bitcoin. Прошло 12 лет с момента запуска Bitcoin, однако основная проблема быстродействия так и не была решена. Быстродействие данного

блокчейн составляет всего лишь около 7 транзакций в секунду (Transactions-per-second (TPS)), частота обновления блоков составляет 1 раз в 10 минут. Алгоритмом консенсуса, используемого в сети, является алгоритм типа Proof-of-Work (PoW) [19].

2. Ethereum. Платформа блокчейна предназначена для создания децентрализованных онлайн-сервисов, работающих на базе смарт-контрактов. Реализована как единая децентрализованная виртуальная машина. Разработчиком Ethereum Бутериным заявлена скорость – 20 TPS. 15 сентября 2022 года был осуществлен переход с PoW протокола на PoS протокол, что позволило увеличить пропускную способность сети, а также уменьшить затраты на обслуживание. Кроме того, на данный момент осуществляется запуск шардинга в сети, что также позволит увеличить число транзакций [24,25].

3. Minter. Блокчейн представлен, как DeFi-платформа со смарт-контрактами и кросс-чейн ликвидностью с использованием широкого набора SDK и API-инструментов. За разработку данного блокчейна отвечает команда приблизительно из 20 российских специалистов. Используемый протокол консенсуса – Delegated Proof-of-Stake (DPoS), идея которого заключается в выборе валидаторов путем голосования. В будущем запланирована интеграция с TON, что позволит участникам производить обмен токенов этих сетей и использовать смарт-контракты. Архитектура Minter позволяет поддерживать транзакции вне сети. Скорость формирования блока составлят 1 раз в течении 5 секунд [26].

Таблица 1

Характеристики существующих блокчейнов

Название блокчейн технологий	TPS	Децентрализация	Шардинг	Масштабируемость	Смарт-контракт	Частота обновления блоков	Доступность	Поддержка языков программирования	Наличие виртуальной машины	Многоуровневость платформы	Принцип верификации
Bitcoin	7-10	да	нет	да	базовые принципы	1 раз в 7-10 минут	Открытий код	C++, Java, JS, Python	-	-	PoW
Ethereum	15-30	да	нет	да	да	1 раз в 12-15 секунд	Открытий код	Python, Go, Mutan, LLL, JS, Solidity, Ruby, Rust	да	да	PoW/ PoS
Minter	2000	да	да	да	да	1 раз в 5 секунд	Открытий код	Goland	-	да	DPoS
Cardano	5000	да	нет	-	да	1 раз в 9 минут	Открытий код	Haskell, Solidity	-	да	PoS
QTUM	10000	да	нет	да	да	-	Открытий код	C++, Solidity	да	да	MPoS
Solana	50000	да	нет	да	да	1 раз в 400 микросекунд	Открытий код	Rust	-	да	PoH/ PoS
Everscale	68000	да	да	да	да	1 раз в 500 микросекунд	Открытий код	C++, Solidity, FIFT, Rust	да	да	PoS
Near	-	да	да	да	да	1 раз в 2 секунды	Открытий код	C++, JS, Python, Rust	-	да	TPoS
Neo		да	-	да	да	-	Открытий код	C#,F#,Java, Python,	-	-	BFT

4. Cardano. Данный блокчейн имеет много общего с Ethereum, так этот проект был учреждён Ч. Хоскинсоном. Это блокчейн платформа для криптовалюты под названием ADA. Cardano может обрабатывать от 50 до 250 TPS. По его словам, добавление технологии масштабирования блокчейна путем создания параллельной сети с двусторонней привязкой в будущем позволит достичь более 5000 TPS. Система ориентирована на запуск смарт-контрактов, децентрализованных приложений и многопартийных вычислений. Высокая степень отказоустойчивости [27].

5. QTUM. Это децентрализованный блокчейн, которая сочетает в себе возможности смарт-контрактов Ethereum с концепцией Bitcoin. Используется механизм консенсуса Mutualized PoS (MPoS), защищающий сеть от атак мошеннических контрактов. В августе 2020 разработчики QTUM протестировали эффективность своего блокчейна на

виртуальном сервере Amazon EC2 и пришли к выводу, что QTUM способен обрабатывать более 10 000 TPS [28].

6. Solana. Это блокчейн третьего поколения, предназначенный для поддержки масштабируемых децентрализованных приложений (DApps) и смарт-контрактов. Он имеет максимальную пропускную способность более 50 000 TPS и период формирования блока всего 400 мс. Solana использует гибридный алгоритм консенсуса, который сочетает Proof-of-History (PoH) с PoS [29].

7. Everscale. Блокчейн с открытым исходным кодом. Платформа Everscale состоит из подмножества рабочих блокчейнов (воркчейнов), их шардчейнов, и их блоков, что синхронизируются с основным для актуализации распределенного реестра. Существует вертикальное и горизонтальное масштабирование, что позволило достичь скорости 68000 TPS в реальных условиях[30]. В основной сети на данный момент запущен только 1 воркчейн, в связи с отсутствием необходимости содержать большее количество. Блокчейн Everscale использует для организации своей роботы PoS протокол.

8. Near. Это блокчейн первого уровня, использующий уникальную технологию шардинга для достижения масштабируемости. Он запущен был в 2020 году как децентрализованная облачная инфраструктура для размещения децентрализованных приложений (DApps). Существует кроссчейн-взаимодействие для организации многоуровневой платформы. Используемый протокол консенсуса – Thresholded Proof-of-Stake (TPoS), напоминающий аукцион для установления минимального порога для валидаторов. Однако на данный момент найти данные по быстродействию данного блокчейна практически невозможно, но теоретически Near позволит обрабатывать миллионы транзакций в секунду [31].

9. Neo. Блокчейн является азиатским некоммерческим проектом, целью которого является создание “умной экономики” [32]. Используемый протокол консенсуса – Byzantine Fault Tolerance (BFT)

Анализ функционирования вышеперечисленных современных блокчейнов и их характеристик подтвердил, что для повышения скорости обработки и финализации транзакций сетью (масштабируемость) блокчейн должен пожертвовать либо децентрализацией, либо безопасностью (рис. 1).

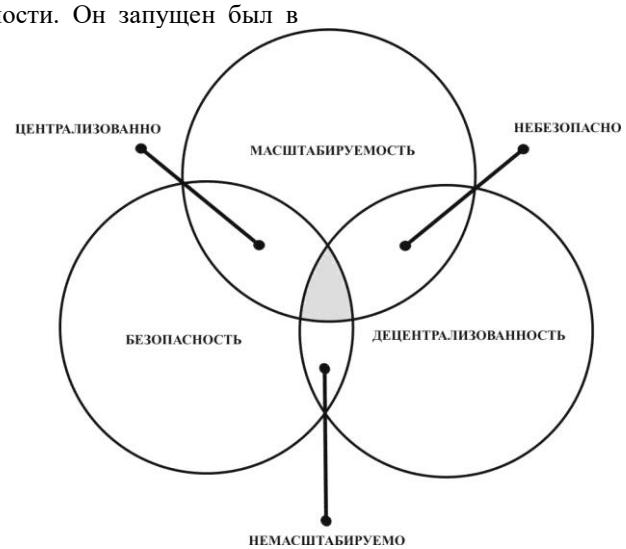

Рисунок 1 – Аспекты трилеммы блокчейна

Таким образом, возникает необходимость решения проблемы достижения оптимизации аспектов трилеммы масштабируемости, предложенной Бутериным [24–26]: децентрализация, безопасность и масштабируемость.

Перспективные пути усовершенствования блокчейн-технологий. Для решения поставленной проблемы необходимо такая организация функционирования блокчейна, которая обеспечит ее безопасное устройство, и нагрузка на узлы системы будет ограничена.

Одним из вариантов решения проблемы масштабирования является использование подходов, основанных на направленных ациклических графах. Направленные ациклические графы представляет собой графическую структуру, не имеющую циклов, при этом все ребра связывают узлы сети (ноды) в одном направлении. Это позволит построить архитектуру сети, используя последовательность вершин в топологическом порядке. Однако данная технология не является блокчейном в чистом виде, так как контроль над передачей информации не требуют доказательства выполнения работы, наличия майнеров и наличия блоков, Направленные ациклические графы представляет собой не “цепь”, а “древо”, где каждая операция подтверждает предыдущие. Технология на сегодняшний день находится на этапе развития и обладает большим потенциалом [16].

Не меньшим потенциалом обладает и использование шардинга, под которым будем понимать горизонтальное разделение данных, метод разделения и хранения одного набора данных в виде множества различных баз данных, возможно находящихся в различных местах. По сути блокчейн – это индивидуальные сервера (ноды), каждая из кото-

рых имеет свою базу данных, которые могут пересекаться между собой, а вместе объединяются в одну большую базу. Для блокчейна шардинг рассматривается как разделение сети на сегменты (шарды). В каждом шарде содержится информация о наборе смарт-контрактов и информации, которые способны~~х~~ функционировать внутри сегмента и между сегментами. В каждо~~й~~м шарде валидируют свои ноды (валидаторы), проверяющие и подтверждающие транзакции и сообщения, когда в обычной схеме каждый валидатор может проверять любую транзакцию и любое сообщение во всей сети.

Такой подход позволяет разделить сеть на несколько более управляемых и не таких больших сегментов, что дает возможность масштабировать сеть и увеличить ее пропускную способность. Классический блокчейн состоит из огромного количества валидаторов и нод, которые исполняются смарт-контракты, а также на которых функционируют децентрализованные приложения, исходя из парадигмы последовательного выполнения каждой транзакции. То есть все валидаторы и ноды обрабатывают каждую транзакцию в сети. Из-за этого прохождение транзакцией всех этапов верификации занимает большое количество времени и чем больше транзакций в сети, тем больше памяти они занимают. Также при появлении узла в сети возникает ситуация, когда новому участнику приходится синхронизировать всю обработанную ранее информацию и не всегда приносит прирост эффективности работы, так как цепочка верификации просто становится длиннее.

Сама идея шардинга заключается в том, чтобы последовательное исполнение транзакций распределить между различными сегментами (шардами) и чтобы каждый шард выступал в роли маленького блокчейна. Валидаторы в них обрабатывали внутренние транзакции и только их. Но при этом сохранить взаимосвязь этих сегментов, для полноценной работы основного целого блокчейна. Как показала практика, данный подход дает возможное решение проблемы масштабирования сети, так как уменьшение нагрузки дает увеличение пропускной способности сети. Однако коммуникация и безопасность являются главными проблемами шардинга. При разделении блокчейна на изолированные сегменты, каждый шард становится отдельной сетью. Пользователи из одного сегмента сети не смогут создавать транзакции с пользователями и приложениями другого сегмента сети, не используя дополнительные методики коммуникации.

В разбитой на сегменты сети потенциально существует опасность мошенничества, так как злоумышленникам проще создать некорректные транзакции в одном шарде, поскольку её будет валидировать меньшее количество нод (стандартная атака “51%”). Таким образом, злоумышленники могут захватить сегмент сети, который будет влиять на работу всего блокчейна. В связи с этим было предложено рандомизировать выбор валидаторов внутрь шарды и внутри всего блокчейна, что снижает вероятность захвата сегмента и использование парадигмы бесконечного шардирования.

На данный момент остаются нерешенными некоторые вопросы безопасности и эффективности шардинга, что оставляет технологию относительно сырой для использования в промышленных масштабах.

Таким образом, основными преимуществами применения технологии шардинга является повышение быстродействия функционирования блокчейна, снижение нагрузки на отдельные ноды сети и снижение технических требований к валидаторам. К недостаткам можно отнести возникновение необходимости в дополнительных методиках коммуникации шардов между собой и повышение опасности мошенничества.

Важным аспектом развития технологии блокчейна является усовершенствование алгоритма консенсуса, который позволит оптимизировать работу и повысить защищенность сети блокчейн особенно с технологией шардинга. Под алгоритмом консенсуса будем понимать метод, с помощью которого распределенные узлы в сети достигают согласия относительно элемента данных [26]. Блокчейн-системы не в состоянии функционировать без выполнения формализованных правил поведения, которым следует все участники сети. Одни алгоритмы позволяют строить надежные децентрализованные системы, другие – блокчейны с большой пропускной способностью и масштабируемостью.

Первым алгоритмом консенсуса, использующимся в блокчейн-системах, и самым распространенным на данный момент является Proof-of-Work (PoW). В основе алгоритма PoW лежит функция, для вычисления которой необходимо затратить много машинного времени и ресурсов, а вот результат вычислений просто проверить. Это могут быть такие функции как хеширование частичной инверсии, функции, базирующие на деревьях Меркла, функции Диффи-Хеллмана, SHA-256 и другие методы.

Альтернативными алгоритмами консенсуса могут быть следующие:

– Proof-of-Stake (PoS). Вклад валидатора определяется долей внесенных денежных единиц криптовалюты от общего количества. Валидаторы подкрепляют добросовестность не затратами на вычисление, а активами внутри сети. Однако при использовании этого алгоритма возникает актуальная проблема отсутствия внесения активов (Nothing of Stake), т.е. валидаторами могут выступать участники без дополнительных затрат. Для ликвидации данной проблемы появились разновидности PoS, использующие принципы представительной демократии. Например, Delegated Proof-of-Stake (DPoS), Mutualized Proof-of-Stake (MPoS), Thresholded Proof-of-Stake (TPoS);

– Proof-of-Capacity, Proof-of-Weigth, Proof-of-Spacetime. Данные алгоритмы консенсуса основаны на доказательстве выделения узлами нодов ресурсов для хранения цифровой информации;

– Proof-of-Authority (PoA). Основная идея заключается в предоставлении повышенных полномочий некоторым валидаторам. Используются в

управляемых и частично централизованных блокчейнах;

– Proof-of-History (PoH). В основу алгоритма положен процесс синхронизации работы всех узлов блокчейна и установления одинакового времени. Создается историческая запись, которая доказывает факт создания в определенный момент времени;

– Byzantine Fault Tolerance (BFT). Семейство алгоритмов консенсуса, направленное на защиту от сбоев сети блокчейна с помощью коллективного принятия решения и уменьшения влияния неисправных узлов.

Сравнение основных алгоритмов консенсуса приведена в табл.2.

В последнее время расширение применения блокчейна в практической жизни приводит тому, что все больше проектов отходят от PoW и перехода к различным альтернативным алгоритмам консенсуса. Модификация алгоритмов идет по пути увеличения безопасности информационных данных, как например в PoS (доказательство доли владения). Для PoS характерно то, что вероятность генерации блока прямо пропорциональна балансу вложений валидатора. Для злоумышленника вкладывать средства для приобретения контроля будет невыгодно, так как курс возрастает прямо пропорционально спросу. Но если всё-таки ему это удается, то атака становится нецелесообразной, так как он подвергает риску и свои вложения [16].

Таблица 2

Характеристики основных алгоритмов консенсуса

Алгоритмы консенсуса	**Примеры проектов**	**Энергозатраты, кВт*ч в день**	**Количество полных узлов**	**Управление**	**Приоритетные характеристики**
PoW	Bitcoin/ Ethereum (до 15.09.2022)	69974983/ 51765837	10102/ 12754	неформальное оффчейн-управление	децентрализованность, безопасность
PoS	Cardano	18630	12	ончейн-управление	масштабируемость
DPoS	Minter	30-45	16-256	ончейн-голосование	масштабируемость, низкое энергопотребление
BFT	Neo	51	7	ончейн-голосование +элементы оффчейн управления	масштабируемость, низкое энергопотребление
TPoS	Near	-	-	ончейн-голосование	масштабируемость

Примечание. Управление блокчейном обычно делится на 2 категории:

1. Ончейн управление – процессы принятия решений проходят через стейкинг и транзакции на блокчейне.

2. Оффчейн управление – процессы принятия решений проходят через неформальные процессы обсуждения и предложения вне блокчейна.

Кроме того, для масштабного внедрения блокчейна в цифровую экономику необходимо развитие не только рассмотренных технических аспектов, но и совершенствование нормативно-правовой базы, описывающей правила эксплуатации технологии и регулирующей отношения, возникающие при её использовании. А также немаловажной является и подготовка специалистов, разбирающихся в этих технологиях.

Заключение. Таким образом, как показано в статье технология блокчейн развивается как обособленная технология, которая применяться далеко за рамками систем криптовалют. Применение данной технологии в различных областях цифровой экономике и бизнесе за рубежом становится все более перспективным. Однако, экспертное сообщество обращает внимание на недостаточную изученность таких аспектов применения блокчейн как информационная безопасность, достоверность данных, быстродействие, эффективность протокола взаимодействия узлов.

1. Проведенный анализ наиболее популярных и производительных блокчейн-технологий позволил выявить и обобщить их преимущества и недостатки с точки зрения технической реализации. Рассмотрены такие блокчейн-системи, как Bitcoin, Ethereum, Minter, Cardano, QTUM, Solana и другие.

Анализ функционирования вышеперечисленных блокчейнов и их характеристик подтвердил, что для повышения скорости обработки и финализации транзакций сетью блокчейн должен пожертвовать либо децентрализацией, либо безопасностью. Таким образом, необходимо найти рациональное сочетание таких свойств технологии как децентрализация, безопасность и масштабируемость.

2. Для решения поставленной проблемы определены перспективные направления усовершенствования блокчейн-технологий, которые позволят обеспечить ее безопасное функционирование и снизить нагрузку на узлы системы. Одним из вариантов решения проблемы масштабирования является использование подходов, основанных на направленных ациклических графах.

Не меньшим потенциалом обладает и использование технологии шардинга, под которым будем

понимать горизонтальное разделение данных. Технология шардинга – перспективная и эффективная технология, позволяющая снизить сетевую нагрузку и нагрузку на процессоры нод блокчейна. На данный момент остаются нерешенными некоторые вопросы безопасности и эффективности шардинга, что не позволяет использовать данную технологию в промышленных масштабах. Но само направление развитие блокчейна является актуальным и перспективным на данный момент.

Важным аспектом развития технологии блокчейна является усовершенствование алгоритма консенсуса, который позволит оптимизировать работу и повысить защищенность сети блокчейн особенно с технологией шардинга. Показано, что одни алгоритмы позволяют строить надежные децентрализованные системы (Proof-of-Work), другие – блокчейны с большой пропускной способностью и масштабируемостью (модификации Proof-of-Stake). В статье проанализированы некоторые алгоритмы консенсуса и определены направления развития.

В дальнейших научных исследованиях за данной тематикой планируется построение модели осуществления консенсуса узлов с учетом шардинга, а также разработка оптимизированного алгоритма консенсуса, учитывающего аспекты безопасности, сетевой нагрузки и времени договоренности между узлами сети.

Список литературы:

1 Nakamoto S. A Peer-to-Peer Electronic Cash System // Bitcoin. https://bitcoin.org/bitcoin.pdf (дата обращения 22.04.2024)

2 Цветкова Л.А. (2017) Перспективы развития технологии блокчейн в России: конкурентные преимущества и барьеры // Экономика науки. Т. 3. № 4. С. 275–296.

3 Deep Shift – Technology Tipping Points and Societal Impact (2015) / World Economic Forum Survey Report. http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24.

4 Хачатурова Э.А., Макаревич М.Л. Блокчейн-технологии: перспективы развития и проблемы правового регулирования // Инновационная экономика: перспективы развития и совершенствования. 2018. №2 (28). С. 105–114.

5 Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024, According to New IDC Spending Guide // URL: https://www.idc.com/getdoc.jsp?containerId=prUS47617821 (дата обращения 22.04.2024)

6 Evolution of blockchain technology / Deloitte / URL: https://www.deloitte.com/insights/us/en/industry/financial-services/ evolution-of-blockchain-github-platform.html (дата обращения 10.08.2022).

7 Сидоров Д.П., Камаева А.А. Технология блокчейн и возможности ее применения в учебном процессе // Образовательные технологии и общество. 2019. Том 22, № 3. С. 94–101.

8 Пряников М.М., Чугунов А.В. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // Internetional Journal of Open Information Technologies. 2017. Том 5. № 6. С.49–55.

9 О стратегия развития информационного общества в Российской Федерации на 2017-2030 годы / Указ Президента Российской Федерации от 09.05.2017 № 203.

10 Декларация принципов “Построение информационного общества – глобальная задача в новом тысячелетии” URL: http://www.gov.karelia.ru/Leader/Inform /Egov/tunis.html (дата обращения 22.04.2024).

11 О стратеги экономической безопасности Российской Федерации на период до 2030 года. / Указ Президента Российской Федерации от 13.05.2017 № 208.

12 Распоряжение Правительства РФ от 28 июля 2017 г. N 1632-р Об утверждении программы “Цифровая экономика Российской Федерации”. Программа “Цифровая экономика Российской Федерации”. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 22.04.2024)

13 Свон М. Блокчейн: Схема новой экономики / М. Свон. – М.: Олимп-бизнес, 2017. – 240 с.

14 Утавкаева И. Х. Теоретические аспекты применения технологии блокчейн // Вестник алтайской академии экономики и права. 2019. №5. С. 143–147.

15 Радюкова Я.Ю., Колесниченко Е.А., Епифанова С.О. Блокчейн: перспективы развития и проблемы внедрения // Известия Юго-Западного государственного университета. 2018. Т. 22, № 3(78) с. 120–127.

16 Утавкаева И. Х., Никитенко В. О., Тутаев И. А. Особенности внедрения технологии блокчейн в цифровую экономику // Вестник алтайской академии экономики и права. 2019. №7. С. 91–95.

17 Сергеева Т.А., Мочалова Я.В. Блокчейн как инструмент повышения экономической безопасности. https://core.ac.uk/download/pdf/322817981.pdf.

18 Лелу Л. Блокчейн от А до Я. Все о технологии десятилетия. – М.: Эксмо, 2018. – 256 с.

19 Антонопулос А. Осваиваем биткойн. Программирование блокчейна. – М.: ДМК Пресс, 2018. – 428 с.

20 Равал С. Децентрализованные приложения. Технология Blockchain в действии. – СПб.: Питер, 2017. – 240 с.

21 Prospects for using of Blockchain technology were discussed at a joint meeting of the Interdepartmental Commission of the Security Council of the Russian Federation on Security in the Economic and Social Sphere, as well as on information security with the participation of experts from the Scientific Council under the Russian Security Council (2017) / Russian Security Council, 29.06.2017. http://www.scrf.gov.ru/news/allnews/2244. (дата обращения 22.04.2024)

22 Эволюция технологии блокчейна / BitNovosti/ URL: https://bitnovosti.com/2017/12/16/evolyutsiya-tehnologii-blockchain/ (дата обращения 3.05.2024).

23 McKinsey Technology Trends OutLook 2022. URL: https:/mckinsey.com (дата обращения 3.08.2022).

24 Santiago Palladino. Ethereum for Web Developers: Learn to Build Web Applications on top of the Ethereum Blockchain. – Apress, 2019. – 349 с.

25 Chris Dannen. Introduction Ethereum and Solidity: Foundations of Criptocurrency and Blockchain Programming for Beginners. – 2017. – 256 с.

26 Delegated Proof-of-Stake как альтернатива PoW и PoS: сравнение и перспективы / forklog.com / URL: https://forklog.com/sp/DPos/ (дата обращения 22.04.2024)

27 Блокчейн Cardano / Bitcointalk.org/ URL: https://bitcointalk.org/index.php? Topic=2238700.0 (дата обращения 22.04.2024)

28 Что такое Qtum (QTUM) / academy.binance.com/ URL: https://academy.binance.com/ru/articles/what-is-qtum-qtum (дата обращения 22.04.2024)

29 Глубокое погружение в Solana / coinmarketcap.com / URL: https://coinmarketcap.com/alexandria/ru/article/solana (дата обращения 22.04.2024)

30 Блокчейн-платформа, управляемая сообществом – Free TON / freeton.com / URL: https://freeton.com/ru/ (дата обращения 22.04.2024)

31 Что такое NEAR Protocol / academy.binance.com/ URL: https://academy.binance.com/ru/articles/what-is-near-protocol-near (дата обращения 22.04.2024).

32 What is NEO? / kraken.com / URL: https://kraken.com/en-gb/learn/what-is-neo (дата обращения 22.04.2024).