DOI: 10.14451/1.215.92

ВЫБОР БЛОКЧЕЙН-ПЛАТФОРМЫ И АЛГОРИТМА КОНСЕНСУСА ДЛЯ ПОСТРОЕНИЯ БИЗНЕС-ПРИЛОЖЕНИЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ*

© 2022 **Бурков Алексей Владимирович**
доктор экономических наук, профессор кафедры прикладной статистики и информатики
Марийский государственный университет, Россия, Йошкар-Ола
E-mail: alexey.burkov@gmail.com

© 2022 **Вершинин Никита Андреевич**
инженер-программист
ООО «Студия цифровых решений»
E-mail: nvershinin1@gmail.com

В статье проводится анализ популярных блокчейн-платформ, которые могут быть использованы для построения бизнес-приложений кредитных организаций. Раскрыты ключевые преимущества использования технологии блокчейн в финансовом секторе. Также описан принцип работы протоколов и алгоритмов консенсуса. Особое внимание уделено сравнению эффективности алгоритмов и их целесообразности применения в коммерческих решениях.

Ключевые слова: *технология блокчейн, блокчейн-платформы, алгоритм консенсуса, протокол консенсуса, кредитная организация, бизнес-приложение, защита данных.*

В последнее время наблюдается всплеск популярности технологии блокчейн. Компании стремятся использовать данную технологию в своих сервисах и приложениях. Одним из наиболее перспективных направлений применения технологии блокчейн является финансовый сектор. Неслучайно блокчейн обрел свою популярность именно в финансовом секторе. Появление первой в мире криптовалюты под названием Биткоин в 2008 году навсегда изменило наше представление о цифровых валютах. Создание блокчейн-сети позволило нам по-новому взглянуть на устаревшую финансовую инфраструктуру, найти различные уязвимости и способы их решения [2].

Сегодня кредитные организации являются одними из наиболее уязвимых объектов финансовой инфраструктуры. Поэтому, при проектировании бизнес-приложений, разработчики прежде всего обращают внимание на способы защиты данных [6]. В этом плане, технологии блокчейн равных нет.

Блокчейн представляет собой сочетание двух логических механизмов: механизма хеширования и механизма достижения консенсуса. С помощью хэш-функций происходит связывание блоков цепи воедино, в то время как алгоритм консенсуса обеспечивает целостность сети в целом [1].

Протокол консенсуса — это набор правил, используемых для управления блокчейн-сетью. Эти правила определяют устройство всей сети: способ взаимодействия между компьютерами, вид поощрений за создание новых блоков, тип данных [3]. Основная функция протоколов консенсуса заключается в проверке и обработке транзакций в распределенной сети с помощью криптографических механизмов. Протоколы используются для решения следующих задач:

- Обеспечение безопасности: протоколы призваны поддерживать защищенность всей сети.
- Поддержание согласованности: при проведении каждой транзакции протоколы обновляют всю базу данных сразу. Любой пользователь блокчейн-сети всегда взаимодействует с актуальным состоянием сети.
- Организация децентрализации: протоколы подтверждают работу всех распределенных узлов в сети.
- Обеспечение масштабируемости: протоколы позволяют масштабировать сеть, а именно увеличивать количество транзакций. Изначально масштабируемость была одной из проблем блокчейнов. Большинство протоколов на сегодняшний день справляются с проблемой увеличения количества транзакций и узлов сети.

В качестве примера функционирования протокола консенсуса рассмотрим вариант проведения транзакции:

- Пользователь создает запрос на проведение

*Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 20-010-00472 А

транзакции. Далее создается новый блок, который в дальнейшем уже не может быть изменен. Свойство неизменности обеспечивается именно протоколом.
– Новый блок отправляется каждому пользователю сети. Распространение блоков по всей сети также выполняется протоколом.
– Узлы сети подтверждают транзакцию.
– За подтверждение транзакции узлам сети отправляется вознаграждение. Отправка вознаграждений все также управляется протоколом.

После выполнения вышеперечисленных шагов транзакция считается исполненной. Таким образом, протоколы задействованы на каждом этапе проведения транзакции, что обеспечивает защищенность, масштабируемость и согласованность.

Алгоритм консенсуса — это механизм проверки выполнения протоколов. Алгоритмы консенсуса позволяют обеспечить достижение согласия между всеми участниками сети о текущем состоянии данных [2].

Согласно исследованию А. Кумари и Н. Деви [5] «Proof-of-Work», «Proof-of-Stake», «Proof of Authority» являются наиболее популярными алгоритмами консенсуса, которые используются в блокчейн-сетях бизнес-приложений финансовых организаций.

«Proof-of-Work» (PoW) — это исторически первый алгоритм консенсуса, который лежит в основе криптовалюты Биткоин. Суть данного алгоритма заключается в создании нового блока путем решения сложной математической задачи. Для решения задачи требуется вычислительная мощность. Этот алгоритм хорошо зарекомендовал себя в блокчейн-сетях, где требуется быстрая масштабируемость и отсутствие любой регуляции. Однако у него есть несколько существенных недостатков. К этим недостаткам относят: затраты на высокопроизводительное оборудование для майнинга новых блоков, низкую скорость транзакций, уязвимость к атакам в небольших сетях [4]. Эти недостатки будут особо критичными в корпоративной среде, по нашему мнению, использование протокола PoW для построения бизнес-приложений не рекомендуется и является экономически неэффективным.

Механизм консенсуса «Proof-of-Stake» (PoS) основывается на доказательстве права собственности. При этом данный механизм не требует сложных вычислений, что позволяет сэкономить средства на приобретение дорогостоящего оборудования. С помощью данного консенсуса владельцы криптовалюты подтверждают транзакции блока на основе количества поставленных на кон монет. Также этот протокол считается менее рискованным с точки зрения возможной атаки на сеть, поскольку он структурирует вознаграждение таким образом, что атака становится менее выгодной.

Разновидностью PoS является алгоритм под названием «Delegated Proof of Stake» (DPoS). В сетях, использующий данный механизм пользователи могут голосовать за так называемых представителей, которые получают право на создание новых блоков в цепи. Эти представители получают определенное вознаграждение за свою работу. Если же выбранный представитель не может создать новый блок, то он не будет допущен к дальнейшему процессу голосования. Все эти процессы происходят автоматически и регулируются алгоритмом консенсуса.

«Proof of Authority» (PoA) — это алгоритм консенсуса, который полагается на авторитетные валидаторы для создания новых блоков. PoA спроектирован с учетом потребностей организаций, которые хотят создать свою собственную блокчейн сеть. Этот алгоритм не является ресурсозатратным, однако требует от валидаторов сохранение целостности своих узлов. «Proof of Authority» также можно описать как механизм, который стимулирует действовать честно, в соответствии правилами сети, поскольку на чашу весов поставлена личность и репутация пользователя [4].

Исходя из проведенного анализа для построения блокчейн-сети кредитной организации рекомендуется использовать алгоритмы «Proof of Authority» или «Proof-of-Stake». Они наиболее подходят для использования в корпоративных сетях, поскольку сочетают в себе высокую защищенность и низкие требования к аппаратным ресурсам.

Успех построения бизнес-приложения с блокчейном также во многом зависит от выбора программной платформы (фреймворка) для разработки. В настоящее время существует ряд коммерческих и открытых платформ для разработки блокчейн-сетей.

Рассмотрим наиболее популярные проекты:

1. **Hyperledger**. Проект с открытым исходным кодом, который разрабатывается фондом Linux. Данный проект предоставляет предприятиям решения для создания защищенных блокчейн-сетей. Hyperledger существует с 2015 года и уже успел себя зарекомендовать при создании различных бизнес-приложений [4]. Данный фреймворк позволяет создавать распределенные сообщения независимо от выбранной криптовалюты. Основной целью проекта Hyperledger является разработка технологической основы с открытым исходным кодом для создания блокчейн-приложений.

Преимущества Hyperledger:

– возможность расширения инструментария разработки, благодаря наличию большой коллекции библиотек;
– открытый исходный код;
– поддержка проекта различными сообществами и компаниями;
– возможность проведения международных транзакций;
– поддержка протоколов PoA и PoS;

Недостатки Hyperledger:
– блокчейн-сеть не является отказоустойчивой;
– дефицит в квалифицированных специалистах по работе с данной сетью.

2. **Quorum** — это еще один корпоративный блокчейн-проект с отрытым исходным кодом, направленный прежде всего на решение проблем в финансовом секторе. Quorum основан на платформе Ethereum. Quorum был разработан при поддержке финансового конгломерата J. P. Morgan [4].

Преимущества Quorum:
– ориентация на финансовый сектор;
– основан на кодовой базе Ethereum, что позволяет использовать смарт-контракты на языке Solidity;
– открытый исходный код;
– высокая производительность.

Недостатки Quorum:
– отсутствие широкой масштабируемости;
– недостаточная конфиденциальность.

3. **Corda** представляет собой корпоративный блокчейн для бизнеса разработкой которого занимается банковский консорциум R3. Этот протокол особенно популярен среди финансовых организаций. В нем используются алгоритмы консенсуса для поддержания прозрачности и безопасности. Проект имеет открытый исходным кодом. На основе Corda можно создавать взаимодействующие сети блокчейн со строгой политикой конфиденциальности.

Преимущества Corda:
– обеспечение повышенной безопасности;
– поддержка JVM-языков;
– стабильность и масштабируемость.

Недостатки Corda:
– ограниченный выбор в консенсусах;
– узкая специализация;
– платная корпоративна версия.

4. **Multichain** — это платформа для разработки и внедрения частных блокчейн-приложений. Платформа помогает разрабатывать и внедрять приложения для организаций финансового сектора. Поскольку на основе данной платформы создаются только частные сети, разрешения для пользователей выдаются на глобальном уровне. Multichain предоставляет только свой API, поэтому взаимодействие может происходить только через интерфейс командной строки на любой платформе: Windows, Linux, MacOS. Также в Multichain есть возможность обмениваться токенами между различными блокчейнами.

Преимущества Multichain:
– простота создания частных блокчейн-сетей;
– тонкая настройка прав доступа;
– возможность обмена токенами между разными сетями;
– расширенный контроль за транзакциями.

Недостатки Multichain:
– закрытый исходный код;
– зависимость от поставщика API.

Таким образом, по нашему мнению, для построения бизнес-приложений кредитной организации наиболее подходящими являются Quorum и Hyperledger. Недостатки, которые присутствуют у этих платформ, не являются критическими и могут быть исправлены при помощи дополнительной разработки. Сочетание открытого исходного кода этих платформ и поддержки лидирующих компаний позволят легче приступить к разработке прикладных решений. Hyperledger Fabric поддерживает различные протоколы консенсуса включая «Proof of Authority» и «Proof-of-Stake». Ключевой особенностью Quorum является поддержка Ethereum, что позволяет использовать широкую существующую базу смарт-контрактов. Перспективу дальнейшего исследования мы видим в тестировании обозначенных блокчейн-платформ и алгоритмов консенсуса для построения бизнес-приложений кредитной организации.

Библиографический список

1. *Липницкий Д. В.* Блокчейн в финансах и банковском секторе: проблемы становления и перспективы // Экономика промышленности. — 2019. — 3 (87). — С. 59—75. — ISSN 2072-1633.
2. *Липницкий Д. В.* Возможности и вызовы для блокчейн в новой индустриализации // Экономика промышленности. — 2019. — 1 (85). — С. 82—100. — ISSN 2072-1633.

3. A Research Survey on Applications of Consensus Protocols in Blockchain / S. Kaur [et al.] // Security and Communication Networks / ed. by D. He. — 2021. — Jan. — Vol. 2021. — P. 1–22. — DOI: 10.1155/2021/6693731. — URL: https://doi.org/10.1155/2021/6693731.
4. A Survey on Blockchain Technology: Evolution, Architecture and Security / M. N. M. Bhutta [et al.] // IEEE Access. — 2021. — Vol. 9. — P. 61048–61073. — DOI: 10.1109/ACCESS.2021.3072849.
5. *Kumari A.*, *Devi N. C.* The Impact of FinTech and Blockchain Technologies on Banking and Financial Services // Technology Innovation Management Review. — Ottawa, 2022. — May. — Vol. 12. — P. 22010204. — ISSN 1927-0321. — DOI: http://doi.org/10.22215/timreview/1481.
6. *Yukhno A. S.* Perspective of blockchain technology application in corporate governance: Recent trands // Management Science. — 2021. — May. — Vol. 11, no. 2. — P. 57–72. — DOI: 10.26794/2404-022x-2021-11-2-57-72.