|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Раздел 1. Аналитический** | | | | | | | | | |
|  |  |  |  |  |  | *ННГАСУ-09.03.02 – 2024* | | | |
|  |  |  |  |  |  |
| *Изм.* | *Кол.уч* | *Лист* | *№ док.* | *Подпись* | *Дат* |
| *Зав. Каф.* | | *Кислицын Д.И.* | |  |  | *Раздел 1* ***Аналитический*** | *Стадия* | *Лист* | *Листов* |
| *Руковод.* | | *Кислицын Д.И.* | |  |  | *ВКР* | *9* | *33* |
| *Разраб.* | | *Самедов Н.Ю.* | |  |  | *Каф. ИСТ гр. ИС-29* | | |
| *Консульт.* | | *Кислицын Д.И.* | |  |  |
| *Н. Контр.* | | *Суханова Н.Т.* | |  |  |

# **Глава 1. Анализ предметной области**

## **Блокчейн и его версии.**

Блокчейн — это распределенный цифровой реестр, который записывает транзакции в цепочке блоков. Каждая транзакция проверяется участниками сети и добавляется в блок, который затем связывается с предыдущими блоками, создавая непрерывную и неизменную цепочку данных. Этот процесс обеспечивает высокую степень безопасности, прозрачности и неизменности записей.

Основные характеристики блокчейна:

- Децентрализация: Управление и валидация транзакций осуществляется множеством участников сети, что исключает необходимость центрального органа.

- Безопасность: Использование криптографических методов для защиты данных и предотвращения их изменения.

- Прозрачность: Все участники сети имеют доступ к полной истории транзакций, что обеспечивает высокий уровень прозрачности.

- Неизменность: после добавления в блок данные становятся неизменяемыми, что предотвращает их фальсификацию.

Поколения блокчейнов:

1. Первое поколение (Blockchain 1.0)

Первые блокчейны, разработанные для криптовалют, таких как Bitcoin.

Основное внимание уделяется децентрализованной передаче цифровых активов и обеспечению безопасности транзакций. Это поколение решает проблему двойного расходования и обеспечивает надежную передачу ценности.

2. Второе поколение (Blockchain 2.0)

Введение смарт-контрактов, что расширяет функциональность блокчейнов. (Ethereum)

Смарт-контракты позволяют автоматизировать выполнение договорных условий и расширяют возможности использования блокчейнов за пределами простых финансовых транзакций, включая децентрализованные приложения (dApps) [26].

3. Третье поколение (Blockchain 3.0)

Решение проблем масштабируемости, интероперабельности и улучшение производительности. (Cardano, Polkadot)

Это поколение направлено на улучшение скорости транзакций и пропускной способности сети, а также на обеспечение взаимодействия между различными блокчейн-сетями.

4. Четвертое поколение (Blockchain 4.0)

Интеграция блокчейна в промышленность и корпоративные приложения, с акцентом на безопасность, масштабируемость и эффективность. (VeChain, Hyperledger)

Платформы этого поколения предназначены для промышленного применения, предлагая высокую производительность, надежность и адаптацию под бизнес-потребности. Они способствуют цифровизации различных отраслей и улучшению бизнес-процессов [4].

Моё блокчейн-решение относится к четвертому поколению (Blockchain 4.0) и обладает следующими ключевыми характеристиками:

Технологическая основа и алгоритм PoA. Решение основано на алгоритме консенсуса Proof of Authority (PoA), который обеспечивает высокую скорость и производительность благодаря использованию авторизованных валидаторов. Это позволяет достичь высокой пропускной способности и низких задержек при обработке транзакций.

Децентрализация и безопасность. Несмотря на использование авторизованных валидаторов, решение сохраняет элементы децентрализации, что снижает зависимость от одного центра управления и повышает устойчивость к атакам. Строгий отбор валидаторов и улучшенные механизмы защиты данных обеспечивают высокий уровень безопасности и надежности системы.

Гибкость и интеграция. Блокчейн-решение предназначено для интеграции в корпоративные и промышленные системы, предлагая гибкость и адаптацию под специфические бизнес-потребности. Оно поддерживает быстрое масштабирование и интеграцию с различными цифровыми сервисами и инновационными бизнес-моделями.

Экономическая эффективность. Разработанный блокчейн снижает операционные издержки и делает транзакции более экономичными благодаря низким затратам на поддержку инфраструктуры и отсутствие необходимости выполнения сложных вычислений, как в системах на основе Proof of Work (PoW).

Масштабируемость и инновации. Созданная система решает проблемы масштабируемости, предлагая надежные и эффективные решения для бизнеса и международных транзакций. Это способствует поддержке и развитию блокчейн-экосистемы, а также открывает возможности для создания новых бизнес-моделей и услуг.

## **Изучение существующих аналогов блокчейнов**

При анализе текущих блокчейн-систем и их механизмов консенсуса можно выявить ряд важных аспектов. Давайте рассмотрим ключевые характеристики некоторых из них:

Bitcoin (Proof of Work):

- Механизм консенсуса: Proof of Work (PoW) требует от майнеров решения вычислительно сложных задач для генерации новых блоков и подтверждения транзакций.

- Недостатки: Высокое энергопотребление, замедление скорости подтверждения транзакций, потенциальная централизация майнинга крупными игроками [1].

Ethereum (Proof of Stake):

- Механизм консенсуса: Ethereum в 2022 году успешно перешел с PoW на Proof of Stake (PoS), где верификация транзакций осуществляется участниками, пропорционально их доле валюты в сети.

- Недостатки: В текущем состоянии Ethereum сталкивается с теми же проблемами, что и Bitcoin [8]. В перспективе PoS может привести к концентрации криптовалюты в руках небольшой группы участников.

Ripple (Протокол консенсуса):

- Механизм консенсуса: Ripple использует уникальный протокол консенсуса, который позволяет достигать согласия по транзакциям без необходимости в вычислительных задачах.

- Недостатки: Система зависит от доверия к центральной организации, управляющей списком узлов, участвующих в процессе консенсуса.

Cardano (Ouroboros Proof of Stake):

Преимущества: Энергоэффективный протокол PoS, строгий академический подход к разработке и высокий уровень безопасности.

Недостатки: относительно новая платформа, которая еще не достигла уровня распространения Ethereum или Bitcoin.

Hyperledger Fabric (Permissioned Blockchain):

Преимущества: Высокий уровень контроля и безопасности, способность к эффективной масштабируемости в корпоративных приложениях.

Недостатки: Отсутствие децентрализации, что может не соответствовать требованиям проектов, предполагающих широкое участие неконтролируемого числа узлов.

Tezos (On-chain Governance):

Преимущества: Механизмы управления, позволяющие автоматически обновлять протокол без хард-форков.

Недостатки: Сложности, связанные с принятием изменений всеми участниками сети, могут замедлить процесс развития платформы.

Теперь рассмотрим, почему механизм консенсуса Proof of Authority (PoA) является предпочтительным для трансграничных финансовых операций:

- Эффективность и скорость: PoA обеспечивает быструю верификацию транзакций за счет использования доверенных узлов, что критически важно для операций в реальном времени.

- Низкая стоимость транзакций: PoA исключает необходимость в значительных вычислительных ресурсах, снижая стоимость транзакций по сравнению с PoW и PoS.

- Высокий уровень безопасности: при адекватной настройке и управлении списком доверенных узлов, PoA может обеспечить высокую защиту от атак.

- Гибкость и управляемость: PoA позволяет гибко управлять списком узлов, адаптируя сеть под специфические требования трансграничных операций [3].

Nonce в блокчейне — это уникальное число, используемое в процессе майнинга для нахождения хеша, соответствующего заданным условиям. В блокчейнах на основе Proof of Work (PoW), майнеры изменяют nonce и пересчитывают хеш до тех пор, пока не найдут подходящее значение, что позволяет добавить новый блок в цепочку. Nonce обеспечивает уникальность и безопасность транзакций [6].

Хеш - результат применения хэш-функции к набору данных, который преобразует входные данные произвольной длины в строку фиксированной длины. Этот хеш является уникальным и практически невозможно восстановить оригинальные данные из него. Хеши используются в криптовалюте для различных целей, таких как создание уникальных идентификаторов для блоков и транзакций, проверка целостности данных, а также обеспечение безопасности и подтверждение подлинности информации.

Блокчейн на базе PoA не требует использования nonce, что необходимо в PoW для генерации блоков. Это исключает ненужные вычисления, позволяя снизить энергопотребление и повысить общую производительность системы. Важно отметить, что PoW подвержен риску 51% атаки, в то время как PoA, благодаря своей структуре и механизмам защиты, значительно менее уязвим к внешним угрозам. В случае попытки взлома одной из узлов, происходит форк сети, и узлы автоматически рассинхронизируются, что предотвращает возможные внешние взломы.

Таким образом, Proof of Authority представляет собой оптимальное решение для системы трансграничных транзакций, обеспечивая высокую скорость обработки, низкую стоимость, повышенную безопасность и удобство управления.

Консенсус-алгоритмы играют ключевую роль в обеспечении безопасности и целостности блокчейна, определяя, каким образом новые блоки добавляются в цепочку и какие правила следует соблюдать для подтверждения транзакций.

В данной главе мы рассмотрим несколько основных консенсус-алгоритмов, а именно Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) и Practical Byzantine Fault Tolerance (PBFT). Каждый из этих алгоритмов имеет свои особенности, преимущества и недостатки, которые необходимо учитывать при выборе подходящего для конкретного блокчейн-проекта.

Цель данной главы - провести сравнительный анализ этих консенсус-алгоритмов, выявить их основные характеристики, преимущества и недостатки, а также оценить их применимость в различных сценариях использования. Этот анализ поможет разработчикам и исследователям принять обоснованное решение при выборе консенсус-алгоритма для своего блокчейн-проекта, учитывая специфику задачи, требования к производительности, масштабируемости и безопасности.

### **1.3. Описание консенсус механизма Proof Of Work (PoW)**

Proof of Work (PoW) — это один из наиболее известных и широко применяемых консенсус-механизмов в блокчейне, который был впервые предложен в биткойн-протоколе. Этот механизм был разработан для обеспечения безопасности и надежности сети путем подтверждения транзакций и создания новых блоков [2].

Принцип работы PoW основан на концепции "трудозатратности", где участники сети должны продемонстрировать выполнение определенной вычислительной работы, чтобы добавить новый блок в цепочку. Этот процесс требует значительных вычислительных ресурсов и времени, что делает его затратным с точки зрения энергии и вычислительной мощности.

Ключевые особенности PoW:

1. Майнеры: Участники сети, называемые майнерами, конкурируют между собой за право создания нового блока. Майнеры решают криптографическую задачу, известную как "хеш-паззл", которая требует значительных вычислительных ресурсов для его решения.

2. Доказательство выполненной работы: после того как майнер найдет корректное решение криптографической задачи, он отправляет его на сеть. Другие участники могут легко проверить, что майнер действительно выполнил работу, проверив результат через простой алгоритм.

3. Сложность задачи: Сложность криптографической задачи (также известной как "сложность хеша" или "цель хеша") регулируется сетью с целью поддержания постоянной скорости создания блоков. Чем выше сложность задачи, тем больше вычислительных ресурсов необходимо для ее решения.

4. Скорость блокогенерации: Протокол PoW регулирует скорость создания новых блоков путем изменения сложности задачи. В среднем, блоки генерируются примерно раз в 10 минут в биткойн-сети.

Преимущества PoW:

- Децентрализация: PoW обеспечивает высокую степень децентрализации, поскольку любой участник сети может стать майнером, внося свой вклад в поддержание безопасности сети.

- Надежность: благодаря высоким затратам на вычислительные ресурсы для атаки сети, PoW считается одним из наиболее надежных консенсус-механизмов.

Недостатки PoW:

- Высокое энергопотребление: Процесс майнинга требует больших объемов энергии, что может привести к негативным экологическим последствиям.

- Склонность к централизации: С развитием специализированных устройств для майнинга (ASIC), сети PoW становятся более склонными к централизации в руках крупных игроков, обладающих большими вычислительными ресурсами.

В целом, PoW был первым успешным консенсус-механизмом в блокчейне, который продемонстрировал высокую степень безопасности и надежности. Однако его недостатки, включая высокое энергопотребление и склонность к централизации, побудили исследователей и разработчиков искать альтернативные консенсус-механизмы, такие как Proof of Stake (PoS) и другие [30].

### **1.3.2 Описание консенсус механизма Proof Of Stake (PoS)**

Proof of Stake (PoS) — это альтернативный консенсус-механизм в блокчейне, который используется для подтверждения транзакций и создания новых блоков. В отличие от Proof of Work (PoW), где участники сети (майнеры) конкурируют за право создания блоков, в PoS новые блоки создаются на основе доли (стейка) владения криптовалютой [27].

Принцип работы PoS основан на следующих основных принципах:

1. Стейкинг (Staking): Участники сети, называемые стейкерами, блокируют определенное количество своей криптовалюты в смарт-контракте или специальном кошельке в обмен на право участвовать в процессе создания блоков и получения вознаграждения.

2. Выбор блокопроизводителя (Validator Selection): В PoS блокопроизводители (валидаторы) выбираются случайным образом среди стейкеров на основе их доли в сети. Чем больше стейк у участника, тем выше вероятность того, что он будет выбран для создания блока.

3. Подписывание блоков (Block Signing): Выбранный валидатор создает новый блок, подписывает его и добавляет в цепочку блоков. Этот процесс требует намного меньше вычислительных ресурсов по сравнению с PoW, так как нет необходимости решать сложные криптографические задачи.

4. Подтверждение блоков (Block Confirmation): Другие участники сети проверяют подписанный блок на его корректность и валидность. Если блок проходит проверку, он добавляется в блокчейн, и валидатор получает вознаграждение за создание блока.

Преимущества PoS:

- Энергоэффективность: PoS потребляет значительно меньше энергии по сравнению с PoW, так как процесс создания блоков не требует вычислительных ресурсов для решения сложных математических задач.

- Децентрализация: PoS также обеспечивает высокую степень децентрализации, поскольку любой участник сети, имеющий достаточный стейк, может стать валидатором и участвовать в создании блоков.

- Низкая вероятность централизации: Поскольку выбор валидаторов осуществляется на основе стейка, а не вычислительной мощности, сети PoS менее подвержены централизации в руках крупных игроков.

Недостатки PoS:

- Проблема "Ничего в обороте" (Nothing at Stake): Некоторые критики утверждают, что PoS подвержен риску "ничего в обороте", когда стейкеры могут одновременно подписывать несколько ветвей блокчейна, что может нарушить его целостность.

- Сосуществование с большими владельцами: PoS также может привести к проблеме сосуществования с крупными владельцами криптовалюты, которые могут иметь большее влияние на сеть из-за своего большого стейка.

В целом, PoS представляет собой эффективный и энергоэффективный консенсус-механизм, который становится все более популярным в блокчейн-пространстве. Он обеспечивает высокую степень децентрализации и безопасности сети при сниженном энергопотреблении по сравнению с PoW.

### **1.3.2 Описание консенсус механизма Delegated Proof of Stake (DPoS)**

Delegated Proof of Stake (DPoS) - это вариация консенсус-алгоритма Proof of Stake (PoS), который предлагает улучшенную масштабируемость и эффективность за счет делегирования прав на создание блоков отдельным участникам сети. В DPoS валидаторы (или делегаты) выбираются голосованием участников сети, что позволяет держателям токенов делегировать свои права на создание блоков другим лицам.

Основные принципы работы Delegated Proof of Stake:

1. Выбор делегатов (Validators Selection): В сети DPoS держатели токенов могут голосовать за кандидатов на роль валидаторов, которые будут создавать блоки и поддерживать работу сети. Число делегатов обычно ограничено, что повышает эффективность сети и улучшает ее масштабируемость.

2. Получение права на создание блоков (Block Production Rights): Делегаты, получившие большее количество голосов от держателей токенов, получают право на создание блоков в сети. Эти делегаты затем могут создавать и подписывать новые блоки в соответствии с протоколом сети.

3. Распределение вознаграждений (Reward Distribution): Делегаты, создавшие блоки, получают вознаграждение в виде токенов сети за свою работу. Эти вознаграждения затем распределяются между делегатами и теми, кто им доверяет и поддерживает их.

4. Проверка подписей (Signature Verification): Другие участники сети проверяют подписанные блоки на их корректность и валидность. Если блок проходит проверку, он добавляется в блокчейн, и делегаты получают вознаграждение за создание блока.

Преимущества Delegated Proof of Stake:

- Масштабируемость: DPoS обеспечивает высокую масштабируемость благодаря ограниченному числу делегатов, что позволяет сети обрабатывать большее количество транзакций в секунду по сравнению с PoW или обычным PoS.

- Эффективность: DPoS потребляет меньше энергии и вычислительных ресурсов, так как процесс создания блоков выполняется ограниченным числом делегатов, выбранных голосованием, в отличие от PoW, где каждый майнер конкурирует за право создания блока.

- Децентрализация и управление: DPoS предоставляет держателям токенов возможность участвовать в управлении сетью, голосуя за делегатов и влияя на решения, принимаемые в сети.

Недостатки Delegated Proof of Stake:

- Централизация ресурсов: DPoS может быть более подвержен централизации, поскольку делегаты, получившие большее количество голосов, могут контролировать значительную часть сети и принимать ключевые решения.

- Потенциальный риск атаки на 51%: В сети DPoS существует риск атаки на 51%, когда один или несколько делегатов получают достаточно большую долю голосов, чтобы контролировать более половины сети.

В целом, DPoS представляет собой эффективный и масштабируемый консенсус-механизм, который обеспечивает высокую производительность и децентрализацию в блокчейн-сетях. Однако необходимо учитывать потенциальные риски централизации и атаки на 51%, а также рассмотреть механизмы смягчения этих рисков при разработке и использовании сети DPoS.

### **1.3.3 Описание консенсус механизма Practical Byzantine Fault Tolerance (PBFT)**

Practical Byzantine Fault Tolerance (PBFT) — это алгоритм консенсуса, разработанный для обеспечения безопасности и надежности в распределенных системах, подверженных вредоносным действиям или сбоям узлов. Он является одним из наиболее известных и широко применяемых алгоритмов в блокчейн-технологиях и распределенных системах.

Вот основные принципы работы алгоритма PBFT:

1. Лидер (Leader): В PBFT узлы в сети поочередно выступают в роли лидера, который инициирует процесс формирования блоков и рассылает их другим узлам. Лидер выбирается из числа узлов с помощью алгоритма выборов.

2. Предложение блоков (Block Proposals): Лидер формирует блок, содержащий транзакции, и рассылает его всем остальным узлам в сети.

3. Подтверждение блоков (Block Confirmation): когда узлы получают предложенный блок, они проводят проверку на его корректность и валидность. Если большинство узлов подтверждает блок, он считается окончательным и добавляется в блокчейн.

4. Консенсусное голосование (Consensus Voting): В PBFT узлы в сети голосуют за подтверждение блока. Если достигается кворум голосов, то блок считается подтвержденным и добавляется в блокчейн.

Преимущества алгоритма PBFT:

- Высокая скорость транзакций: PBFT обеспечивает высокую производительность благодаря параллельной обработке транзакций и относительно небольшому числу узлов, участвующих в консенсусе.

- Отказоустойчивость: Алгоритм PBFT способен обеспечить надежность и отказоустойчивость даже в случае отказа или вредоносных действий части узлов в сети.

- Финальность транзакций: после подтверждения блока большинством узлов он считается финальным и не может быть отменен или изменен.

Недостатки алгоритма PBFT:

- Централизация: В PBFT обычно существует определенное количество узлов, участвующих в процессе консенсуса, что может привести к централизации в системе.

- Требовательность к бесперебойной работе узлов: Для успешной работы алгоритма все узлы должны быть доступны и работоспособны. Отказ или сбой даже небольшого числа узлов может снизить производительность и надежность сети.

В целом, Practical Byzantine Fault Tolerance является эффективным алгоритмом консенсуса, который обеспечивает высокую производительность и отказоустойчивость в распределенных системах. Однако необходимо учитывать его требовательность к централизации и непрерывной работе узлов при проектировании и внедрении в блокчейн-системы.

### **1.3.4 Описание консенсус механизма Proof Of Authority (PoA)**

Proof of Authority (PoA) — это алгоритм консенсуса, который используется для подтверждения блоков в блокчейне. В отличие от более распространенных алгоритмов, таких как Proof of Work (PoW) или Proof of Stake (PoS), где участники сети майнят блоки или ставят на них стейки, PoA опирается на авторитет определенных участников сети, называемых авторитетными нодами [14].

Вот основные принципы работы алгоритма Proof of Authority:

1. Авторитетные ноды (Authority Nodes): В сети PoA существует ограниченное количество авторитетных узлов, которые обладают правом на создание новых блоков и подтверждение транзакций. Эти ноды часто выбираются на основе их репутации, надежности и доверия.

2. Подтверждение блоков (Block Confirmation): Авторитетные ноды формируют новые блоки, содержащие транзакции, и подписывают их своими приватными ключами. После этого они распространяют блоки по сети.

3. Проверка подписей (Signature Verification): Участники сети, получившие новый блок, проверяют подпись авторитетных нод и валидируют блок. Если подпись корректна и блок проходит проверку, он добавляется в блокчейн.

4. Децентрализация: хотя в PoA существует ограниченное число авторитетных нод, сеть может быть децентрализованной в том смысле, что участники сети могут быть размещены в разных географических точках и не зависят от одного центрального управления.

Преимущества алгоритма Proof of Authority:

- Высокая производительность: поскольку авторитетные ноды обладают правом на создание блоков, процесс консенсуса в PoA может быть быстрым и эффективным.

- Надежность: Авторитетные ноды обычно имеют высокий уровень доверия и репутации, что повышает надежность сети и защищает ее от вредоносных атак.

Недостатки алгоритма Proof of Authority:

- Централизация: поскольку авторитетные ноды выбираются централизованным образом и имеют контроль над созданием блоков, сеть может быть более централизованной по сравнению с другими алгоритмами консенсуса.

- Низкая стойкость к атакам 51%: если злоумышленник получит контроль над большинством авторитетных нод, он сможет контролировать сеть и вносить изменения в блокчейн [24].

В целом, Proof of Authority — это эффективный алгоритм консенсуса, который подходит для частных блокчейн-сетей или сетей, где важны скорость и надежность транзакций. Однако следует учитывать его недостатки, такие как возможность централизации и низкая стойкость к атакам 51%.

### **1.3.5 Сравнение существующих блокчейн решений на PoA**

Рассмотрим несколько известных блокчейн-решений, использующих PoA, и сравним их по основным характеристикам.

1. Ethereum (в тестовой сети Kovan)

Описание: Ethereum — это одна из самых популярных и широко используемых блокчейн-платформ. В тестовой сети Kovan применяется алгоритм PoA для повышения скорости и снижения стоимости транзакций.

Преимущества:

* Быстрая обработка транзакций.
* Высокая масштабируемость.
* Широкая поддержка сообщества и разработчиков.

Недостатки:

* Не подходит для основного Ethereum-сети (которая использует PoW и PoS).
* Тестовая сеть, не предназначенная для коммерческих приложений.

2. VeChain

Описание: VeChain — блокчейн-платформа, ориентированная на бизнес-приложения и корпоративные решения. Она использует PoA для обеспечения высокой производительности и безопасности.

Преимущества:

* Высокая скорость транзакций.
* Низкие операционные издержки.
* Фокус на корпоративные приложения.
* Интеграция с IoT для отслеживания и управления цепочками поставок.

Недостатки:

* Центральность системы может вызвать вопросы доверия у пользователей.
* Ограниченная децентрализация по сравнению с другими блокчейнами.

3. POA Network

Описание: POA Network — это независимая блокчейн-платформа, специально разработанная для использования алгоритма PoA. Она ориентирована на создание и управление децентрализованными приложениями (dApps).

Преимущества:

* Высокая скорость и пропускная способность сети.
* Простота развертывания dApps.
* Низкие комиссии за транзакции.

Недостатки:

* Меньшая известность и принятие по сравнению с Ethereum.
* Ограниченное количество валидаторов может вызвать вопросы безопасности и устойчивости.

4. Xooa

Описание: Xooa предоставляет блокчейн-платформу с использованием PoA, ориентированную на разработчиков, чтобы упростить создание и развертывание блокчейн-приложений.

Преимущества:

* Простота использования и интеграции.
* Высокая скорость транзакций.
* Поддержка корпоративных приложений.

Недостатки:

* Ограниченная децентрализация.
* Низкая известность по сравнению с крупными блокчейн-платформами.

Каждое из рассмотренных блокчейн-решений на основе PoA имеет свои уникальные преимущества и недостатки. Ethereum (Kovan) и POA Network подходят для разработчиков, ищущих платформу для создания dApps с высокой производительностью и низкими комиссиями. VeChain и Xooa предлагают решения, ориентированные на корпоративные приложения, с акцентом на высокую скорость транзакций и низкие операционные издержки. Выбор подходящей платформы зависит от конкретных потребностей и требований проекта, а также от баланса между децентрализацией, скоростью и безопасностью. Моё блокчейн-решение на PoA обеспечивает уникальные преимущества, которых нет у существующих решений. Оно предлагает более быструю обработку транзакций и повышенную пропускную способность благодаря оптимизированным алгоритмам консенсуса. Усовершенствованные механизмы синхронизации нод обеспечивают большее удобство пользования.

### **1.3.6 Решение вопросов масштабирования и безопасности**

1. Масштабирование: В контексте выбора консенсус-механизма для блокчейн-системы критическое значение имеет способность обеспечения масштабируемости. Каждый из рассмотренных механизмов обладает своими преимуществами и ограничениями в этом отношении. Например, Proof of Work (PoW) хорошо масштабируется за счет распределенной природы майнинга, но сталкивается с проблемами энергопотребления и скорости транзакций. С другой стороны, Proof of Stake (PoS) и Delegated Proof of Stake (DPoS) обычно более эффективны с точки зрения энергопотребления и скорости, но могут столкнуться с проблемами централизации и безопасности. Решение вопроса масштабирования может включать в себя комбинацию различных механизмов консенсуса или применение масштабируемых технологий, таких как sidechains или state channels.

2. Безопасность: при выборе консенсус-механизма необходимо обеспечить высокий уровень безопасности блокчейн-сети. Каждый из рассмотренных механизмов обладает своими уникальными механизмами обеспечения безопасности. Например, Proof of Work (PoW) обеспечивает высокий уровень защиты благодаря сложности вычислений, необходимых для создания новых блоков. Proof of Stake (PoS) также обеспечивает безопасность, используя стейки для голосования, а Delegated Proof of Stake (DPoS) доверяет валидацию блоков выбранным делегатам. Важно провести анализ рисков и принять решение, основанное на компромиссе между масштабируемостью и безопасностью, учитывая потенциальные атаки и уязвимости.

### **1.3.7 Сравнительный анализ и выводы**

Сравнив различные консенсус-механизмы, можно сделать следующие выводы:

1. Proof of Work (PoW): Этот механизм обеспечивает высокий уровень безопасности и децентрализации, но сталкивается с проблемами масштабирования и энергопотребления.

2. Proof of Stake (PoS): PoS эффективен с точки зрения энергопотребления и скорости транзакций, но может иметь проблемы с централизацией и безопасностью.

3. Delegated Proof of Stake (DPoS): DPoS обеспечивает высокую производительность и масштабируемость, но может столкнуться с проблемами централизации и доверия к делегатам.

4. Practical Byzantine Fault Tolerance (PBFT): PBFT обеспечивает высокую производительность и безопасность, но требует доверия к узлам сети и может быть менее децентрализованным.

5. Proof of Authority (PoA): PoA обеспечивает высокую производительность и безопасность за счет ограниченного числа авторитетных узлов, но сталкивается с проблемой централизации.

В зависимости от конкретных требований к проекту и контекста его применения, выбор консенсус-механизма может варьироваться. Важно учитывать как технические, так и организационные аспекты при принятии решения. В случае моего проекта, я выбрал Proof of Authority (PoA), так как он лучше всего подходит под требования безопасности и производительности, необходимые для успешной работы нашего блокчейн-приложения.

## **1.4 Анализ потребностей и проблем, которые приложение должно решать**

Данное приложение призвано решать ключевые вызовы в сфере международных финансовых операций. Основная проблема, на решение которой направлено приложение, — неэффективность и высокая стоимость традиционных методов международных платежей. Существующие системы часто обременены высокими комиссиями и длительными сроками обработки транзакций, что затрудняет оперативное и экономически выгодное выполнение трансграничных платежей.

Проблема недостаточной прозрачности и безопасности также стоит на повестке дня. В классических финансовых системах отсутствует должный уровень прозрачности операций и защиты данных, что порождает риски и недоверие среди участников финансовых операций.

Кроме того, существует проблема затяжного и обременительного процесса соблюдения регуляторных требований в рамках международных транзакций. Традиционные системы требуют многочисленных проверок и документации для соответствия регуляторным нормам, что увеличивает время обработки транзакций и ведет к дополнительным издержкам.

Таким образом, приложение должно обеспечивать:

- Снижение комиссий и минимизацию задержек в международных платежах;

- Повышение прозрачности и безопасности операций;

- Упрощение процесса соблюдения регуляторных требований.

Отдельное внимание заслуживает обеспечение доверия к узлам блокчейна при отсутствии механизма Proof of Work. Предлагается механизм, позволяющий каждому владельцу ноды модифицировать свой код таким образом, что при изменениях нода автоматически перестанет синхронизироваться с остальной частью сети, исключая риски недобросовестного поведения и повышая надежность системы.

Для успешной интеграции и функционирования блокчейна на территории России необходимо учесть соответствие местному законодательству, особенно в части требований KYC и анти-отмывания денег. Интеграция с уже существующими информационными системами и сервисами окажет существенное влияние на снижение трудностей при внедрении и повышение общей эффективности использования приложения.

Рассмотрение экономической целесообразности применения блокчейна на базе PoA включает анализ рыночной конкуренции, развитие информационных технологий и потенциальные санкции, что может стимулировать широкое принятие данной технологии как альтернативного решения для обхода ограничений и улучшения финансовых операций на международном уровне.

### **1.4.1 Анализ потенциальных уязвимостей и защита от них**

Анализ потенциальных уязвимостей и защита от них играет ключевую роль в обеспечении безопасности и надежности блокчейна на основе Proof of Authority (PoA) для проведения трансграничных транзакций. В этой главе проводится детальный анализ потенциальных уязвимостей блокчейна и рассматриваются методы и меры для их предотвращения.

Основные уязвимости и меры защиты:

1. Атака 51%:

- Описание: В традиционных блокчейнах, таких как Bitcoin, атака 51% происходит, когда один участник или группа участников контролирует более половины вычислительной мощности сети, что позволяет им манипулировать подтверждением транзакций [13].

- Меры защиты в PoA: В блокчейне на основе PoA, где доверие основано на предварительно утвержденном списке валидаторов, риск такой атаки существенно снижен. Вместе с тем, чтобы минимизировать риски, необходимо тщательное управление и регулярная проверка списка валидаторов, а также внедрение механизмов для автоматической рассинхронизации с сомнительными узлами [5].

2. Вредоносные атаки на смарт-контракты:

- Описание: Смарт-контракты могут содержать уязвимости в коде, которые могут быть эксплуатированы для манипулирования выполнением контракта или кражи средств.

- Меры защиты: Реализация многоуровневого процесса аудита кода смарт-контрактов, включая автоматические инструменты проверки и ручной аудит экспертами, а также механизмы быстрого отката транзакций в случае обнаружения аномалий.

3. DDoS-атаки (Distributed Denial of Service):

- Описание: Злоумышленники могут направить чрезмерное количество трафика на сеть, что приведет к перегрузке и невозможности обработки легитимных запросов.

- Меры защиты: Использование распределенной архитектуры сети, методов ограничения скорости запросов, а также применение специализированных сетевых решений для защиты от DDoS-атак.

Дополнительные меры защиты:

- Шифрование данных: необходимо использовать современные алгоритмы шифрования для защиты данных, передаваемых в сети, и хранящихся в блокчейне, включая личные ключи и информацию о транзакциях.

- Механизмы аутентификации и авторизации: Внедрение многофакторной аутентификации и строгих политик доступа для обеспечения того, чтобы только авторизованные пользователи могли выполнять операции.

- Аудит и мониторинг: Разработка систем аудита и мониторинга для отслеживания активности в сети и оперативного реагирования на подозрительные действия.

- Регулярные обновления и патчи: Обеспечение своевременного обновления программного обеспечения и аппаратных компонентов для устранения известных уязвимостей.

- Обучение пользователей: Проведение регулярных тренингов для пользователей с целью повышения осведомленности о потенциальных угрозах и методах их предотвращения.

Эффективная реализация этих мер предосторожности способна обеспечить высокий уровень безопасности и надежности блокчейн-системы на основе PoA, устраняя основные уязвимости и предотвращая потенциальные атаки.

## **1.5 Обзор последних тенденций и инноваций в области блокчейн-технологий**

Сегодняшняя эра цифровых технологий непрерывно предоставляет новые возможности для роста и инноваций. Особое внимание заслуживают последние тенденции в блокчейн-технологиях, которые представляют собой катализатор изменений во многих отраслях, начиная от финансов и заканчивая здравоохранением. Цель данной главы - обсудить ключевые инновации и тенденции в блокчейне, особенно в контексте использования механизма Proof of Authority (PoA) для трансграничных транзакций.

Концепция DeFi революционизировала традиционные финансовые услуги, предлагая децентрализованные альтернативы почти каждому финансовому продукту. В рамках DeFi пользователи могут брать и давать взаймы, торговать криптовалютами и получать доход от стейкинга без посредничества традиционных финансовых институтов. Инновации в DeFi, такие как автоматизированные рыночные механизмы и смарт-контракты, создали основу для новых финансовых моделей [28].

Технология блокчейна постоянно развивается, особенно в области механизмов достижения консенсуса. Важным нововведением является механизм Proof of Authority (PoA), который предоставляет преимущества в виде скорости и энергоэффективности, важных для обработки межграничных транзакций. По сравнению с более ранними системами, такими как Proof of Work (PoW), PoA позволяет немногим выбранным узлам подтверждать транзакции, что делает процесс быстрее и менее ресурсоемким [29].

Интеграция блокчейна с передовыми технологиями, такими как искусственный интеллект (ИИ), интернет вещей (IoT) и облачные вычисления, открывает новые возможности для инноваций. Примеры такой интеграции включают улучшение безопасности данных, управление цепочками поставок и оптимизацию различных бизнес-процессов, повышая тем самым эффективность и прозрачность операций.

Блокчейн находит применение во множестве секторов за пределами финансов, включая здравоохранение, где он помогает в управлении медицинскими данными, и в логистике, где способствует прозрачности и эффективности цепочек поставок. Такие инновации не только улучшают текущие процессы, но и открывают двери для создания новых бизнес-моделей [23].

Одной из ключевых проблем для блокчейна остается его потребление энергии, особенно в сетях, использующих PoW. Однако новые подходы, такие как PoA, значительно снижают энергопотребление, что делает блокчейн более экологически устойчивым. Продолжающиеся исследования и инновации направлены на дальнейшее снижение воздействия блокчейна на окружающую среду [11].

В заключение, последние тенденции и инновации в блокчейне продолжают расширять его возможности и сферы применения. Особое внимание заслуживает PoA, который, благодаря своим уникальным свойствам, открывает новые горизонты для обмена активами. Наблюдая за этими разработками, можно предвидеть значительное влияние блокчейна на будущее цифровой экономики.

## **1.6 Выводы по главе 1**

Я рассмотрел различные аспекты разработки блокчейна на основе механизма Proof of Authority (PoA) для системы трансграничных транзакций. Проведенный анализ выявил, что такой блокчейн способен эффективно решать ряд ключевых проблем, среди которых - высокие комиссии и задержки в международных платежах, неэффективность традиционных финансовых систем, недостаточная прозрачность и безопасность операций, а также сложности соблюдения регуляторных требований.

Изучение существующих аналогов блокчейнов позволило выявить различные механизмы консенсуса, такие как Proof of Work (PoW), Proof of Stake (PoS) и Consensus Protocol. Однако, по результатам анализа, было установлено, что механизм PoA представляет собой наиболее подходящий вариант для решения задач системы трансграничных транзакций, благодаря своей эффективности, низкой стоимости проведения транзакций, высокому уровню безопасности и гибкости управления.

Кроме того, в рамках анализа были выявлены дополнительные особенности предлагаемой системы, такие как возможность изменения кода узлов и автоматическая рассинхронизация сети в случае попытки взлома, что дополнительно повышает ее безопасность и надежность.

Таким образом, на основании проведенного анализа можно сделать вывод о целесообразности и перспективности использования блокчейна на основе механизма PoA для реализации системы финансовых операций.