

МИНПРОСВЕЩЕНИЕ РОССИИ

ФГБОУ ВО «НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. КОЗЬМИ МИНИНА»

Физико-технологический факультет

Кафедра физики, математики и физико-математических наук

Контрольная работа

**ПО ДИСЦИПЛИНЕ «СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ»**

Тема работы: «Системы распределенного реестра»

Студента 1 курса бакалавра

Группа МЭ-23-1

направление подготовки: 44.03.05

«Педагогическое образование»

профиль: «Математика и Экономика»

Варнеевой Татьяны Ивановны

Нижний Новгород

2022

Содержание

Введение	3
Глава 1. Технология распределённых реестров	
1.1. Классификация сетей распределённых реестров	4
1.2. Роли в системе (консенсус, валидация, криптография и смарт контрасты)	7
Глава 2. Преимущества технологии и возможные сферы её применения	
2.1. Локальные и трансграничные платежи	9
2.2. Сделки с ценными бумагами, товарными активами и производными финансовыми инструментами; обмен информацией	10
Заключение	12
Список литературы	13

Введение

В настоящее время наблюдается взрывной рост интереса к технологии распределенной реестровой системы, лежащей в основе популярной криптовалюты bitcoin, появившейся в 2009 году. В практике данной сферы термин "распределенный реестр" активно применяется не только к базе данных, но и к ряду других технологий, включая блокчейн - цепочку блоков транзакций.

Основным стимулом повышенного внимания к технологии распределенных реестров, особенно в финансовой сфере, являются надежды на решение ряда проблем и ограничений, свойственных используемым в настоящий момент методам хранения, учета и передачи финансовой информации.

Многие эксперты признают технологию распределенного реестра революционным инновационным потенциалом в области платежей, клиринга, расчетов и других финансовых операций. Кроме того, ее использование может значительно изменить систему хранения и обслуживания активов, урегулирования обязательств, исполнения контрактов и управления рисками.

Не смотря на огромный потенциал данной технологии, ее развитие все еще находится на ранней стадии, отсутствуют установленные стандарты и типовые решения, а большинство проектов остается в пилотном статусе.

Глава 1. Технология распределённых реестров

1.1. Классификация сетей распределённых реестров

Технология распределённых реестров – это метод обмена и хранения информации, где каждый участник имеет полную копию реестра. Копии реестра синхронизируются на основе протокола распределённого консенсуса, то есть соглашения между участниками о добавлении новой информации. Каждый участник может иметь доступ к истории транзакций. В рамках сетей распределённых реестров (PP), устройства, на которых работает соответствующее программное обеспечение и которые совместно ведут распределённые базы данных, называются узлами. Узлы участников сети подключаются друг к другу для обмена и подтверждения информации, что отличается от традиционных централизованных систем, где есть единственный источник достоверных данных. Распределённые реестры обеспечивают возможность хранения актуальных копий базы данных на нескольких узлах, обеспечивая при этом повышенную надежность операций. Блокчейн представляет собой вариант реализации сети распределённых реестров, где данные о совершенных транзакциях структурируются в виде связанных блоков.

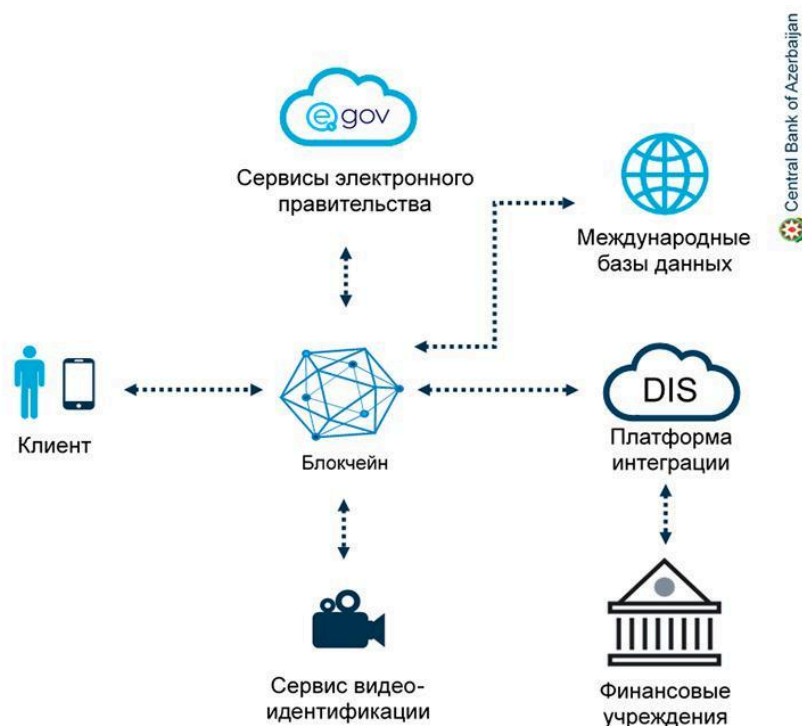


Рис. 1. Технология блокчейн

Стоит отметить, что не все сети распределенных реестров используют технологию блокчейн. Например, протокол Ripple предусматривает процессинг транзакций без формирования блоков. В случае использования блокчейн каждый новый блок транзакций подтверждается участниками сети как валидный. После того как он присоединяется (встраивается в цепочку), в распределенном реестре выполняются все предыдущие операции. Открытые сети распределенных реестров - это сети, в которых участники не проходят полноценной идентификации, анонимность или псевдоанонимность, доступ к участию в которой не ограничен для широкого круга пользователей, статус не закреплен за определенными участниками, а также отсутствуют централизованные инстанции, управляющие правилами сети, ее конфигурацией и выпуском криптографических ключей. Криптовалютные сети распределенных реестров, такие как bitcoin, обычно представляют собой открытые системы.

Закрытые сети распределенных реестров устанавливают критерии членства, в соответствии с которыми участники допускаются к управлению узлами и получают доступ к сервисам сети. Эти критерии могут включать финансовые требования, например, платежеспособность участника или

возможность получения доступа к ликвидным ресурсам, а также юридические требования, способность участника выполнять договорные обязательства перед системой или наличие соответствующих лицензий на осуществление деятельности. В такой сети участники идентифицируемы, допуск ограничен и регламентирован согласно правилам сети, статус участников, ответственных за валидацию, закреплен за определенными контрагентами, и в большинстве случаев существует некоторая инстанция, управляющая правилами сети. Гибридные сети распределенных реестров сочетают в себе свойства как открытых, так и закрытых сетей.

Финансовый сектор ориентирован в основном на разработку закрытых и гибридных сетей. Они имеют наиболее высокий потенциал применения на финансовом рынке в связи с возможностью создания механизмов управления сетью, ограничения допуска к ней, а также контроля и надзора за действиями участников.

Сети распределенных реестров также классифицируются по различным признакам:

- по объектам транзакций: информация; виртуальная ценность.
- по типу доступа к сети: неограниченный; ограниченный.
- по требованиям к прохождению идентификации: анонимная; псевдоанонимная; полная идентификация.
- по применяемому протоколу достижения консенсуса сети: PoW (Proof-of-work); PoS (Proof-of-stake); PoS + PoW; PBFT (Practical Byzantine Tolerance), Paxos, RAFT; Non-BFT (Non Byzantine Tolerance).

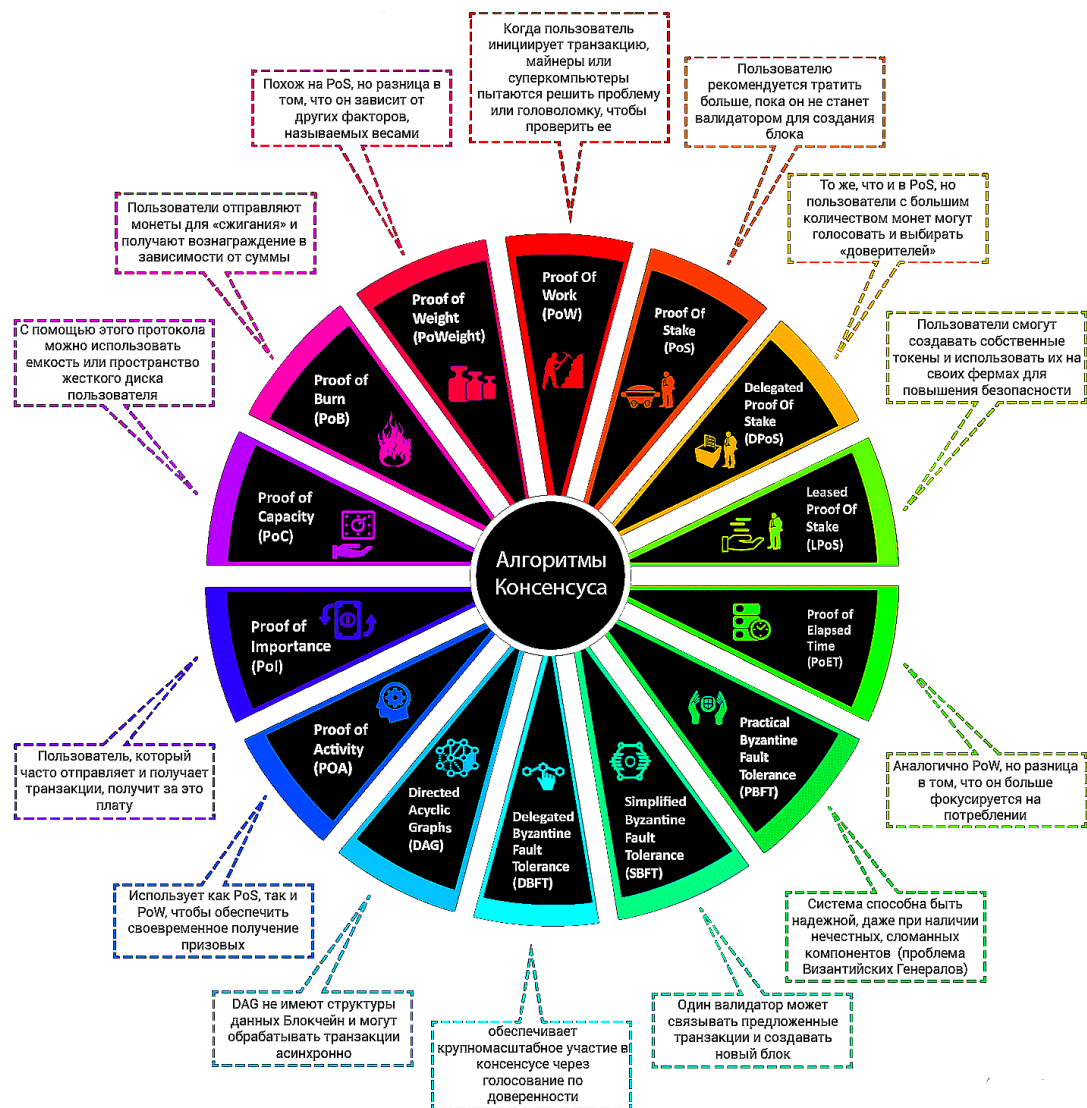


Рис.2. Алгоритмы консенсуса

- по наличию центрального администратора: существует центральный администратор; отсутствует центральный администратор.

Независимо от того, открытая или закрытая сеть распределенных реестров, участники могут иметь различные роли и функции, такие как работа с информацией в отношении существующих активов, оформление новых активов, подтверждение операций, обновление истории операций в реестре. Некоторые участники могут иметь доступ только к просмотру реестра, другим может также разрешаться вносить записи в реестр. Реестры историй сделок и статусов владения ценностями обычно ведутся в качестве общего реестра, которому доверяют все участники.

1.2. Роли в системе (консенсус, валидация, криптография и смарт контрасты)

В рамках системы существуют различные роли участников, включая:

- Пользователь: физическое или юридическое лицо, обладающее правом вносить изменения в реестр.
- Валидатор: узел, которому делегировано право обновлять реестр и принимать участие в достижении консенсуса.
- Посредник: промежуточное технологическое звено между внутренними и внешними участниками.
- Администратор: провайдер определенных услуг в системе, таких как нотариальное заверение, разрешение споров и установление стандартов.

В отсутствие центрального органа, который авторитарно обновляет реестр, валидаторы достигают согласия относительно общего состояния реестра. Процесс консенсуса, как правило, включает два основных этапа: проверку, где каждый валидатор идентифицирует и проверяет корректность вносимых изменений в реестр, и достижение соглашения об обновлении информации в реестре и утверждение изменений с использованием механизмов, которые предотвращают конфликты в реестре.

Технология распределенных реестров использует различные криптографические методы и инструменты. Например, в решениях на основе технологии блокчейн, цепь блоков создается с использованием механизмов хеширования. Каждый блок в цепи содержит хеш предыдущего блока и свой порядковый номер. Новый блок подтверждает транзакции, содержащиеся в нем, и дополнительно подтверждает транзакции в предыдущих блоках, обеспечивая неизменность хранимой информации.

Для гарантии неизменности и подлинности транзакций они подписываются электронной цифровой подписью, которая может быть проверена с использованием открытого ключа отправителя транзакции. Значение хеш-функции от открытого ключа отправителя используется в

качестве идентификатора отправителя, обеспечивая идентификацию участников сети.

Смарт-контракт представляет собой электронный договор, исполнение прав и обязательств по которому осуществляется через автоматические цифровые транзакции в распределенном реестре в строго заданной последовательности и при наступлении определенных обстоятельств. Смарт-контракты могут зависеть от наступления определенных событий. Например, они могут использоваться при размещении корпоративных облигаций, где контракт автоматически выполняет купонные платежи при определенных событиях.

Однако взаимозависимость и одновременное автоматизированное исполнение смарт-контрактов могут привести к появлению негативных и непредсказуемых событий в финансовой экосистеме. Некоторые примеры уязвимостей смарт-контрактов включают проект TheDAO, который потерял значительную сумму из-за ошибки в коде и требовал вмешательства разработчиков для решения проблемы.

Глава 2. Преимущества технологии и возможные сферы её применения

2.1. Локальные и трансграничные платежи

Технология распределенных реестров имеет несколько преимуществ, которые стимулируют участников финансового рынка заниматься исследованиями, разработкой и внедрением данной технологии. Ниже перечислены основные преимущества:

1. Упрощенный характер проведения транзакций, особенно в случае многосторонних трансграничных сделок.
2. Непрерывное функционирование сети, обеспечивающее бесперебойность и гарантированность обработки транзакций.

3. Снижение необходимости документарного оформления процесса проведения сделок между участниками.

4. Повышенная прозрачность и неизменность ведения реестров сделок.

5. Повышенная устойчивость благодаря распределённости и наличию большого количества копий данных.

В настоящий момент электронные трансграничные платежи часто включают промежуточную стадию конвертации средств через систему корреспондентских отношений между банками, что влечет за собой выплату нескольких комиссий. Однако технология распределенных реестров предлагает решения, позволяющие осуществлять прямое заключение сделок без лишних посредников. Это потенциально способствует сокращению количества этапов, необходимых для проведения трансграничных платежей, и способствует установлению прямых отношений между сторонами.

Важным шагом в развитии технологии является разработка Межреестрового протокола (Interledger Protocol, ILP), который облегчает передачу операций между различными реестрами и обеспечивает точки соединения между двумя или более распределенными реестрами. Протокол ILP представляет собой набор процедур для оптимального пути платежей и зашифрованного депонирования средств в совместимых реестрах, а затем исполняет эти депонированные операции после подтверждения получателя. Протокол ILP разрабатывается как открытый стандарт для повышения совместимости и упрощения передачи цифровых активов, позволяя участникам из разных стран с разными платежными системами легче взаимодействовать друг с другом

2.2. Сделки с ценными бумагами, товарными активами и производными финансовыми инструментами; обмен информацией

Кроме того, технология распределенных реестров нашла применение в области сделок с ценными бумагами, товарными активами и производными финансовыми инструментами. Крупные биржи изучают решения на основе

распределенных реестров с целью улучшения существующих процессов расчетов и клиринга сделок на биржах. Участники финансового рынка видят потенциал технологии распределенных реестров для сокращения рисков и издержек при торговых операциях с ценными бумагами. Существующие процедуры, требующие ручного выполнения или дублирования в нескольких организациях, вызывают значительные затраты. Технологические решения на базе распределенных реестров разрабатываются для снижения и разделения затрат на поддержку такой учетной инфраструктуры.

Другим аспектом преимуществ технологии распределенных реестров является ее потенциал для обмена информацией. Благодаря возможности создания неизменяемых распределенных реестров возникают новые способы обмена информацией между аудиторами и органами банковского надзора. Например, архитектура решения может быть спроектирована таким образом, чтобы аудиторы или органы банковского надзора имели доступ только для просмотра определенных частей общего реестра. Это позволяет более эффективно выполнять нормативные требования к отчетности, а органам надзора получать более достоверную информацию о происхождении активов и истории операций, осуществляемых участниками. Подключение органа надзора к сети в качестве узла позволяет получать данные о совершенных операциях сразу после их передачи в сеть, что упрощает надзорные мероприятия и сокращает затраты на них.

Заключение

В настоящее время ведущие мировые финансовые институты, регуляторы и технологические компании активно занимаются исследованием и разработкой пилотных проектов в области технологии распределенных реестров, а также разработкой соответствующих регуляторных подходов. Когда дело касается финансовой информации, эта технология может предоставить новые способы передачи и записи информации о правах собственности на цифровые активы, обеспечить неизменяемое и безопасное хранение информации, управление идентификационными данными и доступ участников к общедоступному, но распределенному реестру. Технология может быть использована для совершения переводов и платежей (в том числе международных), расчетов по ценным бумагам, а также обмена и хранения информации. Ее использование может помочь решить ряд проблем и ограничений, существующих в существующих системах. При этом ключевые игроки на рынке разрабатывают разные подходы к своим проектам. Учитывая раннюю стадию развития технологии распределенных реестров, существует множество вопросов, связанных с ее развитием и применением (включая технологические, юридические и управленческие риски). Технология распределенных реестров может оказать значительное влияние на финансовый рынок. Возможные изменения включают модернизацию существующей системы, устранение некоторых посреднических функций или, в крайнем случае, некоторых институтов. Более того, эта технология может способствовать появлению новых небанковских участников, которые не обязательно соответствуют законам о финансовом посредничестве, что может привести к изменениям в ценообразовании услуг и оказать влияние на конкурентную среду.

Список литературы

1. «Развитие технологии распределённых реестров» Центральный банк Российской Федерации, 2017 г. ([Consultation_Paper_171229\(2\).pdf \(cbr.ru\)](#))
2. «Технологии распределенного» Центральный банк Российской Федерации, 2022 г. ([Технологии распределенного реестра \(cdto.wiki\)](#))
3. «Технология распределенного реестра простыми» PROSTOCOIN, 2020 г. (<https://prostocoin.io/blog/dlt>)
4. «Алгоритмы Консенсуса в Блокчейне: POW, POS и другие» Деньги в Сети, 2020 г. (https://yandex-deengi.ru/sovety/konsensusa-eto.html?utm_referrer)
5. «Технология блокчейн» 2023 г. (<https://triptonkosti.ru/18-foto/tehnologiya-blokchejn-prezentaciya.html>)