Грант Президента Российской Федерации №18-1-007918 «Обучение цифровизации основных процессов управления представителей менеджмента в сфере образования и культуры регионов РФ»

Методика для обучения/консультирования сотрудников региональных и муниципальных органов власти в сфере образования и культуры

Модуль 11. Памятка по технологиям распределенных реестров: перспективы применения в управлении в сфере образования и культуры

Оглавление

Введение. Базовые понятия и классификация технологий распределённых реестров 3
1. Проблематика и риски применения технологий РР.....5
2. Преимущества и недостатки технологий распределенных реестров.....7
3. Применение технологий РР в сфере образования и культуры 7
3.1. Цели и задачи разрабатываемой системы.....7
3.2. Описание программной архитектуры.....8
3.3. Структура smart-контрактов.....9
Заключение.....10

Введение. Базовые понятия и классификация технологий распределённых реестров

Распределенный реестр (РР)— это база данных, которая распределяется между сетевыми узлами или вычислительными устройствами. Каждый из узлов может получать данные от других узлов, при этом храня полную копию реестра базы данных. Обновления таких узлов происходит независимо друг от друга. Затем узлы голосуют за обновления, чтобы удостовериться, что большинство узлов согласно с окончательным вариантом. Голосование и достижение согласия в отношении одной из копий реестра называется консенсусом, этот процесс выполняется автоматически с помощью алгоритма консенсуса. Как только консенсус достигнут, распределенный реестр обновляется, и последняя согласованная версия реестра сохраняется в каждом узле. Распределенные реестры не все используют последовательность блоков для достижения достоверного консенсуса в распределенной системе защищенным от злоупотреблений способом. Так, например, протокол Ripple[1] подразумевает транзакционный процессинг без формирования блоков.

Особенность таких реестров является возможность синхронизации между ранними и более поздними копиями, а изменения отражаются в них в течение очень короткого отрезка времени (минут, секунды). Это позволяет избегать ручной сверки разных копий реестров, процесс автоматизирован. У участников такой сети узлов есть индивидуальная копия базы данных, которую они могут изменять по своему усмотрению.

Главная особенность распределенных реестров — это отсутствие единого центра управления.

Блокчейн[2] — это один из видов распределенного реестра. Блокчейн распределен в одноранговой сети и управляется с помощью этой сети. Так как это частный случай распределенного реестра, он может существовать без центральной власти или управляющего сервера, а качество данных в блокчейне обеспечивается репликацией базы данных и доверием, основанном на вычислениях. Однако структура блокчейна отличается от структуры других видов распределенных реестров. Данные в блокчейне сгруппированы и организованы в блоки. Блоки соединены друг с другом и защищены криптографическими методами. В сущности, блокчейн — это постоянно растущий реестр записей. В блокчейн можно только добавлять данные. Нельзя удалять или изменять данные, сохраненные в предыдущих блоках. Технология блокчейн используется для записи событий, управления записями, обработки транзакций, отслеживания операций с активами и голосований.

Каждый блокчейн — это распределенный реестр, но не каждый распределенный реестр — блокчейн. В обоих случаях подразумевается децентрализация и достижение консенсуса между узлами. Кроме того, в блокчейне данные организованы в блоки, и разрешено только добавлять новые данные.

Для наглядности на рисунке 1 показано отличие в архитектуре связей централизованных, децентрализованных и распределенных реестров.

[1] Подробное описание принципа действия протокола Ripple доступно по ссылке: https://ripple.com/files/ripple_consensus_whitepaper.pdf

[2] По данным электронного ресурса, режим доступа свободный: https://ethclassic.ru

Рис. 1 Архитектура связей реестров

Классификация сетей распределенных реестров[3]:

- Открытые сети распределенных реестров – это сети, в которых участники не проходят полноценной идентификации (анонимность или псевдоанонимность), допуск 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.
- 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 различные требования, например, юридические (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.

Сети распределенных реестров также классифицируются по различным признакам:

- по объектам транзакций:
  - информация;
  - виртуальная ценность (ценность, аналог которой отсутствует в реальном мире»);
- по типу доступа к сети:
  - неограниченный (сети, в которых участникам позволено осуществлять любую деятельность);
  - ограниченный (сети, которые ограничивают виды деятельности участников);
- по требованиям к прохождению идентификации:
  - анонимная;
  - псевдоанонимная;
  - полная идентификация;
- по применяемому протоколу достижения консенсуса сети:

[3] По материалам доклада Банка России «Развитие технологий распределенных реестров», декабрь 2017 год.

– PoW (Proof-of-work) – право удостоверения блока дается участнику на основании выполнения им некоторой достаточно сложной работы, которая удовлетворяет заранее определенным критериям.
– PoS (Proof-of-stake) – право удостоверения блока дается держателю счета, когда количество его средств и срок владения ими соответствуют заданным критериям. Формулы расчета критериев могут незначительно различаться.
– PoS + PoW – гибрид PoW и PoS, когда блоки могут удостоверяться как через вычисляемые критерии PoS, так и PoW-перебором. Цель такого подхода – усложнить пересчет всей цепочки (с самого первого блока), возможный в случае использования PoS в чистом виде.
– PBFT (Practical Byzantine Fault Tolerance), Paxos, RAFT – алгоритмы многоэтапного установления консенсуса сети (устойчивые к «византийскому поведению»[4]). Алгоритмы данной группы позволяют сетям РР функционировать с небольшими затратами и имеют значительную пропускную способность, но слабоустойчивы к увеличению количества участников.
– Non-BFT (Non Byzantine Fault Tolerance) – алгоритмы консенсуса, неустойчивые к поведению, при котором часть участников начинает работать против сети. Такие алгоритмы применимы в закрытых сетях с полной идентификацией.

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

Независимо от того, открытая или закрытая сеть РР, участники могут иметь различные роли и функции (работа с информацией, подтверждение операций, обновление истории операций в реестре и прочие). Некоторые участники могут иметь доступ только к просмотру реестра, другим может также разрешаться вносить записи в реестр. Реестры историй и статусов владения «ценностями» обычно ведутся в качестве общего реестра, которому доверяют все участники.

Smart-контракт – это договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре в строго определенной им последовательности и при наступлении определенных им обстоятельств. Исполнение смарт-контрактов может зависеть от наступления определенных событий. При наступлении определенного события такой контракт автоматически начинает совершать требуемые транзакции.

1. Проблематика и риски применения технологий РР

Как и с большинством новых технологий, довольно сложно в полной мере оценить все будущие способы использования и риски. И в случае с каждой новой технологией вопрос не в том, хороша ли сама по себе технология или плоха. Несмотря на то, что все чаще проводятся эксперименты по внедрению технологий распределенных реестров, и прежде чем они смогут стать практическим решением, необходимо решить ряд вопросов. Вопросы следующие: какое применение может найти технология? для какой цели? и в каком виде она может быть применена и как гарантирует безопасность?

[4] «Задача византийских генералов» – задача синхронизации узлов распределенной системы в случае, когда некоторые узлы могут предоставлять ненадежную или недостоверную информацию («византийское поведение»)

Некоторые риски, которые предстоит принять во внимание для обеспечения применения и распространения технологии РР в сфере образования и культуры, возникают в следующих аспектах:

- **Безопасность.** Криптография играет основную роль в обеспечении безопасности систем распределенных реестров. Эффективное управление криптографическими ключами и данными доступа – это особенно важный вопрос в контексте применения технологии распределенных реестров, поскольку в случае потери или раскрытия ключей, или данных доступа существует риск понести существенные потери. Утерянные ключи могут стать причиной невозможности использования или доступа к информации, что, в свою очередь, приведет к безвозвратной потере узла сети. Необходимость сохранять конфиденциальный характер закрытых ключей – сложная и проблематичная задача, которая зависит от ряда факторов, включая надежность алгоритмов и протоколов, используемых для создания, хранения, распространения, отзыва и уничтожения ключей.
  Дополнительно возникает необходимость в точном определении, какая информация будет вноситься в систему и становиться доступной другим участникам. Этот вопрос особенно сложен в случае обмена информацией между конкурентами (образовательными и культурными организациями), которая может включать сведения о клиентах этих организаций.
  Необходимо также обеспечить соблюдение законов и нормативных актов о конфиденциальности информации. Участники должны будут согласовать уровень предоставления информации, а также то, будет ли по-прежнему полный пакет информации доверяться центральному учреждению (например, регулятору). Кроме того, как отмечалось раннее, распределенное хранение информации предполагает наличие копии распределенного реестра на каждом узле – участнике сети, что затрудняет обеспечение конфиденциальности хранимых данных и разграничение доступа для различных участников сети.
- **Масштабируемость и скорость работы.** Технологические ограничения производительности и масштабируемости сетей на основе технологии распределенных реестров связаны с пропускной способностью и временем подтверждения транзакций, а также с размером и скоростью распространения распределенной базы записей. Алгоритмы согласования и криптографические проверки увеличивают время ожидания и ограничивают количество операций, которые сети распределенных реестров могут обрабатывать одновременно.
  Система на основе технологии распределенных реестров должна обладать масштабируемостью, необходимой для удовлетворения текущих потребностей, и быстрой скоростью совершаемых операций, сравнимой со скоростью традиционных централизованных решений. В противном случае она вряд ли будет приемлема для образовательных и культурных организаций или государственных органов.
- **Управление информацией.** Внедрение технологии распределенных реестров ведет к тому, что участники пользуются общей информацией, хранящейся в реестре с историей, которую крайне сложно (или практически невозможно) изменить. Очень важно, чтобы такая общая информация была достоверна. Это требование может быть сложно выполнить при внесении информации в реестр несколькими участниками. Необходимо принять решение о том, кто может создавать новые записи и как проверяется подлинность и верность новой информации, вводимой в систему. Кроме того, должны быть определены способы выявления ошибок и заведомо мошеннических транзакций, а также способы решения этих проблем. Вопросы правдивости или достоверности вносимой информации требуют рассмотрения с точки зрения норм этики и морали.

- **Регулирование.** Прямых запретов применения технологии РР не установлено, к ее использованию применяются общие нормы законодательства, в том числе требования по идентификации участников, обеспечению защиты персональных данных и конфиденциальной информации, обеспечению прав потребителей.

Можно ожидать, что в России и в мире по мере развития практики применения технологии РР может потребоваться разъяснение порядка применения общих норм законодательства или разработка специального регулирования отдельных аспектов применения технологии РР.

2. Преимущества и недостатки технологий распределенных реестров

Технологии распределенных реестров позволяют сокращать цепочку посредников в процессе передачи и обмена той или иной информацией между узлами, а также способствуют уменьшению затрат на доверие между участниками реестра. Использование распределенных реестров снижает зависимость от органов-посредников: банков, юристов, нотариусов и так далее. Можно выделить несколько преимуществ технологии распределенных реестров:

- непрерывное функционирование сети, бесперебойность, гарантированность обработки процессов передачи информации;
- снижение необходимости документарного оформления процесса обмена информацией между участниками;
- прозрачность и неизменность ведения реестров;
- повышенная устойчивость системы реестров благодаря распределенности и наличию большого количества копий данных.

По мнению многих экспертов[5], технология распределенного реестра обладает прорывным инновационным потенциалом и может способствовать радикальному изменению системы обслуживания и хранения информации, урегулирования обязательств, исполнения контрактов и управления рисками.

Несмотря на большой потенциал технологии, в настоящий момент она находится на ранней стадии развития, отсутствуют устоявшиеся стандарты и типовые решения, а большинство проектов находится в статусе пилотных. В докладе Центрального банка РФ «Развитие технологий распределенных реестров», так же отмечается, что взаимозависимость и одновременное автоматизированное исполнение смарт-контрактов могут способствовать появлению негативных и непредсказуемых событий.

3. Применение технологий РР в сфере образования и культуры

Реализация технологии РР позволила разработать технологию[6] smart контрактов, обеспечивающую неизменное выполнение заранее определенных последовательностей событий, отражающихся в распределенном реестре. Далее приведен пример использования такой технологии в сфере высшего профессионального образования.

3.1. Цели и задачи разрабатываемой системы

Целями внедрения разрабатываемой системы распределенного реестра являются:

- повышение прозрачности системы поступления и обучения в вузе;

[5] «The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services», World Economic Forum

[6] Автор И. Е. Савельев, описание доступно в статье журнала «Прикладная информатика» Часть. 13. № 2 (74). 2018. Приведен авторский текст и рисунки.

- борьба с фальсификацией дипломов, тем самым повышается ценность документов о получении высшего образования.

Задачами, решаемыми с помощью разрабатываемой системы, являются:

- ведение базы абитуриентов;
- ведение информации по контролю успеваемости обучающихся;
- ведение информации о государственных экзаменах и защите выпускных квалификационных работ;
- ведение реестра выданных дипломов.

Стоить отметить, что разрабатываемая система не предназначена для полноценной автоматизации ведения внутреннего учета деятельности учебного заведения. На данный момент, с одной стороны, существует ФИС ГИА и приема — Федеральная информационная система обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего образования. Данная система используется для контроля корректного зачисления абитуриентов в учебные заведения[7].

Также существует Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении. Данный реестр создан для обеспечения снижения оборота поддельных документов об образовании[8].

В данных системах хранится информация, содержащая персональные данные второй категории — персональные данные, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к первой категории (расовая, национальная принадлежность, политические, религиозные и философские убеждения, состояние здоровья)[9]. С учетом объемов хранимой информации данные системы относятся к первому классу систем с точки зрения Информационной системы персональных данных (ИСПДн), что приводит к обязательной сертификации на соответствие требованиям информационной безопасности систем вузов, интегрированных с ФИС ЕГЭ и приема.

3.2. Описание программной архитектуры

Разрабатываемая архитектура является анонимизированной средой передачи данных между генератором информации в лице учебных заведений и поставщиками данной информации в лице Министерства науки и высшего образования РФ (далее Минобрнауки России), а также прочих сервисов, например, сервиса проверки подлинности документов о наличии высшего профессионального образования.

С точки зрения открытости разрабатываемую распределенную информационную систему можно отнести к открытым с настраиваемой политикой доступа, т. е. читать данные сможет любой пользователь системы, но создавать новые записи в базе данных возможно только при наличии доступа к контакту. Также возможна реализация закрытого блокчейна для использования только вузами и государством в лице Минобрнауки России.

В отличие от текущих систем, в разрабатываемой системе будут отсутствовать персональные данные. Они будут находиться только внутри сети вузов и в ИС, принадлежащих государству. Вместо ФИО абитуриентов и студентов в системе предполагается хранить их хешированные значения. Архитектура в разрезе программного обеспечения и интеграционного взаимодействия с точки зрения учебного заведения представлена на рис. 2. Хранение персональной информации, а также учет основной деятельности учебного заведения ведется в его внутренней информационной системе. В демилитаризованную зону (DMZ) сети учебного заведения выносится нода сети

[7] Система ФИС ГИА и приема. URL: http://priem.edu.ru/NewsArchive.aspx.

[8] Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении. URL: http://frdocheck.obrnadzor.gov.ru

[9] Федеральный закон от 27.07.2006 №152‑ФЗ «О персональных данных».

разрабатываемой системы. В данном участке сети персональные данные заменены на их захешированные значения. Взаимодействие с другими нодами системы осуществляется по протоколу UDP[10]. Интеграционное взаимодействие внутренней ИС учебного заведения предлагается организовать с помощью JSON-RPC интерфейса на стороне ноды УЗ. При этом взаимодействие будет односторонним, что является одним из требований к организации DMZ-зоны.

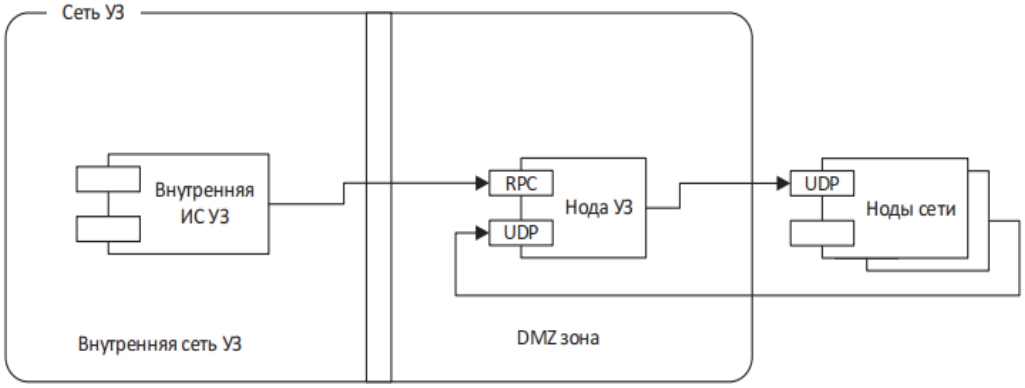

Рис. 2 Архитектура системы с точки зрения учебного заведения

3.3. Структура smart-контрактов

Предполагается, что государством в лице Минобрнауки России будет разработано несколько вариантов «Умных контрактов». При регистрации вуза в системе для него будет создан экземпляр контракта, соответствующий его особенностям. Каждый экземпляр smart- контракта будет соответствовать деятельности одного вуза. При наличии нескольких филиалов один экземпляр smart-контракта будет соответствовать филиалу учебного заведения.

Для разработки smart-контракта потребуется выделить основные сущности, а также бизнес-процессы. Для описания основных бизнес-процессов потребуется ввести несколько основных сущностей:

- Абитуриент — описывает поступающего человека до момента его поступления в вуз, используется для создания общей базы абитуриентов и контроля исполнения правил поступления в учебные заведения.
- Учащийся — основная сущность, описывающая состояние учащегося, используется во всех основных бизнес-процессах в части контроля успеваемости.
- Преподаватель. Данная сущность используется для добавления информации об успеваемости учащихся, о защите ВКР учащихся.

Общий реквизитный состав основных сущностей составляет основу реализации хранения данных в разрабатываемом smart-контракте[11].

Далее из всех бизнес-процессов учебного заведения выделены основные действия (события), которые имеют непосредственное отношение к контролю успеваемости студентов и получению ими дипломов. Данные события[12] и их характеристика относятся к прикладным.

Дополнительно потребуется ввести несколько административных событий:

- добавление нового преподавателя;
- закрепление дисциплины за преподавателем;
- назначение комиссии для государственного экзамена и защиты ВКР;

[10] Описание протокола UDP https://ru.wikipedia.org/wiki/UDP

[11,12] Подробный состав представлен в статье журнала «Прикладная информатика» Часть. 13. № 2 (74). 2018. Автор И. Е. Савельев

- назначение периодов для внесения данных по контролю успеваемости учащихся и защите дипломов.

С точки зрения программного кода smart‑контракта списки учащихся, преподавателей, а также информация об успеваемости являются глобальными переменными smart‑контракта. Прикладные и административные события — методы smart‑контракта, в случае успешного исполнения которых генерируются системные события (Events), используемые внешними системами (Учетной системой УЗ и информационными системами в Минобрнауки России)[13]. Согласно данным Минобрнауки России, в 2017 г. общая численность студентов составила 3032738 чел., выпущено было 732625 студентов. Общее количество образовательных организаций с филиалами составило 1417[14]. Таким образом, число выпускников на вуз составило 517 человек. При среднем размере транзакции (Записи нового события) в 1 Кб ежегодный прирост базы данных оценивается в 2–3 Гб при 100% использовании разрабатываемой системы всеми учебными заведениями страны.

Открытым остается вопрос о необходимости первоначальной регистрации абитуриентов в системе. Предлагаемая архитектура распределенного реестра в дальнейшем может быть использована и в других социальных институтах. Соответственно, потребуется единая система сквозной аутентификации пользователей системы. Для реализации данной функции возможна интеграция с порталом Госуслуг, соответственно, функция генерации личного адреса в разрабатываемой системе может быть передана на портал Госуслуг.

Архитектура распределенного реестра, рассматриваемая в примере, позволяет решить задачи учета абитуриентов и повышения прозрачности поступления в учебные заведения, а также снизить оборот поддельных документов об образовании.

Заключение

Большинство государств еще не определили собственную позицию по отношению к технологии распределенных реестров. Все страны, в которых были сделаны официальные заявления о потенциальных намерениях в сфере регулирования, отмечают высокий потенциал технологии и демонстрируют желание поддержать развитие рынка, в том числе за счет отсрочки регуляторных мер. Однако следует отметить, что ни одно государство еще не приблизилось к созданию полноценной регуляторной среды в сфере использования распределенных реестров ввиду того, что регулирования требуют сервисы, построенные на их основе, а не сама технология.

Распределенные реестры представляют собой концептуальные прорывы в управлении данными, которые могут найти применение в различных сферах, в том числе в сфере образования и культуры. Возможность ведения устойчивых к несанкционированным изменениям РР может привести к новым способам обмена информацией между такими участниками, как специалисты Минобрнауки России, РОИВ и их подведов, муниципальных органов управления, образовательных и культурных региональных и муниципальных организаций. Например, архитектуру решения можно спроектировать таким образом, чтобы участники в зависимости от роли в системе имели различные права доступа к определенным частям общего реестра. Это позволит эффективнее выполнять нормативные требования к отчетности, а органы Минобрнауки России смогут получить более достоверную информацию о процессах в образовательных организациях. Имея подключение к сети в качестве узла, Минобрнаука России будет

[13] Супибекова А. К., Эсеналиева Г. А. «Применение Smart‑contract в платформе Ethereum» // Вестник КГУСТА. 2017. №2 (56). С. 73–77.

[14] Сводные отчеты по форме ФСН № ВПО‑1 на начало 2017/18 учебного года. URL: https://минобрнауки.рф/министерство/статистика/информация‑2017/во‑2017/ФСН‑ВПО‑1–2017

получать данные о процессах сразу же после их передачи в сеть, что может упростить выполнение контрольных мероприятий и сократить затраты на них.

На сегодняшний день технологии блокчейн уже позволяют строить системы, устойчивые к изменениям записанной информации и автоматизирующие учет основных бизнес процессов многих сфер государственного управления, экономики, образования и других сфер. Цифровая среда дает возможность анализировать и изменять информацию об объектах, которые часто вовсе не рассматриваются в качестве объектов интеллектуального права. К таковым можно отнести сложные информационные модели, различные коды и алгоритмы. Но на данный момент ни одна из ведущих стран в блокчейн-сфере не решилась на внедрение технологии распределенного реестра в область регистрации интеллектуальных прав и о глобальном регистре, который бы содержал подобные данные, пока речи не идет.