

Смарт-технологии безопасной трансформации бизнес-процессов организации

Романчук Анна Тадеушевна, Кириченко Егор Русланович

*Гродненский государственный университет им. Янки Купалы,
факультет математики и информатики,
кафедра системного программирования и компьютерной безопасности
студенты 3 курса специальности «Компьютерная безопасность»*

Научный руководитель Кадан Александр Михайлович, к.т.н., доцент

В работе проведено исследование платформ Ethereum и Hyperledger Fabric с точки зрения их возможного применения для автоматизации задач управления корпоративными ресурсами организации. Основное внимание уделено различным аспектам использования технологий разработки смарт-контрактов на основе концепции блокчейн. Обоснован выбор наиболее подходящей платформы (с учетом специфики организации, требований реализации бизнес-процессов, нормативно-правовой базы), позволяющей реализовать отдельные бизнес-процессы учебного заведения в виде смарт-контрактов. В качестве типового бизнес-процесса учебного заведения, допускающего реализацию с использованием смарт-контрактов на базе платформы Hyperledger Fabric, рассмотрен бизнес-процесс «Проведение текущей аттестации», входящий в состав стандарта СТУ 20 «Мониторинг и измерения» системы менеджмента ГрГУ им. Янки Купалы.

Ключевые слова: БИЗНЕС-ПРОЦЕССЫ, СМАРТ-ТЕХНОЛОГИИ, СМАРТ-КОНТРАКТЫ, БЛОКЧЕЙН, ETHEREUM, HYPERLEDGER FABRIC.

В настоящее время технологии автоматизации и цифровизации выходят на передовые позиции в жизни общества. Об этом свидетельствует, в частности, появление декрета № 8 «О развитии цифровой экономики» [1], подписанного Президентом Республики Беларусь. Белорусскому обществу предоставлены беспрецедентные условия для развития ИТ-отрасли, а Республике Беларусь даны серьезные конкурентные преимущества в создании цифровой экономики XXI века. Во всяком случае, среди молодого поколения о блокчейне и криптовалюте знает каждый. С появлением технологий блокчейн во многом упростился процесс совершения деловых сделок, и данная технология привела к понятию как смарт-контракт. Отрадно отметить, что Республика Беларусь является первой страной мира, законодательно закрепившей использование смарт-контрактов.

Понятие смарт-контракта

Смарт-контракт – это перечень обязательств, описанных в цифровой форме, и протоколы для выполнения этих обязательств сторонами. Основное преимущество смарт-контрактов в том, что использование аппаратного и программного обеспечения может значительно упростить и сделать более надежным заключение и контроль многих видов договорных отношений (например, в области залогов, разграничения прав собственности, кредитных отношений и т.д.). Если говорить простым языком, смарт-контракт – это набор правил и последовательность действий для исполнения.

Современные смарт-контракты обладают следующими характеристиками [2]:

- Смарт-контракты состоят из условий «если..., то...», в результате исполнения которых происходит запись информации в распределенный реестр, приводящей к изменению его состояния.
- Правила выполнения смарт-контрактов не могут быть изменены после согласования со всеми участниками.
- Смарт-контракты создаются с применением языков программирования, вследствие чего минимизируются возможности разночтений, при этом спектр возможных правил контракта ограничен той логикой, которая поддается жесткой алгоритмизации на уровне программного кода;
- Среда запуска и поддержки исполнения смарт-контрактов предоставляет надежный механизм верификации, обеспечивающий прозрачность с точки зрения подтверждения корректности и подлинности учета операций, и при этом сводит к минимуму раскрытие данных верификатору и прочим третьим лицам.

Преимущества смарт-контрактов

Среди преимуществ использования смарт-контрактов обычно выделяют [3]:

- Автономность. Используя смарт-контракты, отсутствует необходимость пользоваться для проведения транзакций услугами брокера или юриста. В этом же случае исключаются воздействия третьей стороны, ведь исполнение обязательств происходит в автоматическом режиме, а не несколькими участниками, которые могут допустить ошибку.
- Доверие. Все созданные документы находятся в зашифрованном состоянии в едином грощбухе. Такой способ хранения исключает потерю бумаг или нарушение их достоверности. Так же, как и изменение общедоступного адреса смарт-контракта.
- Резервное копирование. Система исключает потерю счёта или прописанной функции в контракте, ведь блокчейн многократно дублируется.
- Безопасность. В процессе использования смарт-контрактов задействуются криптографические инструменты и шифрование интернет-страниц, что обеспечивает документам высокую защиту. И чтобы взломать код приложений и увести деньги, потребуются невероятные способности и изобретательность.
- Скорость. Люди тратят на сбор и обработку документов многие часы времени. В то время как единожды запрограммированное приложение проделывает всю работу само.
- Экономия денег. Такие контракты позволяют избежать посредников в виде банков и официальных лиц, благодаря чему можно сэкономить на их услугах.
- Точность. Умные контракты, помимо достижения быстроты и дешевизны сделки, позволяют при этом избежать неточностей при введении данных, которые иногда допускаются при заполнении форм вручную.

Недостатки смарт-контрактов

Также смарт-контрактам присущи недостатки [4], которые, важно отметить, не являются критичными и не умаляют общие достоинства технологии:

- Правовой статус. Для работы умных контрактов используется криптовалюта, а ее пока не принимают в качестве официального финансового инструмента во всех странах.
- Ошибки. Для составления умного контракта нужно прописывать всевозможные условия и варианты развития сделок, чем сложнее процесс, тем труднее создать смарт-контракт.
- Неосведомленность. Те, кто знает хоть что-то о смарт-контрактах, слабо понимают, как они работают, а основная масса людей о них даже и не слышала.
- Безопасность использования. Включает комплекс проблем - от возможности логических ошибок при проектировании и ошибок при реализации кода, до проблем безопасности использования смарт-контрактов, допускающих сговор участников.

Популярные блокчейн-платформы

Сравнение платформ Ethereum и Hyperledger Fabric

Для проведения сравнительного анализа были выбраны 2 платформы:

- Ethereum как проверенная временем;
- Hyperledger Fabric как частный блокчейн, что весьма хорошо подходит для университета.

В ходе опыта, а также в ходе изучения источников [5] получил следующие данные:

- Использование: платформа Ethereum популярна у обобщенных приложений и в основном используется для бизнеса в потребительских операциях, платформа Hyperledger, предпочитаемая для бизнеса и деловых операций, главным образом используемая на предприятиях.
- Конфиденциальность: у Ethereum она прозрачная, в свою очередь у Hyperledger очень частная, поэтому транзакции конфиденциальны.
- Способ пирингового участия: платформа Ethereum может быть и частной, и общественной, поэтому является сетью без получения разрешения на допуск, Hyperledger Fabric поскольку является частной сетью, требуется разрешение на допуск в контент сети.
- Консенсусный механизм: в Ethereum алгоритм «Доказательство доли» как консенсус достигается через майнинг, в Hyperledger Fabric опирается на подключаемый консенсусный алгоритм при отсутствии майнинга.
- Программный язык: смарт-контракты Ethereum пишутся программным языком Solidity, Hyperledger Fabric опирается на программный язык Google – Golang, а также JavaScript, Java.
- Криптовалюта: Ethereum питается родной криптовалютой Ether, Hyperledger Fabric не имеет встроенной родной криптовалюты.
- Время развертывания узла: Ethereum занимает ~20 минут, Hyperledger Fabric ~1

час.

- Стоимость транзакции: Ethereum – \$0.094, Hyperledger Fabric – бесплатна.

Обе платформы предоставляют достаточный функционал для реализации системы на основе смарт-контрактов для ГрГУ им.Янки Купалы.

Что касается доступности предоставляемого платформой блокчейна, то Ethereum сейчас предоставляет возможность создания не только публичной сети, но и приватной. Однако в таком случае предполагается размещение ее в облаке, местоположение серверов которого обычно неизвестно, что противоречит пункту 1.2 Указа Президента Республики Беларусь № 60 от 1 февраля 2010 г. «О мерах по совершенствованию использования национального сегмента сети Интернет» [6]:

1.2. государственные органы и организации обеспечивают создание, функционирование и систематическое обновление интернет-сайтов с использованием информационных сетей, систем и ресурсов национального сегмента сети Интернет**, размещенных на территории Республики Беларусь и зарегистрированных с учетом требований пункта 3 настоящего Указа.*

Hyperledger Fabric же, в свою очередь, позволяет развернуть действительно приватную сеть блокчейна. Также весьма удобно, что для данной блокчейн сети вам не нужно майнить (добывать с помощью выполнения вычислительных операций) криптовалюту.

Бизнес-процесс проведения текущей аттестации

Исследуем действующий в ГрГУ им. Янки Купалы бизнес-процесс «Проведение текущей аттестации». Далее рассмотрим этапы, формы проведения, участников и условия выбранного учебного бизнес-процесса.

Каждый семестр заканчивается проведением текущей аттестации студентов по каждой из изучаемых ими дисциплин в виде экзамена, зачета, дифференцированного зачета. Вид аттестации определяется учебным планом по специальности. Текущая аттестация является одним из ведущих компонентов в контроле качества университетского образования.

Допуск студента к текущей аттестации осуществляется по умолчанию: если в отношении студента не принято решение о недопуске его к текущей аттестации, и не оформляется документально. Недопуск студента к текущей аттестации принимается на заседании кафедры по представлению одного из преподавателей, ведущих данную дисциплину, и оформляется документально – путем внесения информации о недопуске в протокол заседания кафедры и оформления выписки из протокола, которая представляется в деканат вместе с зачетной или экзаменационной ведомостью после экзамена.

В случае, если студент, не допущенный кафедрой к текущей аттестации, в дальнейшем выполняет в полной мере требования учебной программы, успешно демонстрирует преподавателю результаты самостоятельной работы по учебному материалу пропущенных занятий, преподаватель в форме докладной записки просит декана допустить данного студента к текущей аттестации. Данная докладная записка действительна только при наличии визы заведующего кафедрой. Студенту выписывается ведомость текущей аттестации вне экзаменационной группы, в которой назначается дата проведения пересдачи в соответствии с графиком пересдач.

Студент, сдавший все зачеты и защитивший курсовые работы (проекты), предусмотренные учебным планом специальности для текущего семестра, сдавший дифференцированный зачет по практикам, которые проводились в период после предыдущей экзаменационной сессии, допускается к экзаменационной сессии. Допуск осуществляется деканом в письменной форме с указанием допуска путем внесения соответствующей записи в зачетную книжку студента. Запись может осуществляться с использованием специального штампа. Студенты, не сдавшие зачеты, не защитившие курсовые работы (проекты), не сдавшие зачеты по практикам, которые проводились в период после предыдущей экзаменационной сессии, не допускаются к экзаменационной сессии. Недопуск осуществляется путем записи «не допущен» в экзаменационной ведомости, сопровождаемой подписью декана или уполномоченного заместителя декана. Преподаватель не имеет права принимать экзамен у студента, не допущенного к экзаменационной сессии.

Формами проведения текущей аттестации являются:

- экзамен;
- зачет;
- дифференцированный зачет.

Результаты текущей аттестации оцениваются:

- для зачета – отметками «зачтено», «не зачтено». Положительной является отметка «зачтено»
- отметками в баллах по 10-балльной шкале. Положительными являются отметки не ниже 4 баллов.

Процедура проведения текущей аттестации представлена в стандарте А 20-006(приложение 1).

Программа зачета или экзамена реализуется в форме перечня вопросов к зачету или экзамену и утверждается на заседании кафедры не позднее первого месяца семестра, в котором осуществляются мероприятия текущей аттестации.

Исходя из проведенного анализа бизнес-процесса «Проведение итоговой аттестации» можно спроектировать следующие основные сущности и перечислимые типы:

1. Сущность «Бизнес-процесс»

- *Поля:*
 - Идентификатор
 - Название
 - Состояние
 - Дата начала
 - Перечень этапов
 - Текущий этап
- *Методы:*
 - Посмотреть бизнес-процесс

- Активировать бизнес-процесс
- 2. Сущность «Этап»
 - *Поля:*
 - Идентификатор
 - Название
 - Длительность
 - Исполнитель
 - Ответственный
 - Состояние
 - Дата начала
 - Дата окончания
 - Позитивный этап
 - Отрицательный этап
 - Входные данные
 - Выходные данные
 - Требуемые выходные данные
 - *Методы:*
 - Посмотреть этап
 - Отправить этап на подтверждение
 - Подтвердить этап
 - Отклонить этап
- 3. Сущность «Пользователь»
 - *Поля:*
 - Идентификатор
 - ФИО
 - Должность
 - Email
 - Приватный ключ
 - *Методы:*
 - Войти в систему
 - Выйти из системы
 - Посмотреть список доступных бизнес-процессов
- 4. Сущность «Данные»
 - *Поля:*
 - Идентификатор
 - Ссылка на файл
 - Дата последнего изменения
 - *Методы:*

- Посмотреть данные
- 5. Перечислимый тип «Состояние бизнес-процесса»
 - В ожидании
 - В процессе
 - Окончен
- 6. Перечислимый тип «Состояние этапа»
 - В ожидании
 - В процессе
 - В ожидании подтверждения,
 - Окончен
 - Отклонен

Заключение

В работе изучены аспекты технологий для разработки смарт-контрактов и платформ, использующих концепцию блокчейн. Приведено сравнение различных платформ и выбрана наиболее подходящая (с учетом специфики организации, требований организации бизнес-процессов, нормативно-правовой базы) платформа, позволяющая реализовать смарт-контракты. Изучен бизнес-процесс учебного заведения (на примере стандартов системы менеджера ГрГУ им. Я.Купалы. Стандарт СТУ 20.Мониторинг и измерения).

Литература

- 1.
2. Аналитический обзор по теме «смарт-контракты» [Электронный ресурс] // D-russia: экспертный центр электронного государства. – Режим доступа: http://d-russia.ru/wp-content/uploads/2018/10/SmartKontrakt_18-10.pdf. – Дата доступа: 10.10.2019.
3. Преимущества и недостатки смарт-контрактов [Электронный ресурс] // Polygant: информационный ресурс. – Режим доступа: <https://polygant.net/ru/blog/preimushhestva-i-nedostatki-smart-kontraktov/>. – Дата доступа: 25.10.2019.
4. Mamaeva N.V., Burkov A.V. Comparative analysis of the cryptocurrency market // Scientific enquiry in the contemporary world: theoretical basics and innovative approach, 2017. № 11. С. 86–88.
5. Hyperledger против Corda R3 и против Ethereum: Полное руководство [Электронный ресурс] // 101 Blockchains: блог о блокчейн. – Режим доступа: <https://101blockchains.com/ru/hyperledger-против-corda-r3-и-против-ethereum/>. – Дата доступа: 10.11.2019.
6. О мерах по совершенствованию использования национального сегмента сети Интернет [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: <http://pravo.by/document/?guid=3871&p0=P31000060>. – Дата доступа: 10.11.2019.

