Список использованных источников:

1.Physics Simulation [Электронный ресурс]. — Режим доступа : https://docs.unrealengine.com/en-us/Engine/Physics – Дата доступа: 14.03.2019г.

2. Apex [Электронный ресурс]. — Режим доступа : https://docs.unrealengine.com/en-us/Engine/Physics/Apex – Дата доступа: 14.03.2019г.

3. Н.Г.Бураго – Институт проблем механики им. А.Ю. Ишлинского РАН, Москва, 119526, Россия – Вычислительная механика сплошных сред. – 2008. – Т. 4, № 4. – С.5-20

ПРОГРАММА ЛОЯЛЬНОСТИ ДЛЯ КЛИЕНТОВ СПОРТИВНЫХ КЛУБОВ НА БАЗЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Евсаев П.В., Беликова Т.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фролов И.И. – к.т.н.,доцент

Исследования рынка клиентской лояльности показывают, что эффективность программ лояльности падает. Это связывают с неудобствами, связанными с хранением большого количества дисконтных карт/установкой большого количества мобильных приложений. Разработка системы, являющейся единой точкой управления программами лояльности для организаций и их клиентов видится своевременным и актуальным.

По прогнозам экспертов, объем рынка клиентской лояльности к 2020 году подойдет к отметке в 48 миллиардов долларов США. Несмотря на внушительный оборот, исследования показывают, что эффективность программ лояльности снижается. Это связывают с тем, что каждая программа лояльности требует использования карты либо мобильного приложения, что снижает привлекательность каждой следующей программы для потребителя. Создание единой системы для запуска программ лояльности снизит поставщикам товаров и услуг издержки на обслуживание собственной CRM системы и позволит иметь единый канал связи с аудиторией потребителей всех организаций-участников сети. С точки зрения пользователя, наличие подобной системы позволит иметь единую точку управления всеми бонусными баллами и акционными предложениями.

При выборе инструментов для разработки проекта, выбор был сделан в пользу стека Hyperledger. Стек Hyperledger позволяет создавать блокчейны с ограничением прав доступа для участников сети, определять собственную модель взаимодействия между участниками сети через строго определенный набор транзакций. Возможность обновления чейнкода дает возможность проводить разработку в итерационном формате, постепенно расширяя функциональности системы. Использование привилегированного блокчейна и обязательный процесс идентификации пользователя снижает риск атаки на сеть и снимает необходимость взимать плату за проведение транзакции.

В соответствии с бизнес-целями, в сети необходимо и достаточно наличие двух типов участников: организация и потребитель. Организации должны иметь право управлять программами лояльности, участники - иметь возможность вступать/выходить из программ лояльности. Оба типа участников должны иметь право осуществлять переводы токенов программ лояльности другим участникам сети.

Процесс запуска программы лояльности может выглядеть следующим образом: при создании организацией программы лояльности, у нее создается кошелек, на который поступает весь объем эмитированных в рамках программы лояльности токенов. Далее, организация высылает клиентам приглашения. Когда потребитель принимает приглашение, у него создается привязанный к этой программе лояльности кошелек, на который/с которого ему могут поступать токены. Токены являются уникальными для программы лояльности и могут быть реализованы либо переданы другому клиенту-участнику программы.

Для доступа к управлению своими ресурсами участникам сети необходимо пройти процесс идентификации. При регистрации, новому участнику сети ему выдается персональный сертификат, выпущенный доверенным для проекта центром выдачи сертификатов. Соответствующая сертификату пара ключей сохраняется локально и будет использована при следующем входе в систему.

В качестве направлений для развития создаваемой системы можно рассмотреть возможность запуска совместных программ лояльности для нескольких организаций, реализовать интеграцию с действующими CRM системами. Наличие гибкого, функционирующего по описанному алгоритму проекта поможет решить существующие проблемы на рынке клиентской лояльности, а использование распределенного реестра для хранения данных об операциях дает хороший фундамент для развития проекта с точки зрения финансового аудита.

Список использованных источников:

1. Mastering Bitcoin. Programming the open blockchain / Andreas M. Antonopoulos // O'Reilly Media 2017 – 416 p.
2. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition / Imran Bashir // Packt Publishing 2018 – 656 p.
3. Blockchain: A Practical Guide to Developing Business, Law and Technology Solutions интернета вещей / Joseph J. Bambara // McGraw-Hill Education, 2018 – 320 p.

МИКРОСЕРВИС ДЛЯ УДАЛЁННОГО УПРАВЛЕНИЯ ЧПУ СТАНКОМ

Жук Д.А., Басов Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Селезнев И.Л. – к.т.н.,доцент

Удаленный доступ позволяет пользователю, находящемуся на одном компьютере, взаимодействовать с удаленной машиной и выполнять на ней интерактивный сеанс работы. Удаленный доступ позволяет создать впечатление, что терминал пользователя или его рабочая станция присоединены напрямую к удаленной машине, посылая каждый символ, нажатый на клавиатуре пользователя на удаленную машину и отображая каждый символ, возвращенный с удаленной машины, на экране терминала пользователя.

Удаленный доступ — функция, которая даёт пользователю возможность подключаться к компьютеру при помощи другого устройства через интернет. Пользователь работает с файлами и программами точно так же, как если бы он находился возле этого компьютера. Эта функция пригодится тем компаниям, в которых большинство сотрудников находится за пределами офиса, аутсорсинге или в командировках. Им не нужно будет скачивать все необходимые для работы данные на внешний носитель или отправлять их по почте — достаточно связаться с офисным компьютером. Удаленный доступ используется системным администратором для управления работой системы и устранения ошибок, а также руководителями, желающими проконтролировать процесс выполнения работы своими сотрудниками. Применяется он и для дистанционной формы обучения в образовательных учреждениях.

Есть два способа организации удаленного доступа

- виртуальный рабочий стол - DaaS (desktop as a service);
- установка специализированного ПО.

Первый способ - desktop as a service. Этот способ предоставляет пользователю доступ к готовому удаленному рабочему столу. В него может входить весь необходимый пользователю функционал, который при необходимости возможно расширить. Работать можно с любого устройства - рабочий стол везде будет один и тот же. Все действия выполняются не на ПК пользователя, а на сервере поставщика услуг, нагрузка на клиентскую машину минимальна, поэтому и требованиях характеристикам не существенны. Для работы данные пользователя ии программы размещаются в сети интернет, а не на локальном сервере. Воспользоваться ими можно из любого удобного места, где есть интернет соединение. Примерами таких программ являются Vmware ESXi, Microsoft Hyper-V, Citrix XenServer.

Во втором способе для создания удаленного подключения используется специальное программное обеспечение. Важной частью является возможность постоянного доступа в интернет, сервера, рабочих машин, обладающих необходимыми параметрами. Через интернет два компьютера связываются удалённым подключением. Если рабочий ПК находится в локальной сети, то получить доступ к нему извне возможно только с помощью специальных программ. Такое программное обеспечение делает возможным подключение к другому компьютеру из любого удобного места. Программ дают возможность работать так, как если бы пользователь работал непосредственно за компьютером. Возможно видеть рабочий стол и выполнять все действия на удаленном устройстве, изменять настройки ПО, обмениваться файлами, шифровать передаваемые данные, подключать веб-камеры, удаленные проекторы и прочие сетевые устройства. Примерами такого ПО являются Team Viewer, RAdmin, Ammyy Admin.

Минусом этого способа является необходимость в настройке сетевого оборудования. Помимо этого, необходимо понимать, что уменьшается безопасность сети, появляется шанс проникновения сторонних лиц в локальную сеть.

Большинство ЧПУ станков, как правило оснащено ПК с устаревшими комплектующими, малопроизводительными, способными лишь запускать программу для управления станком. Иногда возникают ситуации, в которых нужно изменить программу, и для этого необходим ещё один полноценный рабочий компьютер.