Использование комплекса основанных на симуляторах решений для обучения основам блокчейн технологий

Общее описание

Данная разработка позволяет более эффективно объяснить особенности работы и применения технологий, основанных на блокчейне. Разработка основана на результатах преподавания курса «Технология Блокчейн в цифровой логистике и управлении цепями поставок», значительно переработанных и адаптированных для курса “Digital Supply Chain Management” («Управление цифровыми цепями поставок»).

В оригинальной реализации разработка применяется на англоязычном курсе, но это не является ограничением или особым требованием. При проведении семинарского занятия используются элементы формирующего оценивания для учета активности. Формой контроля освоения темы является выполнение домашнего задания. Для самопроверки студентов используется специально подготовленный интерактивный квиз.

Студенты часто имеют достаточно поверхностное представление о принципах работы блокчейна. При этом сама технология относительно сложная, базируется на использовании результатов из нескольких областей науки. Поэтому для объяснения работы в рамках курса применяется комплекс из нескольких цифровых решений, каждое из которых позволяет разобрать и закрепить отдельные важные составляющие работы с блокчейн системами и достичь понимания студентами преимуществ и недостатков их использования.

В случае с блокчейн системами есть три основных компонента, взаимодействие которых с одной стороны, формирует их сложность и неочевидность, с другой — уникальность:

-криптография;

-программирование;

-сетевое взаимодействие.

Следует отдельно подчеркнуть факт того, что эти направления не изучаются на многих учебных программах, что усложняет восприятие материала. При этом с каждым годом растет вероятность того, что студенты столкнутся с данной технологией в академической или профессиональной деятельности. Системы, связанные с криптографией, к которым в том числе относится блокчейн, не относятся к интуитивно понятным, поэтому симуляция работы блокчейна в интерактивном формате игры на семинаре эффективна.

Предложенное образовательно-методическое решение состоит из игры-симулятора для проведения семинарского занятия, домашнего задания с методическим рекомендациями по его выполнению, а также интерактивного квиза для закрепления пройденного материала. Опциональное решение: использование тестовой сети реально существующей блокчейн системы для учета активности студентов по ходу реализации курса.

Для данного примера используются несколько цифровых инструментов, использующих компьютерное моделирование: бесплатная версия системы имитационного моделирования Anylogic для выполнения технической части домашней работы, а также интерактивный материал, выполненный на языке программирования R и размещенный на арендованном автором разработки сервере.

Требуемые цифровые инструменты

Пререквизитом для семинарского занятия является лекция, на которой рассмотрены теоретические основы технологии блокчейн.

Для проведения занятия в данном формате требуются:

-документ с общим доступом (google docs, Яндекс.Документы, miro, другой аналогичный сервис). Данный документ используется в качестве открытого реестра для генерации и записи транзакций;

-генератор алгоритма шифрования SHA-256: онлайн интерфейс или собственное решение, например, на python или R:

Собственная разработка: http://45.132.19.138:3838/sha256/

Стороннее решение (резерв): https://crypt-online.ru/crypts/sha256/

Для выполнения домашней работы:

-установленная бесплатная версия системы моделирования Anylogic (версии 6+) и подготовленный документ с методическими указаниями выполнения задания;

-работа с интерактивным квизом (http://45.132.19.138:3838/DSCM2/#section-blockchain-andcryptography-topic-2);

Опционально: для возможности дальнейшего учета активности в блокчейне:

-установленный криптокошелек (предпочтительно MetaMask) с настроенной тестовой (транзакции внутри сети полностью бесплатны) сетью Goerli Ethereum.

Подготовка к игре в начале семинарского занятия [10–15 минут]

Рассмотрим более подробно структуру занятия. Для его проведения крайне желательно использовать компьютерный класс.

В начале занятия проводится небольшой опрос, позволяющий определить, насколько усвоен лекционный материал. Корректные ответы во время дискуссии оцениваются баллами активности (1 ответ — 1 балл). Вновь объясняется, что для работы системы, основанной на блокчейне, требуется определить:

-минимальный состав блока;

-количество участников и способ обмена информацией.

Каждый блок состоит из трех частей: хеш предыдущего блока, полезная информация, «подпись» участника сети и хеш блока. Хеш (англ. “hash”) — это результат шифрования информации с использованием криптографического алгоритма, в данном случае, SHA-256.

Отдельно подчеркивается, что блокчейн — это концепция, которая может быть реализована многими способами и один из них: работа студентов на занятии эмулирует процесс добавления блоков. В качестве реестра данных используется подготовленный документ в свободном доступе. В реальном блокчейне (в классической реализации) используется награда за найденный (корректно подписанный) блок, на занятии в качестве «награды за найденный блок» используются

дополнительные баллы активности (1 блок — 2 балла). Набранные баллы активности добавляются в общее количество баллов активности, которые используются в расчете оценки за предмет, не являются результирующим элементом оценивания (ПУД приложен к заявке). В авторской реализации курса для учета баллов используются напечатанные на 3D принтере фигурки роботов, что согласуется с общей цифровой направленностью курса.

Симуляция работы блокчейна подразумевает участие нескольких узлов сети (в их роли выступают студенты). Минимальное количество студентов для успешного проведения занятия: 5.

Процесс игры по имитации работы блокчейна на семинаре [40–50 минут]

Игра начинается с генерации «генезис блока» или первого блока блокчейна. В качестве примера можно использовать фразу из «генезис блока» сети биткоин: “Chancellor on the brink of a second bailout”. Фраза записывается первой строкой в открытый онлайн-документ, доступ к которому есть у студентов. Состояние документа выводится на проектор.

Задача участников сети найти, какой символ можно добавить к подписи блока, чтобы результирующий хеш начинался с заданной комбинации символов, например, «00». В качестве шаблона подписи студенты используют свою фамилию (или фамилию и инициалы, если в группе есть однофамильцы) и числовой индекс.

Результат для первого блока можно показать на примере «подписи» на базе фамилии преподавателя:

“chancellor on the brink of second bailout

Surname312”

Хеш: **00**f29a0e0bb5d926c119a58420d8d58dcb540bc01433e6a947dddf6baf70af75

То есть на подбор для подписи Surname потребовалось бы 313 попыток поиска нужного значения индекса (если начинать подбор с нуля) для генерации нужного хеша. В среднем вероятность составляет 1/16*1/16 = 1/256. Для записи хеша обычно используется шестнадцатеричная система исчисления, поэтому каждый дополнительный символ целевой строки в среднем увеличивает сложность в 16 раз.

Если в аудитории 20 студентов, то есть вероятность, что кто-то найдет нужную комбинацию цифр для своей фамилии с 5–10 попытки. Поиск выполняется фактически «перебором», добавляются случайные цифры к фамилии.

Важно: каждый студент может проверить, что данная комбинация действительно генерирует правильный хеш. Например:

Пример 1:

“chancellor on the brink of second bailout

Ivanov14”

00a406e51575e6dcd3226530e18f8d8f3af01cdac065d54aecec6519537caceb

Пример 2:

“chancellor on the brink of second bailout

Petrov599”

00a3f6879345bc1ac1e59829b1739a2bdc41837fab341015b546f88862a8085c

Первый нашедший корректное значение студент (при последовательном переборе в примерах выше это будет студент Ivanov: корректно найденное значение с 15-й попытки) получает 2 балла активности, по аналогии с реальными блокчейн системами, где за найденный блок выдается вознаграждение в виде криптовалюты.

В данном случае сохраняется достаточно высокий уровень случайности, поэтому используется только формирующая часть оценивания. Случайность награды — это свойство, критически важное для надежной работы блокчейн систем, поэтому для корректной симуляции оно обязательно должно быть реализовано.

На следующем этапе, начиная с блока номер два, формируется блокчейн, то есть блоки связываются между собой.

Содержание второго блока:

“00a406e51575e6dcd3226530e18f8d8f3af01cdac065d54aecec6519537caceb

Ivanov: 2 points”

Первая строка: хеш предыдущего блока. Вторая строка — это «полезная информация», в данном случае запись о заработанных студентом баллах активности.

Таким образом можно провести несколько раундов добавления блоков в блокчейн. Начиная с третьего или четвертого блока можно повысить сложность поиска, добавив еще один «0» к целевой строке. (было «00», стало «000»). Всего можно провести 5–7 раундов добавления блоков в зависимости от скорости нахождения блоков студентами.

Вопросы для обсуждения на занятии после проведения игры [10–15 минут]:

-по содержанию блока N невозможно определить, кто именно найдет значение хеша для следующего блока N+1, почему это критически важно для надёжной работы системы;

-время нахождения блока зависит от целевого значения хеша: “00” и “000” отличаются по сложности в среднем в 16 раз, “00” и “0000” — в 256 раз, зачем нужно динамическое управление сложностью целевого значения;

-можно повысить шансы отдельного студента на то, чтобы найти корректное значение хеша в несколько раз быстрее, если подбором для одной фамилии занимается, например, два студента: один проверяет только четные, а второй только нечетные значения;

-почему важна децентрализация системы и не должно быть отдельных участников с вычислительными мощностями, превышающими 50% всей мощности всей сети;

-почему перебор вручную (как это выполняется во время занятия) это очень неэффективный способ, намного лучше использовать компьютерные вычисления;

-в реальных системах для поиска нужного значения хеша используется не фамилия, а криптографический адрес, что позволяет сохранить анонимность участников сети.

Первые четыре вопроса проверяют, насколько хорошо студенты усвоили нас семинарском занятии логику работы блокчейна как технологии. Предпоследний пункт вопросов для обсуждения (про перебор вручную) — это взаимосвязь с технической частью домашнего задания, которое выдается в

конце занятия. Последний пункт связан с тем, как можно интегрировать блокчейн технологии в реализацию курса. Каждый корректный ответ в процессе дискуссии оценивается одним или двумя баллами активности, в зависимости от полноты и качества ответа.

Следующий этап: обсуждение использования блокчейн систем в реальной жизни. В частности, можно ли их использовать для учета активности на занятиях.

Учет активности в блокчейне [5–10 минут на занятии и/или отдельно после занятия представить информацию в письме или сообщении]

По причине того, что кейс использования блокчейна для учета активности возможен, можно предложить (в зависимости от направления изучаемого курса) дублировать статистику по активности студентов на курсе в бесплатной тестовой блокчейн сети, с повышением «веса» данной активности, например, на 10%. Больший «вес» подтвержденной в блокчейне активности обусловлен тем, что эти данные невозможно подделать — они защищены криптографически.

Студентам направляется инструкция по созданию адреса в блокчейн, данные по активности подтверждаются отправкой с адреса преподавателя транзакций с бесплатными токенами. В авторской реализации курса использовалась работа с токенами тестовой сети Goerli Ethereum. При этом сохраняется анонимность данных (т.к. соответствие адресов криптокошельков и студентов есть только у преподавателя). При работе с тестовой блокчейн сетью все транзакции полностью бесплатны, поэтому работа с Goerli Ethereum ничем не отличается от работы с любым свободно распространяемым программным обеспечением.

Домашняя работа

Домашняя работы состоит из двух частей: технической (50%) и нетехнической (50%). В курсе две домашние работы с одинаковым весом, более подробная информация представлена в ПУД.

Для выполнения технической части («компьютерная симуляция») используется компьютерная версия алгоритма работы, который рассматривался на занятии, но с большим фокусом на то, почему однажды добавленные данные в корректно реализованных блокчейн системах почти невозможно изменить.

Для выполнения нетехнической части студентам предлагается выбрать две компании из одной индустрии, которые внедрили различные решения, основанные на использовании блокчейна в свою работу, и проанализировать специфику и реализацию решения. Критерии оценки задания могут отличаться в зависимости от курса и образовательной программы. Задание выполняется в командах из 2–3 человек.

Дополнительный контроль

Для закрепления материала студентам также предлагается пройти интерактивный квиз, реализованный при помощи пакета для создания обучающих материалов learnr (https://rstudio.github.io/learnr/) на языке программирования R, с возможностью запуска и анализа результатов работы программного кода прямо при выполнении квиза.

Структура решения

Таблица 1. Сопоставление компонентов методики

	Взаимодействие участников сети	Работа с криптографическими функциями в явном виде	Скорость работы	Анализ применения реальных систем	Основной фокус
Игра в аудитории	да	да	низкая	опосредованный	теория
Компьютерная симуляция	нет	да	высокая	опосредованный	теория
Домашнее задание (нетехническая часть)	нет	нет	неприменимо	явный	практика
Учет активности в тестовой сети блокчейна	да	нет	неприменимо	опосредованный	практика
Интерактивный квиз	нет	да	выскокая	опосредованный	практика и теория

Вывод

Таким образом, данная разработка позволяет использовать разнообразные методы симуляции для анализа сложной компьютерной системы — блокчейна. Применяемые методы позволяют более детально рассмотреть отдельные блоки компонентов системы. Каждый из рассмотренных этапов проведения занятия является более сложным в техническом плане, чем предыдущий, но предложенная структура позволяет выполнить последовательный и плавный переход от работы с активностью на семинаре к взаимодействию с тестовой сетью реальной блокчейн системы, с фокусом на самой контринтуитивной и специфической частью технологии: криптографии.

Системы, основанные на блокчейне обрели достаточно высокую популярность за последние 6 лет. Во многом они все еще остаются нишевыми из-за их внутреннего устройства, но находят применение в ситуациях, когда их преимущества значительно перевешивают недостатки. Умение определять их возможную область применения и взаимосвязь с другими современными цифровыми технологиями — важный навык для студентов.

Понимание базовой структуры работы блокчейн систем важно для студентов, обучающихся на образовательных программах, посвященных логистике и управлении цепями поставок, управлению бизнесом, маркетингу, финансовому менеджменту, юриспруденции, праву, бизнес-информатике.

Описание домашней работы:

Homework #1

Information about homework. Deadline: **06.11.2023**. Team size: **three** students maximum.

Please send the files to maksim.rozhkov@hse.ru

The homework consists of two parts:

-technical part (40%)

-non-technical part (60%)

This homework covers two digital technologies: simulation (we've already used simulation/modeling in excel at seminars) in SC and blockchain. In the technical part you'll combine these technologies in one model. In non-technical part you'll need to assess the impact of blockchain implementation in a selected industry.

It's impossible to omit technical part because of the essence of the course which is directly linked to information technologies.

For the technical part you will need Anylogic software (free PLE version):

Official link (you can use fake name and email):

https://www.anylogic.ru/downloads/personal-learning-edition-download/

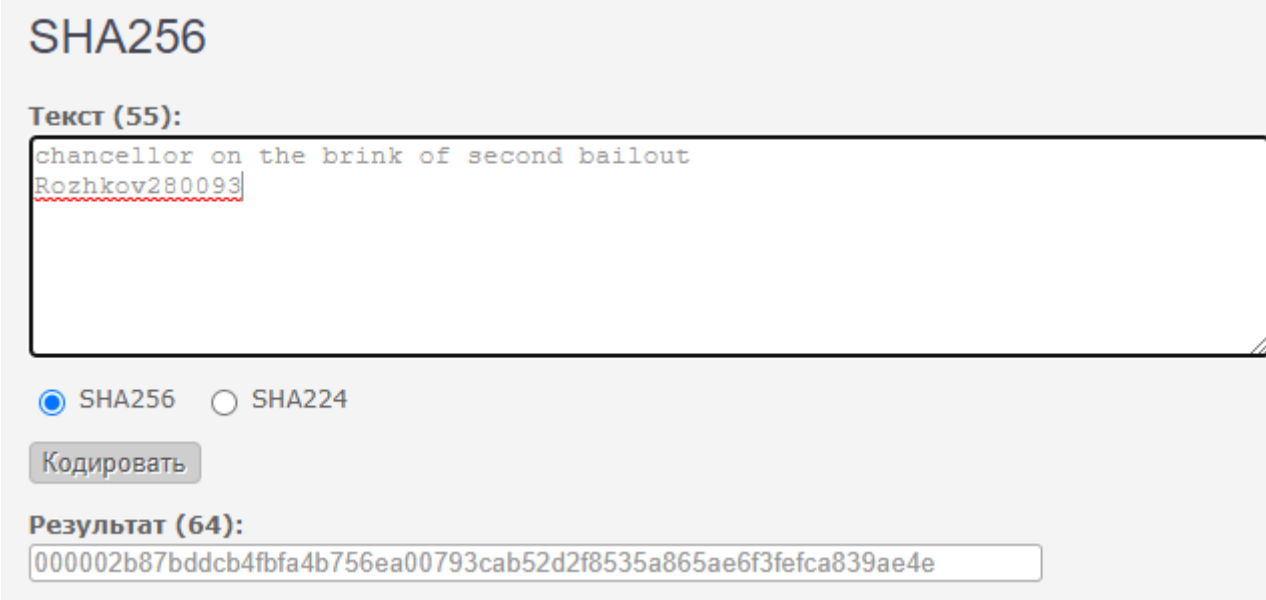
Non-official link:

https://disk.yandex.ru/d/xndLQf-1sXHoeA

Technical part (40%):

1. (25%) Build a simulation model following the manual "Developing blockchain model class". You can start from page #5 if you use model template. Please send the model and fulfill an additional task.
   Additional task: find correct nonceIndex for generating hash starting with required amount of zeros, using a text data of this format:
   "chancellor on the brink of second bailout\n" + "Rozhkov"
   (you insert your surname for the task and you can change the phrase if you want to)

   In case of my surname it will be nonceIndex=280094 for hash starting with "00000"
   (enumeration starts with 0)



Please find the nonceIndex indexes for “0”, “00”, “000”, “0000”, “00000”. You can use the surname of any team member for the task.

2. (15%) Build an extended version of a simulation model following the manual “Developing blockchain model_class_part2”. This model has some simplified blockchain with protection from hacking.
3. (10%) Build an extended version of a simulation model following the manual “Developing blockchain model_class_part3”. This model has an additional Proof-Of-Work blockchain protection and uses some more complex structure

Result: three *.alp files

Links:

Model template https://disk.yandex.ru/d/Vv_IiabAfxdZhg

Model development manual part 1 https://disk.yandex.ru/d/0G1gBRzp7qVDLA

Model development manual part 2 https://disk.yandex.ru/d/ChVJVwbr7ixU1g

Model development manual part 3 https://disk.yandex.ru/i/UkBSYPObbZ-Bhg

Non-technical part (60%):

1. There are a lot of blockchain services providers, like Hyperledger, Amazon, IBM. These companies have a lot of successful blockchain implementation cases. Please select an industry from a file and prepare a work about it.
   Please add team data in the course file: https://3dsmax.sol-domain.org/ Sheet: **HW1**
2. Work structure:

   Please compare and analyze at least **two** implementation cases for selected industry in your work:

   Theoretical part (from 3 pages):

   a. Selected industry features and supply chain specifics

b. Literature review (other relevant cases, scientific articles (>4) related to blockchain [journals, conferences])

Practical part (from 5 pages):

c. Company's SC strategy
d. Features of blockchain solution used
e. How the blockchain-based solution is integrated with other digital SC technologies
f. Logistic processes changes
g. Financial effect estimation
h. Supply chain performance change estimation
i. Limitations
j. Future development

File formatting: standard for HSE University. Please pay attention to **correct referencing**.

Formatting guide https://disk.yandex.ru/d/wvN-Urvyque25Q

Result: *.docx file

Additional information

Interactive tutorial with a small quiz and SHA256 hash generator (it's **not** calculated in grade):

http://45.132.19.138:3838/DSCM