**Лабораторный проект**

Цель: реализовать распределённый реестр произвольного назначения (т. е. с произвольным содержанием блоков/транзакций).

Детали.

1. Язык программирования и формат хранения блоков произвольный.
2. Численность группы исполнителей: не более 4-ёх человек.
3. Разрешается использовать готовые решения для криптографических алгоритмов.
4. Демонстрация на защите проекта должна сопровождаться запуском не менее 4-ёх узлов.
5. На защите проекта должен выступить каждый из исполнителей, рассказав о своём вкладе в разработку.

Задание 1.

Реализация одноранговой (peer-to-peer) сети для обмена сообщениями.

Каждый узел сети представляет собой запущенное приложение. Опционально (по желанию), можно использовать для каждого узла отдельную виртуальную машину.

Каждый узел сети знает адреса остальных узлов, может отправить запрос (текстовое сообщение) любому другому узлу (подобно клиенту) и принять запрос от другого узла (подобно серверу).

Для организации сети можно использовать сокеты (socket) непосредственно или более абстрактные объекты.

Задание 2.

Определить содержание и структуру транзакций и блоков. Разработать объекты для их хранения в программе.

Реализовать возможность передачи блоков и транзакций между участниками сети. В рамках учебной задачи достаточно установить соединения между каждой парой участников и распространять новые транзакции и блоки широковещательной рассылкой.

Реализовать blockchain в произвольном формате (например, БД) и механизм взаимодействия цепочки блоков на диске с программой. Примеры функций: добавить блок в цепочку, узнать текущий баланс, найти транзакцию по hash-значению.

Задание 3.

Реализовать пользовательский интерфейс (в простейшем случае — консоль) с возможностью создания транзакций пользователем и получения информации о балансе (и других параметров, при желании). В рамках учебной задачи достаточно создать по одному счёту для каждого участника и при запуске приложения сообщить открытые ключи (адреса) всех остальных.

Реализовать функцию создания транзакции. По указанной для перевода сумме необходимо найти непотраченные транзакции. В качестве выходов транзакции указать получателя и сдачу на счёт отправителя.

Задание 4.

Организовать хранение полученных транзакций и их проверку (корректность подписи, ссылку на существующие непотраченные транзакции)

Реализовать формирование новых блоков из полученных транзакций. В рамках учебной задачи достаточно зафиксировать количество транзакций для одного блока (например, 4 транзакции на блок). В качестве алгоритма консенсуса можно использовать Proof of Work, подбирая соответствующее поле блока до тех пор, пока hash блока не будет содержать указанное число нулей в старших битах (параметр сложности подобрать экспериментально из соображений отладки ПО).

Принимающий чужой блок участник должен проверить корректность PoW и транзакций, а затем добавить блок в свою цепочку.