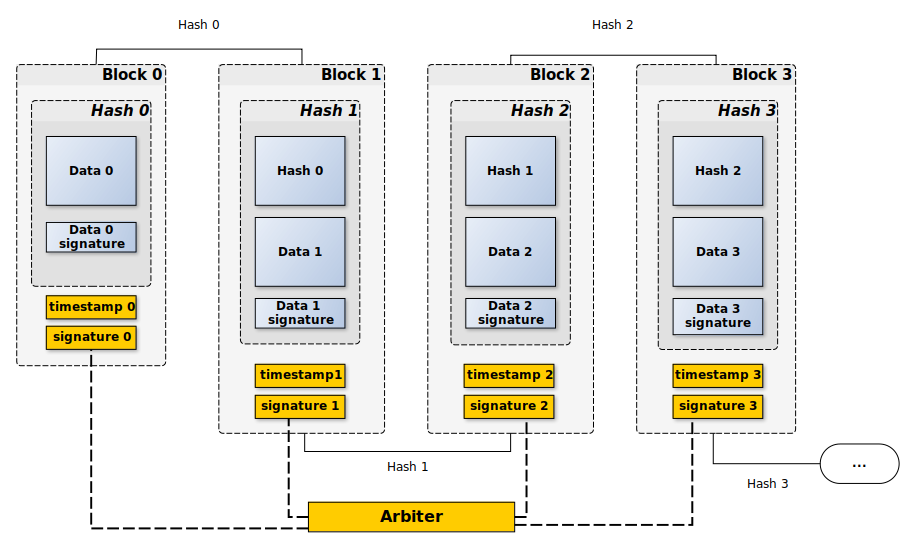
Практическое занятие 3.2.

Рассматривается публичный реестр, формируемый владельцем. Проблема доверию к держателю реестра. Распространенная практика — наличие третьей незаинтересованной стороны, арбитра, которому доверяют все участники (держатель реестра, пользователи реестра).

В этой схеме арбитру может быть недоступна сама информация в блоках, достаточно, что бы он «закрыл» блок, подписав значение хеш-функции от данных блока.

**

Получение подписи от арбитра:

1) формирование блока (вычисление и запись хеша предыдущего блока, запись данных, подписание данных и внесение подписи в блок);

2) вычисление хеша блока (от совокупности хеша предыдущего блока, данных и подписи данных);

3) передача хеша блока арбитру для подписи;

4) получение от арбитра метки времени и значения подписи, и внесение этих сведений в блок.

Рассмотренная выше схема может работать в условиях, когда заинтересованные стороны ведут копию реестра, присоединяя очередной блок по мере поступления в «мастер»-копию.

В рамках этой схемы заинтересованные стороны могут выступать в роли поставщика информации, размещаемой в блоках. Тогда уместно будет подписывать данные в блоке самим поставщиком, роль арбитра будет заключаться в подписи хеша блока.

**ЗАДАНИЕ (6 баллов):**

*Разработать программу, формирующую блок-чейн на базе криптостойкой хеш-функции.   
Требования: использование схемы с арбитром, закрывающим блок, возможность ввода и сохранения данных в блоках, просмотр информации в блоке, проверка достоверности информации в выбранном блоке, верификация всей цепочки, хранение информации либо с использованием СУБД, либо в каком-то ином виде на носителе с долговременным хранением данных.*

*В качестве арбитра необходимо использовать API, предоставляемое преподавателем.*

**Альтернативное задание (6 баллов):**

В созданном на прошлом занятие блок-чейне закрывайте блок подписью арбитра (API предоставлено преподавателем), реализуйте верификацию.