Практическое занятие 3.1.

**Управление системами децентрализованных реестров**

Доклад центробанка России о распределенных реестрах: https://cbr.ru/Content/Document/File/50678/Consultation\_Paper\_171229(2).pdf

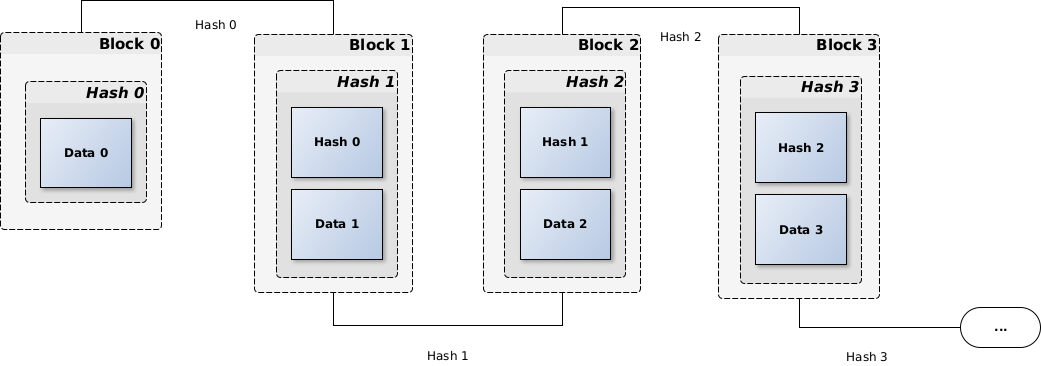
Компоненты управления:

1. протоколы программного обеспечения;
2. правила и нормы вне протоколов;
3. управление сообществом;

Цель использования децентрализованных реестров:

Надежность, доступность, верифицируемость

Вариант хранения верифицируемых данных — блок-чейн (block chain)

**Хеш-функция:**

Определим как отображение массива (произвольной длины) байт в массив байт ограниченной длины.

*H: M → h*

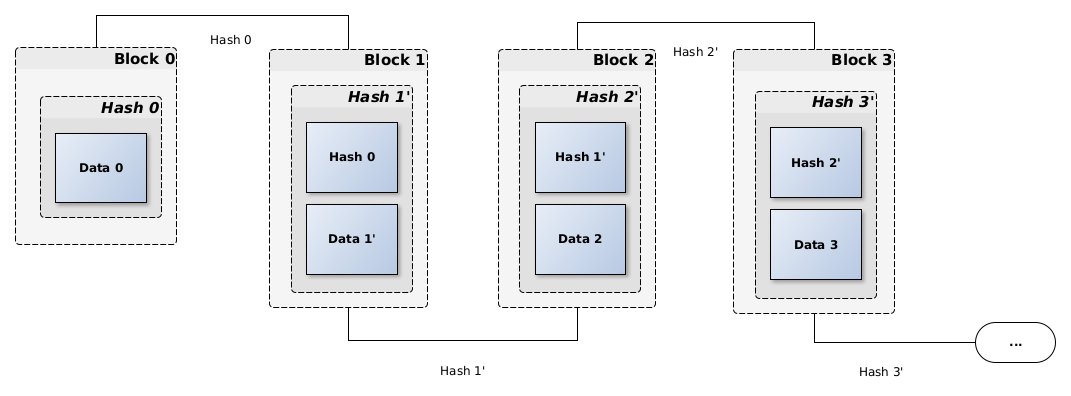
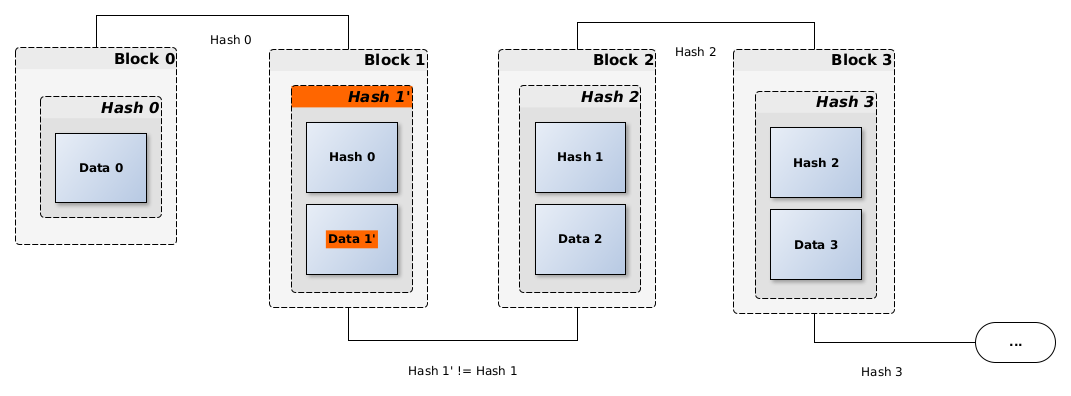
Коллизии хеш-функции:

Ǝ M ≠ N: H(M) = H(N)

Криптографическая стойкость хеш-функций:

* Для заданного значения *h* вычислительно сложно найти *M: H(M) = h*
* Для заданного *N* вычислительно сложно найти *M: H(M) =H(N)*
* Вычислительно сложно найти пару *M* и *N: H(M) =H(N)*

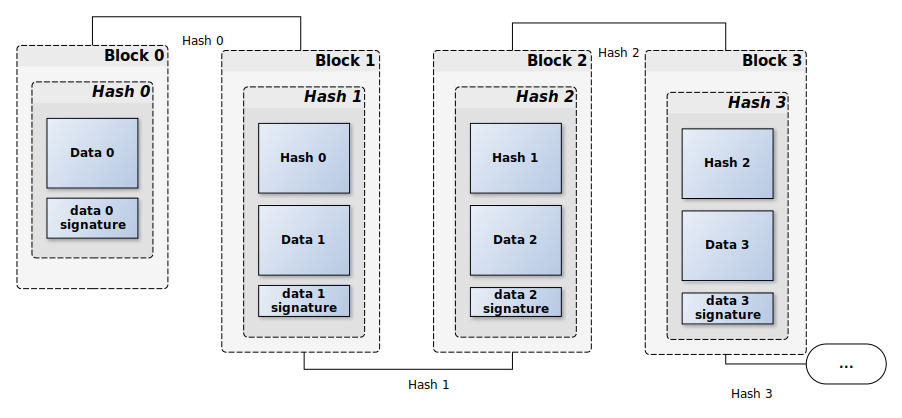
Остается проблема: владелец блок-чейна имеет возможность контроля целостности, и при этом может подменить данные, пересчитав и переписав хеши в последующих блоках.



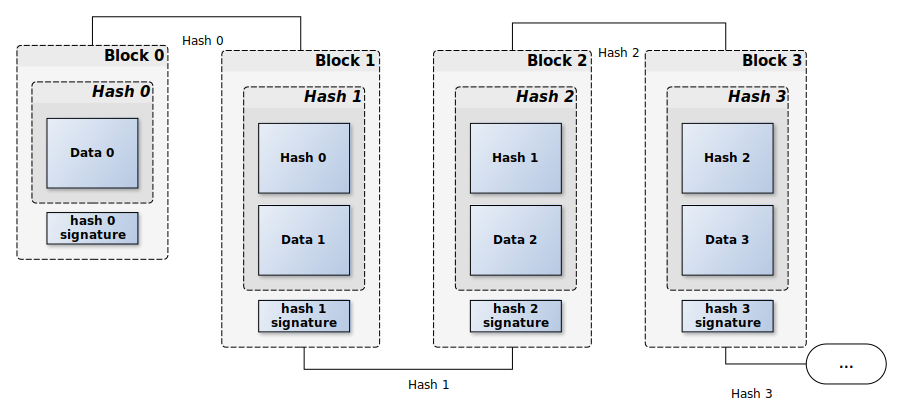
Следующая проблема: владелец блок-чейна не определит подмену, если пересчет хешей осуществит кто-то другой.

1) Массив данных подписывается электронной подписью владельца блок-чейна (фактически вычисляют значение *h* некоторой хеш-функции от массива данных *M*, затем подписывают это значение *h*

Значение подписи храниться вместе с данными

*Схема 1*

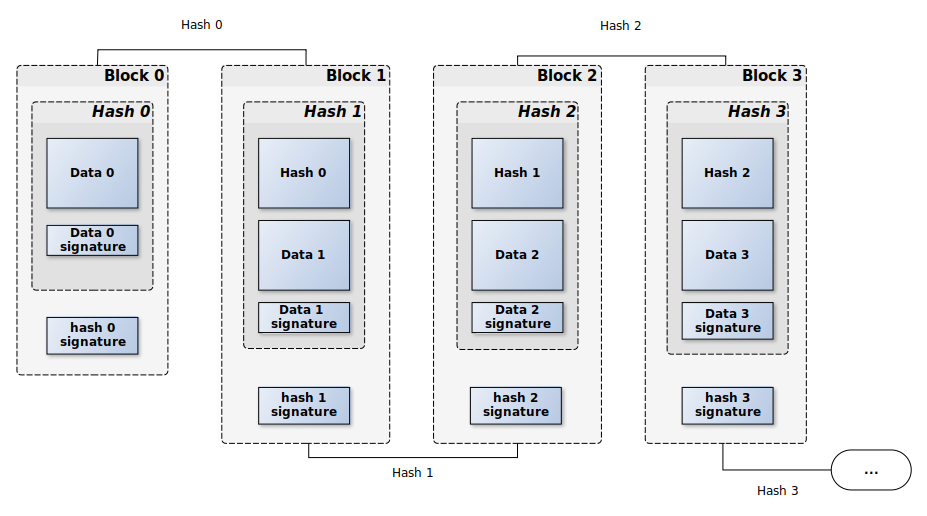
2) Значение хеш-функции, расчитанной по блоку, подписывается электронной подписью владельца блок-чейна, подпись храниться в блоке



*Схема 2*

В этом случае говорят, что ***блок закрыт*** владельцем подписи.

3) Комбинируют 1-й и 2-й варианты, подписывая как данные, так и значение хеш-функции.

*Схема 3*

Считаем, что созданы условия при которых получение закрытого ключа подписи неосуществимо.

**ЗАДАНИЕ (12 баллов):**

*Разработать программу, формирующую блок-чейн на базе криптостойкой хеш-функции.   
Требования: использование 3-й схемы, наличие ввода и сохранения данных в блоках, возможность просмотра 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.*

Сформулируйте протокол работы блок-чейна.

Параметры:

1) Формат и инструменты хранения данных;  
2) процедура хеширования данных;

3) процедура подписи данных;

4) процедура хеширования блока;

*5) процедура подписи хеша блока.*

**АЛЬТЕРНАТИВНОЕ ЗАДАНИЕ (6 баллов):**

*В предложенном коде реализуйте использование 3-й схемы и хранение информации либо с использованием СУБД, либо в каком-то ином виде на носителе с долговременным хранением данных.*