Децентрализация

Децентрализация

1. Кто хранит книгу транзакций?

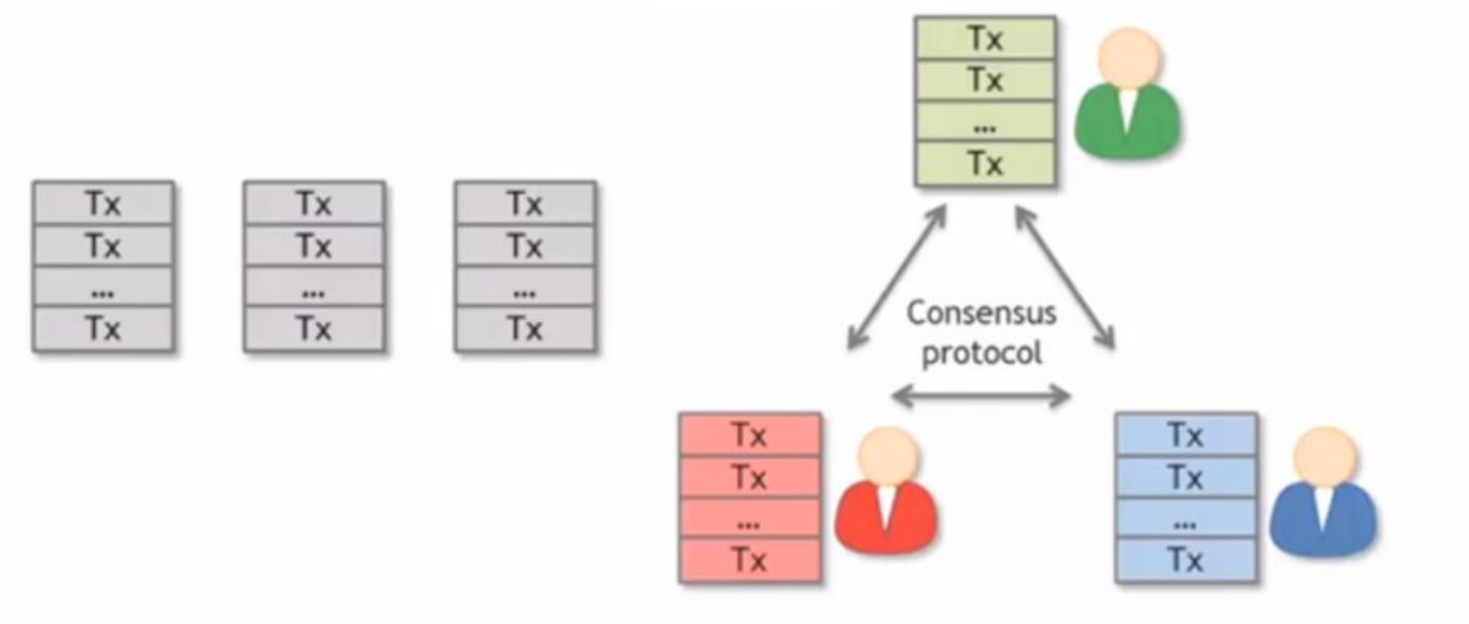
2. Кто имеет власть утверждать действительность транзакций?

3. Кто создает новые биткойны?

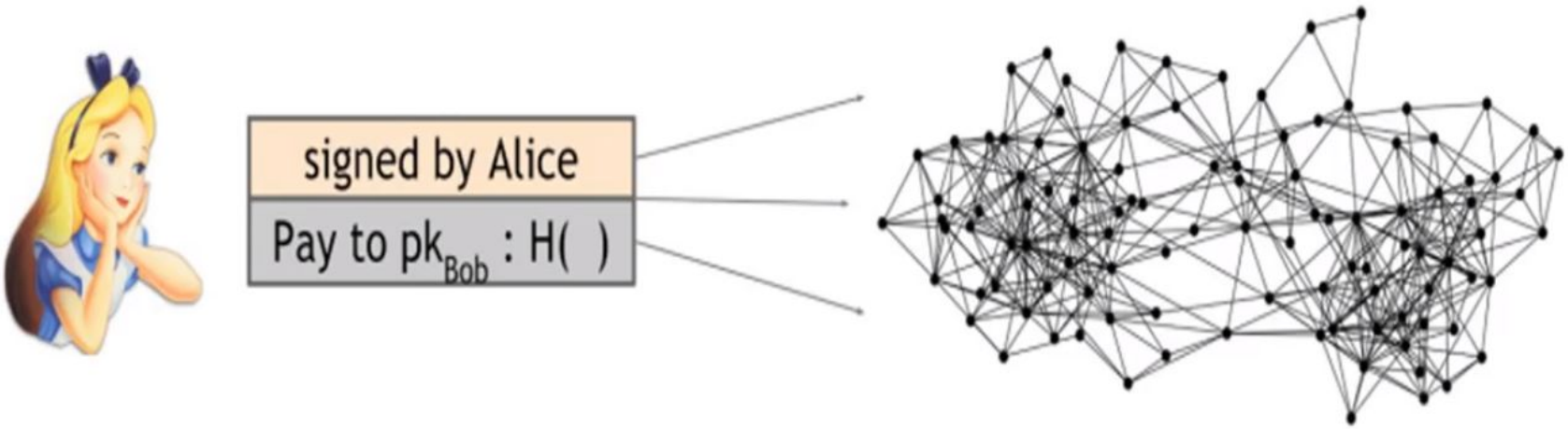
4. Кто определяет, как изменяются правила системы?

5. Как биткойны получают обменную стоимость?

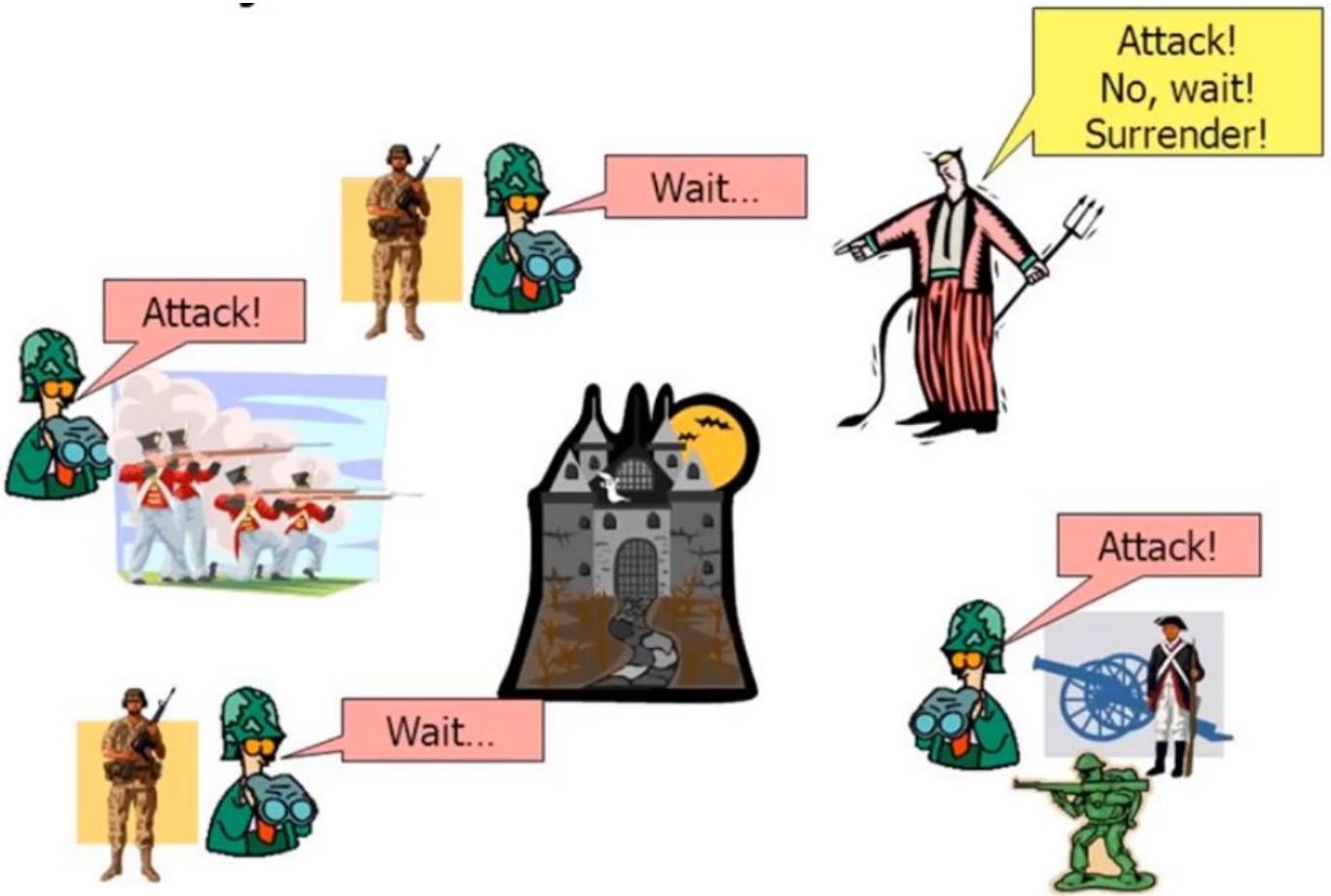
Распределенный консенсус



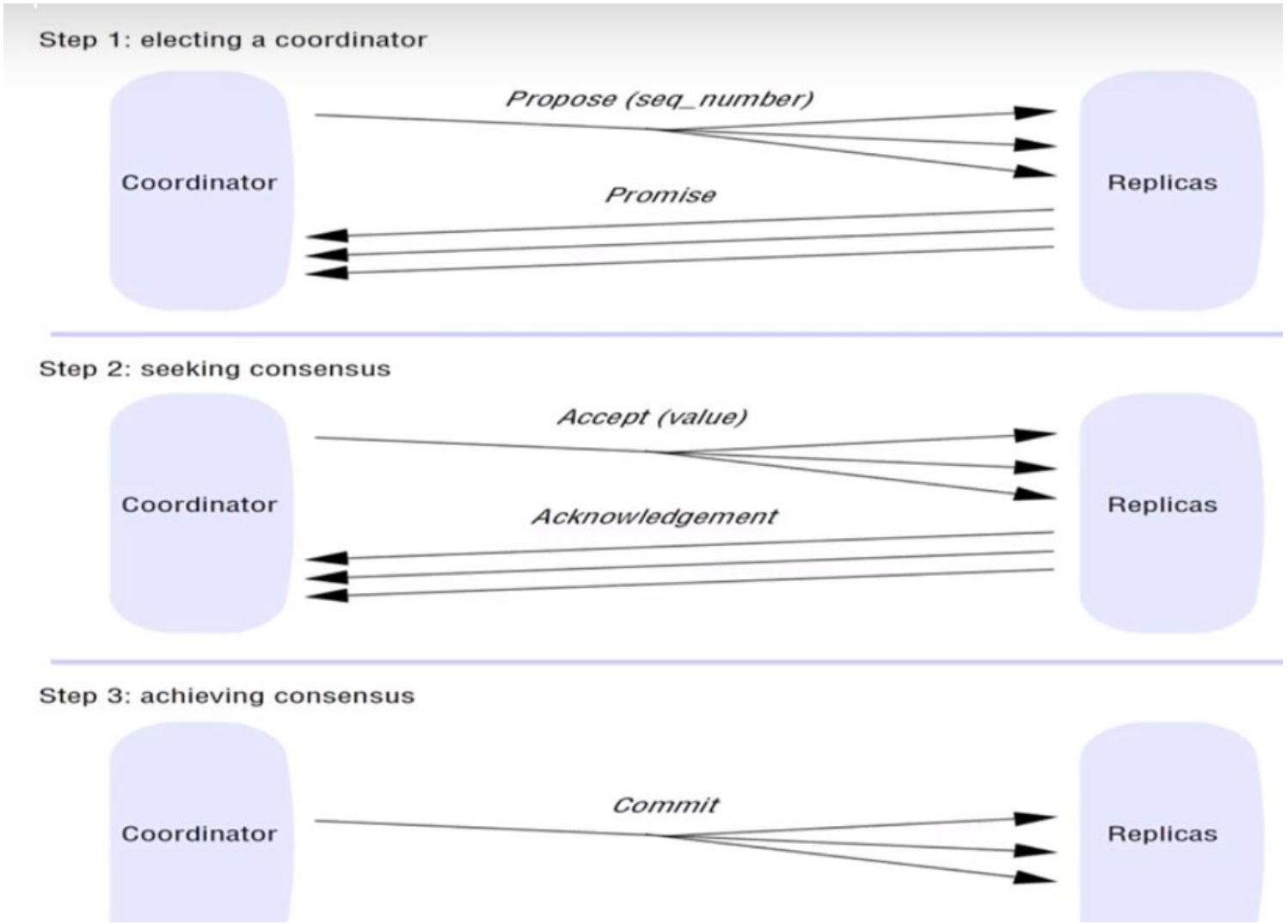
Распределенный консенсус



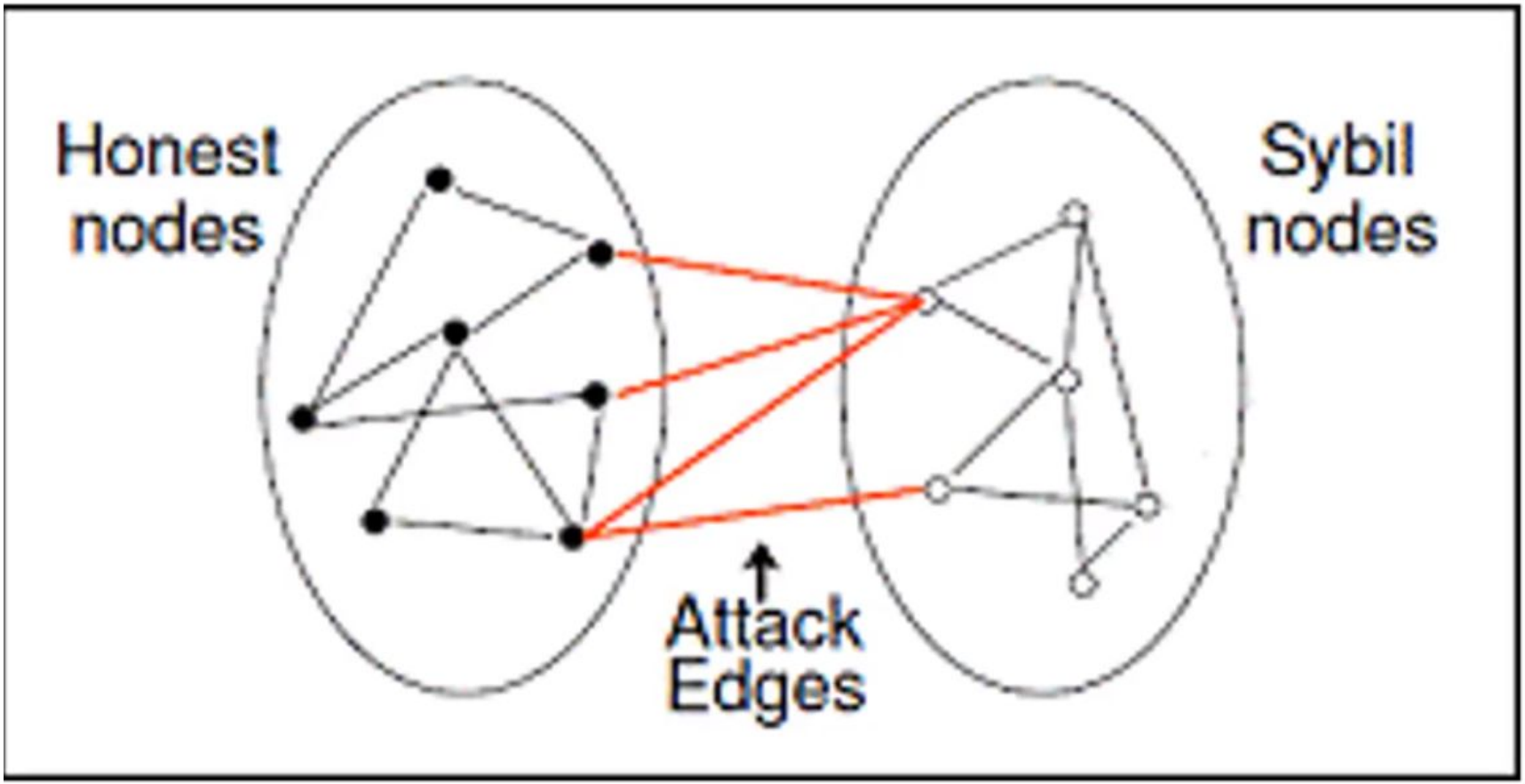
Проблема византийский генералов



Консенсус


Step 1: electing a coordinator
Coordinator
Propose (seq_number)
Promise
Replicas
Step 2: seeking consensus
Coordinator
Accept (value)
Acknowledgement
Replicas
Step 3: achieving consensus
Coordinator
Commit
Replicas

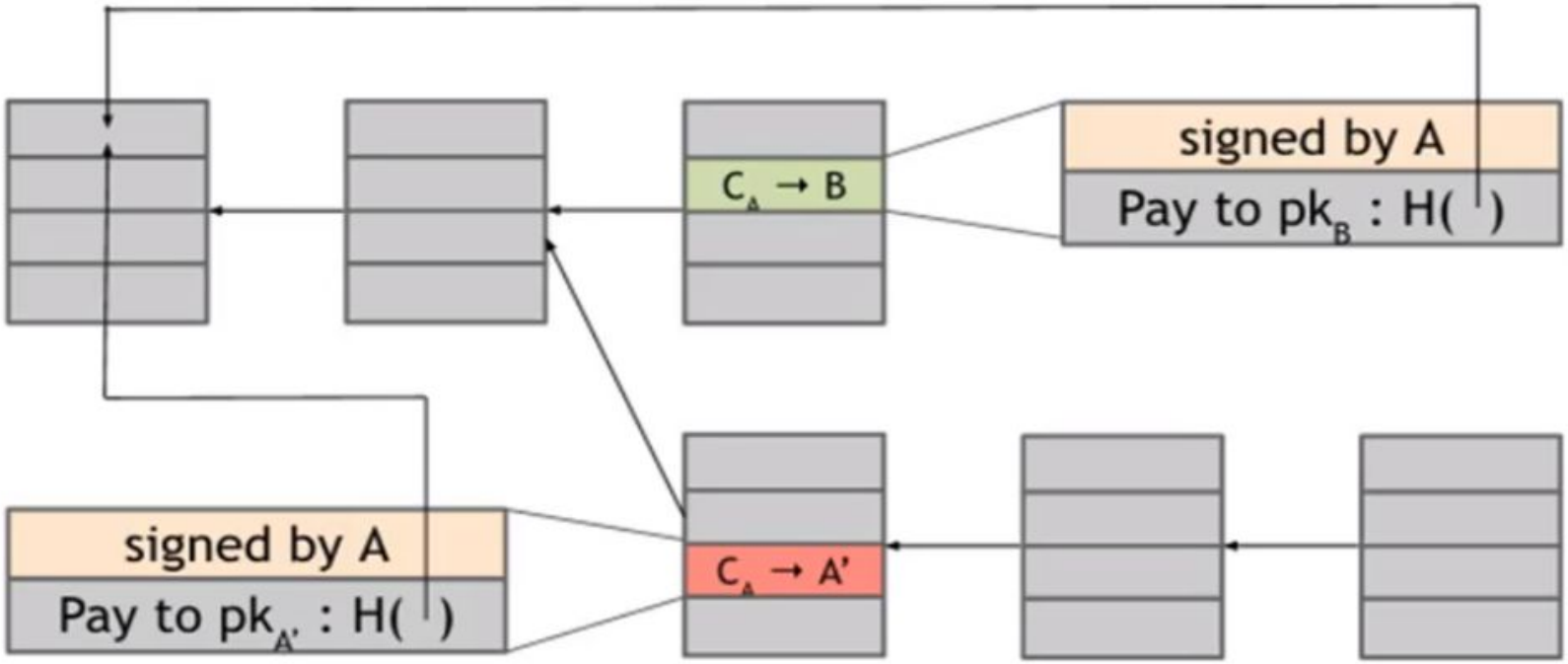
Атака «Сибил»



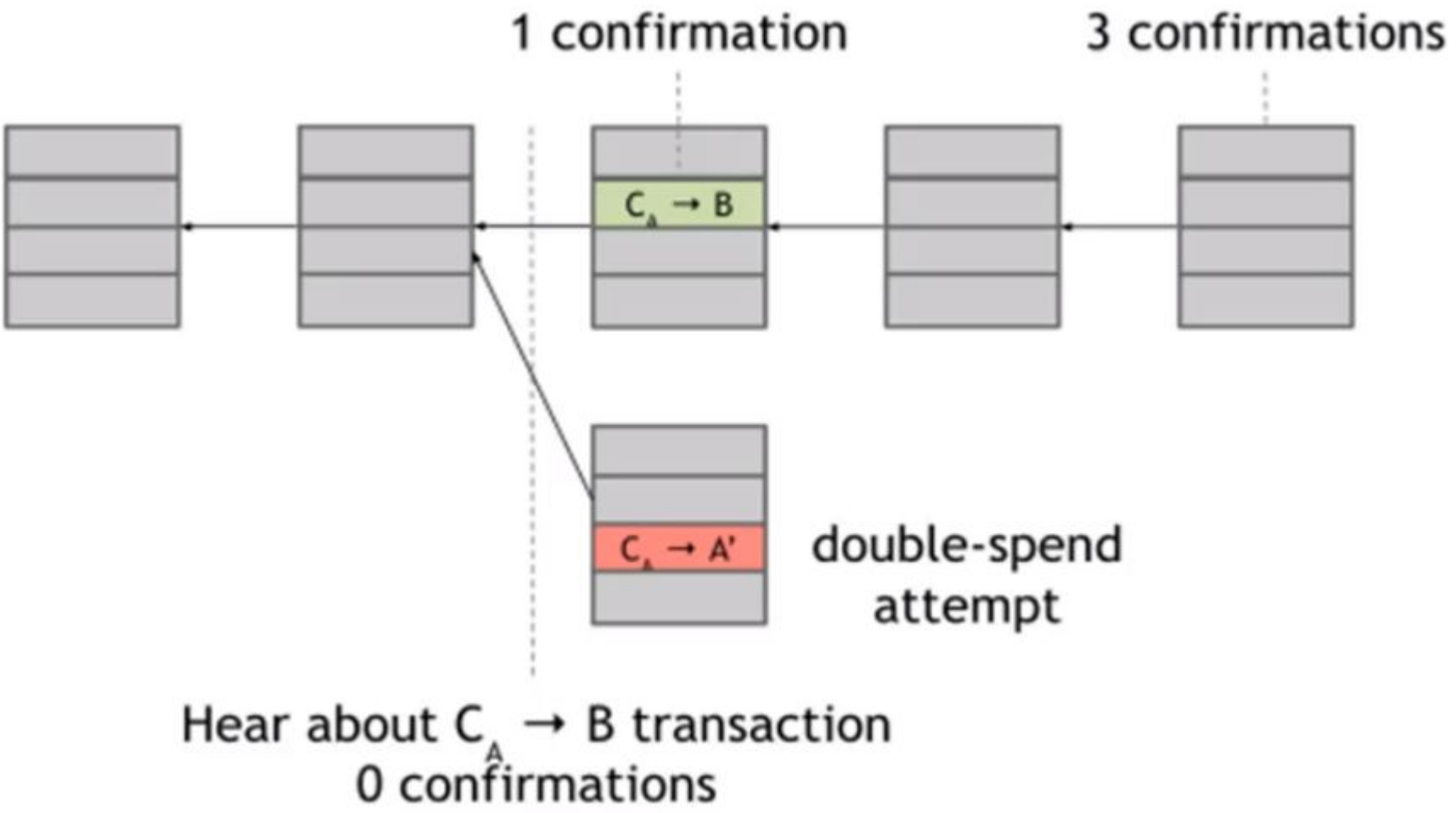
Упрощенный алгоритм консенсуса в биткоине

1. Новые транзакции передаются всем узлам.
2. Каждый узел собирает новые транзакции в блок
3. В каждом раунде случайный узел получает возможность транслировать свой блок.
4. Другие узлы принимают блок только в том случае, если все транзакции в нем действительны (все подписи валидны).
5. Узлы выражают свое принятие блока, включая его хеш в следующем блоке, который они создают.

Атака двойной траты



Атака двойной траты



Вариант №1 контрольной работы

Реализовать смарт-контракт «Аукцион». Работает он следующим образом:

1. При первом платеже он принимает эфиры и запоминает адрес переводящего деньги и сумму перевода
2. При следующем платеже. Проверяется, что если сумма перевода меньше или равна запомненной, то платеж отклоняется.
3. При получении эфиров смарт-контракт проверяет общее число переводов денег, если оно больше чем 10 смарт-контракт отклоняет платеж
4. По запросу смарт-контракт выдает информацию о сумме наибольшей оплаты.

Вариант №2 контрольной работы

Реализовать смарт-контракт «Средний платеж». Работает он следующим образом:

1. Принимает очередной платеж. Запоминает сумму посл. платежа
2. Не принимает платеж меньше чем 1 finney.
3. По запросу смарт-контракт выдает информацию о средней сумме платежа и максимальной сумме.