«МИРЭА-РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНСТИТУТ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ И СПЕЦИАЛЬНОГОПРИБОРОСТРОЕНИЯ

Кафедра КБ-4 «Автоматизированные Системы Управления»

Доклад на тему

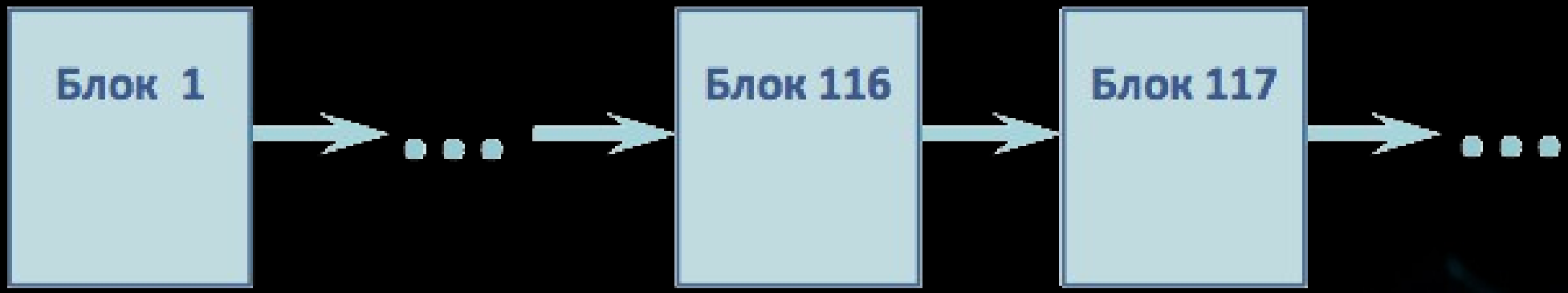
«ПРИМЕНЕНИЕ ОРИЕНТИРОВАННОГО АЦИКЛИЧЕСКОГО ГРАФА В БЛОКЧЕЙН СЕТИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ И СКОРОСТИ ТРАНЗАКЦИЙ»

Котилевец И.Д.

Суздаль 2018

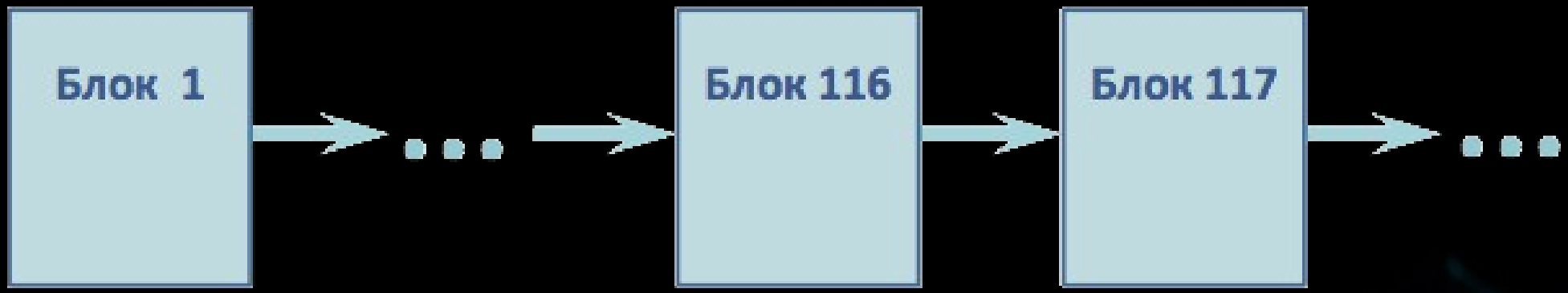
Что такое блокчейн?

Блокчейн — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию.

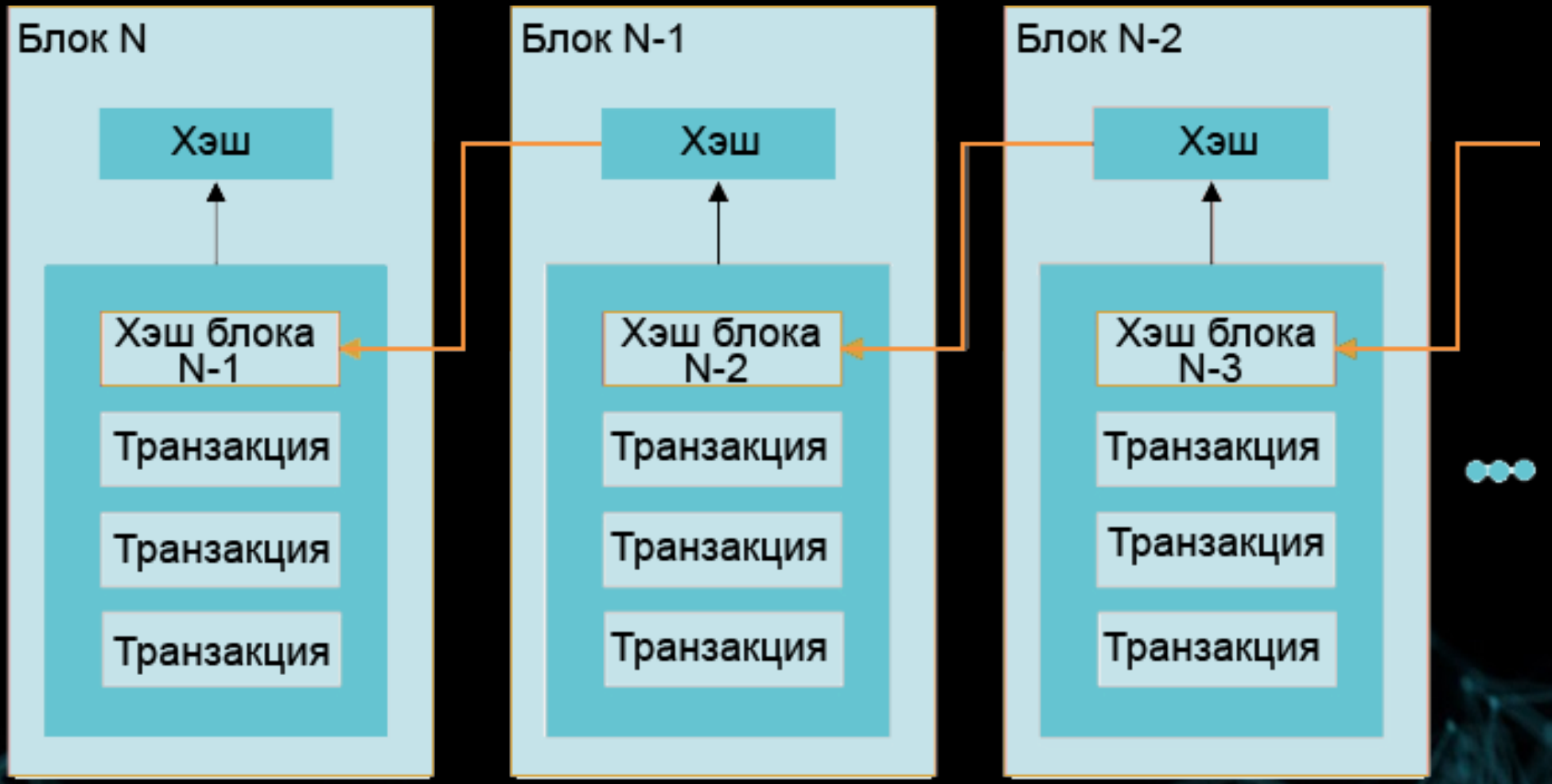


Что такое блокчейн?

Блокчейн — выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию.



Структура блокчейн



От чего защищает блокчейн?

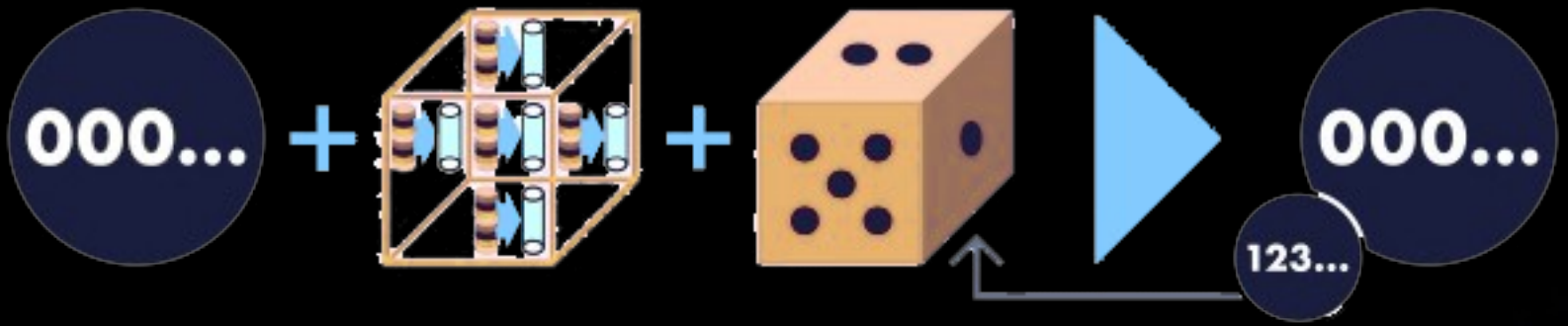
- Атаки типа man-in-the-middle;
- Манипулирование данными;
- DdoS-атаки;
- Взлом устройств Интернета Вещей.

Недостатки блокчейн

- Ограничения масштабируемости;
- Низкая скорость транзакций;
- Ненадёжность механизмов достижения консенсуса;
- Отсутствие управления и стандартов;
- Ограниченная конфиденциальность.

Proof-of-Work

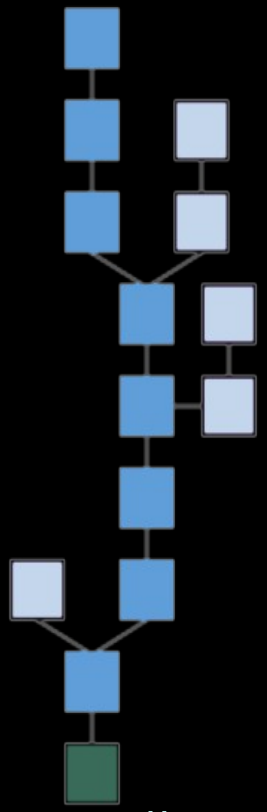
Proof-of-Work — алгоритм защиты распределенных систем от злоупотреблений, суть которого сводится к необходимости выполнения определенной сложной и длительной задачи и возможности быстро и легко проверить результат.



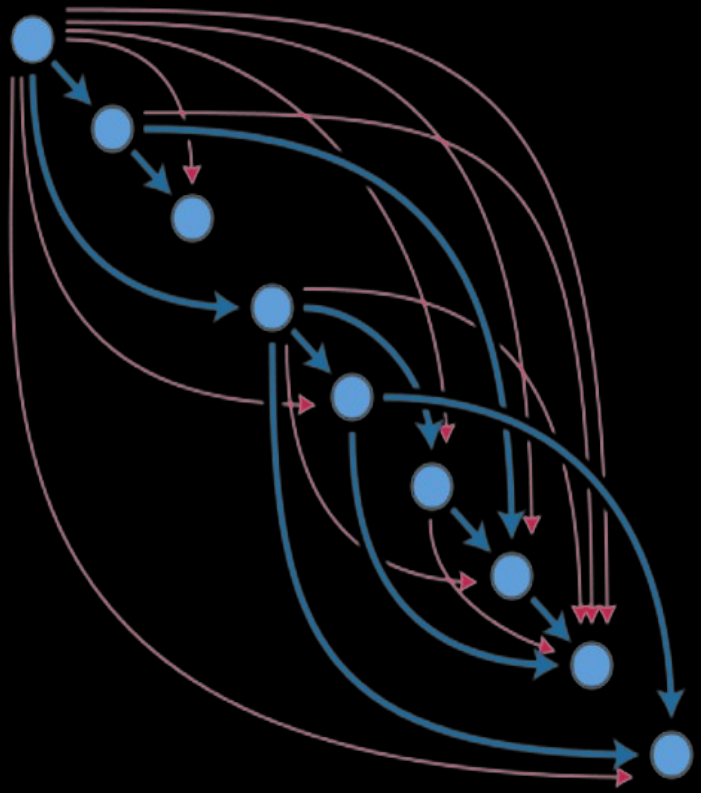
Ориентированный ациклический граф

Ориентированный ациклический граф — орграф, в котором отсутствуют направленные циклы, но могут быть «параллельные» пути, выходящие из одного узла и разными путями приходящие в конечный узел.

Структура ориентированного ациклического графа

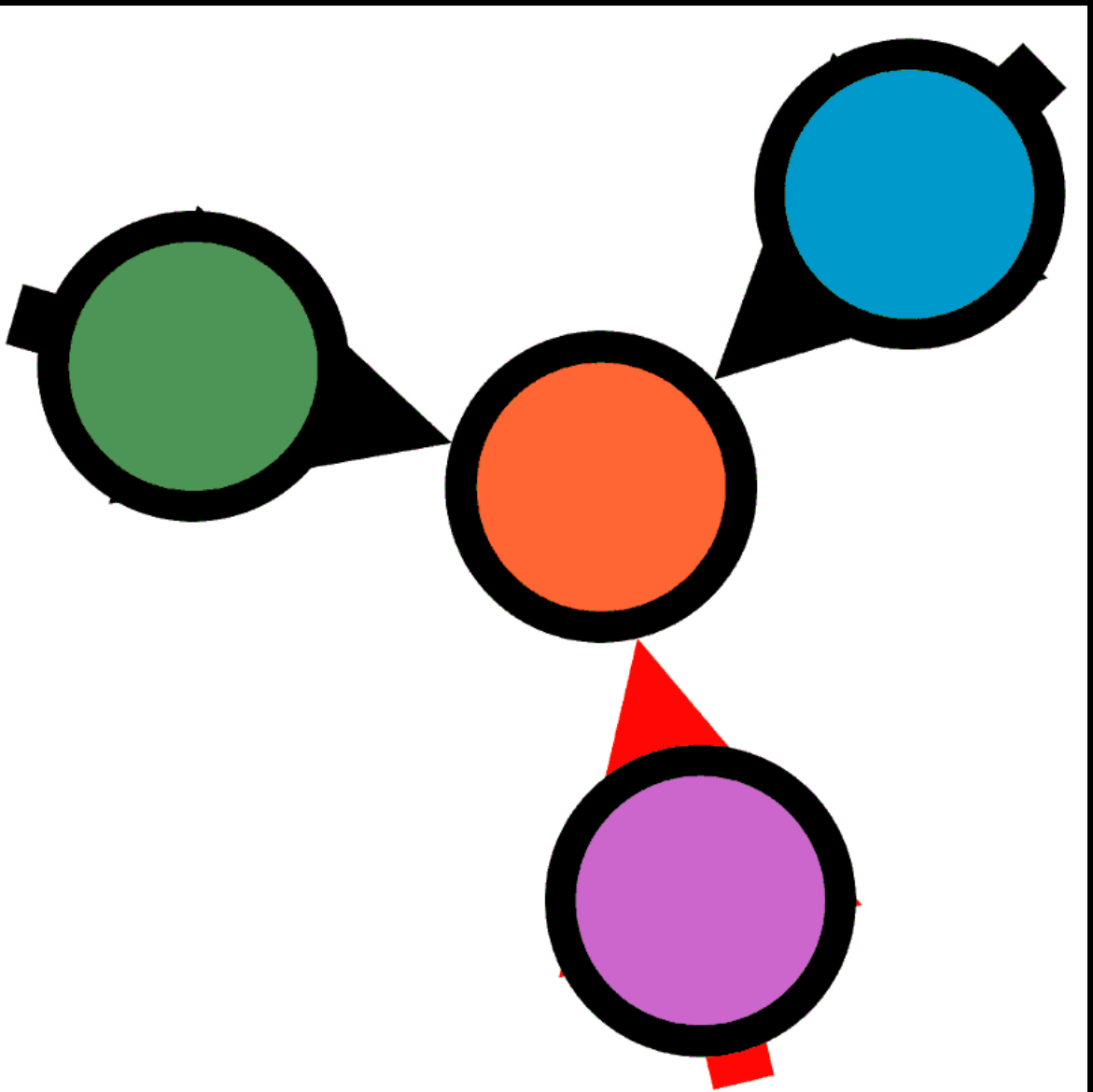


Блокчейн



Ориентированный ациклический граф

Ориентированный ациклический граф в сети блокчейне с тремя узлами



Цветные круги обозначают блоки
Красные стрелки соответствуют граням графа.
Черные стрелки обозначают ветки, которые были или будут отброшены.

Заключение

Применение ориентированного ациклического графа в блокчейне позволит достичь:

- Гибкой масштабируемости;
- Высокая скорость транзакций в секунду;
- Формирования древовидной структуры транзакций, где каждая будет считаться подтвержденной и неизменной.

Спасибо за внимание