# Отказоустойчивые протоколы блокчейн консенсуса без лидера

**Студент**:

Афанасьева Анастасия Сергеевна, БПМИ206

**Руководитель**:

Янович Юрий Александрович

Доцент

Факультета компьютерных наук НИУ ВШЭ

Кафедры технологий моделирования сложных систем

# Мотивация выбора протоколов без лидера

| Проблема | Решение |
| --- | --- |
| **нет устойчивости к цензуре** (гарантии, что любая транзакция честного участника будет включена в блокчейн) | **алгоритмы без лидера**, работающие в присутствии злоумышленников с Византийским поведением |

# Постановка задачи

- N заранее известных участников
  f из них могут иметь Византийское поведение
- Модель сети: частично-синхронная / асинхронная
- Византийские участники:
  - ведут себя произвольно, могут вступать в сговор
  - могут влиять на сеть, но не способны задерживать сообщения навсегда
  - не могут выдавать себя за других участников

$N > 3f$

# Цель

проанализировать и сравнить такие алгоритмы блокчейн консенсуса без лидера в условиях различных византийских атак

# Задачи

- поиск и изучение соответствующих алгоритмов консенсуса
- реализация одного или нескольких алгоритмов
- реализация симулятора для экспериментов
- моделирование и проведение экспериментов
- построение графиков и анализ результатов

# Актуальность

В статьях, представляющих такие алгоритмы:

- замеры только хорошего случая, нет злоумышленников
- только случай Fail-Stop отказов, нет Византийских атак
- нет сравнения работы алгоритма при различной доле злоумышленников

# Существующие алгоритмы

1. DBFT
2. HoneyBadgerBFT, BEAT, Aleph
3. Snowflake

# Симулятор

- каждый участник в своём потоке
- сеть эмулирована
- транзакции - просто числа, можно считать хешами
- нет верификации транзакций

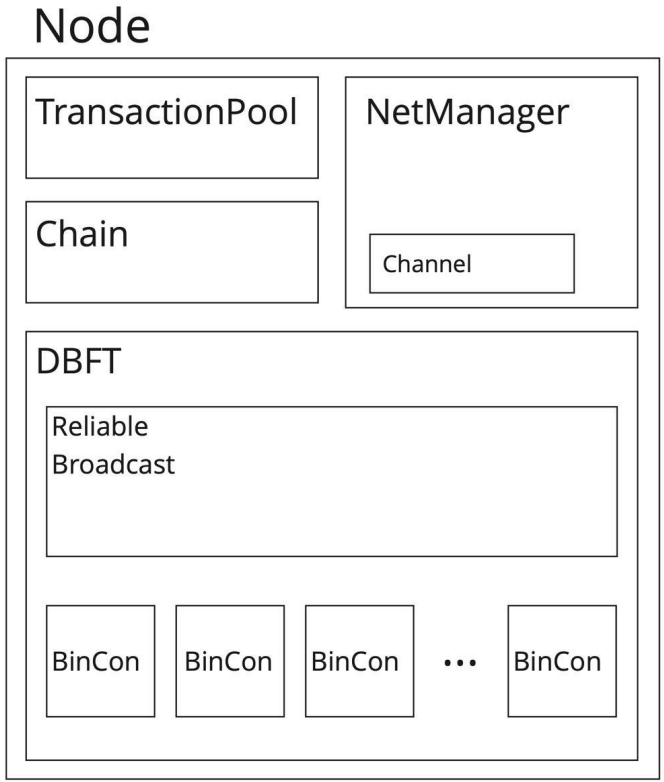
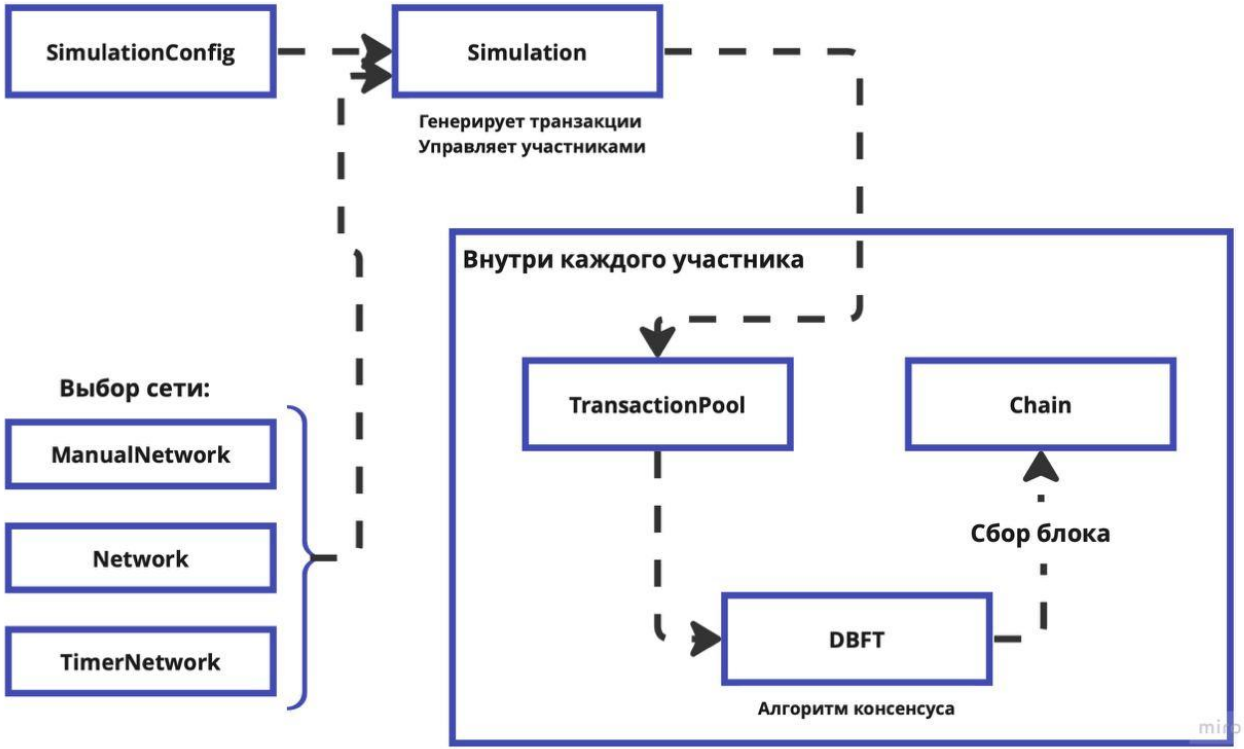


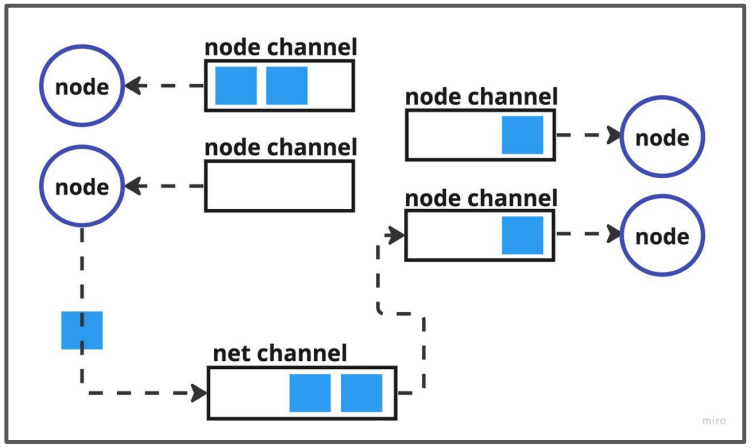

Схема участника сети

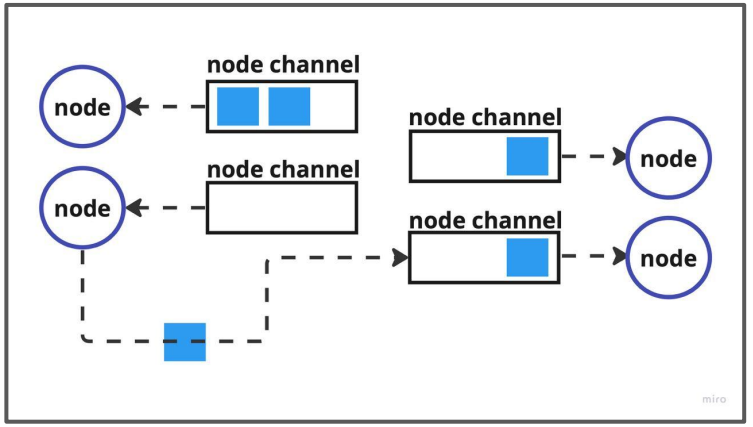
# Симулятор


SimulationConfig
Simulation
Генерирует транзакции
Управляет участниками
Внутри каждого участника
Выбор сети:
ManualNetwork
Network
TimerNetwork
TransactionPool
Chain
Сбор блока
DBFT
Алгоритм консенсуса

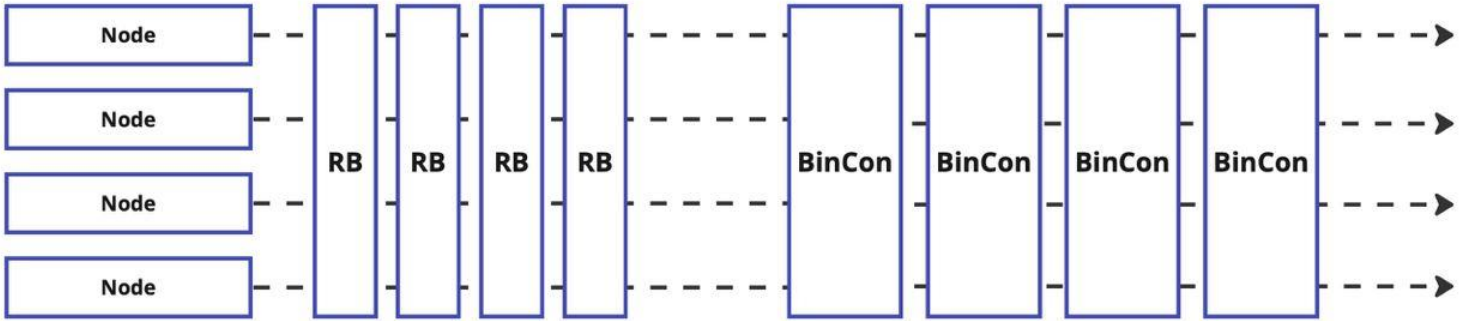
# Сеть

| Сеть | Каналы | Назначение |
|---|---|---|
| ManualNetwork | потокобезопасные очереди, дополнительный канал у сети | тестирование |
| Network | потокобезопасные очереди | тестирование |
| TimerNetwork | планировщики из Boost.Asio, сообщения с таймерами | эксперименты |



# Алгоритм DBFT



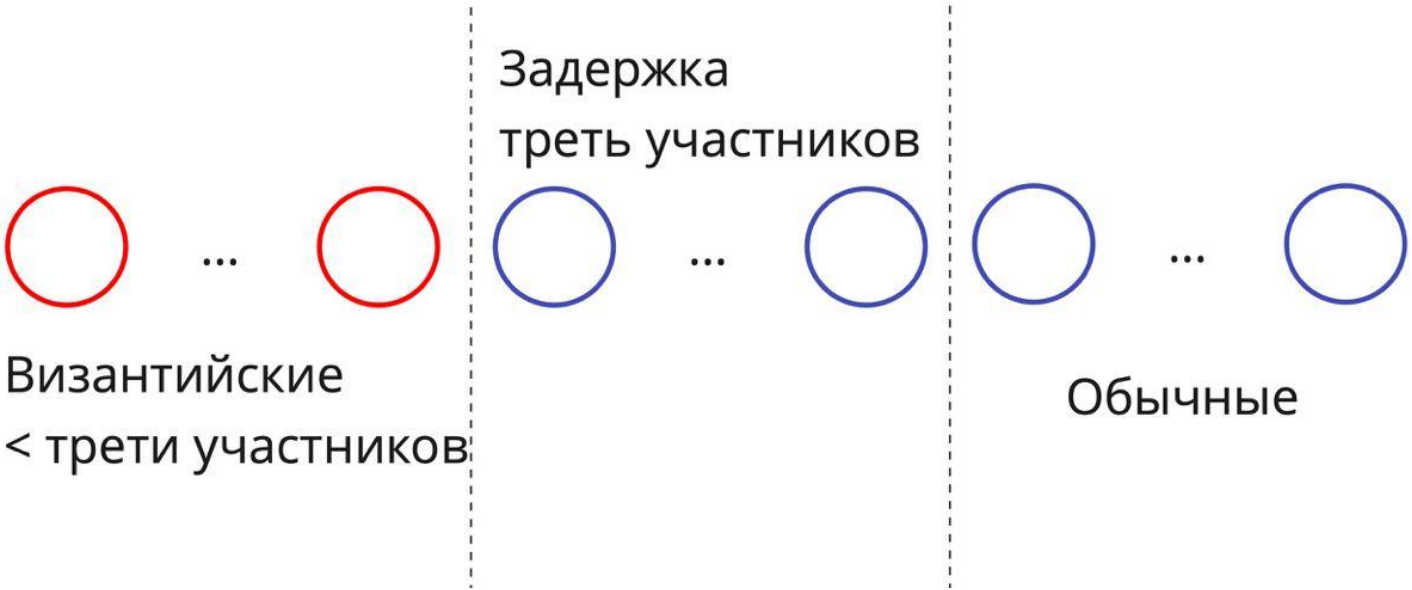

RB - надёжный broadcast
BinCon - бинарный консенсус

# Модели Византийского поведения

- Rejector - сразу отправляет во все бинарные консенсусы все сообщения со значением 0 на всех этапах

- BinConCrasher - сразу отправляет во все бинарные консенсусы все сообщения с обоими значениями (и 0, и 1)

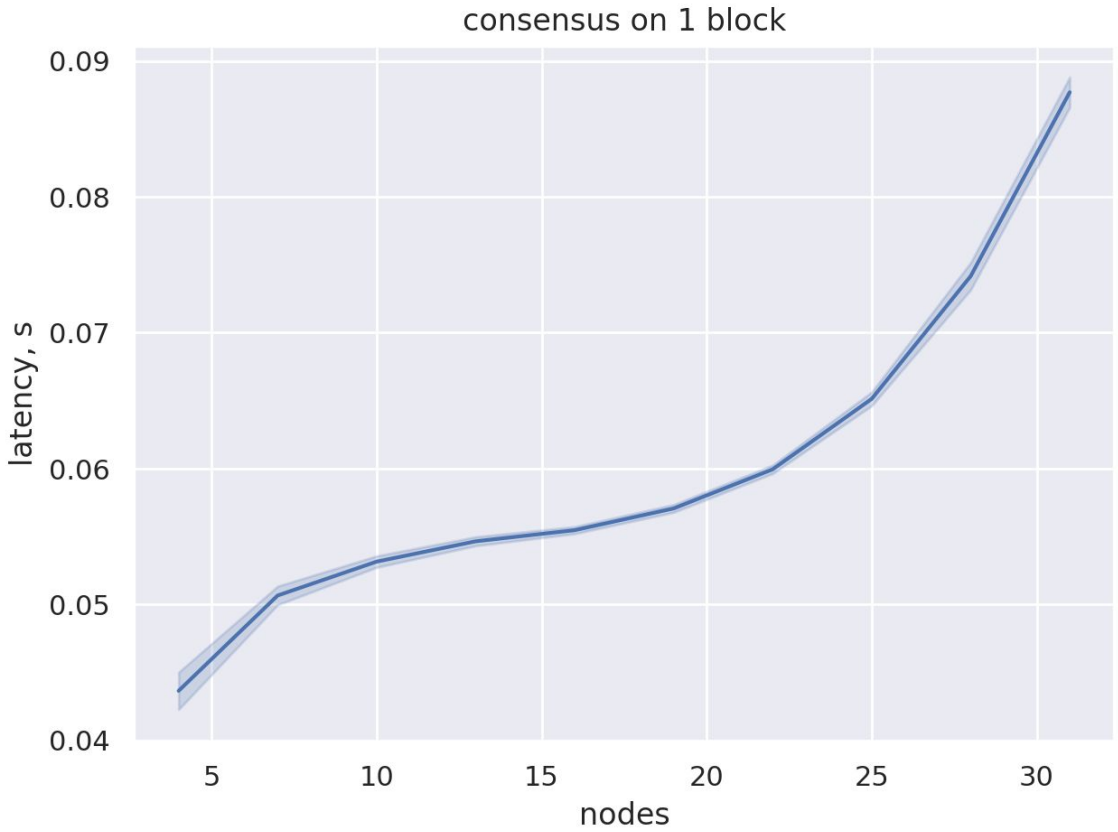
# Модели Византийского поведения



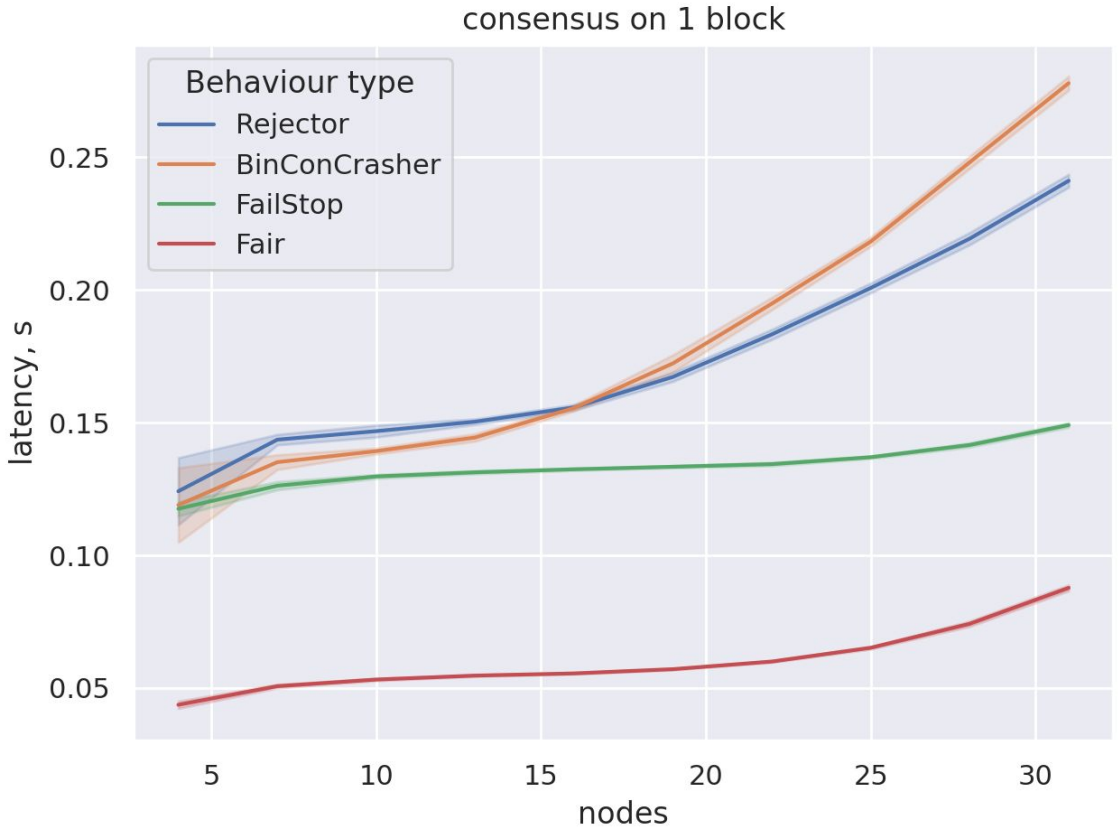

задержка сообщений, пока не завершатся (N - f) алгоритмов консенсуса

# Эксперименты

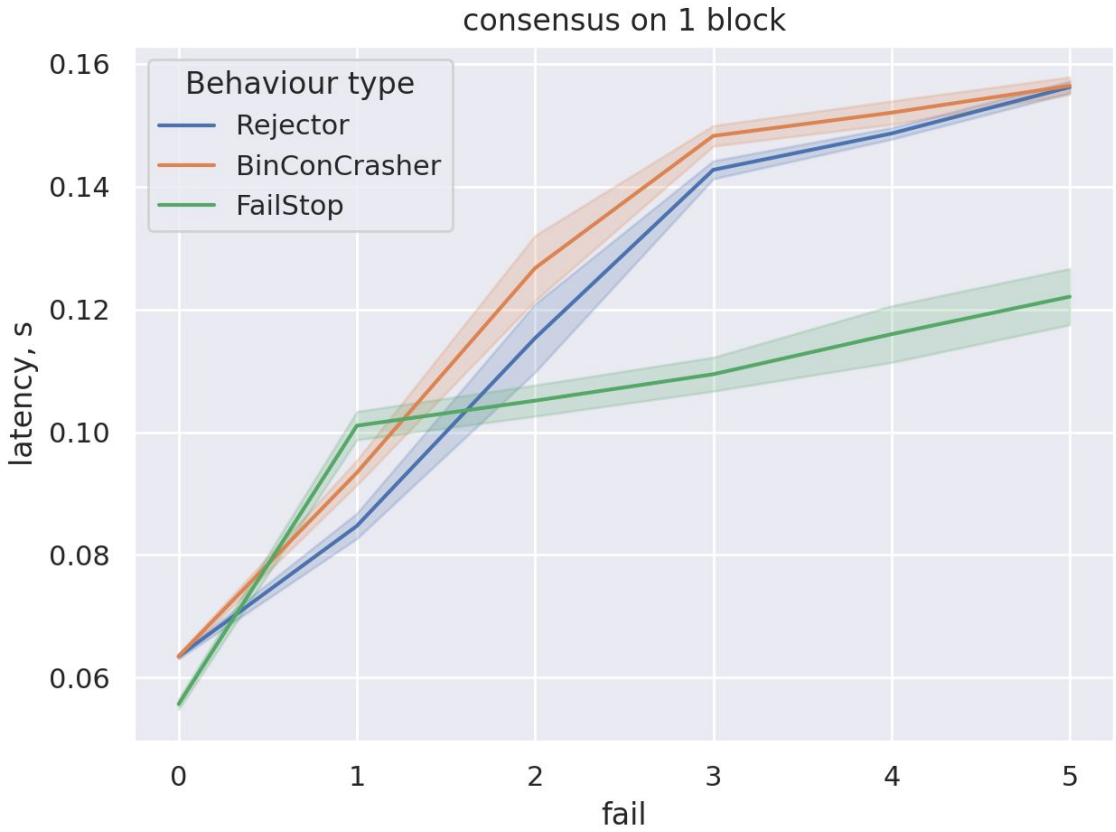
- замеры на 32 ядерном компьютере
- от 4 до 31 участника



# Эксперименты: максимальное число злоумышленников



# Эксперименты: различная доля злоумышленников



# Выводы

- найдено 5 соответствующих алгоритмов
- реализован симулятор блокчейна с алгоритмом консенсуса DBFT
- предложено 2 модели Византийского поведения, атакующих бинарный консенсус
- получилось достичь увеличения времени поиска блока в 2 - 2,5 раза

# Направления дальнейшей работы

- поиск других детерминированных протоколов
- добавление в симулятор протоколов из представленного списка
- расширение модели симулятора
  - сделать сложнее модель транзакций
  - увеличить число участников сети