**Министерство науки и высшего образования Российской Федерации**
**Федеральное государственное бюджетное образовательное учреждение высшего образования.**
**Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет).**
**(МГТУ им. Н. Э. Баумана)**

# Методы решения задачи византийских генералов

Студент: ИУ7-55Б Талышева Олеся Николаевна
Руководитель: Кострицкий Александр Сергеевич

2024 г.

# Формализация задачи византийских генералов

Задача византийских генералов моделирует ситуацию, где n генералов должны достичь единого решения (атаковать или отступать) при наличии ненадёжных участников (до m предателей). Генералы обмениваются приказами и информацией, чтобы минимизировать риск неблагоприятного исхода.

Возможные исходы:

1) Благоприятный: все верные генералы атакуют.
2) Промежуточный: все верные генералы отступают.
3) Неблагоприятный: часть генералов атакует, часть отступает.

Предатели могут искажать приказы главнокомандующего или дезинформировать других генералов. Задача заключается в нахождении алгоритма, обеспечивающего консенсус среди верных генералов, несмотря на вмешательство предателей.

# Сравнение методов решения задачи византийских генералов

| Критерий | Алгоритм Лэмпорта | Proof of Work (PoW) | Proof of Stake (PoS) | Delegated Proof of Stake (DPoS) |
|---|---|---|---|---|
| Тип системы | синхронная | асинхронная | асинхронная | асинхронная |
| Устойчивость к предателям | $n \geq 2*m + 1$ | > 50% вычислительных мощностей у честных узлов | > 50% доли у честных узлов | > 2/3 голосов доверенных делегатов |
| Эффективность | высокая | низкая | средняя | высокая |
| Масштабируемость | ограниченная n | ограниченная скоростью вычислений | высокая | очень высокая |
| Безопасность | высокая | высокая, но уязвима к 51%-атаке | высокая (при распределённой доле) | зависит от честности делегатов |
| Область применения | надёжные синхронные сети | криптовалюты, распределённые сети | криптовалюты, DeFi | высоконагруженные блокчейн-системы |

где n – общее число генералов, m – количество предателей среди них