Метод контроля и поддержания связности узлов в крупномасштабных коммуникационных сетях беспилотного транспорта

Бусыгин Алексей, a.busygin@ibks.spbstu.ru

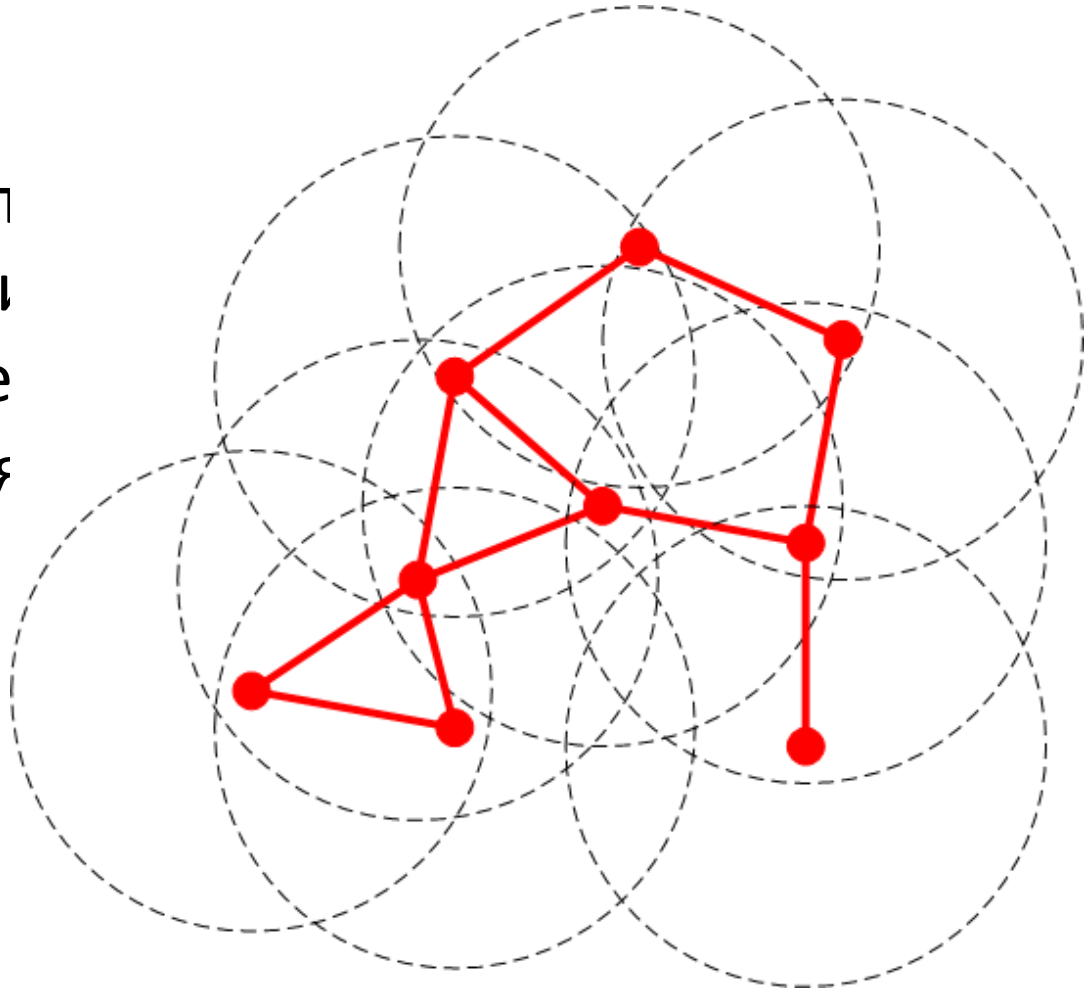
При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение о предоставлении субсидии № 14.578.21.0224 от 03.10.2016, уникальный идентификатор соглашения RFMEFI57816X0224)

Коммуникационные сети беспилотного транспорта

Особенности:

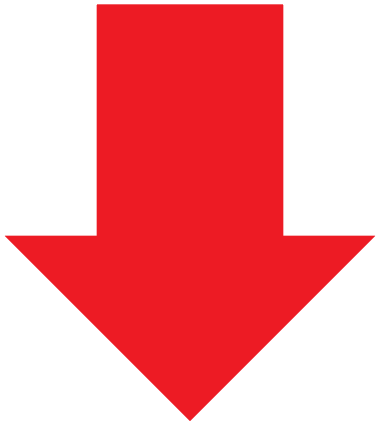
- Одноранговая сет
- Самоконфигураци
- Самовосстановле
- Беспроводная свя

MANET
VANET



Защита от специфичных угроз

Hello flood, Sinkhole, Wormhole, Blackhole, Sybil

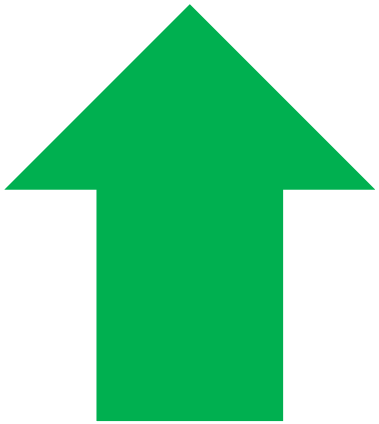


Блокчейн

Хранение данных аутентификации и маршрутизации

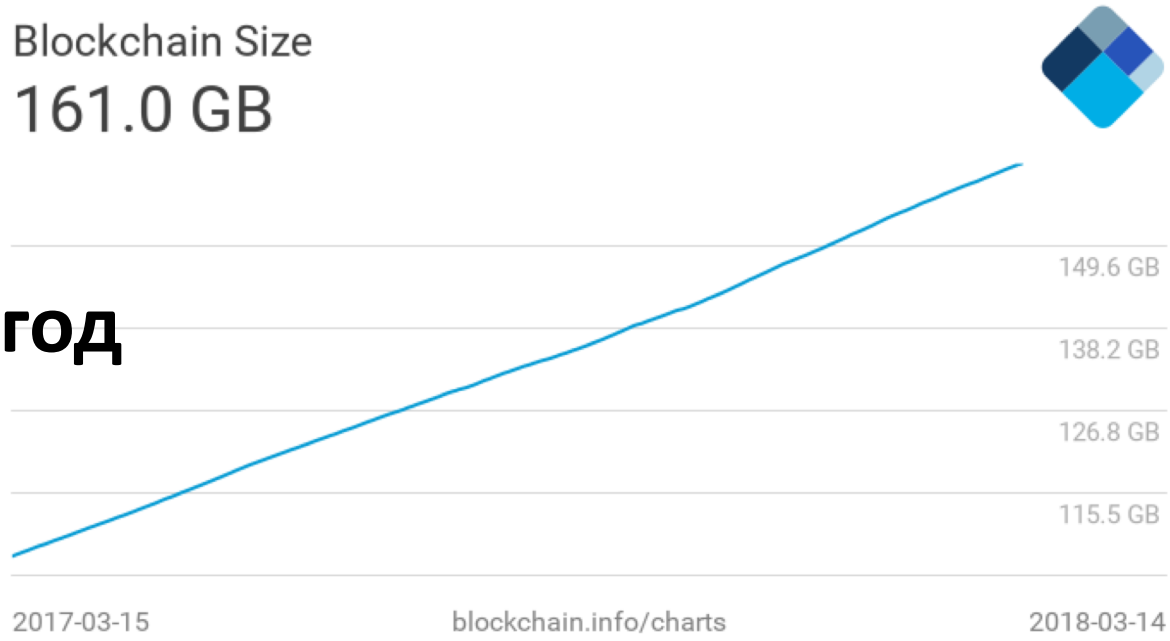
А. Бусыгин, А. Коноплев, *Материалы 26-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации»*, 101-102 (2017)

Интерактивная аутентификация, *географическая маршрутизация*, многолучевая маршрутизация, *история изменений топологии сети*



Проблема неограниченного роста Блокчейна

- Расход дисковой памяти
- Увеличение времени запуска новых узлов



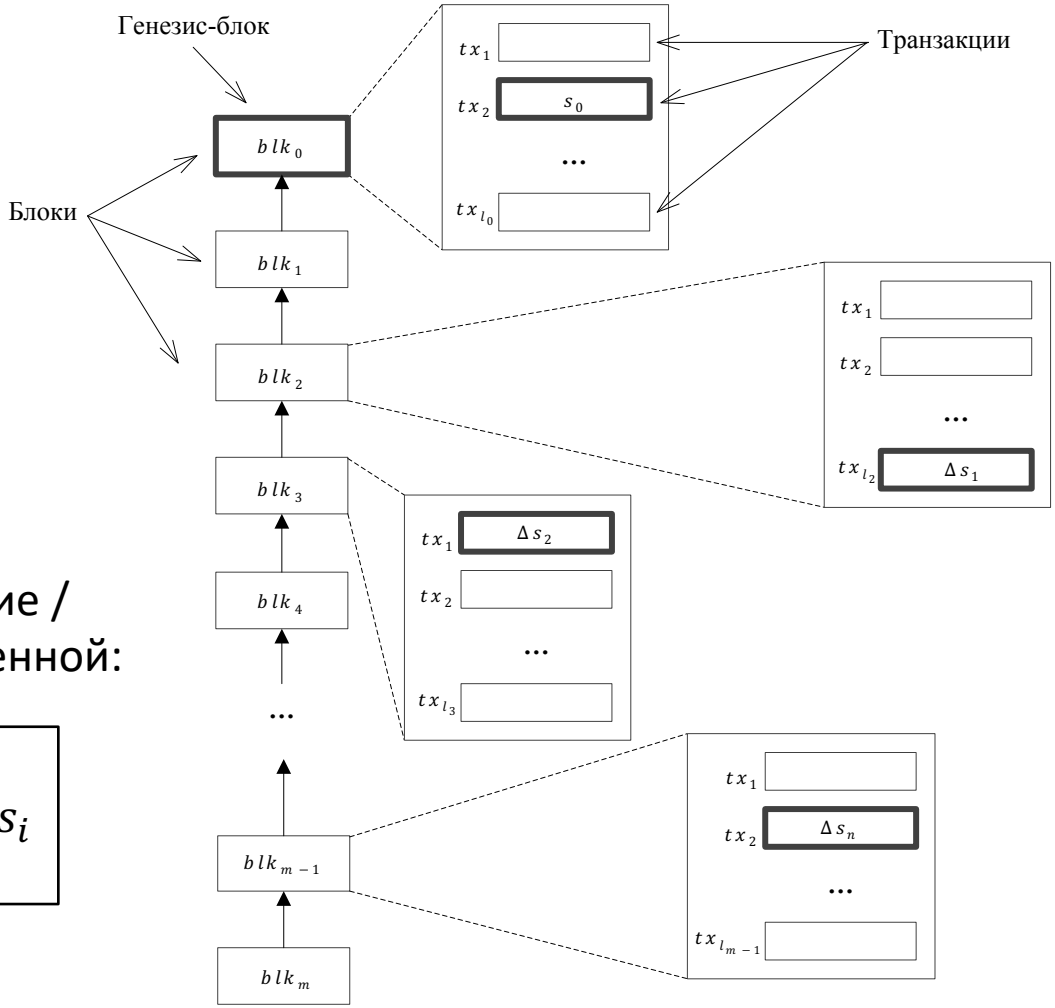
55 ГБ/год

Существующие решения

- Отбрасывание транзакций после верификации и обработки
- Сокращение объёма сериализованных данных блокчейна
- Офчейн-транзакции
- Шардинг
- Распределённые хэш-таблицы

Лишь замедляют рост блокчейна и не решают проблему времени запуска новых узлов

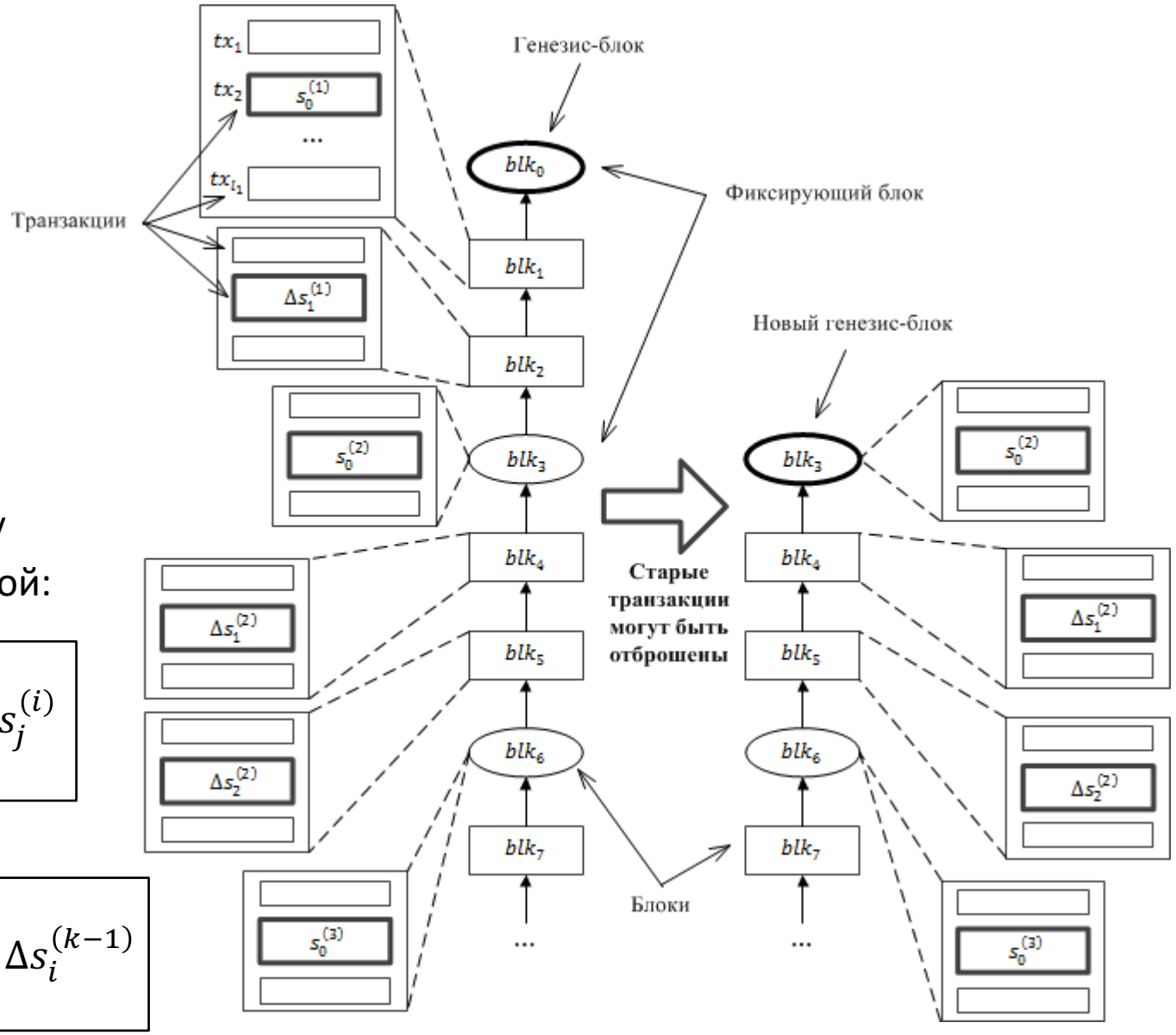
Базовая модель блокчейна



Текущее состояние / значение переменной:

$$s = s_0 + \sum_{i=1}^{n} \Delta s_i$$

Блокчейн с плавающим генезис-блоком



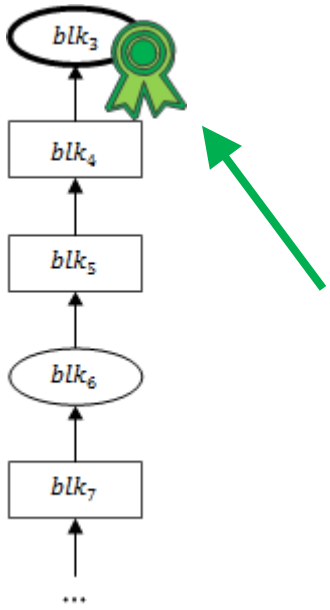
Текущее состояние / значение переменной:

$$s = s_0^{(k)} + \sum_{i=k}^{m} \sum_{j=1}^{n_i} \Delta s_j^{(i)}$$

$$s_0^{(k)} = s_0^{(k-1)} + \sum_{i=1}^{n_{k-1}} \Delta s_i^{(k-1)}$$

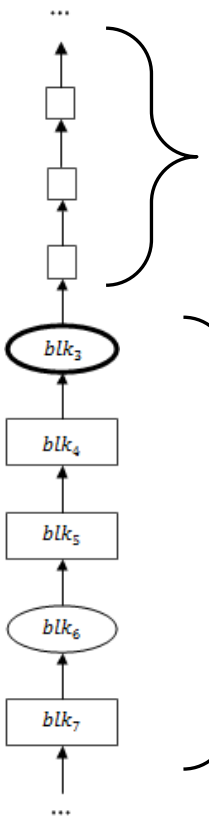
Защита от подделывания блокчейна

Загрузка с доверенных узлов



Цифровая подпись доверенного узла

Сохранение proof-of-work



Заголовки блоков

Блоки с транзакциями

Сравнение с аналогами

	Необходимость загрузки и верификации всех транзакций при старте нового узла	Размер блокчейна от времени	Возможность локального доступа к блокчейну
Отбрасывание обработанных транзакций	Да	O(t)	**Да**
Сжатие данных	Да	O(t)	**Да**
Офчейн-транзакции	Да	O(t)	**Да**
Шардинг, DHT	Да	O(t)	Нет
Блокчейн с плавающим генезис-блоком	**Нет**	O(t)	**Да**
Блокчейн с плавающим генезис блоком + загрузка с доверенных узлов	**Нет**	**O(1)**	**Да**

Вывод

- Предложенный метод позволяет решить проблемы, связанные с неограниченным ростом блокчейна
- Возможность применения технологии Блокчейн в коммуникационных сетях беспилотного транспорта
- Метод применим только для транзакций с ограниченным сроком актуальности