



# НЕОБИТ

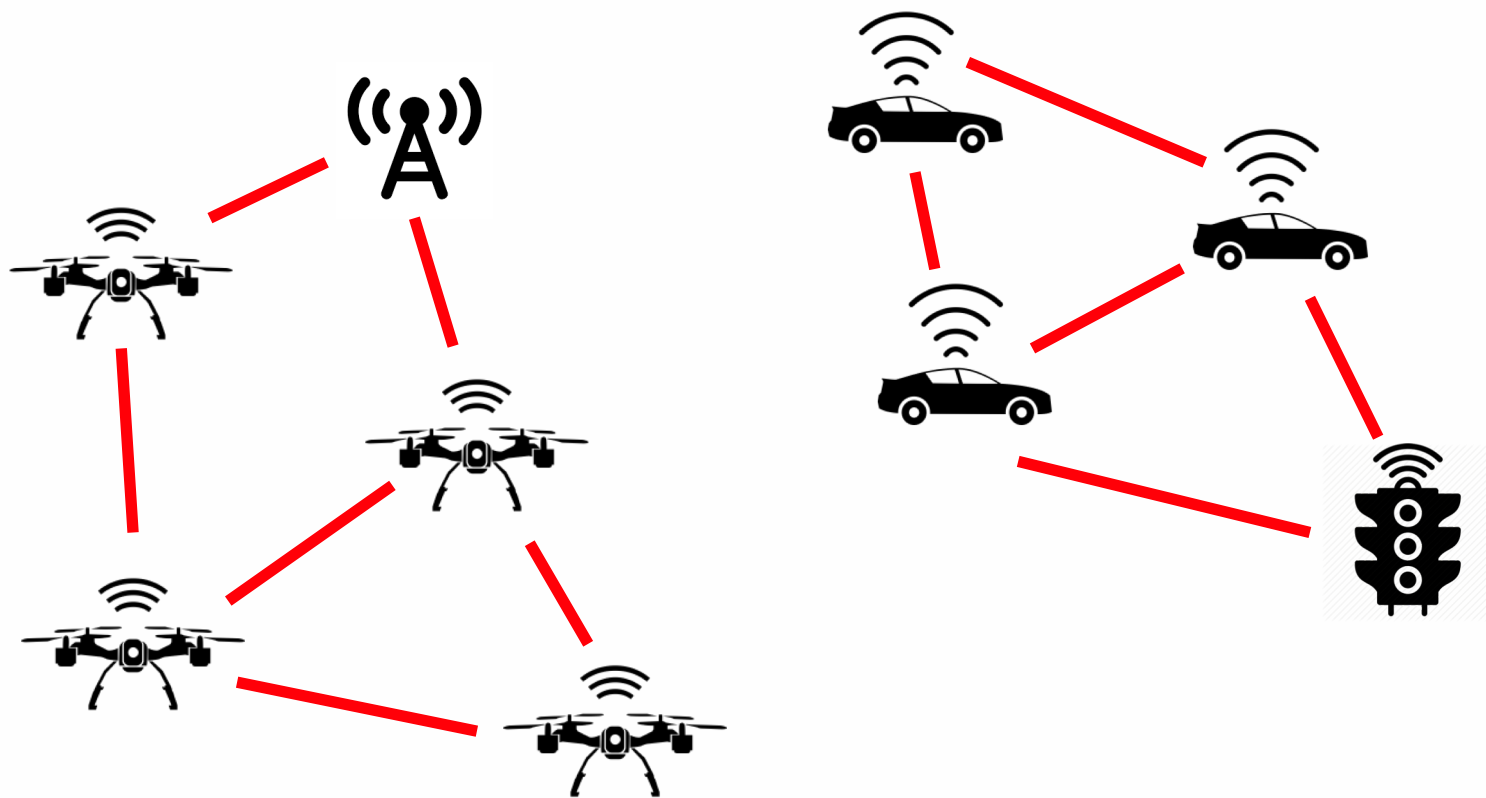
НОВЫЕ  
БЕЗОПАСНЫЕ  
ИНФОРМАЦИОННЫЕ  
ТЕХНОЛОГИИ

## Обеспечение безопасности динамических сетей Интернета вещей на основе децентрализованных моделей доверия

Алексей Бусыгин  
[busygin@neobit.ru](mailto:busygin@neobit.ru)

# Динамические сети Интернета вещей

- MANET
- VANET
- FANET
- SANET
- MWSN



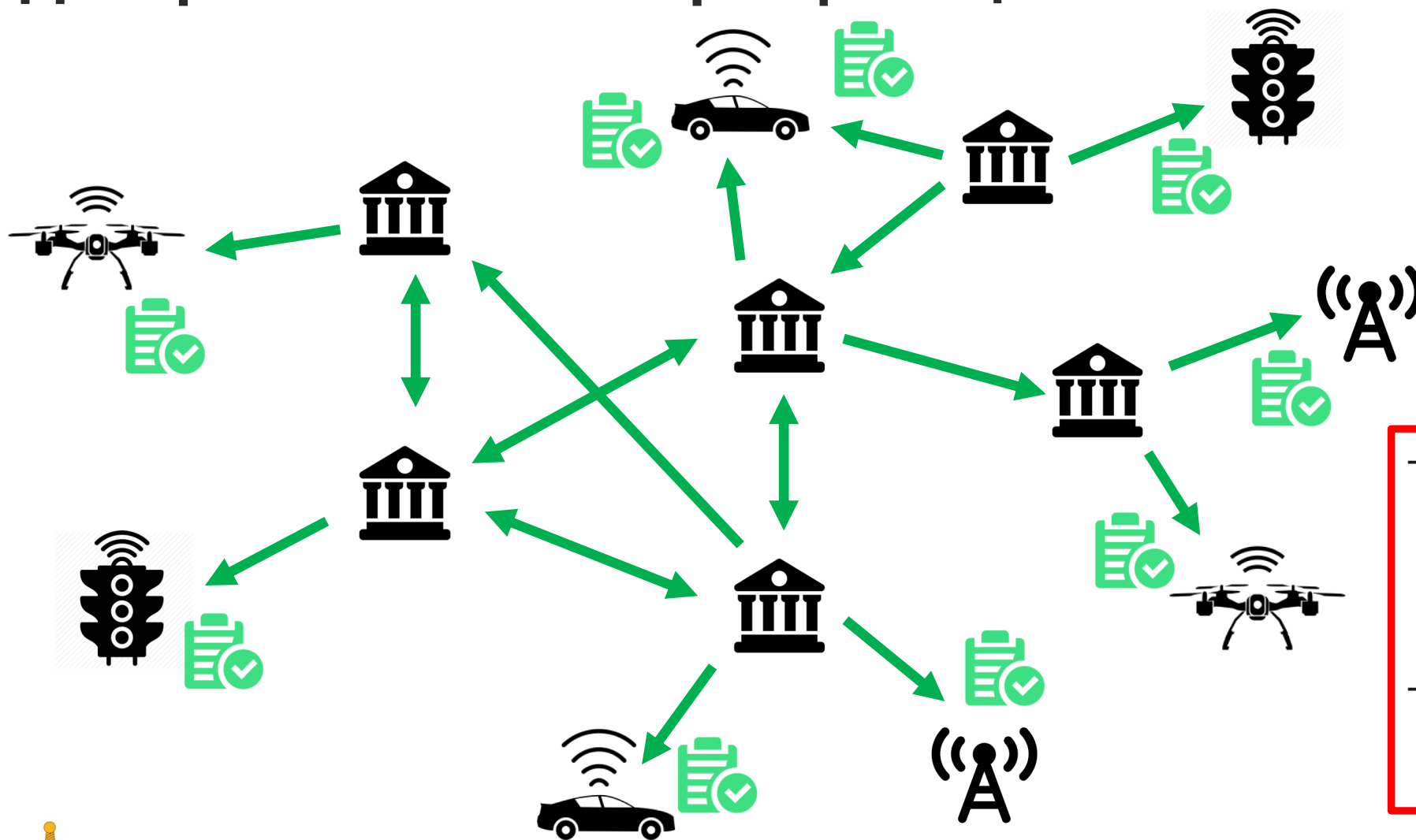
# Особенности динамических сетей



MANET	VANET	FANET	MWSN
<ul style="list-style-type: none"><li>• <b>Динамическая топология</b></li><li>• <b>Отсутствие жёсткой структуры сети</b></li><li>• Однонаправленные и двунаправленные каналы связи</li><li>• Ограниченная пропускная способность</li><li>• Отсутствие контролируемой зоны</li></ul>	<ul style="list-style-type: none"><li>• <b>Частые разрывы каналов связи</b></li><li>• Предсказуемые шаблоны передвижений</li><li>• Отсутствуют ограничения на энергопотребление</li><li>• <b>Относительно высокие вычислительные мощности</b></li><li>• <b>Требования к низкой задержке при передаче данных</b></li></ul>	<ul style="list-style-type: none"><li>• <b>Высокая мобильность узлов</b></li><li>• Большие расстояния</li><li>• Коммуникации в пределах видимости</li><li>• <b>Относительно высокие вычислительные мощности</b></li></ul>	<ul style="list-style-type: none"><li>• <b>Ограниченная вычислительная мощность</b></li><li>• <b>Ограниченный энергоресурс</b></li><li>• Низкий уровень доступности узлов</li></ul>



# Доверие на основе сертификации



- Модель не предназначена для защиты от скомпрометированных узлов
- Не предназначена для защиты от внутреннего нарушителя



# Репутационные модели

$H_p(t)$  – история сетевых взаимодействий узла  $p \in P$  в момент времени  $t \in T$ .

$$H_p(t_1) \subseteq H_p(t_2), \quad t_1 \in T, t_2 \in T, t_1 < t_2.$$

Система узлов описывается множеством:

$$\{H_p(t) | p \in P\}.$$

Входные данные алгоритмов вычисления репутации:  $I \neq \{H_p(t) | p \in P\}$ .

Работа с абстракцией истории взаимодействий:

$$I = \text{Abstract}(H_p(t)).$$

Неполнота истории взаимодействий:

$$I = (H_p(t) \cap H_p(t'')) / H_p(t'), \quad t' < t'' < t.$$

Доступна информация не от всех узлов:

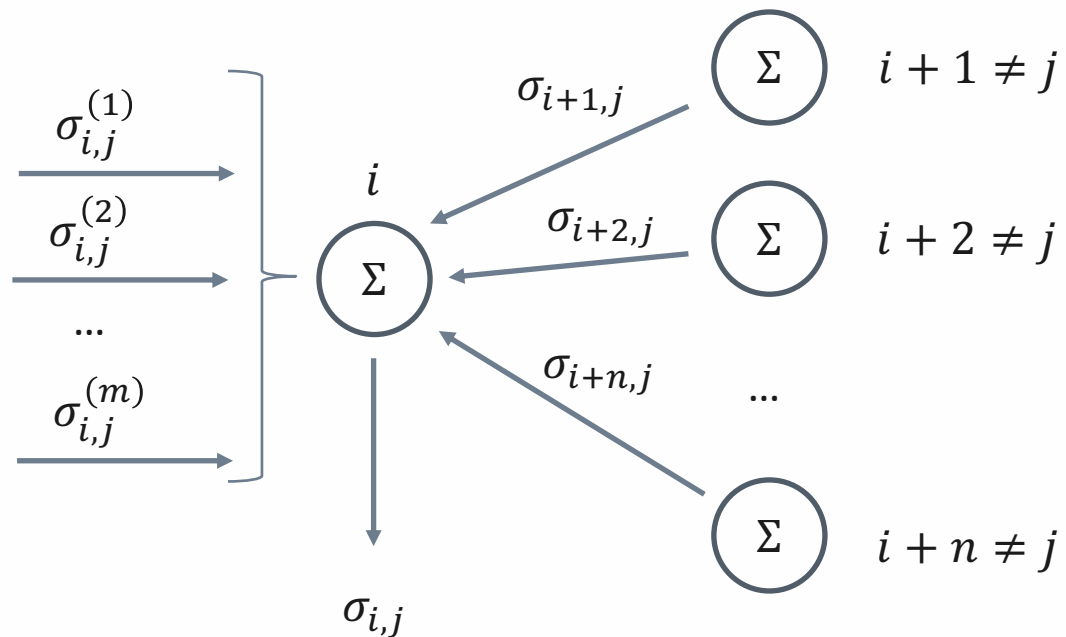
$$I = \{H_p(t) | p \in P', P' \subset P\}.$$



# Простой счёт

$\sigma_{i,j}^{(k)}$  – субъективная оценка  $k$ -ого взаимодействия узла  $i$  с узлом  $j$ .

$\sigma_{i,j}$  – субъективная оценка всех взаимодействий узла  $i$  с узлом  $j$ .



+ Простая модель  
+ Абсолютные оценки репутации

– Сложность оценки эффективности



# Транзитивная модель



+ Математический аппарат цепей Маркова

Репутационные оценки нормализуются и сводятся к матрице переходов цепи Маркова:

$$C = (c_{ij})_{i=1, j=1}^{m, m}$$

$$\vec{t} = \lim_{n \rightarrow \infty} C^n \vec{p}$$

- Не дают абсолютную оценку репутации
- Негативный отклик неотличим от нейтрального
- Вычислительная сложность



# Вероятностная модель

## Баесовские методы

- + Учёт ложных рекомендаций
- + Ранжирование рекомендаций по времени

## Бета-распределение

- + Транзитивное доверие

Субъективная логика:

$$P(x) + P(\bar{x}) + u = 1$$

- Бинарные рейтинги

## Распределение Дирихле

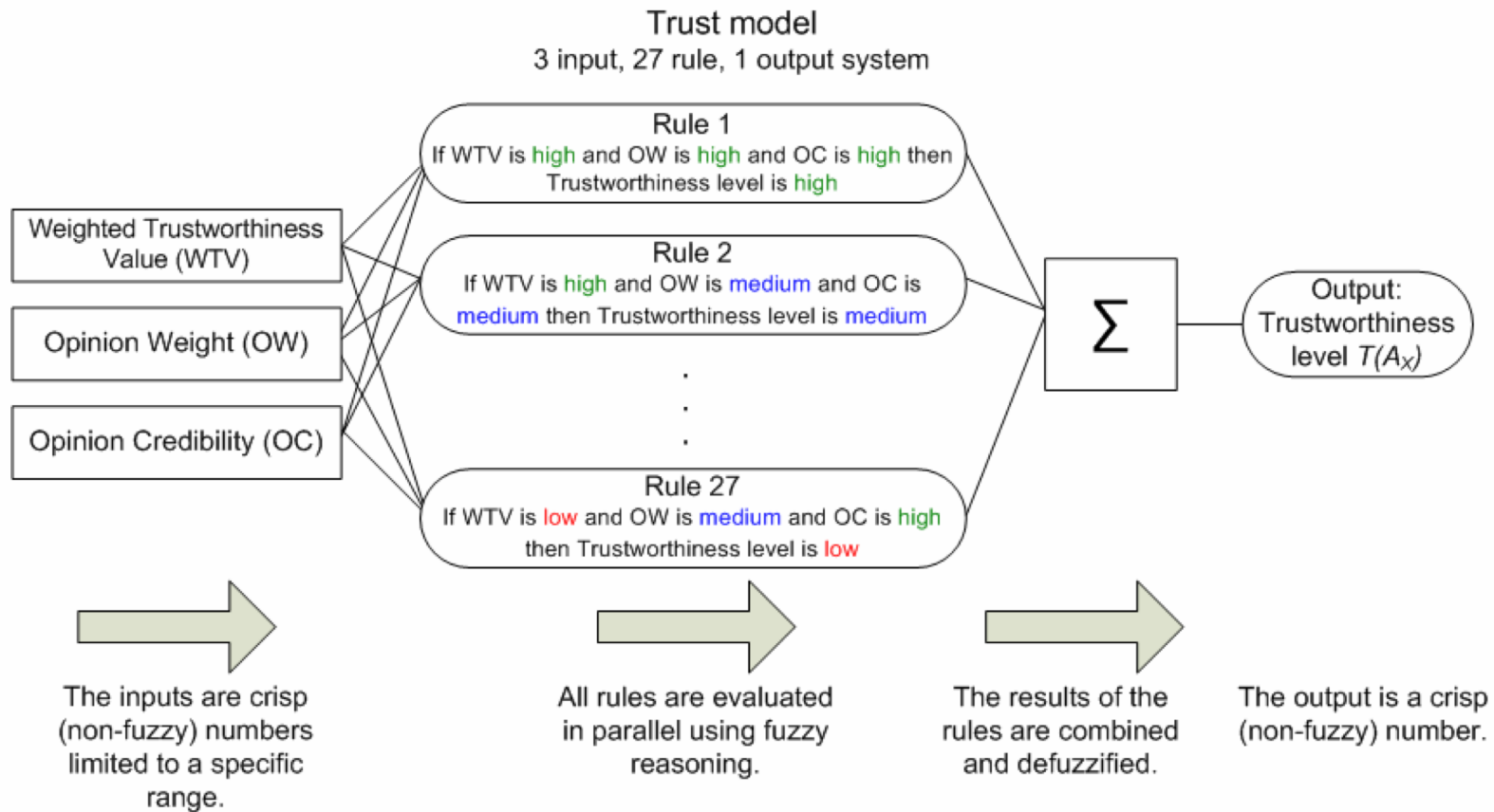
- + Рейтинги основаны дискретной заранее заданной шкале

- Отсутствие транзитивного доверия





# Нечёткая логика



Правила составляются экспертным путём

Аналитическое сравнение разных наборов правил представляется сложным.



# Промежуточные выводы

Доверие, основанное на сертификации статично и не защищает от скомпрометированных узлов или внутреннего нарушителя

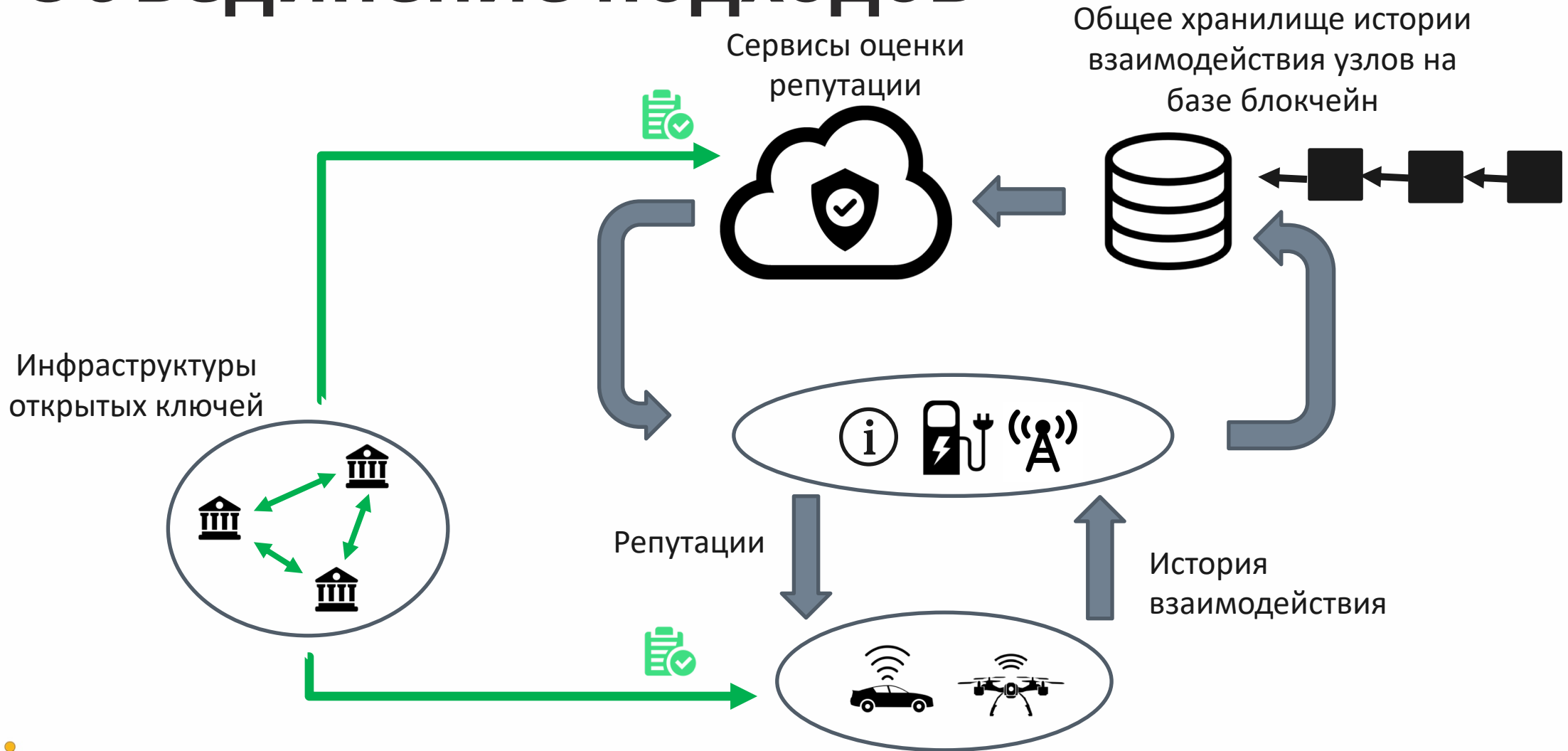
Оценка репутации в режиме онлайн затруднена

Необходимо обеспечить сложность смены идентификатора узла, к которому привязана оценка репутации

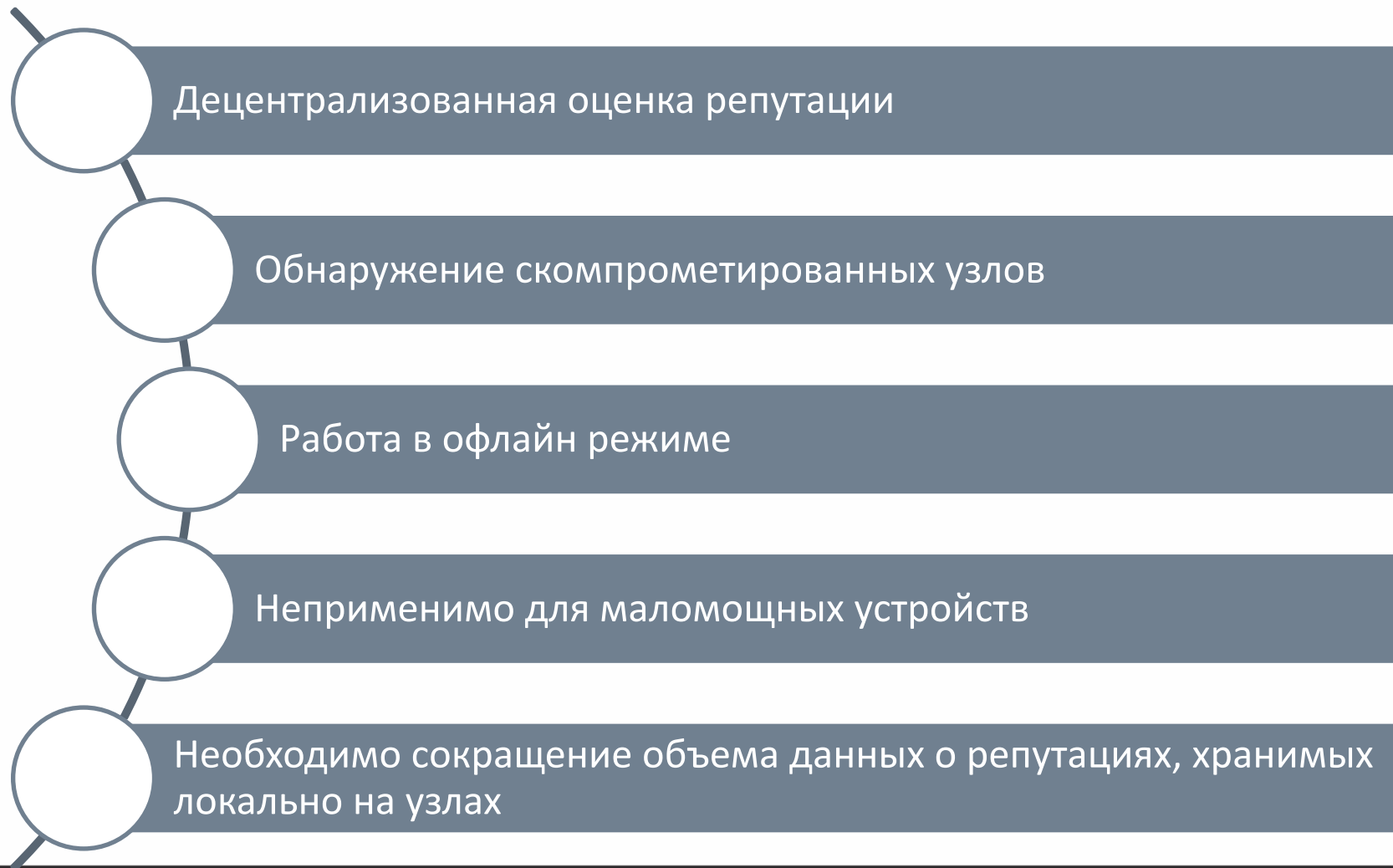
Необходимо обеспечить децентрализованный доступ к истории взаимодействия как можно большего количества узлов



# Объединение подходов



# Выводы о применимости подхода





# НЕОБИТ

Адрес: 195220 Санкт-Петербург, ул.  
Гжатская, д. 21, "Г"

Телефон: 535-88-67

Сайт: [www.neobit.ru](http://www.neobit.ru) / [www.необит.рф](http://www.необит.рф)