НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

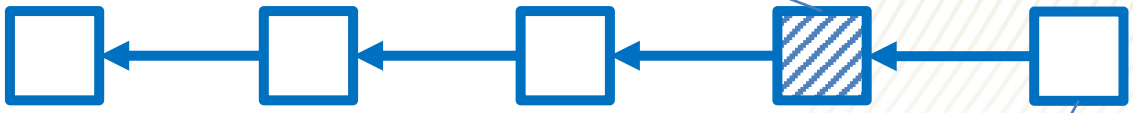
НЕОБИТ

Оценка защищённости блокчейн-систем от угроз, обусловленных неравномерным распределением вычислительных мощностей

Алексей Бусыгин
busygin@neobit.ru

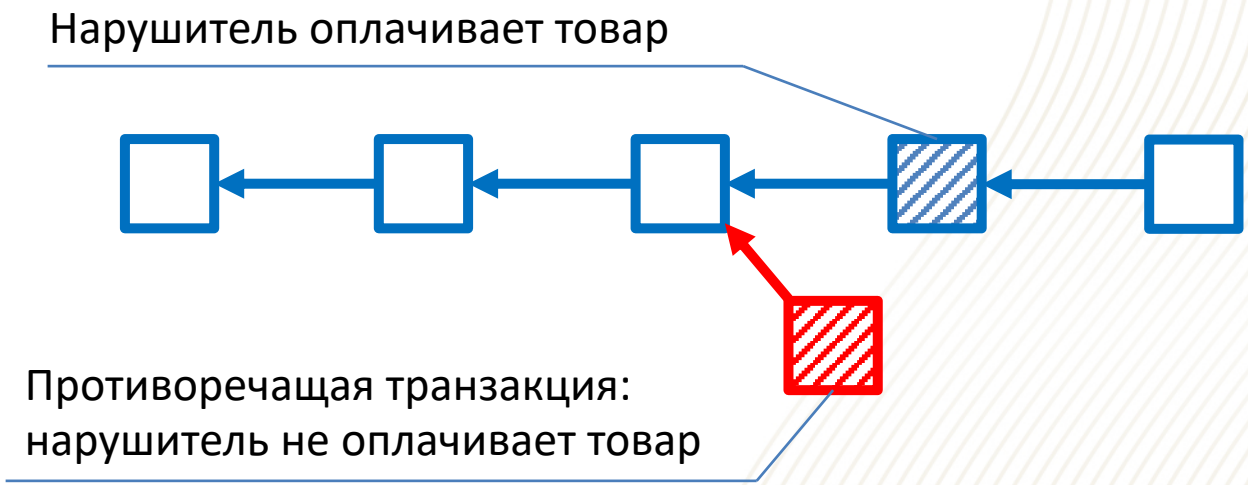
Атака большинства (1)

Нарушитель оплачивает товар

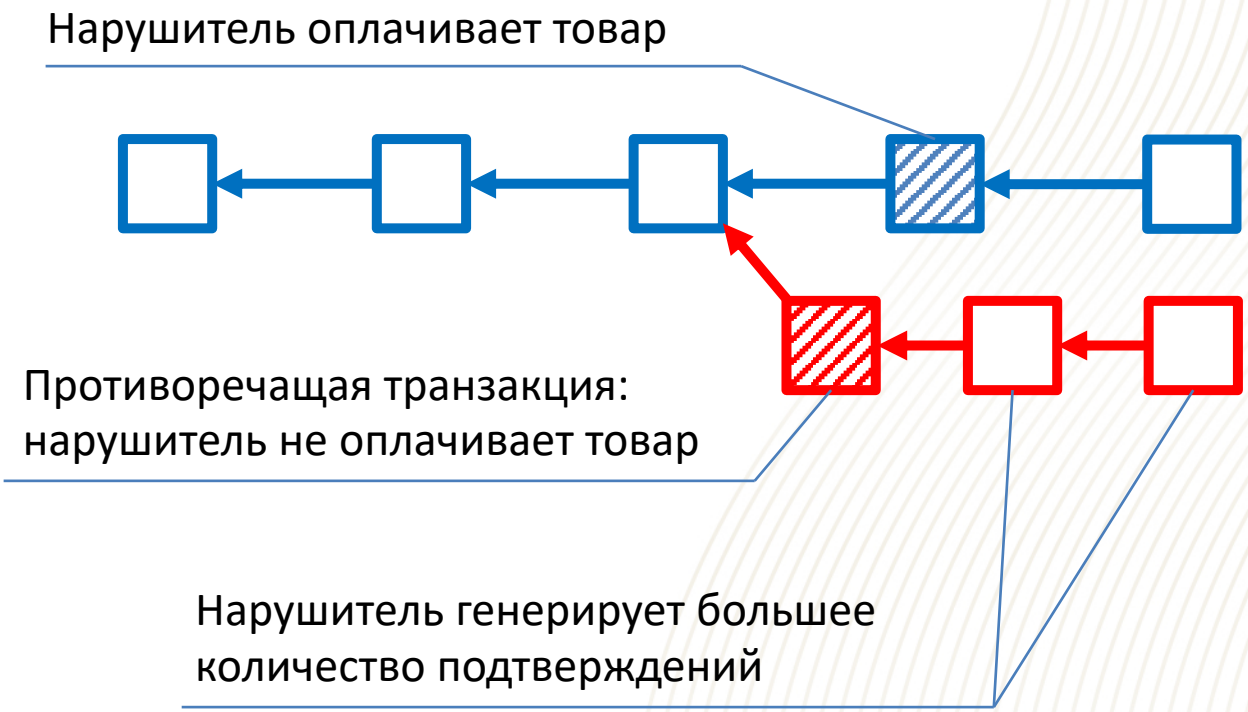


Подтверждение транзакции,
продавец передаёт товар нарушителю

Атака большинства (2)

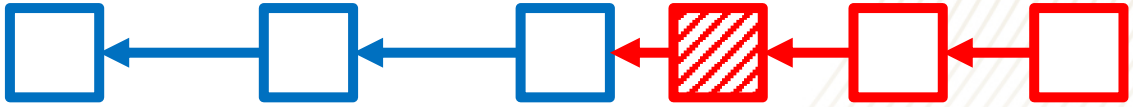


Атака большинства (3)



Атака большинства (4)

Цепочка с меньшим количеством подтверждений отбрасывается.



Нарушитель получает товар без оплаты.

Механизмы защиты

Механизм защиты	Недостатки
Контрольные точки	• Транзакции после контрольной точки не защищены
Штраф за отложенную публикацию блоков	• Не обеспечивает защищённость в блокчейн-системах с низкой вычислительной мощностью • Может приводить к разделению блокчейна (fork) • Время подтверждения транзакций значительно увеличивается
Удостоверяющий центр	• Введение единой точки отказа
Объединение блокчейн-систем (merged mining)	• Родительская блокчейн-система остаётся уязвимой к атаке

Вероятность успешной атаки

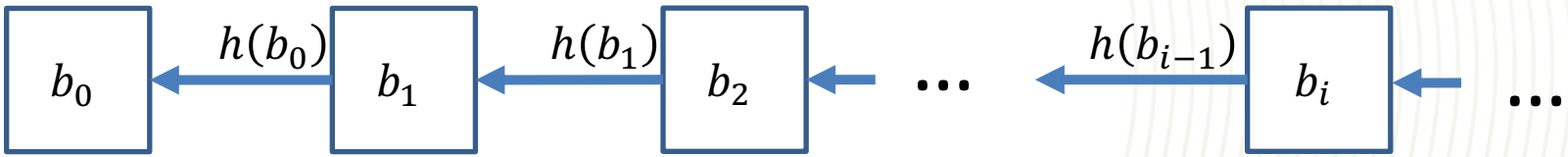
$$P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

$$\lambda = z\frac{q}{p}, \qquad p = 1 - q.$$

q – вероятность того, что следующий блок в цепочке будет сгенерирован нарушителем.

Применение оценки на практике затруднено, т.к. параметр q неизвестен.

Модель блокчейн-системы



$$b_i \in B = H \times N \times T \times D$$

Хеш-образ предыдущего блока $h(b_{i-1})$

$\#N = 2^n$

$n \in N$

$h(b_i(n)) \leq h_{\max}$

$h_{\max}$ – константа

Временная метка

Данные

Блокчейн-система замкнута: общая вычислительная мощность постоянна.

Оценка общей вычислительной мощности блокчейн-системы

Вероятность успешной генерации i-ого блока (выбора $n \in N$, такого что $b_i(n) \leq h_{\max}$):

$$p = \frac{h_{\max}}{2^n}$$

Математическое ожидание количества попыток генерации нового блока:

$$M = \frac{2^n}{h_{\max}}$$

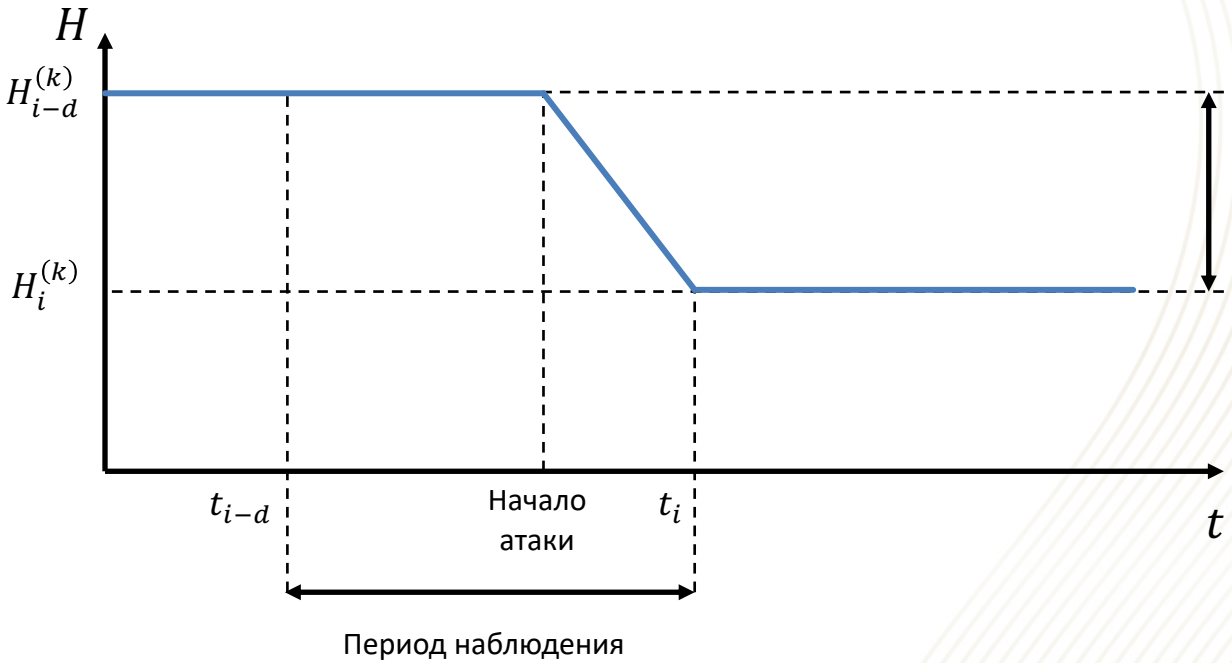
Оценка вычислительной мощности блокчейн-системы (хеш/с) в момент генерации i-ого блока:

$$H_i = \frac{M}{t_i - t_{i-1}} = \frac{2^n}{h_{\max} \cdot (t_i - t_{i-1})}$$

Усреднённое значение для k последних блоков:

$$H_i^{(k)} = \frac{1}{k} \sum_{j=0}^{k} H_{i-j}$$

Оценка возможностей нарушителя



$$\Delta H = \max\left(\left\{H_n^{(k)}\right\}_{n=i-d}^{i}\right) - H_i^{(k)}$$

$$q = \frac{\Delta H}{\max\left(\left\{H_n^{(k)}\right\}_{n=i-d}^{i}\right)} \quad \rightarrow \quad P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

- Оценка вероятности реализации угроз, обусловленных неравномерным распределением вычислительных мощностей

$$P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

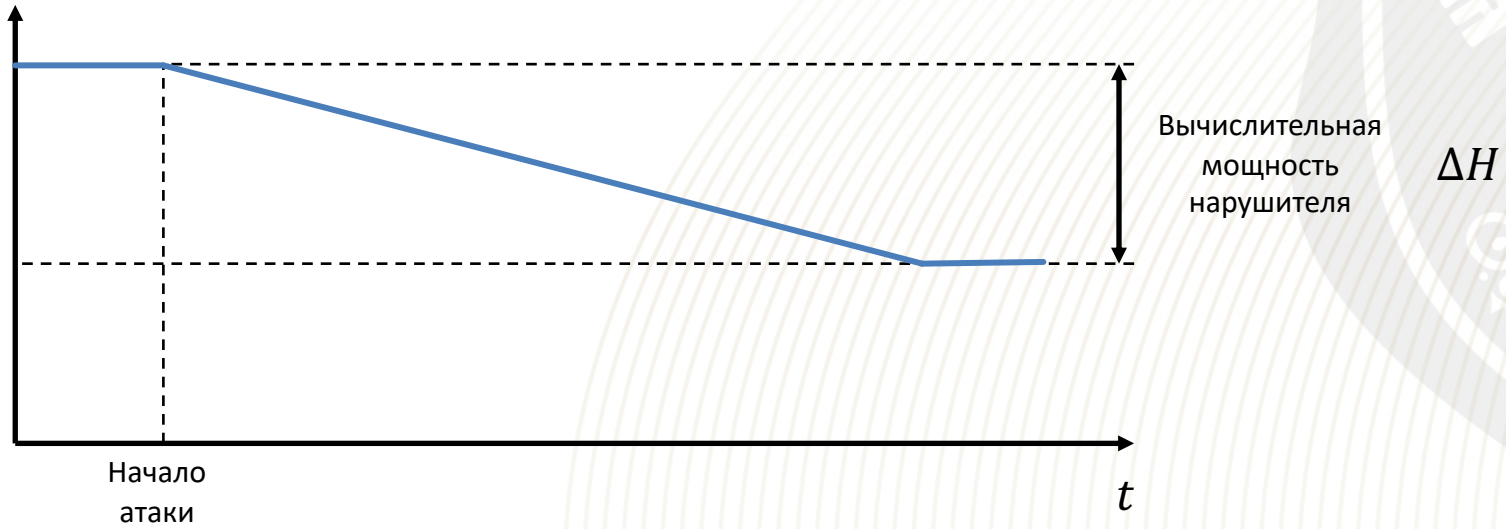
- Индикатор начала атаки, сигнал к фиксированию контрольной точки

- Способ выявления последовательностей блоков сгенерированных нарушителем ($H_i^{(k)}$ для последовательности блоков нарушителя равна ΔH)

Ограничения предложенного метода

- Модель не применима для не замкнутых систем (нарушитель может купить/арендовать высокопроизводительный вычислительный кластер)

- Выявление атаки при медленном снижении общей вычислительной мощности блокчейн-системы:



НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

НЕОБИТ

СПАСИБО ЗА ВНИМАНИЕ!