УДК 004

МЕТОД АНАЛИЗА ПРИНАДЛЕЖНОСТИ АККАУНТОВ ОДНОМУ ВЛАДЕЛЬЦУ В БЛОКЧЕЙН-СЕТЯХ

И. З. САФИНА
Научный руководитель А. Н. КАБИРОВА, канд. техн. наук, доц.
Казанский национальный исследовательский технический университет им. А. Н. Туполева-КАИ
Казань, Россия

В современном мире блокчейн-технологии развиваются очень быстрыми темпами. Это, в свою очередь, приводит к развитию мошеннических действий в данной области. В связи с этим для обеспечения безопасности и конфиденциальности информации представляется актуальным задача разработки метода анализа принадлежности аккаунтов одному владельцу в блокчейн-сетях.

В основу разработанного метода легли элементы уже известных методик: эвристического, графового анализа и метода анализа временных интервалов. Для разработки метода были применены 14 метрик (правил). Данные метрики используются для вычисления вероятности связи между указанными аккаунтами. При этом метрика имеет свою степень важности, и за срабатывание метрики присваивается фиксированный балл (табл. 1). Максимальная сумма баллов равняется 20.

Табл. 1. Метрики выявления связей

Метрика	Количество баллов	Степень важности
Первый адрес взаимодействия после первого пополнения	1	Средняя
Множества общих транзакций, выполненных подряд после первого пополнения	6	Очень высокая
Транзакции в один и тот же час после первого пополнения	1	Средняя
Прямые транзакции между кошельками	1	Ключевая
Сходство текущего баланса	1	Средняя
Сходство количества транзакций	1	Средняя
Первое пополнение с одного источника (центральной биржи)	1	Средняя
Первое пополнение с одного источника	1	Ключевая
Первое пополнение на схожую сумму	1	Средняя
Сходство суммы первой транзакции	1	Средняя
Первая транзакция в один и тот же день	1	Средняя
Первая транзакция в один и тот же час	1	Средняя
Взаимодействие с одними и теми же адресами	2	Высокая
Сходство суммы всех переводов	1	Средняя

Как видно из табл. 1, метрики «Прямые транзакции между кошельками» и «Первое пополнение с одного источника» являются ключевыми и напрямую

влияют на результат расчета вероятности. Метод расчета вероятности принадлежности аккаунтов одному владельцу заключается в следующем: проверить, сработало ли хотя бы одно из ключевых правил.

1. Ключевое правило не сработало. Тогда берется сумма баллов сработавших правил и делится на 22.

2. Ключевое правило сработало. Тогда считается общая сумма баллов для всех сработавших правил, умножается на соответствующий множитель (табл. 2) и делится на 22.

Табл. 2. Взаимосвязь количества баллов и множителя

Количество баллов	Множитель	Количество баллов	Множитель	Количество баллов	Множитель	Количество баллов	Множитель
1	17,6	6	3,3	11	1,92	16	1,35
2	8,8	7	2,9	12	1,78	17	1,29
3	6,23	8	2,55	13	1,64	18	1,22
4	4,67	9	2,32	14	1,52	19	1,157
5	3,96	10	2,11	15	1,44	20	1,1

Таким образом, методика расчета вероятности позволяет учитывать вес каждого правила с учетом их значимости. Ключевые правила существенно увеличивают вероятность связи между адресами, в то время как остальные правила медленно увеличивают вероятность, подтверждая принадлежность адресов одному владельцу.

Необходимо отметить, что все использованные цифры в расчетах, а также перечень требуемых метрик были определены с помощью экспертов, работающих в этой сфере.

После определения всех правил разработанный метод был реализован в виде веб-приложения на языках TypeScript и HTML.

На начальном экране веб-приложения пользователь видит заголовок «Анализ кошельков» и инструкцию по вводу адресов кошельков. Адреса должны начинаться с префикса '0x' и быть записаны в шестнадцатеричной системе счисления, содержащей 40 символов. На этом этапе пользователи могут добавить или удалить поля для ввода адресов. Минимальное количество полей – 2, а максимальное – 100, при этом в поле ввода можно вставить заранее скопированные адреса. При вводе адресов система автоматически проверяет их корректность. После нажатия на кнопку «Отправить» приложение начинает процесс получения и анализа транзакций, о чем свидетельствует появление соответствующей надписи на экране.

Окно с результатами анализа введенных адресов содержит все пары адресов, вероятность принадлежности этих пар адресов одному владельцу в процентах, а также список сработавших правил для данных пар адресов.