

УДК 004.89

ОБНАРУЖЕНИЕ НЕЛЕГАЛЬНЫХ ТРАНЗАКЦИЙ БИТКОЙНА ПРИ ПОМОЩИ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ

С.А. Ильина¹

Научный руководитель: доцент, к.ф.-м.н. М.Е. Семенов^{1,2}

¹Национальный исследовательский Томский политехнический университет,

Россия, г. Томск, пр. Ленина, 30, 634050

²Научно-технологический университет «Сириус»,

Россия, Краснодарский край, пгт Сириус, проспект Олимпийский, д. 1, 354340,

E-mail: sai8@tpu.ru

DETECTION OF ILLICIT BITCOIN TRANSACTIONS USING GRAPH NEURAL NETWORKS

S.A. Ilina¹

Scientific Supervisor: Assoc. Prof., PhD. M.E. Semenov^{1,2}

¹Tomsk Polytechnic University, Russia, Tomsk, Lenin str., 30, 634050

²Sirius University of Science and Technology, Russia, Krasnodar region, Sirius, Olimpiyskiy str. 1, 354340

E-mail: sai8@tpu.ru

Abstract. This article discusses possible methods for solving the problem of classifying bitcoin transactions into licit and illicit ones. The proposed options for solving this problem of anti-money laundering analytics based on graph neural networks with different architecture. The results of computational experiments using data from the Elliptic Data Set are presented.

Введение. Главным преимуществом криптовалют, начиная с появления биткойнов, стала возможность совершения недорогих анонимных переводов как внутри одной страны, так и через границы. Однако анонимностью криптовалют стали пользоваться и злоумышленники для нелегального оборота товаров и услуг. Но несмотря на то, что анонимность позволяет преступникам скрываться, база транзакций криптовалют открыта, что делает возможным проведение AML-аналитики (Anti-money laundering) с целью выявления нелегальных транзакций.

Данная работа посвящена развитию подходов решения задач AML-аналитики – исследованию возможности объединения структуры графовых нейронных сетей (Graph Neural Network, GNN) с алгоритмом случайного леса (random forest, RF) на примере задачи классификации транзакций биткойна.

Данные. В статье [1] анонсирован открытый набор данных – Elliptic Data Set [2]: граф с $n=203\,769$ вершинами, соответствующих транзакциям биткойна, и 234 355 рёбер, соответствующих потокам биткойна. Каждая вершина имеет 166 признаков и размечена на классы: 1 – нелегальные (4 545 вершин), 2 – легальные (42 019 вершин), *unknown* – неизвестные. Отношение миноритарного класса к мажоритарному составляет: 0,1, что говорит о несбалансированности выборки. Также набор данных содержит 49 различных временных шагов, распределённых равномерно с интервалом около двух недель, каждый шаг содержит одну компоненту связности графа, несвязанную с другими временными шагами, на одном шаге содержатся транзакции, которые были зафиксированы с интервалом не более трёх часов друг от друга.

Используемые структуры и алгоритмы. В данной работе предлагается несколько вариантов структуры GNN для решения задачи классификации: свёрточные графовые сети (Graph Convolution Network, GCN), графовые сети внимания (Graph Attention Networks, GATs).

Основной принцип GNN заключается в реализации некоторой функции τ , отображающей граф G и один из его узлов в m -размерное Евклидово пространство [3]: $\tau(G, i) \in \mathbf{R}^m, i = 1, 2, \dots, n$. В случае набора данных Elliptic Data Set мы решаем задачу бинарной классификации: каждой i -ой вершине входного графа G необходимо приписать метку: 1 – нелегальная или 2 – легальная.

При обучении GNN в общем случае применяется какая-либо вариация алгоритма прямого распространения, основа которого заключается в том, что на каждой итерации алгоритма вершины графа агрегируют информацию о своих соседях соответствующего уровня. Таким образом, по мере повторения этого процесса вершины получают всё больше информации от более удалённых вершин. Информация о соседях некоторой вершины поступает в функцию агрегации (1), где по некоторому правилу суммируются векторы состояния вершин. Функция агрегации имеет вид:

$$AGG\left(\left\{h_u^{(k-1)}\right\}_{u \in N(v)}\right) = f\left(h_u^{(k-1)}\right), \quad (1)$$

где $h_u^{(k-1)}$ – вектор признаков вершины u на $(k-1)$ шаге, $N(v)$ – множество соседей вершины v , f – заданное правило суммирования векторов состояния. Затем полученные значения передаются в функцию обновления состояния вершины v (2), которая по некоторому правилу, изменяет вектор состояния данной вершины:

$$h_v^{(k)} = UPDATE^{(k)}\left(h_v^{(k-1)}, AGG^{(k)}\left(\left\{h_u^{(k-1)}\right\}_{u \in N(v)}\right)\right). \quad (2)$$

На выходе алгоритма получают граф с исходной топологией, но с дополнительными признаками вершин, которые определяют принадлежность вершины к какому-либо классу [4].

Кратко опишем особенности использованных моделей нейросетей. GCN включают свёрточные графовые слои для уменьшения пространства признаков входного графа. Последовательное применение нескольких таких слоёв позволяет в конечном итоге получить граф с пространством признаков требуемой, в рамках задачи, размерности. Таким образом, данный тип графовых нейронных сетей позволяет обрабатывать большие графы, а также графы, вершины или рёбра которых имеют большое количество признаков. Архитектура GAT позволяет использовать модели внимания для решения задач на графах. Сети GAT содержат в себе графовые слои внимания (graph attentional layers), которые производят агрегацию состояний соседей вершины с учётом коэффициентов внимания α [5]:

$$AGG\left(\left\{h_u^{(k-1)}\right\}_{u \in N(v)}\right) = \sum_{u \in N(v)} \alpha_{u,v}^{(k-1)} h_u^{(k-1)}.$$

Вычислительные эксперименты и их обсуждение. Согласно экспериментам [1] алгоритм RF превосходит по точности GCN: 95,6% и 81,2% соответственно. Однако в таком случае не используется вся информация, хранящаяся в структуре графа. Поэтому было выдвинуто предположение о возможном повышении эффективности классификации GCN путём объединения структуры сети с алгоритмом RF. В качестве входных данных был выбран 27 временной шаг из набора Elliptic Data Set [2]. Граф с 1653 вершинами и 1717 рёбрами разделён случайным образом на обучающую и валидационную выборки в соотношении 85 к 15. В первом случае, проводилась классификация при помощи свёрточной GNN, состоящей из трёх слоёв. Первый слой сворачивает пространство признаков до 128, второй до 2 и третий

до 1 – класса транзакции. В качестве функции активации в GCN используется полулинейный элемент – ReLU, для всех слоёв, кроме последнего, где используется логистическая функция – сигмоида. Использование логистической функции на последнем слое GCN позволяет привести значения признаков всех вершин к значению от 0 до 1, после чего к данному вектору применяется алгоритм случайного леса для определения класса вершин – 1 или 2. Данная конфигурация сети за 100 эпох обучения показала точность: 98,6 % на этапе обучения, 96,8 % на этапе валидации. Эти результаты действительно имеют более высокую точность, относительно классификации только случайным лесом или только GCN.

Следующая серия экспериментов была посвящена классификации при помощи GAT сети состоящей из трёх графовых слоёв внимания. В этой конфигурации сети используется та же комбинация функций активации и алгоритма случайного леса, что и в случае с GCN. Данная модель за 100 эпох обучения показала точность 98,9 % на обучающей выборке и 97,6 % на валидационной. Результаты классификации приведены в Таблице 1: модель с применением сети GAT показывает меньшее число ошибок в случаях определения легальных транзакций. В остальном представленные модели дают близкие результаты.

Таблица 1

Матрицы ошибок

Класс	Этап обучения				Этап валидации			
	GCN		GAT		GCN		GAT	
	1	2	1	2	1	2	1	2
1	63	9	62	10	10	3	10	3
2	66	1267	7	1326	9	226	3	232
	GCN+RF		GAT+RF		GCN+RF		GAT+RF	
1	66	6	66	6	10	3	10	3
2	13	1320	9	1324	5	230	3	232

Заключение. Проведённые нами вычислительные эксперименты подтвердили предположение о возможности повышении точности классификации при использовании комбинации GNN с алгоритмом случайного леса. При классификации графовых структур, в том числе AML-анализе, важно использовать всю информацию, отражённую в графе, не ограничиваясь использованием пространства признаков.

Финансирование проекта осуществлялось Министерством науки и высшего образования Российской Федерации (Соглашение № 075-10-2021-093; Проект FMF-RND-2122).

СПИСОК ЛИТЕРАТУРЫ

1. Weber M. et. al. (2019), Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. KDD '19 Workshop on Anomaly Detection in Finance, New York, USA, 7 pp.
2. Elliptic Data Set [Электронный ресурс]. – Режим доступа: <https://www.kaggle.com/datasets/ellipticco/elliptic-data-set>, свободный (дата обращения: 19.03.2023)
3. Scarselli F. et. al. (2009) The graph neural network model, IEEE Transactions on Neural Networks, 20(1), pp. 61-80.
4. Hamilton W.L. et. al. (2017) Inductive Representation Learning on Large Graphs. NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems, pp. 1025–1035
5. Veličković P. et. al. (2017) Graph Attention Networks. 6th International Conference on Learning Representations.