TGC: Transaction Graph Contrast Network for Ethereum Phishing Scam Detection

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

ACSAC 2023
December 4-8, 2023 • Austin, Texas, USA

Sijia Li, Gaopeng Gou, Chang Liu, Gang Xiong, Zhen Li, Junchao Xiao, Xinyu Xing

Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences
Northwestern University

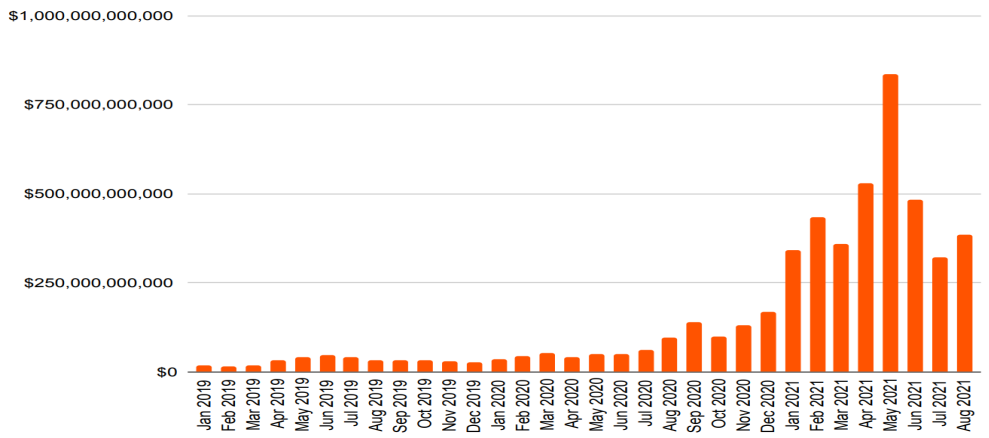
Background

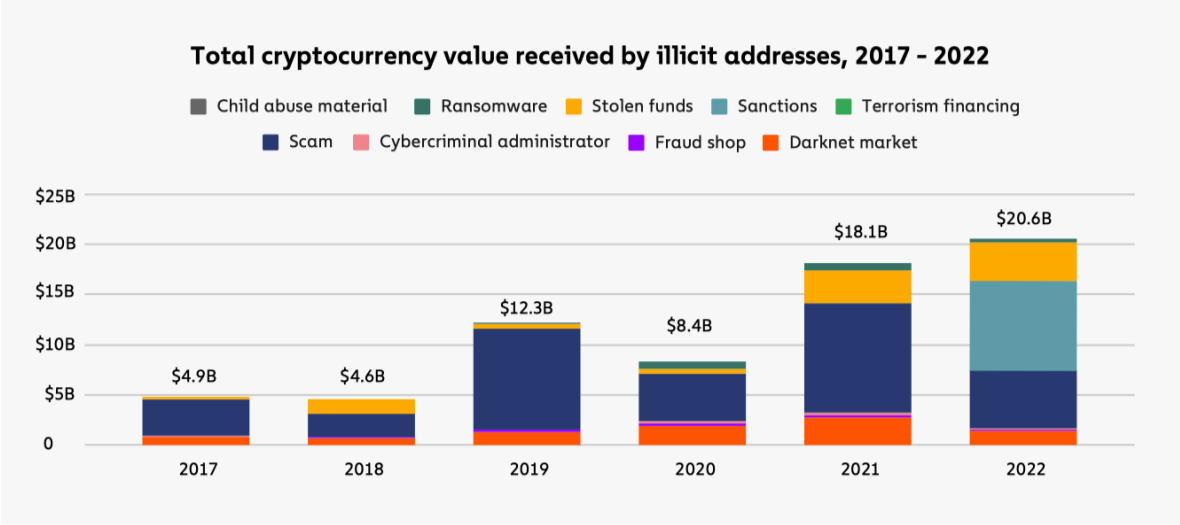
The Growth of Scam on Cryptocurrency

- Cryptocurrency-based crime hit a new all-time high in 2022, with illicit addresses receiving $20.6 billion over the course of the year.

- the rise of decentralized finance (DeFi) and the allure of blockchain's anonymity have given rise to a plethora of cybercrimes

- **Increased focus on cryptocurrency security issues**

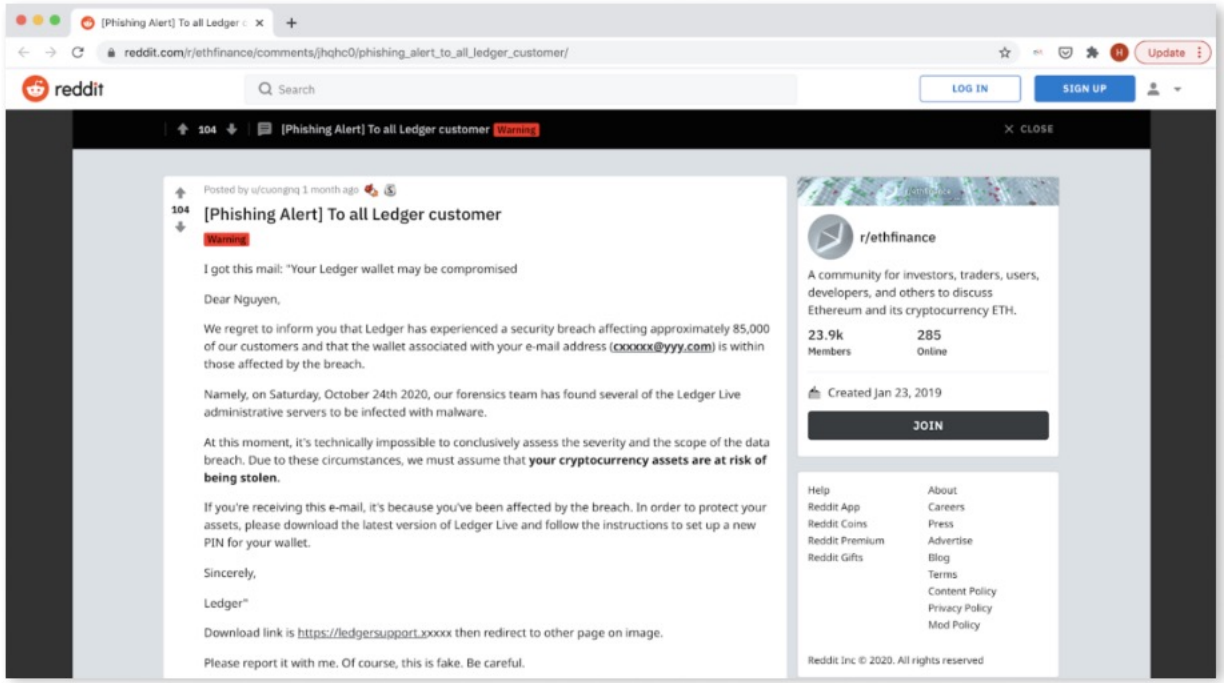




Background

Phishing Scams on Ethereum

- high visibility and lots of potential victims
- victims lost $645,000 within the first week of the phishing campaign, and the attacker's illegal profits exceeded $3,000,000 in just one month
- phishing scams are the most deceptive scams



A reddit post describing the phishing emails.

- **identifying phishing scams on Ethereum becomes a crucial research topic**

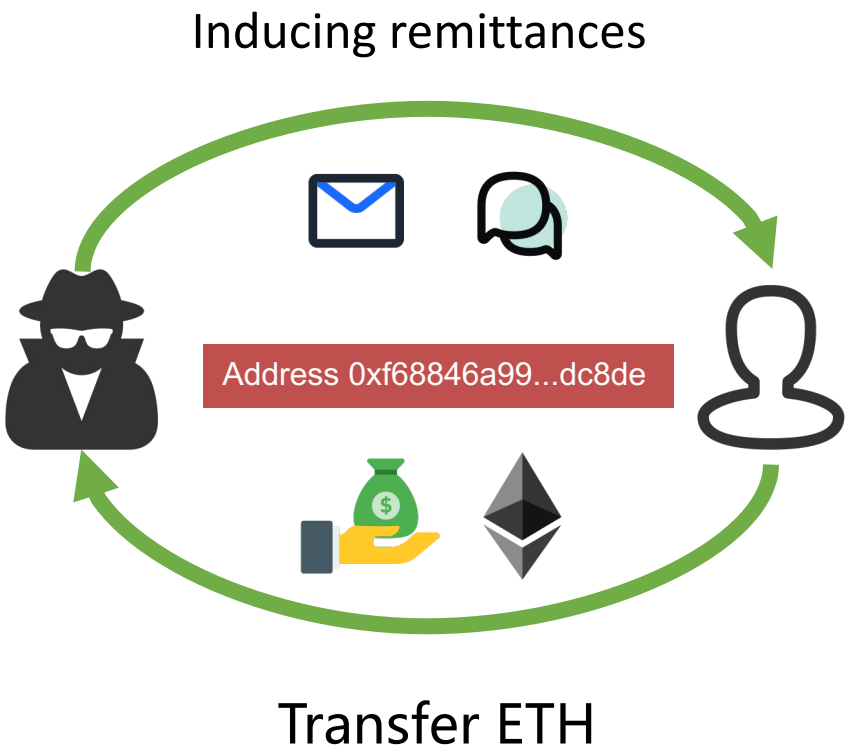
Background

Phishing

- exploits user vulnerabilities to obtain personal property and confidential information

Phishing Scams on Ethereum

- Take high-reward propaganda to induce remittances (email/chat)
  - offering additional Ether coins as incentives
  - visit fraudulent platforms or websites
  - promise high returns if purchase digital assets
- **no fixed platforms pattern!**

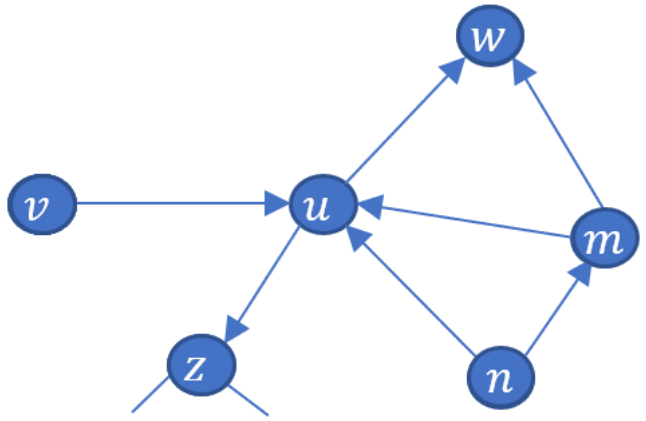


Limitation

Task

The address of Ethereum ----> the node in the graph
Transaction relationship ----> edge between nodes

Learn efficient node representations through the transaction network and classify nodes



$$\mathcal{G} = (\mathcal{V}, \mathcal{E})$$

Traditional Machine Learning

- Using manual-designed features as node embedding
- Limitation :
  Rely on professional knowledge to extract features
  Inefficient and non-automated

Limitation

Network Representation Learning

- Using graph neural network to mining deep features
- Limitation :

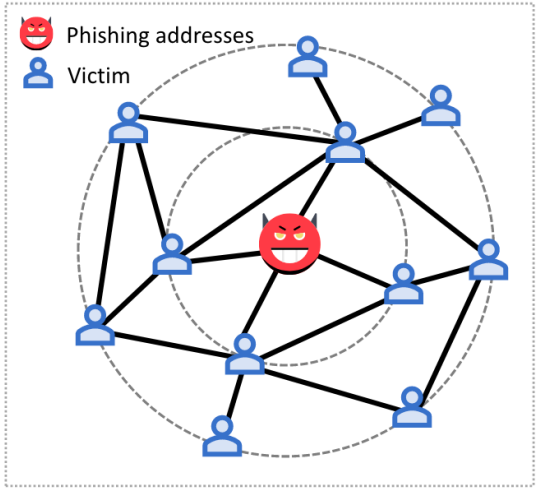
  overlook the unique challenges of Ethereum phishing scams

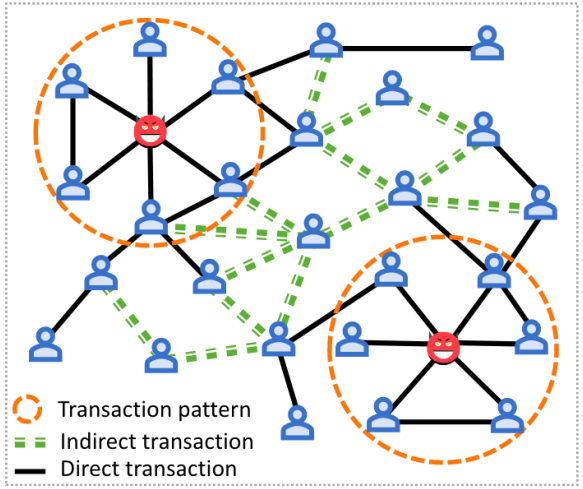
  Weak node representation

] unsatisfactory performance

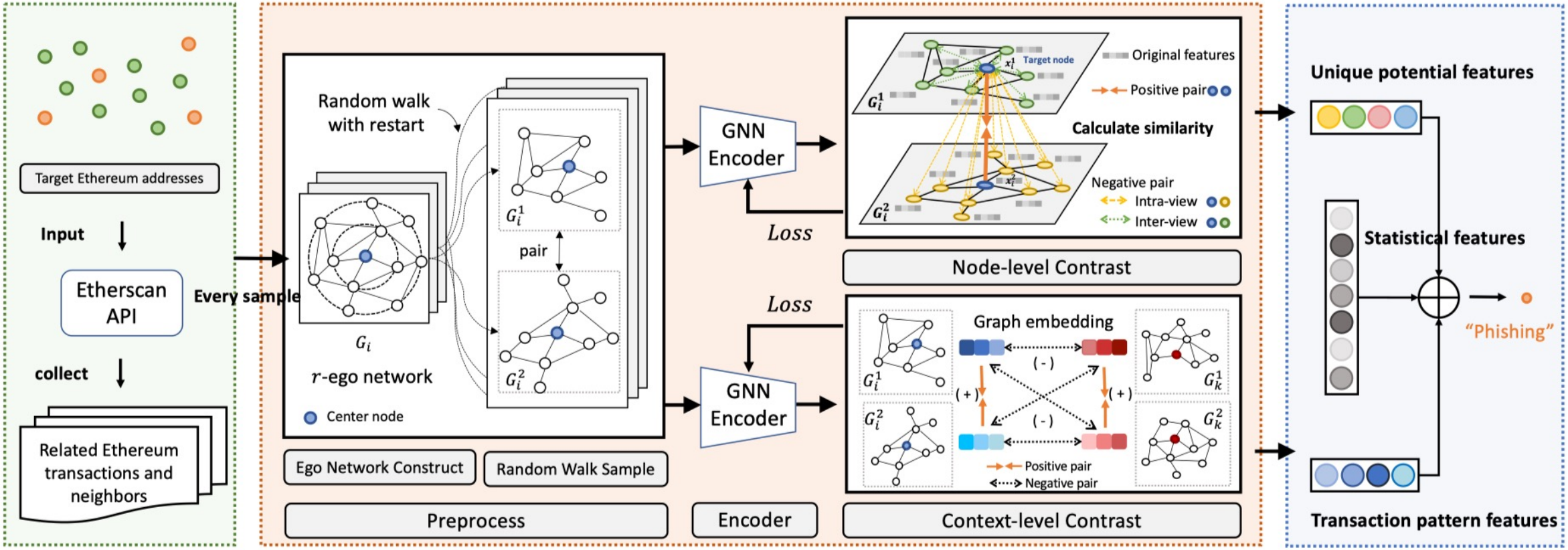
Challenges

- **The natural camouflage**
  - 97.99% of neighbors are normal addresses
- **Sparsity of distribution**
  - low proportion (0.345%)
  - sparse distribution
- **Large scale and dynamic nature**
  - Ethereum transaction network is both vast and dynamic





TGC



Data collection

Collect relevant addresses and transactions

Transaction Graph Contrast Network

construct the sample centered r -ego networks and build two different views

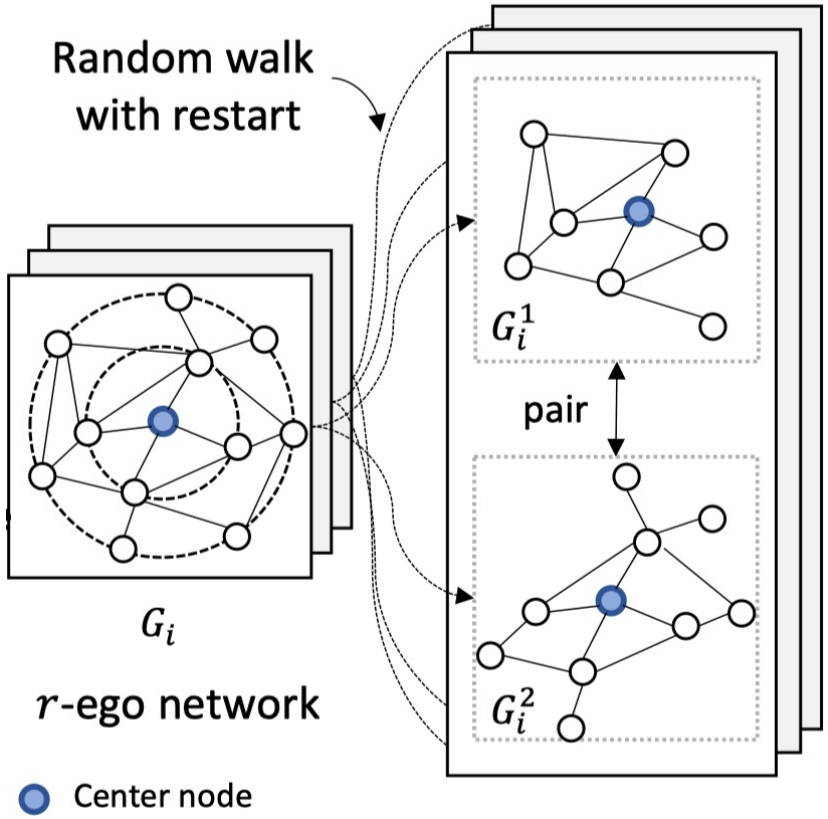
use two designed contrastive modules learn the discriminative representation of phishing addresses

Phishing address detection

Combine the outputs and feed into the classifier to get the result

TGC

Ego Network Construct & Subgraph Sampling

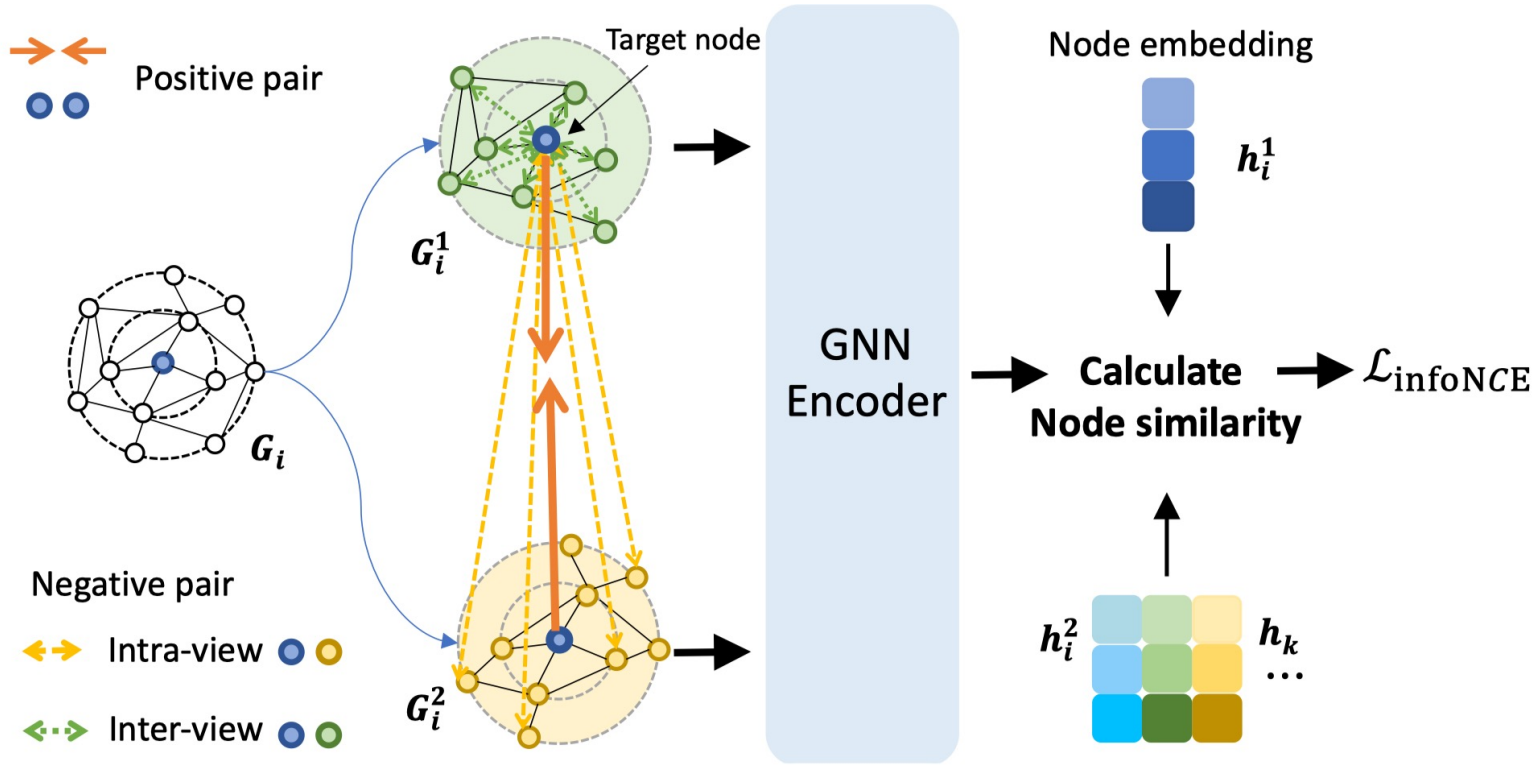


- Construct a local substructure of each sample node
- " r-ego network "
  consists of the r-order neighbors of the central sample node and the connection relationships between them
- Random walk with restart (RWR) sampling strategy
  - each ego network is sampled twice
  - generating two local subgraphs
- Each sample gets a carefully designed pair of "local subgraph vs. local subgraph"

Learn unique characteristics different from their neighbors

TGC

Node-level Contrast



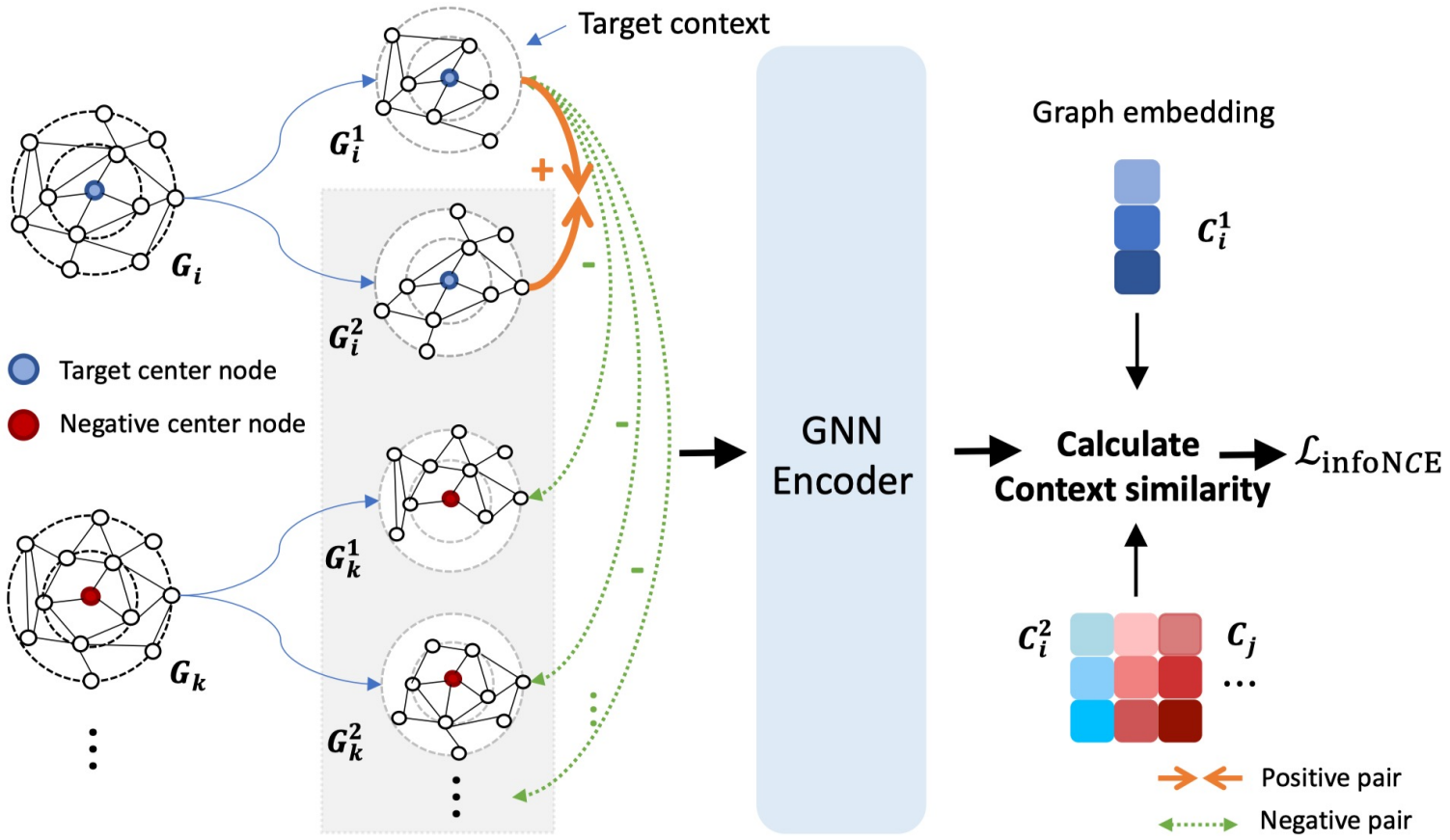
- Instance pair
  " Target node vs. node "
- Treat neighbors as the negative samples
  - Intra-view negative pair
  - Inter-view negative pair
- Positive samples are the representation of the same node in different views
- Contrastive Loss

$$\ell_n\left(\mathbf{x}_i^1\right) = -\log \frac{e^{\theta\left(\boldsymbol{h}_i^1, \boldsymbol{h}_i^2\right)/\tau}}{e^{\theta\left(\boldsymbol{h}_i^1, \boldsymbol{h}_i^2\right)/\tau} + \sum_{k \neq i} e^{\theta\left(\boldsymbol{h}_i^1, \boldsymbol{h}_k\right)/\tau}}$$

Learn unique characteristics different from their neighbors

TGC

Context-level contrast



- Instance pair
  " Target context vs. context "
- Treat subgraphs which generated by different r-ego networks as a negative pair
- Generated by the same r-ego networks as a positive pair
- Contrastive Loss

$$\ell_c\left(\mathcal{G}_i^1\right) = -\log \frac{e^{(C_i^{1\top} C_i^2)/\tau}}{\sum_{j=1}^{N} e^{(C_i^{1\top} C_j)/\tau}}$$

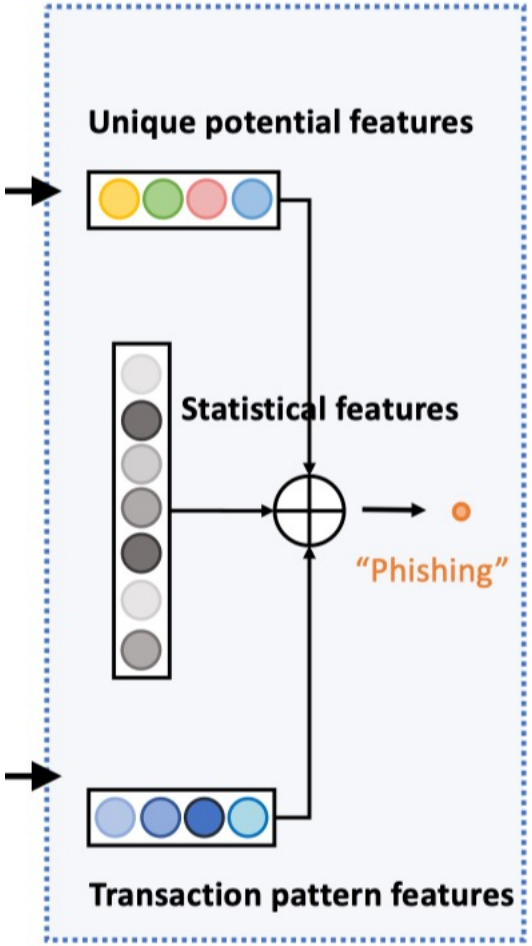
Capture the transactional structural patterns behind phishing and normal addresses

TGC

Phishing Addresses Detection

Final Node Representation – concat the three features

- **Unique potential features**
  - Learned from the Node-level Contrast module
- **Transaction pattern features**
  - Learned from the Context-level Contrast module
- **Statistical features**
  - Extract from subgraph
- **Classifiers**
  - XGBoost



Phishing address detection

Evaluation - Dataset

Data Collection

- As of March 2023, 5,639 phishing addresses.
- randomly select 25,000 active normal addresses
- Labeling – Etherscan
- labeled nodes being the central nodes, Two-layer BFS
- 9,237,535 Ethereum addresses and 219,927,673 transaction records.

Dataset	#Total Nodes	#Labeled	#Edges	#Average Degree
D_1	30,000	106	24,965,770	832.2201
D_2	40,000	140	27,642,111	691.0701
D_3	50,000	166	31,597,197	631.9566
D_4	60,000	207	33,072,308	551.2143
D_5	70,000	238	34,450,265	492.1537
D_6	80,000	269	35,872,229	450.3111
D_p	9,237,535	5,639	219,927,673	23.8080

- Generate a large graph based on the transaction information crawled around all labeled phishing nodes, and select the largest connected component
- Sample with random walks to obtain subgraphs of different sizes

Evaluation - Baselines and Metrics

Baselines

Feature-based - Features only [1] are 219-dimensional statistical features from the node's 1-order and 2-order neighbors.

Random walk-based - DeepWalk [3], Node2Vec [4], and LINE [5] **.** both topological information and node attributes are involved.

Deep learning-based - SDNE [6], E-GCN [7], GraphSAGE [8] , TSGN[2] and GAT [9]

Metrics

- Recall
- Precision
- F1-score

[1] Weili Chen, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, and Yutong Lu. 2020. Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem.. In IJCAI. 4506–4512.
[2] Wang, Jinhuan, et al. "Tsgn: Transaction subgraph networks for identifying ethereum phishing accounts." *Blockchain and Trustworthy Systems: Third International Conference, BlockSys 2021, Guangzhou, China, August 5–6, 2021, Revised Selected Papers 3*. Springer Singapore, 2021..
[4] Aditya Grover and Jure Leskovec. 2016. node2vec: Scalable feature learning for networks. In ACM SIGKDD. 855–864.
[5] Jian Tang, Meng Qu, Mingzhe Wang, Ming Zhang, Jun Yan, and Qiaozhu Mei. 2015. Line: Large-scale information network embedding. In WWW. 1067–1077.
[6] Daixin Wang, Peng Cui, and Wenwu Zhu. 2016. Structural deep network embedding. In ACM SIGKDD. 1225–1234.
[7] Liang Chen, Jiaying Peng, Yang Liu, Jintang Li, Fenfang Xie, and Zibin Zheng. 2020. Phishing scams detection in ethereum transaction network. ACM Transactions on Internet Technology (TOIT) 21, 1 (2020), 1–16.
[8] William L Hamilton, Rex Ying, and Jure Leskovec. 2017. Inductive representation learning on large graphs.. 1025–1035.
[9] Petar Veličković, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Lio, and Yoshua Bengio. 2017. Graph attention networks.

Evaluation - Conventional Comparison Results

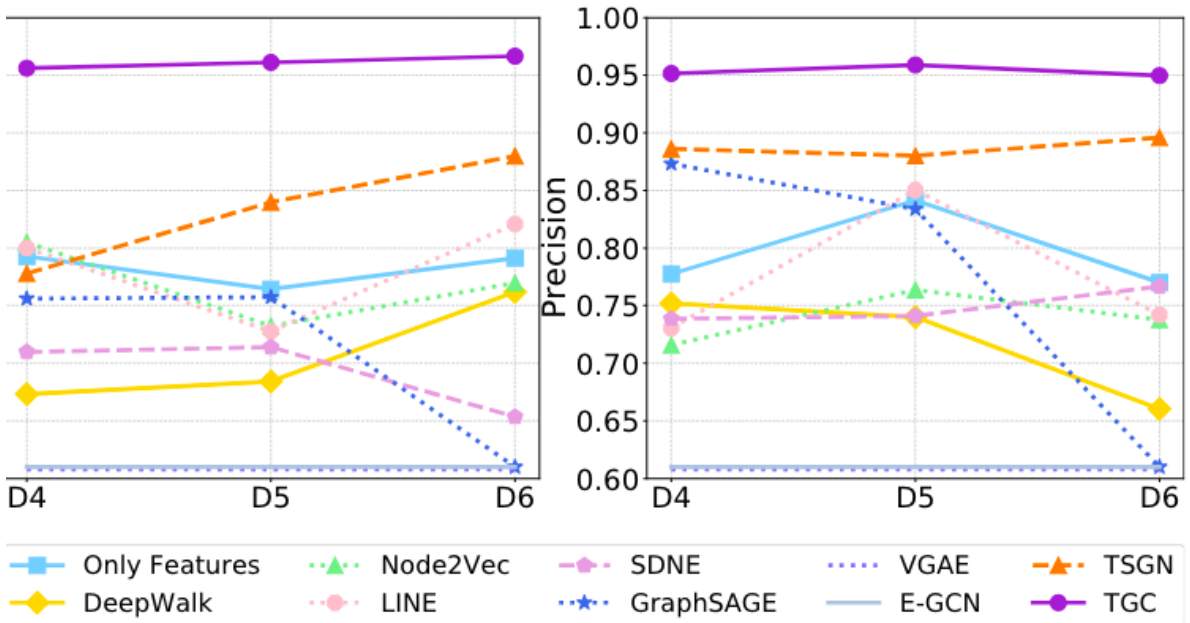
Method	Training Data	D_1			D_2			D_3		
		F1	Recall	Pre	F1	Recall	Pre	F1	Recall	Pre
Only Features	X	0.7713	0.7572	0.7859	0.7459	0.7759	0.7181	0.7825	0.7484	0.8198
DeepWalk	A	0.7108	0.7572	0.6697	0.7597	0.7747	0.7452	0.7639	0.7097	0.8271
Node2vec	A	0.7478	0.7624	0.7337	0.7931	0.8182	0.7695	0.7496	0.8065	0.7003
LINE	A	0.7990	0.8721	0.7373	0.7636	0.7470	0.7810	0.7666	0.8000	0.7359
SDNE	A	0.7447	0.6492	0.8732	0.7377	0.6838	0.8009	0.7472	0.7581	0.7367
GraphSAGE	X, A	0.8027	0.7709	0.8372	0.8273	0.8617	0.7956	0.8257	0.8097	0.8423
GAT	X, A, Y	0.8110	0.7749	0.8506	0.8577	0.8458	0.8699	0.8453	0.8194	0.8729
E-GCN	X, A, Y	0.8136	0.8796	0.7568	0.8650	0.8735	0.8566	0.8670	0.8516	0.8829
TSGN	X, A, Y	0.8174	0.7382	0.9156	0.8444	0.8261	0.8636	0.8892	0.9065	0.8727
TGC	X, A	**0.9261**	**0.9164**	**0.9360**	**0.9528**	**0.9565**	**0.9490**	**0.9550**	**0.9581**	**0.9519**

Conclusions

- TGC outperforms all the other compared methods by a significant margin, especially in large graphs
- TGC has better node representation capability than exiting Ethereum phishing detection methods
- Network representation methods based on deep learning are not performing well

Evaluation - Large-scale Data Comparison Results

Method	D_4	D_5	D_6
Only Features	0.7850	0.8010	0.7806
DeepWalk	0.7104	0.7111	0.7075
Node2vec	0.7577	0.7477	0.7534
LINE	0.7637	0.7842	0.7794
SDNE	0.7239	0.7273	0.7056
GraphSAGE	0.8105	0.7938	OOM
GAT	OOM	OOM	OOM
E-GCN	OOM	OOM	OOM
TSGN	0.8286	0.8595	0.8878
TGC	**0.9538**	**0.9600**	**0.9580**



Conclusions

- The TGC subgraph sampling training method can remain lightweight in large-scale network scenarios
- TGC has better node representation capability and stable performance than other methods on large graphs

Evaluation - Dynamic Data Comparison Results

Dataset	#Total Nodes	#Labeled	#Edges	#Average Degree
Train	4,824,725	2,273	24,965,770	5.1745
Test	4,412,810	2,355	27,642,111	6.2640

Method	Retrain	Conn	F1	Recall	Pre
Only Features	✗	✗	0.7260	0.6333	0.8506
E-GCN	✓	✓	0.5009	0.4856	0.5172
TSGN	✗	✗	0.7663	0.7887	0.7451
TGC	✗	✗	**0.9237**	**0.9291**	**0.9183**

Creation time	Number of phishing addresses
2016	5
2017	340
2018	1928
2019	523
2020	1050
2021	218
2022	533
2023	31

Conclusions

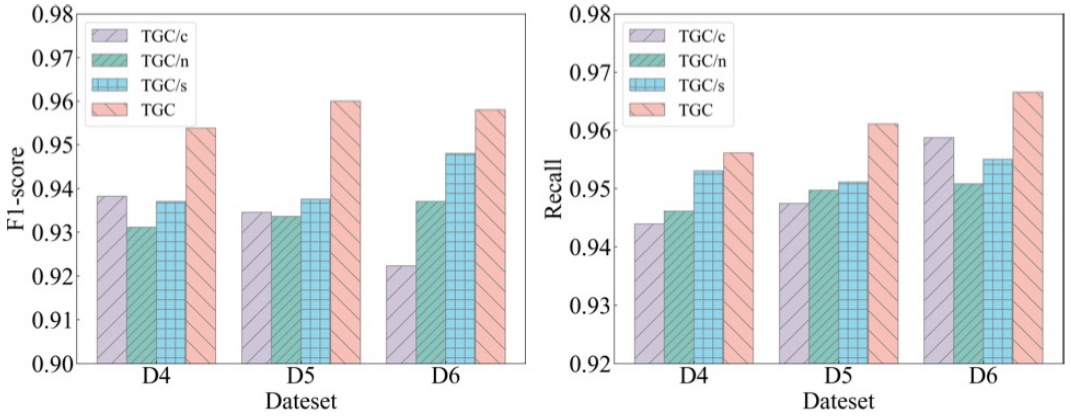
- TGC can detect emerging addresses in real-world scenarios without model retraining, and has no requirement on the overall connectivity of the transaction network
- Subgraph training combine contrastive learning scheme is able to help improve embedding quality

Evaluation - Few-shot & Ablation Study & Sensitivity Analysis

Few-shot Results

Method	100%	80%	50%	20%	10%
Only Features	0.7260	0.7154	0.7092	0.6870	0.6610
E-GCN	0.5009	0.5283	0.4091	0.2292	0.2087
TSGN	0.7663	0.7280	0.5800	0.4554	0.1473
TGC	**0.9237**	**0.8983**	**0.8635**	**0.8750**	**0.8409**

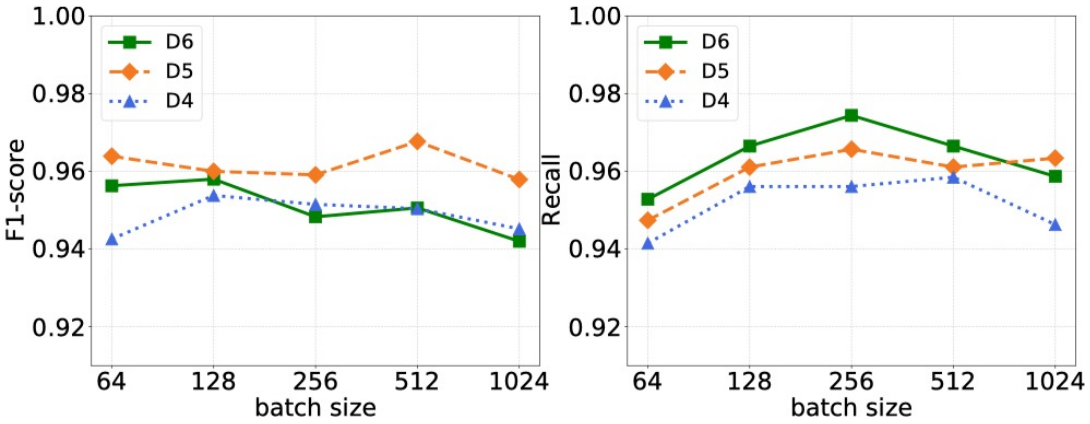
Ablation Study



Observation Results

- our proposed TGC method is least affected by the reduction of data size
- All modules in TGC are important
- TGC is robust to hyperparameter perturbation.

Sensitivity Analysis



Conclusion

- We propose a **Transaction Graph Contrast Network (TGC)** to enhance phishing scams detection performance on Ethereum

- TGC inputs subgraphs instead of the entire graph for training, which eases the model's requirements for machine configuration and data connectivity, and can be well adapted to dynamic networks

- Motivated by the natural camouflage and sparsity distribution of phishing addresses, we design **node-level contrast** and **context-level contrast** to learn the unique properties and universal transaction patterns of phishing addresses

- We hope that our work demonstrates the serious threat of phishing scams on Ethereum and calls for effective countermeasures deployed by the blockchain community.

THANK YOU FOR LISTENING

Sijia Li
lisijia@iie.ac.cn