WHITEPAPER

An AI-based Blockchain security monitoring system

Table of Content

Abstract

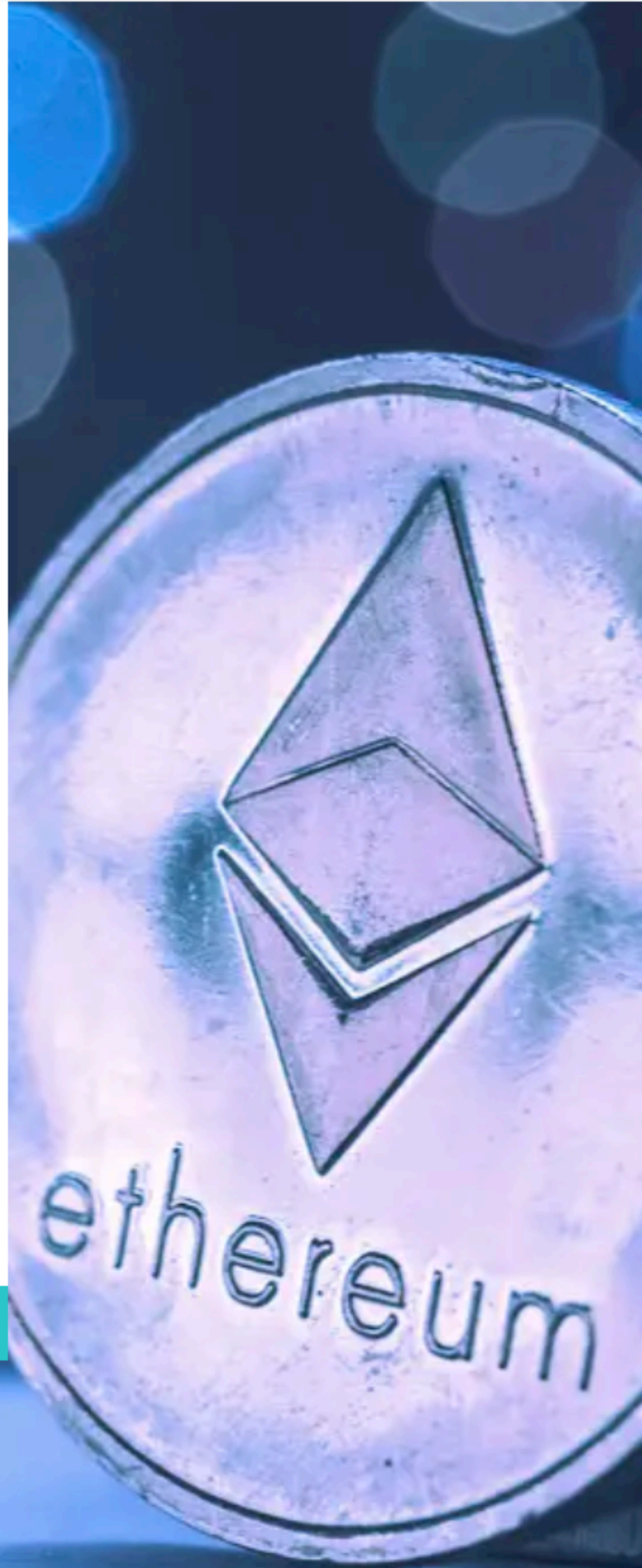
In today's cyberspace, it is essential to take measures to strengthen the security of each layer in the blockchain architecture. This paper focuses on the lowest level layer in the blockchain, particularly the P2P network that allows the nodes to communicate with each other and share information. This layer is a vital component of any blockchain, including Ethereum, due to the decentralised nature of its architecture. However, a malicious node could be used by an attacker to exploit specific vulnerabilities in the P2P network layer in order to carry out a variety of attacks on the blockchain, such as a Distributed Denial of Service (DDoS) attack, an eclipse attack, or a Sybil attack. Consequently, this layer is still prone to many threats inherited from P2P networks, and there is a need to analyse and understand the P2P networks of blockchain systems by collecting data and extracting insights from the network behaviour to reduce those risks using advanced AI algorithms.

This paper proposes Tikuna, an open-source P2P security-focused solution for monitoring and detecting potential attacks on the Ethereum blockchain network at an early stage. Furthermore, this approach employs an unsupervised Long Short-Term Memory (LSTM) method based on the Return Neural Network (RNN) to detect P2P-relevant security incidents. Finally, as an additional security measure, Tikuna provides the user with the option to add pre-configured health check alerts for the P2P network.

Introduction

Ethereum was formally introduced by Vitalik Buterin in his whitepaper in 2014 [1] and launched in 2015 as a public cryptocurrency blockchain platform that supports smart contract functionality with Ether (ETH or Ξ) as it is a native cryptocurrency and Solidity its programming language [2]; it is the second largest cryptocurrency after Bitcoin, with around $234 billion as of August 2022 [3].

Furthermore, like any technology, even though blockchain technology is both highly secure and distributed, it still offers opportunities for attacks. For example, in blockchain networks, there are cases in which the dApps, average users, or the network itself are exposed to many daily risks due to particular vulnerabilities. Therefore, understanding the risks that are associated with blockchain networks and effectively developing security-focused solutions such as *Tikuna* to reduce those risks is essential to any blockchain security.

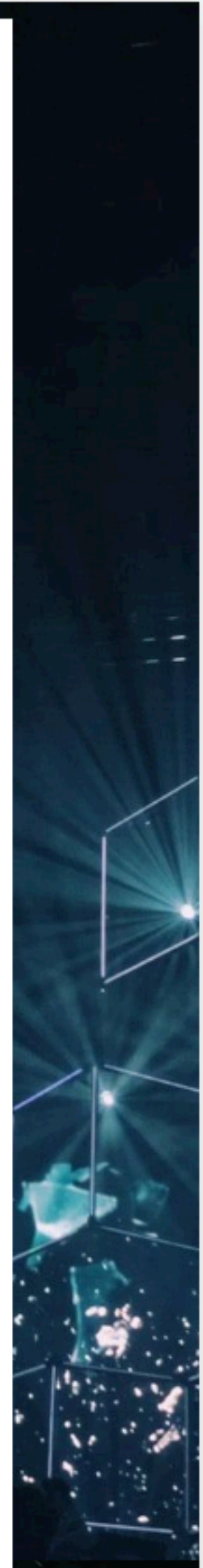


Why Should You Be Concerned About P2P Network Security?

The peer-to-peer network (also known as the P2P network), is a decentralized network communications technology that includes a number of nodes that store and distribute data collectively and each node in the network operates as an individual peer. The communication is carried out in this network without any central authority; hence, all nodes obtain the same amount of power and are responsible for the same activities. In addition, due to the decentralized nature of its architecture, the P2P network is one of the fundamental components of the blockchains that enable the creation and operation of cryptocurrencies [5].

Furthermore, the P2P network enables the nodes (also referred to as clients) of a blockchain to exchange data, including transactions and blocks. However, a malicious node could be used by an attacker to exploit specific vulnerabilities in the P2P network layer in order to carry out a variety of attacks on the blockchain, such as a Distributed Denial of Service (DDoS) attack, an eclipse attack, or a Sybil attack [6-8].

Moreover, the Ethereum P2P protocol [4] was influenced by the kademlia Distributed Hash Table (DHT). Despite the fact that kademila possesses valuable properties, it has several limitations in terms of its security [9-10], such as the eclipse attacks [7-8], where it is still possible to perform it against the Ethernet P2P network participants as well as deanonymization attacks as presented in [11]. Therefore, it is impossible to provide any guarantee that a peer-to-peer network is secure. Nevertheless, by employing a variety of detection and mitigation approaches [12-13], it is possible to reduce or eliminate the severity of these risks significantly. For example, monitoring the health of the blockchain network by collecting data and deriving insights could assist in the detection process of different incidents as well as enhance network status visibility.



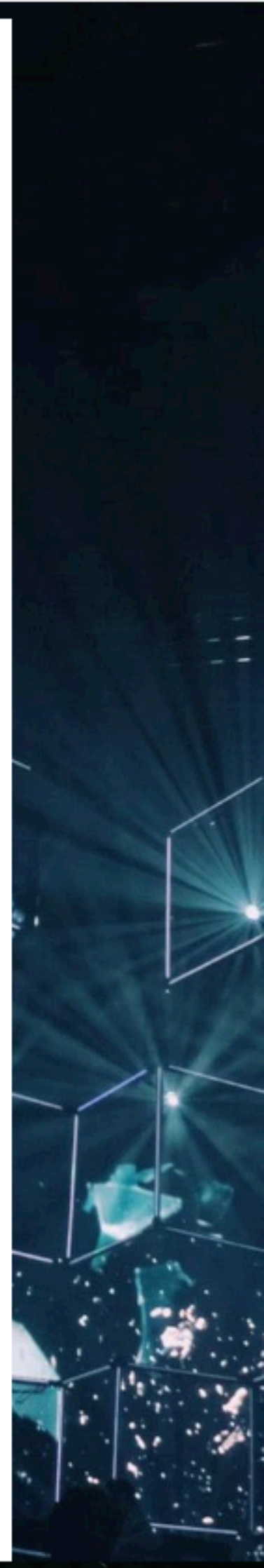
Types of P2P Network Attacks

A number of vulnerabilities in the blockchain's P2P networks can be exploited by adversaries to perform a variety of attack vectors on the blockchain network layer [14-22], including the following:

1) Eclipse Attack [19-20, 22]: an eclipse attack is an attack that can be carried out against a single victim node or the whole network, where the adversary isolates the victim node within the P2P network by gaining complete control of the node's access to information or control over everything that the node sees. In addition, this attack exploits several vulnerabilities, including the vulnerability to establish limitless nodes, uncapped incoming connections vulnerability, and public peers or fixed peers selection vulnerability.

2) Censorship Attack [17]: during this type of attack, the adversaries will use the nodes on the network that they have created with fake identities (i.e., Sybil nodes) to propagate all messages, with the exception of those that were published by the peer that they are trying to attack. In addition, the major objective of the attacker is to censor the target and stop its messages from being transmitted to the rest of the network.

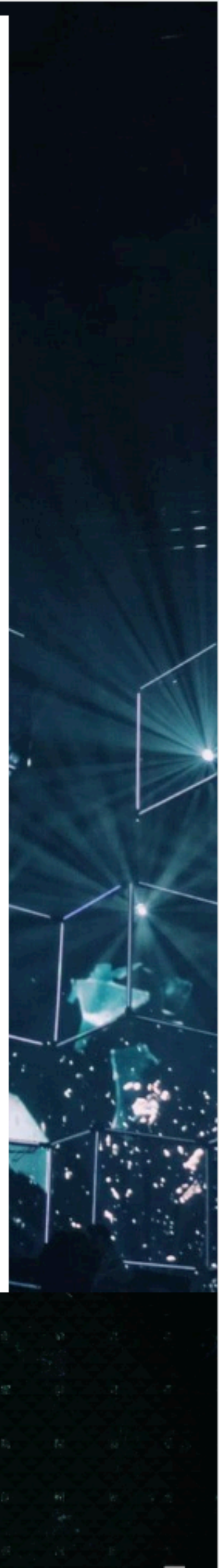
3) Sybil Attack [25-26]: which is also known as pseudospoofing, is an attack that can target any P2P network, such as blockchain networks, in which a single adversary creates a large number of nodes on the network with fake identities in order to gain a moresignificant presence in the network and eventually take control of the network. Additionally, this kind of attack might be used to carry out other kinds of attacks as well, such as an eclipse attack or a censorship attack.



Types of P2P Network Attacks

4) Cold Boot Attack [17]: during this attack, both genuine and nodes with fake identities (so-called Sybil nodes) join the network at the same time; genuine peers attempt to build their network while connecting to both Sybil and genuine peers. Since there is no score accumulated from a warm, genuine network to secure the network, the Sybils are able to seize control. Additionally, there are two possible scenarios for the attack: I) when the network bootstraps with Sybils joining from the start or II) when new nodes join the network when it is under attack.

5) Flash & Covert Flash Attack [17]: during a Flash attack, Sybils will simultaneously connect and launch attacks against the targeted network. On the other hand, in the Covert Flash Attack, Sybils join the network and act normally for a period of time in order to build up their score. Then, they carry out a coordinated attack in which they stop propagating messages altogether in an effort to disrupt the network entirely. Furthermore, as the adversaries act appropriately up until that point and establish a proper profile, it is difficult to identify the attack before the attackers become malicious.



Tikuna Architecture and Overview

Tikuna is a proof-of-concept peer-to-peer network security monitoring system developed for the Ethereum blockchain. It will accomplish this by utilizing different techniques, including machine learning, to extract security and performance insights for the early detection of relevant incidents. We also would like to support the Ethereum community by providing an open-source cutting-edge tool that is capable of collecting security-related data from the state of the P2P network and improving network visibility by providing insights about the network's current state.

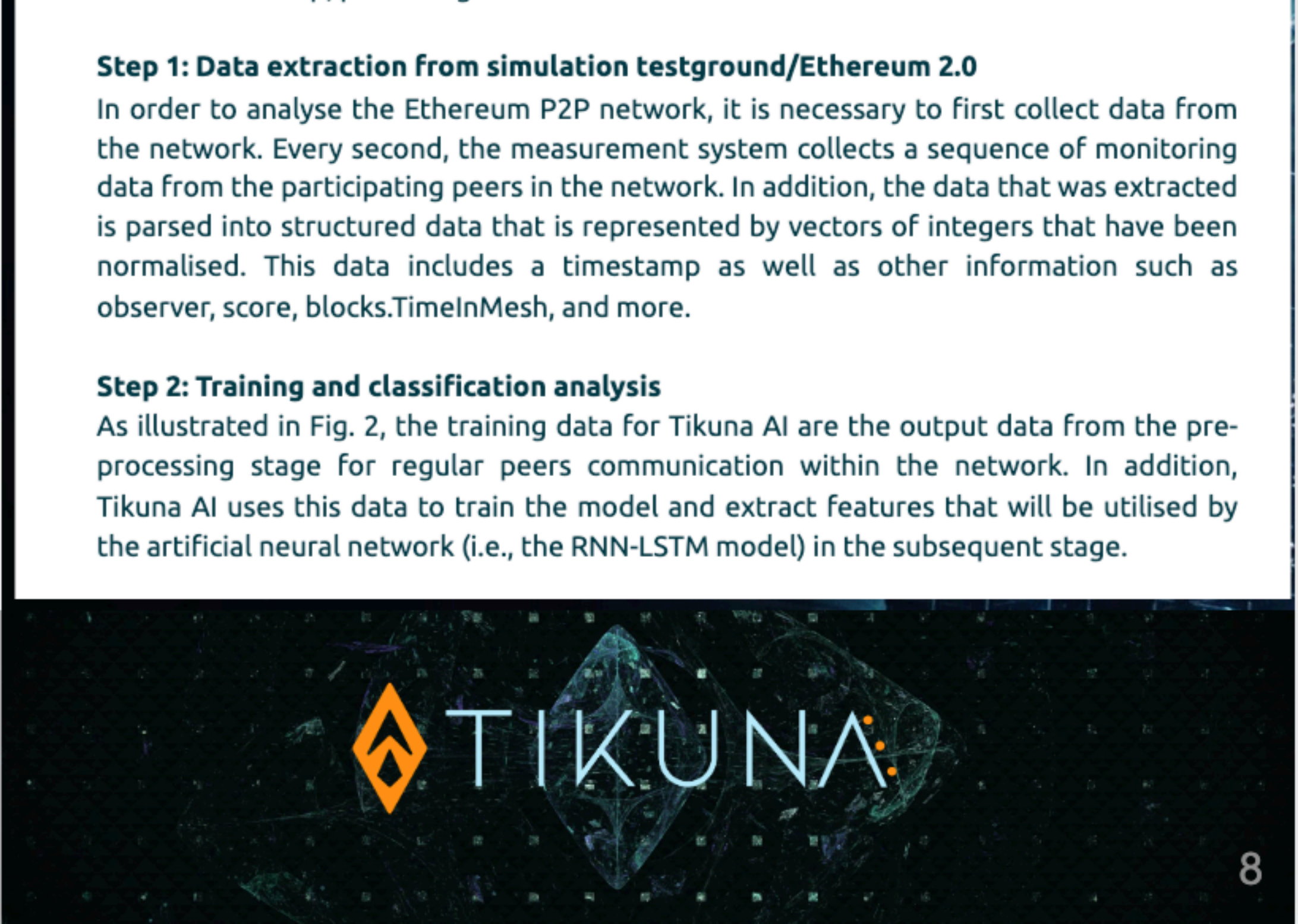
The architecture of Tikuna is depicted in Fig. 1, it consists of the following three primary steps: the data extraction from the simulation testground/Ethereum 2.0, the training and classification analysis, and the detection of P2P-relevant security incidents. Moreover, as an additional step, pre-configured health check alerts are included.

Step 1: Data extraction from simulation testground/Ethereum 2.0

In order to analyse the Ethereum P2P network, it is necessary to first collect data from the network. Every second, the measurement system collects a sequence of monitoring data from the participating peers in the network. In addition, the data that was extracted is parsed into structured data that is represented by vectors of integers that have been normalised. This data includes a timestamp as well as other information such as observer, score, blocks.TimeInMesh, and more.

Step 2: Training and classification analysis

As illustrated in Fig. 2, the training data for Tikuna AI are the output data from the pre-processing stage for regular peers communication within the network. In addition, Tikuna AI uses this data to train the model and extract features that will be utilised by the artificial neural network (i.e., the RNN-LSTM model) in the subsequent stage.



Tikuna Architecture and Overview

Step 3: Detection of P2P-relevant security incidents

In this step, as shown in Fig. 2 a Long Short-Term Memory (LSTM) method [27-29] is used by the Tikuna AI. The LSTM is based on a Return Neural Network (RNN), and it can remember long-term dependencies over the input data (i.e., a series of monitoring data). In addition, a forecasting loss function is used to evaluate how well the neural network models the training data by comparing the target and predicted output values with the goal of minimizing this function (i.e., to train the model to detect anomalies based on previous observations under the assumption that normal peers monitoring data follows a consistent pattern). Consequently, Tikuna AI detects P2P-relevant security incidents when the peers monitoring data deviate from the regular pattern.

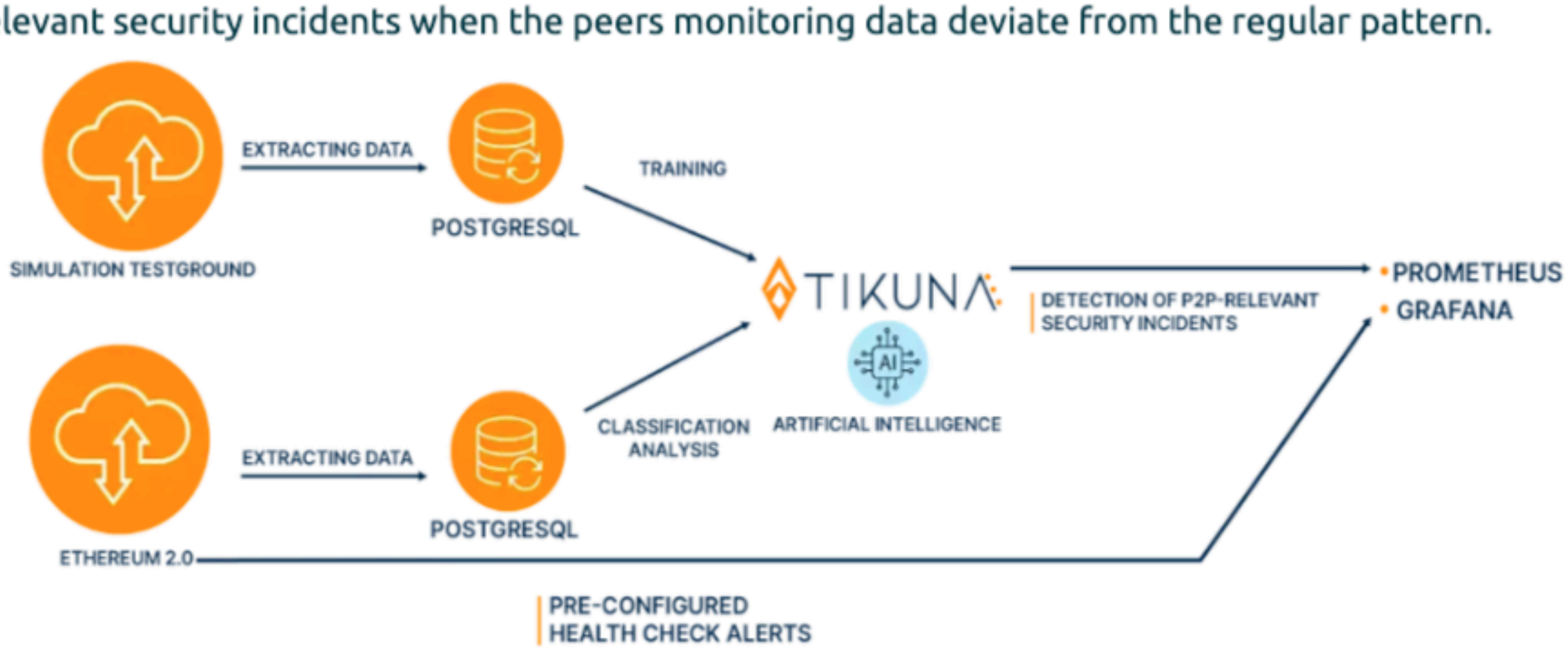


Fig.1 Tikuna Architecture

Fig.2 Tikuna AI Flow Diagram

Bibliography

[1] Ethereum, White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. https://github. com/ethereum/wiki/wiki/White-Paper, abgerufen: 2018-04-17.

[2] G. Wood, Yellow Paper: A Secure Decentralised Generalised Transaction Ledger, EIP150 Revision. http://paper.gavwood.com/, abgerufen: 2018-04-11.

[3] CoinMarketCap."Today's Cryptocurrency Prices by Market Cap, https://coinmarketcap.com/"

[4] The Ethereum Foundation. Devp2p—Ethereum peer-to-peer networking specifications. https://github.com/ethereum/devp2p

[5] T. Neudecker and H. Hartenstein, “Network layer aspects of permissionless blockchains,” IEEE Commun. Surv. Tut., vol. 21, no. 1, pp. 838–857, Jan.–Mar. 2018.

[6] M. Saad et al., “Exploring the attack surface of blockchain: A comprehensive survey,” IEEE Commun. Surv. Tut., vol. 22, no. 3, pp. 1977– 2008, Jul.–Sep. 2020.

[7] Guangquan Xu, Bingjiang Guo, Chunhua Su, Xi Zheng, Kaitai Liang, Duncan S. Wong, Hao Wang, Am I eclipsed? A smart detector of eclipse attacks for Ethereum, Computers & Security, Volume 88, 2020,101604, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101604.

[8] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on bitcoin’s peer-to-peer network., in: USENIX Security Symposium, 2015, pp. 129–144.

[9] H. Chen, M. Pendleton, L. Njilla, and S. Xu, ``A survey on Ethereum systems security,'' ACM Comput. Surv., vol. 53, no. 3, pp. 1 43, May 2021, doi: 10.1145/3391195.

[10] König, Lukas, Stefan Unger, Peter Kieseberg and Simon Tjoa. “The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks.” J. Internet Serv. Inf. Secur. 10 (2020): 110-127.

[11] Y. Gao, J. Shi, X. Wang, R. Shi, Z. Yin and Y. Yang, "Practical Deanonymization Attack in Ethereum Based on P2P Network Analysis," 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021, pp. 1402-1409

[12] Min Du, Feifei Li, Guineng Zheng, and Vivek Srikumar. Deeplog: Anomaly detection and diagnosis from system logs through deep learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), pages 1285–1298, 2017.

Bibliography

[13] van Ede, T., Aghakhani, H., Spahn, N., Bortolameotti, R., Cova, M., Continella, A., van Steen, M., Peter, A., Kruegel, C. & Vigna, G. (2022, May). DeepCASE: Semi-Supervised Contextual Analysis of Security Events. In 2022 Proceedings of the IEEE Symposium on Security and Privacy (S&P). IEEE.

[14] H. Chen, M. Pendleton, L. Njilla, and S. Xu, ``A survey on Ethereum systems security,'' ACM Comput. Surv., vol. 53, no. 3, pp. 1 43, May 2021, doi: 10.1145/3391195.

[15] Guangquan Xu, Bingjiang Guo, Chunhua Su, Xi Zheng, Kaitai Liang, Duncan S. Wong, Hao Wang, Am I eclipsed? A smart detector of eclipse attacks for Ethereum, Computers & Security, Volume 88, 2020,101604, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101604.

[16] A. H. H. Kabla et al., "Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review," in IEEE Access, vol. 10, pp. 71632-71655, 2022, doi: 10.1109/ACCESS.2022.3188637.

[17] Vyzovitis, D., Napora, Y., McCormick, D., Dias, D., & Psaras, Y. (2020). GossipSub: Attack-Resilient Message Propagation in the Filecoin and ETH2.0 Networks. arXiv. https://doi.org/10.48550/arXiv.2007.02754

[18] M. Cortes-Goicoechea and L. Bautista-Gomez, "Discovering the Ethereum2 P2P Network," 2021 Third International Conference on Blockchain Computing and Applications (BCCA), 2021, pp. 81-88, doi: 10.1109/BCCA53669.2021.9657041.

[19] Karl Wüst and Arthur Gervais. 2016. Ethereum Eclipse Attacks. Technical Report. ETH Zurich.

[20] Yuval Marcus, Ethan Heilman, and Sharon Goldberg. 2018. Low Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. Cryptology ePrint Archive, Report 2018/236. https://eprint.iacr.org/2018/236.

[21] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1977–2008, 2020.

[22] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in Proc. 24th USENIX Security Symposium (USENIX Security '15), 2015, pp. 129–144.

[23] SlowMist. (2018). Billions of Tokens Theft Case Cause by ETH Ecological Defects. Available: https://mp.weixin.qq.com/s/ia9nBhmqVEXiiQdFrjzmyg

[24] https://thehackernews.com/2018/06/ethereum-geth-hacking.html

[25] Eisenbarth, JP., Cholez, T. & Perrin, O. Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention. J Netw Syst Manage 30, 65 (2022). https://doi.org/10.1007/s10922-022-09676-2