Protocols and Guidelines to Enhance the Endpoint Security of Blockchain at User's End

Mohd Azeem Faizi Noor* [1], Khurram Mustafa [2]

{azeemfaizif@gmail.com[1], kmfarooki@gmail.com[2]}

Department of Computer Science, Jamia Millia Islamia, Jamia Nagar New Delhi 110025[1,2]

Abstract. Blockchain is a distributed, immutable ledger that is used to record transactions, track assets, and build trust. Prominent among the several desirable assurances is enhanced security. It appears to be secure in the sense that no one can tamper with data. Despite the fact that Blockchain can provide a tamper-proof record of transactions, it is not immune to ever-increasing attacks. Endpoint insecurity risks jeopardize users' privacy, sensitive data, and system resources. Sensitive information leads to the disclosure of the private key, which may lead to losses including crypto-currency from the user's wallet. Previous experiences reveal and enable us to witness many typical attacks. In such cases, the invaders injected malicious codes and gained access to the user's email, after which they used the user's sensitive data for their nefarious purposes. They have been continuously benefited by the malicious codes. As a result, we review vulnerabilities, hacking and the risks associated with it. Some simplistic measures and security enhancement environments are identified. Thus, we highlight a few highly simplistic necessary protocols, recommendations, and technology as a solution to avoid endpoint exploitation at the user's end.

Keywords: Endpoint Security, Blockchain, Protocols, Remote Browser Isolation, Trusted Execution Environment.

1. Introduction

The Blockchain is a neoteric and emerging technology that was coined by a pseudonymous person Satoshi Nakamoto in October 2008 through white-paper literature [1]. He never revealed any personal information. Many persons and organizations claimed and many are claimed by others as Nakamoto but none of them is correct [2]. Blockchain is a publicly available ledger of transactions. The ledger transactions can be composed of finance (economic, money), tangible assets (homes, land), intangible assets (software, copyrights), and much more alike [3]. It stores data permanently in a series of blocks. The data cannot be altered or removed. Blocks are the data structure and each block is linked with its previous block through a hash value. These blocks are verified by the Consensus algorithm and Miners [4].

Thus, Blockchain technology can be regarded as an integrated multi-field infrastructure construction that combines Cryptography, Mathematics, algorithms, Economic model etc [5]. As a unique virtue, this technology completely removes the intermediary or central authority from the chain of (financial and non-financial) transactions/activities. Consequently, no centralised control exists for blockchain. Hence, Blockchain may be referred to as a shared, immutable ledger that facilitates the recording of transactions and the tracking of assets in a

ICIDSSD 2022, May 24-25, New Delhi, India

DOI 10.4108/eai.24-5-2022.2318925

network. Assets may be either tangible (such as a house, car, cash, or land) or intangible (intellectual property, patents, copyrights, branding). Among the desirably celebrated features are its assurance towards immutability, decentralization, enhanced security, distributed ledgers, consensus, and faster settlement.

Blockchain's block consists of a block header and block body. The block header contains Block version, Merkle tree root, Timestamp, Nonce, Difficulty level and Parent block hash. The block body consists of several transactions. The maximum number of transactions in a block is dependent on the block size and size of each transaction [6].

To exchange a unit of value - such as digital currency, land asset title or digital representation of some other asset. The transaction details are broadcasted over the Blockchain network. The miners evaluate and authenticate the transaction details in the block through a mathematical puzzle and generate the block's hash value. This process is called Proof of Work [1].

Next, each such block of transactions is time-stamped with a cryptographic hash. This information is broadcasted in the group where most of the networks verify the block validity with the c*onsensus* algorithm. Eventually, the block is added to the previous block hash, which successfully creates a chain of records and a unit of value exchanges**. Figure 1** depicts the whole process. This record is auditable, immutable and transparent [7]

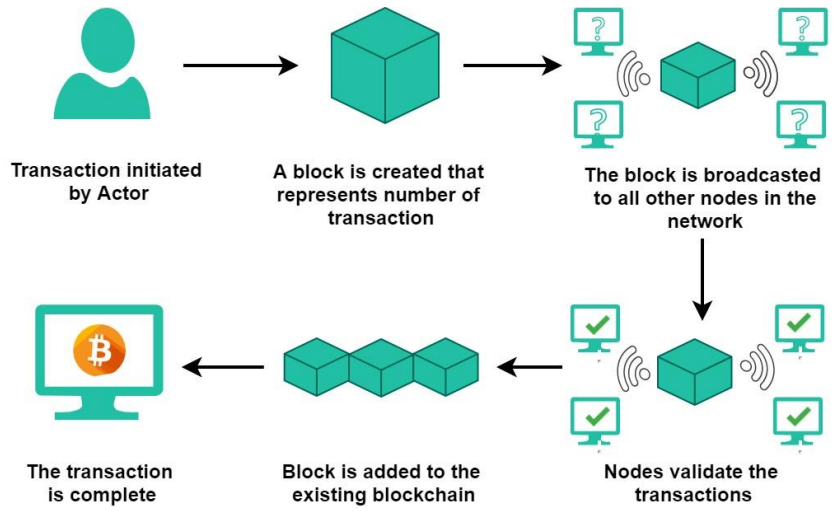

Fig. 1. Working of Blockchain

Blockchain also suffers from several vulnerabilities. The prominent among them is called endpoint vulnerability. It typically originates outside the blockchain framework. When end-users interact with the blockchain, they enter new data to the blockchain-based services from their device. It is the transient moment when endpoint security is needed highly. As a result, data on the blockchain is most susceptible during the process of accessing blockchain services.

It is easy for hackers to enter into the less secure personal computers, laptops and android devices [8].

Blockchain security is a comprehensive risk management system for blockchain networks encompassing cybersecurity infrastructure, assurance services and best approaches to mitigate risks associated with Blockchain. Although, Blockchain produces tamper-proof ledgers of transactions but is not immune to cyberattacks and frauds. The hackers manipulated known vulnerabilities and succeeded in numerous heists and attacks over the year. Some known heists are Mt Gox ($450 million), Coincheck ($533 million), BitFinex ($72 million), Bithumb ($32 million [9] [10].

To the best of our knowledge, no dedicated article has been published that discusses the procedures and principles that must be followed to prevent and avoid endpoint penetration in the blockchain. So, it is utter important to highlight and discuss the protocols that will guide and help users to avoid any troubles. This brief treatise covers the critical genesis in section 2, an overview of endpoint security in section 3, mitigation measures as recommendations in section 4, security enhancement in section 5, followed concluding remarks.

2. Genesis

Lee [10] studied and investigated hacking incidents from 2011 onwards. He distributed all incidents among four classes, namely Platform breach, Access point attack, DApps exploit and Endpoint Hacking. He also mentioned that Distributed applications (dApps), online web-based wallets using MultiSig authentication, or third-party organizations or exchanges are the most common ways for a node to interface with Blockchain. Any data originating from that node to the Blockchain has no further data protection or security safeguards after it has been authenticated.

According to an analysis of the trend of security breaches in Bitcoin, many security breaches have happened, including DDoS attacks and private account hacking via Trojan horse or viruses from advertisements [11]. Intruders are attempting to gain access to the system using Blockchain's flaws and openness to steal the crypto-coin. The intruders cannot be tracked, identified, or punished because of the anonymity feature of Blockchain [12] [13].

In Taylor’s [14] selected scholarly papers, the fourth most common issue is privacy and public key infrastructure. The user's activities and attitude have a significant impact on the security and protection of a hot wallet [15]. Raziel [16] explains endpoint vulnerabilities' problems, insecure key storage or an insecure platform could easily lead to exposure. He also predicted the threat of quantum computing for the key combination.

The experts have ranked the high revenue of the Blockchain market. It is expected by the end of 2024, the corporations will spend $20 billion per year on blockchain technical services [17]. This earning can be useless if endpoint security loopholes are not addressed timely. Kara Coppa, Co-Founder of BLACKFX, showed concern over endpoint security in an interview. Megan Squire, the Cybersecurity expert, told in 2017 that "*we real people should work on improving security where we are most vulnerable—on our own devices*." Thus, it

appears critical to address the user's originated endpoint insecurity and ensure the safety of key combinations and user privacy.

3. Endpoint Security

It refers to the practice of safeguarding the endpoints of end-user devices such as desktops, laptops, and smartphones devices from being exploited by malware, malicious code and lazy behaviour of users. Such an endpoint represents key vulnerable points of entry for cybercriminals. With organizational workforces becoming more mobile and users connecting to internal resources from off-premise, endpoints are susceptible to cyberattacks [18]. In the premise of Blockchain, endpoints are the platforms where users interact with the blockchain. Many times, these platforms include mining systems and other personal computers. The endpoints are the platforms where human beings interact with the blockchain. Its example includes Desktops, Laptops, Smartphones, Tablets, Servers etc. The general objectives for targeting endpoint include, but are not limited to:

- Take control of the device and abuse computational resources to execute malware, malicious code, keylogger and cryptojacking [19].
- Access assets on the endpoint to disrupt the services and usage, either for ransom or completely for disruption.
- Enter into an organization to access high confidential data including the private key.
- Exfiltrate the data by malicious actors for the unauthorized movement of data like data theft, data extrusion, data exportation, data leakage, and data exfiltration[1].

Moreover, the *distributed endpoints* are under the command of some organizations and have some layer of heterogeneity. In contrast, the *decentralised endpoints* are the nodes and may be fully homogeneous. *Distributed endpoints* have multi-layer security. Thus, many security tools and technology exist like firewalls, Endpoint Detection and Response (EDR), Antivirus tools, Intrusion Detection Systems (IDS), Network Monitoring etc. The attacker has to penetrate or bypass these securities to reach their targets, databases, applications etc. In contrast, a *decentralised endpoint* does not equip itself with such security tools and has a single layer of authentication [10] [20]. If an invader invades it successfully then he can easily exploit target's vulnerability. Though not universal, some DApps and Crypto Exchange organizations provide the facility of multi-layer but varying security assurances [10] [21].

There exist many reasons behind the compromise of endpoint devices. From the Brute Force attack to the lazy behaviour of users, several possibilities exist. Bithumb exchange was compromised twice through endpoint hacking and lost about $32 million [22]. The attacker sent malicious emails to the Bithumb users to get the account-related information and many users click on the email's link. In 2018, the Coincheck exchange was hacked and lost $534 million. The exchange kept the consumer's assets on a hot wallet that was connected to external networks. Apart from this, blockchain appears lacking at a multi-signature security mechanism.

[1] https://awakesecurity.com/glossary/data-exfiltration/

LocalBitcoins, BTC-E, Allinvain, Cryptsy are the exchanges /organizations that were hacked through malware/ trojan horse/ keylogger etc. In the Bithumb 1st ever attack, the attacker entered into one of the employee desktops and got the information of 31506 users stored in an unencrypted excel file [9] [10].

Thus, Endpoint security is a strategy to reduce endpoint security breaches. The attacker target endpoint for their malevolent intentions. Endpoint compromise opens the door to several attacks and heists. The attack intends to obtain wallet information to steal crypto-coins. As a corollary, wallet breaches, key breaches, malicious code injection, and other issues arise. Table 1 lists the various types of attacks and their potential countermeasures. An awareness and guidelines may prevent endpoint breaches. Table 2 shows the different heists due to the unawareness of the users.

Table 1. Different attacks due to insecure endpoint

Attack types	*Description*	*Target*	*Adverse effect*	*Possible countermeasures*	*Reference*
Cryptojacking/ malicious code	Malicious code is injected in the web browser	User's system	Data stealing and abuse computational Resource, chain splitting	MineGuard – A software tool	[6]
Wallet theft	Hackers gaining access to hot wallets and destroy or stole private keys	Wallet / exchanges	Loss of cryptocoin and permanent account loss	Use of different types of cold wallet and backups locally. Use threshold Signature to achieve two -factor security	[6] [7] [15] [25]
key infrastructure breach	Bypass the authentication process	User's account	Cryptocoin and account loss	The blockchain applications allow for end users to authenticate in some way with another entity or service so that they do not need to rely on a vulnerable central server of information.	[14]
ECDSA	ECDSA nonce value reused. Lattice based algorithm to compute private ECDSA keys	Private key	Loss of account	Update RFC 6979	[6][9]

Table 2. Heists and attacks due to user's unawareness

Attacks/Heist	*Breach*	*Root causes*	*Amount ($)*	*Preventions*	*Reference*
Coincheck (2018)	Malware injected	Coincheck chose to keep all of its XEM tokens in a hot wallet. The hacker gained access to an employee's computer and installed malware aimed to steal digital wallet private keys.	533 million	a minor amount of currency should be kept in a hot wallet. passive funds must be stored in a well-protected cold wallet. Keep monitor activity constantly	[22] [27]
Bithumb 1st and 2nd (2017 & 2018)	Endpoint breaches	An employee's PC has been hacked. The personally identifiable information of 31,800 online users was stolen because files were not encrypted. In the second heist, users were duped via phishing emails.	32 million	Use reputed encryption services. Beware of malicious mail	[22] [10]
NiceHash (2017)	Employee system breaches	Hackers infiltrated into the system using a compromised company engineer's credentials	63 million	Nicehash support suggests to secure email, password, use two-factor authenti-cation and beware of fake website	[6]
Bitfinex (2016)	Server/ Infrastructure Breach	The smart contract was poorly designed. The multi-signature key management system's key stakeholders are blindly signing off transactions.	72 million	Systematic controls to prevent and detect analogous transactions. End to end security review using scenarios	[15] [23]
Gatecoin (2016)	Platform/ exchange breach	the attacker managed to bypass multi-signature protection placed on cold storage by altering the exchange's systems to instead use hot wallets	2 million	Use indirect address for cold storage	[22]
BTC-E (2014)	Malware injected/ endpoint breach	To acquire credentials, a hacker was able to post a malware link on an ajax chat software and propagate it to BTC-e users	26 million	----------	[10]

Many users do not care about private keys and personal information security. They share it with other users and websites frequently. Often such carelessness reveals very sensitive information and the phisher takes advantage. One such experiment was done by Brengel and Rossow [24] where they investigated explicit keys leakage on an open-source intelligence platform (OSINT). Another research done by Pal, Alam, Thakur and Singh [25] suggests that

the keys can be revealed through a side channel, replay attack, weak encryption, brute force etc. Companies or organizations that permit the employee to Bring Your Own Device (BYOD), laptops or smartphones for use at work usually face endpoint device security issues. Thus, to counter the users' endpoint attacks some protocols and guidelines may prove handy as threat mitigation measures at least but not the last.

4. Mitigation Measures

Blockchains are neither perfect nor ultimate regarding security. They suffer from vulnerabilities but most of them relates to limitation of users [18]. Technology is no panacea, but the user must be responsible and adhere to protocols for minimizing the risk of cyber-attack, hacking, and stealing. Endpoints must be protected from known, unknown and zero-day threats; delivered through malware and exploits whether a machine is online or offline, on-premise or off, connected to the organization's network or not. A purposeful review of the relevant literature reveals typical measures, in various forms of simple guidelines that are highly likely to reduce threats, including the following.

- Ensure awareness of the associated risks, vulnerabilities, threats, possible intrusions, attack patterns, security guidelines, and policies.
- Use a real-time scanning antivirus for the system that detects a malware, cross-site scripting attacks, key logger etc.
- Keep the system updated with the latest software versions and the appropriate patches.
- Never keep blockchain keys in a text file, word document, or other file formats in an unencrypted way.
- Use a reputed encrypted application and encrypt the hard disk.
- Never share the security key with others [26]. If it is a must to share the security key then use the email feature of the blockchain wallet. Never use any other email service.
- Never allow BYOD, it has become an easy way for hackers to enter into an organization and steal sensitive data.
- Under Task Manager, keep monitoring CPU usage, Memory usage, Processes etc. A high value of utilization hints any malware, keylogger or malicious scripting is running on the system without the user's consent [27].
- Never keep all assets in an Online wallet. It is recommended to use both an online wallet and an offline wallet. Use an online wallet for holding a small portion of crypto-assets for transactions. Use offline wallet for holding the rest (larger part) of crypto-assets. If a user uses more than one storage type strategy to hold the assets, he will minimize the risk of theft and loss [15].

Existing endpoint vulnerabilities pose a security risk to blockchain systems. These flaws enable the execution of various security threats to the normal functionality of Blockchain platforms. Here are a few typical measures to prevent endpoint breaches.

- A log file must be maintained in a decentralized manner. If multiple logs are recorded within a few minutes then the user has to solve some questions or calculations or Non-interactive zero-knowledge proof (NIZK) [12].

- A zero-day attack is a software module mechanism that arises when no countermeasures exist against a vulnerability. When such vulnerability is exploited, software distributors need to issue a security patch to address it. But this is not an easy task [28]. Zero-day assaults can be prevented through antivirus software and frequent system updates, but not always. A zero-day attack is labelled as a higher security risk than Denial of Service (DoS) [29]. Al-rimy, Maarof and Shaid [30] proposed a 0-day aware crypto-ransomware early detection model for such an attack.

- To use blockchain without endpoint security risks, organizations may use public-private keys with hidden system IP addresses.

5. Endpoint Security Enhancement

In the midst of the global health crisis, the year 2020 was a watershed moment for security in general. Malicious actors are seen swiftly adapt the changing environment and find new ways to exploit vulnerabilities. Thus, the threat landscape is constantly changing and security measures need to be continuously enhanced to be in the comfort zone. Most generally, the security risks include losing security keys, personal user security, malware & keyloggers, and wallet theft. Various technologies may enhance the security of endpoint in blockchain and will keep safe the lazy or not-so-sensitive users. Solutions are generally perceived through Remote Browser Isolation, Trusted Execution Environment, Public-Private-IP Address, User Awareness, Monitor Resources Usage, and Zero-day attack patch [28] [31]. The prominent but simplest few are identified and introduced as follows.

- *Remote Browser Isolation (RBI):* Remote Browser Isolation is typical of Browser Isolation that takes place remotely by relocating the execution of all browsing activity from the user's PC to a remote server (secure environment). This remote server can be hosted in the cloud or on-premise within an enterprise's network. At the end of each browsing session, it destroys the browsing environment automatically. If the user ever comes across any malicious code, it gets erased at the termination of the session. When the user reconnects to the secure virtual browser, he or she is presented with a new malware-free environment. To prevent the device from being infected with malware, the user should use the Remote Browser Isolation technique.
- *Trusted Execution Environment:* A Trusted Execution Environment (TEE) is a secure area of a device's main processor that is parted from the system's main operating system. It guarantees that data is stored, processed and protected in a safe environment. A TEE is considered to be more secure than a traditional processing environment since it runs in parallel with the operating system and uses both

hardware and software. It also guarantees isolation of data and code residing inside against unauthorized access and modification. The different hardware-assisted TEE is Intel SGX, AMD SEV, ARM TrustZone etc [31].

6. Conclusion

In recent times, the tremendous potential of Blockchain applications is not hidden from the world. Every next person wants to update with its latest information. Denial of services of blockchain applications may suffer due to many vulnerabilities at its endpoints. Such vulnerabilities need to be mitigated, and simple measures as protocols/guidelines may prove handy. The strategy to maintain security keys is to maintain secure endpoints. Beyond the proposed measures and environments, Biometric identification can be remarkably helpful in keeping the security key safe. However, there is a need for a quantum-resistant cryptographic algorithm to produce a quantum-secured blockchain network and other viable options for signature-based authentication to signature-less authentication.

References

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review (2008)

[2] Luntovskyy, A.; Guetter, D.: Cryptographic technology blockchain and its applications. Vol. 560, pp. 14–33. Lecture Notes in Electrical Engineering, Springer Verlag (2019)

[3] Hayat Mosakheil, J.: Security Threats Classification in Blockchains (2018)

[4] Azeem Faizi Noor, M.; Khanum, S.; Anwar, T.; Ansari, M.: A Holistic View on Blockchain and Its Issues. pp. 21–44. (2020)

[5] Luon-Chang, L.; Tzu-Chun, L.: A survey of blockchain security issues and challenges. Vol. 19, no. 5, pp. 653–659. International Journal of Network Security (2017)

[6] Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A.: Exploring the Attack Surface of Blockchain: A Systematic Overview. pp. 1–30. (2019)

[7] Conti, M.; Sandeep, K.; Lal, C.; Ruj, S.: A survey on security and privacy issues of bitcoin. Vol. 20, no. 4, pp. 3416–3452. IEEE Communications Surveys and Tutorials (2018)

[8] Martin, R.:5 Blockchain Security Risks and How to Reduce Them- IgniteLtd. (2018) Retrieved: - 8 August 2019 from https://igniteoutsourcing.com/publications/blockchain-security-vulnerabilitiesrisks.

[9] Er-Rajy, L.; El Kiram My, A.; El Ghazouani, M.; Omar A.: Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures. Vol. 22, no. 3, pp. 1–29. Journal of Internet Banking and Commerce (2017)

[10] Jae Hyung, L.: Systematic approach to analyzing security and vulnerabilities of blockchain systems. (2019)

[11] Zhao, J. L.; Fan S., Yan, J.: Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Vol. 2, no. 1. Financial Innovation, Springer Open (2016)

[12] Feng, Q.; He, D.; Zeadally, S.; Khan, M. K.; Kumar, N.: A survey on privacy protection in blockchain system. Vol. 126, pp. 45–58. Journal of Network and Computer Applications (2019)

[13] Li, X.; Jiang, P. Chen, T.; Luo, X.; Wen, Q.: A survey on the security of blockchain systems. Vol. 107, pp. 841–853. Future Generation Computer Systems (2020)

[14] Taylor, P. J.; Dargahi, T.; Dehghantanha, A.; Parizi, R. M.; Choo, K. K. R.: A systematic literature review of blockchain cyber security. Vol. 6, no. 2, pp. 147–156. Digital Communications and Networks (2020)

[15] Zamani, E.; He, Y.; Phillips, M.: On the Security Risks of the Blockchain. Vol. 60, no. 6, pp. 495–506. Journal of Computer Information Systems (2020)

[16] Raziel, M.: The Good & Bad News about Blockchain Security. (2018) Retrieved: - 20 January 2022 from https://www.darkreading.com/endpoint/the-good-bad-news-about-blockchain-security

[17] Mitic.: 45 Blockchain Statistics & Facts That Will Make You Think: The Dawn of Hypercapitalism. (2022) Retrieved: - 25 January 2022 from https://fortunly.com/statistics/blockchainstatistics/#gref

[18] N. A.: Using Endpoint Security to Protect Your Data. (2019) Retrieved: - 20 January 2022 from https://blockgeni.com/using-endpoint-security-to-protect-your-data

[19] Elrom, E.: Security and Compliance. pp. 419–466. The Blockchain Developer, Apress (2019)

[20] Richardson, M.: Blockchain security vs standard cybersecurity. (2018) Retrieved: - 21 January 2021 from https://blockchaintrainingalliance.com/blogs/news/blockchain-security-vs-standard-cybersecurity

[21] Jin, H.; Luo, Y.; Li, P.; Mathew, J.: A review of secure and privacy-preserving medical data sharing. IEEE Access (2019)

[22] N.A.: Blockchain threat report – Mcafee. (2018) Retrieved: - 02 February 2022 from https://www.mcafee .com /enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf

[23] Boireau, O.: Securing the blockchain against hackers. pp. 8-11. Network Security (2018)

[24] Brengel M.; Rossow, C.: Identifying key leakage of bitcoin users. Vol. 11050. Springer International Publishing (2018)

[25] Pal, O.; Alam, B.; Thakur V.; Singh, S.: Key management for blockchain technology. Vol. 7, no. 1, pp. 76–80. ICT Express (2021)

[26] Hasanova, H.; jun Baek, U. M.; Shin, G.; Cho, K.; Kim, M. S.: A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Vol. 29, no. 2, pp. 1–36. International Journal of Network Management (2019)

[27] Dasgupta, D.; Shrein, J. M.; Gupta, K. D.: A survey of blockchain from security perspective. Vol. 3, no. 1, pp. 1–17. Journal of Banking and Financial Technology (2019)

[28] Singh, S.; Sanwar, H.; Yoon, B.: Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. Vol. 9, pp. 13938–13959. IEEE Access (2021)

[29] Dongjin, X.; Liang, X.; Limin, S.; Min, L.: Game Theoretic Study on Blockchain Based Secure Edge Networks (2017)

[30] Al-rimy, B. A. S.; Maarof, M. A.; Shaid, S. Z. M.: A 0-day aware crypto-ransomware early behavioral detection framework. Vol. 5, pp. 758–766. Springer Science and Business Media Deutschland GmbH, Lecture Notes on Data Engineering and Communications Technologies *(2018)*

[31] Coppolino, L.; D'antonio, S.; Mazzeo, G.; Romano, L.; and Campegiani, P.: Facing the Blockchain Endpoint Vulnerability, an SGX-based Solution for Secure eHealth Auditing. (2021)