**Block Chain Based Open Source Malware Detection System**

**Dr. Amit Kumar Tiwari** Assistant Professor, *Dept. of* *Computer Science & Engineering. United Institute of Technology.* Prayagraj,India

**Adrit Bose** Student (UG), *Dept. of Computer Science & Engineering.United Institute of Technology.* Prayagraj,India.

**Abstract - At present, antivirus programs and security organizations work independently, so when they discover a threat such as malware, they do not share the information with others. This project proposes that if they establish mutual relationships with other businesses, we will be able to access a comprehensive list of all the potential risks and malware.**

**One of the key benefits of utilizing block chain technology is that it operates on a decentralized network, which means each user is a server, making it nearly impossible to manipulate this database. Thus, this list will be continuously updated without any interruptions with the help of block chain technology. In other words, block chain technology has the potential to solve the problem of information sharing among security organizations and antivirus programs. The idea is to establish a reciprocal relationship among various businesses to create a massive list of all potential risks and malware.**

**Utilizing block chain technology is advantageous because it is decentralized, and each user operates as a server for the network, which makes it difficult to manipulate the data. Therefore, the database will be kept up-to-date seamlessly without any interruptions.**

# **INTRODUCTION**

The cyber security system is constantly at risk, and one of the main causes is the lack of information on unknown threats or malware, which further leads to unanticipated server or system failures.

The goal of this project is to create a block chain that contains a comprehensive system of discovered viruses, malware, and other associated dangers. Block chain is being employed because of its immutable and distributive properties, which will keep the entered data secure. This project has been maintained as an open source since its goal is to keep the material public and accessible to as many individuals as possible. Since this block chain would be a public block chain (permission), real-time updating is absolutely necessary to keep the project operational. Each user has the ability to read it, but only authorised users have the ability to verify the accuracy of the data entered. To date, only authorised antivirus and related companies have this ability.

The concept behind the Block Chain Based Malware Detection System is to build a block chain that functions as a database for all the data.

All the information on the system is information on viruses that were found there and the damage they caused.

Problem Found: There isn't a ready-to-use database with all the data on viruses and malware in a system that can't be altered, is easily accessible to anyone worldwide, and is immutable.

The reason why block chain technology is being employed is to provide a database with all the facts and data regarding viruses and malware, as well as their easily accessible solutions for users, and to ensure that the data existing in that system cannot be altered.

# **Identified Problem**

The cybersecurity system is always at the most significant risk due to various factors, one of which is the unavailability of unidentified threats and malware information. This lack of information about emerging threats and malware strains can have severe consequences, including unexpected server or system failures. The following points expand on this statement:

1. Rapidly Evolving Threat Landscape: The cybersecurity landscape is constantly evolving, with hackers and cybercriminals developing new and sophisticated malware techniques. These threats can exploit vulnerabilities in systems and networks, leading to unauthorized access, data breaches, and system failures. Without timely information about these unidentified threats, cybersecurity systems are left vulnerable to attacks.

2. Lack of Awareness: If cybersecurity systems do not have access to up-to-date threat intelligence and malware information, they may remain unaware of new malware strains circulating in the wild. This lack of awareness can result in delayed or inadequate responses to potential threats, making it easier for malware to infiltrate and compromise systems.

3. Zero-Day Vulnerabilities: Zero-day vulnerabilities are security flaws in software or systems that are unknown to the vendor or the cybersecurity community. Cybercriminals often exploit these vulnerabilities to launch targeted attacks before a patch or fix is available. Without knowledge of these vulnerabilities, cybersecurity systems cannot adequately protect against zero-day attacks, leaving systems exposed and at risk of failure.

4. System and Server Failures: Malware infections can lead to system and server failures, disrupting critical operations, causing data loss, and impacting business continuity. By remaining unaware of unidentified threats, cybersecurity systems cannot proactively detect and mitigate malware infections, increasing the likelihood of system failures and associated financial and reputational damages.

5. Lack of Proactive Defense: The unavailability of unidentified threat information hampers the ability to implement proactive defense measures. Effective cybersecurity strategies involve anticipating and mitigating threats before they can cause significant damage. However, without knowledge of emerging threats and malware strains, organizations are forced to rely on reactive measures, such as incident response and remediation after an attack has occurred.

Addressing the unavailability of unidentified threats and malware information is crucial to enhancing the overall security posture of cybersecurity systems. By leveraging advanced threat intelligence platforms, collaboration with security vendors, and incorporating blockchain-based malware detection systems, organizations can significantly reduce the risk of unexpected server or system failures. These solutions enable real-time information sharing, rapid detection, and response to emerging threats, bolstering the resilience and effectiveness of cybersecurity defenses.

1. **EXPECTED SOLUTION**

To tackle the challenges of unidentified threats and enhance cybersecurity, a decentralized blockchain network can be developed. This network will serve as a secure and tamper-resistant platform for storing malware signatures and the necessary technologies to address these threats. As time goes on, the decentralized network will continuously update and strengthen the system, making it more robust.

The proposed system will utilize a decentralized blockchain network, which is distributed among multiple participants. This ensures that no single entity can control or manipulate the stored information, providing strong protection against attacks. Each malware will have a unique signature stored in the blockchain, enabling real-time detection by comparing incoming files or network traffic.

In addition to malware signatures, the blockchain network will store the technologies and techniques required to resolve the associated threats. This comprehensive collection of information aids in the effective detection and mitigation of malware. As the blockchain network operates, new blocks containing updated signatures and threat resolution technologies will be added, ensuring that all nodes have access to the latest information.

Consensus mechanisms, such as proof-of-work or proof-of-stake, will be implemented to validate and agree upon updates to the blockchain. This ensures the integrity and consistency of the stored information across the network. By incorporating consensus, the system maintains a trustworthy and tamper-resistant repository.

Overall, the decentralized blockchain network provides a resilient and adaptable solution for storing and sharing malware signatures and threat intelligence. It fosters collaboration, transparency, and collective defense against evolving cyber threats. The continuous updates and strengthening of the system over time make it highly effective in enhancing cybersecurity.

# **RELATED WORK**

1. Smart Contracts and Chaincode A smart contract and the ledger, as seen from the perspective of an application developer, make up the core of a Hyperledger Fabric blockchain system. A smart contract specifies the executable logic that creates new facts that are added to the ledger, as opposed to a ledger, which contains facts about the present and past states of a collection of business objects. A chaincode can be used for low level system programming of the Fabric blockchain, however administrators often utilise it to aggregate related smart contracts for deployment. This chapter will concentrate on the existence of smart contracts and chaincode as well as their use.

2. A case study on business model innovations using Blockchain: focusing on financial institutions (JaeShup Oh SookMyung Women’s University, Seoul, Republic of Korea, and Ilho Shong Dongguk University, Seoul, Republic of Korea) Blockchain is a distributed ledger created by blocks containing transaction details connected in chronological order to form a series of chain. It is a distributed ledger in which participants of Blockchain peer-to-peer (P2P) network, and not the central administrator, generate blocks. The possibilities of use of Blockchain are acknowledged in many different fields, resulting in many developments and studies being conducted, and investments are being made actively (Cho and Park, 2017). From the perspective of financial institutions, the emergence of Blockchain does not just have technical significance – emergence of highly efficient database system – but has the possibility that if the business model of existing financial institutions or financial intermedi42 aries disappear, the financial services relying on them may disappear altogether or be partially replaced, and financial transaction patterns of consumers can be changed. On the other hand, it is expected that the areas of use of Blockchain will be expanded to become the means to increase financial inclusion beyond being a new business model for the financial institutions (Santander, 2015).

3. Building a Transparent Supply Chain (by Vishal Gaur and Abhinav Gaiha) Blockchain, the digital record-keeping technology behind Bitcoin and other cryptocurrency networks, is a potential game changer in the financial world. But another area where it holds great promise is supply chain management. Blockchain can greatly improve supply chains by enabling faster and more cost-efficient delivery of products, enhancing products’ traceability, improving coordination between partners, and aiding access to financing

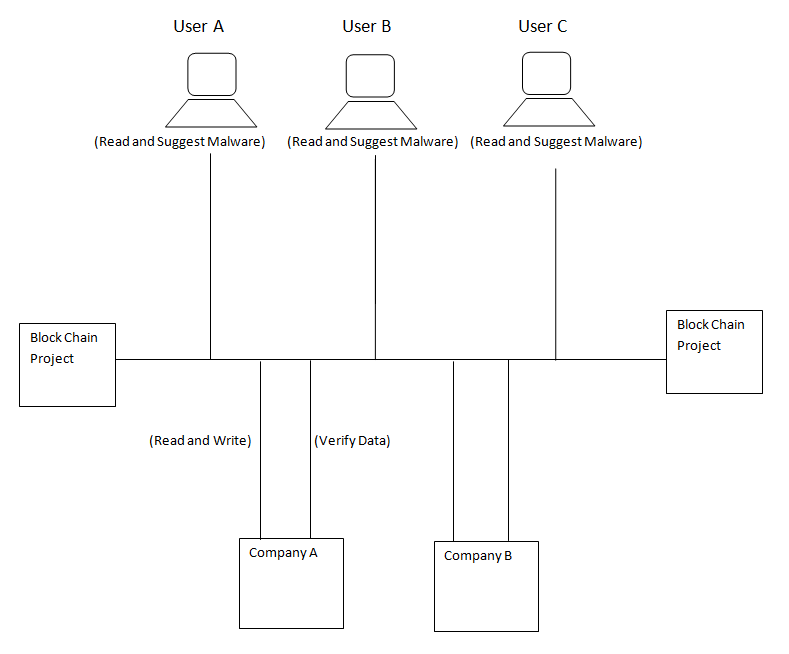
4. Blockchain in capital market The capital markets industry is going through profound changes in business dynamics due to regulation, technology-led market disruption, and transformed economics of core business areas. The era of digitalization has resulted in sweeping changes to the industry mindset – while many firms took nearly a decade to stabilize after the 2008 crisis, they were soon confronted with expectations of a new way of doing business as a result of the digital revolution. These new expectations meant changing norms in an industry with long-persisting issues

5. Blockchain in Institutional Capital Markets Hyperledger Composer is a set of collaboration tools for building blockchain business networks that make it simple and fast for business owners and developers to create smart contracts and blockchain applications to solve business problems. Built with JavaScript, leveraging modern tools including node.js, npm, CLI and popular editors, Composer offers business centric abstractions as well as sample apps with easy to test devops processes to create robust blockchain solutions that drive alignment across business requirements with technical development..

1. **METHODOLOGIES**

Blockchain technology works by creating an environment that is secure and transparent for the financial transactions of virtual values such as Bitcoin. Hash codes of each block keep records safe in the blockchain. This is mainly because irrespective of the size of the information or document, the mathematical hash function provides a hash code of the same length for each block. So, attempting to change a block of information would generate a completely new hash value . A network that is open to everyone and concurrently maintains user’s anonymity undoubtedly raises trust issues regarding the participants. So, to build the trust the participants need to go through several consensus algorithms such as Proof of Work and Proof of Stake. The digital cryptocurrency Bitcoin uses the first-ever blockchain technology . It is a digital store of value that enables peer to peer transactions over the internet without the intervention of a third party. The blockchain network is a decentralized structure that consists of scattered nodes (computers) that inspect and validate the authenticity of any new transactions that attempt to take place. This combine agreement is done through several consensus models by the process of mining. The process of mining demonstrates that each node trying to add a new transaction has gone through and solved the complex computational puzzle through extensive work and deserves to get a reward in return for their service.

1. **Block Diagram**

****

# **Model (purposed work)**

Given the immutable nature of a block chain and the fact that this particular project will function using one of the many models now available, the answer to the question of which model best fits a block chain is that none of them do.

1. **System Model**

In order to choose a specific model for this project, I read several research papers and articles about which model would be appropriate. Eventually, I came across a research paper titled "Block chain Enabled Smart Contract Based Applications: Deficiencies with the Software Development Life Cycle Models," where it was stated on line 6 of paper 14 that "due to the "immutability" feature of block chain enabled smart contracts, inherited from the underlying blockchain, this project is particularly

Reason why no preferable SDLC model is included in it. Research paper Source:

<https://arxiv.org/ftp/arxiv/papers/2001/2001.10589.pdf>

1. **Simulation Environment**

This project doesn't need a special system environment to work; all that is needed is for some basic block chain libraries to be assembled together with the necessary data in one location. The user can upload their file to websites like virus total and have their file scanned to get the name, and then they can scan that name in this immutable malware data block chain system to get the information and the solution. Additionally, there are no specific hardware requirements, making it as easy to use as possible. Additionally, because it is open source and accessible to everyone, more people can benefit from it.

1. **Simulation Parameters**

The Simulation parameters are basically the parameters on which this project would work, the backbone of this very project is depend on the immutable data that has been entered in it, in this the data of virus/malware data are the very parameters of this project and as the time passes more and more discovery of these threat would take place and respectively the data would be then get featured in this project as well and reason why as the time will keep passing on the very parameters would keep getting increase in it and it will be more and more useful.

# **Result and Analysis**

Since this project is entirely based on block chain technology, the chain of data keeps getting longer and longer as will user interaction, which will gradually strengthen the mass of this project. Here, according to the output of the programme, the total data of all viruses/malware will be shown along with their related solutions. The community that would be involved in the development of this project would be every authorised antivirus/security company since they would continually find and present the fundamental information about the malware so that other companies in the same industry would stay in touch with one another. and contribute to this open source system for the benefit of each individual.

The main debate around this project may centre on its effectiveness. Its effectiveness may not be very high, but as has been stated, it will continue to climb with time, making the project worthy for further development.

# **REFERENCES**

* Narayanan, A., Chandrasekaran, K. (2019). Blockchain-based malware detection and analysis. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 28-35). IEEE.
* Tariq, M. H., Yaqoob, I. (2018). A blockchain-based malware detection and mitigation framework for IoT devices. IEEE Access, 6, 29725-29733.
* Gupta, R., Kaur, P. (2021). Malware detection using blockchain technology. Journal of Ambient Intelligence and Humanized Computing, 12(7), 6875-6888.
* Alazab, M., Meinel, C., Song, H. (2018). Blockchain-based malware detection: a new solution for cyber security. In 2018 IEEE/ACM 4th International Conference on Big Data Computing Applications and Technologies (BDCAT) (pp. 211-216). IEEE.
* Abdellatif, A., Elshazly, H. (2019). Blockchain-based malware detection system for cloud computing environments. In 2019 5th IEEE International Conference on Computer and Communications (ICCC) (pp. 1575-1579). IEEE.
* Zhang, J., Li, J., Li, B., Guan, X. (2019). Malware detection based on blockchain technology. In 2019 IEEE International Conference on Smart Internet of Things (SmartIoT) (pp. 179-184). IEEE.
* Kuo, T. T., Lin, H. F., Chen, Y. L. (2020). BlockChain-based IoT Malware Detection and Prevention System. IEEE Transactions on Industrial Informatics, 16(4), 2763-2772. 45
* Haq, S. U., Ahmed, E., Yasin, U., Qureshi, A. R. (2021). A blockchain-based malware detection system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 12(12), 12707-12723
* Narula, S., Gupta, M., Jangir, S. (2020). A review of blockchain technology for cyber security. International Journal of Engineering and Advanced Technology (IJEAT), 9(4), 5024- 5030. This article provides an overview of how blockchain can be used for cyber security, including for malware detection and prevention.
* Dangi, N., Chaudhary, R., Chaudhary, V. (2020). Block Chain based Anti-Malware System. International Journal of Engineering Research and Technology, 9(9), 1248-1252. This paper describes a blockchain-based anti-malware system that can detect and prevent malware attacks by leveraging blockchain’s secure and decentralized architecture.
* Ren, X., Li, H., Wang, H., Huang, Y. (2019). Malware Detection Based on Blockchain Technology. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 754-758). IEEE. This conference paper presents a malware detection system that uses blockchain technology to securely store and share malware signatures, enhancing the accuracy of malware detection.