International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Implementation of Blockchain in Erp for Cybersecurity

Nedko Tagarev

University of National and World Economy, Department of National and Regional Security, Sofia, "8 - mi dekemvri" str.19
Email: *ntagarev[at]gmail.com. com*

Abstract: ***Blockchain technology has a role beyond cryptocurrency. The ERP also has a role beyond financial and accounting analyses. Blockchain is a key technology of the Fourth Industrial Revolution, removing the boundaries between physical and digital spaces. It creates new innovative opportunities and disrupts existing businesses by enabling decentralized digital transformation. This article examines ERP and blockchain technologies, as well as their combination. The added value that both technologies bring to cyber security and the possibility to increase this value by adding an additional effect is discussed. Considered as an example of contributing to the effect, the process of checking for vulnerabilities.***

Keywords: ERP, Blockchain, Cybersecurity

1. Introduction

"The scientific publication is in fulfillment of the objectives of the National Scientific Program "Security and Defense", financed by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the Decision of the Council of Ministers No.731 of October 21, 2021 and according to Agreement No. D01 - 74 /19.05.2022. "

Enterprise Resource Planning (ERP) software integrates and manages an organisation's core business processes in a centralised system. Our system gives organisations complete and real - time control over all essential business functions, including finance, supply chain, human resources, manufacturing, and customer relationship management.

Organisations can streamline operations, reduce costs, increase efficiency, and improve decision - making by implementing an ERP system. ERP software also helps to standardise business processes, ensure compliance with rules, and provide the only source of truth for data.

Examples of popular ERP software include SAP, Oracle, Microsoft Dynamics, and Infor.

ERP implementation can significantly improve an organisation's cybersecurity posture by providing a centralised system for managing and controlling access to sensitive data. Here are some ways in which ERP can help improve cybersecurity:

1) ERP implementation can significantly improve an organisation's cybersecurity posture by providing a centralised system for managing and controlling access to sensitive data.
2) ERP systems can provide role - based access control, ensuring that employees only have access to the data and applications they need to perform their work functions. Minimising the risk of insider threats and unauthorised access is crucial.
3) ERP systems can encrypt sensitive data and monitor access to it, helping prevent data breaches and cyber - attacks. They can also provide audit tests and logs, which can be used to detect safety incidents and investigate breaches.
4) ERP systems can help organisations comply with industry regulations and standards like GDPR, HIPAA, and PCI DSS by providing data protection, privacy, and compliance management tools.
5) In the event of a security incident, an ERP system can provide real - time alerts and notifications, enabling organisations to respond quickly and effectively to mitigate the incident's impact.
6) ERP systems can help organisations manage their third - party vendors and suppliers, ensuring they comply with security policies and procedures and provide adequate security for the data they handle.

Blockchain technology can be used in ERP systems to improve business processes' security, transparency, and efficiency. We can integrate Blockchain
into ERP in several ways:

1) Using blockchain technology can establish a supply chain that is both transparent and secure. [1]. Organisations can ensure products' authenticity, safety, and compliance by integrating Blockchain with an ERP system to track their movement from manufacturer to end consumer.
2) Blockchain technology enables the creation of automated intelligent contracts integrated with an ERP system to execute business processes like invoicing, procurement, and payments. Smart contracts can eliminate intermediaries and reduce fraud and error risk.
3) Blockchain can track assets such as inventory, equipment, and vehicles. By integrating Blockchain with an ERP system, organisations can have real - time visibility into the location, status, and condition of assets, optimising their use and reducing costs.
4) Blockchain provides a secure and transparent system for storing and sharing data, which can assist organisations in complying with regulations like GDPR, HIPAA, and PCI DSS. By integrating Blockchain with an ERP system, organisations can protect sensitive data and meet compliance requirements.
5) Blockchain enables organisations to conduct transactions without traditional financial institutions,

DOI: https://dx.doi.org/10.21275/SR231015000353

creating a decentralised financial network. [2] By integrating Blockchain with an ERP system, organisations can reduce transaction costs and increase financial processes' speed and efficiency.

Blockchain technology can improve cybersecurity in several ways:

1) Blockchain technology provides an immutable and tamper - proof data storage system. Data stored on a blockchain cannot be changed or deleted, and we record each transaction transparently and securely. This record helps prevent data breaches and cyberattacks, as any attempt to change or delete data on the Blockchain can be easily detected.
2) Blockchain technology works on a decentralised network, meaning that data is not stored in a central location. Data is securely distributed across multiple nodes in the network, making it extremely difficult for hackers to gain access and steal it. Decentralisation also reduces the risk of a single point of failure since the failure of one node does not lead to loss of data.
3) Blockchain technology can be used to verify the identity of users and devices in a secure and transparent manner. Blockchain - based identity management systems can help organisations prevent unauthorised access to sensitive data and systems.
4) Smart contracts are contracts that can execute themselves as the terms of the agreement are directly written into code. This programming feature allows them to function automatically when certain conditions are fulfilled. Smart contracts can automate cybersecurity processes, like threat detection and incident response. Reducing human error and increasing speed are critical in improving cybersecurity operations.
5) Blockchain technology uses advanced encryption algorithms to secure data and transactions. These transactions make it difficult for hackers to break the encryption and access sensitive data.

2. Theoretical Background

The United States is significantly transitioning towards a more advanced, flexible energy infrastructure. However, this transition comes with its own set of challenges. As the integration of distributed energy generation resources and grid - connected smart devices continues to advance, utilities are presented with new and exciting opportunities. However, this advancement also poses significant security challenges due to the unprecedented volume, speed, and complexity of data transfers and transactions. By addressing these challenges head - on, utilities can ensure a safe and reliable energy network for all. The power grid is already vulnerable to cyberattacks, and these new developments put it at an increased risk.

Pacific Northwest National Laboratory (PNNL) is currently evaluating and testing distributed ledger technologies (DLTs), such as blockchains, to enhance the nation's power grid's security, reliability, and resilience

. These innovative technologies can offer a decentralised and tamper - proof platform for secure exchange of information and transactions among the various energy resources and devices connected to the grid. DLTs can also help in the early detection and prevention of cyberattacks and ensure the uninterrupted and efficient functioning of the power grid. [3] Adopting blockchain technology in cybersecurity could revolutionize how we secure digital data. Its inherent decentralisation, verifiability, and immutability characteristics can offer unprecedented data authenticity, reliability, and integrity. In order to effectively address security challenges in the digital world, it is crucial to understand the factors that influence adoption decisions. Doing so can create a safer and more secure digital environment for everyone. [4]

Companies like Oracle, SAP, Infor sell ERP systems as packaged software. ERP systems can be standard or bespoke. An important point to note is that while ERP transforms an organisation's internal operations and how it interacts with stakeholders, it does not connect one organisation to another or create a network among partners/stakeholders. […] With Blockchain, ERP systems can integrate across partners and provide immutable data and transaction audit trails. [5]

The enterprise resource planning (ERP) software is an integrated database system that enables businesses to centralise their data, allowing them to manage and control their inner processes, thus enabling informed decision - making for future operations. The system's real - time updating capabilities ensure the smooth functioning of all industry sectors through constant communication between various functions, thereby reducing the likelihood of severe errors. The immediate access to data also allows for quickly identifying any potential setbacks in ongoing processes.

The software's functionality empowers enterprises to streamline their operations, increasing efficiency while reducing risks and costs. By leveraging the software's capabilities, firms can make informed decisions that optimise their processes and maximise resources, leading to improved bottom - line performance. […] The integration allowed for the optimisation of operations across multiple companies while facilitating trusted data - sharing. Data - sharing is particularly beneficial for financial transactions, as banks and financial institutions can exercise greater control over internal data operations, ensuring secure processes. By using Blockchain, financial organisations can handle sensitive information with the least risk, thus providing their clients safe and reliable services. [6] We are still unsure if Blockchain can operate the same number of transactions as ERP systems with his current version. It has not yet proven its performance. Nevertheless, there is much work to prove its capabilities, and we believe that improving blockchain technology will also increase its adoption. That is why we propose developing the integration between ERP and blockchain technology to benefit from both advantages. We believe that the future is the integration between technologies rather than replacement. [7]

ERP software oversees and streamlines all significant business processes. It is a database centre point that enables an organisation to do back - office work efficiently and continuously with the assistance of integrated applications. As the ERP framework utilises a database administration framework, Blockchain also utilises a real - time scalable database that encourages the verification of ideas, stages, and applications. [8] By integrating Blockchain technology, organisations can achieve coherence between supply and demand; this reduces stockouts and lost sales, leading to more significant business advances and competitive supply chains. [9]

Organisations implement Enterprise Resource Planning (ERP) systems to manage business operations, including accounting, procurement, project and supply chain management, risk and compliance. It is increasingly recognised that blockchain technology offers an attractive option for the secure and immutable storage of data for these operations. Blockchains are decentralised ledgers composed of an immutable record of data shared across a cluster of computers or "nodes, " which register transactions in "blocks" of data, thus providing a secure and transparent method of data storage. In blockchain implementation, an integrating layer for transactions is deployed, becoming an integral part of the core of any enterprise blockchain project. Organisations must leverage blockchain technology to ensure a secure and highly efficient method of managing their business operations. [10] At the heart of the Blockchain lies a communal digital ledger, which is immutable. Transactions are recorded in a public or private peer - to - peer network. As all network members share the Blockchain, it is a single source of truth. [11]

Centralised networks with limited IP addresses are vulnerable to cyber attacks, which hackers can easily penetrate using simple schemes such as phishing. Once hackers gain access, they can cause extensive damage, as recent ransomware attacks cost companies an average of USD 4.24 million. However, the decentralised nature of blockchain technology presents a possible solution, as these complex networks are much more difficult for hackers to infiltrate. [12]

The cybersecurity industry is a beneficiary of Blockchain's unique features that create an almost impenetrable wall between the hacker and the system. The inherent decentralisation, cryptographic principles, and consensus - based nature of Blockchain make it impossible for data to be tampered with. Additionally, it provides high standards of data transparency and integrity. [13]

In cybersecurity, Blockchain provides an alternative path to achieve greater security. Most people do not commonly use this path, which is less welcoming to cybercriminals. This approach decreases vulnerabilities, offers robust encryption, and improves data verification, potentially eliminating the need for passwords. [14] Blockchains require consensus protocols to achieve agreement among participants when adding a new block. As central authority is absent, the consensus protocol is highly vulnerable to attacks like the majority (51%) and selfish mining attacks. These attacks can easily take control of the blockchain network and dictate its consensus decisions, making it critical to evaluate and test the consensus protocol thoroughly to ensure that it can always reach the expected resolution without fail. [15] Protecting blockchain network access is fundamental in securing data access (particularly in private blockchains). When an attacker can access the blockchain network, they can access all its data. Therefore, authentication and authorisation controls must be implemented, similar to other technologies. [16] When developing an enterprise blockchain application, it is crucial to prioritise security at every layer of the technology stack. Additionally, it is essential to consider how to handle governance and permissions for the network. An all - encompassing security strategy for an enterprise blockchain solution comprises traditional and technology - specific security controls. [17] Blockchain networks have a limited block volume and transaction processing capacity per second, making evaluating the network's scalability crucial. Adopting Blockchain technology involves replacing existing systems, which can pose challenges for companies. [13]

3. Model for Implementation of Blockchain In ERP for Cybersecurity and Example

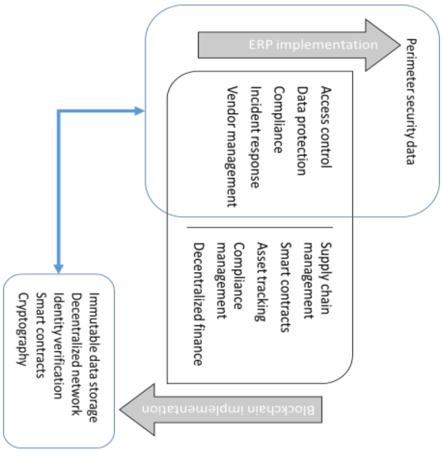

Figure 1: A model for adding value to cybersecurity by implementing Blockchain in ERP

There are many differences between an organisation's traditional cybersecurity and blockchain cybersecurity. The question is how to use these differences to mutual advantage. The first and foremost difference has to do with perimeter defence. Classic cybersecurity primarily protects an organisation's information perimeter, including its information assets. This protection is based on specific protection mechanisms created by the organisation or a trusted party. With blockchain security, we do not have a security perimeter. The main idea is that based on smart contracts, every single transaction is recorded by all participants in the chain, making it almost impossible to manipulate the information.

Another critical area is the so - called trust zones or places where data is stored, shared and processed. On the one hand, when it comes to classic protection, these places are managed by the interested party or by a trusted third party, which may be the relevant service provider. With Blockchain, there is no such environment, as the places to store the information may be unknown, and the participants in the process are also unknown. In this case, security is ensured by cyclically checking the code and identifying previous omissions and errors that can be corrected.

One of the fundamental activities in cybersecurity is vulnerability assessment. It involves a testing process to identify and categorise security defects with appropriate levels of severity. This process can involve various automated and manual techniques with different degrees of thoroughness to ensure comprehensive coverage. Using a risk - based approach, vulnerability assessments can target different technology layers, including host, network, and application layers. [18]

The classic vulnerability check goes through three stages:
1) Check for vulnerabilities;
2) Treatment of vulnerabilities;
3) Validation of the performed activities.

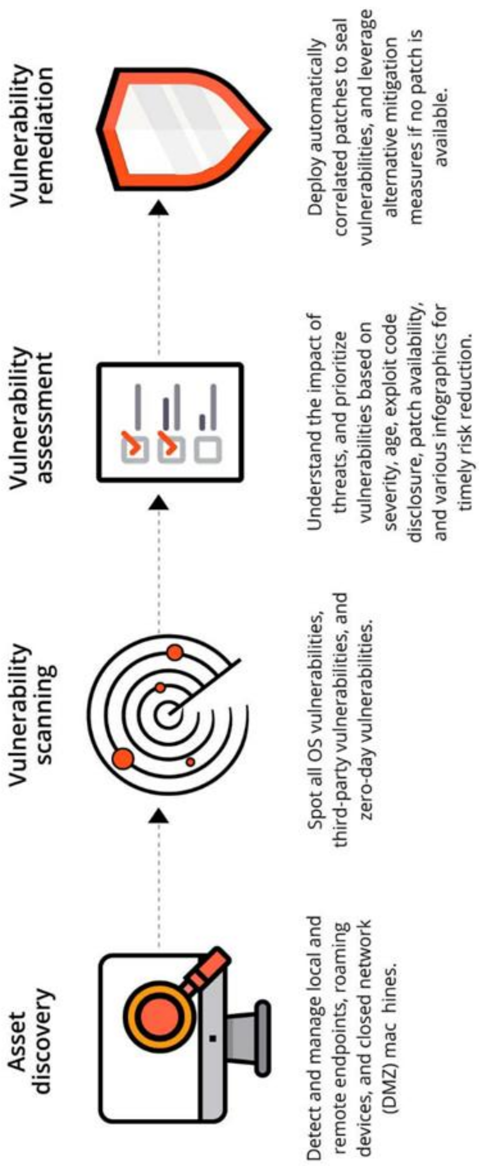
Vulnerability remediation
Deploy automatically correlated patches to seal vulnerabilities, and leverage alternative mitigation measures if no patch is available.
Vulnerability assessment
Understand the impact of threats, and prioritize vulnerabilities based on severity, age, exploit code disclosure, patch availability, and various infographics for timely risk reduction.
Vulnerability scanning
Spot all OS vulnerabilities, third-party vulnerabilities, and zero-day vulnerabilities.
Asset discovery
Detect and manage local and remote endpoints, roaming devices, and closed network (DMZ) mac hines.

Figure 2: Vulnerability Assessment Process [source: https: //www.manageengine. com/vulnerability - management/vulnerability - assessment. html [19]]

First, it is extremely important that each of these activities is performed by a different person to obtain a reliable result. When checking for vulnerabilities, we use ready - made tools or those developed by our organisation. We enter specific data, an IP address, by identifying known vulnerabilities. This process is semi - technical work. The next step is the treatment. Treatment involves patching, firmware, software updates, etc. It should be remembered that only some vulnerabilities can be fixed.

Nevertheless, it should be paid attention to the consequences if exploited by an attacker. In this part, we have a semi - technical activity. The third step is validation of the performed activities. Technical knowledge is optional for this step. It is related to the audit of the implementation of the set goals and tasks concerning cyber security. Usually, these goals and tasks are related to a specific time and volume of work.

It is possible to exercise greater control over these processes by utilising ERP and Blockchain technologies. I. e., activity flows are accounted for through ERP, and transaction validation is done through Blockchain.

The main idea behind implementing the Blockchain lies in the possibility of blocking the processing of the content and preserving the integrity of the information. With Blockchain, it is almost impossible to present alternative data. This is due to smart contracts. I. e., the transactions made are stored in many places, which allows to establish the truth of the information and the truthful information.

Conclusion

Blockchain technology improves cloud security by enhancing data confidentiality, integrity, and availability. Depending on the chosen Blockchain solution and technology, an organisation can configure the necessary security levels for the system, even down to the level of an individual record, if required. [20]

Implementing an ERP system can enhance an organisation's cybersecurity by offering a centralised platform for managing and regulating sensitive data access, monitoring usage, and providing instant alerts and notifications in case of security breaches. Blockchain technology allows users to operate all types of transactions securely and transparently. Blockchain has become vital to Enterprise Resource Planning (ERP) as it can verify and authenticate identities. This feature is crucial for many business transactions. Blockchain offers digital certificates, allowing easy identification, verification, and authentication of members' identities. This is particularly useful for audits since Blockchain immutably records every identity and transaction. By using Blockchain, organisations can be sure that all members' identities are accurate and secure, making the auditing process more efficient and reliable. This makes it possible to track who did what, when and how accurately. [21]

Integrating blockchain technology with an ERP system can create a secure, transparent, and efficient process for managing data, reducing costs and risks.

Overall, blockchain technology can provide a secure and transparent system for storing and sharing data, verifying identities, and automating cybersecurity processes, reducing the risk of cyber - attacks and data breaches.

The literature suggests that Blockchain can improve supply chain management, data sharing, network architecture, business process automation, and auditability in ERP systems. However, successfully implementing blockchain technology in ERP systems requires careful consideration of its limitations, potential risks, and compatibility with existing ERP infrastructure.

Blockchain in ERP is still a concept that has yet to be found in a business application. Embracing using ERP data to establish a cybersecurity posture is still tricky. On the other hand, the advantages of blockchain technology concerning the problem under consideration are undeniable.

References

[1] 'Top 10 uses of blockchain in supply chain', Mar.01, 2023. https: //supplychaindigital. com/top10/top - 10 - uses - of - blockchain - in - supply - chain (accessed Apr.13, 2023).

[2] 'Blockchain Facts: What Is It, How It Works, and How It Can Be Used', Investopedia. https: //www.investopedia. com/terms/b/blockchain. asp (accessed Apr.13, 2023).

[3] 'Blockchain for Cybersecurity and Grid Modernization | PNNL'. https: //www.pnnl. gov/projects/blockchain - cybersecurity - and - grid - modernization (accessed Apr.12, 2023).

[4] R. M. Parizi, A. Dehghantanha, A. Azmoodeh, and K. - K. R. Choo, 'Blockchain in Cybersecurity Realm: An Overview', in Blockchain Cybersecurity, Trust and Privacy, K. - K. R. Choo, A. Dehghantanha, and R. M. Parizi, Eds., in Advances in Information Security. Cham: Springer International Publishing, 2020, pp.1–5. doi: 10.1007/978 - 3 - 030 - 38181 - 3_1.

[5] A. Banerjee, 'Blockchain Technology: Supply Chain Insights from ERP', in Advances in Computers, Elsevier, 2018, pp.69–98. doi: 10.1016/bs. adcom.2018.03.007.

[6] 'Why integrating Blockchain and ERP is a Great Idea - Blockchain Council', May 21, 2021. https: //www.blockchain - council. org/blogs/why - integrating - blockchain - and - erp - is - a - great - idea/ (accessed Apr.12, 2023).

[7] M. Hader, A. El Mhamedi, and A. Abouabdellah, Blockchain Integrated ERP Fora Bette Supply Chain Management.2020, p.143. doi: 10.1109/ICIEA49774.2020.9102084.

[8] T. Parikh, 'The ERP of the Future : Blockchain of Things'.

[9] 'Blockchain and trade finance', IBM Blog, Mar.08, 2021. https: //www.ibm. com/blog/blockchain - and - trade - finance/ (accessed Apr.12, 2023).

[10] E. C. Rica, 'Why Integrating ERP Systems into Blockchain is a Great Idea?', Medium, Nov.24, 2020. https: //eoscostarica. medium. com/why - integrating - erp - systems - into - blockchain - is - a - great - idea - e384b298a4a8 (accessed Apr.12, 2023).

[11] S. Orthmann, 'The Role of Blockchain in ERP: Beyond Cryptocurrency'. https: //www.erpadvisorsgroup. com/blog/blockchain - erp - beyond - cryptocurrency (accessed Apr.12, 2023).

[12] I. at Work, 'How Blockchain Will Revolutionize Cyber Security', IEEE Innovation at Work, Mar.16, 2022. https: //innovationatwork. ieee. org/how - blockchain - will - revolutionize - cyber - security/ (accessed Apr.12, 2023).

[13] 'Role of Blockchain in Cybersecurity', GeeksforGeeks, Sep.19, 2021. https: //www.geeksforgeeks. org/role - of - blockchain - in - cybersecurity/ (accessed Apr.12, 2023).

[14] I. Limited, 'Blockchain Technology in Cybersecurity | Infosys'. https: //www.infosys. com/insights/cyber - security/cybersecurity - blockchain. html (accessed Apr.12, 2023).

[15] 'Blockchain has high potential but be aware of cyber threats', World Economic Forum, Feb.21, 2023. https: //www.weforum. org/agenda/2023/02/blockchain - has - high - potential - but - beware - of - cyber - threats - 8642651f20/ (accessed Apr.12, 2023).

[16] E. Piscini, D. Dalton, and L. Kehoe, 'Blockchain & Cyber Security. Let's Discuss An assessment of the security of blockchain technology, Deloitte, 2022, [Online]. Available: https: //www2. deloitte. com/tr/en/pages/technology - media - and - telecommunications/articles/blockchain - and - cyber. html

[17] 'What is Blockchain Security? | IBM'. https: //www.ibm. com/topics/blockchain - security (accessed Apr.12, 2023).

[18] 'What Is a Vulnerability Assessment and How Does It Work? | Synopsys'. https: //www.synopsys. com/glossary/what - is - vulnerability - assessment. html (accessed Apr.11, 2023).

[19] 'Vulnerability Assessment Tool | Security Vulnerability Assessment - ManageEngine Vulnerability Manager Plus'. https: //www.manageengine. com/vulnerability - management/vulnerability - assessment. html (accessed Apr.11, 2023).

[20] 'Blockchain + Cybersecurity | CSA'. https: //cloudsecurityalliance. org/research/topics/blockchain/ (accessed Apr.12, 2023).

[21] Y. Benjelloun, '7 ways integrating blockchain can boost your ERP capabilities'. https: //www.finboot. com/post/7 - ways - integrating - blockchain - can - boost - your - erp - capabilities (accessed Apr.12, 2023).

Author Profile

Dr. Nedko Georgiev Tagarev is a senior assistant in the Department of "National and Regional Security" at the University of National and World Economy. He graduated from the Sofia Mathematical High School. He teaches the disciplines "Economic Analysis and Planning", "Cyber Security", "Internet Security", etc., in the bachelor's and master's degrees. There are over 50 publications in Bulgaria and abroad, in the fields of Cyber Security (Information Security), Economic Analysis and Security Policies. He participated in more than 10 projects (university and international). His interests are in the areas of economic analysis and planning in defense and security, security policy, corporate security and cyber security. He is a member of national and international organizations. Participant in dozens of national and international conferences.