



Enhancing Sustainable Development Through Blockchain: A Study on Risk Management and Data Integrity

Ozden Senturk^{*}, Ali Baghirov^{*}

Economy Department, Institute of Social Sciences, Istanbul University, 34000 Istanbul, Turkey

^{*} Correspondence: Ozden Senturk (ozden.senturk@ogr.iu.edu.tr)

Received: 10-10-2023

Revised: 12-11-2023

Accepted: 12-20-2023

Citation: Senturk, O. & Baghirov, A. (2023). Enhancing sustainable development through blockchain: A study on risk management and data integrity. *J. Organ. Technol. Entrep.*, 1(2), 110-126. <https://doi.org/10.56578/jote010204>.



© 2023 by the authors. Published by Acadlore Publishing Services Limited, Hong Kong. This article is available for free download and can be reused and cited, provided that the original published version is credited, under the CC BY 4.0 license.

Abstract: In the realm of sustainable development, the integrity and transparency of data play pivotal roles. This study investigates the utility of blockchain technology in augmenting the monitoring and auditing facets of sustainable development initiatives. It is posited that blockchain's inherent attributes—namely its robustness in ensuring data integrity and fostering trust—hold substantial promise in enhancing environmental performance and informed decision-making. Specifically, applications in environmental impact reporting and supply chain management are examined. The findings suggest that blockchain technology can significantly contribute to these areas by offering unprecedented levels of transparency and reliability in data handling. However, the potential of blockchain is not without its challenges. The study underscores the imperative of addressing network security and data privacy concerns. It is argued that effective governance structures and risk management strategies are essential to fully leverage the benefits of blockchain, whilst concurrently mitigating inherent risks. The integration of blockchain into risk management processes notably impacts environmental, social, and corporate governance (ESG) objectives. A critical analysis of the risks associated with blockchain-based processes is conducted, culminating in the development of strategic recommendations aimed at minimizing these risks. The ultimate goal is to bolster corporate effectiveness, efficiency, and yield cost benefits through the deployment of secure and reliable blockchain solutions. The study posits that the judicious integration of blockchain technology can lead to substantial improvements in organizational performance, particularly in the context of sustainable development. Emphasis is placed on the need for continual analysis and refinement of risk management strategies in the evolving landscape of blockchain technology, to ensure that its application remains both impactful and responsible.

Keywords: Risk; Risk management; Blockchain; Blockchain technology; Digitalism

JEL Classification: G32, H11, M10

1. Introduction

The concept of risk management has been used since the 1940s to help organizations achieve their goals faster and more completely. Although there is more than one definition of the concept of risk, in general terms, risk is defined as the probability of an event that will affect an organization's achievement of its goals and is evaluated as a combination of the concepts of impact and probability (Bozkurt, 2016).

In other words, risk management, as a concept, is the procedure for managing any risks that may arise in organizations, evaluating these risks, and taking measures to eliminate the identified risks at the most appropriate time. Over time, the process of moving from the risk management model to the enterprise risk management implementation model has accelerated with the realization that risk management is not sufficient to address all the effects of risk. This new methodology emphasizes a proactive approach, including the impact of events and processes on each other. Adopting and implementing this method has been the most fundamental way of reducing the risks arising from the uncertainty of the future and keeping them within acceptable limits (Pehlivanlı, 2014).

Beyond the use of traditional methods, blockchain technology, which is at the heart of our study, enables the peer-to-peer transfer of digital assets without the need for an intermediary or centralized system. The link between

traditional risk management practices and the integration of blockchain technology lies in the transformative capabilities that blockchain brings to address the limitations of traditional risk management. Traditional risk management practices often involve centralized systems, manual processes, and reliance on intermediaries, which can lead to inefficiencies, a lack of transparency, and increased susceptibility to fraud. Although blockchain technology also offers a decentralized and secure framework that can revolutionize the identification, assessment, and management of risks, it is possible to divide the relationship, stages, and connections between blockchain technology and traditional risk management into several parts, and we can list them as follows:

Decentralization and Transparency:

Traditional Risk Management: Traditional risk management always relies on centralized databases and systems, which makes it vulnerable to potential delays and failures at times.

Blockchain Integration: It is a transparent system that is resistant to any intervention. It is connected to a decentralized network system, which ensures that all participants can access the information there smoothly and clearly. All these features eliminate fraud and manipulation maneuvers.

Immutable Recordkeeping:

Traditional Risk Management: Traditional risk management is a system that fails to keep track of past and current transactions, as well as events, and is prone to difficulties in this regard.

Blockchain Integration: Blockchain technology is a technology that has a system that records and protects all information included in the system. Any data entered into the system cannot be changed, and this data cannot be interfered with in any way. This specificity provides reliability and efficiency for blockchain technology. Thus, all kinds of data theft and fraud are prevented.

Smart Contracts for Automated Compliance:

Traditional Risk Management: Unlike traditional risk management, blockchain technology does not automatically record our data. Data must be manually included in this system. The fact that the data is manual makes your intervention in the system realistic. While human intervention is not possible in blockchain technology, human activity and human intervention are inevitable in traditional risk management.

Blockchain Integration: The system utilizes smart contracting, which is self-executing contracts with hard-coded rules. This simplifies the compliance measure, ensures the application of predefined guidelines, and reduces the risk of non-compliance through automatic triggering action when certain conditions are met.

Enhanced Security:

Traditional Risk Management: Centralized systems are more resistant and equipped against cyber threats and security vulnerabilities.

Blockchain Integration: Blockchain technology uses cryptographic techniques to ensure the reliability of transactions made within it. These techniques provide an environment that is resistant to tampering and cyberattacks. The actions taken reduce the problem of unauthorized access and data breaches to zero.

Efficiency and Cost Reduction:

Traditional Risk Management: Manual systems and processes used in traditional risk management contribute to increased operational costs.

Blockchain Integration: It reduces the total cost and provides an efficient process. It moves the process forward without intermediaries, which causes the process to progress and conclude faster. At the same time, cost-effective processes are common for this system. All of these contribute to operational efficiency.

Supply Chain Transparency:

Traditional Risk Management: The traditional risk management system has difficulties in the supply chain system regarding traceability and transparency. These difficulties have a negative impact on the risk assessment process.

Blockchain Integration: It guarantees a transparent and traceable supply chain by recording every transaction in an immutable ledger. This transparency helps identify and reduce the risks related to the supply chain. Building blockchain technology provides a number of benefits in terms of overcoming the constraints of conventional risk control. These limitations can include a lack of transparency, data modification, and central control. We will explore these topics through supporting cases or examples:

Transparency:

Traditional limitation: When we look at supply chains, financial transactions, and general processes, we can say that traditional risk management is invisible in terms of these transactions. The issue of invisibility raises questions in terms of transparency and reliability. Therefore, sometimes there are difficulties in verifying and interpreting the data correctly.

Blockchain solution: Unlike the difficulties of traditional risk management mentioned above, the blockchain system offers transparency in terms of obtaining, storing, accessing, and interpreting data.

Example: IBM Food Trust uses the blockchain to boost transparency in the supply of food. It reduces the risk of contamination and provides food security, allowing customers and consumers to track the origins and journey of the product.

Data Manipulation:

Traditional limitation: centralized systems and databases are vulnerable to risks. It is open to data manipulation. The reason for this is that once data is entered into these systems, it cannot be changed again.

Blockchain solution: The decentralized nature of blockchain makes it resilient. Each block in the chain contains a unique identifier (hash) of the previous block, creating a secure and tamper-proof record.

Example: Everledger uses blockchain to track and verify the authenticity of diamonds. This ensures that information about each diamond, including its origin and ownership history, cannot be tampered with, reducing the risk of fraud in the diamond industry.

Centralized Control:

Traditional risk management is generally highly sensitive and vulnerable to attacks and system failures. In this aspect, traditional risk management is mostly used in banks and central financial authority institutions.

Blockchain solution: Unlike traditional risk management, which depends on the central authority system mentioned above, blockchain is versatile and eliminates the dependence on a single central system. In this respect, blockchain technology creates a system that is more reliable and protected against threats.

Example: Bitcoin, which is the first and more common blockchain technology that we can take as an example, operates as a blockchain-based system without being dependent on a central authority. It does not need intermediaries and is not subject to censorship. At the same time, it cannot be managed by a single institution or organization. All these opportunities allow it to provide a safer space.

Smart Contracts for Automated risk Management:

Traditional Restrictions: Traditional methods and traditional contracts and agreements have a more complex structure in nature. Their mixed structure allows them to work with more than one tool, but when more than one opportunity arises, some errors, delays, and risks arise.

Blockchain Solution: Intelligent agreements are fully self-executing agreements in which the terms of the agreement are written straight into the code. By automating and implementing the application of the contract conditions, they minimize the risk of the errors and defaults that are associated with conventional agreement management.

Example: Being one of the most widely used smart contract blockchains, Ethereum provides a more clear, efficient, and transparent way of automatically identifying contracts. For example, insurance policies can be auto-triggered, and payments can be carried out based on pre-defined terms, thereby lowering the fraud risk and delays.

Blockchain brings a new perspective to traditional risk management. It is a technology that is known for its decentralized nature and is increasingly getting attention. Thanks to its cryptographic nature, it provides the reliability of data and is resistant to manipulation because of its immutability. With these qualities, it can lead to more effective identification, assessment, and mitigation of risks by improving the risk management process. At the same time, blockchain technology also brings risks. Like any new technology, there may be vulnerabilities and errors. Nevertheless, the advantages and conveniences it offers are attracting more and more attention and interest day by day (TUBITAK, 2023).

At this point, it is necessary to mention the concept of risk. Risk can be defined as the possibility that situations, events, and factors that may occur in the future may affect the achievement of the institution's objectives. Over time, the concept of enterprise risk management has evolved to replace the concept of risk management, which refers to taking actions to identify, assess, manage, and mitigate risks at all levels using specific methodologies. Enterprise risk management, which was developed as a result of the realization that traditional risk management was not sufficient to achieve the objectives of institutions, can be defined as a process based on the identification and management of risks to provide reasonable assurance that the basic organization of the institution will achieve its objectives. The concept of enterprise risk management has been developed to prevent factors such as increasing competitiveness of organizations, economic fluctuations or uncertainties, compliance with corporate strategy, compliance with developing information technologies, reducing the effectiveness of business and transaction processes, and contributing to the achievement of corporate objectives.

Objectives such as adapting to changing conditions, reducing operational losses, effective communication, efficient resource allocation, harmonizing risk management and internal structure, realizing the strategic plan, identifying opportunities, and taking timely action against threats have raised the expectations of institutions from the concept of enterprise risk management to a high level; however, today, institutions have turned to modern information technology solutions and applications to increase their competitiveness, provide cost advantages, enable data usage, and ensure information security. Blockchain is a technology that can meet expectations as a comprehensive infrastructure or reliable database that is believed to have these features. It has been found that blockchain, which is a new technology, has advantages due to its structure as well as inherent risk.

2. Literature Review

The body of existing literature pertaining to blockchain integration and sustainable risk management is characterized by a diversity of research domains. Investigations in the field of blockchain and risk management

predominantly focus on how blockchain affects risk management projects, as highlighted by El Khatib et al. (2023). A significant aspect of the literature concentrates on the relations and effects of blockchain on the risk management process. El Khatib et al. (2023) examine the impact of blockchain technology and IoT on project risk management. Blockchain and the Internet of Things (IoT) provide the platform that project managers use to mitigate risks. The objectives of the study are to explore the impact of blockchain and IoT on managing risks during project planning, execution, implementation, and closure. Therefore, the study identifies the opportunities that project managers have to optimize their project risk management. The study uses a structured questionnaire and interviews with a sample of 30 respondents to understand the correlations between variables. The findings show that businesses use IoT and blockchain technology platforms to create risk mitigation plans and implement and periodically update project management tools. When we scan the literature, another piece of research we come across on this subject is "Smart Solutions: Risk Management and Blockchain Technology, which is written and published by Bashynska et al. (2019). The study examines, describes in more detail the features of the functioning of crypto-assets and blockchain technology, identifies their inherent risks, and proposes a mechanism for managing these risks by incorporating crypto-asset risk management units in the culture of risk management. Yao & Qin (2021) examine blockchain-based supply chains and financial risk management. The study examines the current supply chain finance risk management, which has problems such as asymmetric operation information and difficult risk control. For this reason, the paper proposes research on supply chain finance risk management based on block chain technology. Combining the technical characteristics of block chain and the business model of supply chain finance, we analyze the causes of its operational risk, trade authenticity risk, payback risk, and contingency risk, and use the physical sensors to react and track data in real time to improve the efficiency of supply chain risk control; replace the signing of legal documents in various disciplines with electronic signatures to solve the problem of trade authenticity risk; program the transaction contract and contract-related clauses to provide trust for both sides of the transaction and improve transaction efficiency. Implement a comprehensive risk management strategy, design early warning and emergency management processes, and realize supply chain financial risk management based on block chain technology. Nathani & Singh (2020), in their article "Using Blockchain for Effective Risk Management in Supply Chain: A Qualitative Study," analyze and explore the possibility of using blockchain for effective risk management in the supply chain of today's company by doing a qualitative study. In this exploratory study, experts were identified in the field of analysis, and they were interviewed and probed further for their opinions and better understanding of the field of study. As we see in the literature review, different types of articles have been written and presented on this subject. However, the subject is new and open to further research.

2.1 Concepts of Risk, Risk Management and Corporate Risk Management

This section provides general definitions of the terms risk, risk management and enterprise risk management.

2.2 Definition of Risk

Risk is defined as events that have the potential to occur in the future in the course of an organization's activities. In another definition of the concept, risk is defined as possible negative deviations from the results determined to achieve the goal (Gönen, 2017).

According to another definition, risk is considered "a combination of probabilities regarding the consequences of an event, and it is generally stated that the term risk is used only in cases where there is at least one possibility of negative consequences, and in some cases, the risk arises from the possibility of deviation from the expected result or events". According to the definition of the United Nations Economic Commission for Europe, risk is defined as the probability of a loss or the combination of the probability of damage to property or the environment and the severity of the damage (Kalkan & Deniz, 2013).

As can be seen from the definitions, risk is the probability of an event occurring due to the positive or negative uncertainty of an event affecting potential gain or loss. The point to be considered here is the concept of "probability." The concept of risk, for instance, can no longer determine whether there will be a gain or loss as a result of an event if its occurrence is certain. This is because the occurring event has left the framework of probability and has acquired the phenomenon of certainty (Attila, 2015).

Risk, in the context of blockchain technology, refers to the potential threats, vulnerabilities, and uncertainties associated with the adoption, implementation, and use of blockchain solutions within an organization. These risks can manifest themselves in various forms, including technological, regulatory, operational, and strategic challenges. Understanding and managing these risks is critical for organizations seeking to effectively realize the benefits of blockchain technology.

2.3 Risk Management

The concept of risk is defined as events or situations that may have a negative impact on the achievement of

goals and objectives, while events or situations that may have a positive impact on goals and objectives can be expressed as opportunities. The resulting concept of risk management includes stages such as identifying, determining, evaluating, reviewing, and reporting risk-related strategies and should be applied consistently throughout the organization. This stable and consistent application has led to another concept, enterprise risk management. Corporate risk management, which will be discussed in the following sections, can be expressed as a process that requires the assessment of institutions or organizations as a whole (Financial Reporting Council, 2014).

In other words, risk management is the process of identifying, assessing, managing, and controlling potential events and situations in order to provide reasonable assurance that the organization's objectives will be achieved. Institutions and organizations can create a risk portfolio at a general level to perform risk management. To do this, they should collect the risks they are likely to encounter and create a whole with their risk profiles. In this way, they can also determine the correlation between risks (Gönen, 2017; Kayahan & Murat, 2022).

Risk management is a system that includes stages such as risk identification, risk classification, risk analysis, risk tolerance, and risk response. Institutions have the opportunity to turn risks into opportunities if they establish a risk management system appropriate to their organizational structure.

Risk management in the context of blockchain involves the systematic identification, assessment, and mitigation of potential risks associated with the use of blockchain technology (Atilla, 2015). It includes strategies, policies, and processes aimed at maximizing potential benefits while minimizing the negative impact of risks. Effective risk management in the blockchain space involves a combination of technological measures, regulatory compliance, and strategic planning as shown in Figure 1.

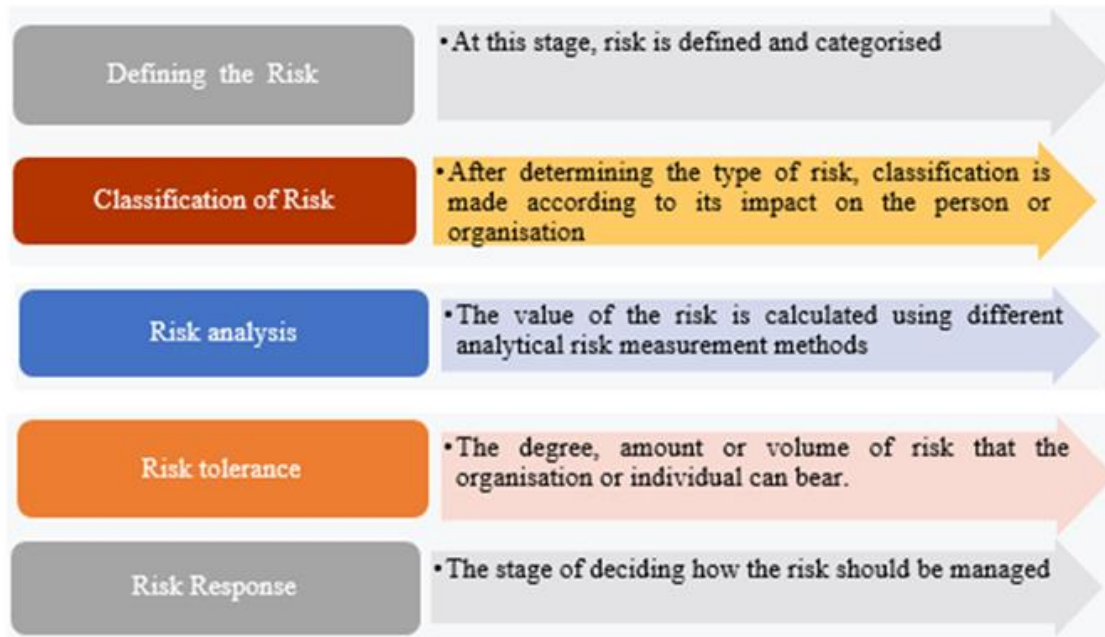


Figure 1. Risk management stages (Atilla, 2015)

2.3.1 Explanation of blockchain's influence on risk and risk management within organizations

Blockchain structure and technology have huge and undeniable effects on risk and risk management, as well as on institutions and organizations. The unique features offered by blockchain technology (decentralized management system form, smart contracts, security, stability, etc.) enable efficient risk management. In the examples below, data on what kind of effects these positive aspects have on companies and institutions is presented:

Decentralization and Reducing Single Points of Failure:

Influence on Risk: Traditional risk management and traditional centralized systems remain vulnerable to single points of failure. These vulnerabilities make traditional risk management vulnerable to systemic failures or cyberattacks.

Blockchain Impact: Blockchain technology works on a network that has multiple nodes that are not connected to the central system but are interrelated. If one of the networks fails and exits the queue, the entire network generally does not fail and exit the queue. This increases the durability and defense threshold of blockchain technology. These situations themselves provide confidence in the system.

Transparency and Immutability:

Influence on Risk: Lack of transparency and openness to manipulation are considered two of the most obvious shortcomings of the traditional system.

Blockchain Influence: It creates an environment of transparency and trust, as every piece of data entered into the blockchain system is not deleted from anyone else in the system. It minimizes the risks and protects information against manipulation.

Smart Contracts and Automation:

Influence on Risk: Conventional contract implementation can cause failures, time delays, and the necessity of brokers, which can result in significant operational and monetary risks.

Blockchain Influence: They are more practical. By automating contract terms, it makes contract terms more clear, approachable, and convenient. It provides a more rapid result and an efficient contract method.

Security Through Cryptography:

Influence on Risk: The most important problems for traditional risk management systems are: cyber security problems and threats, data breaches, and unauthorized access.

Blockchain Influence: To secure data and operations, a blockchain relies on cryptographic techniques. Using cryptocurrency hash functionality and digital signatures makes it extremely resistant to tampering or any unauthorized access.

Regulatory Compliance:

Influence on Risk: Uncertainties in regulators and regulatory articles lead to uncertainties and insecurities in terms of traditional risk management and bring about some operational risks for companies.

Blockchain Influence: The blockchain system's open, traceable, and transparent nature allows companies to be much more secure and protected against potential operational and other risks compared to traditional risk management.

Supply Chain Transparency:

Influence on Risk: Frequent violations of transparency and distrust can lead to inefficiency, fraud, and disruptions in supply chains.

Blockchain Influence: Due to its ability to provide a more transparent and trustworthy record of transactions with its centralized and invariable transaction log feature, it helps supply chains grow and evolve. Through blockchain technologies used in the supply chains, the fraud risks are minimized, and traceability increases as well as accessibility, which increases the authenticity of the products. All stakeholders have real-time access to relevant information about the supply chain, which minimizes the risk of any fraudulent actions.

Tokenization and Financial Risks:

Influence on Risk: Conventional finance systems can be subject to risks related to fraud, latency, and high trading costs.

Blockchain Influence: Demonetization in the blockchain network can make it easier to conduct financial operations, lower costs, and reduce the risk of scams. The use of blockchain-based tokens can improve the management of financial risk by allowing cross-border trades to be more rapid and cost-effective.

In summary, blockchain technologies are reshaping the way institutions handle risk by ensuring a secure, transparent, and more automated infrastructure. It addresses several risks related to traditional systems and provides innovative approaches to improve transparency, trust, and efficiency in business operations. Organizations adopting blockchain need to closely integrate it into their risk management strategies to take full advantage of its benefits (Takaoglu et al., 2019).

2.3.2 Risk management framework

A framework for risk management can be defined as a guide that organizations intend to use to identify, mitigate, and eliminate risks. There are certain stages to establishing a risk management framework. The first stage is the determination of the risk management framework, which starts with the identification of the events that give rise to the risks that organizations are likely to face and continues with the setting of strategic objectives.

Another stage, called risk requirements, is the determination of the organization's risk-related strategies. In order to achieve this, risk models must first be identified and analyzed. At this stage, threats and opportunities are expected to be identified and reported in order to ensure accurate and complete information flows.

The feasibility analysis, which will determine the needs and costs required for the realization of risk management and the cost of the necessary workforce, and the completion of the customized risk management framework after the analyses are completed. The last stage of the risk management framework is reporting. The purpose of this is to provide internal and external reporting by explaining the risks that the organization will have and the risks taken by the users.

2.4 Enterprise Risk Management

Until the 2000s, traditional risk management was able to meet the needs of organizations in terms of managing

risk in line with their objectives. Changing conditions over time, the phenomenon of globalization, the acceleration of technological developments, changes in the way institutions and organizations view risk, changing expectations, and changing legal regulations have paved the way for the development of a different approach to risk management. However, the new areas and needs created by these developments have led to the emergence of different types of risks. The differentiation of the types of risks and the need to create solutions for these different risks have become a necessity for both private companies and public institutions (Kızılboğa, 2013). The Commission on Sponsoring Organizations of the Treadway Committee (COSO), which is accepted as an international authority, defined the concept of enterprise risk management as "a process established to provide reasonable assurance of achieving the organization's objectives and to identify possible events that may affect the organization and to manage the risks arising from them." Thus, enterprise risk management has begun to approach events from a systematic perspective by adopting a proactive style of action (Coyne & McMickle, 2017).

The practices established by institutions and organizations within the enterprise risk management process are influenced by factors such as the external environment, the field of activity, the organizational structure, the size, and the technological infrastructure of the institution. Therefore, the organization will develop models depending on and in accordance with its internal and external dynamics (Usman & Kaygusuz, 2019). A reasonable level of assurance is expected from enterprise risk management in terms of reliability of reporting and compliance with legislation. Achieving the objectives in this category depends on the controls and how the related activities are carried out (COSO, 2017).

Updated in 2017, the concept of enterprise risk management consists of five interrelated components and twenty principles. The components are listed as follows (Pehlivanlı, 2014) as shown in Figure 2:

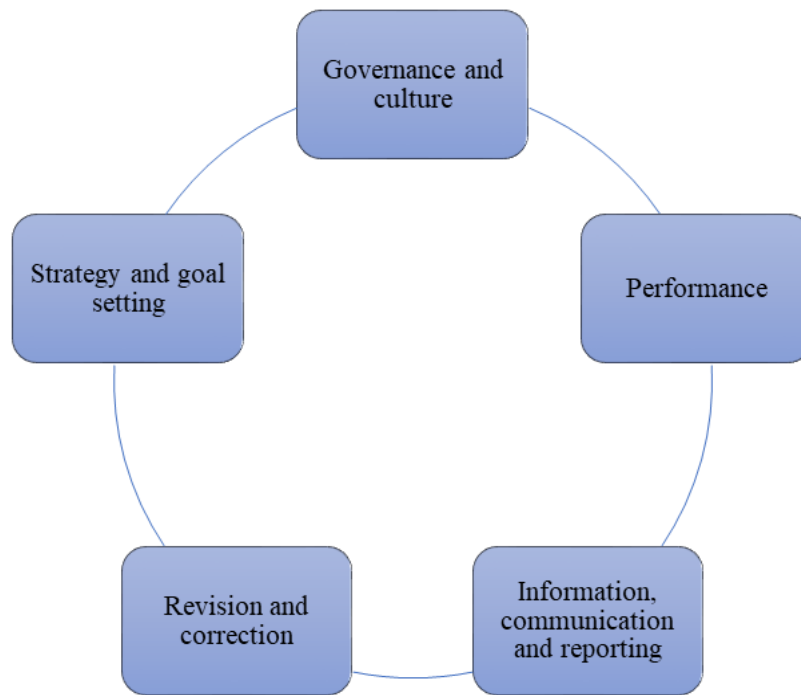


Figure 2. Key components of enterprise risk (COSO, 2017)

The governance and culture component are the basic component of organizational risk management. While governance is related to how roles, authorities, and responsibilities will be distributed between the stakeholders and management, culture is related to the core values and mission of the organization. The strategy and target setting component is the component where the risk appetite in line with the strategy is determined and the targets and risks are determined and form the basis for evaluation. Performance components are listed by identifying the risks that may affect the achievement of organizations' strategies and objectives.

The review and correction component are the component where the performance is evaluated according to the targets set, how corporate governance practices work, and whether they create added value for the organization. The information, communication, and reporting component are characterized as the component that provides access to, sharing, and continuity of information. It can be evaluated as reporting on risk and performance at the last stage as a result of obtaining and processing information.

2.4.1 Expected impact of enterprise risk management

Enterprise risk management aims to ensure that risk management is based on solid foundations and to improve

the performance of organizations to adapt to changes in technology, economic factors, and changing expectations. In this respect, CRM (Enterprise Risk Management);

- Adapt to evolving and changing situations
- Minimize operational losses
- Ensure interaction and communication between units
- Increase confidence in the assessment process for systematic risks
- Create appropriate responses to risks
- Reduce the cost of risk management
- Efficiency in resource allocation
- Harmonize risk management and the internal structure of the institution
- Increase competitiveness
- Alignment with a defined strategy
- Adoption of a proactive management philosophy
- Better identification and analysis of opportunities and threats
- It has expectations, such as the protection of the corporate image (Akçakanat, 2012)

In particular, the different concepts and expectations expressed by COSO are the issues that organizations should consider at this point. The concept of value is the most important one. The Enterprise Risk Management Framework published by COSO defines the basic components, creates a common language for risk management, and provides guidance or advice on this issue (Coyne & McMickle, 2017).

2.4.2 Impact of blockchain technology on the evolution of enterprise risk management

Especially the era of globalization and the world of rapid technological change have had an undeniable impact on enterprise risk management (ERM). Here are the key ways blockchain is impacting and changing ERM practices:

Transparency and Traceability:

Impact: Thanks to its transparency, immutable system, and traceability, blockchain prevents and eliminates the formation and development of corporate risks.

Change in ERM: Blockchain technology enhances and strengthens ERM applications because it prevents fraud and provides more transparent processing for ERM.

Supply Chain Risk Management:

Impact: With its features that improve transparency and accountability, blockchain technology prevents fraud and all kinds of unethical practices and minimizes risks in such cases.

Change in ERM: To integrate the blockchain in the evaluation and minimization of risks in a global network of supply chains, ERM schemes are emerging. By leveraging the visibility and real-time data offered by blockchain, enterprises are now capable of addressing and reducing risks in a more proactive way.

Decentralization and Reduced Counterparty Risks:

Impact: Blockchain technology is of great importance in reducing risks within global markets and reducing the need for another intermediary for financial institutions.

Change in ERM: Applications of the ERM fit into the decreasing dependence on centralized organizations. The decentralized nature of blockchain will minimize the risk of fiscal loss due to the failures or misuse of brokers.

Smart Contracts Automating Risk Responses:

Impact: Smart contracts automate the execution of predefined terms, allowing for automatic risk responses.

Change in ERM: Since smart contracts make automated risk minimization strategies available, ERM is becoming more proactive and effective. Enterprises can respond to risks in real time on the basis of previously defined circumstances, thus reducing the influence of unpredictable incidents.

Compliance and Auditability:

Impact: Obviously, the unchangeable character of the blockchain provides transparency and an auditable record, making it simple to achieve legislative and regulatory approval.

Changing ERM: Emerging ERM applications are evolving towards the use of the blockchain for managing compliance. By offering real-time, controllable logs to regulators, organizations can indicate global and local regulatory compliance in a quickly evolving regulatory climate.

Global Payment Systems and Financial Risk Management:

Impact: Contrary to conventional risk methodologies, blockchain technology is preferred for its affordable cost as well as its good transaction rate and safe and secure procedures in cross-border transactions. Being fast and trustworthy lowers financial risks and prevents exchange rate fluctuations.

Change in ERM: Emerging ERM networks are able to accommodate the shifting environment of overseas operations. By facilitating financial risk identification and governance in real time, blockchain allows institutions to act in an educated way against volatile exchange rate fluctuations.

Data Security and Privacy:

Impact: Cryptographic technology, including cryptographic techniques, helps to eliminate worries regarding

data security, data violations, and any unauthorized access, thereby ensuring data security.

Change in ERM: Blockchain is a central component of ERM applications to secure sensitive data. Blockchain's decentralized and cryptographic nature protects data against emerging threats to data security and cybersecurity.

Cross-Organizational Collaboration:

Impact: Through distributed, centralized notebooks with shared records, blockchain promotes confidence and collaboration among several parties.

Change in ERM: By utilizing the blockchain for safe and more transparent sharing of information, ERM implementations are aligning with a more collaborative paradigm. This is particularly valid for those industries where more than one enterprise has to collaborate on risk management efforts.

In summary, as enterprises are facing the complexities of technological disruption and the challenges of globalization, ERM practices are also evolving to take full advantage of blockchain's unique features, improving resilience and adaptability in an evolving business landscape.

2.4.3 Blockchain technology and risk

Although blockchain technology is practical and useful, it also has some risks. Understanding and effectively managing these risks is very important for companies and organizations, as well as for institutions and organizations that want to adopt the blockchain system. We can discuss some of the challenges and risks of blockchain technology under a few headings in the following categories: (101 Blockchains, 2021).

Security Risk:

Although having software cryptographic features makes blockchain a safe technology, research has shown that the system may have 51% vulnerabilities.

Management Strategy: It is necessary to constantly monitor security vulnerabilities. For this, penetration tests and security checks must be carried out. Implementation of multi-signature wallets for enhanced security. Continuous monitoring and response to potential security incidents.

Regulatory and Compliance Risks:

The blockchain-regulated space is developing, and the compliance landscape can vary widely and globally.

Governance Strategy: Stay up-to-date on the regulatory evolution in relevant jurisdictions. Work with legal specialists to assure compliance with current and forthcoming regulations. Have a flexible regulatory infrastructure that can accommodate the changing environmental landscape.

Interoperability Challenges:

Interoperability between different blockchain networks and legacy systems can be challenging.

Management Strategy: Use standardized protocols to enhance interoperability. Choose blockchain platforms that support industry standards. Invest in middleware solutions that facilitate communication between diverse systems.

Scalability Concerns:

As building blockchain grids grows, the scalability of the network is becoming a major concern, leading to reduced transaction processing times.

Management Strategy: Explore solutions for scalability, such as fragmentation or side chains. Regularly upgrade, analyze, and optimize the blockchain protocol. Explore hybrid or off-chain scaling when suitable.

Lack of Standardization:

Lack of standardization can hinder widespread adoption and integration of blockchain solutions.

Management Strategy: Participate in industry consortia working towards standardization. Collaborate with other organizations to establish common standards. Select widely accepted blockchain platforms with active developer communities.

Smart Contract Risks:

Smart contracts, while powerful, are susceptible to bugs and vulnerabilities that can lead to financial losses.

Management Strategy: Thoroughly audit and test smart contracts before deployment. Use established frameworks and best practices for smart contract development. Implement mechanisms for pausing or upgrading contracts in cases of identified vulnerabilities.

Privacy Concerns:

Blockchain's transparent and immutable nature can pose challenges to privacy, especially in public blockchains.

Management Strategy: Utilize privacy-focused blockchain solutions or implement privacy features. Consider permissioned or consortium blockchains where privacy requirements can be better controlled. Comply with privacy regulations and inform users about data handling practices.

Human Error and Governance:

Human errors in coding, configuration, or governance can have significant consequences.

Management Strategy: Implement robust governance structures and processes. Conduct regular training for developers and administrators. Establish clear protocols for updates, changes, and access control.

Managing the risks of blockchain technology requires a comprehensive approach that combines technological solutions, regulatory compliance, and proactive governance. Organizations should stay abreast of the evolving

blockchain risk landscape and continually update their risk management strategies to address emerging challenges. Regular audits, collaboration with industry stakeholders, and adherence to best practices are essential components of effective risk management in the blockchain space.

2.5 Types of Risk

Different risk classifications have been made in relation to different risks faced by institutions and organizations. These risks, in their most general form, are listed below:

- **Strategic risks:** These can be defined as the risks that affect the objectives set by the organization in the medium and long term. Such risks can be classified as risks with an economic dimension, risks with a political dimension, or risks arising from the external environment.
- **Operational risks:** Risks faced by management and staff in carrying out day-to-day activities.
- **Reputational risks:** Including risks that may affect the image of the organization.
- **Information technology risks:** This is defined as the risks that may arise from technological deficiencies.
- **Regulatory risks:** Risks that may arise for environmental reasons or risks that may arise in complying with national or international legislation.
- **Human resource risks:** It can be categorized as a risk that may arise from inadequate professional human resources or the loss of key personnel.

In order for an organization to manage risk effectively, it must first determine its attitude toward risk. It can also be expressed as the determination of the attitude to be taken towards the risk by senior management. In this sense, organizations may not control the risks they face or are likely to face and may adopt strategies with their responses to risk. In this context, risks can be responded to in four basic ways:

- Risk avoidance is the process of stopping or terminating activities that cause risk. It is an effective way of determining a new strategy.
- Accepting risk allows institutions or organizations to accept risks within their risk appetite without taking any precautions. In some cases, taking action against a risk may be more costly than accepting the risk. In such cases, organizations can accept the risk as it is.
- Controlling risk is the preferred form of risk management for organizations, as it is defined as establishing controls to reduce the probability of occurrence to a level acceptable to management.
- Transferring risk is the process of transferring unavoidable risks to a third party outside the organization. Purchasing services or insurance can be considered a risk transfer transaction.

2.6 Risk Life Cycle Concept

The risk life cycle is a concept that describes the stages of the use of the risk model determined by the organizations as shown in Figure 3.

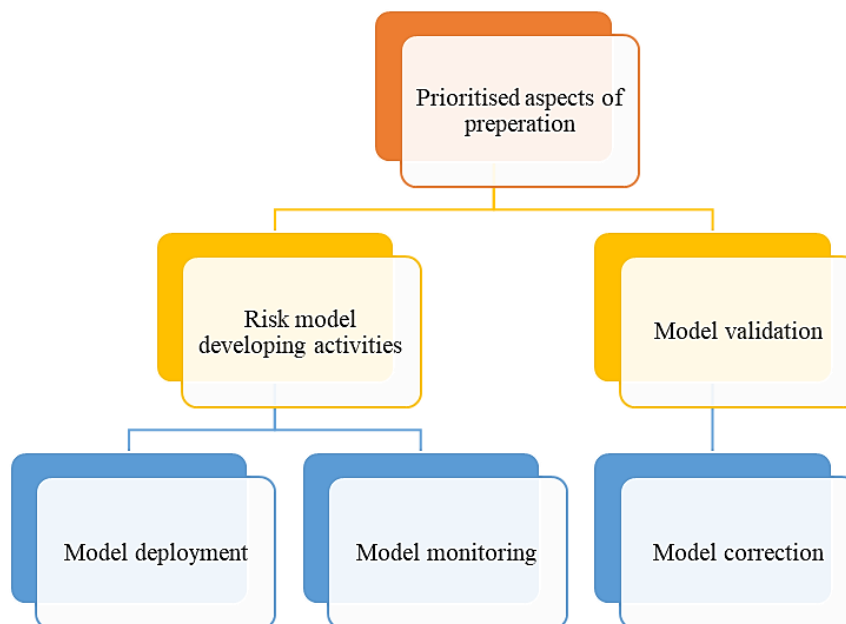


Figure 3. Risk lifecycle model (Open Risk Manual, 2022)

- **Preparation and priority considerations** is the first stage of the model that initiates the risk lifecycle. It defines the scope and objectives of the risk model. This stage may include documents consisting of a plan, project or programme, depending on the management of the organisation implementing the risk model.
- **Model development activities**, this stage consists of the main activities created for the model. Data collection, data review, model development, analysis and documentation are examples of these main activities.
- **Model validation**, this stage is the stage of reviewing and validating the activities performed in stage 2.
- **Model deployment**, this phase includes production implementation, acceptance testing, user training. This stage can be defined as an operational model that processes real data and is fully embedded in the organisation's systems and associated risk processes.
- **Model monitoring**, where the model is continuously monitored for performance and errors. A risk model monitoring report is produced at this stage.
- **Model adjustment** (modification), the model may need to be recalibrated using additional (e.g. more recent) data if suggested by the monitoring report or other current information.
- **Model decommissioning**, if monitoring or other conditions indicate that the model is no longer fit for purpose, the model may need to be decommissioned.

2.7 Current Global Technological Risks

Starting at the end of 2019 and showing its effects in many areas since the first quarter of 2020, the private and public sectors have taken serious steps to adapt faster to rapidly developing technological changes. Digital-based technologies that facilitate working life and social life, such as e-commerce, e-learning, e-government, virtual conferencing, and remote working, have also brought various risks. Table 1 below shows the technological risks identified by the World Economic Forum (2023).

Table 1. Global technological risks (World Economic Forum, 2023)

Negative Consequences of Technological Developments	Intentional or unintended negative consequences of technological advances on individuals, businesses, ecosystems and/or economies: AI, brain-computer interfaces, biotechnology, geo-engineering, quantum computing, etc.
Disruption of Critical Information Infrastructure	Degradation, saturation or closure of critical physical and digital infrastructure or services as a result of a systematic reliance on cyber networks and/or technology: AI intensive systems, internet, utilities, satellites, etc.
Digital Inequality	Unequal access to critical digital networks and technology between and within countries as a result of unequal investment capacities, lack of necessary skills in the labour force, insufficient purchasing power, government restrictions and cultural differences.
Digital Power Concentration	Concentration of critical digital assets, capabilities and knowledge by a smaller number of individuals, businesses or governments results in discretionary pricing mechanisms, lack of impartial oversight, unequal private and/or public access, etc.
Failure of Cyber Security Measures	Business, government and cybersecurity infrastructure Failure of Cyber Security and/or measures are falling behind or becoming obsolete due to increasingly sophisticated and frequent cybercrime, resulting in economic disruption, financial loss, geopolitical tensions or social instability.
Failure of Technology Management	States adopt digital infrastructure, protocols and/or standards that are incompatible with the lack of globally accepted frameworks or regulations for the use of different critical digital networks and technology.

3. Blockchain

Blockchain, which consists of a distributed system used for recording and monitoring transactions on a network, has found its place in many sectors today. Thanks to its decentralized system, secure structure, and automation capability, it has gradually attracted the attention of the public sector, especially the private sector. First introduced by Satoshi Nakamoto in 2008, the concept has kept growing over the years. Operations that can be carried out independently from a central government or without the support of reliable third parties are quite innovative and have formed the fundamental structure of today's cryptocurrencies (Ünal & Uluyol, 2020).

3.1 Blockchain Concept

A blockchain is a decentralized system that uses a chain of blocks to track transactions. It is a distributed database where all transactions are recorded and cannot be changed or stolen. The technology's cryptographic features ensure data security and anonymity. Blockchain is useful for transactions that require multiple steps of verification and validation. It provides secure transactions, reduces compliance costs, and shortens data transfer

time. Data in blockchain transactions is encrypted to protect user anonymity and prevent data alteration (Ünal & Uluyol, 2020).

3.2 Basic Structure of Blockchain Technology

When block chain systems are analyzed, we see that they consist of six layers: application layer, contract layer, adaptation layer, consensus layer, network layer, and data layer. As each layer is important in the structure, the most important layer among the six layers is the reconciliation layer. The compatibility of the settlement algorithm to be selected with the features of the system to be established is of great importance. In order to design and implement a successful blockchain system, it is necessary to work with experienced software developers and computer scientists. In addition, consistent optimization of variables such as user volume and data load to be encountered in the future is of great importance (Liu & Li, 2018). An important concept within the blockchain structure is smart contracts. Smart contracts can be considered the parts where dynamic work is done in blockchains. Smart contracts are digital contracts. These contracts developed for the solution of a special situation appear as a code in the block chain system (Kaur et al., 2023; Kumar et al., 2023; Tanriverdi et al., 2019). Some structural concepts related to block chain technology are shown in the Table 2.

Table 2. Blockchain basic concepts (Yavuz & Avunduk, 2021)

Peer-to-Peer Network (P2P)	A peer-to-peer communication model in which interconnected nodes share resources with each other without using a "peer" centralised management system is called a peer-to-peer network. Each machine in the network is responsible for its own resources and can act as both server and client.
Encryption	Encryption is a method of concealment and disclosure known as encryption and decryption by means of mathematical operations. Through encryption, any data set is transformed into a seemingly random data set using a regular structure, which no one except the recipient can retrieve.
Knot	It is a name given to devices in the blockchain network. A computer, telephone or any active device can be a node as long as it is connected to the Internet and has an IP address. The basis of blockchain technology depends on the operation of the node.
Hasting	The process of accepting an input of any length and using an algorithm to convert it into an encrypted fixed output is called summarisation hasting.
Block	The structure that stores data in the block chain structure is called a block. Block structures are connected to each other in a time- linear manner.
Consensus	The blockchain is governed by rules called consensus. Thanks to these rules, it is determined which changes are allowed to be made in the database and by whom these changes can be made.

3.3 Blockchain Types

- **Open Blockchain (Permissionless):** It is a type of block chain in a structure where anyone can join the network in question. This system is considered a completely independent block chain system that does not require central authority.
- **Private Blockchain (Authorized):** In the private blockchain system, only permitted users can join the network. Participation in the consensus within the network can be defined as public or requiring permission.
- **Consortium Blockchain:** Consortium blockchain networks are considered a mixture of open and private blockchain networks. It is a system in which the node can be pre-selected by the authorized person or organization.

4. Blockchain Integration and Sustainable Risk Management

Block chain technology involves various risks since it is a structure created to produce solutions to the problems in current applications. Various failures and errors that may occur in the block chain may cause risks to arise. Today, in order for a business to be considered a successful application model, it must include a number of elements that go beyond economic efficiency. These elements include the establishment of a sound corporate risk management structure, a commitment to ethical values, and environmental responsibility. Good governance means more than just fulfilling legal requirements and policy procedures; it requires businesses to adopt an approach focused on medium- and long-term value creation (Bozkuş Kahyaoğlu, 2019).

The underlying reason behind this new approach is the increasing tendency of business managers to create sustainable and long-term business value rather than short-term profit-making goals. This necessitates businesses and senior managers adopting the concept of sustainability and developing strategies in this direction. In this process, taking into account social and environmental factors as well as economic performance has become a part of the overall success and reputation of businesses. Blockchain technology has practical implications for sustainable risk management, particularly through its inherent features such as transparency. Following is a closer look at case studies on how blockchain transparency can be applied in risk management:

Supply Chain Transparency:

Application: In the context of the supply chain, building blockchain technology provides a more flexible and transparent environment that prevents counterfeiting, fraud, and all kinds of illegal and unethical behaviors, thereby lowering risks.

Case Example: Both Walmart and IBM have implemented their blockchains to keep track of the source of food products. This enables quick detection and elimination of any contaminated products by ensuring supply chain transparency. The transparency and visibility that blockchain brings help ensure the safety and integrity of products, helping with sustainability and risk control.

Environmental and Social Impact Tracking:

Application: Nowadays, in order to monitor and optimize the social and environmental impacts of products and services, blockchain technology can be used. Use in this context is very important in terms of sustainability, and it helps to better manage the risk of sustainability.

Case Example: To track the origins of its diamonds, Everledger is using a blockchain to make sure that diamonds are obtained from an ethical source and are kept conflict-free. Transparency at this level in the entire supply chain mitigates the risk of working with less ethical suppliers and promotes more sustainable business practices.

Renewable Energy Certificates:

Application: Furthermore, blockchain frameworks can be used to build transparent and monitorable frameworks to handle renewable certificates, ensuring proper verification and reporting, as well as minimizing the risk of green laundering.

Case Example: According to the Energy Web Foundation, a blockchain is used to track and commercialize renewable energy certificates. This highly transparent system allows both consumers and businesses to be able to verify the origin of their energy, thus reducing the risk of investing in energy that is mistakenly branded as "green" power.

Ethical Labor Practices:

Application: By providing a more transparent and accountable account of workforce circumstances and equitable labor practices, blockchain can be implemented to drive the implementation of ethical labor in supply chains.

Case Example: As a blockchain startup, Provenance has partnered with British retailer Co-op to monitor the supply chain of fresh goods. This enables transparency in labor enforcement, mitigating the risk of supporting providers who work in abusive working conditions.

Carbon Footprint Tracking:

Application: By enabling carbon emissions to be tracked in a transparent way across the supply chain, blockchain could help to manage and mitigate organizations' potential environmental risks.

Case Example: Foundation Poseidon is already using a blockchain to keep track of its carbon credits for retail purchases. This allows consumers to have a transparent view of the carbon impact of their purchases and promotes environmental choices, thereby contributing to sustainable risk management.

Insurance and Smart Contracts:

Application: Building on blockchain-based clever contracts could be implemented in the insurance sector to help automate and simplify claims handling, increase transparency, and decrease fraud risk.

Case Example: As a blockchain platform, Aeternity has cooperated with PayPerMile to build a blockchain-based infrastructure solution for the automotive industry. The smart contracts on the blockchain will automatically trigger insurance payments according to predefined conditions, such as accidents or damage. This lowers the risk of fake demands and ensures the transparency of the compensation payment process, thus contributing to sustainable risk management practices.

Transparent Impact Investments:

Application: By providing a clear and accountable track record of how their funds are utilized for environmental or social projects, blockchain could be used for impact investment, thereby reducing the risk of misappropriation or green laundering.

Case Example: Through its platform, ImpactPPA uses blockchain to monitor and verify the impacts of renewable energy projects funded through its platform. This enables traders to have a transparent view of the impact of their investments on social and environmental outcomes, thereby reducing the risk of investing in projects that are not aligned with their sustainability goals.

Public Sector Accountability:

Application: In the public sector, blockchain can improve its transparency and accountability, minimize the risk of fraud, and allow efficient resource reallocation in government programs.

Case Example: The government of Estonia has introduced e-governance initiatives, including the use of blockchain in e-governance, secure data exchange, and e-residency. This not only provides transparency in government processes but also reduces the risk of bribery by maintaining an invariable and controllable register of the government's operations.

Transparent Carbon Markets:

Application: Using a decentralized and fully verifiable carbon credit register, it can facilitate more transparent carbon markets and mitigate the risk of fraudulent carbon offset projects.

Case Example: Together, IBM and Veridium Laboratories have collaborated to build a blockchain-based platform to keep track of carbon credits. This enables full transparency in the market for carbon offsets, thereby minimizing the risk of investing in loans that do not have a real and quantifiable effect on cutting emissions.

To summarize, the transparency of blockchain plays a crucial role in sustainable risk management when implemented in diverse sectors. By maintaining a tamper-proof and open public ledger, blockchain helps institutions build trust, reduce the risks associated with unethical practices, and contribute to a more sustainable and transparent global economy. The case examples illustrate practical applications of blockchain transparency in addressing specific risks and developing sustainable business practices.

4.1 Risk Management in the Structure of Blockchains

While the risk management nature of blockchain technology offers a number of complex and multilayered challenges, it also carries technological risks such as cryptographic vulnerabilities, software bugs, and network security issues. The technology promises security through its highly decentralized nature and immutable transaction records, but these systems also carry technological risks, such as cryptographic vulnerabilities, software bugs, and network security issues. Furthermore, the operational aspects of blockchain applications involve risks, in particular the centralization of mining pools and the control of transaction power.

(1) Impact of Blockchain on Sustainability Goals

One of the most important concepts of today is the concept of sustainability. Blockchain technology has an important role in achieving the goals set against the concept of sustainability. This technology, which has concepts such as reliability, transparency, and data integrity, offers the fastest and most reliable way to achieve sustainability goals today. It ensures achieving sustainable development goals and facilitates the monitoring and auditing of development projects. For example, blockchain-based systems can verify sustainable initiatives by making environmental impact reporting more transparent and unmanipulable.

(2) The Role of Blockchain in Environmental Risk Management

Today, the use of blockchain technology in the management of environmental risks is quite common and an effective tool. In this regard, it is necessary to emphasize the importance of blockchain technology, for example, in monitoring and reporting carbon emissions, documenting them, and obtaining updated data from real-time and accurate databases in a protected manner. Likewise, tracking products and materials from source to consumer in waste management and recycling processes ensures environmental sustainability, which is of critical importance. Blockchain-based systems offer new opportunities in environmental impact reporting. For example, a company's carbon footprint or waste management practices can be reported transparently on the blockchain. This not only helps companies improve their environmental performance but also enables consumers and investors to make more informed decisions (Ünsal & Kocaoğlu, 2018).

(3) Social Responsibility and Blockchain

Today, blockchain technology is widely used in socially oriented projects as well as in environmental and other projects. For example, very productive feedback has been received when using blockchain technology in social responsibility projects. Blockchain technology can also contribute to promoting ethical and fair trade practices by providing a broad resource and detailed information about products and services. The transparency and reliability of the system also make it successful when used in socially oriented projects.

(4) Validation of Sustainable Initiatives

Blockchain also plays an important role in verifying sustainable initiatives and projects. For example, sustainable resource utilization or green energy projects can be recorded on the blockchain to verify that these projects are indeed sustainable. This is especially important in the areas of green investments and sustainable financing.

(5) The Role of Blockchain in Corporate Governance and ESG Compliance

Blockchain in corporate governance can be an important tool for achieving ESG goals. Blockchain-based solutions used in the assessment and reporting of companies' ESG performances increase the reliability and accessibility of this information. In this way, investors and other stakeholders can more accurately assess the sustainability performance of companies.

(6) Risk Assessment and Monitoring Methods

Blockchain technology can also improve risk assessment and monitoring methods. In particular, real-time monitoring of sustainability-related risks, the development of early warning systems, and the analysis of complex data sets can become more effective with blockchain-based solutions. Risk practitioners aim to minimize risks as much as possible by using blockchain technology. However, since the network structure of the system in question is a new structure, the risks it brings are new, and the risks can be found within the network itself. For example, any organization may need an authorized network to operate effectively. Without an appropriate management

system in this regard, it will not be easy for the organization to advance blockchain solutions. However, permissions should be layered to prevent sensitive data from leaking. Risk practitioners also consider that blockchain can be a tool for communicating risks.

These features of the blockchain can be seen as an important tool in achieving sustainability goals, and this technology is expected to be used more and more in projects aimed at sustainable development goals. In an effective blockchain, the sections included in the sustainable risk management framework should be analyzed effectively by institutions. A process that starts with the correct definition of targets, processes, and components should be continued with appropriate action plans. In this way, organizations will be able to increase their ability to meet the risk of block chain technology-based business processes. Creating a reliable risk management strategy, governance framework, and controls framework in order to take action and respond to the possibility of encountering risks is considered a strategic step for these organizations as shown in Figure 4.

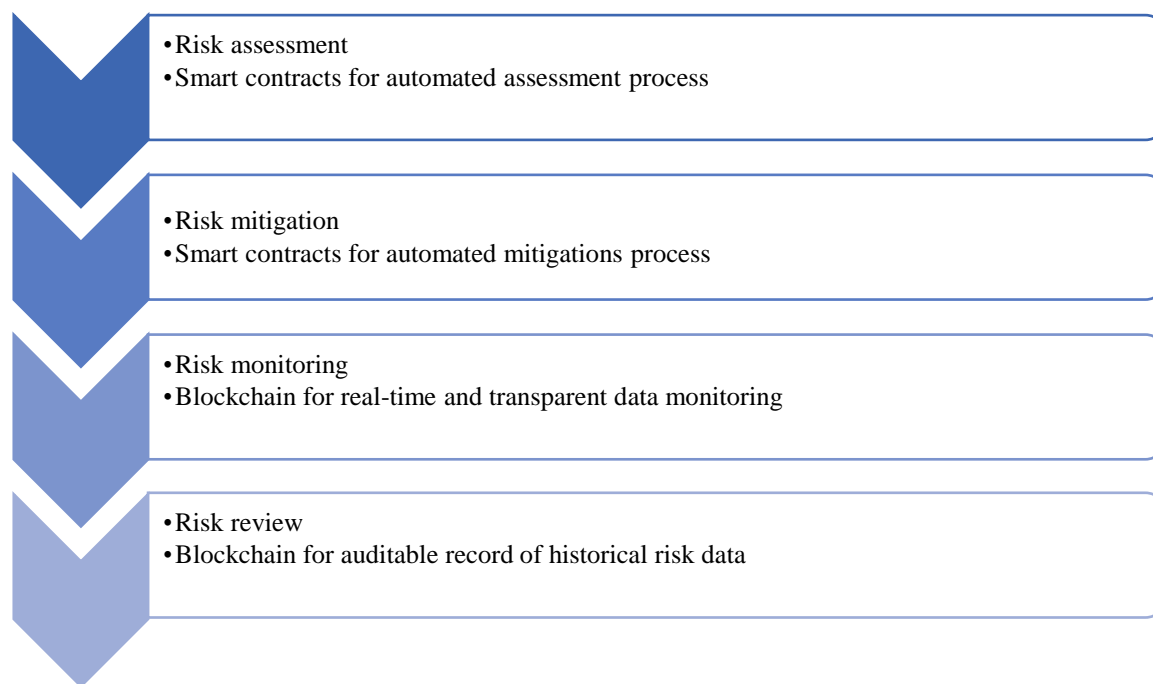


Figure 4. Incorporation of blockchain into the risk management framework

5. Conclusion

Blockchain technology, with its significant potential for revolution, is continuously emerging in several fields. Many individuals and businesses find it appealing to exploit the benefits of this technology, as it can seamlessly adapt to quickly evolving digital systems. Despite implementing measures to enhance its ability to withstand technology-related risks, including cyber security risks, it is crucial to thoroughly assess the various aspects of the system, such as security, management, efficiency, and flexibility. It is important to carefully guide any actions taken in this area. Like any emerging technology, the blockchain also presents inherent hazards due to its structure. Many institutions are investing in many sectors to harness the benefits of blockchain technology, including clearing transactions, cross-border payments, identity management, and finance. The primary objective of blockchain technology is to optimize the efficiency and cost-effectiveness of institutional business processes, while simultaneously mitigating risks. Nevertheless, as the chain itself carries inherent hazards, it is crucial to identify such dangers and implement regulatory steps to mitigate them. It is essential to conduct relevant tests, implement controls, and maintain ongoing monitoring efforts to address the risks associated with blockchain-based business processes. Blockchain technology possesses a framework that facilitates the fast execution of business activities while ensuring unalterable security by eliminating intermediaries involved in current company operations. Institutions tend to favor efficiency-enhancing features, such as cost reduction, interactive capabilities, and streamlined agreement processes. Institutions and organizations should continuously monitor the progress of this emerging technology and assess its contribution to the organization. Establishing a mature ecosystem with blockchain technology is a time-consuming process for enterprises. Technological endeavors and developments are crucial for enhancing the system's reliability. Hence, it is crucial to attain a sufficient degree of maturity in technical investments and endeavors. Nevertheless, it is imperative to develop strategic plans to mitigate the potential dangers associated with blockchain technology. An imperative is to build a risk management system

capable of executing information technology audits, offering regulatory assistance, conducting efficient risk assessments, and designing and evaluating controls. Establishing an effective and suitable risk management framework is crucial for establishing corporate operations, management, and efficiency. Enhancements, enhanced efficiency, and improved performance of the company, together with an elevated reputation and the creation of additional value in areas such as sustainability, will be achievable. Developing risk management methods is crucial in order to mitigate the possible hazards associated with blockchain and maximize the opportunities presented by this technology. Organizations must implement measures, such as permissioned network topologies and tiered security protocols, when using this technology (Ünsal & Kocaoğlu, 2018).

The report emphasizes that blockchain technology has the capacity to yield substantial advantages, including enhanced efficiency, safety, and transparency. Nevertheless, it is crucial to recognize the potential hazards linked to this nascent technology. The study investigates many facets of blockchain hazards, encompassing security, governance, efficacy, and robustness. The results underscore the necessity of implementing a thorough risk management strategy to efficiently leverage the advantages of blockchain technology while minimizing any drawbacks. The framework should encompass the proactive identification and management of risks, along with the implementation of measures such as testing, controls, and continuous monitoring. Organizations that choose to invest in blockchain technology must address the obstacles related to its maturity and incorporate strategic planning, IT controls, regulatory advice, risk assessment, and control design into their risk management framework. By doing so, individuals can not only mitigate potential hazards but also optimize their business processes and improve managerial efficiency (Deloitte, 2017a; Deloitte, 2017b).

Future Directions:

For the future, we need to say clearly that the development of blockchain technology will continue and it will become an even higher level technology. Therefore, all institutions and organizations must be open to and keep up with this change and development within the framework of their plans for the future. Future research on this topic should be based mainly on the following:

Continuous Risk Monitoring:

Build out methodologies for achieving real-time risk monitoring in blockchain ecosystems. Innovate the combination of machine learning and artificial intelligence for the proactive risk identification.

Legal and Regulatory Frameworks:

Survey the emerging legislative and Regulatory environment for Blockchain. Assess the effect of the emerging regulatory climate on risk management strategies.

Interoperability Solutions:

Conduct and develop solutions to increase the interoperability between various blockchain networks. Explore the standardisation efforts to ease smooth integration.

User Education and Training:

Deliver training courses to increase user understanding and awareness of the risks of blockchain. Conduct development of training modules for institutions to enable the competent handling of blockchain technologies.

Scalability and Performance:

Look for solutions that are able to scale to address the performance difficulties related to expanding blockchain networks. Evaluate the impact of the scalability on the risk control strategies.

In summary, while the blockchain has tremendous potential to achieve its sustainability goals, the realisation of this potential will require a cautious focus on risk management practices and governance structures. Institutions must navigate the intricacies of the blockchain risks, apply effective risk governance frameworks and stay agile in the face of technology advances in order to realise the full benefit of this potentially transformative new technology.

Data Availability

The data used to support the research findings are available from the corresponding authors upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

- 101 Blockchains. (2021). *Blockchain risk assessment and enterprise management framework*. <https://101blockchains.com/enterprise-blockchain-risk-assesment/>
- Akçakanat, Ö. (2012). Kurumsal risk yönetimi ve kurumsal risk yönetim sürec'i. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 4(7), 30-46.
- Attila, İ. (2015). Gayrimenkul geliştirme projelerinde risk yönetimi. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 29(2), 387-406.

- Bashynska, I., Malanchuk, M., Zhuravel, O., & Olinichenko, K. (2019). Smart solutions: Risk management of crypto-assets and blockchain technology. *Int. J. Civ. Eng. Technol.*, 10(2), 1121-1131.
- Bozkurt, C. (2016). Risk, kurumsal risk yönetimi ve iç denetim. *Denetışim*, 4, 17-30.
- Bozkuş Kahyaoğlu, S. (2019). Sürdürülebilirlik ve kurumsal yönetim. In Aysel Gündoğdu (Ed.), *Türkiye'de Sürdürülebilir Finans Uygulamaları*. Gazi Kitabevi, Ankara.
- COSO. (2017). *Enterprise risk management integrating with strategy and performance*. <https://www.coso.org/enterprise-risk-management>
- Coyne, J. G. & McMickle, P. L. (2017). Can blockchains serve an accounting purpose. *J. Emerg. Technol. Account.*, 14(2), 101-111. <http://doi.org/10.2308/jeta-51910>.
- Deloitte. (2017a). *Blockchain risk management*. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf>
- Deloitte. (2017b). *Risk management and governance of digital assets*. <https://www2.deloitte.com/us/en/pages/advisory/articles/blockchain-risk-management.html>
- El Khatib, M., Alnaqbi, A., Alnaqbi, A., Alsuwaidi, H., & El Khatib, A. (2023). How blockchain and IoT affect project risk management. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, pp. 1-7. <https://doi.org/10.1109/ICBATS57792.2023.10111397>.
- Financial Reporting Council. (2014). *Guidance on risk management, internal control and related financial and business reporting*. London: Financial Reporting Council.
- Gönen, S. (2017). Risk raporlamasına ilişkin kuramsal yaklaşım. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 6, 293-301.
- Kalkan, M. E. & Deniz, V. (2013). Risk kavramı üzerine. *TTB Mesleki Sağlık ve Güvenlik Dergisi*, 13(48), 43-48.
- Kaur, A., Kumar, P., Özen, E., & Vurur, S. (2023). Unveiling the blockchain technology: An analysis of adoption and inventions. In *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management* (pp. 33-48). Emerald Publishing Limited.
- Kayahan, C. & Murat, T. (2022). The evolution of financial risk management. *J. Corp. Gov. Insur. Risk Manag.*, 9(S1), 155-168. <https://doi.org/10.51410/jcgirm.9.1.10>.
- Kızılboga, R. (2013). *Kurumsal Risk Yönetimi Odaklı İç Denetim Ve İstanbul Büyükşehir Belediyesi İçin Bir Model Önerisi*, Marmara Üniversitesi (Turkey) ProQuest Dissertations Publishing.
- Kumar, P., Özen, E., & Vurur, S. (2023). Adoption of blockchain technology in the financial sector. In *Contemporary Studies of Risks in Emerging Technology, Part A* (pp. 271-288). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-80455-562-020231018>.
- Liu, Q. & Li, K. (2018). Decentralization transaction method based on blockchain technology. In *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, Xiamen, China (pp. 416-419). <https://doi.org/10.1109/ICITBS.2018.00111>.
- Nathani, M. U. & Singh, J. S. K. (2020). Using blockchain for effective risk management in supply chain: A qualitative study. *Glob. Bus. Manag. Res.*, 12(3), 60-76.
- Open Risk Manuel. (2022). *Risk model lifecycle*. https://www.openriskmanual.org/wiki/Risk_Model_Lifecycle
- Pehlivanlı, D. (2014). *Modern İç Denetim*. İstanbul: Beta Yayınları.
- Takaoğlu, M., Özer, Ç. & Parlak, E. (2019). Blockchain technology and possible implementation areas in Turkey. *Int. J. East. Anatol. Sci. Eng. Des.*, 1(2), 260-295.
- Tanriverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blok zinciri teknolojisi nedir? Ne değildir? Alanyazın incelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217. <https://doi.org/10.17671/gazibtd.547122>.
- TUBİTAK. (2023). <https://blokzincir.bilgem.tubitak.gov.tr/>
- Ünal, G. & Uluyol Ç. (2020). Blok zinciri teknolojisi. *Bilişim Teknolojileri Dergisi*, 13(2), 167-175. <https://doi.org/10.17671/gazibtd.516990>.
- Ünsal, E. & Kocaoğlu, Ö. (2018). Blockchain technology: Use cases, open issues and future expectations. *Eur. J. Sci. Technol.*, 13, 54-64. <https://doi.org/10.31590/ejosat.423676>.
- Usman, Ö. & Kaygusuz, S. Y. (2019). Steps to be applied in enterprise risk management. *Muhasebe ve Denetime Bakış*, 18(56), 109-128.
- World Economic Forum. (2023). The Global Risk Report 2023. <https://www.weforum.org/publications/global-risks-report-2023/>
- Yao, F. G. & Qin, Z. N. (2021). Block chain based supply chain financial risk management research. *J. Phys.: Conf. Ser.*, 1744(2), 022027. <https://doi.org/10.1088/1742-6596/1744/2/022027>.
- Yavuz, E. & Avunduk, H. (2021). Tedarik zinciri yönetiminde blok zincir teknolojisinin kullanımı. *Izmir Democ. Univ. Soc. Sci. J.*, 4(1), 33-56.