Journal of Organizations, Technology and Entrepreneurship
https://www.acadlore.com/journals/JOTE

The Impact of Blockchain Technology on Reducing Cyber Risks

Ali Baghirov*

Social Sciences and Economy, Istanbul University, 34000 Istanbul, Türkiye

* Correspondence: Ali Baghirov (elibagirov13@gmail.com)

Received: 04-17-2024 **Revised:** 06-12-2024 **Accepted:** 06-20-2024

Citation: Baghirov, A. (2024). The impact of blockchain technology on reducing cyber risks. *J. Organ. Technol. Entrep.*, *2*(2), 122-135. https://doi.org/10.56578/jote020205.

© 2024 by the author(s). 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: Blockchain technology, which gained prominence with the advent of Bitcoin in 2008, has garnered significant attention across various sectors due to its inherent transparency, security, and decentralization. The ability to operate without central authorities has facilitated more efficient and secure transactions, particularly in an increasingly digital environment where cybersecurity has become a critical concern. Cybersecurity, defined as the protection of electronic systems, networks, and data from malicious threats, is paramount for individuals, organizations, and nations. Blockchain has emerged as a promising solution in the cybersecurity domain, offering enhanced data integrity and immutability. Each block in the chain is cryptographically linked to the previous one, making data tampering exceedingly difficult. The decentralized nature of blockchain, requiring validation from multiple participants, reduces the risk of single-point failures and enhances protection against cyberattacks, such as Distributed Denial of Service (DDoS) attacks. Blockchain aligns closely with the Confidentiality, Integrity, and Availability (CIA) triad in cybersecurity by employing encryption techniques and private keys for data protection, ensuring immutability of records, and providing continuous access through distributed networks. While its potential applications are broad, ranging from healthcare to supply chain management and Internet of Things (IoT), several limitations still hinder blockchain's widespread adoption in cybersecurity. Chief among these are issues related to scalability and resource management, as high transaction volumes can lead to inefficiencies in speed and cost. Emerging solutions, such as hybrid blockchain models, sidechains, and sharding, are being explored to address these challenges. Despite these obstacles, blockchain presents a resilient framework capable of enhancing cybersecurity measures across multiple sectors. Continued research and innovation are necessary to overcome existing limitations and fully unlock the potential of blockchain in reducing cyber risks. As blockchain technology evolves, its role in fortifying defences against cyber threats is expected to become increasingly pivotal, providing a robust and adaptive mechanism to combat future cyberattacks.

Keywords: Blockchain technology; Cyber security; Risk management; Data integrity; Decentralization; Scalability

1. Introduction

In recent years, the rapid advancements in technology have especially brought issues such as data security and privacy to the forefront. With the developments in information technology, individuals, organizations, and nations are increasingly facing technological risks. In light of these developments, it is becoming evident that security measures need to be equally advanced and technology-based. In the field of cybersecurity, blockchain technology is being considered as a reliable tool, due to its advantages in ensuring the security of sensitive and critical information (Iansiti & Lakhani, 2017). By adopting blockchain, individuals, companies, institutions, and nations can mitigate the risks of financial loss and reputational damage (Bashir, 2017). In the first section of the study titled "The Impact of Blockchain Technology on Reducing Cyber Risks", concepts related to blockchain technology are defined, followed by an explanation of its historical development in stages. The applications of blockchain technology are also discussed in this section. The second section provides definitions of the concepts of cybersecurity and risk in general terms. One of the topics in the second section, risk management in the digital age, addresses technology-based risks that may arise as technology advances. While the second section concludes with an exploration of cybersecurity risks, the third section discusses the potential advantages of using blockchain

technology to mitigate these risks in the field of cybersecurity.

2. Methodology

The research was conducted using a review approach. This approach involves a comprehensive review of the existing literature in order to understand the impact of blockchain technology on cybersecurity. The research reviewed academic articles, industry reports, and other key publications related to cyber security. In addition, case studies reflecting real-world applications and data from sectors using blockchain technology were analysed.

3. Blockchain Technology

The idea of blockchain technology was succinctly put forward for the very first time by Satoshi Nakamoto in the year 2008 in a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Figure 1). In this paper, Bitcoin was meant for everybody, and people would use it as any new digital currency that was going to be introduced into the world market, while blockchain was described as a chain of blocks that have been digitally signed (Kırbaç, 2020). Generally stating, upon trying to understand the meaning of the word blockchain technology, it is a database that embodies blocks of information and is self-distributed. Crypto currency and its transactions are developed, registered, and validated using specialized software technologies. This is a system in which algorithms are used in the addition and exploitation of information blocks. In all of these activities, in a particular cross-sectional perspective, every single transaction made has been stored in a database. Bipartisan transactions exist in the blockchain besides the approval of the extra party, which has acted as the overseer of all the activity (Lewis et al., 2017).

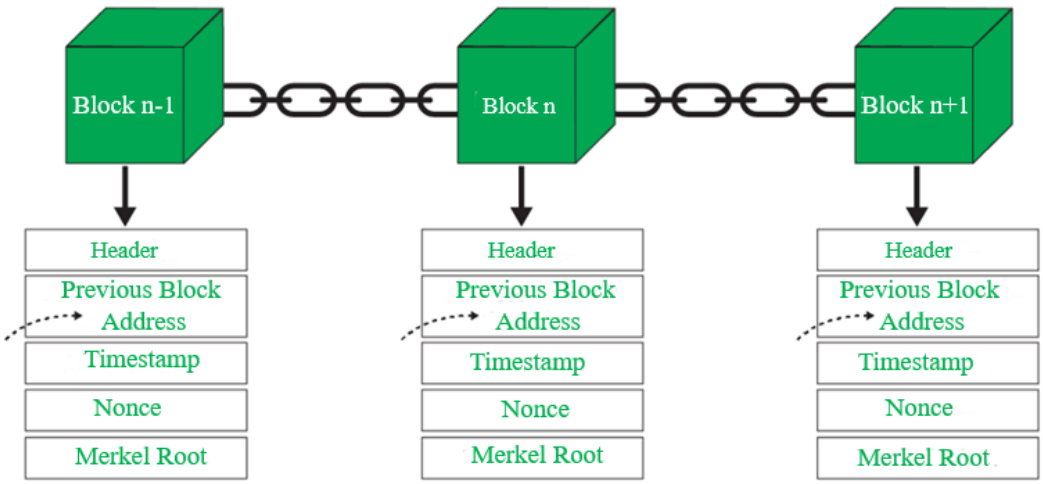

Figure 1. Blockchain structure

Prior to attempting to provide a detailed understanding of the blockchain and the technology behind it, it is important to define the basic terms on which the whole picture relies. Those terms are presented as follows (Palabıyık, 2020).

Data: As referred to here, such information is typically regarded as data but is typically viewed as an unformatted, unfashionable source of information normally devoid of overlying structures. Generally, data can include abstract conceptions. It can be characterized as usually concerning facts, things, or people.

Database: Database means systems of data stores. Databases were developed in the early 1960s as more complex digital storage methods were evolving. The ability to carry out transactions more securely, even in a P2P manner, at a much lower cost compared to traditional banking methods warrants the benefit of using faster-working encryption techniques, mainly cryptology. Cryptography is used to hide or protect information from any access apart from the owner.

Node: The mechanism that ensures the operation and survival of blockchain technology is referred to as a node. To function as a node, a mechanism must have an IP address and be connected to the internet. Devices like phones, printers, or other electronic devices that meet these criteria can be used as nodes. The role of nodes is to store copies of blocks consisting of transactions and to process these transactions into blocks. The more nodes a system has, the stronger it is considered to be. In light of this information, blockchain can be defined as a technical plan for decentralized databases maintained securely through cryptographic methods. According to a widely accepted definition by Russian programmer Vitalik Buterin, blockchain is described as a "magical computer where anyone can load programs, these programs can execute autonomously, their transaction history can be seen by everyone,

and the programs are cryptologically secured".

3.1 The Historical Evolution of Blockchain Technology

Phase 1 (1991 – 2008): The Early Years of Blockchain Technology

The foundational work that laid the groundwork for blockchain technology was first introduced by Haber & Stornetta (1991) in a paper that discussed the concept of creating a timestamp for securing digital documents. The purpose of this timestamp was to ensure the authenticity of a document by making the creation date and time visible, preventing any later alteration (Narayanan, 2016). Their approach allowed multiple records to be stored in a single block, which also contributed to increased efficiency in the overall system. Initially known as Blockchain 1.0, the technology was primarily used for cryptocurrency transactions, focusing on secure verification and storage of information. The lack of a need for a trusted intermediary or any third party was one of the main reasons blockchain was favored for digital currencies. Blockchain 1.0 primarily centered around applications like smart contracts, smart ownership, digital identities, passports, bonds, securities, intangible assets, patents, and notarized documents (Wang et al., 2017). When we look at Blockchain 3.0, its applications extend far beyond cryptocurrencies, touching sectors such as government, healthcare, science, art, culture, finance, and various markets. In particular, Blockchain 3.0 is used in non-financial areas through distributed ledger technology (DLT). A key example is its use in supply chain management, where it brings transparency and traceability to complex processes (Bakan & Şekkeli, 2019).

Phase 2 (2008-2013): Formation and Operations of Bitcoin

Blockchain 1.0: Blockchain 1.0 represents the first generation of blockchain technology, focusing on fundamental aspects of digital currency and its foundational technology. This phase is characterized by the development and deployment of basic blockchain platforms, protocols, and digital currencies.

Key Characteristics of Blockchain 1.0: Blockchain 1.0 involves the creation of a fundamental technology platform that includes the core blockchain infrastructure and its underlying protocols. This technology enables the establishment of decentralized systems that record and verify transactions without the need for intermediaries.

Digital Tokens and Currencies: The primary application of Blockchain 1.0 is in digital tokens, cryptocurrencies, or digital currencies. These applications use blockchain technology to facilitate payments and manage transactions in a decentralized manner. Example - Bitcoin: To understand Blockchain 1.0, one must closely examine Bitcoin, the pioneering technology that defined this era. Bitcoin was introduced as the first decentralized digital currency, leveraging blockchain technology to provide a secure and transparent means of conducting financial transactions.

Bitcoin operates on a blockchain that records all transactions in a public ledger. One of the key features of Bitcoin is its principle of preventing double spending, ensuring that each Bitcoin can be spent only once. This principle is a direct application of the Blockchain 1.0 technology. The core principle of Blockchain 1.0 was transactions over the internet without needing a centrally trusted third party in between. Decentralization that eliminates middlemen and enables direct peer-to-peer transactions carried out among the parties.

Transition to Blockchain 2.0: While Blockchain 1.0 provided the foundation for digital currencies, it required improvement to add additional features for better functionality and programmability. This gave birth to what is known as Blockchain 2.0 (the same fundamental thinking of Blockchain 1.0 upon which it was built). Blockchain 2.0: The second generation of blockchain technology includes other mechanisms such as smart contracts or programmable money; and the next stages of the development of blockchain are a new trend for future works and research in this area. These developments offer a stronger and more extensible platform for native blockchain applications that can scale to reach hundreds of thousands—something the community says the current network still cannot handle (Dujak & Sajter, 2019).

Conclusion: Blockchain 1.0 represents the initial phase of blockchain technology, focusing on the creation and application of digital currencies like Bitcoin. Its primary contributions include establishing a decentralized framework for conducting transactions and eliminating the need for intermediaries. The technology paved the way for subsequent developments, such as Blockchain 2.0, which expands the capabilities of blockchain with programmable and contract-based functionalities.

3.2 Cryptocurrencies and Cryptography

Cryptography, derived from the Greek term meaning "hidden writing", encompasses much more than just the concept of secret writing. In the context of digital currencies, cryptography is used not only to secure transactions but also to verify the authenticity of data, akin to a digital fingerprint. Cryptocurrencies are a type of digital or virtual currency that employs cryptography for security purposes, thereby enabling to verify and control the

generation of additional units, as well as to secure the transfer of assets on top of blockchain networks. It is this particular application of cryptography that underpins the essential security and legitimacy of digital currencies (Roy, 1952).

3.3 Historical Context of Cryptocurrencies and Cryptography

The first and most established real development of cryptographic currencies started with the introduction of Bitcoin in 2009. Some other advancements originate from this sentiment, yet among them, one thing is totally clear: we all insanely need to employ Bitcoins. Compared to Identity 1 & 0 in the 1990s, these ideas had further changed and progressed to better systems when managing and securing digital assets.

Modern Cryptocurrencies: Immutable Ledgers Power Modern Cryptocurrencies Once tokens are first issued, they are then placed on blockchains in order to keep a secure and unalterable ledger of transactions. This development represents a significant advancement over earlier systems.

3.4 Characteristics of the Cryptocurrencies

Cryptographic Security: Cryptocurrencies leverage cryptographic methods to secure transactions and control the issuance of new units. This ensures that transactions are private, secure, and tamper-proof.

Digital Fingerprints: Cryptography techniques also play a role in proving the integrity of data, just like how a digital fingerprint confirms the uniqueness of a document or transaction.

Decentralization: Unlike traditional currencies controlled by governments and financial institutions, cryptocurrencies operate independently of any central authority. This decentralization is a core feature that differentiates them from conventional money.

Liquidity and Adoption: Cryptocurrencies are liquid only to the extent that people recognize and adopt them. When a larger number of people and institutions come to accept and use cryptocurrencies, then the liquidity of these coins can be on par with traditional fiat currencies approved by governments.

Value Storage and Transfer: Cryptocurrencies aid in storing value and facilitating its transfer. They do not just stand for digital money but are explicitly created to act as currency under different systems.

Cryptocurrencies vs. Blockchain: Of these applications, Block is famous through its association with Bitcoin. Bitcoin represented the first and by far the most common use of cryptocurrency, although there are many other practical applications of blockchain in today's world.

Applications Beyond Bitcoin: Blockchain is not only the basis for various other cryptocurrencies, there are already additional application layers for blockchain, such as smart contracts and decentralized finance applications. Cryptocurrencies are arguably the first thing that a layman will associate blockchain with, but they are not even a primary application of blockchain.

Advantages of Cryptocurrencies: Independence from Central Authorities: Cryptocurrencies provide a system that operates independently of central banks and governments. This can offer greater privacy and control over one's financial assets.

1. Global Accessibility: Cryptocurrencies can be bought and used internationally, eliminating the barriers of conducting business internationally strictly with fiat money.

2. Innovation in Financial Systems: Cryptocurrencies and the underlying blockchain technologies are a source of innovation influencing how transaction processes are managed.

Conclusion: Cryptocurrencies are one of the revolutionary use cases of cryptographic methodologies and blockchain. They provide an efficient, secure, and, above all, liberal way of managing and sharing valuable assets. This paper explains that as the knowledge and use of cryptocurrencies increase, they can bring changes to several industries/sectors and even shift paradigms of the existing financial systems.

4. The Bitcoin System

Bitcoin is mostly referred to as an electronically generated currency that shares features of both money and commodities and is not subject to the control of any organization. This is an innovation in the financial market and has features that differ them from other currencies.

1. Neutrality of Bitcoin: Bitcoin's neutrality means that people without prejudice to their characteristics or situations can use the currency. What this simply implies is that Bitcoin can be used across cultural, religious, linguistic, geographical, political, and economic boundaries.

2. Global Accessibility: Bitcoin can be utilized by individuals regardless of their location or background. This universal applicability makes it a versatile tool that can operate within any political regime, religious system, or economic framework.

3. Financial Inclusion: This is one of the key features of Bitcoin, which is primarily designed for the audience

without a bank account – the unbanked. Approximately 53% of unbanked individuals have found Bitcoin to be a viable alternative to conventional financial services.

4.1 Definitions of Bitcoin

The term "Bitcoin" can be confusing because it encompasses three distinct concepts:

Blockchain Technology Platform: bitcoin is under the blockchain technology that is a distributed database that holds transaction information. This underlying technology is what makes Bitcoin work and be secure.

Transaction Process: Bitcoin can be defined as the flow of digital values in-between participants within the blockchain. This is a procedure by which each new transaction in the Bitcoin network is generated, validated, and documented.

Cryptocurrency: Bitcoin is also used to refer to the actual money in the digital currency form known as Bitcoins. As the most well-known and widely used digital currency, it serves as a unit of account and a medium of exchange within its ecosystem (Swan, 2015).

4.2 Characteristics of Bitcoin

Decentralization: Another reason that readily explains why Bitcoin cannot be owned by a single centre or authority is that it is decentralized. Instead, the decentralized system of nodes votes on the validity of a transaction and records it.

Anonymity: In Bitcoin transactions, people are not identified by their real names but by digital aliases (or handles). Although the transactions are stored in an open-access public ledger known as the blockchain, the parties involved are not disclosed to the public.

Independence from Central Authorities: Bitcoin is an unregulated and uncontrolled currency with no backing support from any country, bank, or international organization. This independence allows it to function outside the traditional financial system and enables open participation without requiring prior approval.

Public Participation: Bitcoin runs entirely in the open and permission-less where membership to the protocol is as easy as installing a client and gaining admission to the most extensive distributed database in global history. It is also characterized by the freedom of entry and exit to and from the industry and is open to all types of participants.

Bitcoin represents a significant departure from traditional financial systems through its decentralized nature, neutrality, and independence from central authorities. By leveraging blockchain technology, Bitcoin provides a secure and transparent method for transferring value, offering financial services to individuals who may be excluded from conventional banking systems. Its unique characteristics contribute to its growing adoption and influence in the global financial landscape (Litke et al., 2019).

Token: A token is a concept that represents ownership or entitlement to a particular asset or utility. In the context of both the digital world and the physical world, tokens can serve as instruments or means for acquiring or accessing specific resources or rights.

4.2.1 Bitcoin keys

In the Bitcoin network, users utilize keys to manage and transfer their assets. These keys are essential for conducting transactions and securing Bitcoin holdings. Here's a breakdown of how Bitcoin keys and wallets function. There are many types of Bitcoin keys:

Private Key: Due to these social aspects, the private key holds importance in the Bitcoin environment. It is used to verify approving the transfer of Bitcoin and affirm ownership of it. A private key should also be kept rather secure because anyone who gains access to it will control and utilize the associated Bitcoins.

Public Key: Another key is the public key, which is derived from the private key, and works to generate the Bitcoin address. It is also shared with others to receive the Bitcoin transactions. The public key is accessible and can be exposed to anyone, at the same time, the private key must be protected well.

Transaction Authorization: In order to spend Bitcoins, holders of this currency have to sign some certain transactions with the help of a private key. To a degree, it can confirm that the user has approved of the given transaction and that he or she has control over the Bitcoins being transferred.

Securing Assets: The integrity or security of Bitcoin is anchored on the private key through which it is protected. It is owned by a private key, and if, for instance, this key is stolen or misplaced, then the Bitcoins will be as good as gone since there is no way one can regain them from the lost key.

Bitcoin Wallets: Bitcoin wallets are programs or physical devices holding the user's private keys. These wallets help users perform their Bitcoin transactions in a secure way. They don't store the Bitcoins, instead, they store the keys that help to control and spend the Bitcoin on the actual block chain.

4.2.2 Bitcoin wallets

Software Wallets: These are applications that are used on computer systems and new generation hand held apparatuses. They are very useful but have the possibility to contain a virus or be hacked.

Hardware Wallets: These are physical devices designed to securely store private keys offline. They offer enhanced security against online threats.

Paper Wallets: These involve printing the private and public keys on paper. While they are secure from online attacks, they can be easily damaged or lost.

Importance of Key Security:

Privacy and Security: To avoid compromise on the private key, it needs to be encrypted, and the original key should be placed in a way that cannot be opened by anyone else. Since the private key is associated with the Bitcoins, when it is lost or hacked, the Bitcoins can be spent by anyone. As a result, one should ensure private keys are not exposed to persons who have a different intention of using this bitcoin by any chance.

No Increase in Bitcoin Holdings: Just as storing or managing more keys does not represent or entitle the holder to the possession of extra Bitcoin. Instead, it may lead to an increase in the number of keys, but the total Bitcoin balance remains unchanged (Lewis, 2015).

In the Bitcoin network, keys are fundamental to managing and securing Bitcoin assets. Private keys allow users to sign transactions and control their Bitcoins, while public keys facilitate receiving transactions. Bitcoin wallets store these keys and enable secure management of transactions. The security of private keys is critical to protecting Bitcoin holdings, and users must take measures to safeguard their keys to prevent unauthorized access and potential loss of assets.

4.2.3 The development of Ethereum and smart contracts (2013-2018)

Vitalik Buterin was involved in the development of Bitcoin, but he was aware of its downsides and the absence of progress in distributed computing. He saw a blockchain that would not be confined by the bounds of Bitcoin, as there were, progressively, a long list of disadvantages. From this vision, Ethereum was created. Following the launch of Bitcoin, an advancement was realized in the technology of the year 2013 with the creation of Ethereum (Underwood, 2016). Most people got to know it publicly as a blockchain system that has further features as compared to bitcoin. Bitcoin's major update in July 2014 was Ethereum, whose inception in 2015 changed its focus to the birth of a platform for decentralized applications. Another big feature that Ethereum pioneered was the use of smart contracts. These are self-executing contracts with the terms directly written into code. They automate and enforce agreements without the need for intermediaries, enabling complex transactions and applications. Ethereum's platform facilitates the creation and deployment of dApps, which operate on a decentralized network, enhancing security and reducing the risk of centralized control. Ethereum's development from 2013 to 2018 marked a transformative period in blockchain technology. By introducing smart contracts and enabling the creation of decentralized applications, Ethereum expanded the potential uses of blockchain beyond cryptocurrency. Its robust developer community and the significant increase in Ether's market value underscored its growing importance and impact on the blockchain ecosystem.

4.2.4 Blockchain 2.0

Blockchain 2.0 represents the second generation of blockchain technology, building upon the foundational concepts introduced by Bitcoin (often referred to as Blockchain 1.0). While Blockchain 1.0 was primarily focused on digital currency and the basic functionalities of a decentralized ledger, Blockchain 2.0 extends these capabilities by introducing more advanced features and use cases.

Key Features of Blockchain 2.0

Smart Contracts: Smart contracts are self-executing contracts where the terms of the agreement are directly written into code. They automatically enforce and execute contractual agreements without the need for intermediaries.

Function: These contracts run on blockchain networks like Ethereum and facilitate, verify, or enforce the negotiation or performance of a contract, reducing the need for trust and intermediaries.

Decentralized Applications (dApps): dApps are applications that run on a decentralized network, rather than a centralized server. They leverage smart contracts to provide functionalities without relying on a central authority.

Function: dApps can serve various purposes, such as financial services (DeFi), digital identity, supply chain management, and more. They offer increased transparency, security, and resistance to censorship.

Enhanced Blockchain Platforms

Ethereum: One of the most prominent examples of Blockchain 2.0, Ethereum provides a platform for developing and deploying smart contracts and dApps. Its flexibility has led to the creation of numerous innovative projects and use cases.

Other Platforms: Other blockchain platforms, such as Binance Smart Chain (BSC), Polkadot, and Cardano, also exemplify Blockchain 2.0 by offering unique features and improvements over Ethereum.

Tokenization: Tokenization refers to the process of creating digital tokens on a blockchain to represent various

assets, rights, or units of value.

Function: Tokens can represent anything from digital assets (like cryptocurrencies) to physical assets (like real estate) and can be used in various applications, including financial transactions, voting systems, and loyalty programs.

Interoperability: Interoperability refers to the ability of different blockchain networks to communicate and interact with each other.

Function: Blockchain 2.0 technologies often focus on improving interoperability, allowing different blockchain platforms to share data and value seamlessly. This helps in creating a more connected and functional ecosystem.

Scalability Improvements: Scalability is the ability of a blockchain network to handle a growing number of transactions and users efficiently.

Function: Blockchain 2.0 platforms work on enhancing scalability through various techniques, such as sharding, layer-2 solutions, and consensus algorithm improvements, to support a larger user base and transaction volume.

Decentralized Finance (DeFi): Blockchain 2.0 has enabled the growth of DeFi platforms, which offer financial services like lending, borrowing, and trading without traditional intermediaries.

Non-Fungible Tokens (NFTs): NFTs are unique digital assets representing ownership of specific items or content, such as art, collectibles, and virtual real estate. They have gained popularity due to their ability to represent and trade digital ownership.

Supply Chain Management: Blockchain 2.0 technologies are used to enhance transparency and traceability in supply chains, allowing for better tracking of goods and verification of their origins.

Blockchain 2.0 comes as a major leap in the development of the technology by bringing in an extensive application that goes beyond digital currency to include smart contracts, decentralized applications, and many other inventions. The extended features and capabilities help make Blockchain 2.0 usable in a wider context, thus fostering growth within the blockchain ecosystem.

4.3 Smart Contracts

The concept of smart contracts was initially introduced in 1994 by legal scholar Nick Szabo. Szabo's ideas on smart contracts and blockchain technology are so closely aligned with those of the elusive Satoshi Nakamoto that for a long time, many believed Szabo might be Nakamoto.

4.3.1 Definition and functionality: What are smart contracts?

Smart contracts are digital agreements that are similar to traditional contracts but are designed to be secure, transparent, and self-executing. They enable the negotiation or execution of a contract — without relying on central authorities. These contracts can automate processes related to ownership, payment, shares, or valuable assets. They operate on blockchain technology, ensuring that transactions are executed when predefined conditions are met.

Key Characteristics:

1. Autonomy: Once a smart contract is deployed, it operates independently. The initiating party does not need to maintain constant interaction with the contract.
2. Self-Sufficiency: Smart contracts manage their own resources and execute transactions based on the programmed conditions without external input.
3. Decentralization: Smart contracts are not controlled by a single entity but are distributed across a network, eliminating the need for centralized intermediaries.

How Smart Contracts Work?

Execution: Smart contracts are stored and executed on the blockchain. They automatically carry out the terms of the agreement when the specified conditions are met. For example, in a corporate transaction, the smart contract could ensure that the transfer of assets only occurs once both parties have fulfilled their obligations. In an insurance claim scenario, a smart contract might automatically trigger a payout if a flight is delayed beyond a specified time.

Trust and Security: Since smart contracts operate on a blockchain, they provide a secure and transparent way to manage agreements. Parties involved do not need to trust each other personally; they can trust the code of the smart contract and the blockchain's integrity.

Differences from Traditional Contracts:

Autonomy: Smart contracts operate independently once deployed, without requiring ongoing interaction from the initiating party.

Self-Sufficiency: They manage their own execution and transactions based on predefined conditions and programmed rules.

Decentralization: Unlike traditional contracts, which may rely on central authorities or intermediaries, smart contracts operate on a decentralized network, reducing reliance on intermediaries and central points of failure.

Impact on Transactions, Efficiency:

Smart contracts streamline and automate processes, reducing the need for intermediaries and thereby decreasing costs and transaction times.

Transparency: Transactions and contract executions are recorded on the blockchain, providing a transparent and immutable record that all parties can access.

Security: The use of cryptographic techniques and the decentralized nature of the blockchain ensure that smart contracts are resistant to tampering and fraud.

Smart contracts represent a significant advancement in how agreements are made and executed. By leveraging blockchain technology, they offer a secure, autonomous, and decentralized way to facilitate and enforce agreements. Their ability to operate independently, manage their own resources, and eliminate the need for intermediaries has made them a cornerstone of the Blockchain 2.0 era, enabling new applications and innovations across various industries.

Blockchain Platforms: As a result of the information, we have gained about blockchain systems, if we need to explain what needs to be done to benefit from these systems, one option is to obtain sufficient and advanced software equipment. Open source codes can be a great guide along this path.

Types of Blockchain Consensus Protocols: All blockchains have their own technology. All chains use different systems to improve themselves day by day in order to become better. As a working principle, any node in a Blockchain network can propose a new piece of information to be added to the blockchain. In order to prove whether it is legal or not, the nodes must be subject to some kind of agreement. This is where the "consensus mechanism" comes into play.

4.3.2 Phase 4 (2018-2020): Applications and Blockchain 3.0

The birth and development of Blockchain are not limited to Ethereum and Bitcoin. The studies carried out aim to improve Blockchain capabilities and complete the shortcomings of Bitcoin and Ethereum. The fact that cryptocurrencies do not charge transaction fees and provide more reliable verification processes makes objects suitable for the internet environment. In addition, it is also looking for solutions to the problems related to Blockchain 1.0. Second-generation Blockchain platforms also have sector waves. With the developing technology, some companies have preferred to be involved in this technology in order to increase their efficiency. Large companies are making large investments in order to work with experts in this field in order to have a more advantageous entry into this path. For example, companies such as Microsoft have pioneered the discovery of private, hybrid, and federated Blockchains. In this direction, new Blockchain technology is discovered and implemented every day. From this perspective, it becomes difficult to see the final point that cryptocurrency technology can reach.

Blockchain 3.0

The Blockchain 3.0 concept is used to refer to a wide range of applications that do not include currency, trade, financial markets, or other economic activities. Such applications are generally preferred in art, health, science, education, and similar areas. There are also applications that have not been implemented but are still in the idea stage. Blockchain technologies are used for many transactions in daily life. Almost all business lines are changing to benefit from this technology. For example, in recent years, many changes have been made in the transportation and supply chain fields, and this application has started to be used. Blockchain brings together shared ledgers through smart contracts to securely protect an asset and ensure its transfer. Objective assets such as transportation trucks, resources used as financial terms such as bonds, and digital assets such as music can be transported through a business network (Derviş, 2020).

4.4 Blockchain Application Areas ·

Blockchain technology generally emerges in the banking sector, internet security systems, purchasing and supply chain, IoT, insurance, individual and public transportation, online data storage, foundation and donation transactions, voting / election affairs, public applications, health applications, energy sector, real estate and title deed systems, digital identity, smart city structures, smart contracts and examination of their legal compliance, and education field applications. In Turkey, its adaptations can generally be in question in every field. Blockchain can be integrated into all ready systems. The most important reason for this is that Turkey is a developing country, technological innovations have been followed in many areas, from banking to supply chains, through businesses investing in the country, necessary investments have been made and continue to be made.

Banking Applications: The applications of blockchain technology in the banking field have moved to a different dimension with the emergence of cryptocurrencies. In this sense, studies have been carried out primarily on the shopping of cryptocurrencies, and Forex systems have also been used. Another different use of blockchain technology in the banking field is in credit and money transfer transactions.

Supply Chain: Logistics, transportation, and product procurement within the scope of supply chain are seen as potential application areas for the Blockchain technology. With the use of Blockchain technology within the scope of supply chain management, all kinds of such transactions have been recorded, and transactions have become more secure and transparent.

IoT: The idea of IoT is based on the idea that all devices that can be connected to the Internet can exchange

information with one another through cloud networks. The IoT systems also mentioned today are also referred to as the technical interactions of a range of Internet-related devices. In this regard, it is reported that 20 billion devices were using IOI in 2020 to understand the existing picture. In other words, there is a community of devices, and there are far more devices in this world than the population of this world. Blockchain technology is used to protect IoT devices or to manage them. In this regard, vital applications rely on Ethereum smart contracts, which are utilized with the advantage of real-time communication among the objects.

Insurance: With the use of blockchain technology, protecting data structures becomes very important. With the use of this technology, contributions such as combating fake policies, increasing pricing accuracy, defining profitable customer accounts, reducing file costs, creating loyalty bonuses for customers and thus attracting more, improving customer experience, and reducing operating costs can be made. It is also possible to use blockchain technology specifically for transactions such as data entry and identity verification, premium calculation, and risk assessment.

Individual Transportation and Public Transportation: After the "Uber" activities, which are especially implemented abroad in terms of transportation, many similar applications have also come into use. It is possible to use Blockchain technology in all of these applications and, in addition to this, in public transportation. It is in a position to pay the relevant price as a result of transportation through smart wallets, which are a sub-branch of Blockchain technology.

Online Data Storage: These transactions can be carried out with the help of cloud systems; however, even today, there is an ongoing security concern in cloud systems. Blockchain technology has made significant progress in protecting and securely storing such data. As mentioned above, it is very important that the security problems that have not yet been solved in cloud systems can be solved with Blockchain technology.

Foundation and Donation Transactions: There have been donation transactions in every society and every civilization throughout history. When examined within this framework, a process with a large volume in terms of money is followed in the world. Foundations related to donation transactions are also carried out within the scope of legislation and legal processes in countries. Blockchain technology is needed for these transactions to be carried out safely and transparently. With Blockchain technology, it is also possible to carry out foundation and donation transactions, which also have an important place in our culture, confidentially according to our traditions.

Election Affairs: Voting and election processes have become the focus of attention all over the world. The attractiveness of winning the election and the processes that follow have opened the door to a negative application that can be made in the election. It is also possible to see many examples of election fraud in history. For these reasons, the security of elections and, in addition, facilitating voters' participation in elections are of great importance. In order to prevent fraudulent behavior in elections, many countries around the world are switching to electronic election applications; however, this system also has its vulnerabilities. In particular, the claim of cyber intervention in the recent elections held in the United States has occupied the agenda and caused the election system to be questioned. With the decentralized structure of blockchain technology, the issue of election security is also becoming more functional. While there can be no cyberattack with blockchain technology, the security of elections can also be achieved. In theory, it seems quite easy to establish an election system with blockchain technology. A smart contract is made regarding how the election will be held, and a digital wallet is created. There is a single "coin" in this wallet and the voter can transfer the "coin" in his wallet, to the candidate he wants and complete the voting process. Electronic election systems developed with blockchain technology have not yet been fully implemented in the world. It is still on the world agenda as a research topic; This system, which can be developed further, has many areas of use due to its structure.

Health Application: With advancing technology, the health sector has become one of the application areas of Blockchain technology. Blockchain technology can be used for issues such as accessing patient information within the hospital, viewing patient history in other hospitals, and monitoring medication, in addition to ensuring the correct flow of data due to the importance of hospital systems.

Energy Management: With the help of smart contracts that can be created with Blockchain technology, energy management can be moved to a much more transparent and reliable point. Blockchain technology can be used in energy panels installed on the roofs of houses, wind panels, generators, and even much larger capacity power plants. In addition, projects are being worked on in countries such as Australia, Germany, and America to make energy distribution systems with Blockchain-based systems.

Smart Cities: Smart cities are a system that is directly connected to the concepts of smart public services, smart transportation, smart energy, smart health services, smart agriculture, and smart education. The idea of smart cities first emerged with the development of the concept IoT. All systems and ecosystems interact together, and many local problems, including traffic accidents, sudden health problems, and the resulting death rates, can be solved with this technology.

Smart Contracts: Smart contracts are in a very important position in solving many problems experienced today. These practices, which are contracts, also have a legal counterpart. In order for these studies to be carried out in a more systematic way, it would be very useful to make a legislative arrangement on Blockchain technology and its legal compliance.

Educational Applications: Educational applications are carried out online, whether formally or remotely; the documents, certificates, and diplomas received as a result of education are of great importance. For these reasons, by implementing Blockchain technology, people will be able to store their documents, diplomas, and certificates wherever they are in the world and access them whenever they want.

Internet Security: Today's dependence on technology and the internet, in turn, means developing new business models and systems for businesses; however, this new situation also creates new gaps and opportunities that cyber attackers can take advantage of. The risks associated with these new areas can be minimized if the necessary precautions can be taken in these technological systems. Despite this, it would not be realistic to say that this risk will definitely be completely eliminated. It should be known that businesses with large databases in particular are the main targets of cyber attackers (Figure 2).

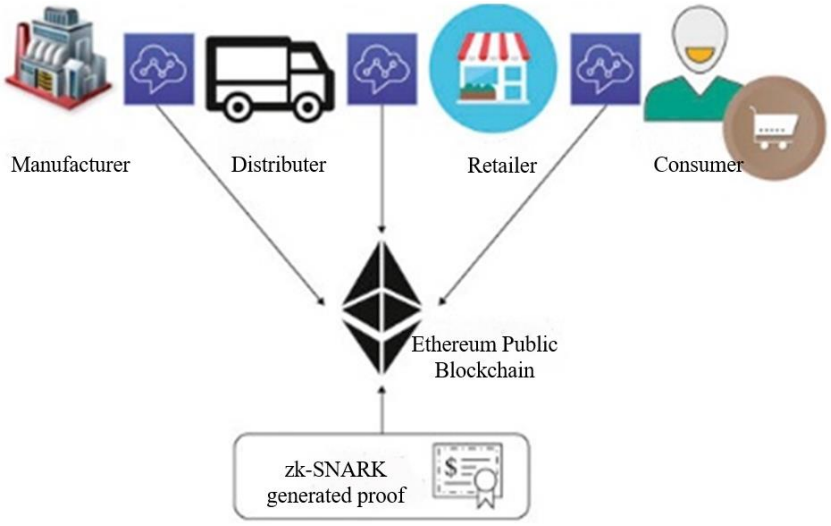

Figure 2. The overview of blockchain enabled supply chain

5. Cyber Security Concept and Cyber Risks

While the concept of cyber refers to a virtual reality belonging to computer networks and the internet environment, the concept of cyber security can be defined as the protection of information security and privacy in the cyber world (Bucan, 2019). In another definition, cyber security is expressed as protecting against threats that may arise against mobile devices, electronic systems, networks and data. The comprehensive definition of the European Telecommunications Standards Committee is expressed as a collection of tools, policies, security concepts, security measures, guides, risk management approaches, best practices, assurance and technologies that can be used to protect the assets of institutions and users (Ünver et al., 2009). The concept of cyber security is to ensure that the data stored within the information and communication systems is protected against cyber threats and attacks during the execution of work and transactions. In addition to personal and institutional losses, it is likely that economic, political and social damages will be experienced at a national level as a result of the failure to protect the elements of cyber security during the execution of work and transactions. The concepts of "Confidentiality, Integrity and Availability", which are among the basic concepts of cyber security, are expressed as the CIA 3. The concept of confidentiality refers to the need for information to be known and used by authorized persons, the concept of integrity refers to the completeness and consistency of information, and the concept of accessibility refers to the accessibility of information by authorized persons. Cybersecurity, which aims to protect institutions and individuals, requires a continuous fight against cyberenvironment threats by following up-to-date technical developments, regularly reviewing and implementing policies and procedures (Deloitte, 2006).

5.1 Concept of Risk and Risk Management

Risk can be expressed as the probability of occurrence of any development that may occur during a process. Risk management is defined in detail in advance and evaluated as the process of eliminating or minimizing risks that may occur while institutions or businesses are performing their activities. Risk management is the entirety of strategic steps taken within the scope of time, cost, and quality planning in which the negative effects of foreseen risks are determined (Kasımoğlu, 2021). Blockchain technology includes various risks as it is a new structure created with the aim of producing solutions to the problems in existing applications. Blockchain's security vulnerabilities, disruptions that may occur in encryption codes, and individual errors that may occur due to lack of

specialization can cause various risks.

5.2 Risk Management in the Digital Age

Digitality is expressed as the electronic display of digital data through a screen. The digital age is expressed as the period in which information and data are stored in virtual environments that can be developed with a completely provable, digital technology and used with the formation of a semantic network (Kasımoğlu, 2021). When the historical process is examined, there are four major revolutions in terms of production and economy in the world. Industry 1.0 emerged in 1784 with mechanical production facilities based on water and steam, and Industry 2.0 emerged in 1870 with the commissioning of production based on division of labor and electrical energy (İleri & Furat, 2020). Industry 3.0, where the concept of digitality first emerged, came to light in 1969. During this period, electricity began to be actively used in the production mechanism. Industry 4.0, which entered our lives with the digital age, first emerged in 2011. This period also appears as a period when digital transformation continues to occur rapidly. In this period, where advanced technological tools are used in production lines, demands are met quickly. As it is known, especially before the Industry 4.0 period, risk management and the risk management processes that developed accordingly necessarily include management methods based on variable decisions where human decisions are the best alternative. In the digital age, the management of time, quality and cost rates in production processes with human decisions; It is a matter of rationalizing risk management with automated production processes, the IoT, artificial intelligence, and data management (Kasımoğlu, 2021). The technologies developed in this process and the automation of routine processes make risk management easier.

5.3 Cyber Risks and Attack Methods

Since threats to be experienced in cyber security may have devastating effects on individuals, institutions and states, this issue is seen as one of the important problems in today's digital world. The great losses that will be experienced due to the spread of cyberattack with complex methods necessitate taking such risks seriously in advance. In particular, institutions or users who provide their operational transactions in the digital environment may face cyber risks more intensely. For this reason, even if the type and intensity of risks vary, a high level of awareness should be taken in this regard (Akın & Tanç, 2022). Today, cyberattack methods have diversified with the effect of developing technologies. Some of these are:

- *Data fraud:* Incorrect entry of data during data entry or modification of data with special techniques.
- *Salam technique:* This technique used in the banking sector is the transfer of the balance after the comma in the accounts to other accounts.
- *Trojan Horse (Spyware):* Thanks to malicious software such as Trojan Horse, they can change the system structure of the computer and also access the user's passwords and other personal information.
- *Malicious software (Malicious Software):* They are pieces of code prepared for specific purposes, such as viruses.
- *Logic bombs:* It is the placement of a desired malicious piece of code into a program.
- *Phishing:* Fake websites are usually used. The end user who thinks that an e-mail has come to him from a shopping site can fall into this trap by entering his credit card information on this web page or by replying to the e-mail.
- *Chameleon:* With some tricks and deceptions in the background, it simulates the user names and passwords in multi-user systems and saves them in a secret file, giving a warning that the system will be temporarily closed for maintenance. In the meantime, the hacker using the chameleon program accesses this secret file and obtains the user names and passwords.
- *Spam:* It is defined as e-mails sent in large volumes without the knowledge of the recipients and for commercial purposes.
- *Dumpster diving:* Recovering deleted information with advanced methods.
- *Substitution:* Users with limited or no access to the system use the information and authority of other users who have access to the system.
- *Hacking:* Breaking system security with skill and illegal means and obtaining data.
- *Social engineering:* A method of gathering information based on gaining people's trust and convincing the other party (Aslay, 2017).

6. Reducing Cyber Security Risk with Block Chain Technology

The concept of cyber security covers the infrastructures, applications, systems of states, institutions, and generally speaking users, as well as all data stored in the cyber environment. The same concept aims to be created and maintained in a way that can resist security risks in the cyber environment against the relevant parties. The

main objectives of cyber security are to ensure the accessibility, integrity, and confidentiality of information. If we need to define the concept of cyber risk, it can be expressed as risks that may cause financial loss or loss of reputation as a result of an institution's error or failure arising from information technologies. Determining cyber risks and ensuring security by taking precautions are important for states, companies, institutions, and users. Failure to protect information and data from such risks has the potential to affect both financial losses and loss of reputation. Google's servers were attacked in 2017 in what is called a DDos attack. The amount of concurrent web requests that can be processed by a server is finite. These types of attacks are conducted at the owner company or institution of the website with the purpose of abuse the infrastructural constraints. They want to send multiple requests more than the limit of the web resource, so the system should not work effectively. When in 2020 Amazon's servers were exposed to the same type of attack, it was designed upon the concept that blockchain is the solution that cannot be attacked through the decentralized approach (https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks). Blockchain technology increases expectations every day in protecting users' digital identities and data integrity. Major companies around the world are making significant investments in providing security in the field of cybersecurity with this technology. Blockchains will play an important role in preventing fraudulent activities with consensus mechanisms that can provide security and in improving cyber defense with basic features such as immutability, transparency, data encryption, and operational flexibility. The advantages that blockchain technology can provide in this field, based on the concepts CIA 3 of cyber security, are listed below:

1. Privacy: According to the National Institute of Standards and Technology (NIST), privacy is the inability to disclose sensitive information to individuals, institutions or processes with limited or no authority. In blockchain technology, it is essential to ensure the protection of network access and data access, especially in private blockchains. Because the probability of an attacker who gains network access to the blockchain to access the data increases with an attack, it is more sensitive to apply authentication and authorization controls. Since chain protocols in open blockchains allow everyone to join the network, there is no need to control network access. However, in private blockchains, security controls are applied to protect network access. Considering the risks that technology may inherently contain, institutions and organizations should evaluate their changing risk profiles over time, the level and type of cyber risks they may encounter, the type of cybersecurity program they will implement, and the requirements they need to have to meet such risks. In line with these requirements, blockchain will be able to provide advanced security control by utilizing the public key infrastructure to verify the identities of the parties and to encrypt their communications. Full encryption of data blocks, applicability to processed data, and development in encryption standards will reduce the risk of an attacker accessing the blockchain network and reading and obtaining data even if they reach the data. Encrypting data on the blockchain will provide institutions and users with a high level of protection from the perspective of data privacy and access control (Piscini et al., 2017).

2. Integrity: The concept of integrity includes protecting information against inappropriate modification or destruction, non-rejection of information, and ensuring its authenticity. Data encryption, data digestion, or the use of digital signatures can be given as examples of ensuring data integrity. The unique features of blockchain, immutability and traceability, provide institutions and users with a reliable way to ensure data integrity. Blockchain technology will support the monitoring of users against any reaction, due to the distributed ledger structure, in determining whether there is a difference in the processing power of one of the nodes in the network or preventing and controlling the division of the ledger. In this technology, transactions can be tracked back to the most recent date by digitally signing and having a time trace for each transaction added to the blockchain. Blockchain technology, which has a non-rejection feature, increases the reliability of the system as it is cryptographically associated with ensuring information security. This is due to the transparency and auditability in the structure of the technology. From a cyber security perspective, it provides assurance to users that the data is authentic, has not been stored or corrupted (Piscini et al., 2017).

3. Accessibility: Accessibility can be defined as the timely use of information that can be accessed in a reliable way. DDoS attacks, which are one of the most common types of attacks, cause interruptions in internet services and can even cause interruptions in application solutions that carry blockchain features. However, the traditional non-distributed structure and decentralized structure of the technology in question will greatly reduce the interruption. For example, Bitcoin, one of the most common and well-known crypto assets today, has emerged as the most tested platform against cyber attacks to date. With its peer-to-peer structure and continuously operating network structure, the combination of the technology in question provides a flexible structure. The fact that both public and private blockchains have more than one node will allow the network to continue operating by stopping the operation of the node under attack in the event of an attack (Piscini et al., 2017). The advantages of blockchain technology in cyber security can be briefly summarized as follows:

- Due to the distributed nature of a blockchain, a single access point increases the resilience of the overall network against attack.
- Blockchains improve the overall robustness and integrity of shared ledgers because consensus among network participants is required to validate new blocks of data.

- Blockchains narrow the scope of malware due to their enhanced transparency.
- Blockchains can include multiple layers of security established at both the network level and the individual participant level.

7. Conclusion

With the Fourth Industrial Revolution that entered our lives in 2011, many changes have emerged. Industry 4.0 has a large-scale impact on the innovation of new technologies. In this context, when the concepts of the IoT, Cyber Physical Networks and the Internet of Services that form the basis of Industry 4.0 are considered (Mougayar, 2016), it is seen that the industrial revolution that took place is internet-based. Blockchain technology, which developed during this period, can be an important opportunity to raise the status of our country from a developing country to a developed country with its use in many areas. The biggest reason for this is that reaching the levels of today's developed countries is through catching up with the conditions of the age. Industry 4.0 and Blockchain technology are two major concepts focused on this. The codes of the future lie beneath these concepts.

A general assessment is that in order to benefit from the impact of blockchain technology on cyber security risks, it is known that traditional risk management decisions need to be reviewed and improved and that today's technological opportunities should not be ignored in risk management (Lam, 2014). In risk management, especially uncertainties need to be managed with realistic methods within the framework of risk factors (Fisher & Narain, 2003). In this context, as stated above, it is very important to improve the risk management field with Blockchain technology, which is one of the important technological tools in the digitalization age we are in, and to develop a new risk-focused (cyber risk-focused) management approach. While storing large amounts of data centrally can cause major data loss due to cyberattacks as a result of the presence of a security vulnerability, unauthorized access will become almost impossible by storing the data in a decentralized manner using Blockchain (Sarmah, 2018). This technology can be used to protect against unauthorized access during data or information transfer by using encryption. Blockchain has various potentials in protecting the cyber security field with its distributed ledger structure. It can support the prevention of financial losses and reputational risks in business and transaction processes with its decentralized structure. The technology in question, which provides solutions for ensuring the accuracy, originality, immutability and integrity of data and information, can also contribute to the reduction of security threats. Blockchain has the potential to open a new era in cybersecurity with its decentralized nature, but considering that every developing technology brings its own risks, attention should be paid to the sensitivity of ensuring scalability and data privacy in order for blockchain technology to achieve an efficient result in the field of cybersecurity (Wu & Tran, 2018). In terms of cybersecurity, advanced technologies such as blockchain should be used to develop hardware and software operations, physical interfaces and effective management, and to support users with technical training such as ISO 27001, a robust and secure communication method, including cybersecurity training, network communication protocols, data access control and cryptography. When evaluated from the perspective of Turkey, it is seen that the studies prepared by the Presidency Digital Transformation Office focus on the development and dissemination of domestic and national technologies aimed to be used in all areas, especially the public sector, by working together with universities, industry, private sector and civil society organizations. Again, as part of digitalization, Turkey's first national strategy document in the field of artificial intelligence, the "National Artificial Intelligence Strategy 2021-2025", was officially put into effect with the Presidential Circular No. 2021/18 published in the Official Gazette No. 31574 on August 20, 2021 (Presidential Digital Transformation Office). The strategy in question is being developed in cooperation with the Presidency Digital Transformation Office and the Ministry of Industry and Technology and with the participation of other relevant parties. The National Artificial Intelligence Strategy and other technological development studies show that Turkey will take important steps in areas such as digitalization, cybersecurity and artificial intelligence.

References

Akın, S. & Tanç, A. (2022) The importance of cyber security risks in the audit of information systems in enterprises. *Erciyes Acad.*, *36*(2), 707-722. https://doi.org/10.48070/erciyesakademi.1101315.

Aslay, F. (2017). Cyber attack methods and Turkey's cyber security current situation analysis. *Int. J. Multi. Stud. Innovative Technol.*,*1*(1), 24-28.

Bakan, İ. & Şekkeli, Z. H. (2019). Blockchain technology and its applications in supply chain management. *OPUS Int. J. Soc. Res.*, *11*(18), 2847-2877. https://doi.org/10.26466/opus.563240.

Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing Ltd, Birmingham.

Bucan, S. D. A. (2019). *Cyber attacks and countries cyber security policies*. [Doctoral Dissertation. İstanbul Bilgi Üniversitesi], Turkey.

Cabantous, L., Hilton, D., Kunreuther, H., & Michel-Kerjan, E. (2011). Is imprecise knowledge better than conflicting expertise? Evidence from insurers' decisions in the United States. *J. Risk Uncertainty*, *42*, 211-

232. https://doi.org/10.1007/s11166-011-9117-1.
Deloitte. (2006). *Risk intelligence in the age of global uncertainty. Prudent preparedness for myriad threats*. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskintelligenceintheageofglobaluncertainty.pdf
Derviş, N. Ş. (2020). *The role of fintech ecosystem in the use of blockchain technology: The case of Turkey and Malta*. [Master's Thesis. Marmara University], Turkey.
Dujak, D. & Sajter, D. (2019). Blockchain applications in supply chain. In *Smart Supply Network* (pp. 21-46). Cham: Springer.
Fisher, A. C. & Narain, U. (2003). Global warming, endogenous risk, and irreversibility. *Environ. Resour. Econ.*, *25*, 395-416. https://doi.org/10.1023/A:1025056530035.
Haber, S. & Stornetta, W. S. (1991). *How to Time-Stamp a Digital Document*. Springer, Berlin.
Iansiti, M. & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Bus. Rev.*, *95*(1), 118-127.
İleri, Y., & Furat, M. (2020). A roadmap for digitalization of industrial processes. *Avrupa Bilim ve Teknoloji Dergisi*, 349-357. https://doi.org/10.31590/ejosat.araconf45.
Kasımoğlu, B. (2021). *Risk-based management in construction production process in the digital age: Blockchain technology*. [Master's Thesis. Bursa Uludağ University], Turkey.
Kırbaç, G. (2020). *Investigation of blockchain in supply chain with quality function deployment in 3PL companies*. [Doctoral Dissertation. Katip Çelebi University], Turkey.
Lam, J. (2014). *Enterprise Risk Management: From Incentives to Controls*. John Wiley & Sons, Hoboken.
Lewis, A. (2015). *A gentle introduction to blockchain technology*. https://www.scirp.org/reference/referencespapers?referenceid=2306854
Lewis, R., McPartland, J., & Ranjan, R. (2017). Blockchain and financial market innovation. *Econ. Perspect.*, *41*(7), 1-17.
Litke, A., Anagnostopoulos, D., & Varvarigou, T. (2019). Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. *Logist.*, *3*(1), 5. https://doi.org/10.3390/logistics3010005.
Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, Hoboken.
Narayanan, A. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, Princeton.
Palabıyık, Ö. (2020). *Possible impacts of blockchain technology on banking sector employment: A qualitative research in Kırklareli Province*. [Master's Thesis. Kırklareli University], Turkey.
Piscini, E., Dalton, D., & Kehoe, L. (2017). *Blockchain and cyber security*. https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html
Roy, A. D. (1952). Safety first and the holding of assets. *Econometrica J. Econometric Soc.*, *20*(3), 431-449. https://doi.org/10.2307/1907413.
Sarmah, S. S. (2018). Data migration. *Sci. Technol.*, *8*(1), 1-10, https://doi.org/10.5923/j.scit.20180801.01.
Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Somerville.
Underwood, S. (2016). Blockchain beyond bitcoin. *Commun. ACM*, *59*(11), 15-17. https://doi.org/10.1145/2994581.
Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). Ensuring cyber security: Current situation in Turkey and necessary measures. Bilgi Teknolojíleri Ve Iletişim Kurumu, 1606570. https://www.btk.gov.tr/uploads/undefined/sg.pdf
Wang, J., Wu, P., Wang, X., & Shou, W. (2017). The outlook of blockchain technology for construction engineering management. *Front. Eng.*, *4*(1): 67-75. https://doi.org/10.15302/J-FEM-2017006.
Wu, J. & Tran, N. K. (2018). Application of blockchain technology in sustainable energy systems: An overview. *Sustainability*, *10*(9), 3067. https://doi.org/10.3390/su10093067.