THE MAIN TRENDS IN THE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGIES AND THE PROSPECTS FOR THEIR USE TO PROTECT FRAUD

Iryna Mihus[1], Hisham Jadallah Mansour Shakhatreh[2]

[1]Doctor of Science (Economics), Professor, «KROK» University, Kyiv, Ukraine, Researcher, Scientific Center of Innovative Research, Estonia, e-mail: irynamihus@gmail.com, ORCID: https://orcid.org/0000-0001-6939-9097

[2]Ph.D. (Law), Assistant Professor, Faculty of Law, Jadara University, Jordan, e-mail: dr_hisham_shakhatreh@yahoo.com, ORCID: https://orcid.org/0000-0001-8693-5744

Citation:
Mihus, I., Shakhatreh, H.J.M. (2023). The main trends in the development of blockchain technologies and the prospects for their use to protect fraud. *The development of innovations and financial technology in the digital economy:* monograph. OÜ Scientific Center of Innovative Research. 2023. 230 p. PP. 207-229, https://doi.org/*10.36690/DIFTDE-2023-207-229*

Abstract. *The monograph examines the main stages of the development of blockchain technologies. The use of blockchain technologies in the activities of various companies is analyzed. The purpose of the study is to analyze the main trends in the development of blockchain technologies and the prospects for their use for fraud protection. The research methodology includes the use of the historical method to study the main stages of the development of blockchain technologies and study the practices of using blockchain by various companies. The research methodology is based on the use of data from the Report to the Nation and the results of other surveys, for a comparative analysis of types of economic fraud by volumes, periods, territorial affiliation and countermeasures. The relationship between the stages of evolution and the levels of the blockchain has been established. The main types of blockchains are systematized (public blockchains; private blockchains; semi-private blockchains; sidechains; permissioned; distributed ledger; shared ledger; fully private proprietary blockchains; tokenized blockchains; blockchains without tokens). The peculiarities of the practical implementation of blockchain technologies in the activities of companies in various sectors of the economy have been studied. A SWOT analysis was conducted that revealed that blockchain technology will undoubtedly continue to evolve, impacting many industries, including government, retail, information technology, travel, healthcare, education, agriculture, and entertainment. The 8 most risky departments in which various types of fraud occur have been identified. It was found that corruption is also the most common in each department. Thus, in the Operations Department, the second most common types of fraud are Billing (16%) and Noncash (16%); in the Accounting department - Check and payment tampering (29%); in the Executive / upper management department - Billing (31%); in the Sales Department - Noncash (18%); in the Customer service department - Noncash (17%); in the Administrative Support Department - Billing (23%); in the Purchasing - Billing department (27%); in the Department of Finance - - Billing (26%). One of the ways to improve the use of blockchain technologies should be: increasing the confidentiality of operations; scaling block chains; establishing compatibility between different blockchain systems; strengthening the security of blockchain operations; an individual approach to the use of blockchain technologies.*

Keywords: *blockchain technology; tiers of blockchain; types of blockchain; company; fraud; antifraud.*

The modern world is impossible to imagine without information technology, which actively accompanies our whole life. Unfortunately, along with their development, there are technologies that can use information about you for their own purposes. Blockchain technologies have been developed to counter such operations. Blockchain technology is a "chain of blocks", where each block is unique and has a specific reference to the previous one, which provides great difficulty in changing and / or deleting data elements.

Blockchain technology is one of the greatest innovations of the 21st century, given the impact it has on various sectors of the economy, including medicine, logistics, financial calculations, education, public administration and other areas.

Economic fraud, unfortunately, is an integral part of any business, which, in order to achieve its goals, must also fight its consequences and prevent its occurrence. The management of each company is aware of the need for such work and creates the conditions for neutralizing possible manifestations of economic fraud. The COVID-19 pandemic has significantly affected the activities of all companies and their business processes. In turn, this could not but affect the transformation of both the types of economic fraud and the tools to neutralize them.

According to S. Makridakis, A. Polemitis, G. Giaglis and S. Louca (2018), due to the significant number of benefits that blockchain can bring to each industry, its level of importance is compared with the role of the Internet in the early 1990s [1]. Researchers of the blockchain claimed that it was actively used in various fields. So, K. Fanning & D. P. Centers (2016), I. Eyal (2017), A. Simpson (2018) and others studied the use of blockchain in the financial sphere [2-4]. A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz (2018), S.-C. Cha, J.-F. Chen, C. Su and K.-H. Yeh (2018), K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, (2018), C. Qu, M. Tao and R. Yuan (2018), S. Huckle, R. Bhattacharya, M. White and N. Beloff (2016), Y. Zhang and J. Wen (2017) and others studied the use of blockchain in the Internet of Things [5-10]. J. Zhang, N. Xue and X. Huang (2016), C. Esposito, A. De Santis, G. Tortora, H. Chang and K.-K. R. Choo (2018), M. A. Engelhardt (2017) studied the possibilities of using blockchain in health care [11-13]. R. Dennis and G.

Owen (2015), A. Schaub, R. Bazin, Omar Hasan and L. Brunie (2016), R. Dennis and G. Owenson (2016) in their works describe the impact of blockchain on business reputation [14-16]. The use of blockchain in supply chain management deserves special attention [17-19].

The rapid growth of Blockchain technology in recent years has opened up many gaps and directions for further research. However, in our opinion, it is necessary to study the study of effective practices of using blockchain technologies by companies in various industries.

The research of many scientists has studied the nature of fraud. Recent reviews of the relevant literature acknowledge that fraud is a social construction (Cooper, Dacin, & Palmer, 2013 [20]; Taylor, 2007 [21]; Toms, 2017 [22]). A study of types of fraud has shown that they differ depending on the type and financial activity (Biegelman, 2013 [23]; Goldmann, 2010 [24]). The main types of fraud in the field of company management are corporate fraud (Comer, 2003 [25]; O'Gara, 2004 [26]) and management fraud (O'Gara, 2004 [26]). The main types of financial fraud are: financial fraud (Pontell/Frid, 2000 [27]; Young, 2006 [28]; Harrington, 2012 [29]; Gough, 2013 [30]), securities fraud (Cronin/Evansburg/Garfinkle-Huff, 2001 [31]; Wang, 2010 [32]; Straney, 2011 [33]; Yu, 2013 [34]), accounting fraud (Henselmann/Hofmann, 2010 [35]; Kat/Lakeman, 2010 [36]), financial statement fraud (Zack, 2013 [37]), financial institution fraud (Pontell/Calavita/Tillman, 1994 [38]; Shepherd/Wagner/Williams, 2001 [39]), fiduciary fraud (Rosoff/Pontell/Tillman, 2014 [40]), bank fraud (Subramanian, 2014 [41]), investment fraud (Naylor, 2007 [42]), brokerage fraud (Stoneman/Schulz, 2002 [43]), and insurance fraud (Viaene/Dedene, 2004 [44]).

The most complete classification of types of fraud is presented in the materials of the Association of Certified Fraud Examiners (Table 3.4). Association of Certified Fraud Examiners (ACFE) is an anti-fraud organisation situated in USA providing training and education. ACFE has conducted detailed studies of fraudulent occurrences of financial statement frauds to recognize such financial statement which are manipulated. ACFE has also enlisted some of the most frequently used tactics to perpetuate frauds in financial statements.

Table 3.4. Occupational fraud and abuse classification system (the fraud tree)

Type	Kind	Scheme			
Corruption	*Conflicts of Interest*	Purchasing Schemes			
		Sales Schemes			
		Invoice Kickbacks			
	Bribery	Bid Rigging			
		llegal Gratuities			
	Economic Extortion				
Financial Statement Fraud	*Net Worth/ Net Income Overstatements*	Timing Differences			
		Fictitious Revenues			
		Concealed Liabilities and Expenses			
		Improper Asset Valuations			
		Improper Disclosures			
	Net Worth/ Net Income Understatements	Timing Differences			
		Understated Revenues			
		Overstated Liabilities and Expenses			
		Improper Asset Valuations			
		Improper Disclosures			
Asset Misappropriation	*Cash*	Theft of Cash on Hand			
		Theft of Cash Receipts	Skimming	Sales	Unrecorded
					Understated
				Receivables	Write-Off Schemes,
					Lapping Schemes
					Unconcealed
				Refunds and Other	
			Cash Larceny		
		Fraudulent Disbursements	Billing Schemes		
			Payroll Schemes		
			Expense Reimbursement Schemes		
			Check and Payment Tampering		
			Register Disbursements		
	Inventory and All Other Assets	Misuse	Asset Requisitions and Transfers		
		Larceny	False Sales and Shipping		
			Purchasing and Receiving		
			Unconcealed Larceny		

Source: systematized by the author on the basis of Report to the Nation [45]

The three main types of Occupational fraud are:

1) Corruption is a scheme in which an employee misuses their influence in a business transaction in a way that violates their duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest).

2) Financial statement fraud is a scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g., employee files fraudulent expense report claiming personal travel or nonexistent meals).

3) Asset misappropriation is a scheme in which an employee steals or misuses the employing organization's resources (e.g., theft of company cash, false billing schemes, or inflated expense reports).

The purpose of the article is to study the main trends in the development of blockchain technologies and the prospects of their use for fraud protection.

The research methodology includes the use of the historical method to study the main stages of development of blockchain technologies and the study of blockchain use practices by different companies. Every two years, ACFE researchers publish the results of a global survey in the so-called «Report to the Nation». Based on expert assessments, this report demonstrates not only the types of fraud, but also the global losses from them. The research methodology is based on the use of Report to the Nation data and the results of other surveys presented on the ACFE website for a comparative analysis of types of economic fraud by volumes, periods, territorial affiliation and countermeasures.

We propose to begin the study of the practice of using blockchain technology by studying the main stages of its development (Fig. 3.9).

Throughout these five years, there was a growing interest in using blockchain for applications other than cybercurrency. This trend continues into 2021 as governments and enterprises look to blockchain to handle a variety of use cases. This includes voting, real estate, fitness tracking, intellectual rights, the internet of things and vaccine distribution.

Each of the described stages of development of blockchain technologies is associated with Tiers of Blockchain (table 3.5).

Table 3.4. The ratio of the main stages of development of blockchain technology and Tiers of Blockchain

Periods	Tiers of Blockchain	Description
2008-2013	Blockchain 1.0	This Blockchain is basically used for cryptocurrencies and it was introduced with the invention of bitcoin. All the alternative coins as well as bitcoin fall into this tier of blockchain. It also includes core applications as well.
2013-2015	Blockchain 2.0	Blockchain 2.0 is used in financial services and industries which includes financial assets, options, swamps and bonds etc. Smart Contracts was first introduced in Blockchain 2.0 that can be defined as the way to verify if the products and services are sent by the supplier during a transaction process between two parties.
2015-2018	Blockchain 3.0	Blockchain 3.0 offers more security as compared to Blockchain 1.0 and 2.0 and it is highly scalable and adaptable and provides sustainability. It is used in various industries such as arts, health, justice, media and in many government institutions.
From 2018 to now	Generation X	This vision the concept of singularity where this blockchain service will be available for anyone. This blockchain will be open to all and would be operated by autonomous agents

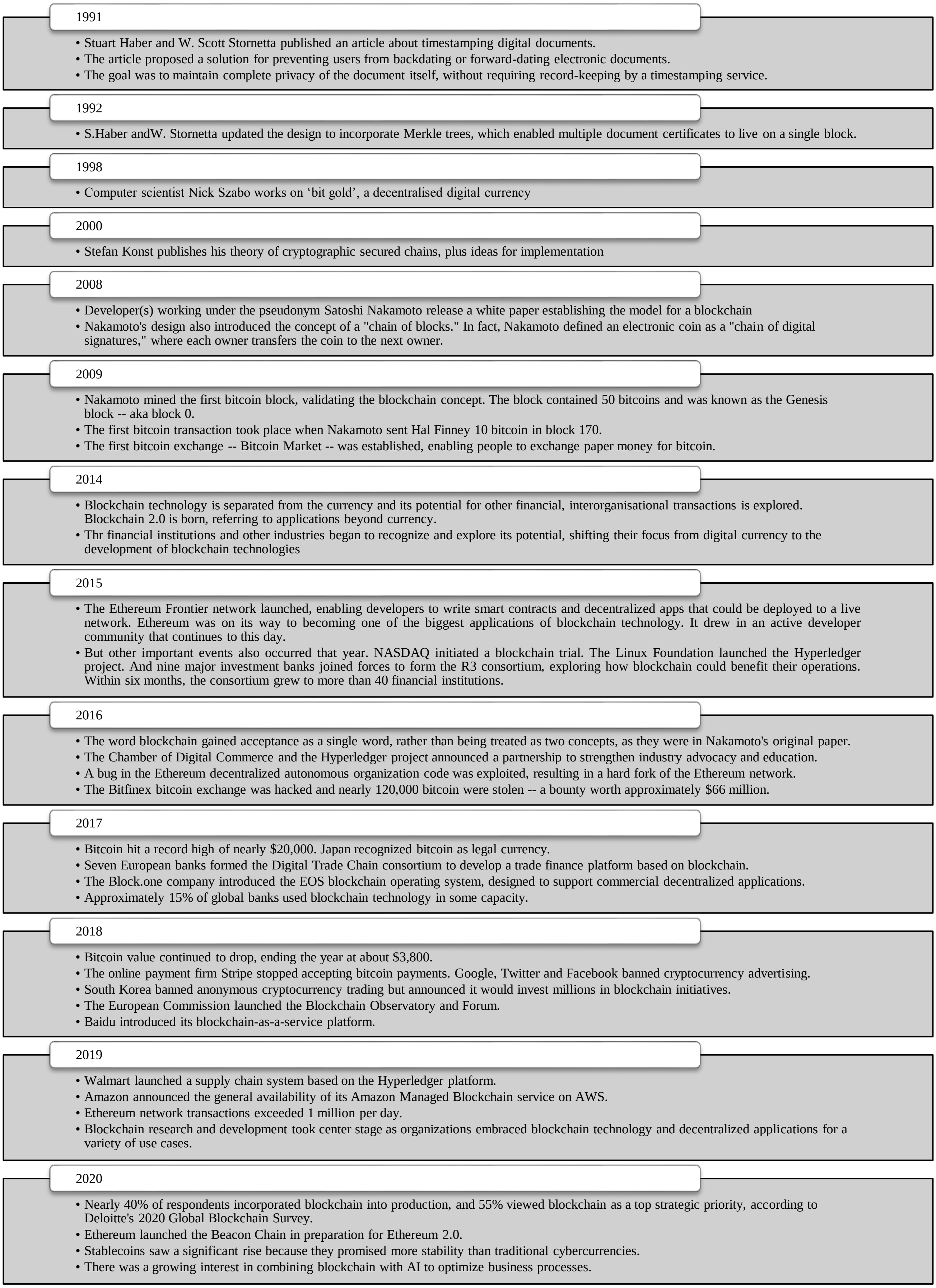
Source: systematized by the author on the basis [16-19]

The most scholars distinguish three main types of blockchain: public blockchain, permissioned blockchain, private blockchain [16-18, 46-49]. However, Blockchain has evolved greatly in the last few years and based on its different attributes, they can be divided into multiple types.

The most complete classification of blockchain types is given by Simanta Shekhar Sarmah (2020) [19]:

1. *Public Blockchains.* Public blockchains are open to the public and any individual can involve in the decision-making process by becoming a node, but users may or may not be benefited for their involvement in the decision-making process. No one in the network has ownership of the ledgers and are publicly open to anyone participated in the network. The users in the blockchain use a distributed consensus mechanism to reach on a decision and maintain a copy of the ledger on their local nodes.

2. *Private Blockchains.* These types of blockchains are not open to the public and are open to only a group of people or organizations and the ledger is shared to its participated members only.



1991

- Stuart Haber and W. Scott Stornetta published an article about timestamping digital documents.
- The article proposed a solution for preventing users from backdating or forward-dating electronic documents.
- The goal was to maintain complete privacy of the document itself, without requiring record-keeping by a timestamping service.

1992

- S.Haber andW. Stornetta updated the design to incorporate Merkle trees, which enabled multiple document certificates to live on a single block.

1998

- Computer scientist Nick Szabo works on ‘bit gold’, a decentralised digital currency

2000

- Stefan Konst publishes his theory of cryptographic secured chains, plus ideas for implementation

2008

- Developer(s) working under the pseudonym Satoshi Nakamoto release a white paper establishing the model for a blockchain
- Nakamoto's design also introduced the concept of a "chain of blocks." In fact, Nakamoto defined an electronic coin as a "chain of digital signatures," where each owner transfers the coin to the next owner.

2009

- Nakamoto mined the first bitcoin block, validating the blockchain concept. The block contained 50 bitcoins and was known as the Genesis block -- aka block 0.
- The first bitcoin transaction took place when Nakamoto sent Hal Finney 10 bitcoin in block 170.
- The first bitcoin exchange -- Bitcoin Market -- was established, enabling people to exchange paper money for bitcoin.

2014

- Blockchain technology is separated from the currency and its potential for other financial, interorganisational transactions is explored. Blockchain 2.0 is born, referring to applications beyond currency.
- Thr financial institutions and other industries began to recognize and explore its potential, shifting their focus from digital currency to the development of blockchain technologies

2015

- The Ethereum Frontier network launched, enabling developers to write smart contracts and decentralized apps that could be deployed to a live network. Ethereum was on its way to becoming one of the biggest applications of blockchain technology. It drew in an active developer community that continues to this day.
- But other important events also occurred that year. NASDAQ initiated a blockchain trial. The Linux Foundation launched the Hyperledger project. And nine major investment banks joined forces to form the R3 consortium, exploring how blockchain could benefit their operations. Within six months, the consortium grew to more than 40 financial institutions.

2016

- The word blockchain gained acceptance as a single word, rather than being treated as two concepts, as they were in Nakamoto's original paper.
- The Chamber of Digital Commerce and the Hyperledger project announced a partnership to strengthen industry advocacy and education.
- A bug in the Ethereum decentralized autonomous organization code was exploited, resulting in a hard fork of the Ethereum network.
- The Bitfinex bitcoin exchange was hacked and nearly 120,000 bitcoin were stolen -- a bounty worth approximately $66 million.

2017

- Bitcoin hit a record high of nearly $20,000. Japan recognized bitcoin as legal currency.
- Seven European banks formed the Digital Trade Chain consortium to develop a trade finance platform based on blockchain.
- The Block.one company introduced the EOS blockchain operating system, designed to support commercial decentralized applications.
- Approximately 15% of global banks used blockchain technology in some capacity.

2018

- Bitcoin value continued to drop, ending the year at about $3,800.
- The online payment firm Stripe stopped accepting bitcoin payments. Google, Twitter and Facebook banned cryptocurrency advertising.
- South Korea banned anonymous cryptocurrency trading but announced it would invest millions in blockchain initiatives.
- The European Commission launched the Blockchain Observatory and Forum.
- Baidu introduced its blockchain-as-a-service platform.

2019

- Walmart launched a supply chain system based on the Hyperledger platform.
- Amazon announced the general availability of its Amazon Managed Blockchain service on AWS.
- Ethereum network transactions exceeded 1 million per day.
- Blockchain research and development took center stage as organizations embraced blockchain technology and decentralized applications for a variety of use cases.

2020

- Nearly 40% of respondents incorporated blockchain into production, and 55% viewed blockchain as a top strategic priority, according to Deloitte's 2020 Global Blockchain Survey.
- Ethereum launched the Beacon Chain in preparation for Ethereum 2.0.
- Stablecoins saw a significant rise because they promised more stability than traditional cybercurrencies.
- There was a growing interest in combining blockchain with AI to optimize business processes.

Figure 3.9. The main stages of development of blockchain technologies

Source: systematized by the author on the basis [16-19, 46-51]

3. *Semi-private Blockchains.* In a semi-private blockchain, some part of the blockchain is private and controlled by a group or organizations and the rest is open to the public for anyone to participate.

4. *Sidechains.* These blockchains are also known as pegged sidechains where coins can be moved from blockchain to another blockchain. There are two types of sidechains naming one-way pegged sidechain and two-way pegged sidechain. One-way pegged sidechain allows movement from one sidechain to another whereas two-way pegged sidechain allows movement on both sides of two sidechain.

5. *Permissioned.* Ledger In this type of blockchain, the participants are known and already trusted. In permissioned ledger, an agreement protocol is used to maintain a shared version of the truth rather than a consensus mechanism.

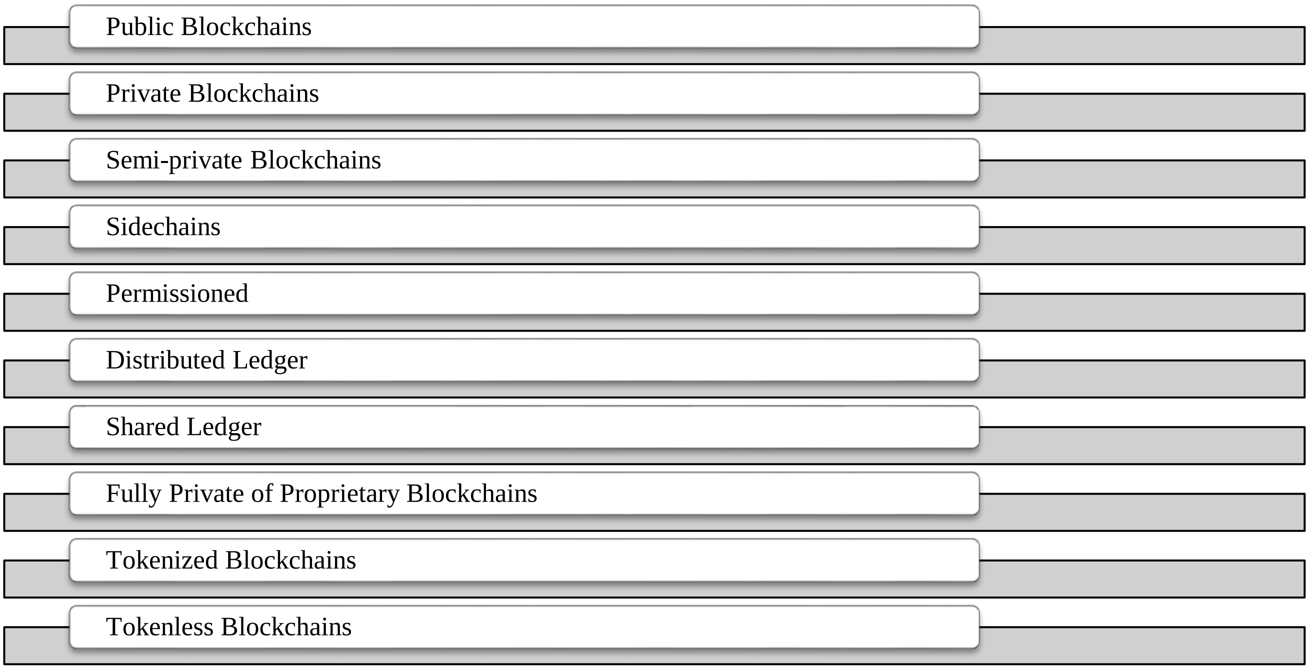
6. *Distributed Ledger.* In a distributed ledger blockchain, the ledger is distributed among all the participants in the blockchain and it can spread across multiple organizations. In distributed ledger, records are stored contiguously instead sorted block and they can be both private or public.

7. *Shared Ledger.* Shared ledger can be an application or a database that is shared by public or an organization.

8. *Fully Private of Proprietary Blockchains*. These types of Blockchains are not a part of any mainstream applications and differ the idea of decentralization. These type of blockchains come in handy when it is required to shared data within an organization and provide authenticity of the data. Government organizations use private of proprietary Blockchains to share data between various departments.

9. *Tokenized Blockchains.* These are standard blockchains which generate cryptocurrencies through consensus process using mining or initial distribution.

10. *Tokenless Blockchains*. These blockchains are not real blockchains as they do not have the ability to transfer values, but they can be useful when it is not required to transfer value between nodes and there is only the need to transfer data among already trusted parties.



Public Blockchains

Private Blockchains

Semi-private Blockchains

Sidechains

Permissioned

Distributed Ledger

Shared Ledger

Fully Private of Proprietary Blockchains

Tokenized Blockchains

Tokenless Blockchains

Figure 3.10. Classification of the main types of blockchains by Simanta Shekhar Sarmah

Source: systematized by the author [19]

Blockchain's transparent and decentralized platform has become attractive to companies in many industries that tend to use blockchain for a variety of business purposes. The list of companies that have implemented blockchain technologies in their activities is shown in Table 2.

Banking and payment systems have begun to use the blockchain to make their transactions more efficient and secure. The use of blockchain technologies in financial calculations allows you to efficiently and securely transfer funds using decentralization technology.

Blockchain is also becoming increasingly popular in the healthcare industry, as it is able to restore lost trust between clients and healthcare facilities. With the help of the blockchain, authorization and identification of patients has become easier, and fraud with prescriptions and medical data, as well as the loss of records can now be avoided.

Thanks to the blockchain's ability to efficiently store and verify documents, the legal industry has begun to use the blockchain to securely verify records and documents. Blockchain can significantly reduce litigation and battles by providing an authentic means of verifying and validating legal documents.

Industries such as Insurance, Education, Private transport and Ride sharing, government and public benefits, retail, real estate etc. have started implementing blockchain to reduce costs, to increase transparency and to build trust.

Blockchain technologies have also begun to be used in the public sector, for example during elections. Rigging of election results can be avoided with an effective use of blockchain. Voter registration and validation can be done using blockchain and ensure the legitimacy of votes by creating a publicly available ledger of recorded votes.

Table 3.5. List of Enterprises Implementing Blockchain

Company	Sector	Blockchain Solution
Ford	Auto	Leveraging blockchain technology to enhance the mobility technologies
Toyota	Auto Industry	Planning to use blockchain technology to enhance autonomous driving technology
HSBC	Bank	Using blockchain technology to fully digitize their record keeping and increasing the security of vault system
Anheuser Busch InBev	Beverage	Using blockchain for their beverage supply chain and increasing transparency
Alibaba	e-commerce	Using blockchain technology to track luxury goods in its e-commerce platforms
Tencent	e-commerce/ retail	Solution for verifying invoice authenticity and for ensuring tax compliance
UnitedHealthcare	Healthcare	Using blockchain technology to improve doctors directories to enable accurate insurance claim fillings
Metlife	Healthcare	Using blockchain technology for storing patients medical records for insurance purposes
AIA Group	Insurance	Launched the first of its kind bancassurance for sharing policy data
Prudential	Insurance	Unveils a blockchain powered trading platform for small and medium-sized enterprises
BHP Billiton	Mining	Leveraging blockchain technology for supply chain management
Shell	Oil	Planning to use blockchain for crude oil trading to get rid of corruption
Pfizer	Pharmaceutical	Tracking records and managing the digital inventory of pharmaceutical products
JLL	Real Estate	Exploring blockchain for Spanish commercial real estate valuation
Walmart	Retail	Using blockchain technology to track product movement from farmers to stores
Nestle	Retail	Using blockchain technology in supply management to track baby food products
Baidu	Search giant	Using blockchain to enhance intellectual rights management
Maersk	Shipping	Blockchain system for tracking movement of shipments between ports
UPS	Shipping	Blockchain powered logistics monitoring and management solution
FedEx	Shipping	Working on blockchain solution for settling customer disputes
Samsung	Tech	Intends to use blockchain technology to enhance supply chain management when it comes to electronics shipments
Facebook	Tech	Exploring the use of blockchain to enhance data security and users privacy
Apple	Tech	Patented blockchain technology for time stamping data
Google	Tech	Exploring the use of blockchain technology to enhance cloud service security and for data protection
British Airways	Travel Industry	Implementing blockchain to manage flight data as well as verifying traveler’s identity

Source: systematized by the author [46-47]

SWOT-analysis of the practical use of blockchain in companies has shown that this technology has sustainable prospects. Blockchain technology will no doubt continue to evolve, affecting many industries, including government, retail, information technology, travel, healthcare, education, agriculture and entertainment.

One of the ways to improve the use of blockchain technologies should be:

- increasing the confidentiality of operations;
- scaling of chains of blocks;
- establishing compatibility between different blockchain systems;
- strengthening the security of blockchain operations;
- individual approach to the use of boccein technologies.

Based on the scientific research on the practical use of blockchain in various fields SWOT-analysis was performed (Fig. 3.11).

Strengths	**Weaknesses**
- One of the biggest advantages of Blockchain is dissemination which allows a database to be shared without a central body or entity. - Users are empowered to control their information and transaction. - Blockchains provide complete, consistent and up to date data without accuracy. - Since blockchain does not have any central point of failure due to its decentralized network, it can withstand any security attack. - As no central authority is required, users can be assured that a transaction will be executed as protocol commands.	- Blockchains are expensive and resource intensive as every node in the blockchain repeats a task to reach consensus. - In blockchain, users verify a transaction based on certificate authentication, land titles, cryptocurrencies, etc. But there is no way to reverse a transaction even if both the parties involved in the transaction are ready to do so or if the transaction go sour due to some reason. - One of the disadvantage of blockchain is its complexity and complicacy to understand for a general human being. Blockchain is full of complex concepts and processes which is not yet refined so that common man can easily digest and consume the information on how to use it and hence it's not yet ready for mainstream use.
Possibilities	**Threats**
- Blockchains provide transparency and immutability to the transactions as all the transactions cannot be altered or deleted. - Blockchain's peer-to-peer connections help to identify fraud activities in the network and distributed consensus. - By using blockchain, sensitive business data can be protected using end to end encryption. - Users in a blockchain can easily trace the history of any transaction as all the transactions a blockchain are digitally stamped. - Blockchain are resilient to cyber-attacks due to peer-to-peer nature and network would operate even when some of the nodes are offline or under security attack. - Multiple copies of the data can be stored in the blockchain and hence users can avoid storing sensitive data in one place	- A transaction in the blockchain is settled only when all the nodes in the blockchain successfully verifies the transaction. This could be a very slow process as the block inserted needs to be verified to mark the transaction as authentic by all the nodes. - The size of blockchain grows with an addition of a block. A node needs to store the entire history of the blockchain to be a participant in validating transactions, causing the blockchain to grow continuously. - In blockchain, all the transaction related information is available publicly which can become a great liability when distributed ledgers are used in sensitive environments such as dealing with government data or patients medical data. The ledgers need to be altered and access should be limited with proper clearance only.

Figure 3.11. SWOT-analysis of the practical use of blockchain in companies

Source: developed by the author [46-51]

Based on the results of Report to the Nation, fraudsters do not necessarily limit themselves to one method of stealing. According to Report to the Nation, 40% involved more than one of the three primary categories of occupational fraud. As noted, 32% of fraudsters committed both asset misappropriation and corruption schemes as part of their crime, 2% misappropriated assets and committed financial statement fraud, 1% engaged in both corruption and financial statement fraud, and 5% included all three categories in their schemes.

Analysis of the average monthly losses of companies from various types of economic fraud, presented in Fig. 3.12, shows that the biggest losses the company has from the Financial statement fraud.

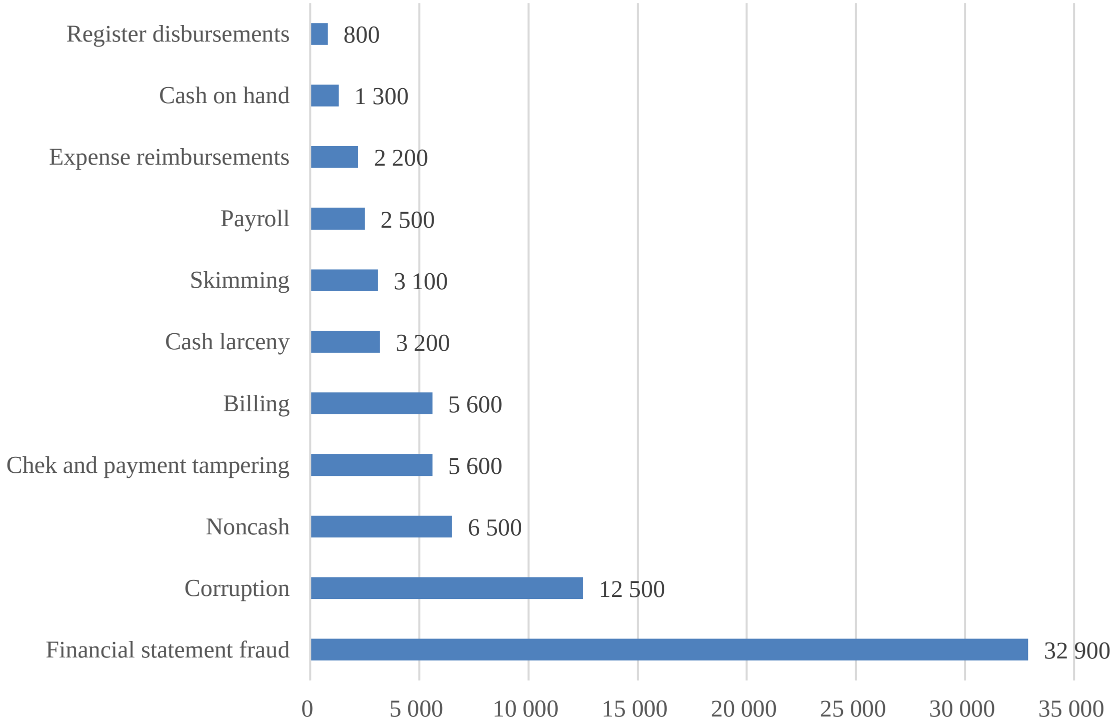


Figure 3.12. The average monthly loss of companies from various types of economic fraud, $

Source: systematized by the author on the basis of Report to the Nation [45]

The average period of fraud, according to Fig. 3.13, is 18 months, indicating that all cases of fraud were not spontaneous. Each case of fraud was preceded by training, which could last from 6 to 12 months.

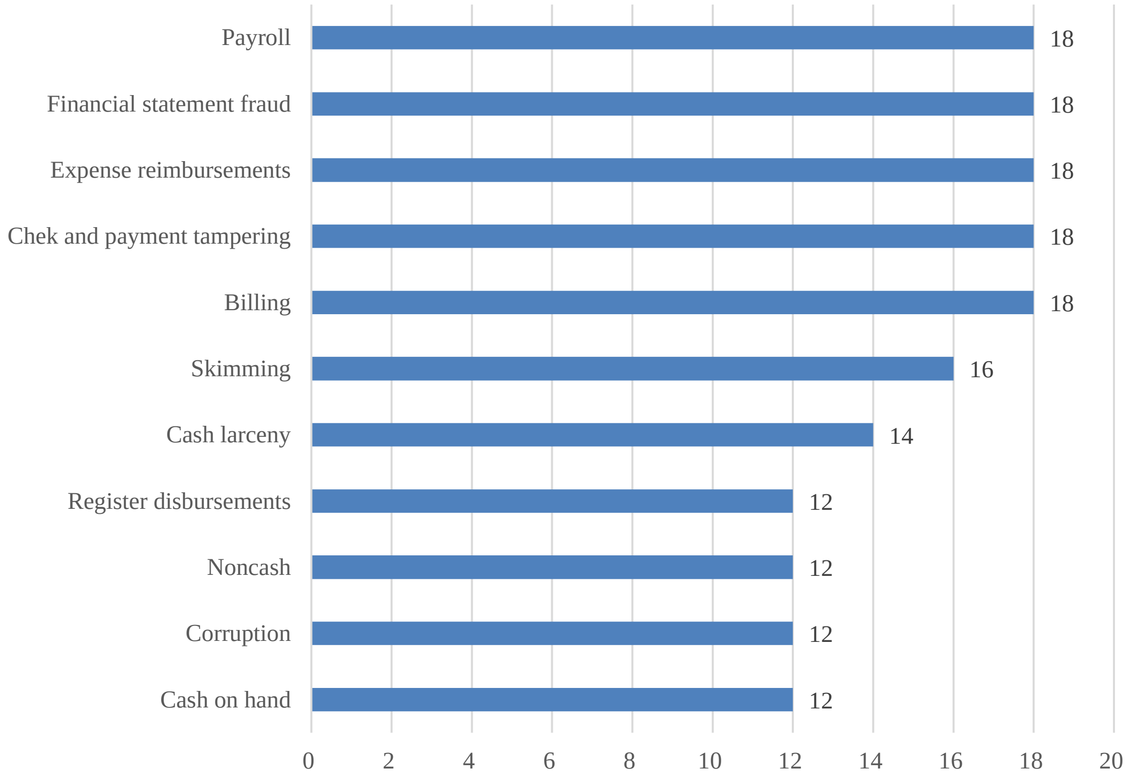


Figure 3.13. The average period from various types of economic fraud, months

Source: systematized by the author on the basis of Report to the Nation [45]

Analyzing various industries and cases of fraud, we found that the most common is corruption, which occurs in more than 40% (Insurance, Retail, Banking and financial services, Education), more than 50% (Health care, Technology, Food service and hospitality, Construction, Information, Transportation and warehousing, Manufacturing) and more than 60% (Energy). We believe that corruption in each of the industries has its own specifics and different types (Table 3.6).

The eight departments listed in Table 3.7 account for 76% of all professional fraud in the report presented in the Report to the Nation. In this table, we have identified the frequency of different types of professional fraud that have occurred in each department. The information obtained can help companies assess the risks of fraud and implement effective anti-fraud tools in these high-risk areas.

Table 3.6. The most common occupational fraud schemes in various industries

Industry	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Banking and financial services	351	10%	11%	14%	14%	46%	8%	11%	11%	4%	2%	10%
Government and public administration	198	21%	8%	7%	9%	57%	12%	8%	16%	16%	3%	8%
Manufacturing	194	26%	5%	9%	7%	59%	10%	12%	23%	10%	4%	8%
Health care	130	20%	6%	8%	8%	50%	11%	9%	18%	12%	2%	9%
Energy	97	24%	9%	6%	8%	64%	16%	8%	13%	6%	3%	2%
Retail	91	19%	10%	9%	9%	43%	7%	4%	24%	5%	7%	14%
Insurance	88	15%	9%	8%	10%	40%	9%	5%	8%	10%	2%	11%
Technology	84	21%	6%	10%	6%	54%	14%	8%	30%	5%	1%	1%
Transportation and warehousing	82	20%	9%	15%	4%	59%	11%	7%	22%	9%	4%	11%
Construction	78	24%	8%	10%	14%	56%	17%	18%	24%	24%	3%	9%
Education	69	26%	9%	12%	12%	49%	12%	12%	19%	14%	4%	12%
Information	60	15%	5%	5%	8%	58%	12%	12%	33%	7%	2%	7%
Food service and hospitality	52	19%	10%	21%	17%	54%	13%	13%	29%	19%	10%	17%

Source: systematized by the author on the basis of Report to the Nation [45]

Table 3.7. The most common occupational fraud schemes in high-risk departments

Department	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Operations	273	16%	7%	8%	11%	48%	9%	6%	16%	8%	1%	6%
Accounting	230	24%	15%	13%	29%	33%	10%	10%	7%	16%	3%	19%
Executive/upper management	206	31%	9%	10%	12%	65%	18%	22%	21%	13%	2%	12%
Sales	203	11%	6%	7%	2%	51%	8%	6%	18%	4%	2%	11%
Customer service	140	8%	10%	16%	11%	44%	6%	7%	17%	6%	3%	10%
Administrative support	131	23%	8%	15%	15%	37%	16%	5%	12%	12%	5%	10%
Purchasing	131	27%	1%	4%	2%	82%	5%	2%	14%	3%	0%	2%
Finance	95	26%	7%	11%	12%	48%	20%	14%	12%	7%	3%	12%

Source: systematized by the author on the basis of Report to the Nation [45]

It was found that corruption is also the most common in each department. In the Operations Department, the second most common types of fraud are Billing (16%) and Noncash (16%); in the Accounting department - Check and payment tampering (29%); in the Executive / upper management department - Billing (31%); in the Sales Department - Noncash (18%); in the Customer service department - Noncash (17%); in the Administrative Support Department - Billing (23%); in the Purchasing Department - Billing (27%); in the Department of Finance - Billing (26%).

The most common occupational fraud schemes by region are presented in Table 3.8.

Table 3.8. The most common occupational fraud schemes by region

Schemes	Latin America and Caribbean	Eastern Europe and Western/Central Asia	Middle East and North Africa	Southern Asia	Sub-Saharan Africa	United States and Canada	Western Europe
Corruption	57%	59%	59%	71%	62%	37%	44%
Billing	20%	13%	16%	18%	19%	24%	19%
Noncash	17%	15%	17%	15%	19%	18%	24%
Financial statement fraud	11%	17%	8%	15%	9%	8%	10%
Cash on hand	11%	9%	7%	12%	8%	11%	13%
Cash larceny	6%	5%	7%	11%	5%	10%	9%
Expense reimbursements	15%	2%	9%	10%	7%	17%	10%
Skimming	9%	7%	9%	10%	7%	13%	7%
Check and payment tampering	9%	5%	6%	5%	10%	15%	9%
Payroll	11%	4%	9%	4%	5%	16%	8%
Register disbursements	2%	3%	4%	2%	1%	4%	3%

Source: systematized by the author on the basis of Report to the Nation [45]

Table 3.8 shows that the most common occupational fraud schemes in all countries are corruption, with Southern Asia having the highest levels. Among other types of occupational fraud schemes, Billing can be found most often in Latin America and Caribbean region, Noncash - in Western Europe region, Financial statement fraud - in Eastern Europe and Western / Central / Asia region, Cash on hand - Western Europe region, Cash larceny - in Southern Asia region, Expense reimbursements - in United States and Canada region, Skimming - in United States and Canada region, Check and payment tampering - in United States and Canada region, Payroll - in United States and Canada region, Register disbursements - in United States and Canada region and Middle East and North Africa region.

It is very important to identify the tools that should be used to identify occupational fraud. The main tools of occupational fraud are initially detected by region are presented in Table 3.9.

Table 3.9. The main tools of occupational fraud are initially detected by region

Control	Latin America and Caribbean	Eastern Europe and Western/Central Asia	Middle East and North Africa	Southern Asia	Sub-Saharan Africa	United States and Canada	Western Europe
Tip	58%	41%	41%	51%	48%	32%	41%
Internal audit	11%	23%	24%	16%	10%	18%	16%
Management review	10%	9%	9%	7%	11%	16%	10%
Automated transaction/data monitoring	3%	5%	4%	1%	4%	5%	9%
By accident	5%	6%	1%	5%	5%	7%	6%
Document examination	5%	1%	4%	9%	6%	5%	6%
External audit	2%	4%	5%	3%	4%	4%	5%
Account reconciliation	3%	4%	7%	5%	6%	5%	2%
Surveillance/monitoring	1%	2%	-	1%	2%	5%	2%
Confession	-	-	1%	-	1%	1%	1%
Notification by law enforcement	1%	2%	2%	1%	2%	2%	1%
Other	-	1%	1^	1%	1%	1%	1%

Source: systematized by the author on the basis of Report to the Nation [45]

According to the study, tip, internal audit and management review are used to identify company fraud in all regions.

Every company understands that it is not enough to detect fraud, but it is very necessary to periodically use anti-fraud controls. The most common anti-fraud controls are presented in Figure 3.14.

The most common anti-fraud controls on the results of the Nations Report are the External audit of financial statements (82%) and Code of conduct (82%). The least effective anti-fraud controls are Job rotation / mandatory vacation (25%) and Rewards for whistleblowers (15%).

The most common anti-fraud controls by region are presented in Table 3.10.

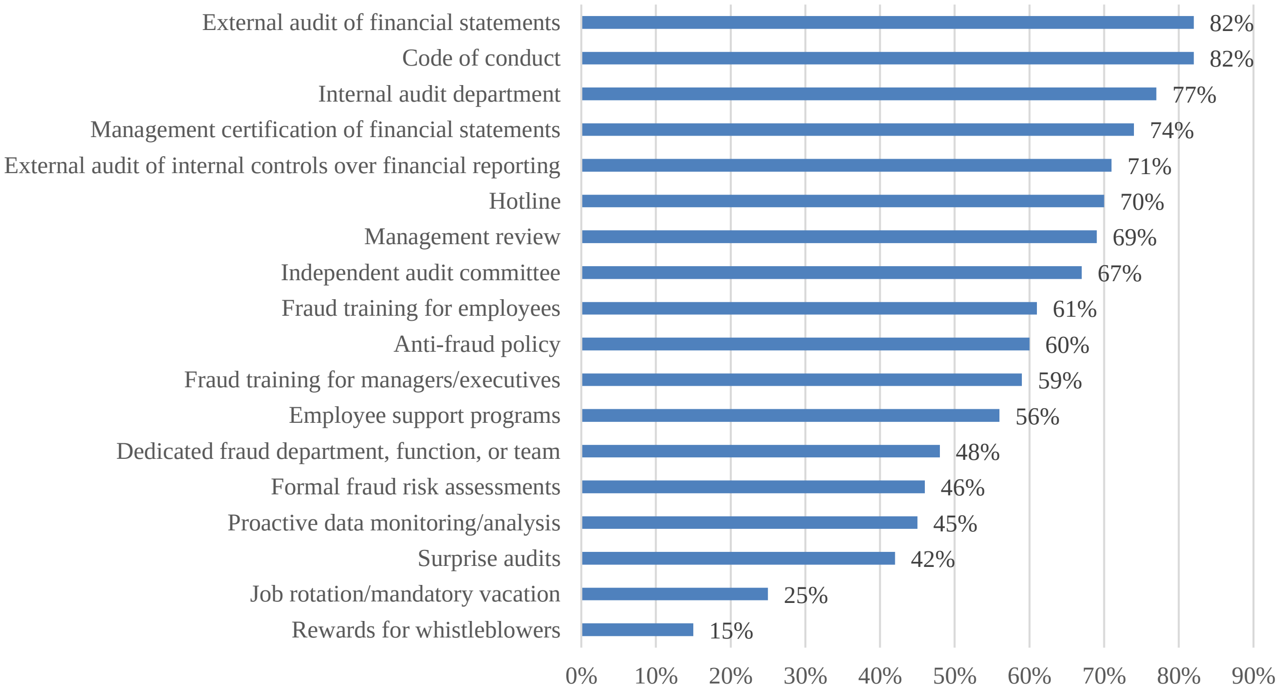


Figure 3.14. The most common anti-fraud controls

Source: systematized by the author on the basis of Report to the Nation [45]

Table 3.10. The most common anti-fraud controls by region

Control	Latin America and Caribbean	Eastern Europe and Western/Central Asia	Middle East and North Africa	Southern Asia	Sub-Saharan Africa	United States and Canada	Western Europe
Code of conduct	84%	83%	82%	88%	89%	74%	84%
Internal audit department	81%	81%	86%	85%	87%	66%	74%
External audit of financial statements	76%	83%	89%	91%	87%	72%	90%
Management review	70%	71%	71%	72%	72%	63%	72%
Management certification of financial statements	69%	68%	79%	84%	83%	65%	78%
Independent audit committee	69%	69%	71%	76%	74%	56%	65%
Hotline	67%	75%	68%	72%	76%	63%	68%
External audit of internal controls over financial reporting	65%	66%	70%	85%	76%	63%	77%
Fraud training for managers/executives	52%	60%	54%	66%	62%	55%	58%
Anti-fraud policy	52%	52%	60%	63%	69%	51%	56%
Fraud training for employees	52%	62%	58%	63%	67%	55%	59%
Employee support programs	50%	21%	32%	45%	58%	66%	51%
Dedicated fraud department, function, or team	35%	55%	44%	53%	56%	41%	47%
Formal fraud risk assessments	32%	37%	43%	45%	53%	42%	52%
Proactive data monitoring/analysis	30%	40%	43%	42%	47%	43%	48%
Surprise audits	28%	46%	48%	48%	47%	35%	40%
Job rotation/mandatory vacation	21%	21%	24%	33%	30%	20%	25%
Rewards for whistleblowers	5%	12%	14%	24%	18%	14%	7%

Source: systematized by the author on the basis of Report to the Nation [45]

Table 3.10 shows that in most countries in the region as anti-fraud controls use Code of Conduct - Sub-Saharan Africa (89%), Latin America and Caribbean (84%), Eastern Europe and Western / Central Asia (83%) , United States and Canada (74%), as well as External audit of financial statements - Southern Asia (91%), Western Europe (90%) and Middle East and North Africa (89%).

It should be noted that a large number of companies use proactive data monitoring/analysis (from 30% to 48%), an integral part of which is blockchain technology.

We believe that the creation and use of blockchain technologies in financial transactions is a necessary condition to protect companies from various types of fraud.

To solve this problem, we propose an algorithm for creating and using blockchain technologies at the enterprise (Figure 3.15).

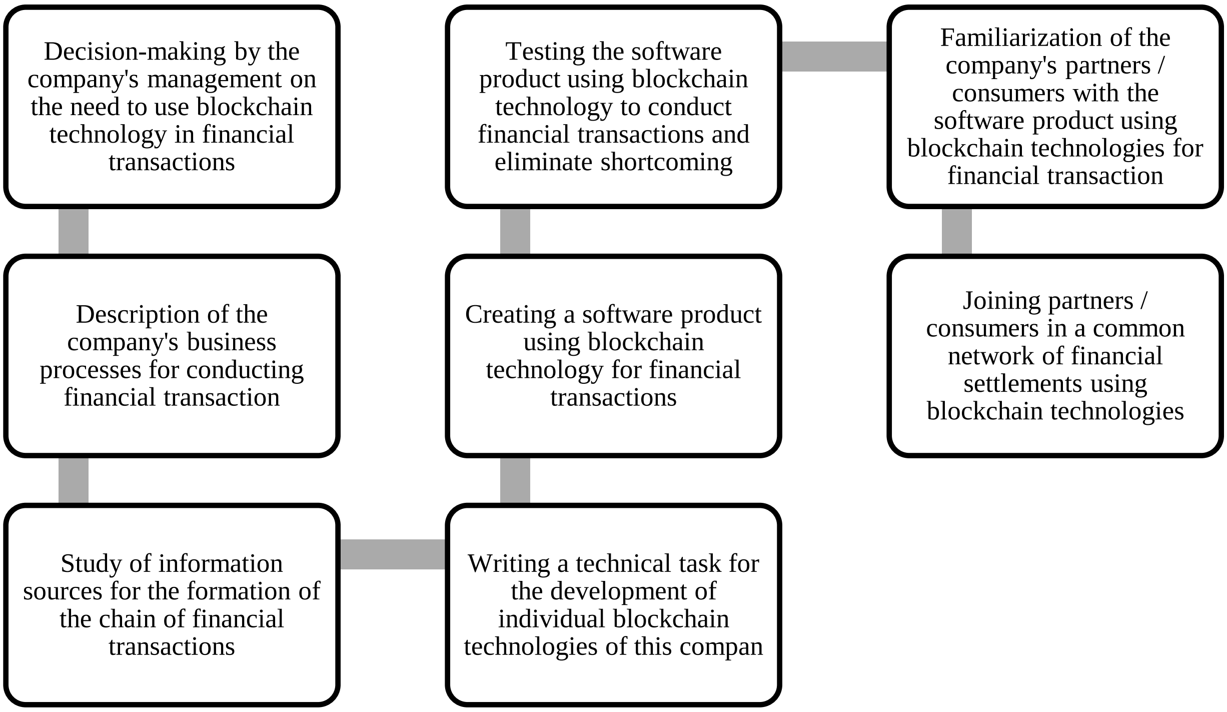

Decision-making by the company's management on the need to use blockchain technology in financial transactions
Description of the company's business processes for conducting financial transaction
Study of information sources for the formation of the chain of financial transactions
Writing a technical task for the development of individual blockchain technologies of this compan
Creating a software product using blockchain technology for financial transactions
Testing the software product using blockchain technology to conduct financial transactions and eliminate shortcoming
Familiarization of the company's partners / consumers with the software product using blockchain technologies for financial transaction
Joining partners / consumers in a common network of financial settlements using blockchain technologies

Figure 3.15. The main stages of creation and use of blockchain technologies for financial transactions of the company

Source: developed by the author

To substantiate the need for the introduction of blockchain technologies at the company level, in the context of ensuring internal control over financial transactions between different countries, a SWOT analysis was conducted (Fig. 3.16).

Strengths	Weaknesses
- the ability to track changes in financial documents; - minimization of delays in the preparation of financial documents; - reduction of administrative efforts on internal control of financial transactions; - improving the business reputation of enterprises that use blockchain technologies; - easier fraud detection, etc.	- immature mechanism and little experience in the application of blockchain technologies in Ukraine; - the need to transform the system of interaction between subjects of financial transactions; - the need to develop regulatory support for the use of blockchain technologies in Ukraine
Possibilities	**Threats**
- compliance with general trends in the development of financial relations; - improving the efficiency of fraud detection activities; - transparency of information and computer confirmation of transactions performed	- lack of a universal approach in determining the criteria for cross-border exchange of financial information to be used by different stakeholders; - blockchain technology must be adopted by all stakeholders to ensure that it works properly

Figure 3.16. SWOT-analysis of the implementation of blockchain technologies for financial transactions of companies between different countries

Source: developed by the author

In Figure 3.16 shows the results of a SWOT analysis of the implementation of blockchain technologies at the company level for financial transactions of companies between different countries. The most significant main advantages are: the ability to track changes in financial documents; minimization of delays in the preparation of financial documents; reduction of administrative efforts on internal control of financial transactions; improving the business reputation of companies that use blockchain technology; easier to detect fraud.

At the same time, among the threats are: the lack of a universal approach in determining the criteria for cross-border exchange of financial information to be used by different stakeholders; blockchain technology must be accepted by all stakeholders for it to work properly.

So, although the blockchain is still under development, it can dramatically change the way we do business, especially in the financial transactions of companies between different countries and can be used to ensure the economic security of enterprises.

According to the results of the study, the following conclusions can be drawn:

The relationship between the stages of evolution and Tiers of Blockchain has been established: 2008-2013 (Blockchain 1.0); 2013-2015 (Blockchain 2.0); 2015-2018 (Blockchain 3.0); From 2018 to now (Generation X). The main types of blockchain (public blockchains; private blockchains; semi-private blockchains; sidechains; permissioned; distributed ledger; shared ledger; fully private of proprietary blockchains; tokenized blockchains; tokenless blockchains) are systematized.

Based on the Report to the Nation prepared by the Association of Certified Fraud Examiners (ACFE), the average monthly loss of companies from various types of economic fraud and the period from various types of economic fraud were analyzed. It is established that the largest monthly losses of the company are from the Financial statement fraud, which lasts an average of 18 months. The frequency of cases of different types of fraud depending on the industry is analyzed. It is established that the most common companies in every industry are corruption.

The 8 most risky departments in which various types of fraud occur have been identified. It was found that corruption is also the most common in each department. Thus, in the Operations Department, the second most common types of fraud are Billing (16%) and Noncash (16%); in the Accounting department - Check and payment tampering (29%); in the Executive / upper management department - Billing (31%); in the Sales Department - Noncash (18%); in the Customer service department - Noncash (17%); in the Administrative Support Department - Billing (23%); in the Purchasing - Billing department (27%); in the Department of Finance -- Billing (26%).

One of the ways to improve the use of blockchain technologies should be: increasing the confidentiality of operations; scaling of chains of blocks; establishing compatibility between different blockchain systems; strengthening the security of blockchain operations; individual approach to the use of blockchain technology. The main stages of creation and use of blockchain technologies for financial transactions of the company are offered, which will allow to carry out anti-fraud controls more effectively.

References:

1. S. Makridakis, A. Polemitis, G. Giaglis and S. Louca, (2018). "Blockchain: The next breakthrough in the rapid progress of AI" *Artificial Intelligence-Emerging Trends and Applications*, London, U.K.:IntechOpen.
2. K. Fanning and D. P. Centers, (2016). "Blockchain and its coming impact on financial services", *Corporate Accounting Finance*, vol. 27, pp. 53-57.
3. I. Eyal, (2017). "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities", *Computer*, vol. 50, no. 9, pp. 38-49.
4. A. Simpson, (2018). "Australian regulation of blockchain and distributed ledger technology in banking and finance", *J. Banking Finance Law Pract.*, vol. 29, no. 2, pp. 73-91.
5. A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, (2018). "On blockchain and its integration with IoT. Challenges and opportunities", *Future Gener. Comput. Syst.*, vol. 88, pp. 173-190, Nov.
6. S.-C. Cha, J.-F. Chen, C. Su and K.-H. Yeh, (2018). "A blockchain connected gateway for BLE-based devices in the Internet of Things", *IEEE Access*, vol. 6, pp. 24639-24649.
7. K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, (2018). "Decentralized consensus for edge-centric Internet of Things: A review taxonomy and research issues", *IEEE Access*, vol. 6, pp. 1513-1524.
8. C. Qu, M. Tao and R. Yuan, (2018). "A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes", *Sensors*, vol. 18, no. 9, pp. 2784.
9. S. Huckle, R. Bhattacharya, M. White and N. Beloff, (2016). "Internet of Things blockchain and shared economy applications", *Procedia Comput. Sci.*, vol. 98, pp. 461-466, Oct.
10. Y. Zhang and J. Wen, (2017). "The IoT electric business model: Using blockchain technology for the Internet of Things", *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983-994.
11. J. Zhang, N. Xue and X. Huang, (2016). "A secure system for pervasive social network-based healthcare", *IEEE Access*, vol. 4, pp. 9239-9250.
12. C. Esposito, A. De Santis, G. Tortora, H. Chang and K.-K. R. Choo, (2018). "Blockchain: A panacea for healthcare cloud-based data security and privacy?", *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31-37, Jan./Feb.
13. M. A. Engelhardt, (2017). "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector", *Technol. Innov. Manage. Rev.*, vol. 7, no. 10, pp. 22-34.
14. R. Dennis and G. Owen, (2015). "Rep on the block: A next generation reputation system based on the blockchain", *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, pp. 131-138, Dec.
15. A. Schaub, R. Bazin, Omar Hasan and L. Brunie, (2016). "A trustless privacy-preserving reputation system", *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*, pp. 398-411.
16. History of blockchain. URL: https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/what-is-blockchain/history.
17. A timeline and history of blockchain technology. URL: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology.
18. Y. Zou, T. Meng, P. Zhang, W. Zhang and H. Li, (2020). "Focus on Blockchain: A Comprehensive Survey on Academic and Application," *IEEE Access*, vol. 8, pp. 187182-187201, doi: 10.1109/ACCESS.2020.3030491.
19. S. Sh. Sarmah. (2018). Understanding Blockchain Technology. *Computer Science and Engineering.* 8(2): 23-29 DOI: 10.5923/j.computer.20180802.02.
20. Cooper, D. J., Dacin, T., & Palmer, D. (2013). Fraud in accounting, organizations and society: Extending the boundaries of research. Accounting, Organizations and Society, 38, 440–457.

21. Taylor, J. (2007). Company fraud in Victorian Britain: The Royal British Bank scandal of 1856. The English Historical Review, 122, 700–724

22. Toms, S. (2017). Fraud and financial scandals. In J. F. Wilson, S. Toms, A. de Jong, & E. Buchnea (Eds.), The Routledge Companion to business history (pp. 358–372). Abingdon and New York: Routledge.

23. Biegelman, Martin T., 2013: Faces of Fraud: Cases and Lessons from a Life Fighting Fraudsters. Hoboken, NJ: Wiley.

24. Goldmann, Peter, 2010: Fraud in the Markets: Why It Happens and How to Fight It. Hoboken, NJ: Wiley.

25. Comer, Michael J., 2003: Investigating Corporate Fraud. Aldershot, UK: Gower Publishing.

26. O'Gara, J. D., 2004: Corporate Fraud: Case Studies in Detection and Prevention. Hoboken, NJ: Wiley.

27. Pontell, Henry N., Alexander Frid, 2000: International Financial Fraud: Emerging Trends and Issues. In: Delbert L. Rounds (ed.), International Criminal Justice: Issues in a Global Perspective. Need-ham Heights, MA: Allyn & Bacon, 32–47.

28. Young, Michael R., 2006: Accounting Irregularities and Financial Fraud: A Corporate Governance Guide. 3rd edition. Chicago: CCH.

29. Harrington, Brooke, 2012: The Sociology of Financial Fraud. In: Karin Knorr Cetina/Alex Preda (eds.). The Oxford Handbook of the Sociology of Finance. Oxford: Oxford University Press, 393–410.

30. Gough, Leo, 2013: The Con Men: A History of Financial Fraud and the Lessons You Can Learn. Harlow, UK: Pearson Education.

31. Cronin, Julia K./Amanda R. Evansburg/Sylvia R. Garfinkle-Huff, 2001: Securities Fraud. In: American Criminal Law Review 38, 1277–1343.

32. Wang, Ke, 2010: Securities Fraud, 1996–2001: Incentive Pay, Governance, and Class Action Lawsuits. El Paso: LFB Scholarly Publishing.

33. Straney, Louis L., 2011: Securities Fraud: Detection, Prevention and Control. Hoboken, NJ: Wiley.

34. Yu, Xiaoyun, 2013: Securities Fraud and Corporate Finance: Recent Developments. In: Managerial and Decision Economics 34, 439–450.

35. Henselmann, Klaus/Stefan Hofmann, 2010: Accounting Fraud: Case Studies and Practical Implications. Berlin: Erich Schmidt Verlag.

36. Kat, Micha/Pieter Lakeman, 2010: Boekhoudfraude: 13 schokkende fraudezaken in binnenen buitenland. Den Dolder, Netherlands: Belfra Publishers for Success.

37. Zack, Gerard M., 2013: Financial Statement Fraud: Strategies for Detection and Investigation. Hoboken, NJ: Wiley.

38. Pontell, Henry N./Kitty Calavita/Robert Tillman, 1994: Corporate Crime and Criminal Justice System Capacity: Government Response to Financial Institution Fraud. In: Justice Quarterly 11, 383–410.

39. Shepherd, Matthew J./Scott N. Wagner/Natasha M. Williams, 2001: Financial Institutions Fraud. In: American Criminal Law Review 38, 843–890.

40. Rosoff, Stephen/Henry Pontell/Robert Tillman, 2014: Profit without Honor: White-Collar Crime and the Looting of America. Upper Saddle River, NJ: Pearson Education.

41. Subramanian, Revathi, 2014: Bank Fraud: Using Technology to Combat Losses. Hoboken, NJ: Wiley.

42. Naylor, R. Thomas, 2007: The Alchemy of Fraud: Investment Scams in the Precious-metals Mining Business. In: Crime, Law and Social Change 47, 89–120.

43. Stoneman, Trace Pride/Douglas J. Schulz, 2002: Brokerage Fraud: What Wall Street Doesn't Want You to Know. Chicago: Dearborn Trade Publishing.

44. Viaene, Stijn/Guido Dedene, 2004: Insurance Fraud: Issues and Challenges. In: The Geneva Papers on Risk and Insurance: Issues and Practice 29, 313–333.

45. Report to the Nations. URL: www.acfe.com.

46. Mihus I. (2022). Possibilities of using blockchain technologies to protect fraud. *Science Notes of KROK University*, (1(65)), 84–94.

47. Iredale G. (2021). Top 20+ Enterprises Implementing Blockchain Technology. URL: https://101blockchains.com/enterprises-implementing-blockchain.

48. The evolution of blockchain: Transactions, contracts and applications URL: https://cointelegraph.com/explained/the-evolution-of-blockchain-transactions-contracts-and-applications

49. R. Sheldon (2021). A timeline and history of blockchain technology. URL: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

50. M. Dabbagh, M. Sookhak and N. S. Safa, (2019). "The Evolution of Blockchain: A Bibliometric Study," *IEEE Access*, vol. 7, pp. 19212-19221, doi: 10.1109/ACCESS.2019.2895646.

51. M. N. M. Bhutta et al., (2021). "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048-61073, doi: 10.1109/ACCESS.2021.3072849.