Computer Science and Information Systems 20(3):977–996 https://doi.org/10.2298/CSIS220308039S

Comprehensive Risk Assessment and Analysis of Blockchain Technology Implementation Using Fuzzy Cognitive Mapping

Somayeh Samsamian[1], Aliakbar Hasani[2,*], Saqib Hakak[3], Fatemeh Esmaeilnezhad Tanha[4], and Muhammad Khurran Khan[5]

[1] Master of Bussiness Administration, Department of Industrial Engineering and Management, Shahrood University of Technology
[2] Associate professor, Department of Industrial Engineering and Management, Shahrood University of Technology
aa.hasani@shahroodut.ac.ir
[3] Canadian Institute for Cybersecurity, Faculty of Computer Science, University of New Brunswick, Fredericton, Canada
[4] Ph.D. student, Department of Economics, Marche Polytechnic University, Ancona, Italy
[5] Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

Abstract. Identifying and assessing potential risks of implementing new technologies is critical for organizations to respond to them efficiently during the technology life cycle. Blockchain has been introduced as one of the emerging and disruptive technology in the field of information technology in recent years, which system developers have noted. In this study, a comprehensive set of risks have been identified and categorized based on the literature findings to identify the risks of blockchain implementation. Critical risks are defined by performing a two-stage fuzzy Delphi method based on the experts' opinions. Then, possible causal relationships between considered risks are identified and analyzed using the fuzzy cognitive mapping method. Finally, the most important risks are ranked based on the degree of prominence and the relationships between them. Industry enterprise resource planning system based on blockchain technology has been studied as a case study. The obtained results indicate that the technology's immaturity has the most impact, the high investment cost is the most impressive risk, and privacy has a critical role in risks relationships. In addition, the high investment cost has the highest priority among other risks and the privacy and issues with contract law are ranked second and third, respectively.

Keywords: Risk Assessment, Blockchain, Fuzzy Cognitive Mapping, Fuzzy Delphi, Enterprise Resource planning.

1. Introduction

Implementing new technology is one of the organization's tactical decisions; it will have significant and long-term effects on the organization's processes and overall

* Corresponding author

performance. Hence, the successful implementation of new technology is important [1]. In recent years, after the Internet emersion, blockchain technology has been introduced as one of the most important information technologies [2]. Bitcoin and Ethereum are the most popular cryptocurrencies developed based on blockchain technology. The early adopters of this technology were traders and merchants [3]. Blockchain usage has increased continuously because of its extensive advantages such as decentralization, immutability, transparency, security, and anonymity [4]. Nevertheless, these significant features will not be effective without recognizing and analyzing the risks of blockchain implementation [5]. According to the conducted studies in the literature, various risks of blockchain implementation have been identified in an enterprise. One of the identified risks is a lack of technology maturity, which has significant effects on how issues such as governance and authority are conceptualized and performed [6]. Scalability is another risk of blockchain implementation that arises when better and qualified technological infrastructures are needed to more efficiently launch blockchain technology [7]. The other risk is facing new concepts without sufficient awareness during blockchain implementation, which makes using this technology difficult for users. Some of these complicated concepts are public key, private key, and cryptography. In addition, the lack of skilled human resources is another risk of blockchain implementation [8]. In addition, emerging technology implementation needs high investment without necessarily a short return period [9]. All potential risks should be identified and evaluated for successful blockchain implementation (see Figure 1).

In recent years, enterprise resource planning system (ERP) has attracted more attention as an efficient solution for integrating all business processes in the organization. Data exchange security is a key point of security issues in ERP systems. Blockchain technology offers an opportunity to build highly integrated, smarter, secure, and flexible ERP systems [10]. Therefore, it is expected to see more development of blockchain-based ERP systems in future years.

By increasing in number as well as types of risks and then potential causal relationships between them with high uncertainty, an integrated and systematic risk analysis model is required to consider experts' opinions. Despite the importance of this issue, only a few studies have been conducted on the risk identification and analysis of blockchain implementation. Therefore, in this study, the comprehensive set of risks of blockchain implementation has been identified based on the literature and experts' opinions. Then the potential causal relationships between these risks have been analyzed. Industry ERP systems based on blockchain technology have been studied as a case study in Iran. Experts' opinions are extracted via the two-phase fuzzy Delphi method. Next, the final identified risks are weighted and prioritized using the fuzzy cognitive mapping (FCM) technique.

Figure 1. Steps of successful blockchain implementation in the enterprise

2. Literature Review: Blockchain Implementation Risks

This section provides a comprehensive review of blockchain implementation risks which are categorized into eight general groups as follows: Technical (T), Security (S), Organizational (O), Legal (L), Financial (F), Environmental (E), Cultural (C), and Social risks (I).

Staples and Chen [11] studied the risks and opportunities of using blockchain systems and smart contracts. They found that providing a neutral ground between organizations would reduce the technical risks compared to centralized databases and blockchain computing platforms. Kim and Kang [12] investigated the potential risks and challenges of blockchain technology as a means of eliminating illicit activities in various domain areas such as supply chain and logistics, government and public sectors, and international trade. They realized that blockchain technology may not always bring socio-economic benefits without a strategic planned policy. In another study, Zamani et al. [13] analyzed blockchain security risks at the operational level. For this purpose, required standards and rules related to blockchain implementation are investigated and analyzed in numerous blockchain incidents to determine the root cause of the most vulnerable aspects of this technology. Harris [14] also discussed the risks of blockchain relying, such as manipulation of the majority consensus, limiting the access of minors, privacy, anonymity, and pseudo-anonymity, speed and accuracy of transaction, scalability and storage issues, taxation, regulation, and issues with contract law in underdeveloped countries for transparent transaction among parties, reducing corruption and facilitating trust. Lu and Huang [4] examined blockchain implementation risk in four aspects of the trade, management and decision making, monitoring, and cyber security in the oil and gas industry. The results of this study showed that there is not

enough understanding of blockchain in the oil and gas industry. The current blockchain implementation status in the oil and gas industry is still experimental and investment is not enough compared with available capacities. Blockchain can provide many opportunities for this industry, such as reducing transaction costs and improving transparency and efficiency. In another study, Bürer et al. [15] focused on applied use cases for implemented blockchain architectures in the aspect of energy usage, risks and opportunities while guaranteeing a reliable distribution network and supply security are achieved. Norta and Matulevičius [16] examined the protection of an official formal blockchain authentication protocol by using security risk patterns. Based on the results, they have identified some major risks that threaten the protocol. Sayeed and Marco-Gisbert [17] evaluated the agreement of blockchain and security mechanisms against 51% of attacks in aspect of several main security risks. Their analysis presented that all of the applied security techniques are failed to protect against mentioned attack, lack power of the implemented security policies, and need to stronger policy to overcome this failure. In another study, Prewett et al. [18] mentioned that blockchain adoption as a transformative technology is unavoidable for future business enterprises. Therefore, appropriate attention to risks and challenges before, during, and after blockchain implementation will guarantee long-term success. Furthermore, Feng et al. [19] examined the cyber risk management of blockchain networks with a theoretical game approach. They have proposed a new approach to cyber risk management for blockchain services. In particular, they used cyber insurance as an economic tool to counteract the cyber risks posed by attacks on blockchain networks. They considered a blockchain services market which is consisted of infrastructure, a blockchain provider, an internet insurer, and users. Furthermore, White et al. [5] surveyed fundamental technologies of private blockchain and how the auditor can evaluate and respond to the risks of blockchain applications. Biswas and Gupta [20] analyzed the risks of blockchain implementation in industries and services. This study presented a framework for investigating blockchain risks to acceptance and its successful implementation in various industries using the DEMATEL technique. They identified and categorized a group of risks by using the existing literature and experts' opinions. Afterwards, they evaluated the causal relationships among these risks and ranked them based on their degree of prominence and relationships. This study's results showed that scalability and market-based risks are the most significant risks.

At the same time, high sustainability costs and inappropriate economic behavior have the greatest impact on the successful blockchain implementation. In another study, Öztürk and Yildizbaşi [9] examined the risks of blockchain implementation in supply chain management using the multi-criteria decision-making method. This study determined the existing risks in supply chain processes with blockchain technology and evaluated these risks emerging during technological transformation. This study discussed security, financial, organizational, and environmental risks. They used Fuzzy hierarchical analysis and fuzzy TOPSIS methods. The obtained results are as follows: (a) high investment costs, data, and facilities security are important, (b) less complex supply chain integrations can coordinate faster than blockchain technology development, and (c) integration is harder for health and logistic sectors. Moreover, Özkan et al. [21] evaluated the risks of blockchain technology using the multi-criteria decision-making method based on Fuzzy Pythagorean sets. Their goal was to find the most vital risks for real-life case studies. This process considered organizational, environmental/cultural, security, technical and financial risks prioritization. As a result,

security related risks are identified as the most important. In another study, Drljevic et al. [22] examined perspectives on risks and standards affecting blockchain technology requirements' engineering. This study's results indicate a gap in the normative frameworks that affect the sustainable adoption and use of blockchain technology.

Despite the importance of analyzing implementation risks of blockchain as a disruptive technology, only a few studies have focused on this issue. Therefore, the comprehensiveness risks assessment model is developed in this study to cover an extensive set of potential risks and ultimately analyze their causal relationships. Tables 1 and 2 summarize the conducted studies on identification and evaluation of blockchain implementation risks and comparison of current study with other studies.

Table 1. Classification of potential risks of blockchain (BC) implementation

Study	Type of risks								Analysis method	Case study	Results
	T	S	O	L	F	E	C	I			
KPMG [23]	*	*	*	*	*				Systematic Literature Review	Bank industry	Importance of risk assessment for increasing efficiency and effectiveness of BC implementation
Zetzsche et al [24]				*					Descriptive research method	Legal Risks of Blockchain	Importance of considering legal related risks for successful BC implementation
Staples et al [11]	*								Description and analysis	Smart contracts	Importance of no limitation for BC type selection in accordance to organization requirements
Lindman et al [25]	*			*					Review of previous literature	Research agenda	Indicating on importance of risks of organizational issues, competitive environment, and technology design issues
Caron [26]	*	*	*	*					Descriptive research method	Identifying risk on the road to distributed ledgers	Increased in BC risks because of immaturity of regulatory framework for BC technology
Kim and Kang [12]	*		*	*					Descriptive research method	Anti-corruption	a holistic and coordinated effort is required because of a black box nature of a BC
Tarr [27]	*	*		*					Review of previous literature	Insurance industry	Via BC and linked smart contracts, there is considerable potential for frictional delays and the risks of human error to be controlled.
Harris [14]	*	*		*	*				Fundamental research method	Blockchain technology in underdeveloped countries	BC technologies deal significant hurdles for implementation in underdeveloped countries
Santhana and Biswas [28]	*	*	*	*	*			*	Fundamental research method	Risk performance in China's strategy	To respond to BC risks, organizations should consider establishing a robust risk management strategy, governance, and controls framework.
White et al [5]	*	*	*	*					Descriptive research method	Blockchain security risk assessment and the auditor	Indicating on risks include technological risks, data security risks, interoperability risks, and third-party vendor risks.
Özkan et al[21]	*	*	*	*		*	*		MCDM (PF-AHP)	British telecommunication company	Security and its related risks have more critical during BC implementation.

Table 2. Classification of potential risks of blockchain implementation

Study	Type of risks							Analysis method	Case study	Results
	T	S	O	L	F	E	C	I			
Biswas and Gupta [20]	*	*	*	*	*				DEMATEL	Industry and Services	Top importance of scalability, transaction-level risks, market-based risks, and regulatory risks.
Sayeed and Marco-Gisbert [17]		*							Analytical descriptive	Mechanisms against the 51% attack	A security policy accepting a restricted number of blocks by totally disregarding the longest chain rule must be discovered to diminish the risks of 51% attack successfully.
Norta, et al [16]		*							Project management life cycle	General	Security requirements and -controls necessary process are proposed to mitigate the BC risks.
Lu, et al [4]	*	*		*					Systematic Literature Review	Oil and gas industry	Indicating on primarily technological, regulatory and system transformation risks.
Bürer, et al [15]	*	*				*			Fundamental research method	Energy industry of emerging business models and related risks	Indicating the importance of reliability/stability risks of power resources management.
Prewett, et al [18]	*	*	*	*	*		*		Systematic Literature Review	General	Indicating on reputational and business continuity risks.
Wang [29]					*				Fuzzy Neural Networks	Supply chain Financial Risk	Indicating on supply chain financial credit, financing enterprises, core enterprises, and the overall operation of supply chain finance risks.
Drljevic, et al [22]	*	*	*	*	*	*	*			General	Indicating on an identified gap in normative frameworks that affect the adoption and sustainable use of BC technology.
Öztürk and Yildizbaşi [9]	*	*	*	*		*		*	Systematic Literature Review	Supply chain management	Indicating on investment risk, data security and utility risks and coordination and integration risks.
Esmaeilnezhad Tanha et al. [33]	*		*	*	*	*		*	Fuzzy Delphi and FBWM	Cyber physical systems	Top importance of technical challenges for BC implementation
Zhang and Song [34]		*			*	*			BWM	Supply chain	Top priority of cooperation complexity and increased costs
Nguyen et al., [35]	*	*		*					Mixed-methods risk analysis	Maritime container shipping	Gap of encouraging legal and technological environments for BC implementation
Sadeghi et al., [36]	*	*			*			*	Fuzzy MCDM	Construction organizations	Critical blockchain risks facing construction organizations are communication and information, supply chain management, financial, and corporate social responsibility
Gorbunova et al., [37]	*								Systematic Literature Review	BC applicability in various sectors	A comparative analysis of the challenges that could become a baseline for potential future research activities in the BC and DLT fields
Current Study	*	*	*	*	*	*	*	*	Fuzzy Delphi and FCM	Blockchain-based ERP software development	Prioritizing all of the considered risk based on the holistic model

3. Research Method: Integrated Fuzzy Delphi and FCM

In this study, an integrated analysis technique incorporates the fuzzy Delphi technique, and the fuzzy cognitive map is applied. Uncertainty of risks assessment process is handled by fuzzy approach.

3.1. Fuzzy Delphi Technique: Risk Identification and Assessment

In this study, the Fuzzy two-phase Delphi method is used to identify and evaluate the potential risks based on the experts' opinions. For this purpose, verbal expressions are used to measure the extracted viewpoints. In the first phase, a semi-open questionnaire has been developed for potential risks identification and assessment based on the results of the conducted studies in the literature. The proposed risk name, definition, and classification are validated based on the experts' opinions. New risks and their related information could be proposed by experts. The fuzzy technique is applied to handle the uncertainty of risk assessment by representing verbal expressions with the triangular fuzzy number (TFN) (see Table 3) [30]. Based on the final results of the first phase, the second phase questionnaire is developed. In the second phase, the relative importance of concluded risks is evaluated by experts. Achievement of consensus (i.e., results from convergence status) is calculated at the end of the second phase. The Delphi evaluation process will be finalized if this consensus measure (i.e., the difference between the averages of two successive obtained defuzzy results of Delphi phases) is less than 0.1. The applied Delphi method is stopped at the second phase.

Table 3. Triangular fuzzy numbers for a five-point scale [31]

Verbal expressions		TFN
FCM	Fuzzy Delphi	
Strong positive	Strongly agree	(0.6,0.8,1)
Positive	Agree	(0.4,0.6,0.8)
Ineffective	Neutral	(0.2,0.4,0.6)
Negative	Disagree	(0,0.2,0.4)
Strong negative	Strongly disagree	(0,0,0.2)

3.2. Fuzzy Cognitive Map: Cause-and-Effect Analysis

In this study, the FCM method has been used as an analysis tool which uses a graph-based system to present the causal relationships of influencing risk factors in decision-making. The analysis graph of the FCM consists of two key elements: node and edge.

Nodes represent the main factors of the concepts that define a system of blockchain implementation risks analysis. Edges represent the potential causal relationships between the considered nodes. Fuzzy binary numerical descriptions are used to introduce causal effects into the cognitive map instead of positive or negative symbols. The edge of each fuzzy cognitive map between concepts (i.e., risks) of C_i and C_j is

related to a relative weight variable from -1 to 1. This variable indicates the strength of the related relationship. There are three different types of possible causes between each pair of risks, C_i and C_j [32]:

- $W_{ij} > 0$ which determines a positive cause. If the value of C_i increases, this will lead to an increase in C_j value.
- $W_{ij} < 0$ which determines negative causation. If the value of C_i increases, this will decrease C_j value.
- $W_{ij} = 0$ which indicates no causal relationship between considered concepts.

The FCM of considered concepts is represented mathematically by an adjacency weight matrix with $n \times n$ size. The three types of variables in the cognitive map are as follows: transmitter variables, receiver variables, and ordinary variables. These variables are calculated via their out-degree (*OUT*) and in-degree (*IN*). *OUT* and *IN* are the row and column sums of absolute values of a variable in the adjacency matrix that present the cumulative strengths of exiting relations variables, respectively (see equations 1-2). Transmitter, receiver, and ordinary variables have a positive *OUT* and zero *IN*, a positive *IN* and zero *OUT*, and both a non-zero *IN* and *OUT*, respectively. The centrality of a variable (*IMP*) is the summation of the related *IN* and *OUT* indexes (see equation 3).

$$IN = \sum_{i=1}^{n} W_{ik} \tag{1}$$

$$OUT = \sum_{k=1}^{n} W_{ik} \tag{2}$$

$$IMP = IN + OUT \tag{3}$$

It should be mentioned that a three-point Likert scale has been used to present the experts' opinions about the effect of each risk on others (see Table 2). Fuzzy triangular evaluation (FTE) is presented by equations (4). Rank of each risk is determined based on the related calculated FTE. The mean of fuzzy number (MFN) is calculated by equation (5) for conducted assessment. All final fuzzy evaluations are defuzzified by equation (6).

$$\text{Fuzzy evaluation } (FTE) = (m_l^i, m_m^i, m_u^i) \tag{4}$$

$$\text{Mean of fuzzy number } (MFN) = \frac{\sum_{i=1}^{n} (m_l^i, m_m^i, m_u^i)}{n} \tag{5}$$

$$W^{df} = \frac{m_l + 2m_m + m_u}{4} \tag{6}$$

4. Research Findings

In this section, based on the applied two-phase fuzzy Delphi and fuzzy cognitive mapping, the main results of identifying and evaluating blockchain implementation risks are presented for the blockchain-based ERP software as a case study.

Table4. Identified risks based on the literature review as an input of the applied Delphi method include risk type (TR) and name (R)

TR	Risk		TR	Risk	
Technical (T)	Architecture and design risk	T1	Security (S)	Data security risks	S1
	Oracle risk	T2		Cryptography, key management, and tokenization	S2
				Cyberattacks	S3
	Speed and accuracy of transactions	T3		Vulnerability	S4
				Transaction leakage	S5
	Consensus mechanism and network management	T4		Privacy	S6
				Criminal activity	S7
	Lack of technological maturity	T5		Double spending	S8
	Lack of customer awareness	T6		The complexity of the blockchain system compared to existing systems	S9
	Level of Access to technology	T7		Compatibility of different blockchain platforms	S10
	Sustainable infrastructure lackness	T8			
Financial (F)	Limiting the Access of Miners	F1	Social (I)	Information sharing obstacles	I1
	High investment cost	F2	Environmental (E)	Wasted resources	E1
	Usage cost	F3			
	Taxation	F4			
	Scalability and performance	F5			
	Technology Implementation and Acquisition	F6			
	Training cost	F7			
	Storage Limitations	F8			
	Lack of research and development Units	F9			
Organizational (O)	Resistance from the incumbents	O1		High energy Consumption	E2
	Vendor risk	O2	Cultural (C)	Smart contract risk	C1
	Distinctive opportunities	O3		Blockchain myths	C2
	Applicability to use blockchain as a solution	O4		Lack of implement transparent structure	C3
	Chain defense	O5		Participatory persuasion	C4
	Business continuity and disaster recovery	O6		Tracking transactions	C5
	Lack of skilled human resources	O7	Legal (L)	Compatibility risk	L1
				Issues with Contract Law	L2
	Lack of management support	O8		Regulation	L3
	Lack of equipment and tool	O9		Working within limitations of blockchain	L4
				Jurisdiction	L5
	Resistance to change technology	O10		Data management and segregation	L6
				Compliance risk	L7
	Strong hierarchical structure and bureaucracy	O11		Data control	L8
				User identity	L9
	Strict administrative control	O12		Decentralization	L10
				Regulatory Hurdles	L11
	Mind set of people needs to be changed	O13		Lack of control over malicious operations and information	L12
	Stable network connection	O14			

4.1. Case study profile: Blockchain-based ERP Systems

In this section, based on the applied two-phase fuzzy Delphi and fuzzy cognitive mapping, the main results of identifying and evaluating blockchain implementation risks are presented for the blockchain-based ERP software as a case study.

The market size of global ERP software was achieved at USD 50.57 billion in 2021 and is expected to keep growing in future years. The ERP system would provide a centralized and integrated system for enterprises. The capabilities of ERP systems could be boosted by integrating with blockchain technology. Once blockchain is integrated into the ERP system, it optimizes system operations, internal data control, and business processes such as intercompany transactions. A client-server technology is at the core of an enterprise's integrated management systems, which are now information-centric systems that use common standards for communication infrastructure, applications, databases, data exchange, and security [10]. The integration of ERP and blockchain systems improves the transparency and reliability of financial transactions in financial and accounting systems. In addition, potential contradictions in terms of invoices, shipments, returns and purchases are also reduced.

Integrating ERP with blockchain has twofold benefits: creating more transparency and reducing costs. Blockchain uses its capabilities to monitor business processes and facilitate their entry into the blockchain network. Finally, this study investigates the risks of implementing ERP systems based on blockchain in one of the biggest information technology and services companies in Iran. The company name could not be mentioned because of a confidential issue. Research experts are selected in the field of blockchain technology for developing ERP systems.

4.2. Results of Identifying and Evaluating Risks

The final summary of the identified risks of blockchain implementation based on the literature review is presented in Table 4. These findings are considered input data for the applied two-phase fuzzy Delphi method. The final results of the second phase of fuzzy Delphi are presented in Table 5.

According to the evaluation of identified risks of blockchain implementation, the value of 0.7 has been determined as the priority threshold based on the experts' viewpoints to prepare the FCM questionnaire for risk assessment. For this purpose, a set of 24 risks has been selected with priority values greater than the considered threshold. These risks have been analyzed and evaluated using the FCM approach to investigate the potential causal relationships. Then, influential risks are identified by analyzing each risk's impact on other risks. By preparing a questionnaire, experts were asked to examine the risks carefully and use verbal expressions via the Likert scale to determine the type and intensity of the impact of each risk on others.

Finally, week casual relations between risks are removed from the constructed cognitive map because of the realized low importance weight. For instance, two relations, including O8-L4 and L1-T5, are removed from the map. For developing a group-based FCM, a simple average of obtained fuzzy evaluation for each casual relation is calculated and defuzzified. The final calculated weights of risks are presented in Table 6.

Table 5. Ranking of the final identified risks by the Delphi method

Risk	Score value		Rank	Risk	Score value		Rank
	FTE	MFN			FTE	MFN	
T1	2.666	0.444	29	O5	3.000	0.500	12
T2	2.867	0.478	19	O6	2.600	0.433	31
T3	4.000	0.667	1	O7	2.400	0.400	43
T4	3.667	0.611	6	O8	3.200	0.533	7
T5	2.800	0.467	22	O9	2.600	0.433	35
T6	3.200	0.533	7	O10	2.600	0.433	31
T7	2.067	0.344	52	O11	2.267	0.378	47
T8	3.000	0.500	12	O12	2.067	0.344	52
S1	2.467	0.411	36	O13	2.067	0.344	50
S2	2.733	0.456	27	O14	2.867	0.478	20
S3	2.267	0.378	47	E1	2.467	0.411	36
S4	3.000	0.500	12	E2	3.000	0.500	12
S5	1.667	0.278	61	L1	3.800	0.633	3
S6	3.000	0.500	12	L2	3.800	0.633	4
S7	2.467	0.411	36	L3	4.000	0.667	1
S8	3.200	0.533	54	L4	2.800	0.467	22
S9	2.600	0.433	21	L5	3.200	0.533	7
S10	2.600	0.433	43	L6	2.400	0.400	43
F1	1.933	0.322	56	L7	1.867	0.311	58
F2	3.200	0.533	7	L8	1.933	0.322	56
F3	2.400	0.400	40	L9	2.733	0.456	27
F4	2.267	0.378	46	L10	1.800	0.300	60
F5	3.000	0.500	12	L11	2.600	0.433	30
F6	3.200	0.533	7	L12	2.200	0.367	49
F7	2.600	0.433	31	I1	2.467	0.411	36
F8	2.000	0.333	54	C1	1.867	0.311	58
F9	2.600	0.433	31	C2	2.800	0.467	22
O1	2.067	0.344	50	C3	3.800	0.633	4
O2	2.800	0.467	22	C4	3.000	0.500	12
O3	2.400	0.400	40	C5	2.400	0.400	40
O4	2.800	0.467	22				

In Table 7, weights of unrelated risks are zero and weights of related risks are non-zero, which are presented in blue-colored cells. Then, the graph-based structure of the proposed fuzzy cognitive map is analyzed using FCMAPPER software. The output of this mathematical analysis obtained based on the Graph theory is investigated. The final ranking of each risk is done based on the centrality index (see Table 7).

The in-degree and out-degree indicate whether the considered risk mainly influences other risks or if other risks influence it or both, respectively. The contribution of each risk in the FCM can be regarded by determining its centrality, which indicates how connected the risk is to other risks and what the cumulative strength of these connections is. The obtained results of the proposed FCM show that blockchain immaturity has the highest impact. The high investment cost risk has been influenced greatly by other risks. Privacy has the highest centrality index. Then, the graph of the proposed FCM for presenting casual relationships between considered risks is analyzed by PAJEKT software depicted by Gephi software (see Figure 2).

Table 6. Final FCM results (per hundred)

	T2	T3	T4	T5	T6	T8	S2	S6	S9	F2	F5	F6	O4	O5	O8	E2	L1	L2	L3	L4	L9	C2	C3	C4
T2	0	0	0	0	0	0	47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	40
T3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	57	0	0	0	0	0	0
T4	0	0	0	0	0	0	0	0	0	0	0	0	0	57	0	0	0	0	0	0	0	0	0	0
T5	0	0	0	0	53	0	0	0	0	59	0	0	0	0	60	0	0	0	0	0	0	0	67	0
T6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	60	0	0	0	60	0	0
T8	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0	60	0	0	0	0	0	0	0	0
S2	0	40	60	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0	0	0	0
S6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	47	60	0	0	0
S9	0	0	0	53	0	0	0	0	0	0	33	0	0	0	0	0	0	0	53	0	0	0	63	0
F2	0	0	0	0	0	0	0	0	0	0	0	70	0	0	0	0	0	0	0	0	0	0	0	0
F5	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0	0	0	57	0	0	0	0
F6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	27	0	60	0	0	0	0	0	0	0
O4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0
O5	0	0	0	0	0	0	0	37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O8	0	0	71	0	0	0	67	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	22
E2	0	0	0	0	0	0	0	0	0	73	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	70	37	0	0	0	0
L2	0	0	0	0	0	0	0	67	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0
L3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L4	57	37	0	0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0
L5	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C2	0	0	0	0	0	0	0	53	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C3	0	0	0	0	0	0	0	0	0	67	0	0	0	0	0	0	0	0	0	0	70	0	0	0
C4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	43	0	0	0	0	0	0

Table 7. FCM Measures Summary

	Risk	Out-degree	In-degree	Centrality
S6	Privacy	1.07	0.35	3.42
L2	Issues with Contract Law	1.17	2.23	3.40
F2	High investment cost	0.70	2.69	3.39
O8	Lack of management support	2.23	0.87	3.02
T5	Lack of technological maturity	2.39	0.53	2.92
L1	Compatibility risk	1.07	1.83	2.90
L4	Working within limitations of blockchain	1.43	1.40	2.83
S2	Cryptography, key management, and tokenization	1.63	1.13	2.76
C3	Lack of implement transparent structure	1.37	1.70	2.67
O5	Chain defense	0.37	0	2.07
S9	The complexity of the blockchain system compared to existing systems	2.03	1.30	2.03
L9	User identity	0.63	1.31	1.93
T4	Consensus mechanism and network management	0.57	1.10	1.88
E2	High energy Consumption	0.73	1.23	1.83
L3	Regulation	0.60	0.53	1.83
T6	Lack of customer awareness	1.20	0.70	1.73
F6	Technology Implementation and Acquisition	0.88	0.57	1.58
T2	Oracle Risk	0.87	0.77	1.44
T3	Speed and accuracy of Transactions	0.57	0	1.37
T8	Lack of sustainable energy infrastructure	1.30	0.60	1.30
C2	Blockchain myths	0.53	0.62	1.13
C4	Participatory persuasion	0.43	0.62	1.05
F5	Scalability and maintenance	0.72	0.33	1.05
O4	Applicability to use blockchain as a solution	0.63	0.01	0.64

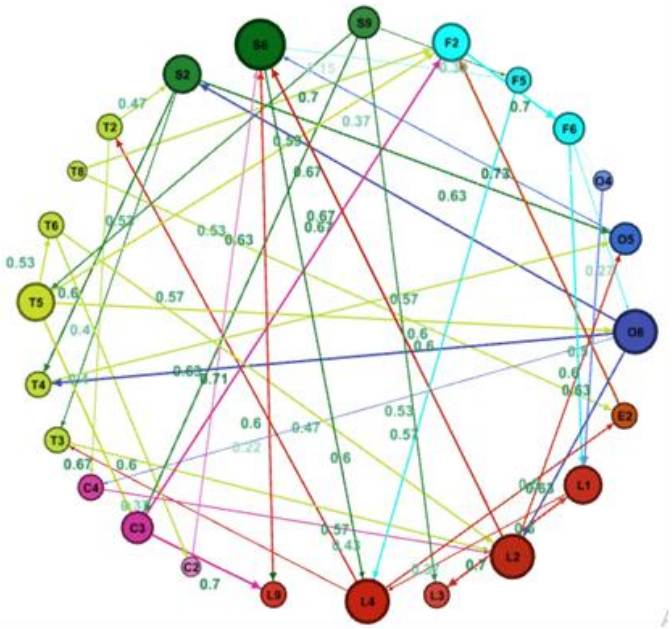

Figure 2. Proposed FCM for risks assessment of blockchain implementation

In figure 2, each weight of two risks (i.e., nodes) relation value is presented above the related arrow. The set of risks with high impacts are selected as the most important risks of blockchain implementation (see Table 8).

Figure 3. Cluster of lack of technological maturity risk (T5)

Analysis of the out-degree index shows that technological immaturity has the most impact on other risks. Therefore, figure 3, the network cluster includes the risks related to the technology immaturity risk that should be analyzed. The results indicate that to reduce the risk of lack of technological maturity is necessary to enhance the lack of management support (O8). Also, other factors that increase high investment cost (F2),

such as high energy consumption of electricity and other similar things, should be minimized. The lack of implementation of a transparent structure (C3) due to the newness and anonymity of blockchain technology for users is another risk that is affected by the immaturity of blockchain technology. Improving the users' knowledge of blockchain technology at the various organizational levels could be an efficient strategy for dealing with the mentioned risk.

Table 8. Final ranking of blockchain implementation risks

	Risk	Rank		Risk	Rank
F2	High investment cost	1	F6	Technology Implementation and Acquisition	13
S6	Privacy	2	T3	Speed and accuracy of Transactions	14
L2	Issues with Contract Law	3	T2	Oracle Risk	15
O5	Chain defense	4	C4	Participatory persuasion	16
L1	Compatibility risk	5	C2	Blockchain myths	17
L4	Working within limitations of blockchain	6	T6	Lack of customer awareness	18
L9	User identity	7	T5	Lack of technological maturity	19
T4	Consensus mechanism and network management	8	F5	Scalability and maintenance	20
L3	Regulation	9	O4	Applicability to use blockchain as a solution	21
C3	Lack of implement transparent structure	10	O8	Lack of management support	22
S2	Cryptography, key management and tokenization	11	T8	Lack of sustainable energy infrastructure	23
E2	High energy Consumption	12	S9	The complexity of the blockchain system compared to existing systems	24

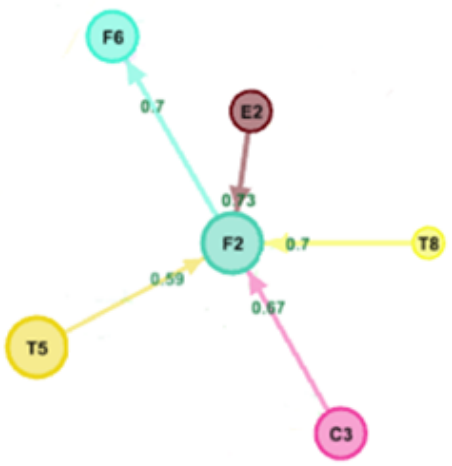

Figure 4. Cluster of high investment cost (*F2*)

Figure 4 shows high investment costs as the most influential risk of blockchain implementation, from other risks. The related cluster includes critical risks such as high energy consumption, lack of sustainable energy infrastructure, and lack of implement transparent structure. Providing more efficient and reliable energy resources could decrease the operational cost of using blockchain technology and diminish an organization's vulnerability to this technology implementation.

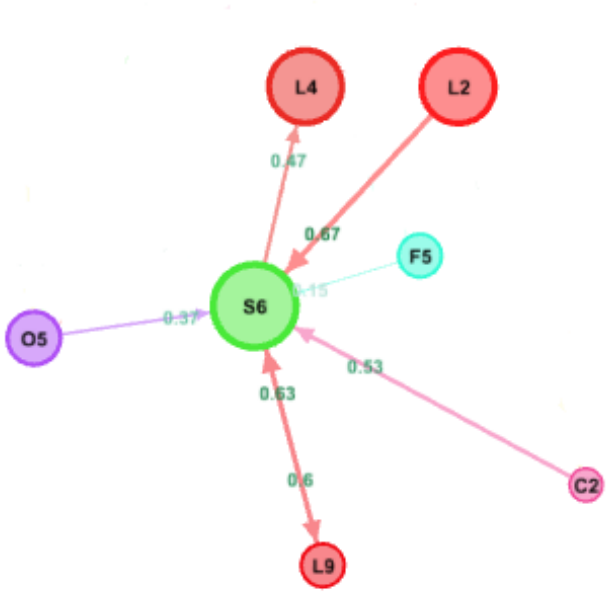

Figure 5. Cluster of privacy risk (*S6*)

Figure 5 presents the critical role of risks related to law issues such as contract law issues, working within blockchain limitations, and user identity. In addition, chain defence methods of mining pool attacks for blockchain security issues, network communication and smart contracts for blockchain security issues, and privacy thefts for blockchain privacy issues are so important in analyzing the privacy risk. Blockchain would be defined in three general types: public, private, and consortium. The private blockchain has a lot of supervision, which is only under certain individuals' control. Accordingly, a private blockchain would be used as much as possible to deal with the risk of privacy.

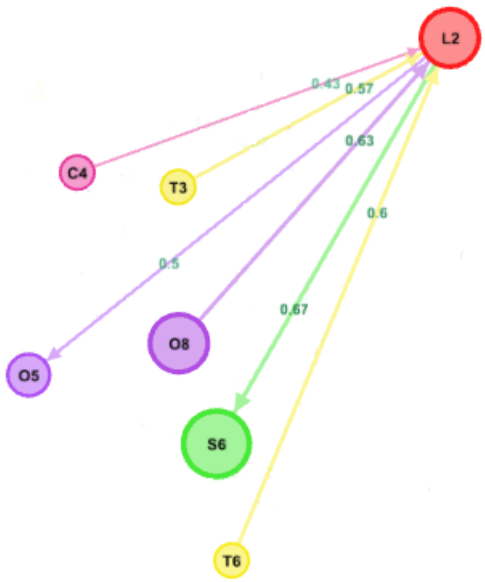

Figure 6. Cluster of risk of contract law (*L2*)

Figure 6 presents the cluster of contract law as a second important risk in term of the centrality index. Obtained results indicate that technological issues such as transaction speed and accuracy as well as customer awareness have the most impact on this critical risk. In addition, organizational and security aspects of an enterprise, such as chain defense and privacy, are affected by the risk of contract law.

5. Conclusion

Blockchain has a great potential for changing attitudes toward traditional businesses to be more cost-effective and reliable. Blockchain is an innovative technology which has been accepted widely by various industries. This emerging technology has several advantages, such as eliminating intermediaries, transparency, and traceability. Nowadays, businesses are exploring how to use this emerging technology to efficiently influence their enterprise and avoid the implementation of potential risks. Therefore, identifying and assessing the extensive implementation risks are very important and have a critical impact on organization performance. Risk management could be a more challenging task by increasing the number of risks and potential causal relationships between them. For this purpose, the fuzzy cognitive mapping technique has been used in this study to analyze the complex system of blockchain risk implementation as a disruptive technology. In this study, the evaluation and analysis of blockchain implementation risk are handled via the fuzzy cognitive mapping technique. For this purpose, after a comprehensive literature review, the potential risks of blockchain implementation have been identified and examined in eight general categories: technical, security, organizational, legal, financial, environmental, cultural, and social.

Finally, various risks have been identified and investigated based on the experts' opinions using the two-phase fuzzy Delphi method for determining the most important risks. Then, constructed map of risks are analyzed via FCM in terms of influencing other risks, affected by other risks, and impotence in the risks network.

Obtained results indicate that financial risk, including high investment cost is the most important implementation risk of blockchain as a revolutionary technology. This critical cost-based risk has been mentioned in other studies because of high energy dependence, the difficult process of integration, and the implementations high costs [34], [36]. By developing new generation of blockchain technology, these technologies based challenges would be more improved in term of operational cost of using blockchain. Law related risks have a significant role among the top ten assessed risks. This importance could be seen by analyzing the central index for critical risks such as privacy. In addition, issues with contract law have various critical impacts on the organizational and privacy risks and are impacted by technology risks. Regarding the environmental context, specific laws and regulatory support were considered as the most important factors [33], [35]. These key soft aspects should also be more developed in proper harmony with the common technological aspects of the blockchain technology, which have been of most noted until now. Although the immaturity of blockchain has a critical impact on other considered risks in term of the out-degree index, it is expected this influencing role decreases over time as a consequence of the further evolution of blockchain technology. The risk of the high investment cost of blockchain usage is affected by the novel as well as sustainable energy-providing approach. Required supportive infrastructures, including both technical and non-technical elements simultaneously, may stimulate the development, diffusion, commercialization, and penetration coefficient of new blockchain-based applications which could be integrated with others disruptive information technologies such as IoT, cloud-computing, and other cyber-physical systems [33].

Therefore, this threat with a high impact on other risks in term of out-degree index could be transformed into an opportunity by using more cost-efficient energy resources and outweighing obtained benefits by blockchain. Therefore, the assessed network of risks that have high dynamics should be analyzed by considering the effects of time on related issues and potential feedbacks over time. For this purpose, the systems dynamics analysis approach can be used for future researches.

References

1. Farshidi S, Jansen S, de Jong R, Brinkkemper S. A decision support system for software technology selection. Journal of Decision systems. 2018. 27(sup1): p. 98-110.
2. Efanov, D. and P. Roschin, The all-pervasiveness of the blockchain technology. Procedia computer science, 2018. 123: p. 116-121.
3. Böhme R, Christin N, Edelman B, Moore T. Bitcoin: Economics, technology, and governance. Journal of economic Perspectives. 2015. 29(2): p. 213-38.
4. Lu H, Huang K, Azimi M, Guo L. Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. Ieee Access. 2019. 27(7): p. 41426-44.
5. White, B.S., C.G. King, and J. Holladay, Blockchain security risk assessment and the auditor. Journal of Corporate Accounting & Finance, 2020. 31(2): p. 47-53.
6. Swan, M., Blockchain: Blueprint for a new economy. 2015: " O'Reilly Media, Inc.".

7. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. in International workshop on open problems in network security. 2015. Springer.
8. Britchenko, I., T. Cherniavska, and B. Cherniavskyi, Blockchain technology into the logistics supply. 2018.
9. Öztürk, C. and A. Yildizbaşi, Barriers to implementation of blockchain into supply chain management using an integrated multi-criteria decision-making method: a numerical example. Soft Computing, 2020. 24(19): p. 14771-14789.
10. Hrischev, R. ERP systems and data security. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
11. Staples M, Chen S, Falamaki S, Ponomarev A, Rimba P, Tran AB, Weber I, Xu X, Zhu J. Risks and opportunities for systems using blockchain and smart contracts. Data61. CSIRO), Sydney. 2017.
12. Kim, K. and T. Kang. Does technology against corruption always lead to benefit? The potential risks and challenges of the blockchain technology. in Paper submitted to OECD's Anti-Corruption and Integrity Forum. https://www. oecd. org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology. pdf. 2017.
13. Zamani, E., Y. He, and M. Phillips, On the security risks of the blockchain. Journal of Computer Information Systems, 2020. 60(6): p. 495-506.
14. Harris, C.G. The risks and dangers of relying on blockchain technology in underdeveloped countries. in NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. 2018. IEEE.
15. B Bürer MJ, de Lapparent M, Pallotta V, Capezzali M, Carpita M. Use cases for blockchain in the energy industry opportunities of emerging business models and related risks. Computers & Industrial Engineering. 2019. 137:106002.
16. Norta, A., R. Matulevičius, and B. Leiding, Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns. Computers & Security, 2019. 86: p. 253-269.
17. Sayeed, S. and H. Marco-Gisbert, Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 2019. 9(9): p. 1788.
18. Prewett, K.W., G.L. Prescott, and K. Phillips, Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate accounting & finance, 2020. 31(2): p. 21-28.
19. Feng S, Wang W, Xiong Z, Niyato D, Wang P, Wang SS. On cyber risk management of blockchain networks: A game theoretic approach. IEEE Transactions on Services Computing. 2018. 14(5): p. 1492-504.
20. Biswas, B. and R. Gupta, Analysis of barriers to implement blockchain in industry and service sectors. Computers & Industrial Engineering, 2019. 136: p. 225-241.
21. Özkan B, Kaya İ, Erdoğan M, Karaşan A. Evaluating blockchain risks by using a MCDM methodology based on Pythagorean fuzzy sets. InInternational conference on intelligent and fuzzy systems 2019. 23: p. 935-943. Springer, Cham.
22. Drljevic, N., D.A. Aranda, and V. Stantchev, Perspectives on risks and standards that affect the requirements engineering of blockchain technology. Computer Standards & Interfaces, 2020. 69: p. 103409.
23. KPMG, Realizing blockchain's potential, in Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/ realizing-blockchains-potential.pdf. 2018.
24. Zetzsche, D.A., R.P. Buckley, and D.W. Arner, The distributed liability of distributed ledgers: Legal risks of blockchain. U. Ill. L. Rev., 2018: p. 1361.
25. Lindman, J., V.K. Tuunainen, and M. Rossi, Opportunities and risks of Blockchain Technologies–a research agenda. 2017.
26. Caron, F., Blockchain: Identifying risk on the road to distributed ledgers. ISACA Journal, 2017. 5: p. 1-6.
27. Tarr, J.-A., Distributed ledger technology, blockchain and insurance: Opportunities, risks and challenges. Insurance Law Journal, 2018. 29(3): p. 254-268.

28. Santhana, P. and A. Biswas, Blockchain risk management–risk functions need to play an active role in shaping blockchain strategy. Accessed: Dec, 2017. 7: p. 2019.
29. Wang Y. Research on supply chain financial risk assessment based on blockchain and fuzzy neural networks. Wireless Communications and Mobile Computing. 2021 Feb 17;2021.
30. Ishikawa, A., et al., The max-min Delphi method and fuzzy Delphi method via fuzzy integration. Fuzzy sets and systems, 1993. 55(3): p. 241-253.
31. Habibi, A., F.F. Jahantigh, and A. Sarafrazi, Fuzzy Delphi technique for forecasting and screening items. Asian Journal of Research in Business Economics and Management, 2015. 5(2): p. 130-143.
32. Papageorgiou E, Papageorgiou K, Dikopoulou Z, Mouhrir A. A web-based tool for Fuzzy Cognitive Map Modeling, 2018. Fort Collins, USA.
33. Esmaeilnezhad Tanha, F., Hasani, A., Hakak, S., Reddy Gadekallu, T. Blockchain-based cyber physical systems: Comprehensive model for challenge assessment, Computers and Electrical Engineering, 2022. 103, 2022, 108347.
34. Zhang, F., Song, W., Sustainability risk assessment of blockchain adoption in sustainable supply chain: An integrated method, Computers & Industrial Engineering, 2022. 171, 108378.
35. Nguyen, S., Shu-Ling Chen, P., Du, Y. Risk assessment of maritime container shipping blockchain-integrated systems: An analysis of multi-event scenarios, Transportation Research Part E: Logistics and Transportation Review, 2022. 163, 102764.
36. Sadeghi, M., Mahmoudi, A. and Deng, X. Blockchain technology in construction organizations: risk assessment using trapezoidal fuzzy ordinal priority approach, Engineering, Construction and Architectural Management, 2022. https://doi.org/10.1108/ECAM-01-2022-0014
37. Gorbunova, M., Masek, P., Komarov, M., Ometov, A. Distributed Ledger Technology: State-of-the-Art and Current Challenges. Computer Science and Information Systems, 2022. 19 (1), 65-85.

Samayeh Samsami is a graduate student in the master of business administration from the Shahrood University of Technology. Her current research interests include Risk Management and Applications of CPS in logistics.

Aliakbar Hasani is an associate professor at the department of industrial engineering and management, Shahrood University of Technology. His current research interests include Risk Management and System Analysis.

Saqib Hakak is an assistant professor at the Canadian Institute for Cybersecurity, faculty of computer science, University of New Brunswick. His current research interests include Risk Management and Blockchain Technology.

Fatemeh Esmaeilnezhad Tanha is a graduate student in the master of business administration from the Shahrood University of Technology. Her current research interests include Risk Management and applications of CPS in logistics.

Muhammad Khurran Khan is a global thought leader and influencer in cybersecurity. He is a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University.

Received: March 08, 2022; Accepted: January 25, 2023.