Computer Standards & Interfaces 69 (2020) 103409

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Perspectives on risks and standards that affect the requirements engineering of blockchain technology

Nusi Drljevic (Nusret)[a,*], Daniel Arias Aranda[a], Vladimir Stantchev[b]

[a] Department of Business and Economics, University of Granada, Spain
[b] Institute of Information Systems, SRH University Berlin, Germany

ARTICLE INFO

Keywords:
Blockchain
Sustainable blockchain
Technology adoption
Risk management
Perceived risks
Blockchain measurement framework
Business transformation

ABSTRACT

Blockchain aims to transform businesses and other forms of transactions from a centralized, human-based to a shared, algorithm-based trust model, which enables a new risk management paradigm. Misaligned incentives in different principal – agent scenarios are important risk factors from governance point of view. With blockchain, these misalignments are accounted for algorithmically, therefore novel governance models are possible. What role do risks play in terms of deciding for, or against the adoption of blockchain? How to best define requirements to achieve it? This paper explores standards and risk as factors, which can support or hinder the sustained application of blockchain in a broad scope of environments. We conducted a systematic literature review that outlines a current understanding of perceived risk surrounding the adoption and use of blockchain technology in the context of requirements engineering. Furthermore, selected models for managing risks are presented. Finally, areas where deeper research is required are identified. We conclude that a gap exists in normative frameworks that affect the adoption and sustainable use of blockchain technology. Closing this gap can support the sustainable use of blockchain technology.

1. Introduction

Blockchain is a shared, distributed and synchronized ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible, such as a house, car, money, land, or intangible, such as intellectual property, energy, patents or copyright. Virtually anything of value can be tracked and traded on a blockchain network [12]. A ledger is comprised of unchangeable, digitally recorded data in blocks. These blocks are stored in a chain and are spread across multiple servers in a public or private peer-to-peer network to eliminate manipulation. The synchronization of the ledger database, the agreement of content and transactions within the ledger, requires a validating consensus protocol between all parties [3]. The protocol effectively manages the risks associated with entries on the ledger, e.g., double spending. Blockchains can be either private, or permissioned, which allows only selected parties to submit and validate transactions, or public and unpermissioned, which enables anybody to submit a transaction and participate in validating the network. Hybrid versions exist as well. These alternatives present different challenges with respect to risk management.

There appears to be high expectations and potential promise for blockchain technology's contribution to sustainable socio-economic advances, due to the technology's functions for increasing the transparency and traceability of goods, services and any other assets, facilitating market access and improving the efficiency of transactions. However, major risks arise in various research literature and specialized media publications as to whether the technology is far enough in its development to be adopted and applied.

A clear understanding of related requirements standards and perceived risks surrounding blockchain could provide insights into the transformative nature of this technology in its relatively early stages of maturity. Blockchain adoption requires businesses to transform, not only in terms of becoming decentralized and transparent, but also employing requirements engineering and risk management across all stages of the innovation life-cycle, i.e. throughout end-to-end transformation process [8,16,23]. Furthermore, without considering potential risks and challenges, the price to pay due to reverse effects might surpass the potential socio-economic benefit expected from blockchain [19].

Specific risks in blockchain adoption include: missing return-on-invest (ROI) and missing business value [33], unsustainable usage scenarios [22,27], as well as insufficient understanding of the technology potential that is directly attributable to missing standards and requirements engineering practices in the subject matter [34,36].

[*] Corresponding author.
E-mail addresses: nusi@correo.ugr.es (N. Drljevic), darias@go.ugr.es (D.A. Aranda), vladimir.stantchev@srh.de (V. Stantchev).

https://doi.org/10.1016/j.csi.2019.103409
Received 28 November 2019; Received in revised form 25 December 2019; Accepted 27 December 2019
Available online 28 December 2019

There is a general consensus in society and industry that both a focused discussion and a standardization framework for risk and requirements management in the relatively young blockchain business context has yet to emerge [22,23,27], and we seek to highlight, advance and contribute to the discourse in this domain. This assumption could be rooted in hypotheses such as: (1) Business leaders and decision makers are eager to apply a standard-based requirements management framework to invest in and enhance the sustainable adoption of blockchain technology in context of business transformation. (2) Market players and users depend upon standard-based approaches in order to sufficiently manage blockchain risks and requirements along the entire adoption process. An example for such standard is the ISO/IEC/IEEE 29148 standard.[1] Developed and supported by the leading international standardization organizations, the standard uses a lifecycle based approach to outline processes and products related to the engineering of requirements.

This systematic literature review identifies a selection of existent frameworks and models for managing blockchain-related risks. While primarily focused on scientific, peer-reviewed journals, reports from leading global consultancy firms such as Deloitte, KPMG and global policy making bodies such as OECD (Organisation for Economic Cooperation and Development) or UNECE (United Nations Economic Commission for Europe) were also screened.

The rest of this work is structured as follows: in Section 2 we outline our materials and methods and formulate four research questions. In Section 3 we present our results and how they answer the four research questions. In Section 4 we discuss our results in the context of blockchain, risk management and sustainability. Then, in Section 5 we provide a conclusion and an outlook on future research directions.

2. Materials and methods

Following from the hypotheses and the research questions, sources on risks related to blockchain requirements and standards were sought out, specifically looking at blockchain's potential for reimagining business processes. Governance, performance, scalability and other key standardization and requirements areas were identified and explored. Two specific areas were excluded on purpose from the systematic literature review:

- Sources focused on blockchain as a method for use in risk management – our work focuses on risk management for blockchain adoption, not blockchain adoption for risk management.
- Sources focused on blockchain applications in the context of trading Bitcoin or other cryptocurrencies – this is a growing research area with very interesting developments, but it is out of the scope of this work.

2.1. Main research questions

Based on the two hypotheses from Section one we operationalized our research problem to the following research questions:

RQ1. How is risk defined within business and technology contexts, and why is it relevant?
RQ2. What are the perceived risks across various industries and use-case categories that affect the adoption and sustained use of blockchain technology?
RQ3. What methods and standards are in current use for assessing and managing these risks?
RQ4. What are the current research gaps in the area of risk management within the adoption and standards-based application of blockchain technology?

RQ1 is related to the definition of risk that is needed for examining both hypotheses. RQ2 examines the relationship between risks and adoption of blockchain technology. RQ3 is intended to provide answers to the main pillar of both hypotheses, the importance of standards-based approaches, by uncovering what approaches are currently in use. Finally, RQ4 aims to identify specific gaps in the state-of-the-art research that directly impact both hypotheses.

2.2. Methods and approach

In approaching these research questions, we took a quantitative secondary research method to data and information retrieval following the method of a systematic literature review (SLR). We drew from sources within this research field from the databases and citation indexes Web of Science, Elsevier's Science Direct, SSSR, Research Gate and Academia.edu and employed methods such as keywording across titles and abstracts. Due to the vibrant development of the topic in the industry and the fast-moving landscape of blockchain adoption, we focused on sources from the last five years and included also relevant industry sources (soc. grey literature). The search string that we used to identify relevant sources was (``blockchain`` OR ``distributed ledger`` OR ``smart contracts``) AND ``risk management``. The research was aimed at identifying existing standards and models for managing blockchain-related risks and requirements, as well as answering the research questions. While the available scientific research in this field has increased along with the continued application of blockchain across various industries, the number of sources specifically focused on risk management for adoption, requirements engineering and standards-based use of blockchain technology remains comparably low.

3. Results

Following the method proposed in Section 2, we conducted our review primarily in the summer of 2019 and did a validation at the end of the same year. The initial search conducted on Elsevier's Science Direct database yielded 623 results for “risk management blockchain” with an increase in publication volume from 13 articles in 2015 to 219 articles in 2019. A subsequent review of all these results showed that only a selection of these academic publications directly treats the risks involved with adopting and implementing blockchain. The majority addresses the value of the technology as a method of risk management in various use-case categories [33,35,36]. We identified from these over 600 results 34 primary sources that were directly relevant for answering our RQs and relied on the frequency of viewings, citations, and sharings as a means of assessing their importance.

Our systematic literature review was successful in providing answers to the four research questions (RQ) that we formulated in Section 2. Below, we present these results for each research question.

3.1. RQ1. How is risk defined within business and technology contexts, and why is it relevant?

The term risk is used and defined in a variety of ways, depending on the context and use case. Most definitions support the common understanding, that risk refers to uncertainty and undesirable outcomes. We considered the definitions of risk and risk management from four different viewpoints. Table 1 presents the perspectives of general definition, technology, business and project management.

A consideration of risk is relevant from these multiple perspectives, as all four approaches highlight the need for risk management as a key management practice during any value creation process. It is important to reflect on the contexts of our findings in Table 1. The general perspective is one very prevalent in the investment world. The business perspective is oriented towards negative externalities and how to mitigate their impact. Risk management is applied across various industries and specific use cases and applications. The Information

[1] See https://standards.ieee.org/standard/29148-2018.html

Table 1
Risk definition.

Perspectives	Definition
General	A situation involving exposure to danger. The possibility that something unpleasant or unwelcome will happen [16].
Business	A probability of threat of damage, injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action [16,29].
Technology (ITIL)	A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred. Risk can also be defined as uncertainty of outcome and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes [17].
Project management	Dual perspective: Overall risk is defined as the effect of uncertainty on the project as a whole. Individual risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objective [14].

Technology Infrastructure Library (ITIL) focuses on providing a structured approach for IT service management and defines risk management in this context as the process, which is responsible for identifying, assessing and controlling risks [17]. Furthermore, in the perspective of project management, the context is put on the impacts of uncertainty on the project's success.

Risk management can be understood as two phases within an overall process, the first being the identification and assessment of risks. This includes the analysis of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risks can be assessed both quantitatively and/or qualitatively. The second phase is the on-going management of these risks, as well as the measures for their mitigation [14].

Exposure to business risk is a factor that could lower revenue, profit or even lead to failure for any company. Anything that threatens a company's ability to meet its objectives is understood as a business risk. These risks can be of various nature and derive from different areas.

General business risks include low customer satisfaction, market acceptance, slower time-to-market, lack of intelligence and data analytics, unmet product or service fit, cashflow, brand fatigue, data security, exchange rates, lack of expertise, dynamic market changes, poor leadership, regulatory compliance, technology downtime [31].

In the context of blockchain adoption and sustainable use, it seems that a certain degree of perceived risk can be a key decision-making factor and that this level of perceived risk could vary between industries and use cases.

We take the example of Kim and Kang [21] to highlight the importance of risk consideration throughout the end-to-end transformation process with blockchain applications. With their report on blockchain's role as a technology to combat corruption, the authors cite mainstream institutions (i.a. UN, Word Wide Web Consortium, RAND Corporation, the International Monetary Fund - IMF) that presently explore blockchain technology as a tool to empower global communities. The authors conclude, however, that blockchain is a double-edged sword: without considering risks at all stages in a structured way, the technology could have a negative ripple effect and actually hinder sustainable growth.

Looking at the current blockchain market, there is evidence that 92% of blockchain projects over the past few years have failed due to a lack of identifying and managing a broad set of risks, deficient requirements engineering and subpar standardization [18]. This stands in contradiction to the vision and ambition of broad adoption and use.

To illustrate, we take the recent collaboration between blockchain technology provider IBM and shipping and logistics giant Maersk as an example [13]. Officially launched in August 2018, the joint venture is a platform called TradeLens, which aims to simplify the cost, complexity and size of global shipping networks, while offering more transparency and efficiency. The solution uses distributed ledger technology to establish a shared, immutable record of all the transactions that take place in the network, so that various permissioned trading parties can gain access to that data in real-time [13].

IBM has admitted that its blockchain-based trade platform is struggling to gain traction with other carriers. This is a direct result of missing standards and governance problems, and it signifies risk inherent to building networks amongst competitors [13].

3.2. RQ2. What are the perceived risks across various industries and use cases that affect the adoption and sustained use of blockchain technology?

The 2019 World Economic Forum report on building value with blockchain technology highlights the need for a new analytic framework for assessing and managing blockchain technology-related risks. Blockchain's unique properties place increased control into the hands of individuals, rather than large-scale entities such as corporations, governments and research institutions [34]. This shift toward open, democratized means of conducting transactions is at the core of blockchain business transformation in this area. Understanding how decision makers perceive the risks involved with transitioning to blockchain is central to the risk management process.

It appears that some risks and challenges to sustainable blockchain use are perceived as standard across all industries and use cases, whereas others are based on specific applications of blockchain technology. Nevertheless, no normative taxonomy of blockchain risks could be located within the scope of this research. Among the sources reviewed, issues of scalability [25,26], performance [25,26], governance [32], security and change management (including requirements management) [34,35] are important areas of risk, which can be seen as prevalent and overarching. A broad range of risks relevant to more specific blockchain applications are identified throughout the sources reviewed as presented in Table 2. The content of this table was derived from the set of sources that we already specified at the beginning of this section. Most journal reports in this review attempt to identify and treat individual risk considerations, rather than to present integrated solutions.

For example, Zheng et al. [36] present a survey of blockchain challenges and opportunities. Herein, they summarize scalability, privacy leakage and selfish mining as three typical, standard challenges particular to blockchain. These are then broken-down – e.g. scalability into issues such as performance and latency – in order to take individual approaches to mitigating and managing the risks these challenges present.

The aforementioned Kim and Kang [21] focus on the following risks and challenges of the technology: data governance and privacy, technology-related issues and resistance by the incumbent market players.

Multiple sources identify the realm of governance, or regulatory frameworks as an area of weakness and, thus, a key risk category [2,7,10,11,19–22,32]. The following table provides an overview of key risks identified in the literature. This list provides an overview of the range of risks among reviewed publications.

In most cases, it appears that risks are treated on a case-by-case basis, missing standards-based approaches to requirements management. With the example of governance, no standardized framework that is unique to blockchain seems to be available. Gikay [10] argues, however, that while blockchain is a new technology, the legal transactions it enables are not entirely novel and could largely be managed under the existent regulations. His report works with the assumption

Table 2
Risk parameters taken from the literature, in alphabetical order.

Identified risk	Reference
Access and user rights	KPMG [23]
Architecture design	Caron [7]
Authorizing and provisioning management	KPMG [23]
Business continuity	Deloitte [30]
Change management	KPMG [23]
Compliance	Caron [7]
Consensus protocol	Deloitte [30]
Costs	OECD [27]
Customer experience	Panchev [28]
Data confidentiality	Deloitte [30]
Energy consumption	OECD [27]
Enforcement of contract	Deloitte [30]
Governance	Deloitte [30], Beck et al. [2]
Integration	Caron [7]
Interoperability	KPMG [23]
Key management	Deloitte [30]
Legal liability	Deloitte [30], Kim and Lee [21], OECD [27]
Liquidity	Deloitte [30]
Performance	KPMG [23]
Privacy	KPMG [23]
Regulatory	Deloitte [30]
Reputation	Deloitte [30]
Scalability	KPMG [23]
Security	Deloitte [30], KPMG [23]
Strategy	Deloitte [30]
Supplier	Deloitte [30]
User experience	Panchev [28]

that identifying and utilizing existing legal frameworks could be a method of risk management in this area.

The scope and speed of blockchain adoption speaks for change and requirements management being a standard area of perceived risk. It has been said that 80% of the blockchain technology is related to the change in business processes and 20% to implementation of the technology [23]. Even for those who refrain from blockchain adoption, a degree of change and requirements management will be required for continuing cooperation with partners who adopt and implement blockchain into their business models. Manski [25] explores blockchain as a possible means of “technological commonwealth” and refers to sectors of the global economy that are predicted to be impacted more quickly than others by the introduction of blockchain technology. These are particularly those industries that benefit from less centralized and more accelerated interconnectivity between different systems, for example healthcare, identity management, media, public services, finance and supply chain management. For these industries, the risk considerations surrounding change management – including the risks involved with *not* adopting blockchain – should be of primary concern.

Business and technology consultancy firm KPMG outlines eight key areas of risk consideration: access and user management, authorizing and provisioning management, data management, interoperability, scalability and performance, change management, privacy, and security [23].

In their 2018 treatment, the OECD identifies an extensive list of possible risks and obstacles as these relate to individual sectors. For example, they identify risks related to supply chain, such as fragmentation, difficulty controlling data quality, upfront costs and lack of access. Additionally, they state risks to healthcare, such as privacy rules and data security. Finally, the report addresses risks to energy, such as scalability, technical performance and energy consumption [22].

In addition to scientific journals and reports from global consultancies and policy makers, there is a wealth of references to blockchain across specialized media publications. Valuable insights into perceived risks and risk management can also be culled from these sources. For instance, a discussion of hurdles to blockchain's becoming mainstream defines performance, scalability, as well as the lack of user experience (UX) or customer experience (CX) as risk considerations [28]. Other identified risks include security, compliance, architecture & design and system integration [7]. “Lack of originality” – or the question of blockchain's value in comparison with other database technologies - is often cited as a risk, along with lack of transparency, lack of evaluation methodology and consensus inefficiencies, with respect to energy consumption [8]. Overarching, standard risk considerations such as governance and system design are also frequently mentioned among specialized media sources [1].

It can be assumed that many of these areas of perceived risks result from missing standards and unclear requirements surrounding blockchain technology as a relatively novel and complex innovation. At this early stage of development, higher levels of uncertainty could influence higher levels of perceived risk [7, 19]. The aforementioned hypotheses were formed based on this assumption. In order to counter uncertainty, it can be expected that business leaders, decision makers and users would be eager to apply a normative risk management framework – complete with integrated guidelines – to enhance the sustainable adoption of blockchain technology in the context of business transformation.

3.3. RQ3. What methods are in current use for assessing and managing these risks?

It appears that researchers and organizations hold the common belief that, in order to respond to blockchain risks, stakeholders should consider establishing a robust risk management strategy, along with a framework for governance and controlling. It seems that various examples are arising, albeit fragmentary and not normative. Kim and Lee [21] present a guideline for investors to aid in preventing potential threats. The authors also suggest using international standards such as from National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) to develop risk management policies based upon individual needs.

Table 3 provides an overview of additional models and approaches for managing risks as a basis of sustainable blockchain usage.

CohnReznick [4], for instance, focus on six self-defined “high-level risks related to adoption of blockchain technology”: scalability, technology implementation and acquisition, data security and confidentiality, regulatory hurdles, jurisdiction, storage limitations. Different considerations within each of these six categories are then paired with a blockchain focus level (platform, nodes, development, user,

Table 3
Models and approaches for management of blockchain-related risk.

Publisher/Author	Type of Model	Key Functions	Benefits
CohnReznick [4] 2018	Singular risk-based strategy	Risk mitigation	Identification of risk considerations and respective control areas across six levels of blockchain
Deloitte [30] 2018	Framework for blockchain risk management	Risk management	Framework for embedding three perceived risk categories - standard, value transfer, smart contract – within business objectives and operations
KPMG [23] 2018	Blockchain Maturity Model	Eight risk identification areas and maturity scoring	Identification of maturity levels and spotting of opportunities for improvement when implementing and using blockchain technology
OECD [22] 2018	Blockchain Primer	Risk identification	Pairing of risk across three policy areas

security incidents, asset management), and assigned certain control areas, which can be understood as individual methods for managing risks.

Leading global technology consultancy firms such as Deloitte and KPMG deal with blockchain risks systematically and strive to define methods for managing their defined risks as an enhancement to their profile of consulting services. In each of these cases, individual hierarchies of risks were presented. Deloitte [30] provides a risk management framework, which embeds three categories of risk considerations - "standard", "value transfer" and "smart contract" – within wider business objectives and processes, then assigns operating models for dealing with these categories, respectively. KPMG [22] identifies eight specific blockchain risk areas and apply these through a maturity model in order to assess and manage blockchain adoption and implementation throughout the whole innovation life-cycle.

As previously mentioned, the OECD Blockchain Primer [22] also takes an individual approach to identifying risks according to three policy areas: (1) upfront costs for supply chain; (2) data security for healthcare applications; (3) energy consumption, which presents a particularly contradictory issue when looking for value creation regarding blockchain usage in the energy sector.

An additional method to risk management is the establishment of common standards such as the NIST risk management framework.[2] This framework does not appear to be considered by any of the sources that we assessed. This may be due to the fact that the framework is more oriented towards security controls and its relevance is not immediately clear for practitioners. For instance, interoperability is a key risk area, as the connecting of different types of blockchains with each other for transactions and trading present new risks and obstacles. In 2017, multiple projects launched protocols for how independent blockchains could best communicate in a decentralized and scalable way. Companies such as Aion, ICO, Wanchain and others came together to found the Blockchain Interoperability Alliance. This alliance is focused on developing a common set of standards for blockchain interoperability to ensure that the shared vision of a global ecosystem of connected blockchains will be achieved [8].

3.4. RQ4. What are the current research gaps in the area of risk management within the adoption and standards-based application of blockchain technology?

Due to the novelty of the technology there appears to be a range of research gaps. In this context we would like to highlight three major gaps:

(a) First, we recognized a general lack of focused research into "sustainable blockchain use", which becomes apparent through initial keyword searches. Moreover, research and documentation of the impact of blockchain projects is lacking, thus creating a gap in content to support optimization and improvement as practices of sustainable use [5,6,15,36]. This reflects a clear need for standards and structured requirements management in the area.

(b) Furthermore, there is currently no normative, universally applicable framework for risk management of blockchain technology. We derive this gap from the finding that each of the reviewed sources employs different risk terminologies, categories, taxonomies etc. An integrated, comprehensive risk management framework can be beneficial for businesses and users across industries and use cases.

(c) The third gap identified within the scope of this research is the lack of applied studies, which track the development of risks to blockchain applications over the short and long-term. An example from the development sector makes this lack evident. MERL (monitoring, evaluation, research, and learning) practitioners Burg et al. [5] examined 43 blockchain use cases and reported on the sheer lack of documentation or evidence supporting value claims of blockchain in the international development space and cite this as a critical gap for potential adopters. This finding again represents a strong evidence for the need for standards and structured requirements management in the area.

3.5. Other relevant findings

While not providing a direct answer to the research questions, there are several recent publications that are still of relevance to this review. One is a similar review paper that looks at blockchain use-cases in healthcare [20] where a similar epistemological gap in methods is identified. Another one that is worth mentioning is [24] – A proposed set of building blocks for global blockchain deployments in supply-chain scenarios that also identifies challenges similar to the ones that we are observing.

4. Discussion of results

Our results provided answers to the research questions that we formulated. Still, these answers should be considered in their appropriate context. With RQ1 our analysis shows that risk is considered from four dominating perspectives - general, technological, business-oriented and project-management based. While these paradigms are sound, our analysis identifies an important gap – often risks reside at the cross-sections of the different domains, e.g. business-technology alignment. Blockchain, being a transformative technology, very often poses exactly such kind of risks and current risk definitions miss this point.

In the context of RQ2 our analysis identified a variety of specific risks that are (or should be) considered in the context of blockchain adoption. Nevertheless, these specific risks are not considered in aggregation and important cumulative scenarios are currently out of scope. An example of a cumulative scenario would be the case where several risk factors coalesce to lead to a risk that is considerably higher than anticipated – ill-defined governance rules in a blockchain can result in misconfigured access rights for users which can result in missing compliance with regulations. Simultaneously, ill-defined governance can also lead to risks related to the enforcement of contract.

The analysis in the context of RQ3 shows further open research fields and challenges. The identified key functions exhibit certain overlaps and in the same time appear to be incompatible with each other. Furthermore, there are both holistic [23,30] and partial [21] approaches that we identified. Areas of overlap converge along risk identification [4,22,23,30], while incompatibilities are observed in the areas of risk management and mitigation.

Looking at RQ4 our analysis showed that the research landscape around the topic is still in its early stage, resulting in large research gaps throughout the field. Within these, we focused on three distinct research gaps – the standards-based use of blockchain technology, the need for a general framework that addresses risk and requirements management in the context of blockchain technology, as well as the lack of applied studies that monitor and assess blockchain-related projects. Of course, these three areas are closely connected to one another – a generally applicable framework or standard will provide methods to assess risks and manage requirements within blockchain projects, which will in turn allow for the long-term monitoring and assessment of these projects, and ultimately this will result in a more sustainable use of blockchain technology that moves beyond the campaign-like approach that dominates the current landscape.

There appears to be a general gap between what practitioners in the blockchain area suggest and what has been a range of state-of-the-art approaches in the software engineering and information security research and practice. This is exemplified by the absence of the NIST risk management framework in the considerqations of the sources that we

[2] https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

identified.

While we deem our results credible, there are certain limitations that we would like to state clearly. Our results represent a snapshot of the development as it has been published until the middle of the year 2019. Furthermore, they only go back to 2015. Ongoing activities that are still not published or activities that started before or after these points are not reflected. Furthermore, we considered only English language publications. This may have limited the results in the context of different aspects, more specifically we have probably missed current applied studies of blockchain usage if these were only published in languages different from English. Furthermore, there is still a certain terminological uncertainty in the field. The terms "blockchain", "distributed ledger", "smart contracts" and other related ones are strong and recognizable buzzwords which may lead to them being misattributed to activities and projects that have only limited relevance to the area. While we have assessed all of our sources thoroughly, we have not made any efforts to validate their claims with our own primarily field research, e.g., visiting specific locations where these projects are being deployed. All these aspects introduce certain biases in our results, affecting their reliability and reproducibility. However, we minimized these biases by using a variety of literature targeting both researchers and industry. The diversity of perspectives minizimes our personal biases and improves the reliability of the findings. With regard to internal validity, authors point to the systematic conduct of the review.

With regards to external validity, the broadness and the comparable level of industry experience improve the generalizability of the findings.

5. Conclusion and Outlook

This work aims to present perspectives on risks and standards that affect the requirements engineering of blockchain as applied to the adoption and standards-based use of blockchain technology. We have operationalized the research problem into four research questions:

RQ1. How is risk defined within business and technology contexts, and why is it relevant?
RQ2. What are the perceived risks across various industries and use cases that affect the adoption and sustained use of blockchain technology?
RQ3. What methods are in current use for assessing and managing these risks?
RQ4. What are the current research gaps in the area of risk management within the adoption and standards-based application of blockchain technology?

RQ1 provided the definition of risk that we needed for examining both hypotheses. RQ2 illuminated the relationship between risks and adoption of blockchain technology. RQ3 gave answers to the main assumption of both hypotheses, that standards-based approaches are important, by showing us what approaches are currently in use. Finally, RQ4 allowed us to identify specific gaps in the state-of-the-art research that directly impact both hypotheses.

To find answers to these questions, we conducted a systematic literature review. The results of the literature review provided answers that we have presented in Section 3 and discussed in Section 4. While these results are bound to the biases and uncertainties that are discussed in Section 4, they can be summarized as follows:

Risks are defined within the perspectives of general risk management, as well as the technological, the business-oriented and the project-management based paradigm. They are measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred [17]. There are 27 perceived risks that span areas from access control, through compliance and governance, to user experience. There are four major methods currently in use to assess and manage these risks. These were proposed and are backed by academics, technology consultancies and international organizations. With respect to the research gaps, we found that the research landscape around the topic is still in its early stage, with large research gaps spread throughout the field. We analyzed three distinct research gaps – the sustainable use of blockchain technology, the need for a general framework that addresses risk management in the context of blockchain technology, as well as the lack of applied studies that monitor and assess blockchain-related projects, and found that these three areas are closely connected to one another – a finding that explains the general immaturity of the field.

As far as future research directions are concerned, broader research activity, as well as incentives for conducting research into requirements and risk management for standards-based blockchain usage, are required. A focused discussion of requirements management and a standardization framework for the sustainable application of blockchain have yet to emerge. Closing the gaps in both the research and management domains could provide great opportunity in terms of identifying novel forms of leadership and consultancy.

We conclude that risk management within various blockchain environments could benefit from a consideration of risk and requirements parameters in alignment with the general understanding of risk and the four viewpoints previously defined – general, business, technology and project management.

Based upon high interest across various industries and use cases, our hypotheses point to sound methods for managing risk along the entire adoption process as being key to sustainable adoption and use of blockchain technology. A concrete outlook that we are currently working on, will be an integrated, normative framework for operationalizing risk parameters, along with a tool for better evaluating and managing these individual risks. Such a framework could then be applied and tested across industries and use cases, then optimized based upon results and further developed for market maturity.

Governance is key aspect of any such normative framework. We uphold the argument that a well-planned governance policy needs to be developed to maximize the benefits of the blockchain technology and to ensure its sustained usage across all life-cycle stages. Furthermore, we agree that blockchain governance issues could largely be regulated under the existing legal rules without the need for sweeping reform [10]. An analysis of which legal frameworks come into question could support further research into risk management.

Based on our findings in Section 3, it becomes clear that several other general risk areas should be key aspects of any such normative framework. For instance, interoperability has been identified as a common area of risk, but also as an obstacle and opportunity for mainstream adoption of public and private blockchains. As discussed in 2.1.5, the Blockchain Interoperability Alliance's progress could be tracked, in order to follow the development of a common set of standards for blockchain interoperability [8]. Another example of a common risk area for blockchain adoption that we have identified, is change management [22–26]. This points to a more general problem with technology adoption. While various, general models for the adoption of blockchain technologies exist [23,30], there appears to be no unified, holistic framework for managing the business transformation process and its related risks. These gaps in the management of key risk areas also represent great opportunity in terms of further research.

To close the gap in terms of applied studies, which track the development of risks to blockchain applications over the short and long-term, real-time case studies with a normative blockchain risk management framework could be conducted. Findings and insights could be fed into a collaborative, shared, transparent platform in order to support the enhancement of sustainable blockchain adoption. For instance, the aforementioned IBM + Maersk project [9] could have been monitored and evaluated with a normative, holistic risk management tool which could then provide insights across a globally accessible database for shared learning.

In closing: our results in Section 3 demonstrate that risk management is important for a successful adoption and use of blockchain technology. Due to the transformative nature of blockchain technology, the practice of risk management takes on a particular importance in the context of business transformation. To cite the World Economic Forum, a blockchain application does not represent an end goal. Conversely, blockchain technology should be understood as a strategic change effort, which requires rethinking business models, rethinking relationships between companies and between companies and customers [34]. This level of transformation calls for appropriate risk management practices.

CRediT authorship contribution statement

Nusi Drljevic: Conceptualization, Data curation, Investigation, Methodology, Resources, Writing - original draft. **Daniel Arias Aranda:** Methodology, Supervision, Validation, Writing - review & editing. **Vladimir Stantchev:** Conceptualization, Methodology, Supervision, Validation, Writing - review & editing.

Declaration of Competing Interest

None.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.csi.2019.103409.

References

[1] Baydakova, A.Bond rating agency Moody's warns on risks of private blockchains. Available online: https://www.coindesk.com/bond-rating-agency-moodys-warns-on-risks-of-private-blockchains (accessed on 29.05.2019).

[2] R. Beck, C. Müller-Bloch, J. King, Governance in the blockchain economy: a framework and research agenda, J. Assoc. Inf. Syst. 19 (10) (2018) 1020–1034.

[3] Brakeville, S.; Perepa, B.Blockchain basics: introduction to distributed ledgers. Available online:https://developer.ibm.com/tutorials/clblockchain-basics-intro-bluemix-trs/ (accessed on 10.04.2019).

[4] K. Bugle, M. Goldsmith, G. Marountas, T. McDermott, Risk and Control Considerations for Blockchain Technology, CohnReznick LLP, NYC, USA, 2018, pp. 4–8.

[5] Burg, J.; Murphy, C.; Pétraud, J.P.Blockchain for international development: using a learning agenda to address knowledge gaps. Available online: http://merltech.org/blockchain-for-international-development-using-a-learning-agenda-to-address-knowledge-gaps/ (accessed on 26.06.2019).

[6] Business Dictionary – Risk. Available online:http://www.businessdictionary.com/definition/risk.html (accessed on 26.06.2019).

[7] F. Caron, Blockchain. Identifying risks on the road to distributed ledgers, ISACS J. 5 (2017) 1–6.

[8] De Castillo, M.Coindesk. Available online: https://www.coindesk.com/interoperability-boost-ripple-sends-blockchain-transaction-across-7-different-ledgers/ (accessed on 09.08.2019).

[9] Deshwali, S.Risks of blockchain projects - Why do so many blockchain projects fail? Available online.

[10] A.A Gikay, European conusumer law and blockchain based financial services: a functional approach against the rhetoric of regulatory uncertainty, TLR 24 (1) (2019) 27–48.

[11] V. Grewal-Carr, S. Marshall, Blockchain: Enigma. Paradox. Opportunity, Deloitte LLP, London, UK, 2016, pp. 10–12.

[12] Gupta, M.*Blockchain for the Enterprise*. Manav Gupta: USA, 2018; #-#.

[13] Hill, R. Emergent Tech – IBM Struggles to Sign Up Shipping Carriers to Blockchain Supply Chain Platforms Reports. Available online: ibm_struggles_to_sign_up_shipping_carriers_to_blockchain_supply_chain_platform_reports (accessed on 26.06.2019).

[14] Hillson, D.Managing overall project risk. Available online:https://www.pmi.org/learning/library/overall-project-risk-assessment-models-1386(accessed on 26.06.2019). https://hackernoon.com/risks-of-blockchain-projects-why-so-many-blockchain-projects-fail-569bbce27af8 (accessed on 29.05.2019).

[15] Iansiti, M.; Lakhani, K.The truth about blockchain. Harvard business review, January-February2017. Available online: https://hbr.org/2017/01/the-truth-about-blockchain (accessed on 09.08.2019).

[16] Investopedia - Business Risk. Available online: https://www.investopedia.com/terms/b/businessrisk.asp (accessed on 04.06.2019).

[17] J. Van Bon, A. De Jong, A. Kolthof, M. Pieper, R. Tjassing, A. van der Veen, T. Verheijen, Foundations of IT Service Management Based on ITIL Vol. 3 Van Haren, 2008.

[18] James, A.92% of blockchain projects have already failed, average lifespan of 1.22 years. Available online: https://bitcoinist.com/92-blockchain-projects-already-failed-average-lifespan-1-22-years/ (accessed on 26.06.2019).

[19] T.A Khan, Governance, security and authentication issues related to blockchain within cross-border trade, UN/CEFACT Blockchain Conference, Rome, Italy, 30th UN/CEFACT Forum, 201704 October.

[20] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.

[21] C.Y. Kim, K Lee, Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats, Proceedings of the International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 2018, pp. 1–6 January 29-31.

[22] K. Kim, T. Kang, Does technology against corruption always lead to benefit? The Potential Risks and Challenges of the Blockchain Technology, Paris, France, OECD Global Anti-Corruption and Integrity Forum, 2017, pp. 12–15 March 30-31.

[23] N.V. KPMG, Blockchain Maturity Model. Helping You to Get from Proof-of-Concept to Production 4-5 KPMG, Netherlands, 2017, pp. 8–10.

[24] A. Litke, D. Anagnostopoulos, T. Varvarigou, Blockchains for supply chain management: architectural elements and challenges towards a global scale deployment, Logistics 3 (1) (2019) 5.

[25] S. Manski, Building the blockchain world: technological commonwealth or just more of the same? Strateg. Change 26 (2017) 511–522.

[26] R. Maull, P. Godsiff, C. Mulligan, A. Brown, B Kewell, Distributed ledger technology: applications and implications, Strateg. Change 26 (5) (2017) 481–490.

[27] OECD Blockchain Primer, 2018. Available online:http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf (accessed on 21.05.2019).

[28] Panchev, K.Why today's blockchain cannot be mainstream. Available online:https://www.trendingtopics.at/bulgaria/why-todays-blockchain-cannot-be-mainstream/ (accessed on 29.05.2019).

[29] Risk management, risk analysis, templates and advice. Available online:https://www.stakeholdermap.com/risk/business-risk.html (accessed on 26.06.2019).

[30] P. Santhana, A. Biswas, Blockchain Risk Management – Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy, Deloitte Development LLC, 2018, pp. 4–8.

[31] P. Satyavolu, A. Sangamnerkar, Blockchain's Smart Contracts Driving the Next Wave of Innovation Across Manufacturing Value Chain, Cognizant, 2016, pp. 6–9 White Paper.

[32] D. Tapscott, A. Tapscott, Blockchain Revolution. How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, Penguin Random House, NYC, USA, 2018 #-#.

[33] Vota, W.Blockchain use case failure: 43 projects and zero impact found. Available online: https://www.ictworks.org/blockchain-impact-failure/#.XRPQMXtS_YI (accessed online 26.06.2019).

[34] S. Warren, D. Treat, Building Value With Blockchain technology: How to Evaluate Blockchain's Benefits, World Economic Forum, Geneva, 2019.

[35] J.L. Zhao, S. Fan, J. Yan, Overview of business innovations and research opportunities in blockchain and introduction to the special issue, FIN 2 (1) (2016) 28.

[36] Z. Zheng, S. Xie, H.N. Dai, X. Chen, H Wang, Blockchain challenges and opportunities: a survey, IJWGS 14 (4) (2018) 352–375.