



Security Architectural Approaches and Risk Assessment Methods for Blockchain Systems: A Review and Future Directions

SABREEN AHMADJEE, Department of Cybersecurity, College of Computing, Umm Al-Qura University, Saudi Arabia
CARLOS MERA-GÓMEZ, Escuela Superior Politecnica del Litoral, Guayaquil, Ecuador and University of Birmingham, Birmingham, United Kingdom of Great Britain and Northern Ireland
RAMI BAHSOON, University of Birmingham College of Engineering and Physical Sciences, Birmingham, United Kingdom of Great Britain and Northern Ireland
RAJKUMAR BUYYA, Cloud Computing and Distributed Systems (CLOUDS) Lab, Melbourne, Australia

Amid the widespread use of blockchain technology, the escalating frequency of cyberattacks exploiting its inherent security challenges underscores the critical necessity for a robust and adaptable security risk assessment approach. The distinctive attributes and intricate internal structure of blockchain not only attract malicious actors but also elevate the risk of ill-informed architectural design decisions, potentially introducing security vulnerabilities. This study addresses this imperative by conducting a systematic literature review, classifying publications that elucidate secure architectural design approaches and categorising those that delineate methods for assessing security risks associated with blockchain and smart contracts. The findings reveal four prevalent approaches supporting secure architectural design—decision models, taxonomies, design patterns and guidelines—alongside contributions in blockchain risk assessment encompassing risk identification, analysis and evaluation methods. Furthermore, the study identifies unresolved architectural design challenges and proposes future research directions in this evolving landscape.

CCS Concepts: • **Software and its engineering** → **Risk management**; • **Security and privacy** → **Distributed systems security**; **Software security engineering**; • **General and reference** → **Surveys and overviews**;

Additional Key Words and Phrases: Blockchain, Smart Contract, Security, Risk Assessment

ACM Reference format:

Sabreen Ahmadjee, Carlos Mera-Gómez, Rami Bahsoon, and Rajkumar Buyya. 2025. Security Architectural Approaches and Risk Assessment Methods for Blockchain Systems: A Review and Future Directions. *Distrib. Ledger Technol.* 5, 1, Article 7 (December 2025), 21 pages.
<https://doi.org/10.1145/3721140>

1 Introduction

Blockchain is a disruptive technology intended to implement secure, decentralised distributed systems, in which transactional data can be shared, stored and verified by participants without needing a central authentication or

Authors' Contact Information: Sabreen Ahmadjee (corresponding author), Department of Cybersecurity, College of Computing, Umm Al-Qura University, Saudi Arabia; e-mail: smahmadjee@uqu.edu.sa; Carlos Mera-Gómez, Escuela Superior Politecnica del Litoral, Guayaquil, Ecuador and University of Birmingham, Birmingham, United Kingdom of Great Britain and Northern Ireland; e-mail: cjmera@espol.edu.ec; Rami Bahsoon, University of Birmingham College of Engineering and Physical Sciences, Birmingham, United Kingdom of Great Britain and Northern Ireland; e-mail: r.bahsoon@cs.bham.ac.uk; Rajkumar Buyya, Cloud Computing and Distributed Systems (CLOUDS) Lab, Melbourne, Australia; e-mail: rbuyya@unimelb.edu.au.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM 2769-6480/2025/12-ART7

<https://doi.org/10.1145/3721140>

verification authority. The distinguishing properties and internal complex structure of blockchain technology enable the development of new security risks. Moreover, the widespread usage of this technology, especially after the emergence of smart contracts, or blockchain-based computer programs, has incentivised attackers to exploit their existing security challenges [55].

Numerous malicious attacks have occurred because of poorly designed or vulnerable blockchain-based systems and/or smart contracts. For instance, in July 2020, an unauthorised third party accessed the e-commerce and marketing database of the Ledger company Web site [36]. This cyberattack caused a massive data breach. Scammers used this data and applied phishing attacks to trick users into revealing the keys to the company’s crypto wallet. Scammers also sent e-mails that included users’ data and threatened them, asking them to pay a ransom. Making a poor decision to store sensitive data in an insecure, off-chain, centralised database facilitated these attacks. This sort of incident emphasises the necessity of *secure-by-design* approaches to orchestrate the creation of secure blockchain-based systems. A robust architectural design is the first step in *secure-by-design* processes [49], which allow security to be incorporated into the system from the ground up.

In this article, we provide a **Systematic Literature Review (SLR)** that identifies existent approaches to architect and design secure blockchain-based systems and smart contracts. The following are this article’s main contributions:

- A classification of existing publications that contribute to providing secure architectural design approaches. Four commonly used approaches are identified: decision models; taxonomies; design patterns and guidelines.
- Categorisation of publications that support blockchain risk-assessment methods. The publications contribute to several security risk-assessment phases that comprise security risk identification, risk analysis and/or risk evaluation.
- Determination of certain blockchain security architectural design challenges that are yet unresolved and made proposal for future research directions.

Existing studies focus on reviewing the approaches, frameworks and/or automation tools that are leveraged in blockchain and smart contract testing [22, 56]. However, the approaches for assessing security issues’ root causes at the early design stages are neglected. Even though there is a study [13] that reviewed the state of knowledge on perceived risk related to the adoption and application of blockchain technology, approaches related to security risk assessment were not investigated. To the best of our knowledge, we are the first study that conducted an SLR to investigate, classify and analyse the current approaches and methods for architecting and designing secure blockchain-based systems and smart contracts.

The rest of this article is structured as follows. Section 2 presents a brief overview of blockchain, smart contracts and risk assessment. Section 3 provides the research methodology used to conduct the SLR and Section 4 presents the findings of the review. Analysis of the findings is provided in Section 5. Section 6 presents the future directions, the gap analysis and the potential threats to the validity of the work. Related reviews are contrasted with ours in Section 7, and finally, Section 8 summarises the article.

2 Preliminaries

This section provides a brief overview of blockchain, smart contracts and risk assessment.

2.1 Blockchain Overview

Blockchain is a chain of ordered blocks, which are distributed across thousands of nodes, each block connecting to the previous block via a cryptographic hash of its content [21]. The block is seen as immutable because it cannot be modified retroactively without the modification of all the subsequent blocks. Generally, each block contains a list of transactions, a hash of the current block, a hash of the previous block, a timestamp and other information such as a nonce value. Each node participating in the blockchain network can create a cryptographically signed

transaction and then exchange it with peers in the network to provide non-repudiation to the stored transactions. Cryptographic mechanisms used by blockchain technology add integrity to the system. This technology is based on a decentralised peer-to-peer network that dispenses with the need to trust a centralised controller. Trust in the blockchain is built by relying on its protocols, mechanisms and cryptographic algorithms. Transparency and visibility are high in blockchain because data stored in the chain is publicly accessed by all the participants in the network.

2.2 Smart Contracts

A smart contract is a decentralised code agreement designed to impose an automatic negotiation of a series of instructions without requiring approval by a central authority [58]. The structure of a smart contract is similar to the structure of the class in object-oriented languages. The contract could consist of state variables, functions and events. Additionally, the contract can leverage other contracts by using inheritance. A smart contract code is stored and run on top of the blockchain and the correct execution of the contract is enforced by the blockchain properties, namely transparency and immutability. Once a contract is deployed, its program code is fixed and cannot be modified. This condition distinguishes smart contract programs from regular computer programs.

2.3 Risk Assessment

The standard for information security management systems, ISO 27001 [29], follows the principles and guidelines for risk management provided in ISO 3100 [28]. According to ISO 3100, risk assessment is the overall process of (i) risk identification; (ii) risk analysis and (iii) risk evaluation. First, risk identification aims to find threats that may prevent the achievement of objectives. Then, risk analysis intends to understand the inherent characteristics of the risk, including uncertainties, sources, impact and likelihood. Finally, the risk evaluation focuses on the support towards the decision-making behind the comparison between the results of the risk analysis and pre-established risk criteria.

3 Research Methodology

This section describes the methodology of our work which is based on Kitchenham and Charters [30], who offered widely recognised SLR guidelines in software engineering. In particular, we conducted the review in several distinct stages: (i) identifying the review **Research Questions (RQs)**; (ii) establishing the search strategy; (iii) determining the inclusion and exclusion criteria; (iv) applying the study selection procedure; (v) assessing the quality of the final set of included studies and (vi) extracting and analysing the data.

3.1 RQs

We intend to examine the following RQs:

- RQ1: What are the common security architectural design approaches used when architecting blockchain-based systems and smart contracts?
- RQ2: What are the existing frameworks, models and methodologies for security risk assessment in blockchain-based systems and smart contracts?
- RQ3: What are architectural design challenges that are yet unresolved and what are future research directions that help solve them?

RQ1 is designed to provide an overview of the existing security architectural design approaches used in architecting blockchain systems and smart contracts. Several blockchain architectural methods have been developed in recent years, and we aim to investigate to what extent security aspects are considered in these approaches. Additionally, we want to understand the purpose and limitations of these approaches. RQ2 is devised to determine current methods for assessing the security risks linked to blockchain and smart contracts. It is important to emphasise

that our research focuses on the security risk assessment methodologies for blockchain adaption rather than on how blockchain technology is employed as a solution for use in risk management or as a method to provide security to applications such as blockchain-based **Internet of Things (IoT)** applications.

3.2 Search Strategy

Studies were selected by entering keywords into the search feature of five major publishers or search engines: (i) IEEE Explore; (ii) ACM Digital Library; (iii) Science Direct; (iv) ISI Web of Science and (v) Scopus. The keywords were chosen to encourage the emergence of research findings that would aid in addressing the two RQs. The search strings for the search are as follows:

- ('Blockchain' OR 'Smart contract') AND ('Secure') AND ('Architecture Analysis' OR 'Architectural Analysis' OR 'Architectural Design') AND ('Methodology' OR 'Frameworks' OR 'Approach' OR 'Model').
- ('Blockchain' OR 'Smart contract') AND ('Secure') AND ('Architecture' OR 'Architectural') AND ('Risk') AND ('Assessment' OR 'Analysis').

We filtered the results of these searches by applying the inclusion and exclusion criteria, which are presented in the following section. To complement and enhance the search process, a snowballing strategy was employed as defined by Wohlin [59]. This strategy refers to identifying more articles by utilising a paper's reference list, which is known as 'backwards snowballing', or citations, which is known as 'forwards snowballing'. We conducted forwards and backwards snowballing iterations until no more papers fulfilling the inclusion criteria were found.

As the blockchain technology topic is actively growing in the industry and the technology is being rapidly adapted, we considered including relevant grey literature, specifically industry sources and standards from the leading global consultancy firms that have published white papers, guidelines or approaches that discuss the security architectural design of blockchain systems.

3.3 Study Selection

Because not all the papers returned by the search were relevant to the study questions, they had to be screened first. As a result, we identified the selection criteria that were used to verify that the outcomes were objective. The following are the inclusion and exclusion criteria that we established:

Inclusion Criteria (I)

- *I1*: Studies published in peer-reviewed journals, conference proceedings, workshops or book chapters. Publications must be of a scholarly nature and demonstrate rigorous peer-review processes.
- *I2*: Studies that explicitly discuss topics related to blockchain technology and/or smart contracts, covering theoretical, technical or practical aspects, including [64] and [66], among others.
- *I3*: Studies focusing on the analysis, assessment or management of security risks specifically within the context of blockchain and/or smart contract applications. This includes works that propose frameworks, methodologies or evaluations related to security risks, such as [24].
- *I4*: Studies addressing security architectural design approaches for blockchain and/or smart contracts. This includes research proposing architectural frameworks, patterns or best practices aimed at enhancing the security of these technologies, such as [39] and [15].

Exclusion Criteria (E)

- *E1*: Studies originating from disciplines outside computer science, where blockchain is mentioned solely as a secondary component or tool in the application (e.g., finance, healthcare or supply chain studies focusing on blockchain's functional integration), such as [10] where blockchain used as a component to provide security for healthcare IoT systems.
- *E2*: Studies not written in English, as language barriers limit accessibility and comprehensive analysis.

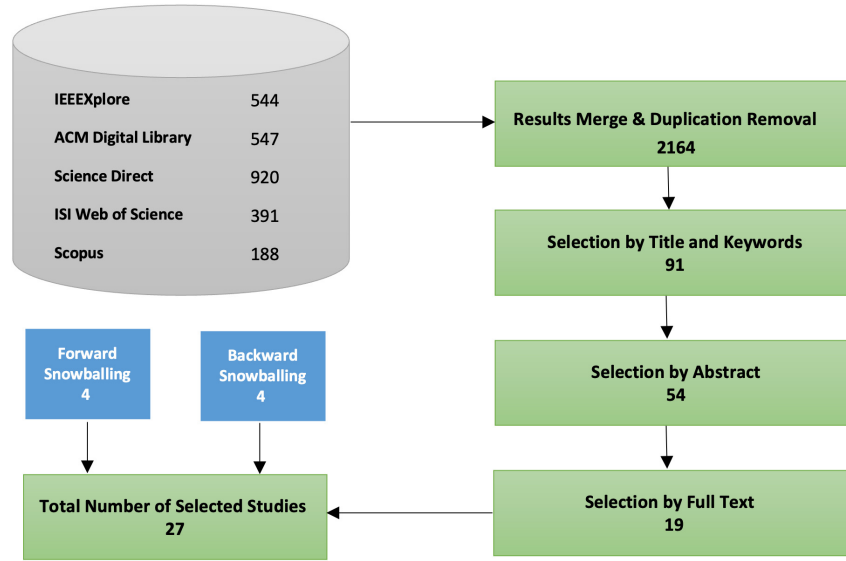


Fig. 1. Search and academic papers selection procedure.

– *E3*: Studies that were not freely available (i.e., the publisher’s database requires members to make an additional fee to provide access to the full text of the article).

Three rounds of filtering were used to determine the final selection of research papers. Figure 1 presents the search and selection processes.

- *First Round*: We selected papers based on metadata, including title, venue name and keywords. In this round, we considered the criteria I1 and E1.
- *Second Round*: We independently chose papers by reading the papers’ abstracts. In this round, we considered criteria I2 and E2.
- *Third Round*: We independently chose papers by reading the full text of the papers selected in the previous round. In this round, we considered criteria E3, I2, I3 and I4.
- *Snowballing*: Additional articles were discovered using forwards and backwards snowballing. All inclusion and exclusion criteria were considered.

After round three and the snowballing step, we applied Equation (1) to calculate Cohen’s kappa (k) [53], which is a statistical measure to assess the agreement between two reviewers deciding the same issue:

$$k = (P_o - P_e) / (1 - P_e), \quad (1)$$

where P_o is the probability of the observed agreement, and P_e is the probability of random agreement. We got a P_o of 0.90, and a P_e of 0.60, which produced a k of 0.75, indicating substantial agreement. To resolve the disagreements, a discussion that involved all the reviewers was conducted. As a result of this discussion, 27 studies were included in our SLR.

Manual Search. We started searching for publications of well-known institutions and organisations that regularly produce publications related to blockchain, such as Deloitte [12], KPMG [34] and **National Institute of Standards and Technology (NIST)** [44]. Additionally, we expanded our research by conducting a manual search using the Google search engine to cover other industrial publications. Finally, we selected eight grey publications that matched our inclusion criteria.

3.4 Quality Assessment

In this study, the criteria presented by Yang et al. [69] were customised to assess the quality of the selected studies. Three essential characteristics of empirical studies were considered in this research: rationality, rigour and credibility.

- *Rationality* assesses whether the study clearly defines its research context and objectives.
- *Rigour* evaluates whether the research approach is methodical, scientific and comprehensive.
- *Credibility* examines whether the findings are reliable, meaningful and acknowledge potential limitations.

The most commonly used quality criteria for each characteristic, as identified in previous SLRs in software engineering, were adopted. The following eight quality criteria were applied to each selected study:

Rationality

- (1) Is the paper based on empirical research?
- (2) Is the context of the study stated clearly?
- (3) Is there a clear description of the research objectives?

Rigour

- (1) Does the method adequately address the research objectives?
- (2) Is the data collection method fully described?
- (3) Is data analysis sufficiently described?

Credibility

- (1) Is there a clear description of the results?
- (2) Do the researchers discuss limitations or threats to the validity of the results?

Two reviewers separately scored each of the eight studies' criteria using a Boolean matrix (0 or 1), where 1 indicates that the study fulfils the quality assessment question, and 0 indicates that the study does not fulfil the quality assessment question. A group discussion involving all authors was held if there were any discrepancies between the reviewers, and the study was reviewed again to determine the final score. Table 7 illustrates the scores of each study.

3.5 Data Extraction

Data extraction is the process of gathering data items that were used to analyse the final studies and answer our two RQs. This study's data extraction mostly comprised demographic information, information related to blockchain security architectural design approaches and information related to security risk assessment methods. Table 1 shows the extracted items. Demographic information can be statistically demonstrated, while the information related to the RQs requires in-depth analysis. The data extraction method was first applied to a collection of 10 highly cited studies in the field of blockchain architecture. The collected data were merged and classified. We selected the main concepts and aspects that resulted in the first draft of our classification. Next, we examined the entire collection of selected studies to develop the classification.

3.6 Data Synthesis

This section aims to provide a concise summary of the data that was extracted to fulfil the study's objectives. The data that was extracted for this study is both quantitative and qualitative. A descriptive analysis method was applied to synthesise a set of quantitative data, including the distribution of the studies' publication years, publication venues and quality scores. The purpose and focus area of each selected study was also described. The thematic synthesis method [26] was used to synthesise the qualitative data and answer the study's RQs. The

Table 1. Extracted Data Items

Item	Association
Title of the study	Demographic
Year of the study	Demographic
Venue of the study	Demographic
Type of security architectural method	RQ1
Purpose of the security architectural method	RQ1
Security risk assessment method	RQ2
Purpose of the risk assessment method	RQ2

Table 2. Publication Venues of Selected Studies

Publication Channel	Selected Studies
Journals	[2, 3, 6, 8, 9, 15, 16, 20, 24, 25, 51, 68, 71]
Conferences	[31, 39, 40, 42, 48, 50, 52, 54, 62–66]
Workshop	[61]

qualitative data refers to the type of blockchain security architectural approaches and security risk assessment methods. To answer RQ1, a categorisation process was conducted, and the blockchain security architectural design approaches were classified into categories that have similar characteristics. Then the purpose of each approach was explained. To answer RQ2, the security risk identification and security risk analysis and evaluation approaches were identified and thoroughly explained. Section 4 (Results) and Section 5 (Analysis) present all the extracted and synthesised information.

4 Results

This section demonstrates the distribution of publications in different venues over time, the distribution of the quality assessment scores of selected studies and the aim and focus of each article.

4.1 Demographics of Selected Studies

As only peer-reviewed articles were included in this study, Table 2 illustrates the selected studies in each publication venue. As shown, half of the included studies were published at conferences and the other half were published in journals. However, most of the journal papers received high scores on the quality assessment. For instance, only journal papers received a full quality assessment score of eight, while only one conference paper received a score of seven, as shown in Figure 2. This demonstrates the quality scores of the included studies according to the quality criteria presented in Table 7. Figure 2 shows eight studies received a score of six. Most of these studies provided no details on their data collection methods, and they did not discuss limitations or threats to the validity of their results. Only one study received the lowest score, which is three. This study was not empirical research; it provided no information about the data collection methods, and there was no clear description of the results and study limitations.

4.2 Purpose of Selected Studies

Each selected article was read in full before essential information was retrieved and summarised in Table 3, which explains the aim of each study as well as its focus area.

Figure 3 shows the percentages of different focus areas of the 27 selected studies. The focus areas identified in the selected studies highlight that a quarter (25%) of all studies are mostly concerned with blockchain security issues as they discuss popular blockchain security attacks and threats. Blockchain selection and blockchain

Table 3. Main Purpose and Focus Area of the Primary Studies

Study	Purpose	Focus Area
[15] [64]	Equips blockchain decision-makers with a decision support model to select a suitable blockchain platform for their applications Provides an experience report about blockchain architectural decisions to decide or discard the adoption of a decentralised solution based on blockchain	Blockchain selection
[52]	Provides a methodology that assists the selection of blockchain for a given set of requirements and also offers guidance throughout blockchain configuration	
[24]	Provides a risk analysis methodology to facilitate understanding of the security implications in the adoption of blockchain	
[25]	Introduces a layered security reference architecture for blockchain that identifies origins of known security threats and their potential mitigation mechanisms	
[71]	Discusses the blockchain's basic architecture and its potential security and trust issues at the data, network, consensus, smart contract and application layers	Blockchain security
[51]	Presents a discussion on a set of attack vectors and security threats to blockchain-based solutions	
[3]	Presents a security risk assessment methodology that enables a systematic quantification of the risk associated with blockchain technology and its ecosystem	
[63]	Provides architects with a decision model to assist them in selecting the appropriate architectural design patterns for blockchain-based applications	
[42]	Identifies the main threats to blockchain and assesses how these threats may adversely impact a blockchain-based solution	
[65]	Categorises design patterns for blockchain-based applications, including one category of security patterns	
[16]	Introduces a multi-criteria framework for selecting the most-suitable consensus protocols depending on the identified criteria, priorities and other requirements	
[40]	Assesses attacks that target consensus protocols with respect to their potential implementation in an IoT blockchain environment	Consensus protocol
[20]	Introduces an evaluation framework of blockchain consensus algorithms and discusses security design principles to deal with different attacks	
[8]	Proposes a classification framework of consensus protocols to serve as a comprehensive and integrated taxonomy	
[48]	Provides a brief discussion of architectural aspects of smart contracts and a security mechanism to be followed when designing smart contracts	Smart contracts
[61]	Elaborates a set of security design patterns for smart contracts	
[50]	Presents a discussion of security issues related to blockchain adoption in IoT environments	
[68]	Provides a catalog of architectural tactics for achieving a set of required quality attributes in the design of IoT systems based on blockchain	
[9]	Presents an analysis of security issues at each layer of a blockchain architecture and the potential impact of security attacks against a blockchain system	IoT
[66]	Proposes a taxonomy that captures some architecturally relevant blockchain characteristics in relation to their support for various quality attributes	Quality attributes
[62]	Provides a methodology to identify whether blockchain is useful depending on the problem requirements, and if so, what type of blockchain might be appropriate	Blockchain access type
[54]	Presents a map with the main design dimensions for blockchain networks	Blockchain network design
[39]	Provides design guidelines that detail a number of Ethereum design patterns and their map to solidity coding practices	Self-sovereign identity
[6]	Presents a penetration testing framework for smart contracts and decentralised apps that assesses the security risk of several attacks	Penetration testing
[2]	Complements the information security controls framework for blockchain established by the International and National Information Security Standards	Information security
[31]	Provides risk analysis and risk management guidelines based on NIST and ISO standards for cryptocurrency exchange	Cryptocurrencies

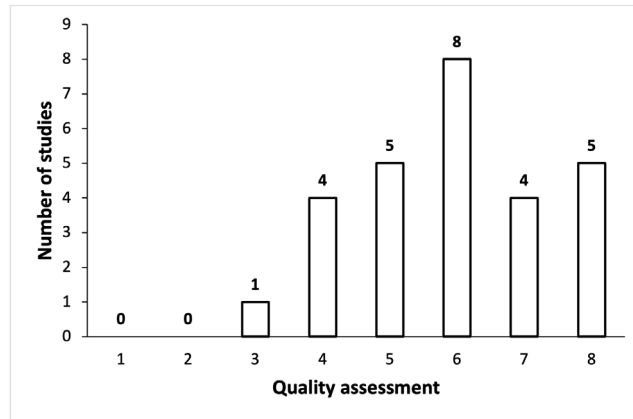


Fig. 2. Quality scores of the included studies.

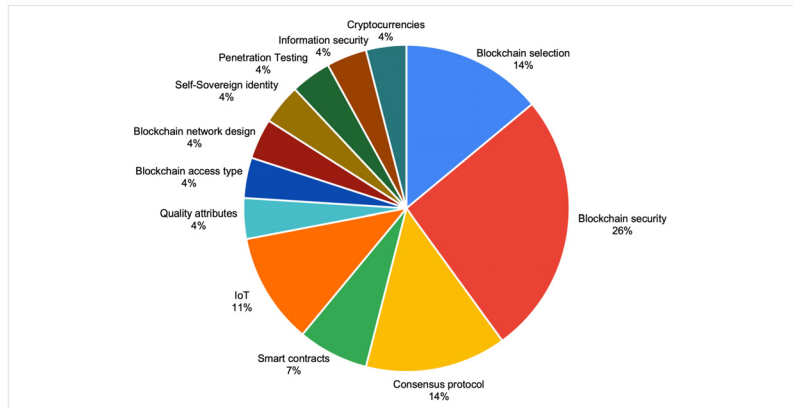


Fig. 3. Chart of focus areas of selected studies.

consensus mechanisms are both the second-most-popular areas, at 14%. The studies related to blockchain selection aim to help select a suitable blockchain platform, while the studies related to consensus mechanisms are mostly concerned with exploring multiple consensus protocols. Some studies also aim to assist decision-makers in selecting the most suitable one. IoT is the third-most-common focus area, at 11% and is mostly concerned with security issues and quality attributes related to blockchain-based IoT. Smart contracts are the fourth-most-common area, with 7%. The studies focus on a few architectural design aspects of smart contracts. The least-common areas on our list are related to quality attributes, blockchain access types, blockchain network design, self-sovereign identity, penetration testing, information security and cryptocurrencies, each accounting for 4%.

5 Analysis of the Selected Publications

The first two RQs are analysed in-depth in this section. Figure 4 depicts the classification of the selected publications and the percentage of studies per category.

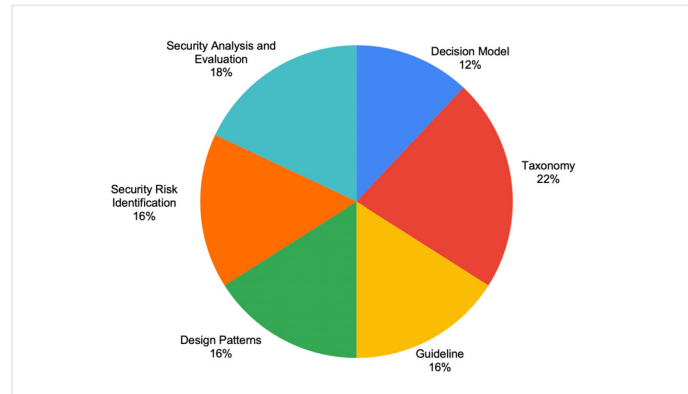


Fig. 4. Chart of the classification of selected publications.

Table 4. Categories of Secure Architectural Design Approaches

Category	Studies
Decision Model	[15, 16, 62, 63]
Taxonomy and classification	[8, 9, 20, 25, 64, 66, 71]
Guideline	[48, 50, 52, 54, 64]
Design patterns	[39, 40, 63, 65, 68]

5.1 Security Architectural Design Approaches (RQ1)

Based on our results, we broadly classify the selected studies into four commonly used approaches that support the secure architectural design of blockchain-based systems. These are (i) decision models; (ii) taxonomies; (iii) design patterns and (iv) guidelines. A representative selection of studies that belong to these categories can be found in Table 4. Since some studies contribute to multiple categories, they appear more than once in the table.

Decision Models. In our context, decision models refer to the models that support the analysis and inform architecture-related design decisions with regard to blockchain-based systems and smart contracts. One of the aims of a decision model is to link components from the problem space to their solution space counterparts. Four studies [15, 16, 62, 63] contributed to the architectural design decision model.

Farshidi et al. [15] provided a **Multi-Criteria Decision Model (MCDM)** for the blockchain platform selection problem. The authors stated that their decision model involves 121 blockchain features that can be linked to 28 blockchain platform alternatives and multiple quality attributes, including security. However, the blockchain features were briefly explained as the study focused on the methodology of building the decision model. Although the study considered security and listed a few security issues, the authors failed to analyse any of these issues and did not explicitly discuss how blockchain features are associated with security quality attributes.

Xu et al. [63] proposed a decision model that allows designers to choose suitable patterns for blockchain applications. The work provided patterns for several blockchain architectural components, including smart contracts and blockchain oracles. It proposed two security decision models, one for authentication and the other for authorisation. Several security quality attributes were considered with regard to the patterns, including integrity, availability and confidentiality. However, security issues that might arise when employing these patterns were not discussed.

Only one element of blockchain architecture was discussed in previous studies [16, 62]. Filatovas et al. [16] proposed the use of MCDM to select an appropriate consensus protocol for blockchain applications. Wüst et al. [62] provided a decision model for choosing a suitable blockchain type: permissioned or permissionless. Because neither study's main focus was security, they only discussed a few security attributes, such as integrity and availability, and mentioned some security issues.

Taxonomies. In software engineering, taxonomies help with knowledge categorisation and organisation, enabling practitioners and researchers to comprehend and analyse a complicated design space as well as assess and compare design solutions.

Xu et al. [66] proposed taxonomies of the architectural components of blockchain systems and demonstrated how these components affected system quality attributes such as performance. However, impacts on security attributes, possible attacks and their subsequent threats were missing. Attacks were classified in the study by Zhang et al. [71] based on blockchain layers: data, networks, consensus, smart contracts and applications.

Xu et al. [64] classified design decisions into blockchain decisions and application decisions and then conducted a tradeoff analysis of the related quality attributes. Their research briefly analysed security and discussed a few security attacks. Homoliak et al. [25] classified security vulnerabilities and threats in four layers: the consensus layer, the network layer, the state machine layer and the application layer. Brotsis et al. [9] only analysed blockchain architectural components that are suitable for IoT applications. The study also classified attacks based on several aspects including identity, service and manipulation.

Previous studies [8, 20] focused solely on the architectural decisions of the blockchain consensus protocols. Bouraga [8] classified 28 consensus protocols based on four criteria: origin, design, performance and security. In terms of security, they showed whether the considered consensus protocol addressed Sybil attacks, denial of service attacks, 51% attacks and eclipse attacks. Fu et al. [20] introduced three evaluation dimensions of blockchain consensus algorithms: effectiveness, decentralisation and security. The study reviewed the security design principles for resisting several attacks, including double spending attacks, Sybil attacks and eclipse attacks.

Guidelines. The guidelines refer to well-established concepts and outlines that work in practice and, as a result, offer knowledge and insights.

Staderini et al. [52] presented a guide to selecting the most appropriate type of blockchain. The proposed guidelines considered some blockchain architectural criteria, including consensus protocols and smart contracts. The study discussed a number of attacks, such as 51% attacks and mining attacks. Richard et al. [48] briefly explored smart contract architecture. The study suggested a smart contract development model that is divided into three classes in the form of the development cycle, security mechanism and development support. Several tasks were assigned to the security mechanism class, including input filtering, bug detection and vulnerability metrics. The study failed to examine or discuss any security-related issues.

Previous studies [50, 54] analysed types of blockchain; Tran et al. [54] analysed the consensus protocol, while Sargsyan et al. [50] discussed node architecture. Both studies discussed security briefly. Despite the fact that these studies claimed to provide blockchain architectural design guidelines, their proposed guidelines failed to provide a precise and clear set of steps to be followed by blockchain systems architects.

Design Patterns. These refer to repeatable solutions that can be applied to common blockchain or smart contracts' architectural design problems.

Xu et al. [65] presented security patterns that enhance the immutability, integrity and non-repudiation of blockchain systems. The study also proposed design patterns that provide solutions to common security issues related to smart contracts built on Ethereum blockchain. Two studies [40, 68] presented a catalogue of architectural solutions for blockchain-based IoT applications. Yáñez et al. [68] discussed multiple blockchain architectural elements and their related security attributes; however, the security issues of these architectural elements were not discussed. Mackenzie et al. [40] only discussed several blockchain consensus protocols for IoT application and their related attacks. In addition, Liu et al. [39] only presented and discussed design patterns for blockchain-based self-sovereign identity, and the study briefly analysed the security issues of some presented patterns.

Table 5. Blockchain Security Risk Assessment Methods

Method	Studies
Security risk identification	[6, 24, 25, 31, 51]
Security analysis and evaluation	[2, 3, 6, 25, 31, 42]

Based on our findings, there are only four industry sources that provide approaches for architecting blockchain systems and for analysing security. NIST [67] provided an overview document of blockchain technology to assist practitioners in understanding how this technology works. The document organises concepts, components, models and other elements related to blockchain technology, as well as discusses several security attacks including 51% attacks, Sybil attacks, DDoS attacks and double spending attacks. The American Council for Technology-Industry Advisory Council [19] also provided a blockchain playbook that defines a process incorporating several phases, including a technology selection phase, to help adopt the technology. In the selection phase, the playbook discusses several architectural components such as smart contracts and consensus protocols and discusses the security attributes of such components. However, both documents lack a thorough analysis of security problems that are associated with blockchain architectural components.

The European Union Agency for Cybersecurity [17] produced a report that explained several blockchain components, including consensus mechanism, smart contracts and sidechains. Their report also discussed several traditional and blockchain-specific cybersecurity issues. Finally, each issue was mapped to essential best practices to aid practitioners in developing secure blockchain systems. The report, however, is only concerned with blockchain-related challenges in the financial sector.

The German Federal Office for Information Security [18] produced a document that highlighted the security attributes of several blockchain components and discussed possible attacks that targeted each component. The document also assessed and compared the security attributes of public and private blockchains.

5.2 Blockchain Security Risk Assessment Methods (RQ2)

Based on our results, we found that the selected studies related to RQ2 contribute to blockchain risk identification, risk analysis and risk evaluation methods. Table 5 lists these studies. Some of the research helps to either identify security risks or analyse and calculate such risks. A few publications, however, have an impact on both areas, as Table 5 shows. The primary contribution of each study is described in the following paragraphs.

Security Risk Identification. We found several studies that contributed to blockchain security risk identification methods.

Homoliak et al. [25] proposed a threat-risk model that involves six elements: (i) the kind of blockchain users (owners); (ii) assets that are present at the application layer; (iii) threat agents or malicious users; (iv) threats that emerge from blockchain architectural components' vulnerabilities; (v) countermeasures; (vi) risks that are caused by threats and malicious users and lead to asset corruption or losses. However, the model fails to provide clear steps or a guide to blockchain practitioners on how to employ such a model in their system design.

In Schlatt et al. [51], the attack vectors were classified based on several blockchain architectural components, including consensus protocols, application wallets and smart contract language. The work proposed a research framework from an information security perspective to help analyse the identified attacks. Kim et al. [31] only concentrates on cryptocurrency exchange platforms. The study analyses their related vulnerabilities and provides security enhancement recommendations based on NIST and ISO/IEC 13187:2011 [27] standards. Hebert and Di Cerbo [24] proposed a partial risk assessment methodology to identify security risks in various elements of blockchain architecture. It also suggested using threat modeling methodology to analyse the identified risks. However, the evaluation and ranking of the consequences of these risks were not considered in the methodology.

Security Risk Analysis and Evaluation. We found several studies that proposed blockchain security risk analysis and/or evaluation methods.

A penetration testing framework for blockchain applications was proposed by Bhardwaj et al. [6]. The study performed penetration testing on a commercial blockchain application to identify and rank the consequences of the potential threats. However, the study only considered a few security issues that were solely related to smart contracts. Al Ketbi et al. [2] proposed blockchain security controls and their implementation guidelines to fill the gap in the existing national and international standards. The study evaluated, ranked and recommended security controls that could be implemented. However, the security attacks that were imposed as a consequence of the blockchain architectural components were not considered.

Al Mallah et al. [3] classified blockchain security threats into four categories: network threats; double spending threats; private key threats and smart contract threats. The study also assessed the threat risk impact based on the author's observations and opinions. Case studies of blockchain applications were not employed to show how to identify and assess threats in a real work example. Morganti et al. [42] proposed a cybersecurity risk assessment framework for blockchain-based smart mobility. The framework first determined the impact and probability of occurrence of each threat and then ranked the corresponding risks.

We found four industrial sources that contributed to blockchain risk assessment methods. In 2017, KPMG [32] released a white paper that investigated two specific blockchain attacks and explained how these attacks can be avoided. The paper also proposed a security framework that blockchain architects can use to identify and mitigate security risks that have arisen as a result of the use of blockchain. In 2018, KPMG [14] published another white paper that identified 10 specific blockchain risk areas and provided a five-level approach to assess the identified risks. Security attributes and issues were briefly discussed.

Deloitte provides a risk management framework that involves three risk considerations, including standard risks, value transfers and smart contracts [45]. The information security risks of blockchain wallets and smart contracts are superficially explained, as the main aim of this framework is not security. The World Economic Forum provides a toolkit that involves a five-step approach for blockchain cybersecurity risk management [43]. The risk assessment template and the guide for filling it out are also provided. The toolkit provides a risk identification checklist involving multiple risk factors. However, security issues related to blockchain architectural and design decisions were missing.

6 Discussion

Based on the results of this review, along with our observations and analysis, this section addresses the third RQ by discussing research directions that warrant further investigation and outlining specific limitations. It also explains how our proposed categorisation and classification can be leveraged to design secure blockchain applications. Finally, it highlights potential threats to the validity of our work and the measures taken to mitigate them.

6.1 An Outlook for Future Directions (RQ3)

Systematic Blockchain Secure-by-Design Approaches. According to our results, only a few studies [15, 16, 54, 62, 66] have provided systematic approaches with clear steps for the design and architecture of secure blockchain-based systems. However, security is not the focus of these studies. Security tends to be briefly discussed as an architectural quality attribute and in the context of blockchain architectural design decisions for integration.

Lack of systematic security in design approaches and security standards [46] that assist practitioners in the early stages of blockchain development may lead to catastrophic incidents, such as attacks that caused a permanent freeze of 280M USD [11] due to a design problem in smart contracts. Moreover, since blockchain-based systems contain several architectural components, each with a relatively complex internal structure, a lack of systematic methods can overcomplicate the design of secure blockchain systems and smart contracts. Therefore, researchers

need to establish comprehensive and systematic secure-by-design approaches to orchestrate decision-making and architectural design processes with respect to blockchain systems and smart contracts. This is also one of the recommendations made by Wan et al. [57], in which the authors conducted a comprehensive study to investigate how practitioners view and practice smart contract security.

Comprehensive Risk Assessment and Management in Blockchain System Architecture. As the results show, there is a lack of complete methodologies that provide a clear guide to the identification, quantification and management of security risks related to blockchain systems' architectural design decisions. The selected publications either provide partial risk assessment methods with no clear guide on how to employ them or focus only on a few security issues that relate to blockchain architectural components. Moreover, security attributes are not the focus of some publications [15, 16, 62, 66], and security is only briefly or superficially discussed. Due to the lack of methods for identifying, analysing, assessing and managing a broad set of security issues, a large percentage of blockchain projects have failed [13]. Consequently, there is an urgent need for a general framework, approaches and methodologies that address security risks in the context of blockchain architecture. This need is also highlighted in Radanliev's studies [46] and [47]. The availability of such approaches enables the architecting of blockchain systems that are secure-by-design, have manageable security risks and lower the chances of security breaches and project failure.

Systematic Approaches to Design and Implement Secure Smart Contract. There have been several initiatives in smart contract security, resulting in the definition of several vulnerabilities for smart contracts and tools for finding them. However, smart contract security is still in its early stages and many other challenges require attention, such as the security implications of design decisions in smart contracts, including programming languages and off-chain integration. Despite the number of smart contract vulnerabilities discovered by researchers [4, 11, 23, 25, 38], there is no reference classification that organises and collects security issues based on criteria such as implications, ramifications, cost of exploitation and resolution. Therefore, systematising the process of smart contract security from the early design stage, including the standards, best practices, tools and approaches, is an essential step towards designing secure smart contracts.

Many security vulnerabilities in smart contracts stem not only from design flaws, but also from implementation errors, as noted by Bhargavan et al. [7]. These implementation-level issues, such as re-entrancy bugs and improper exception handling, can lead to severe exploits, with the DAO attack of 2016 serving as a prominent example of how a re-entrancy vulnerability, introduced during implementation, resulted in catastrophic consequences. Furthermore, Atzei et al. [5] underscore that both design and implementation errors contribute to critical failures in smart contracts. In light of this, adopting systematic approaches that address both design and implementation phases are essential. Secure development practices, including formal verification, rigorous code reviews and comprehensive testing, should be integrated alongside secure design principles to provide a robust defence against potential vulnerabilities.

6.2 Demonstrating the Use of the Proposed Categorisation in Secure Blockchain Design and Risk Evaluation

When building healthcare blockchain applications, architects can make informed decisions by leveraging our proposed categorisation that assists in architecting and designing secure blockchain-based systems and smart contracts. For example, a combination of existing guidelines, decision models and risk assessment methodologies can be used to ensure robust, secure and compliant systems.

Architects can begin by consulting established guidelines to identify the most suitable blockchain technology for their specific use case. For instance, healthcare applications often require a balance between privacy, scalability and accessibility. Guidelines can help architects evaluate whether a public, private or consortium blockchain is most appropriate based on the application's requirements. In addition to guidelines, architects can leverage existing decision models to select the most appropriate design components for their healthcare blockchain

systems. Decision models provide structured frameworks to evaluate and prioritise key architectural decisions, such as choosing a consensus mechanism that balances security and performance (e.g., Proof of Authority for faster transaction speeds in private healthcare networks). For example, in the context of a healthcare application for secure data exchange, decision models can guide the integration of smart contracts to automate access control while ensuring auditability and compliance with security policies.

To further strengthen the security of healthcare blockchain applications, architects can employ established security risk analysis and assessment methodologies. These methodologies, such as STRIDE, allow architects to identify, analyse and address potential security threats during the design phase. Specifically, security risk identification involves identifying threats such as data breaches, unauthorised access or malicious smart contracts that could compromise sensitive patient information. Risk evaluation focuses on assessing the likelihood and potential impact of identified risks, enabling architects to prioritise the implementation of appropriate countermeasures. Finally, the results of the risk assessment can inform the adoption of design patterns and architectural solutions that minimise vulnerabilities, such as implementing robust cryptographic protocols or multi-factor authentication for access control.

By integrating these approaches, architects can create a comprehensive roadmap for building secure, efficient and compliant blockchain systems for healthcare.

6.3 Threats to Validity

Based on Wohlin et al. [60], we identified the following types of threats, which may affect the validity of our study.

External Validity. Although we followed a systematic approach to include studies on architecture design approaches for building secure blockchain systems and smart contracts, there is the risk of missing some papers. To mitigate this potential threat, we applied backward and forward snowballing search methods to examine additional papers; the snowballing strategy was explained in Section 3.2. Moreover, we considered the inclusion of grey literature to enhance the generalisability of the results.

Construct Validity. There are potential biases during the study selection and data extraction processes. To mitigate this threat, the authors independently worked on the process for selecting papers. Any disagreement was resolved by having a group discussion. The possibility of bias introduced during the data extraction process was reduced by ensuring that everyone reviewing the studies had a common understanding. We also made sure that the data extraction procedure matched the RQs.

Conclusion Validity. Another threat arose because we cannot guarantee the completeness of our classification of blockchain secure architectural design approaches and security risk assessment methods, as there might be additional categories that could enrich the classification. To mitigate this threat, we iteratively refined our classification each time a new concept was encountered in the literature. Nevertheless, the classification is adaptable to evolve and cope with new additions and changes.

7 Related Work

The academic community is becoming increasingly interested in problems related to blockchain technology. Unfortunately, there is still a dearth of comprehensive literature reviews that look at certain areas of software engineering, including architectural design approaches for building secure blockchain-based systems. Based on the methods employed to apply the reviews by the existing literature, we categorise them into three groups: SLRs, surveys and comprehensive reviews. The studies, their methodologies and their focus areas are listed in Table 6.

SLRs. Drljevic et al. [13] conducted an SLR that demonstrates the state of knowledge with regard to the perceived risk related to the adoption and application of blockchain technology. The study sheds light on risk definitions that are related to technology, business and project management. The connection between blockchain technology adoption and risks is also clarified. The study emphasises the importance of standards-based approaches for the

Table 6. Related Works, Their Methods and Focusing Area

Study	Methods	Focus Area
[13]	SLR	Risk management of blockchain
[70]	SLR	Blockchain topics and challenges
[56]	SLR	Smart contract applications
[1]	SLR	Architectural decisions of blockchain systems
[22]	Survey	Security issues of blockchain
[37]	Survey	Security issues of blockchain
[33]	Comprehensive review	Blockchain standards
[46]	Comprehensive review	Regulations on blockchain security risks
[47]	Comprehensive review	Financial and security risks of blockchain

Table 7. Quality Assessment

Study	Rationality			Rigour			Credibility		Total
	Empirical	Context	Objectives	Method	Data	Analysis	Results	Limitations	
[15]	1	1	1	1	1	1	1	1	8
[63]	1	1	1	1	0	1	1	1	7
[16]	1	1	1	1	1	1	1	0	7
[66]	1	1	1	1	0	1	1	0	6
[62]	1	1	1	1	0	1	1	0	6
[64]	1	1	1	1	0	1	1	0	6
[52]	0	1	1	1	0	1	0	0	4
[50]	1	1	1	1	0	1	0	0	5
[54]	1	0	1	1	0	1	1	1	6
[9]	1	1	1	1	0	1	1	0	6
[48]	0	0	1	1	1	1	0	0	4
[39]	0	1	1	1	0	1	0	0	4
[68]	1	1	1	1	1	1	1	1	8
[65]	0	1	1	1	0	1	1	0	5
[25]	1	1	1	1	1	1	1	1	8
[24]	1	1	1	1	0	1	1	0	6
[71]	0	1	1	1	0	1	1	0	5
[6]	1	1	1	1	1	1	1	0	7
[2]	1	1	1	1	0	1	1	0	6
[51]	1	1	1	1	1	1	1	1	8
[3]	1	1	1	1	0	1	1	0	6
[31]	1	1	1	1	0	1	0	0	5
[42]	0	1	1	1	0	1	1	0	5
[61]	1	1	1	1	1	1	1	0	7
[40]	0	1	1	1	0	1	0	0	4
[20]	0	1	1	0	0	1	0	0	3
[8]	1	1	1	1	1	1	1	1	8

effective adoption and application of blockchain. The study concluded that there are significant research gaps in the field of risk management with regard to the use of blockchain technology, a conclusion that is consistent with

our findings. However, in contrast to our study, security risk assessment approaches have not been investigated in this study.

In 2016, Yli-Huumo et al. [70] conducted a mapping study to investigate the available topics and challenges that were related to blockchain technology. They found most of the studies focused on Bitcoin systems, and only a few papers investigated other blockchain topics such as smart contracts. According to that study, blockchain security architectural design approaches were ignored in the considered studies. This is nearly consistent with our findings, as we found no studies investigating security architectural design methods prior to 2016, and we only found one study [64], published in 2016, which sheds light on several blockchain design decisions.

The improvement of smart contracts and decentralised application development was the focus of a systematic literature study carried out by Vacca et al. [56]. The study included the frameworks and automation tools that are employed in smart contract testing. They found that many of the currently used methods and tools only deal with particular smart contract-related problems and challenges.

In our previous study [1], we developed a taxonomy that defines and classifies the key architectural decisions regarding blockchain-based systems. This taxonomy resulted from an approach partially guided by an SLR. The review's findings indicate that the dimensions of key architectural decisions include: (i) blockchain access type; (ii) data storage and transaction computation; (iii) consensus mechanism; (iv) block configuration; (v) key management; (vi) cryptographic primitives; (vii) chain structure; (viii) node architecture and (ix) smart contracts. The study demonstrates a mapping approach that associates each dimension with potential security attacks and threats. MITRE's attack tactic categories [41] and Microsoft STRIDE threat modeling [35] classify attacks and their posed threats, respectively. However, in this study, we conducted an SLR to investigate existing architectural analyses of security approaches related to blockchain-based systems and smart contracts. Based on the findings, this study broadly classifies existing publications that contribute to providing security-by-design approaches. Additionally, the study presents a categorisation of publications that support blockchain risk assessment methods.

Surveys of Literature. Guo and Yu [22] conducted a survey on the security of blockchain technology. The study evaluated blockchain security through risk analysis to identify extensive blockchain security risk categories, examined actual attacks against the blockchain and possible defects and their underlying causes, as well as presented newly developed blockchain security countermeasures. Leng et al. [37] conducted a survey to review the state of blockchain security research. Based on the selected papers, the study classified the security of the blockchain into three levels: the process level, the data level and the infrastructure level. The study also investigated the existing solutions for addressing security issues. Studies [22] and [37] both presented an extensive review of blockchain security issues, and their reviews can be used to support the building of secure blockchain systems. However, security design issues and security risk assessment methodologies, which assist in avoiding security problems at the early stages, have not been investigated in these studies.

Comprehensive Reviews. König et al. [33] provided a comparative analysis of 19 blockchain standards published by organisations that work and focus on information security. Security management and technical security are among the criteria that are used to compare the content of the standards. The study, however, only considered organisational standards in the comparison and excluded other types of grey literature such as white papers and industrial reports. They also ignored academic literature, which can also aid in the adoption of reliable and secure blockchain technology.

The study of Radanliev [46] employs a review and case study approach, analysing secondary data on cybersecurity. Its significance lies in integrating knowledge from the United States, European Union, United Kingdom and international cybersecurity standards, applying this to new blockchain projects. The findings highlight that cybersecurity standards are not developed in close collaboration between the US and EU, despite the US leading in the field. Moreover, the security standards for cryptocurrencies, IoT and blockchain technologies have not kept pace with the rapid technological advancements. A key insight from the research is that while the crypto market has grown into a multi-trillion-dollar industry, it has also experienced over a 70% decline from its peak, leading

to significant financial losses. Despite these impacts, both cybersecurity standards and financial regulations for blockchain remain underdeveloped.

In 2024, Radanliev [47] provides a comprehensive exploration of financial and cybersecurity risks associated with blockchain technologies, particularly within the context of the Metaverse. It emphasises the growing cybersecurity risks in the context of blockchain, especially within cryptocurrency trading. Additionally, the research addresses the prevalence of fraudulent blockchain ventures, such as Ponzi schemes and the significant risks these pose to individual investors. By reassessing traditional financial risk assessment methods, the study offers new insights into evaluating the long-term viability of blockchain projects. Ultimately, the research underscores the importance of robust risk assessment frameworks to mitigate financial and cybersecurity threats in both developed and developing economies, as blockchain technologies continue to evolve and expand in practical applications.

While the three studies mentioned support our finding regarding the lack of security standards and risk assessment frameworks, to the best of our knowledge, our work is the first to explore and categorise current architectural design approaches and security risk assessment methods for building secure-by-design blockchain-based systems. This distinguishes our research from previous efforts.

7.1 Unique Contributions and Advancements in Blockchain Security Research

This study offers a distinctive perspective and novel contributions that differentiate it from prior research in the field of blockchain security and architectural design. While earlier works, such as those by Drljevic et al. [13], Yli-Huumo et al. [70] and Vacca et al. [56], primarily focused on specific challenges like blockchain adoption risks, smart contract testing or broader blockchain topics, they lack a comprehensive exploration of security-by-design methodologies. Similarly, surveys by Guo and Yu [22] and Leng et al. [37] provided valuable insights into blockchain security risks but fell short in addressing early-stage security design and risk assessment frameworks. Comprehensive reviews, such as those by König et al. [33] and Radanliev [46] and [47], were often constrained to specific standards or geographical insights, overlooking the integration of security principles into blockchain architectures.

In contrast, this study is groundbreaking in systematically investigating and categorising both architectural design approaches and security risk assessment methodologies specifically tailored for secure blockchain systems. By building upon a taxonomy of key architectural decisions from prior work [1], this research connects these decisions with potential security threats, employing well-established models such as MITRE's attack tactic categories and Microsoft's STRIDE framework.

Moreover, this study provides a clear classification of existing publications into security-by-design approaches and risk assessment frameworks, offering actionable guidance for researchers and practitioners. This dual focus on design principles and risk management fills a critical gap in the literature, providing a foundation for developing resilient and secure blockchain systems. These contributions ensure that this research stands apart as both a reference point for academics and a practical guide for industry stakeholders.

8 Summary and Conclusions

This article presented an SLR to investigate current approaches and methods that assist in architecting and designing secure blockchain-based systems and smart contracts. We selected 27 academic studies and 6 industrial reports that satisfied the defined inclusion criteria. We found that the approaches provided by a set of selected studies can be classified into four categories: (i) decision models; (ii) taxonomies; (iii) design patterns and (iv) guidelines. The other set of selected studies contributed to several security risk assessment phases: (i) security risk identification and/or (ii) security risk analysis and evaluation.

We argued that the development of secure blockchain systems requires leveraging security architectural design approaches. However, based on our review results, we found there is a lack of systematic security architectural-centric approaches, security standards and complete security risk assessment methodology. We concluded that

there is a critical need for a generic framework, methods and approaches that handle security risks in the context of blockchain architecture at the early architectural and design stages. Additionally, we also advocated the need for international standards and frameworks on regulatory oversight for value-oriented risks in blockchain-based applications.

In this article, we presented several research directions that deserve further investigation in the field of security architectural design decisions for blockchain systems and smart contracts. These are as follows: (i) a systematic approach to assist architects in making secure architecture design and configuration decisions for blockchain-based systems; (ii) an approach for assessing smart contracts' security risks and (iii) a decision support model for blockchain oracle platform selection.

References

- [1] Sabreen Ahmadjee, Carlos Mera-Gómez, Rami Bahsoon, and Rick Kazman. 2022. A study on blockchain architecture design decisions and their security attacks and threats. *ACM Transactions on Software Engineering and Methodology* 31, 2, Article 36e (April 2022), 45 pages.
- [2] Maitha Al Ketbi, Khaled Shuaib, Ezedin Barka, and Marton Gergely. 2021. Establishing a security control framework for blockchain technology. *Interdisciplinary Journal of Information, Knowledge, and Management* 16 (2021), 307.
- [3] Ranwa Al Mallah, David López, and Bilal Farooq. 2021. Cyber-security risk assessment framework for blockchains in smart mobility. *IEEE Open Journal of Intelligent Transportation Systems* 2 (2021), 294–311.
- [4] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. 2016. A survey of attacks on Ethereum smart contracts. *IACR Cryptology ePrint Archive* 2016 (2016), 1007.
- [5] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. 2017. A survey of attacks on Ethereum smart contracts (SoK). In *Proceedings of the 6th International Conference on Principles of Security and Trust (POST '17), Held as Part of the European Joint Conferences on Theory and Practice of Software (ETAPS '17)*. Springer, 164–186.
- [6] Akashdeep Bhardwaj, Syed Bilal Hussian Shah, Achyut Shankar, Mamoun Alazab, Manoj Kumar, and Thippa Reddy Gadekallu. 2021. Penetration testing framework for smart contract blockchain. *Peer-to-Peer Networking and Applications* 14, 5 (2021), 2635–2650.
- [7] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova, Aseem Rastogi, Thomas Sibut-Pinote, Nikhil Swamy, et al. 2016. Formal verification of smart contracts: Short paper. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, 91–96.
- [8] Sarah Bouraga. 2021. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications* 168 (2021), 114384.
- [9] Sotirios Brotsis, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, and Stavros Shiaeles. 2021. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Computer Networks* 191 (2021), 108005.
- [10] Neelam Chauhan and Rajendra Kumar Dwivedi. 2022. A secure design of the healthcare IoT system using blockchain technology. In *Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 704–709.
- [11] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys* 53, 3 (2020), 1–43.
- [12] Deloitte. 2022. Risk Advisory. Retrieved from https://www2.deloitte.com/uk/en/services/risk-advisory.html?icid=top_risk-advisory
- [13] Nusi Drljevic, Daniel Arias Aranda, and Vladimir Stantchev. 2020. Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards & Interfaces* 69 (2020), 103409.
- [14] Dennis de Vries, Eamonn Maguire, Kiran Nagaraj. 2018. Realizing Blockchain's Potential. Retrieved from <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/realizing-blockchains-potential.pdf>
- [15] Siamak Farshidi, Slinger Jansen, Sergio España, and Jacco Verkleij. 2020. Decision support for blockchain platform selection: Three industry case studies. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1109–1128.
- [16] Ernestas Filatovas, Marco Marcozzi, Leonardo Mostarda, and Remigijus Paulavičius. 2022. A MCDM-based framework for blockchain consensus protocol selection. *Expert Systems with Applications* 204 (2022), 117609.
- [17] European Union Agency for Cybersecurity. 2017. Distributed Ledger Technology & Cybersecurity—Improving Information Security in the Financial Sector. Retrieved from <https://www.enisa.europa.eu/publications/blockchain-security>
- [18] German Federal Office for Information Security: Bonn. 2019. Towards Secure Blockchains. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.html
- [19] American Council for Technology-Industry Advisory Council. 2021. Blockchain Playbook Online—Beta. Retrieved from <https://rb.gy/g5ci8e>
- [20] Xiang Fu, Huaimin Wang, and Peichang Shi. 2021. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Science China Information Sciences* 64, 2 (2021), 1–15.

- [21] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. 2015. The bitcoin backbone protocol: Analysis and applications. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 281–310.
- [22] Huaqun Guo and Xingjie Yu. 2022. A survey on blockchain technology and its security. *Blockchain: Research and Applications* 3, 2 (2022), 100067.
- [23] Huru Hasanova, Ui-jun Baek, Mu-gon Shin, Kyunghee Cho, and Myung-Sup Kim. 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management* 29, 2 (2019), e2060.
- [24] Cédric Hebert and Francesco Di Cerbo. 2019. Secure blockchain in the enterprise: A methodology. *Pervasive and Mobile Computing* 59 (2019), 101038.
- [25] Ivan Homoliak, Sarad Venugopalan, Daniël Reijsbergen, Qingze Hum, Richard Schumi, and Pawel Szalachowski. 2020. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys & Tutorials* 23, 1 (2020), 341–390.
- [26] Xin Huang, He Zhang, Xin Zhou, Muhammad Ali Babar, and Song Yang. 2018. Synthesizing qualitative research in software engineering: A critical review. In *Proceedings of the 40th International Conference on Software Engineering (ICSE '18)*. ACM, New York, NY, 1207–1218.
- [27] IEC. 2011. *Information Technology—Server Management Command Line Protocol*. ISO. Retrieved March 23, 2022 from <https://www.iso.org/standard/53458.html>
- [28] ISO/IEC. 2018. ISO 31000:2018 Risk Management—Guidelines. Retrieved from <https://www.iso.org/standard/65694.html>
- [29] ISO/IEC. 2022. ISO/IEC 27001:2022 Information Security Management Systems. Retrieved from <https://www.iso.org/standard/27001>
- [30] Staffs Keele. 2007. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
- [31] Chang Yeon Kim and Kyungho Lee. 2018. Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats. In *Proceedings of the 2018 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 1–6.
- [32] Eamonn Maguire and Kiran Nagaraj. 2017. Securing the Chain. Retrieved from <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/05/securing-the-chain.pdf>
- [33] Lukas König, Yuliia Korobeinikova, Simon Tjoa, and Peter Kieseberg. 2020. Comparing blockchain standards and recommendations. *Future Internet* 12, 12 (2020), 222.
- [34] KPMG. 2022. KPMG. Retrieved from <https://home.kpmg/xx/en/home.html>
- [35] David LeBlanc and Michael Howard. 2002. *Writing Secure Code*. Pearson Education.
- [36] Ledger. 2020. E-commerce and Marketing Data Breach. Retrieved from <https://bit.ly/2WI33EC>
- [37] Jiewu Leng, Man Zhou, J. Leon Zhao, Yongfeng Huang, and Yiyang Bian. 2022. Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing* 15, 4 (2022), 2490–2510.
- [38] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020), 841–853.
- [39] Yue Liu, Qinghua Lu, Hye-Young Paik, and Xiwei Xu. 2020. Design patterns for blockchain-based self-sovereign identity. In *Proceedings of the European Conference on Pattern Languages of Programs 2020*, 1–14.
- [40] Beverley Mackenzie, Robert Ian Ferguson, and Xavier Bellekens. 2018. An assessment of blockchain consensus protocols for the Internet of Things. In *Proceedings of the 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*. IEEE, 183–190.
- [41] MITRE. 2018. MITRE ATT&CK. Retrieved from <https://attack.mitre.org/>
- [42] Giacomo Morganti, Enrico Schiavone, and Andrea Bondavalli. 2018. Risk assessment of blockchain technology. In *Proceedings of the 2018 8th Latin-American Symposium on Dependable Computing (LADC)*. IEEE, 87–96.
- [43] Francis Jee Nadia Hewett, Sumedha Deshmukh. 2020. Cybersecurity. Retrieved from <https://widgets.weforum.org/blockchain-toolkit/cybersecurity>
- [44] NIST. 2022. Standards & Measurements. Retrieved from <https://www.nist.gov/>
- [45] Abhishek Biswas Prakash Santhana. 2017. Blockchain Risk Management Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf>
- [46] Petar Radanliev. 2023. Review and comparison of US, EU, and UK regulations on cyber risk/security of the current blockchain technologies: Viewpoint from 2023. *The Review of Socionetwork Strategies* 17, 2 (2023), 105–129.
- [47] Petar Radanliev. 2024. The rise and fall of cryptocurrencies: Defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. *Financial Innovation* 10, 1 (2024), 1.
- [48] Richard, Harjanto Prabowo, Agung Trisetyarso, and Benfano Soewito. 2020. Smart contract development model and the future of blockchain technology. In *Proceedings of the 2020 the 3rd International Conference on Blockchain Technology and Applications*, 34–39.
- [49] Joanna C. S. Santos, Katy Tarrit, and Mehdi Mirakhorli. 2017. A catalog of security architecture weaknesses. In *Proceedings of the 2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*. IEEE, 220–223.
- [50] Gohar Sargsyan, Nicolas Castellon, Raymond Binnendijk, and Peter Cozijnsen. 2019. Blockchain security by design framework for trust and adoption in IoT environment. In *Proceedings of the 2019 IEEE World Congress on Services (SERVICES)*, Vol. 2642. IEEE, 15–20.

- [51] Vincent Schlatt, Tobias Guggenberger, Jonathan Schmid, and Nils Urbach. 2022. Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International Journal of Information Management* (2022), 102470.
- [52] Mirko Staderini, Enrico Schiavone, and Andrea Bondavalli. 2018. A requirements-driven methodology for the proper selection and configuration of blockchains. In *Proceedings of the 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 201–206.
- [53] Stephanie. 2014. *What is Cohen's Kappa Statistic?* Statistics How To. Retrieved May 16, 2022 from <https://www.statisticshowto.com/cohens-kappa-statistic/>
- [54] Nguyen Khoi Tran and M. Ali Babar. 2020. Anatomy, concept, and design space of blockchain networks. In *Proceedings of the 2020 IEEE International Conference on Software Architecture (ICSA)*. IEEE, 125–134.
- [55] Petar Tsankov, Andrei Dan, Dana Drachler-Cohen, Arthur Gervais, Florian Bünzli, and Martin Vechev. 2018. Securify: Practical security analysis of smart contracts. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*. ACM, New York, NY, 67–82.
- [56] Anna Vacca, Andrea Di Sorbo, Corrado A. Visaggio, and Gerardo Canfora. 2021. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software* 174 (2021), 110891.
- [57] Zhiyuan Wan, Xin Xia, David Lo, Jiachi Chen, Xiapu Luo, and Xiaohu Yang. 2021. Smart contract security: A practitioners' perspective. In *Proceedings of the 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, 1410–1422.
- [58] Shuai Wang, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han, and Fei-Yue Wang. 2019. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, 11 (2019), 2266–2277.
- [59] Claes Wohlin. 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14)*. ACM, New York, NY, Article 38, 10 pages.
- [60] Claes Wohlin, Per Runeson, Martin Höst, Magnus C. Ohlsson, Björn Regnell, and Anders Wesslén. 2012. *Experimentation in Software Engineering*. Springer Science & Business Media.
- [61] Maximilian Wohrer and Uwe Zdun. 2018. Smart contracts: Security patterns in the Ethereum ecosystem and solidity. In *Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE, 2–8.
- [62] Karl Wüst and Arthur Gervais. 2018. Do you need a blockchain? In *Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 45–54.
- [63] Xiwei Xu, HMN Dilum Bandara, Qinghua Lu, Ingo Weber, Len Bass, and Liming Zhu. 2021. A decision model for choosing patterns in blockchain-based applications. In *Proceedings of the 2021 IEEE 18th International Conference on Software Architecture (ICSA)*. IEEE, 47–57.
- [64] Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran, and Shiping Chen. 2016. The blockchain as a software connector. In *Proceedings of the 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. IEEE, 182–191.
- [65] Xiwei Xu, Cesare Pautasso, Liming Zhu, Qinghua Lu, and Ingo Weber. 2018. A pattern collection for blockchain-based applications. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs (EuroPLoP '18)*. ACM, New York, NY, Article 3, 20 pages.
- [66] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. 2017. A taxonomy of blockchain-based systems for architecture design. In *Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA)*. IEEE, 243–252.
- [67] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. 2019. Blockchain technology overview. arXiv:1906.11078. Retrieved from <https://arxiv.org/abs/1906.11078>
- [68] Wendy Yáñez, Rami Bahsoon, Yuqun Zhang, and Rick Kazman. 2021. Architecting Internet of Things systems with blockchain: A catalog of tactics. *ACM Transactions on Software Engineering and Methodology* 30, 3, Article 35 (April 2021), 46 pages.
- [69] Lanxin Yang, He Zhang, Haifeng Shen, Xin Huang, Xin Zhou, Guoping Rong, and Dong Shao. 2021. Quality assessment in systematic literature reviews: A software engineering perspective. *Information and Software Technology* 130 (2021), 106397.
- [70] Jesse Yli-Huumo, Deokyoong Ko, Sujin Choi, Sooyong Park, and Kari Smolander. 2016. Where is current research on blockchain technology?—A systematic review. *PLoS One* 11, 10 (2016), e0163477.
- [71] Peiyun Zhang and Mengchu Zhou. 2020. Security and trust in blockchains: Architecture, key technologies, and open issues. *IEEE Transactions on Computational Social Systems* 7, 3 (2020), 790–801.

Received 5 March 2024; revised 29 December 2024; accepted 29 December 2024