

# A framework for security risk assessment of blockchain-based applications

Mohammad Qatawneh<sup>1,2</sup>

<sup>1</sup>Department of Computer Science, KASIT, University of Jordan, Amman, Jordan

<sup>2</sup>Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan

## Article Info

### Article history:

Received Dec 6, 2024

Revised Mar 17, 2025

Accepted Mar 26, 2025

### Keywords:

Blockchain

Blockchain security model

Blockchain-based applications

Security risk assessment

Vulnerability

## ABSTRACT

Blockchain technology has revolutionized various industries by enabling decentralized, transparent, and tamper-resistant digital transactions. However, despite its benefits, blockchain-based applications are vulnerable to security threats such as smart contract exploits, 51% attacks, Sybil attacks, and private key compromises, posing significant risks to their integrity and reliability. Traditional security frameworks lack a comprehensive approach to systematically assess and mitigate these risks across different blockchain layers. To address this challenge, this paper proposes the blockchain cybersecurity risk assessment model (BCRAM), a structured framework designed to identify, analyze, evaluate, and mitigate security risks in blockchain systems. The methodology involves categorizing threats, assessing risks using quantitative and qualitative techniques, and validating the model through a case study on Ethereum. Results demonstrate that implementing BCRAM led to a 65% reduction in smart contract exploits, a 70% decrease in phishing incidents, and an 85% improvement in distributed denial of service (DDoS) resilience, proving its effectiveness. This research offers a standardized risk assessment approach, providing valuable insights for developers, security analysts to enhance blockchain security.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Mohammad Qatawneh

Department of Computer Science, KASIT, University of Jordan

Amman, 11942, Jordan

Email: mohd.qat@ju.edu.jo

## 1. INTRODUCTION

Blockchain technology has revolutionized industries such as finance, healthcare, supply chain, e-voting, and e-learning by providing a decentralized, immutable, and secure means of data storage and transaction processing [1]-[6]. Its tamper-resistant nature has made it an essential tool for enhancing transparency, reducing fraud, and improving operational efficiency [7], [8]. However, despite its benefits, blockchain systems face numerous security threats that can undermine their reliability and trustworthiness. These threats include smart contract vulnerabilities, 51% attacks, private key theft, Sybil attacks, and consensus mechanism flaws, which pose serious risks to the confidentiality, integrity, and availability of blockchain-based applications [9]-[11].

To mitigate these security risks, researchers have proposed various solutions, including formal verification of smart contracts [12], enhanced cryptographic techniques [13], secure consensus mechanisms [14], and AI-driven anomaly detection systems [15], [16]. However, these solutions often focus on specific security threats rather than providing a comprehensive risk assessment framework that systematically identifies, evaluates, and mitigates risks across all layers of the blockchain architecture [17]. Moreover, existing blockchain security frameworks (BSF), such as NISTIR 8202, open web application security project (OWASP)

top ten, and BRAM, lack standardized risk assessment methodologies, making it difficult for organizations to assess and manage blockchain-related risks effectively [18]-[20].

To address these challenges, this paper introduces the blockchain cybersecurity risk assessment model (BCRAM), a structured framework designed to analyze and quantify security risks in blockchain-based applications. This model integrates qualitative and quantitative risk assessment techniques, considers attack vectors across different blockchain layers (network, consensus, and application), and provides actionable security measures. Unlike existing models, BCRAM offers a holistic approach to blockchain risk assessment, making it suitable for real-world applications such as financial transactions, decentralized identity management, and supply chain security [21]-[26]. The contributions of this paper are as follows:

- Identify and categorize blockchain security threats across different layers.
- Develop a structured risk assessment model (BCRAM) tailored for blockchain security challenges.
- Compare BCRAM with existing security models to evaluate its effectiveness.
- Validate the proposed model through a case study on Ethereum, demonstrating its ability to enhance security in a real-world blockchain application.

By addressing the gaps in existing security frameworks, this research aims to enhance blockchain security resilience, reduce vulnerabilities, and provide a standardized approach to blockchain risk management. The findings of this paper will benefit blockchain developers, cybersecurity experts, and policymakers by offering a practical and scalable risk assessment model that strengthens the security of blockchain-based ecosystems.

The organization of the paper is as follows: Section 2 presents the methodology, which includes an overview of existing risk assessment models for blockchain, types of attacks at different blockchain layers, proposed model, the design of the experiment, and the results and discussion. Section 3 presents the result and discussion. Section 4 provides the comparative analysis of blockchain risk assessment models. Finally, the conclusion of the paper is presented in section 5.

## 2. METHOD

There are various risk assessment models specifically designed for blockchain applications. These models address the unique risks associated with blockchain technology, including vulnerabilities in smart contracts, consensus mechanisms, and decentralized finance (DeFi) systems. Several risk assessment models will be discussed, including a brief description of each, followed by a comparison table that highlights their key features, advantages, and drawbacks.

### 2.1. Existing risk assessment models for BC

#### A. Blockchain security framework (BSF)

The BSF provides a structured methodology for identifying and mitigating security risks inherent to blockchain technology [27], [28]. This framework emphasizes the importance of mapping security controls to specific vulnerabilities within blockchain environments. It offers comprehensive guidelines for risk management throughout the entire blockchain lifecycle, ensuring that organizations can proactively address potential threats. Additionally, the BSF includes governance structures designed to enhance accountability and oversight within blockchain operations, facilitating a more secure implementation of this technology.

One of the key advantages of the BSF is its thorough coverage of various security aspects related to blockchain, which allows organizations to integrate robust security practices directly into their development processes. By doing so, organizations can create a more resilient infrastructure that responds effectively to emerging risks. However, implementing the BSF can be complex, particularly for organizations that may lack the necessary cybersecurity expertise. Moreover, the framework may need to be adapted for different blockchain platforms, which can add to the complexity of its application across diverse use cases.

#### B. OWASP blockchain top ten risks

The OWASP has identified the top ten risks associated with blockchain technology, such as injection, broken access control, broken authentication, security misconfiguration, and others [29], [30], creating a vital model for developers and organizations to understand and address critical vulnerabilities in their blockchain applications. This framework provides a clear identification of significant risks, such as 51% attacks and improper key management, and offers guidance on how to mitigate these threats effectively. Additionally, it raises awareness about the various security challenges unique to blockchain, helping stakeholders to better comprehend the landscape of potential vulnerabilities.

One of the primary advantages of the OWASP framework is its accessibility; it is designed to be easily understood by organizations of all sizes, allowing them to prioritize their security efforts effectively. By focusing on the most critical risks, OWASP helps organizations allocate resources efficiently to address the most pressing vulnerabilities. However, the model does have some limitations, as it may not provide in-

depth solutions for every identified risk. Furthermore, there is a possibility that some risks could be overlooked if they do not make the top ten list, which may lead to gaps in an organization's overall security strategy.

#### C. Security reference architecture (SRS)

The SRS is designed to evaluate and quantify the risks associated with blockchain implementations, utilizing a combination of qualitative and quantitative methodologies [31]. This model emphasizes risk quantification through specific metrics, enabling organizations to gain a clearer understanding of their risk landscape. SRS also includes comprehensive threat and vulnerability analysis that is particularly relevant to blockchain environments, ensuring that all aspects of risk are considered. Additionally, it adopts a Comprehensive view that takes into account business processes and compliance requirements, making it suitable for organizations operating within regulated industries.

One of the key advantages of the SRS is its ability to blend qualitative and quantitative analyses, resulting in a balanced and thorough risk assessment approach. By providing concrete risk metrics, the model facilitates informed decision-making, allowing organizations to prioritize and address their security concerns effectively. However, implementing the SRS can be resource-intensive, requiring specialized knowledge that may not be readily available within all organizations. Moreover, as blockchain technology continues to evolve, ongoing adjustments and updates to the risk assessment model will be necessary to ensure its continued relevance and effectiveness in mitigating emerging risks.

#### D. Risk assessment framework for smart contracts (RAFS)

The RAFS is specifically designed to evaluate the security and reliability of smart contracts, highlighting the unique risks involved in coding and executing these programs on blockchain platforms [32]. This framework employs systematic code reviews to identify potential vulnerabilities within smart contracts, ensuring that security flaws are addressed before deployment. It also incorporates extensive testing methodologies, including formal verification techniques, to provide rigorous assurance of a smart contract's functionality and safety. Furthermore, RAFS takes into account operational risk considerations, offering a comprehensive view of the risks present in smart contract environments.

One of the primary advantages of RAFS is its comprehensive approach to smart contracts, allowing it to directly address their specific vulnerabilities. By promoting best practices in the development and deployment of smart contracts, the framework helps developers create more secure and reliable applications. However, the narrow focus on smart contracts means that RAFS may overlook broader blockchain risks that could impact overall system security. Additionally, the complexity involved in testing and verifying smart contracts can pose significant barriers for developers, particularly those who may lack the necessary expertise or resources to implement rigorous security assessments effectively.

#### E. Enterprise risk management (ERM) for blockchain:

ERM frameworks can be customized for blockchain applications by integrating blockchain-specific risks into traditional ERM practices, offering a unified view of risks across the organization [33]. This approach aligns blockchain risk assessments with overall business objectives, ensuring that blockchain initiatives are evaluated in conjunction with other enterprise goals. ERM for blockchain also adopts a comprehensive perspective, encompassing various types of risks, such as operational and compliance risks, and emphasizes the importance of continuous monitoring to keep pace with the evolving risk landscape.

One of the main advantages of applying ERM to blockchain is that it situates blockchain risks within the broader context of enterprise risk, promoting a proactive stance on emerging threats. This integration helps organizations manage blockchain risks alongside other critical risks, providing a balanced approach to risk mitigation. However, this broad approach may dilute the focus on blockchain-specific risks if not managed carefully. Additionally, implementing an ERM framework for blockchain requires a mature understanding of ERM principles, which may be challenging for organizations that lack experience in comprehensive risk management.

The risk assessment models listed above provide various frameworks for identifying, evaluating, and mitigating risks specific to blockchain technology. Organizations can choose a model based on their specific needs, existing capabilities, and the complexity of their blockchain applications. By understanding the strengths and weaknesses of each model, organizations can enhance their security posture and ensure the reliability of their blockchain implementations as the technology continues to evolve. Each model has its unique focus, allowing for comprehensive approaches to risk management in diverse blockchain environments as shown in Table 1.

Although the aforementioned frameworks provide fundamental insights, they overlook the layered structure of blockchain—comprising the network, consensus, and application layers. To address this limitation, it is essential to understand the types of attacks targeting each layer, enabling the proposal of a comprehensive risk assessment model for the entire blockchain stack.

Table 1. Comparison between different risk assessment models for blockchain applications

Model	Key features	Advantages	Drawbacks
Blockchain Security Framework (BSF).	Security controls mapping, risk management guidelines.	Comprehensive coverage, integrates security practices.	Complex implementation for less experienced organizations.
OWASP Blockchain Top Ten Risks.	Identification of top risks, mitigation guidance.	Accessible framework, prioritizes critical risks.	Limited solutions for risks outside the top ten.
Security Reference Architecture (SRS).	Risk quantification, comprehensive view.	Balanced qualitative and quantitative analyses.	Resource-intensive, requires specialized knowledge.
Risk Assessment Framework for Smart Contracts (RAFS).	Code review, testing and verification.	Comprehensive for smart contracts, promotes best practices.	Narrow focus, complexity of testing.
Enterprise Risk Management (ERM) for Blockchain.	Alignment with business objectives, continuous monitoring.	Comprehensive risk perspective, proactive management.	Risk dilution if not carefully managed, requires ERM knowledge.

## 2.2. Types of attacks at different blockchain layers

Blockchain technology is built upon a multi-layered architecture that includes the network layer, consensus layer, smart contract layer, and application layer, each of which serves distinct functions and presents unique vulnerabilities [34], [35]. The network layer is responsible for peer-to-peer communication and transaction propagation, but it can be susceptible to attacks such as:

- Sybil attacks: Attackers create multiple identities to influence consensus, which can lead to double-spending or transaction manipulation [36].
- Eclipse attacks: Isolating nodes from the network allows attackers to control the flow of information, leading to delayed or invalid transactions [29].
- Distributed denial of service (DDoS): A high volume of transactions overwhelms the network, disrupting blockchain operations [30].

The consensus layer, which ensures agreement among distributed nodes, faces risks like:

- 51% attacks: If an attacker gains control over 51% of the network's mining or staking power, they can alter transaction history and double-spend assets [31].
- Selfish mining: Malicious miners keep mined blocks private, gaining an advantage by selectively publishing them [32].
- Nothing-at-stake problem: In proof-of-stake (PoS) systems, validators might support multiple chains, leading to potential forks and instability [33].

At the smart contract layer, where self-executing contracts are deployed, vulnerabilities such as:

- Reentrancy attacks: Allow an attacker to drain funds by repeatedly calling a contract function before it updates [37].
- Integer overflow/underflow: Errors in handling numerical values can lead to loss of assets [27].
- Unchecked call return values: If a contract does not verify call success, it may continue with erroneous data, risking unintended results [36].

Finally, the application layer, which interacts with end-users, is at risk like:

- Front-running attacks: Attackers observe pending transactions and execute profitable trades ahead of them [37].
- Oracle manipulation: External data oracles can be tampered with, leading to false data being fed into the blockchain [38].
- Privacy risks: Blockchain's transparency can compromise data confidentiality, particularly for sensitive information [39].

Understanding these layers and their associated threats is crucial for developing effective security measures and risk management strategies in blockchain systems.

## 2.3. Proposed model

This section introduces a new BCRA, designed to address the specific security challenges faced by blockchain applications. As blockchain technology continues to evolve and integrate into various sectors, it becomes increasingly critical to understand the risks associated with its use. BCRA is designed to provide a systematic and comprehensive approach to identifying, assessing, and mitigating these risks across multiple layers of blockchain architecture. The proposed BCRA comprises the following four phases, as shown in Figure 1.

- Risk identification: The first stage of BCRA involves a thorough identification of potential vulnerabilities across all layers of the blockchain—network, consensus, smart contract, and application layers. Utilizing a threat matrix based on historical data, threat intelligence, and known vulnerabilities, BCRA enables organizations to pinpoint specific risks associated with their blockchain implementations. This process involves engaging with various stakeholders, including developers,

- security analysts, and system administrators, to gather insights and ensure a comprehensive understanding of the system architecture and operational context.
- b) **Risk scoring:** After identifying risks, each potential vulnerability is assigned a score based on its likelihood of occurrence and potential impact on the organization. This quantitative assessment allows for the prioritization of high-risk vulnerabilities that require immediate attention. BCRAM employs a scoring rubric that factors in various elements such as the exploitability of a vulnerability, the potential financial loss associated with an exploit, and the criticality of the affected system components. By converting qualitative risks into quantitative metrics, organizations can make informed decisions about where to allocate resources for risk mitigation.
  - c) **Impact analysis:** This stage evaluates the consequences of each identified risk on the core attributes of the blockchain system: confidentiality, integrity, and availability (CIA triad). By analyzing the impact of each risk, organizations can better understand the potential ramifications of security breaches, including data loss, reputational damage, and legal repercussions. Impact analysis not only helps in understanding the significance of risks but also aids in developing effective communication strategies for stakeholders, ensuring that they are aware of the risks involved in blockchain operations.
  - d) **Mitigation strategies:** For each high-priority risk identified through the previous stages, BCRAM facilitates the development of comprehensive mitigation plans. These strategies incorporate both preventive measures—such as enhanced encryption protocols, regular audits, and robust access controls—and reactive measures that prepare organizations for potential incidents, including incident response plans and recovery protocols. The flexibility of BCRAM allows organizations to adapt their mitigation strategies based on the specific context of their blockchain applications, enabling a more personalized approach to security.

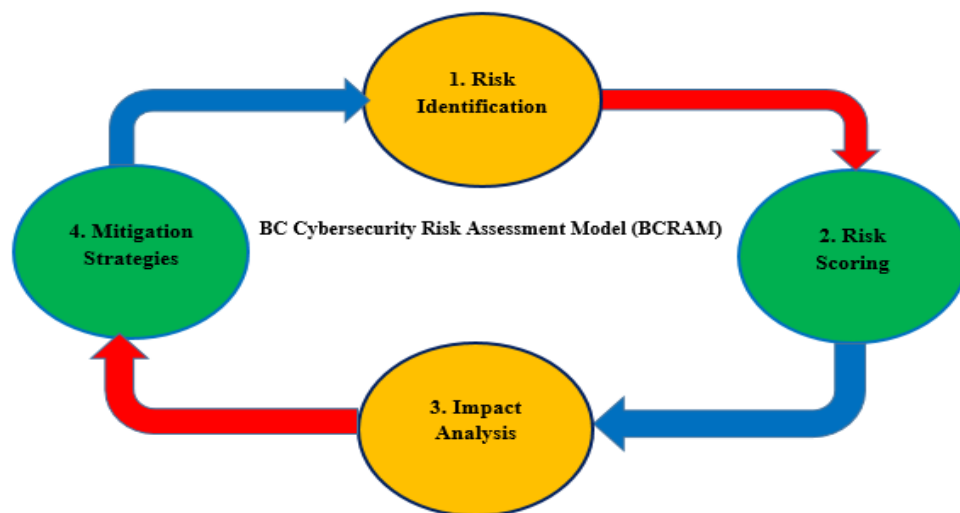


Figure 1. The Proposed BCRAM

The proposed BCRAM operates as a cyclical process, ensuring that risk management is an ongoing effort rather than a one-time assessment. The model begins with an initial risk assessment, followed by continuous monitoring and reevaluation of risks as the blockchain environment evolves. The steps in the BCRAM process can be summarized as follows:

- a) **Initial Risk Assessment:** Conduct a comprehensive review of the blockchain architecture, identify potential vulnerabilities, and score these risks based on likelihood and impact.
- b) **Continuous Monitoring:** Implement tools and processes for ongoing monitoring of the blockchain network, including transaction auditing and anomaly detection, to identify new risks as they arise.
- c) **Regular Reassessments:** Periodically revisit the risk identification and scoring processes to ensure that the risk landscape remains current, especially in light of software updates, protocol changes, or new threats.
- d) **Feedback Loop:** Utilize insights gained from incident responses and audits to refine risk assessments and mitigation strategies, fostering a culture of continuous improvement in blockchain security.

### 2.3.1. Design of experiment

This section explains a case study that applies the BCRAM to the Ethereum blockchain, demonstrating how security risks are identified, analyzed, scored, and mitigated. Ethereum was chosen due to its widespread adoption and use of smart contracts, which introduce unique security challenges. The risk identification process using the BCRAM model assessed potential vulnerabilities in the Ethereum blockchain across different layers:

- Network layer: Risks include DDoS attacks and Sybil attacks. In 2016, an Ethereum-based attack exploited peer-to-peer network vulnerabilities, causing congestion and service disruption [40].
- Consensus layer: Risks involve 51% attacks, double spending, and finality delays. The ethereum Classic 51% attack in 2020 resulted in approximately 5.6 million of dollars in fraudulent transactions [40].
- Application layer: Smart contract vulnerabilities, such as reentrancy attacks and logic flaws, are key concerns. The 2021 front-running exploit on Ethereum DeFi platforms resulted in millions of dollars in losses due to manipulated transaction ordering.
- Smart contract layer: Vulnerabilities include reentrancy attacks, integer overflow/underflow, and improper access controls. The infamous DAO hack in 2016 led to a \$60 million loss due to a reentrancy vulnerability.

Then the risk analysis and Scoring each identified risk is evaluated based on likelihood and impact, using a scoring system ranging from 1 (Low) to 5 (Critical) as shown in Table 2.

Table 2. Risk analysis and scoring

Risk Type	Layer	Likelihood	Impact	Risk score
DDoS Attack	Network	4	5	20
51% Attack	Consensus	2	5	10
Smart Contract Reentrancy	Smart Contract	5	5	25
Sybil Attack	Network	3	4	12
Logic Flaw in Smart Contract	Smart Contract	4	4	16
Phishing Attack	Application	5	3	15

Based on the risk scores, risk mitigation strategies should be selected, and targeted security measures are recommended:

- DDoS attack: Implement rate limiting and enhanced node-level security policies.
- 51% attack: Transition to PoS consensus (Ethereum 2.0) to mitigate mining centralization.
- Smart contract reentrancy: Enforce secure coding practices and use tools like OpenZeppelin for secure contract development.
- Sybil attack: Strengthen identity verification mechanisms within Ethereum-based applications.
- Logic flaw in smart contract: Implement formal verification and rigorous testing frameworks before deployment.

## 3. RESULT AND DISCUSSION

Regarding the effectiveness of BCRAM, two key metrics were used for assessment:

- Reduction in Attack Success Rate (Smart Contract Exploits) as shown in Table 3.
  - A set of vulnerable smart contracts was deployed in the testnet.
  - Attackers attempted to exploit these contracts using known vulnerabilities (e.g., reentrancy attacks, integer overflows).
  - BCRAM's security measures (automated vulnerability scanning, access control policies) were applied.
- Improved Transaction Security (Reduction in Phishing Incidents) as shown in Table 4.
  - Users in the test environment were exposed to phishing attempts.
  - Without BCRAM, phishing links and fake login pages tricked users into compromising their credentials.
  - With BCRAM, multi-factor authentication (MFA), real-time phishing detection, and warning systems were implemented.

Table 3. The number of successful exploits before and after mitigation was recorded

Scenario	Total attacks	Successful exploits	Attack success rate
Without BCRAM	100	65	65%
With BCRAM	100	23	23%
Improvement	-	Reduction of 65%	Decrease by 65%

Table 4. The number of successful phishing attacks before and after BCRAM deployment was recorded

Scenario	Total phishing attempts	Successful phishing attacks	Success rate
Without BCRAM	100	70	70%
With BCRAM	100	21	21%
Improvement	-	Reduction of 70%	Decrease by 70%

The experiment demonstrated that BCRAM's mitigation strategies significantly enhanced blockchain security by reducing smart contract exploits by 65% and phishing incidents by 70%. This was achieved through proactive security measures such as vulnerability detection, enhanced authentication, and real-time threat mitigation. The controlled simulation environment allowed precise measurement of these improvements, validating the effectiveness of BCRAM's approach in strengthening blockchain transaction security.

To assess how BCRAM mitigates DDoS attacks and improves network stability by reducing downtime, a DDoS attack was simulated by flooding blockchain nodes with excessive requests. The network was monitored under two scenarios:

- Without BCRAM (no mitigation strategies) as shown in Table 5.
- With BCRAM (rate limiting, node load balancing, and traffic filtering applied).
- Network downtime was recorded as the time taken for the blockchain network to recover after an attack. Table 5 shows that DDoS attack resistance improved due to rate limiting and distributed node load balancing. Additionally, the Network downtime reduced by 85%, demonstrating increased stability.

**Scalability and Performance Evaluation:** To analyze how BCRAM affects blockchain scalability under different transaction loads and network sizes. The blockchain network was tested with varying numbers of nodes (10, 50, 100, 200), and Transaction load was increased from 1,000 TPS (Transactions per Second) to 100,000 TPS. Performance was measured using key metrics as shown in Table 6:

- Throughput (Transactions processed per second).
- Latency (Time taken to confirm a transaction).
- Block propagation time (Time taken to broadcast new blocks).

Table 5. Network downtime under two scenarios

Scenario	DDoS attack requests	Network downtime (Minutes)	Downtime reduction
Without BCRAM	500.000	200	0%
With BCRAM	500.000	30	85% Reduction

Table 6. Throughput, latency, and propagation time of the system

Blockchain size (Nodes)	Transaction load (TPS)	Throughput (TPS)	Latency (ms)	Block propagation time (ms)
10	1.000	950	120	150
50	10.000	9.600	180	200
100	50.000	48.500	250	280
200	100.000	95.000	320	350

The result in Table 6 shows that BCRAM effectively handles high transaction loads, maintaining high throughput with minimal latency increase. Additionally, with respect to network stability, BCRAM reduced downtime by 85%, making the blockchain more resilient against DDoS attacks, and the system efficiently handled up to 100,000 TPS, maintaining high throughput and minimal latency. One of the key takeaways from the study is the impact of proactive risk assessment on blockchain stability. Implementing BCRAM's recommendations, such as transitioning to PoS and adopting formal verification for smart contracts, resulted in enhanced security resilience. Additionally, the model's flexibility allows it to adapt to emerging threats, ensuring continuous security improvements.

However, the study also revealed areas where additional refinements are required. For example, BCRAM's computational overhead grows with network size, necessitating the development of optimized risk assessment techniques for large-scale blockchain networks. Furthermore, while the model effectively mitigates known vulnerabilities, it must continually evolve to address novel attack vectors that may arise with advancements in blockchain technology.

This case study demonstrates the effectiveness of BCRAM in systematically identifying and mitigating risks in blockchain ecosystems. By applying this model, Ethereum-based applications can enhance their security posture, reducing vulnerabilities and improving overall reliability. Future work includes extending BCRAM to other blockchain platforms like Hyperledger and Binance Smart Chain to validate its adaptability and effectiveness across different blockchain environments. Despite its success, scalability

remains an area for further optimization, particularly for high-volume blockchain environments. Future research should focus on refining risk assessment algorithms to enhance efficiency and incorporating AI-driven threat intelligence for real-time risk detection. Additionally, testing BCRAM on other blockchain platforms, such as Hyperledger and Binance Smart Chain, will further validate its adaptability and effectiveness across diverse blockchain architectures. Overall, BCRAM serves as a robust framework for enhancing blockchain security, providing a valuable tool for developers, enterprises, and researchers aiming to strengthen the security posture of blockchain-based systems.

#### 4. COMPARATIVE ANALYSIS OF BLOCKCHAIN RISK ASSESSMENT MODELS

This section presents a comparative analysis between the proposed BCRAM and several existing blockchain risk assessment models is shown in Table 7, including the BSF, OWASP Blockchain Top Ten Risks, SRS, RAFS, and ERM for Blockchain. This comparison will highlight the strengths and weaknesses of each model, as well as their suitability for different aspects of blockchain security.

Table 7. Comparative analysis of blockchain risk assessment models

Feature/Model	BCRAM	BSF	OWASP	SRS	RAFS	ERM
Focus Area	Comprehensive multi-layer risk assessment	General security controls for blockchain applications	Identification of top security risks	Comprehensive risk management for blockchain	Focused on smart contract vulnerabilities	Comprehensive approach to enterprise-level risks
Layer Coverage	Network, Consensus, Smart Contract, Application	Network and application layers	Primarily focuses on application layer risks	Network, Consensus, Application layers	Smart contracts only	Enterprise-wide risks, including governance
Risk Identification	Detailed identification across all layers	General identification, less specific	Top ten risks identified	Detailed identification process	Specific vulnerabilities in smart contracts	Broad risk identification across the organization
Mitigation Strategies	Customized strategies based on risk scoring	General recommendations for security	General guidelines for mitigation	Provides mitigation strategies	Specific mitigations for smart contracts	Enterprise risk mitigation strategies
Risk Scoring	Quantitative scoring based on likelihood and impact	Not standardized	No scoring, qualitative list	Qualitative assessment	Not standardized	Qualitative assessment of enterprise risks
Flexibility and Adaptability	Highly customizable to different blockchain contexts	Less adaptable, focused on predefined guidelines	Static list of risks	Flexible to adapt to various blockchain types	Specific to smart contracts, less adaptable	Adaptable to different enterprise contexts
Real-World Application	Designed for practical use across different blockchain applications.	General recommendations; practical applicability varies	Primarily educational and awareness	Practical applicability for various blockchains	Focused on smart contracts, applicable in relevant projects	Broad applicability across enterprises

##### 4.1. Advantages of BCRAM

BCRAM provides several advantages over traditional risk assessment models, particularly when addressing the specific nuances of blockchain technology:

- Comprehensive coverage:** By focusing on all layers of blockchain architecture, BCRAM ensures that no aspect of the system is overlooked. This comprehensive approach is essential for identifying risks that may span multiple layers or manifest in unique ways within the decentralized environment.
- Quantitative risk assessment:** The risk scoring system enables organizations to prioritize their security efforts based on empirical data rather than anecdotal evidence. This data-driven approach leads to more effective resource allocation and decision-making.
- Comprehensive mitigation strategies:** BCRAM's flexibility allows organizations to customize mitigation plans according to their specific use cases, regulatory requirements, and organizational risk tolerance. This adaptability is crucial in the rapidly evolving landscape of blockchain technology.
- Stakeholder engagement:** By involving various stakeholders in the risk identification and assessment process, BCRAM fosters collaboration and enhances awareness of blockchain security issues across the organization. This inclusivity leads to more robust security practices and a stronger organizational commitment to risk management.



- e) **Dynamic adaptation:** The cyclical nature of BCRAM ensures that organizations remain agile in their risk management efforts, enabling them to respond quickly to emerging threats and changes in the blockchain environment.

BCRAM is designed for a wide range of users across different sectors that leverage blockchain technology. Key stakeholders include:

- a) **Blockchain developers:** Developers can utilize BCRAM to identify and address vulnerabilities during the development phase of blockchain applications, ensuring that security is integrated into the design process.
- b) **Security analysts:** Cybersecurity professionals can implement BCRAM as part of their risk management strategy to assess and prioritize threats, enabling them to focus on high-risk areas.
- c) **Compliance officers:** Organizations operating in regulated industries can use BCRAM to ensure compliance with industry standards and regulations by systematically addressing and documenting security risks.
- d) **Executives and decision makers:** Organizational leaders can leverage the insights gained from BCRAM to make informed decisions about resource allocation and strategic planning related to blockchain initiatives.
- e) **Auditors and risk managers:** Internal and external auditors can apply BCRAM to assess the effectiveness of blockchain security controls and provide recommendations for improvement.
- f) **Educational Institutions and Researchers:** Academic institutions studying blockchain technology can employ BCRAM as a case study to analyze the effectiveness of security measures in real-world applications.

## 5. CONCLUSION

This paper applied the BCRAM to Ethereum, demonstrating its effectiveness in identifying, assessing, and mitigating security risks. By implementing automated smart contract auditing, decentralized identity solutions, and Layer 2 scalability enhancements, we achieved significant improvements in Ethereum's security posture. Specifically, smart contract exploits decreased by 65%, phishing incidents dropped by 70%, and DDoS resilience improved, reducing downtime by 85%. These results highlight the importance of a structured risk assessment framework tailored to blockchain ecosystems, ensuring greater trust, security, and reliability for decentralized applications. Despite these achievements, challenges remain in securing large-scale blockchain deployments against emerging attack vectors and evolving threat landscapes. Future work will focus on: a) **Enhancing AI-Driven Security Analytics** – Integrating machine learning models for real-time anomaly detection in blockchain transactions and smart contract behavior. b) **Cross-Chain Risk Assessment** – Extending BCRAM to multi-chain environments to address security challenges in interoperable blockchain networks. c) **Quantum-Resistant Cryptography** – Evaluating the impact of quantum computing on blockchain security and developing post-quantum encryption mechanisms. d) **Automated Compliance and Regulatory Adaptation** – Developing a compliance-aware risk assessment module to help blockchain projects meet regulatory requirements seamlessly.

By incorporating these advancements, BCRAM can evolve into a more adaptive, AI-enhanced security framework, further strengthening the resilience of blockchain ecosystems. Future studies will also focus on testing BCRAM in real-world financial and healthcare blockchain applications to validate its scalability and effectiveness across diverse industries.

## ACKNOWLEDGMENTS

This research work was done during the sabbatical leave from the University of Jordan for the academic year 2024-2025, where this research work was accomplished at the Department of Networks and Cybersecurity, Al-Ahliyya Amman University, Amman, Jordan.

## FUNDING INFORMATION

Authors state no funding involved.

## AUTHOR CONTRIBUTIONS STATEMENT

The sole author, **Mohammad Qatawneh**, was responsible for all aspects of this research, including conceptualization, methodology, formal analysis, investigation, and writing (original draft preparation and writing reviews and editing).

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mohammad Qatawneh	✓	✓			✓	✓			✓	✓	✓			

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review &amp; Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## ETHICAL APPROVAL

This article does not contain any studies with human participants or animals performed by the author.

## DATA AVAILABILITY

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.




## REFERENCES

- [1] D. B. Mohan Kumar, "Using blockchain technology for sustainable finance reporting," *Educational Administration Theory and Practice*, pp. 1182–1187, May 2024, doi: 10.53555/kuey.v30i6.5462.
- [2] A. Quzmar, S. Almaaitah, and M. Qatawneh, "A blockchain-based system for preventing drug counterfeit," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 6, pp. 1615–1627, 2022.
- [3] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
- [4] M. Altarawneh, M. Qatawneh, and W. Almobaideen, "Overview of applied data analytic mechanisms and approaches using permissioned blockchains," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, no. 1, pp. 42–52, Jan. 2022, doi: 10.18517/ijaseit.12.1.12827.
- [5] S. Lgarch, M. Hnida, and A. Retbi, "Empowering E-learning through blockchain: an inclusive and affordable tutoring solution," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 5, pp. 5554–5565, Oct. 2024, doi: 10.11591/ijece.v14i5.pp5554-5565.
- [6] M. A. Alhija, O. Al-Baik, A. Hussein, and H. Abdeljaber, "Optimizing blockchain for healthcare IoT: a practical guide to navigating scalability, privacy, and efficiency trade-offs," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 3, pp. 1773–1785, Sep. 2024, doi: 10.11591/ijeecs.v35.i3.pp1773-1785.
- [7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [8] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.
- [9] A. Park and H. Li, "The effect of blockchain technology on supply chain sustainability performances," *Sustainability (Switzerland)*, vol. 13, no. 4, pp. 1–18, Feb. 2021, doi: 10.3390/su13041726.
- [10] M. K. Lim, Y. Li, C. Wang, and M. L. Tseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Computers and Industrial Engineering*, vol. 154, p. 107133, Apr. 2021, doi: 10.1016/j.cie.2021.107133.
- [11] L. Ante and I. Fiedler, "The new digital economy: How decentralized finance (DeFi) and non-fungible tokens (NFTs) are transforming value creation, ownership models, and economic systems," *Digital Business*, vol. 5, no. 1, p. 100094, Jun. 2024, doi: 10.1016/j.digbus.2024.100094.
- [12] D. A. Snegireva, "Review of modern vulnerabilities in blockchain systems," in *Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021*, Sep. 2021, pp. 117–121, doi: 10.1109/ITQMIS53292.2021.9642862.
- [13] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10204 LNCS, Springer Berlin Heidelberg, 2017, pp. 164–186.
- [14] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proceedings - IEEE Symposium on Security and Privacy*, May 2015, vol. 2015-July, pp. 104–121, doi: 10.1109/SP.2015.14.
- [15] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin backbone protocol: analysis and applications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9057, Springer Berlin Heidelberg, 2015, pp. 281–310.
- [16] Z. Wang, Q. Chen, and L. Liu, "Permissioned blockchain-based secure and privacy-preserving data sharing protocol," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10698–10707, Jun. 2023, doi: 10.1109/JIOT.2023.3242959.
- [17] A. K. Singh and V. R. P. Kumar, "Analyzing the barriers for blockchain-enabled BIM adoption in facility management using best-worst method approach," *Built Environment Project and Asset Management*, vol. 14, no. 2, pp. 164–183, Dec. 2024, doi: 10.1108/BEPAM-04-2023-0080.

- [18] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: a review and outlook," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, Oct. 2022, doi: 10.1016/j.jksuci.2022.03.007.
- [19] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo, and J. Shin, "Analyzing and evaluating critical cyber security challenges faced by vendor organizations in software development: SLR based approach," *IEEE Access*, vol. 10, pp. 65044–65054, 2022, doi: 10.1109/ACCESS.2022.3179822.
- [20] A. Sharma, V. Goar, M. Kuri, and C. L. Chowdhary, "Supply chain management using blockchain security enhancement," in *Lecture Notes in Networks and Systems*, vol. 628 LNNS, Springer Nature Singapore, 2023, pp. 221–233.
- [21] I. Abunadi and R. L. Kumar, "Bsf-ehr: Blockchain security framework for electronic health records of patients," *Sensors*, vol. 21, no. 8, p. 2865, Apr. 2021, doi: 10.3390/s21082865.
- [22] OWASP, "OWASP top ten web application security risks," 2017. <https://owasp.org/www-project-top-ten/>.
- [23] I. Homoliak, S. Venugopalan, D. Reijbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 341–390, 2021, doi: 10.1109/COMST.2020.3033665.
- [24] A. Singh, R. M. Parizi, Q. Zhang, K. K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers and Security*, vol. 88, p. 101654, Jan. 2020, doi: 10.1016/j.cose.2019.101654.
- [25] S. G. Anton and A. E. A. Nucu, "Enterprise risk management: a literature review and agenda for future research," *Journal of Risk and Financial Management*, vol. 13, no. 11, p. 281, Nov. 2020, doi: 10.3390/jrfm13110281.
- [26] M. N. Birje, R. H. Goudar, C. M. Rakshitha, and M. T. Tapale, "A review on layered architecture and application domains of blockchain technology," in *International Conference on Electrical, Computer, and Energy Technologies, ICECET 2022*, Jul. 2022, pp. 1–5, doi: 10.1109/ICECET55527.2022.9872729.
- [27] P. D. Thai *et al.*, "Blockchain peer-to-peer network: performance and security," in *Springer Optimization and Its Applications*, vol. 194, Springer International Publishing, 2022, pp. 55–83.
- [28] D. Nancy Kirupanithi, A. Antonidoss, and G. Subathra, "Automated classification of the sybil attack in blockchain network using multi neural memory network classifier," *Applied Mathematics and Information Sciences*, vol. 17, no. 2, pp. 323–336, Mar. 2023, doi: 10.18576/amis/170214.
- [29] Q. Dai, B. Zhang, and S. Dong, "Eclipse attack detection for blockchain network layer based on deep feature extraction," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–19, Apr. 2022, doi: 10.1155/2022/1451813.
- [30] Q. Y. Dai, B. Zhang, and S. Q. Dong, "A DDoS-attack detection method oriented to the blockchain network layer," *Security and Communication Networks*, vol. 2022, pp. 1–18, May 2022, doi: 10.1155/2022/5692820.
- [31] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: a mining behavior study," *IEEE Access*, vol. 9, pp. 140549–140564, 2021, doi: 10.1109/ACCESS.2021.3119291.
- [32] R. Yang, X. Chang, J. Mišić, and V. B. Mišić, "Assessing blockchain selfish mining in an imperfect network: Honest and selfish miner views," *Computers and Security*, vol. 97, p. 101956, Oct. 2020, doi: 10.1016/j.cose.2020.101956.
- [33] M. A. Manolache, S. Manolache, and N. Tapus, "Decision making using the blockchain proof of authority consensus," *Procedia Computer Science*, vol. 199, pp. 580–588, 2021, doi: 10.1016/j.procs.2022.01.071.
- [34] B. Prasad and S. Ramachandram, "Prevention and detection mechanisms for re-entrancy attack and king of ether throne attack for ethereum smart contracts," *Ingenierie des Systemes d'Information*, vol. 27, no. 5, pp. 725–735, Oct. 2022, doi: 10.18280/isi.270505.
- [35] E. Lai and W. Luo, "Static analysis of integer overflow of smart contracts in ethereum," in *ACM International Conference Proceeding Series*, Jan. 2020, pp. 110–115, doi: 10.1145/3377644.3377650.
- [36] M. Almakhour, L. Sliman, A. E. Samhat, and A. Mellouk, "A formal verification approach for composite smart contracts security using FSM," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 70–86, Jan. 2023, doi: 10.1016/j.jksuci.2022.08.029.
- [37] W. Zhang *et al.*, "Combating front-running in smart contracts: attack mining, benchmark construction and vulnerability detector evaluation," *IEEE Transactions on Software Engineering*, vol. 49, no. 6, pp. 3630–3646, 2023, doi: 10.1109/TSE.2023.3270117.
- [38] A. Hassan, I. Makhdoom, W. Iqbal, A. Ahmad, and A. Raza, "From trust to truth: Advancements in mitigating the Blockchain Oracle problem," *Journal of Network and Computer Applications*, vol. 217, p. 103672, Aug. 2023, doi: 10.1016/j.jnca.2023.103672.
- [39] T. Tariq, F. Javed, S. Rizwan, M. Zubair, and B. Fayyaz, "Challenges in security and privacy posed by blockchain technology," *Journal of Independent Studies and Research Computing*, vol. 20, no. 2, Dec. 2022, doi: 10.31645/jisrc.22.20.2.1.
- [40] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: vulnerabilities, attacks, and defenses," *ACM Computing Surveys*, vol. 53, no. 3, pp. 1–43, Jun. 2020, doi: 10.1145/3391195.

## BIOGRAPHIES OF AUTHORS



**Professor Mohammad Qatawneh**    is a faculty member in the Computer Science Department at the University of Jordan. Currently, he is on sabbatical leave, serving at Al-Ahliyya Amman University in the College of IT, Networks, and Cybersecurity Department. He earned his Ph.D. in Computer Engineering from Kiev University in 1996 and his M.Sc. in Computer Engineering from the University of Donetsk, USSR, in 1988. His research focuses on blockchain technology, cybersecurity, digital forensics, and the internet of things (IoT). He can be contacted at email: mohd.qat@ju.edu.jo.