Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 12, No. 1, 2025

Research on Network Attack Early Warning and Defense Strategies for Blockchain Networks

Youpeng Huang, Yong Lv

Beijing Institute of Economics and Management, Beijing, 100102, China

Abstract: Blockchain technology has gained significant attention due to its decentralized and secure nature. However, despite its robustness, blockchain networks are not immune to attacks. This research aims to explore the early warning and defense strategies for network attacks in blockchain systems. By analyzing existing vulnerabilities and attack vectors, we propose a comprehensive framework for detecting and mitigating threats. The study emphasizes the importance of proactive measures to enhance the security posture of blockchain networks.

Keywords: Blockchain Networks; Network Attacks; Early Warning; Defense Strategies.

1. Introduction

Blockchain technology has emerged as a transformative force in various industries, offering a secure and transparent method for recording transactions. Its decentralized nature ensures that no single entity can control the network, thereby providing a high level of resistance to tampering and manipulation. Despite these inherent strengths, blockchain networks are not immune to cyber threats. As the adoption of blockchain technology continues to grow, the attack surface expands, necessitating a thorough understanding of potential vulnerabilities and the development of robust defense strategies.

The core principles of blockchain—decentralization, immutability, and consensus mechanisms—provide a robust foundation for secure transactions. However, these same principles introduce unique challenges in terms of network security. For instance, the consensus mechanisms that underpin blockchain networks can be exploited by attackers to gain control or manipulate transactions. Similarly, the immutability of blockchain data can paradoxically become a liability if malicious actors manage to alter the ledger.

This research aims to delve into the various types of attacks that can be launched against blockchain networks, including but not limited to 51% attacks, double-spending attacks, and Sybil attacks. By analyzing these vulnerabilities, we seek to develop comprehensive early warning systems and defense strategies. The ultimate goal is to enhance the security posture of blockchain networks, ensuring their resilience against emerging threats.

The importance of proactive measures cannot be overstated. As blockchain technology becomes more integrated into critical infrastructure, the consequences of a successful attack can be severe. Therefore, understanding the potential attack vectors and developing effective countermeasures is crucial for the long-term viability and adoption of blockchain technology.

In summary, this paper will explore the vulnerabilities inherent in blockchain networks, propose early warning systems to detect potential threats, and develop defense strategies to mitigate the impact of attacks. By doing so, we aim to contribute to the ongoing effort to secure blockchain technology and ensure its continued growth and adoption across various industries.

2. Background

Blockchain technology, first introduced with Bitcoin in 2008, has since evolved into a versatile platform for various applications beyond cryptocurrencies. The foundational principles of blockchain—decentralization, immutability, and consensus mechanisms—have been pivotal in establishing its reputation for security and transparency.

Decentralization ensures that no single entity can control the network, distributing power and responsibility among multiple nodes. This distributed architecture enhances security by eliminating single points of failure and reducing the risk of centralized control.

Immutability refers to the permanent and unchangeable nature of recorded transactions. Once a transaction is added to the blockchain, it cannot be altered without consensus from the entire network. This feature ensures the integrity and authenticity of the data stored on the blockchain.

Consensus Mechanisms are critical for maintaining the integrity of the blockchain. They enable nodes to agree on the validity of transactions and the order in which they are added to the ledger. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Each mechanism has its own set of advantages and trade-offs, influencing the security and efficiency of the network.

Despite these robust principles, blockchain networks face unique security challenges. The decentralized nature of blockchain introduces complexities in managing and securing the network. Additionally, the immutability of data can sometimes work against the network, as it becomes difficult to correct errors or address fraudulent activities once they are recorded.

Furthermore, the integration of blockchain with other technologies and systems introduces new vulnerabilities. For example, the interaction between blockchain and traditional financial systems can create new attack vectors, while the use of smart contracts can expose the network to coding errors and exploitation.

Understanding these challenges is crucial for developing effective defense strategies. This research aims to analyze the vulnerabilities and attack vectors specific to blockchain networks, with the goal of enhancing their security posture and ensuring their resilience against emerging threats.

3. Scope and Objectives

The scope of this research is focused on the analysis of common attack vectors and the development of effective early warning and defense strategies for blockchain networks. Specifically, the study aims to:

Identify Vulnerabilities: Conduct a comprehensive analysis to identify the key vulnerabilities in blockchain networks. This includes examining the potential weaknesses in the network architecture, consensus mechanisms, and smart contracts. By understanding these vulnerabilities, we can better prepare for and mitigate potential attacks.

Develop Early Warning Systems: Propose and implement early warning systems that can detect potential attacks in real-time. This involves leveraging advanced techniques such as anomaly detection and behavioral analysis to identify suspicious activities. The goal is to create a proactive defense mechanism that can alert network administrators to potential threats before they escalate.

Propose Defense Strategies: Develop and evaluate defense strategies to mitigate the impact of identified attacks. This includes enhancing consensus mechanisms, improving smart contract security through rigorous auditing, and promoting the use of decentralized exchanges to reduce centralization risks. The objective is to create a multi-layered defense framework that can effectively counteract various attack vectors.

Case Studies: Analyze real-world case studies of blockchain network attacks, such as the Ethereum DAO attack and the Bitcoin Cash fork. These case studies will provide insights into the practical implications of vulnerabilities and the effectiveness of defense strategies. By examining these incidents, we can learn valuable lessons and refine our approaches to blockchain security.

Future Directions: Explore future trends and technologies that could impact blockchain security, such as the integration of artificial intelligence and machine learning, the potential threat posed by quantum computing, and the development of interoperability standards. By staying abreast of these developments, we can anticipate and prepare for emerging threats.

By focusing on these objectives, this research aims to contribute to the ongoing effort to secure blockchain technology and ensure its continued growth and adoption across various industries. The ultimate goal is to enhance the security posture of blockchain networks, making them more resilient against cyber threats.

4. Literature Review

4.1. Types of Attacks on Blockchain Networks

Understanding the various types of attacks that can target blockchain networks is crucial for developing effective defense strategies. This section reviews some of the most common and impactful attacks, including 51% attacks, double-spending attacks, and Sybil attacks.

51% Attacks:

1. **Description**: A 51% attack occurs when an attacker gains control of more than 50% of the network's hashing power. With this control, the attacker can manipulate transaction confirmations, potentially reversing transactions and double-spending coins.

2. **Impact**: This type of attack undermines the trust in the network's consensus mechanism and can lead to significant financial losses. It highlights the importance of having a distributed and diverse network of miners.

3. **Mitigation**: Strategies include increasing the network's hash rate, diversifying mining pools, and implementing economic incentives to discourage centralization.

Double-Spending Attacks:

1. **Description**: In a double-spending attack, an attacker spends the same cryptocurrency more than once by creating conflicting transactions. This can occur in various ways, such as by exploiting timing vulnerabilities or manipulating the network's consensus process.

2. **Impact**: Double-spending attacks can result in financial losses for users and undermine the trust in the currency. They highlight the need for robust transaction verification mechanisms.

3. **Mitigation**: Techniques such as transaction confirmation times, consensus algorithms, and network monitoring can help mitigate this risk.

Sybil Attacks:

1. Description: A Sybil attack involves an attacker creating multiple fake identities (nodes) to gain control over the network and influence consensus decisions. This can be particularly effective in networks with weak identity verification mechanisms.

2. **Impact**: Sybil attacks can disrupt the network's consensus process, leading to incorrect decisions and potential security breaches. They highlight the importance of strong identity verification and network governance.

3. **Mitigation**: Strategies include implementing identity verification protocols, using reputation systems, and fostering a community-driven governance model.

These attacks are not only theoretical threats but have been demonstrated in real-world scenarios, underscoring the need for continuous research and development of defense mechanisms. By understanding the nuances of these attacks, researchers and practitioners can develop more effective strategies to protect blockchain networks.

Table 1. Common Types of Blockchain Attacks

Attack Type	Description	Impact
51% Attack	Control >50% of hashing power	Manipulate transactions, reverse confirmations
Double-Spending	Spend same currency twice	Financial loss, trust erosion
Sybil Attack	Create multiple fake identities	Influence consensus, disrupt network

4.2. Existing Defense Mechanisms

To counteract the various attack vectors targeting blockchain networks, several defense mechanisms have been developed and implemented. These mechanisms aim to enhance the security and resilience of blockchain systems by addressing vulnerabilities and strengthening the network's defenses.

Consensus Mechanisms:

1. **Description**: Consensus mechanisms are fundamental to

blockchain networks, ensuring that all nodes agree on the validity of transactions and the state of the ledger. Common mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).

2. Impact: These mechanisms provide a robust framework for validating transactions and preventing malicious activities. PoW, for example, relies on computational power, while PoS and DPoS rely on stakeholder participation and delegation, respectively.

3. Advancements: Researchers are exploring hybrid consensus models and more efficient algorithms to balance security and scalability.

Smart Contract Audits:

1. **Description**: Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. However, they are prone to coding errors and vulnerabilities.

2. **Impact**: Regular audits of smart contracts help identify and fix these vulnerabilities before they can be exploited by attackers. This is crucial for maintaining the integrity and security of the network.

3. Best Practices: Industry standards and tools for automated code analysis and manual code reviews are being developed to enhance the security of smart contracts.

Network Monitoring:

1. Description: Continuous monitoring of network traffic is essential for detecting suspicious activities and potential attacks. This involves analyzing transaction patterns, node behavior, and network anomalies.

2. Impact: Real-time monitoring can help in identifying and responding to attacks promptly, minimizing their impact. Machine learning and AI techniques are increasingly being used to enhance the accuracy and efficiency of monitoring systems.

3. Challenges: Balancing the need for detailed monitoring with privacy concerns and network performance is a key challenge.

Decentralized Exchanges (DEXs):

1. Description: DEXs are platforms that allow users to trade cryptocurrencies directly from their wallets without relying on a central authority.

2. Impact: By eliminating intermediaries, DEXs reduce the risk of centralized points of failure and enhance the security of transactions.

3. Development: Efforts are underway to improve the user experience and scalability of DEXs, making them more accessible to a wider audience.

Zero-Knowledge Proofs (ZKPs):

1. Description: ZKPs allow one party to prove to another that a statement is true without revealing any additional information beyond the truth of the statement itself.

2. Impact: This technology enhances privacy and security by enabling confidential transactions and data sharing without compromising on trust.

3. Applications: ZKPs are being integrated into various blockchain applications to improve security and efficiency.

These defense mechanisms, when combined, form a comprehensive framework for protecting blockchain networks. Ongoing research and development are essential to stay ahead of emerging threats and to continuously improve the security posture of blockchain systems.

5. Methodology

5.1. Data Collection

Data collection is a critical component of this research, as it provides the foundation for analyzing vulnerabilities and developing defense strategies. The data collection process involved a systematic approach to gather relevant information from various sources.

Academic Journals and Conference Proceedings:

1. Sources: Databases such as IEEE Xplore, ACM Digital Library, and arXiv were extensively searched for peer-reviewed articles and conference papers focusing on blockchain security.

2. Criteria: Articles were selected based on their relevance to the research objectives, including studies on attack vectors, defense mechanisms, and case studies of real-world attacks.

Industry Reports and Whitepapers**:**

1. **Sources**: Reports from blockchain companies, security firms, and industry associations were reviewed. These included documents from organizations like Chainalysis, Coin Metrics, and the Blockchain Research Institute.

2. Criteria: Reports were chosen for their detailed analysis of current threats and emerging trends in blockchain security.

Case Studies and Incident Reports:

1. Sources: Detailed case studies of notable blockchain attacks, such as the Ethereum DAO attack and the Bitcoin Cash fork, were analyzed. These incidents were documented in various forums, news outlets, and technical blogs.

2. Criteria: Case studies were selected for their relevance to the research objectives and their ability to provide insights into the practical implications of vulnerabilities.

Expert Interviews and Surveys:

1. Sources: Interviews with blockchain security experts and surveys of industry professionals were conducted to gather qualitative data on current challenges and future directions.

2. Criteria: Participants were selected based on their expertise in blockchain security and their contributions to the field through publications, presentations, and community engagement.

Data Processing and Analysis:

1. Screening: Collected data was screened to ensure its relevance and reliability. Duplicate or irrelevant information was removed.

2. Categorization: Data was categorized based on the type of information (e.g., attack vectors, defense mechanisms, case studies) to facilitate analysis.

3. Synthesis: The data was synthesized to identify common themes and patterns, which informed the development of the research framework and analysis.

By following this systematic approach, the research ensures that the data collected is comprehensive, relevant, and reliable, providing a solid foundation for the analysis and conclusions drawn in this study.

5.2. Analysis Framework

The data analysis framework is designed to systematically assess the vulnerabilities and effectiveness of defense strategies for blockchain networks. The framework is structured into four main stages:

Threat Modeling:

1. Objective: Identify potential threats and their impact on the blockchain network. This involves mapping out the attack surface and understanding how different types of attacks can

exploit vulnerabilities.

2. Techniques**:** Use of threat modeling tools and methodologies to visualize and analyze potential attack paths. This includes identifying entry points, attack vectors, and the potential impact on network integrity and security.

Vulnerability Assessment:

1. Objective: Evaluate the weaknesses in the network architecture and protocols. This involves a detailed examination of the blockchain's design, consensus mechanisms, and smart contract implementations.

2. Techniques: Conducting code reviews, penetration testing, and security audits to identify coding errors, configuration vulnerabilities, and other weaknesses. Tools such as static analysis tools and dynamic testing frameworks are used to automate parts of this process.

Risk Analysis:

1. Objective: Quantify the likelihood and impact of different attack scenarios. This involves assessing the probability of attacks occurring and the potential consequences for the network.

2. Techniques: Use of risk assessment matrices and probabilistic models to evaluate the risk associated with each vulnerability. This includes considering factors such as the frequency of attacks, the potential financial loss, and the impact on user trust.

Defense Strategy Development:

1. Objective: Propose and evaluate defense mechanisms based on the analysis. This involves developing strategies to mitigate identified vulnerabilities and enhance the network's security posture.

2. Techniques: Designing and testing defense mechanisms, such as enhanced consensus algorithms, secure smart contract practices, and improved network monitoring systems. Simulation and scenario-based testing are used to evaluate the effectiveness of these strategies.

By following this structured framework, the research aims to provide a comprehensive analysis of blockchain network security, identifying key vulnerabilities and proposing effective defense strategies. This approach ensures that the analysis is thorough, data-driven, and aligned with the research objectives.

6. Results

6.1. Vulnerabilities in Blockchain Networks

The analysis of blockchain networks reveals several critical vulnerabilities that can be exploited by attackers. Understanding these vulnerabilities is essential for developing effective defense strategies.

Centralized Points **of Failure**:

1. Description: Despite the decentralized nature of blockchain, certain components such as mining pools and centralized exchanges can become centralized points of failure. These entities, if compromised, can significantly impact the network's security and integrity.

2. Example: The concentration of mining power in a few large mining pools can lead to a 51% attack, where an attacker gains control of the majority of the network's hashing power. This was demonstrated in the Bitcoin Gold attack in 2018, where a 51% attack resulted in the theft of millions of dollars worth of cryptocurrency.

3. Impact: Such attacks undermine the trust in the network's consensus mechanism and can lead to financial losses and reputational damage.

Smart Contract Vulnerabilities:

1. Description: Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, are prone to coding errors and vulnerabilities. These vulnerabilities can be exploited by attackers to steal funds or disrupt network operations.

2. Example: The DAO attack in 2016 highlighted the risks associated with smart contracts. An attacker exploited a vulnerability in the DAO's code to drain millions of dollars worth of Ether. This led to a contentious hard fork of the Ethereum network.

3. Impact: Smart contract vulnerabilities can result in financial losses, legal liabilities, and damage to the network's reputation. They also highlight the need for rigorous auditing and testing of smart contracts.

Interoperability Issues:

1. Description: The integration of blockchain with other systems and technologies can introduce new vulnerabilities. Interoperability often requires the use of APIs and other interfaces, which can become entry points for attackers.

2. Example: The integration of blockchain with traditional financial systems can expose the network to new attack vectors. For instance, a vulnerability in an API used for trading could allow an attacker to manipulate transaction data.

3. Impact: Interoperability issues can compromise the security of the blockchain network and the systems it interacts with. They require careful planning and secure implementation to mitigate risks.

By identifying and understanding these vulnerabilities, researchers and practitioners can develop targeted defense strategies to enhance the security posture of blockchain networks. Addressing these vulnerabilities is crucial for ensuring the long-term viability and adoption of blockchain technology.

Table 2. Vulnerabilities in Blockchain Networks

Vulnerability	Description	Example	Impact
Centralized Points	Mining pools, exchanges	Potential for single point of failure	Undermine trust, financial loss
Smart Contract Errors	Coding mistakes	Exploitable bugs	Financial loss, legal liabilities
Interoperability Issues	Integration with external systems	New attack vectors	Compromise security, integration risks

6.2. Early Warning Systems

Early warning systems are critical for detecting and mitigating potential threats to blockchain networks. These systems leverage advanced technologies and methodologies to identify suspicious activities and alert network administrators in real-time.

Anomaly Detection:

1. Description: Anomaly detection systems use machine learning algorithms to identify unusual patterns in network traffic. These algorithms analyze historical data to establish baseline behavior and detect deviations from this baseline.

1. Techniques: Techniques such as statistical analysis, clustering, and neural networks are used to identify anomalies. For example, a sudden increase in transaction volume or unusual transaction patterns can trigger an alert.

2. Effectiveness: Anomaly detection can help in identifying early signs of attacks, such as a 51% attack or a Sybil attack, allowing for timely intervention.

Behavioral Analysis:

1. Description: Behavioral analysis involves monitoring the behavior of nodes in the network to identify potential attackers. This includes analyzing transaction patterns, node activity, and communication logs.

2. Techniques: Techniques such as graph theory and social network analysis are used to identify suspicious behavior. For instance, a node that consistently attempts to manipulate consensus or create conflicting transactions can be flagged.

3. Effectiveness: Behavioral analysis can help in detecting insider threats or coordinated attacks, enhancing the network's resilience.

Real-Time Alerts:

1. Description: Real-time alert systems are designed to notify network administrators immediately when suspicious activities are detected. These systems integrate with existing monitoring tools and can send alerts via email, SMS, or push notifications.

2. Techniques: The use of automated alerting mechanisms ensures that threats are addressed promptly. For example, an alert can be sent when an anomaly is detected, triggering an immediate investigation.

3. Effectiveness: Real-time alerts minimize the time to respond to threats, reducing the potential impact of an attack and enhancing the network's overall security posture.

Integration with Human-in-the-Loop:

1. Description: Effective early warning systems also involve human oversight. Analysts can review alerts, validate detections, and take appropriate action. This human-in-the-loop approach ensures that false positives are minimized and that responses are well-informed.

2. Techniques: Analysts can use dashboards and visualization tools to monitor network activity and investigate alerts. Collaboration tools can facilitate communication and coordination among team members.

3. Effectiveness: Human oversight enhances the accuracy of detections and ensures that appropriate actions are taken, balancing the need for automation with the importance of human judgment.

By implementing these early warning systems, blockchain networks can significantly enhance their security posture. These systems provide a proactive defense mechanism, allowing for timely detection and mitigation of potential threats. Addressing these vulnerabilities is crucial for ensuring the long-term viability and adoption of blockchain technology.

6.3. Defense Strategies

Developing effective defense strategies is crucial for mitigating the vulnerabilities identified in blockchain networks. This section outlines several key defense mechanisms and their implementation considerations.

Enhanced Consensus Mechanisms:

1. Description: Enhancing consensus mechanisms involves developing more robust algorithms that can withstand various attack vectors. This includes exploring hybrid models and more efficient consensus protocols.

2. Techniques: Techniques such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) can provide stronger security guarantees. For example, PoS reduces the energy consumption of mining while maintaining network security.

3. Challenges: Implementing new consensus mechanisms requires careful consideration of network performance, scalability, and community acceptance. Transitioning from existing mechanisms can also be complex.

Secure Smart Contracts:

1. Description: Ensuring the security of smart contracts involves rigorous auditing and testing processes. This includes automated code analysis and manual reviews to identify and fix vulnerabilities.

2. Techniques: Tools such as static analysis tools, formal verification methods, and secure coding practices can enhance the security of smart contracts. For instance, using formal verification can mathematically prove the correctness of contract logic.

3. Challenges: The complexity of smart contracts and the rapid pace of development can make it challenging to keep up with security best practices. Continuous monitoring and updates are essential.

Decentralized Exchanges (DEXs):

1. Description: Promoting the use of DEXs reduces the risk of centralized points of failure by eliminating intermediaries. DEXs allow users to trade cryptocurrencies directly from their wallets.

2. Techniques: Implementing DEXs requires robust trading algorithms and secure transaction processing. For example, using atomic swaps can ensure that trades are executed without the need for trust.

3. Challenges: Ensuring the liquidity and user experience of DEXs can be challenging. Scalability and security must be balanced to prevent attacks.

Zero-Knowledge Proofs (ZKPs):

1. Description: ZKPs enhance privacy and security by allowing transactions to be verified without revealing sensitive information. This technology can be integrated into various blockchain applications.

2. Techniques: Implementing ZKPs involves developing efficient cryptographic protocols. For example, zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) can provide strong privacy guarantees.

3. Challenges: The complexity of ZKPs and the need for specialized hardware can limit their adoption. Ensuring the security of these protocols is critical.

Continuous Monitoring and Updates:

1. Description: Continuous monitoring of network activity and regular updates to software and protocols are essential for

maintaining security. This includes proactive threat detection and response.

2. Techniques: Using advanced monitoring tools and automated alerting systems can help in identifying and responding to threats promptly. Regular security audits and updates can address emerging vulnerabilities.

3. Challenges: Balancing the need for continuous monitoring with resource constraints can be challenging. Ensuring that all nodes are updated in a timely manner is crucial for network security.

By implementing these defense strategies, blockchain networks can significantly enhance their security posture. These strategies provide a multi-layered approach to protecting against various attack vectors, ensuring the long-term viability and adoption of blockchain technology.

7. Case Studies

7.1. Case Study 1: Ethereum DAO Attack

In 2016, the DAO (Decentralized Autonomous Organization) on the Ethereum network was attacked, resulting in the theft of millions of dollars worth of Ether. The attack highlighted the vulnerabilities in smart contracts and led to a hard fork of the Ethereum network.

Table 3. Ethereum DAO Attack Details

Event	Date	Impact	Outcome
DAO Attack	June 2016	$50M stolen	Hard fork

7.2. Case Study 2: Bitcoin Cash Fork

The Bitcoin Cash fork in 2017 was triggered by a disagreement over block size limits. This incident demonstrated the challenges in achieving consensus among network participants.

Table 4. Bitcoin Cash Fork Details

Event	Date	Reason	Outcome
Fork	August 2017	Block size limits	New chain: Bitcoin Cash

8. Discussion

8.1. Challenges in Implementing Defense Strategies

1. Balancing Security and Efficiency: Enhancing security often comes at the cost of efficiency, which can affect network performance.

2. Regulatory Compliance: Blockchain networks must comply with various regulations, which can complicate security measures.

3. Continuous Monitoring: The dynamic nature of blockchain networks requires continuous monitoring and adaptation of defense strategies.

8.2. Future Directions

1. AI and Machine Learning: Leveraging AI and machine learning to improve threat detection and response times.

2. Quantum Computing: Preparing for the potential impact of quantum computing on blockchain security.

3. Interoperability Standards: Developing standardized protocols for blockchain interoperability to reduce vulnerabilities.

9. Conclusion

Blockchain technology offers a promising solution for secure and transparent transactions. However, the increasing adoption of blockchain networks has also exposed them to various attack vectors. This research has identified key vulnerabilities and proposed comprehensive early warning and defense strategies. By implementing these strategies, blockchain networks can enhance their security posture and protect against potential attacks.

Acknowledgments

This research was supported by the R&D Program of Beijing Municipal Education Commission (SM202114073 001).

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2] Buterin, V. (2014). A next-generation smart contract and decentralized application platform.

[3] Szabo, N. (1997). Formalizing and securing relationships on public networks.

[4] Zohar, A. (2015). Bitcoin under the hood.

[5] Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable.

[6] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts.

[7] Biryukov, A., Khovratovich, D., & Ponomarev, V. (2016). Equihash: Asymmetric proof-of-work based on the generalized birthday problem.