The International Journal of Business Management and Technology, Volume 9 Issue 2 February 2025
ISSN: 2581-3889

Research Article Open Access

Bugs and Risks in Blockchain Technology Usage

Dr. Eldad Bar Lev (Ph.D.)
Economic International Affairs and Business
(Law Student)

ABSTRACT: Blockchain technology has revolutionized multiple industries by offering decentralized and secure solutions for financial transactions, smart contracts, and data management. However, it also presents significant challenges, including security vulnerabilities, scalability limitations, regulatory uncertainties, and environmental concerns. This paper explores the key risks associated with blockchain technology, including coding errors, cyberattacks, human factor risks, and legal ambiguities. Additionally, it highlights potential solutions and best practices to mitigate these risks, ensuring the continued development and adoption of blockchain-based systems. The findings underscore the importance of security audits, regulatory clarity, and sustainable innovations in enhancing blockchain resilience.

KEYWORDS: Blockchain, Smart Contracts, Cybersecurity, 51% Attack, Scalability, Regulatory Risks,

JEL CLASSIFICATION

O33, K24, G28, D81, L86

I. Introduction

Blockchain technology has emerged as one of the most transformative innovations of the 21st century, finding applications in various fields, including cryptocurrencies, smart contracts, supply chain management, and decentralized finance (DeFi). While it offers numerous advantages such as security, transparency, and decentralization, it also introduces significant risks and challenges. This article provides an in-depth examination of the key bugs and risks associated with blockchain technology, incorporating additional research and analysis.

II. Bugs in Code and Smart Contracts

Smart contracts are self-executing programs stored on the blockchain that trigger actions based on predefined conditions. Since these contracts operate autonomously and are immutable after deployment, any coding errors can lead to severe financial losses and security vulnerabilities.

Security Bugs

- Flaws in smart contract code can create openings for malicious actors to manipulate transactions and drain funds.
- Exploits often occur due to programming errors in languages such as Solidity, which is used for Ethereum-based smart contracts.

Notable Cases

- **The DAO Hack (2016)**: A vulnerability in the smart contract allowed hackers to siphon off 3.6 million Ether, leading to a controversial hard fork in Ethereum. o *Source: Buterin, V. (2016). "A Call for a Temporary Moratorium on The DAO." Ethereum Blog.*
- **Parity Wallet Bug (2017)**: A coding flaw led to the accidental freezing of over 500,000 Ether worth millions of dollars.

Solutions

- **Formal Verification**: Mathematical proofs to ensure smart contract correctness.
- **Third-Party Audits**: Engaging cybersecurity firms to analyze code before deployment.

2. Security Attacks on the Blockchain Network

Despite its decentralized nature, blockchain networks remain susceptible to various cyberattacks.

51% Attack

- Occurs when an entity gains control of more than 50% of the network's hashing power, allowing them to double-spend transactions or alter records.
- **Example**: Bitcoin Gold suffered a 51% attack in 2018, leading to double-spending losses of approximately $18 million.

Sybil Attacks

- Attackers generate multiple fake identities to dominate a decentralized network, undermining trust.

Cryptographic Weaknesses

- **Quantum Computing Threat**: Future quantum computers could potentially break existing cryptographic algorithms like SHA-256.

o *Source: Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."*

- Researchers are developing quantum-resistant encryption techniques.
-

III. Scalability Issues

Blockchain networks struggle with scalability, particularly as transaction volumes increase.

Challenges

- **Transaction Throughput**: Bitcoin processes only ~7 transactions per second (TPS), whereas Visa handles 24,000 TPS.
- **Long Processing Times**: Congestion in networks like Ethereum results in slow confirmation times.
- **High Transaction Fees**: Increased demand leads to costly gas fees.

- **Layer 2 Scaling Solutions**: Lightning Network (Bitcoin), Optimistic Rollups (Ethereum).
- **Sharding**: A technique that partitions blockchain data to improve speed and efficiency. o *Source: Ethereum Foundation (2020). "Scalability Solutions and Layer 2."*

IV. Regulatory Uncertainty and Legal Risks

Blockchain technology operates in a gray regulatory area, with legal frameworks evolving worldwide.

Key Issues

- **Unclear Regulations**: Governments are still formulating policies regarding cryptocurrencies and DeFi platforms.

- **Legal Risks**: Countries like China have banned cryptocurrency transactions, while others impose strict taxation policies.

Sources

- *Financial Stability Board (2021). "Regulatory Frameworks for Cryptocurrencies."*

- The European Union's **MiCA (Markets in Crypto-Assets Regulation)** aims to provide clearer legal guidelines.

V. Loss of Private Keys and Human Factor Risks

One of blockchain's most unique features is that users have full control over their assets, but this comes with risks.

Common Risks

- **Loss of Private Keys**: Unlike traditional banking, losing a private key means permanent loss of funds.

- **Fraud & Phishing**: Hackers trick users into revealing credentials through deceptive emails or fake websites.

Preventive Measures

- **Cold Storage**: Storing private keys offline for enhanced security.

- **Multi-Signature Wallets**: Requiring multiple approvals for transactions. o *Source: Antonopoulos, A. (2017). "Mastering Bitcoin: Unlocking Digital Cryptocurrencies."*

VI. Environmental Concerns

Blockchain networks, especially Proof-of-Work (PoW) systems, consume vast amounts of electricity.

Environmental Impact

- Bitcoin mining consumes more electricity annually than some entire countries, such as Argentina.

- Increased carbon footprint from mining operations.

Potential Solutions

- **Transition to Proof-of-Stake (PoS)**: Ethereum's shift to PoS aims to reduce energy consumption by over 99%.

- **Green Blockchain Projects**: Research into eco-friendly mining alternatives.

VII. Conclusion and Future Recommendations

Blockchain technology continues to evolve, shaping the digital economy and offering transformative potential across multiple sectors. However, as adoption grows, the need for robust security mechanisms, efficient regulatory frameworks, and sustainable solutions becomes more critical. The risks associated with blockchain—ranging from security vulnerabilities to environmental concerns—demand comprehensive strategies for mitigation and improvement.

A key takeaway from this discussion is that security remains a paramount issue. Smart contract vulnerabilities, cyberattacks, and risks posed by quantum computing require ongoing research and development of cryptographic techniques that can withstand emerging threats. Additionally, implementing regular security audits and third-party evaluations is crucial to ensuring the reliability of blockchain-based applications.

Scalability is another persistent challenge. Without improvements in transaction throughput and cost-efficiency, blockchain networks may struggle to support widespread adoption. The exploration of Layer 2 solutions, sharding, and alternative consensus mechanisms will play a significant role in improving blockchain performance and accessibility.

From a regulatory perspective, global cooperation is necessary to establish fair and transparent guidelines that protect consumers while fostering innovation. Governments and international organizations must work alongside blockchain developers and businesses to create legal frameworks that enhance security without stifling technological advancements. Addressing regulatory uncertainty will provide a more stable foundation for blockchain-based financial services, ensuring compliance and protecting users from illicit activities.

Environmental concerns associated with energy-intensive mining practices must also be addressed. The transition to Proof-of-Stake and other eco-friendly consensus mechanisms presents a viable solution to reducing blockchain's carbon footprint. Further investment in green blockchain initiatives and sustainability-focused research will be critical for balancing innovation with environmental responsibility.

VIII. Future Recommendations.

1. **Enhanced Security Measures:**

- Encourage the adoption of formal verification techniques to ensure the correctness of smart contracts.
- Implement robust security audits and bug bounty programs to identify vulnerabilities before deployment.
- Promote multi-signature authentication and cold storage solutions to minimize asset loss risks.

2. Regulatory Clarity and Compliance:

- Establish global regulatory frameworks that provide legal clarity while supporting innovation.
- Encourage collaboration between governments and blockchain developers to create fair compliance guidelines.
- Monitor and adapt regulations to address emerging risks such as decentralized finance (DeFi) fraud and illicit activities.

3. **Scalability and Efficiency Improvements:**

- Accelerate the implementation of Layer 2 scaling solutions such as the Lightning Network and Optimistic Rollups.
- Develop and test new consensus mechanisms beyond Proof-of-Work (PoW) and Proof-of-Stake (PoS) to enhance efficiency.
- Optimize blockchain data storage using compression techniques and off-chain solutions.
-

4. **Education and Awareness Initiatives:**

- Promote blockchain literacy through educational programs, ensuring that users understand best security practices.
- Raise awareness about phishing attacks and fraud prevention strategies.
- Encourage academic and industry research to explore the long-term implications of blockchain technology.

5. **Sustainability and Energy Efficiency:**

- Foster innovation in eco-friendly blockchain projects that reduce energy consumption.
- Support the transition from PoW to PoS mechanisms to enhance sustainability.
- Encourage blockchain adoption in green initiatives, such as carbon credit tracking and renewable energy distribution.

By addressing these risks and implementing proactive measures, blockchain technology can achieve its full potential while maintaining safety, efficiency, and trust in the digital economy. Ongoing research and collaboration will be essential in shaping a future where blockchain remains a secure and scalable solution for industries worldwide.

References

[1] Antonopoulos, A. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.*

[2] Buterin, V. (2016). *A Call for a Temporary Moratorium on The DAO.* Ethereum Blog.

[3] Financial Stability Board (2021). *Regulatory Frameworks for Cryptocurrencies.*

[4] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[5] Ethereum Foundation (2020). *Scalability Solutions and Layer 2.*