Decoding Blockchain Security

7 Best Practices for a Resilient Future

Introduction

Visionary government policies, massive digitization projects, and a tech-savvy population have fueled blockchain efforts in the GCC (Gulf Cooperation Council) and the Middle East. Governments are investing significantly in blockchain to diversify their economies, improve public systems, and strengthen cybersecurity measures. The Emirates Blockchain Strategy 2021 from the UAE and Saudi Arabia's Vision 2030 focus on using blockchain's promise.

In finance, blockchain is bringing changes to how cross-border transactions work. The UAE started the Digital Currency Cross-Border Payment Pilot to lower costs and include more people in the financial system. In healthcare, blockchain plays a role in sharing patient records, like the National Unified Medical Record in the Kingdom of Saudi Arabia. Logistics businesses are using blockchain to improve package tracking and reduce fraud. The energy field also benefits from blockchain, with the Dubai Electricity and Water Authority's work in the Green Energy Market being a clear example of this effort.

Blockchain technology is poised to transform industries, which makes adopting robust security practices crucial. This guide explores the developments in blockchain by examining trends, key challenges, regional and global regulations, and essential steps to secure the use of blockchain.

Emerging Trends in Blockchain Security

Blockchain security continues to evolve as new patterns emerge and direct its progression. Organizations should be mindful of the key developments:

i. **Decentralized Finance (DeFi)**: DeFi platforms introduce new security risks, such as weak smart contracts, flash loan exploits, and attacks on decentralized autonomous organizations (DAOs). Protecting these platforms is vital since they manage large sums of assets.

ii. **Tokenization**: Tokenizing assets applies to both physical and digital items. It offers a way to represent and transfer ownership. Companies need to consider security issues when dealing with tokenized assets in both digital and physical forms.

iii. **Interoperability and cross-chain security**: As blockchain networks grow, interoperability is becoming more critical. Blockchain security needs to focus on safe interactions and transactions between different chains.

iv. **Blockchain-as-a-Service (BaaS)**: BaaS helps businesses use blockchain easily by offering ready-made networks and tools through cloud platforms. It lets organizations build and run blockchain applications without the hassle of setting up or managing their own networks. This setup also ensures they can handle more transactions in the future as their needs grow.

v. **Focus on Decentralized Identity (DID)**: People are paying more attention to protecting decentralized identity systems. These systems let users manage their identity data while complying with KYC and AML checks. Blockchain is being tested as a safe way to give individuals control over their digital identities.

vi. Quantum computing: The rapid progress in quantum computing has experts convinced that it will soon be capable of breaking encryptions that are in use today. Blockchain projects must explore quantum-resistant cryptography to prepare their systems for the future.

Blockchain Regulatory Landscape

To successfully adopt blockchain, organizations must stay updated with the region's regulatory landscape. Here we list some of the laws, compliance requirements, and recent developments that organizations must be aware of

- **The United Arab Emirates (UAE)** is embracing blockchain through its Emirates Blockchain Strategy and the Virtual Asset Service Providers (VASP) Framework. Organizations must understand the laws shaping how blockchain is used in key areas like healthcare, education, transport, and finance.
- **The Kingdom of Saudi Arabia's** Vision 2030 focuses on using technology, including blockchain, to push its goal of economic diversification. The Saudi Arabian Monetary Authority (SAMA) has shown interest in blockchain by exploring its use in finance.
- **Other GCC countries** are also moving towards adopting blockchain. Bahrain and Kuwait have established regulatory sandboxes to test Fintech innovations. Bahrain, Qatar, and Kuwait's central banks have also released various guidelines and started initiatives. Organizations working in these areas must understand local rules well to stay compliant.
- **Egypt, Jordan, and Turkey** are showing more and more interest in blockchain's potential across different areas. This interest will lead to the formation of new regulatory systems in the coming years.
- **International collaboration** is also on the rise. Many countries are joining forces to deliver cross-border blockchain projects. Some GCC nations are reviewing or testing central bank digital currencies (CBDCs).

Key Considerations for Securing blockchain

When it comes to blockchain security, most challenges faced by organizations today can be addressed with careful planning. To succeed, teams need to foresee and tackle possible problems ahead of time.

Here we list a few key considerations:

i. **Blockchain infrastructure risks**: The 2016 DAO hack on Ethereum exploited a recursive call vulnerability, resulting in a $60 million loss and a controversial chain split. Weak infrastructure security can leave systems open to vulnerabilities that can compromise the immutability and reliability of the ledger, which can undermine the trustworthiness of the entire blockchain network.

ii. **Consortium blockchain vulnerabilities**: In 2020, a permissioned Hyperledger Fabric setup had weak access control settings that risked exposing data, showing why strong governance matters. Consortium blockchains bring together multiple groups working on a shared network. Keeping this shared space secure comes with its own set of tricky challenges. Ignoring these issues can cause arguments, give way to unauthorized access, and risk leaking confidential information shared by consortium participants.

iii. **Crypto exchange security**: In 2019, hackers targeted Coinbene and Cryptopia through hot wallet breaches and insider involvement, causing more than $40 million in losses. Blockchain exchanges attract hackers because of the valuable digital assets they manage. Weak security systems to protect trading platforms, secure user funds, or enforce KYC can allow unauthorized access, fund theft, service interruptions, and a loss of trust from users.

iv. **Benchmarking and comparative analysis**: Organizations need to benchmark and compare their blockchain security to measure it against global standards. This kind of comparison offers valuable insights into how effective their security protocols are and pinpoints where they can get better. It keeps blockchain systems in line with security practices followed worldwide. Skipping benchmarking might cause organizations to miss new threats, like the 2022 Ronin Network hack, where a $625 million loss occurred due to weaknesses in validator node security.

v. **Privacy and evolving laws**: GDPR violations became a concern when blockchain's unchangeable records clashed with the "right to be forgotten," leading to unclear legal situations. Balancing blockchain's transparency with a user's right to privacy, while accommodating developing laws, presents a considerable problem. To comply with new rules, adapting remains necessary.

vi. **Knowledge and skill gap**: Many errors in smart contracts, like the Parity Wallet freeze in 2017, happen because developers lack experience or miss rare issues. Strong blockchain security depends on deep knowledge of cryptography, smart contract building, and decentralized networks. However, there is a shortage of adequately skilled experts. Staying on top of the evolving security demands will require teams to develop the right skillsets.

Best Practices for Blockchain Security

Tackling new trends and challenges demands a comprehensive and holistic security strategy. Businesses can strengthen their blockchain setup by addressing these issues head-on, meeting regulations, and adapting as global blockchain security standards change.

Below is a list of best practices that large crypto organizations, including exchanges and crypto platforms, use to secure their blockchain systems and apps.

1. **Build a strong blockchain infrastructure**
    i. **Blockchain network review**: Conduct a comprehensive review of the blockchain network. It must include nodes, consensus systems, and data handling to identify and fix security risks. It should also involve strength-testing consensus setups to validate that they can handle attacks. Additionally, access controls, storage methods, encryption, and backup provisions must be evaluated.

    ii. **Blockchain network monitoring**: Use robust systems for continuous network surveillance. Many global platforms use consensus systems like Proof of Stake (PoS) to show their commitment to keeping their networks secure, which helps them gain trust from their clients and users.

2. **Evaluate exchange and wallet security**
    i. **Review the crypto exchange security**: Evaluate security to identify weaknesses. Examine transaction behavior to spot anomalies. Keep software updated and install patches regularly to fix known issues and maintain a safe working environment.

    ii. **Secure digital wallet key management**: Highlight the importance of handling keys with multi-signature wallets. Strategies like distributed key storage, using HSMs (Hardware Security Modules), regular key rotation, multi-party computation (MPC), and secure backup and recovery processes help create a strong system to protect keys. These steps reduce the risks of unauthorized access and help safeguard digital assets.

3. **Review smart contract and token security**
    i. **Smart contract audits**: Teams must check smart contracts to identify vulnerabilities. A deep review of the contract should spot problems that might harm its reliability, usability, or security. This check should cover code vulnerabilities and access controls, among other parameters.

    ii. **Token security protocols**: Establish strong safety systems to protect tokens, including encryption and restricted access. Big companies use advanced methods like offline storage, two-step verification, approved withdrawal lists, protections against DDoS attacks, and behavior tracking to guard digital assets.

4. **Enhance consortia interoperability with strong governance**
    i. **Consortium blockchain evaluation**: Assess the challenges collaborative networks face. Implement security measures that meet the specific needs of consortium blockchains. Use clear governance rules, enforce and update smart contracts for consortium activities, apply strong encryption for shared data, and conduct regular security training sessions for members.
    ii. **Interoperability checks**: Perform extensive testing to confirm that systems work well together and integrate. Shared frameworks, standard APIs, unified libraries, and teamwork across various organizations can highlight ways to support interoperability.
5. **Comply with privacy and regulatory mandates**
    i. **Privacy-focused technologies and regulatory compliance**: Use selective disclosure methods to improve privacy. Encrypt private information and provide cryptographic proofs of transaction validity to let users complete transactions. Conduct thorough compliance reviews to check whether regulations are being followed.
    ii. **User education and awareness**: Run tailored programs to teach blockchain security and encourage a habit of cyber resilience. Create guides and training tools, and host workshops for developers, users, and others involved in the blockchain system.
6. **Plan for resilience and scalability**
    i. **Incident response planning**: Teams should build and test plans to respond to security issues in blockchain systems. A good response plan helps teams act in an organized and prepared way. This significantly mitigates the impact of security breaches.
    ii. **Scalability planning**: Organizations should make sure the systems they create today can manage growing transaction numbers in the future without hurting their performance or security. To achieve this, they must fine-tune network throughput, use sharding, adopt Layer 2 solutions to ease congestion, perform regular tests to check performance, and work closely with blockchain solution providers.
7. **Proactive defense and threat intelligence**
    i. **Red teaming**: Work with red teaming experts to apply diverse approaches and strategies that simulate real-world attacks. This can identify possible gaps in blockchain security systems. Teams can use it to test how well current security measures work and to check how ready internal teams are to react to threats.
    ii. **Blockchain threat intelligence**: Use threat intelligence tools to stay updated on changing risks and weaknesses related to blockchain. Monitor security forums and advisories to prevent issues. Feed this data into security plans and incident responses. Share knowledge with the blockchain community to boost shared security.

Summary

Embracing blockchain requires a strong commitment to security. It is this commitment that will position governments and businesses as pioneers in leveraging decentralized technology based on trust and transparency.

To successfully adopt blockchain and make meaningful changes, organizations must prioritize the assessment of critical areas such as smart contracts, token safety, system interoperability, scalability, and user education and awareness.

Taking a strategic and holistic approach will help organizations launch a secure framework for mass adoption of blockchain and pave the way for a resilient future.

Want to conduct a comprehensive analysis of your blockchain security measures? Write to us!

Why team up with Protiviti

Protiviti is your trusted partner in a landscape where innovation and security intersect.

Technology keeps progressing, business strategies shift, and regulations continue to change. We tackle business challenges in a dynamic world to deliver innovative, efficient, and practical solutions.

As a global consultancy in Internal Audit, Risk, Business, and Technology, we help you step into the future with confidence.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Niraj Mathur
Managing Director
+971 502547507
Niraj.Mathur@protivitiglobal.me

Mohammad Sikkandar Sha
Director
+971 564868585
Sikkandar.Sha@protivitiglobal.me

Our Offices in the MENA

Abu Dhabi
Emirates Real Estate Corporation
Building, 7th Floor, Office 707-711
Al Falah Street, Al Danah,
P.O. Box 32468, Abu Dhabi, UAE

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area
Manama, Kingdom of Bahrain

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE

Egypt
Cairo Complex
Ankara Street Bureau 1
First Floor, Sheraton Area
Heliopolis - Cairo, Egypt

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
P.O. Box 1773, Safat 13018, Kuwait

Oman
Al-Ufuq Building, 2nd Floor
Office No. 26, Shatti Al Qurum
P.O. Box 1130, P.C. 112
Ruwi Muscat, Oman

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay
Doha, Qatar

Saudi Arabia - Dammam
Q1-5, The Business Quarter
Salman Al Farisi St,
Al Khalidiyyah Al Janubiyyah,
Dammam, Eastern Province, 32221,
Kingdom of Saudi Arabia

Saudi Arabia - Jeddah
King Abdulaziz Branch Road
Ash shati district , Building No. 7524
P.O. Box 3675, Jeddah 23412
Kingdom of Saudi Arabia

Saudi Arabia - Riyadh
Al-Ibdaa Tower, 9th & 18th Floor
King Fahad Branch Road, Al-Olaya,
Building No. 7906, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia

Face the Future with Confidence®

149892_SEP2025