

Episode 4

Security & compliances



Ghan Vashishtha



What will this webinar teach us?

Enterprise blockchain security and compliance norms, risks to weigh in before enterprise blockchain adoption

- Monitoring and security tools required to configure and manage your infrastructure.
- Technical showcase of the major new risks for enterprise blockchain and smart contract deployments
- Resources required to monitor for security vulnerabilities and updates in the blockchain and smart contract software
- Importance of a secure blockchain infrastructure management platform, its benefits, how these work, and the deployment patterns when considering secure communications for blockchain interactions
- Explore the web3 security tools
- Key examples of how enterprise-grade security offered by Zeeve for deployment and web3 infrastructure management can benefit businesses



Key pillars of blockchain security

1

Confidentiality

2

Data Integrity

3

Availability



Security Differs by Blockchain Types:

When building a blockchain application, it's critical to assess which type of network will best suit your enterprise goals. Private and permissioned networks can be tightly controlled and preferable for compliance and regulatory reasons. However, public and permissionless networks can achieve greater decentralization and distribution.

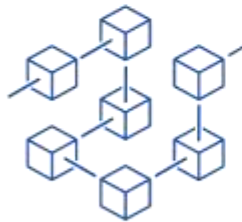




Public blockchains are public, and anyone can join them and validate transactions.



Private blockchains are restricted and usually limited to business networks. A single entity, or consortium, controls membership.



Permissionless blockchains have no restrictions on processors.



Permissioned blockchains are limited to a select set of users who are granted identities using certificates.





Zeeve Football World Cup Contest



Contest open till 18th December, 2022, 6:30 PM IST Click this link to participate NOW and SPREAD the word.

How fraudsters attack blockchain technology



Hackers and fraudsters threaten blockchains in four primary ways:

1. Phishing
2. Routing
3. Sybil and
4. 51% attacks.





A comprehensive security strategy for an enterprise blockchain solution includes using traditional security controls and technology-unique controls. Some of the **security controls specific to enterprise blockchain solutions** include:

1. Identity and access management
 2. Key management
 3. Data privacy
 4. Secure communication
 5. Smart contract security
 6. Transaction endorsement
- 
- 



Risk considerations that you should consider

1. Standard risk considerations
2. Smart contract risk considerations
3. Value transfer risk considerations



Standard risk considerations

Strategic

Business
continuity

Reputational

Information
security

Regulatory

Ops and IT

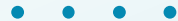
Contractual

Supplier

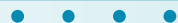


Smart contract risk considerations

Business and regulatory



Enforcement of contract



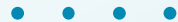
Legal liability

Information security



Value transfer risk considerations

Consensus protocol



Data confidentiality

Key management



Liquidity



10 Enterprise Blockchain Implementation Risks to Consider

1. Improper Logging & Monitoring
2. Insecure Deserialization
3. Sensitive Data Exposure
4. Cross-Site Scripting(XSS)
5. Injection
6. Security Misconfiguration
7. XML External Entities(XXE)
8. Broken Access Control
9. Using components with vulnerabilities
10. Broken Authentication

Components of an effective blockchain risk management framework

Risk considerations that you should consider

Business objectives

Growth / innovation

Client experience

Cost reduction

Improved time to market

Risk and compliance management

Core processes, supporting functions

Information technology

Human resources

Compliance

Finance

Other

Risk considerations

Standard risk considerations

Standard risk considerations

Standard risk considerations

Strategic Reputational Business continuity Security
Regulatory Ops and IT Contractual Supplier

Consensus protocol Data Confidentiality
Key Management Liquidity

Business and regulatory
Enforcement of contracts
Legal Liability
Governance

Operating model components

Governance and oversight

Policies and standards

Management processes

Tools and technology

Risk metrics and reporting

Risk culture



Blockchain Security tips and best practices

When designing a blockchain solution, consider these key questions:

1. What is the governance model for participating organizations or members?
2. What data will be captured in each block?
3. What are the relevant regulatory requirements, and how can they be met?
4. How are the details of identity managed? Are block payloads encrypted? How are the keys managed and revoked?
5. What is the disaster recovery plan for the blockchain participants?
6. What is the minimal security posture for blockchain clients for participation?
7. What is the logic for resolving blockchain block collisions?



Solutions to resolving blockchain risks and ensuring compliance

Administrators must define the security controls that mitigate the risks and threats based on the following three categories:

1. Develop a risk model that can address all business, governance, technology and process risks.
2. Enforce security controls that are unique to blockchain
3. Apply conventional security controls
4. Enforce business controls for blockchain





Address

Zeeve Deeptech Pvt Ltd
1283, ATS Greens, Sector-93A
Noida, India 201304

Zeeve Technologies Ltd.
2001, Regal Tower, Business Bay,
Dubai, UAE

Zeeve Inc.
395 Santa Monica Place, Unit 308,
Santa Monica, California - 90405



Contact

- Email: success@zeeve.io
- <http://www.zeeve.io>



USA



Dubai



India