Risk and Compliance Audit for Production Readiness of Blockchain Applications

Vishnupriya P T

Manager, KPMG India

—

27 May 2023

Agenda

- Setting the Context
- Production Readiness in Blockchain Context
- Risk Areas in Blockchain
- Typical Vulnerabilities
- Control Areas in Blockchain
- Conclusion

01

Setting the Context

Why do we need Risk and Compliance in Blockchain?

Threats and vulnerabilities are constantly evolving

$17.9B
Estimated global spend on blockchain solutions by 2024

Anonymity, immutability, and distributed control make blockchain a disruptive technology. They are also its greatest vulnerabilities.
- Stuart Madnick, MIT

Unique risks in blockchain space while regulatory boundaries are hazy

Multiple frameworks for assessments but lack of standards to provide guidance

$1.76T
Blockchain boost in global GDP by 2030

The Music Has Stopped': Crypto Firms Quake as Prices Fall

NYT, June 2022

Source : 51 Critical Blockchain Statistics: 2023 Data Analysis & Market Share - Financesonline.com

Regulatory Challenges in Blockchain

Data Security and Privacy

There are several regulations that are relevant to data security and privacy irrespective of the type of implementation.

Industry Specific Regulatory Issues

Depending on the use case of blockchain implementation, additional compliance requirements may be required to be adhered to.

Internal / External Audits

Depending on the scope of the blockchain use case and skills possessed by the auditing team, the coverage for blockchain specific risk may be shallow or deep.

Geography Specific Challenges

There are challenges with region specific requirements that organizations must be aware of prior to deploying blockchain in production.

Status of Crypto Regulation

There are 4 categories of geographies with regards to cryptocurrency regulation as mentioned below.

Source : PwC Global Crypto Regulation Report 2023 - Amended to include the BCBS rules

Global Regulatory Challenges of Cryptocurrency

Across cryptocurrency implementations, there are five major challenges that are encountered by investors and auditors alike. They are mentioned below.

01
Legal Qualification

02
Asset tracking and recovery

03
Lack of investor protection mechanism

04
Volatility

05
Complexity due to multiple jurisdictions

03

Production Readiness in Blockchain Context

Production readiness in the context of blockchain

Some of the key areas to assess production readiness for blockchain implementations are

Governance

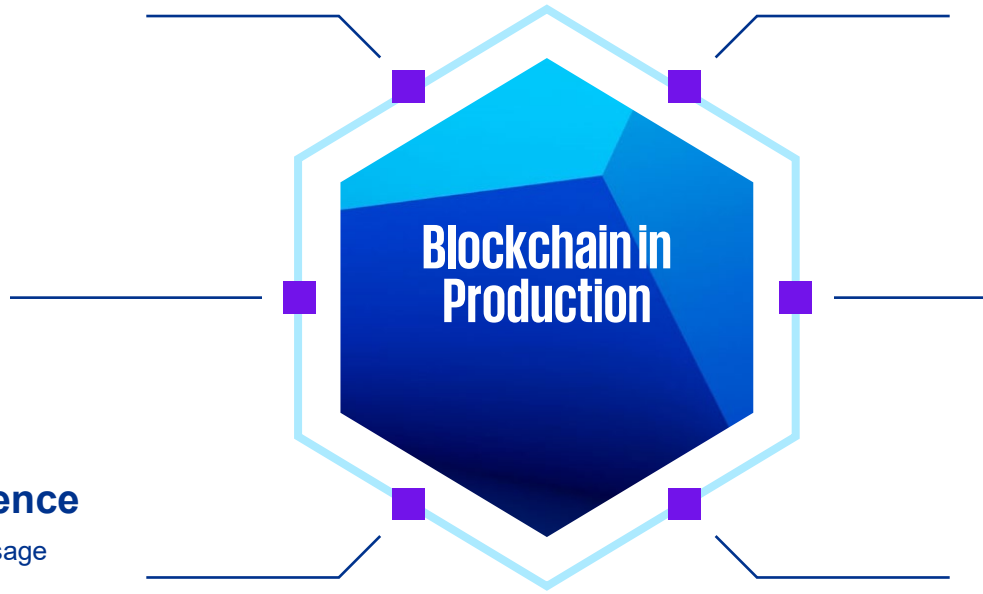
Defined roles and responsibilities
Stakeholder accountability
Defined process (e.g. Change management process)

Compliance

Regulatory Compliance
Contractual obligations

Infrastructure Resilience

Scale for anticipated customer usage



Interoperability

Compatibility with existing systems
Reuse existing functionality
Consistent processes

Security

Identify vulnerabilities
Independent Assessments
Consider the scope of coverage for testing

Documentation / Training

User familiarization
Support

04

Risk Areas in Blockchain

Key Risk Areas

Risk in blockchain applications is not always in the implementation. In some use cases, risk is introduced due to inherent flaws in processes and design of the system.

Untested code

Multiple node failure / System Disruptions

Regulatory Compliance

Strength of encryption protocols

Interoperability

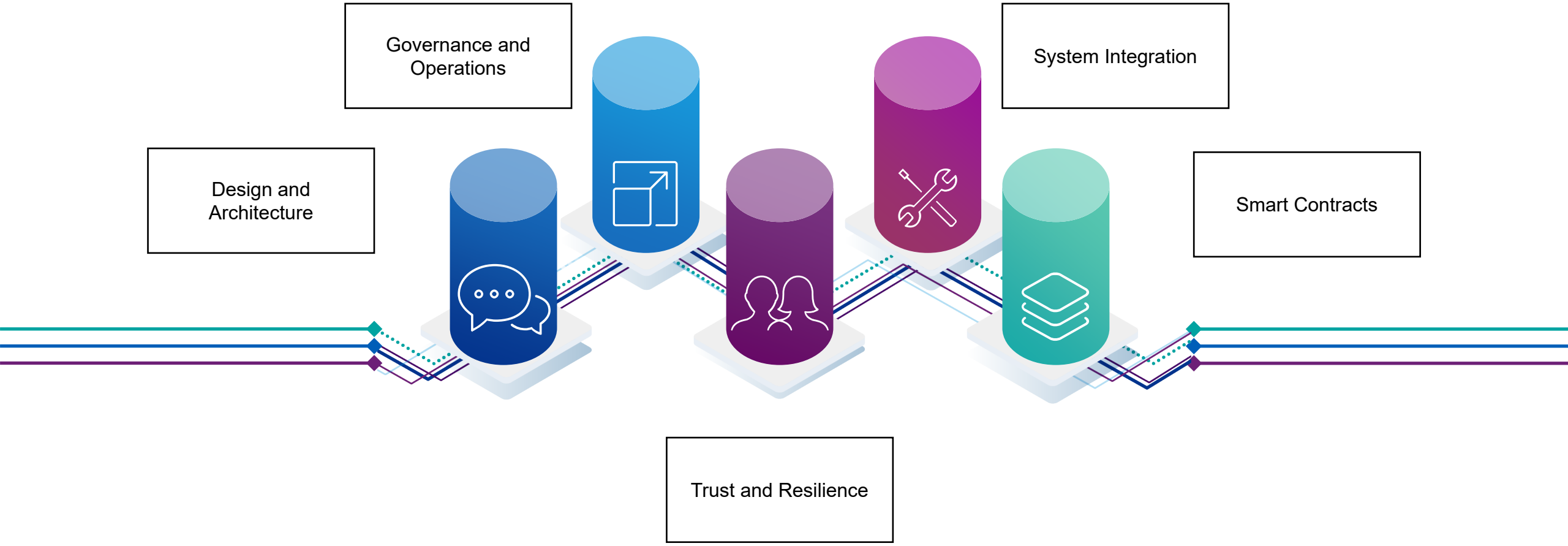
Data Privacy

Design and robustness of consensus mechanism

Design of smart contracts

ASC Risk Assessment Framework

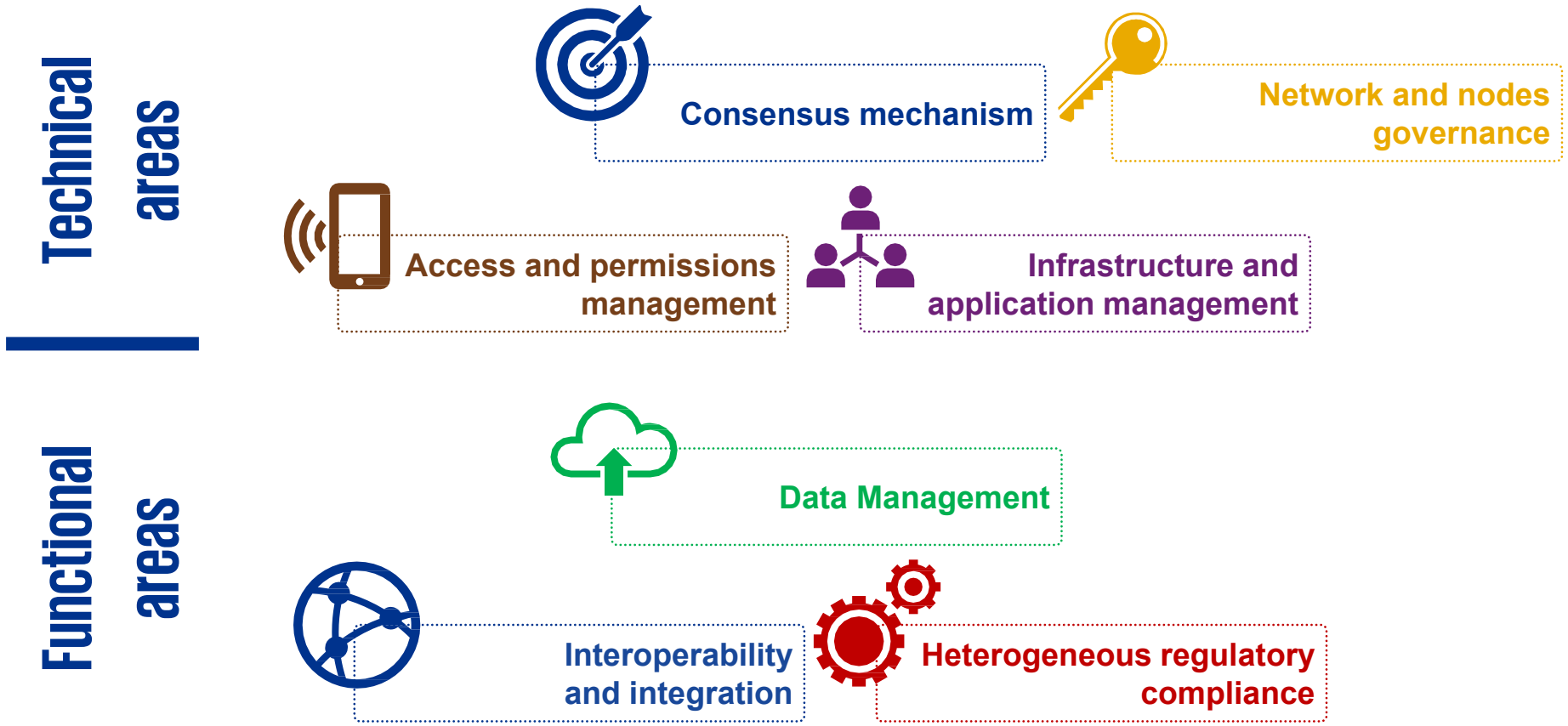
Accredited Standards Committee registered with ANSI has provided a Risk Assessment Framework for Blockchain implementation covering the following five pillars.



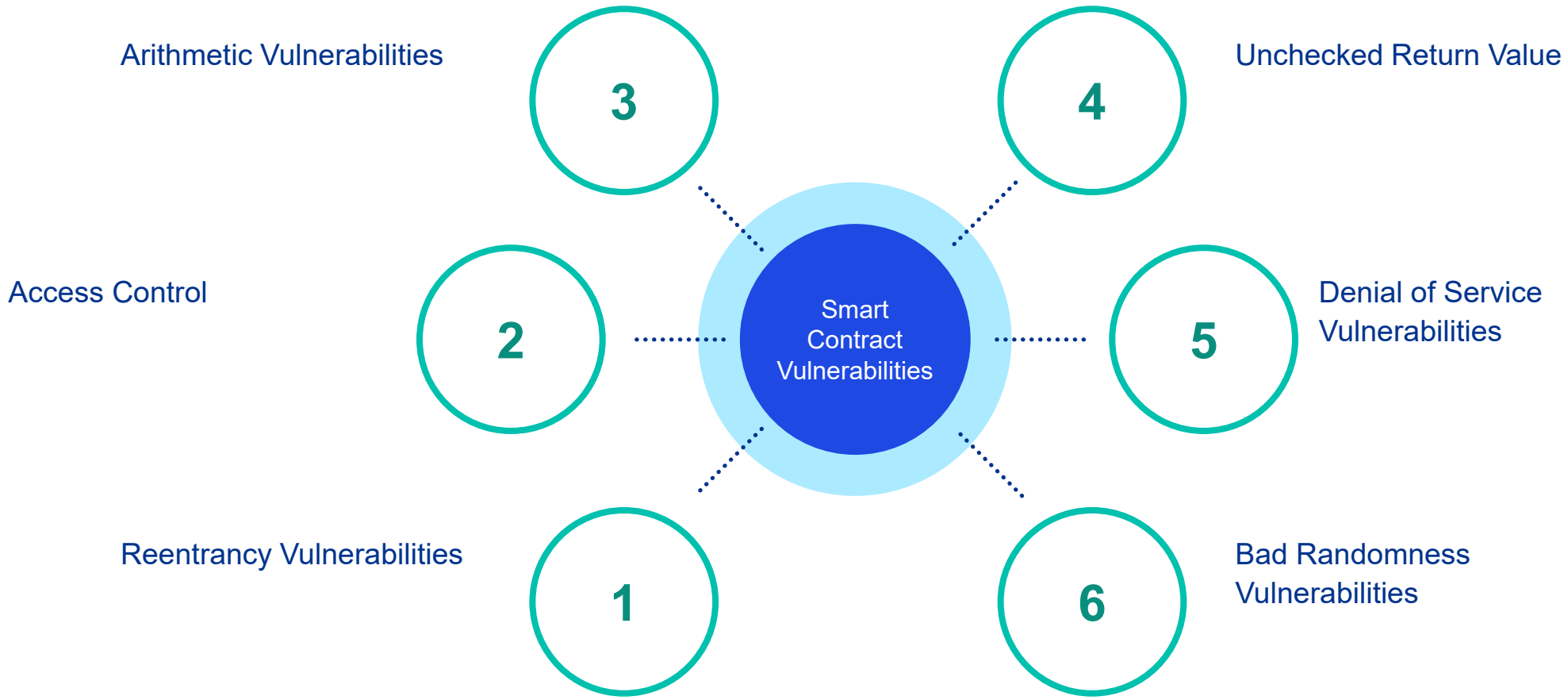
Typical Vulnerabilities

Vulnerabilities – Where are They?

There are 7 domains that are primarily relevant to validate the existence of risks and vulnerabilities in a blockchain implementation.



Smart Contract Vulnerabilities



System Level Vulnerabilities

01
EOS Vulnerability

The EOS Vulnerability

EOS is an open-source smart contract platform. Attackers writing vulnerability in the parsing function allowed malicious smart contracts to exploit the EOS blockchain software.

02
The Verge Hack

The Verge Hack

The Verge cryptocurrency was hacked through the combination of its own built-in features like Flexible Timestamps, Difficulty Updates, Consensus Algorithm

03
GDAC Hack

GDAC Hack

One of the first attack on a centralized crypto exchange in 2023 GDAC, a South Korean CEX, was hacked for almost $14 million on April 9 after the culprit gained control over the exchange’s hot wallets.

04
The Veritaseum hack

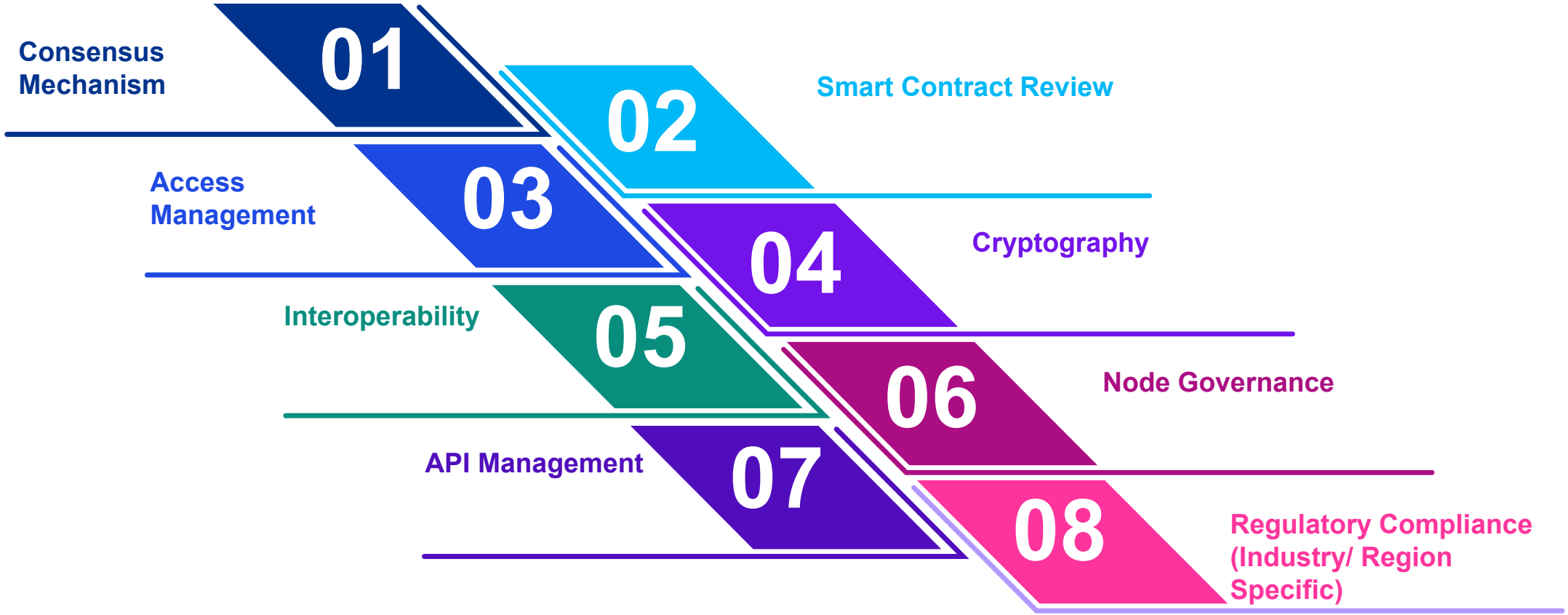
The Veritaseum hack

The Veritaseum cryptocurrency's smart contract allowed reentrancy attack, In a reentrancy attack, an attacker can run a smart contract's function repeatedly before the state of the contract is changed,.

06

Typical Controls in Blockchain

Control Areas in Blockchain



ASC Risk Assessment – Control Areas

Accredited Standards Committee registered with ANSI has provided a Risk Assessment Framework for Blockchain implementation covering five pillars.

Data provenance	Proprietary systems	Standards	Identity management
Data integrity	Smart contract security assessment	Change management	APIs
Data confidentiality	Inception and execution of smart contracts	Managed services (hosted)	Interoperability
Nodes	Governance	Other external blockchain or other distributed networks (multi-chain)	External data sources
Programming languages	Maintenance responsibilities	Cryptographic algorithms	
Code review and maintenance	Access management	Public key infrastructures	
Open source	Jurisdictional laws, regulations, and rules	Resilience, data persistence and continuity of operations	

- Design and Architecture
- Governance and Operations
- Trust and Resilience
- System Integrations

Typical Controls

- Data Provenance: Ownership, origin and lineage of on chain and off chain components are maintained
- Data Integrity: Integrity of on-chain data and the transactions are maintained and known throughout
- Data confidentiality: Governance over authorized roles, sensitivity on what can be stored
- Node Risk Management: Managing access rules, business rules, monitoring performance and updates
- Programming language Considerations: Language in use is appropriate for use case and technical architecture diagram is maintained
- Periodic Code Review: Code reviews are performed whenever changes are introduced in the code supporting the platform.
- System Integrations: API security, system resiliency,
- Smart Contract Security Assessment: Smart contracts are assessed for security and quality
- Governance: Governance in Consensus protocols, access management, change management and applicable regulations
- Consensus Protocol Vetting mechanism: Process exists to vet any changes to consensus mechanism in the platform.
- Access Management: Authorization of roles assigned, process of granting and revoking access provided to the DLT platform
- Change Management: Changes are authorized, tested, approved and verified prior to implementation
- **Cryptography: Hashing for data integrity, digital signatures for identity management, certificate management**
- Interoperability: Interoperating with multiple DLT platforms, legacy systems

Smart Contract Audit Tools

Mythx is a security analysis platform that provides smart contract analysis and vulnerabilities detection

Mythx

Quantstamp is a smart contract security audit tool Ever since it came into existence, the tool has been used by various organizations and Maker Foundation is one of them. Users can fetch detailed vulnerability reports including their impact on the contracts code and their severity

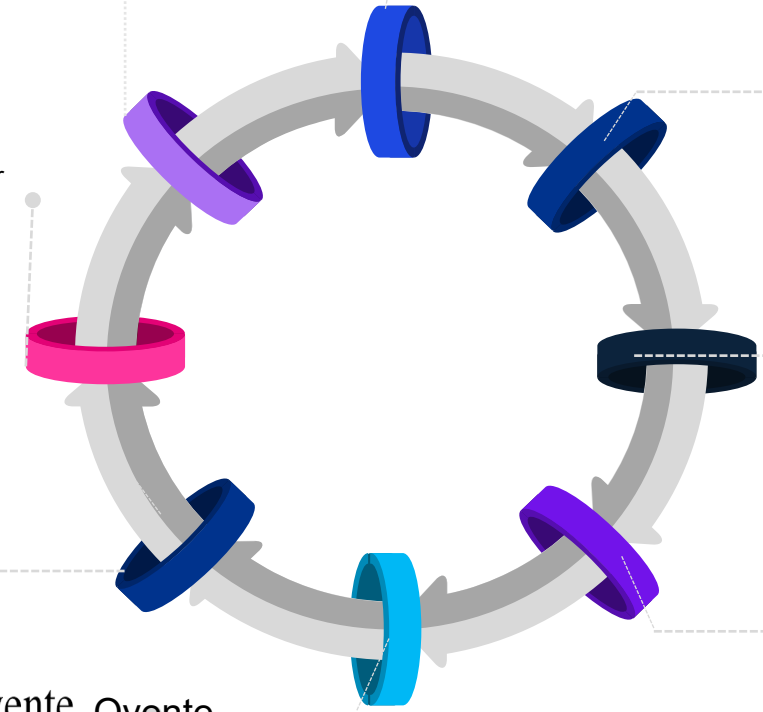
Quantstamp

Slither is a solidity static analysis framework. It runs a suite of vulnerability detectors. It provides an API to write custom analyses

Slither

Cyberscan

It is a convenient tool that helps investors to quickly gain insight into a given cryptocurrency token. The tool is very simple and easy to use, all you need to do is paste the smart contract address to the related field



CertiK is a top smart contract security audit platform that identifies flaws in smart contracts code using formal verification. it uses both static and dynamic methods to find potential vulnerabilities and errors in the smart contract.

Certik

Smartcheck

SmartCheck is a unique tool that identifies flaws in smart contracts code using machine learning algorithms. It provides developers with detailed reports citing potential attack scenarios and source code locations

It is an open-source security audit tool. it help auditors detect gas limit vulnerabilities and potential divisions. This tool creates a visual representation of the smart contract's flow graph to help developers understand

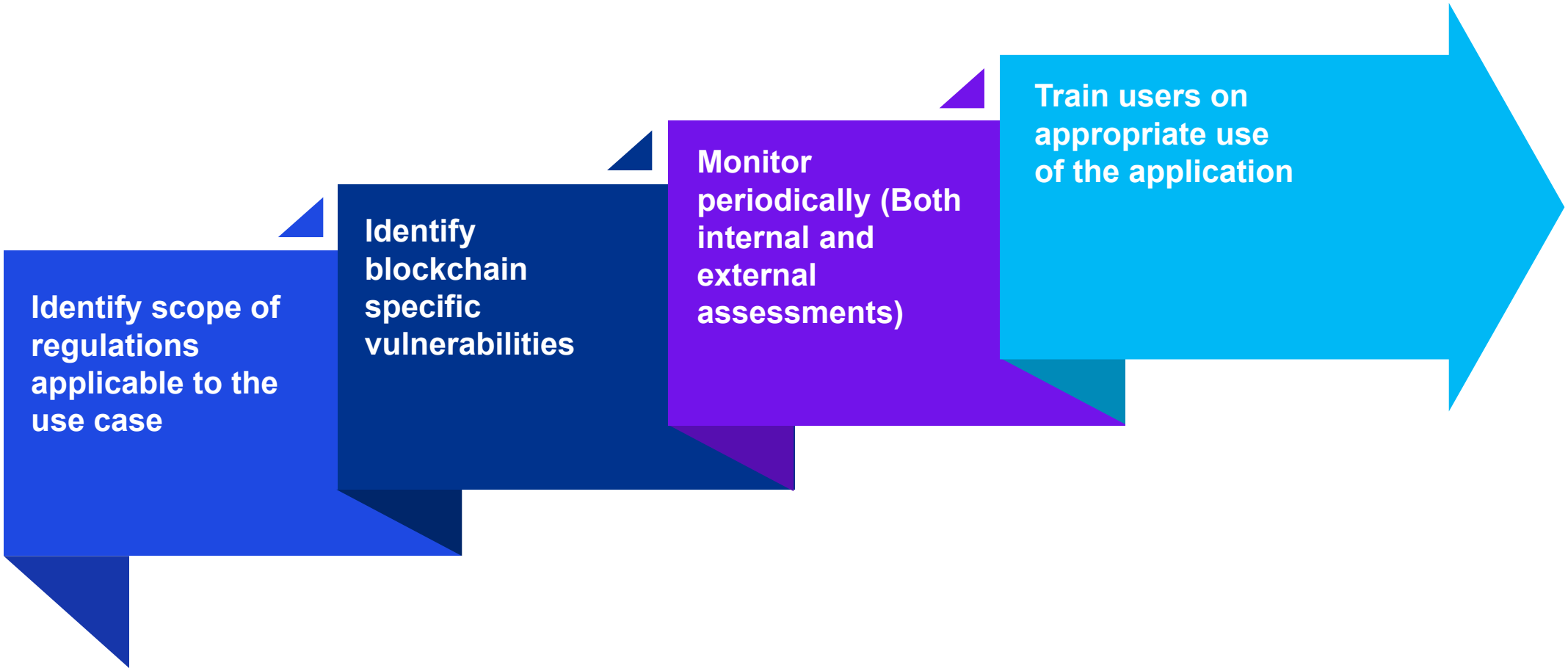
Oyente

BlockchainSentry

It is a Cloud based and provides a cyber security platform that uses blockchain technology for scanning, analyzing, prioritizing and providing remediation suggestions to help users in identifying and fixing contract vulnerabilities

Key Takeaways

A few takeaways from today's session-



Thank you

Vishnupriya Pallikaranai Thirumalai
Manager, Digital Trust
KPMG India
LinkedIn – www.linkedin.com/in/vishnupriya-pt