



Auditing blockchain solutions

October 2018

[KPMG.com/in](https://www.kpmg.com/in)

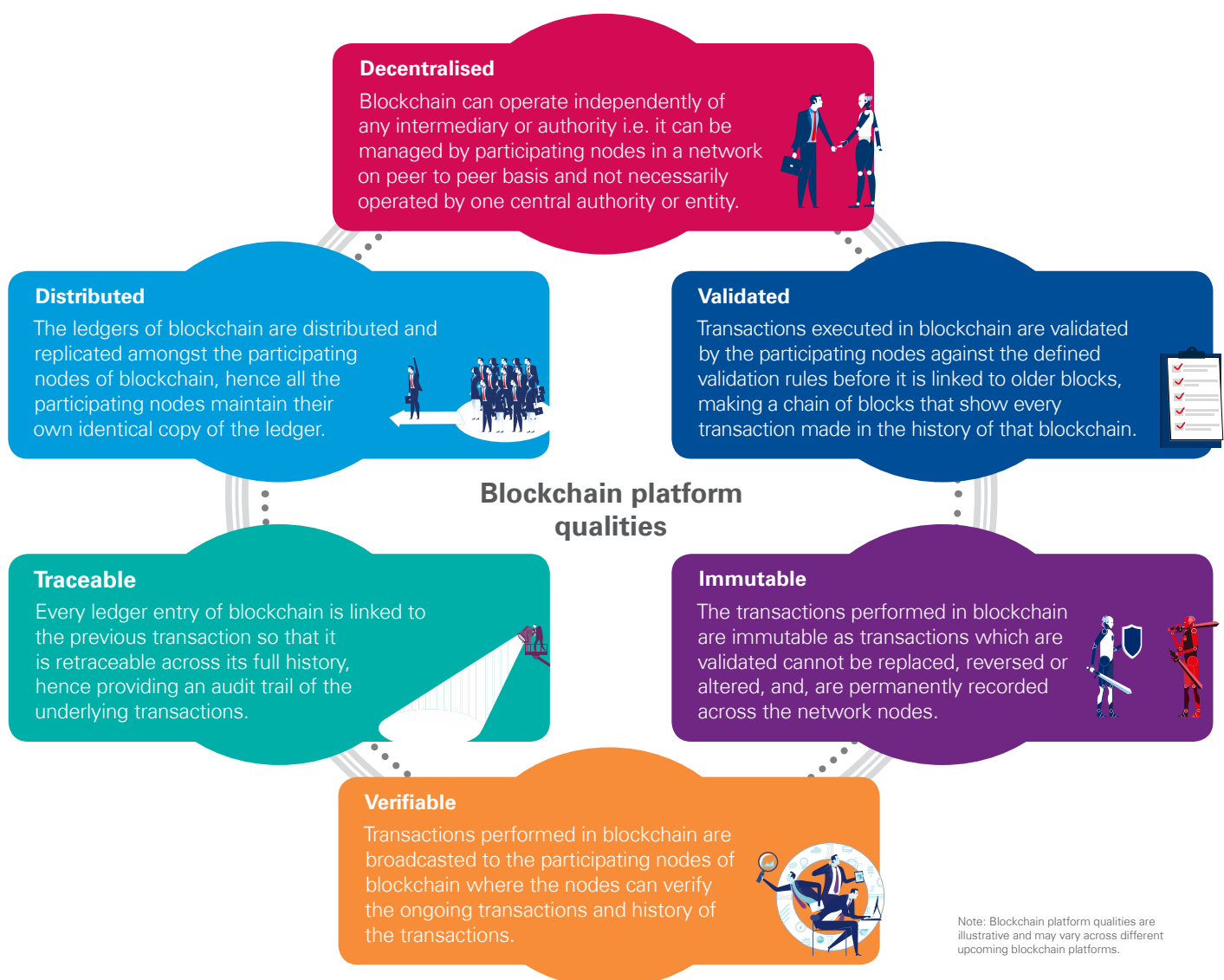
Introducing the chain of blocks

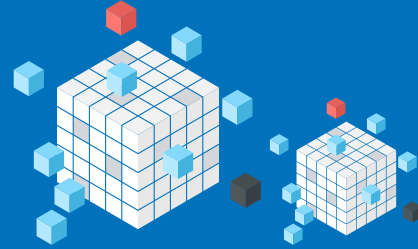
In the current digital era, businesses across the world are running transactions of humongous volumes. Blockchain technology is a step towards modernisation of digital infrastructure and allows the reorganisation of data and assets. Blockchain solutions across industries are helping solve complex problems with use of its platform and technology qualities, yet it remains a question whether we are ready to handle the risks that these solutions can bring in.

Traditional models of audit fail to take into consideration many of the risks associated with blockchain-enabled processes, and hence there is

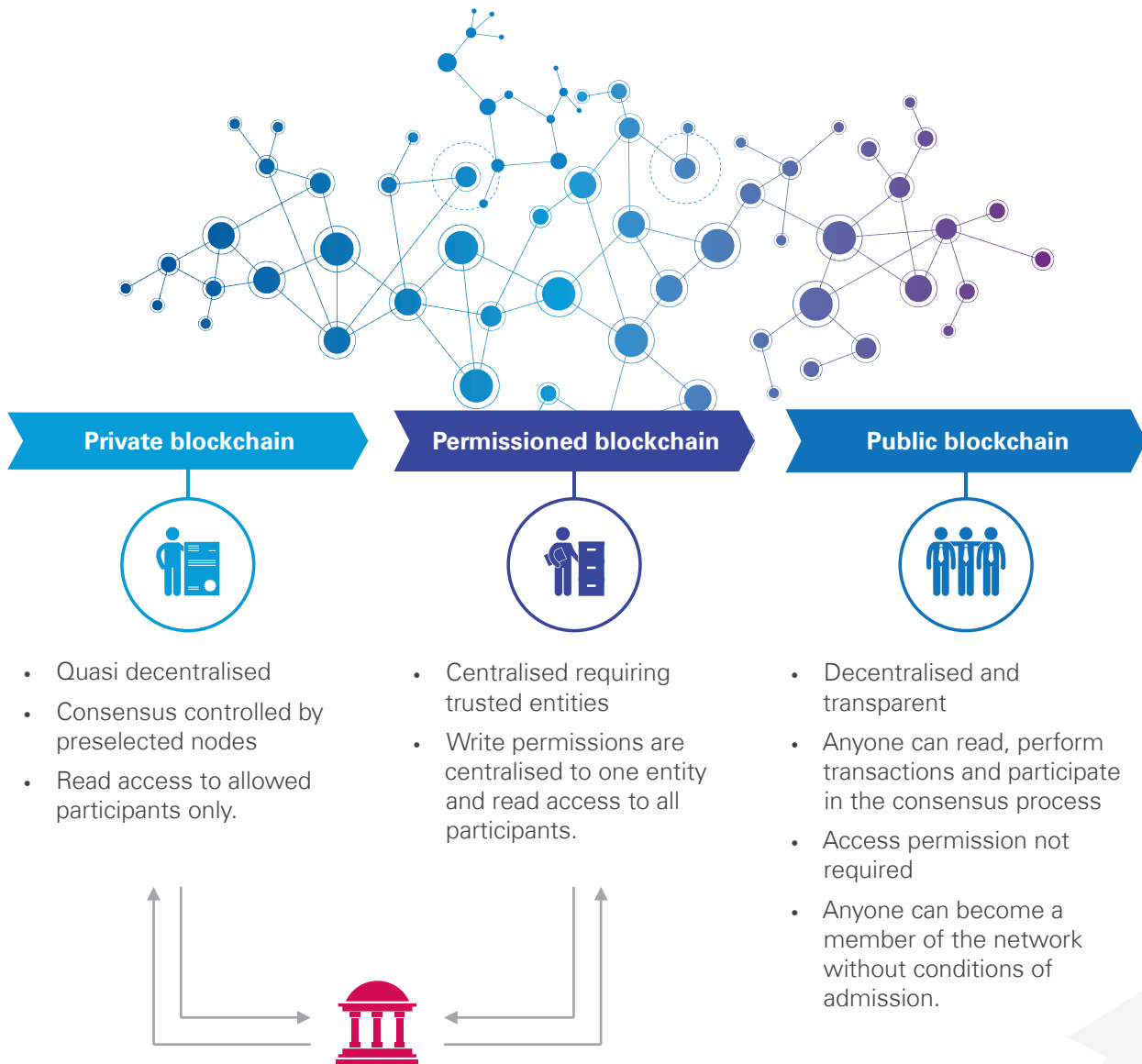
a need to understand the specific set of risks and develop an evolved auditing approach for blockchain-based solutions.

This whitepaper explores potential audit areas from a supporting technology controls perspective that organisations should consider while implementing blockchain solutions. Auditors reviewing processes built on blockchain can adopt this audit framework to test controls around the implementation of such solutions.

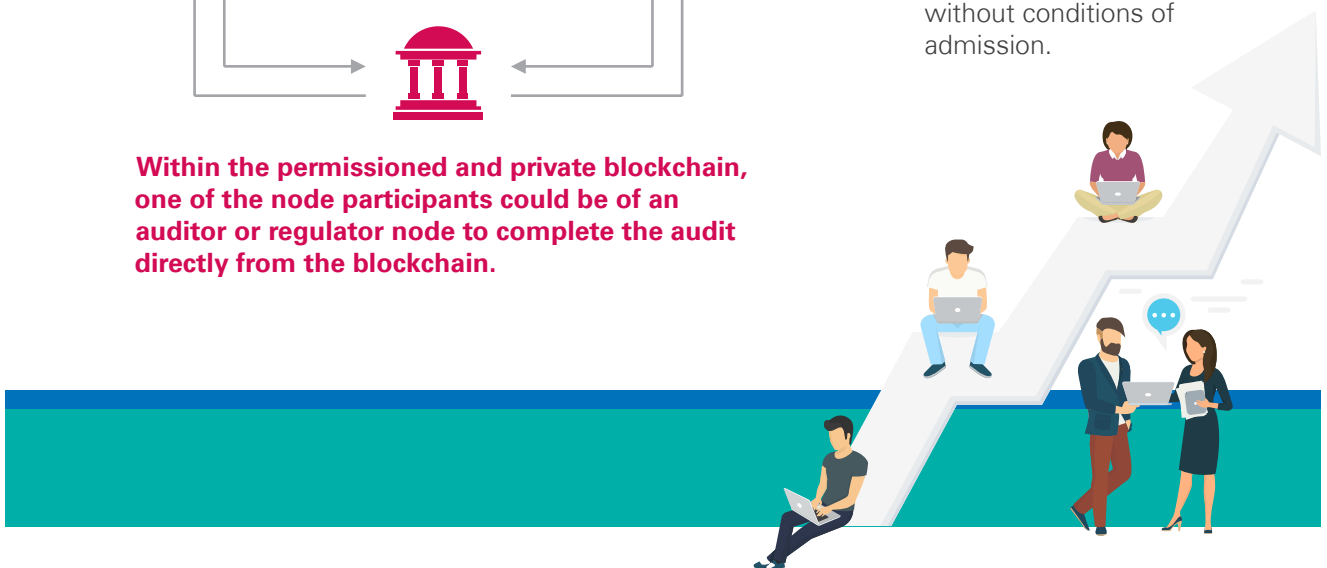




Implementation options of blockchain



Within the permissioned and private blockchain, one of the node participants could be of an auditor or regulator node to complete the audit directly from the blockchain.



Breaking the boundaries

Blockchain's first use case which made headlines¹ was financial transactions using bitcoin. Since then, there has been an extensive research into blockchain's potential. Today, various blockchain-enabled real world use cases have shown capabilities to revolutionise many industrial sectors such as financial services, healthcare, automotive, telecommunication, media and entertainment, retail and agriculture.

Tracking prescription drugs and preventing counterfeit products



In response to the need to secure the pharmaceutical supply chain, blockchain-based system acts as an interoperable system, and can track change of ownership of prescription medicines. It has the ability to verify the origin of serialised global trade identifiers and trace the source of drugs to their original manufacturers. Data

privacy can be also met using zero knowledge technology where all transactions posted to the blockchain are fully encrypted. A zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any additional information.

Adopting trade finance solution to facilitate paperless trade and transparency



Blockchain solution digitises and automates paperwork filings for the import and export of goods by enabling end users to securely submit, stamp and approve documents across national and organisational boundaries. This solution provides thorough supply chain visibility that enables all parties involved i.e. network of

shippers, freight forwarders, ocean carriers, ports and customs authorities in a global shipping transaction to securely and smoothly exchange shipment events in real time. They can also see the status of customs documents or view bills of lading and other data as part of trade finance.



Use cases across sectors

01

Telecommunication

Blockchain can streamline the internal operations of telecom industry such as billing, roaming, network function virtualisation management, digital asset transactions, mobile money and identity-as-a-service.



02

Healthcare

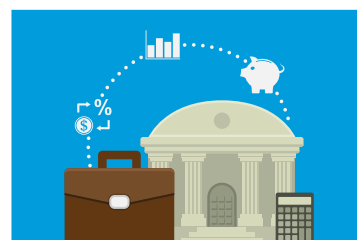
Blockchain has use cases in the healthcare/ pharmaceutical sector to improve electronic medical records, and for facilitating new drug development and medical innovation.



03

Banking

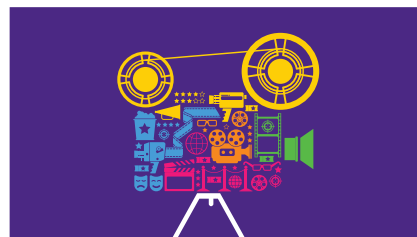
Blockchain can be used for derivative trading to connect potential buyers and sellers on a decentralised network to update the information on a continuous basis.



04

Media

Blockchain can help in maintaining the database of digital rights to avoid copyright issues, use smart contracts for payment of media owners and track the ownership of concert tickets.



05

Retail

For food safety, blockchain can allow consumers to track the origin of food items and enforce transparency in food supply chain from farm origination details to storage of food in retail stores.



06

Automotive

Blockchain can help the automotive industry in product life cycle management thus tracking the full history of a vehicle from pre-production to sale.



Risks in the landscape

It is becoming apparent that blockchain presents a plethora of opportunities for several sectors, however, it is not a foolproof solution.

Blockchain solutions and their implementations pose risks which include the following:



Difficulties in tracking and implementing 'right to be forgotten' privacy mechanism for personal information erasure



Misconfigured access permissions, consensus and proof of stake mechanisms leading to transaction trust issues



Issues arising out of lack of governance mechanisms leading to non compliance of transactions and regulatory penalties



Concerns around unencrypted personal and confidential information contained in global transactions leading to regulatory concerns



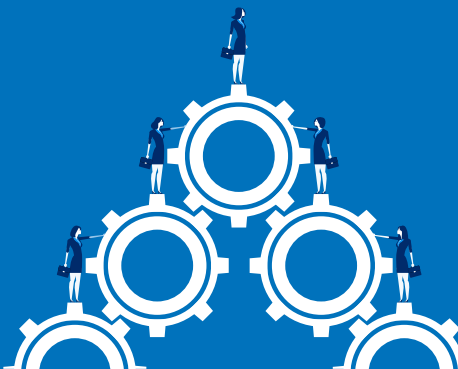
Challenges in interconnecting different blockchain protocols and data formats creating solution implementation roadblocks



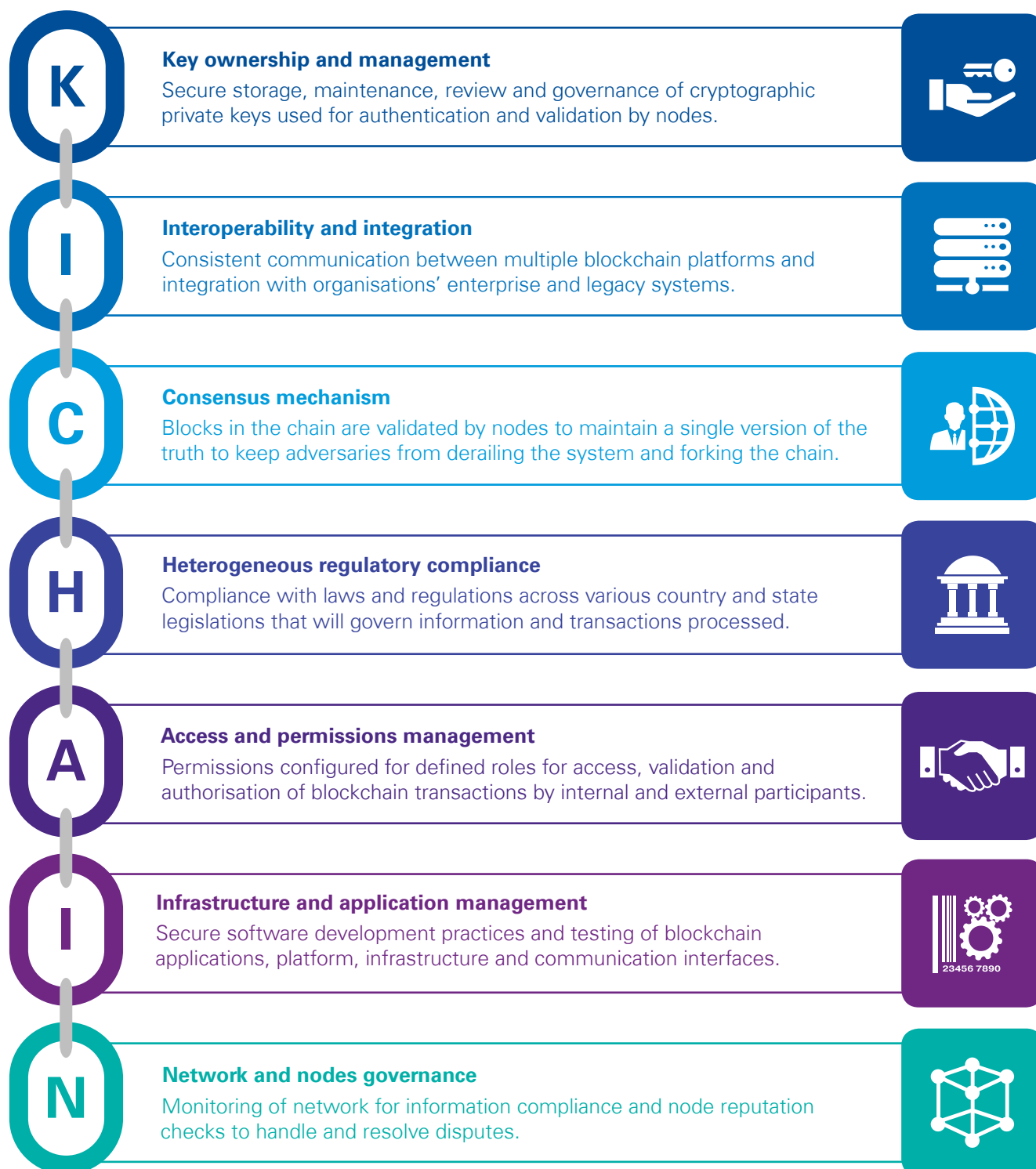
Challenges in securely maintaining the cryptographic keys or weak encryption leading to permanent loss of the whole data



These are the risks that elicit the need for an audit framework to build trust towards the technology. Leveraging an effective audit framework can help harness and mitigate a number of specific risks that blockchain brings to the table.



KPMG in India's framework for auditing blockchain solutions has been developed keeping in mind specific risks that blockchain models entail.



KPMG in India's blockchain solutions audit framework

Framework modules	Risk areas	Audit areas
Key ownership and management 	- Accidental loss of stored cryptographic keys resulting in inability to claim asset ownership - Inability to change cryptographic private keys shared with other participants for legitimate business needs - Unsecure or unencrypted storage, transmission and use of cryptographic private keys.	- Key generation and decommissioning - Key maintenance and governance - Logging and auditing of key usage - Key management infrastructure - Key traceability and version control - Hash algorithm management.
Interoperability and integration 	- Misinterpretation or misuse of data sent by disparate blockchain platforms - Security issues of Application Program Interface (API) used for integrating blockchain platform with enterprise system - Data quality and legacy issues when interfacing with legacy systems.	- Interface/API documentation review - Data mapping and integration - Data validation checks and rules - Intermediary platform and protocols - Interoperability connectors and plugins - Secure interfaces and API review.
Consensus mechanism 	- Uncontrolled changes, majority hash rate attack or hijack by a coalition of dishonest counterparties - Inconsistencies due to forking issue creating two versions of groups and ledgers - Inaccurate timestamps when connecting to a node to alter a node's network time counter.	- Consensus protocol design - Consensus change control procedure - Review of consensus rules - Transaction log and audit trail - Consensus override handling - Consensus hijack monitoring.
Heterogeneous regulatory compliance 	- Unencrypted Personally Identifiable Information (PII), Patient Health Information (PHI) or Financial data published in global transactions - Differing privacy, regulatory and compliance requirements for cross-border data flow - Inability to remove or change sensitive or confidential data impacting 'right to be forgotten' principle.	- Country specific laws - Industry regulatory compliance - Cross-border privacy regulations - Platform compliance standards - Data sensitivity in transaction blocks - Data classification standards.



Framework modules	Risk areas	Audit areas
Access and permissions management 	- Corporate data stored on blockchain is discoverable without explicit authorisation - Privilege escalation through confused deputy problem to misuse the authority - Misconfigured restrictions and insecure deserialisation by authorised user on permissioned blockchain.	- Group and user permissions - Roles and level of access - Discretionary access control - Enrollment and termination procedures - Segregation of duties and conflict of permissions.
Infrastructure and application management 	- Inconsistent development and unsecure coding practices for blockchain platform and application - Lack of Software Development Life cycle (SDL) processes, adequate testing and documentation - Security vulnerabilities related to development, configuration, implementation and deployment.	- Software development life cycle - Platform and application documentation - Secure coding principles and development practices - Bug tracking and application patching - Cybersecurity testing.
Network and nodes governance 	- Lack of intermediary or governing body to settle and resolve asset, identity or transaction disputes - Network centralisation, collusion, spam and unauthorised controlling of network operations - Unclear accountability of blockchain functioning, information protection, transaction validations.	- Governance and dispute resolution - Network compliance and node reputation checks - Single point of failure analysis - Network monitoring and spam analysis - Data leakage prevention mechanism.

Concluding thoughts

Blockchain is anticipated to disrupt and innovate industries with use of its business models making use of digital ledger technologies. Yet, the sheer excitement over this innovative technology and its promising potential has eclipsed the possible threats and risks arising from its implementation.

As blockchain continues to build significant momentum, companies cannot turn a blind eye to security and risk management any longer. Blockchain may even provide a false sense of security through some primary features around cryptography and

immutability. It is now time to seriously think about its true risks and take steps towards applying audit considerations for assessing those risks.

Moving forward, we believe organisations implementing this technology and the auditors entrusted with the task of validating and reviewing solutions built on this technology might need to adopt a customised audit framework for blockchain. By leveraging this framework, organisations can be better equipped to implement secure and resilient solutions around this emerging technology.

KPMG in India contacts:

Mritunjay Kapur

National Head

Markets and Strategy

Head - Technology, Media and Telecom

T: +91 124 307 4797

E: mritunjay@kpmg.com

Akhilesh Tuteja

Partner and Head

Risk Consulting

Co-leader – Global Cyber Security

T: +91 124 307 4800

E: atuteja@kpmg.com

Atul Gupta

Partner and Head

IT Advisory - Risk Consulting

National Leader - Cyber Security

T: +91 124 307 4134

E: atulgupta@kpmg.com

Kunal Pande

Partner

IT Advisory - Risk Consulting

National Leader - FS in Risk Consulting

T: +91 98926 00676

E: kpande@kpmg.com

Priya Rajaram

Director

IT Advisory - Risk Consulting

T: +91 99204 53147

E: prajaram@kpmg.com



Follow us on:

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is meant for e-communication only.