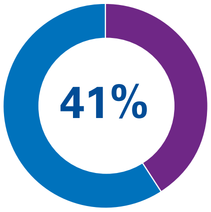
KPMG

Blockchain

KPMG technology risk insights

What is blockchain?

Blockchain is a system in which a record of transactions is maintained across multiple computers (nodes) that are linked in a peer-to-peer network. It removes the need for intermediaries such as banks or brokers to serve as a third party.



41 percent of business leaders believe their companies should have invested more in blockchain over the past five years.[1]

$19b

Global spending on blockchain solutions has been forecasted at $19 billion by 2024.[2]

How does blockchain work?

Cryptography

A blockchain is a chain of blocks that contain transaction information:

- Each block of data contains a unique hash key, which is like a fingerprint, used to identify a block and its contents.
- Each block contains transactions, a hash, and a copy of the hash of the previous block (with the exception of the genesis block, which has no previous block hash). This concept makes the blockchain immutable. If data from a previous block changes, then its hash changes, disconnecting it from the proceeding chain of blocks.

Distributed ledger

Instead of relying on a central authority to manage the ledger, blockchains use a distributed peer-to-peer network:

- When someone joins the network, they download a full copy of the blockchain. Each new user, or computer, to the network is called a node.
- Distributed peer-to-peer architecture provides benefits of higher availability than traditional client-server based networks, as there is no single point of failure.

Consensus

New transactions are sent to all nodes, which then get validated and grouped into blocks:

- Consensus ensures that peers on the network agree upon a consistent state of records.
- Once consensus is reached, the new block is posted on every node's blockchain.
- Nodes will reject blocks whose data violates the protocol's rules or appears to have been tampered with.
- Common consensus mechanisms include Proof of Work (PoW) and Proof of Stake (PoS).

Smart contracts

The main difference between a traditional contract and a smart contract is that smart contracts are automated:

- A contract is created between parties.
- Parties can choose to remain anonymous.
- Predefined triggers are initiated.
- The contract self executes as defined by the source code.
- A participant can analyze all activities and make informed decisions.
- The data captured can be used for analytics and reporting.
- Data is fed into blockchains and used for smart contract execution from external sources, specifically data feeds and APIs; a blockchain cannot directly "fetch" data. These real time feeds are called 'oracles' which operate very much like middleware between the data and the smart contracts.

Sources

[1] AP News, "CFOs Are Ready for Digital Transformation in 2021, New Survey Shows," February 2021

[2] Yahoo! Finance, "Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024, According to New IDC Spending Guide," April 2021

Key blockchain risks

Adoption of blockchain technology exemplifies a firm's investment in innovation, but with innovation comes new risks.

To unlock the full potential of distributed ledger technologies, organizations should proactively identify and mitigate all risks posed by the adoption of the technology.

KPMG is here to help maximize your company's investment while helping to manage potential risks.

Governance

- Blockchain Design and Standards
- Policies and Procedures
- Vendor Management
- Identity Access Management
- Regulation and Compliance
- Asset Provenance
- Anti-Money Laundering
- Sanctions

Infrastructure

- Blockchain Network Risks
- Software Vulnerabilities
- Protocol Management
- Integration
- Interoperability
- Node Management
- Consensus Mechanism

Data

- Data Management
- Privacy Management
- Disaster Recovery
- Offchain Information Management
- Blockchain Bloat
- Data Integrity
- Know your Customer

Key management

- Public and Private Key Management
- Entropy
- Key/Protocol Security
- Sharding
- Multi-sig
- Wallet Management
- Hardware Security Module (HSM) Access

Smart contracts

- Smart Contract Development
- Smart Contract Design
- Code Review and Maintenance
- Denial of service Risks
- External Source Risk
- Legal Risks

Development

- Underdeveloped standards:
  - Currently, blockchain doesn't have proper standards due to its rapid growth. With different organizations working on their "own" blockchain, it is hard to standardize them.
- Standardization across industries and blockchains:
  - The wide variety of frameworks means that there is a lack of standardization. This is potentially one of the biggest risks that the current blockchain projects suffer from. These standards apply across the complete blockchain ecosystem including Initial Coin Offerings, cryptocurrencies, frameworks, and so on.
- Integration and interoperability into existing systems and between blockchains
- Untested code:
  - The quality of the code remains a big concern to most of the blockchain solutions. Decentralized organizations need to take extra care when they deploy their solutions. One such example is the Decentralized Autonomous Organization (DAO). It is an autonomous system that automates the whole organization.
  - The DAO Hack is one of the most infamous hacks regarding blockchain technology. Created in 2016 and known as "The DAO," the incident resulted in the loss of approximately $50 million of Ether through an exploitation in the open source code.*

**A $50 million hack just showed that DAO was all too human, Wired,* June 18, 2016.

Blockchain use cases span across industries and functions

Retail

Tokenized loyalty

Enabling a loyalty ecosystem across partners driven by a single, blockchain-based wallet that allows customers to seamlessly accrue, redeem, or convert loyalty points across the company's business units and service offerings

Healthcare and life sciences

Drug supply chain

Digital trust infrastructure, backed by blockchain, enables participants to authenticate vaccines, validate capacity to fulfill orders, predict demand, and take preventative actions against shortages

Central bank digital currency

Virtual currency

Leveraging the distributed ledger to implement a virtual currency strategy to support the development of the national economy and diversify the sources of income for central banks

Procurement

Fixed assets tracking

Tracking the shipment, disposition, distribution, and lease lifecycle of physical assets, such as laptops, printers, copiers, etc., to reduce administrative cost, and automate inefficient manual processes

Manufacturing

Parts provenance and customs tracking

Leveraging the digital ledger to track parts as they are shipped, imported, machined, and exported through international sites to optimize tax payments and inventory management

Federal government

Grants management

Transparency and traceability into the distribution of funds with an auditable transaction record and simplified means to identify and verify qualifying recipients

How KPMG can help

KPMG provides an experienced lens to understanding, developing, and maintaining the security and compliance of distributed ledger technologies.

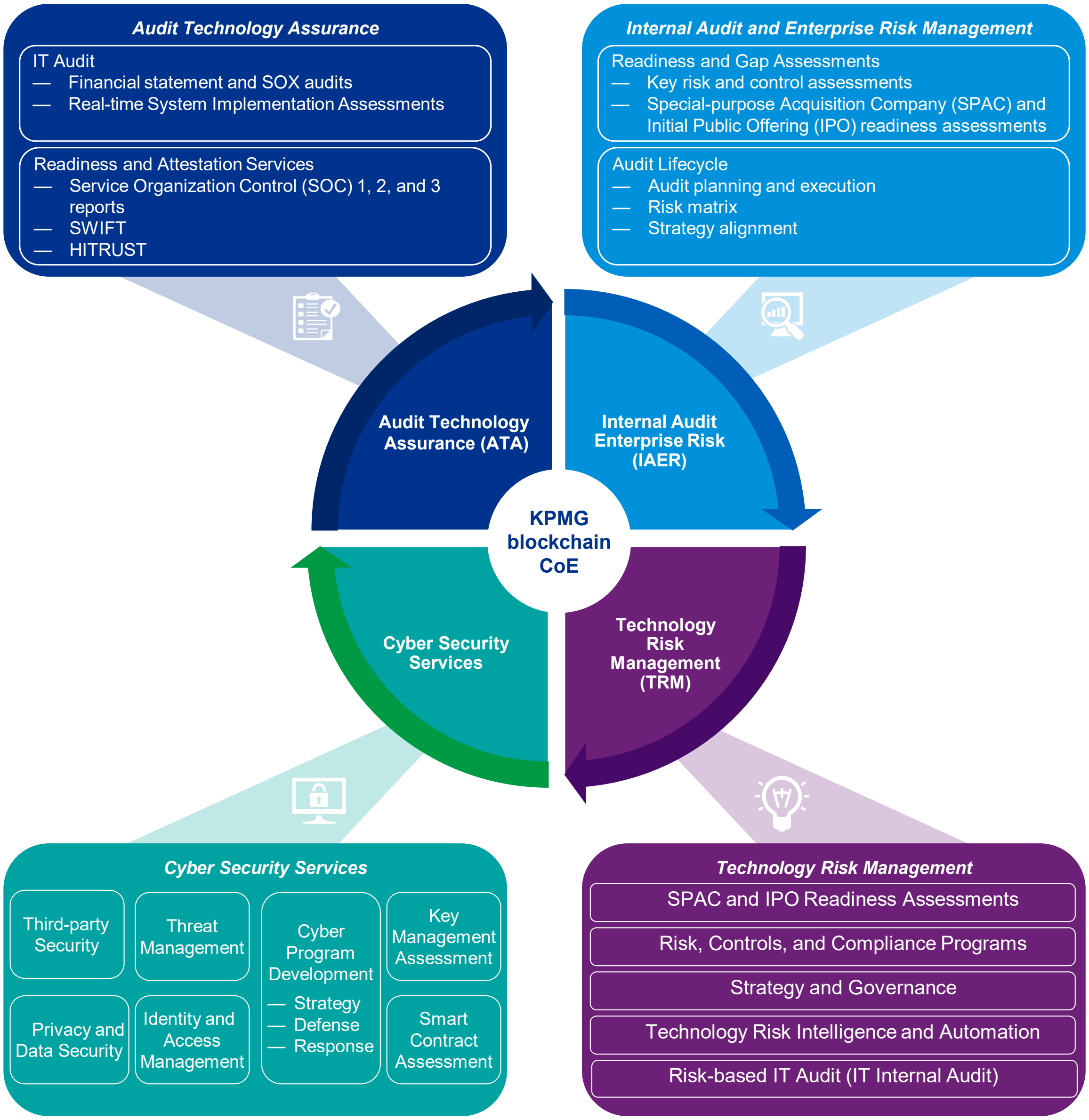
Our approach is founded upon rigorous assurance-based processes combined with an in-depth knowledge of information technology (IT) and industry-specific applications by a team of subject matter professionals who offer you perspectives in raising the bar.

Our extensive experience, methodology, and tools enable clients to adopt and maintain secure distributed ledger technology with confidence.

Our services encompass the full lifecycle of both blockchain solutions and cryptocurrency businesses. These services include strategic realization, regulatory guidance, risk assessment, control design and assessment, IT audit and attestation support, and information and cyber security. Additionally, we work closely with the KPMG Audit, Tax, and broader Advisory service lines to help deliver a full offering of services for our clients.

KPMG Blockchain Solutions

Our robust services help enable our clients to identify, manage, and mitigate risks posed by the adoption of distributed ledger technologies.



Audit Technology Assurance

IT Audit
- Financial statement and SOX audits
- Real-time System Implementation Assessments

Readiness and Attestation Services
- Service Organization Control (SOC) 1, 2, and 3 reports
- SWIFT
- HITRUST

Internal Audit and Enterprise Risk Management

Readiness and Gap Assessments
- Key risk and control assessments
- Special-purpose Acquisition Company (SPAC) and Initial Public Offering (IPO) readiness assessments

Audit Lifecycle
- Audit planning and execution
- Risk matrix
- Strategy alignment

Audit Technology Assurance (ATA)
Internal Audit Enterprise Risk (IAER)
KPMG blockchain CoE
Cyber Security Services
Technology Risk Management (TRM)

Cyber Security Services

- Third-party Security
- Threat Management
- Cyber Program Development
  - Strategy
  - Defense
  - Response
- Key Management Assessment
- Privacy and Data Security
- Identity and Access Management
- Smart Contract Assessment

Technology Risk Management

- SPAC and IPO Readiness Assessments
- Risk, Controls, and Compliance Programs
- Strategy and Governance
- Technology Risk Intelligence and Automation
- Risk-based IT Audit (IT Internal Audit)

For more information, visit read.kpmg.us/TRM

Contact us

Bryan McGowan
Principal
Technology Risk Management
T: 816-802-5856
E: bmcgowan@kpmg.com

Brian Consolvo
Managing Director
Technology Risk Management
T: 757-646-6378
E: bconsolvo@kpmg.com

Ahmed Saleh
Director
Technology Risk Management
T: 402-661-8713
E: amsaleh@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/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 endeavor 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 upon such information without appropriate professional advice after a thorough examination of the particular situation.