Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2GVAp6n

Q My organization has initiated a project to use blockchain technology. We have been hearing about this technology becoming the backbone of digital currency, but we have also heard that there are many issues related to digital currency. How can we assess risk associated with blockchain technology?

A Any new technology-based solution has associated risk. Organizations adopting such technologies always seek to strike a balance between benefits to be realized against that risk. Blockchain technology is no exception. Organizations are considering many different use cases of this technology, primarily organizations that are transaction-oriented financial institutions. Many other organizations are using blockchain technology solutions for endeavors such as identity management, software-defined perimeter (SDP) and cryptoauthentication.[1]

Most financial institutions have initiated projects to develop solutions around blockchain technology as they facilitate the maintenance of distributed ledgers,[2] which involve a distributed database maintained over a network in which network participants can share and retain identical records (ledger) that are secured using cryptography. Since these records are maintained in a decentralized manner, it is referred as a distributed ledger.[3]

Risk management consists of identification, analysis, assessment and evaluation of risk associated with technology. One needs to understand not just the technology, but also the uncertainties that may impact the objectives of the organization due to the use of technology.[4] Therefore, one needs to consider the objectives of the organization in using new technology. It is important to understand different use cases organizations are considering around blockchain technology.

Blockchains fall into two types:[5]

1. Open, or permissionless, as are used in Bitcoin and other open cryptocurrencies, which allow any party to participate in the network without any vetting (of credibility or otherwise)
2. Closed, or permissioned, which are formed by consortiums or an administrator who evaluates entities wishing to participate on their blockchain infrastructure/framework[6]

Blockchain technology is being considered by many organizations, such as those involved in banking and finance, supply chain, and logistics, for applications that involve multiple users and multiple transactions in a distributed environment. Many banks have initiated projects to develop solutions using blockchain technologies. Other applications that are being considered include SDP and asset management, identity management, and supply-chain management. Financial organizations, particularly banks and security markets, are collaborating with developers to create financial technologies (FinTech).

Risk management for solutions developed using blockchain or distributed ledger technology (DLT),[7] therefore, must be considered for different objectives related to governance, processes, operations and resources, including human resources. In the case of Bitcoin and other digital currencies, recent events have indicated that the absence of a central governing body has created concerns as no party is responsible or accountable for the proper operation of the system that may represent risk to user organizations.

Many market participants are working to develop solutions using private blockchain networks, in which implementing a governance structure can be managed as the participants are trusted parties.

The risk associated with blockchain technologies is similar to the risk associated with other technologies and current business processes, with some small differences for which organizations need to consider appropriate risk vs. benefits. Risk management for any technology-based application requires understanding of three aspects:

1. Organizational objectives related to benefit realization for deploying the application
2. Factors that will introduce uncertainties (e.g., threats and vulnerabilities) in achieving objectives
3. Cost associated with implementing controls to mitigate the risk

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

Based on these aspects, one can approach the risk management solution for blockchain-based applications. The following areas may be considered for risk management:

- **Strategic**—The technology must be considered a priority:
  - Leadership—Should the organization wish to take lead and invest in new technologies or should it wait until those technologies mature? The decision depends upon the organization's risk culture and risk appetite.
  - Transparency—Should the system be an open network, like digital currencies, or closed within strategic business partners?
- **Continuity**—Considering the nature of technology and the related complexities, the organization needs to consider the risk associated with continuity.
- **Transformation**—There is risk associated with implementation. Current business processes will need to undergo change and organizations need to consider how the changes are going to affect historical data.
- **Reputation**—The failure of new technology may result in materializing risk associated with loss of reputation.
- **Information security:**
  - Technology—Blockchain technology is said to be secured since it uses encryption. However, risk associated with the encryption technology and key management has to be addressed.
  - Systems and processes—Risk due to process control failures needs to be considered. Incidents related to Bitcoin are due to the failure of controls in these areas.
  - People—Humans are the weakest link in security. Collusion and social engineering particularly can result in security incidents.
- **Regulatory noncompliance**—Because blockchain is a new technology, regulators are cautious about its use. Depending upon the nature of the use cases, regulatory compliance must be considered while developing and using the technology. Consideration must also be given to cross-border data transmission and regulations related to anti-money-laundering.
- **Operational**—Current policies and procedures need to be revisited to meet the requirements of the new technology.
- **Contractual and supplier**—Considering collaboration between multiple parties and vendors, there need to be appropriate service level agreements (SLAs) between administrators and participating organizations.
- **Confidentiality of data**—Since all participating organizations have access to the records and data, the risk associated with confidentiality of data needs to be considered. This is also linked to regulatory compliance.
- **Privacy of data**—As with confidentiality of data, privacy of data is an important aspect that needs to be evaluated before implementing blockchain technology.

Blockchain technology is still new, but it is likely to transform current business methods that may expose organizations to new risk, challenges and competitive advantages/disadvantages. Organizations should establish an appropriate risk management strategy, effective governance and use of a controls framework.

Author's Note

The views expressed here are generic and based on available information and should not be considered as complete guidance on this topic.

Endnotes

1 Block Armour, "Next Gen Cybersecurity," *www.blockarmour.com/*
2 Financial institutions often refer to blockchain technology as distributed ledger technology (DLT); however, DLT is a use case of blockchain technology. World Bank Group, "Distributed Ledger Technology and Blockchain," 2017, *http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf*
3 Financial Industry Regulatory Authority, "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry," January 2017, *https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf*
4 International Organization for Standardization, "Risk Management, ISO 31000," 2018, *https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf*
5 Deloitte, "Risks Posed by Blockchain-Based Business Models," *https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html*
6 *Ibid*.
7 *Op cit* Financial Industry Regulatory Authority