RISK AND CONTROL CONSIDERATIONS FOR BLOCKCHAIN TECHNOLOGY

CohnReznick

ADVISORY • ASSURANCE • TAX

CONTENTS

INTRODUCTION

Over the past few years, we have seen disruptive technologies profoundly change how business is done and services are delivered. Among the latest disruptive technologies is blockchain. No matter whom you talk to, what conferences you attend, or which internet sites you visit, blockchain is at the forefront of almost every conversation and on the minds of many executives.

Cryptocurrencies, perhaps the best-known application of blockchain, are gaining in popularity. Meanwhile, other applications and initiatives that use the underlying blockchain technology are currently being designed, built, and prototyped. Organizations in many industry verticals are enthusiastic about blockchain and believe that there could be numerous adoptions, applications, and uses of the technology to enhance efficiencies, effectiveness, and, in some instances, remove roadblocks to improve sharing of data, streamline operations, and enhance the quality of data and services.

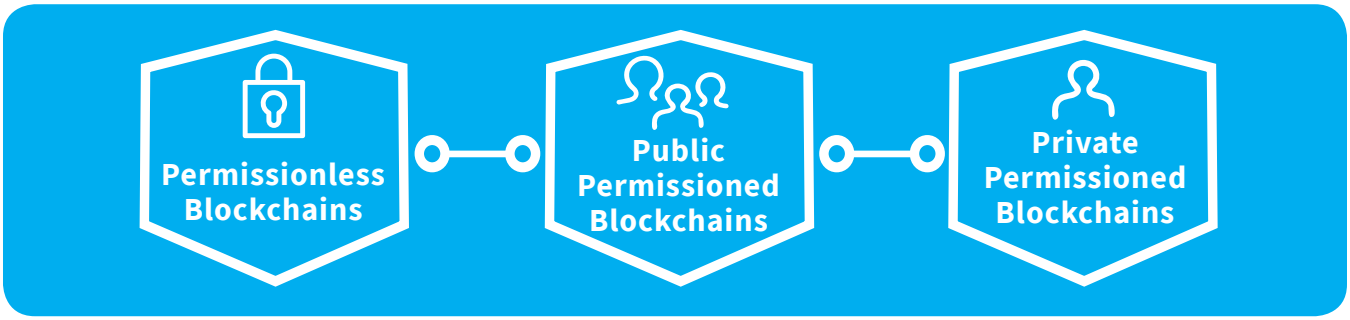
But as blockchain goes mainstream, many unanswered questions remain, along with risks that may not have been fully considered. Some of the questions and risks concern implementation of the technology within an existing IT environment and challenges around data security and privacy.

To begin, let's define the technology. Blockchain is a type of distributed ledger that enables records to be stored and sorted into blocks. It's a type of a database, but unlike a centralized or decentralized database stored on one or many servers, blockchain is installed on individual IT assets of the users of the database. The best way to understand blockchain technology is to imagine a collaborative spreadsheet (database) that is currently open in 10 locations by 10 different people. Each IT asset has an identical copy of the database and is updated in real time as transactions are executed. Every time a user in the chain updates the spreadsheet, the change is reflected on each of the other nine open versions of the spreadsheet, thereby preserving the integrity of data across the chain. No transaction can be erased or changed, a feature that is called immutability, and every transaction is anonymous. Simply put, blockchain is a network of many separate instances of the same database that ensures data integrity across all instances. This protects data against malfunction, natural disaster, and/or malicious activity.

There are three different types of blockchains: permissionless, public permissioned, and private permissioned.

1. **Permissionless blockchains**, also known as public blockchains, allow any party to participate in the network. Anyone can transact, and anyone can access and read transactions within the network using tools such as Block Explorer. Permissionless blockchains can reduce infrastructure costs but are slow, open, and are hindered by scalability and privacy issues, especially for healthcare and financial services organizations. Bitcoin and Ethereum are examples of permissionless blockchains.

2. **Public permissioned blockchains**, also referred to as permissioned blockchains, are blockchains in which a consortium or an administrator determines the participation of an entity on the blockchain network. The consortium or the administrator can sanction transactions and predefine the update process within the blockchain by using the consensus algorithm that is deployed on the network. Additionally, scalability and privacy issues can be handled by the participants, and the administrator or consortium can actively monitor for suspicious activity across the network. Public permissioned blockchains are suitable for use with a group of known and predetermined peers who allow public access to the data while protecting sensitive information. Only a few selected entities can control the system, ensuring that no individual entity can tamper with the system.



3. **Private permissioned blockchains**, commonly referred to as private blockchains, resemble public permissioned blockchains but do not make data available for public view and are controlled by a single organization. Advantages of private blockchains include a reduction in overall transaction costs and data redundancies, tighter privacy, and simplified data handling.

Regardless of the type of blockchain an organization uses, several instances of blocks should be maintained within the company's network and should be implemented behind the network security layers to help protect sensitive data. This allows data on each instance to be updated regularly to ensure data integrity. It also enables greater data accessibility, with the option to connect to the server/asset closest to the user's geographic location.

To help ensure data protection within the blockchain, the technology employs hashing to verify that the data ("block") being added to the database ("chain") is identical to the data being added to the other instances of the database. In addition, public and private keys are used to verify that only authorized personnel can access and/or modify the data. Initially, the user modifying the data employs both the public and private keys to initiate the change. Once the change has been sent to the other instances of the database, the public key is used to ensure that the block is duplicated in each instance. To validate that an individual is authorized to make a change, the data change block includes the user's private-key information to enable traceability and accountability of alterations to the data.

FUTURE OF THE BLOCKCHAIN TECHNOLOGY

Blockchain technology will very likely impact businesses across industries, including financial services, healthcare, oil and gas, retail, entertainment, advertising, media, energy, and the public sector. In financial services, for example, blockchain can be used to make international payments, and trade stocks, bonds, and commodities. It can also provide an audit trail for regulators.

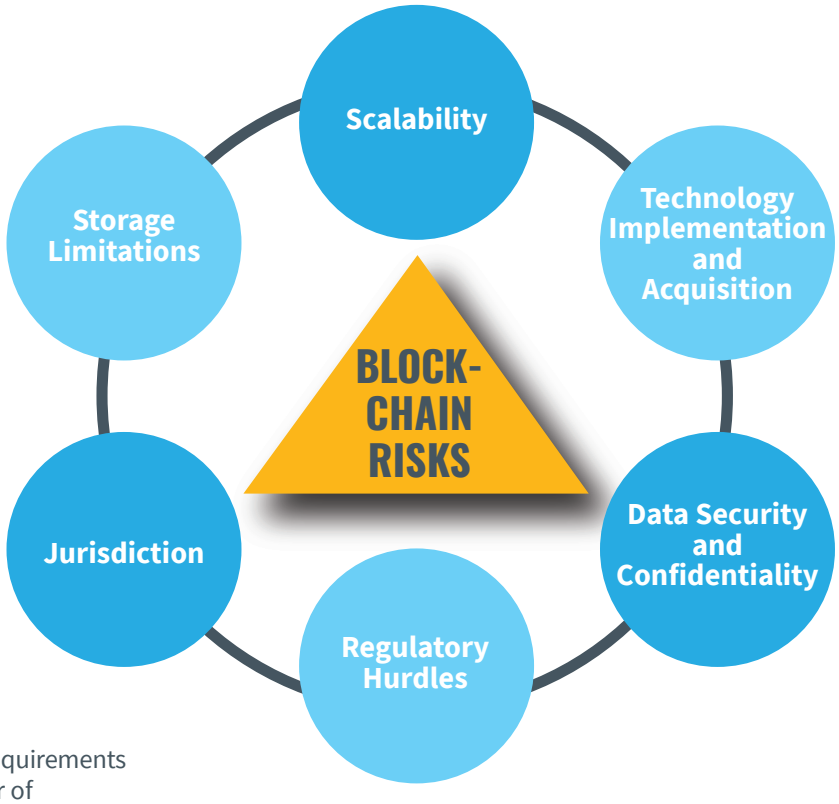
Blockchain can also be employed to create new forms of assets and to trade existing illiquid ones, such as mobile minutes, energy credits, and frequent-flyer miles.

It is widely believed that blockchain will be a disruptive technology that will enable financial services, healthcare, government, and other industries to offer trust as a service.

More importantly, blockchain has ushered in the era of a "programmable economy." In other words, a global market powered by algorithmic businesses and organizations that run on blockchain-based networks and use rules encoded in software or artificial intelligence to engage in economic activity.

HIGH-LEVEL RISKS RELATED TO ADOPTION OF BLOCKCHAIN TECHNOLOGY

The successful adoption and operation of any new technology depends on effective management of risks associated with that technology. Blockchain is no different. Organizations will need to ensure that blockchain technology and its associated applications are correctly implemented and that adequate risk-management strategies are in place. This will be essential to effective data security, confidentiality, privacy, and accountability within the organization's network and across its ecosystem of business partners and vendors.



While today's most high-profile risks involve blockchain-based cryptocurrencies, threats may evolve as new applications come online. As we continue to explore the use cases for blockchain and distributed ledgers, it is important that business leaders understand the current risks.[1] These include:

1. **Scalability:** The significant computational requirements per transaction limits the maximum number of transactions to seven per second, yet there are over 27 million users and 210,000 daily transactions.

2. **Technology implementation and acquisition:** Blockchain is not typically a stand-alone system but a component of a broader IT topology. Development and implementation of blockchain within an IT environment should follow the organization's software development lifecycle process. Organizations will need to enhance their processes to allow for consideration of design choices such as the use of blocks and nodes instead of conventional databases, as well as the use of public versus private blockchain or a consensus protocol that meets organizational needs and business strategy. Adding to the complexity of a blockchain environment are requirements like integration with other blockchains, legacy IT, and third-party systems.

   Organizations will need a holistic approach to adoption and/or implementation of blockchain technology based on thorough vetting of design strategies, business and technical requirements, IT infrastructure, and architecture enhancements.

3. **Data security and confidentiality:** Not all data on a distributed ledger should be accessible and available to others. While technical solutions (and private blockchain) may resolve this issue for some, any business considering blockchain technology should determine who will have access to the data. Furthermore, it's feasible that hackers may be able to obtain the keys to access the data on the distributed ledger, especially considering users can have multiple points of access to the DLT. In blockchain, possession of keys and ownership of content are synonymous.

[1]The risks identified include just a few examples that have come to forefront in the last few years. This list is by no means comprehensive, and other risks may have been identified and will be encountered as blockchain becomes more prevalent

[2]Blockchain.com, Blockchain Charts: Transactions per Day, Retrieved August 6, 2018

4. **Regulatory hurdles:** Due to organizational structure, industry regulatory requirements, and a lack of established governance frameworks, many organizations may need a considerable amount of time to adopt blockchain. Others may simply choose not implement the technology.

5. **Jurisdiction:** Jurisdictional issues can become problematic in a distributed ledger environment. Contracts may require consent to a specific jurisdiction as part of the terms of use for the technology. Even if such terms are present, organizations should consider if they will be deemed enforceable and, if so, how they will be enforced.

6. **Storage limitations:** While blockchain eliminates the need for a central server to store transactions and device IDs, the ledger must be stored on the nodes themselves. Consequently, the ledger will increase in size over time. Because a blockchain database must store data indefinitely, the conventional recurring payment model does not work, and data storage must cover long-term costs. Organizations should consider these costs as part of the decision-making process for blockchain implementation.

ENHANCEMENT OF INFORMATION TECHNOLOGY GENERAL CONTROLS

Management of blockchain/DLT requires specific procedures to mitigate the risks related to technology that can be identified, quantified, monitored, and controlled. While organizations that adopt blockchain will continue to implement and monitor IT controls through the use of standardized frameworks, key control enhancements should be considered in the following domains:

1. **Information security policies:** Policies for data management, identity management, and cryptography should be updated.

2. **Physical security:** Blockchain/DLT will require continued focus on hardware security and key management.

Management of blockchain/DLT requires specific procedures to mitigate the risks related to technology that can be identified, quantified, monitored, and controlled.

3. **Key management and cryptography controls:** Organizations should focus on controls that support the generation of cryptographic keys; also, maintenance, renewal, and security of the keys will be critical.

4. **Computer operations:** Organizations will be required to refresh their infrastructure security controls, including anti-virus, zero-day exploits, back up and restore, and remote access.

5. **Logical access controls:** Blockchain will require enhancements of access controls like HR on-boarding/off-boarding and identity-based access and key provisioning.

Organizations will need to enhance their IT general controls to align with the dynamics and complexity of the blockchain environment. Outlined on the next page are a few key blockchain focus areas, along with risk considerations and controls, that organizations should consider for a secure blockchain environment.

BLOCKCHAIN FOCUS	RISK CONSIDERATIONS	CONTROL AREAS
Platform	1. Lack of a coherent blockchain strategy and roadmap 2. Inadequate management oversight of blockchain adoption 3. Failure to evaluate and monitor usage of blockchain	• System quality models and platform evaluation
Nodes	1. Lack of controls to prevent unauthorized personnel from accessing encryption keys 2. Poorly implemented encryption and key management processes 3. Inaccurate implementation of consensus protocol may lead to incomplete transaction processing and data integrity issues	• Cryptography key management • Virtualization • Consensus protocol mechanisms
Development	1. Inability to align business process changes with standardized blockchain technology 2. Inability to demonstrate compliance with specific requirements (e.g., the GDPR's "right to be forgotten") 3. Security vulnerabilities introduced by blockchain ecosystem partners 4. Failure to secure interfaces between blockchain technology and traditional applications 5. Failure to protect against new vulnerabilities in virtualization technologies	• Cybersecurity • Application security • Data protection • Compliance
User	1. Insecure integration of traditional applications and blockchain identity management components	• Security roles and restrictions • Identity management
Security Incidents	1. Ineffective incident investigation due to impermanence of virtual systems 2. Delayed data breach notification due to complex identification of affected partners	• Cyber-incident response planning
Asset Management	1. Insufficient tracking of virtual assets	• Ownership and monitoring of hardware tokens

INTEGRATION OF BLOCKCHAIN INSTANCES

Implementation of blockchain/DLT requires the technology to be seamlessly integrated with other blockchain solutions, business systems, and technologies. Consequently, it is critical that all interconnected applications and systems communicate with each other and interface data on a real-time basis.

In addition to the general IT controls framework, organizations should focus on the following areas when planning for blockchain/DLT or implementing/integrating applications that are based on such technology:

1. **Data conversion and legacy system integration:** Blockchain/DLT solutions within an organization most likely will be integrated with other legacy platforms like web servers, databases, mainframes, and third-party applications. Organizations should analyze existing legacy applications, cleanse and transform legacy data so that it is readable by blockchain/DLT interfaces, and implement tools and processes to load complete and accurate data.
2. **Key management for logical access:** Any user can access only data that is stored within their block, and access to the block is governed using public/private keys. This requires that organizations have effective key and digital-certificate management infrastructure and solutions in place to protect and maintain the public and private keys. Additionally, organizations considering public permissioned blockchains will need to manage and protect the integrity of the consensus algorithm within their respective environments. Organizations that leverage identity and access management (IAM) solutions within their environment will have to determine how to effectively integrate blockchain solutions with their existing IAM strategy and footprint.
3. **Access considerations for hardware security:** Transacting blockchain data requires access to the ledger file or interfaces, which must be signed by a specific private key. These private keys are typically stored on hardware-based tokens that are either linked to physical badges, PIV/CIV cards, or biometric authentication mechanisms. Security and management of the private keys require a holistic security approach that includes the disparate hardware mechanisms that support the public key infrastructure and physical security of the external media used to store keys.

Blockchain is positioned to revolutionize how organizations operate, manage transactions, and design and sell products and services. Ultimately, the technology can enable businesses to harness the power of artificial intelligence to carry out economic activity.

> Organizations that understand the risks surrounding this disruptive technology, and develop and implement a singular risk-based strategy are better prepared for the programmable economy of tomorrow.

As with most disruptive technologies, however, businesses will likely need help deciding strategic uses for blockchain, selecting the right solution, and integrating the technology with existing IT systems and business processes.

Organizations that understand the risks surrounding this disruptive technology, and develop and implement a singular risk-based strategy are better prepared for the programmable economy of tomorrow.

COHNREZNICK'S TECHNOLOGY RISK, CYBERSECURITY, AND PRIVACY TEAM

CohnReznick provides dynamic and scalable technology risk and cybersecurity solutions designed to meet the needs of growth-focused companies that are looking to leverage disruptive technologies such as blockchain. Our technology risk framework provides a comprehensive, flexible approach that helps companies assess and remediate emerging blockchain technology risk. We provide end-to-end solutions, from strategic emerging technology adoption assessments to comprehensive risk management solutions to secure and control risks around blockchain technology.

CONTACT

Bhavesh Vadhani
Principal, Technology Risk and Compliance Leader
bhavesh.vadhani@cohnreznick.com

Shahryar Shaghaghi
Principal, Cybersecurity and Privacy Leader
shahryar.shaghaghi@cohnreznick.com

Contributing authors: George Marountas, Michael Goldsmith, Kiran Bhujle, and Thomas McDermott
Research credit: Eric Leyden

ABOUT COHNREZNICK

CohnReznick LLP is one of the top accounting, tax, and advisory firms in the United States, combining the deep resources of a national firm with the hands-on, agile approach that today's dynamic business environment demands. With diverse industry expertise, the Firm provides companies with the insight and experience to help them break through and seize growth opportunities. The Firm, with origins dating back to 1919, is headquartered in New York, NY with 2,700 employees in offices nationwide. CohnReznick is a member of Nexia International, a global network of independent accountancy, tax, and business advisors. For more information, visit www.cohnreznick.com.

CohnReznick
ADVISORY • ASSURANCE • TAX

1301 Avenue of the Americas
New York, NY 10019
212-297-0400

cohnreznick.com