KPMG

Missing link

Navigating the disruption risks of blockchain

kpmg.com

Blockchain disruption

By now, most people have heard of blockchain, the breakthrough technology underlying the digital currency Bitcoin.

Blockchain is poised to disrupt the third-party trust model that underpins traditional transactions. Blockchain's distributed ledger technology is protected by advanced cryptography and authenticated by a peer-to-peer consensus system, rather than a central clearing house. As a result, proponents believe it can provide a more transparent and secure means of recording and transmitting transactions.

It is no wonder businesses across the world are increasing their interest in the blockchain.

> Recent World Economic Forum research found that 58 percent of technology executives expect 10 percent of global gross domestic product to be stored on blockchain by 2025.[1]

Such bold predictions for future use cases and adoption have led venture capitalists to invest an estimated half a billion dollars in blockchain companies in the last year alone.[2] Meanwhile, financial services incumbents are exploring ways to adapt the blockchain concept for uses far beyond currencies, such as smart contracts, supply chain operations, and infrastructure transformation.

As more global enterprises adopt blockchain technology, corporate leaders must evaluate and address the associated risks. While blockchain will not eliminate the need for internal controls, it is likely to alter their design and operation. Legacy risk frameworks and control environments must evolve. And organizations must strengthen governance models to mitigate risks posed by regulatory actions in response to blockchain technology.

In this paper, we will explore key risk considerations to both providers and users (i.e., participants) in the blockchain ecosystem and offer considerations for navigating the coming disruption responsibly.

[1] Deep Shift: Technology Tipping Points and Societal Impacts, World Economic Forum Report, September 2015

[2] State of Blockchain Q1 2016 Report: Blockchain Funding Overtakes Bitcoin, Coindesk, May 2016

KPMG

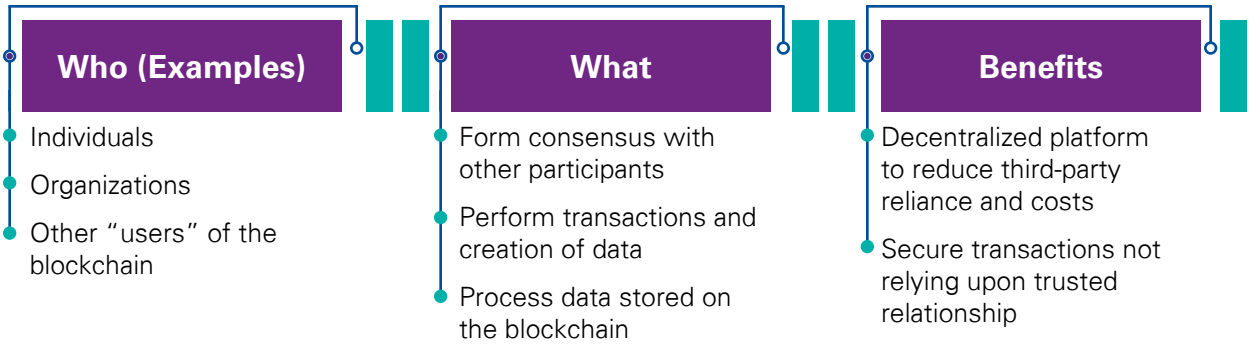
Blockchain risk considerations

The risks introduced by blockchain are dependent upon the viewpoint of the stakeholder. Participants are putting at risk their financial instruments and transactions, while providers are managing a service based upon a complex emerging technology. We have identified five unique risks from each vantage point:

Participants	Providers
— Interoperability	— Scalability
— Auditability	— Regulatory
— Control and collusion	— Trust and accreditation
— Data management and governance	— Change management
— User access and provisioning	— Access and user management

Risks to blockchain participants

To help illustrate these risks, we have identified the involved parties (who), their use cases (what), and the benefits they could gain by using blockchain technology. We then determined the key considerations for each of these unique risks, as applicable to providers and participants separately.



Interoperability

Risk: Integrating blockchain with legacy IT platforms is a potentially costly operational challenge. Participants will need to convert data models and business processes and incorporate new authentication and communication protocols.

Considerations:

— Introduce blockchain technology in a contained, manageable fashion to limit disruption to existing technology and processes.

— Converge the technology and processes in a controlled manner.

— Identify specific data elements that will be exchanged between current internal systems and blockchain software to help maintain data interoperability.

Auditability

Risk: For transactions stored on a blockchain, companies may lack the ability to provide information necessary for legal discovery, forensic investigations, and audit purposes.

Considerations:

— Enable the ability to extract corporate data from the blockchain, including the relevant metadata, to allow for detailed analysis outside the blockchain environment.

— Determine whether your corporate data would be discoverable by other participants on the blockchain without your explicit authorization.

— Create specialized APIs into the blockchain platform in your reporting and query software to enable customized business reporting.

Control and collusion

Risk: A single participant, or collusion among a group of participants, could obtain control of the blockchain by achieving consensus without other participants. This could effectively block, delay, or modify transactions.

Considerations:

— Understand the consensus algorithm and the risks related to a takeover attack before entering a blockchain relationship.

— Identify the large parties who are active participants to understand where collusion risks may be presented.

Data management and governance

Risk: Although blockchain uses a persistent, distributed ledger that grows with every transaction, large volumes of transactions and the presence of corporate data outside of the network presents risks similar to cloud computing environments. Further, transactions may have additional metadata that is not part of the blockchain transaction, which will have to be secured and transferred outside of the process while maintaining the ability to reconcile with the blockchain.

Considerations:

— Hold blockchain providers to similar standards as outsourced technology platforms, requiring them to provide attestation reports, security certifications, and other assurance to participants.

— Define classification standards for all types of data in the blockchain platform, including metadata not in actual transactions.

— Specifically manage the types of data stored and transmitted on a blockchain platform.

— Apply data classification standards to protect and encrypt sensitive information.

User access and provisioning

Risk: Blockchain relies on unique addresses that are assigned to each member, which are used for both sending and receiving and are authenticated via Public Key Infrastructure (PKI). There may not be a system available that can adequately restrict access to private keys, create a role-based access model, and help prevent segregation of duties concerns.

Considerations:

— Require individual identification and accountability for blockchain transactions conducted by employees of the organization, similar to current transactional systems.

— Update identity access management systems to help control and monitor authentication to blockchain environments, including permitting which specific actions can be performed (e.g., data reading, applying signatures, processing payments, and payment acceptance).

— Invest in specialized software to help manage and provision encryption keys to the blockchain platform to help protect the privacy of transactions.

KPMG

Blockchain risk considerations (continued)

Risks to blockchain providers

Who (Examples)	What	Benefits
Platform and application developers	Initial set of blockchain tailored toolsets	Monetization through licensing, subscription, or transaction fees
Infrastructure hosting providers	Enablement of use case development	
Corporate consortiums	Development of domains' specific language for use cases	
Government or regulatory bodies	Providing cloud-based infrastructure to support blockchain environments	
Nonprofit organizations		

Scalability

Risk: Current blockchain platforms have not been proven to handle the types of high-volume transactions typical in the financial services environments that blockchain promises to disrupt.

Considerations:

— Monitor blockchain platform activity for spikes in transactional frequency and unexpected processing delays.

— Enforce cutoff dates where the current blockchain will end. After reaching consensus, a new blockchain would begin based on the balances calculated at consensus of the old blockchain.

— Limit the amount of metadata that can be included in a transaction.

— Slow down consensus by increasing the size of transaction blocks.

Regulatory

Risk: A product or application of blockchain may be rendered inoperable due to regulatory constraints or lack of regulatory adoption.

Considerations:

— Work together with highly regulated industries, such as financial services, to help overcome and influence regulatory actions.

— Understand applicable international privacy laws that may restrict where data could be stored or accessed, effectively limiting participants to certain geographies.

Trust and accreditation

Risk: Participants may resist joining blockchain relationships without assurance regarding the security, privacy, and integrity of their transactions and data.

Considerations:

— Provide transparency with the internal controls environment supporting the blockchain platform.

— Utilize industry-accepted accreditations (e.g., ISO 27001, NIST 800-53) and third-party attestations (e.g., SOC 1/2, PCI) to demonstrate effectiveness of the blockchain control environment.

Change management

Risk: Changes to the blockchain platform would require agreement and implementation from all participants, which may decrease the velocity with which new functionality and features can be introduced.

Considerations:

— Create provider-specific logical access rights, which are separated from those of a participant, to permit development, approval, and migration of platform and software logic changes. Data changes would require consensus from participants.

— Establish legal agreements and a charter—which all members must sign—that clearly defines how changes will be managed for the blockchain.

— Define clear policies communicating participant responsibilities for approving changes, including consensus mechanisms and transparent change notifications.

Access and user management

Risk: With participants from multiple organizations, user authorities may be difficult to segregate and manage by organization and by job role.

Considerations:

— Provide a blockchain identity access management system to enforce consistent user authentication and provisioning controls across the platform.

— Communicate participant control responsibilities regarding self-management of user credentials to the blockchain platform.

— Provide transparency to the level of access rights and abilities the provider has within the blockchain platform.

KPMG

Trading derivatives with blockchain: A risk-based case study

In trading many over-the-counter (OTC) derivatives, financial services organizations typically rely on a number of platforms and methods that conform to the International Swaps and Derivatives Association's (ISDA) master agreement, including real-time financial pricing systems, trade execution and settlement software, and cash management and payment systems.

Making trades using blockchain technology could reduce costs, complexity, and risks associated with the current electronic trading system for OTC derivatives.

Key advantages of trading OTC derivatives using blockchain include:

- There is near real-time settlement of trades.
- Derivative securities and cash can be traded using a single system.
- The initiating party can instantly verify the counterparty has the security or cash to make the planned trade without the need to contact a third party, or even the counterparty.
- Trades are near instantaneously verified by all other members of the blockchain, without the need for a third-party clearinghouse.
- Regulatory reporting is simplified because regulators can be nontrading members of the blockchain who instantly receive trade information without any additional regulatory reporting from each organization.
- There is real-time inventory and pricing for securities because all members of the blockchain can see all transactions taking place and independently identify the historical pricing and ownership of individual securities.
- There is decreased risk in the event of a disaster or failed competitor because data in the blockchain is distributed securely across members and can never be altered.
- There is opportunity for a pseudo-exchange where members of the blockchain can put offers out for trades to the entire network. Members could choose to accept those trades, which will be executed and settled in near real time with less counterparty risk compared to trading on a traditional exchange.

Derivative trading risks

Providers and participants both must consider the risks that come along with the advantages of blockchain and should consider the following risks as they explore implementation of blockchain technology for this use case.

Participant risks

Example of participants for trading OTC derivatives with blockchain include:

- Broker/Dealers
- Fund Administrators
- Investment Banks
- Insurance companies

Interoperability issues	1	*There are often disparate trade execution, settlement, and accounting systems used by the front, middle, and back office of an OTC derivative trading desk. The volume of changes to the technology and business processes will present a costly challenge for a successful implementation of blockchain technologies.*
Auditability issues	2	*Blockchain technology inherently provides a verified and validated log of all transactions executed. However, every transaction executed by a participant will require complete and accurate association to an accountable individual. Maintaining this audit trail and reconciling the differences will present a continuous challenge.*
Control and collusion issues	3	*Loss of control or collusion between participants could result in the loss of consensus across all parties in the blockchain. Without consensus there could be incorrect or fraudulent modification of existing trades in addition to blocked or delayed trade execution and settlement.*
Data management and governance issues	4	*Not all relevant or required data for each trade may be stored within the blockchain. Reconciling and maintaining this data between the blockchain and other relevant systems will require unique data management and governance in order to maintain compliance with regulatory requirements.*
User access and provisioning issues	5	*Responsibilities and appropriate duties across the front, middle, and back office may change drastically given the near real-time settlement made possible by blockchain. Identifying and maintaining appropriate segregation of duties will require new and different considerations.*

KPMG

Derivative trading risks (continued)

Provider risks

Example of providers for trading OTC derivatives with blockchain include:

- Emerging Market Security Registers
- Distributed Platforms
- Existing Exchange Markets

Scalability issues	1	*The volume of OTC derivative trading is constantly variable, and understanding and predicting the velocity and volume of trades happening in the blockchain will require constant analysis. Failure to efficiently and effectively manage the scale required of the blockchain may impact the SLA required by participants or lead to unnecessary costs.*
Regulatory issues	2	*New and changing requirements from regulators such as the Financial Industry Regulatory Authority (FINRA), the Financial Crimes Enforcement Network (FinCEN), and the U.S. Securities and Exchange Commission (SEC) could impact the way the blockchain operates and force changes on the provider that could impact their ability to legally operate the blockchain or maintain the SLA required by participants.*
Trust and accreditation issues	3	*There are currently no industry-standard attestation reports for blockchain providers. Current attestation reports (e.g., SOC 1) do not provide full coverage over the services provided by a blockchain provider. Obtaining and maintaining the trust of participants could result in significant costs and use of resources.*
Change management issues	4	*In order to preserve consensus and ability of participants to trade securities, the provider will need to coordinate and manage changes while maintaining the SLA required by participants. Failure of the provider to effectively manage changes across all participants could result in an SLA breach.*
Access and user management issues	5	*Inappropriate access of participant user credentials or the private blockchain network could result in inappropriate or fraudulent trades. Differentiating between valid trades and trades made using compromised participant credentials may be difficult or not possible.*

About KPMG's Emerging Technology Risk Services

Technology's influence on business is undeniable. Cloud, connectivity, mobile, cybersecurity, Internet of Things, and FinTech are disrupting the status quo and transforming the way business is done, and forcing organizations to think faster, become more flexible, and align technology to the business.

KPMG LLP's (KPMG) Emerging Technology Risk (ETR) Services Network helps clients responsibly navigate this new digital world. ETR's technology specialists and risk management professionals evaluate the business and deploy KPMG power to develop adaptable business methodologies that enhance the balance of risk and reward in emerging technology adoption.

KPMG

About KPMG

KPMG LLP, the audit, tax and advisory firm, is the U.S. member firm of KPMG International Cooperative ("KPMG International"). KPMG is a global network of professional firms providing Audit, Tax and Advisory services. We operate in 155 countries and have more than 174,000 people working in member firms around the world.

Contact us

Phillip Lageschulte
Global Lead
Emerging Technology Risk
T: 312-665-5380
E: pjlageschulte@kpmg.com

Michael Krajecki
Director
Emerging Technology Risk
T: 312-665-2919
E: mkrajecki@kpmg.com

Martin Sokalski
Managing Director
Emerging Technology Risk
T: 312-665-4937
E: msokalski@kpmg.com

Kiran Nagaraj
Managing Director
Emerging Technology Risk
T: 212-872-3056
E: kirannagaraj@kpmg.com

Contributors

Alexander Bates
Senior Associate
Emerging Technology Risk
T: 312-665-2423
E: alexanderbates@kpmg.com

Sam Wyner
Manager
Emerging Technology Risk
T: 212-954-4903
E: swyner@kpmg.com

kpmg.com/socialmedia