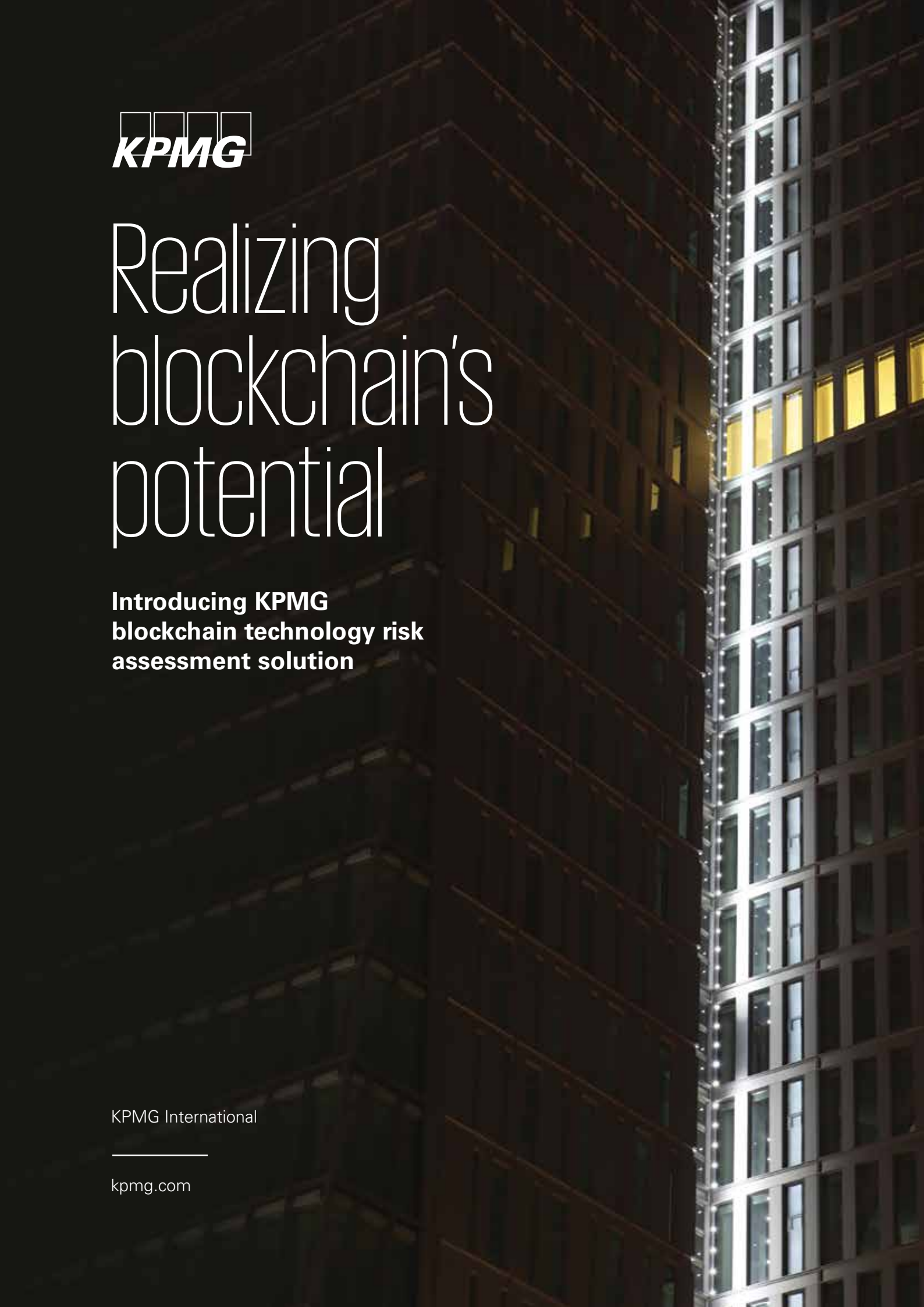


Realizing blockchain's potential

Introducing KPMG blockchain technology risk assessment solution

KPMG International

kpmg.com

> As a new technology, blockchain brings with it specific risks not relevant to other IT systems. Not factoring blockchain-specific risks into the technology assessment can easily leave companies open to security breaches.

Foreword

Recent interest and investment in blockchain has grown exponentially which is not surprising given its potential to disrupt existing business models, transform business processes, introduce operational efficiencies, realize cost savings and spark new revenue streams. What was once an obscure technology is now seen as applicable to a growing range of activities and industries — from funds transfer and securities trading to supply chain management and healthcare.

Rapid growth of the technology and the growing menu of blockchain platforms coupled with its differences from traditional technology has made it challenging for companies to understand how to best apply, employ and harness the value of blockchain while managing associated risks — risks they might not fully be aware of.

The KPMG blockchain technology risk assessment solution (the solution) enables companies to assess blockchain platforms and capabilities for technology and security risks throughout the full product life cycle, from platform selection to proof of concept and into full production. The assessment is conducted by KPMG's blockchain subject matter professionals who utilize advanced tools and techniques to evaluate the architecture, code, and security aspects of blockchain platforms.

KPMG member firm professionals built this solution with a number of different stakeholders in mind as each might require a different perspective or level of depth to conduct their assessment — from blockchain product owners, chief information officers, chief information security officers, and technology risk leaders to the heads of audit.

There is no doubt blockchain has the ability to live up to its enormous hype — but it will only do so if organizations invest responsibly into blockchain with a good understanding of the key risks and mitigation plans.

Building on *Securing the chain*

In 2017, KPMG International released a whitepaper entitled, *Securing the chain*[1] in which we examined two specific incidents whereby security associated with blockchain initiatives were breached, and how these incidents could have been avoided. We also introduced an overarching blockchain technology and security framework that companies and blockchain consortia can use to identify and respond to security threats and risks related to the use of blockchain. The framework underpins many of our full life-cycle blockchain-related services, including our blockchain technology risk assessment solution discussed in this paper. It can also be used to assist Information Risk Management departments in developing a bespoke blockchain risk and control framework for their organization.

Eamonn Maguire
Global Distributed Ledger Services Lead, Financial Services,
KPMG International
Director, Financial Services Advisory,
KPMG in the US

Kiran Nagaraj
Global Cryptoasset Lead, Distributed Ledger Services
KPMG International
Managing Director, Emerging Technology Risk Services
KPMG in the US

Dennis de Vries
Distributed Ledger Services Lead,
KPMG in the Netherlands

[1] Securing the chain, KPMG International, May 2017 (https://home.kpmg.com/xx/ena/home/insights/2017/05/securing-the-blockchain-fs.html)

When it comes to blockchain, one size does not fit all

> While they might have the same general functions, different blockchain platforms have differing security and technology risks.

Many companies have moved beyond simple experimentation into proof-of-concept and use-case development. A small but rapidly growing number have even started to move blockchain solutions into production.

As more organizations look to achieve value from blockchain, it has become apparent that they need a consistent framework for assessing security and technology risk of blockchain solutions across their full life cycle, from design to production deployment.

The reality is there is no one-size-fits-all approach for leveraging blockchain. While they might have the same general functions, different blockchain platforms may also have different security and technology risks. To this end, companies should not make assumptions as to what a blockchain is capable of doing, or how safely and securely it can complete a specific task. Organizations need to evaluate the various solutions across their life cycle to make sure it fits their needs and risk appetite.

Understanding the two types of blockchains

- **Public blockchain:** In a public blockchain, access is wide-open; anyone can become a node and participate in the blockchain. Bitcoin is a prime example of a public blockchain.
- **Private blockchain:** In a private blockchain, access is limited to specific users — such as a group of banks — through a permissions-based private network. Anyone outside of the private blockchain cannot see or participate in blockchain transactions.

Public versus private blockchains

	Public blockchain	Private blockchain
Participation in network	Open	Closed
Transactional privacy	Not prioritized except for so-called anon-coins	Adjustable to the wishes of the participants
Economic incentive for participation	Built-in	Contractually organized
Centralization	Fully decentralized	Varying degree of decentralization
Commonly used for paid social networking	Payments, remittances, prediction markets, distributed storage, paid social networking	Asset servicing, foreign exchange (FX), provenance tracking, trade finance, health care, insurance contracts

The risk profile of public and private blockchains varies significantly. As a new technology, blockchain brings with it specific risks not relevant to other IT systems. Not factoring blockchain-specific risks into the technology assessment can easily leave companies open to security breaches.

Implementing blockchain? Get it right the first time

Although every blockchain implementation is unique, they will typically incorporate the following characteristics or some combination thereof:

Immutable digital ledger: An unmodifiable and persistent record of transactional activity using well-known, trusted, and tested cryptographic principles.

Consensus mechanism: Mechanisms whereby independent participants have an agreed upon method as to how transactions are executed and added to the blockchain without relying on intermediaries.

Identity and ownership: While identity may not always tie to a real-world identity, blockchain typically relies on these concepts via cryptographic principles to prove the ability to interact with the blockchain and demonstrate ownership.

While these characteristics offer exciting possibilities, the challenge is that they also bring with them their own specific risks. For example, with blockchain's immutability, data on a blockchain cannot be deleted. In a use case where customer information is included in a blockchain transaction, blockchain participants may find themselves in breach of privacy regulations (e.g. as General Data Protection Regulation (GDPR) Article 17) if they cannot comply with a request of a customer enacting their 'right to be forgotten'.

KPMG's blockchain assessment solution is designed to help organizations understand and assess the full scope of security and technology risks associated with blockchain initiatives they undertake or applications they are working to implement. The solution is designed to span the life cycle of security and technology risks pertaining to blockchain.

The solution also allows you to evaluate the level of maturity of controls related to in-use blockchain solutions. By evaluating the maturity level of existing risk controls, organizations can determine where they are well protected and where they need to establish stronger controls.

> "The KPMG assessment solution enables organizations not only to evaluate specific risks related to potential blockchain implementation projects, but also to evaluate the level of maturity of controls related to in-use blockchain solutions."

> If you are at proof-of-concept stage, the solution allows you to assess weaknesses in your existing systems before you go live.

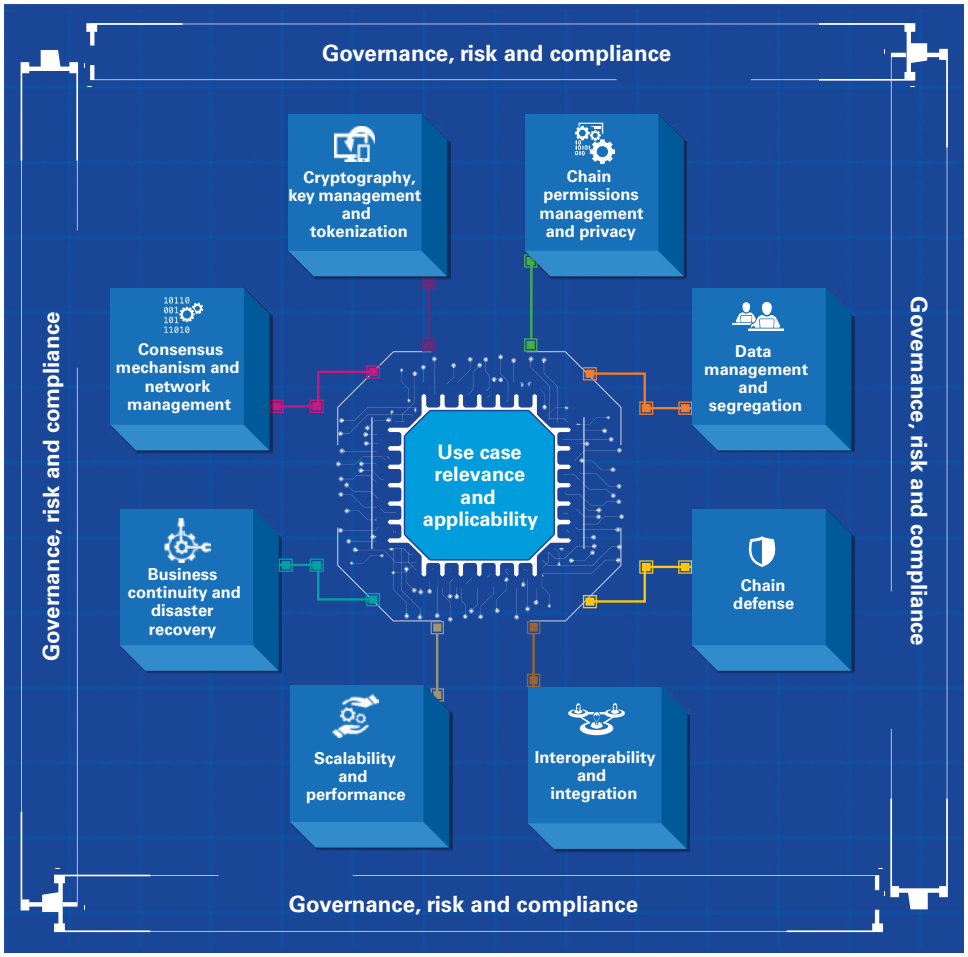
Key benefits of the KPMG blockchain technology risk assessment solution can include:

	Design	Develop	Deploy	Operate
Provides a holistic model for evaluating blockchain-solutions: A tested model for assessing the risks associated with blockchain initiatives or solutions. KPMG professionals developed the model based on in-depth experience, research and knowledge of IT risk standards, and then tested it with a number of clients globally.	✓	✓	✓	✓
Supports clear identification into blockchain risks: Gain specific insights into the 10 key risk areas associated with your blockchain implementation, including the strength of your existing or proposed controls.	✓			✓
Confidently move from proof-of-concept to production: There are specific risks associated with the shift from proof-of-concept to production systems. If you are at the proof-of-concept stage, the model can help you to assess weaknesses with your existing system before you go live.	✓		✓	
Enables the creation of a concrete action plan: The risk assessment provides clear pointers to critical risk areas and areas where you have less mature controls so that you can address potential gaps or weaknesses. The risk assessment also provides you with indications on how to improve your controls to a higher maturity level.	✓	✓	✓	✓

Risk assessment areas

Through member firms' extensive experience, we have identified 10 key risk categories associated with blockchain implementations. A number of these risk dimensions are inter-dependent, driving the collective maturity of a blockchain implementation. These dimensions also take on different variations throughout the life cycle of a blockchain.

KPMG blockchain technology risk assessment framework — Key risk areas



> A number of these risk dimensions are inter-dependent, driving the collective maturity of a blockchain implementation.

1. Consensus mechanism and network management

Consensus mechanism and network management risks relate to the potential for inappropriate, unauthorized, or inaccurate transactions to be recorded in the blockchain. A consensus mechanism, core to most blockchain technologies, is the means by which the participants in a blockchain platform determine if a transaction is acceptable and should be accepted in the blockchain. For example, a leader-based consensus mechanism allows the leader to review and accept all transactions for the blockchain which are simply acknowledged and put into the blockchain by other nodes. If ineffective, incorrect transactions could be recorded.

2. Cryptography, key management and tokenization

Within a blockchain, each user maintains a set of public and private cryptographic keys. As a result, there needs to be identified procedures to ensure these keys are managed appropriately (e.g. distribution, usage, revocation) so that only approved individuals are accessing the blockchain.

For improved security, there may be a need to engage multiple individuals (within the same participant organization) before completing a transaction. In these instances, multi-signature format keys and a solution will need to be developed and managed to ensure that approval processes are followed prior to a transaction being recorded. Ineffective management of these keys could result in unauthorized transactions or tokens being made.

3. Chain permissions management and privacy

Private blockchains, as previously noted, are based on the principle that only approved users can join and participate in them. Usage by unauthorized parties pose a significant risk both to the integrity and privacy of the blockchain and to the transactions being recorded. Private blockchains require authentication of participant identities in addition to user access management policies and procedures similar to other sensitive IT systems to allow for only authorized user access.

In a private blockchain, there may be different types of users that should only be permitted to perform certain actions or view specific transactions. For example, in a private blockchain there could be a regulator present on the network. That regulator could have its chain permissions set so that it is only able to view transactions that are in a specific state. In contrast, a business participant in the blockchain should only be able to transact with non-regulator parties and not be able to view or action transactions that it is not party to.

Private blockchains may initially create a less risky environment for a solution, but risks of inappropriate entitlements to perform actions or the ability to have read-only views into transactions can have a significant impact on a solution's risk profile.

As of July 2018, production use cases for private blockchains are still few and far between. Because of this, many of the important risks and mitigating factors may have yet to be identified. The lack of lessons to learn from others' risks are not yet clear, increasing the need for a framework — based approach to blockchain risk.

4. Use case relevance and applicability

Currently, there are any number of use cases being undertaken with respect to blockchain. As part of this process, companies should consider whether it is relevant to use a blockchain solution given their specific needs and objectives, and whether the identified blockchain solution is the most applicable method to enable the blockchain. For example, a blockchain solution that does not support automatic updates to smart contracts based on external sources of data may not be the most effective when it comes to managing logistics and tracking packages.

5. Data management and segregation

Any companies involved in a blockchain need to assess whether they have the capabilities to manage the use case once built. This includes managing all aspects of data, including confidentiality, integrity, and the availability of data such as identifying data sources and understanding how activities will occur when data is not available. Companies also need to ensure that their blockchain activities are compliant with appropriate regulations such as GDPR.

Adequate data management is particularly critical when two interacting parties on a blockchain want to keep their transaction anonymous from the other members of the network.

In addition to general usage rights, some transactional information may be live on the blockchain, commonly referred to as 'on chain', while other information might be stored off the blockchain, or 'off chain'. There should be identified processes in place to manage the movement of funds between hot and cold storage so that assets or funds are not transferred without the appropriate permissions.

- **Cold storage** refers to private key storage solutions that are completely offline and typically located at physically secure locations. These solutions typically live their full life cycle without ever connecting to the internet.
- **Hot storage** refers to private key storage systems that are connected to the internet and can be used to make transactions in real time.

It is important that data management and segregation risks should be considered in tandem with chain permissions management and privacy risks as the two categories overlap.

6. Chain defense

Companies using blockchain cannot underestimate security requirements or make assumptions regarding blockchain defense mechanisms. It is important to identify and verify checks on security and network monitoring processes to reduce risks associated with smart contracts or other attacks.

While a blockchain provider should conduct source code analysis as a matter of course, companies should conduct their own due diligence on the source code and any smart contracts running on top of it to ensure there are no gaps. As the blockchain evolves, companies should continue to monitor and manage blockchain security in a proactive manner.

Case study

Spotlight on an Asian stock exchange

A large Asian stock exchange recently announced plans to implement a blockchain-enabled solution for recording shareholdings and managing the clearing and settlement of equity transactions. KPMG professionals conducted a detailed review of the security design and architecture of the platform against security objectives identified by management. This supported the stock exchange's decision to move forward with the solution.

As the stock exchange was leveraging a proprietary distributed ledger solution (DLT), it was imperative that it considered the security implications of the design architecture of the DLT platform, the inherent risks and mitigating factors to consider the security of trades executed on the platform.

KPMG professionals from across the member firm network, including emerging technology risk, cyber security services and Lighthouse data and analytics center of excellence collaborated on the assessment by identifying security risks, analyzing the solution's security architecture and design, and performing specific tests to determine if the solution addressed security objectives.

The blockchain assessment framework provided additional areas of considerations with respect to management's security objectives and further opportunities to enhance stakeholder trust in the solution.

> There are many factors that increase complexity and compute demands at the production level than at the use case or even proof-of-concept level (e.g. speed and volume of transactions, number of active participants).

7. Interoperability and integration

Organizations need to be aware that their legacy systems may not be designed to interact with blockchain solutions or capitalize on the advantages offered by them. Comprehensive examination of interoperability and integration is essential to successful implementation of a blockchain solution. Given the immutability of transactions, it is essential that the proper mechanisms are in place to prevent incorrect data from being written onto a blockchain.

Controls should be developed for the blockchain — both independently and with respect to guarding connections between systems. As blockchains are developed or moved from proof-of-concept into production, companies should also ensure a proper focus on change management and testing in order to ensure changes to scale and scope do not affect interoperability and integration.

8. Scalability and performance

Use cases provide tests of the ability of a blockchain to fulfill a specific purpose. However, prior to selecting a solution or moving to a production system, companies should be confident that blockchain will perform under the stresses of a production environment. There are many factors that increase complexity and compute demands at the production level than at the use case or even proof-of-concept level (e.g. speed and volume of transactions, number of active participants). The successful scalability and consistent performance of a blockchain solution is dependent on a number of factors, including non-blockchain software that it is directly reliant upon. One high profile example includes cryptocurrency exchanges during the sudden market activity increases in late 2017 through early 2018.[2] Therefore, prior to selecting a solution and to implementation, companies should assess whether a solution is production capable and if it can be scaled to grow and align with their use case going forward.

9. Business continuity and disaster recovery

Similar to any other technology implementation, organizations need to have a plan for addressing business continuity and disaster recovery risks pertaining to the blockchain application. The decentralized nature of blockchain technology creates a unique reliance on the other participants of the blockchain network in order to maintain functionality.

Given that private blockchains may have both centralized and decentralized components (e.g. certificate authority, cloud key management system), there needs to be concrete understanding of what will happen should these components be affected by any potential factors. This will ensure any outage is limited and no inappropriate transactions can occur.

10. Governance, risk, and compliance

Overall governance, risk management and compliance support is essential to any blockchain implementation. Given there are different users — sometimes even competitors — involved in the blockchain, companies need to be very clear on specific roles and responsibilities related to the blockchain.

For example, how the organizations will jointly manage changes to blockchain software, onboarding of new nodes, or other activities. Clear and documented roles, responsibilities, and accountabilities can ensure everyone participating in the blockchain is on the same page with respect to compliance processes.

[2] https://www.bloomberg.com/news/articles/2018-01-12/crypto-exchange-kraken-goes-dark-and-user-anxiety-surges

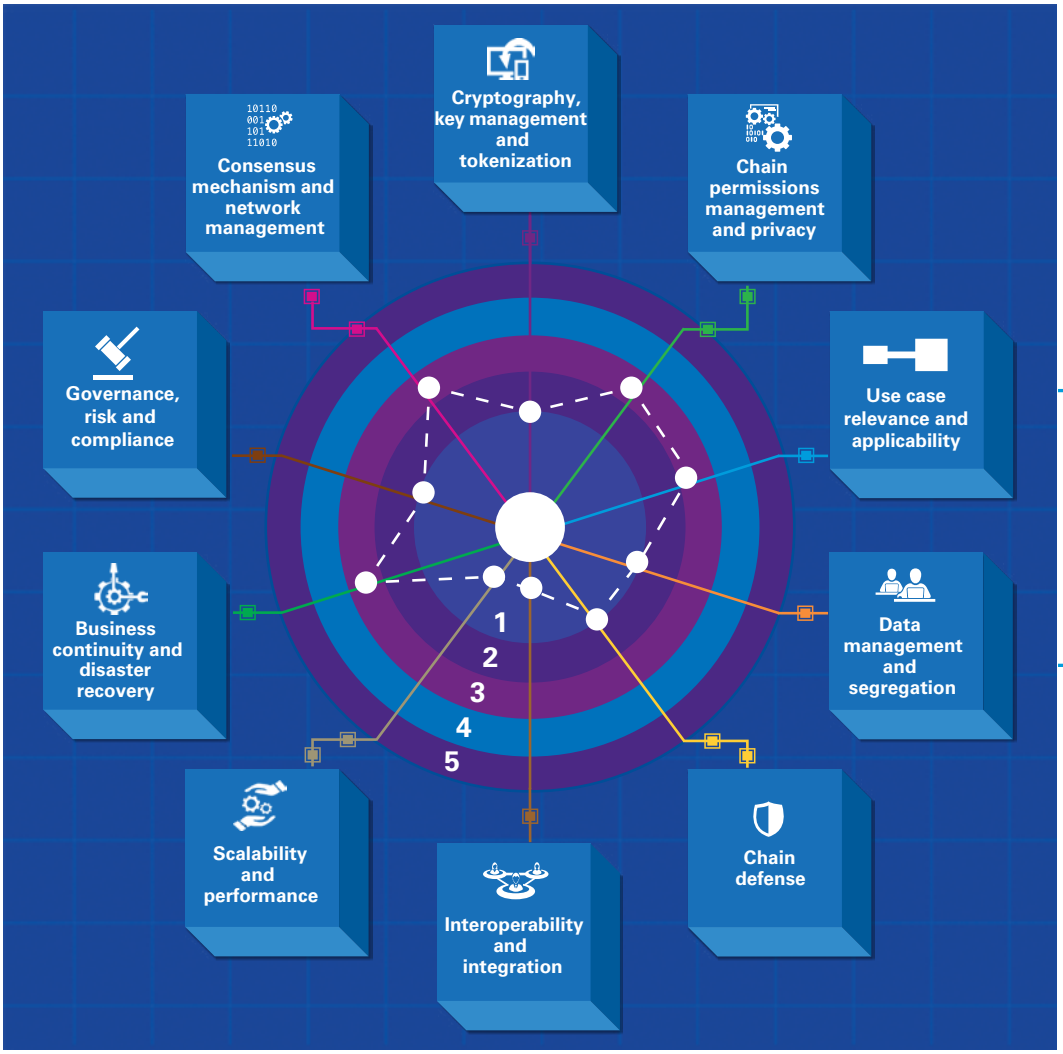
Assessing the risks: A five-level approach

KPMG professionals use a five-level maturity scale to assess the robustness of controls over specific activities. In the figure below, we provide an example of the maturity level of blockchain-specific controls associated with each assessment level. Using this scale, we can assess both your current blockchain-specific risks and define your goal state for the future.

Each of the blockchain risk areas is scored on the maturity scale. This allows us to help companies determine where controls are strongest and where weaknesses or gaps exist that should be recognized or addressed.

Once we have done the initial assessment, we use a spider map to highlight the results of the blockchain risk assessment in a holistic manner so that companies can visually see the current level of maturity of risk controls related to a specific blockchain solution or project.

KPMG blockchain technology risk assessment example output



Level 5 — Value
On boarding and off boarding procedures are defined also for future state operation of the network.

Level 4 — Service
On boarding and off boarding procedures are defined for all network participants and periodic compliance checks take place.

Level 3 — Proactive
Controls are in place to detect unauthorized access.

Level 2 — Reactive
Procedures are in place to ensure data confidentiality.

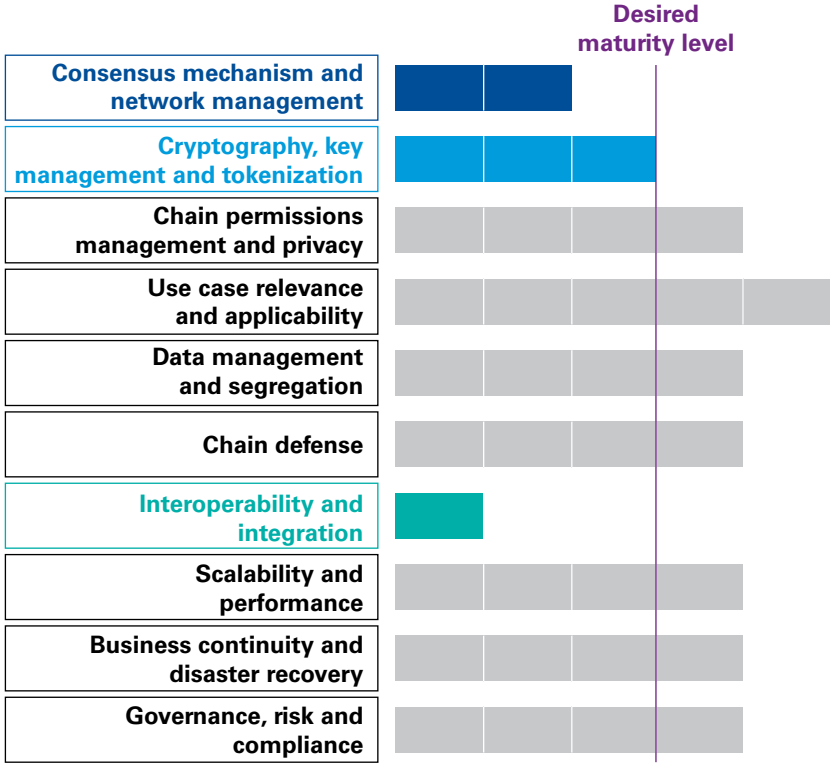
Level 1 — Adhoc
Lack of defined on boarding and off boarding procedures for network participants.

Turning assessment into action

Based on the results of the blockchain risk assessment, we provide recommendations to help organizations respond to weaknesses. The following figure provides an example of what recommendations could look like.

It should be noted that the blockchain risk assessment is not prescriptive, but rather focuses on identifying key areas that warrant further attention and action. Based on the recommendations, actual controls need to be developed based on the unique needs of a blockchain project or solution. As mentioned earlier, there is no one-size-that-fits all.

Recommendations



Recommendation consensus mechanism and network management
The consensus mechanism selected may create challenges when meeting the business continuity requirements of the organization. Additional controls and possibly external attestation reports may be required to further address these risks.

Recommendation cryptography, key management and tokenization
While standards exist for private key ownership and accountability, it is recommended that active monitoring on attempts to access private keys is set up. Secondly, it is recommended that private keys are made unavailable to non-production systems.

Recommendation interoperability
There are no checks for completeness and accuracy between the relevant internal subleger and blockchain which could result in incorrect transactions being posted to or read from the blockchain.

Creating sustainable value through blockchain

There is no doubt that blockchain makes for an exciting value proposition. Yet, you should not jump blindly into blockchain implementations, or move from use cases to productions, without having a holistic picture of the risks.

Just because a solution is blockchain-enabled does not mean it addresses relevant risks regardless of what some blockchain proponents might think. Blockchain is still a very young technology, with new innovations, uses and solutions being introduced every day. There are still many hard-earned lessons to be learned from blockchain implementations. Therefore, making assumptions with respect to key risks and security associated with specific solutions could open the door to significant issues down the road.

To achieve the most value from blockchain, both now and in the future, you must take responsibility for its safety and security. There are no opportunities or shortcuts to learn from others' mistakes. By conducting a blockchain risk assessment and then addressing key risks associated with your specific blockchain activities, you can make sure you are well positioned to leverage the efficiencies and cost-effectiveness provided by blockchain without opening yourself up to unexpected risks.

> "To achieve the most value from blockchain, both now and in the future, you must take responsibility for its safety and security."

Case study

Rabobank

Rabobank is a multinational cooperative bank and the second largest financial service provider in the Netherlands, serving over 10 million customers worldwide. It is the leading financial service provider worldwide in the agri-food (wholesale, rural and retail) business, and is especially active in banking, lending, bank assurance and factoring within this sector.

Like many banks, Rabobank had been looking at blockchain and was taking steps to explore the possibilities associated with it. KPMG's professionals worked with Rabobank to test the blockchain technology risk assessment[3] against one of its high impact blockchain projects.

Rabobank commented that the assessment provided concrete pointers as to which areas to focus on and how to improve their maturity. The framework clearly helped to generate an oversight of all IT maturity risks and the corresponding mitigations, thereby helping to focus on improving the areas that need it the most.

[3] The Blockchain Risk Assessment was previously referred to as the Blockchain Maturity Model

“With expertise in more than 40 countries, member firms blend blockchain-based consulting services with KPMG Lighthouse Centers of Excellence to help organizations maximize ROI of their blockchain investments.”

About KPMG Distributed Ledger Services

Embracing a rapidly-advancing new technology that disrupts business as usual is not easy. KPMG Distributed Ledger Services professionals are dedicated to working with you to create relevant, scalable solutions that drive value for your organization.

Our tailored approach supports organizations through a life cycle process focusing on:

- strategic realization
- requirements guidance
- systems and operations integration
- managed services with the potential to address data governance
- third party blockchain assurance and attestation related services
- conventional audit services such as audit and tax services.

With expertise in more than 40 countries, member firms blend blockchain-based consulting services with KPMG Lighthouse Centers of Excellence to help organizations maximize ROI of their blockchain investments.

KPMG Lighthouse is comprised of software engineers, data scientists, data engineers, domain/Industry consultants and visualization specialists. Teams work with financial institutions to evaluate trends in blockchain and other emerging technologies and to identify the technical solutions best able to meet their unique requirements. KPMG Lighthouse specialists also help assess security issues and identify other risks associated with blockchain and other emerging technology.

We provide

- deep industry and business expertise
- business-case driven transformation
- blockchain platform agnosticism
- global teams of domain experts, system architects and technical specialists.

Authors

Eamonn Maguire
Global Distributed Ledger Services Lead, Financial Services,
KPMG International
Director, Financial Services Advisory,
KPMG in the US
T: +1 212 954 2084
E: emaguire@kpmg.com

Kiran Nagaraj
Global Cryptoasset Lead, Distributed Ledger Services
KPMG International
Managing Director
Emerging Technology Risk Services
KPMG in the US
T: +1 212 872 3056
E: kirannagaraj@kpmg.com

Dennis de Vries
Distributed Ledger Services Lead
KPMG in the Netherlands
T: +31 206 567451
E: devries.dennis@kpmg.nl

Sam Wyner
Distributed Ledger Services
KPMG in the US
T: +1 212 954 4903
E: swyner@kpmg.com

Additional contacts

Wei Keat Ng
Global COO (Markets) Distributed Ledger Services
KPMG International
T: +44 20 73111889
E: wei.keat.ng@kpmg.co.uk

Laszlo Peter
Director, Innovation & Digital Solutions, Head of Distributed Ledger Services
KPMG Australia
T: +61 2 9455 9018
E: laszlopeter@kpmg.com.au

Catherine Philippe
Partner, IT Financial Services
KPMG in France
T: +33 155688809
E: cphilippe@kpmg.fr

Sven Korschinowski
Head of Fintech and Innovation
KPMG in Germany
T: +49 69 9587 4235
E: skorschinowski@kpmg.com

Said Fihri
Head of Fund Distribution Services, Head of Distributed Ledger Services
KPMG in Luxembourg
T: +352 2251 57892
E: said.fihri@kpmg.lu

Jan Reinmueller
Head of Digital Village Digital + Innovation
KPMG in Singapore
T: +65 65071581
E: jreinmueller@kpmg.com.sg

Anton Ruddenklau
Head of Digital & Innovation Financial Services
KPMG in the UK
T: +44 20 76942224
E: anton.ruddenklau@kpmg.co.uk

Christopher Mottram
National Service Solutions Leader IT Audit and Assurance
KPMG in the US
T: +1 404 979 2100
E: cmottram@kpmg.com

Bernard Wieger
Partner, IT Audit and Assurance
KPMG in the US
T: +1 816 802 5810
E: bwieger@kpmg.com

David Palmer
Managing Director, IT Audit and Assurance
KPMG in the US
T: +1 216 875 8171
E: davepalmer@kpmg.com

Andrew Koh
Partner, Head of Digital Trust Management Consulting
KPMG in Singapore
T: +65 6411 8207
E: andrewkoh@kpmg.com.sg

Edmund Heng
Director, Digital Trust Consulting
KPMG in Singapore
T: +65 6411 8252
E: eheng@kpmg.com.sg

kpmg.com
kpmg.com/socialmedia

Designed by Evalueserve | Publication name: Realizing blockchain's potential | Publication number: 135734-G | Publication date: September 2018