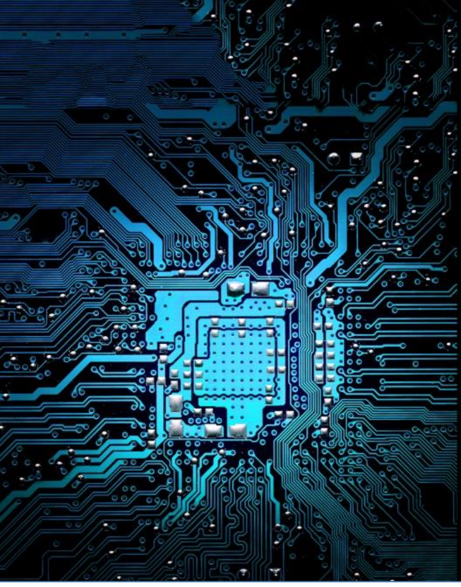

KPMG

R.G. Manabat & Co.

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

Perspectives
24 September 2018

Companies should not make assumptions as to what a blockchain is capable of doing, or how safely and more securely it can complete move up.

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.

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 excerpt was taken from the publication entitled Realizing blockchain's potential.

For more information on KPMG in the Philippines, you may visit www.kpmg.com.ph.