How will blockchain impact an information risk management approach?

Steven van der Weerd MSc
is a senior IT auditor at KPMG Business Assurance.
vanderweerd.steven@kpmg.nl

Blockchain is considered an emerging technology that has the potential to significantly transform the way we transact. The establishment of new asset classes and transactional models substitute conventional payment and settlement platforms. The major advantage that blockchain offers is transparency and elimination of custodial necessity. However, organizations implementing blockchain in their IT environment are also faced with a new set of risks arising from this distributed ledger technology. Before organizations can even consider implementing blockchain, they should understand its implications on their information risk management strategy and how this translates to their business. In this article we will take a closer look at blockchain and how it differs from the more 'conventional' information systems. Based on the uniqueness of blockchain technology, this article will introduce some of the key risks arising from the implementation of this technology in existing IT environments. In addition, the article will describe how these risks affect information risk management. Facebook's Libra platform will be used to apply our insights to a real-life scenario. Lastly, the author will conclude with a brief approach on auditing blockchain systems and what IT auditors might take into consideration when faced with this technology.

INTRODUCTION

Blockchain is considered a breakthrough in the field of distributed computing and has the potential to completely disrupt existing transactional models and business processes. As shown in a global survey conducted by [Delo19] in 2019 (that polled over 1000 senior executives), the technology is increasingly being researched by both public as private organizations. One of the key results of the survey shows that "fifty-three percent of respondents say that blockchain technology has become a critical priority for their organisations in 2019" ([Delo19], p. 3). These developments are substantiated by Laszlo Peter, Head of KPMG Blockchain Services in the Asia Pacific: "Blockchain is certainly here to stay. While funding may have slowed in 2019, it simply shows the growing maturity of the market. It is a sign that investors are moving away from the 'fear of missing out' mentality (...) and are making more mature investment decisions and focusing on more meaningful initiatives" ([KPMG19], p. 16).

Given its *newness*, blockchain can still be considered an innovative type of technology. But there is something peculiar about innovative technologies and its application by organizations: innovation can be considered a journey into the unknown. Innovation is exploring *how* new technologies can be applied to business and IT processes, this brings uncertainty: after all, if you venture into the unknown, you are not particularly certain about what lies ahead; there are risks (downside and upside) as well as opportunities.

Given the profound impact that blockchain might have on organizations and the way they transact with(in) each other, a thorough information risk management strategy should be designed. The risk management approach should be able to identify and address the risks arising from blockchain and how blockchain-powered processes might impact the control environments surrounding these processes. Designing a risk management approach for blockchain will not only enable organizations to remain in control; it will also help organizations design and implement blockchain securely and appropriately in their business and apply the effective operation of governance structures for blockchains that are transacted by multiple organizations. However, before information risk management professionals can start to think of designing a blockchain risk management approach, it is essential that risk professionals profoundly understand blockchain, and how it differs from 'conventional' information systems.

Based on the relatively uniqueness of blockchain technology, this article will introduce some of the key risks arising from the implementation of this technology in existing IT environments and offer an impression on how these risks affect information risk management. This article will reflect on Facebook's Libra platform to apply our insights to a real-life scenario. Lastly, you will find a high-level approach for auditing blockchain systems and what IT auditors might take into consideration when faced with this technology.

UNDERSTANDING BLOCKCHAIN

Blockchain is considered a subset of distributed systems. In general, a distributed system can be defined as a group of independent computing elements working together to achieve a common objective ([Stee16]). Now, distributed systems are all around us: from airplanes to mobile phones, anything can be considered a distributed system to a certain degree. Most of these distributed systems are 'closed', where only authorized computing elements (i.e. agents) are able to access and operate within these systems. These agents trust each other, and communication is considered safe. This makes sense, as we wouldn't want unknown agents to be able to access airplanes or our mobile phones and perform harmful activities.

Another example is the internet. In contrast to the two examples mentioned, the internet is a distributed system where it is possible for unknown agents that do not trust each other, to operate in and perform activities that might be considered harmful to other agents (such as yourself) or even the overall system. If we want to perform certain activities on the internet – such as sending money to a party that you do not necessarily trust – we rely on intermediaries such as financial institutions (banks) to ensure that the amount is actually debited to the bank account of the intended party and credited from the sending party. The banks function as a trusted third party that ensure that both parties involved in the transaction are not able to fraud each other.

How does this relate to blockchain and why exactly is this technology considered a breakthrough in the field of distributed computing ([Kasi18])? On a general level, blockchain is simply one of the ways for multiple parties to reach an agreement (i.e. consensus) on the state of the system (e.g. a ledger or a digital transaction being recorded on that ledger) on a given time without having to rely on a trusted third party or central authority (such as the bank in the example above). Systems that allow for this multi-party consensus are considered to be blockchains ([Weer19]). Where the 'traditional' distributed systems needed a trusted third party if transacting participants wanted to exchange information, value or goods without trusting each other, blockchains delegate this trust to the party's participants themselves (i.e. endpoints); a trusted third party is no longer required.

This article is not intended to go into detail of *how* blockchain delegates trust to the participants (i.e. end points). However, to provide some understanding, a more technical definition introduced by [Rauc18] is provided below.

"A blockchain system is a system of electronic records that:

1. enables a network of independent participants to establish a consensus around
2. the authoritative ordering of cryptographically-validated (signed) transactions.
3. These records are made persistent by replicating the data across multiple nodes and
4. is tamper-evident by linking them together by cryptographic hashes.
5. The shared result of the reconciliation/ consensus process – the ledger – serves as the authoritative version for these records" ([Rauc18], p. 24).

It is important to understand that there are countless ways of designing a blockchain system. However, in the end, all blockchain systems are considered to have one primary objective: to facilitate multi-party consensus whilst operating in an adversarial environment ([Rauc18]). That is, an environment in which participants might not trust each other or behave in such a manner that it is not in line with the best interest of the overall system.

Permissioned versus permissionless

Broadly speaking, blockchains can be categorized "based on their permission model, which determines who can maintain them" ([Yaga18], p. 5). The Bitcoin network can be defined as a permissionless (public) blockchain as anyone is able to produce a block (consisting of transactions), read data that is stored on the blockchain and issue transactions on this blockchain network. Since the network is open for anyone to participate, malicious users might be able to compromise the network. In order to prevent this, "permissionless networks often utilize a multi-party agreement or consensus system that requires users to expend or maintain resources when attempting to produce blocks. This prevents malicious users from easily compromising the system" ([Yaga18], p. 5). In the case of the Bitcoin blockchain, the Proof of Work consensus mechanism is used where block producers are required to expend computational resources in order to produce a block ([Naka08]). Other consensus mechanism examples include Proof of Stake (Ethereum), Proof of Authority (Vechain) and Proof of Elapsed Time (Hyperledger Sawtooth). Although designed differently, all consensus mechanisms aim to discourage malicious behaviour on the blockchain network ([Weer19]).

Permissioned blockchains are restricted access networks: the parties responsible for maintaining the network are able to determine who can access it and a restricted amount of parties are authorized to produce blocks ([Cast18]) in the case of blockchains. Whereas permissionless blockchains are open for anyone, accessing permissioned networks requires approval from the authorised users of said network: "since only authorized users are maintaining the network, it is possible to restrict read access and to restrict who can issue transactions" ([Yaga18], p. 5).

The likelihood of arbitrary or even malicious behaviour on permissioned networks is smaller than on permissionless networks, as only authorized (thus, identified and trusted) users are able to access it. In case a user behaves malicious or not in the best interest of the entire network, access can be revoked by the parties maintaining the network. Although, malicious behaviour is discouraged as a result of the network's restricted access and because a user's identity needs to be determined, consensus mechanisms may still be used to ensure "the same distributed, resilient, and redundant data storage system as a permissionless network (...), but often do not require the expense or maintenance of resources as with permissionless networks" ([Yaga18], p. 5).

Risks arising from blockchain

Now that we have a basic understanding of blockchain and how it differs from the more 'conventional' IT systems, we can take a look at how blockchain technology might affect existing information risk management approaches when it is implemented in existing organizational IT environments. In order to keep this article brief, the author has selected the following set of key risks arising from blockchain that are worthwhile to address (see Figure 1).

Blockchain systems are considered to facilitate multi-party consensus while operating in an adversarial environment

Figure 1. Domains where risks where might arise from using blockchain.

Scalability & Continuity

Reaching consensus requires coordination and communication between nodes that are often spatially separated from each other and located within the participant's internal IT environments. This might eventually result in a lack of scalability or even threaten the continuity of the blockchain system and the (business) process activities of organizations relying on the blockchain system.

Centralization & Collusion

A blockchain is comprised of independent nodes. Although these nodes are operating independently from each other, these nodes might be owned by a single organization or by a collaboration of organizations. Competitors might be blocked from transacting on this system or risk being restricted from using certain functionalities.

Interoperability

With the advent of blockchain adoption, interoperability between the technological generations may be a challenge. A blockchain cannot simply be installed in the existing IT environment of an organization as it must be connected to legacy IT systems, that usually have other compatibility limitations, or perhaps even to other blockchains.

Data Management & Privacy

Any transaction proposal that is accepted to the ledger is considered final. Incorrect, incomplete or even unauthorized transactions might result in unintended consequences such as degraded data integrity or violated privacy requirements due to the fact that personal data is accessible, and the transaction commits cannot be reverted (to adhere to the right to be erased/forgotten). Sensitive personal data cannot be stored directly on the blockchain, but rather 'off-chain' or on a 'sidechain' (parallel blockchain), whereby the blockchain does not contain personal data but points to the protected location where that data is stored and can be removed if needed.

Smart Contracts

Smart contracts are agreements between blockchain participants that are codified into the authoritative ledger. The contract is executed automatically when certain requirements (typically established by the parties involved) are met. If smart contracts are incorrectly designed, this might result in unintended and unforeseen consequences.

Consensus & Network

Achieving consensus in a blockchain generally involves a complex set of mathematical functions and coordination between the network nodes. In addition, in order to ensure that the (majority of the) nodes exhibit honest behaviour, economic game theory needs to be considered in the consensus process as well. If the consensus process is flawed, organizations transacting on this blockchain might be exposed to significant risks – both operational as financial.

Compliance

The immaturity of blockchain technology is visible in the regulatory space as well, where laws and governmental policies for applying and operating blockchain technology are still in an embryonal stage. In addition, by its very nature, blockchains allow for the transacting between parties that do not need to know or trust each other. This exposes an organization to the risk of participating in money laundering of terrorist financing.

Functional requirements

Careful considerations should be made regarding the decision to implement a blockchain; not only regarding the necessity of implementing a blockchain into an existing IT environment, but also which type to select. Selecting or developing a blockchain that does not align with the organization's business or operating model needs might have significant consequences for the organization's business activities that rely on the blockchain.

Cryptographic Key Management

Blockchains employ cryptographic functions such as hashing algorithms and public key cryptography to ensure the integrity of the overall system and guarantee the safety. Improper management of cryptographic keypairs might result in unauthorized access of the system.

Third Party & Governance
Where the effective operation of traditional IT systems (i.e. every organization is the owner of their IT) primarily relies on the control environment of the organization itself, blockchains relies on both the overall control environment of the network as well as the control environments of the individual participating organizations. One can argue whether 'third parties' in a blockchain context are actually 'second parties'. (See further the box on blockchain governance.)

IMPACT OF BLOCKCHAIN ON INFORMATION RISK MANAGEMENT

The field or information risk management is broad in nature and extensively covered in both academics and business. On a general level, information risk management (IRM hereafter) can be defined as "the application of the principles of risk management to an IT organisation in order to manage the risks associated with the field" ([Tech14]). To support the design of an effective IRM strategy, several standards and approaches have been published that aim to help organizations in managing IT risks and designing an IT control environment. Examples of these standards are the Handreiking Algemene Beheersing van IT-Diensten from NOREA, the ISO27001 framework from ISO, the COBIT standard or the COSO management model.

When we consider the abovementioned risks arising from blockchain, it appears that these risks primarily relate to the absence of a trusted third party or a central authority: where current IT environments of organizations can typically be thought of as centralized silos (operated and managed by a single party) that are logically separated from each other, blockchain powered IT environments dissolve these boundaries as organizations transact on the same system.

Extending this development to information risk management, with centralized IT environments, the Information Risk Management organization is primarily concerned with the internal control environment surrounding their centralized IT environment. Generally, this control environment is sufficient to address the risks arising from IT and facilitate the appropriate operation of the IT environment.

However, when organizations implement blockchain systems, they factually open up their IT environment to third parties (perhaps also unknown parties or competitors) that are not necessarily trusted by the organization (i.e. the organization will operate in an adversary environment).

Risks arising from blockchain appear to relate primarily to the absence of a trusted third party or central authority

Taking a closer look at Libra

If we look at this from a more practical perspective, let us take a closer look at Facebook's Libra initiative: a consortium of major organizations – i.e. Facebook, Spotify, Uber and Vodafone – that develop their own blockchain with the objective of operating as a global currency transactional model ([Libr19]). The following stakeholders are involved in the management of the platform:

- The Libra Association governs the network.
- Libra Networks LLC develops the software and infrastructure.
- The actual blockchain network consists of nodes ran by the individual Association members.
- Users (consumers and other organisations) can operate on this network.

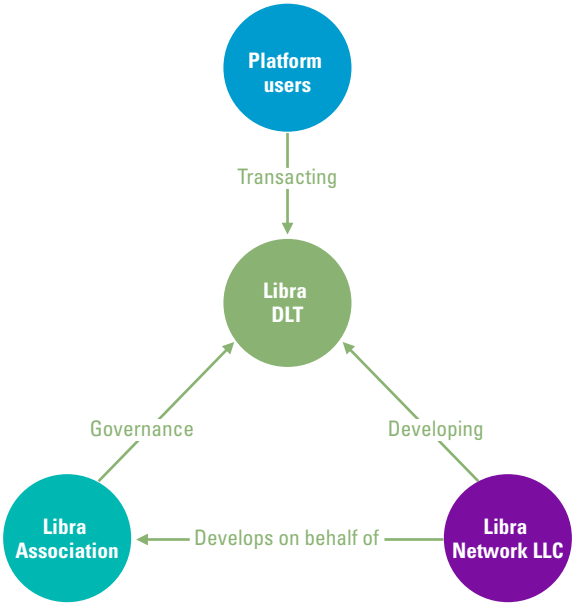

Figure 2. Visualizing Libra's actors and their relationships.

When we take a look at the relationship of the actors involved with Libra, one can argue that the key risks relate to the inherent properties of the Libra blockchain and its multi-party transactional model are as follows:

1. Competitors are collaborating on the platform, but there is no guarantee of fair play and a level playing field.
2. Node validators (organizations involved in the consensus process and validation of transactions taking place on the platform) have no access to each other and it is therefore difficult for these organizations to verify whether they are all adhering to the standards and requirements set by the governing body (the Libra Association) or whether they have an effective operation of their control environments.
3. Furthermore, it is difficult for the governing members to verify that the developing party exercises its responsibilities in an objective manner and does not provide participants (e.g. Facebook) with a competitive advantage over other governing members, but also over organizations that are not part of the network's governance body.

In order to ensure that all stakeholders involved are comfortable with transacting on the Libra platform, the mentioned risks (not limited to) should be addressed first. It appears that addressing these risks i.e. designing an effective information risk management strategy requires multi-party collaboration and governance (see also the box on a blockchain governance case).

Governance considerations

The governance considerations of a platform can make or break the success of not only your organization's implementation but the continuity of the entire platform. An exemplary case is the IBM and Maersk supply chain platform TradeLens. In 2018, the companies announced a joint venture to unify the shipping industry on a common blockchain platform. The platform was developed within a governance model that put major decision-making power in the hands of the founders, allowing them to retain the intellectual property of the shared platform and forcing other logistical companies to invest significantly in blockchain platform software. This resulted in a reluctant reception and very limited onboarding of other participants, limiting the transaction volume via this platform. As a consequence, the tipping point for success couldn't be reached. After restructuring the governance model, other companies, such as CSX, PIL and CEVA, decided to join.

The correct governance model for your platform is not a one-size-fits-all and depends on several factors. These factors include, but are not limited to:

- strategy and mission-criticality
- policy/decision-making and risk sharing
- participant roles, responsibilities and representation
- node management
- type and variety of international regulatory jurisdictions
- desired permission level of features
- cost of ownership, incl. financing and cost charging
- supervisory bodies and assurance

The IT audit will need to stop treating IT environments as singular

Risks	Controls
Centralization & Collusion	
Dynamic node participation might result in the risk of network exclusion of participants	Contractually enforce that the organization will host validator nodes of the network it operates on. At least one node should be owned when transacting on a blockchain
	Monitor network activities to determine which Public Key addresses (i.e. other parties transacting on that blockchain) own validator nodes. If a participant's consensus power increases, proper escalation measures should be designed and enforced.
Network participants might achieve majority control of blockchain network. This might violate the integrity of the network	The organization must contractually enforce that they will host validator nodes for each blockchain system it uses.
	Blockchain participants contractually agree on the distribution of consensus power to prevent one party from achieving majority control.
	Monitor network activities to determine which Public Key addresses (i.e. other parties transacting on that blockchain) own validator nodes. If a participant's consensus power increases, proper escalation measures should be designed and enforced.
	In case of permissionless networks, monitor the network to ensure that centralization of the Validator power is identified appropriately.
Data Management & Privacy	
The inherent nature of blockchains might result in GDPR (e.g. "right to be forgotten") breaches	Establish data definitions and implement gatekeeper controls that ensure confidential and sensitive information is not stored on the blockchain network.
Data might be input incorrectly or incompletely.	The parties responsible for onboarding real-life object representations onto the blockchain ('Oracles') are subject to an ISAE3000 / SOC2 audit and is provided to the organisation that relies on such data.

Table 1. An extract of a blockchain risk and control framework.

AUDITING BLOCKCHAIN

To mitigate the risks arising from blockchain, organizations are able to design control environments surrounding their blockchain systems and business processes transacting on those systems. To give you an example of controls that might be designed, the author has included a small part of controls intended to mitigate risks related to the *Centralization & Collusion* domain and the *Data Management & Privacy* domain introduced earlier.

When we extend this to the field of IT audit, we might consider the approach of an IT auditor to become less singular and more driven from an ecosystem perspective. The IT auditor does not stop at the boundaries of the IT (control) environment of the organization; it extends to the control environment of the bigger network, consortium and the individual participants with which the organization transacts. Therefore, IT auditors need to equip themselves with the capabilities of auditing a governing network i.e. consortium and develop skillsets to properly assess multi-party risks.

In the author's opinion, IT auditors will extend their focus to third party (smart) contracts, resolution models and how consensus is configured – both from a technical as well as an economic game theory perspective. The IT audit will need to stop treating IT environments as singular and start treating it as a risk ecosystem that is comprised of multiple actors.

For further details on assessing and auditing blockchain implementations, please refer to [KPMG18] and [ISAC19].

The IT auditor will increasingly shift towards a consortium or ecosystem auditor

CONCLUSION

The topic of blockchain and its impact on information risk management can be elaborated on and encompass an entire book by itself. If organizations want to remain in control of their blockchain-enabled IT environment, only to consider that the internal IT control environment is no longer sufficient: organizations need to start taking into account the control environment of the entire blockchain network, but also the internal control environments of each participating organization acting as a node validator. The IT control environment of an organization implementing a blockchain therefore becomes an 'ecosystem' where its own control environment and information risk management strategy is dependent on the control environments of the broader ecosystem and its individual participants. In essence, the shift towards distributed ledger technology results in a shift to *distributed control environments* as well.

Blockchain technology has the potential to digitize supply chains, business processes, assets and transactions. How will the Information Risk Management organization and the IT auditor conduct their risk assessment? How can an effective control environment be designed when organisations become part of digital ecosystems? These are valid questions that ought to be resolved before organizations can think of harnessing the full potential of blockchain technology. The author is convinced that the Information Risk Management professional and IT auditor have an exciting future ahead of them and are able to provide a great contribution in helping transform organizations in an appropriate and controlled manner.

References

[Cast18] Castellon, N. , Cozijnsen, P. & Goor, T. van (2018). Blockchain Security: A framework for trust and adoption. Retrieved from: https://dutchblockchaincoalition.org/uploads/DBC-Cyber-Security-Framework-final.pdf.

[Delo19] Deloitte (2019). 2019 Global Blockchain Survey. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

[ISAC19] ISACA (2019). Blockchain Preparation Audit Program. Retrieved from: https://next.isaca.org/bookstore/audit-control-and-security-essentials/wapbap

[Kasi18] Kasiderry, P. (2018). How Does Distributed Consensus Work? Retrieved from: https://medium.com/s/story/lets-take-a-crack-at-understanding-distributed-consensus-dad23dodc95.

[KPMG18] KPMG (2018). Blockchain Technology Risk Assessment. Retrieved from: https://home.kpmg/xx/en/home/insights/2018/09/realizing-blockchain-potential-fs.html.

[KPMG19] KPMG (2019). The Pulse of Fintech 2019. Retrieved from: https://home.kpmg/xx/en/home/campaigns/2019/07/pulse-of-fintech-h1-19-europe.html.

[Libr19] Libra Association Members (2019). An Introduction to Libra.

[Naka08] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: https://bitcoin.org/bitcoin.pdf.

[Rauc18] Rauchs, M. et al. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. Retrieved from: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.

[Stee16] Steen, M. van & Tanenbaum, A.S. (2016). A brief introduction to distributed systems, *Computing, 98*, 967-1009.

[Tech14] Techopedia (2014). IT Risk Management. Retrieved from: https://www.techopedia.com/definition/25836/it-risk-management.

[Weer19] Weerd, S. van der (2019). An exploratory study on the impact of multi-party consensus systems for information risk management.

[Yaga18] Yaga, D. et al. (2018). Blockchain Technology Overview, NISTIR8202. Retrieved from: https://csrc.nist.gov/publications/detail/nistir/8202/final.

About the author

Steven van der Weerd MSc started as a consultant with KPMG IT Assurance & Advisory in 2015. He has performed numerous audit and advisory engagements within the financial services sector. He focuses on financial markets with an emphasis on the banking, payments and leasing sectors. He is specialized in IT audit innovation and developing information risk management approaches for (emerging) technologies, with a specific emphasis on blockchain technology. He is also involved in KPMG's Blockchain taskforce and in NOREA's Knowledge Group on Supply Chain Digitisation focused on blockchain controls.

The author likes to thank Raoul Schippers for his addition on blockchain governance.