Blockchain: with great power comes great responsibility

Creating a blockchain maturity model

Blockchain is seen as a new technology which potentially enables enormous cost savings and efficiency gains. Private blockchains allow the user to have more control over its configuration; they allow the user to specify which parties can participate and set the ground rules. However with great power comes great responsibility: it is crucial that these blockchains are set-up correctly in order to be able to rely on the benefit of blockchain, immutability. In this article we examine the intricate world of blockchain risks and give a first impression of a blockchain maturity model to enable organizations to work effectively and securely with blockchain.

Ir. H. Spenkelink
is a senior consultant at KPMG Digital Ledger Services.
spenkelink.hardwin@kpmg.nl

INTRODUCTION

Blockchain is seen as a new technology which potentially enables enormous cost savings and efficiency gains. It is almost impossible not to hear the word blockchain in the news at least once a day. It is applicable for a wide range of use cases and therefore in almost all industries there are organizations looking at the use of blockchain technology to optimize or enhance their processes.

The advantages of blockchain technology seem to have no boundaries. However, while current experimentation with blockchain is mostly in the proof-of-concept phase, what will happen when blockchains start to enter the business domain? The immutability of blockchain networks means that once data is shared it cannot be revoked. Are traditional IT risk frameworks still sufficient to keep such risks under control? In this article we examine the intricate world of blockchain risks and give a first impression of a blockchain maturity model to enable organizations to work effectively and securely with blockchain.

> One has to get the entire value chain 'on board' before starting to use blockchains

PUBLIC VERSUS PRIVATE BLOCKCHAINS

This article is the second in a series of articles about blockchain. In the first article [Spen16] an overview was given of the benefits of using blockchain and the differences between a public and a private blockchain.

The article ended with the conclusion that blockchains get their value from having multiple parties working together and sharing business processes in a value chain. Public versus private implementations each have their own pros and cons and therefore are different. To recap, please see Table 1 below.

Using blockchain technology is much more than simply introducing new IT; existing business processes and even entire business models will be changed by adopting this innovation. Blockchains deliver most of their value in having multiple parties work together in an efficient and effective manner, which means that the process of redesigning existing business processes is not a standalone action. One has to get the entire value chain 'on board' before starting to use blockchains.

This article focuses on the use of private blockchains, or more accurately called Distributed Ledger Technology (DLT). Currently most implementations of blockchain in the market are based on a DLT platform, such as Hyperledger or Corda. Businesses choose such a type of platform because they want to keep a certain level of control over their blockchain implementation, and a private blockchain or DLT enables them to do so.

Table 1. Key differences between public versus private distributed ledgers.

	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
Transaction volume supported	Low	High
Commonly used for	Payments, remittances, prediction markets, distributed storage, paid social networking	Asset servicing, FX (Foreign eXchange), provenance tracking, trade finance, health care

Distributed Ledger Technology

When using a public blockchain, as the name suggests, anyone can connect to the existing infrastructure of, for example, Bitcoin or Ethereum. This means that one can simply start transacting on this network without setting up an IT infrastructure to facilitate this.

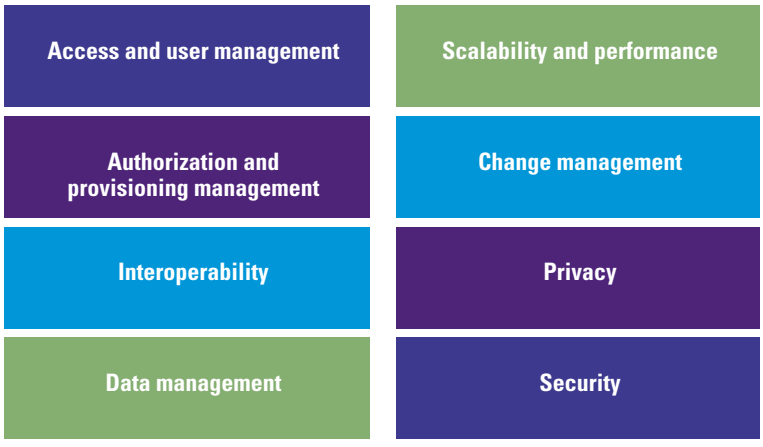
Access and user management

User access management of blockchain technology is a new concept, for which so far no best practices and standards have been found and set. Blockchain uses unique addresses which are assigned to each participant in the network. This address is used for transactions (sending and receiving) and enable participants to authenticate themselves and these transactions by using a public key.

The provisioning process of these key-pairs (unique identifier) and assigning access rights is different for each DLT implementation. Due to the fact that DLT heavily relies on digital identity, this means that adequate management and security around the process of providing and storing the cryptographic keys is of great importance. In addition, users from multiple organizations, with user access authorizations are difficult to manage because the network is distributed, at this moment there is no oversights/supervisory body which checks on valid access rights.

This results in risks of unauthorized access of participants (organizations) and users due to the lack of an overall supervision/oversight that manages access for user and participants.

Figure 1. DLT risk areas.



Unlike public blockchains, the nature of private blockchains is more similar to a traditional IT system in that the users of the platform have to set up and maintain the infrastructure themselves. So a group of banks running, for example, a trade finance blockchain on a private ledger will have to select the DLT implementation they see as most suitable and start deploying this on a set of nodes that they host. On top of this they have to configure settings, such as the consensus mechanism to use, the nodes which are allowed to connect to the network and the creation of identities.

As one can imagine, the greater flexibility of private blockchains also incurs a greater responsibility and getting grip on the risks involved in running such a platform is essential.

Therefore the writer of this article has carried out systematic research into the IT risks involved in implementing distributed ledger technology for financial transaction processes. This has resulted in a DLT maturity model which can be used to assess the state of a DLT implementation and how well certain DLT-specific IT risks are under control.

To clarify the concept of IT risk for the reader, the following definition by ISACA [ISACA09] is taken as leading:

"The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise."

DLT IT Risks

The basis of the model has been a thorough literature review of DLT IT risks. A set of 51 papers was selected and analysed for DLT IT risks.

The studies related to IT risks were used in combination with existing literature on financial services to build the IT risk areas. Implementing DLT technologies exposes an organization to several IT risk factors, these risks can be summarized into eight *DLT risk areas*, which are shown in Figure 1.

Some of the risks in the eight areas overlap with more traditional IT implementations, while other risks are completely new, due to the decentralized nature of a DLT system. For example, a new risk is the fact that all nodes need to upgrade their software version at the same time in order to prevent the blockchain from forking. However, this 'new' risk falls under a 'traditional' category of change management.

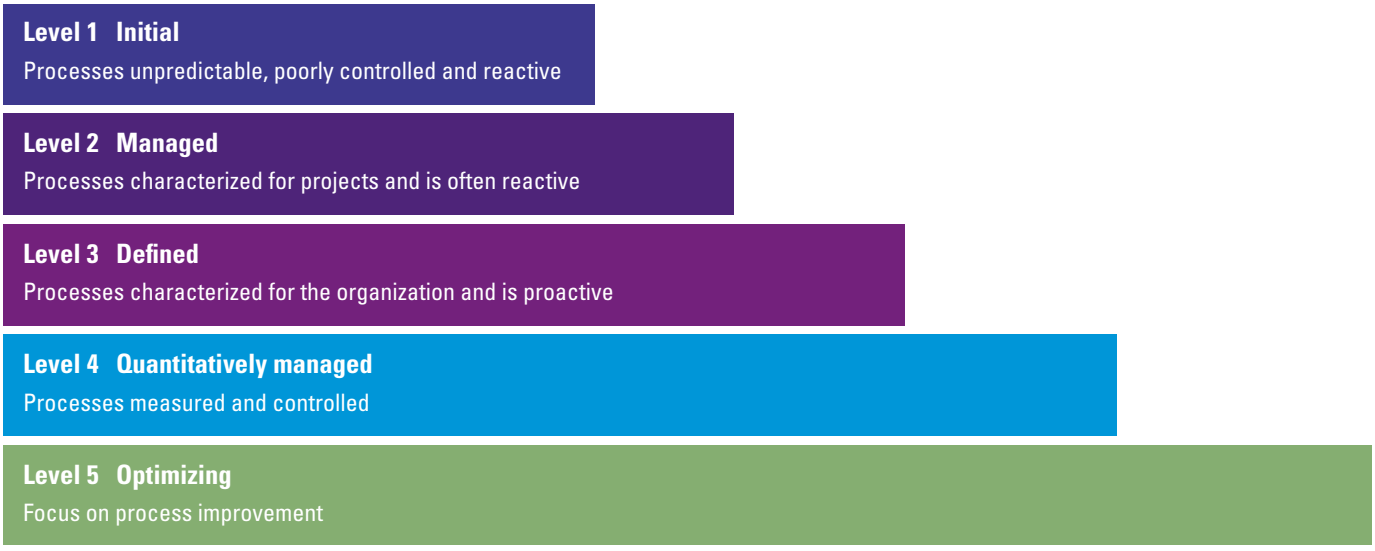
To get an impression of how DLT influences these risk areas, see the box about the impact on access and user management.

IT MATURITY MODELS

Maturity can be described as 'a measure to evaluate the capabilities of an organization with regard to a specific discipline' ([Rose05]). A maturity model helps organizations to grow towards maturity by showing the current standings and providing a roadmap towards increased maturity. In order to mature, a set of benchmark indicators is necessary. In the field of IT maturity, there are several models, mostly focusing on a sub-section of IT maturity, such as service integration, open source or DevOps. However, as noted by Becker et al. [Beck10] IT maturity models have rarely been conceptualized in detail and it is mainly the Capability Maturity Model (CMM) and its successor Capability Maturity Model Integration (CMMI) that have had a large impact in the area of IT maturity. In their analysis of IT maturity models Becker et al. conclude that 15 out of 20 articles refer to CMM(I) as the de facto IT maturity model.

Therefore, the authors have decided to use the CMMI maturity model as a basis for developing the DLT risk maturity model. The CMMI model uses five maturity levels to measure maturity, these five levels are the basis for assessing DLT Risk maturity (see Figure 2 on CMMI maturity levels).

Figure 2. CMMI maturity levels.



Creating a DLT IT maturity model

Figure 3 depicts the steps to arrive at the maturity model. The sub-risks have been identified for each of the eight DLT risk areas detailed in Figure 1. The next step was translating each of these sub-risks into maturity self-assessment questions. In order to keep this article brief we have included a small part of the maturity model in the section below.

Area: access and user management

1. Unauthorized access of participants
Within Permissioned DLTs network the risk of unauthorized access still exist. Because at this moment every participant can grant new members access to the network, it is possible that unauthorized/untrusted parties will gain access.

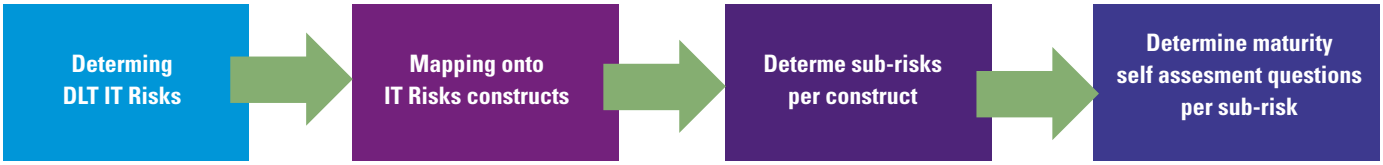
2. Users are not uniquely identifiable
DLT uses unique addresses which are assigned to each participant in the network. This address is used for transactions (sending and receiving) and enables participants to authenticate themselves and these transactions by using a public key.

The provisioning process of these key-pairs (unique identifier) and assigning access rights is different for each DLT implementation. Due to the fact that DLT heavily relies on digital identity this means that adequate management and security around the process of providing and storing the cryptographic keys is of great importance.

Table 2. Risk area: access and user management.

Risk	ID	Maturity self-assessment questionnaire	Maturity level
Unauthorized access of participants	1.1.1	Is there a procedure in place that describes the onboarding/leaver process for user/participants in the network (DLT)?	If yes: maturity level 2
	1.1.2	Is there a supervision/oversight function that manages access for user and participants?	If yes: maturity level 3
	1.1.3	Are there security controls in place that detect unauthorized access attempts?	If yes: maturity level 3
	1.1.4	Procedures are in place for account recovery.	If yes: maturity level 3
	1.1.5	Are there monitoring controls in place to check on a periodic basis if the authorized users/participants still have the correct access rights (SOLL/IST)?	If yes: maturity level 4

Figure 3. Creating a DLT IT maturity model.



The entire DLT landscape is still very much in development

3. Authentication mechanisms are not working
The DLT mechanism relies on unique addresses that are assigned to each member, which are used for sending/receiving and authenticating transactions via a PKI infrastructure. Inadequate authentication mechanisms could result in authentication risks and being unable to correctly authenticate counterparties and existence of assets ([Berk17], [Lage16], [Walc15]).

Based on the three risks found for the ***a****ccess and user management* area, for this study the overall risks measurement scales developed by NIST 800-53 [NIST13], OWASP [OWASP08] and COBIT [Hard08], [ISACA09] were adapted to measure the maturity level. The table below summarizes the maturity self-assessment questions for sub-risk *'Unauthorized access of participants'* of the access and user management area.

CASE STUDY – WHAT DID WE LEARN?

After validation of the model with IT risk managers, DLT experts and developers, the model was tested against a real life DLT use case at the Rabobank.

Rabobank group

Rabobank is a multinational cooperative bank and the second largest financial service provider in the Netherlands, serving over ten 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, the Rabobank is looking at DLT and is taking steps to explore the possibilities of this new technology. This provides a good opportunity to test the DLT maturity model against a high impact blockchain project.

While the specific details of this use case cannot be shared publicly, some overall conclusions of applying the blockchain maturity model can be given.

The entire DLT landscape is still very much in development. An often used DLT platform for example is Hyperledger Fabric. This platform has only been in a stable version 1.0 since July 2017 (one month before conducting this case study). It became apparent that when implementing a DLT platform the focus is on getting this platform up and running as quickly as possible, which leads to certain risk areas getting more attention and with others to be resolved at a later time.

During the interview it was noted that many of the maturity indicators were steps that Rabobank was thinking of implementing, but that were not implemented at that moment in time.

The Rabobank commented that the maturity model provided concrete pointers as to which areas to focus on and how to improve their maturity. The framework clearly shows which areas are lacking in IT risk maturity, thereby helping to focus on improving the areas that need it the most.

IN CONCLUSION

A DLT enables multiple parties in a value chain to work together and share data and processes very efficiently. This reduces administrative work, reduces the risk of fraud by creating an audit trail of transactions and enables the automation of common business processes with the use of smart contracts. However, due to the nature of a DLT system, implementation also introduces new and specific risks that do not exist in current financial transaction processing systems. This is because a DLT system is an interconnected system in which multiple parties cooperate and share data, combined with the fact that all transactions logged on this system are irreversible.

The literature study shows that most IT risks associated with DLT need a different approach than more 'traditional' IT risks. The challenge for financial services firms that want to use DLT is therefore to convert these IT risks into mitigating procedures that eliminate these risks. In addition, it is concluded that the necessary steps must be taken before DLT can replace existing technologies.

By combining an IT risk maturity model with DLT specific risks as found in the current literature, a maturity model can be created to measure DLT IT risk maturity. This enables the user of the framework to assess maturity and give specific and prioritized recommendations tailored to the situation.

The case study shows the value of having a DLT maturity assessment, as it can help not only by giving an impression of the current state, but it also helps to create a well-founded and prioritized action plan to improve maturity levels. The overall conclusion is that DLT is still a very immature technology and more research will have to be performed about keeping control over a DLT system and making sure that all IT risks are properly dealt with.

Visit our website for more information about the KPMG Blockchain Maturity Model: https://home.kpmg.com/nl/en/home/insights/2017/12/blockchain-maturity-model.html.

The necessary steps must be taken before DLT can replace existing technologies

References

[Beck10] J. Becker, B. Niehaves, J. Pöppelbuß, A. Simons, *Maturity Models in IS Research*, ECIS 2010 Proceedings, http://aisel.aisnet.org/ecis2010/42/, 2010.

[Berk17] A. Berke, *How Safe Are Blockchains? It Depends.*, Harvard Business Review, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends, 2017.

[Hard08] G. Hardy, J. Heschl, J. Clinch, *Aligning COBIT, ITIL V3 and ISO/ICE 270002 for Business Benefit. A Management Briefing from ITGI and OGC*, ISACA.org, http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf, 2008.

[ISACA09] ISACA, *The Risk IT Framework*, ISACA.org, http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf, 2009.

[Lage16] P. Lageschulte, M. Krajecki, M. Sokalski, K. Nagaraj, *Missing link - navigating the disruption risks of blockchain*, KPMG, https://advisory.kpmg.us/insights/2016/09/navigating-blockchain.html, 2016.

[NIST13] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, 2016.

[OWASP08] OWASP, *OWASP Testing Guide*, OWASP.org, https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf, 2008.

[Rose05] M. Rosemann, T. Bruin, *Towards a Business Process Management Maturity Model*, ECIS 2005 Proceedings, http://aisel.aisnet.org/ecis2005/37, 2005.

[Spen16] H. Spenkelink, G. Hough, *Blockchain: from hype to realistic expectations*, Compact 2016-4, https://www.compact.nl/articles/blockchain/, 2016.

[Walc15] A. Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, Legislation and Public Policy, nr. 18, p. 837-894, https://www.academia.edu/18602560/The_Bitcoin_Blockchain_as_Financial_Market_Infrastructure_A_Consideration_of_Operational_Risk, 2015.

About the author

Ir. Hardwin Spenkelink is a senior consultant at KPMG Digital Ledger Services. He first got interested in cryptocurrencies and distributed ledgers in 2013 when he started mining his own cryptocurrencies. In 2014 he graduated with a masters' degree at the University of Twente on the topic of the adoption of cryptocurrencies. In the same year he started working at KPMG IT Advisory as a consultant and has kept very active in the distributed ledger space. Last year (2016) he joined the newly formed global KPMG Distributed Ledger Services team as a senior consultant.