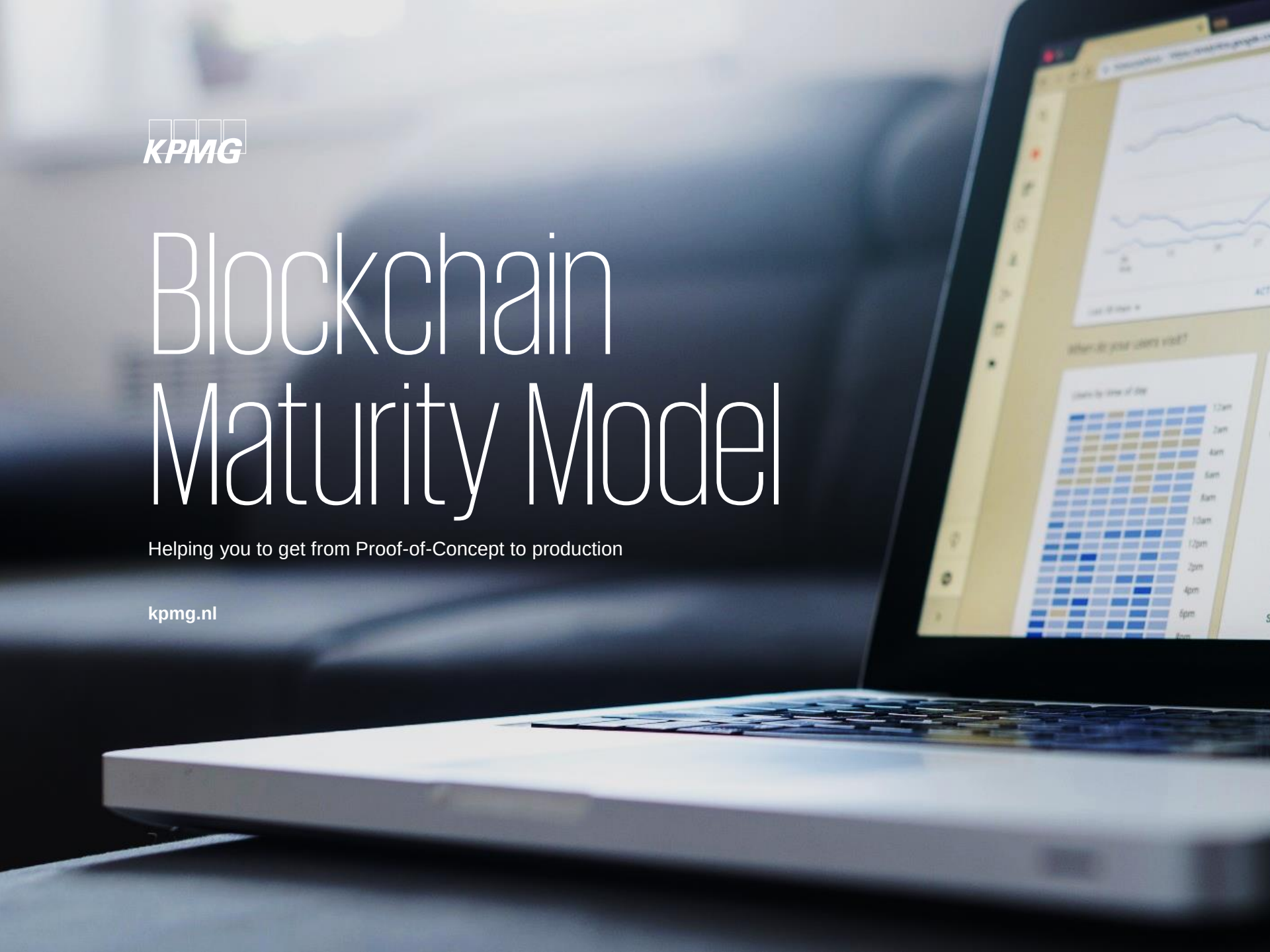


KPMG

Blockchain Maturity Model

Helping you to get from Proof-of-Concept to production

kpmg.nl

What is the blockchain maturity model?

Introduction

— Blockchain or Distributed Ledger Technology (DLT) is seen as a revolutionary new technology that might enable potentially significant cost savings and efficiency gains.

— Blockchain enables multiple parties in a value chain to efficiently work together based on a single source of truth. This facilitates sharing data between multiple parties, transferring value in a digital way and eliminating the need for costly reconciliations.

New risks

— Due to the nature of blockchain, implementing distributed ledger technology also introduces new and specific risks that do not exist in more traditional centralized systems.

— This raises the question whether new blockchain implementations will be sufficiently in control when moving from proof-of-concept phase to production.

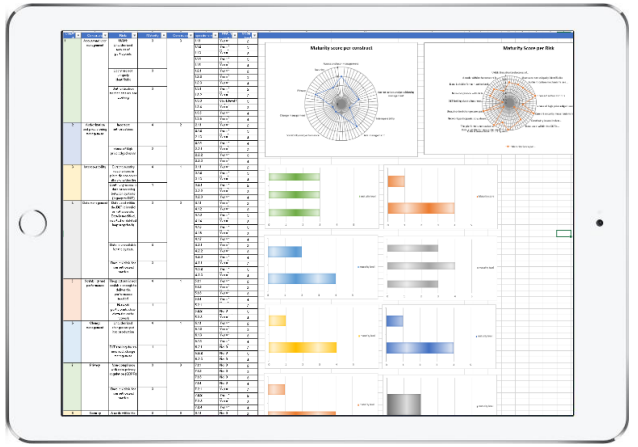
— KPMG has identified eight specific blockchain risk areas including interoperability, security, access management, privacy and scalability.

Quick scan

— KPMG has developed a blockchain maturity model which helps to get a grip on the specific risks associated with blockchain implementations.

— This framework helps you to get an understanding of the IT risk maturity of the blockchain implementation in all eight risk areas.

— The assessment enables you to identify weak points and to spot opportunities for improvement. The overall report provides you with concrete pointers as to how to improve and raise your blockchain maturity level.



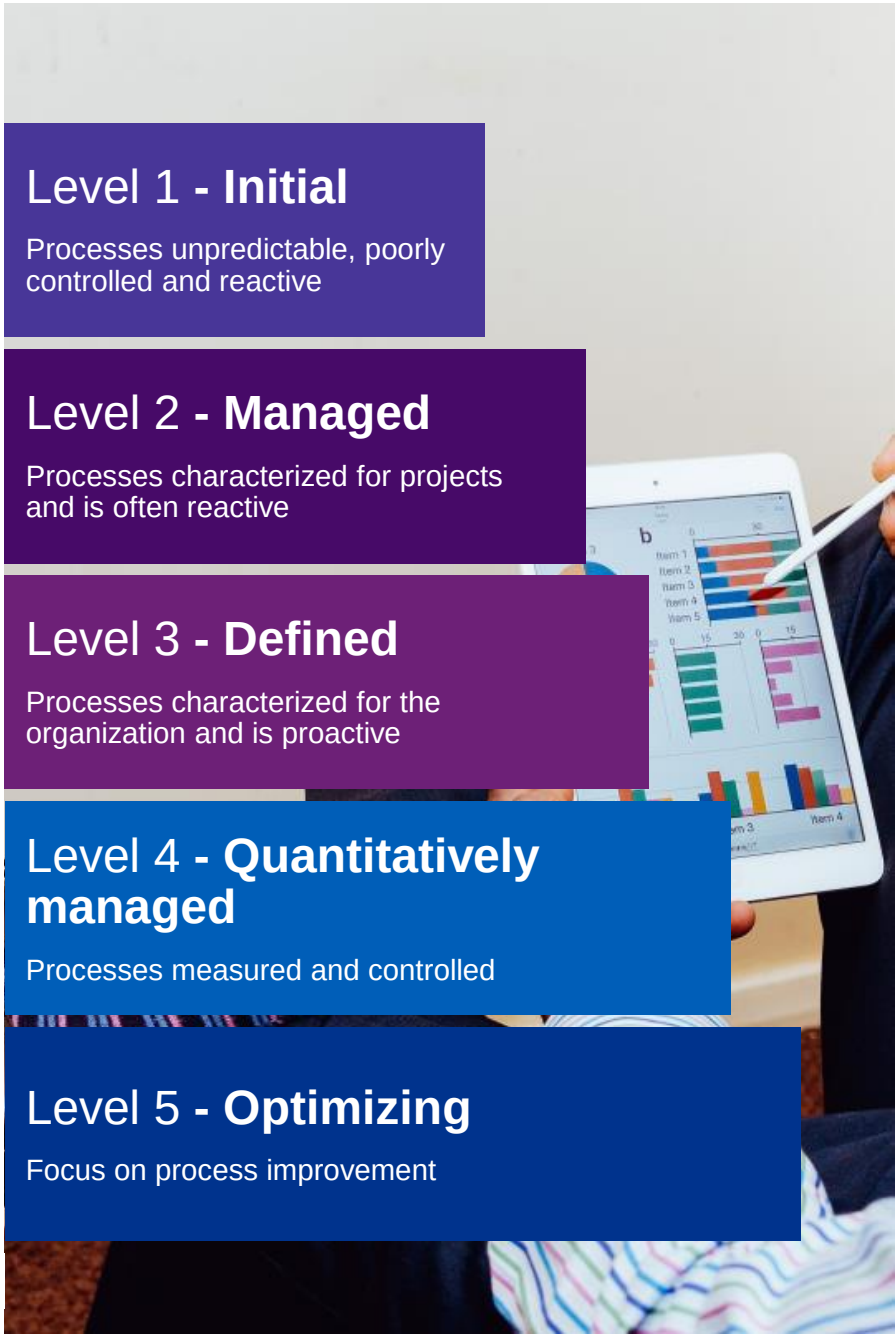
Which levels does the maturity model contain?

Maturity levels

The KPMG Blockchain Maturity model is based upon the Capability Maturity Model (CMMI) for IT maturity. CMMI is a model owned by ISACA, the international professional body for IT governance. The CMMI uses five maturity levels to measure maturity, ranging from 1 (processes unpredictable, poorly controlled; lowest level) to 5 (focus on process improvement; highest level). The scale is further explained in the figure on the right. Based on the CMMI scale you can easily define your ambition level for blockchain maturity.

Scoring

KPMG scores each blockchain risk area against the CMMI maturity model resulting in a maturity score per risk area. This helps you to identify which risk areas are below your desired maturity level. KPMG provides specific recommendations to improve the maturity level and help you get your blockchain Proof-of-Concept to production level from an IT governance perspective.



What are the risk areas of the blockchain maturity model?

1. Access and user management

This risk area focuses on blockchain specific access and user management risks such as:

management of cryptographic keys, unauthorized access of participants and uniquely identifiable users

2. Authorization and provisioning management

This risk area focuses on blockchain specific authorization and provisioning management risks such as:

segregation of duties, incorrect authorizations and abuse of high privileged or over authorized users.

3. Data management

This risk area focuses on blockchain specific data management risks such as:

data confidentiality, integrity and availability.

4. Interoperability

This risk area focuses on blockchain specific interoperability risks such as:

integrating with legacy systems, failure to fully integrate IT legacy and blockchain internal control mechanisms.

5. Scalability and performance

This risk area focuses on blockchain specific access and user management risks such as:

management of cryptographic keys, unauthorized access of participants and uniquely identifiable users

6. Change management

This risk area focuses on blockchain specific change management risks such as:

agreement by all participants, slow adoption and forking.

7. Privacy

This risk area focuses on blockchain specific privacy risks:

append-only data structure, the 'right to be forgotten' and GDPR.

8. Security

This risk area focuses on blockchain specific security risks:

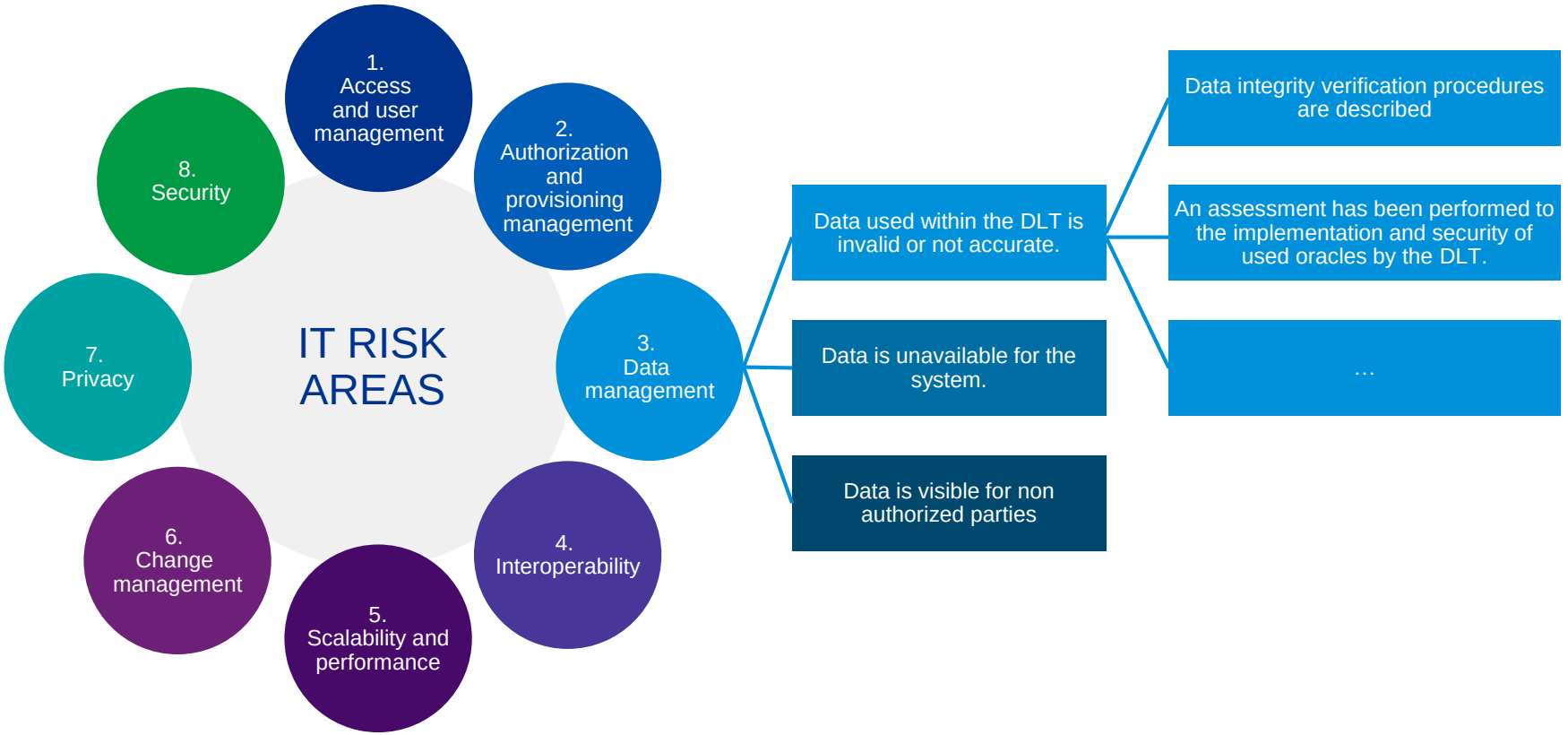
the consensus mechanism chosen, the number and location of nodes.

How does the maturity model scoring work?

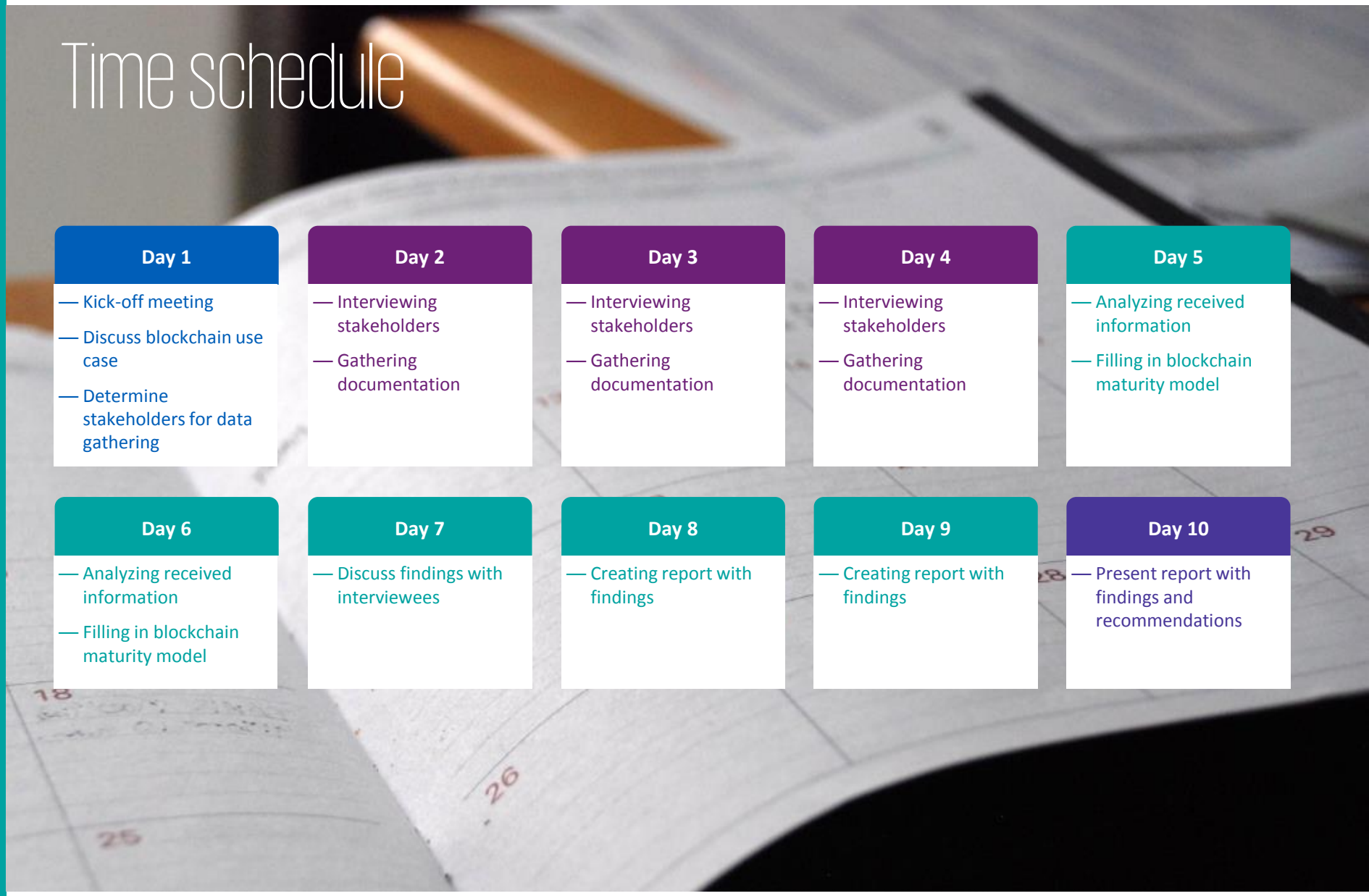
The model contains blockchain specific risks grouped in eight IT risk areas.

Each of these risk areas contains multiple risks.

For each risk a number of controls have been defined to allow KPMG to assess the maturity on the specific risk.



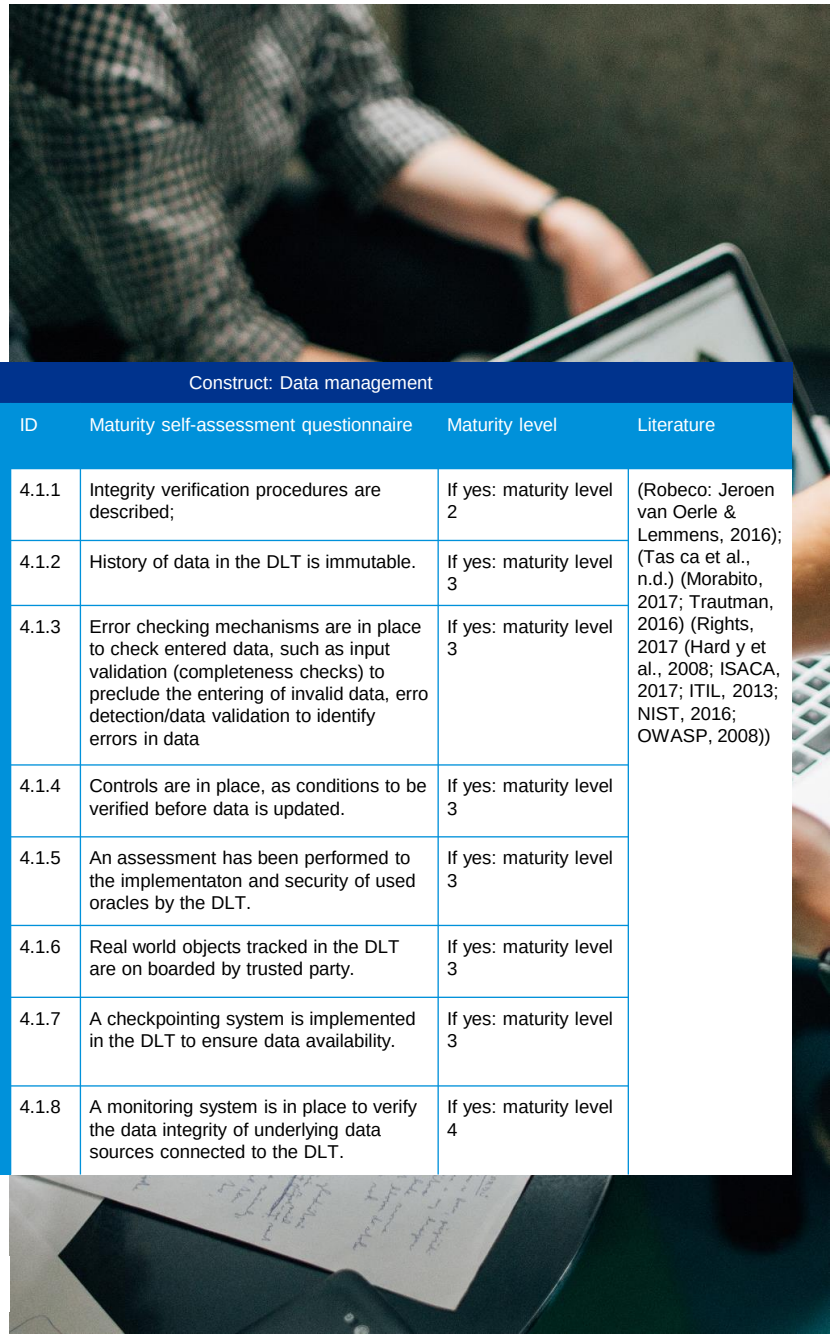
Time schedule



Day 1	Day 2	Day 3	Day 4	Day 5
— Kick-off meeting — Discuss blockchain use case — Determine stakeholders for data gathering	— Interviewing stakeholders — Gathering documentation	— Interviewing stakeholders — Gathering documentation	— Interviewing stakeholders — Gathering documentation	— Analyzing received information — Filling in blockchain maturity model

Day 6	Day 7	Day 8	Day 9	Day 10
— Analyzing received information — Filling in blockchain maturity model	— Discuss findings with interviewees	— Creating report with findings	— Creating report with findings	— Present report with findings and recommendations

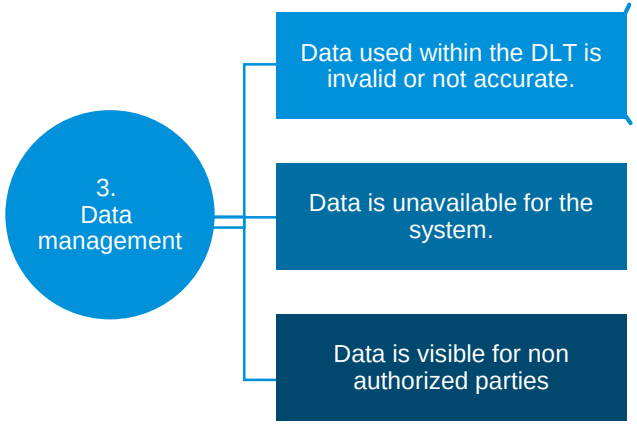
Maturity assessment in detail



Assessment questions

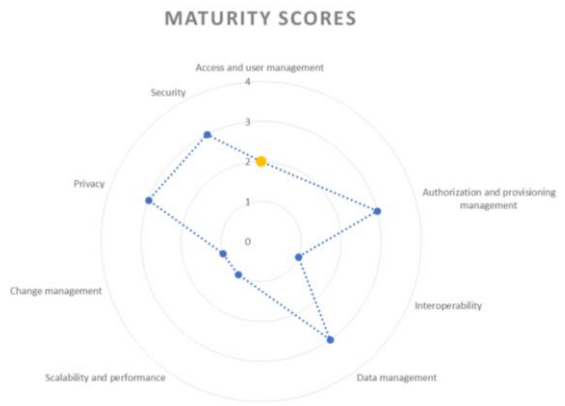
— The full model consists of 8 risk areas, each risk area has several risks and for each risk there is a set of maturity questions

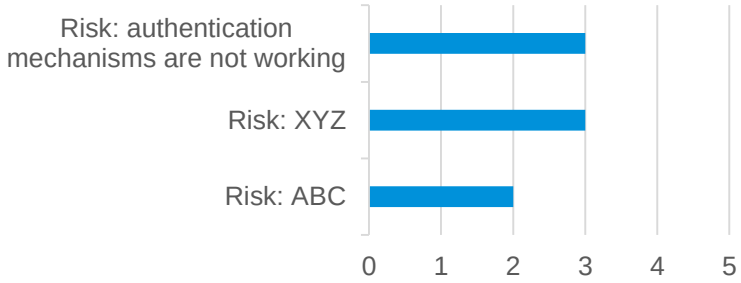
— To give an example we have taken one risk from the ‘Data management’ category and the table on the right shows the associated maturity assessment questions.



Construct: Data management				
Risk	ID	Maturity self-assessment questionnaire	Maturity level	Literature
Date used within the DLT is invalid or not accurate. Data is modified, inserted or deleted inappropriately	4.1.1	Integrity verification procedures are described;	If yes: maturity level 2	(Robeco: Jeroen van Oerle & Lemmens, 2016); (Tas ca et al., n.d.) (Morabito, 2017; Trautman, 2016) (Rights, 2017 (Hard y et al., 2008; ISACA, 2017; ITIL, 2013; NIST, 2016; OWASP, 2008))
	4.1.2	History of data in the DLT is immutable.	If yes: maturity level 3	
	4.1.3	Error checking mechanisms are in place to check entered data, such as input validation (completeness checks) to preclude the entering of invalid data, erro detection/data validation to identify errors in data	If yes: maturity level 3	
	4.1.4	Controls are in place, as conditions to be verified before data is updated.	If yes: maturity level 3	
	4.1.5	An assessment has been performed to the implementaton and security of used oracles by the DLT.	If yes: maturity level 3	
	4.1.6	Real world objects tracked in the DLT are on boarded by trusted party.	If yes: maturity level 3	
	4.1.7	A checkpointing system is implemented in the DLT to ensure data availability.	If yes: maturity level 3	
	4.1.8	A monitoring system is in place to verify the data integrity of underlying data sources connected to the DLT.	If yes: maturity level 4	

Access and user management





Score:
2 - Managed

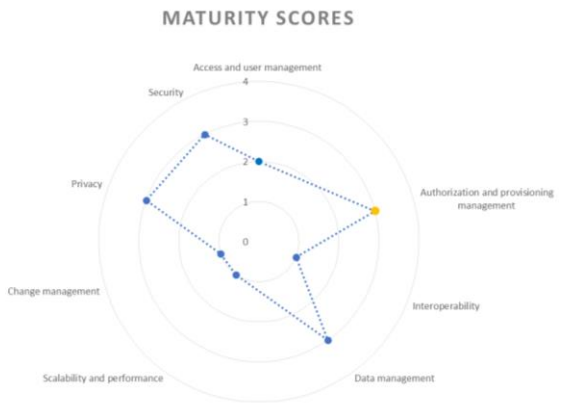
- Level 1 - Initial
- Level 2 - Managed
- Level 3 - Defined
- Level 4 - Quantitatively managed
- Level 5 - Optimizing

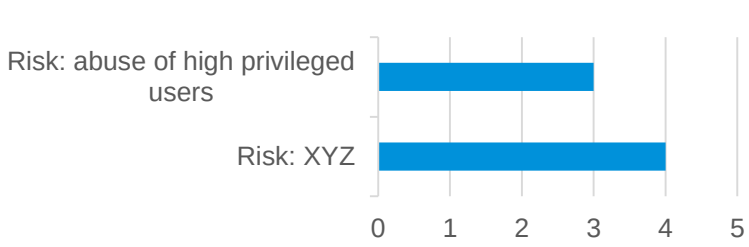
Risk: authentication mechanisms are not working, maturity level 3
Procedures regarding certificate generation, distribution, storage, use and destruction exist on a technical level. Business procedures are yet to be written. The platform uses standard login methods, however in the first phase the system will use dedicated login system. Due to regulation that differs per country the authentication mechanisms used to interface with the DLT can be different for each participant. Digital certificates can be stored both on a hardware device and in software, however periodic checks to confirm the correct working of certificate storage are not performed. Periodic re-issuing/revocation of certificates is not implemented.

Risk: XYZ, maturity level 3
Analysis here

Risk: ABC, maturity level 2
Analysis here

Authorization and provisioning management





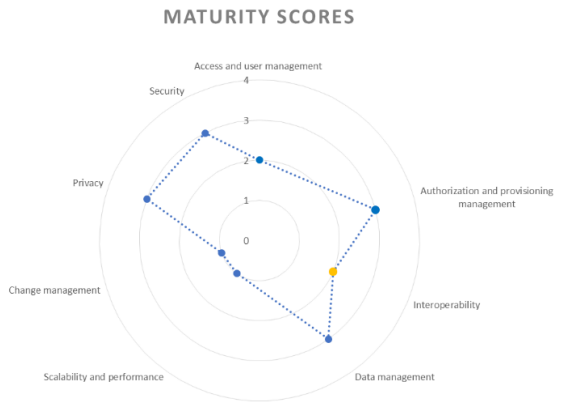
Score:
3 - Defined

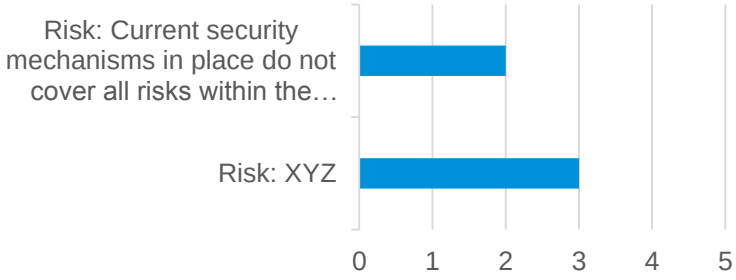
- Level 1 - Initial
- Level 2 - Managed
- Level 3 - Defined
- Level 4 - Quantitatively managed
- Level 5 - Optimizing

Risk: abuse of high privileged users, maturity level 3
Procedures are in place that ensure that super user access and authorization is restricted to an appropriate (limited) group of individuals. System enforced dual controls on super user actions are not in place. However periodic reviews of the actions of high privileged users are taking place.

Risk: XYZ, maturity level 4
Analysis here

Interoperability





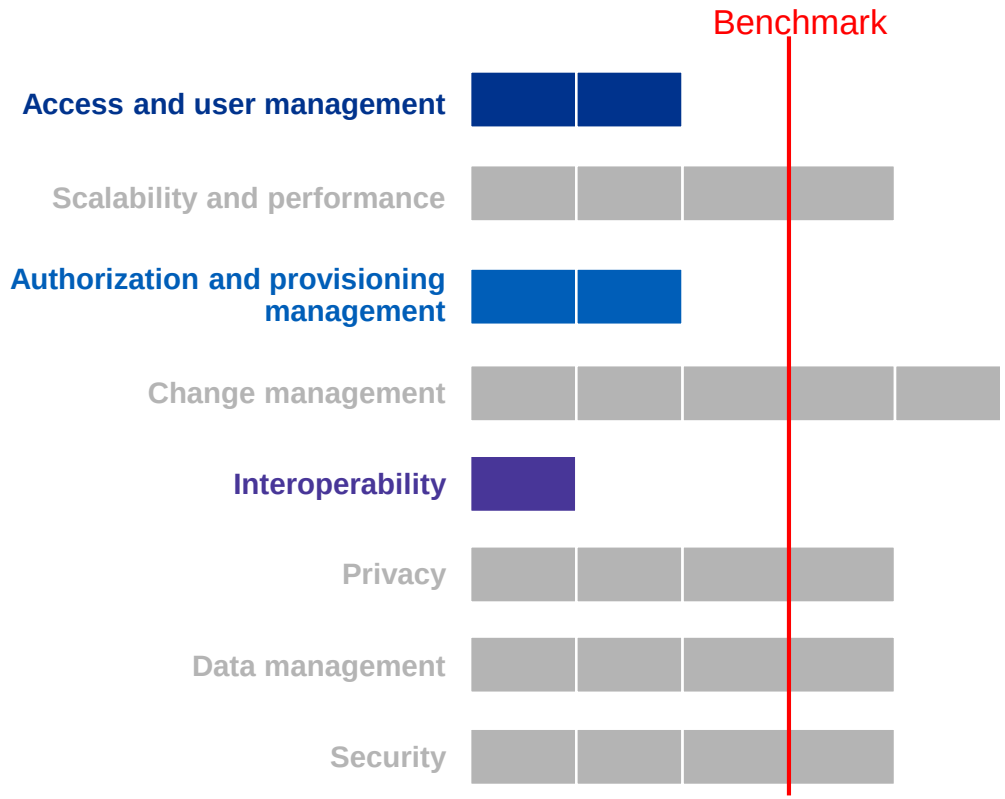
Score:
2 - Managed

- Level 1 - Initial
- Level 2 - Managed
- Level 3 - Defined
- Level 4 - Quantitatively managed
- Level 5 - Optimizing

Risk: security mechanisms do not cover all risks, maturity level 2
There is a process in place in which the orgnization documents interface characteristics, security requirements and nature of information communicated between legacy systems and blockchain. However, there are no monitoring controls in place to check the correct working of interfaces between blockchain and legacy systems. Also no periodic reviews of interface standards have been scheduled.

Risk: XYZ, maturity level 3
Analysis here

Blockchain maturity model assessment recommendations



Recommendation Access and user Management
While the preventative controls are implemented, we do see room for improvement on implementing more detective controls such as periodic checks on access rights and associated digital identities. Another suggestion would be to perform monitoring to be able to spot when malicious actors are trying to obtain access to the system.

Recommendation Authorization and provisioning management
While authorizations for regular users are thoroughly managed, the access of high privileged users is inadequately supervised and dual control is lacking. Implementing dual control on super user actions is recommended.

Recommendation Interoperability
It is recommended to implement monitoring on all connections from the blockchain implementation to legacy systems. Additionally it is recommended to perform periodic reviews of interface standards.

The benefits of the maturity model

CLEAR INSIGHT INTO BLOCKCHAIN RISKS

This framework helps you to get an understanding of the IT risk maturity of the DLT implementation from eight risk areas.

FROM PROOF-OF-CONCEPT TO PRODUCTION

Going from proof-of-concept to a production ready system requires a good view on IT risks. The maturity model identifies weaknesses in your existing blockchain solution.

CONCRETE ACTION PLAN

The assessment gives concrete pointers to risk areas for improvement and concrete recommendations how to improve and raise to the next blockchain maturity level.

UNIQUE AND VALIDATED MODEL

This assessment with its specific blockchain focus is unique in the current market and is based upon solid research, IT risk standards and years of experience and was validated with clients.

Credentials

Digital Trade Chain - Rabobank

— KPMG has performed a blockchain maturity assessment on the We.Trade (formerly known as Digital Trade Chain) proof-of-concept which the Rabobank is running together Deutsche Bank, HSBC, KBC, Natixis, Société Générale, Unicredit and Banco Santander.

— We.trade is a blockchain-based digital platform for managing and tracking domestic and cross-border Open Account trade transactions securely.

— The aim of the platform is to make domestic and cross-border commerce easier for European small and medium-size (SME) businesses by harnessing the power of blockchain.

— With a schedule to go live at Q2 2018, it will be one of the very first blockchain applications running in a production setting.

Chris Huls
Teamlead Blockchain
at Rabobank

"The blockchain maturity model enabled us to get a clear grip on our IT risks when implementing a new blockchain solution"

Contact details

Hardwin Spenkelink

Senior consultant

KPMG Digital Ledger Services

Mob: +31 (0) 6 10 125 756
Spenkelink.Hardwin@kpmg.nl

Dennis de Vries

Lead KPMG Digital Ledger Services Netherlands

Mob: + 31 (0) 6 43 817 117
deVries.Dennis@kpmg.nl

Martijn Berghuijs

Director KPMG Innovation Advisory

Mob: +31 (0)6 51 366 540
Berghuijs.martijn@kpmg.nl