Blockchain Maturity Model

Vurore
Amsterdam, 20 maart 2018
Introduction of Hardwin

2013 – Became interested in Bitcoin, started mining Bitcoin

Feb 2014 – Graduate student at KPMG
Topic: the adoption process of cryptocurrencies

Sept 2014 – Junior Consultant at KPMG ITA
Financial Services

Jan 2017 – Senior Consultant at KPMG Digital Ledger Services

Sept 2017 – Thesis: Innovation and IT maturity for Distributed Ledger Technology in the financial sector

Hardwin Spenkelink
Senior consultant
KPMG Digital Ledger Services
Agenda

1. Blockchain recap

2. Blockchain maturity model
01

Blockchain recap
Blockchain was introduced through Bitcoin, which proved **value transfer** over the internet **without a trusted third party** is technically possible.

The essence of blockchain is **sharing a ledger amongst multiple parties** in a value chain, thus creating a platform providing a single source of truth and eliminating the need for (costly) reconciliation.

As blockchain is all about creating a **single source of truth** for a value chain, in principle a blockchain solution for a single client does not make sense. Consequently value chains are organizing in consortia to create value chain platforms.

In blockchain trust is not provided through a trusted third party, but provided at transaction level through a smart combination of **PKI, hashing, Merkle trees, cryptography and open source code**.

As multiple parties maintain a copy of the shared ledger, the **consensus mechanism to decide on valid transactions** is fundamental. As Bitcoin’s Proof of Work is expensive and energy consuming, various alternatives have been developed.

Where there is only 1 internet protocol (TCP/IP), various 15 – 20 **blockchain protocols are currently competing**. Most protocols are open sourced under the Linux foundation.

Bitcoin uses a permissionless public ledger completely transparent to all parties (blockchain). Most experiments use a private permissioned shared ledger to which a limited number of parties have access. **Distributed Ledger Technology** is the term that captures both.

Blockchain might be a perfect solution for digital assets, however very few truly digital assets currently exist. The weak spot in any blockchain solution will be the **link between any asset in the real world** (e.g. house, car, share) and the blockchain.

Smart contracts is a piece of code stored on the blockchain using inputs / events to **automatically transfer value**. While still in its infancy smart contracts might have potential to **automate processes currently performed by trusted third parties**.

Key hurdles for transformation to a blockchain based world seem solving **digital identity** and **digital currency**. Incumbents (in particular current trusted third parties) are likely to resist implementation due to shifting roles and business models.
Digital Ledger Technology - A potential game-changer?

Traditional Ledger
Present
— Ledgers record business activities such as transactions and contracts, today each party owns individual ledgers
— This solution is well established and working, but inefficient, expensive and fraud vulnerable

Digital, Distributed Ledger
Future
— Decentralized system building one digital, encrypted, public ledger, distributed across the network
— No possibility of changing information in the ledger without consensus of the whole network

Benefits of Digital, Distributed Ledgers
— Trust between all engaged business partners
— Increase Efficiency through usage of a distributed ledger
— Quality and Integrity of stored data
Functional process of digital ledgers

<table>
<thead>
<tr>
<th>Initiate the transaction</th>
<th>Add the transaction to the network</th>
<th>Broadcast</th>
<th>Validate via consensus and confirm</th>
<th>Immutable, encrypted block</th>
<th>Transaction completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple parties transact</td>
<td>The transaction is added to the network’s block and cannot be deleted</td>
<td>The block is broadcasted to every party in the network</td>
<td>The network verifies, validates, and approves</td>
<td>The confirmed block is added to the chain</td>
<td>Parties have access to a shared, single source of truth</td>
</tr>
</tbody>
</table>

Consensus mechanism applied

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
The complexity of the current blockchain ecosystem

The following illustration demonstrates participants involved in the market space.

- **Applications and use-cases**
  - Document Digitization
  - Trade Finance
  - Cross-border Payments
  - Digital Identities/KYC
  - OTC Derivatives
  - Smart Contracts
  - Corporate Actions
  - Asset Tokenization
  - Fixed Income Trading
  - Record Keeping
  - Clearing and Trade Settlement

- **Consensus mechanisms**
  - Leader based
  - Proprietary distributed ledger consensus
  - Federated consensus
  - Node-to-node (N2N)
  - Proof of work
  - Proof of stake
  - Delegated Proof of stake
  - Round Robin
  - PBFT and derivatives
  - Swirlds hashgraph

- **Platform Technologies/providers**
  - Digital Asset
  - Tendermint
  - NASDAQ (Linq)
  - SETL
  - Ripple
  - Intel (Sawtooth)
  - BlockEx
  - Symbiont
  - Corda (R3 CEV)
  - DPactum
  - Multichain
  - Hyperledger
  - Ethereum
  - Stellar
  - PBFT
  - Bitcoin
  - Consensys
  - Paxos
  - Coinprism
  - Symbiont
  - Blockchain

- **Infrastructure technologies/providers**
  - Public/private cloud – AWS, Azure, Nimbrix etc.
  - In-house systems/data centers
  - Non-DLT/Traditional Infrastructure
  - DLT-specific Infrastructure

- **Successful market examples, tests and implementations**

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks of KPMG International.
MANY Distributed Consensus Mechanisms now Competing

Illustrative and not exhaustive

New Consensus mechanisms appearing regularly (e.g. NEM and Proof of Importance)
Hashing explained

- The foundation of Blockchain is **Hashing** and **Encryption**
- Hashing is a long-established and well-proven computing technique
- Hashing is a **one-way process**, creating fixed length hexadecimal data from source information
- The original information cannot be discerned or re-created from the hash data

---

**Input**

- Fox
- The red fox jumps over the blue dog
- The red fox jumps over the blue dog

**SHA256 Hashing Algorithm**

**Output**

- DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2d17
- 34DE 6621 FDE5 F98A 422A DA03 115F BCB8 FF51 6761
- FF31 7881 AA03 67FD 4266 98FA EEFA CC27 BA06 9256
- 276F 806F 5004 DEA2 6412 90DA BB41 690F 0AAC 98FF

---

**Input**

- Effectively Impossible

**Output**
Public/Private key explained 1/2

Meet Bob and Alice

• Bob and Alice use a BTC Wallet service (probably by downloading an App to their Smartphone)

• As they download the BTC Wallet, they are assigned a Private and Public Key by the Wallet, which are stored in the wallet software on their behalf

Bob

52ED879E 70F71D92
Big random number
Bob’s Public Key
Bob’s Private Key

Key generation function

Alice

DF66CC81 2186FEFD
Big random number
Alice’s Public Key
Alice’s Private Key

Key generation function
Bob and Alice can now use their Private and Public keys to exchange information secretly, even over the public Internet using digital signatures and encryption.

Encryption with Keys is different to hashing, since the encrypted data can be converted back to the original information (Decrypted) through the use of the Keys.
Blockchain protocols characteristics

<table>
<thead>
<tr>
<th>Permissioned Private Ledgers</th>
<th>Permissioned Public Ledgers</th>
<th>Permissionless Public Ledgers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consensus by PBFT or other mechanism</td>
<td>• Consensus by Proof of Work, Proof of Stake, Voting Pools or other mechanism</td>
<td>• Consensus by Proof of Work</td>
</tr>
<tr>
<td>• Decentralised, only permissioned entities may read and write the ledger</td>
<td>• Decentralised, only permissioned entities may write the ledger, but anyone may view the ledgers contents</td>
<td>• Distributed, anyone can read and write the ledger, as long they meet certain criteria and follow certain rules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traditional Centralized Database Ledgers</th>
<th>Oracle Database</th>
<th>SQL Server</th>
<th>red hat</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consensus by automated or manual reconciliation using intermediaries</td>
<td>Hyperledger</td>
<td>MultiChain</td>
<td>Ripple</td>
</tr>
</tbody>
</table>

High Throughput

Centralised

Decentralised

Distributed
The Hyperledger project

HYPERLEDGER MODULAR UMBRELLA APPROACH

**Infrastructure**
Technical, Legal, Marketing, Organizational
Ecosystems that accelerate open development and commercial adoption

**Frameworks**
Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities

**Tools**
Typically built for one framework, and through common license and community of communities approach, ported to other frameworks
Hyperledger Fabric v1 Transaction flow

1. \(<\text{PROPOSE}, \text{clientID}, \text{chaincodeID}, \text{txPayload}, \text{timestamp}, \text{clientSig}>\)
2. \(<\text{TX-ENDORSED}, \text{peerID}, \text{txID}, \text{chaincodeID, readset, writeset}>\)
3. \(\text{BROADCAST(blob)}\)
4. \(\text{DELIVER(seqno, prevhash, block)}\)

Ordering service (consensus)

- Collect “sufficient” no. of TX-ENDORSED Msgs into an endorsement (to satisfy endorsement Policy (EP))
- Simulate/Execute tx
- Sign TX-ENDORSED
- Validate(readset)
- Validate(endorsement, chaincodeID, EP)

(client (C))

(orderers)

(ending peer (EP1))
(ending peer (EP2))
(ending peer (EP3))

(committing peer (CP4))
(committing peer (CP5))
Blockchain maturity model
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.

Level 1 - Initial
Processes unpredictable, poorly controlled and reactive

Level 2 - Managed
Processes characterized for projects and is often reactive

Level 3 - Defined
Processes characterized for the organization and is proactive

Level 4 - Quantitatively managed
Processes measured and controlled

Level 5 - Optimizing
Focus on process improvement
What are the risk areas of the blockchain maturity model?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Management of cryptographic keys</td>
<td>• Segregation of duties</td>
<td>• Data confidentiality</td>
<td>• Integrating with legacy systems</td>
</tr>
<tr>
<td>• Unauthorized access of participants</td>
<td>• Incorrect authorizations</td>
<td>• Data integrity</td>
<td>• Monitoring of interconnections</td>
</tr>
<tr>
<td>• Uniquely identifiable users.</td>
<td>• Abuse of high privileged or over authorized users</td>
<td>• Data availability</td>
<td>• Integrating legacy IT and blockchain internal control mechanisms</td>
</tr>
<tr>
<td>• ...</td>
<td>• ...</td>
<td>• ...</td>
<td>• ...</td>
</tr>
</tbody>
</table>

5. Scalability and performance

• Scalability
• System failure or downtime
• Adding extra nodes
• ...

6. Change management

• Agreement by all participants
• Slow adoption
• Forking
• ...

7. Privacy

• Append-only data structure
• The ‘right to be forgotten’
• GDPR regulation
• ...

8. Security

• The consensus mechanism
• The number of nodes
• Location of nodes
• ...

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
Risk area example

Hyperledger Fabric v1.0

1. Access and user management
- Management of cryptographic keys
- Unauthorized access of participants
- Uniquely identifiable users
- ...

© 2018 IBM Corporation

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
Risk area example

Hyperledger Fabric – Architected for Performance & Scalability

1. **Client Apps** submit transactions to endorsers

2. **Endorsers** will each execute the proposed transaction. None of these executions will update the ledger

3. **Ordering service** accepts endorsed transactions and orders them according to the plug-in consensus algorithm, then delivers them on the channel to connected peers.

4. **Committing Peers** on the channel receive transactions, validate them and then commit to ledger.

© 2018 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
How does the maturity model scoring work?

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

1. Access and user management
2. Authorization and provisioning management
3. Data management
4. Interoperability
5. Scalability and performance
6. Change management
7. Privacy
8. Security

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.

- Data integrity verification procedures are described
- An assessment has been performed to the implementation and security of used oracles by the DLT.
- Data used within the DLT is invalid or not accurate.
- Data is unavailable for the system.
- Data is visible for non authorized parties
- ...
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.

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Maturity self-assessment questionnaire</th>
<th>Maturity level</th>
<th>Literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1</td>
<td>Integrity verification procedures are described;</td>
<td>If yes: maturity level 2</td>
<td>(Robeco: Jeroen van Oerle &amp; Lemmens, 2016); (Tasca et al., n.d.) (Morabito, 2017; Trautman, 2016) (Rights, 2017 (Hardy et al., 2008; ISACA, 2017; ITIL, 2013; NIST, 2016; OWASP, 2008))</td>
</tr>
<tr>
<td>4.1.2</td>
<td>History of data in the DLT is immutable.</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.3</td>
<td>Error checking mechanisms are in place to check entered data, such as input validation (completeness checks) to preclude the entering of invalid data, error detection/data validation to identify errors in data</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.4</td>
<td>Controls are in place, as conditions to be verified before data is updated.</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.5</td>
<td>An assessment has been performed to the implementation and security of used oracles by the DLT.</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.6</td>
<td>Real world objects tracked in the DLT are onboarded by trusted party.</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.7</td>
<td>A checkpointing system is implemented in the DLT to ensure data availability.</td>
<td>If yes: maturity level 3</td>
<td></td>
</tr>
<tr>
<td>4.1.8</td>
<td>A monitoring system is in place to verify the data integrity of underlying data sources connected to the DLT.</td>
<td>If yes: maturity level 4</td>
<td></td>
</tr>
</tbody>
</table>
Maturity scores

Overall score

- After the assessment has been completed, all the scores for each risk area are visualized in a spider graph.

- Each risk area has obtained an overall score, ranging from level 1 to level 5, depicted in the graph on the right. The scores are elaborated in the details slides.
Blockchain maturity model assessment findings

**Access and user management**

<table>
<thead>
<tr>
<th>MATURITY LEVELS</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

**Detailed score overview**

- This risk area has obtained an overall score of level two as depicted on the right.

- The overall risk area score is always the lowest scoring sub-risk. In this case the lowest sub-risk score was a two, leading to an overall risk area level two score.

**Risk: authentication mechanisms are not working**

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**

Analysis here

**Risk: ABC**

Analysis here

**Risk: XYZ**

Analysis here
Blockchain maturity model assessment findings

Authorization and provisioning management

Risk: abuse of high privileged users
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
Analysis here
Blockchain maturity model assessment findings

Interoperability

<table>
<thead>
<tr>
<th>MATURITY LEVELS</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Risk: current security mechanisms do not cover all risks within the new (DLT/DLT) environment
There is no process in place in which the organization documents interface characteristics, security requirements and nature of information communicated between legacy systems and blockchain. Additionally, no monitoring controls are 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
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.
Blockchain maturity assessment

— Rabobank is a multinational cooperative bank and the second largest financial service provider in the Netherlands, serving over 10 million customers worldwide.

— Rabobank is very active in developing blockchain use cases. They have run many projects on various topics such as: KYC, payments, trade finance and the food value chain. These projects vary from proof-of-concept stage to production-ready systems.

— KPMG assisted Rabobank in their blockchain journey by applying the blockchain maturity model to one of their blockchain projects.

“The blockchain maturity model enabled us to get a clear grip on our IT risks when investigating a new blockchain solution”

Chris Huls
Teamlead Blockchain at Rabobank
Credentials

We are the world’s largest humanitarian agency Fighting Hunger Worldwide.

wfp.org
Thank you

Hardwin Spenkelink
Senior consultant
KPMG Digital Ledger Services

Spenkelink.Hardwin@kpmg.nl
+31 (0) 6 101 257 56