

Blockchain / DLT:

- ERP integration
- Control frameworks
- Use cases

ISACA NL Square Table
(in association with NOREA)

7 April 2021

Koen Revet, Siddharth Durbha & Ronald Koorn

Introduction

Koen Revet



Manager

KPMG Enterprise Solutions

Market lead ERP & Blockchain

Siddharth Durbha



Associate Director Risk Consulting

KPMG India

Project Lead TC307 committee for developing
ISO standards for Block Chain/DLT Security,
Governance & Interoperability

Ronald Koorn



Partner

KPMG IT Assurance & Advisory

Member of ISACA GDPR & Privacy &
NOREA Keteninformatiemgt.

Agenda

- Introduction
- **Crash course Blockchain/DLT concepts (optional)**
- Blockchain (Control) Frameworks
- ISO standard
- ERP Integration demo
- Case studies
- Q&A

How it all started back in 2008

Bitcoin: A Peer-to-Peer Electronic Cash System



Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

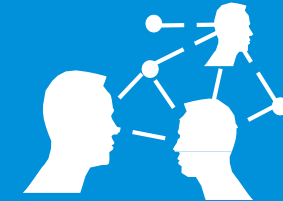
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

CRYPTOGRAPHY



Value transfer via
the internet

PEER TO PEER NETWORK



without a trusted
third party

CONSENSUS MECHANISM



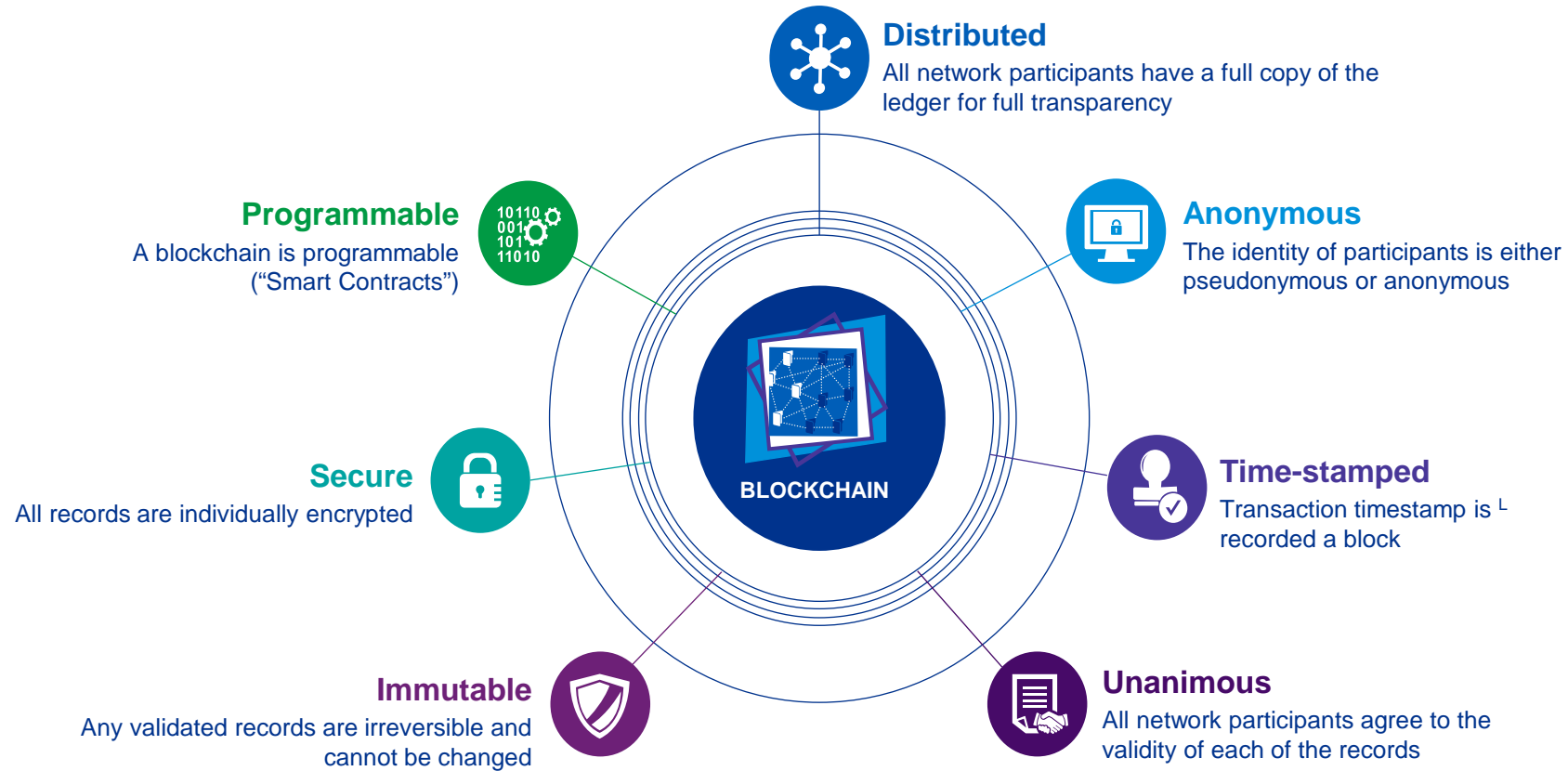
validated by nodes
within a network

DECENTRALIZED LEDGER



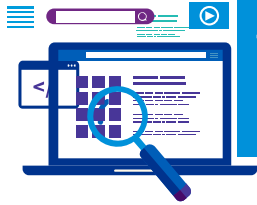
completely
transparently

Properties of Digital Ledger Technology (DLT)



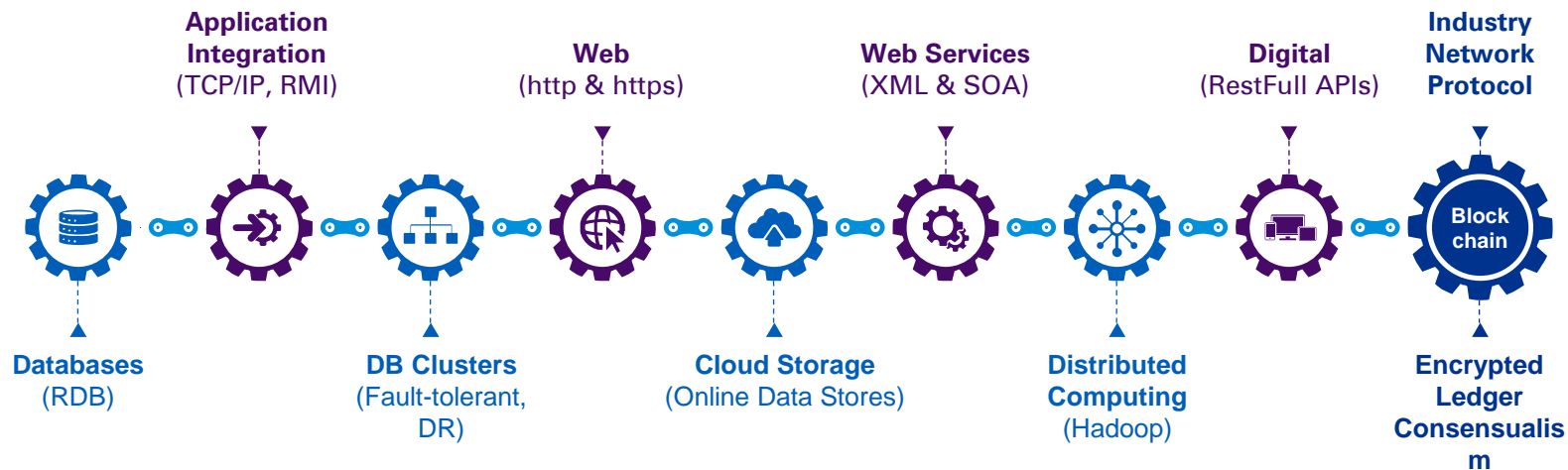
Source: KPMG Research

Is it (solely) an architecture?



The concept of a **Distributed Ledger (DLT)** was synthesized in 1990. Blockchain was introduced as a distributed ledger platform for the Bitcoin application as the ultimate incarnation of a decentralized ledger by anonymous consensus.

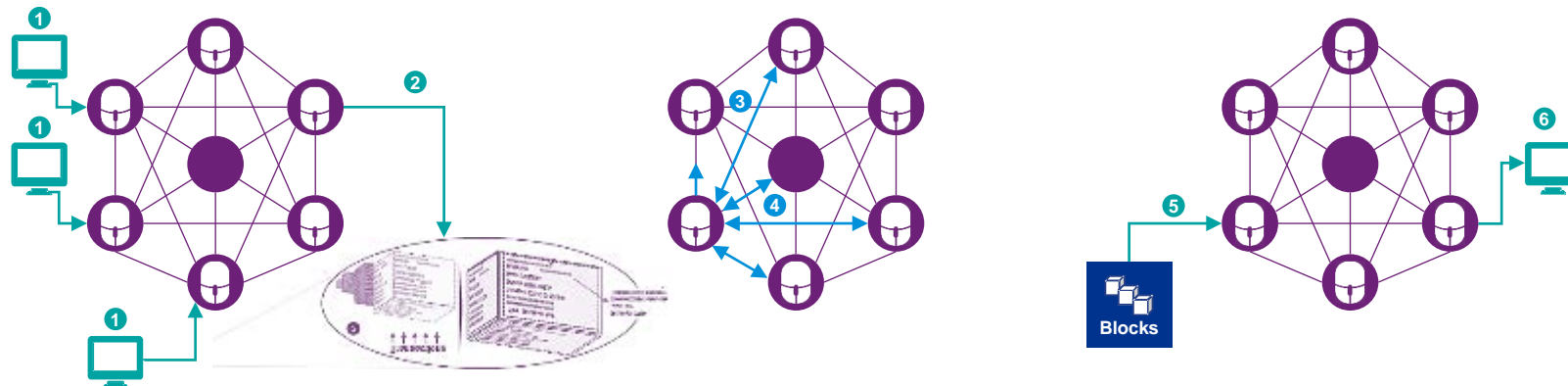
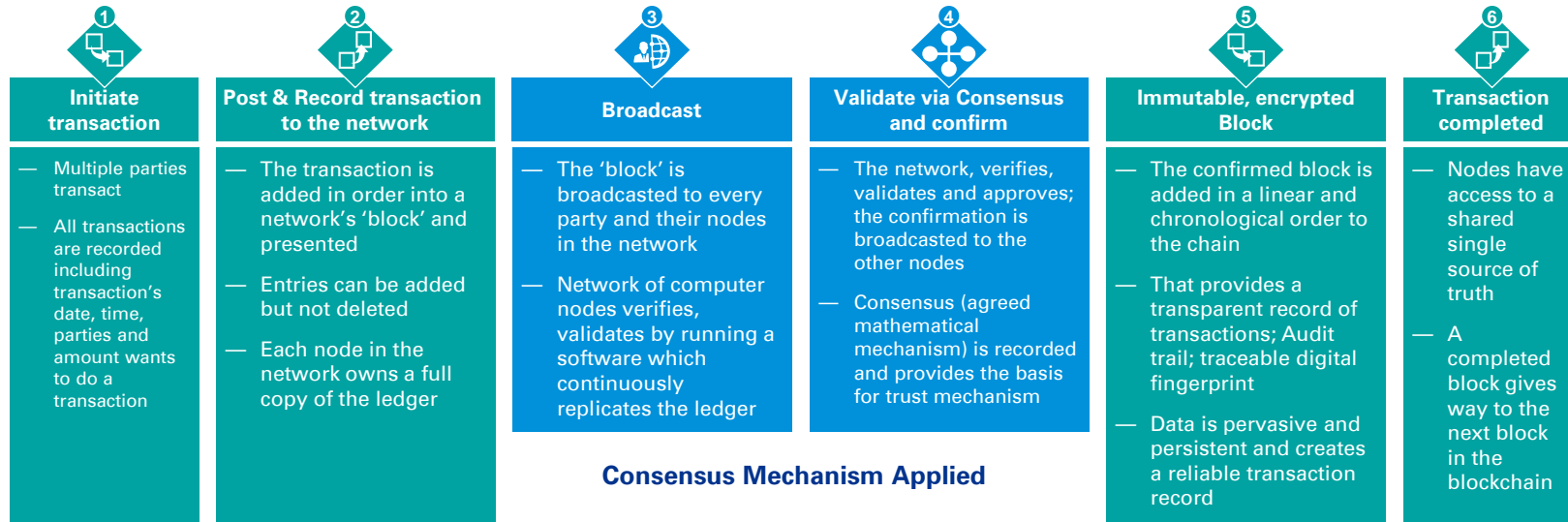
The spectrum of available distributed ledger technology aims to solve the problems of data redundancy and costly reconciliation processes with unique organizational models and consensus procedures.



Source: KPMG Research

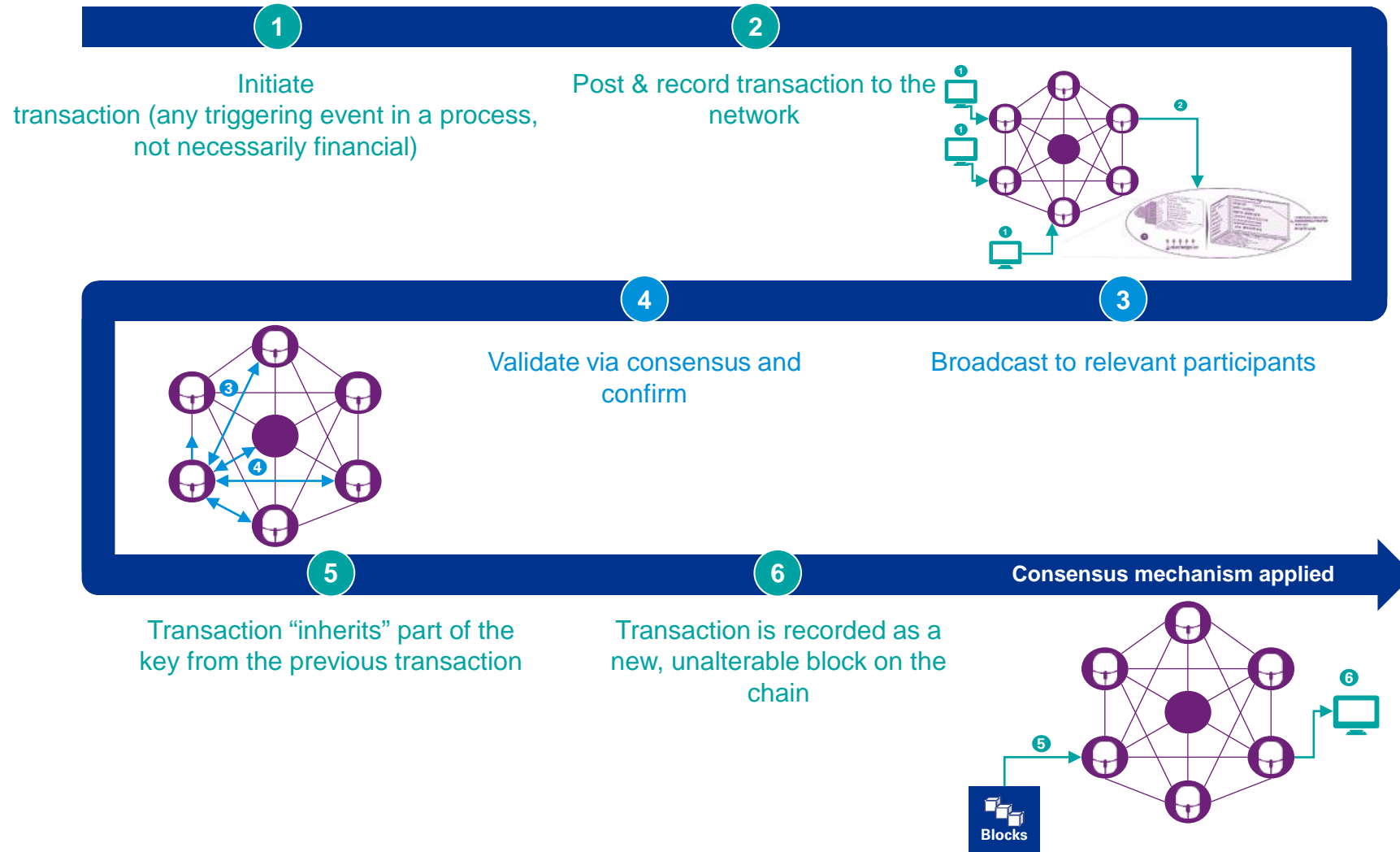
Digital Ledger Technologies (DLTs)

DLTS ARE A WAY OF ORDERING AND VERIFYING TRANSACTIONS IN A DISTRIBUTED LEDGER



Source: KPMG Research

How does it work?



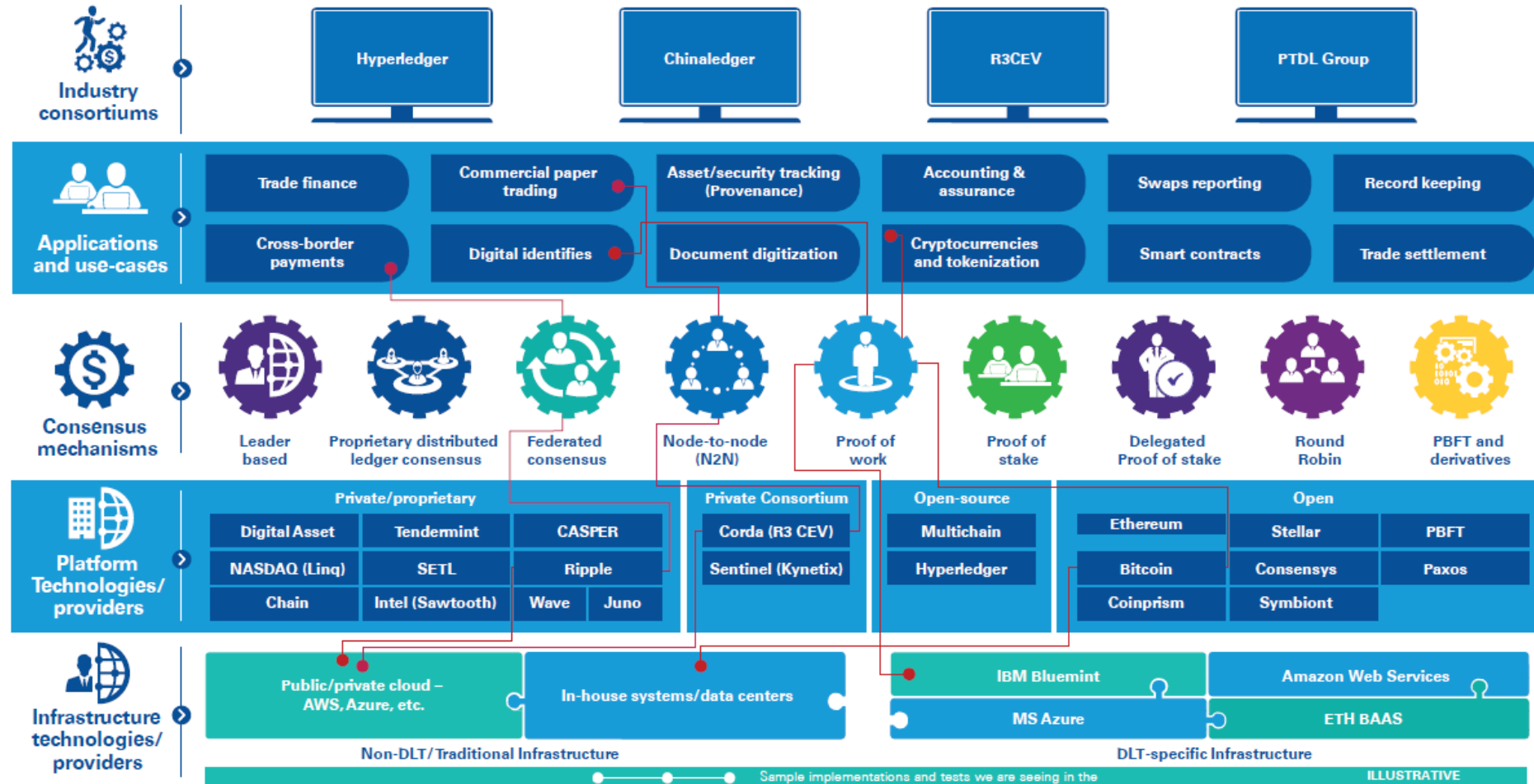
Permissioned vs. permissionless

Blockchain-
architecture options

Architecture based on read, write, or commit
permissions granted to the participants

		Permissionless	Permissioned
Architecture based on ownership of the data infrastructure	Public	<ul style="list-style-type: none"> Anyone can join, read, write, and commit Hosted on public servers Anonymous, highly resilient Low scalability 	<ul style="list-style-type: none"> Anyone can join and read Only authorized and known participants can write and commit Medium scalability
	Private	<ul style="list-style-type: none"> Only authorized participants can join, read, and write Hosted on private servers High scalability 	<ul style="list-style-type: none"> Only authorized participants can join and read Only the network operator can write and commit Very high scalability

DLT Landscape



Source: KPMG Research

What are the main benefits?



Enable trust

No need for a intermediary to store and transfer value or guarantee data integrity.



Streamlined data reconciliation

Consensus mechanism to validate transactions.



Immutability

Validated records are irreversible and cannot be changed.



Transparency

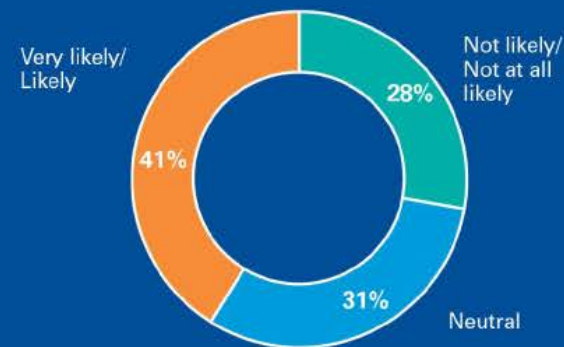
All network participants have a full copy of the ledger for full transparency.

KPMG Blockchain survey

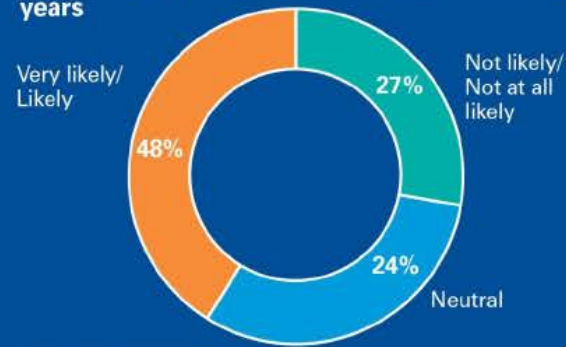
KPMG Technology Industry Innovation Survey: Blockchain

Now in its seventh year, the Survey includes responses from more than 740 global leaders in the technology industry. Twelve countries are represented and seventy-six percent of the respondents are C-level executives. The online survey was conducted from December 2018 to January 2019.

Likelihood your company will implement blockchain technology in the next three years



Likelihood that blockchain will change the way your company does business in the next three years



Percentages do not sum to 100% due to rounding.

Biggest challenges with adopting blockchain technology in the next three years



Partial list. Percentages do not sum to 100%.

Greatest disruption resulting from blockchain initiatives in the next three years



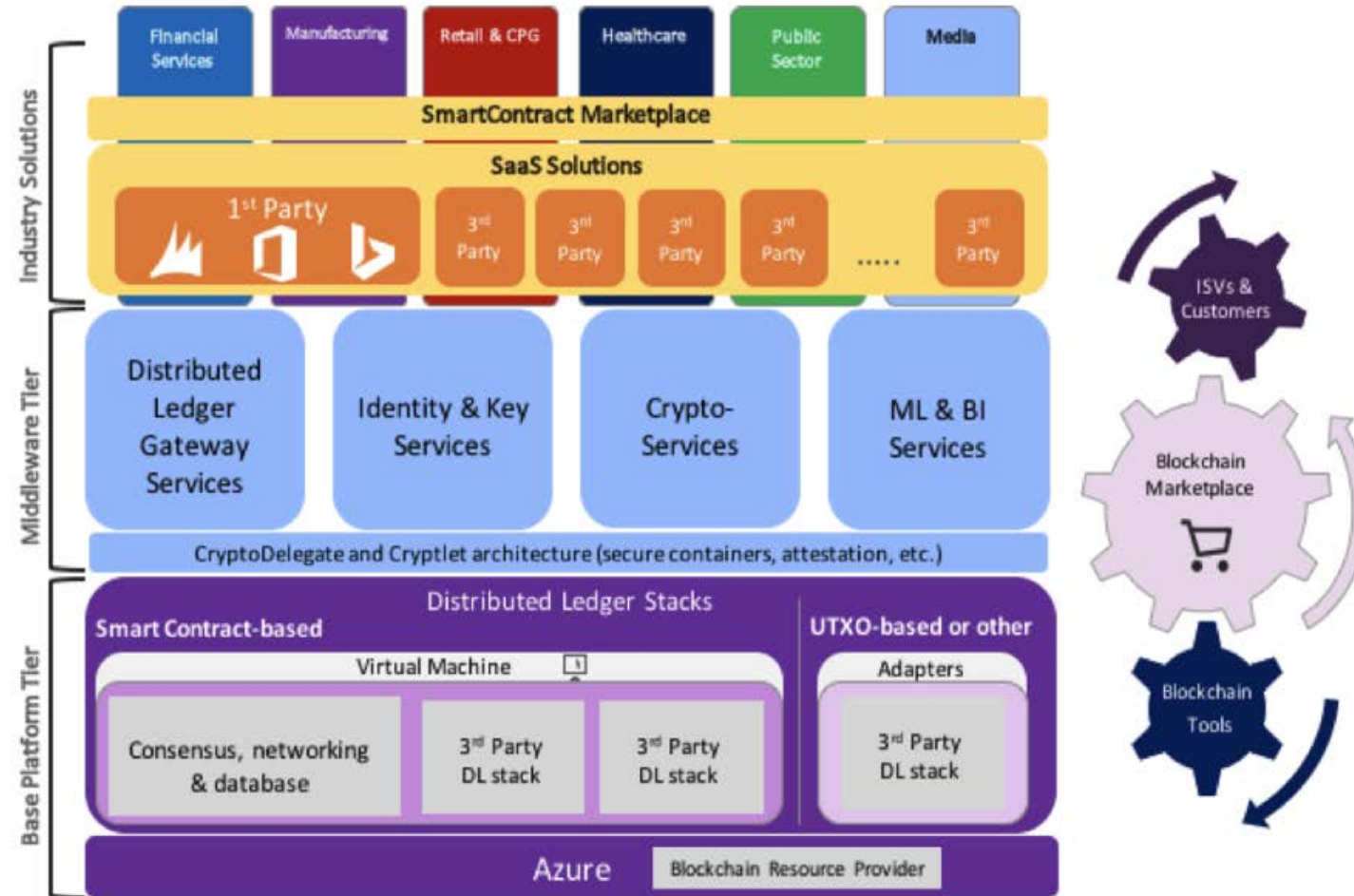
Partial list. Percentages do not sum to 100%.

Top benefits with adopting blockchain technology



Partial list. Percentages do not sum to 100%.

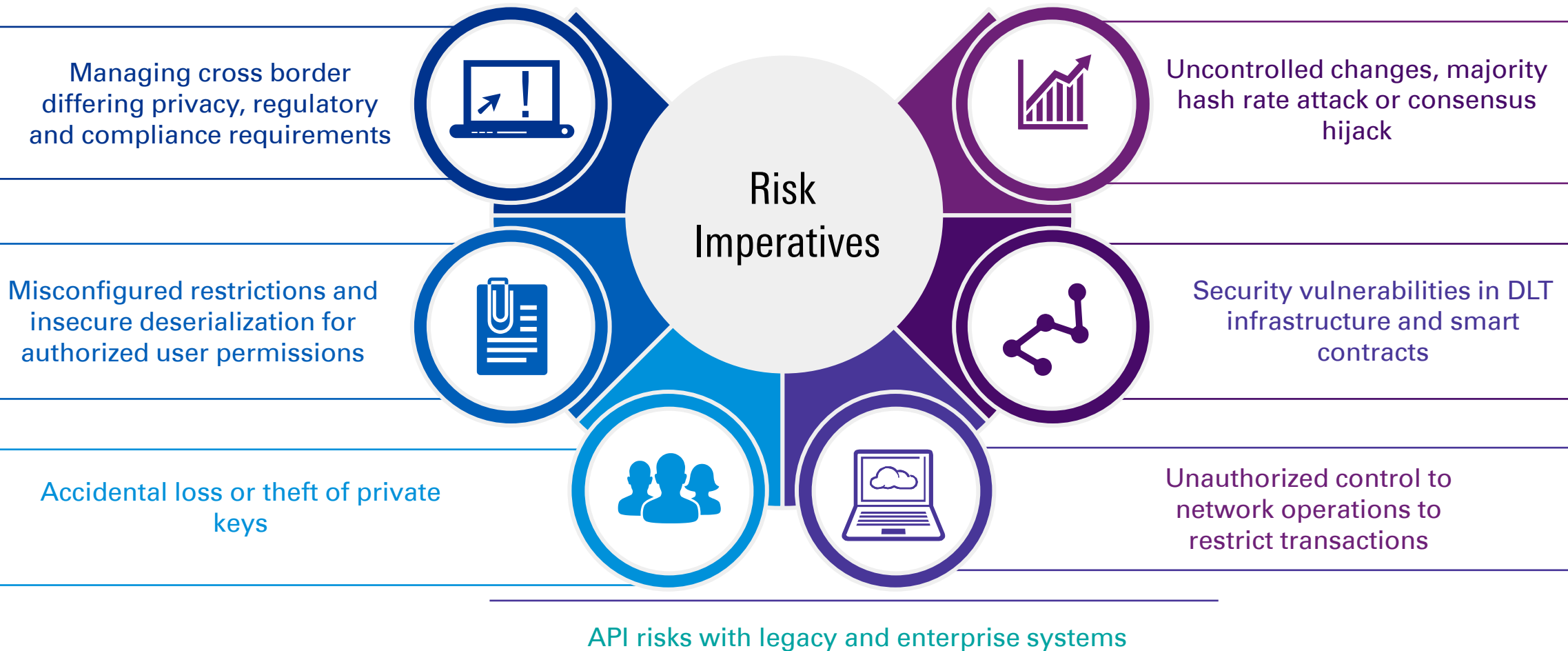
Sample Cloud-based Blockchain Stack (MS Azure)



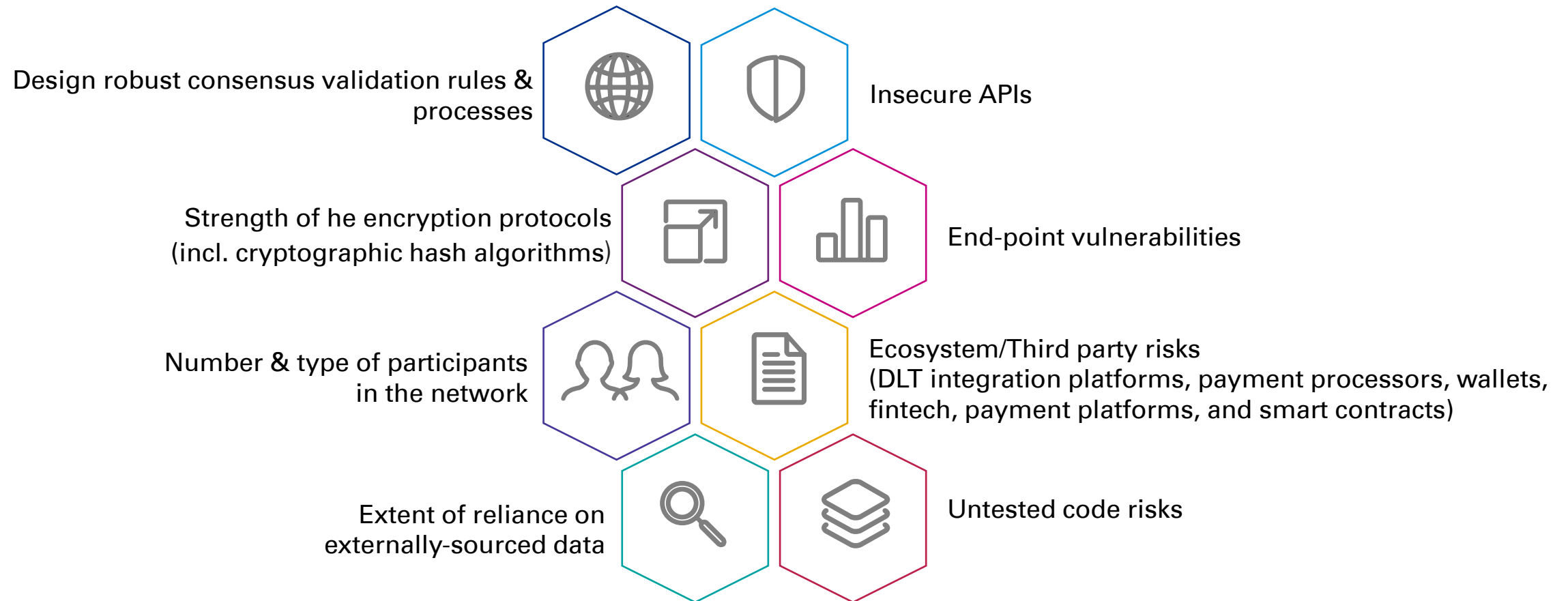
Agenda

- Introduction
- Crash course Blockchain/DLT concepts
- **Blockchain (Control) Frameworks**
- ISO standard
- ERP Integration demo
- Case studies
- Q&A

Potential Blockchain risks



Key considerations for protecting from cyber attacks (in case of permissioned DLTs)



Illustrative control areas for protecting from cyber attacks



Why need a Blockchain Control Framework?

- **Complete coverage of all key risks / areas**
- **Structured set of ‘good practices’**
- **Embedding in PDCA cycle**
- **Standardized trust levels & achieving Interoperability**
- **Providing auditing & certification criteria**

And why not apply a framework?

- **Strait-jacket & substantial effort to implement fully**
- **Absence of data (entry) integrity & ‘soft controls’**
- **Frameworks do not provide answers to all key questions, such as:**
 - Which protocol to select?
 - How to develop secure smart contracts?
 - How to integrate Blockchain with ERP systems?

Blockchain Platforms/protocols

	Exonum	Hyperledger	Openchain	Graphene	Corda	MultiChain
Code type	Open-source	Open-source	Open-source	Open-source	Open-source	Open-source
Community	Regular updates	Regular updates	Not very active	Not very active	Regular updates	Regular updates
Industry focus	FinTech, GovTech LegalTech	Cross-industry	Cross-industry	Cross-industry	Financial services	Financial services
Governance	The Bitfury Group	The Linux Foundation	Coinprism	Cryptonomex	R3 consortium	Coin Science
Ledger type	Private and permissioned	Private and public	Private	Private and public	Permissioned	Private
Cryptocurrency	None	None	Aircoin	Bitshares	None	None
Language	Rust	Python	JavaScript	C++	Kotlin, Java	C++
Smart contract functionality	Yes	Yes	Yes	Yes	Yes	Yes
Best projects	Land registry and land cadastre systems for Georgia and Ukraine	Banking app for Postal Savings Bank of China, DLT.sg Singapore blockchain apps	Used in projects for Adobe, Arm, Cisco, Comcast, GitHub, Harman, Hitachi, HPE, Qualcomm, Siemens, Sony, Toyota, Western Digital, and Wind River	Steemit, BitShares, Peerplay	Banking systems for Bangkok Bank, BBVA, BNP Paribas, HSBC, ING	Wolfram Resear
	Exonum	Hyperledger	Openchain	Graphene	Corda	MultiChain

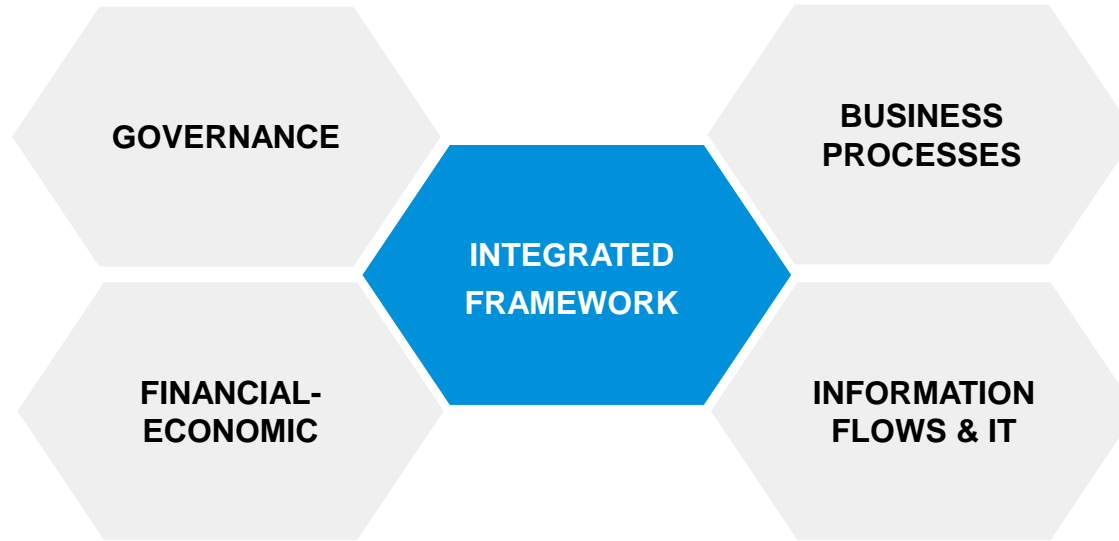
Blockchain / DLT Control Frameworks

- **ISACA**
- **NOREA**
- **ISO**
- **Others (see next)**

Blockchain Control Frameworks

	ISACA	NOREA	COSO	ISO	Maltese government	Cloud Security Alliance	Others frameworks
Publication(s)	<ol style="list-style-type: none"> Blockchain Framework & Guidance Blockchain Audit Preparation Guide 	Blockchain Control Framework (i.o.)	Blockchain & Internal Control	Blockchain/DLT Security, Governance & Interoperability (i.o.)	System Auditor Control Objectives (part C)	DLT Security Framework for Financial Services	<ul style="list-style-type: none"> CPA Canada University of Cambridge KPMG
Version/ date(s)	<ol style="list-style-type: none"> 2020 2019 	2021 (Q3/4)	2019	2022 – 2023	2018	2021 – 2022 (i.o.)	Various
Origin	ISACA HQ (International / US)	Netherlands	US	International	Malta Digital Innovation Authority	International	idem
Language	English	Dutch	English	English	English	English	English
Nature framework	<ol style="list-style-type: none"> Controls & Security Audit 	Control & Audit (limited Security)	Control	Security, Governance & use cases	Audit	Security	Audit & Control
DLT components addressed	<ul style="list-style-type: none"> Governance Infrastructure Data Key management Smart contracts 	<i>See next page</i>	<ul style="list-style-type: none"> Nodes Protocols Private keys Smart contracts 	<i>See next section</i>	<ul style="list-style-type: none"> Virtual Financial Assets DLT Platforms Smart contracts 	<ul style="list-style-type: none"> More security-oriented domains than DLT domains 	Various, incl. cryptocurrencies
Focus areas (with criteria/ requirements)	<ul style="list-style-type: none"> Pre-implement. Governance Development Security Transactions Consensus 	<i>See next page</i>	<ul style="list-style-type: none"> Control Environm. Risk Assessment Control Activities Information & Communication Monitoring Activit. 	<i>See next section</i>	<ul style="list-style-type: none"> Functionality & Compliance with Regulatory Reqs System Ops Organiz. & Mgt. Communication Risk Mgt & ToD ITGC / SOC areas Privacy 	<ul style="list-style-type: none"> Governance & Compliance IAM & key mgt. Secure coding Network/Consensus Metrics Data integrity Vendor Mgt Transactions Ops & systems Maintenance 	Various
Other aspects	Separate Excel for specifying adjusted/ additional controls	Addresses DLT case studies		Part of broader set of Blockchain/DLT standards	Partly based on local legislation	Based on work by The Depository Trust & Clearing Corporation	Maturity Model (KPMG)

NOREA Blockchain Control Framework



Audit domein	Control doelstelling	Risico ID	Risico-Gebied	Beheers-maatregel	Korte omschrijving
Governance Domein					
Financieel domein					
Processen domein					
IV-IT domein					

Governance domain

- Strategic objectives
- Governance & management
- Legislation & regulation
- Organisational setup

Financial domain

- Financial-economic objectives

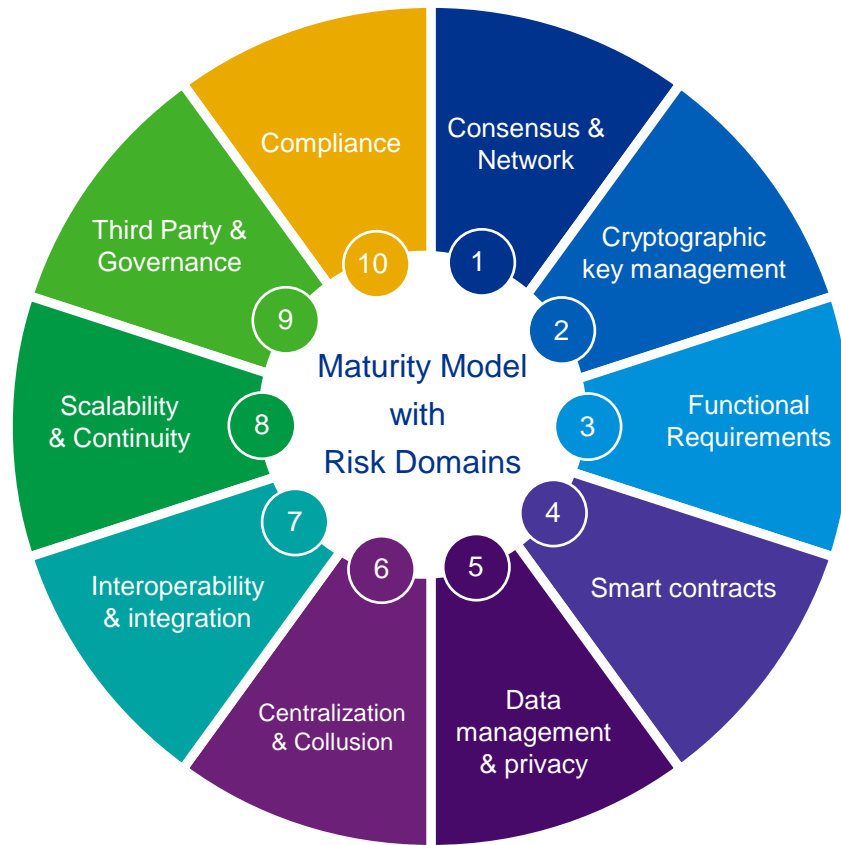
Process domain

- Business processes
- Social-organisational processes
- Marketing & Communication

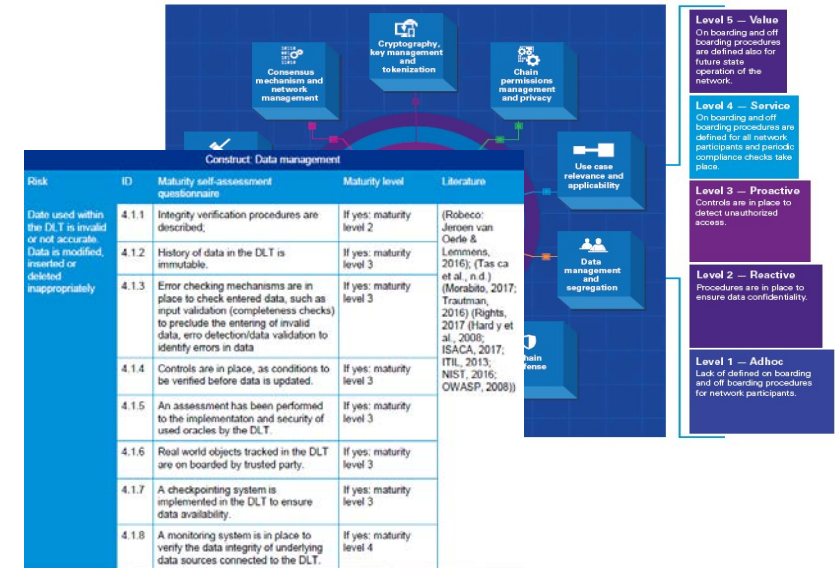
IV-IT domain

- Data Management & data architecture
- Interconnectivity
- Data Privacy & Security
- Cryptographic key management
- Smart contracts
- Centralization & Collusion
- Interoperability & Integration
- Scalability & Continuity
- Platform standardisation & Migration

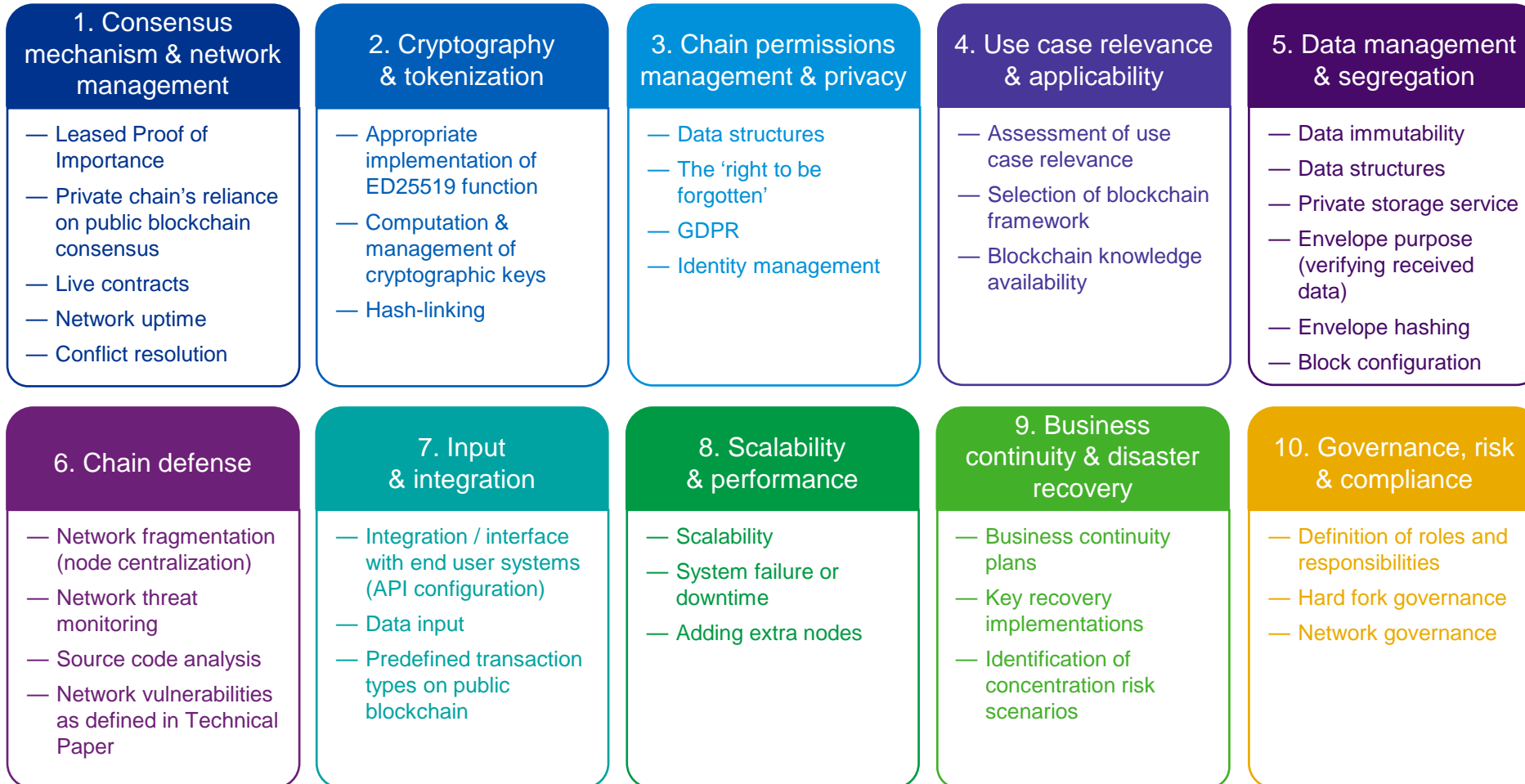
KPMG Blockchain/DLT Maturity Model



KPMG blockchain technology risk assessment example output



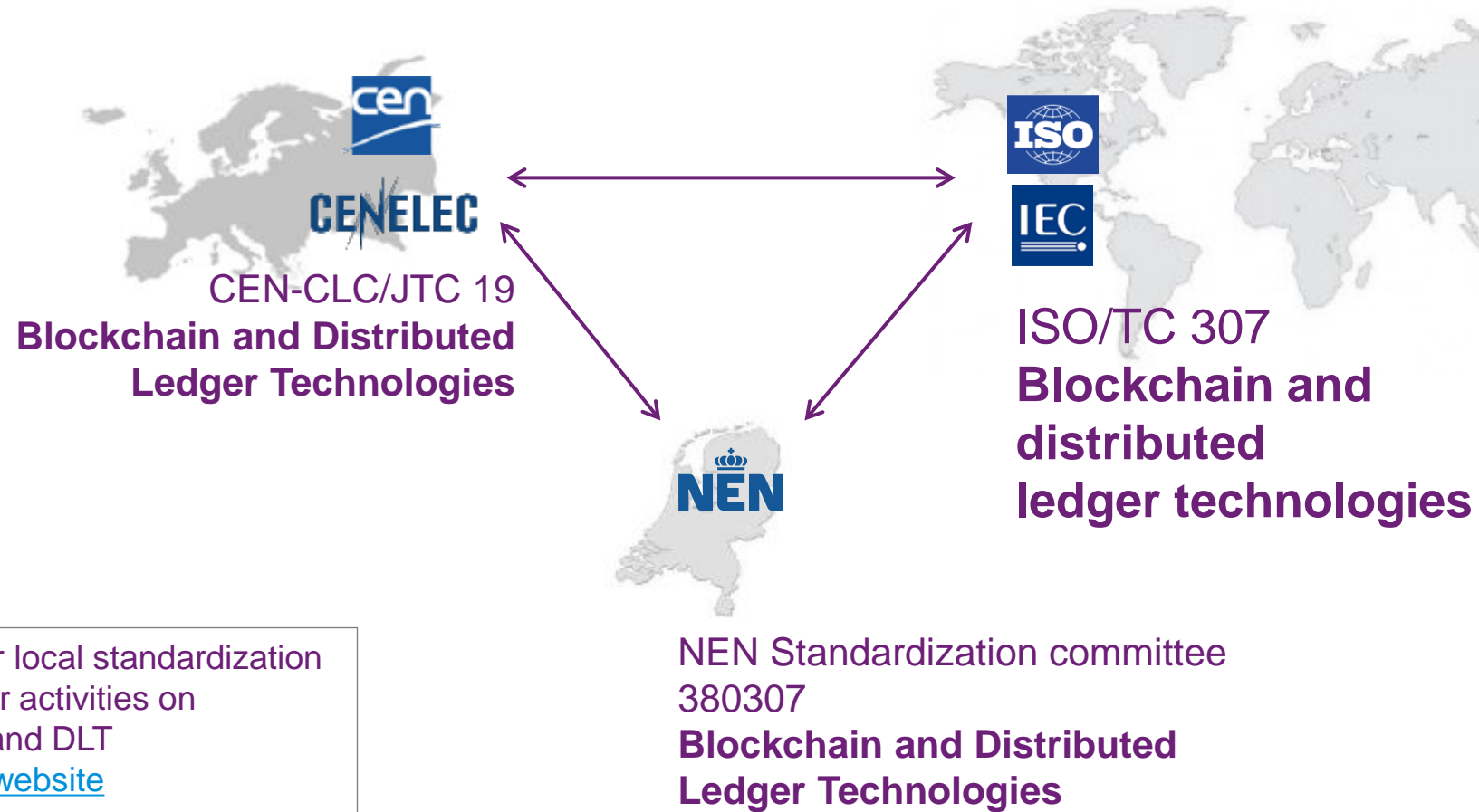
KPMG Blockchain/DLT building blocks & focus areas



Agenda

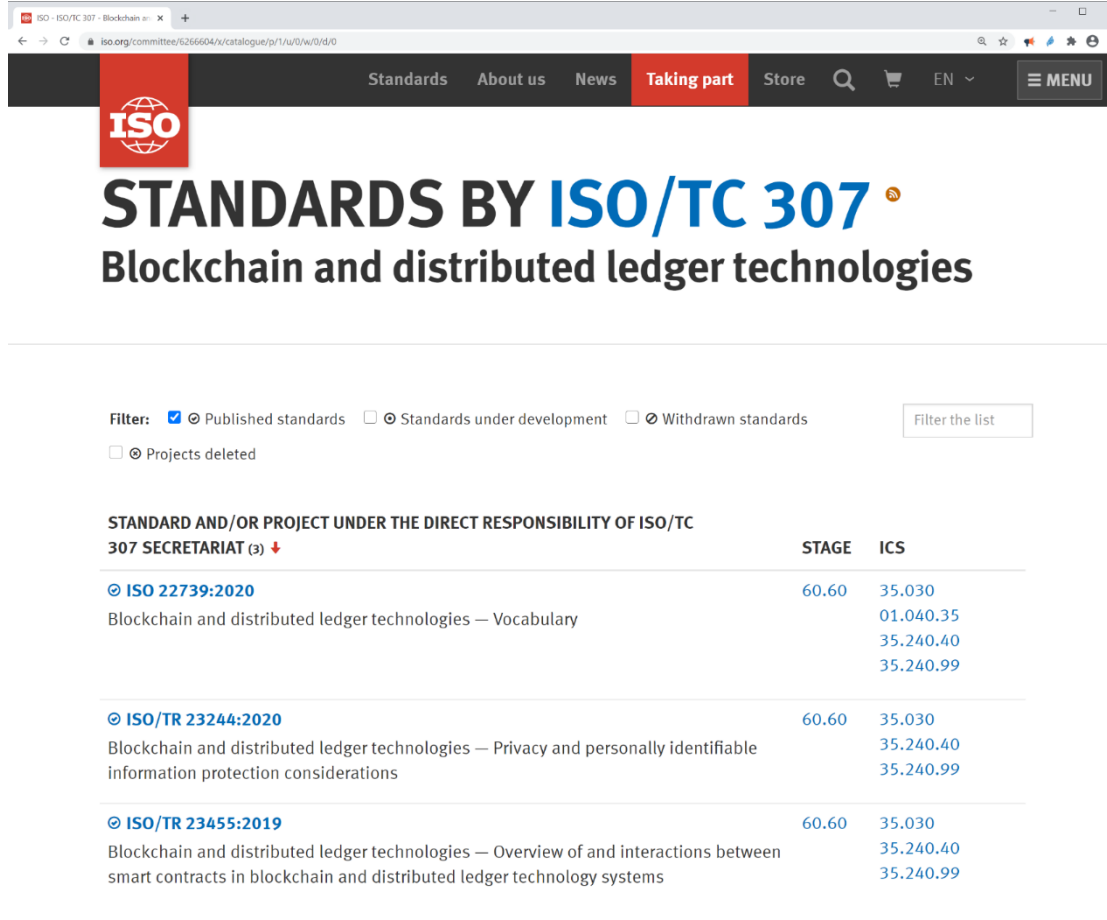
- Introduction
- Crash course Blockchain/DLT concepts
- Blockchain (Control) Frameworks
- **ISO standard**
- ERP Integration demo
- Case studies
- Q&A

The world of standardization



Contact your local standardization body for their activities on Blockchain and DLT via the [ISO website](#)

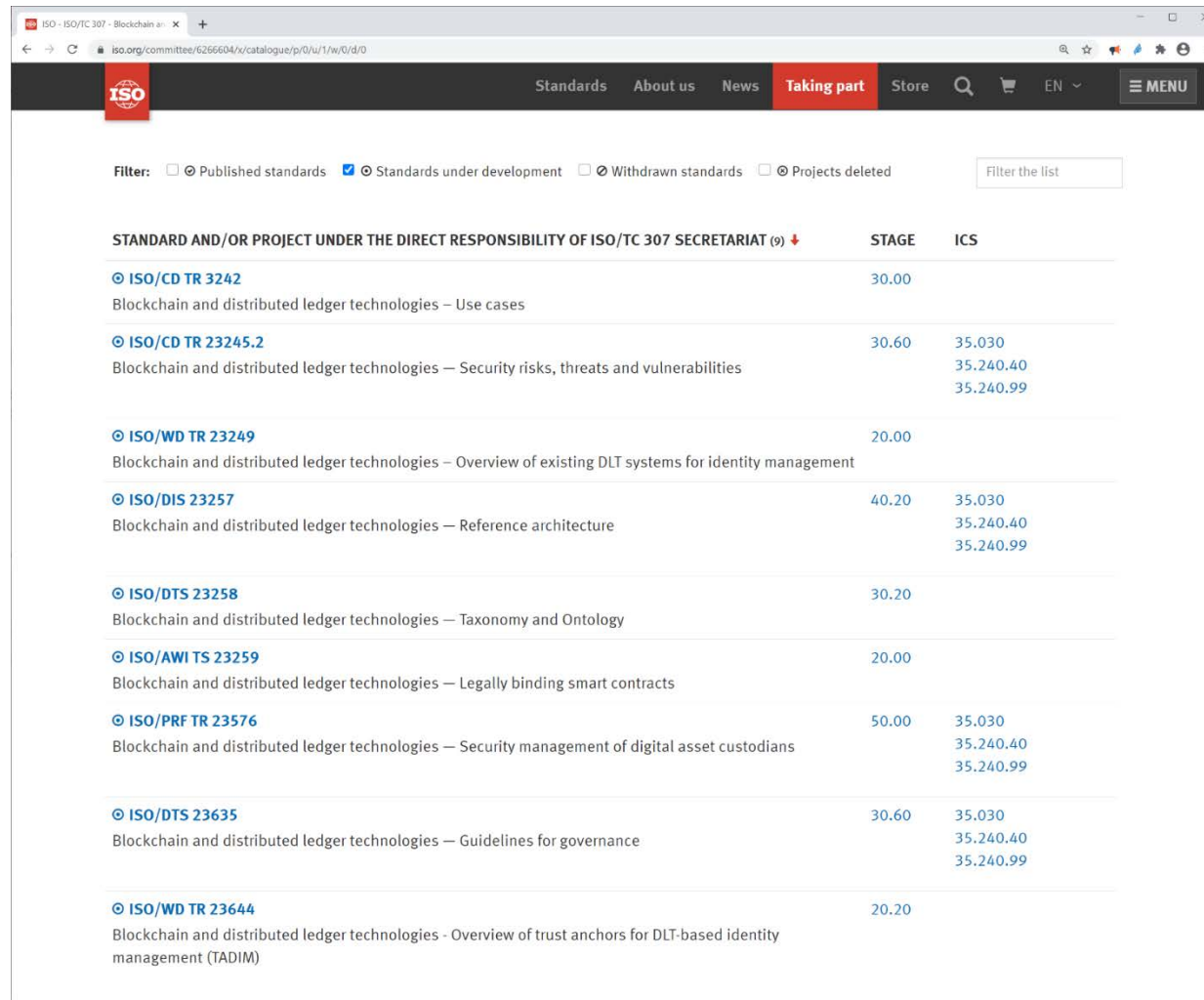
Published Standards



The screenshot shows the ISO website's 'STANDARDS BY ISO/TC 307' page. The page title is 'STANDARDS BY ISO/TC 307 Blockchain and distributed ledger technologies'. Below the title, there are filter options: 'Published standards' (checked), 'Standards under development', 'Withdrawn standards', and 'Projects deleted'. A 'Filter the list' button is also present. The main content area lists three standards under the heading 'STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 307 SECRETARIAT (3)'. Each standard entry includes the standard number, title, stage, and ICS numbers.

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 307 SECRETARIAT (3)	STAGE	ICS
ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary	60.60	35.030 01.040.35 35.240.40 35.240.99
ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations	60.60	35.030 35.240.40 35.240.99
ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	60.60	35.030 35.240.40 35.240.99

Influencing the contents of standards



The screenshot shows the ISO website's 'Standards' section, filtered for 'Standards under development'. The table lists various standards and projects under the direct responsibility of ISO/TC 307 Secretariat, including ISO/CD TR 3242, ISO/CD TR 23245.2, ISO/WD TR 23249, ISO/DIS 23257, ISO/DTS 23258, ISO/AWI TS 23259, ISO/PRF TR 23576, ISO/DTS 23635, and ISO/WD TR 23644. Each entry includes a description, a stage number, and associated ICS numbers.

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 307 SECRETARIAT (9)	STAGE	ICS
ISO/CD TR 3242 Blockchain and distributed ledger technologies – Use cases	30.00	
ISO/CD TR 23245.2 Blockchain and distributed ledger technologies — Security risks, threats and vulnerabilities	30.60	35.030 35.240.40 35.240.99
ISO/WD TR 23249 Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management	20.00	
ISO/DIS 23257 Blockchain and distributed ledger technologies — Reference architecture	40.20	35.030 35.240.40 35.240.99
ISO/DTS 23258 Blockchain and distributed ledger technologies — Taxonomy and Ontology	30.20	
ISO/AWI TS 23259 Blockchain and distributed ledger technologies — Legally binding smart contracts	20.00	
ISO/PRF TR 23576 Blockchain and distributed ledger technologies — Security management of digital asset custodians	50.00	35.030 35.240.40 35.240.99
ISO/DTS 23635 Blockchain and distributed ledger technologies — Guidelines for governance	30.60	35.030 35.240.40 35.240.99
ISO/WD TR 23644 Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)	20.20	

Check out relevant
[ISO standards under development](#)

Influencing the contents of standards

- Participate in *ISO working groups* through a local standardization committee via your [national standardization body](#)
- Dutch organizations can participate via [NEN](#).
- Influence standards under development.
 - Write parts of new standards
 - Comment
 - Vote
- Share knowledge with other committee members.

Focus Areas in DLT Systems Audit in other Global Forums

At a high level, the following areas remain the focal points for DLT Audit in global forums other than ISO

ITUT DLT Audit Focus Areas

- Providing assurance on the DLT technologies
- Audit of related off chain components
- Auditing transactions on DLT
- Providing assurance on the DLT technologies**
- Security Aspects
- Environmental Aspects



****Providing assurance on the DLT technologies (ITUT)**

Roles are designed and enforced as required by regulation;

- An appropriate governance has been put in place, which defines how the DLT solution must operate, how to identify, monitor and react to risks and how to manage changes and corrections in a decentralized environment;
- Development, tests and deployments take into consideration the specific risk of the DLT technologies, in particular:
 - i) Direct technological risks: i.e., used keys properties, cryptographic techniques, data structures, sidechains, wallet, consensus mechanisms, etc.;
 - ii) Usage of technologies in the solution: i.e., handling keys/devices, granting and revoking key holders, key backups, wallet management, signing transactions, etc.;
 - iii) Design, approval, testing, and management of smart contracts; iv) Security of the network.

Source "Technical Report FG DLT D5.1 Outlook on distributed ledger technologies"

Introduction to AHG02 – Guidelines for auditing DLT-based platforms (1/2)

This document provides frameworks and guidance on domains and areas which should be considered while performing audit procedures for DLT systems.

These guidelines are developed with the objectives of aiding auditors involved in the audit of DLT systems (both public and private) that describes in the series of ISO/TC 307 standards.

This guidance is applicable to an array of organizations and is not bound by type or size.

This document will cover the following types of audits (based on ISO 19011:2018):

- Internal Audit
- External Audit
- Third party Audits (Audit of vendors, third and fourth parties)

Establishing focus areas for securing DLT platforms

Keeping in mind risks associated with blockchain platforms and evolving attack vector with this emerging technology, we'll be reviewing in-place controls and DLTs across following domains:

- **Pre-implementation:** Suitability of DLT platform for the selected use case, architecture review
- **Implementation & Development** – Security by design, vulnerable source code, weak endpoints
- **Key ownership and management** - Secure storage, maintenance, review and governance of cryptographic private keys used for authentication and validation by nodes.
- **Interoperability & Integration** - Consistent communication between multiple blockchain platforms and integration with organizations' enterprise and legacy systems.
- **Consensus Mechanism** - Blocks in the chain are validated by nodes to maintain a single version of the truth to keep adversaries from derailing the system and forking the chain.
- **Heterogenous regulatory compliance** - Compliance with laws and regulations across various country and state legislations that will govern information and transactions processed.
- **Access & permissions management** - Permissions configured for defined roles for access, validation and authorization of blockchain transactions by internal and external participants.

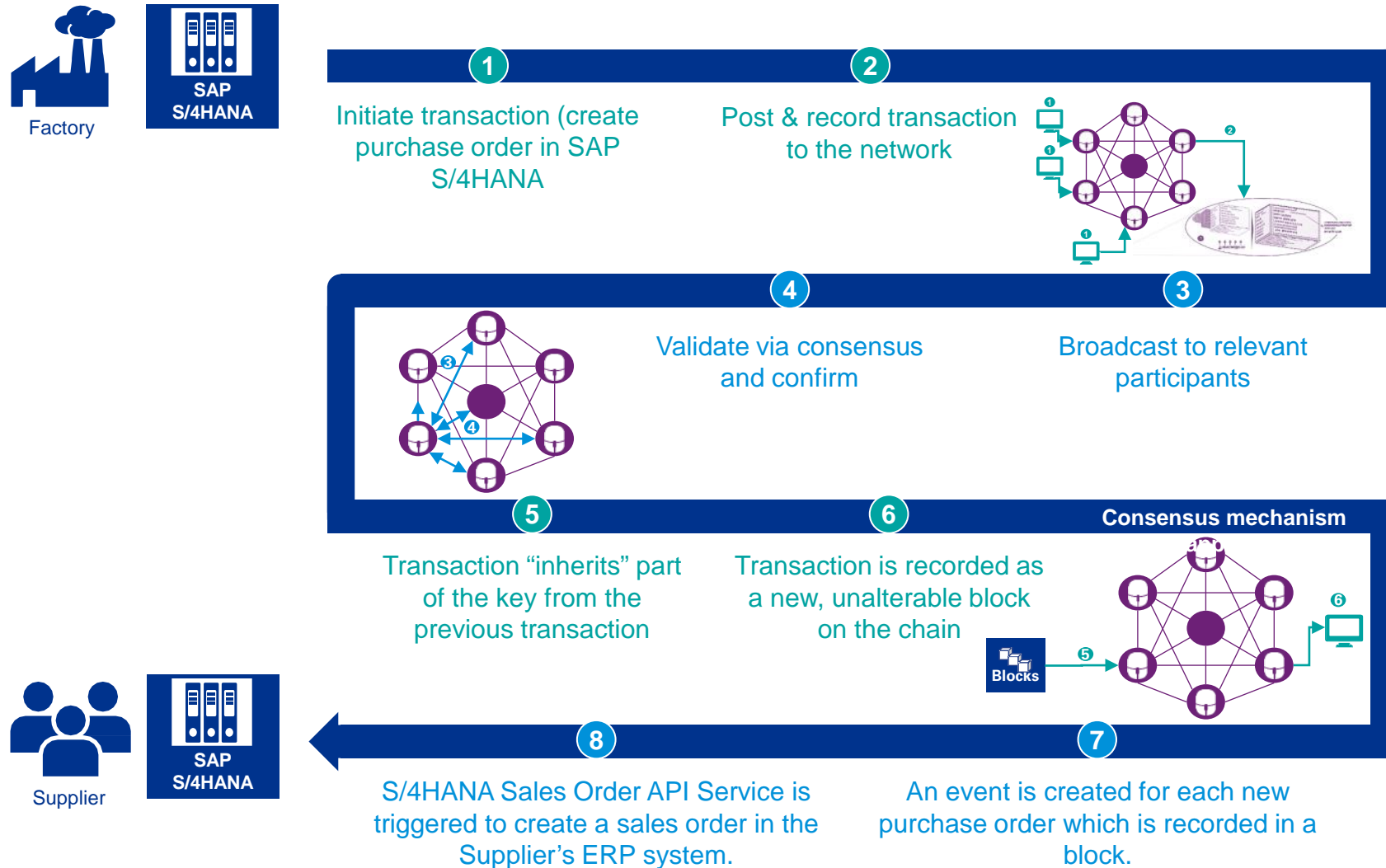
Introduction to AHG02 – Guidelines for auditing DLT-based platforms (2/2)

- **Infrastructure & application management** – Secure software development practices and testing of blockchain applications, platform, infrastructure and communication interfaces.
- **Network & node governance** – Monitoring of network for information compliance and node reputation checks to handle and resolve disputes.
- **Smart contracts** – The enterprise supports secure coding practices for blockchain source code (e.g., smart contracts or chaincode) to mitigate information security risk proactively. Smart contracts automate the business logic execution over the DLT.
- **Network-Vulnerability Management** – The enterprise effectively manages blockchain network vulnerabilities through monitoring, remediation actions and communication to relevant stakeholders.
- **Endpoint Security** – End user devices using the blockchain solution are properly managed by the enterprise (i.e., the end users' devices are tracked, hardened and addressed if compromised).
- **Vendor Due Diligence** – Due diligence for vendors/suppliers/contractors administrative and operational processes to ensure ongoing alignment between the enterprise's strategic objectives and DLT solutions.
- **Business Continuity and Disaster Recovery** – Private or permissioned DLT has both centralized and decentralized components, there needs to be a concrete understanding of what will happen, should these components be affected by any potential factors.
- **Transactions** – Validate transactions and monitoring mechanism in place

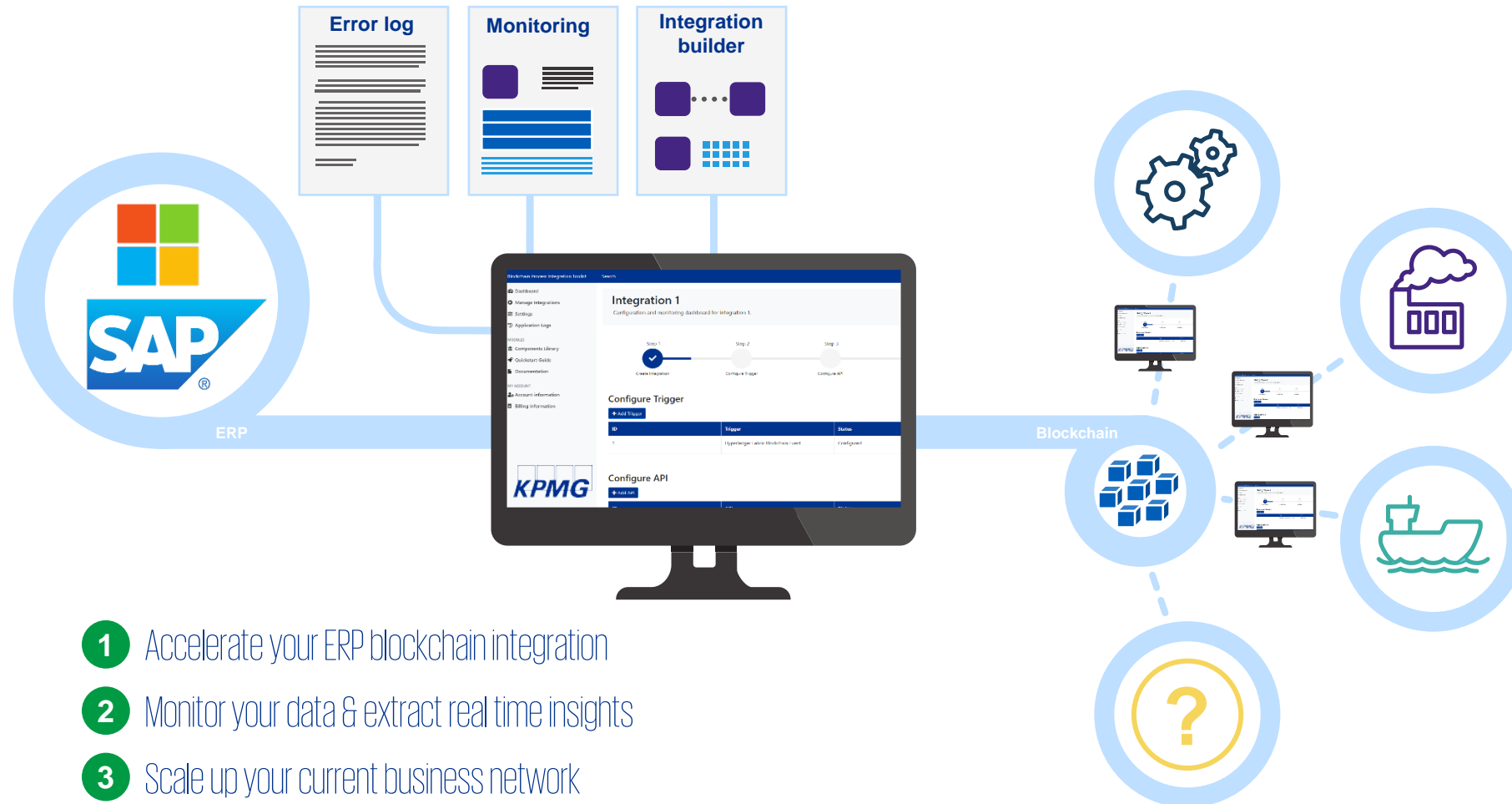
Agenda

- Introduction
- Crash course Blockchain/DLT concepts
- Blockchain (Control) Frameworks
- ISO standard
- **ERP Integration demo**
- Case studies
- Q&A

Companies need to integrate with ERP systems

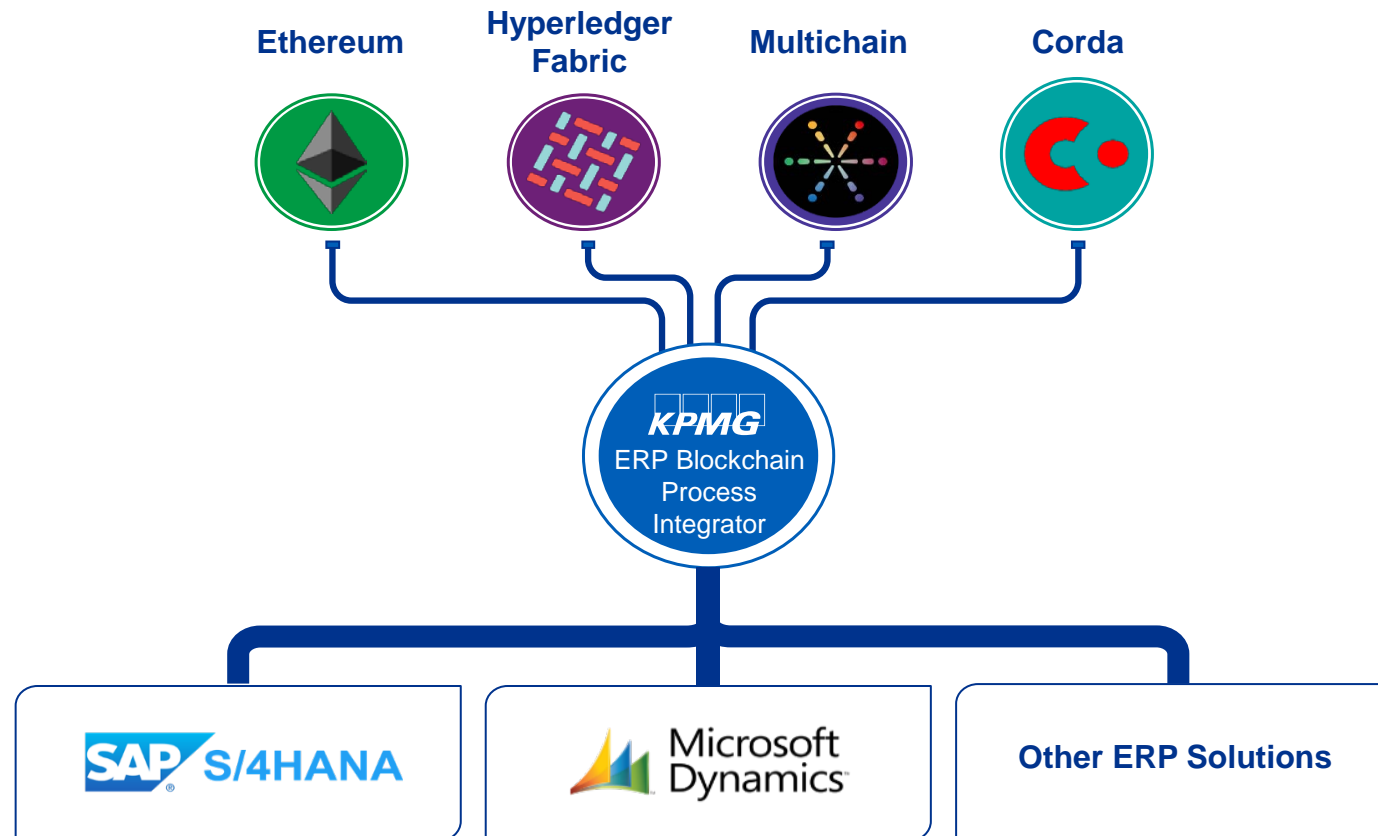


ERP Blockchain Process Integration (1/2)



- 1 Accelerate your ERP blockchain integration
- 2 Monitor your data & extract real time insights
- 3 Scale up your current business network

ERP Blockchain Process Integration (2/2)



About the project

- This demo shows how SAP S/4HANA can be integrated with blockchain technology. The aim is to investigate the technical setup of a blockchain in an ERP scenario.
- Blockchain is used as a data interface layer between ERP systems. The program on the blockchain manages sales orders in the Supplier's system triggered by the creation of purchase orders in the Factory's system.
- This demo does not focus on creating a business case for applying blockchain to integrate P2P and O2C processes, but it shows how to integrate a blockchain platform with transactional data in SAP.

Block 44

Hash of the previous block's header
0NUNJ8opVtoJQVY3asthoxG+Przf8sN/EOx19tUVxw=

Hash of this block's data segment
5J5lv/CQHccRJEackBnoZ715ra3D0f6Km/mqIXoQZE=

Transaction 1

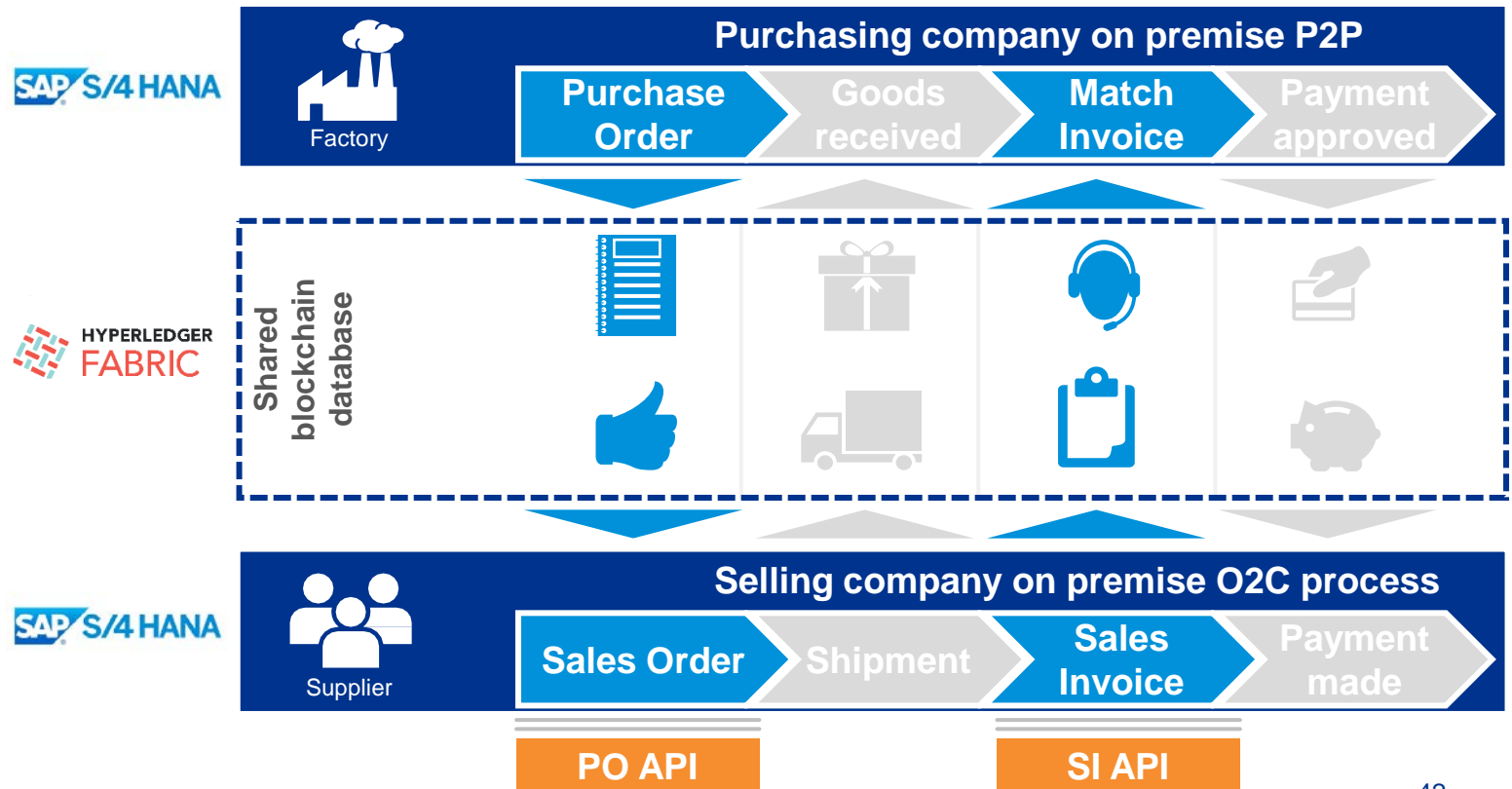
Transaction ID
7c56675c98b3f4c2f80467c3256297eb0e2e93b0a3e91d430a8ab9db3bad909

Chaincode
SAP-Blockchain-Demo

Event (purchase-order-created)
450000005

Writes

```
{
  "key": "4500000005",
  "value": {
    "PurchaseOrderByCustomer": "4500000005",
    "SalesOrderType": "OR",
    "SalesOrganization": "ZNL1",
    "DistributionChannel": "Z1",
    "OrganizationDivision": "Z1",
    "SoldToParty": "Customer X",
    "CustomerPaymentTerms": "0002",
    "IncotermsClassification": "CFR",
    "IncotermsTransferLocation": "Amstelveen",
    "to_Item": [
      {
        "Material": "PC",
        "RequestedQuantity": "100",
        "RequestedQuantityUnit": "Laptop",
        "ProductionPlant": "ZNL1",
        "ShippingPoint": "ZNL1"
      },
      {
        "Material": "PC",
        "RequestedQuantity": "200",
        "RequestedQuantityUnit": "Laptop",
        "ProductionPlant": "ZNL1",
        "ShippingPoint": "ZNL1"
      }
    ]
  }
}
```



ERP Blockchain Integration Demo

- The end user experience is a real-time connection with an external partner's system. The blockchain runs on the background and does not change the user experience compared to other real-time integration types.
- Before a sales order is created in the Supplier's system, both entities run the same business logic to update the blockchain with new purchase order data.
- More complex business logic can be programmed in the chaincode program to apply relevant validations for shared transactional data, e.g. contractual agreements, rebate calculations, compliancy checks.

“Just real-time integration?”



“What's new?”

Customer Reference	Document Date	Sales document type	Sales Document	Item Sold-to party	Material	Order Quantity (Item)	Sales	Net Value (Item)	Document currency
abdc01	19.11.2018	OR	1	10 ZC00000001	TEST01	1 PC	10,00	EUR	
test alp	14.12.2018	OR	2	10 ZC00000001	TEST01	1 PC	10,00	EUR	
TEst	03.01.2019	OR	3	10 ZC00000001	TEST01	1 PC	10,00	EUR	
Order 12345	04.01.2019	OR	4	10 ZC00000001	TEST01	1 PC	10,00	EUR	
Test	04.01.2019	OR	5	10 ZC00000001	TEST01	1 PC	10,00	EUR	



Factory

A shared transaction registry is maintained based on business logic agreed to by both members.

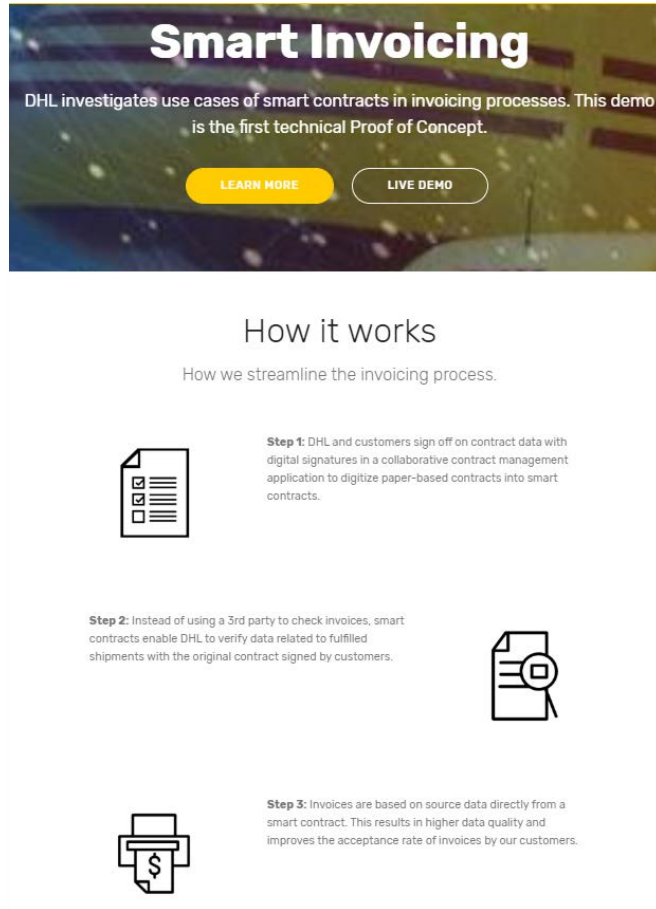


Supplier

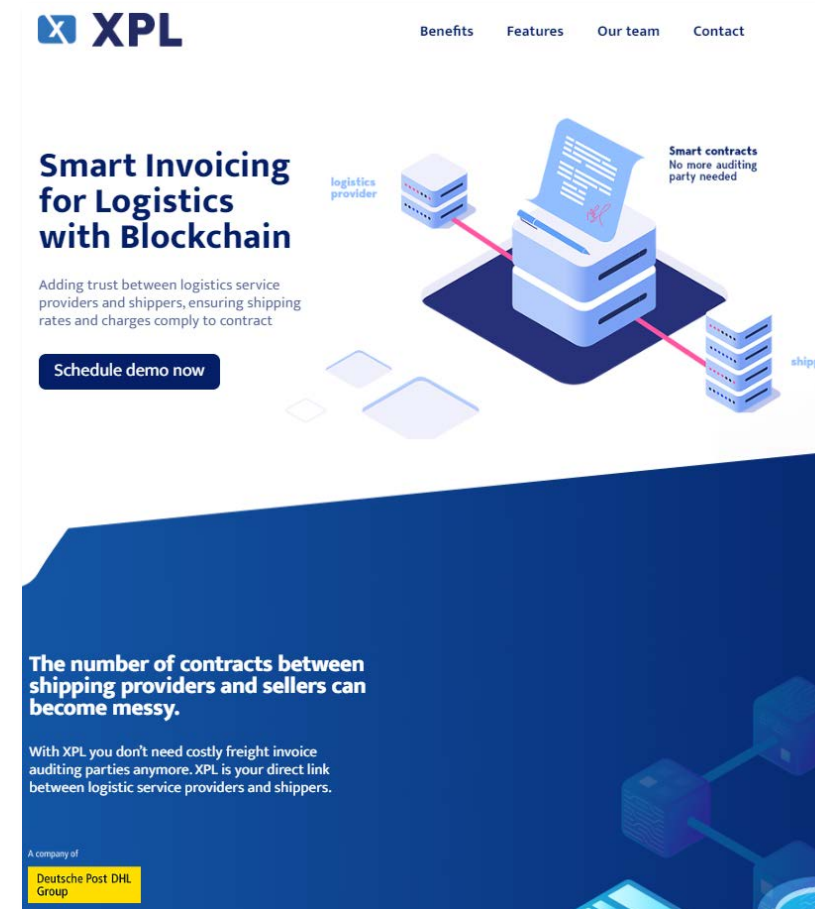
Agenda

- Introduction
- Crash course Blockchain/DLT concepts
- Blockchain (Control) Frameworks
- ISO standard
- ERP Integration demo
- **Case studies**
- Q&A

Case Study #1: Projects beyond experimentation



2017 – Proof of Concept



2020 – A company of Deutsche Post DHL Group – [Link](#)

Case Study #2: Decentralized Digital Passport platform covering Industrial Equipment

Assistance Required for:

1. Examining the risks and threats that are unique to blockchain implementation, and then design and implement key blockchain security controls, alongside business controls and conventional controls
2. Build a blockchain security reference framework that can be applied across blockchain projects and solutions for various industry use cases and deployments that span on-prem and Software as a Service (SaaS) environments.



Client Challenges:

1. Unique security risks introduced by blockchain technology
2. Regulatory and compliance requirements impacting blockchain activities
3. Minimize the risk exposure due to the services used by third parties
4. Client needed to ensure that the information security controls are designed adequately and implemented effectively for this solution.



KPMG Approach:

1. Performed information risk assessment for this private permissioned blockchain solution, in an agile method, including detailed technology risk assessment, interface assessment, cloud assessment, code scanning, VAPT, etc.
2. Supported the team in designing the key blockchain controls and provided assurance on control implementation
3. Re-aligned the existing process and guidelines to include blockchain security aspects and build a reference architecture and security handrails for business use.

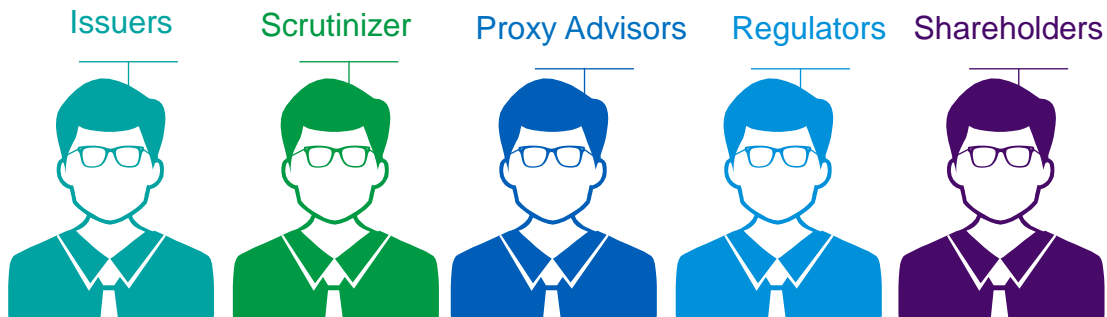
Case Study #3: e-Voting/Virtual AGM solution

Distributed Ledger Technology based e-voting solution

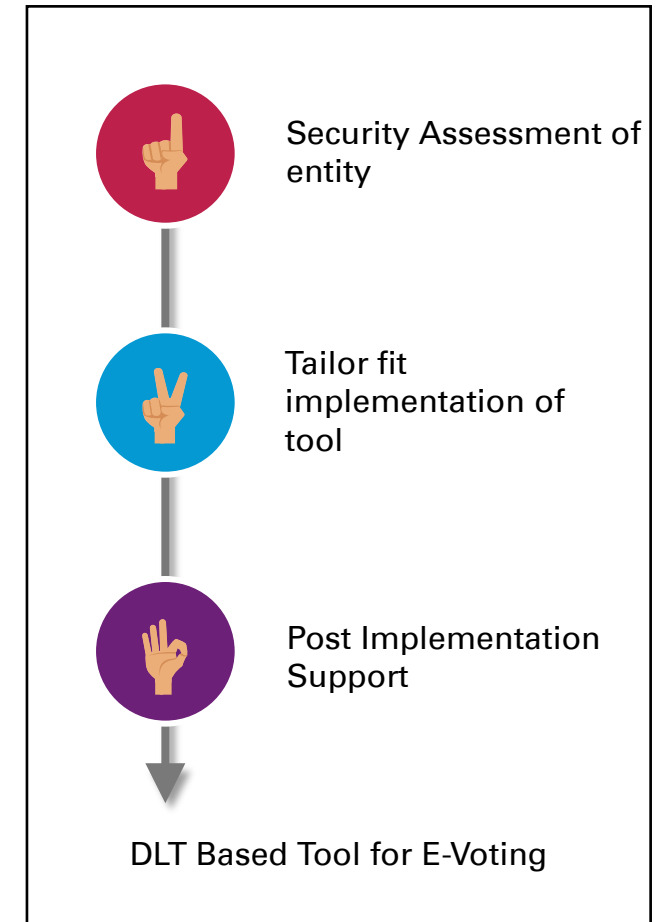
KPMG has developed an e-Voting Solution based on Distributed Ledger Technology (DLT) to execute end-to-end functionalities with respect to corporate events and e-voting by shareholders (including minority shareholders) where all relevant stakeholders are onboarded to our platform. Some key functionalities are:

- Initiate events
- Notify all stakeholders regarding announcement of events
- Use the DLT based e-voting solution to cast votes
- Report the results to issuers and regulators onboarded to the platform.
- Dashboards customized to provide results of voting sessions

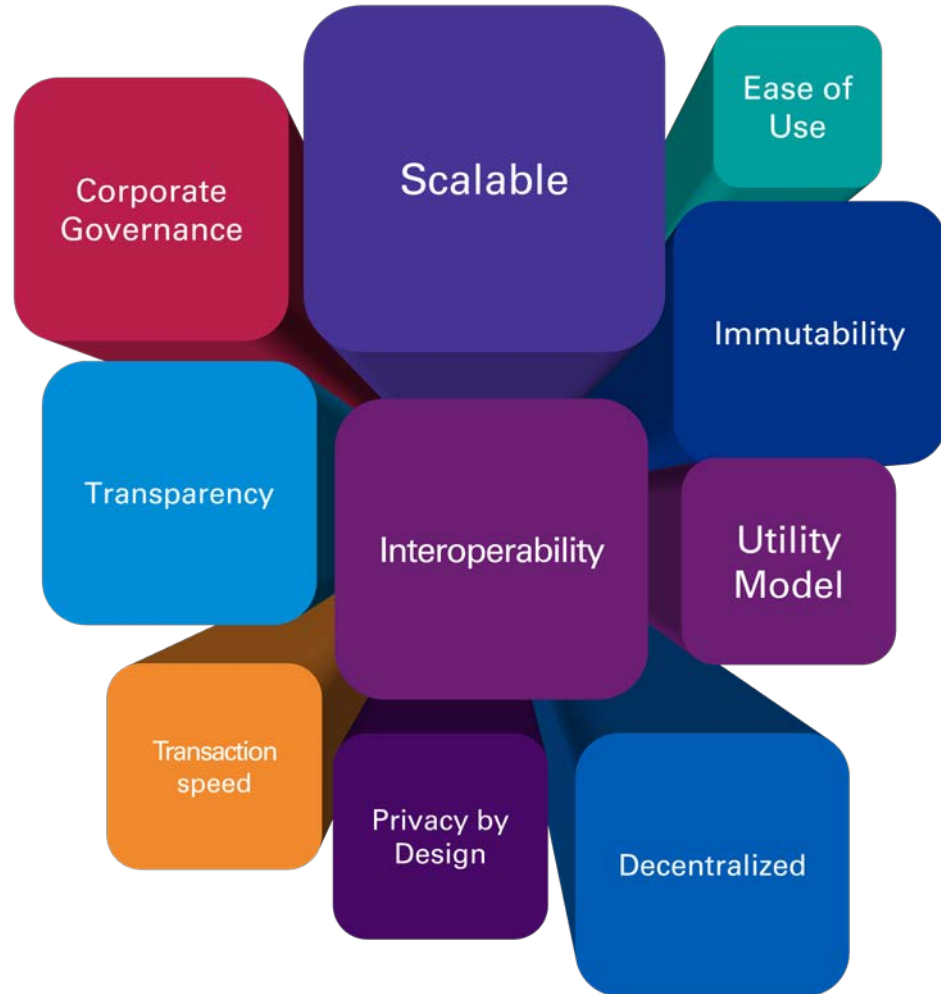
Stakeholders of the e-Voting Solution



Implementation Strategy



Highlights of e-Voting solution



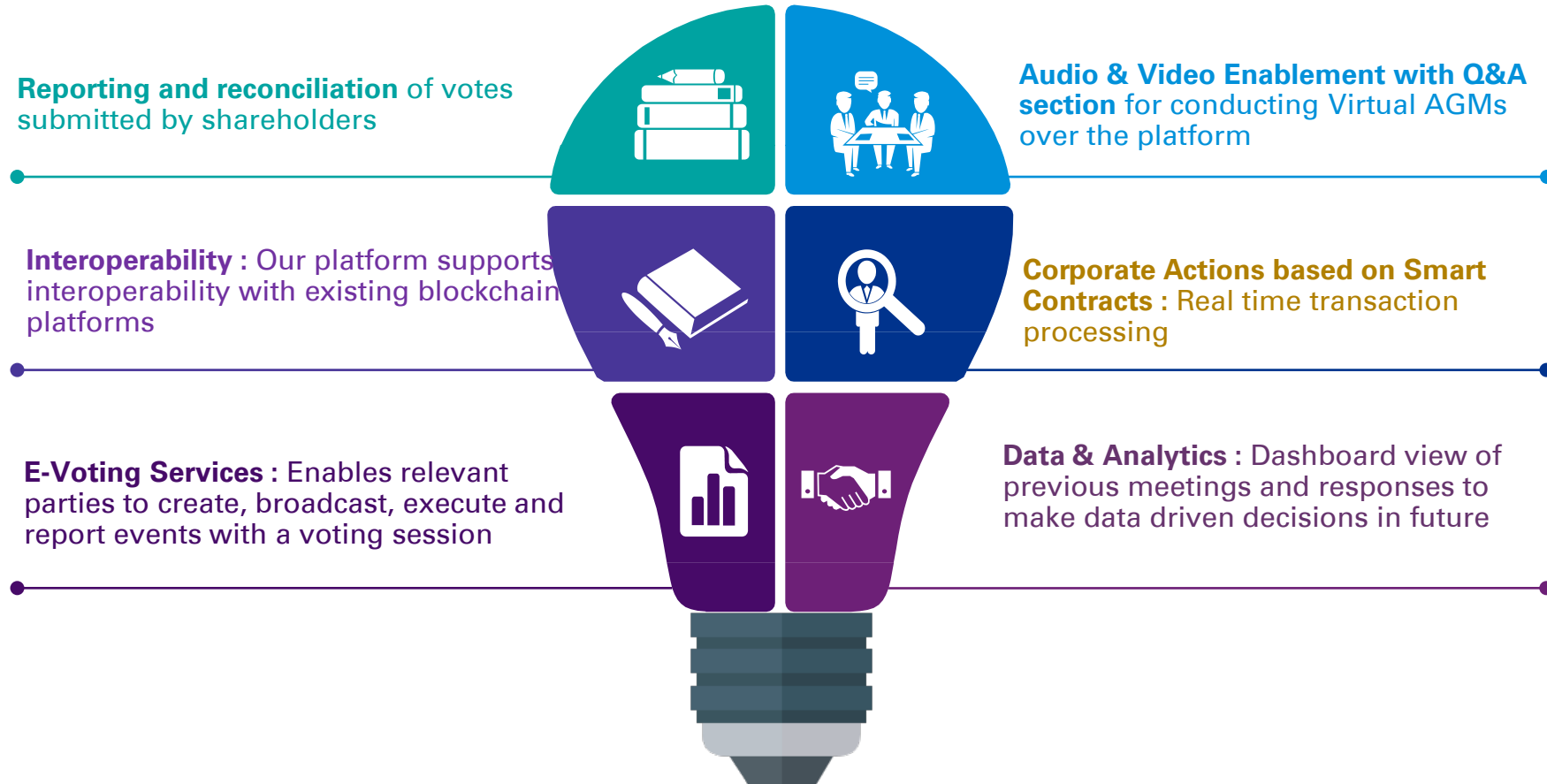
Applicability to Organisations

- Track Internal Corporate Governance in organizations during Annual General Meetings (AGM) or any important board meetings
- Making unbiased decisions by the stakeholders of listed/unlisted companies, trusts, HUFs, etc.

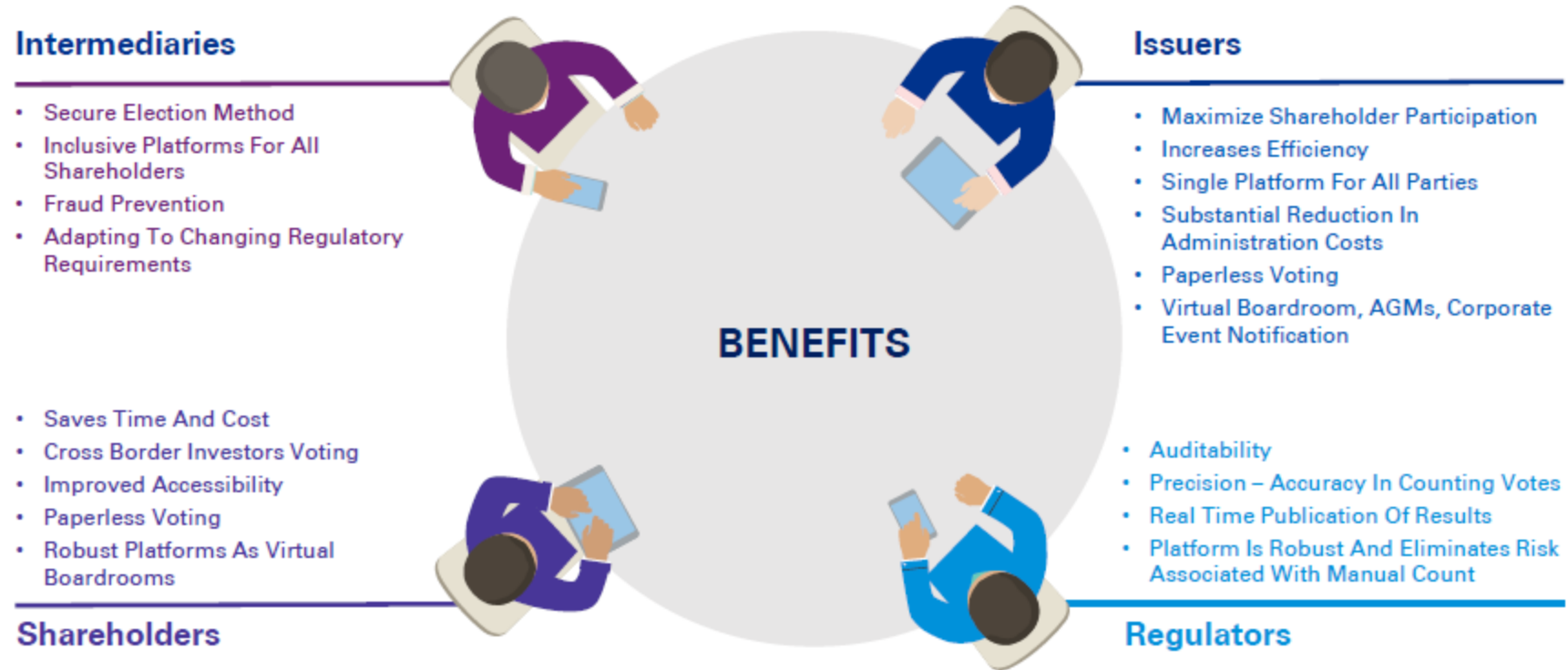
Features of Solution

- Solution is built on **Hyperledger Fabric**
- Nodes for issuers, intermediaries, shareholders, regulators and asset managers
- It provides **interoperability** with existing blockchain platforms
- **Dynamic onboarding** of nodes with built in **Identity and Access Management**
- **Secure authentication and voting mechanism** to track votes casted by shareholders
- **Reporting and reconciliation** of votes submitted by shareholders

Functionalities



Benefits to Stakeholders



Any questions?



Contact us for a demo or questions



Koen Revet

T: +316 2292 8127

E: revet.koen@kpmg.nl



Siddharth Durbha

E: siddharthdurbha@kpmg.com



Ronald Koorn

T: +316 2292 8127

E: koorn.ronald@kpmg.nl

Visit KPMG ERP & Blockchain

Useful links:

ERP & Blockchain article:

<https://www.compact.nl/articles/start-small-think-big>

DLT in supply chains:

<https://www.compact.nl/articles/enhancing-due-diligence-in-supply-chain-management/>

Case study & video:

<https://home.kpmg/au/en/home/services/blockchain-services/blockchain-platform.html>

NOREA: Blockchain & Assurance:

<https://www.norea.nl/download/?id=6535>

Blockchain & Information Risk Management:

<https://www.compact.nl/articles/how-will-blockchain-impact-an-information-risk-management-approach/>

Securing the chain:

<https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/05/securing-the-chain.pdf>

Realizing Blockchain's potential:

<https://home.kpmg/content/dam/kpmg/co/pdf/2018/09/kpmg-realizing-blockchains-potential.pdf>