LARS HUPEL

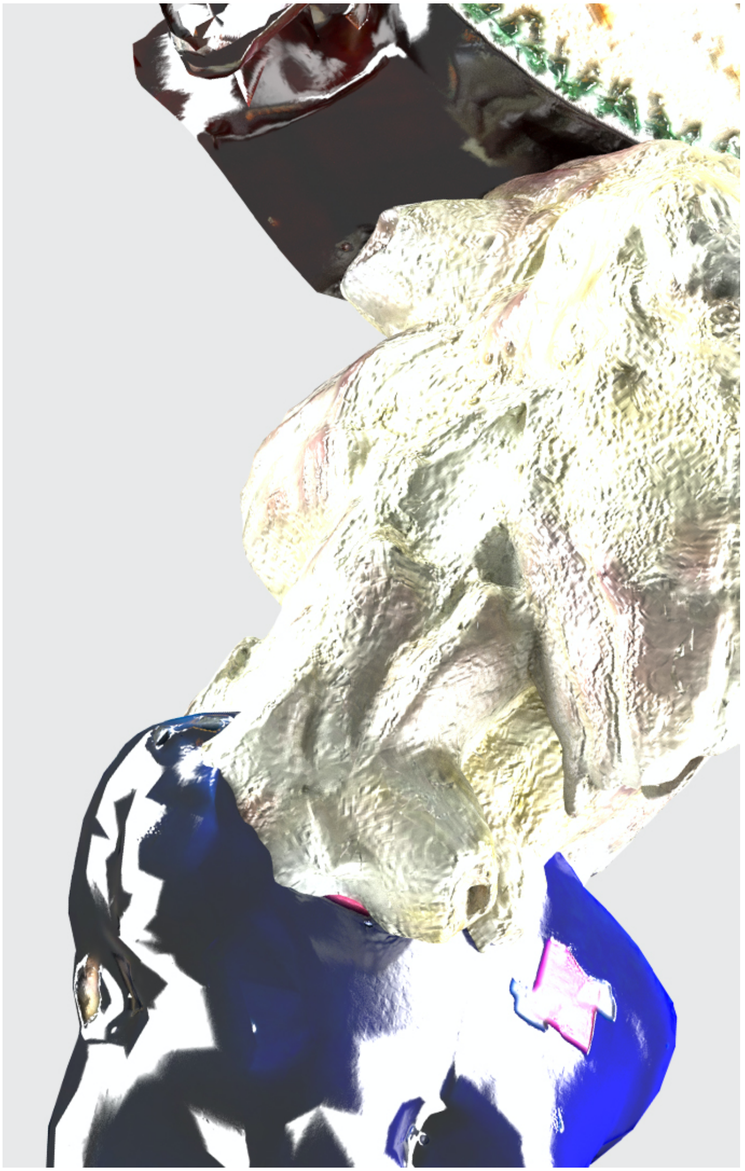
Blockchain Use Cases

When does Blockchain really make sense?

INNOQ

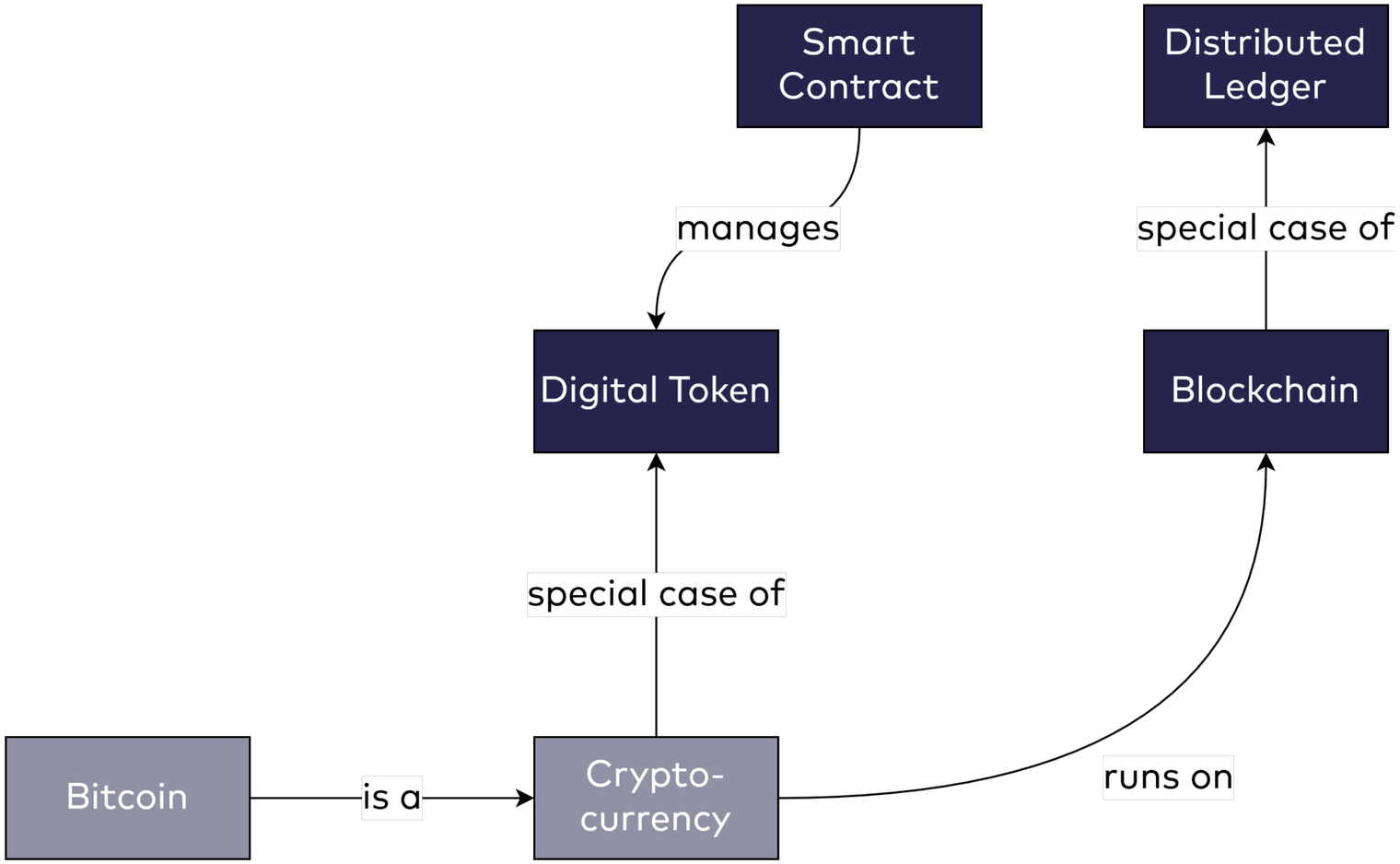
Agenda

- Quick introduction
- Assessment
- Business modelling
- Examples



Quick introduction
What is Blockchain?

Blockchain terminology



Definition: Distributed ledger

"A *distributed ledger* is an append-only store of transactions which is distributed across many machines"

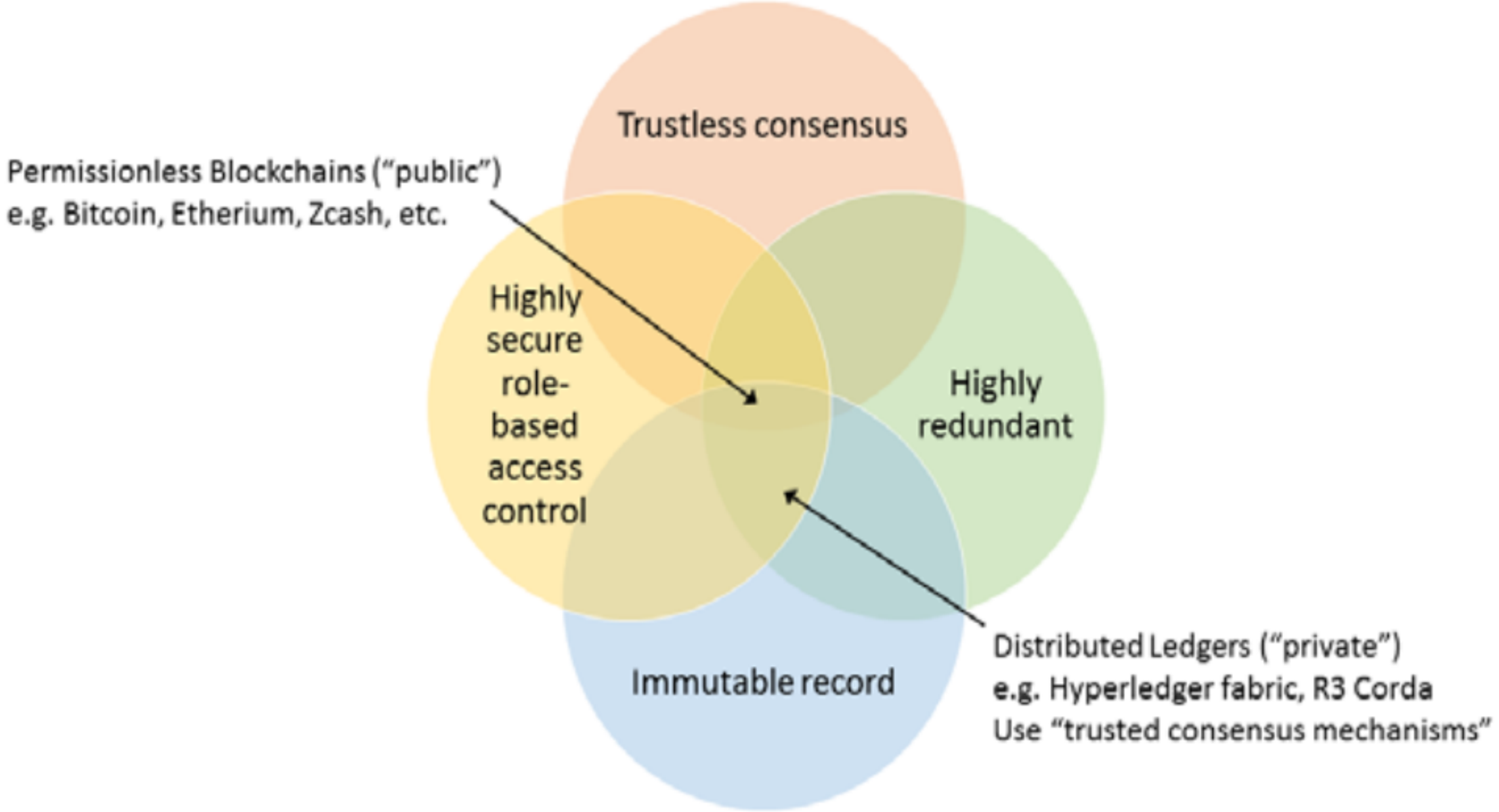
Xu, Weber, Staples: "Architecture for Blockchain Applications"

Definition: Blockchain

"A *blockchain* is a distributed ledger that is structured into a linked list of *blocks*. Each block contains an ordered set of *transactions*. Typical solutions use cryptographic hashes to secure the link from a block to its predecessor."

Xu, Weber, Staples: "Architecture for Blockchain Applications"

Core Attributes of Blockchain Technology



Blockchain and Suitability for Government Applications (DHS)

Identity & Access control

Read access

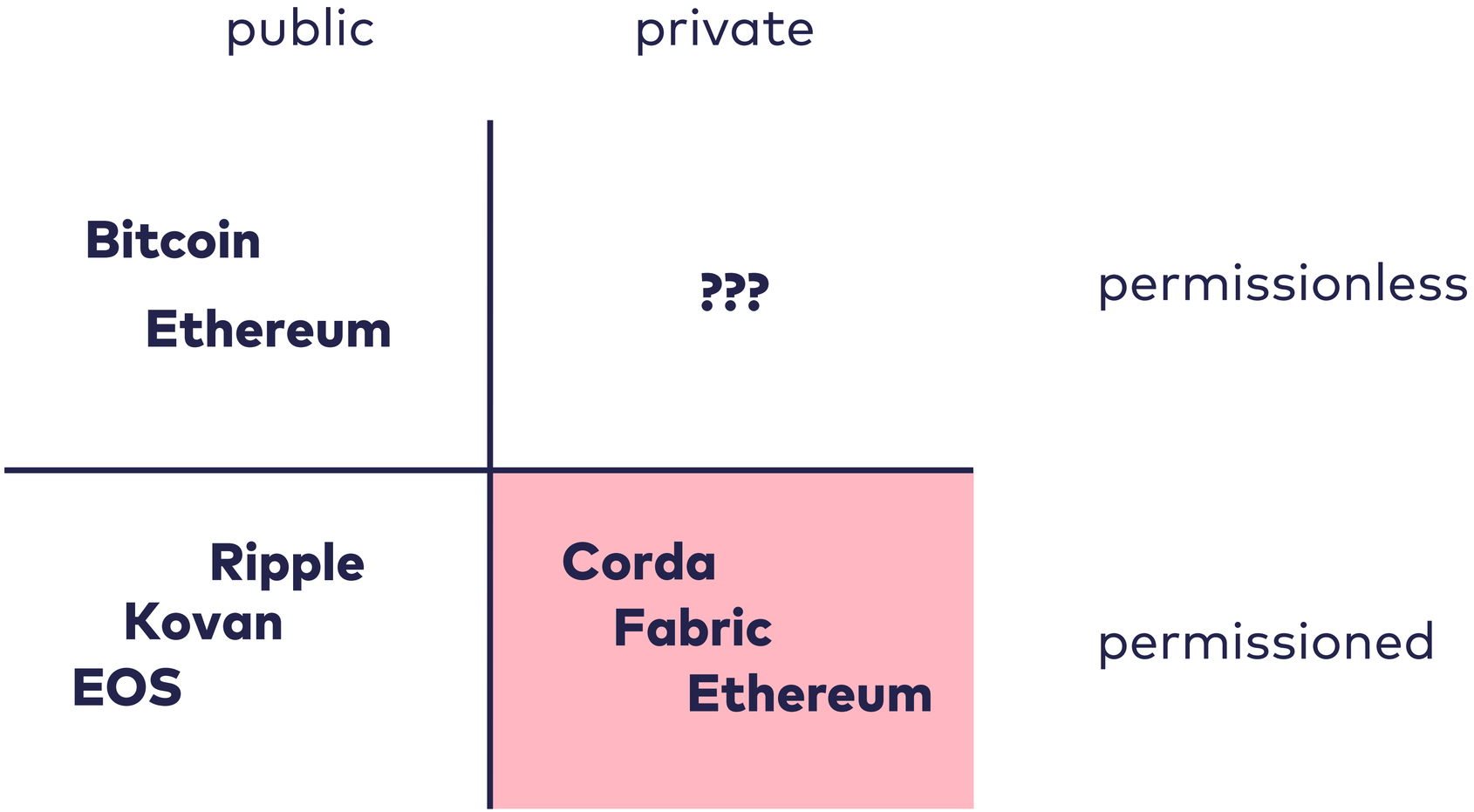
- Public (anyone can read)
- Private (only a set of identified users may read)

Block creation privileges

- Permissionless (anyone can mine)
- Permissioned (only a set of trusted nodes may create blocks)

TeleTrusT-Positionspapier “Blockchain” (2017)

Access control



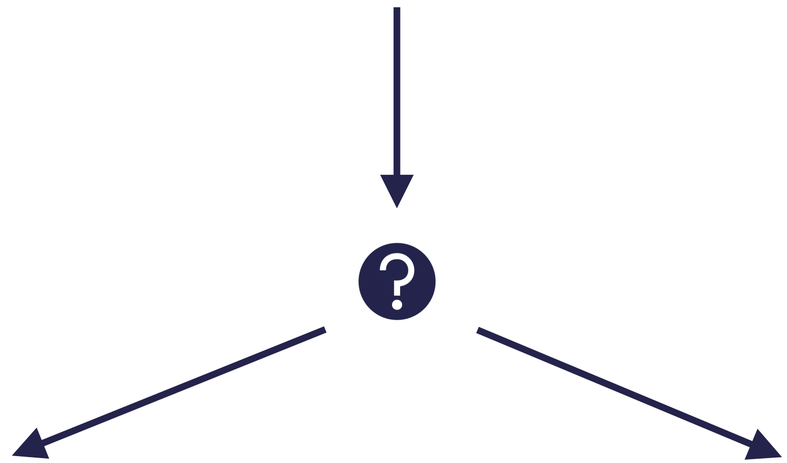
Assessment

Do I need blockchain?

Which blockchain do I need?

The problem with blockchain

Formal description, properties, proofs
Computer science parlance
Formulas and symbols



Actual, real, peer-reviewed, scientific papers

Marketing by (possibly fraudulent) startups/companies; hype-driven

Criterion: Decentralization

No need for blockchain if:

- there is a single trusted organization
- you trust it to not be malicious
- you trust in its competency and security practices
- you trust in its longevity

Criterion: History

No need for blockchain if:

- you trust available information to be correct
- you trust it has not been tampered with
- you trust it is complete

Criterion: Access

No need for proof of work if:

- you control who participates
- there is a separate onboarding process

Criterion: Identity

No need for proof of work if:

- participants are who they say they are
- participants have the authority to do what they do
- there is a trusted arbitrator

Criterion: Processes

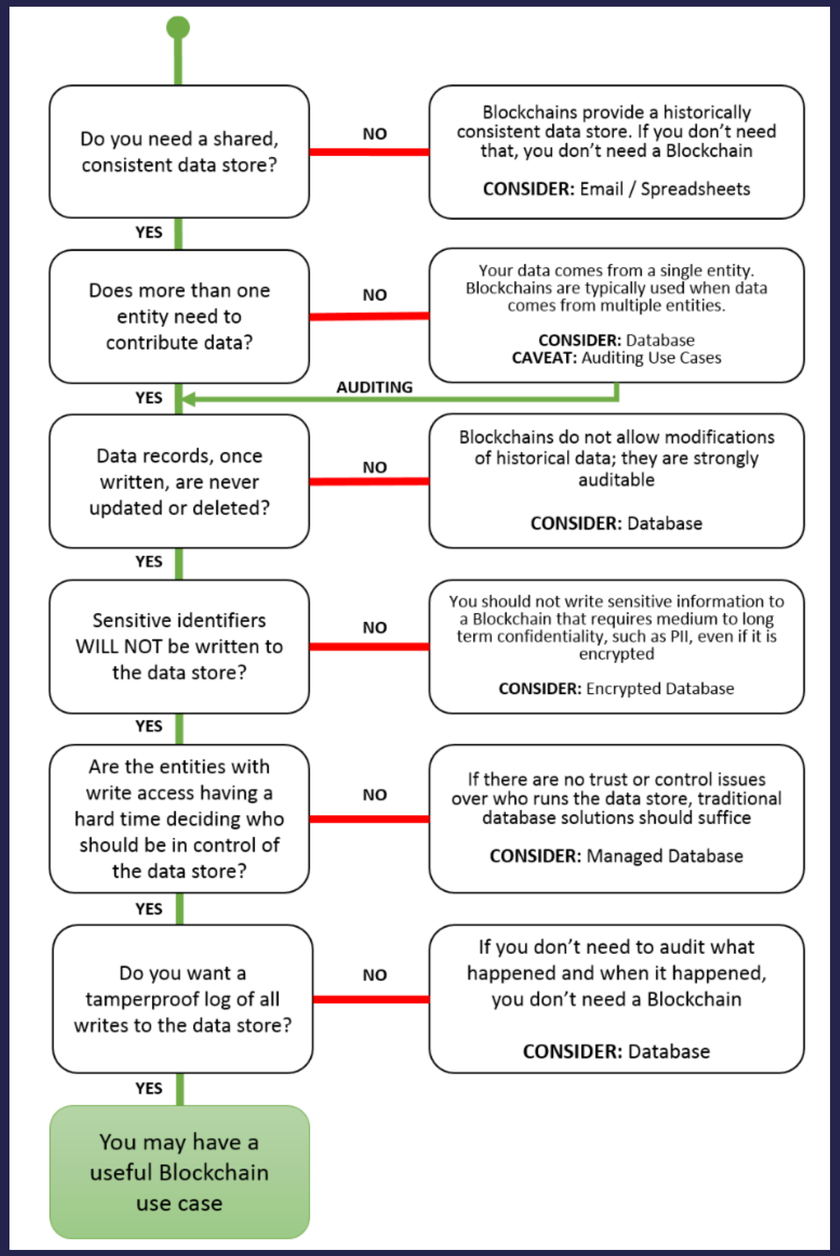
No need for smart contracts if:

- computation follows the expected rules
- you trust code is correct
- you trust code has not been tampered with

Criterion: Privacy

No legal standing for a public blockchain if:

- some or all of the data is supposed to be private
- some or all of the data is supposed to be visible to a subset of users
- pseudonymity is not sufficient

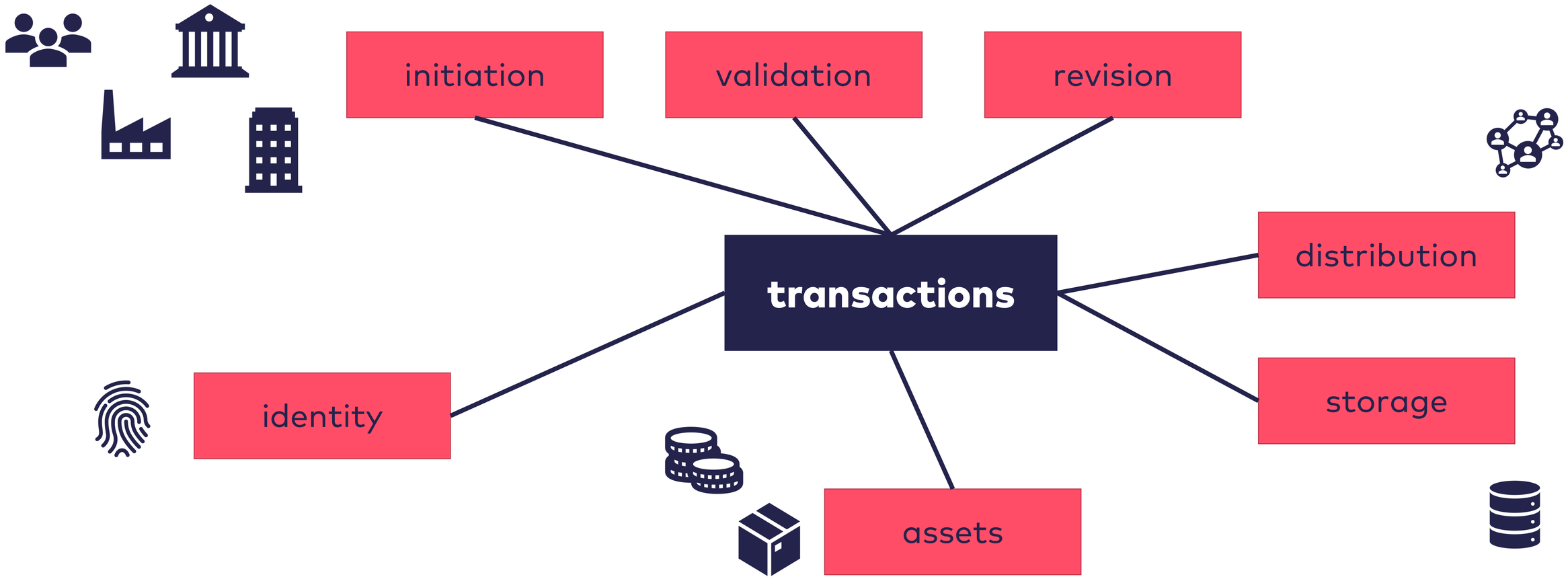


National Institute of Standards and Technology, NISTIR 8202

Business modelling
How do I implement a blockchain?

Guidelines for modelling

Identify entities involved in a blockchain:



Examples

Where could I use blockchains?
Where shouldn’t I?

Non-profits

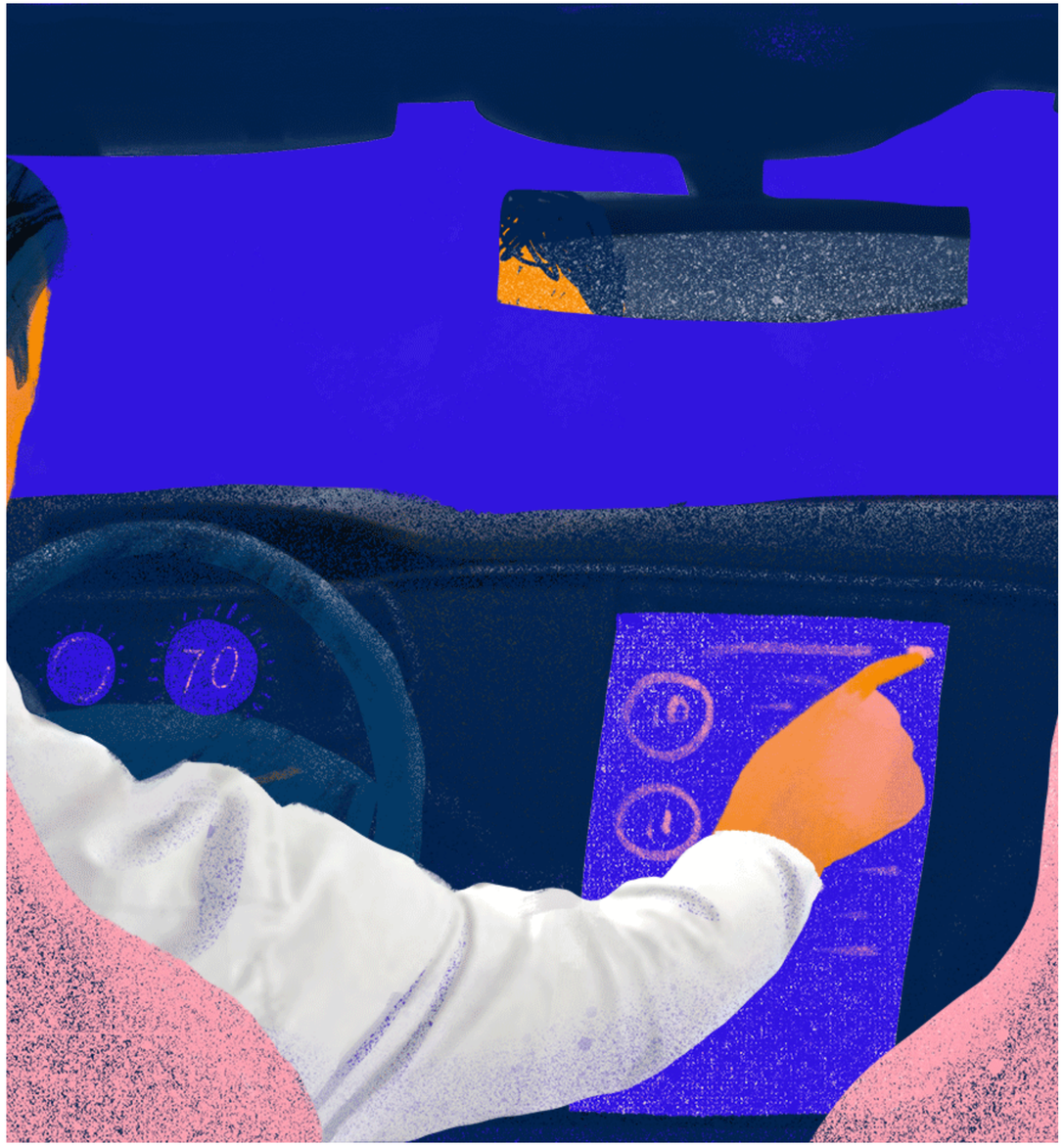
- non-profits and charities need to prove that donations are handled properly
- minimal administrative and financial overhead
- transparent cashflow and accounting
- existing certifications demand high level of transparency & provide guidance for donors

Merchants

- Germany has a strong cash payment culture
- impossible to trace cashflow: good for customers, bad for tax authorities
- legislation demands immutable accounting records at point of sale
- cash register manipulations are common
- difficult to implement

Property

- sales of used cars are fraught with problems
- relevant information like previous accidents, mileage, or modifications may not be obvious to buyer
- tracking of sales is important for legal reasons
- also applies to other types of regulated property such as real estate



Innovation

- proving knowledge of an idea without revealing it is difficult
- national (or international) patent offices check novelty and assign protection
- patent system heavily misused (“patent trolls”)

Education

- the iSAQB e.V. provides an organizational and curricular framework for software architecture education
- multiple independent companies may offer training and examination
- certificates are interchangeable

iSAQB certified training "Distributed Consensus"

15% off with code BLOCKCHAINUSE15

https://www.innoq.com/en/trainings/blockchain-verteilter-konsens/

INNOQ

www.innoq.com

OUR OFFER

Product Development & Design
Software Development & Architecture
Technology Consulting
Infrastructure & Operations
Knowledge transfer, coaching & training

FACTS

~150 Employees
8 locations in
GER & CH
Founded in 1998

FOCUS

Web applications
SaaS
IoT
Self-Contained
Systems

TECHNOLOGIES

(Selection)

Java/Spring
Ruby/Rails
JavaScript
Python
AWS
Kubernetes

CLIENTS

Finance • Telco • Logistics • E-Commerce • Fortune 500 • SMEs • Startups

AXA METRO ebay SOUNDCLOUD VORWERK solarisBank

Get in touch

Dr. Lars Hupel

✉️ lars.hupel@innoq.com

🐦 twitter.com/larsr_h

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim am Rhein
Germany
+49 2173 3366-0

Ohlauer Str. 43
10999 Berlin
Germany
+49 2173 3366-0

Ludwigstr. 180E
63067 Offenbach
Germany
+49 2173 3366-0

Kreuzstr. 16
80331 München
Germany
+49 2173 3366-0

Hermannstrasse 13
20095 Hamburg
Germany
+49 2173 3366-0

innoQ Schweiz GmbH

Gewerbestr. 11
CH-6330 Cham
Switzerland
+41 41 743 0116

Dr. Lars Hupel

Lars is a consultant with INNOQ in Munich, Germany. He is known as one of the founders of the Typelevel initiative which is dedicated to providing principled, type-driven Scala libraries in a friendly, welcoming environment. A frequent conference speaker, he is active in the open source community, particularly in Scala. He also enjoys programming in and talking about Haskell, Prolog, and Rust.