Synergie von DLT und IOT: Anforderungsanalyse und praktische Verprobung

Masterarbeit von Sebastian Kanz

April 2020

Gliederung

1 EINLEITUNG

2 THEORETISCHE GRUNDLAGEN

3 METHODIK & UMSETZUNG

4 ERGEBNISSE

5 AUSBLICK

6 DISKUSSION

Einleitung

Motivation

These

IOT-Anwendungsfall: Pay-As-You-Use

Einleitung
Motivation

500 Mrd.

IOT-DEVICES BIS 2035 [1]

IOT
GROßES POTENTIAL

IOT
VIELE STAKEHOLDER

BLOCKCHAIN-TECHNOLOGIE ALS ENABLER?

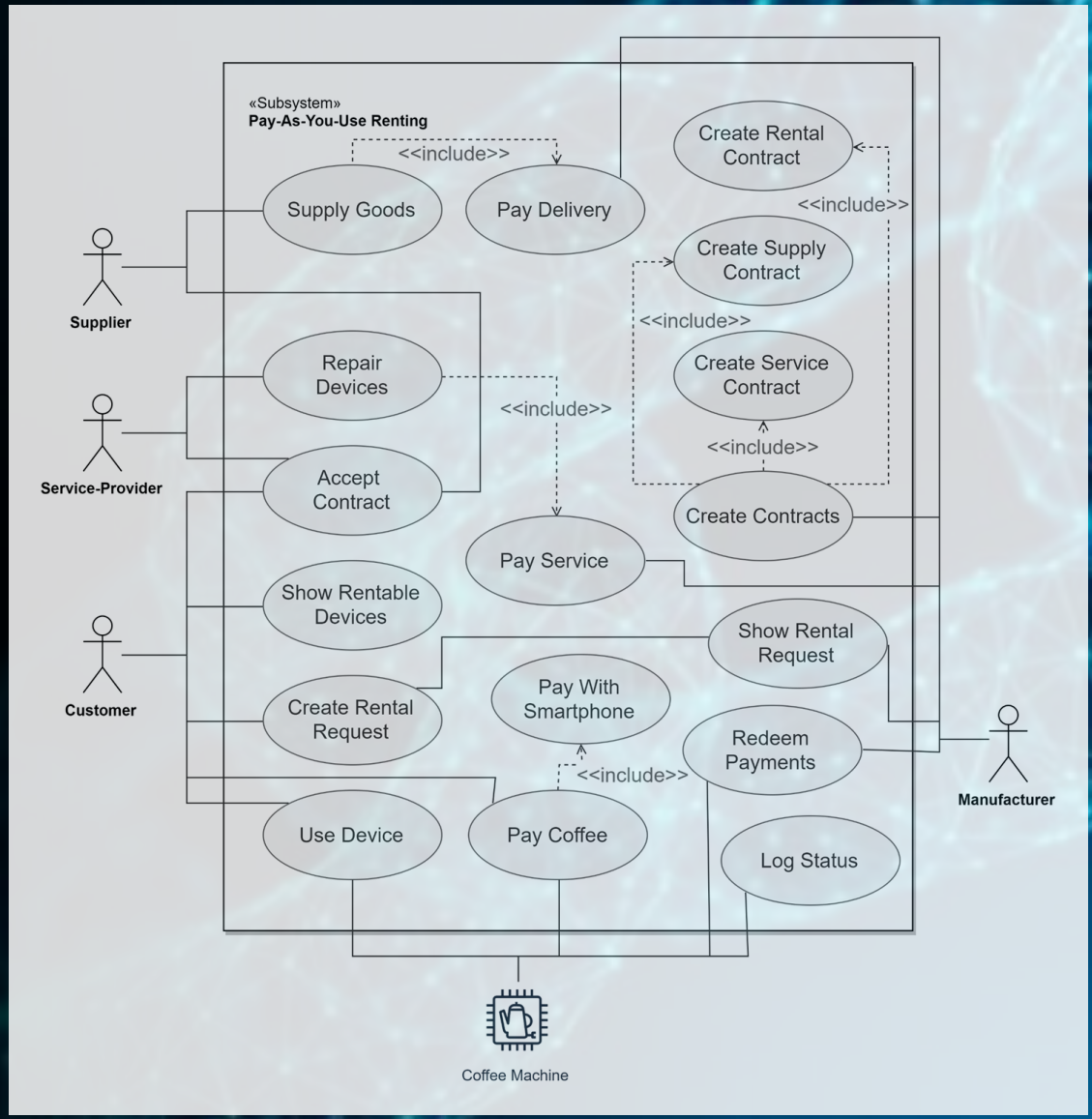
Einleitung
These

„DLT eignet sich als Technologie für IOT und die nicht-funktionalen Anforderungen sind für alle DLT-IOT-Anwendungsfälle gleich.“

Einleitung

IOT-Anwendungsfall: Pay-As-You-Use

- Vermietung von Kaffeemaschinen über eine einheitliche Plattform
- Abbildung und automatische Prozessierung von Miet-, Service- und Lieferverträgen
- Prepaid-Guthaben kann durch den Kunden per Smartphone an der Kaffeemaschine eingelöst werden



Theoretische Grundlagen

Distributed Ledger Technologies

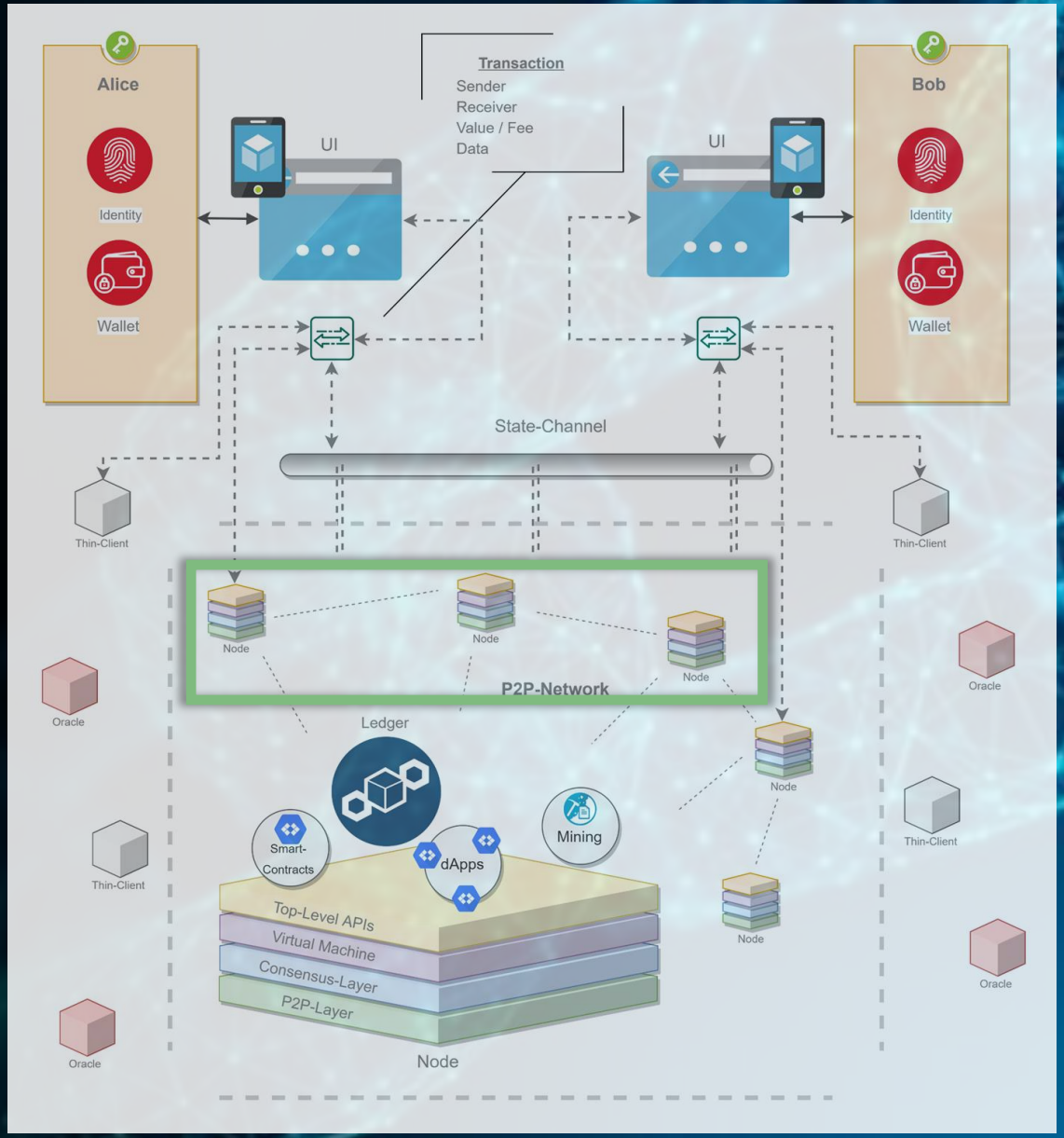
Internet of Things

Theoretische Grundlagen

Distributed Ledger Technologies

Kernelemente im Kontext dieser Arbeit

- **P2P-Netzwerk von Nodes**

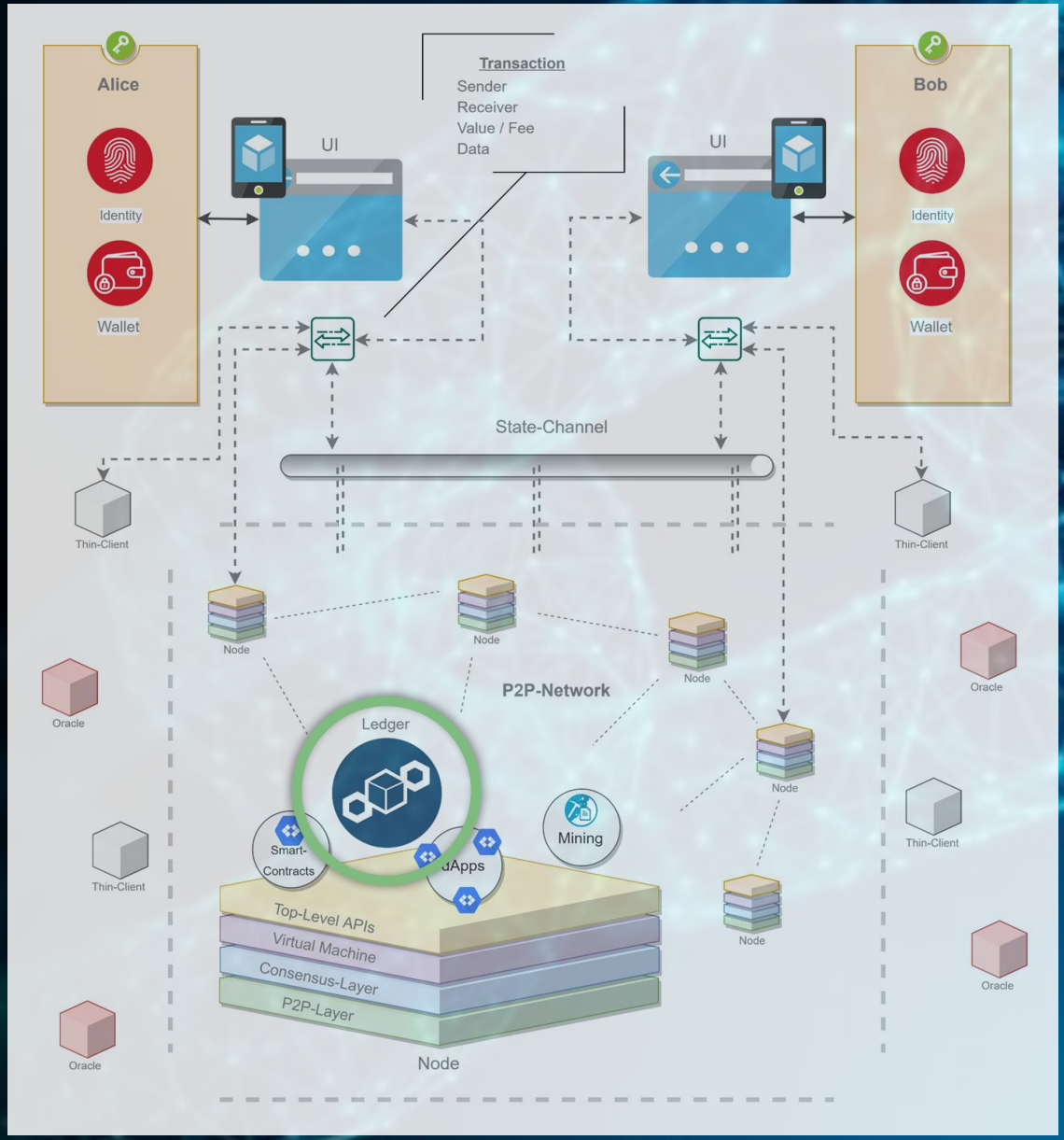


Theoretische Grundlagen

Distributed Ledger Technologies

Kernelemente im Kontext dieser Arbeit

- P2P-Netzwerk von Nodes
- **Zentraler Ledger**

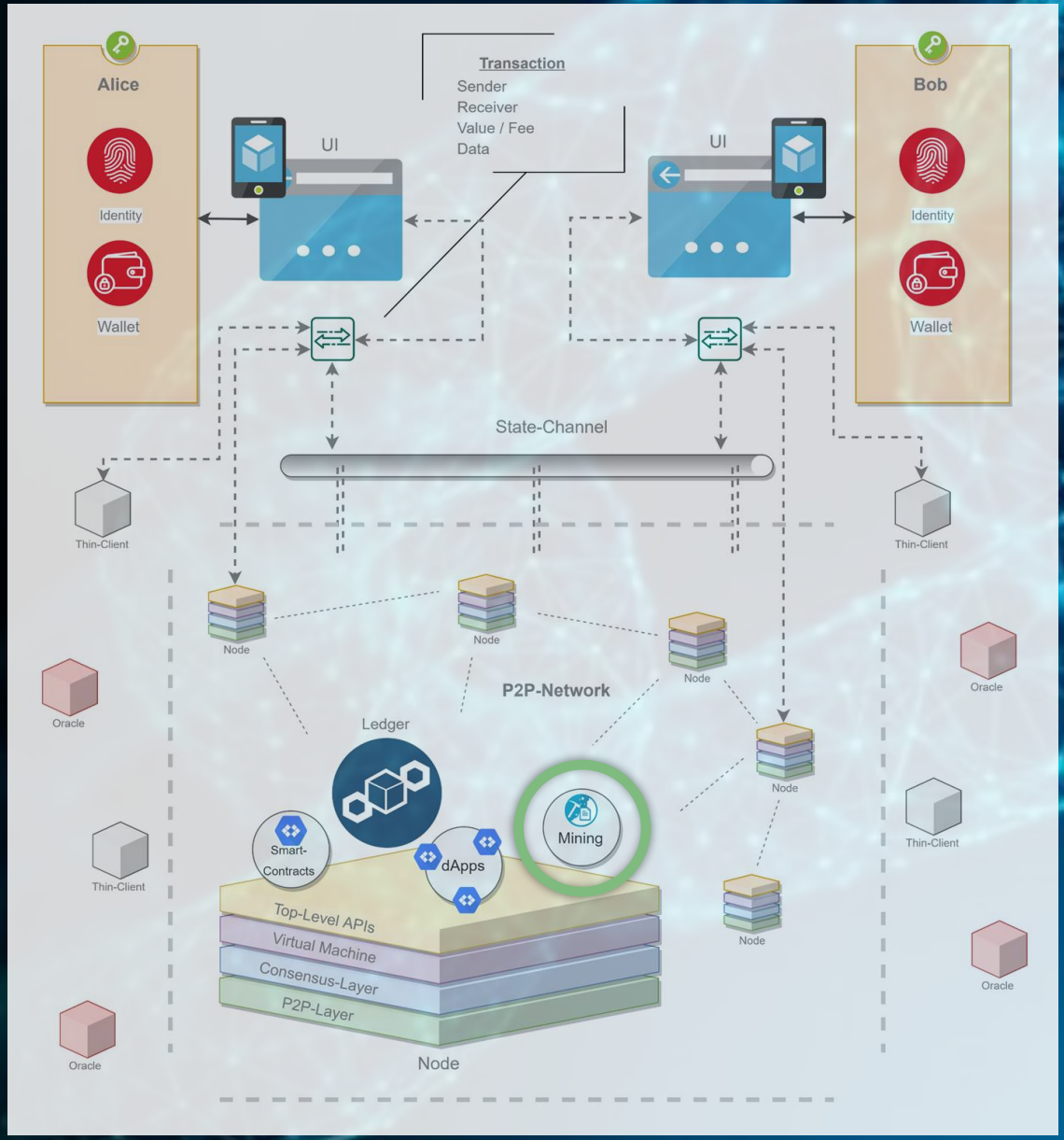


Theoretische Grundlagen

Distributed Ledger Technologies

Kernelemente im Kontext dieser Arbeit

- P2P-Netzwerk von Nodes
- Zentraler Ledger
- **Konsensprotokoll**

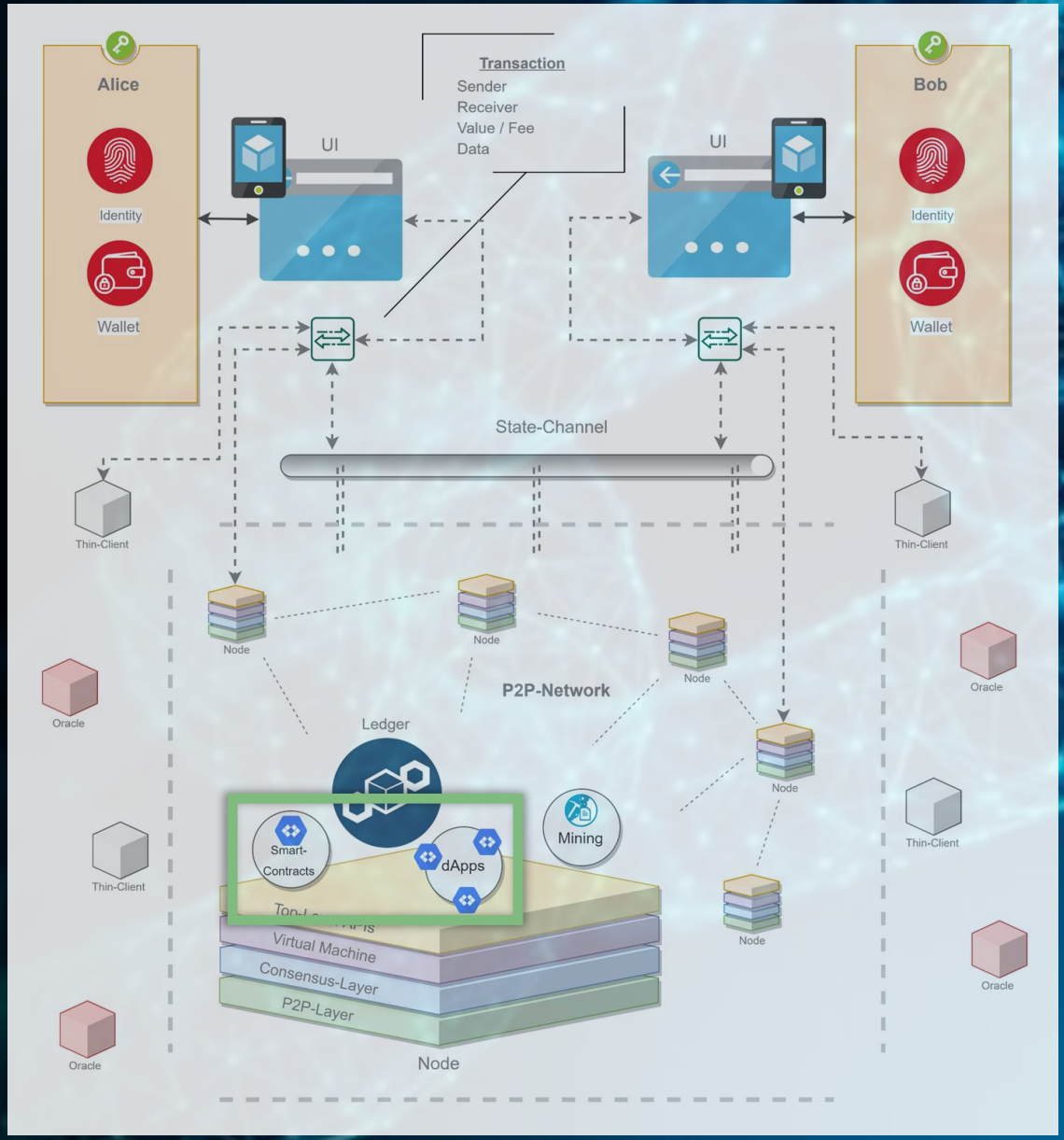


Theoretische Grundlagen

Distributed Ledger Technologies

Kernelemente im Kontext dieser Arbeit

- P2P-Netzwerk von Nodes
- Zentraler Ledger
- Konsensprotokoll
- **Smart-Contracts & dApps**

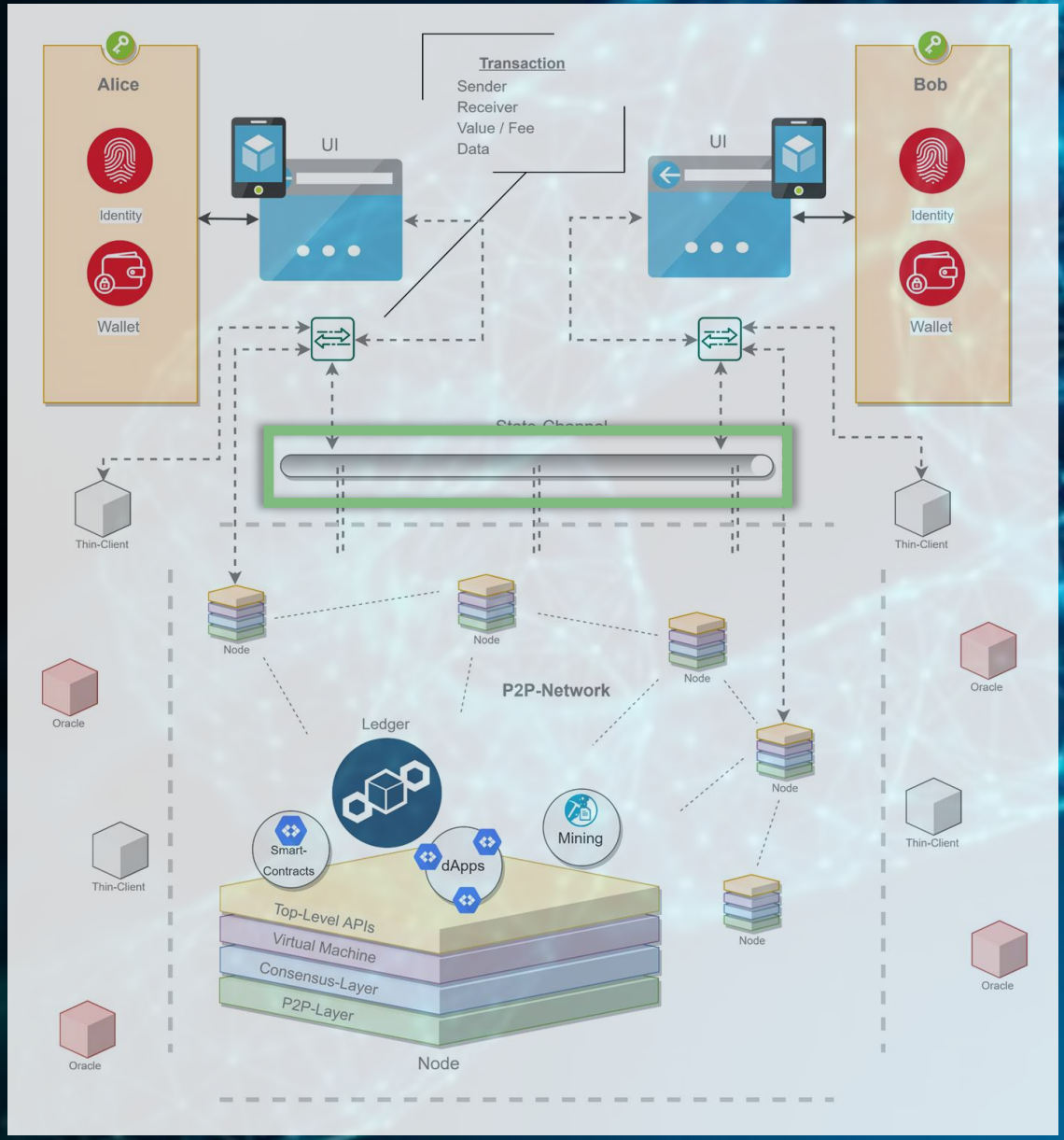


Theoretische Grundlagen

Distributed Ledger Technologies

Kernelemente im Kontext dieser Arbeit

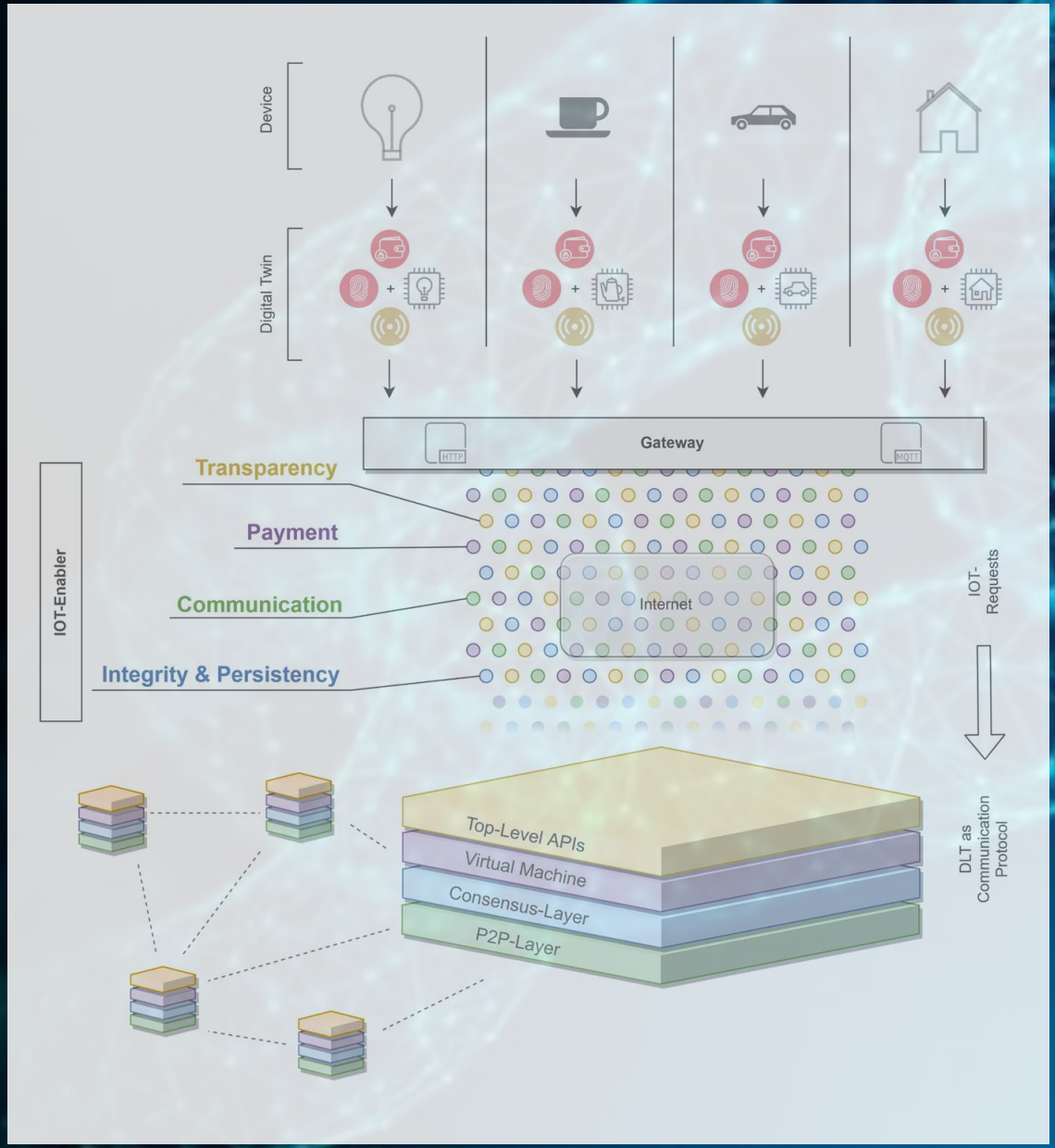
- P2P-Netzwerk von Nodes
- Zentraler Ledger
- Konsensprotokoll
- Smart-Contracts & dApps
- **State-Channel**



Theoretische Grundlagen

Internet of Things

- Digital Twin
  - Identitiy
  - Wallet
  - Sensor / Actor
  - Logic



Methodik & Umsetzung

Anforderungsevaluierung

Auswahl relevanter DLTs

Implementierung

State-Channel

Methodik & Umsetzung

Die Anforderungsevaluierung bestätigte einen gemeinsamen Technologiekontext.

1. Standards & Normen evaluieren
2. Klassifizierungsmodell ableiten
3. Anforderungsanalyse durchführen
4. DLT-Relevanz prüfen
5. Anforderungen transferieren auf DLT

Ergebnis (Anforderungen an DLT im Kontext IOT):

- Smart-Contracts
- Oracle-Services
- Zahlungsmittel
- Asynchronität
- Performanz
- Verschlüsselung

Methodik & Umsetzung

Die Implementierung wurde auf Basis von Ethereum umgesetzt.

Zugrundliegende Kriterien

- Business Relevance [2]
- Github Activity [3]
- Blockchain Activity [4]
- IOT Suitability [5]

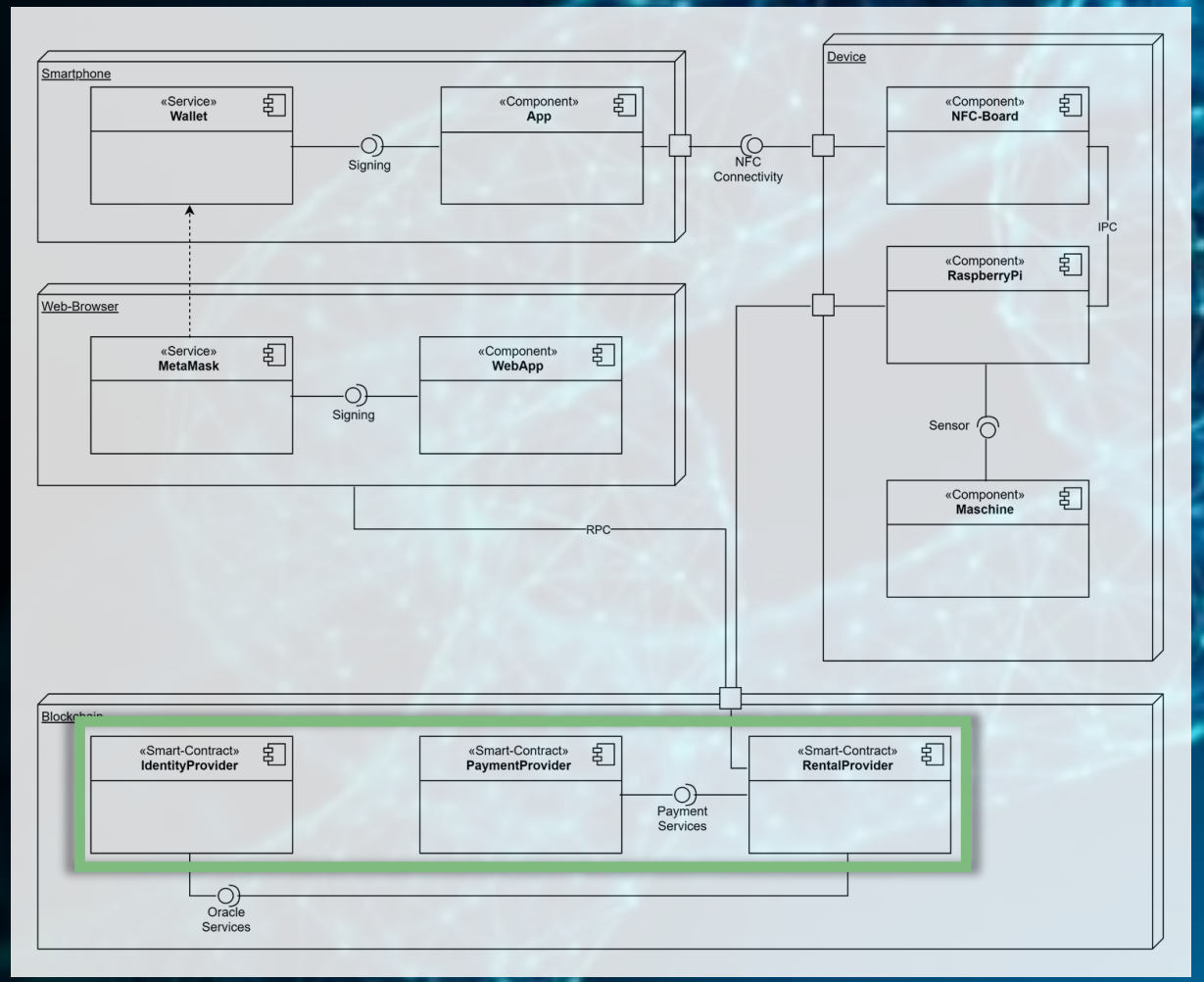
	Smart-Contracts	Payment	Oracle-Services	Perf (TPS)	Async.	Tx Encrypt.
Bitcoin	(yes)	yes	(yes)	<10	yes	no
BitcoinCash	(yes)	yes	(yes)	<100	no	no
Corda	yes	(yes)	yes	~1.000	yes	yes
EOS	yes	yes	yes	>1.000	yes	no
Ethereum	yes	yes	yes	>10	yes	yes
Hyperledger	yes	(yes)	yes	-	yes	yes
IOTA	no	yes	no	>100	yes	yes
Quorum	yes	yes	yes	<1.000	yes	yes
Ripple	no	yes	no	>1.000	yes	no
Stellar	yes	yes	(yes)	>1.000	yes	no
Tron	yes	yes	yes	<1.000	yes	no

Methodik & Umsetzung

Die Anwendung profitiert von einem modernen Technologie-Stack.

Eingesetzte Technologien

- **Solidity Smart-Contracts**

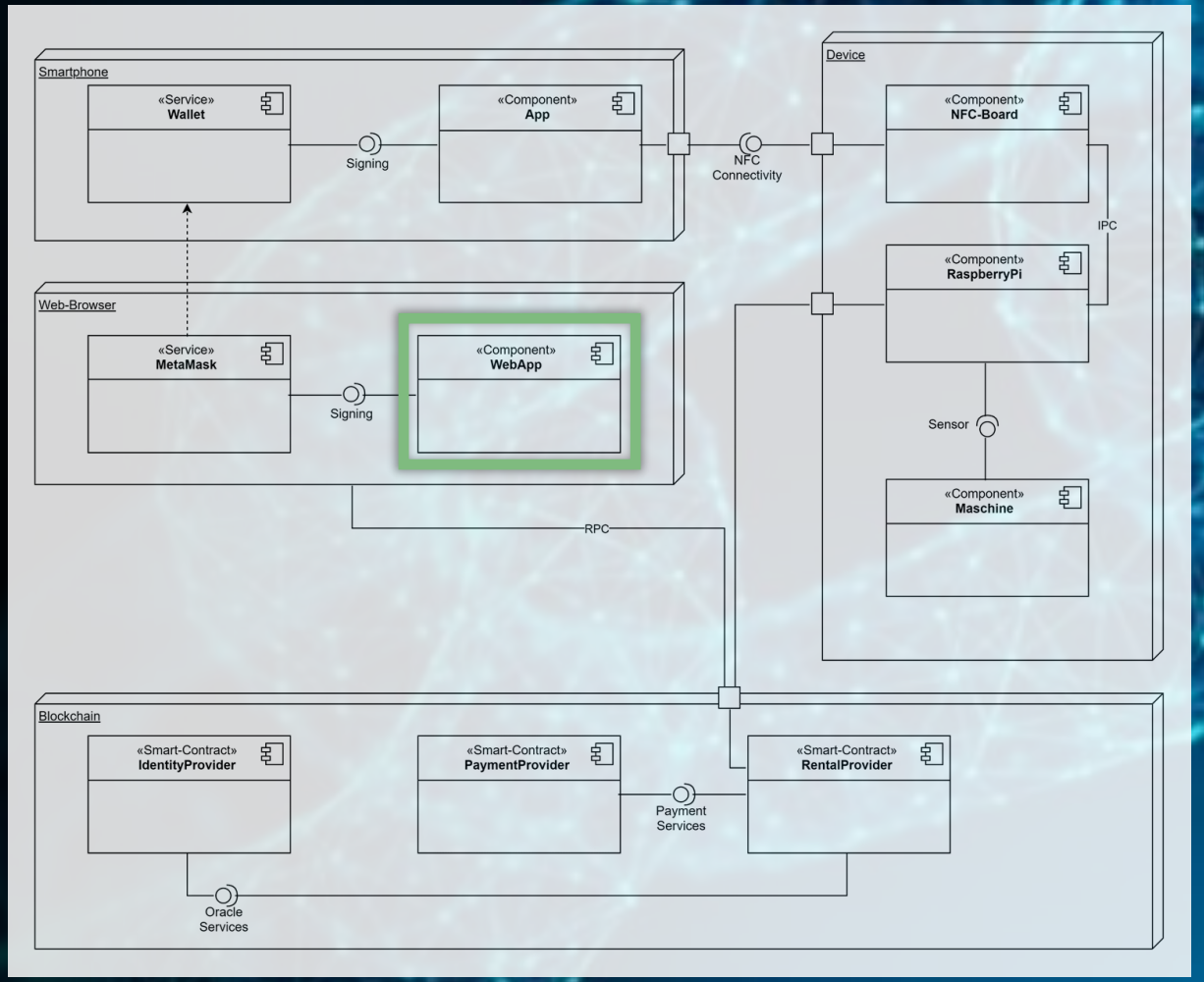


Methodik & Umsetzung

Die Anwendung profitiert von einem modernen Technologie-Stack.

Eingesetzte Technologien

- Solidity Smart-Contracts
- **ReactJS Web-App**

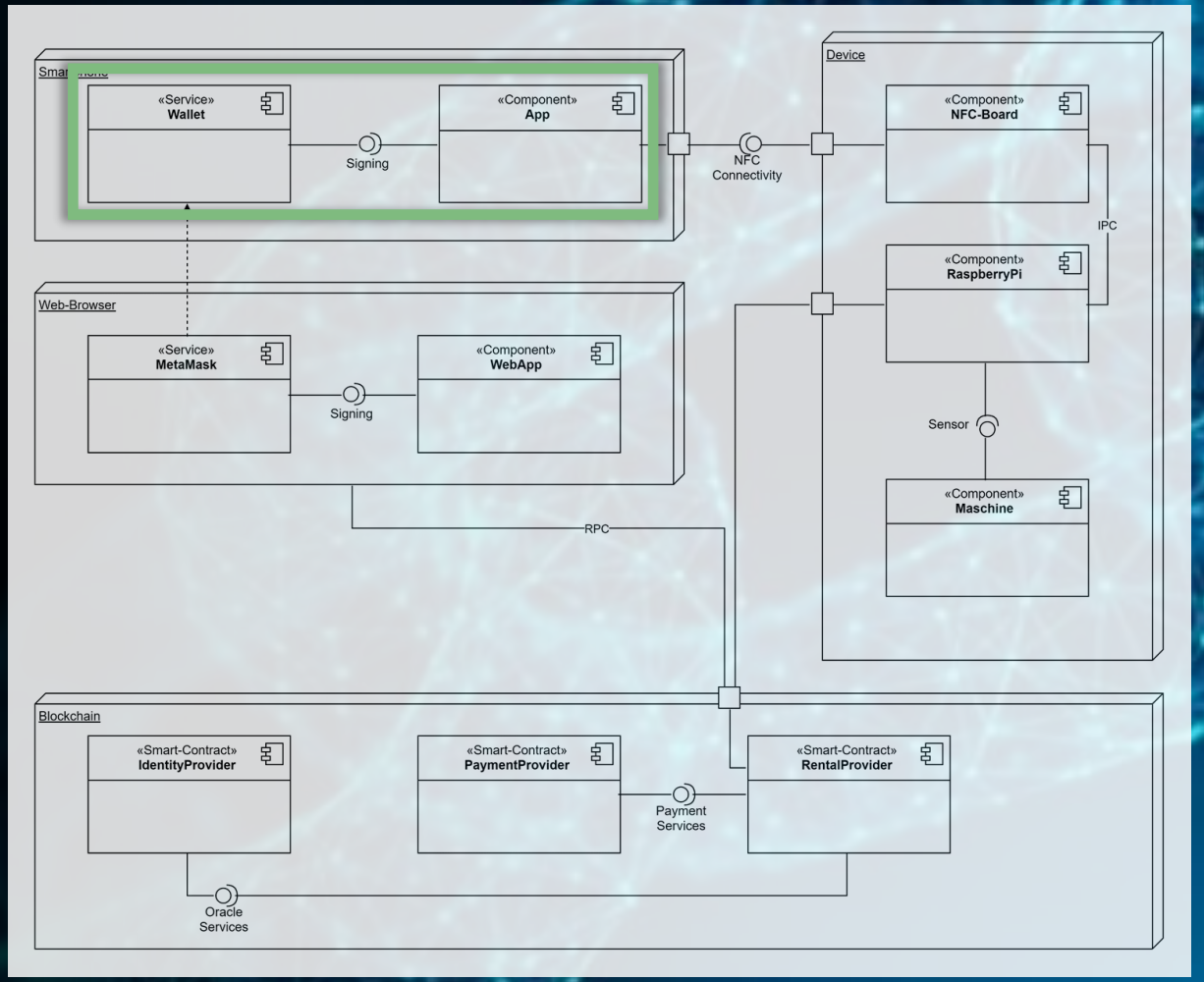


Methodik & Umsetzung

Die Anwendung profitiert von einem modernen Technologie-Stack.

Eingesetzte Technologien

- Solidity Smart-Contracts
- ReactJS Web-App
- **Android Wallet-App**

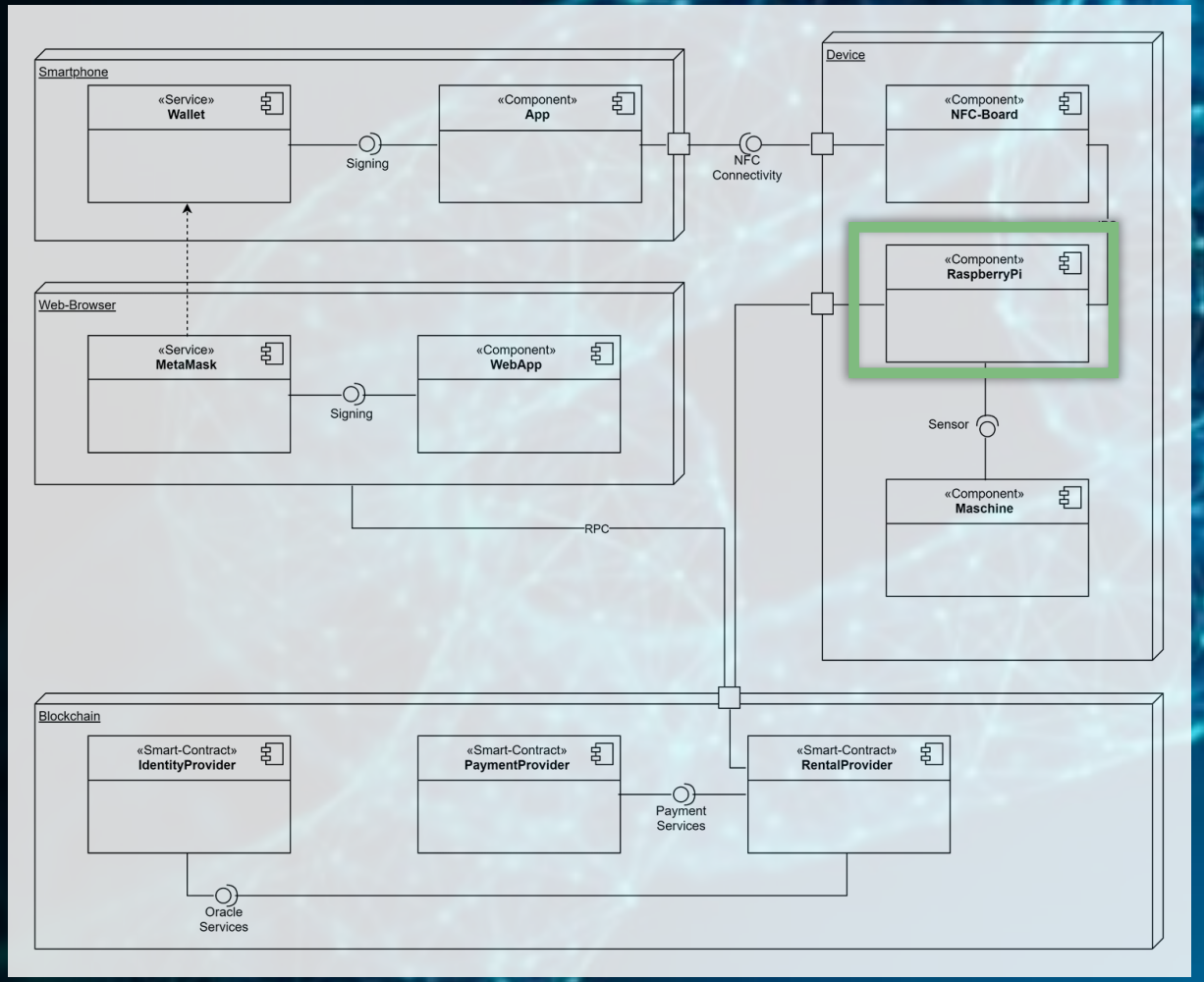


Methodik & Umsetzung

Die Anwendung profitiert von einem modernen Technologie-Stack.

Eingesetzte Technologien

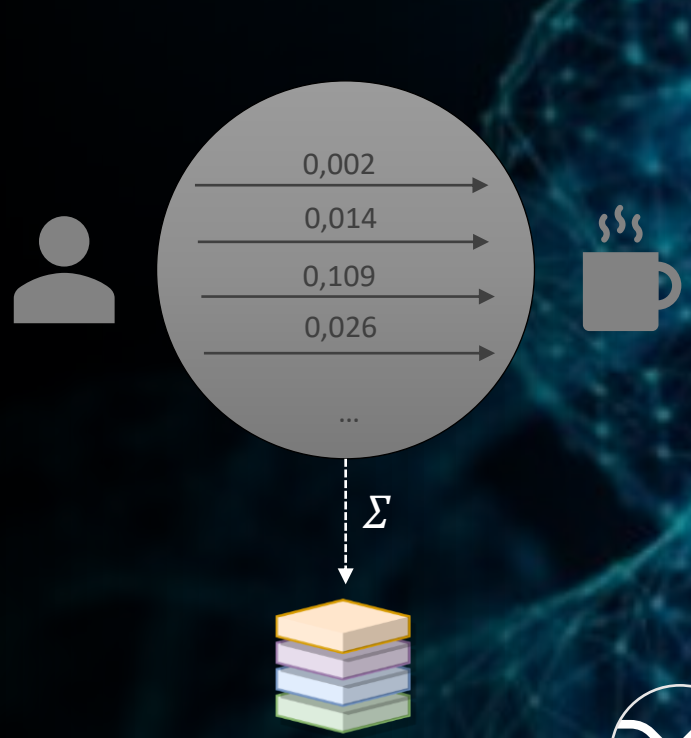
- Solidity Smart-Contracts
- ReactJS Web-App
- Android Wallet-App
- **NodeJS / C-Backend (Kaffeemaschine)**



Methodik & Umsetzung

State-Channel sind eine mögliche Antwort auf das Skalierungsproblem von Blockchains.

- 2,5 * 40 * 10.000 = 1.000.000 Transaktionen pro Tag (11,6 TPS)
- Asynchronität führt zu Offline-Fähigkeit
- Umsetzung mittels Smart-Contract („One-way Payment-Channel“)
- Ergebnis: 20.000 Transaktionen pro Woche (2858 Transaktionen pro Tag, bzw. 0,03 TPS)



Ergebnisse

Anforderungserfüllung

Fazit

Demo

Ergebnisse

Die Umsetzung war ein Erfolg.

- Instantane Transaktionen (1,3 TPS in der Endausbaustufe)
- Jährlicher Umsatz von 82.000.000 € bei jährlichen Transaktions-kosten von 78.000 €
- POC erfolgreich umgesetzt
- schnelles Prototyping durch das „Kommunikationsprotokoll Blockchain“

Fazit

Die Ergebnisse bestätigen die These.

Kernaussagen

(1) IOT kann von DLT profitieren.

(2) Ein Prototyp wurde erfolgreich umgesetzt…

(3) … und damit die Machbarkeit des Anwendungsfalls nachgewiesen.

DLT eignet sich als Technologie für **dezentrale und asynchrone** IOT-Anwendungsfälle…

…, **an denen mehrere, sich gegeneinander nicht vertrauende Parteien teilnehmen**…

…und **die Basis** aller nicht-funktionalen Anforderungen ist für alle DLT-IOT-Anwendungsfälle gleich.

Ergebnisse

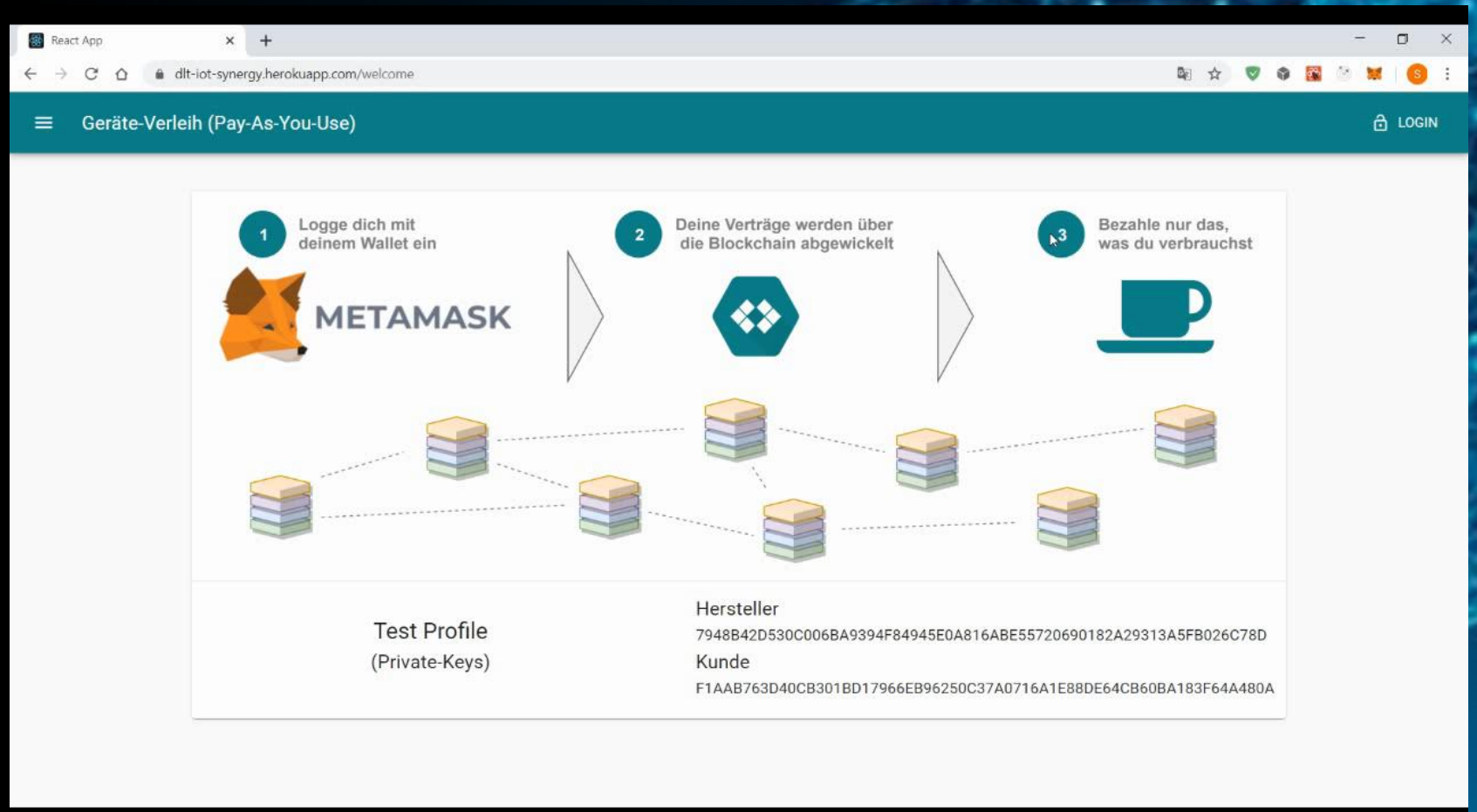
Demo

(1) Initiale Vertragserstellung

(2) Prepaid-Guthaben aufladen

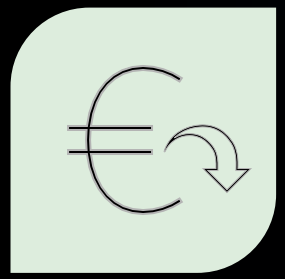
(3) Bezahlung von Kaffee mittels Smartphone

(4) Bezahlungen verrechnen



Ausblick

Ausblick
Future Work



- Offchain Funktionalität (z.B. IPFS)
- Proxy Smart-Contracts zur Verlagerung

- Zero-Knowledge Proofs (z.B für Kaffeekonsum, Quittungen, etc.)
- Onchain Wallets mit Guardians zur Key-Recovery

Diskussion

Fragen?

Anmerkungen?

Quellen

[1] Cisco. Internet of Things. 2016. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glancec45-731471.pdf (Stand: 22.04.2020)

[2] Michael del Castillo. “Blockchain 50: Billion Dollar Babies”. In: Forbes (2019). https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/#6dfb0c0657cc (Stand: 22.04.2020)

[3] Github Activity, Coincodecap, https://coincodecap.com/coins und https://www.cryptomiso.com/ (Stand: 29.12.2019)

[4] Blockchain Activity, https://blocktivity.info/ (Stand: 31.12.19)

[5] Suitability, https://cryptoslate.com/cryptos/iot (Stand: 30.12.19)

Alle Grafiken wurden vom Autor selbst entworfen.

Icons: https://thenounproject.com/

Hintergrundbild: https://www.tradearena.cz/obrazek/5c332920d59b4/blockchain-scm_590x408.jpg

Backup

Backup

Berechnungen & Tabellen

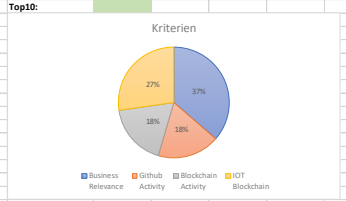
Story	Description	Task	Description	Requirement	Description
Story A1 "Agieren auf Plattform"	"Als Akteur möchte ich in meiner Rolle als [A] auf der Plattform agieren."	Task A1.1	Akteuere können sich an der Plattform registrieren und gemäß ihrer Rolle miteinander agieren.	Requirement A1.1.1	Jeder Akteur auf der Platform kann eindeutig identifiziert werden.
				Requirement A1.1.2	Ein Akteur registriert sich und meldet sich auf der Plattform an, bevor er dort agieren kann.
				Requirement A1.1.3	Ein Akteur agiert immer mit einer bestimmten Rolle auf der Platform: Manufacturer, Customer, Supplier, Service-Provider oder Gerät. Ein Akteur kann mehrere Rollen haben.
				Requirement A1.1.4	Es existiert eine Oberfläche, auf die jeder Akteur Zugriff hat. Dort kann er sich registrieren und anmelden.
				Requirement A1.1.5	Ein Akteur hat eine (mehrere) verifizierte Rolle(n).
		Task A1.2	Akteure können über die Plattform miteinander kommunizieren.	Requirement A1.2.1	Akteure kommunizieren über die Plattform.
				Requirement A1.2.2	Die Kommunikation der beteiligten Akteure wird sofort übermittelt.
				Requirement A1.2.3	Die Kommunikation zwischen den Akteuren ist nachvollziehbar und eindeutig zuordenbar.
				Requirement A1.2.4	Die Kommunikation zwischen den Akteuren kann nicht gelöscht oder manipuliert werden.
				Requirement A1.2.5	Akteure können nur den Inhalt ihrer eigenen Nachrichten einsehen.
				Requirement A1.3.1	Akteure schließen Verträge über die Plattform ab.
				Requirement A1.3.2	Verträge sind rechtlich bindend.
				Requirement A1.3.3	Akteure können Verträge ablehnen oder annehmen.
				Requirement A1.3.4	Es existiert eine Oberfläche, auf die jeder Akteur Zugriff hat. Dort kann er Vertragsanfragen erstellen. Auf der Empfängerseite muss eine Oberfläche existieren, die diese Anfragen anzeigt.
				Requirement A1.3.5	Der Vertragsgegenstand kann nicht durch Dritte manipuliert werden.

Anforderungsauflistung
IOT-Anwendungsfall

	Business Relevan	Github Activit	Blockchain Activit	IOT Blockcha	Total
	2	1	1	1,5	
	forbes	cryptomismo coinzodiacap	blocktivity	cryptolate	
Bitcoin	x	x			3
Bitcoin SV			x		1
BitcoinCash	x	x			3
Cardano		x			1
Corda	x				2
Cosmos		x			1
EOS		x	x		2
Ethereum	x	x	x		4
Hyperledger	x				2
INT Chain				x	1,5
IOST			x		1
IoT Chain				x	1,5
IOTA		x		x	2,5
KIN			x		1
LBRY Credits		x			1
Lisk		x			1
Monero		x			1
Nano			x		1
Particl		x			1
Quorum	x				2
Ripple	x				2
Ruff				x	1,5
SDChain				x	1,5
Steem			x		1
Stellar		x	x		2
Syscoin		x			1
Telos			x		1
Tron		x	x		2
WAVES		x			1
Zcash		x			1

Business Relevance	Wichtigstes Kriterium
Github Activity	Github Activity und Blockchain Activity sind gleich wichtig; Kriterien für Aktivität rund um diese Block
Blockchain Activity	Github Activity und Blockchain Activity sind gleich wichtig; Kriterien für Aktivität rund um diese Block
IOT Blockchain	Wichtiger als Aktivität, nicht so wichtig wie Business Relevance

Top10:



DLT-Auswahl, Kriteriengewichtung

Beschreibung	Anzahl	Einheit		Sender	Transaktion	Einzelkosten GAS	WEI	ETH	Euro	Transaktion	Transaktionen pro Maschine (einmalig) Anzahl
GAS-Price	5	GWEI		Hersteller	Vertrag erstellen	426.609	2.133.045	0,002133	0,42	Vertrag erstellen	1
ETH-Kurs	196,04	Euro			Quittung einlösen	157.927	789.635	0,00079	0,15	Quittung einlösen	0
Anzahl Kaffeemaschinen	10.000	Maschinen	(Annahme)								
Mitarbeiter pro Kaffeemaschine	40	Mitarbeiter	(Annahme)								
Mitarbeiter gesamt	400.000	Mitarbeiter		Kunde	Vertrag anfragen	197.964	989.820	0,00099	0,19	Vertrag anfragen	1
Liter Kaffee pro Jahr pro Person	164	Liter			Vertrag annehmen	162.743	813.715	0,000814	0,16	Vertrag annehmen	1
Tassen Kaffee (0,2l) pro Jahr	820	Tassen			Prepaid aufladen	28.805	144.025	0,000144	0,03	Prepaid aufladen	0
Arbeitstage (abzgl. 30 Tage Urlaub)	230	Tage									
Tassen Kaffee (0,2l) pro Tag	2,24	Tassen									
Prepaid-Guthaben ausreichend für	5	Tage (Arbeitswoche)									
Preis pro Tasse Kaffee	0,25	Euro	(Annahme)								
Umsatzvolumen pro Maschine und Woche	**157,69**										
Prepaid Guthaben pro Maschine aufladen	200	Euro	(Annahme, plus Puffer)								
Gesamtumsatz (jährlich)	**82.000.000**	Euro									
Gesamtumsatz pro Maschine (jährlich)	**8.200**	**Euro**									
	112										
		https://www.lohnsteuer-kompakt.de/faq/0/704/wie_viele_arbeitstage_kann_ich_in_der_steuererklaerung_fuer_fahrtkosten_ansetzen									

Kostenberechnung, IOT-Anwendungsfall

Backup

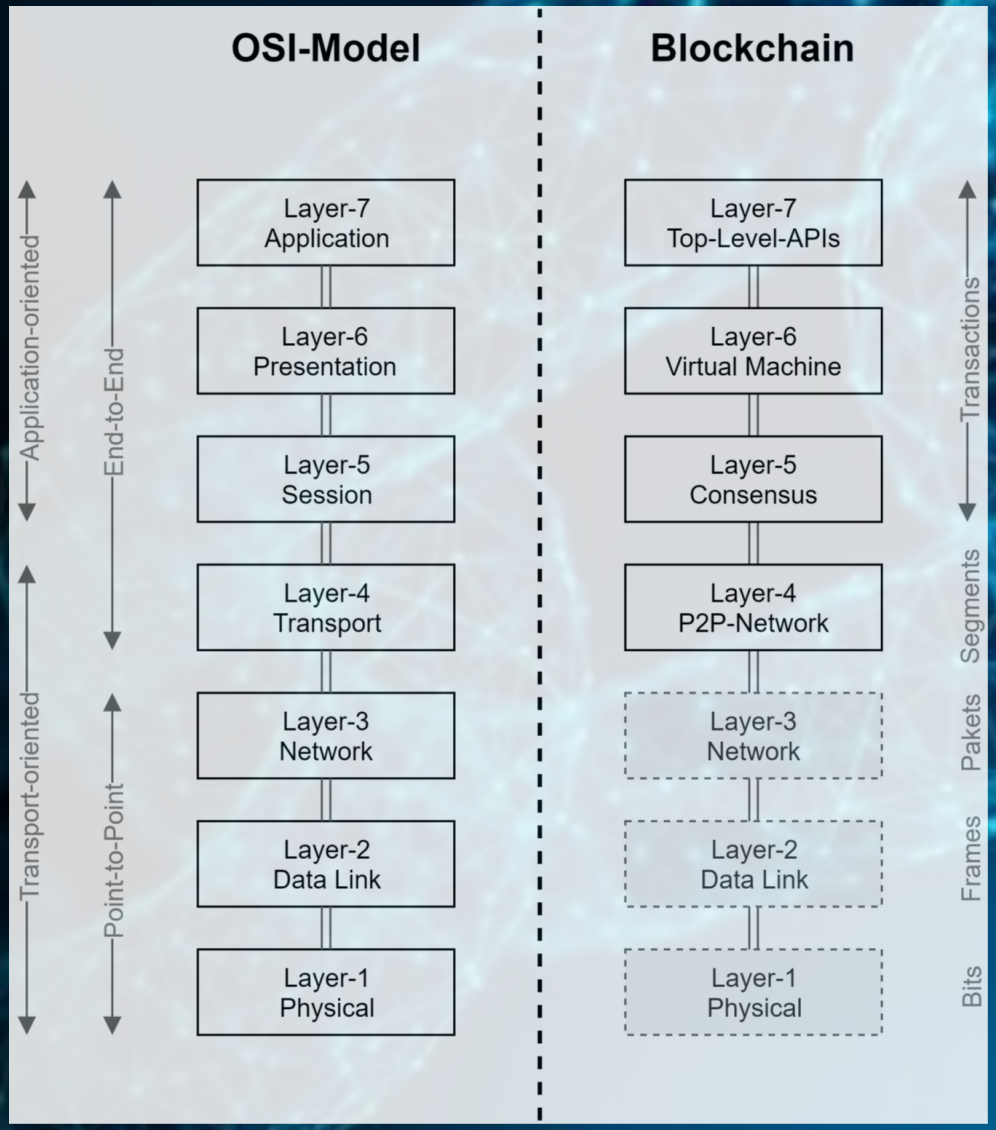
Blockchain als Kommunikationsprotokoll

Protokoll:

„Festlegung von Standards und Konventionen für eine reibungslose Datenübertragung zwischen Computern“ –Duden

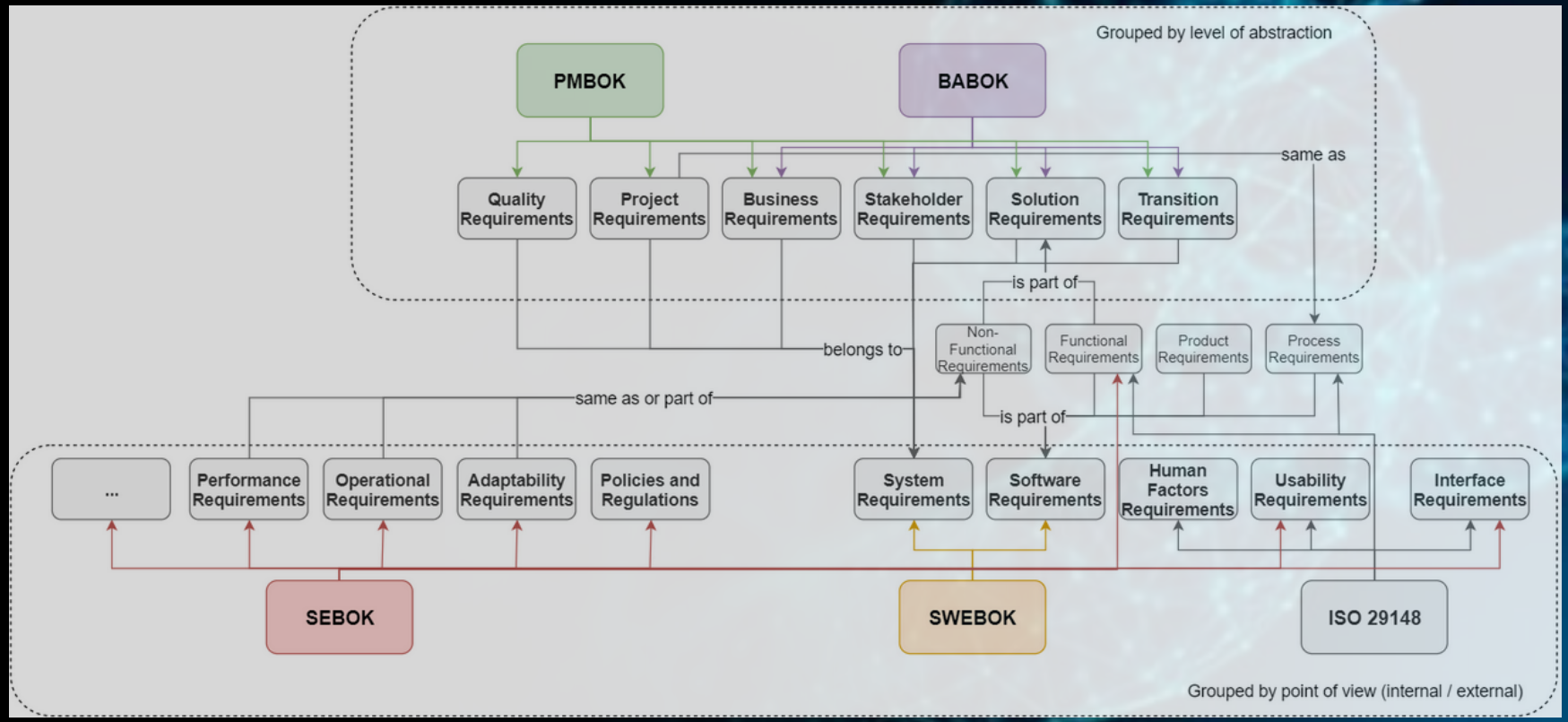
Kommunikationsprotokoll:

„Übermittlungsvorschrift bei der Datenübertragung, die die gesamten Festlegungen für Steuerung und Betrieb der Datenübermittlung in einem Übermittlungsabschnitt [...] umfasst“ – Gabler Wirtschaftslexikon



Backup

Anforderungsklassifizierung – Standards



Backup

Anforderungsklassifizierung – Eigenes Modell