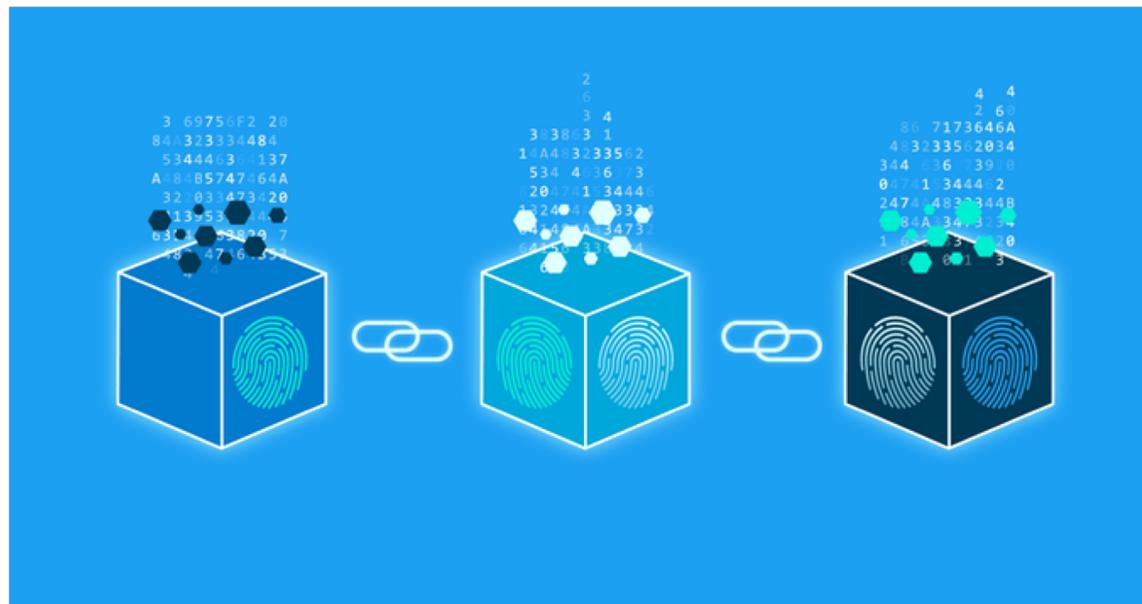


Blockchain: Versprechen und Realität im Gesundheitswesen



Lukas Huber, MSc

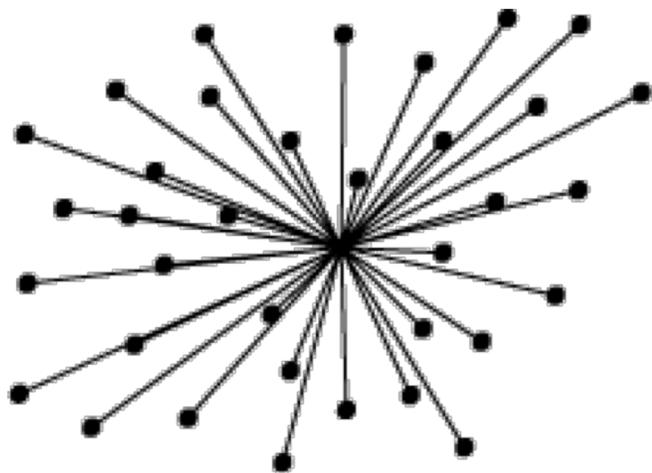
eHealth Research and Innovation Unit,

UNIT - University for Health Sciences, Medical Informatics and Technology, Austria

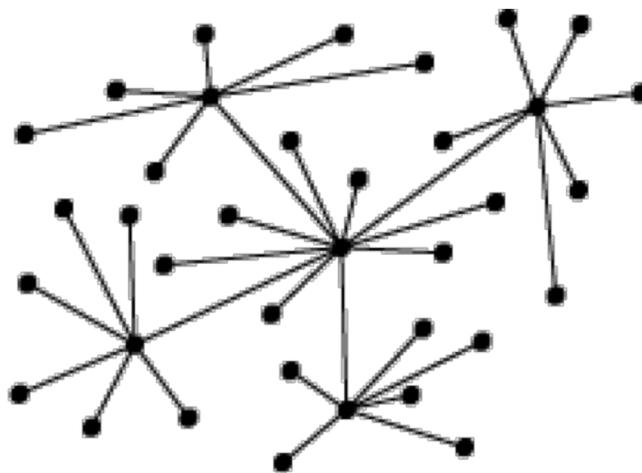
ÖGBMT 2018, Hall in Tirol

<https://empowerpk.org/learn/courses/blockchain-development/>

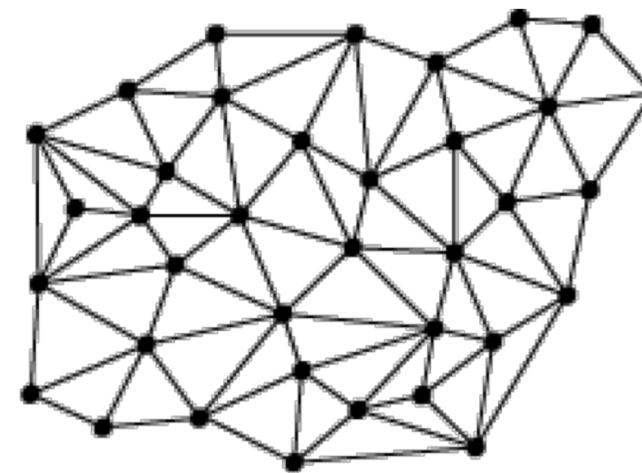
Blockchain - Topologie



centralised



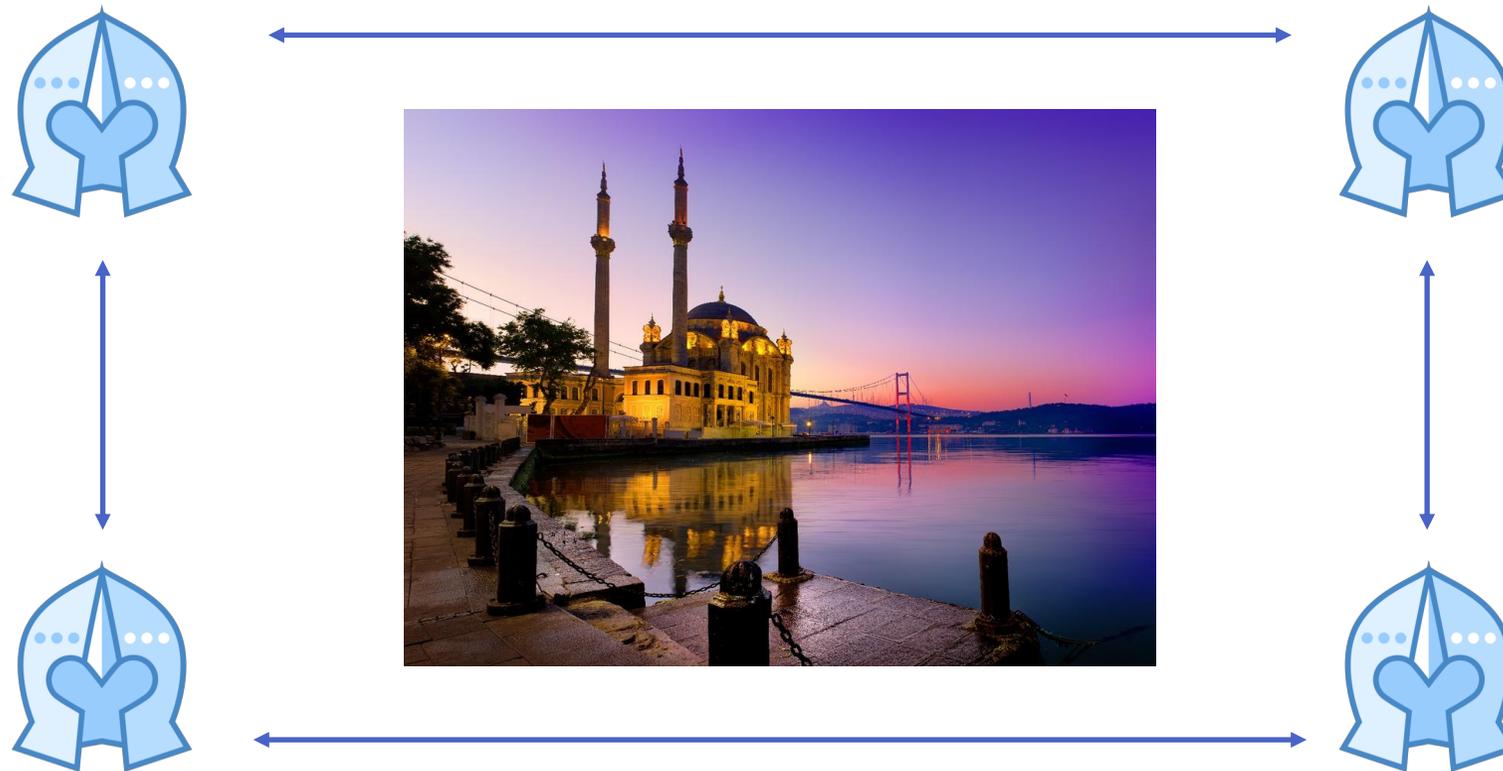
decentralised



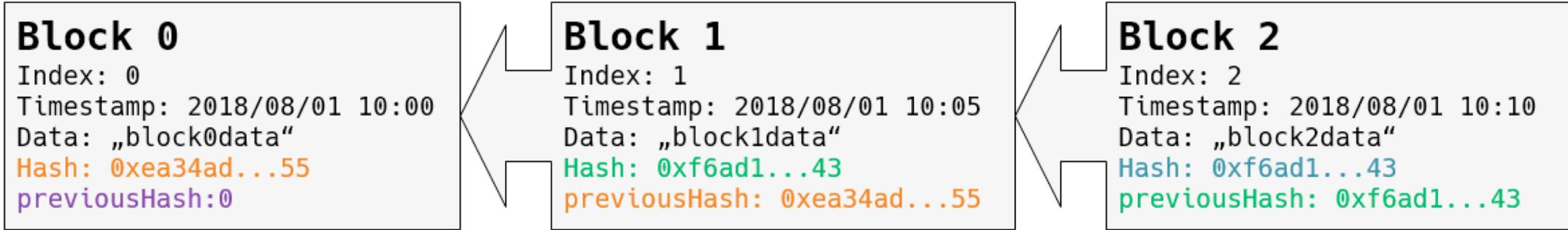
distributed

<https://commons.wikimedia.org/wiki/File:Centralised-decentralised-distributed.png>

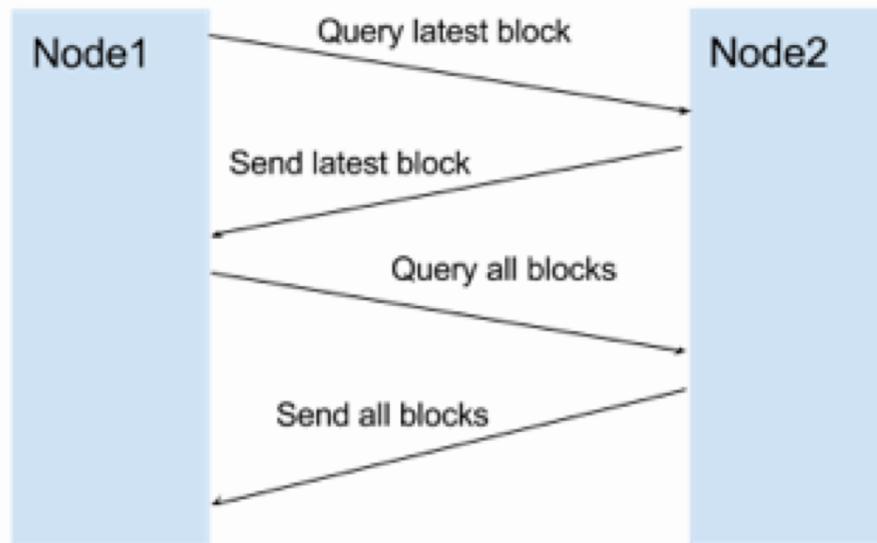
Byzantinische Generäle?



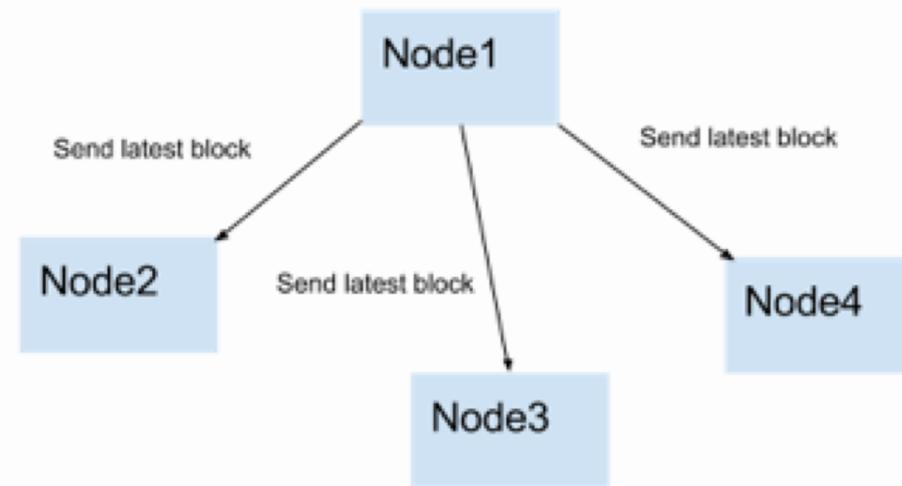
Blockchain - Grundaufbau



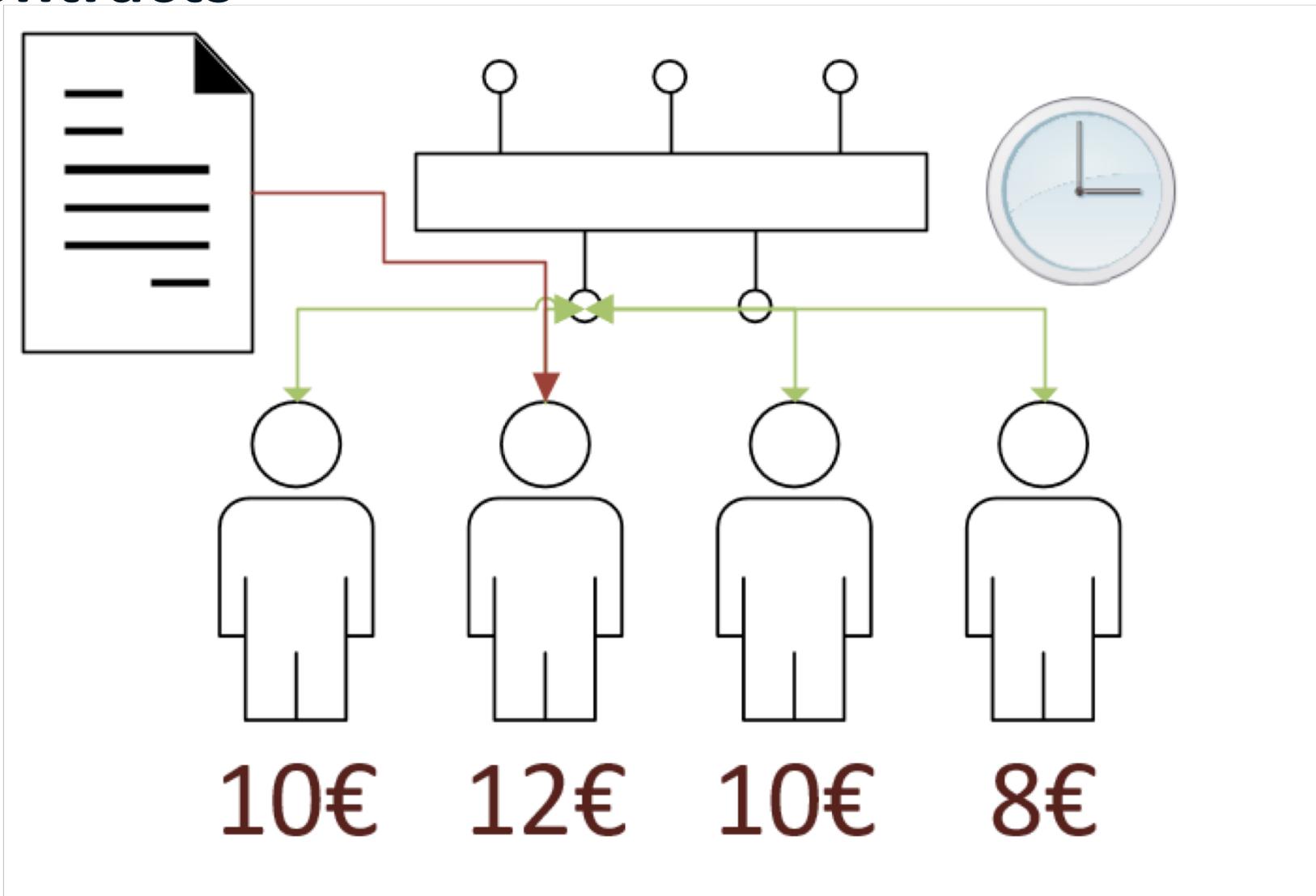
Node1 connects and syncs with Node2



Node1 generates a block and broadcasts it



Smart Contracts





Technologien: Ethereum

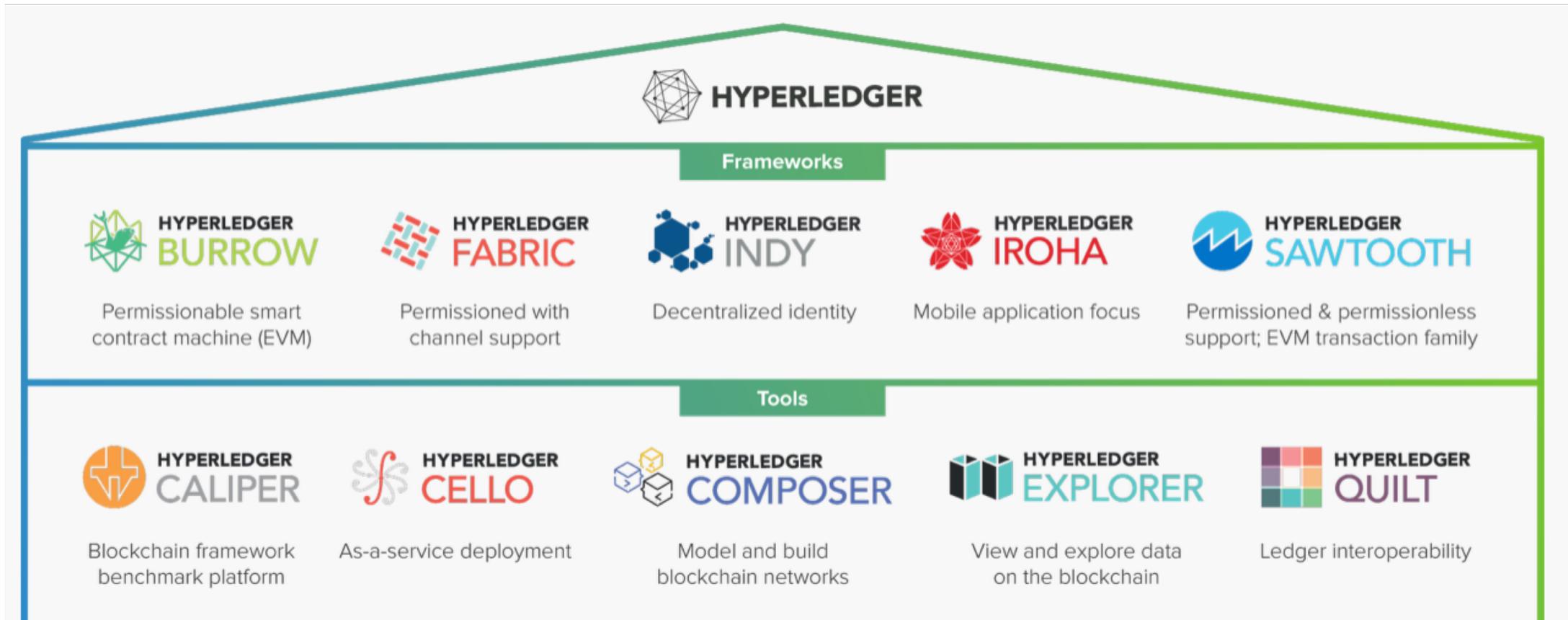


Technologien: Hyperledger



Teil der Linux Foundation

Fokus: Blockchain-Technologien für Business



Standards

Enterprise Ethereum Alliance

- offene, standard-basierte Architektur und Spezifikation zur Verbreitung von Enterprise Ethereum
- **TRUST, PRIVACY & PERFORMANCE**

IEC 62351 Sicherheit in Energiemanagementsystemen

ISO/TC 307 Blockchain and distributed ledger technologies

Deloitte Use Cases:

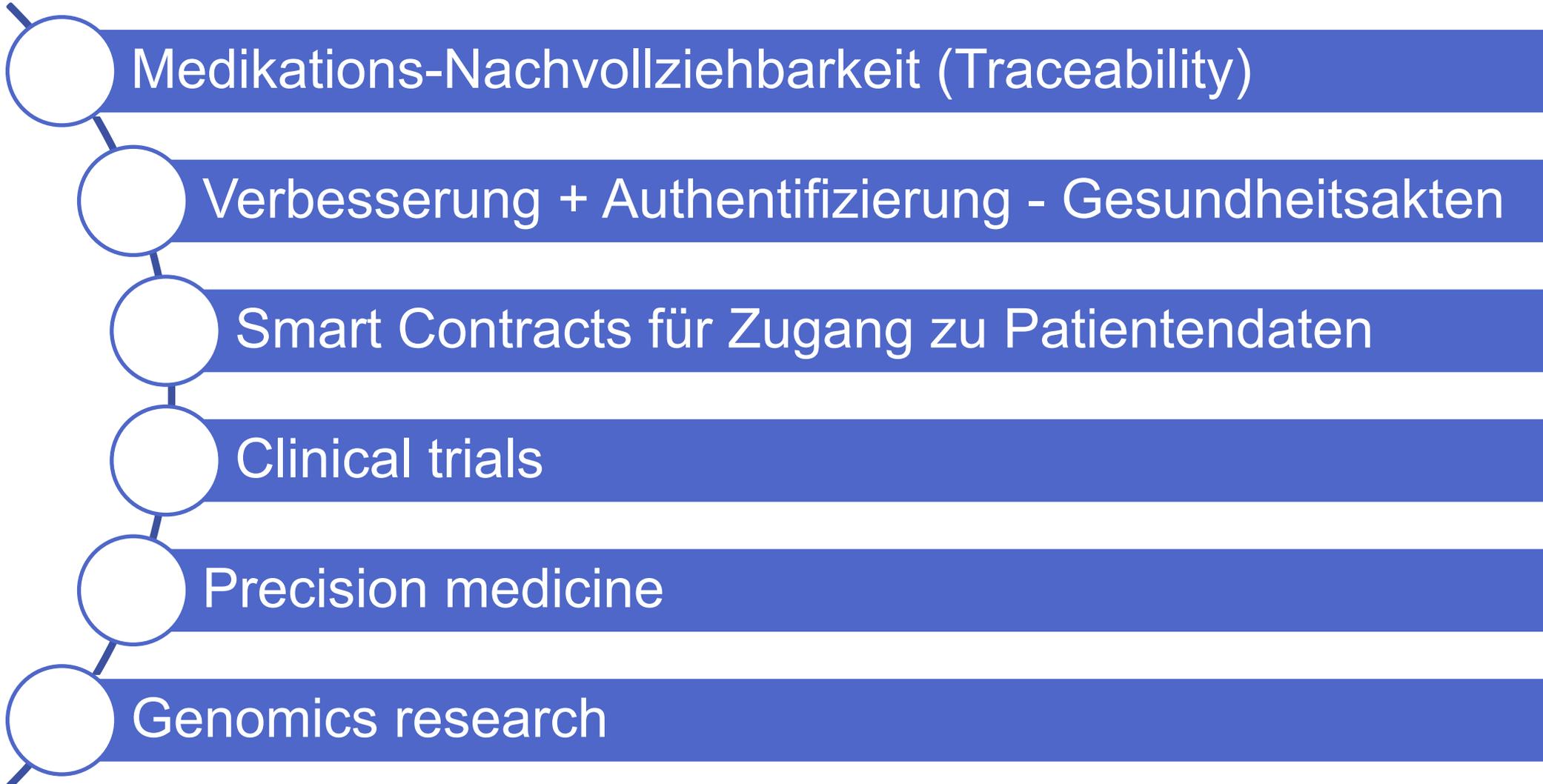
Disintermediation

Transparenz und
Nachvollziehbarkeit

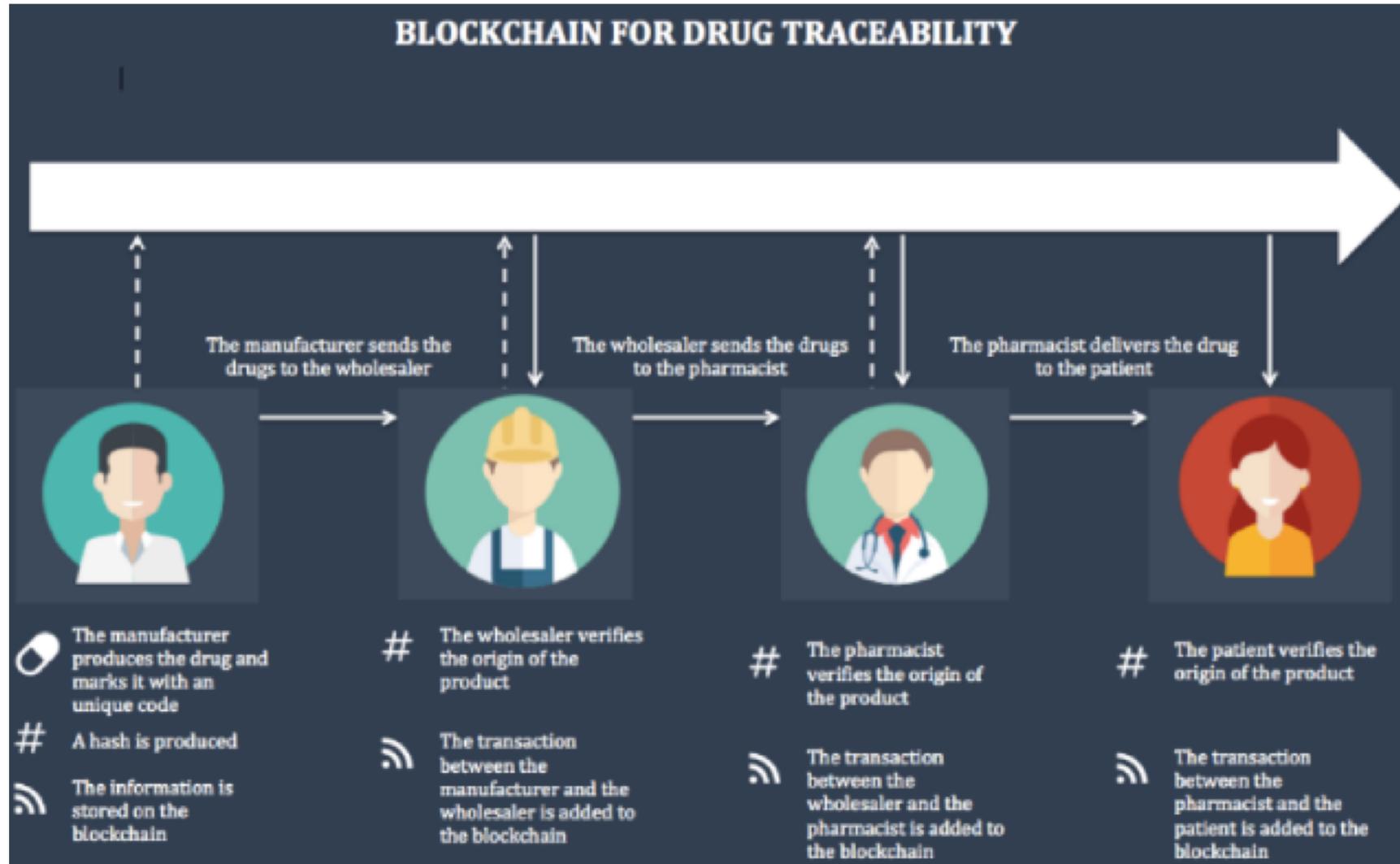
Industrie-
Kollaboration

Neue Business-
Modelle

Potentiale im Gesundheitswesen



Beispiel: Medikament - Versorgungskette



Beispiel: Daten - Blockchain

4 Patients can share their identity with health organizations



The patient's private key links their identity to blockchain data



The private key can be shared with new health organizations



With the key organizations can then uncover the patient's data



Data remains non-identifiable to those without the key

MedRec – Proof of Concept

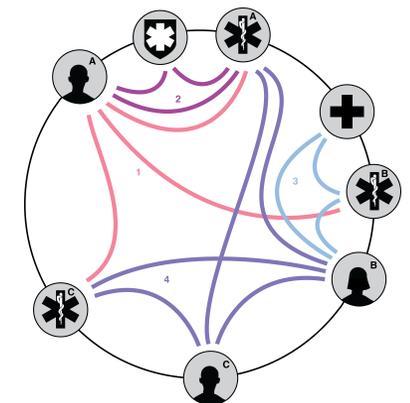
Dezentralisiertes
Record-
Management-
System von EHRs

Umfassendes,
unveränderlicher
Log

Authentifizierung,
Vertraulichkeit
und
Verantwortlichkeit

“Data sharing”

verwendet
Ethereum Smart
Contracts



FHIRChain

Setzt "Shared
Nationwide
Interoperability
Roadmap" um
(ONC/US)

Security/Privacy,
Vertrauen,
Skalierbarkeit und
interoperable
Datenstandards

FHIR
Datenelemente +
Token-basiertem
Design

Basiert auf
Designprinzipien
von Satoshi
Nakamoto in C#

Große Nodes in
P2P Topologie

MyHealthMyData (EU-Projekt (2016-2019))

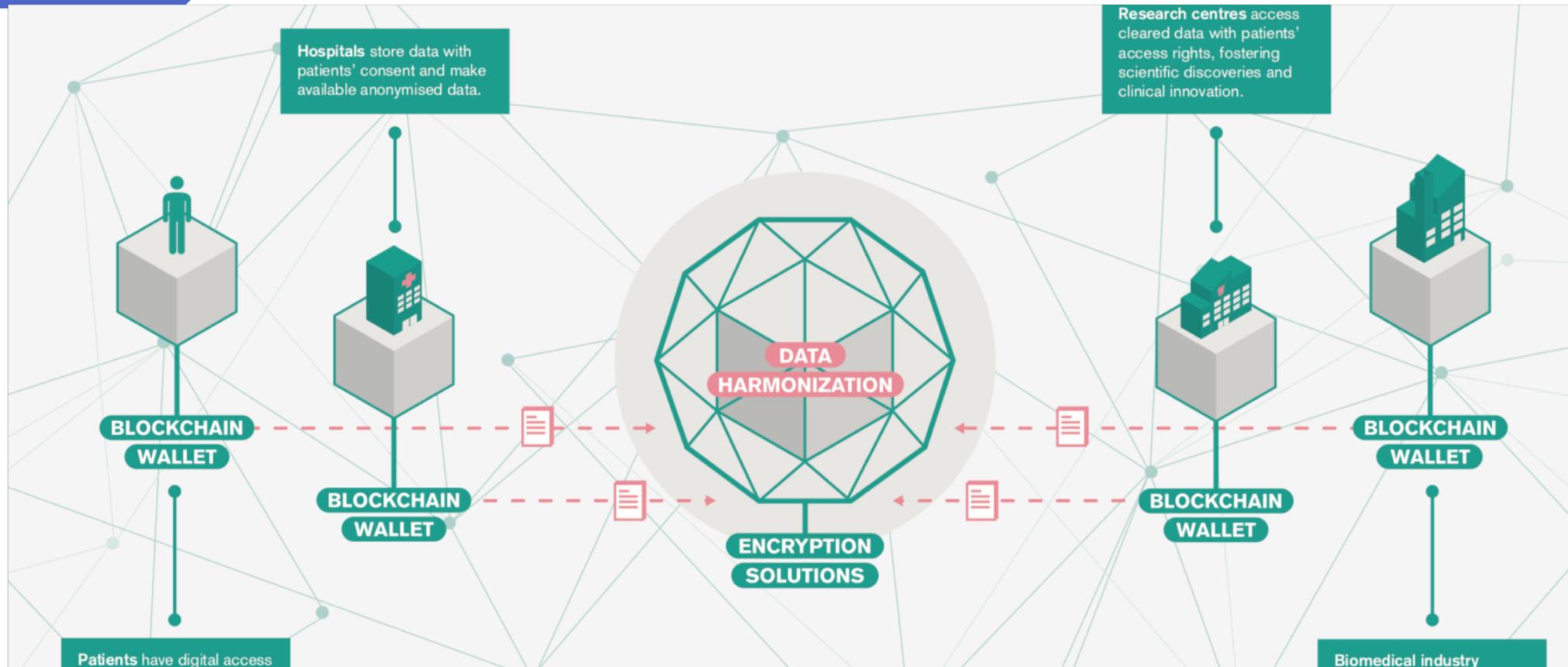
Blockchain-Technologie ermöglicht:

Dynamische Zustimmung

Persönliche Daten-
"Accounts"

De-Identifikation und Verschlüsselung

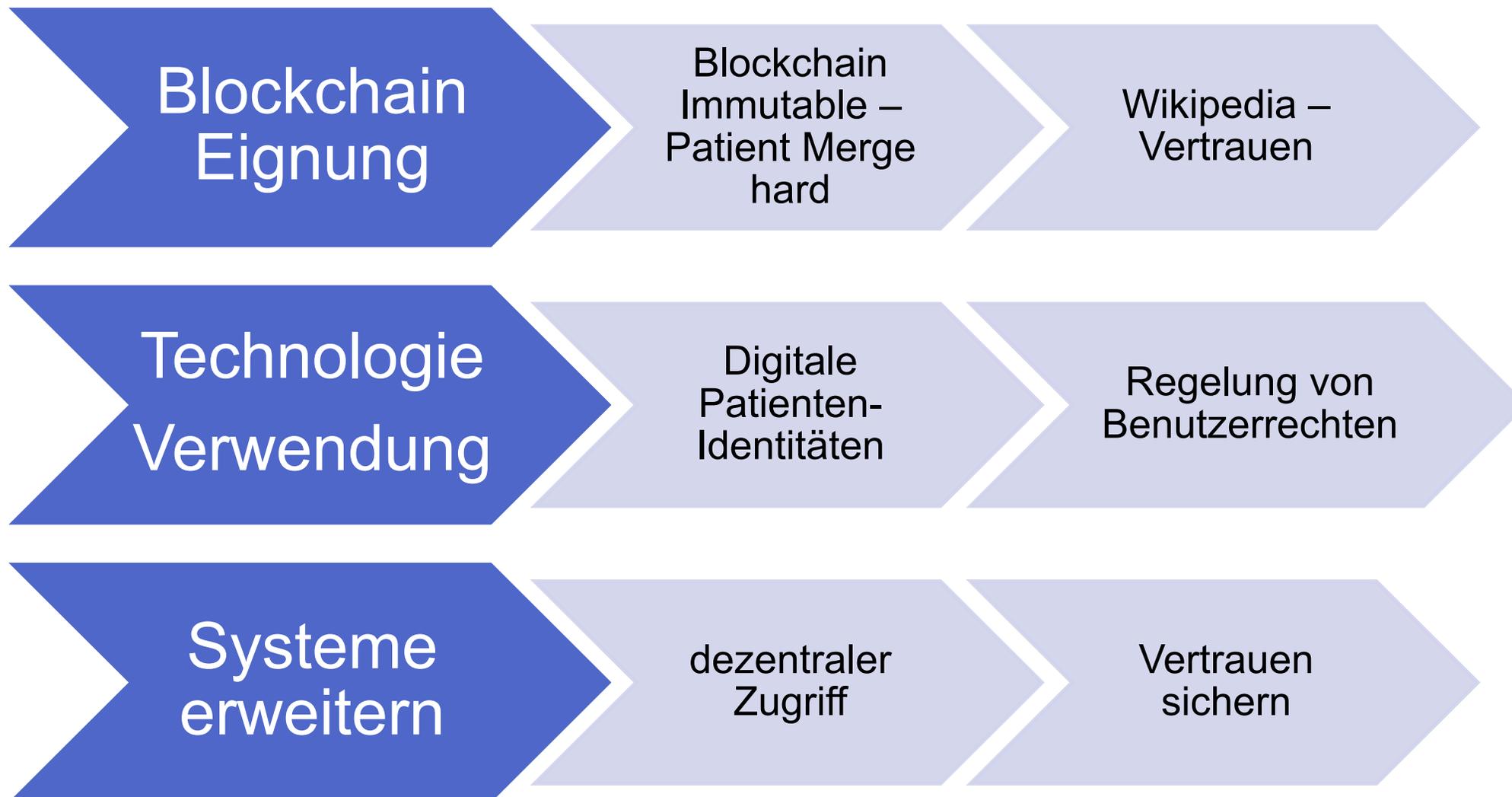
Big Data Analytics



Herausforderungen



Ausblick



Vielen Dank für die Aufmerksamkeit

Kontakt:

Lukas Huber

- **Tel:** +43 (0)50 8648 3814
- **Email:** lukas.huber@umit.at
- **Internet:** <https://ehealth.umit.at/>

Blockchain – Facing Challenges in Healthcare - beyond Cryptocurrencies

ÖGBMT Jahrestagung 2018

Patrick Mangesius
Deutsch, September 2018



Herausforderungen und Anforderungen für das moderne Gesundheitswesen

Allgemein

- Teilnehmer sind untereinander vernetzt
- Vernetzung über standardisierte Schnittstellen
- Austausch medizinischer Information

Krankenhäuser

- Reduktion von Mehrfachuntersuchungen
- Bereitstellung von Untersuchungsergebnissen für Zuweiser
- Unterstützung einer kooperativen Versorgung, intersektorale Kommunikation

Ärzte und Zuweise

- Zugriff auf Vorbefunde und Medikation
- Einfache Überweisung an Spezialisten oder Spitäler für detaillierte Diagnostik
- Verständigung über Untersuchungsergebnisse

Patienten

- Zugriff auf eigene Dokumente
- Teilnahme am Behandlungsprozess
- Vergabe von Berechtigungen



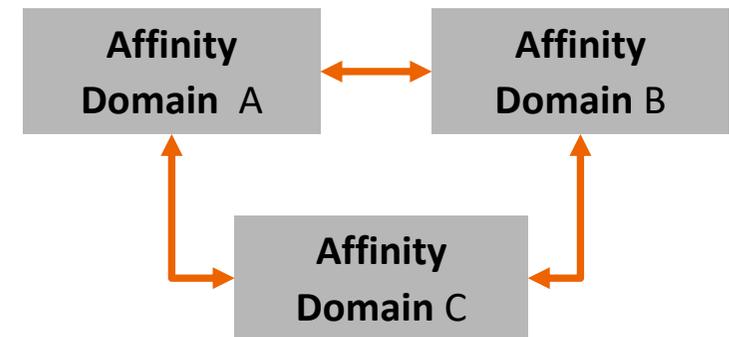
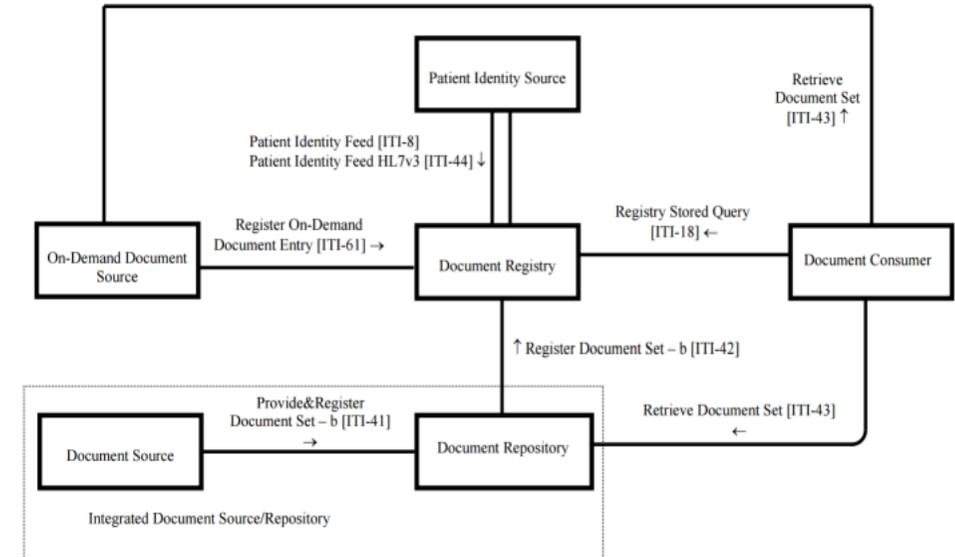
- Interoperabilität ist einer der Schlüsselfaktoren um einen lückenlosen Patientenpfad durch das Gesundheitssystem zu ermöglichen
- Ziel: Gesamtheitliches Patientenbild
- Im Laufe der Zeit jedoch entstehen Patientendaten verteilt in einzelnen Institutionen
- **Informationssilos verhindern die ganzheitliche Sicht auf den Patienten**

IHE (Integrating the Healthcare Enterprises)

- gegründet 1998
- Entwicklung von industrieunterstützten Standards zum verknüpfen Industrieinitiative von Systemen
- IHE XDS (Cross-Enterprise Document Sharing)

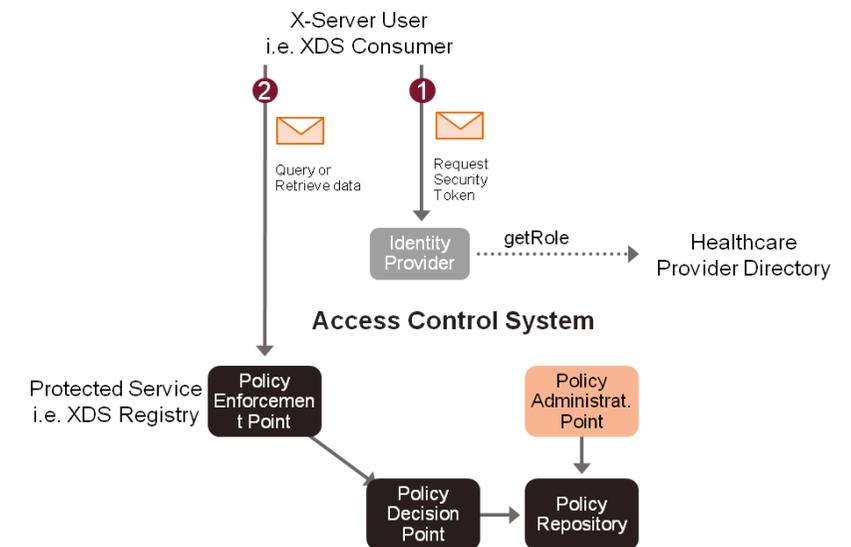
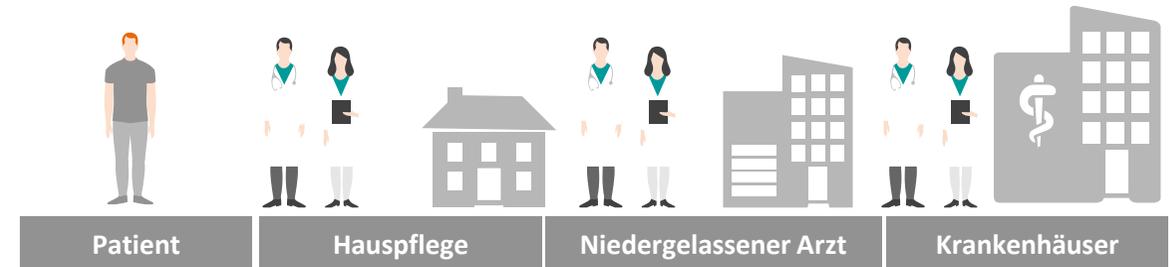


- IHE XDS und aufbauende Profile werden genutzt um standardisiert und strukturiert Patientendaten, Dokumente und medizinische Bilder zwischen den Akteuren des Gesundheitssystems auszutauschen
- Regionale Gesundheitsnetze (IHE Affinity Domains) werden aufgebaut und gegenseitig verknüpft
- ELGA (Österreich), EPD (Schweiz), EFA (Deutschland)
- Dabei steht nicht nur das Teilen von Daten sondern die Unterstützung von institutionsübergreifenden Behandlungswegen im Mittelpunkt



Berechtigungssysteme in IHE Netzwerken

- Die Einbindung unterschiedlichster Akteure benötigt ein feingranulares und dennoch flexibles Berechtigungssystem
- In IHE Netzwerken wird mittels den Profilen XUA/XUA++ ein engmaschiges Berechtigungssystem auf Basis von Oasis XACML Policies aufgebaut
- Diese XACML Policies werden innerhalb einer Affinity Domain in einem Policy Repository (PR) abgespeichert und dedizierte Komponenten werten diese nach standardisierten Vorgaben aus



Regeln und Zustimmungen

Domain vs. Patient

Domain Policies

- Gesetzliche Rahmenbedingungen und organisatorische Regelungen werden in Domain Policies abgelegt
- Sie sind stets einer Domain zuordenbar und können entsprechend in einem lokalen Policy Repository gepflegt werden

Patienten Policies

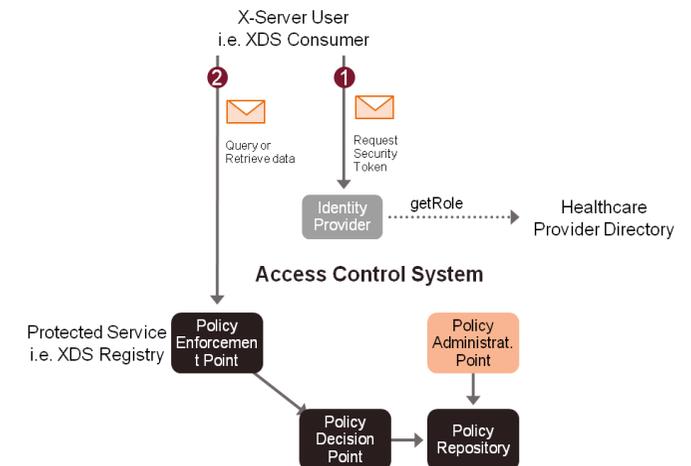
- Patienten können domainübergreifend behandelt werden. Daher müssen von Patienten erfasste Policies domainübergreifend bekannt und evaluiert werden
- IHE Netzwerke sind auf domainebene dezentral – es wird grundsätzlich keine zentrale Verwaltungsinstanz benötigt
- Um Policies entsprechend domainübergreifend anzuwenden gibt es u.a. zwei Möglichkeiten
 - Einführung zentraler Komponenten z.B. auf nationaler Ebene
 - Schaffung eines dezentralen, verteilten Policy Repositories

Authentifizierung

- Client system fordert einen SAML Security Token an
- Identity Provider (IDP) stellt den Security Token aus
- Security Token wird in später folgenden Transaktionen mitgeliefert

Authorisierung

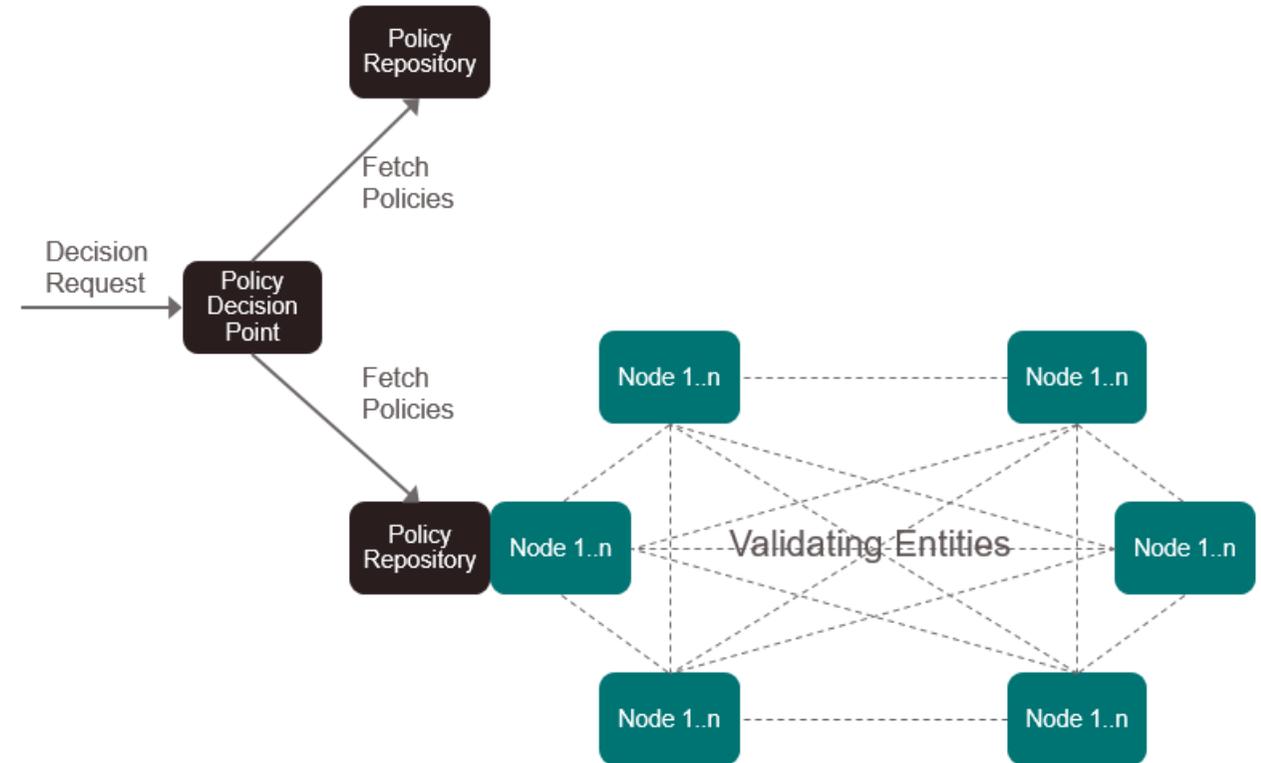
- Jedes Service wird von einem PEP (Policy Enforcement Point) geschützt
- Unter Befragung des Policy Decision Point (PDP) und des Policy Information Point (PIP) wird die Entscheidung getroffen, ob die Abfrage berechtigt ist oder nicht
- Die Entscheidung wird aufgrund der Policies getroffen, welche sich im Policy Repository (PR) befinden. Diese sind in XACML geschrieben und beschreiben das Verhalten des Berechtigungssystems auf Ressource, Subject, Environment und Action



```
<Subjects>
  <Subject>
    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">1.2.3.4.5.6.7.8.9</AttributeValue>
      <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:id"
      />
    </SubjectMatch>
  </Subject>
</Subjects>
<Resources>
  <Resource>
    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">1.1.1.1.17.1487067482136.549929</AttributeValue>
      <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#dateTime"
        AttributeId="urn:ihe:iti:xds-b:2007:documentId"
      />
    </ResourceMatch>
  </Resource>
</Resources>
```

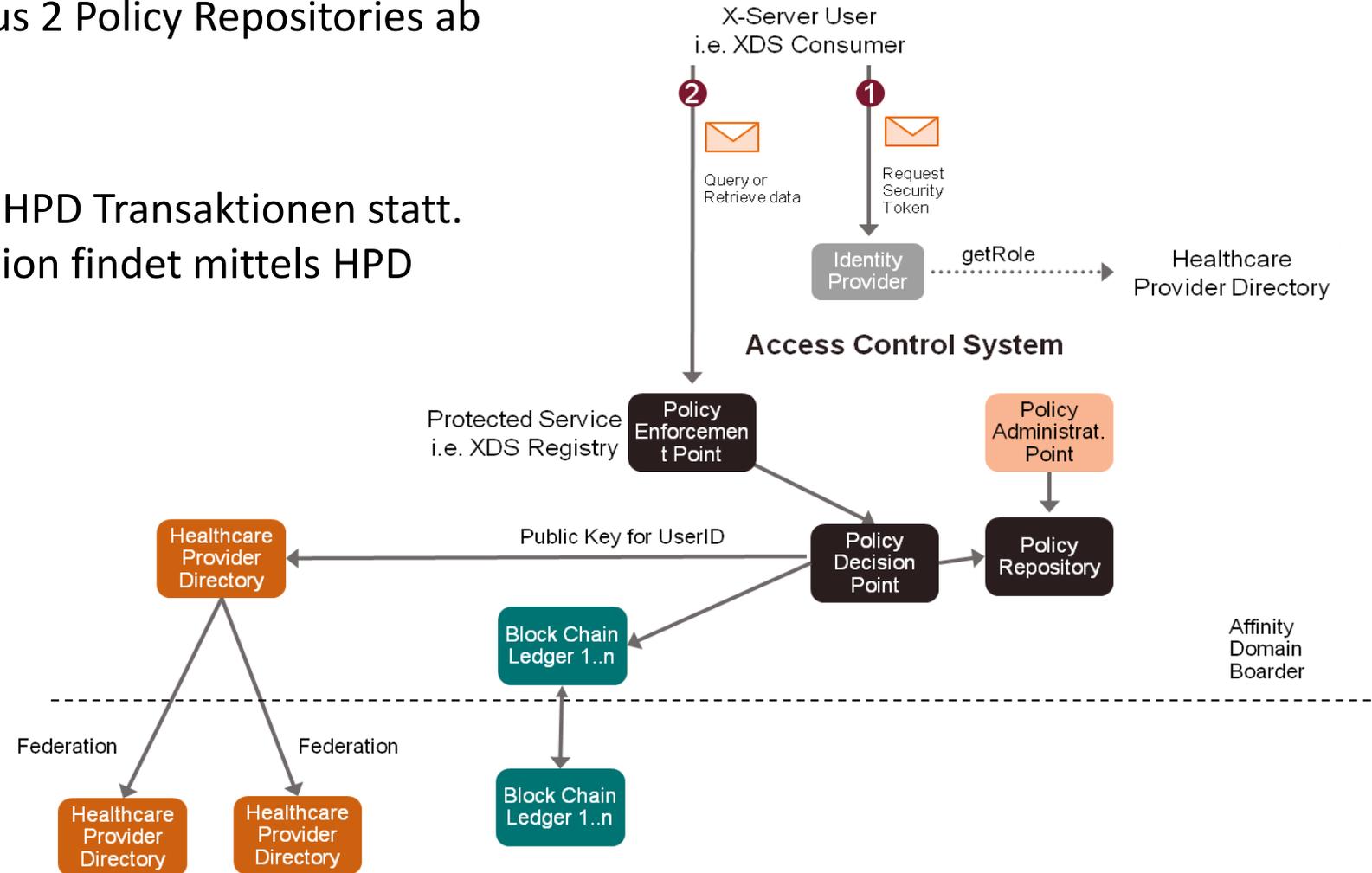
Ergebnis: Policy Repositories

- Entwicklung eines verteilten Policy Repositories auf Blockchain Basis
- Dieses Repository beinhaltet ausschließlich Patienten/Benutzer spezifische Policies
- Bereits existierende Repositories, welche gesetzliche Rahmenbedingungen abdecken, bleiben unangetastet
- XACML Policies werden in einem Ledger aus mehreren Nodes gespeichert, wobei in jeder Affinity Domain mindestens 1 Node stehen sollte



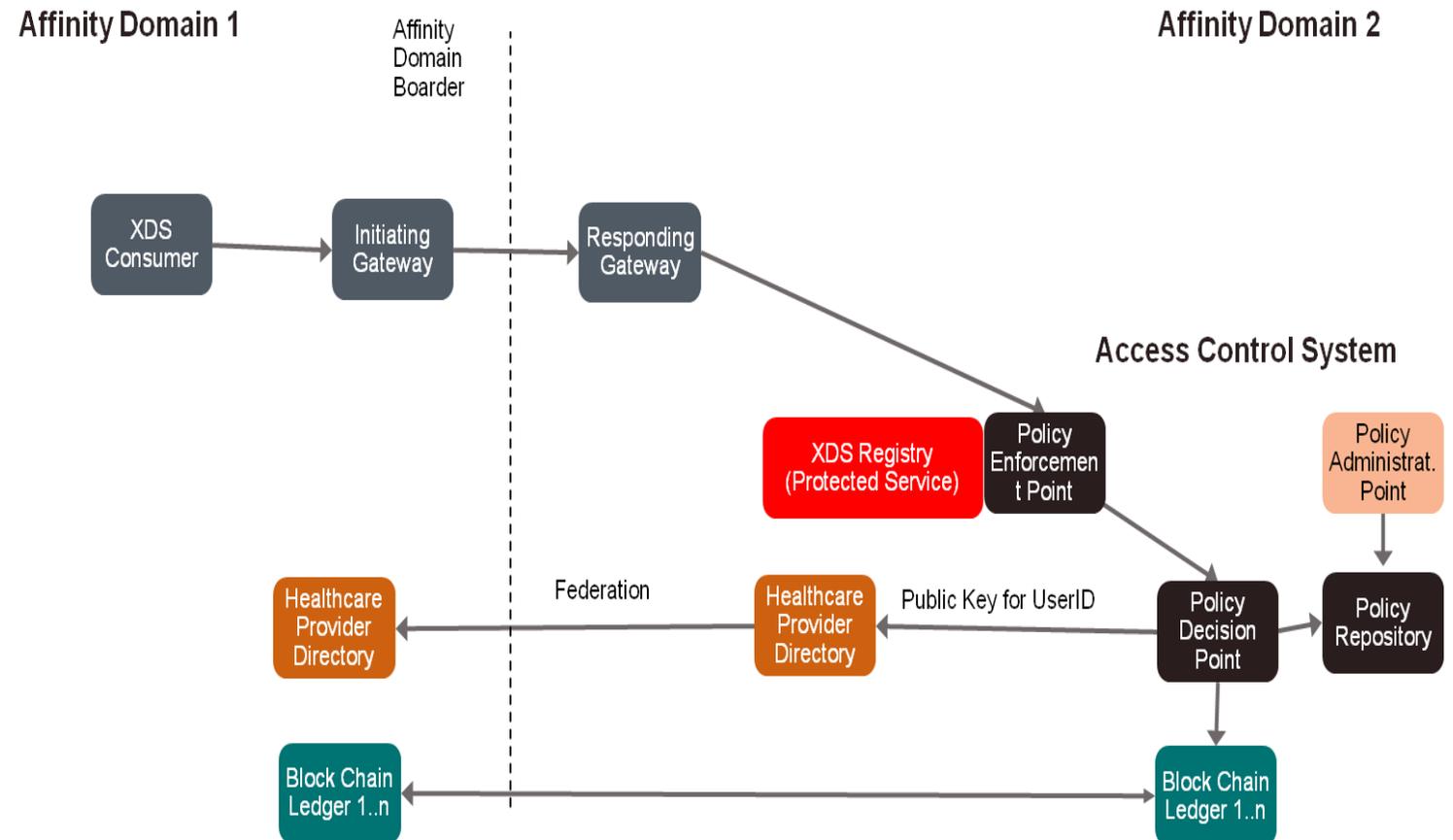
Gesamt Workflow

- Policy Decision Point frägt Policies aus 2 Policy Repositories ab und wertet sie parallel aus
- Benutzer Auflösung findet über IHE HPD Transaktionen statt. Domain übergreifende Kommunikation findet mittels HPD Federation (Option) statt



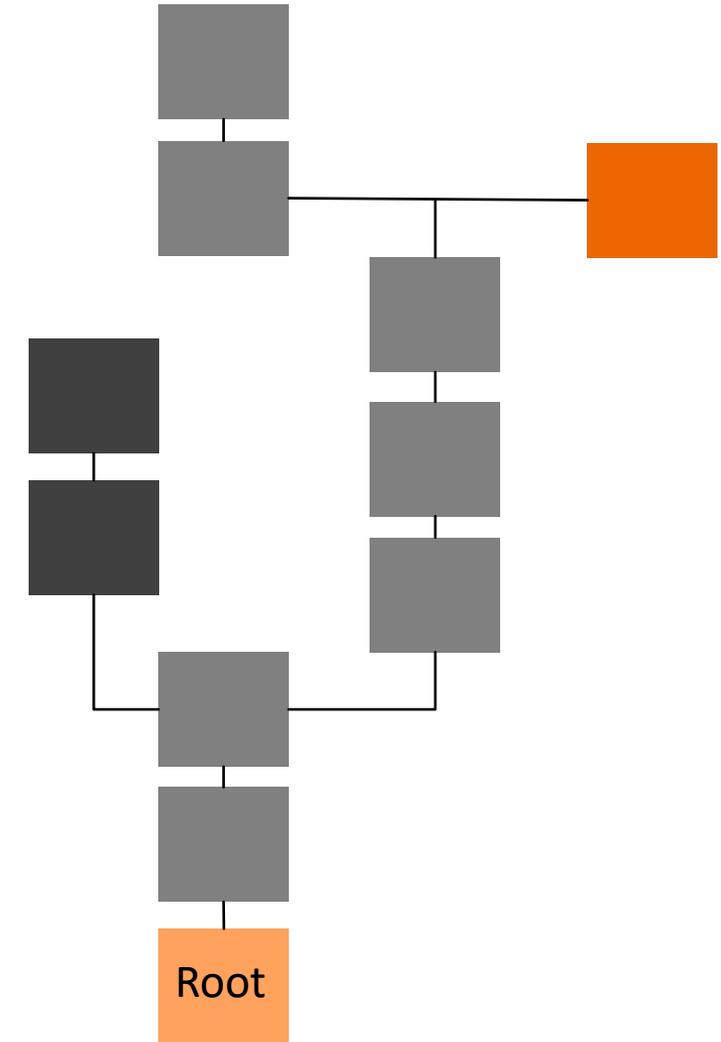
Gesamt Workflow

- Durch das gesamtheitliche Bild der Policies über Domänengrenzen hinweg können Berechtigungen direkt an der Datenquelle exekutiert werden

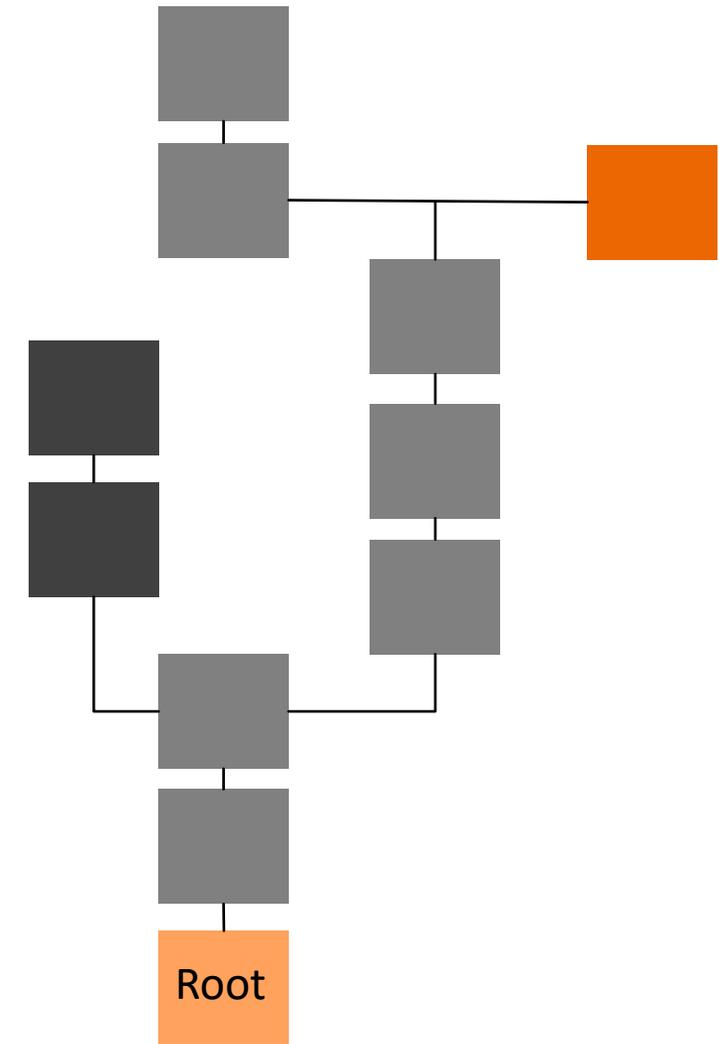


Diskussion: Policy Repository auf Blockchain Basis

- Der Einsatz von Blockchain als Technologie des Backends eines Policy Repositories stellt Folgendes sicher:
 - Gesamtheitliches Bild der Policies
 - Transaktions- und Manipulationssicherheiten
 - Nachverfolgbarkeit
 - Verteiltes Vertrauens- und Validierungssystem
- In bestehende Affinity Domains wird ein 2. Policy Repository angebunden
- Bestehende Workflows werden nicht angepasst. Dies ermöglicht eine nahtlose Integration in bereits produktive Systeme



- Last- und Funktionstests
- Laborszenarien und Validierung der Implementierung gegen gestellte Anforderungen
- Evaluierung der Ledger Konfiguration und Parametrisierung
- Handhabung und Auflösung von Policy Konflikten
 - Lokales Policy Repository
 - Verteiltes Policy Repository auf Blockchain Basis mit unterschiedlichen Autoren



.....
**ITH icoserve technology for healthcare GmbH –
A Siemens Healthineers Company**
Innrain 98
6020 Innsbruck
Austria.....

.....
Patrick Mangesius
Head of R&D eHealth Solutions @ ITH

patrick.mangesius@ith-icoserve.com
.....

*Thank you
for your attention*