Cyber Security Treffen
Rotkreuz, 22. Februar 2018

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Informatik

# Das elektronische Patientendossier

# Einsatz neuer Sicherheitstechnologien

**Günter Karjoth**

Datenschutz im Kanton Zürich

# Hackerangriffe auf Spitäler und Verwaltungen

**INTERVIEW** / von Dorothee Vögeli / 4.5.2017, 22:06 Uhr

Die Digitalisierung hat ihre Schattenseiten: Der kantonale Datenschutzbeauftragte Bruno Baeriswyl registriert vermehrt Hackerangriffe auf öffentliche Spitäler und Verwaltungen.

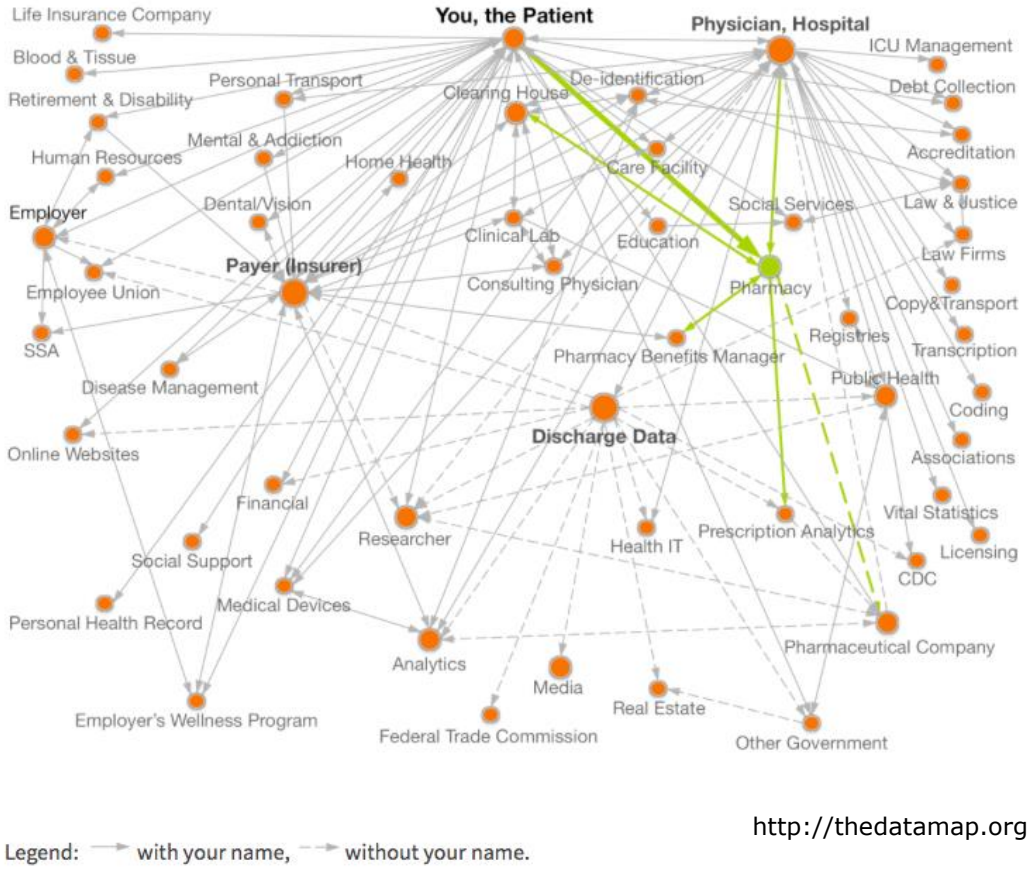

Spitäler besonders betroffen

# Mangelhafter Datenschutz im Kanton Zürich

Do 23.06.2016 - 17:26 Uhr | Aktualisiert 23.06.2016 - 17:26
von Christoph Grau

# Akteure im Gesundheitswesen

- Patient
- Versicherungen
- Ärzte
- Spitäler
- Spitex
- Apotheken
- Forschung
- Industrie
- Bundesämter
- Arbeitgeber
- …




http://thedatamap.org

Vom Papier zum Computer

# Elektronisches Patientendossier: Alle Macht den Patienten!

Mittwoch, 14. Juni 2017, 8:47 Uhr
**Peter Buchmann, SRF Digital**

Denn der Fokus des Gesetzes liegt vor allem auf dem Patienten: «[...] die Qualität der medizinischen Behandlung [soll ] gestärkt, die Behandlungsprozesse verbessert, die *Patientensicherheit* erhöht und die Effizienz des Gesundheitssystems gesteigert sowie die *Gesundheitskompetenz* der Patientinnen und Patienten gefördert werden», steht im **Bundesgesetz über das elektronische Patientendossier**.

https://www.srf.ch/news/panorama/elektronisches-patientendossier-alle-macht-den-patienten

# Das elektronische Patientendossier

Ein virtuelles Dossier, über das *dezentral abgelegte behandlungsrelevante Daten* aus der Krankengeschichte einer Patientin oder eines Patienten oder ihre oder seine selber erfassten Daten in einem *Abrufverfahren* in einem konkreten Behandlungsfall zugänglich gemacht werden können.

(elektronisches Patienten-Dossier)

# «Landkarte EPD»

Schematische Darstellung der Akteure und deren Systeme

Herstellende | «EPD-Sicht»
Anwendende | EPDG Rechtsraum
Anwendung | X Rechtsraum

Hochschule Luzern – Informatik

Alternativ: Anbindung KIS via Kommunikationsserver (z.B. Produkte Orchestra oder JCAPS)

Hersteller Primärsystem

Anwender Anwendung

Zugriffsportal – z.B. für das Erteilen von Zugriffsrechten durch die Patienten. Patient kann bis auf die Dokumentenebene über die Zugriffsrechte bestimmen.

Patientin/Patient entscheidet über die Stufe der jeweiligen Inhalte: »nützliche», «medizinische» (Standard), «sensible» oder «geheime Daten».

Stammgemeinschaft = Gruppierung mit eigenem Portalzugang für den Patienten (wie z.B. Vivates, Evita usw.) Gemeinschaft = Gruppierung ohne Portalzugang für den Patienten (nur Einlieferung)

Solche Lösungen (wie z.B. Vivates und Evita) sind als reine Gesundheitsdossiers nicht im Rechtsraum des EPDG agieren (z.B. im Zusammenhang mit einer Stammgemeinschaft), so sind sie innerhalb des Rechtsraumes tätig.

«Arzt-Sicht»: Z.B. über Viewer / Webzugang / App seiner «Stamm-gemeinschaft». Vom Patienten bestimmt: Patient entscheidet - nur Leserecht oder auch Schreibrecht.

Zugriff **«eingeschränkt»** = «nützliche» **«normal»** «nützliche» und «medizinische» **«erweitert»** «nützliche», «medizinische», «sensible»

Im Notfall: Anwender muss Zugriff schriftlich begründen. Generell: Ohne spezifische Zuweisung durch Patient = «normal». Zugriff kann z.B. auf 6 M... befristet we...

Stammgemeinschaften / Gemeinschaften (Affinity Domain bzw. Community)

Alle Inhalte aus den Stammgemeinschaften und Gemeinschaften zusammen bilden das «elektronische Patienten-Dossier». Bei einer Abfrage werden die Inhalte «zusammengetragen». Das EPD ist also ein «virtuelles Gebilde» über alle Stammgemein-schaften und Gemeinschaften hinweg.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Verzeichnisdienste BAG**
CPI: Community / Portal Index
HPD: Healthcare Provider Directory
MDI: Metadata Index-Service

**Bilateraler Daten-/Informationsaustausch**

Spitäler

Praxen

z.B. SMEEX

Pflege

Therapeuten

Spitex

Apotheken

Weitere – z.B. Labors

z.B. PACS

Authentifizierung Identifizierung der Benutzenden

Direkter Austausch mit de...rderten Profilen

Zugang über ... eHealth-Connector BEACHTE **

Weitere, andere API (...)

Dateiformate wie z.B. PDF mit Metadaten (auch Bilder, Dicom, XML ...)

Direkter Austausch mit den geforderten Profilen

ID-Provider im EPD ... bewegt sich im EPDG-Rechtsraum

IHE

EPDG Rechtsraum

Repository(s) Registry MPI Policy

Z.B. Vivates...

Z.B. Evita...

** Integration eHealth Connector

**Repository(s)** = physikalischer Speicherort der EPD-Dokumente, die jederzeit abrufbar sein sollen, sofern ein Zugriffsrecht besteht.

**MPI** = «Master Patient Index»

**Affinity Domain bzw. Community** = technische und organisatorische Einheit, EPD-Gemeinschaft.

**Registry** = zentrale Datenbank einer Gemeinschaft, in der alle Verweise/Links auf die EPD-Dokumente dieser Gemeinschaft gespeichert sind.

**API** = *application programming interface – Schnittstelle zur Anwendungsprogrammierung.*

** Der eHealthConnector ist keine eigene Software-Komponente, die als Applikation installiert und genutzt werden kann. Es handelt sich vielmehr um eine SW-Library, welche in die Primärsysteme als Bibliothek eingebunden werden kann, damit unter anderem die Funktionen zur Kommunikation mit Affinity Domains genutzt werden kann.

Zugang auf die Gemeinschaften durch Az mit vielen verschiedenen Passworten? Nein! Arzt lässt sich im nationalen HPD *(Health Professional Directory)* registrieren. Plattformanbieter nehmen bei einer Anmeldung im EPD die Anmeldeangaben des Arztes und lassen sie im Hintergrund mit dem nationalen HPD abgleichen *(sichere Identifikation)*.

Folie

Bei Quellen mit z.B. grossen Datenfiles/Datenmengen ist eine «ausgelagerte» Aufbewahrung für die Anzeige im Abfragefall zugelassen. Z.B. PACS.

AMHERD & PARTNER
Beratung · Entwicklung · Training Burgstrasse 34 · 8545 Rickenbach Sulz ZH
amherdundpartner@icloud.com



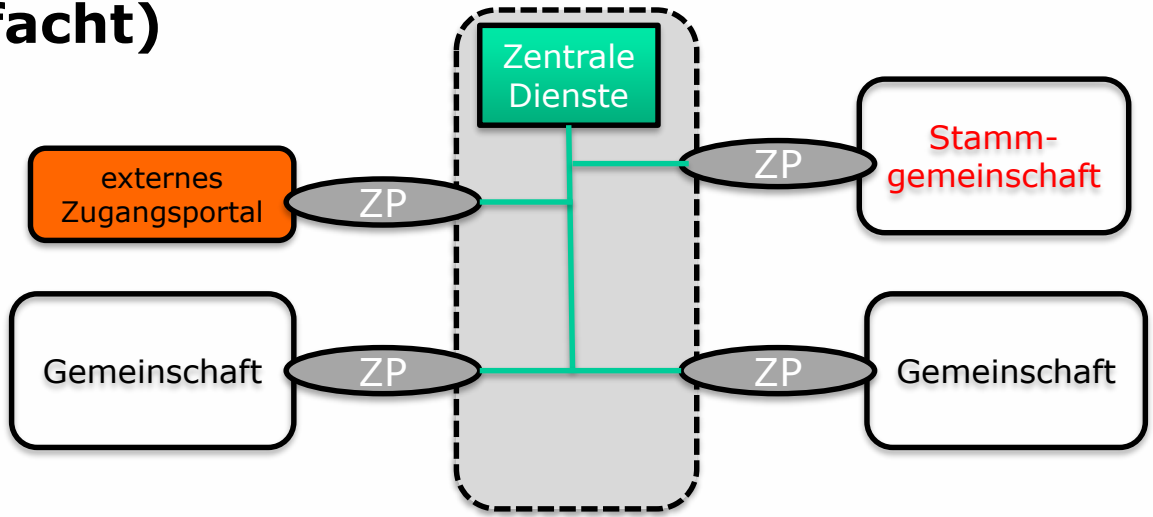
08_2016

# Architektur (vereinfacht)

- gleichberechtigte Gemeinschaften, die über Zugangspunkte ZP kommunizieren

- schweizweite Verzeichnisse
  - der Gemeinschaften
  - der Rollen

- Stammgemeinschaft




  - Einwilligung des Patienten, dass eine bestimmte Person in Wahrnehmung einer bestimmten Rolle Zugriff auf bestimmte Dokumente hat
  - selbst Zugriff auf ihr Dossier erhalten

# Wer hat Zugriff auf meine Daten?

**Beim elektronischen Patientendossier hat eine Patientin immer die Kontrolle über alle Akten.**

☛ Grundsätzlich gilt, dass nur Personen das ePD einsehen können, denen der Patient ein Zugriffsrecht erteilt hat.

**Wirklich ?**

# Wo sind meine Daten gespeichert?

- Bei der Umsetzung dieser Anforderungen lässt das Gesetz den Akteuren maximale Freiheit. *Das oberste Prinzip ist, die Daten möglichst dort zu speichern, wo sie erfasst werden und nicht in einer Zentrale.*
- Gemeinschaften: Spitäler, Heime aber auch Apotheken, Hausärzte und die Spitex können sich darin zusammen schliessen. Sie organisieren sich selber und wählen einen eigenen Anbieter, der die technische Infrastruktur für das elektronische Patientendossier bereitstellt.
- Eine Gemeinschaft, die neben den oben genannten Gruppen auch die Patienten selbst ins System aufnimmt, wird als Stammgemeinschaft bezeichnet.

➢In den Speichern der jeweiligen Gemeinschaften liegen also nie alle Unterlagen der Patienten. Spitäler oder Ärzte kopieren nur gerade diejenigen Daten ins elektronische Dossier, die für andere behandelnde Ärzte wichtig sind.

# PATIENTEN-FOKUSSIERTES ELEKTRONISCHES PATIENTENDOSSIER

# Ziel

Die Patientin soll sich nicht nur auf die Zuverlässigkeit der Akteure im Gesundheitswesen verlassen müssen, sondern eine aktive Rolle beim Zugang auf ihre Patientenakte spielen.

# Realisierung

- erlaubt dem Patienten mittels kryptographischer Zugriffskontrolle sein Patientendossier selber zu erstellen, zu verwalten und Gesundheitsfachpersonen für einen Zugriff zu autorisieren

- Dokumente werden unter verschiedenen Schlüssel verschlüsselt abgelegt
  - USB Stick, Dropbox, ...
  - kein Vertrauen in den „Datenspeicher" notwendig

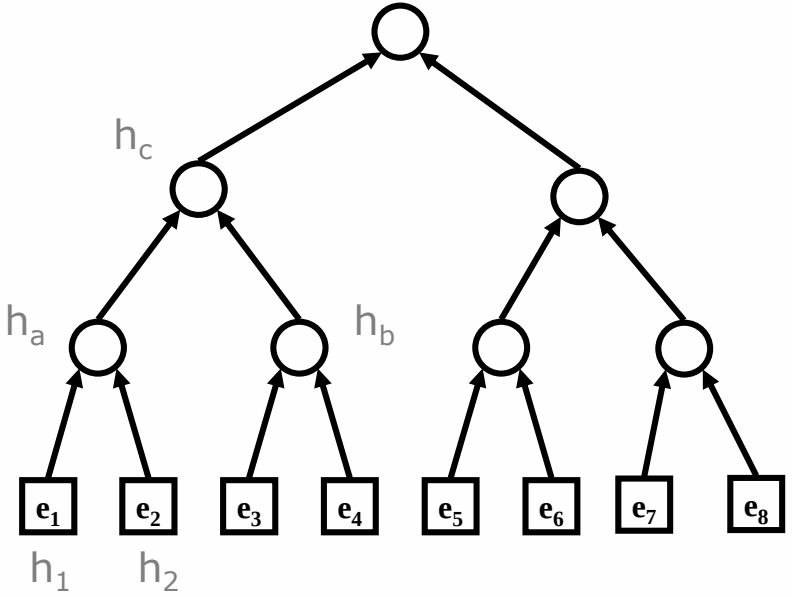
- Zugriff wird erteilt, in dem der entsprechende Schlüssel und die Datei oder Link übergeben wird

# Hash Tree [Merkle]

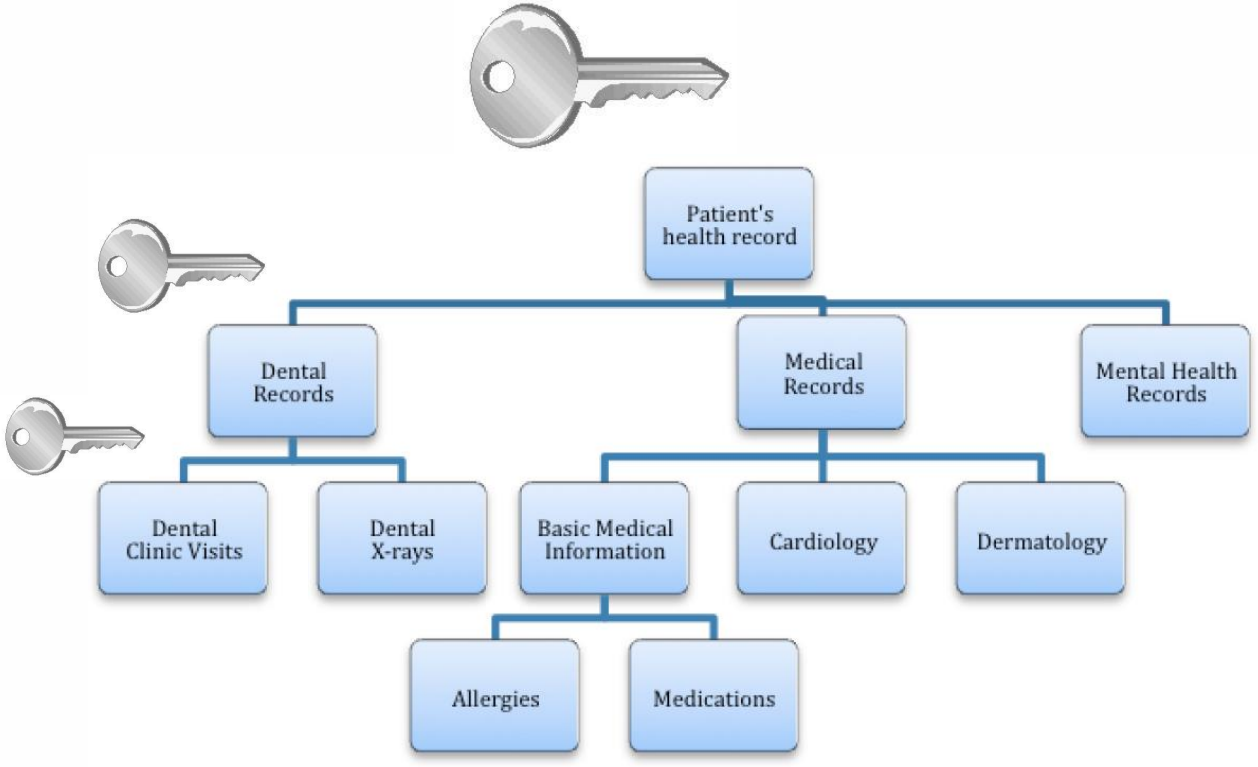
## Hierarchical Hashing Scheme

- $h_1$ = hash($e_1$)
- $h_2$ = hash($e_2$)
- $h_a$ = hash($h_1$, $h_2$)
- $h_c$ = hash($h_a$, $h_b$)

  …



# Hierarchische Dokumentenstruktur



# Einsichten

- Technisch realisierbar, aber
  - Löschen von Einträgen nur schwer möglich
  - Verantwortung über sicheren Betrieb bei den Patienten

- Unterstützung nötig durch
  - Intuitive Nutzerführung
  - Sicherer Verwaltung der Schlüssel (Wallet)

- Metadatenverschlüsselung

☛ Verbesserung möglich durch
  - identity-based encryption,
  - attribute-based encryption

☛ Integrität und Nachvollziehbarkeit der medizinischen Daten

Data Provenance

# INTEGRITÄT UND NACHVOLLZIEHBARKEIT DER MEDIZINISCHEN DATEN


7/10 7:30
SYS
mmHg
118
DIA
mmHg
78
PULSE
/min
70
OMRON

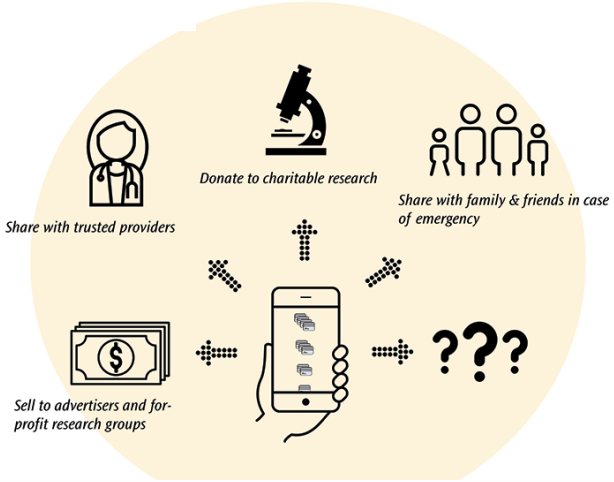

HOSPITAL


kg
59.1
Withings

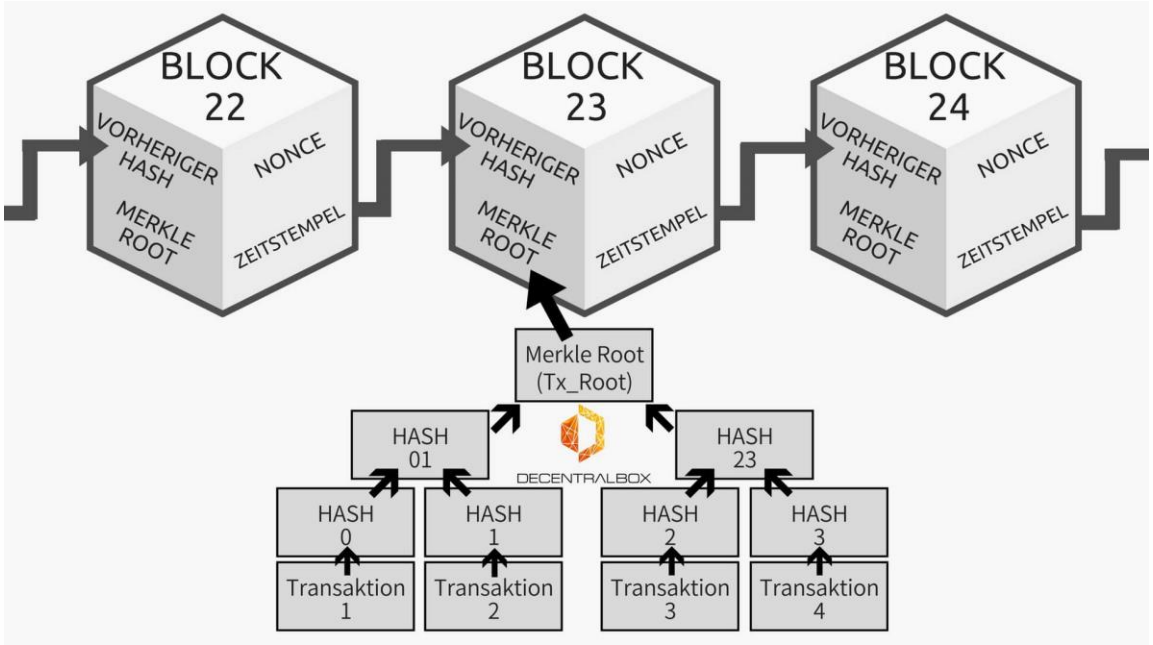

69

# Ziele

- Protokollierung der Weitergabe von medizinischen Daten
- Aufnahme von medizinischen Daten aus Quellen mit unterschiedlicher Integrität/Qualität



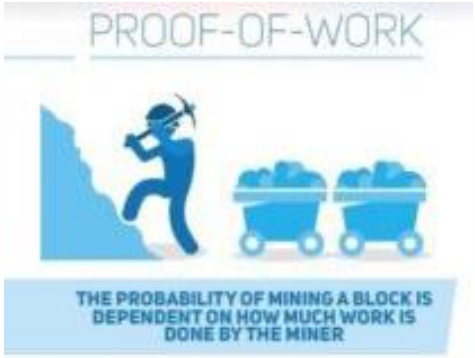
# Blockchain – A public ledger




Bildquelle: decentralbox.com

# Vertrauensmodell

- Proof of Work
- Proof of Stake
- Proof of Activity
- Proof of Reputation
- …

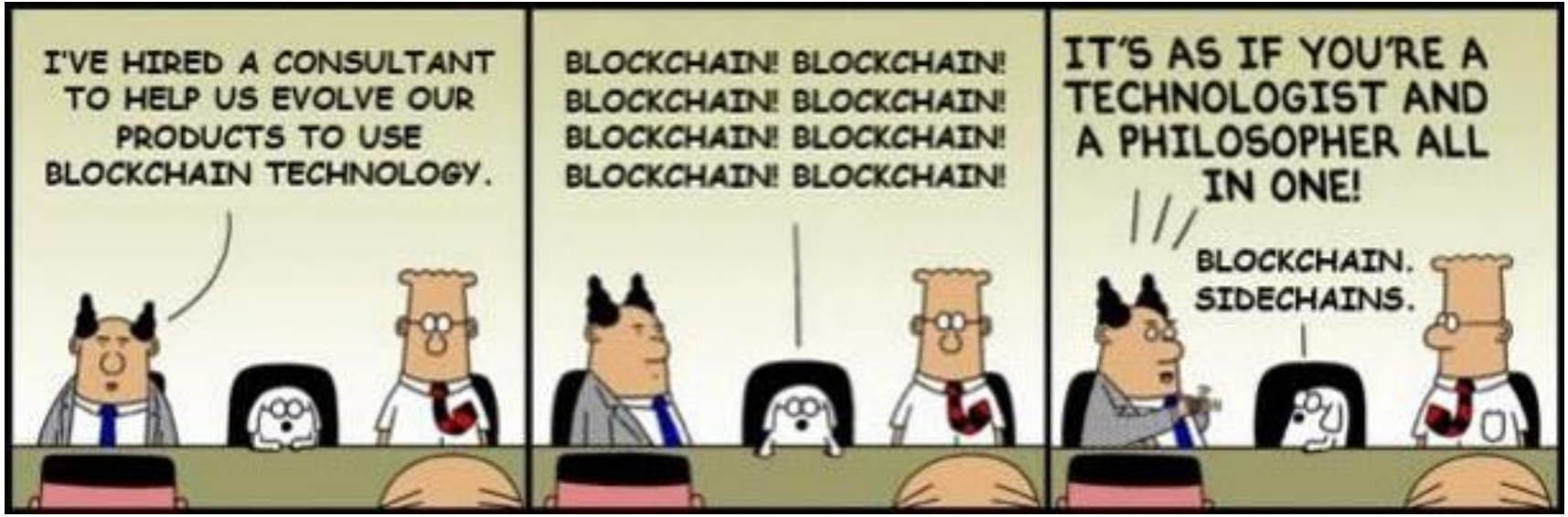



# Viele offene Fragen

- wie sieht eine Transaktion aus ?

- eine Blockchain pro Patient ?
- kann ein Patient mehrere Identitäten haben („addresses“) ?
- public or private blockchain ?

- Smart Contracts
  - Benachrichtigung über Weitergabe von Daten an Patienten
  - Alarmierung über „Fehlbehandlung“
  - ...


I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN.
SIDECHAINS.