1. Ziel des Vorhabens

Präambel

Zur Realisierung des angestrebten Projektes „Digitale Patienten Akte (DPA) und eHealth Wearable im Verbund mit Blockchain Technologie planen wir eine eigene Gesellschaft gegründet.

Zweck der zu gründenden Gesellschaft ist es, durch Innovationen und deren wirtschaftliche Verwertung die europäische Gesundheits- und Pflegewirtschaft auf dem weltweit schnell wachsenden Gesundheitsmarkt zu stärken.

Mit innovativen Technologien, wie Blockchain und NB-IoT (für die telematische, interdisziplinäre Vernetzung) wird die Digitalisierung der Abläufe im Gesundheitswesen verbessert und Bürger, Patienten, Gesundheits- oder Pflegedienstleister können einfacher miteinander vernetzt werden (E-Health).

Allgemeine Beschreibung

Wenn Daten über die Gesundheit eines Menschen bei Bedarf an jedem Ort sehr schnell zur Verfügung stehen, kann das Leben retten. Unser Projekt hat als Zielsetzung die Schaffung einer „universellen digitalen Gesundheitsakte“, genauer die Entwicklung einer mobilen Krankenakte über die Blockchain.
Es besteht dann die Möglichkeit, dass ein Patient bei der Konsultation eines Arztes diesem sofort über einen lokalen Rechner ein vollständiges Bild von seiner Krankengeschichte, seinen Allergien, den verordneten Medikamenten und Impfungen etc. verschaffen kann.
Gleichzeitig ist die Zusammenführung von Krankendaten mit den Daten aus Wearables (IoT) geplant. Damit verbunden ergeben sich für den gesamten Gesundheitsbereich neue Perspektiven.
Wearables sind eine weitere wichtige Innovation, die im Bereich des Gesundheitswesens ein immenses Potenzial besitzt, aber auch erhebliche Sicherheitsrisiken beinhaltet. Die meisten aktuellen Wearable-Produkte sind meist nur ein "sekundärer Bildschirm“ der mit einem Mobiltelefon zusammen arbeitet. Unser Konzept eines mobilen, autarken eHealth-Wearables ändert dies.
Da auf jedem Wearable ein Betriebssystem läuft, das anfällig für Angriffe werden könnte, bietet die Verwendung von Blockchain-Technologie auch auf dieser Ebene einen weiteren wichtigen Schritt für die Sicherheit des Konzeptes. Die erfassten Daten des Patienten werden damit sicher in der Blockchain gespeichert, anstatt auf dem Gerät am Handgelenk. Bei der Blockchain handelt es sich um das sogenannte Protokoll des Vertrauens. Dieses Netzwerk des Vertrauens, das universelle Sicherheit bietet, lässt sich vom Patienten, über biometrische Sensoren (z.B. Armband) und medizinische Geräte (Herzschrittmacher, Insulinpumpe etc.) aufspannen.
Betrachtet man alle sensiblen Informationen, die mit der Gesundheit verbunden sind: Identität, Krankheiten, Behandlungen, Bezahlung, etc. erkennt man, dass die Gesundheit eines Individuums eine der persönlichsten Dinge ist, die es gibt. Nicht nur, dass diese Datensätze wertvolle Informationen über die körperliche und geistige Geschichte des Einzelnen enthalten, sie beinhalten zusätzlich auch viele andere kritische Informationen. Wie zum Beispiel Geburtsdatum, Sozialversicherungsnummer, und andere Informationen, die von hohem Wert für Hacker sind und beispielsweise beim Identitätsdiebstahl hilfreich sind. Trotz dieser bekannten Gefahren kommt es aber immer wieder in erheblichem Masse zu Datenlecks/datenschutzrechtlichen Verletzungen
Auch die Speicherung von medizinischen Daten in der Cloud ist keine praktikable Option in unserer Gesellschaft, da Cloud Services für Angriffe und Datenverlust extrem anfällig sind. Offensichtlich gibt es aktuell nur noch einen Weg und das ist mit einer dezentralen Lösung, der Blockchain
Hier sind nur zwei Beispiele aus den USA für bekannte Datenlecks:

- Anthem: 80 Millionen Datensätze von Patienten und Angestellten-Daten
- UCLA Health: 4,5 Millionen Datensätze von Patienten.

In jedem dieser Fälle war es eine Lücke im Netzwerk die es möglich machte, dass alle Daten für Hacker verfügbar waren.

Ein einziger Angriffspunkt und Fehler kann zu immensen Verletzungen der Privatsphäre der Patienten führen.
Der Einsatz einer Blockchain kann das zusammen mit digitalen Signaturen und Kryptographie verhindern.
Die Daten werden ge-hashed und verschlüsselt in der Blockchain abgelegt und unter der Benutzung von multiplen Signaturen kann verschiedenen Personen oder Personen-Gruppen Zugriff gewährt werden sobald eine Freigabe durch autorisierte Personen vorliegt. Beispielsweise kann, indem man diese Technologie nutzt die Freigabe auf eine Patientenakte nur dann erfolgen sobald der Arzt, die Schwester UND der Patient die Erlaubnis erteilen. Ein weiter Vorteil liegt darin begründet, dass der Patient die vollständige Kontrolle über seine Daten behält, aber z.B. Teilinformationen anonymisiert weitergeben kann. Hier wäre ein denkbares Szenario Medikamenten-Forschung, Erhebungen von Gesundheitsträgern etc.
Die Möglichkeit, dass Versicherungsträger, Krankenhäuser, Ärzte und Patienten ein transparentes, verteiltes System wie die Blockchain verwenden, das transparent und öffentlich verfügbar ist, vermeidet Redundanzen im Gesundheitswesen und gleichzeitig Sicherheitsrisiken. Eine dramatische Verringerung der Kosten ist die Folge.
Der Einsatz der Blockchain kann wie angeführt mehrere Problemstellungen und Herausforderungen lösen, denen sich das Gesundheitswesen, insbesondere im Rahmen der voranschreitenden Digitalisierung gegenübersieht. Die digitale Erfassung von Patientendaten, die digitale Patientenakte und Abrechnungswesen seien hier exemplarisch genannt.
Wenn man die Blockchain dafür im Rechnungswesen einsetzt kann man sie im nächsten Schritt für das Management der Patientenakte verwenden. Die Blockchain erlaubt verschiedenen Organisationen, den Zugriff über das öffentliche Netzwerk auf die gewünschten Daten, ohne deren Integrität und Sicherheit zu kompromittieren. Patientendaten können erstellt, freigegeben, und jederzeit von verschiedenen Stellen, beispielsweise behandelndem Arzt, Physiotherapeut, Patient selbst, IoT-Sensor, erweitert werden und das bei gleichzeitiger Gewährleistung von Sicherheit, Anonymität, Transparent und Integrität.
Am Ende, das schafft eine Win-Win Situation für alle Beteiligten

Beispiel Szenario „Screenoritis“

Blockchain und Gesundheit können auf vielfältige Weise miteinander verbunden werden. Angefangen vom Health Monitoring (permanente Überwachung von Blutdruck, Blutsauerstoff, Puls, etc.), hin zu Datenanalysen und Diagnostik.
Um das mögliche Potential in einer Zukunft mit Blockchain greifbarer zu machen, möchten wir ein Szenario mit der chronischen fiktiven Krankheit namens Screenoritis* darstellen.
Zunächst ist es wichtig zu wissen, dass Screenoritis zwar zu problematischen Zuständen führen kann, die Krankheit selbst ist jedoch nicht tödlich. Zu den Symptomen zählen plötzliche Lähmungserscheinungen, Herzrasen, Bluthochdruck, Schlaflosigkeit bis hin zu kurzfristigen Gedächtnisverlust.
Die gute Nachricht ist, Screenoritis ist behandelbar und reversibel,
Gerade die korrekte Diagnose dieser Krankheit erfordert eine längerfristige Erfassung und Analyse der Gesundheitsdaten des Betroffenen, da es sich hier um spontan auftretende Symptome handelt die erst über einen längeren Zeitraum zu erkennbaren Indikatoren werden.
Der betroffene Patient ist 34 Jahre alt, liebt seine Arbeit und arbeitet überdurchschnittlich engagiert in seinem Beruf. Es ist Donnerstagnachmittag und der Betroffene ist nach einem anstrengenden Arbeitstag erschöpft und beschließt eine Pause zu machen
Es ist ein schöner sonniger Tag und so beschließt er einen Spaziergang am Fluss zu machen Nach etwas mehr als zwei Kilometern verspürt er eine leichte Übelkeit und Benommenheit. Er verlangsamt sein Tempo, bricht aber dennoch nach 100m zusammen. Ein Jogger der aus der Gegenrichtung vorbeikommt, findet den Bewusstlosen und verständigt den Notruf
Wenn die Ambulanz eintrifft scannen die Ersthelfer sein Fitnessarmband und damit seine HealthChain ID, einen einzigartigen Identifier für Gesundheitsinformationen. Als der Patient sich bei HealthChain angemeldet hat, legte er Regeln fest und benannte Personen die Zugriffe auf seine DPA erhalten und gewähren können. Die Ersthelfer verknüpfen die HealthChain ID des Patienten mit ihrer eigenen, die bestätigt, dass sie validierte Ersthelfer sind.

Danach lösen sie einen Broadcast im HealthChain Netzwerk aus, der automatisch die vier Notfallkontakte die der Patient festgelegt hat alarmiert und auffordert den Ersthelfern Zugriff auf seine Gesundheitsakte zu gewähren. Zehn Sekunden später, nachdem zwei der Kontakte den Zugriff gewährt haben, können die Ersthelfer auf die DPA zugreifen.
Ein paar Stunden später wacht der Patient im Krankenhaus auf, er ist soweit wieder in Ordnung, jedoch aufgeregt und möchte wissen was mit ihm passiert ist. Der behandelnde Arzt erklärt ihm, dass er an Screenoritis erkrankt ist.
Nachdem ein paar grundsätzliche Dinge geklärt wurden, fragt der Arzt ob er einwilligt anonymisierte Daten einer öffentlichen Studie zur Verfügung zu stellen – das ist inzwischen allgemeiner Usus und er hat kein Problem damit. Er ist gewillt seine Anamnese, Daten über den aktuellen Vorfall und die Ergebnisse der Tests die gerade stattfinden zu teilen.
Der Patient möchte mehr über die Menschen erfahren denen das Selbe zugestoßen ist und wie er seine Situation verbessern kann. Er und viele andere wählten diese Option um ihre Daten in einem isolierten Netzwerk zu teilen. Im Vergleich zur heute üblichen allgemeinen "Google"-Suche, sucht der behandelnde Mediziner Kriterien basiert und matched das Patienten-Profil gegen andere, um die maßgeblichen gemeinsamen Kriterien zu entdecken, wie zum Beispiel Geschlecht, Alter, Beruf, Arbeitsplatz oder Wohnort.
Obwohl die Screenoritis weit verbreitet ist und es Medikamente gibt die die Symptome lindern, ist die Heilung immer noch kompliziert und zugrundeliegenden Ursachen erfahren kaum Beachtung in der medizinischen Forschung. Also Teilnehmer an der Grundlagenforschung entdeckt der Patient, dass es eine Crowdfunding Kampagne gibt um ein Medikament zu entwickeln, dass die Ursachen der Screenoritis heilt.
Seine Teilnahme wird durch "Smart Contracts" geregelt, die ihm bedingten Zugang zu den Medikamenten gewähren sobald sie verfügbar sind. Im Gegensatz zum traditionellen Crowdfunding, wird der Zugang treuhänderisch verwaltet bist die Medikamente verfügbar sind.
Jetzt, nachdem der Patient ein genaues Verständnis seiner Situation hat, konsultiert er einen Spezialisten, der ihm tägliche Übungen und eine genau abgestimmte Medikation verordnet. Die genaue Einhaltung von beidem ist unabdingbar für den Erfolg der Therapie und wird vom Versicherungsträger entsprechend vergütet. Mit einem Wearable, das sowohl Position und Bewegungen, den allgemeinen Gesundheitszustand überwacht und an die Einnahme der Medikamente erinnert, sind die relevanten Daten sowohl für den behandelnden Arzt als auch den Versicherer jederzeit verfügbar.
Zusätzlich zu den reinen Überwachungsfunktionen liefert das Wearable noch weitere Vorteile, es liefert wichtige biometrische Daten zur Langzeiterfassung und kann aufgrund gewisser Faktoren die gemeinsam auftreten (z.B. Sturz + stark sinkender Blutdruck + erhöhter Puls = Schockzustand), Gefahrensituationen für den Träger erkennen und automatisch Ersthelfer alarmieren.
Solange sich der Patient an die vereinbarte Behandlung hält, werden alle Behandlungskosten automatisch beglichen – ganz ohne Papierkram.
Gesundheitswesen und Blockchain passen hervorragend zusammen. Gemeinsam können sie in eine Patienten zentrierte Zukunft führen, die den Ansatz grundlegend verändert, wie wir uns um uns selbst und andere kümmern, in der man den Zugang zu wichtigen Informationen die sich auf unsere Gesundheit beziehen nahtlos mit anderen teilen wird. Wir werden im Gegenzug für neue Behandlungen, die wir wünschen, Vorabzahlungen leisten und das im Gegensatz zu undurchsichtigen Risikomodellen und Bewertungen. Versicherungsleistungen werden aufgrund unseres überprüfbaren Gesundheitsverhaltens berechnet.
* Screenoritis ist eine fiktive Krankheit.

2. Stand der Wissenschaft und Technik

Allgemein

Die Blockchain-Technologie findet beinahe in jeder Industrie Einsatzfelder und kann Prozesse schneller, sicherer und kostengünstiger machen. Doch hat Blockchain auch das Potenzial uns Menschen zu helfen? Genau mit dieser Frage beschäftigen sich aktuell Experten aus Healthcare und der IT Branche. So ist es beispielsweise denkbar, dass es eine dezentrale Datenbank gibt, die die gesamte Krankengeschichte und alle Informationen eines Patienten gebündelt beinhaltet und verwaltet. Auf der einen Seite ist diese Vorstellung vielleicht nicht jedermanns Sache. Aber auf der anderen Seite könnten so Behandlungen deutlich schneller ablaufen, da Patienten nicht zu Beginn eines neuen Aufnahme- oder Behandlungsgespräches ihre komplette Krankengeschichte berichten müssten. Durch die

Verschlüsselung und das dezentrale Netzwerk ist sichergestellt, dass die Daten nur von berechtigten Personen eingesehen werden können. Es ist fast unmöglich die Datenkette einer Blockchain zu hacken, allein aus dem Grund, weil kein richtiger Inhalt vorhanden ist. In der Blockchain würden im oben genannten Use Case ausschließlich Referenzen gespeichert werden, die auf die Krankenakte beziehungsweise Datensätze hinweisen. Diese Anhaltspunkte sind in Form von „Hashes“ in der Blockchain gespeichert. Individuen und Organisationen besitzen individuelle Schlüssel, mit denen der Teil der gespeicherten Informationen, für den sie eine Berechtigung besitzen, einsehbar ist. Bei jeder Änderung der Datensätze müssen alle Teilnehmern der Blockchain zustimmen. Somit ist ein Schutz vor Datenmissbrauch sichergestellt.
Auch bei klinischen Forschungen ist der Einsatz von Blockchain denkbar. Beispielsweise könnten Informationen von Bluttest-Ergebnissen effizienter genutzt und verteilt werden. Wenn früher vier bis sechs Testverfahren nötig waren, könnte durch die Blockchain zukünftig nur ein Bluttest ausreichen. Verschiedene Labore, Forscher und Ärzte können gleichzeitig auf die geteilten Informationen zugreifen. An dieser Stelle, könnten einerseits die Patienten entlastet und andererseits eine Reduktion der operativen sowie administrativen Aufgaben im Krankenhaus erreicht werden.

Wearables/IoT

Wearable - Beschreibung

Das zu entwickelnde Wearable/IoT Device besitzt folgende grundlegenden Merkmale:

- Feedback für Rettung (SOS-Button)
- Fernüberwachung mehrerer Gesundheitsparameter
- Prävention
- Automatische Alarmierung in gesundheitskritischen Situation (Schock, Stürze, etc.)
- GPS-Tracking
- Dynamischer Datenabgleich durch Anbindung an die Patienten-Blockchain- Service Plattform
- Element der Device Blockchain

Die erfassten Daten können je nach Einsatzgebiet an verschiedene Applikationen und Personen weitergeleitet werden. Denkbar sind zum Beispiel folgende Szenarien

- Persönlicher Gesundheitsberater/Assistenz (APP)
- Ein Remote Assistenz System inkl. Hotline/ Rettungsdienst
- Eine Blockchain basierende Gesundheits-Cloud

Das geplante Wearable wird mehre neue Technologien integrieren die eine umfassende Erfassung von relevanten Gesundheitsdaten ermöglicht. Neben Sicherheit und Datenerfassung werden auch Aspekte wie Akzeptanz durch die Anwender, Einfachheit der Wartung, Langlebigkeit, Widerstandfähigkeit sowie Konnektivität eine wichtige Rolle spielen
Zu den erfassten Gesundheitsdaten zählen (aktuelle Planung)

- Blutdruck (nicht invasiv, erlaubt permanente Überwachung)
- Puls
- Blutsauerstoffgehalt
- EKG
- Bewegungsmuster/ Aktivität

Zu den erweiterten Daten zählen (aktuelle Planung)

- Bewegung (hier z.B. Sturzerkennung)
- GPS Koordinaten (z.B. bei Demenzkranken proaktive Alarmierung bei Verlassen von vorgegebenen Bereich/Geo-Fencing)

Als erweiterte Funktion kann das Wearable z.B. einen auslesbaren NFC Chip beinhalten der es ermöglicht z.B. Allergien, Blutgruppe, oder auch Ansprechpartner etc. auch ohne Zugriff auf die Patientenakte dem Rettungspersonal zur Verfügung zu stellen.

Das gesamte System verfügt über mehrere Funktionen zum Beispiel für die statistische Analyse im Gesundheitsmanagement für Ältere oder Demenzkranke, Datenanalyse, Fernüberwachung von Risikopatienten, proaktiven Rettungsdienst, Gesundheitsintervention.

Ein weiteres Ziel ist die tiefgreifende Analyse für Personal Management und damit die verbundene Optimierung der Betreuung und der Abläufe im Pflegebereich.

Da das Wearable selbst auch Element einer Blockchain ist wird absolute Datensicherheit gewährleistet., die Authentizität der Daten garantiert und die Interaktion mit den erwähnten Diensten transparent und universell gestaltet.

Betrachtung IoT

IoT, das Internet of Things schafft aktuell neue Möglichkeiten und Wettbewerbsvorteil in allen aktuellen Geschäftsfeldern und schafft zusätzlich neue Geschäftsfelder. Es berührt heute jeden Bereich des alltäglichen Lebens, nicht nur was Daten betrifft, sondern eben auch das Wie, Wann und Wo der Datenerfassung. Die Technologien die schlussendlich das „Internet der Dinge" geschaffen haben, verändern jedoch nicht nur das bekannte Internet von heute, sie verändern auch alles was mit dem Internet auf die eine oder andere Art verbunden ist. Die verbundenen Geräte (Wearables Sensoren etc.) und ihre Gateways am Rande des Netzwerkes (privat/öffentlich/industriell) sind nun in der Lage Dienste, Aktionen, Reaktionen ohne menschliche Interaktion anzufordern in dem sie selbständig auf Änderungen reagieren. Dies geschieht von der einfachsten Ebene wie dem Seifenspender bis hin zu komplexen Abläufen in der Produktion.
Gerade das Generieren Sammeln und das Analysieren von Daten ist ein essentieller Teil des Internet der Dinge, und genau deshalb muss die Sicherheit der Daten (Konsistenz, Plausibilität, Authentizität) m ganzen Life-Cycle besondere Beachtung finden. Das Management der Daten auf allen Ebenen, die angesprochen wurden von der untersten des Sensors bis hinauf zur komplexen Steuerung ist extrem komplex und herausfordernd, da die Daten über Systemgrenzen hinweg mit verschiedenen Wertigkeiten, Richtlinien und Intentionen fließen.
Bei genauer Betrachtung der verschiedenen Technologien und physischen Komponenten erkennt man, dass es sich hierbei um ein "System aus Systemen" handelt die das "Ökosystem" des IoT bilden und man diese Komplexität immer in Betracht ziehen muss. Die technische Architektur und Struktur solcher Systeme die, den sie einsetzenden Organisationen einen Geschäftsvorteil bringen sollen, sind meist extrem komplex, denn die Architekten dieser Lösungen fokussieren in der Regel auf integrierte Ansätze die alle Komponenten vom „Edge-Device" über Protokolle (Kommunikation/Transport), Anwendungen bis hin zur Analyse alles aus einer Hand bieten wollen, um so ein geschlossenes funktionsfähiges IoT-System anzubieten. Der hohe Grad an Komplexität jedoch bringt neue Herausforderungen für die IoT-Sicherheit mit sich um erfolgreich zu verhindern, dass eine einzelne Komponente zum Einfallstor für einen Angriff werden kann.

Herausforderungen an die Sicherheit bei IoT Geräten

Gleichgültig welche geschäftliche Rolle jemand im Ökosystem des Internet of Things innehat – Gerätehersteller, Softwareentwickler, Anbieter von Cloudlösungen oder Dienstleister, er muss der veränderten Herausforderungen die diese neue Technologie an seine Expertise stellt bewusst sein
Die Handhabung dieser enormen Datenmenge die bereits existiert und die in Zukunft durch das IoT noch in nicht geahntem Maß wachsen wird, stellt eine immense Herausforderung dar. Zur schieren Menge der Daten gesellt sich eine unausweichliche Komplexität, die durch die nahtlose Verbindung von zahlenmäßig unbegrenzten Geräten entsteht. Zielsetzung muss sein, diese wahre Sintflut an Daten zu kanalisieren und in nutzbringende Informationen zu verwandeln. Unsere im Moment existierenden Sicherheitstechnologien spielen bereits eine Rolle dabei, die Risiken der IoT Sicherheit etwas einzudämmen, aber sie sind bei weitem nicht ausreichend. Ziel ist es die erhobenen Daten sicher an den

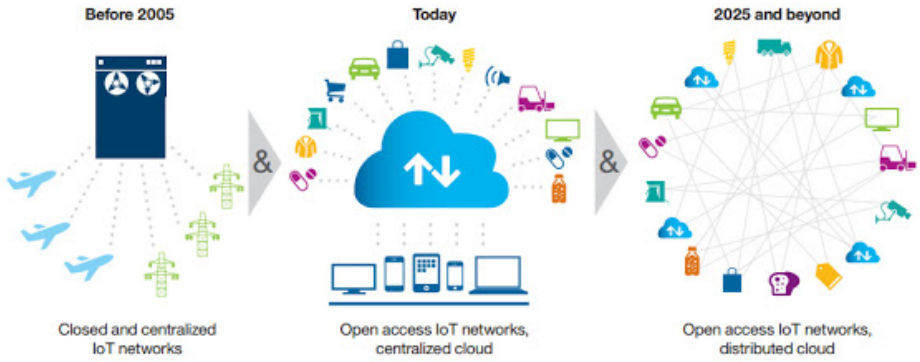
richten Ort, zur richtigen Zeit, im richtigen Format an die richtige Person zu bringen; was jedoch aus vielen Gründen leichter gesagt als getan ist

Wie geht man mit den Herausforderungen und Gefahren um?

Die Gartner Group prognostizierte, dass im Jahr 2017 mehr als 20% aller im IoT Umfeld aktiven Unternehmen Sicherheitslösungen anbieten werden, um ihre IoT-Geräte und -Dienste zu schützen, IoT-Geräte und -Dienste vergrößern die Angriffsoberfläche und die Anzahl der möglichen Angriffsvektoren für Cyberattacken alleine dadurch, dass sie frühere „offline"-Geräte in Online-Assets verwandeln die mit allen möglichen Netzwerken, Apps, Cloud-Lösungen etc. im gesamten Internet kommunizieren können. Die Antwort auf diese Gefahren kann nur sein, dass man die bekannten Sicherheitsstrategien erweitert und an die neuen Gegebenheiten anpasst, die sich durch den Einsatz dieser „online"-Assets ergeben.
Bei jedem Roll-Out von IoT-Devices müssen die Sicherheits-Strategien und Techniken neu überdachte und an die individuellen Möglichkeiten/Fähigkeiten der involvierten Geräte und der mit ihnen verbundenen Netzwerke und Infrastrukturen angepasst werden. BI Intelligence erwartet in einer aktuellen Analyse, dass sich die Ausgaben für Lösungen, die die Sicherheit von IoT Geräten bieten innerhalb der nächsten vier Jahre verfünffachen werden.
International Data Corporation (IDC) schätzt, dass 90% aller Organisationen die IoT ohne richtige Konzepte implementieren, bis zum Jahresende 2017 an eklatanten IoT-basierenden Sicherheitslücken in ihrer Back-End IT leiden werden.

Die optimale Plattform für Sicherheit bei IoT

Anwendungen und Lösungen für das Internet of Things zu entwickeln erfordert beispiellose Zusammenarbeit, Koordination und Verbindung zu jedem einem Element der Lösung und einen permanenten Blick auf das Ganze, da jeder Teil des Systems jeden anderen mit beeinflusst und damit das System als Ganzes. Jedes Device muss als einzelne Komponente funktionieren aber eben auch im Verbund mit den anderen Geräten, alle Devices zusammen wiederum mit den verbundenen Systemen und Infrastrukturen, das heißt sie müssen mit diesen kommunizieren und interagieren und das auch sicher. Das ist mit herkömmlichen, althergebrachten Ansätzen durchaus realisierbar, jedoch bedeutet es einen immensen Kosten- und Zeitaufwand und ist zudem noch extrem komplex und damit natürlich anfällig für Störungen und Sicherheitslücken solange sich nicht neue Denkansätze finden und man sich bezüglich IoT-Sicherheit nicht vom aktuellen zentralisierten Model verabschiedet.



Die Probleme des aktuellen zentralisierten Modells

Alle aktuellen IoT Ökosysteme hängen von zentralisierten, verwalteten Kommunikationsmodellen ab; auch als klassisches Client/Server Paradigma bekannt. Alle Devices werden durch Cloud-Dienste/-Server identifiziert, authentifiziert und miteinander verbunden, die immense Rechen- und Speicherleistung bieten müssen. Jede Verbindung zwischen den Geräten muss zwangsläufig und exklusiv über das Internet stattfinden, auch wenn sie nur wenige Zentimeter voneinander entfernt sind
Während dieses Modell nun mehr seit Jahrzehnten jegliche Art von IT-Geräten miteinander verbunden hat und dies sicher auch noch im Bereich IoT in kleinen Netzen mit begrenzten, klar umrissenen Aufgaben funktionieren wird (z.B. Smart-Home), stößt es bei den stetig wachsenden Anforderungen der

aktuellen Einsatzgebiete und mit Sicherheit bei den zukünftigen sich entwickelnden Netzwerken des IoT an seine Grenzen und wird scheitern.
Existierende IoT-Lösungen sind durch die hohen Infrastruktur- und Wartungskosten, die mit dem zentralisierten Cloud-Ansatz, der riesige Serverfarmen und Netzwerkinfrastrukturen inkl. Komponenten benötigt, extrem kostenintensiv und teuer. Alleine die reine Kommunikationsverarbeitung wird bei diesem Ansatz alle Grenzen sprengen sobald die Anzahl wie erwartet in den Bereich von mehreren zehn Milliarden wachsen wird.
Selbst wenn man auf irgendeine Art wie auch immer die ökonomischen und technischen Herausforderungen löst, bleiben Cloud-Server und -Infrastrukturen ein Engpass und ein Single Point of Failure der das gesamte Netz beeinträchtigen kann, bis hin zum vollständigen Zusammenbruch des Netzes, dies ist gerade in kritischen Bereich ein immenses Risiko
Zusätzlich erschweren die proprietären Protokolle und Konzepte der verschiedenen Hersteller und ihre grundsätzlich verschiedenen Methoden in Punkto Sicherheit die sogenannte Machine-to-Machine (M2M) Kommunikation schwierig, teuer und unsicher. Aktuell gibt es keine einzige Lösung die alle bekannten Geräte miteinander verbinden, noch garantieren könnte, dass die Cloud-Dienste die die verschiedenen Hersteller anbieten, interoperabel und kompatibel sind,

Die Lösung: Dezentralisierte IoT Netzwerke

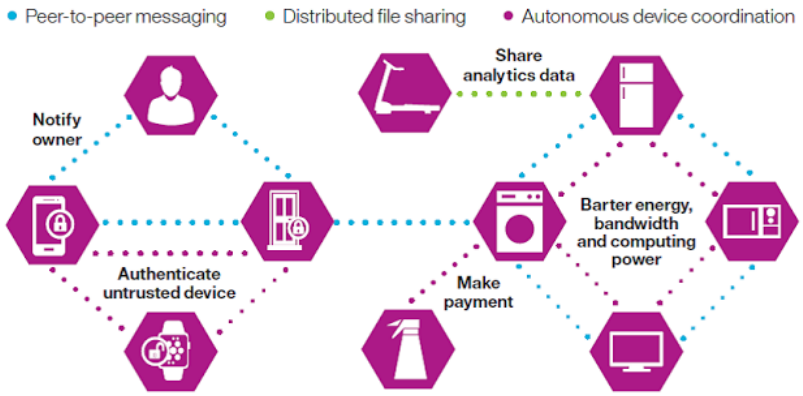
Ein dezentralisierter Ansatz zum IoT-Netzwerk löst viele der oben angeführten Probleme. Der Einsatz eines standardisierten Peer-to-Peer Kommunikationsmodels, um die hunderte von Milliarden von Transaktionen die zwischen den Geräten stattfinden zu verwalten, reduziert die entstehenden Kosten signifikant, im Unterschied zu den Cloud-Lösungen nach dem klassischen Model mit riesigen Serverfarmen und zugehöriger Storage- und Netzwerk-Infrastruktur. Ebenso wird verhindert, dass der Ausfall eines Knotens, einer Leitung oder generell einer einzelnen Komponente das gesamte IoT Netzwerk zum Erliegen bringt.
Wie auch immer, der Ansatz der Peer-to-Peer Kommunikation bringt neben allen Vorteilen auch gewisse Herausforderungen mit sich. Hauptsächlich ist dies die Frage nach Sicherheit. Bekannterweise ist gerade IoT-Sicherheit wesentlich mehr als nur das einfache Schützen von sensiblen Daten. Die von uns vorgeschlagene Konzeption muss sowohl Datenschutz und -Sicherheit in großen IoT-Netzen gewährleisten und eine Methode zur Validierung und Konsensfindung bei Transaktionen bieten um Diebstahl und Ausspähung zu verhindern.
Um die Funktionalität bestehender traditioneller IoT-Lösungen ohne zentralisierte Kontrollinstanzen abzubilden, muss ein dezentralisierte Ansatz drei fundamentale Aufgaben erfüllen:

- Peer-to-Peer Messaging
    - Peer-to-Peer (P2P) Connection (von englisch peer „Gleichgestellter“, „Ebenbürtiger“) und Rechner-Rechner-Verbindung sind synonyme Bezeichnungen für eine Kommunikation unter Gleichen, hier bezogen auf ein Rechnernetz. In einigen Kontexten spricht man auch von Querkommunikation.
    - Typische, aber nicht notwendige Charakteristika von Peer-to-Peer-Systemen sind:
        - Peers weisen eine hohe Heterogenität bezüglich der Bandbreite, Rechenkraft, Online-Zeit, … auf.
        - Die Verfügbarkeit und Verbindungsqualität der Peers kann nicht vorausgesetzt werden („Churn“).
        - Peers bieten Dienste und Ressourcen an und nehmen Dienste anderer Peers in Anspruch (Client-Server-Funktionalität).
        - Dienste und Ressourcen können zwischen allen teilnehmenden Peers ausgetauscht werden.
        - Peers bilden ein Overlay-Netzwerk und stellen damit zusätzliche Such-Funktionen zur Verfügung.
        - Peers haben eine signifikante Autonomie (über die Ressourcenbereitstellung)
        - Das P2P-System ist selbstorganisierend.

- Alle übrigen Systeme bleiben konstant intakt und nicht skaliert.

- Autonomous device coordination
  - Da kein zentraler Kontrollmechanismus vorhanden ist und auch keine cloud-basierte „Schiedstelle“ müssen die Devices in der Lage sein untereinander einen Konsens betreffend verschiedener Faktoren (Bandbreite, genutzte Rechenkapazität, Energieverbrauch) auszuhandeln.

- Secure, distributed, data-sharing capabilities
  - Daten werden verteilt erfasst, sind sicher gespeichert und können zugleich von verschiedenen Teilnehmern der Blockchain je nach Regelwerk genutzt werden



Blockchain als Lösungsansatz

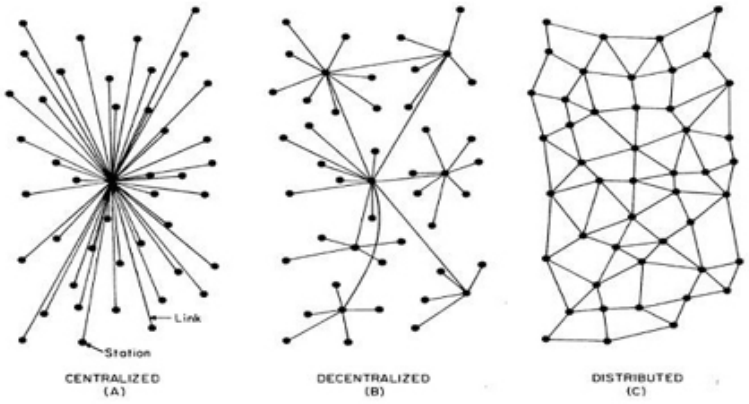
Blockchain, das “verteilte Hauptbuch” als Technologie die das Fundament und Rückgrat von BitCoin darstellt ist aktuell in den Fokus der Industrie und anderer Organisationen gerückt. Die Blockchain Technologie bietet einen ganz neuen Ansatz, wie Transaktionen und digitale Interaktionen protokolliert und gespeichert werden. Primäres Designziel sind Sicherheit, Transparenz, eine systemimmanente Widerstandsfähigkeit gegen Ausfälle, Prüffähigkeit und Effizienz. Dieses Konzept beinhaltet ein immenses Potential, vor allem im Bereich IoT. Oftmals wird die Technologie als jung bezeichnet, jedoch liegen ihre Ursprünge bereits im Jahr 1996.
Wir werden im Weiteren statt des Begriffes „verteiltes Hauptbuch“ den Begriff „distributed Ledger“ verwenden, da er mit seinem Bedeutungen- Hauptbuch, Kontobuch, Bestandsbuch - je nach Kontext zutreffender ist.

Blockchain

Was ist die Blockchain

Erste Grundlagen zur kryptografisch abgesicherten Verkettung einzelner Blöcke wurden 1991 von Stuart Haber & W. Scott Stornetta, 1996 von Ross J. Anderson und 1998 von Bruce Schneier & John Kelsey beschrieben. Parallel dazu arbeitete 1998 auch Nick Szabo an einem Mechanismus für eine dezentralisierte digitale Währung, die er „Bit Gold“ nannte. Im Jahr 2000 entwickelte Stefan Konst eine allgemeine Theorie zu kryptografisch abgesicherten Verkettungen und leitete daraus verschiedene Lösungen zur Umsetzung ab.

Das Konzept der Blockchain als verteilte Datenbank wurde erstmals 2008 von Satoshi Nakamoto im White Paper zu Bitcoin beschrieben. Im Jahr darauf veröffentlichte er die erste Implementierung der Bitcoin-Software und startete dadurch die erste öffentlich verteilte Blockchain.
Obwohl es keine wirklich allgemein akzeptierte Definition von Blockchain gibt, können wir festhalten , dass die ”distributed Ledger“-Technologie grundsätzlich das Erstellen von irreversiblen, nicht manipulierbaren Transaktionssätzen auf einer sicheren, verschlüsselten und transparenten Plattform erlaubt
“Distributed” oder „verteilt“ beschreibt die der Plattform innewohnende Struktur., welche die Kontrolle und das “Eigentum” von einer zentralisierten Instanz weg hin zu vielen Entitäten verlagert. Jede Entität die an den Transaktionen teilnimmt, bestätigt ihre Validität indem sie erlaubt, dass Daten über das Netzwerk verteilt gespeichert werden, dies durch Software die einer spezifischen Blockchain zugeordnet ist. Transaktionen werden gegenüber allen an ihnen teilnehmenden Entitäten, durch Replikation der Datenbanken und nachfolgende Authentifizierung der teilnehmenden Entitäten innerhalb des Blockchain-Netzwerkes validiert. Blockchain ist eine neue Art Daten so zu organisieren dass Transaktionen durch einen Konsens aller an ihnen beteiligten Entitäten verifiziert und protokolliert werden. Das System basiert auf einem verbindlichen „Hauptbuch“ in dem alle Transaktionen protokolliert werden
Im Gegensatz zu aktuell eingesetzten Datenbank-Systemen die das “Hauptbuch” an einer zentralen Stelle halten, verlangt die Blockchain von jeder teilnehmenden Entität eine Kopie des „Hauptbuches“ zu speichern. Dies bedeutet, dass jede potentielle Änderung an den Datensätzen mit den Kopien alle teilnehmenden Entitäten abgeglichen werden muss, bevor sie zugelassen wird. Das bedeutet einen starken Schutz gegen unautorisierte Änderungen und ist ein hoher Sicherheitsgewinn gegenüber herkömmlichen Systemen



Beispiel Szenario „Gerichtsakte“

A steht vor wegen des Vorwurfs B’s Portemonnaie gestohlen zu haben vor Gericht.
Üblicherweise wird die Verhandlung mitprotokolliert und jede Aussage A’s würde festgehalten. Sollte A das Verbrechen zugeben, würde diese Aufzeichnung als unzweifelhafter Beweis für sein Eingeständnis gelten. Das Dokument wird später im Gericht in einem verschlossenen Archiv hinterlegt.
A’s Komplize C versucht A zu helfen indem er eine Kopie des Archivschlüssels anfertigt und die Einträge im Protokoll löscht. Da es keine weiteren Einträge betreffend das Geständnis gibt, kann niemand beweisen, dass A geständig war.
Das ist, stark vereinfacht, die Art und Weise wie aktuelle Systeme arbeiten. Der Komplize C war nicht autorisiert auf das Archiv und das darin befindliche Journal zuzugreifen, dennoch verschaffte er sich Zugang und Zugriff auf die Daten und missbrauchte beides. A’S Verbrechen würde aus den Akten getilgt und fand soweit es das Gericht betrifft nie statt.
Nun betrachten wir das Szenario als verteiltes System. A bestiehlt B doch diesmal befinden sich zehn Zeugen mit Smartphones dabei und jeder nimmt die Szene auf, egal ob das Geständnis vor Gericht oder den Diebstahl selbst. Nun gibt es zehn verteilte Beweise (Records) der Tat/des Geständnisses und keinen einfachen Weg diese zu manipulieren, so dass jedes Video dasselbe zeigt.
Die einzige Möglichkeit wäre eben ein Konsens aller Zeugen den Beweis zu löschen oder zu verändern

Wenn alle Zeugen sich kollektiv darauf einigen, dass der Beweis so bestehen bleibt wird der Vorfall geschlossen und als Tatsache abgeschlossen und in das Hauptbuch eingetragen so dass er nicht mehr geändert werden kann.
Sobald ein Eintrag abgeschlossen wurde wird er als Block bezeichnet. Dieser Block wird über das gesamte Netz verteil und dann von jedem Empfänger re-validiert und der eigenen Version des Hauptbuches hinzugefügt.
“Ledger” bezieht sich auf die fortwährende und dauerhafte Aufzeichnung von mit einem Zeitstempel versehene, prüffähige Transaktionen. Jede Transaktion wir unter Zuhilfenahme von kryptographischer Validierung aufgezeichnet und in einem Stapel von Daten (Batch/Stack) abgelegt. Jeder Stapel wird als Block bezeichnet. Jeder Block bezieht sich auf den vorgehenden Block und identifiziert diesen durch komplexe Verschlüsselungsverfahren und schmiedet damit eine sichere Kette von prüffähigen Transaktionen
Der Einsatz der Blockchain ermöglicht den Aufbau eines nicht manipulierbaren Protokolls von Transaktionen. Dieses Transaktionsprotokoll wird nicht an einer einzigen Stelle gespeichert, sondern verteilt auf viele Knoten, verwaltet von Vielen und permanent aktualisiert durch die Replikation der verteilten Datenbank. Diese dezentralisierte Struktur, kombiniert mit dem prüffähigen Hauptbuch der Transkationen ist eine Technologie die wie geschaffen ist für Applikationen und Devices denen in einer immer mehr vernetzten Welt vertraut werden muss.

eHealth: Herausforderungen an die Sicherheit

Insbesondere zentralisierte Datenbanken könnten ihrerseits von Anwendungen der Blockchain profitieren.
Der CTO der Non-Profit Group Patient Privacy Rights Andrian Gropper ist der Meinung, dass diese zentralisierten Datenbanken signifikant herunterskaliert werden sollten, schließlich enthalten diese Datenbanken die Patientenakten von mehreren Millionen Patienten.
“Damit haben wir ein El Dorado für Datenräuber geschaffen. Zehntausende von Leuten im Personal von Krankenhäusern haben Zugriff auf diese Daten und für den Nutzer sind diese Systeme komplett undurchschaubar.” (Andrian Gropper)
Das ist ein im Gesundheitsbereich bekanntes Problem, das einen immensen Angriffsvektor darstellt. Erst im letzten Jahr haben Datenräuber den größten Hack im Gesundheitsbereich, den es jemals gab, durchgeführt. Es wurden die Daten von mehr als 78 Millionen Patienten offengelegt. Im März wurde das klinische Informationssystem MedStar Systems gehackt und musste offline genommen werden.
Diese Misere wird weitergehen – die Daten des Gesundheitswesens sind fast hundertmal wertvoller als gestohlene Kreditkartendaten.
“Die einzige Hoffnung, diese Art von persönlicher Information sicher zu verwalten, ist, sie wieder in die Hände einer dezentralen Gruppe zu geben. Die Blockchain wird dabei eine zentrale Rolle spielen.”
Genau das motiviert eine patientenzentrierte Gesundheitsplattform auf der Blockchain-Technologie zu bauen, ein Vorhaben. In unserem Projekt wird die Blockchain als ein Speicher für die Personaldaten, für einen Hash eines Dokuments mit Zeitstempel und für die Rechnungen sein.
Zentralisierte Datenbanken müssen kleiner werden, sie sollten nur die Datensätze gespeichert haben, die ein einzelner Arzt, höchstens eine kleine Gruppe von Ärzten, benötigt. Der Transfer von Daten sollte in den Händen der Patienten sein.
Aktuell gibt es in den USA einzelne Initiativen zum Einsatz der Blockchain im Gesundheitsbereich und der Medikamentenüberprüfung (betreffend Fälschung von Medikamenten). Ein Beispiel dafür ist Saavha. Hier liegt die Aufgabe darin die Integrität von Gesundheitsplänen zu bestätigen. Mit dem Veterans Affairs (VA) Skandal von 2014 und anderen noch existierenden Problemen in diesem Kontext ist diese Dienstleistung besonders interessant, geht es hier doch um große Probleme schlecht gemanagter Wartelisten. Dieses Problem ist laut US-Kongress etwas, was man mit Blockchain Technologie lösen könnte. Wenn man dazu in Betracht zieht dass die VA deutlich strengere Regularien als viele Krankenhäuser besitzt, so müssen zum Beispiel die verwendeten Daten auf einer Festplatte verschlüsselt werden, die in einem abgeschlossenen Raum unter ständiger Beobachtung steht. Und dennoch – die Daten konnten dennoch manipuliert werden.
Eine Konzeption die ganzheitlich sowohl die Erfassung von Gesundheitsdaten/-werten und Speicherung der Patientendaten vorsieht und dabei auch die Erfassungsgeräte mit in die Blockchain integriert ist nach aktuellem Kenntnisstand weltweit einzigartig.

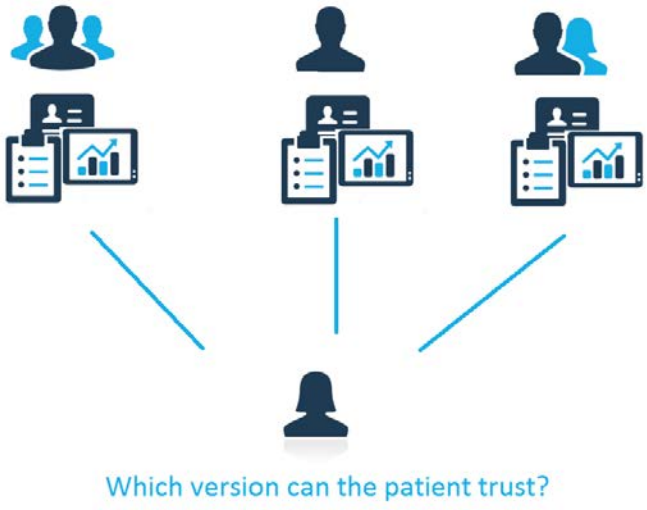
Einsatz der Blockchain im Gesundheits- und Pflegebereich

Der Gesundheitsbereich ist geradezu prädestiniert für den Einsatz der Blockchain Technologie. Zwar hat diese Technologie und die damit verbundenen Konzepte bereits angefangen in der Finanzindustrie und Fintech Unternehmen Fuß zu fassen, wobei hier der Fokus der Diskussion im Moment mehr auf dem steigenden Einfluss von Bitcoin und anderen virtuellen Krypto-Währungen liegt. Healthcare kann jedoch, noch besser als Fintech, zur tragenden Branche bei der Einführung der Blockchain werden, denn im Gesundheitsbereich ist die „Währung" Daten. Die Akzeptanz und Einführung dieses dezentralisierten Systems hat das Potential die drängendsten Herausforderungen in verschiedenen Bereichen wie vor denen der Gesundheitsbereich steht in naher Zukunft zu lösen. Die schiere Masse an Daten unter Kontrolle zu halten und Wege zu finden, wie man sie einfach, sicher und schnell sowohl austauschen, als auch bearbeiten kann, sind die zentralen Herausforderungen für den Gesundheitssektor. Valide Daten werden in jedem Bereich der Pflege benötigt und ebenso müssen valide Daten generiert werden. Die Blockchain Technologie erlaubt es allen Teilnehmenden — Patienten, Pflege-Anbieter, Versicherer, Dienstleister, Behörden — in Echtzeit in Verbindung zu stehen und Informationen auszutauschen, ohne dass Berge von Papier bewegt werden müssen, ohne Zeitverlust, sicher, verschlüsselt und transparent für alle. Ein wichtiger Aspekt ist dabei, dass jeder Teilnehmende an den Transaktionen immer nur die für ihn notwendigen Datensätze erhält.
Jahr für Jahr wächst das Volumen der von Krankenhäusern, Ärzten, Versicherungen und Leistungsträgern gesammelten und generierten Daten immer schneller an. Mit fortschreitender Technologie in der Medizin, zum Beispiel durch Fitnessarmbänder, verbesserte digitale Bildgebungsverfahren etc., vervielfacht sich die Menge der in Datenbanken gesammelten Informationen und erschwert den Austausch und die Auswertung der Gesundheitsdaten immer mehr. Des Weiteren wächst der Verwaltungsaufwand immens, wie auch die Probleme der Validierung immer weiterwachsen. Über die letzten Jahre in denen Digitale Patientenakten Einzug gehalten haben, gab es immer Diskussion zu den Problemen der Interoperabilität zwischen den verschiedenen proprietären Systemen. Viele dieser DPAS (Digitale Patienten-Akten-System) arbeiten alleine aus dem Grund nicht zusammen um eine Existenzberechtigung zu behalten. Die Frage die sich stellt ist: Kann die Blockchain dieses Denken und die verkrusteten Strukturen aufbrechen? Durch ein Datenaufkommen, wie es nie zuvor als möglich gesehen wurde, entsteht ein schmerzvoller Bedarf nach Sicherheit und Transparenz, ebenso verlangen neuen Patienten-zentrierte Ansätze nach neuen Lösungen. Die Blockchain ist eine prüffähige Lösung die Anwendung in vielen Bereichen wie Volksgesundheit, Interoperabilität, Verbraucherverhalten und Datensicherheit finden wird. Aber welchen Auswirkungen wird die Blockchain für die digitale Patienten-Akte haben?
Im bis dato aktuellen Modell liegt die Patientenakte beim Arzt obwohl sie eigentlich aufgefordert sind diese elektronisch zu teilen. Digitale Patienten Akten in der Blockchain, beispielsweise, erlauben es dem Patienten selbst die Kontrolle über ihre Daten auszuüben, sie entscheiden mit wem, wann und wie lange und auf welche Informationen sie Zugriff gewähren. Das findet in einer Blockchain statt, die als "permissioned Ledger" bezeichnet wird. Grundsätzlich gibt es von der Blockchain zwei Arten "permissionless" und "permissioned" Blockchains, während alle Blockchains prüffähige Transaktionen protokollieren, bieten nur die "permissioned" Blockchains die Sicherheit zu wissen mit wem man es zu tun hat. Die Konvergenz mit dieser Technologie der Blockchain führt zu einer effizienten Teilhabe und Kontrolle der Patientendaten.

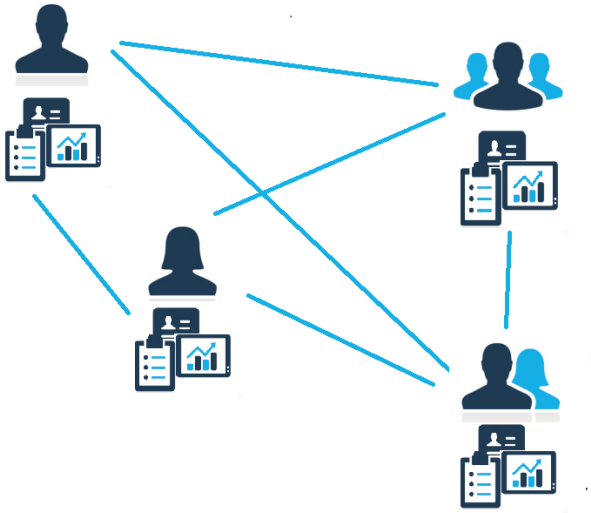
Wichtigkeit der Blockchain für eHealth

Wir beziehen uns hier auf das vorhergehende Beispiel aus "Was ist die Blockchain".
Aktuell agiert der Arzt als der Protokollführer bei Gericht und die digitale Patienten Akte ist das Äquivalent zum offiziellen Verhandlungsprotokoll. Viele Organisationen haben leider in letzter Zeit einen hohen Preis dafür bezahlt um herauszufinden, dass ihre Datenbanken weit entfernt davon sind was man als sicher bezeichnet und noch dazu geben sie in den seltensten Fällen den aktuellen Stand der Gesundheitsgeschichte des Patienten wieder.
Egal ob Hacker wie im Beispiel, unbeabsichtigte Fehler bei der Datenerfassung oder einfach nur dass verschiedene Instanzen gleichzeitig versuchen eine Datensatz zu ändern ohne dabei andere Änderungen korrekt in Rechnung zu ziehen, das „authorative Ledger" der Gesundheitsbrachen ist alles nur nicht unfehlbar.

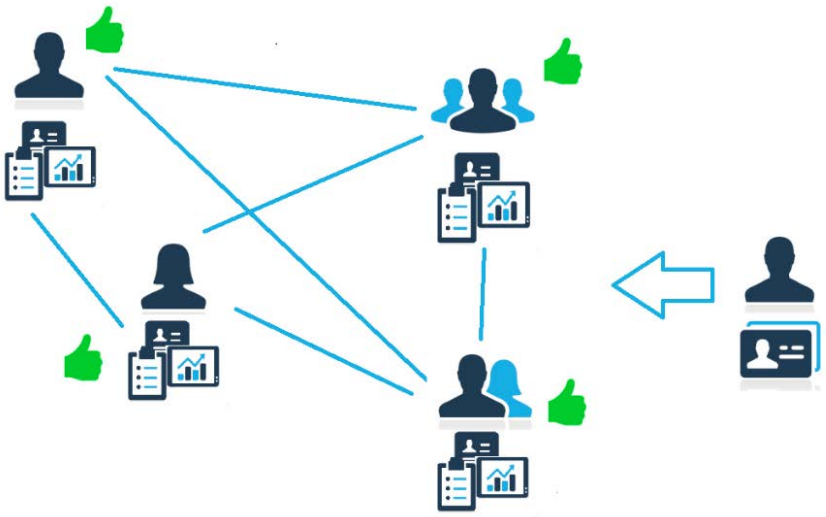
Erschwerend kommt hinzu, dass verschiedene Anbieter (z.B. Krankenhaus, Hausarzt, Facharzt etc.) in der Regel eigene Versionen und Kopien der Patientenakte speichern und verwalten, und keine von ihnen wird natürlich gegen die übrigen validiert und abgeglichen. So kann ein Patient durch aus fünf oder mehr Patienten Akten besitzen, die unterschiedliche Fehler beinhalten (z.B. Unverträglichkeiten oder falsche Blutgruppe) die alle verschiedene gesundheitliche Probleme verursachen könnten



Blockchain bietet die Validierung die der Gesundheitsbereich benötigt und das mit der notwendigen Sicherheit und Vertrauensbasis, der alle Beteiligten vertrauen können. Nicht eine einzelne Entität verantwortet die Datenspeicherung und –verwaltung, sondern alle Beteiligten Entitäten sind für die Datenintegrität und –sicherheit gemeinsam verantwortlich.
Da erstens, niemand die Datensätze verändern kann, ohne dass diese Änderung allen Beteiligten signalisiert wird und damit deren Einverständnis zur Änderung eingeholt wird (Konsens) und zweitens, keine unautorisierten “Teilnehmer” Zugriff auf die Daten haben, ohne das Einverständnis der teilhabenden Entitäten, löst die Gesundheitsbranche zwei der größten und dringlichsten Probleme von Big Data auf einen Schlag.
Die Pflegedienste können schließlich vom Konzept dahingehend profitieren, das es tatsächlich eine einzige DPA existiert auf deren Angaben sie vertrauen können, die quasi in Echtzeit für alle Teilhabenden verfügbar und validiert ist; dies ohne die Notwendigkeit der persönlichen Weitergabe von Daten oder mögliche Übertagungsfehler durch Mitarbeiter.



Entgegen einer gewöhnlichen finanziellen Transaktion bei der jeder Sender Geld an jeden beliebigen Empfänger überweisen kann, egal ob er ihn kennt oder nicht, stellt sich die Situation im Pflegebereich anders dar. Hier muss ganz klar festgelegt werden, welche Daten von wem, wann und wo erfasst werden dürfen (z.B. Wearable, Arzt etc.) und wer danach Zugriff auf welchen Bereich der Daten erhält (Familie, Facharzt, Krankenkasse etc.).
Der kollaborative Ansatz der Blockchain, wie Daten erfasst und geteilt werden verhindert viele grundsätzliche Probleme beim Austausch von Gesundheitsdaten, inclusive der Frage: Wie sehr vertraue ich dem Mittelsmann (Versicherer, Arzt etc.)
Auch wenn schon einige Organisationen versuchen den dezentralisierten Ansatz zu verfolgen, fehlt ihnen immer noch der Ansatz der Prüffähigkeit. Patienten und Anbieter müssen immer noch darauf vertrauen, dass während des elektronischer Gesundheitsinformationsaustausch die übermittelten Daten valide sind, egal wie oft sie zwischen einzelnen Stationen (z.B. Krankenhaus, Facharzt, REHA-Einrichtung oder Pflegeeinrichtung) hin und her geschickt und zwischenzeitlich modifiziert werden. Vor allem da sie oftmals von verschiedene Medien (Papier, Digital) und zwischen verschiedenen Systemen transferiert und konvertiert werden müssen.
Beim Einsatz der Blockchain um Patienten Daten elektronisch zu verwalten und zu teilen ist die Frage nach dem Vertrauen irrelevant. Jeder Patient ist bereits bekannt und überprüft.
Die Auswirkungen für den Gesundheitsbereich sind beeindrucken und können aktuell noch nicht vollumfänglich beurteilt werden. Die Vorteile für das Patientenmanagement, öffentliche Träger, Pflegekoordination und den Patienten selbst sind immens, denn dadurch, dass die Daten durch eine prüffähige Blockchain verfügbar sind, kann jeder Teilhaber sicher sein immer Zugriff auf exakt die gleichen, aktuellen und validen Informationen zu haben.



Patienten müssen sich nicht länger mit der langwierigen und frustrierenden Aufgabe beschäftigen ihre eigenen Daten von fünf oder zehn Quellen zu sammeln und zu koordinieren um sie einem neuen Facharzt zur Verfügung zu stellen. Stattdessen fügen sie einfach den Spezialisten der Blockchain hinzu und er kann auf die benötigten Daten direkt zugreifen, wie alle anderen teilhabenden Entitäten in der Blockchain auch. Der Facharzt wiederum kann absolut drauf vertrauen, dass alle Informationen bezüglich seines Patienten korrekt und valide sind.

3. Erläuterung zur Einordnung in den Fördergegenstand

Beispiel Szenario „Screenoritis“

Blockchain und Gesundheit können auf vielfältige Weise miteinander verbunden werden. Angefangen vom Health Monitoring (permanente Überwachung von Blutdruck, Blutsauerstoff, Puls, etc.), hin zu Datenanalysen und Diagnostik.
Um das mögliche Potential in einer Zukunft mit Blockchain greifbarer zu machen, möchten wir ein Szenario mit der chronischen fiktiven Krankheit namens Screenoritis* darstellen.
Zunächst ist es wichtig zu wissen, dass Screenoritis zwar zu problematischen Zuständen führen kann, die Krankheit selbst ist jedoch nicht tödlich. Zu den Symptomen zählen plötzliche Lähmungserscheinungen, Herzrasen, Bluthochdruck, Schlaflosigkeit bis hin zu kurzfristigen Gedächtnisverlust.
Die gute Nachricht ist, Screenoritis ist behandelbar und reversibel.
Gerade die korrekte Diagnose dieser Krankheit erfordert eine längerfristige Erfassung und Analyse der Gesundheitsdaten des Betroffenen, da es sich hier um spontan auftretende Symptome handelt die erst über einen längeren Zeitraum zu erkennbaren Indikatoren werden.
Der betroffene Patient ist 34 Jahre alt, liebt seine Arbeit und arbeitet überdurchschnittlich engagiert in seinem Beruf. Es ist Donnerstagnachmittag und der Betroffene ist nach einem anstrengenden Arbeitstag erschöpft und beschließt eine Pause zu machen
Es ist ein schöner sonniger Tag und so beschließt er einen Spaziergang am Fluss zu machen Nach etwas mehr als zwei Kilometern verspürt er eine leichte Übelkeit und Benommenheit. Er verlangsamt sein Tempo, bricht aber dennoch nach 100m zusammen. Ein Jogger der aus der Gegenrichtung vorbeikommt, findet den Bewusstlosen und verständigt den Notruf
Wenn die Ambulanz eintrifft scannen die Ersthelfer sein Fitnessarmband und damit seine HealthChain ID, einen einzigartigen Identifier für Gesundheitsinformationen. Als der Patient sich bei HealthChain angemeldet hat, legte er Regeln fest und benannte Personen die Zugriffe auf seine DPA erhalten und gewähren können. Die Ersthelfer verknüpfen die HealthChain ID des Patienten mit ihrer eigenen, die bestätigt, dass sie validierte Ersthelfer sind.
Danach lösen sie einen Broadcast im HealthChain Netzwerk aus, der automatisch die vier Notfallkontakte die der Patient festgelegt hat alarmiert und auffordert den Ersthelfern Zugriff auf seine Gesundheitsakte zu gewähren. Zehn Sekunden später, nachdem zwei der Kontakte den Zugriff gewährt haben, können die Ersthelfer auf die DPA zugreifen.
Ein paar Stunden später wacht der Patient im Krankenhaus auf, er ist soweit wieder in Ordnung, jedoch aufgeregt und möchte wissen was mit ihm passiert ist. Der behandelnde Arzt erklärt ihm, dass er an Screenoritis erkrankt ist.
Nachdem ein paar grundsätzliche Dinge geklärt wurden, fragt der Arzt ob er einwilligt anonymisierte Daten einer öffentlichen Studie zur Verfügung zu stellen – das ist inzwischen allgemeiner Usus und er hat kein Problem damit. Er ist gewillt seine Anamnese, Daten über den aktuellen Vorfall und die Ergebnisse der Tests die gerade stattfinden zu teilen.
Der Patient möchte mehr über die Menschen erfahren denen das Selbe zugestoßen ist und wie er seine Situation verbessern kann. Er und viele andere wählten diese Option um ihre Daten in einem isolierten Netzwerk zu teilen. Im Vergleich zur heute üblichen allgemeinen “Google”-Suche, sucht der behandelnde Mediziner Kriterien basiert und matched das Patienten-Profil gegen andere, um die maßgeblichen gemeinsamen Kriterien zu entdecken, wie zum Beispiel Geschlecht, Alter, Beruf, Arbeitsplatz oder Wohnort.
Obwohl die Screenoritis weit verbreitet ist und es Medikamente gibt die die Symptome lindern, ist die Heilung immer noch kompliziert und zugrundeliegenden Ursachen erfahren kaum Beachtung in der medizinischen Forschung. Also Teilnehmer an der Grundlagenforschung entdeckt der Patient, dass es

eine Crowdfunding Kampagne gibt um ein Medikament zu entwickeln, dass die Ursachen der Screenoritis heilt.
Seine Teilnahme wird durch "Smart Contracts" geregelt, die ihm bedingten Zugang zu den Medikamenten gewähren sobald sie verfügbar sind. Im Gegensatz zum traditionellen Crowdfunding, wird der Zugang treuhänderisch verwaltet bist die Medikamente verfügbar sind
Jetzt, nachdem der Patient ein genaues Verständnis seiner Situation hat, konsultiert er einen Spezialisten, der ihm tägliche Übungen und eine genau abgestimmte Medikation verordnet. Die genaue Einhaltung von beidem ist unabdingbar für den Erfolg der Therapie und wird vom Versicherungsträger entsprechend vergütet. Mit einem Wearable, das sowohl Position und Bewegungen überwacht, an die Einnahme der Medikamente erinnert und den allgemeinen Gesundheitszustand überwacht, sind die relevanten Daten sowohl für den behandelnden Arzt als auch den Versicherer jederzeit verfügbar.
Zusätzlich zu den reinen Überwachungsfunktionen liefert das Wearable noch weitere Vorteile, es liefert wichtige biometrische Daten zur Langzeiterfassung und kann aufgrund gewisser Faktoren die gemeinsam auftreten (z.B. Sturz + stark sinkender Blutdruck + erhöhter Puls = Schockzustand), Gefahrensituationen für den Träger erkennen und automatisch Ersthelfer alarmieren.
Solange sich der Patient an die vereinbarte Behandlung halt, werden alle Behandlungskosten automatisch beglichen – ganz ohne überflüssigen Papierkram.

4. Innovationshöhe des Konzepts im nationalen und internationalen Vergleich

Beim Einsatz der Blockchain Technologie im Gesundheitsbereich handelt es sich um eine Innovation im internationalen Bereich. Es gibt aktuell in den USA mehrere staatliche Initiativen zur Digitalisierung des Gesundheitsbereiches [1], auch unter Zuhilfenahme der Blockchain Technologie, jedoch haben diese keinen Einfluss auf Europa. Als einziges Land in Europa arbeitet Estland an der übergreifenden Einführung einer digitalen Krankenakte, jedoch in Zusammenarbeit mit einem US Unternehmen. [2]
Keine der aktuellen Initiativen geht jedoch so weit wie unser dargestelltes Konzept, das sowohl den Patienten, als auch die mit ihm in Kontakt stehenden Geräte (Wearables) mit in das Gesamtkonzept mit einbezieht. Damit besitzt sowohl das Konzept als auch die daraus entwickelte Lösung, national und international ein absolutes Alleinstellungsmerkmal.
[1] https://www.ehidc.org/innovation-challenge/41-clinical-blockchain-a-patient-experience-messaging-platform
[2] http://www.businessinsider.de/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3?r=US&IR=T

5. Kompetenzen der Mitgründer sowie der Kooperationspartner

Robertino Matausch (Konzeption, Projektmanagement, Sicherheit, Datenschutz)

- Mehr als drei Jahrzehnte Erfahrung im IT-Sektor
- Führungskompetenz:
  - Leitung von internationalen Teams von bis zu 100 Personen und verschiedenen Gewerken
  - Projektleitung und Koordination von IT-Groß-Projekten in Zusammenarbeit mit Accenture, Kudelski , NAGRA, Swiss Telecom, Comaq/HP
- Projektmanager für das Weltwirtschaftsforum Genf
  - Annual Meetings in Davos
  - Jordanien
  - Ägypten
  - New York
- Technischer Projektmanager für
  - WEF
  - BMW Williams F1
  - HP
  - Microsoft
- Technologische Schwerpunkte
  - Datenbanken
  - Hochverfügbare System (Cluster, Cloud)
  - Kryptographie

    - Verteilte Systeme
    - Datensicherheit und Datenschutz

Bertil Maier (IoT, M2M, Systemsoftware)

- Über 35 Jahre Erfahrung im IT Sektor
- Mehrjährige Erfahrung im Bereich
    - Telemedizin
    - Krankenversicherungen,
    - CT und Röntgendiagnostik
    - Administration von klassischen Patientensystemen; Schwerpunkte: Betriebssicherheit und Datensicherheit, 24/7
- Führungskompetenz:
    - Leitung von Entwicklerteam
- IoT – Engineering/ Entwicklung:
    - autarke Systeme
    - vernetzte, automatische Steuerungen, basierend auf Messwertanalysen
    - Hilfsdienste zur Alarmierung
    - Echtzeitanwendungen
    - Lasermessgeräte zur Verkehrsüberwachung
    - Rapid Prototyping mit Raspberry, Arduino und STM Entwicklungsumgebungen
    - maschinennahen Programmierung (Python und C, 42 Assembler Dialekte)
    - Schaltungsdesign
- M2M Kommunikation (WLAN, Bluetooth (LE), NFC, Funktechniken, NB-IoT)
- Entwicklung von serienreifen Platinen mit Bestückung

Chaim Ashar (Tech Scouting, Design, Produktionsplanung)

- Product Design - Product Development - Design Engineering
    - Product Design and development based on Interdisciplinary and technical approach.
    - Technical support for manufacturing - Deep knowledge in materials and production technologies.
- Innovation Management
    - Technology scouting, managing development phases from ideation to
    - successful commercialization, extensive track record of turning consumer, technical &
    - business insights into commercially-viable solutions.
    - Shaping product strategy - developing R&D processes – ensuring competitive advantage.
- Design and Entrepreneurship Educator.
- Business development
    - Experience gained in the European arena with customer engagement at senior level.
    - Ability to develop and sustain customer relationships.
    - Understanding of how to create, seek out and assess new opportunities.
- Project management
- Entrepreneur
    - ecosiv GmbH, PE funded Startup, Munich – Founder.
    - German Product Certification for carbon / ceramic heating panel.
    - “Materialica design award”: best of material.
    - “Materialica design award”: best of Product.
    - Thermosiv Germany – (2003-2009)
    - Production and development of carbon fabrics for heating applications.
    - KIPEE ltd, (2000 - 2005) VC funded Startup Israel – Cofounder.

    - Interactive game platforms.
- Patent rights, strategic co-operations, exit.

Reinier van der Drift (Tymlez, Blockchain Technology)

- Reinier van der Drift ist seit 1984 führend in der ICT Industrie
- Seit 1997 konzentriert er sich besonders auf starke Authentisierungsmethoden
- Seine aktuelles Unternehmen Tymlez entwickelt skalierbare Blockchain Technologien für den Unternehmenseinsatz. Tymlez entwickelt aktuell die schnellste und skalierbarste Blockchain Entwicklungs-/ Plattform-Software auf dem Markt.
- 2009 Gründung von Authasas
- Als Kompetenzpartner bringt er seine mehrjährige Erfahrung in folgenden Bereichen mit ein
    - Blockchain
    - Authentifizierung
    - biometrische Sicherheit

Dieter Kuhl Dipl.Kfm, Dipl.Ing (FH)

- 25 Jahre Führungstätigkeit in der Industrie als Interim Manager, Projektmanager und Geschäftsführer auf Zeit bei mittelständischen Unternehmen
- Umfangreiche Erfahrungen in der Unternehmensführung sowie in der Restrukturierung und Sanierung
- Leistungsschwerpunkte: Management von Liquidität und Cashflow, Controlling, Preisfindungs- und Kostenmanagement, Vertriebssteuerung und Organisation.
- Umsetzung von Wachstums- oder Konsolidierungsstrategien

6. Erläuterungen zur Zusammenarbeit von Unternehmen/Hochschulen/ Forschungseinrichtungen

Es sind enge Kooperation mit der der TU Dresden insbesondere der Fakultät Informatik und der Fakultät Elektrotechnik und Informationstechnik geplant.
Vorgespräche zum Thema gemeinsame Entwicklung und Forschung finden im April statt
Zusätzlich planen wir eine enge Kooperation mit slock.it [1] mit Sitz in Sachsen zu den führenden Unternehmen im Bereich IoT-Blockchain Integration zählen
Für das komplexe Feld des GPS-Tracking wird eine Kooperation mit OriginGPS aus Israel angestrebt [2].
[1] https://slock.it/
[2] https://www.origingps.com/

7. Auswirkungen auf Umwelt und Klima

Die Software Entwicklung selbst ist klimaneutral, ebenso ist eine klimaneutrale Produktion des Wearables geplant.
Die Gesamtkonzeption des Systems wirkt sich nach unserem Ermessen positiv auf die CO2 Balance im gesamten Gesundheitswesen aus. Maßgeblich dafür sind unserer Meinung nach folgende Punkte:

- Vereinfache Erfassung von medizinischen Daten wie zum Beispiel Blutdruck, Blutsauerstoffsättigung und Puls Rate, die sonst üblicherweise ambulant erfasst werden müssten
- Erleichterter Datenaustausch durch die digitale Patientenakte
    - Reduktion von Redundanzen in der Datenhaltung
    - Reduktion von Ausrucken, Versand von Dokumenten
- Optimierungen im Rettungs- und Pflegedienst
    - durch genaue GPS-Erfassung
    - Optimierung der Pflegeabläufe durch telemedizinische Datenerfassung
- Energieeinsparung durch die Reduzierung von redundanten Rechenzentren
- Energieeinsparung durch reduzierte Besuche beim Arzt

8. Ausführliche Beschreibung des Arbeitsplans:

Darstellung der Arbeitsschritte

Arbeitsschritt 1: Systemkonzeption

- Definition der Hardware/ biometrischen Sensoren für das IoT-Device/Wearable
- Modellierung der beiden Blockchains für IoT und Digitale Patientenakte
- Definition der Hard- und Software-Schnittstellen
- Workflow Design
    - Anwendermeinung sammeln, um den optimalen Ablauf der Datenerfassung und den Umfang der benötigten Daten zu erfassen
    - Designstudien für Wearable um höchstmögliche Akzeptanz der Anwender zu erreichen
    - Entwicklung eines Datenmodells in Abstimmung mit Versicherungsträgern und in Abstimmung mit den angeschlossenen Dienstanbietern

- Softwarearchitektur Definition
    - Smart Contract Structures
        - Registrar Contract (RC)
        - Patient-Provider Relationship Contract (PPR)
        - Summary Contract (SC)
    - System Node Description
    - Definition von SW-Modulen, die aus dem Workflowdesign abgeleitet werden. (Primary Software Modules)
        - Backend API Library
        - Tymlez Client
        - Database Gatekeeper
        - EHR Manager
    - DPA Blockchain Mining
        - Proof of Work Concept
    - Definition von HW Modulen die aus dem Workflowdesign abgeleitet werden

Arbeitsschritt 2: Daten Akquisition und Prototyping

- Daten Akquisition
  - Generierung von Daten zur Algorithmenentwicklung. Diese können aus Phantomen oder auch aus Real-Daten, die von Partnern zur Verfügung gestellt werden bestehen.
- Ground Truth Generierung
  - Erstellen einer Datenbank mit Referenzdaten, um die Algorithmen später zu bewerten.
- Algorithmenentwicklung für
  - Task 1: Planung
  - Task 2: Registrierung
  - Task 3: Tracking
  - Task 4: Analysis
- Erste Evaluierung
    - Qualitativer und quantitativer Vergleich der Ergebnisse der einzelnen Algorithmen mit den vorher definierten Referenzdaten (Ground Truth), z.B. Bestimmung der
    - Genauigkeit der Registrierung oder des Trackings.

Arbeitspaket 3: Integration

- User Interface Design
  - Basierend auf dem Workflow und SW Design soll ein Konzept zur Gestaltung einer anwenderfreundlichen graphischen Benutzeroberfläche erstellt werden
- Verbindung von IoT und Digitaler Patientenakte
  - Sicherstellen, dass alle erfassten Daten in der DPA erfasst und gespeichert werden. Überprüfung der Transaktionen
  - Sicherstellen, dass alle IoT Devices sich korrekt authentisieren
- Integration eines Tools zur manuellen Planung und Überprüfung
  - Einbindung der SW Komponente zur Darstellung der DPA mit der Möglichkeit manuelle Korrekturen vorzunehmen.
- Importieren von (manuellen) DPA zum Test der Validierung
- Stabilisierung des Systems
  - Sicherstellung der Korrektheit der entwickelten Algorithmen.
- Optimierung der Integration und Steuerung
  - Basierend auf den Ergebnissen der Stabilisierungsphase werden Optimierungen am System vorgenommen.
- Machbarkeitstest für die automatische Erfassung
  - Hinzuziehen von automatischer Segmentierung für die Identifikation.
- Stabilisierung, erste Performanceevaluierung und Erstellen eines Fallberichts.

Arbeitsschritt 4: Optimierung des Systems
• Pilot-Test- und Validierungsphase • Sonst. Optimierung des Systems

Zeit- und Personalplan IoT/Wearable

Arbeitsschritt 1: Pflichtenheft – Erstellung
• Systemkonzept • Definition des Funktionsumfangs • Erstellung Pflichtenheft • Freigabe Pflichtenheft
Arbeitsschritt 2: Machbarkeitsanalyse Funktions-Prototyp
• Analyse, Komponentenauswahl • Systemsoftware Apps/Desktopsoftware-Software • Hardware • Inbetriebnahme & Test • Tools, Evaluation-Boards, Lizenzen
Arbeitsschritt 3: Prototyp
• Software (System RTOS/Desktop/APP) • Hardware • Realisierung • Zulassungen & Prüfungen/ Inbetriebnahme & Test
Arbeitsschritt 4: 0-Serie (Vorserie)
• Software (System RTOS/Desktop/APP) • Hardware • Prüfsoftware • Prüfvorrichtung • Arbeitsvorbereitung • Realisierung inkl. Zulassungen & Prüfungen • Inbetriebnahme & Test
Arbeitsschritt 5: Vorbereitung der Serienfertigung
Arbeitsschritt 6: Test und Zertifizierung, Listings (CE, SIG etc.)

Zeit- und Personalplan DPA-IoT- Blockchain

Arbeitsschritt 1: Pflichtenheft – Erstellung 15 MT

- Systemkonzept
- Definition des Funktionsumfangs
- Erstellung Pflichtenheft
- Freigabe Pflichtenheft

Arbeitsschritt 2: Definition und Modellierung der Software Prototypen

- Smart Contract Structures
    - Registrar Contract (RC)
    - Patient-Provider Relationship Contract (PPR)
    - Summary Contract (SC)
- System Node Description
- Definition von SW-Modulen, die aus dem Workflowdesign abgeleitet werden. (Primary Software Modules)
    - Backend API Library
    - Tymlez Client
    - Database Gatekeeper
    - EHR Manager
- DPA Blockchain Mining
    - Proof of Work Concept

Arbeitsschritt 3: Umsetzung der Software Prototypen

- Smart Contract Structures
    - Registrar Contract (RC)
    - Patient-Provider Relationship Contract (PPR)
    - Summary Contract (SC)
- System Node Description
- Entwicklung der Module, die aus dem Workflowdesign abgeleitet werden. (Primary Software Modules)
    - Backend API Library
    - Tymlez Client
    - Database Gatekeeper
    - EHR Manager

Arbeitsschritt 4: Alpha Tests

- DPA Blockchain Mining
- Proof of Work Concept Software
- Prüfsoftware
- Prüfvorrichtung
- Realisierung inkl. Zulassungen & Prüfungen
- Inbetriebnahme & Test

Arbeitsschritt 5: Beta-Phase
• DPA Blockchain Mining • Replication • Protokolle • Kryptographie
Arbeitsschritt 6: RC0 - RC1 - RTM
• DPA Blockchain Mining • Replication • Protokolle • Kryptographie

9. Technische und wirtschaftliche Erfolgsaussichten, Risiken

Mögliche technische Risiken

Im Folgenden sind die technischen Risiken und Schwierigkeiten im Zusammenhang mit diesem Projekt aufgeführt. Eine genaue Bewertung der Risiken oder eine Absicherung des Projekts ist zum gegenwärtigen Zeitpunkt vor Beginn von Forschung und Entwicklung schwierig. Dennoch sind die Experten sehr zuversichtlich, die Schwierigkeiten bewältigen zu können.

Das Hauptrisiko des Projekts besteht darin, dass der Algorithmus für die chirurgische Planung, die Analyse der verbliebenen Membran oder das Tracking und die Registrierung die erforderliche Präzision nicht erreichen und nicht mit ausreichender Genauigkeit arbeiten.

Die Benutzeroberfläche oder der Ablauf könnten kompliziert oder zeitaufwendig werden.

Es könnten Schwierigkeiten bei der physikalischen Verbindung zwischen IoT Device und DPA-Blockchain entstehen

Langsame Algorithmen könnten die Lösung im Allgemeinen uninteressant machen.

Der langsame Ausbau oder strategische Entscheidungen betreffend des NB-IoT Ausbaus der Telekommunikationsanbieter könnten dazu führen, dass alternative Kommunikationslösungen in Betracht gezogen werden müssen, was ein Re-Design des Wearables mit sich führt.

Mögliche wirtschaftliche Risiken

Möglicherweise könnten die Kosten für dieses Projekt unterschätzt werden. Um dieses Risiko zu minimieren, wurde das Projekt bereits mit dem Produktmanager und dem Projektleiter besprochen. Die Software-Entwicklungsleitung wurde eng bei der Erstellung dieses Antrags eingebunden.

Es besteht das theoretische Risiko, dass während der Entwicklung dieses Projekts eine neue Technologie aufkommt, die die Verwendung der vorgeschlagenen Lösung überflüssig macht.

Dieses Risiko ist jedoch nicht als erheblich anzusehen.

Wirtschaftliche Verwertungsmöglichkeiten

Welche Möglichkeiten bestehen für die wirtschaftliche Verwertung der zu entwickelnden Technologien:

- Software as a Service – Firmen wie Tierion und Blockcypher zum Beispiel verlangen Gebühren für die Nutzung ihrer API und Infrastruktur
- Professional Services – Die Entwicklung und Umsetzung von Projekten für Firmenkunden.
- Pauschalen & Transaktionsgebühren – Einige Firmen bauen und warten Netzwerke für Konsortien von Partnern auf. Die Wertschöpfung erfolgt hier durch Abonnements, langfristige Verträge oder anfallende Transaktionsgebühren die im Verbund anfallen. Nicht selten sind sie Teilhaber am Netzwerk. Beispiele hierfür: Chain, R3Cev
- Service Level Agreements – Nach dem Aufbau der Plattform und der Infrastruktur für Unternehmenskunden bieten sich Service Dienstleistungen wie Pflege und Wartung an (SLA). Beispiele hierfür: Bloq, Microsoft
- Lizenzierung der Technologie an Partner
- Verkauf einer Entwicklungsplattform
- Outsourcing des Mining (Proof of Work Konzept)
- Einrichtung eines Abrechnungszentrums