



Bild: Pixels; alle anderen: Method Park

Von Bitcoin zur Economy of Things

Digitales Rezept

Die durch Bitcoin bekannt gewordene Blockchain-Technologie verspricht neue Möglichkeiten zur Automatisierung von Geschäftsprozessen. Durch ihre Eigenschaften sind Daten unveränderbar und dezentral verfügbar. Smart Contracts bieten darauf aufbauend die Möglichkeit überprüfbarer Verträge, die ganz oder teilweise ohne menschliche Interaktion ausgeführt werden können.

FABIAN ZACH UND DR. TOBIAS KÄSTNER

Das Internet of Things ist ohne Frage einer der größten Innovationstreiber unserer Zeit. Durch die Vernetzung soll unsere Geschäfts- oder Alltagswelt zum autonomen Handeln mit uns und untereinander befähigt werden. Mit der Digitalisierung vieler analoger Prozesse entsteht jedoch ein Problem: Wie kann die Echtheit digitaler Urkunden und Zeugnisse bzw. die Einzigartigkeit digitaler Wertrepräsentationen garantiert werden? In der analogen Welt fügt man schwer fälschbare Eigenschaften hinzu: Geldscheine enthalten

Wasserzeichen und Dokumente werden handschriftlich unterschrieben, um Kopien vom Original unterscheiden zu können. Doch wie geht das in der digitalen Welt, in der Dokumente inklusive aller Merkmale kopiert werden können?

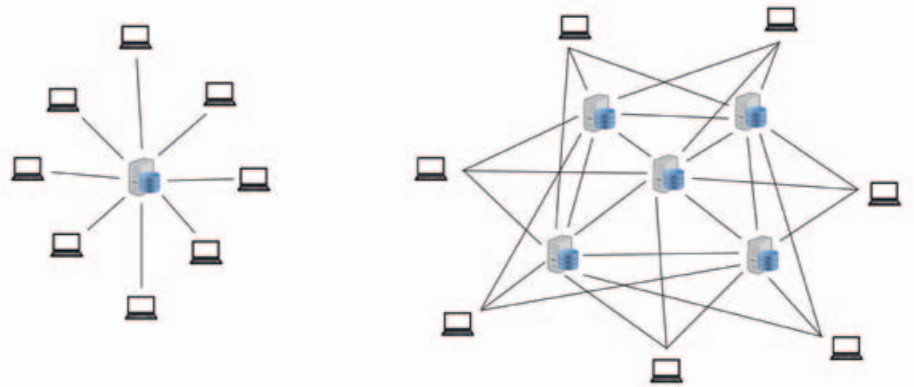
Um die Echtheit zu überprüfen, wird zum Beispiel mittels Public-Key-Kryptographie ein Dokument mit einem privaten Schlüssel signiert und die Echtheit mit dem dazu passenden öffentlichen Schlüssel verifiziert. Eine Möglichkeit, die Einzigartigkeit von Dokumenten zu kontrollieren, ist ein Client-Server-System, bei

dem der Server Besitz und Übergabe von Dokumenten verwaltet. (Bild 1) Doch wer betreibt diesen Server und warum sollte man ihm vertrauen? Sind die Daten vor Veränderung durch nichtauthorisierte Dritte geschützt? Werden die Daten objektiv verarbeitet? Was passiert, wenn dieser Server nicht mehr verfügbar ist? Bitcoin hat es geschafft, diese Probleme mithilfe weiterer kryptographischer Methoden und Dezentralisierung zu lösen. Statt eines zentralen Servers wird die Datenspeicherung und -kontrolle auf viele verschiedene Teilnehmer in

Die Blockchain

Eine Blockchain besteht aus aufeinander aufbauenden Blöcken. Jeder Block setzt sich zusammen aus einem Header und einer als Hash-Baum organisierten Liste von Transaktionen. Aus dem Header wird ein eindeutiger Fingerabdruck (Hashwert) berechnet, der sich durch jede Modifikation des Blockinhalts ändert. Neben Informationen zum Inhalt des Blocks, wie dem Hash-Wert der Wurzel des Transaktionsbaums, enthält der Header auch den Hash-Wert des vorhergehenden Blocks. Da die Veränderung eines Blocks eine Veränderung des Hash-Werts nach sich zieht, der Hash-Wert aber im darauffolgenden Block enthalten ist, können ältere Blöcke nicht verändert werden, ohne dass sich auch alle darauf folgenden Blöcke verändern (Bild 2).

einem Netzwerk (Nodes) verteilt. Sämtliche Daten werden dabei in einer sogenannten Blockchain gespeichert, einer Kette von aufeinander aufbauenden und untrennbar miteinander verknüpften Blöcken (Bild 2 und Kasten »Die Blockchain«). Jeder Node besitzt eine Kopie aller Blöcke und kann Transaktionen auf ihre Korrektheit überprüfen. Wie in einem Grundbuch werden nur neue Einträge hinzugefügt, niemals jedoch alte Einträge gelöscht. Deshalb wird diese Art Blockchain auch als »distributed ledger« bezeichnet. Welcher Stand der Blockchain gültig ist, wird dann durch die Konsensbildung vieler Nodes untereinander entschieden (Kasten »Konsens-Algorithmen«). Die Kommunikation zwischen den Nodes erfolgt dabei nach bewährtem Peer-to-Peer-Verfahren (P2P). Das Bitcoin-



Client/Server

Dezentral

Bild 1: In einem Client/Server-System werden die Daten von einem zentralen Server verwaltet. Der Server ist hier der Single Point of Failure: Fällt er aus, funktioniert das gesamte System nicht mehr. In einem dezentralen System werden die Daten von mehreren Nodes verwaltet, die miteinander kommunizieren. Fällt einer dieser Nodes aus, funktioniert das System weiterhin, da die Daten auf allen Nodes redundant verfügbar sind.

Konzept belegt, dass man mithilfe einer Blockchain ein Werteversprechen austauschen kann, ohne dass die Beteiligten einander oder einer zentralen Kontrollinstanz vertrauen müssen. Einzig die Eigenschaften der Blockchain und des verteilten Computernetzwerkes garantieren die Gültigkeit der Transaktion. Seit mittlerweile acht Jahren bewährt sich dieses Konzept und wird laufend weiterentwickelt.

Die Bitcoin-Blockchain

Auch wenn die Theorie hinter der Bitcoin-Blockchain sehr komplex ist, so bleibt die angebotene Funktionalität doch recht überschaubar. Jeder, der eine entsprechende Anzahl Bitcoins besitzt, kann Beträge an andere Teilnehmer übertragen. Dazu wird eine Transaktion an das P2P-Netzwerk gesendet; die teilnehmenden Nodes prüfen daraufhin die Gültigkeit. Ist die Transaktion korrekt, wird sie in einen der nächsten Blöcke der Blockchain aufgenommen. Das Bitcoin-Netzwerk besteht aus einer Vielzahl an Nodes, die jeweils eine Kopie der Bitcoin-Blockchain besitzen. Ein Teil der Nodes, sogenannte Miner, sammeln Transaktionen und fügen sie als neuen Block hinzu. Als »Belohnung« für das Erstellen eines

lität doch recht überschaubar. Jeder, der eine entsprechende Anzahl Bitcoins besitzt, kann Beträge an andere Teilnehmer übertragen. Dazu wird eine Transaktion an das P2P-Netzwerk gesendet; die teilnehmenden Nodes prüfen daraufhin die Gültigkeit. Ist die Transaktion korrekt, wird sie in einen der nächsten Blöcke der Blockchain aufgenommen. Das Bitcoin-Netzwerk besteht aus einer Vielzahl an Nodes, die jeweils eine Kopie der Bitcoin-Blockchain besitzen. Ein Teil der Nodes, sogenannte Miner, sammeln Transaktionen und fügen sie als neuen Block hinzu. Als »Belohnung« für das Erstellen eines

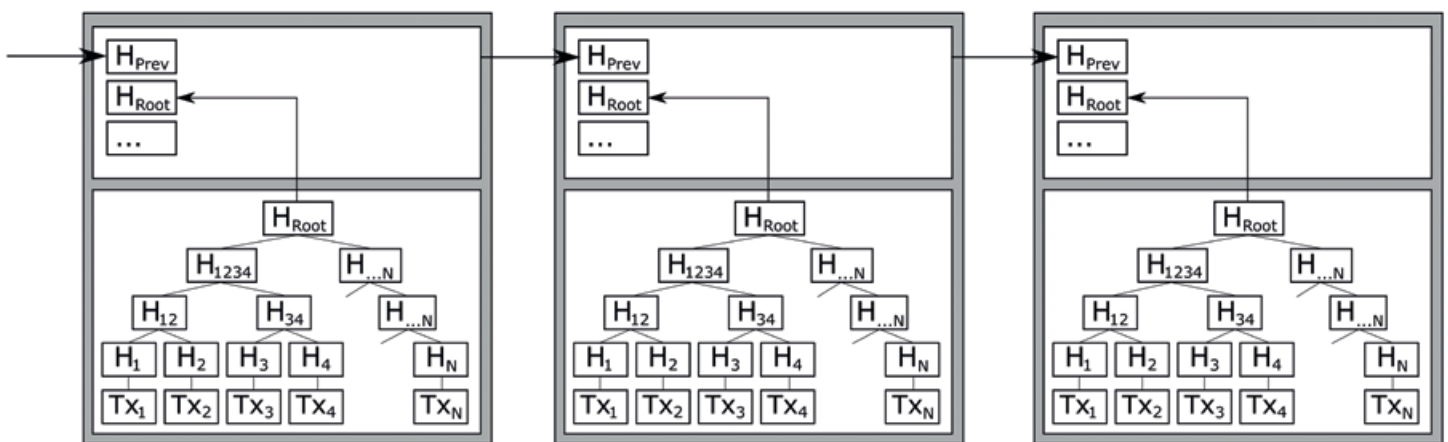


Bild 2: Aufbau einer Blockchain, siehe auch Kasten.

Konsens-Algorithmen

Jeder Node besitzt eine vollständige Kopie der Blockchain und kann neue Blöcke hinzufügen. Jeder neue Block wird per P2P an die anderen Nodes im Netzwerk verteilt, die dann die Korrektheit überprüfen und den Block an die eigene Kopie der Blockchain anhängen. Die jeweils gültige Version der Blockchain ist die mit der größten Anzahl an Blöcken bzw. der größten aufsummierten Schwierigkeit. Um zu verhindern, dass ein Node die Blockchain um beliebige Blöcke erweitert, gibt es verschiedene Konsensalgorithmen.

Beim Proof-of-Work-Algorithmus muss ein rechenintensives Kryptographierätsel gelöst und das Ergebnis im Block vermerkt werden. Die Schwierigkeit des Rätsels wird automatisch an die Rechenkapazität des Netzwerks angepasst, die Lösung ist jedoch ohne großen Rechenaufwand verifizierbar. Die Idee dahinter ist, dass es durch den benötigten Rechenaufwand nicht möglich ist, alte Blöcke in der Kette zu verändern und durch Generierung vieler neuer Blöcke eine längere Kette als die bisher gültige Blockchain zu erzeugen.

Allerdings benötigt der geforderte Rechenaufwand große Mengen Energie, die am Ende lediglich zur Sicherung der Datenintegrität dient. Deshalb wird für neuere Blockchain-Implementierungen an anderen Konsens-Algorithmen gearbeitet. Eine vielversprechende Alternative ist das Proof-Of-Stake. Dabei hinterlegen die Miner eine Kautionsumme, um das Recht zur Erstellung eines neuen Blocks zu erlangen. In periodischen Abständen erhalten sie proportional zu der hinterlegten Kautionsumme pseudozufällig die Chance, einen Block zu erstellen und werden ohne zusätzlichen Rechenaufwand in virtueller Währung belohnt.

neuen Blocks, der den kryptographischen Anforderungen genügt, bekommt der erste Node, der die Aufgabe gelöst hat, neu geschaffene Bitcoins. Ist ein Block komplett, wird er mittels P2P an die anderen Nodes versendet. Sie überprüfen die Korrektheit und fügen den Block der eigenen Blockchain-Kopie hinzu. Das Bitcoin-Netzwerk funktioniert ohne jegliche Zugangskontrolle (»permissionless ledger«). Da jeder einen Node betreiben kann und jeder Node alle Blöcke besitzt, können auch alle darin enthaltenen Transaktionen von jedem eingesehen werden. Dies ist für B2B-Transaktionen oft nicht erwünscht, weshalb andere Blockchain-Projekte Zugangskontrollen eingeführt haben. So lässt sich nachprüfen, wer Zugriff auf die gespeicherten Daten hat. Durch die Kontrolle der Teilnehmer wird auch die Gefahr der Veränderung älterer Blöcke reduziert, da die Nodes bekannt sind und ein Angreifer durch den Konsens vieler von ihm kontrollierter Miner die gültige Version der Blockchain nicht bestimmen kann. Die bei Transaktionen ausführbaren Skripte bieten bei Bitcoin nur eingeschränkte Möglichkeiten; neuere Blockchains konzentrieren sich deshalb auf erweiterte Möglichkeiten zur Ausführung von Geschäftslogik (Smart Contracts). Durch die feste Blockgröße von einem Megabyte und die Dauer des

trollen eingeführt haben. So lässt sich nachprüfen, wer Zugriff auf die gespeicherten Daten hat. Durch die Kontrolle der Teilnehmer wird auch die Gefahr der Veränderung älterer Blöcke reduziert, da die Nodes bekannt sind und ein Angreifer durch den Konsens vieler von ihm kontrollierter Miner die gültige Version der Blockchain nicht bestimmen kann. Die bei Transaktionen ausführbaren Skripte bieten bei Bitcoin nur eingeschränkte Möglichkeiten; neuere Blockchains konzentrieren sich deshalb auf erweiterte Möglichkeiten zur Ausführung von Geschäftslogik (Smart Contracts). Durch die feste Blockgröße von einem Megabyte und die Dauer des

Konsens-Algorithmus von circa zehn Minuten pro Block können theoretisch maximal ungefähr sieben Bitcoin-Transaktionen pro Sekunde ausgeführt werden. Die praktische Anzahl an Transaktionen liegt jedoch momentan bei nur etwas über drei Transaktionen pro Sekunde. Das ist zu wenig für die steigende Zahl an Teilnehmern, so dass teilweise über 100.000 Transaktionen auf ihre Ausführung warten; normalerweise vergehen bis zur Bestätigung einer Transaktion zwischen zehn und zwanzig Minuten.

Blockchain ist nicht nur Bitcoin

Die nächste Generation an Blockchain-Implementierungen baut auf dem Konzept der Bitcoin-Blockchain auf und erweitert es um neue Funktionen. Diese zweite Generation ist in der Lage, sogenannte Smart Contracts auszuführen: Komplexe Geschäftsregeln werden automatisch angewandt, sobald die in einem Smart Contract genannten Bedingungen eintreten. Unter der Schirmherrschaft der Linux Foundation haben sich mehrere Unternehmen wie IBM, Intel und ConsenSys im Hyperledger-Projekt zusammengeschlossen, um gemeinsame Standards und Protokolle für Blockchain-Technologien zu entwickeln. Das Projekt ist eine Sammlung existierender Blockchain-Implementierungen und Tools der beitragenden Unternehmen. Das ursprünglich von IBM und Digital

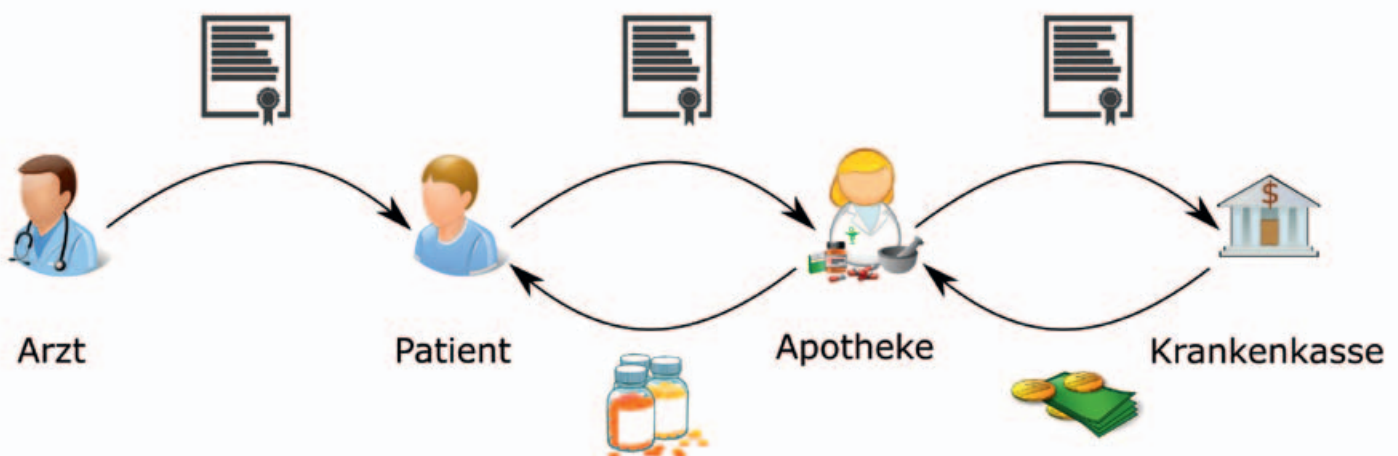


Bild 3: Das digitale Rezept wird jeweils übergeben, indem der Eigentümer im Smart Contract gesetzt wird. Die Modifier im Smart Contract stellen sicher, dass nur der aktuelle Eigentümer das Rezept weitergeben kann. Die Apotheke kann vor der Übergabe des Medikaments überprüfen, ob der Eigentümer im Smart Contract vom Patienten zur Apotheke geändert wurde.

Das digitale Rezept als Smart Contract

```

contract Insurance {
    function () payable {}
    function settleInvoice()
    {
        Prescription p = Prescription(msg.sender);
        require(p.insurance() == address(this));
        require(p.owner() == p.pharmacy());
        require(p.pharmacy() == tx.origin);
        p.pharmacy().transfer(1 ether);
    }
}

contract Prescription {
    address public owner;
    address public physician;
    address public patient;
    address public pharmacy;
    address public insurance;
    string public prescription;
    function Prescription(address _patient, address _insurance, string _prescription) {
        require(_patient != 0x0);
        require(_insurance != 0x0);
        require(bytes(_prescription).length != 0);
        require(msg.sender != _patient);
        owner = msg.sender;
        physician = msg.sender;
        patient = _patient;
        insurance = _insurance;
        prescription = _prescription;
    }
    modifier onlyFor(address account) {
        require(msg.sender == account);
        _;
    }
    modifier onlyWhenOwnedBy(address account) {
        require(owner == account);
        _;
    }
    function transferFromPhysicianToPatient()
    onlyFor(physician)
    onlyWhenOwnedBy(physician)
    {
        require(patient != 0x0);
        require(insurance != 0x0);
        owner = patient;
    }
    function scanPrescriptionInPharmacy()
    onlyWhenOwnedBy(patient)
    {
        pharmacy = msg.sender;
    }
    function tradePrescriptionForMedication()
    onlyFor(patient)
    onlyWhenOwnedBy(patient)
    {
        require(pharmacy != 0x0);
        owner = pharmacy;
    }
    function settleInvoiceWithInsurance()
    onlyFor(pharmacy)
    onlyWhenOwnedBy(pharmacy)
    {
        Insurance i = Insurance(insurance);
        i.settleInvoice();
        owner = insurance;
    }
}

```

Asset entwickelte Fabric Framework bietet die Möglichkeit, modulare Blockchain-Plattformen zu erstellen. Unter anderem kann ein Modul zur Zugangskontrolle (»permissioned ledger«) auf Basis von Zertifikaten konfiguriert werden. Mit privaten Kanälen auf der Blockchain lassen sich Transaktionen zwischen einem Teil der Teilnehmer durchführen, die nicht von anderen Teilnehmern eingesehen werden können. Da durch die Zugangskontrolle die Zahl und Identität der Nodes bekannt ist, kann man außerdem einen einfacheren und energiesparenderen, vor allem aber schnelleren Konsens-Algorithmus wählen.

Neben der Bitcoin-Blockchain haben sich auch andere »permissionless ledger« etabliert, allen voran die des Ethereum-Projekts. Die Ethereum-Blockchain bietet eine Turing-vollständige (universell programmierbar) virtuelle Maschine (Ethereum-VM). Das erlaubt anders als bei Bitcoin die Ausführung beliebiger Smart Contracts. Die Ethereum-Blockchain speichert dazu den Programmcode und -zustand von komplexen Programmen, die weit über simple Überweisungen hinausgehen. Je nach Komplexität und benötigtem Speicherplatz muss man für die Ausführung der Smart-Contract-Operationen mit der virtuellen Währung Ether bezahlen, dem Ethereum-Pendant zu Bitcoin. Damit werden einerseits Denial-of-Service-Attacken verhindert, andererseits ist der Betrag eine zusätzliche Belohnung für Miner, die die Transaktion in ihren Block aufnehmen. Smart Contracts für Ethereum werden mit der eigens entwickelten Programmiersprache Solidity erstellt, die dann in auf der Ethereum-VM ausführbaren Bytecode übersetzt wird. Im Folgenden wird mithilfe der Ethereum-Blockchain ein Smart Contract zur Digitalisierung eines Medikamentenrezepts entwickelt.

Das digitale Rezept

Laut Bundesgesundheitsministerium wurden in Deutschland im Jahr 2014 über 650 Millionen Rezepte mit einem Umsatz von über 33 Milliarden Euro ausgestellt [1]. Die Fälschung

von Rezepten ist gleichbedeutend mit dem Fälschen von Geldscheinen: Entdeckt ein Apotheker ein gefälschtes Rezept nicht, bleibt er unter Umständen auf den Kosten sitzen. Es gibt keine offiziellen Zahlen zu Rezeptfälschungen, aber in bekannt gewordenen Fällen ging der Schaden in Millionenhöhe.[2] Mit der Digitalisierung von Rezepten können einerseits Fälschungen und doppelte Einlösungen verhindert werden, andererseits lässt sich die Abrechnung zwischen Krankenkasse und Apotheke automatisieren.

Der vereinfachte analoge Ablauf (Bild 3) sieht wie folgt aus: Der Arzt stellt ein Rezept auf Papier aus, das Daten zu Krankenkasse, Patient, Arzt und Verordnung enthält, unterschreibt dieses und übergibt es dem Patienten. Dieser tauscht es in einer Apotheke gegen das verschriebene Medikament ein. Anschließend sendet die Apotheke das Originalrezept an die verantwortliche Krankenkasse, die den Betrag erstattet. Die Unterschrift des Arztes bestätigt dabei die Echtheit des Rezepts, die Einzigartigkeit verlangt jeweils die Übergabe des Originalrezepts. Dieser vereinfachte Prozess soll nun beispielhaft als Smart Contract mithilfe der Ethereum-Blockchain umgesetzt werden. Um die beteiligten Smart Contracts möglichst einfach zu gestalten, wird im Beispiel nicht näher auf Themen wie Patientenzuzahlung, Datenschutz und Anbindung externer Daten eingegangen, etwa zu Medikamenten und deren Preise. Durch die Turing-Vollständigkeit der Ethereum-VM ließen sich aber auch diese Vorgänge im Smart Contract abbilden.

Patient, Arzt und Apotheke benötigen einen Ethereum-Account, um mit Smart Contracts interagieren zu können, die auf der Ethereum-VM laufen. Ein Ethereum-Account besteht jeweils aus einem öffentlichen Schlüssel, der den Account identifiziert, und einem privaten Schlüssel, mit dem die eigene Identität bestätigt werden kann. Die Interaktion mit dem Smart Contract funktioniert über eine Distributed App (DApp), die in einem speziellen Browser läuft und in gängiger Webtechnologie

wie JavaScript und HTML entwickelt wird. Die DApp läuft nur auf dem Client, ein Server ist im Gegensatz zu herkömmlichen Webanwendungen nicht nötig.

Um ein Rezept auszustellen, erzeugt der Arzt eine neue Instanz des »Prescription« Smart Contracts mit seinem eigenen öffentlichen Schlüssel und denen des Patienten, der Adresse des Smart Contracts der Krankenkasse sowie dem Inhalt des Rezepts. Der Patient nimmt das Rezept in seine DApp auf. Dann signiert der Arzt mithilfe seines privaten Schlüssels die Übergabe des Rezepts an den Patienten. In der Apotheke legt der Patient die Rezept-Adresse vor, beispielsweise mittels QR-Code. Beim Scan in der Apotheke wird der öffentliche Schlüssel der Apotheke im Smart Contract eingetragen.

Der Patient signiert zum Einlösen des Rezepts die Übergabe an die Apotheke mit seinem privaten Schlüssel. Durch die Übergabe des Rezepts hat der Patient keinen weiteren Zugriff auf das Rezept und kann es damit auch kein zweites Mal einlösen. Zur Abrechnung kommuniziert die Apotheke über den »Prescription« Smart Contract mit der Krankenkasse. Der Smart Contract der Krankenkasse validiert die Daten des Rezepts und veranlasst die Auszahlung des Betrags an die Apotheke (Kasten »Das digitale Rezept ...«).

Literatur:

- [1] [http://www.bundesgesundheitsministerium.de/service/publikationen/gesundheits/details.html?bmg\[pubid\]=2950](http://www.bundesgesundheitsministerium.de/service/publikationen/gesundheits/details.html?bmg[pubid]=2950)
 [2] <https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/05/20/vorsicht-falschung>

Durch die Speicherung der Daten in der Blockchain ist eine nachträgliche Veränderung des Rezepts unmöglich. Da von jedem Ort auf die Blockchain zugegriffen werden kann, entfällt auch das Versenden und Aufbewahren des Rezepts in Papierform. Die Implementierung mittels Blockchain benötigt keine zentralen Server, die Teilnehmer müssen nur einen Ethereum-Account und die DApp besitzen.

Weitere Anwendungen in Aussicht

Noch befindet sich die Blockchain-Technologie am Anfang der Entwicklung; viele Unternehmen investieren momentan in die Erforschung neuer Einsatzgebiete. Das Konzept verspricht hochverfügbaren, sicheren und dezentralen Speicher sowie die transparente Ausführung von Geschäftsprozessen. Durch die dezentrale Speicherung und automatisierte Ausführung von Smart Contracts kann man im Internet of Things Daten ablegen und auswerten, ohne auf zentrale Server- oder Cloud-Lösungen angewiesen zu sein. (ne)



FABIAN ZACH
Software Engineer
Method Park



DR. TOBIAS KÄSTNER
Expert Software Engineer IoT
Method Park