VDE SPEC

Einstieg in die Blockchain Technologie

VDE SPEC 90001 V1.0

VDE

Inhaltsverzeichnis

Vorwort ... 3
1 Anwendungsbereich ... 5
2 Normative Verweisungen ... 5
3 Begriffe und Abkürzungen ... 5
3.1 Begriffe ... 5
3.2 Abkürzungen ... 6
4 Typen von Blockchains ... 7
4.1 Allgemeines ... 7
4.2 Public-Permissionless Blockchain ... 7
4.3 Public-Permissioned Blockchain ... 7
4.4 Private-Permissioned Blockchain ... 7
4.5 Private-Permissionless Blockchain ... 7
5 Blockchain-Anwendungen ... 8
5.1 Allgemeines ... 8
5.2 Finanz- und Versicherungswirtschaft ... 8
5.3 Versicherung ... 8
5.4 Energiewirtschaft ... 8
5.5 Handel und Industrie ... 8
5.6 Logistik und Einkauf ... 9
5.7 Gesundheitswesen ... 9
5.8 Automatisierung in der Verwaltung und für Dienstleistungen ... 9
5.9 Dezentrales Identitätsmanagement zur Authentifizierung/Autorisierung ... 9
5.10 Weitergehende Anwendungspotenziale auf Basis von Smart-Contracts ... 9
6 Sicherheit und Zuverlässigkeit ... 10
6.1 Verschlüsselung von Daten ... 10
6.2 Ablegen von Daten versus Ablegen von Zusammenfassungen ... 10
6.3 Angriffe auf eine Blockchain als Ganzes ... 10
6.4 Software-Bugs und falsche Verwendung von Smart Contracts ... 11
7 Ressourcenbedarf einer Blockchain ... 11
7.1 Speicher- und Rechenbedarf ... 11
7.2 Anreiz mit Coins ... 11
Anhang A Konsensverfahren ... 12
A.1 Allgemeines ... 12
A.1.1 Proof-of-Work (PoW) ... 12
A.1.2 Proof-of-Authority ... 12
A.1.3 Proof-of-Stake (PoS) ... 12
A.1.4 Proof-of-Activity (PoA) ... 12
A.1.5 Proof-of-Burn (PoB) ... 12
A.1.6 Proof-of-Capacity (PoC) ... 12
A.1.7 Proof-of-Elapsed Time (PoET) ... 13
Literaturhinweise ... 14

Vorwort

Veröffentlichungsdatum dieser VDE SPEC: 30. März 2020.

Vorausgegangener VDE SPEC-Entwurf: Roter Leitfaden Blockchain.

Dieses Dokument wurde von der VDE-SPEC-Projektgruppe „VDE/DKE Task Force „Energy Blockchain“, DKE/GRP_Energy Blockchain, des VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (www.vde.com) erarbeitet.

Diese VDE SPEC wurde nach dem VDE SPEC-Verfahren erarbeitet. Die Erarbeitung von VDE SPEC erfolgt in Projektgruppen und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Diese VDE SPEC ist **nicht** Bestandteil des VDE-Vorschriftenwerks oder des Deutschen Normenwerks. Diese VDE SPEC ist insbesondere auch **keine** Technische Regel im Sinne von § 49 EnWG.

Die VDE/DKE Task Force „Energy Blockchain” ist eine Expertengruppe, die im Rahmen dieser Aktivitäten die praktischen Anwendungen der Blockchain Technologie untersucht und die Erkenntnisse in die nationalen und internationalen Expertengruppen der Normung einbringt.

Die vorliegende VDE SPEC zum Thema Blockchain-Technologie ist das Ergebnis einer Literaturrecherche des VDE und der Kommentierungen durch Fachexperten der Task Force „Energy Blockchain” zur online gestellten Version des Roten Fadens. Er stellt für den Einstieg eine Übersicht der wichtigsten Begriffe zusammen. Darüber hinaus werden, thematisch geordnet, am Ende jedes Kapitels Links zu weiterführender Literatur und einschlägigen Informationsseiten im Internet zur Verfügung gestellt.

Rückmeldungen können Sie bitte an folgende Mail-Adresse senden:

Wolfgang.Klebsch@vde.com

Sollten Sie Interesse an der aktiven Mitarbeit in der Task Force „Energy Blockchain“ haben, nehmen Sie bitte Kontakt auf mit Sebastian.Kosslers@vde.com

An dieser Stelle herzlichen Dank an die Experten für ihre wertvollen Inputs:

Nicolai Bartkowiak, Volkswagen

Hans Buhl, Fraunhofer FIT

Gilbert Fridgen, Universität Bayreuth

Philipp Lämmel, Fraunhofer FOKUS

Sven Radszuwill, BDVB

Jasper Reekers, TU Berlin

Bent Richter, Karlsruhe Institute of Technology (KIT)

Sebnem Rusitschka, Blockchain Bundesverband

Philipp Sandner, Vorsitzender des Frankfurt School Blockchain Center

Volker Skwarek, HAW Hamburg

Nils Urbach, Universität Bayreuth

Christian Welzel, Fraunhofer FOKUS

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann die VDE SPEC-Projektgruppe weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass die VDE SPEC-Projektgruppe für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden VDE SPEC entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Im Zuge der Herstellung und/oder Einführung von Produkten in den Europäischen Binnenmarkt muss der Hersteller eine Risikoanalyse durchführen, um zunächst festzustellen, welche Risiken das Produkt möglicherweise mit sich bringt. Nach Durchführung der Risikoanalyse bewertet er diese Risiken und ergreift gegebenenfalls geeignete Maßnahmen, um die Risiken wirksam zu eliminieren oder zu

minimieren (Risikobewertung). Die vorliegenden VDE SPEC entbindet den Nutzer nicht von dieser Verantwortung.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. VDE/DKE ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

In dieser VDE SPEC wurden keine Bezüge zu existierenden Normen und Zusammenhang zum Deutschen Normenwerk festgestellt.

1 Anwendungsbereich

Die vorliegende VDE SPEC zum Thema Blockchain-Technologie ist das Ergebnis einer Literaturrecherche des VDE und der Kommentierungen durch Fachexperten der Task Force „Energy Blockchain“. Er stellt für den Einstieg eine Übersicht der wichtigsten Begriffe zusammen. Darüber hinaus werden, thematisch geordnet, am Ende jedes Kapitels Links zu weiterführender Literatur und einschlägigen Informationsseiten im Internet zur Verfügung gestellt.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

– IEC Electropedia: unter http://www.electropedia.org/

– ISO Online Browsing Platform: unter http://www.iso.org/obp

3.1.1 Blockchain

Eine „Blockchain“ ist eine Datenstruktur, in der Daten vom Design her unveränderbar gespeichert werden. Dies geschieht in Form von verketteten Datenblöcken (daher der englische Begriff „block" "chain“). Neu hinzugefügte Daten werden regelmäßig zu einem neuen Block zusammengeführt, der mit einem Daten-„Fingerabdruck“ (engl. hash) und einem Zeitstempel oder einer aufsteigenden Ordnungszahl versehen wird. In einigen Arten von Blockchains lassen sich auch ausführbare Programm-Logiken [Smart Contracts] fälschungssicher speichern.

Anmerkung 1 zum Begriff hash: Der Hash-Wert ist eine kryptographische Prüfsumme über alle Daten des betrachteten Blocks.

3.1.2 Distributed Ledger

Um Fälschungssicherheit zu erreichen, werden automatisch exakte Kopien generiert und über eine Vielzahl unabhängiger Rechner verteilt, die im Idealfall global verteilt sind und von unterschiedlichsten Teilnehmern und Organisationen betrieben werden

Anmerkung 1 zum Begriff: Vorausgesetzt wird hier, dass eine Blockchain vom Typ „public permissionless“ (siehe 4.2) zum Einsatz kommt.

Da es sich bei den gespeicherten Daten meist um ein Logbuch von Transaktionen handelt, spricht man auch von einem verteilten Hauptbuch, Kassenbuch oder Register, englisch „Distributed Ledger“ (DLT). In der öffentlichen Diskussion werden Blockchain und DLT als synonym angesehen.

Anmerkung 2 zum Begriff: Die Blockchain stellt objektiv nur eine Ausprägung von DLT dar, andere Beispiele sind IOTA/Tangle oder Hashgraph.

3.1.3 Manipulationssicherheit

Der Hash jedes Datenblocks einer Blockchain ist eindeutig. Da bei der Berechnung dieses Wertes jeweils auch der Daten-Fingerabdruck des Vorgängerblocks berücksichtigt wird, ist der Hash des neuesten Blocks zugleich der Daten-Fingerabdruck der gesamten Blockchain.

Anmerkung 1 zum Begriff: Eine Datenstruktur dieses Typs ist als Hash-Baum bzw. Merkle-Tree bekannt und wird in der Kryptographie vielseitig verwendet.

Damit fällt auch die kleinste Änderung älterer Daten beim Vergleich mit anderen Rechnern sofort auf. Manipulationssicherheit wird mit Hilfe automatischer Konsensbildung im Netzwerk erreicht.

3.1.4 Konsensbildung

Die Blockchain kommt als Distributed Ledger ohne eine zentrale Autorität (Intermediär) aus, so dass die Konsistenz der Daten auf andere Weise sichergestellt werden muss. Ein neu anzuhängender Block

muss auf allen im Netzwerk beteiligten Rechnern (Netzwerkknoten) identisch sein. Um das sicherzustellen, sind bestimmte Bedingungen festgelegt, welche ein Block erfüllen muss, um an eine Blockchain gehängt bzw. von allen Knoten akzeptiert zu werden. Bei Unstimmigkeiten wird auf der Grundlage eines vorgegebenen Algorithmus automatisch ermittelt, welche der Kopien verworfen und welche von allen Rechnern anerkannt wird. Dieser Vorgang wird auch Konsensbildung genannt.

Anmerkung 1 zum Begriff: Es wird zwischen implizitem und explizitem Konsens unterschieden. Beim impliziten Konsens erzeugt ein Miner einen Block aufgrund seiner Autorisierung (Proof-of-X-Verfahren). Andere Miner hängen an diesen erzeugten Block einen nächsten Block an, weil sie diesen gerade erzeugten Block genauso berechnet hätten. Beim expliziten Konsens (z. B. Hyperledger Fabric) gibt es eine separate Instanz im System, die erzeugte Transaktionsergebnisse überprüft und über vorgegebene Mehrheitsprinzipien (endorsement policy) bestätigt.

3.1.5
Vertrauen ohne Intermediäre

Traditionell erfordert die Übertragung von Werten (z. B. Geldbeträge, Besitztitel, Zertifikate, Aus-weise, Rechte usw.) Intermediäre (z. B. Banken oder Behörden), denen beide Transaktionspartner vertrauen und welche die Transaktion abwickeln. Nutzer einer Blockchain (oder anderer DLT-Ansätze) vertrauen auf deren kryptographisches Protokoll und darauf, dass ein Großteil der Beteiligten (Peers) sich ehrlich verhält. Zukünftig werden Distributed Ledger in vielen Anwendungsbereichen Intermediär-Funktionen übernehmen und damit verschiedenste Peer-to-Peer-Transaktionen ermöglichen („Vertrauen durch Transparenz“).

3.1.6
Lesen, Schreiben und Löschen

Lesen: Mit entsprechenden Abfragetools (häufig online verfügbar) kann der komplette Datenbestand einer Blockchain durchsucht und ausgelesen werden. Soll Einsehbarkeit verhindert werden, können die Daten auch verschlüsselt in der Blockchain abgelegt werden. Dies führt zu weiteren Herausforderungen wie z. B. der Frage, wo das Schlüsselmaterial abgelegt werden soll (siehe 7.1).

Schreiben: Im Falle einer Blockchain des Typs public-permissionless (siehe 5.2) werden neue Daten nicht direkt angehängt, sondern zunächst an alle Rechner im Netzwerk weitergeleitet, bis nach einigen Minuten ein Rechner alle aufgelaufenen Daten zu einem neuen Block „verpackt“ und an die Blockchain anhängt.

Löschen: Hash-gesicherte Daten können von einzelnen Teilnehmern weder gelöscht noch über-schrieben werden. Dies ist das wichtigste Alleinstellungsmerkmal der Blockchain-Technologie. Falsche Einträge lassen sich grundsätzlich mit einem gültigen Korrektureintrag richtigstellen.

Anmerkung 1 zum Begriff: In Ausnahmefällen können Löschungen auf der Grundlage von Mehrheits-entscheidungen (sog. hard forks) erfolgen. Angreifer können Daten nur dann löschen oder überschreiben, wenn sie mindestens 51 % der Berechnungskapazität kontrollieren.

3.1.7
Smart Contract

In manchen Blockchains sind nur einfache Informationen gespeichert. So enthält die Bitcoin-Blockchain Einträge wie z. B. „Teilnehmer A überweist Teilnehmer B zwei Bitcoins“. Andere Blockchains bieten weitergehende Funktionen: Die Ethereum-Blockchain erlaubt bedingte Transaktionen, wie z. B. „Nach elektronischer Bestätigung der Lieferung des Produkts P überweist A an B den Betrag X“. Damit lässt sich Geschäftslogik automatisch ausführen, man spricht von einem Smart Contract.

Anmerkung 1 zum Begriff: Allgemeiner formuliert, handelt es sich bei einem Smart Contract um ein Programm, das auf Basis eines Konsenses über die Ausführungsergebnisse im DLT-System verteilt und ggf. gespeichert wird. Die einfachste Form des Smart Contracts ist der Token.

In Kombination mit digitalen Werten, die auf einem DLT-System gespeichert sind, werden Smart Contracts zu einer grundlegenden Innovation für neue Geschäftsmodelle.

Anzumerken ist, dass Smart Contracts auf jedem der Rechner im Netzwerk lokal ausgeführt werden. Im Vergleich zu einer zentralen Lösung sind Smart Contracts damit sehr ressourcenaufwändig.

3.2 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen.

DLT	Distributed Ledger
DRM	Digital Rights Management
DSVGO	Datenschutzgrundverordnung

DOA	Distributed Autonomous Organization
ICO	Initial Coin Offering
PoA	Proof-of-Activity
PoB	Proof-of-Burn
PoC	Proof-of-Capacity
PoS	Proof-of-Stake
PoW	Proof-of-Work
TEE	Trusted Execution Environment

4 Typen von Blockchains

4.1 Allgemeines

Bei Blockchains unterscheidet man je nach der Sichtbarkeit der Daten zwischen öffentlichen und privaten Varianten. Bei der privaten Variante ist die Sichtbarkeit beschränkt auf autorisierte Teilnehmer. In beiden Fällen kann das Recht auf Anhängen von Blöcken an die Kette gesteuert werden: man spricht hier von den Eigenschaften „permissioned“ bzw. „permissionless“.

In allen Fällen können auf einer Blockchain gespeicherte Daten verschlüsselt werden, so dass die Teilnehmer zwar die Transaktionen, nicht jedoch die darin transportierten Inhalte sehen können.

ANMERKUNG Ein wichtiger Punkt beim Einsatz von DLT ist die Tatsache, dass die „Unveränderbarkeit“ von Daten auch bedeutet, dass sie nicht gelöscht werden können, was nicht erst mit den neuen Regeln der DSGVO ein Problem darstellen kann. Hierfür existieren bereits Lösungsansätze, die im Einzelfall bewertet werden müssen.

4.2 Public-Permissionless Blockchain

„Jeder darf zugreifen und validieren“

Alle Einträge liegen offen, während alle Teilnehmer anonym oder pseudonym bleiben. Beispiele: Bitcoin-Blockchain, Ethereum, EW Blockchain.

4.3 Public-Permissioned Blockchain

„Jeder darf zugreifen, nur Berechtigte dürfen validieren“.

Der Zugang für Teilnehmer wird durch Technologie gesteuert. Beispiel: Das System Sovrin der Firma Evernym ist eine Konsortiallösung, bei der die Endnutzer des Systems den vorgegebenen Rahmenbedingungen und Regeln unterliegen.

4.4 Private-Permissioned Blockchain

„Nur Berechtigte dürfen zugreifen und validieren“

Alle Teilnehmer sind bekannt. Da sich die Teilnehmer oft untereinander kennen und ihre Anzahl üblicherweise gering ist, vereinfacht sich die Konsensfindung so, dass die Blockerstellung extrem schnell wird. Ein Beispiel ist das System Corda des R3-Konsortiums von 40 Großbanken, dem auch die Deutsche Bank und die Commerzbank angehören. Exergy und Power Ledger sind weitere Beispiele für Blockchains des Typs private-permissioned.

ANMERKUNG Exergy ist ein Energiemarktplatz auf Blockchain-Basis. Power Ledger nutzt die Blockchain-Technologie, um Energiehandel innerhalb von Gebäuden und zwischen Netzwerken zu ermöglichen.

4.5 Private-Permissionless Blockchain

„Jeder kann sich am Validierungsprozess beteiligen, aber nur Berechtigte dürfen zugreifen“

Dieser Blockchain-Typ steht im Verdacht, auf den Schneeball-Effekt aus zu sein und daher eher betrügerische Zwecke zu verfolgen.

ANMERKUNG Ein legales Beispiel könnte sein, dass 40 Banken an einer private-permissionless Blockchain teilnehmen und 5 Banken im Sinne der anderen validieren.

5 Blockchain-Anwendungen

5.1 Allgemeines

Die Bandbreite möglicher Anwendungen der Blockchain-Technologie ist groß und bezieht alle Branchen, von Finanz- und Versicherungswirtschaft, über Energiewirtschaft, Industrie, Handel, Einkauf, Logistik bis hin zu Gesundheitswesen und Verwaltung, mit ein. Inwieweit diese Anwendungen disruptive Innovationen darstellen oder lediglich einen vorübergehenden Hype bedienen, wird sich in der Zukunft zeigen.

5.2 Finanz- und Versicherungswirtschaft

Kryptowährung/Crypto-Asset:

- Inflationsgeschützte und zentralbankunabhängige Alternative zu konventionellen Währungen.
  - In einigen Entwicklungsländern spielen Kryptowährungen bereits eine Rolle als Alternative zur inflationsbelasteten Landeswährung.
- Ausgabe von Crypto-Assets zur Kapitalbeschaffung für Startups - in Anlehnung an normale Börsengänge Initial Coin Offering (ICO) genannt.

Wertpapierabwicklung:

- Digitale Emission von Aktien und anderen Wertpapieren.
- Automatischer Abgleich von Börsentransaktionen zwischen allen Beteiligten.
- Automatische Zinszahlungen und Rückzahlungen bei Fälligkeit.

Compliance-Sicherung („Know-your-Customer"):

- Prävention von Geldwäsche durch das fälschungssichere Festhalten von Transaktionen (Beträge, Zeitstempel, Parteien).

5.3 Versicherung

Versicherungsvertrag als Smart Contract, der in einer Blockchain eingetragen und zeitnah automatisch ausgeführt wird. Beispiele:

- Entschädigungsversicherung für Flugverspätungen (z. B. Fizzy von AXA).
- Nutzungsabhängige Policierung in der Fahrzeug-Versicherung.

5.4 Energiewirtschaft

Im Bereich der Energiewirtschaft kommen nur Blockchains mit eingeschränktem Zugriff und Validierungsrechten in Frage, d. h. Blockchains vom Typ private-permissioned, wie sie im Rahmen des Projekts Hyperledger implementiert werden. In Hyperledger werden Programm-Logiken wie Smart Contracts als „Chaincodes" bezeichnet. In der REDII (Renewable Energy Directive II) der EU-Kommission werden einige Anwendungsideen beschrieben, die den Eigenverbrauch, die Direktvermarktung bis hin zum Peer-to-Peer-Austausch von Energie innerhalb von Erneuerbare-Energie-Communities betreffen. In allen Fällen geht es um digitales Vertragsmanagement und Prozessautomatisierung, wie:

- Peer-to-Peer-Handel zwischen Prosumer und Verbraucher bzw. sonstigen Partnern, z. B. mit Enerchain für Over-the-Counter-Geschäfte.
- Peer-to-Peer- und Token-basierte Geschäfts- und Finanzierungsmodelle für dezentrale Energiesysteme.

Allen diesen Anwendungen ist gemein, dass sie auf nicht regulierte Intermediäre wie Energiehandelshäuser und -börsen oder Clearinghäuser verzichten können.

5.5 Handel und Industrie

Kreativwirtschaft:

- Produktion und Sharing/Vertrieb digitaler Inhalte (z. B. Avatare mit Ausstattung, Musik, Bilder, Videos) in automatisch limitierter Auflage oder sogar als Unikate.
- Abwicklung und Abrechnung des Verleihs digitaler Inhalte (Pay-per-Use; Pay-per-Service).

Verleih:

- Automatische Freischaltung und Abrechnung beim Sharing von Fahrzeugen oder Wohnraum.

Industrieproduktion:

- Absicherung der Integrität von Daten (z. B. 3D-Druck eines Ersatzteils) durch Ablegen eines Fingerabdrucks o.ä. in einer Blockchain bzw. Verhinderung unautorisierter Vervielfältigung.
- Peer-to-Peer-„Handel“ zwischen Maschinen, z. B. Bereitstellung von Diensten, Materialien, Daten.
- Digital Rights Management (DRM), Copyright-relevante Bereiche.

5.6 Logistik und Einkauf

Anwendungen im Bereich Logistik und Einkauf befassen sich grundsätzlich mit der Optimierung des Zusammenspiels und der Kommunikation aller an der Lieferkette beteiligten Parteien. In n-Tier-Supply-Chains schaffen sie auf der Grundlage von Smart Contracts Transparenz über Prozessfort-schritte bzw. Prozessstopper, ohne die Anonymität der Beteiligten aufzuheben.

Transparente Vertriebsketten:

- Überwachung der Gültigkeit von Qualitäts-, Herkunfts-, Bio- oder Fairtrade-Siegeln durch manipulationssichere Dokumentation von Produkteigenschaften und/oder Stationen in der Herstellungs- und Lieferkette (z. B. Blutdiamanten, Tropenholz, Bekleidung usw.).

Zertifizierung:

- Erschwerung von Produktfälschungen, indem digitale Zwillinge individueller Produkte manipulationssicher auf eine Blockchain abgebildet werden (Beispiel: Medikamente).

Qualitätssicherung in innerbetrieblichen Prozessen:

- Manipulationssichere Aufzeichnung von Produktionsdaten, Qualitätsmessungen, Wartungsdaten bis hin zur Absicherung digitaler Zwillinge.

5.7 Gesundheitswesen

- Manipulationssicheres Festhalten (verschlüsselter) Gesundheitsdaten für die Nutzung durch Ärzte, Apotheken und Krankenkassen nach individueller Freigabe durch den Patienten.
- Überwachung von Gesundheits- oder Fitnessdaten zur Beeinflussung von Versicherungstarifen.
- Abrechnung von Ärzten und Apotheken mit Krankenkassen.

5.8 Automatisierung in der Verwaltung und für Dienstleistungen

- Identitätsmanagement bei der Ausstellung von Ausweisen.
- Festhalten von Geburten, Eheschließungen usw. ohne die Notwendigkeit physischer Dokumente.
- Manipulationssichere Verwaltung von Grundstücken (Eigentum, Grundschulden usw.).
- Gewährung von Patenten.
- Automatische Erhebung/Erstattung von Umsatzsteuer und anderen Steuerarten.
- Beweiskräftige Aufzeichnung von Daten als Grundlage z. B. für Buchprüfung/Revision, Gerichtswesen, Notariat, Gutachten usw.

5.9 Dezentrales Identitätsmanagement zur Authentifizierung/Autorisierung

- Vergabe und Verwaltung digitaler Identitäten.
- Zugangsregelung für Gebäude und Organisationen.
- Zugangsregelung für Geräte und Netze.
- Zugangsregelung für Online-Bereiche.
- Abwicklung von Online-Geschäften.

Dezentrales Identitätsmanagement wird vor allem in Entwicklungsländern eine zentrale Rolle spielen.

5.10 Weitergehende Anwendungspotenziale auf Basis von Smart-Contracts

Mit Smart Contracts lassen sich beliebig komplexe Blockchain-Anwendungen realisieren. Sie reichen von einfacheren dezentralen Anwendungen (dApps) bis hin zu dezentralen autonomen Organisationen (DAOs). Damit eröffnen Smart Contracts ein Universum möglicher Anwendungen, von der einfachen bedingten Überweisung bis hin zu weitreichenden oder gar utopischen Potenzialen wie der autonomen Verwaltung einer Gesellschaft.

1) Smart Right and Obligation

Beispiel: Konsument kauft digitalen gestreamten Content.

2) Basic Smart Contract

Beispiel: Vermieter sperrt nicht zahlenden Mieter aus der Ferne aus seinem Apartment aus.

3) Multiparty Smart Contract

Beispiel: Verkäufer leiht Käufer Mittel, um ein Haus zu kaufen.

Weitere Beispiele: Mietkautionskonto, Dividendenauszahlung, Handhabung von Krediten.

4) Distributed Autonomous Business Unit

Beispiel: Eine Unternehmenseinheit hat eigene Anleihen ausgegeben und ermöglicht den Käufern, ihre Zahlungen auf einem Distributed Ledger selbst zu überwachen.

5) Distributed Autonomous Organization (DAO)

Beispiel: Selbstfahrender Elektro-LKW führt gegen Bezahlung autonom Peer-to-Peer-Lieferungen aus, steuert bei Bedarf eine Ladestation an, um zu laden, und bezahlt für die geladene Energie.

ANMERKUNG 1 Ein anderer Name für **Distributed Autonomous Organization** ist **Distributed Autonomous Corporation**. Darüber hinaus gibt es die Distributed Autonomous Cooperative, die in ihrer Komplexität zwischen Organisation und Corporation anzusiedeln wäre.

ANMERKUNG 2 Der Begriff DAO für Distributed Autonomous Organisation ist aufgrund einiger Fehlschläge bereits negativ belegt. Er assoziiert, dass sich Unternehmen algorithmisch abbilden und automatisieren lassen. Ein neutralerer Begriff wäre „Verknüpfte, sich gegenseitig steuernde Smart Contracts“. Kritiker sehen DAO nur als visionäres Wunschdenken. Die Forschungsdisziplin „Operations Research“ beschäftigt sich seit Jahrzehnten damit, Unternehmens- und Entscheidungsabläufe mathematisch zu modellieren. Angesichts der Komplexität dieses Unterfangens erscheint es unwahrscheinlich, dass ein Tool wie die Blockchain das Schaffen könnte.

6) Distributed Autonomous Government

Beispiel: Siedler in einem zuvor unbewohnten Gebiet schaffen sich eigene, sich selbst durchsetzende Regierungsdienste.

7) Distributed Autonomous Society

Beispiel: Siedlergruppen aus verschiedenen Gebieten schließen selbst durchsetzende Handelsabkommen ab.

6 Sicherheit und Zuverlässigkeit

6.1 Verschlüsselung von Daten

Da Daten in einer Blockchain grundsätzlich für jedermann lesbar sind, werden sie (abhängig von der Implementierung) oder auch aus Datenschutzgründen in verschlüsselter Form abgelegt. Für die Verschlüsselung werden üblicherweise bewährte Verfahren wie Public/Private-Key-Kryptografie verwendet, wobei die Teilnehmer für ihr Schlüssel- und Identitätsmanagement selbst verantwortlich sind, d. h. eine Blockchain macht hierzu keine Vorgaben. Im Falle einer Blockchain vom Typ private-permissioned (siehe 5.4) können die Daten auch hinter eine Firewall gepackt werden, wodurch der Zugriff noch beschränkter wird.

An dieser Stelle sei darauf hingewiesen, dass zukünftige Entwicklungen im Bereich des Quantum Computing die Sicherheit der Verschlüsselung wie auch die von Distributed Ledger Technologien an sich grundsätzlich in Frage stellen könnten.

6.2 Ablegen von Daten versus Ablegen von Zusammenfassungen

Da die Datenmengen, die in einer Blockchain abgelegt werden, relativ klein sind, werden dort häufig nicht die Daten selbst, sondern nur eine mathematische Zusammenfassung (meist als Hash) eingetragen. Der Teilnehmer muss sich dann zwar noch anderweitig um die Speicherung der Originaldaten kümmern, kann aber später mit dem Eintrag in der Blockchain deren Zustand zu einem bestimmten Zeitpunkt nachweisen. Dies ist die Grundlage aller notarieller Anwendungen.

6.3 Angriffe auf eine Blockchain als Ganzes

Um eine Blockchain vom Typ public-permissioned mit Proof-of-Work als Ganzes zu manipulieren, muss ein Angreifer die Mehrheit aller Rechner unter seine Kontrolle bringen. Dies ist bei einer Ver-teilung über

viele Länder, Jurisdiktionen und Betreiber und der Offenlegung des Codes als Open Source schwierig und fällt schnell auf. Auf kleinere Systeme hat es bereits erfolgreiche Mehrheitsangriffe gegeben. Die überwiegende Zahl der Angriffe sind jedoch Phishing-Attacken, bei denen Zugangsdaten ausgespäht werden (siehe z. B. den Bitcoin Gold Hack). Andere indirekte Angriffsszenarien sind Mining-Malware, Selfish-Mining, (d)DOS, kompromittierte Crypto-Wallets, Transfer-Trojaner, usw. Im Falle von Proof-of-Burn müsste sich ein Angriff auf diejenigen mit dem meisten Geld fokussieren, um die Vorherrschaft zu gewinnen.

6.4 Software-Bugs und falsche Verwendung von Smart Contracts

Ein Smart Contract (bzw. Chaincode) ist letztlich Software, die Fehler (Bugs) enthalten und dadurch angreifbar sein kann. Das prominenteste Beispiel war ein Fehler, der beim "DAO-Hack" auf der Ethereum-Blockchain im Jahr 2016 ausgenutzt wurde. Die Sicherheit der Blockchain an sich war dadurch jedoch nicht infrage gestellt. Ein anderes Negativbeispiel war Denial-of-Execution bei endloslaufenden Smart Contracts bei z. B. Crypto-Kitties.

Probleme für Smart Contracts entstehen z. B. bei der Interaktion mit externen Systemen in denen das Vertrauen in die Schnittstelle zwischen Blockchain und realer/digitaler Welt fehlt. Stark limitiert ist die Ausführung von komplexen Algorithmen und speicherintensiven Operationen. Solche Anwendungen widersprechen der grundlegenden Eigenschaft von Smart Contracts, dass sie redundant auf allen Nodes ausgeführt werden müssen.

7 Ressourcenbedarf einer Blockchain

7.1 Speicher- und Rechenbedarf

Da alle Daten auf allen beteiligten Rechnern abgelegt und nie wieder gelöscht werden, wächst der Speicherbedarf mit jedem neuen Eintrag. Außerdem ist im Falle von Proof-of-Work eine hohe Rechenleistung erforderlich, um im Wettbewerb der Rechner untereinander als erster ein Puzzle zu lösen und somit einen neuen Block anhängen zu dürfen.

7.2 Anreiz mit Coins

Als Anreiz, Ressourcen bereitzustellen, hat eine public-permissionless Blockchain in der Regel ein Belohnungssystem in Form von Coins bzw. Token, die jeweils spezifisch für eine ganz bestimmte Blockchain sind. Coins werden nach unterschiedlichen Regeln im Rahmen des Konsensverfahrens geschaffen bzw. verteilt. Am bekanntesten sind die Bitcoins der Bitcoin-Blockchain, die - über ihre Rolle als Abrechnungsmechanismus hinaus - vielfach als eine neue Währung gesehen werden.

Anhang A
Konsensverfahren

A.1 Allgemeines

Für das Anhängen eines neuen Blocks gibt es unterschiedliche Verfahren, die sich im Ressourcenbedarf unterscheiden und jeweils ihre eigenen Vor- und Nachteile haben.

A.1.1 Proof-of-Work (PoW)

Proof-of-Work (PoW) bedeutet, dass derjenige Rechner einen neuen Block an die public-permissionless Blockchain hängen darf, der ein vorgegebenes kryptografisches Rätsel als erster gelöst hat und damit die Belohnung in Form von Coins erhält. Diese Selektion nach Rechenleistung verursacht ein Wettrüsten der Miner. Im Fall der Bitcoin-Blockchain konkurrieren inzwischen weltweit riesige Serverfarmen miteinander; der Energieverbrauch liegt in einer ähnlichen Größenordnung wie der eines ganzen Landes wie Irland oder Dänemark; pro Transaktion sind 80 kWh – 200 kWh nötig.

A.1.2 Proof-of-Authority

In Proof-of-Authority-Blockchains werden neue Blöcke von Validatoren erstellt, denen vertraut wird. Hierbei dient die Identität der Validatoren als Grundlage für dieses Vertrauen. Einem Validator, der falsche Blöcke verifiziert, kann nach einer Mehrheitsentscheidung der anderen Validatoren das Stimmrecht entzogen werden. Da ein gewisses Vertrauen in die Validatoren vorausgesetzt wird, ist dieser Konsensusmechanismus am besten für private-permissioned-Blockchains geeignet, bei denen die Identität aller Teilnehmer bekannt ist.

A.1.3 Proof-of-Stake (PoS)

Die Idee des Proof-of-Stake (PoS) ist, das rechenintensive und energieverschwenderische Lösen kryptografischer Rätsel zu vermeiden und zugleich die Transaktionsgeschwindigkeit zu erhöhen. Bei PoS ist die Wahrscheinlichkeit, dass ein Miner für die Erzeugung eines neuen Blocks den Zuschlag erhält, proportional zum wertmäßigen Anteil aller seiner Coins an der Gesamtmenge der existierenden Coins. Die bei der Blockgenerierung generierten Coins und einbehaltenden Transaktionsgebühren werden nach dem Zufallsprinzip über die Coin-Besitzer ausgeschüttet. Die Wahrscheinlichkeit, dass ein Teilnehmer bei der Ausschüttung berücksichtigt wird, hängt davon ab, wie hoch sein Coin-Vermögen ist und wie lange er dieses schon innehat.

ANMERKUNG Neben dieser als Chain-based-PoS bezeichneten Möglichkeit gibt es die BFT-style PoS (Tendermint).

A.1.4 Proof-of-Activity (PoA)

Proof-of-Activity (PoA) ist ein hybrides Konsensverfahren. Die Generierung neuer Blöcke basiert sowohl auf PoW als auch auf PoS. Im ersten Schritt wird anhand eines vorgegebenen Rätsels ein PoW generiert, der nach erfolgreicher Suche ins Blockchain-Netz gesendet wird. Der Block wird erst dann als vollständig angesehen, wenn eine vorgegebene Anzahl von Coin-Besitzern diesen Block mit ihrem Private Key signiert haben. Die Belohnung für die Blockgenerierung (Block-Reward) wird aufgeteilt zwischen dem PoA-Miner und den Teilnehmern, die den Block signiert haben. Auf diese Weise wird die Mining-Arbeit belohnt und zudem eine Art Verzinsung von Coin-Guthaben ermöglicht.

A.1.5 Proof-of-Burn (PoB)

Proof-of-Burn ist eine weitere energiesparende Alternative zu PoW. Um gegen Entgelt Blöcke erzeugen zu können, muss der Miner zuvor Coins vernichtet haben, indem er diese an eine tote Adresse überweist. Je nach Höhe des „verbrannten“ Betrages wird ihm ein Punktewert zugewiesen, der einer bestimmten Hashrate bei PoW entspricht. Der Energieverbrauch ist in diesem Fall minimal. Um Coins verbrennen zu können, müssen diese jedoch zuvor erzeugt worden sein, d. h. PoB setzt das Vorhandensein eines Mining-Verfahrens voraus.

A.1.6 Proof-of-Capacity (PoC)

Proof-of-Capacity sieht vor, dass Miner für die Erzeugung von Blöcken große Datensegmente (sog. Plots) generieren, die auf einer Festplatte gespeichert werden. Dieses Verfahren ist wesentlich energieeffizienter als PoW. Zudem lässt sich die Blockchain damit wirksam gegen Bot-Netze schützen.

A.1.7 Proof-of-Elapsed Time (PoET)

Proof-of-Elapsed Time basiert auf der Idee, in einer vertrauenswürdigen Laufzeitumgebung (Trusted Execution Environment, TEE) ein Lotterieverfahren laufen zu lassen, das über Wartezeiten für vertrauenswürdige Funktionen einen zufälligen Gewinner ermittelt, der den neuen Datenblock generieren darf. Voraussetzung ist, dass alle Teilnehmer tatsächlich Vertrauen in eine gemeinsame TEE haben.

Literaturhinweise

- Das ursprüngliche Papier des Blockchain- und Bitcoin-Erfinders mit dem Pseudonym Satoshi Nakamoto ist nur sechs Seiten lang. Das Verständnis setzt jedoch einen soliden technischen Hintergrund voraus: https://bitcoin.org/bitcoin.pdf
- Die Ethereum-Blockchain mit der besonderen Eigenschaft, dass auf ihr auch Programm-Logiken speichern zu können, beschreibt der Erfinder Vitalik Buterin hier persönlich: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- Wer besser verstehen will, wie eine Blockchain aufgebaut ist und funktioniert, kann folgenden Blockchain-Simulator ausprobieren, der die Zusammenhänge gut verständlich darstellt: https://anders.com/blockchain/
- Das Thema Bitcoin wird gut verständlich beschrieben in dem folgenden Wiki: https://en.bitcoin.it/wiki/Main_Page
- Fraunhofer FIT beschreibt in seinem White Paper „Blockchain: Grundlagen, Anwendungen und Potenziale“ gut verständlich die Eigenschaften und Anwendungen der Blockchain: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf
- Im kanadischen Online-Rechtsmagazin SLAW findet man einen Überblick zu Smart Contracts in verschiedenen Komplexitätsstufen: http://www.slaw.ca/2016/09/19/smart-contracts/
- Einen guten Überblick zu den verschiedenen Blockchain-Typen gibt die Teletrust in einer Broschüre: https://www.teletrust.de/publikationen/broschueren/blockchain/
- Finanzwirtschaft:

  „Solving Challenges in Developing Countries with Blockchain Technology” https://medium.com/@philippsandner/application-of-blockchain-technology-in-the-manufacturing-industry-d03a8ed3ba5eEntwicklungsländer:%20https:/medium.com/@philippsandner/solving-challenges-in-developing-countries-with-blockchain-technology-78ec9b01bae3

  „Islands virtueller Zimbabwe-Dollar” https://bitcoinblog.de/2014/05/13/ein-digitaler-zimbabwe-dollar-fur-island/
- Energiewirtschaft:

  „Disruptive Potential in the German Electricity System – an Economic Perspective on Blockchain” https://www.ewi.uni-koeln.de/cms/wp-content/uploads/2017/07/Disruptive_Potential_in_the_German_Electricity_System_–an_Economic_Perspective_on_Blockchain.pdf

  „Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains” https://arxiv.org/pdf/1801.10228.pdf

  „Vulnerabilities in Smart Meter Infrastructure – Can Blockchain provide a Solution?” http://static.esmt.org/publications/whitepapers/dena_esmt_studie_blockchain_deutsch_2016.pdf
- Verwaltung:

  „Mythos Blockchain – Herausforderung für den öffentlichen Sektor“ https://www.oeffentliche-it.de/documents/10181/14412/Mythos+Blockchain+-+Herausforderung+f%C3%BCr+den+%C3%96ffentlichen+Sektor

  Das BAMF – Blockchain Whitepaper http://www.bamf.de/SharedDocs/Anlagen/DE/Downloads/Infothek/DasBAMF/blockchain-whitepaper.pdf
- Identitätsmanagement:

  „Digitale Identitäten in der Blockchain – Erfahrungen aus der Entwicklung“ https://www.fokus.fraunhofer.de/download/Fh_FOKUS_BlockIdent.pdf

- Mobilitätssektor:

  „Analysis of Blockchain Technology in the Mobility Sector“
  https://medium.com/@philippsandner/analysis-of-blockchain-technology-in-the-mobility-sector-1078e429615f

- Dezentralisierte Geschäftsmodelle:

  „Decentralized Autonomous Co-Operative’s (DAC) and the Rise of the New Commons”“
  https://medium.com/coinmonks/decentralised-autonomous-co-operatives-dac-and-the-rise-of-the-new-commons-721f5e1a7d3

  „Dezentralisierte Geschäftsmodelle durch Tokenisierung verstehen”“
  https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f

  „Dezentralisierte Geschäftsmodelle als neues Finanzierungsmodell und Investmentmodell verstehen”
  https://medium.com/blockchannel/investing-in-tokens-and-decentralized-business-models-e7629efa5d9b

- Angriffsszenarien

  Die Computerwoche beschreibt hier anschaulich mögliche Angriffsszenarien:
  https://www.computerwoche.de/a/wie-bitcoin-und-blockchain-gehackt-werden,3544081

- Sicherheit in Blockchains

  FSCB Working Paper „Security in Blockchain Applications“
  https://medium.com/@fsblockchain/security-in-blockchain-applications-43e73193512d

- Mehrheits-Angriff

  Fortune beschreibt den erfolgreichen Mehrheits-Angriff auf Bitcoin-Gold im Mai 2018:
  http://fortune.com/2018/05/29/bitcoin-gold-hack/

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Stresemannallee 15
60596 Frankfurt

Tel. +49 69 6308-0
service@vde.com
www.vde.com

Bildnachweis Titelseite: denisismagilov | stock.adobe.com

VDE