DANIEL DRESCHER

BLOCKCHAIN GRUNDLAGEN

EINE EINFÜHRUNG IN
DIE ELEMENTAREN KONZEPTE
IN 25 SCHRITTEN

mitp

Daniel Drescher

Blockchain Grundlagen

Eine Einführung in die elementaren Konzepte in 25 Schritten

Übersetzung aus dem Englischen
von Guido Lenz

mitp

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-95845-654-9
1. Auflage 2017

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Authorized German translation from the English language edition, entitled BLOCKCHAIN BASICS: A Non-Technical Introduction in 25 Steps, Daniel Drescher
ISBN 978-1-4842-2604-9
Original English language edition published by Apress, Inc. **USA**.

Lektorat: Sabine Schulz
Sprachkorrektorat: Maren Feilen
Coverbild: © Liu zishan / shutterstock.com
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung

Diese Einleitung beantwortet die allerwichtigste Frage, der sich jeder Autor stellen muss: Warum sollte irgendjemand dieses Buch lesen? Oder genauer: Warum sollte irgendjemand an einer weiteren Publikation zum Thema Blockchain interessiert sein? Im Folgenden erfahren Sie, zu welchem Zweck dieses Buch geschrieben wurde, was Sie davon erwarten können, was Sie nicht davon erwarten können, für wen es geschrieben wurde und wie es aufgebaut ist.

Warum noch ein Buch über die Blockchain?

Die Blockchain ist in der öffentlichen Diskussion und in den Medien ein Trendthema. Einige Enthusiasten behaupten, sie sei die größte Erfindung seit dem Aufkommen des Internets – und entsprechend viele Bücher und Artikel wurden in den letzten Jahren zu diesem Thema verfasst. Wenn Sie allerdings mehr darüber erfahren möchten, wie die Blockchain funktioniert, dann finden Sie sich in einem Labyrinth von Veröffentlichungen wieder, die sich entweder nur oberflächlich mit den technischen Details befassen oder aber die zugrunde liegenden technischen Konzepte auf höchst formalem Niveau behandeln. Dabei wird Sie die erste Kategorie möglicherweise nicht zufriedenstellen, weil diese Bücher technische Details vermissen lassen, die Sie für das Verständnis und eine Bewertung der Blockchain benötigen. Und die andere Kategorie setzt wiederum genau das Wissen voraus, das Sie sich erst noch aneignen möchten.

Das vorliegende Buch schließt die Lücke zwischen den rein technischen Veröffentlichungen zur Blockchain auf der einen und den Werken, die sich vorrangig mit bestimmten Einsatzbereichen oder den erwarteten wirtschaftlichen Auswirkungen oder Zukunftsmöglichkeiten befassen, auf der anderen Seite.

Es wurde geschrieben, weil es ohne ein konzeptuelles Verständnis der technischen Grundlagen nicht möglich ist, spezifische Blockchain-Anwendungen zu verstehen, Geschäftsmodelle von Blockchain-Startups zu bewerten oder der Diskussion über die prognostizierten wirtschaftlichen Konsequenzen zu folgen. Wer die grundlegenden Konzepte nicht begreift, kann den Wert oder die möglichen Effekte der Blockchain im Allgemeinen nicht beurteilen oder vollumfänglich erfassen, welchen Mehrwert bestimmte Blockchain-Anwendungen bieten. In diesem Buch wird daher in erster Linie die Grundidee der Blockchain vorgestellt – denn ein mangelndes Verständnis einer neuen Technologie kann dazu führen,

dass man einfach nur dem Hype folgt und letztendlich enttäuscht ist, wenn sich herausstellt, dass die ebenso unrealistischen wie unfundierten Erwartungen nicht erfüllt werden.

Dieses Buch vermittelt die Konzepte, aus denen die Blockchain besteht, in einer nicht technischen Weise und ebenso kurz wie verständlich. Es befasst sich mit den drei großen Fragen, die mit jeder Einführung einer neuen Technologie aufkommen: Was ist das? Wozu brauchen wir die Technologie? Wie funktioniert sie?

Was Sie nicht von diesem Buch erwarten dürfen

Anwendungen oder Einsatzbereiche der Blockchain werden in dem vorliegenden Buch ganz bewusst ausgespart. Obschon Kryptowährungen im Allgemeinen und Bitcoin im Speziellen sicherlich prominente Einsatzbereiche darstellen, wird die Blockchain-Technologie hier von einem allgemeinen Standpunkt aus betrachtet und erläutert. Diese Herangehensweise wurde gezielt gewählt, um generische Konzepte und technische Muster der Blockchain in den Fokus zu rücken, und nicht etwa einen ganz speziellen und eng umrissenen Anwendungsfall. Damit handelt es sich bei dieser Lektüre ...

- ... nicht um ein Buch, das sich vor allem mit Bitcoin oder anderen Kryptowährungen beschäftigt.
- ... nicht um ein Buch, das sich nur mit einer bestimmten Blockchain-Anwendung befasst.
- ... nicht um ein Buch, das die mathematischen Grundlagen der Blockchain beweisen soll.
- ... nicht um ein Buch über das Programmieren einer Blockchain.
- ... nicht um ein Buch über die rechtlichen Konsequenzen der Blockchain.
- ... nicht um ein Buch über die sozialen, wirtschaftlichen oder ethischen Auswirkungen der Blockchain auf unsere Gesellschaft oder die Menschheit insgesamt.

Allerdings werden einige dieser Punkte auf den folgenden Seiten durchaus in gewissem Umfang und an jeweils geeigneter Stelle angesprochen.

Was Sie von diesem Buch erwarten dürfen

Im Rahmen dieses Buchs werden die technischen Konzepte der Blockchain, zum Beispiel Transaktionen, Hashwerte, Kryptographie, Datenstrukturen, Peer-to-Peer-Systeme, verteilte Systeme, Systemintegrität und verteilte Konsensentscheidungen, auf nicht technische Weise erläutert. Der didaktische Ansatz beruht dabei auf vier Elementen:

- Verständliches Vokabular
- Keine Mathematik, keine Formeln
- Schritt für Schritt durch die Problemdomäne
- Metaphern und Analogien

Kein Fachchinesisch

Dieses Buch wurde mit gutem Grund ohne allzu technisches Vokabular geschrieben. Soweit möglich, wurde auf mathematische oder computerwissenschaftliche Fachbegriffe verzichtet, damit auch technisch weniger bis gar nicht versierte Leser dem Inhalt stets folgen können. Die verbleibenden unvermeidlichen Fachbegriffe werden natürlich vorgestellt und erklärt, denn diese benötigen Sie, um sich an Diskussionen beteiligen und andere Veröffentlichungen über die Blockchain verstehen zu können.

Keine Mathematik, keine Formeln

Wesentliche Bestandteile der Blockchain wie die Kryptographie und Algorithmen beruhen auf komplexen mathematischen Konzepten, die wiederum ihre eigenen speziellen und zum Teil Furcht einflößenden mathematischen Notationen und Formeln mit sich bringen. Allerdings kommen Letztere in diesem Buch absichtlich nicht zum Einsatz, damit die erörterten Inhalte auch für nicht entsprechend vorgebildete Leser überschaubar bleiben und nicht zu komplex werden.

Schritt für Schritt durch die Problemdomäne

Die einzelnen Kapitel dieses Buchs werden aus gutem Grund als *Schritte* bezeichnet: Sie bilden einen Lernpfad, der Stück für Stück das Wissen über die Blockchain aufbaut. Die Reihenfolge dieser Schritte wurde sorgfältig festgelegt. Sie umfassen die Grundlagen der Softwareentwicklung, erklären die Fachbegriffe, zeigen auf, warum genau die Blockchain benötigt wird, und erläutern die individuellen Konzepte, die sie ausmachen, sowie deren Zusammenspiel. Durch die Bezeichnung der einzelnen Kapitel als »Schritte« werden die wechselseitige Abhängigkeit und der didaktische Zweck unterstrichen. Sie bilden eine logische Abfolge, die eingehalten werden muss – es handelt sich in diesem Fall also nicht um Kapitel, die in beliebiger Reihenfolge gelesen werden können.

Metaphern und Analogien

Jeder Schritt, in dem ein neues Konzept vorgestellt wird, beginnt mit einer bildhaften Erläuterung, für die ein Beispiel aus dem Alltag herangezogen wird. Diese Metaphern erfüllen vor allem vier Zwecke:

Erstens bereiten sie den Leser auf ein neues technisches Konzept vor. Zweitens verbinden sie dieses technische Konzept mit einem leicht verständlichen Szenario aus der Alltagswelt und senken so die mentale Hürde, die beim Betreten des neuen Sachgebiets überwunden werden muss. Drittens erleichtern die anhand dieser Gleichnisse aufgezeigten Ähnlichkeiten und Analogien das Erlernen neuer Konzepte. Und viertens dienen sie auch als Gedächtnisstützen, die dabei helfen, neue Konzepte zu verinnerlichen oder abzurufen.

Aufbau des Buchs

Dieses Buch beschreibt insgesamt 25 Schritte, die in fünf große Etappen gegliedert sind. Zusammengenommen bilden sie einen Lernpfad ab, der Ihr Verständnis von der Blockchain nach und nach aufbaut und erweitert. Diese Schritte umfassen verschiedene Grundlagen der Softwareentwicklung, erklären die erforderlichen Fachbegriffe, zeigen auf, warum die Blockchain benötigt wird, erläutern die individuellen Konzepte, die sie ausmachen, sowie deren Zusammenspiel und verweisen auf aktive Entwicklungs- und Forschungsgebiete.

Teil I: Fachbegriffe und technische Grundlagen

In den Schritten 1 bis 3 werden wichtige Konzepte der Softwareentwicklung erläutert. Außerdem lernen Sie die Fachbegriffe kennen, die für das Verständnis der weiteren Schritte unverzichtbar sind. Am Ende von Schritt 3 werden Sie mit den grundlegenden Konzepten vertraut sein und das große Ganze rund um die Blockchain verstehen.

Teil II: Warum die Blockchain benötigt wird

In den Schritten 4 bis 7 wird erklärt, warum die Blockchain erforderlich ist, welche Problemstellung sie löst, warum es wichtig ist, diese Problemstellung zu lösen, und welches Potenzial die Blockchain bietet. Am Ende von Schritt 7 werden Sie eine genaue Vorstellung von der Problemdomäne haben, in der sich die Blockchain befindet, ebenso wie von der Umgebung, in der sie den größten Wert bietet. Außerdem werden Sie verstehen, warum sie überhaupt benötigt wird.

Teil III: Wie die Blockchain funktioniert

Der dritte Teil stellt den Hauptteil dieses Buchs dar, denn hier wird die innere Funktionsweise der Blockchain beschrieben. In den Schritten 8 bis 21 lernen Sie 15 verschiedene technische Konzepte kennen, die in ihrer Gesamtheit die Blockchain ausmachen. Am Ende von Schritt 21 werden Ihnen alle wesentlichen Konzepte der Blockchain geläufig sein und Sie werden wissen, wie diese für sich genommen funktionieren und wie sie zusammen die große Maschinerie namens Blockchain bilden.

Teil IV: Beschränkungen und wie man sie überwindet

Die Schritte 22 und 23 befassen sich mit den grundlegenden Beschränkungen der Blockchain und deren Gründen. Außerdem wird skizziert, wie sie sich überwinden lassen. Am Ende von Schritt 23 werden Sie verstehen, warum die ursprüngliche Idee der Blockchain, wie sie in den zuvor beschriebenen Schritten erläutert wurde, möglicherweise nicht für sehr große kommerzielle Anwendungen geeignet ist und welche Änderungen vorgenommen wurden, um diese Beschränkungen zu überwinden. Außerdem erfahren Sie, wie sich diese Modifikationen auf die Eigenschaften der Blockchain ausgewirkt haben.

Teil V: Verwenden der Blockchain, Zusammenfassung und Ausblick

Die Schritte 24 und 25 befassen sich damit, wie die Blockchain im Alltag eingesetzt werden kann und welche Fragen man sich bei der Wahl einer Blockchain-Anwendung stellen sollte. In diesem Teil werden auch aktive Forschungsgebiete und Bereiche für die weitere Entwicklung aufgezeigt. Am Ende von Schritt 25 werden Sie fundierte Kenntnisse über die Blockchain besitzen und sind damit bereit für komplexere Abhandlungen oder die aktive Beteiligung an laufenden Diskussionen zur Blockchain.

Begleitmaterialien

Auf der englischsprachigen Website `www.blockchain-basics.com` finden Sie Begleitmaterialien zu einigen der Schritte in diesem Buch.

Über den Autor

Daniel Drescher kommt aus dem Bankenwesen und verfügt über langjährige Erfahrung im elektronischen Wertpapierhandel. In den letzten Jahren hat er sich auf die Bereiche Automatisierung, Machine Learning und Big Data im Umfeld des Wertpapierhandels spezialisiert. Daniel hat unter anderem einen Doktor der Ökonometrie von der TU Berlin und einen MSc (Master of Science) in Softwareentwicklung von der University of Oxford.

Über den Fachlektor

Laurence Kirk war erfolgreich als Programmierer von Low-Latency-Finanzanwendungen für die City of London tätig, bevor er sich dem Potenzial der Distributed-Ledger-Technologie zuwandte. Nachdem er für sein Masterstudium nach Oxford gezogen war, gründete er das Consulting-Unternehmen Extropy.io, das mit Startups an der Entwicklung von Anwendungen auf der Ethereum-Plattform arbeitet. Als großer Anhänger verteilter Technologien betätigt er sich aktuell als Entwickler, Evangelist und Coach im Bereich Ethereum.

Teil I

Fachbegriffe und technische Grundlagen

In diesem Teil des Buchs werden die wichtigsten Konzepte der Softwareentwicklung erläutert. Er legt den Rahmen fest, in dem wir unsere Kommunikation über die Technologie im Allgemeinen organisieren und standardisieren. Darüber hinaus erhalten Sie auch eine Einführung in die Konzepte der Softwarearchitektur und der Integrität und erfahren, was diese mit der Blockchain zu tun haben. Am Ende dieses Teils werden Sie den Zweck der Blockchain und ihr Potenzial verstehen.

In diesem Teil:

Schritt 1

Denken in Schichten und relevanten Aspekten

Analysieren von Systemen durch Aufteilen in Schichten und Aspekte

Dieser Schritt bildet die Grundlage für unseren Lernpfad zur Blockchain; er beschreibt, wie wir unsere Kommunikation in Bezug auf Technologien organisieren und standardisieren. Hier wird erklärt, wie Sie ein Softwaresystem analysieren können und warum es wichtig ist, es als Gebilde aus mehreren Schichten zu betrachten. Außerdem zeigt dieser Schritt, welchen Nutzen die verschiedenen Schichten in einem System bringen und wie uns dieser Ansatz beim Verständnis der Blockchain hilft. Und schließlich erhalten Sie auch eine kurze Einführung in das Konzept der Softwareintegrität sowie deren Bedeutung.

Die Metapher

Haben Sie ein Mobiltelefon? Vermutlich schon, denn die meisten Menschen besitzen mittlerweile eins, wenn nicht gar mehrere. Wie viel wissen Sie über die unterschiedlichen drahtlosen Kommunikationsprotokolle, die zum Senden und Empfangen von Daten dienen? Wie viel wissen Sie über die elektromagnetischen Wellen, ohne die diese Form der mobilen Kommunikation nicht funktionieren würde? Mit derartigen Einzelheiten kennen sich wohl die wenigsten von uns aus, denn deren genaue Kenntnis ist für die Benutzung eines Mobiltelefons nicht erforderlich. Und die meisten von uns haben auch gar nicht die Zeit, sich eingehender mit diesen Dingen zu beschäftigen. Wir unterteilen das Mobiltelefon im Geiste in Teile, die wir kennen oder verstehen müssen, und Teile, die wir ignorieren oder als gegeben hinnehmen können.

Und diese Betrachtungsweise einer Technologie ist keineswegs auf Mobiltelefone beschränkt. Wir wenden sie immer wieder an, wenn wir die Bedienung eines neuen Geräts erlernen – sei es eines Fernsehers, eines Computers, einer Waschmaschine usw. Allerdings ist diese Form der gedanklichen Einteilung eine sehr individuelle Sache, denn was uns wichtig ist, richtet sich nach unseren persönlichen Vorlieben, der jeweiligen Technologie, unseren Zielen und unseren Erfahrungen. Ihre gedankliche Einteilung eines Mobiltelefons unterscheidet sich vermutlich von der meinen – obwohl es um dasselbe Gerät an sich geht. Das führt für gewöhnlich

zu Kommunikationsproblemen, insbesondere wenn ich versuchen würde, Ihnen zu erklären, was Sie über ein bestimmtes Mobiltelefon wissen sollten. Daher ist es beim Lehren und Diskutieren von Technologie so wichtig, ein gemeinsames Unterteilungssystem zu schaffen. Dieser Schritt erläutert, wie ein System in Schichten oder andere Bereiche unterteilt wird – und bildet somit die Basis für unsere Kommunikation über die Blockchain.

Schichten eines Softwaresystems

In diesem Buch nutzen wir zwei Arten von Unterteilungen für Systeme:

- Anwendung und Implementierung
- Funktionale und nichtfunktionale Aspekte

Anwendung und Implementierung

Wenn die Bedürfnisse eines Anwenders von den technischen Interna eines Systems getrennt werden, ergibt sich eine Aufteilung in die *Anwendungsschicht* und die *Implementierungsschicht*. Zur Anwendungsschicht gehört alles, was die Bedürfnisse des Anwenders betrifft, zum Beispiel Musik hören, Fotos machen oder Hotelzimmer reservieren. In die Implementierungsschicht gehört alles, wodurch diese Dinge erreicht werden, zum Beispiel das Konvertieren von digitalen Daten in akustische Signale, das Erkennen der Farbe eines Bildpunktes in einer Digitalkamera oder das Übermitteln von Nachrichten über das Internet an ein Buchungssystem. Die Elemente der Implementierungsschicht sind technischer Natur und werden als Mittel zum Zweck betrachtet.

Funktionale und nichtfunktionale Aspekte

Die Unterscheidung zwischen dem »Was« (ein System macht) und dem »Wie« (es etwas macht) führt zu einer Aufteilung in die funktionalen und nichtfunktionalen Aspekte. Beispiele für funktionale Aspekte sind das Übertragen von Daten in einem Netzwerk, die Wiedergabe von Musik, das Aufnehmen von Fotos und das Bearbeiten einzelner Bildpunkte. Beispiele für nichtfunktionale Aspekte sind eine ansprechende grafische Bedienoberfläche, eine schnell laufende Software und die Fähigkeit, Anwenderdaten geschützt und sicher abzulegen. Andere wichtige nichtfunktionale Aspekte eines Systems sind *Sicherheit* und *Integrität*. Integrität bedeutet, dass sich ein System wie beabsichtigt verhält und umfasst verschiedene Teilaspekte z.B, Datensicherheit und Korrektheit.[1] Die Unterschiede zwischen den funktionalen und nichtfunktionalen Aspekten eines Systems kann man sich durch

1 Chung, Lawrence, et al. *Non-functional requirements in software engineering*. Band 5. New York: Springer Science & Business Media, 2012.

einen Rückgriff auf die Grammatik merken: Verben beschreiben Handlungen, also etwas, *was* getan wird; Adverbien dagegen beschreiben den Umstand, also *wie* etwas getan wird. So kann eine Person schnell oder langsam gehen. In beiden Fällen ist die Handlung – Gehen – identisch, aber die Art, wie diese Handlung ausgeführt wird, unterscheidet sich. Man kann also verallgemeinern, dass die funktionalen Aspekte den Verben ähneln, die nichtfunktionalen Aspekte dagegen den Adverbien.

Gleichzeitiges Betrachten von zwei Schichten

Das Identifizieren der funktionalen und nichtfunktionalen Aspekte sowie das Aufteilen in Anwendungsschicht und Implementierungsschicht kann gleichzeitig erfolgen. Das Ergebnis lässt sich in einer zweidimensionalen Tabelle ähnlich der folgenden darstellen, die diese Verfahrensweise am Beispiel der gedanklichen Aufteilung eines Mobiltelefons demonstriert.

Schicht	Funktionale Aspekte	Nichtfunktionale Aspekte
Anwendung	■ Fotos machen ■ Anrufe tätigen ■ E-Mails senden ■ Im Internet browsen ■ Chatnachrichten senden	■ Die grafische Bedienoberfläche sieht schick aus ■ Einfache Bedienung ■ Nachrichten schnell versenden
Implementierung	■ Anwenderdaten werden intern gespeichert ■ Es wird eine Verbindung zum nächstgelegenen Mobilfunkmast hergestellt ■ Bildpunkte in der Digitalkamera abrufen	■ Daten effizient speichern ■ Energie sparen ■ Integrität erhalten ■ Datenschutz sicherstellen

Tabelle 1.1: Beispiel für die *gedankliche* Aufteilung eines Mobiltelefons

Diese Ergebnisaufstellung kann dabei helfen, die Sichtbarkeit (oder eben die Unsichtbarkeit) bestimmter Elemente eines Systems für die Anwender zu erläutern. Funktionale Aspekte der Anwendungsschicht sind die offensichtlichsten Elemente eines Systems, denn sie dienen den offensichtlichen Bedürfnissen der Anwender. Hierbei handelt es sich üblicherweise auch um diejenigen Elemente, über die Anwender etwas lernen. Auf der anderen Seite werden die nichtfunktionalen Aspekte der Implementierungsschicht selten als wichtige Elemente des Systems angesehen, sondern meist als selbstverständlich betrachtet.

Integrität

Die *Integrität* ist ein wichtiger nichtfunktionaler Aspekt in jedem Softwaresystem. Sie umfasst drei Hauptkomponenten:[2]

- *Datenintegrität:* Die im System verwendeten und gepflegten Daten sind vollständig, korrekt und frei von Widersprüchen.
- *Verhaltensintegrität:* Das System verhält sich wie beabsichtigt und weist keine logischen Fehler auf.
- *Sicherheit:* Das System ist in der Lage, den Zugriff auf Daten und Funktionen auf autorisierte Anwender zu beschränken.

Die meisten von uns betrachten die Integrität von Softwaresystemen möglicherweise als Selbstverständlichkeit, da wir in der Regel mit Systemen arbeiten, die sie glücklicherweise bewahren. Das liegt daran, dass die Programmierer und Softwareentwickler viel Zeit und Mühe aufgewendet haben, um ebendiese Integrität in ihren Systemen zu erreichen und zu erhalten. Dadurch sind wir diesbezüglich ein wenig verwöhnt und lassen nur wenig Wertschätzung für den Aufwand erkennen, den die Entwickler tatsächlich betrieben haben, um ein hohes Maß an Integrität zu gewährleisten. Wenn wir jedoch mit einem System arbeiten, bei dem dieser Aufwand nicht betrieben wurde, schlägt unsere Stimmung schnell um. In solchen Situationen haben Sie oftmals mit Datenverlust oder unlogischem Softwareverhalten zu kämpfen oder müssen sogar feststellen, dass Fremde auf Ihre persönlichen Daten zugreifen konnten. Und das sind dann die Momente, in denen Ihr Mobiltelefon, Ihr Computer, Ihr E-Mail-Programm, Ihre Textverarbeitung oder Ihre Tabellenkalkulation Sie wütend machen und Ihre gute Kinderstube vergessen lassen. Bei diesen Gelegenheiten wird sehr schnell deutlich erkennbar, wie wertvoll Softwareintegrität tatsächlich ist. Insofern dürfte es kaum überraschen, dass Softwareexperten viel Zeit auf diesen nur scheinbar unbedeutenden nichtfunktionalen Aspekt der Implementierungsschicht verwenden.

Ausblick

In diesem Schritt haben Sie einige der allgemeinen Prinzipien der Softwareentwicklung kennengelernt. Insbesondere wurden die Konzepte der Integrität und der funktionalen bzw. der nichtfunktionalen Aspekte vorgestellt sowie die Anwendung im Vergleich zur Implementierung eines Softwaresystems beschrieben. Das Verständnis dieser Konzepte hilft Ihnen dabei, das große Umfeld der Blockchain besser zu verstehen. Im nächsten Schritt betrachten wir das große Ganze unter Zugrundelegung der soeben gewonnenen Erkenntnisse.

2 Boritz, J. Efrim. IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems* 6.4 (2005): 260–279

Zusammenfassung

- Eine Analyse von Systemen ist möglich durch deren Aufteilung in:
  - Anwendungs- und Implementierungsschicht
  - Funktionale und nichtfunktionale Aspekte
- Die Anwendungsschicht befasst sich mit den Bedürfnissen des Anwenders, die Implementierungsschicht damit, die Aufgabenstellungen technisch umzusetzen.
- Funktionale Aspekte konzentrieren sich auf das »Was«, die nichtfunktionalen Aspekte auf das »Wie«.
- Den meisten Anwendern sind die funktionalen Aspekte der Anwendungsschicht eines Systems wichtig, während die nichtfunktionalen Aspekte – insbesondere jene der Implementierungsschicht – für Anwender weniger sichtbar sind.
- Die Integrität ist ein wichtiger nichtfunktionaler Aspekt in jedem Softwaresystem. Sie umfasst drei Hauptelemente:
  - Datenintegrität
  - Verhaltensintegrität
  - Sicherheit
- Die meisten Softwarepannen wie Datenverlust, unlogisches Verhalten oder unbefugter Zugriff auf persönliche Daten sind das Ergebnis von Verstößen gegen die Systemintegrität.