

Ausgabe H1/2018

# Blockchain

## Langfristige Zukunftsvision oder medialer Hype?

### Bitcoin

Ein geschichtlicher  
Rückblick

Seite 5

### SEQIS Referenzstory

Erfolgreiche  
Zusammenarbeit mit  
Zelisko

Seite 17

### Blockchain

für IT Analytiker

Seite 21

*Titel: „Heißluftballons“; Künstler: Max Minnichmayr, Technik: Acryl auf Leinwand*

## Lesen Sie in dieser Ausgabe:

### Editorial.....3

### Neulich im Netz.....4

Künstliche Intelligenz zum Nutzen der Menschen

### Bitcoin.....5

Ein geschichtlicher Rückblick

### SEQIS „10 things“.....9

Expertentreff #03/2017:  
„Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse“

### Kryptowährungen.....12

Aus finanzwirtschaftlicher Perspektive betrachtet

### SEQIS Kalender.....14

Alle Termine auf einen Blick

### Gewinnspiel.....16

Gewinnen Sie ein Exemplar des Buches „Managing for Happiness“

### SEQIS Referenzstory:

#### Zelisko.....17

Erfolgreiche Zusammenarbeit im Bereich Testunterstützung

### Die alternative Krypto-

#### währung „Ethereum“.....19

...oder auch „Kennen Sie schon dApps“?

### Blockchain.....21

...für IT Analytiker

### Auflösung Gewinnspiel.....22

Hier finden Sie die Auflösung des Gewinnspiels der letzten Ausgabe H2/2017

### SEQIS „10 things“.....25

Expertentreff #04/2017:  
„Sind Sie (sich) wirklich sicher? – IT Security im Fokus“

### Über SEQIS QualityNews:

Dieses Magazin richtet sich an Gleichgesinnte aus den Bereichen Software Test, IT Analyse und Projektmanagement im IT Umfeld. Die SEQIS Experten berichten über ihre Erfahrungen zu aktuellen Themen in der Branche. Die Leser des Magazins gestalten die Ausgaben mit: Schreiben Sie uns Ihre Meinung im SEQIS Blog ([www.SEQIS.com/de/blog-index](http://www.SEQIS.com/de/blog-index)) oder als Leserbrief.

Wenn Sie dieses Magazin abbestellen möchten senden Sie bitte ein Mail an [marketing@SEQIS.com](mailto:marketing@SEQIS.com).

### Impressum:

Information und Offenlegung gem. §5 E-Commerce-Gesetz und §25 Mediengesetz

Herausgeber: SEQIS GmbH,  
Neusiedler Straße 36, A-2340 Mödling  
Tel: +43 2236 320 320 0  
Fax: +43 2236 320 320 350  
[info@SEQIS.com](mailto:info@SEQIS.com), [www.SEQIS.com](http://www.SEQIS.com)  
Gericht: Bezirksgericht Mödling  
Firmenbuchnummer: 204918a  
Umsatzsteuer-ID: ATU51140607  
Geschäftsführung: Mag. Alexander Vukovic, Mag. Alexander Weichselberger, DI Reinhard Salomon

Druck: druck.at Druck- und Handelsgesellschaft mbH, 2544 Leobersdorf  
Erscheinungsweise: 2x pro Jahr  
Für die verwendeten Bilder und Grafiken liegen die Rechte für die Nutzung und Veröffentlichung in dieser Ausgabe vor. Die veröffentlichten Beiträge, Bilder und Grafiken sind urheberrechtlich geschützt. (Kunstwerke: Lebenshilfe Baden und Mödling, Fotos: © Fotolia.com).

Sämtliche in diesem Magazin zur Verfügung gestellten Informationen und Erklärungen geben die Meinung des jeweiligen Autors wieder und sind unverbindlich. Irrtümer oder Druckfehler sind vorbehalten. Hinweis im Sinne des Gleichbehandlungsgesetzes: Aus Gründen der leichteren Lesbarkeit wird die geschlechtsspezifische Differenzierung nicht durchgehend berücksichtigt. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

### Ihre Meinung ist gefragt!

Nach den QualityNews ist bekanntlich vor den QualityNews! Schon bald arbeiten wir wieder auf Hochtouren an der nächsten, spannenden Ausgabe. Lesen Sie nur das, was Sie wirklich interessiert! Sagen Sie uns, welche Themen Sie spannend finden.

Kontaktieren Sie uns: [marketing@SEQIS.com](mailto:marketing@SEQIS.com)

Join us: [facebook.com/SoftwareTestIsCool](https://www.facebook.com/SoftwareTestIsCool)

Wir freuen uns auf Ihre Vorschläge und Wünsche!





Sehr geehrte Leserin,  
sehr geehrter Leser,

wir freuen uns, Ihnen die erste  
Ausgabe der SEQIS QualityNews  
im Jahr 2018 zu präsentieren.

Wie haben Ihnen die bisherigen  
Ausgaben gefallen? Konnten Sie  
hilfreiche Tipps für Ihren  
Arbeitsalltag mitnehmen oder auch  
an der ein oder anderen Stelle ein  
wenig schmunkeln? Über Feedback  
und Anregungen Ihrerseits freuen  
wir uns.

Auch in dieser Ausgabe stellen wir  
unseren Beiträgen einen nicht-  
technischen Aspekt an die Seite:

Auf den folgenden Seiten finden  
Sie einige Kunstwerke der  
Lebenshilfe Niederösterreich der  
Werkstätten Baden und Mödling.  
Denn nicht nur unsere  
Spezialisten, sondern auch die  
Klienten der Lebenshilfe leben für  
ihre(n) Beruf(ung).

In dieser Ausgabe dreht sich alles  
um das brandaktuelle Thema  
Blockchain. Unsere Experten  
bereiten sich schon lange auf  
diese Entwicklung vor, die auch  
neue Herausforderungen für den  
Software Test und die IT Analyse  
mit sich bringt.

So steht eine hochsensible,  
technische Infrastruktur hinter dem  
Konzept der Blockchain. Diese gilt  
es von Beginn an gewissenhaft in  
Hinblick auf IT Security zu testen  
und eine hochwertige Qualitäts-  
sicherung zu gewährleisten.

Auf den folgenden Seiten geben  
Ihnen unsere Experten einen  
Einblick in die rasante Entwicklung  
der Blockchain und zeigen, worauf  
in diesem Zusammenhang beim  
Test besonders zu achten ist.

Wir wünschen viel Lesevergnügen  
mit unseren SEQIS QualityNews!

Ihre SEQIS Geschäftsleitung



Mag. Alexander Vukovic



Mag. Alexander Weichselberger



DI Reinhard Salomon



Titel: „Roteule“, Künstler: Claudia Toth, Kim Novak, Technik: Acryl auf Leinwand

## Neulich im Netz: Künstliche Intelligenz zum Nutzen der Menschen

von Hansjörg Münster



**Hansjörg Münster**  
ist Principal Consultant und Teamlead bei SEQIS.

Als Allrounder deckt er ein breites Spektrum an Aufgaben ab. Die Schwerpunkte seiner Tätigkeit liegen in den Bereichen Testmanagement, Testautomation und Lasttest.

Ganz oben auf der Prioritätenliste des IT Profis steht, einen Nutzen und Mehrwert in der Qualitätssicherung seiner IT Projekte zu generieren.

**Schon in der SEQIS QualityNews-Ausgabe H1/2017 konnte ich über eine spezielle App für Autisten berichten. Jetzt gibt es eine weitere, neue App, die Menschen mit besonderen Bedürfnissen das Leben erleichtert: Microsoft Seeing AI.**

Ein selbst blinder Entwickler von Microsoft entwickelte eine App, die mittels KI (künstlicher Intelligenz), einem Handy und dessen Kamera dem Blinden per Sprachausgabe sagt, was in der näheren Umgebung geschieht. Microsoft nennt die App „die sprechende Kamera für Blinde“.

Folgende Funktionen bietet die App derzeit an:

- Kurze Texte werden automatisch vorgelesen, sobald

- die Kamera diese erkennt.
- Größere Dokumente werden erkannt und können auch inkl. der Formatierung vorgelesen werden.
- Erkennt die Kamera einen Barcode, startet die App automatisch eine Suche im Netz um den Barcode zu interpretieren. Dies liefert rasch Informationen zu den gescannten Produkten.
- Sobald die Kamera eine Person erkennt, werden diese sowie deren Emotionen beschrieben.
- Im Experimentalstadium befindet sich außerdem noch ein Feature, mit welchem man sich die Situation allgemein beschreiben lassen kann.
- Eine Geldschein-Erkennung

befindet sich ebenfalls gerade noch in der Entwicklung.

Die App steht derzeit nur für iOS zu Verfügung, kann kostenlos heruntergeladen und im Moment leider nur in Amerika bezogen werden. Genauere Informationen bietet Microsoft unter: [www.microsoft.com/en-us/seeing-ai/](http://www.microsoft.com/en-us/seeing-ai/)

Dort befinden sich auch einige Videos, die diese App in Aktion zeigen.

Aus Tester-Sicht ergeben sich dadurch zahlreiche neue, spannende Möglichkeiten, die das Spektrum des Software Tests in Zukunft bereichern werden. ■



## Bitcoin – ein geschichtlicher Rückblick

von Tanja Huber

**Die Geschichte des Bitcoins beginnt im Jahr 2008 mit der Veröffentlichung eines neunseitigen White Papers mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“ unter dem Pseudonym Satoshi Nakamoto. Bis heute ist unbekannt, welche Person oder Personengruppe sich hinter dem Pseudonym verbirgt.**

Das Gründungsdokument selbst ist jedenfalls in Englisch verfasst und mit mathematischen Formalen gespickt, wodurch es die Annahme gibt, dass der Autor oder das Autorenkollektiv aus der Welt der Computerwissenschaftler oder Mathematiker stammen dürfte.

Inhaltlich wird im Dokument eine Alternative der konventionellen, vertrauensbasierten Transaktionsmodelle vorgestellt, wobei ein auf kryptografischen Techniken basierendes, elektronisches Zahlungssystem vorgeschlagen wird.

Dieses basiert auf der Idee, dass zwei vertragswillige Partner direkt

unter sich verhandeln können – ohne dem Einfluss eines vertrauenswürdigen Mittelsmanns, wie einer Bank. Die Überweisung der Beiträge solle direkt von Teilnehmer zu Teilnehmer erfolgen, um so mit einem Peer-to-Peer-Network Doppelausgaben zu verhindern.

Das Bitcoin-Netzwerk entstand am 3. Januar 2009 mit der Schöpfung der ersten 50 Bitcoins. Wenige Tage darauf wurde unter dem Pseudonym von Satoshi Nakamoto auch die erste Version der Bitcoin-Referenzsoftware „Bitcoin Core“ veröffentlicht, eine Open-Source-Referenzimplementierung der Bitcoin-Kryptowährung.

Am 21. Mai 2010 erfolgte die erste Transaktion mit Bitcoins. Laszlo Hanyecz, ein Programmierer aus Florida, sandte 10.000 Bitcoins an einen Freiwilligen aus England, welcher daraufhin ungefähr 19 Euro ausgab, um diesem etwas bei einem Lieferdienst zu bestellen.

Später lud Hanyecz als Beweis,



**Tanja Huber, BA** ist Consultant für Software Test bei SEQIS.

Zusätzlich zu ihrer Erfahrung in den Bereichen Testfallerstellung, Testdurchführung und Testunterstützung ist sie auch in den Bereichen Projekt- und Qualitätsmanagement tätig.

Beim Herangehen an neue Aufgaben ist ihr eine gewissenhafte Vorgehensweise und kreative Aufgabenlösung wichtig. Ebenso legt sie größten Wert auf hochwertige Qualitätssicherung.

dass die Transaktion erfolgreich durchgeführt worden war, das Bild der Bestellung hoch (siehe Abb. 2). Diese Transaktion ist einer der ersten Meilensteine der noch jungen Geschichte der Bitcoins und begründete sogar den „Bitcoin Pizza Day“, welcher jedes Jahr am 22. Mai gefeiert wird.

Schon kurz nach der Gründung der Bitcoins wurde Mt.Gox K.K. gegründet – einer der weltweit größten Handelsplätze, an dem digitale Münzen in reales Geld umgesetzt werden konnten.

Dieses wurde 2009 ursprünglich als eine Tauschbörse für Sammelkarten unter den Namen „Magic: The Gathering Online“ geschaffen und am 18. Juli 2010 zu einer


Der Begriff „Bitcoin“ ist ein Kunstwort aus den englischen Wörtern „Bit“ (ein Kofferwort aus dem Englischen: „binary digit“) und „Coin“ (das englische Wort für Münze) und wird sinngemäß als „digitale Währung“ übersetzt. Das Währungssymbol für Bitcoin ist , ein großes B mit zwei vertikalen Strichen und wurde von Satoshi Nakamoto entworfen. Das Symbol ist angelehnt an \$, dem Dollarzeichen, welches selbst ursprünglich ein Gewichtszeichen für Gold war.



Abb. 1: Bitcoin-Logo  
(Quelle: Satoshi Nakamoto, [https://en.bitcoin.it/wiki/Promotional\\_graphics](https://en.bitcoin.it/wiki/Promotional_graphics))



Bitcoin-Börse umgewidmet. Der Name selbst entstand, in dem man die Anfangsbuchstaben der ursprünglichen Tauschbörse nahm und „eXchange“ hinzufügte: „MTGO X“. CEO dieser Tauschbörse war seit 2011 Mark Karpelès – ein französischer Programmierer, der damals in Tokio mit seiner Firma Tibanne Geschäfte machte.



Abb. 2: Die ersten mit Bitcoins gekauften Pizzen

(Quelle: Laszlo Hanyecz, <https://bitcointalk.org/index.php?topic=137>)

Als ein wichtiger Katalysator für den Durchbruch des Bitcoins gilt die Euro-Krise, welche eine vielschichtige Krise der Europäischen Währungsunion ab dem Jahr 2010 war. Mehrere Krisen, darunter die Bankenkrise, die Wirtschaftskrise und die Staatsschuldenkrise, verstärkten sich hierbei gegenseitig. Dies bewirkte einen Vertrauensverlust in Banken und Staat, wovon der Bitcoin profitierte.

Anfang Februar 2011 war 1 Bitcoin erstmals gleich viel wert wie 1 US-Dollar, wodurch Bitcoin das Interesse der Medien weckte. Artikel im „Time Magazine“ und in der Wirtschaftszeitung „Forbes“ folgten, infolgedessen der Kurs der digitalen Währung immer weiter nach oben schnellte.

Die Zahl der Börsen in Mt.Gox, welcher damals den Großteil des Handels mit Bitcoin abwickelte, explodierte in dieser Zeit regelrecht. Im Jahr 2013 überschritt

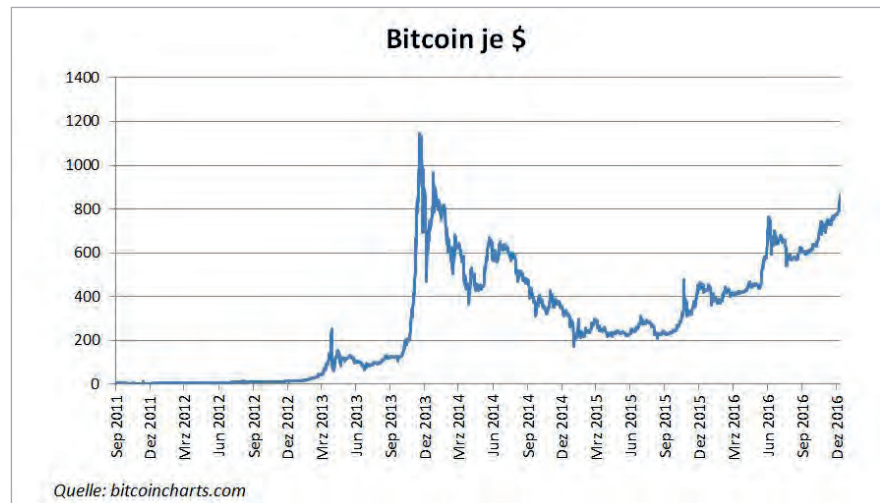


Abb. 3: Bitcoin je Dollar zwischen September 2011 und Dezember 2016  
(Quelle: <https://www.fuw.ch/wp-content/uploads/2016/12/bitcoin-kurs-600x376.jpg>)

der Bitcoin-Wert die 1.000-Dollar-Marke.

Dieser plötzliche Ansturm führte schließlich in die erste weltweite Krise der neuen Währung. Für mehr als zwölf Stunden gingen die Server des Unternehmens unter der Last in die Knie, wodurch der Bitcoin-Kurs kollabierte. Zwar wurde Mt.Gox danach wieder zum Laufen gebracht, doch seither häuften sich ähnliche Probleme immer öfter.

Nachdem Mt.Gox wegen angeblicher technischer Probleme am 7. Februar 2014 sämtliche Auszahlungen an Kunden gestoppt hatte, stellte die Börse am 25. Februar 2014 den Handel ein.

Am 28. Februar 2014 meldete das Unternehmen bei einem japanischen Bezirksgericht Insolvenz an und stellte einen Antrag auf Gläubigerschutz. Mark Karpelès gab seinen Sitz im Vorstand der Bitcoin Foundation zurück.

Karpelès wurden Veruntreuung und gefälschte Transaktionen vorgeworfen – in Japan beides keine Kavaliärsdelikte. Auf einer Pressekonferenz räumte Karpelès

das spurlose Verschwinden von 850.000 Bitcoins ein. In dieser Zeit fiel der Wert auf 450 US-Dollar. Die Gerichtsverhandlungen wurden in der Bitcoin-Gemeinde mit Spannung beobachtet, da Karpelès zu der Zeit als der führende Repräsentant der digitalen Währung galt.

Für die Währung selbst bedeutete dies jedenfalls weltweite Aufmerksamkeit, da die Mitglieder der Bitcoin-Gemeinde durch die Insolvenz ihres Handelsplatzes viel Geld verloren. Nach einem Höhepunkt im Dezember 2013 erreichte der Bitcoin-Kurs im April 2014 einen Tiefpunkt von 340 US-Dollar.

Doch der Beliebtheit des Bitcoins und anderer Kryptowährungen tat diese Enttäuschung keinen Abbruch. Sie wurden und werden zwar weiterhin von vielen Seiten kritisch betrachtet, doch erfreuten sie sich weiterhin reger Nachfrage.

Weiter angefacht wurde diese Nachfrage vermutlich durch einen Gesetzesentwurf in Kalifornien, wonach Bitcoins als legale Alternative zum US-Dollar zugelassen werden könnten.

Tatsächlich wuchs der Kurs immer weiter an und knackte eine Rekordmarke nach der anderen: Anfang des Jahres 2017 wurde die 1.000-Dollar-Marke überschritten, im Oktober 2017 die 5.000-Dollar-Marke und Mitte Dezember 2017 die 15.000-Dollar-Marke.

Dieser rasante Kursanstieg wird vielerorts kritisch beobachtet und gerne mit dem holländischen Tulpenfieberwahn des 17. Jahrhunderts verglichen.

### Geschichtlicher Ausflug:

Die Tulipmania begann mit Charles de l'Écluse, einem der bedeutendsten Botaniker seiner Zeit und Hofbotaniker der Habsburger in Wien. Dieser bekam von einem Gesandten des Herrscherhauses einen Sack Tulpenzwiebel aus Konstantinopel geschenkt, die er, als er nach Holland umzog, mitnahm und dort heranzüchtete. Er verkaufte die Tulpen allerdings nicht, sondern nutzte diese als Heilpflanzen. Für die erste Verbreitung sollen laut Legende Diebe gesorgt haben.

Die Tulpenzwiebel fiel hierbei in Holland auf fruchtbaren Boden, da das Land zu Beginn des 17. Jahrhunderts durch den Ostindienhandel und die Seeräuberei an der Schwelle eines goldenen Zeitalters stand.

Die vermögenden Familien stellten dabei ihren Reichtum zur Schau, indem sie große Anwesen mit riesigen Gärten erwarben. Die Tulpe wurde bald zum Statussymbol, wodurch die Frage nach der Blume immer weiter anstieg. Die Nachfrage wuchs mehr und mehr an, womit das Angebot aufgrund natürlicher Beschränkungen der Tulpe bald nicht mehr mithalten konnte.

Die Tulpe wurde zum Spekulationsobjekt schlechthin, denn bald schon wurden nicht mehr die Blumen selbst, sondern die Rechte daran gehandelt.

Man konnte also Geld an den Tulpen verdienen, ohne jemals eine in die Hand zu nehmen. Für Normalbürger war die Aussicht auf schnellen Reichtum verlockend, weshalb sie oft ihren gesamten Besitz belasteten, um sich Knollen zum Handeln zu kaufen. Die Preise von Tulpen stiegen immer weiter an.

So wurde für eine Tulpe der Sorte „Vizekönig“ zwei Fuder<sup>1</sup> Weizen, vier Fuder Roggen, vier Ochsen, acht Schweine, zwölf Schafe, zwei Fässchen Wein, vier Tonnen Bier, 1.000 Pfund Käse, ein Silberpokal, ein Bett und ein Anzug auf den Tisch gelegt. Doch irgendwann wollten alle nur noch verkaufen und niemand mehr kaufen. Händler blieben auf ihren Tulpen sitzen, welche bald nichts mehr wert waren.

<sup>1</sup> Fuder = Volumenmaß für Flüssigkeiten und feste Stoffe. „Abgeleitet ist das Fuder von der ‚Fuhre‘ (Ladung), die ein zweispänniger Wagen laden konnte.“ (Quelle: Wikipedia)

Quelle: [www.faz.net/aktuell/finanzen/fonds-mehr/historische-finanzkrisen-niederlande-1637-eine-blumenzwiebel-fuer-87-000-euro-1283731.html?printPage=Article=true#pageIndex\\_0](http://www.faz.net/aktuell/finanzen/fonds-mehr/historische-finanzkrisen-niederlande-1637-eine-blumenzwiebel-fuer-87-000-euro-1283731.html?printPage=Article=true#pageIndex_0)

Im Vergleich zur Tulpenblase gibt es allerdings einen entscheidenden Unterschied: Anders als bei Tulpen ist das Angebot von Bitcoins, vergleichbar mit Gold, begrenzt und wird die Anzahl von 21 Millionen zirkulierenden Bitcoins nie übersteigen. Zumindest, wenn man sogenannte Altcoins, also alternative Kryptowährungen, außer Acht lässt.

Ein rascher Wertanstieg ist zudem nicht gleichbedeutend mit einer Blase, denn unter einer Blase versteht man eine künstliche Überbewertung, die zu einer plötzlichen Abwärtskorrektur führen wird.

Viele Experten gehen allerdings genau davon aus und warnen vor Investitionen in das virtuelle Geld – Kryptowährungen seien mit keinerlei Wert hinterlegt und folglich reines Spekulationsobjekt. Im Vergleich zu Gold oder Tulpen haben Bitcoins nur ihren digitalen Wert und sind kein physisches Objekt.

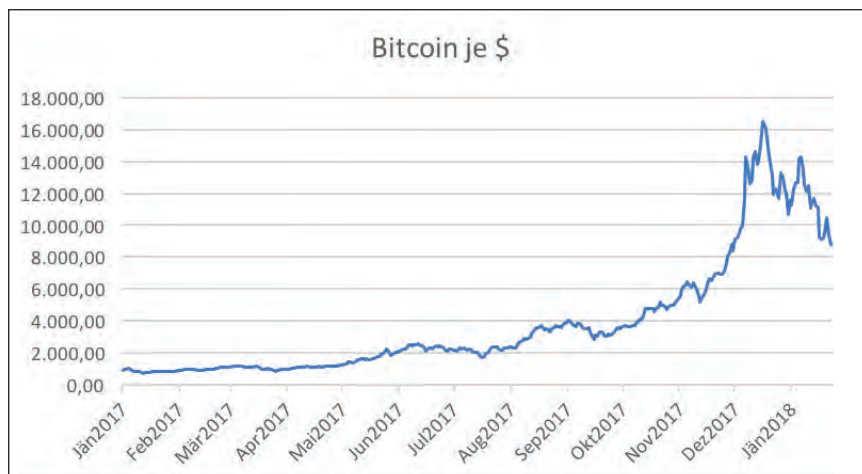


Abb. 4: Historische Bitcoin-Kurse 2017-2018  
(Quelle: <https://www.finanzen.net/devisen/bitcoin-euro-kurs/historisch>)

Die jüngste Entwicklung zeigt bereits einen bedenklichen Kurssturz:

Ausgehend vom Rekordhoch im Dezember 2017 verlor der Kurs im Jänner 2018 um fast 50% an Wert. Am 17. Jänner 2018 erreichte der Wert erstmals wieder einen Wert unter der 10.000-Dollar-Marke.

Als Auslöser des aktuellen Kurssturzes gilt ein Medienbericht aus China, wonach das Land den Handel mit virtuellen Währungen blockieren will.

Auch Südkorea, welches gemeinsam mit China und Japan zur Hochburg im Handel mit Kryptowährungen zählt, plant derartigen Geschäften einen Riegel vorzuschieben.

Doch auch europäische Länder wie Deutschland oder Frankreich wollen den Handel mit Kryptowährungen stärker kontrollieren.

Zurzeit sind Bitcoins somit noch eine Währung, welche von jeglicher staatlichen Kontrolle losgelöst ist und daher gerne als alternative Anlagemöglichkeit gesehen wird.

### Fazit

Als Möglichkeit für schnelles Geld sollte Bitcoin gewiss nicht gesehen werden. Die Spekulation mit Bitcoins stellt ein Risiko dar, da diese im Gegensatz zu beispielsweise Gold oder Tulpen mit keinerlei Wert hinterlegt sind. Der einzige Wert, mit dem sie hinterlegt sind, ist das Vertrauen ihrer Nutzer.

Somit ist es auch nicht verwunderlich, wenn der Wert mit abfallendem Vertrauen sinkt oder durch mediales Interesse steigt.

Allein die geschichtliche Betrachtung zeigt, wie sehr der Wert des Bitcoins mit der medialen Aufmerksamkeit zusammenhängt. Im jetzigen Stadium kann der Bitcoin als interessantes Experiment auf dem Weg zum Aufbau alternativer, internet-gestützter Währungen gesehen werden.

Jedoch weiß niemand, wie sich der Kurs entwickeln und sich die Kryptowährung in Zukunft halten wird. Von einem kann man jedoch mit Sicherheit ausgehen: Die Berichterstattung darüber wird auch in nächster Zeit spannend bleiben. ■



Titel: „Rundeule“, Künstler: Stefan Riesner, Claudia Toth, Technik: Acryl auf Leinwand



## SEQIS „10 things“-Expertentreff #03/2017: „Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse“

von Josef Falk

**Der dritte Expertentreff 2017 beschäftigte sich mit dem Thema „Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse“. Im Mittelpunkt stand dabei der Kreativitätsprozess, um zu innovativen Lösungen zu kommen.**

### 1. Werden Sie sich über Ihre Rolle klar

Wie sehen Sie sich selbst als Analytiker? Als einer, der gewissenhaft Anforderungen sammelt, diese vollständig und widerspruchsfrei aufschreibt und sie während der Entwicklungszeit verwaltet?

Oder sehen Sie Ihre Aufgabe darin, auf der Basis von Wissen über das Fachgebiet, in Abstimmung mit den Stakeholdern, kreative und innovative Lösungen zu entwerfen?

Im ersten Fall benötigen Sie tatsächlich nicht viel Kreativität, da sind andere Soft Skills, wie Genauigkeit und Gewissenhaftigkeit wichtiger. Im zweiten Fall können Ihnen aber diese Tipps wichtige Anregungen liefern.

### 2. Beginnen Sie mit der Lösung

„Nicht in Lösungen, sondern in Anforderungen denken“ – so kann man es oft hören und lesen. Aber: Anforderungen sind niemals innovativ, nur Lösungen sind es. Wenn Sie Neues schaffen wollen, dann müssen Sie sich mit der Lösung beschäftigen – und nicht nur mit den Anforderungen.

Es lässt sich gar nicht vermeiden: Selbst wenn Sie nur wenige Informationen über das Fachgebiet haben, wird sich in Ihrem Kopf bereits ein Bild einer Lösung bilden. Der Tipp ist: Verdrängen Sie diese

Lösung nicht, sondern arbeiten Sie damit. Prüfen Sie sie gegen die Informationen, die sie gesammelt haben. Sprechen Sie mit Ihren Stakeholdern darüber. Ändern Sie diese Lösung, verwerfen Sie sie, wenn es notwendig ist.

Aber akzeptieren Sie diese erste Idee und machen Sie sie zur Ausgangsbasis Ihrer Lösung.

### 3. „Saugen“ Sie alles an Information auf, was Sie kriegen können

Es ist ein Mythos, dass die Stakeholder schon wissen, was sie brauchen – und Sie als Analytiker dieses Wissen nur abholen und sauber aufschreiben müssen.

Im Gegenteil: Von Ihnen wird erwartet, dass Sie Berater sind – und Lösungen vorschlagen. Damit Sie das leisten können, müssen Sie Experte sein.

Und das nicht nur in IT-Fragen, sondern auch auf dem zu bearbeitenden Fachgebiet. Wenn Sie noch nicht Experte sind – dann müssen Sie es schnell werden.

Woher nehmen wir diese Information? Es gibt unzählige Quellen: Fachliteratur, Lehrbücher, Zeitschriften, Online-Blogs, unternehmensinterne Unterlagen, Dokumentation des Alt-Systems, vergleichbare Systeme und Standards – ja, und nicht zuletzt natürlich die Menschen, die in der betroffenen Organisation arbeiten.

### 4. Beziehen Sie technische Lösungsmöglichkeiten in Ihre Überlegungen ein

Innovation – das ist in der IT die Kombination aus Bedürfnissen,



**Mag. Josef Falk** ist IT Analytiker.

Seit dem Abschluss seines Studiums der Betriebswirtschaftslehre in Wien

gestaltet er Lösungen in den unterschiedlichsten Fachbereichen – und ist dabei Mittler zwischen Fachbereich und IT-Entwicklung.

Besonderes Augenmerk legt er bei der Analyse auf den Innovationsgrad. Neben seiner Projektstätigkeit befasst er sich mit der Entwicklung der Business Analyse und ist aktuell Mitglied des Vorstandes des Austria Chapter des IIBA (International Institute of Business Analysis).

technischen Möglichkeiten und Wirtschaftlichkeit. Ohne Einbeziehung der technischen Möglichkeiten gibt es keine Innovation.

„REST“, „NoSQL“, „Internet of things“, „Blockchain“ – das sind nur einige der aktuellen Schlagworte und abhängig vom Fachgebiet gibt es noch viel mehr.

Sie sollten zumindest Grundkenntnisse in den relevanten Technologien haben, damit Sie in der Lage sind, innovative Lösungen vorzuschlagen.

### 5. „Wildern“ Sie in fremden Fachgebieten

„Creativity is just connecting things.“ – so lautet ein Zitat von Steve Jobs. Diese Dinge, die miteinander zu Neuem verbunden werden, müssen nicht immer aus dem aktuell betrachteten Fachgebiet stammen.

Beispiele dafür begegnen uns in unserem (IT-)Leben täglich: Was hat ein Computer mit „Fenstern“ zu tun? Oder mit „Ordern“, mit „Mäusen“?

Vielleicht finden Sie Analogien aus Ihrem Vorprojekt, die Sie auch im aktuellen Projekt anwenden können, vielleicht sogar aus völlig anderen Wissensgebieten, die Sie z.B. aus einem Ihrer Hobbies kennen.

### 6. Verwerfen Sie Ihre Lösung

Ja, es klingt provokant. Ist es auch :-)

Aber es gibt Situationen, da muss es sein. Mit zunehmendem Informationsstand zeigt es sich vielleicht, dass der erste Lösungsansatz, mit dem Sie bisher gearbeitet haben, einfach nicht passt.

In diesem Fall ist Flexibilität gefragt, die es ermöglicht, auch völlig neu zu beginnen. Daher ist es gut, sich möglichst lange nicht festzulegen.

### 7. Lassen Sie das Unterbewusstsein für sich arbeiten

„Da muss ich eine Nacht darüber schlafen!“ Wir alle kennen die Situation, in denen uns rationales Nachdenken nicht mehr weiterhilft.

Dieses Phänomen wird auch in den Kreativitätstheorien von Graham Wallas, James Webb Young und anderen angesprochen. Sie nennen es die „Inkubationsphase“.

In dieser Phase des Kreativitätsprozesses beschäftigt man sich nicht mehr bewusst mit dem zu lösenden Problem – sondern lässt das gesammelte Wissen und die bereits angestellten Überlegungen im Unterbewusstsein wirken.

Das Ergebnis ist sehr häufig ein „Geistesblitz“, in dem die Lösung plötzlich klar auf dem Tisch liegt. Auch Sie hatten schon Geistesblitze, richtig?

### 8. Machen Sie Ihre Ideen anschaulich

Vielleicht haben Sie es ja auch



Titel: „Fasching in Venedig“, Künstler: Sophie Leditznig, Technik: Acryl, Collage und Pappmaché auf Leinwand



Foto: SEQIS Expertentreff „Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse“  
(© SEQIS GmbH)

schon erlebt: Zustimmendes Nicken, aber wenig Feedback, wenn Sie Ihre Prozess- und Datenmodelle präsentieren. Aber kaum liegt dann der erste Screen real vor, sprudeln plötzlich die Ideen: „So war das nicht gemeint!“ und „Da könnte man doch auch...“. Stakeholder haben es gerne konkret. Zeigen Sie Ihnen frühzeitig, wie Sie sich die Lösung vorstellen. Somit geben Sie ihnen die Möglichkeit, frühzeitig zu widersprechen (und natürlich auch zuzustimmen).

Das Instrument dafür nennt man „Prototyping“. Ein Prototyp kann sehr einfach sein. Manchmal reicht eine handschriftliche Skizze. Je weiter der Analyseprozess fortschreitet, desto mehr wird im Prototyp die endgültige Lösung erkennbar sein.

### 9. Kommunizieren Sie Ihre Ideen frühzeitig

Das klassische Vorgehen ist:

Zuerst Anforderungen erheben, dann Lösungen entwickeln.

Der Informationsfluss zwischen Analytiker und Stakeholder geht dabei lange Zeit nur in eine Richtung: Der Analytiker nimmt die Anforderungen vom Stakeholder entgegen.

Im Sinne einer innovativen Lösung ist es zweckmäßig, den Informationsfluss von Anfang an auch in die andere Richtung laufen zu lassen: Der Analytiker teilt den Stakeholdern seine Lösungsideen mit.

So können die Stakeholder darauf aufbauen und eigene Lösungsideen entwickeln, was sowohl die Akzeptanz als auch den Innovationsgrad erhöht.

### 10. Legen Sie sich so spät wie möglich fest

Nichts schränkt die Flexibilität mehr ein, als wenn durch eine neue Idee

viele Stunden an Arbeit vernichtet werden.

Die Gefahr ist groß, dass man in diesem Fall – vielleicht nur unbewusst – neue Ideen einfach nicht mehr zulässt („sunk cost“-Dilemma).

Die Lösung: Stecken Sie erst dann viel Arbeit in die Lösung, wenn Sie sich sicher sind.

Solange die Lösung nur in Ihrem Kopf existiert oder vielleicht in ein paar leichtgewichtigen Arbeitspapieren, haben Sie kein Problem, das Konzept zu ändern – oder auch gänzlich zu verwerfen. Wenn Sie aber schon umfangreiche Daten- oder Prozessmodelle in stunden- oder sogar tagelanger Arbeit geschrieben haben, werden Sie sich hüten, das Konzept wesentlich zu ändern.

Deshalb: Wenn Sie diese Artefakte benötigen, erstellen Sie sie erst dann, wenn die Lösung in Ihrem Kopf fertig ist. ■

### Sie haben unsere bisherigen Veranstaltungen verpasst?

Für Sie haben wir auf unserer Website alle Vorträge in chronologischer Reihenfolge übersichtlich zusammengefasst.

Sie finden dort auch alle Vortragsunterlagen zum Download: [www.SEQIS.com](http://www.SEQIS.com)

### Fortsetzung folgt...

Auch heuer gibt es wieder vier spannende Expertentreffs zu aktuellen IT Trendthemen.

Alle Details zu den Events finden Sie auf Seite 15 und unter [www.SEQIS.com](http://www.SEQIS.com).



## Kryptowährungen – aus finanzwirtschaftlicher Perspektive betrachtet

von Barbara Stummer



**Barbara Stummer, MA** ist bei SEQIS im Bereich Finance tätig.

Nach einem Bachelorstudium mit Schwerpunkt Controlling und einem Masterstudium, das sich mit neuartigen Geschäftsmodellen auseinander gesetzt hat, beschäftigt sie sich gerne mit Trends und unkonventionellen Ansätzen, die alltägliche Problemstellungen mit alternativen, effizienteren Lösungen befriedigen.

**Was sind Kryptowährungen? Wenn von Kryptowährungen die Rede ist, meint man eine virtuelle Onlinewährung. Es geht hier weder um reale Münzen noch um Banknoten.**

Jeder virtuelle Coin verfügt über eine einzigartige ID und wird in aufwändigen Rechenprozessen erzeugt, hat also einen Code, mit dem er eindeutig identifiziert werden kann. Der Wert je Einheit ist dennoch für alle gleich. Dieses Geldsystem, das parallel zum Fiatgeld (Euro, Dollar,...) existiert, arbeitet losgelöst von Banken und Staaten. Das bedeutet, es existiert keine Zwischeninstanz, die die Geldflüsse prüft bzw. Bankgebühren einhebt. Die Überweisungen erfolgen direkt von Nutzer zu Nutzer (Peer-to-Peer

System) und zeichnen sich besonders durch ihre Schnelligkeit aus. Führt man eine internationale Banküberweisung durch, muss diese mehrere Instanzen durchlaufen bis das Geld von der Hausbank des Absenders zur Bank des Empfängers fließt.

Bei Kryptowährungen macht es weder von der Dauer, noch von den Gebühren her einen Unterschied, ob quer über den Erdball transferiert wird oder ob es sich um eine Inlandstransaktion handelt. Daher ist sie bei Personen, die häufig ins Ausland überweisen, besonders beliebt und kann einen Beweggrund darstellen, teilweise auf Kryptowährung umzusteigen.

Aufgrund der fehlenden Kontrolle durch Banken und Staaten sind/waren Kryptowährungen beliebtes Zahlungsmittel im Darknet oder werden für Schwarzgeldgeschäfte missbraucht. Dadurch haftet am Onlinegeld nach wie vor ein zwiespältiges Image.

Bei Kryptowährungen handelt es sich um ein dezentrales System. Dies ist der entscheidende Unterschied gegenüber dem Fiatgeld: Herkömmliche Währungen werden zentral von Banken administriert.

Kryptowährungen hingegen werden dezentral mit Hilfe der Blockchain-Technologie verwaltet. Dies bedeutet, jeder User im Netzwerk hat eine Kopie des Journals über alle erfolgten Transaktionen innerhalb dieses Netzwerks. Bei jeder Transaktion wird die Liste, die in Form einer Blockchain geführt wird, länger, komplexer und dadurch auch

sicherer. Wird nun ein PC im Netzwerk gehackt, schlagen alle anderen im Verbund Alarm. Das tun sie auch, wenn jemand versucht, Beträge zu transferieren, die ihm gar nicht (mehr) gehören.

Die Blockchain ist somit die Kontrollinstanz der Kryptowährungen. Vertippt sich der Nutzer und überweist eine Summe an ein falsches Wallet (Geldbörse für Kryptowährungen), so ist der Betrag verloren. Bestätigte Transaktionen können nicht mehr zurückgezogen werden. Dies ist ein entscheidender Unterschied zur herkömmlichen Banküberweisung.

### Der Bitcoin

Der wohl prominenteste Vertreter am Sektor der Kryptowährungen ist der seit 2009 am Markt existierende Bitcoin. Dieser hat zuletzt Schlagzeilen wegen seines extrem steilen Kursanstiegs gemacht. Innerhalb des letzten Jahres hat die Währung um beachtliche 1.000% zugelegt. Jedoch unterliegt die Kryptowährung auch markanten Kurschwankungen. Daher kann der Wert täglich stark variieren.

Der Bitcoin wirkt sich deflationär im Gegensatz zu so manchem Fiatgeld aus. Das bedeutet, das Geld wird nicht entwertet sondern der Wert wird stetig wachsend erwartet, da es nur eine begrenzte Anzahl an Bitcoins gibt. Die maximale Menge an Bitcoins beträgt 21 Millionen Einheiten. Da Angebot und Nachfrage den Preis bestimmen, treibt ein Engpass den Preis in der Regel in die Höhe. Dies ist auch beim Bitcoin zu erwarten. Es kreuzen sich die Welten der

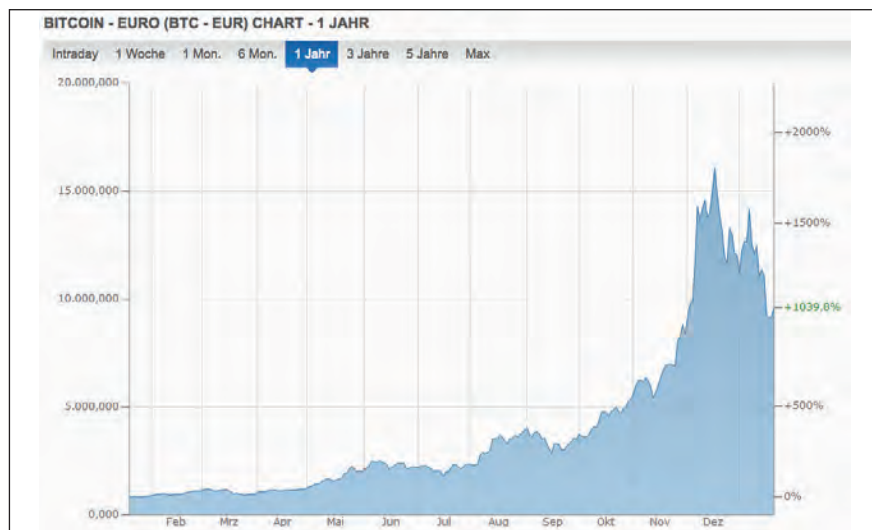


Abb.: Bitcoin-Kurs 2017

(Quelle: <http://www.finanzen.net/devisen/bitcoin-euro-kurs>)

„Online-“ und „Offlinewährungen“ auf Plattformen, auf denen Kryptowährungen gegen herkömmliche Zahlungsmittel an- und verkauft werden bzw. wo beispielsweise Reisen oder Haushaltswaren gegen Kryptowährungen gekauft werden können.

Die Zeiten, in denen man ausschließlich online mit Bitcoins bezahlen konnte, sind vorbei. In den Ballungszentren kann man von Sushi über Fahrtendienste bis zum Einkauf von diversen Beratungsleistungen mit Bitcoins bezahlen.

Die österreichische Hilfsorganisation „Jugend Eine Welt Österreich“ bittet bereits seit 2015 um Bitcoinspenden. So erreicht die Hilfsorganisation eine neue Zielgruppe. Ein Nachteil ist jedoch, dass in Österreich Bitcoins nicht als Währung anerkannt sind und daher handelt es sich bei einer Bitcoin-Spende um eine Sachspende. Sachspenden können steuerlich nur über Umwege abgesetzt werden, indem man schriftlich bestätigt, dass man die Bitcoins treuhändisch der Hilfsorganisation übergeben hat, damit diese sie im Namen des Spenders in Euro umwandelt.

Es gibt zwei Möglichkeiten um an Bitcoins zu kommen: Zum einen kann man sie online gegen Fiatgeld tauschen, zum anderen besteht auch die Möglichkeit welche zu schürfen. Dies bedeutet, man stellt Rechenleistung zur Verfügung um Transaktionen zwischen anderen Nutzern in der Blockchain zu prüfen.

Die Gegenleistung hierfür sind natürlich Bitcoins. Daher tragen die Nutzer selbst Sorge, dass die Vorgänge stets überprüft werden. In Österreich ist das Selbstschürfen nicht mehr lukrativ, da die Energiekosten die Erträge für die erhaltenen Bitcoins fast zur Gänze auffressen. Dies war in den Anfangszeiten des Bitcoins noch nicht der Fall, da es durch die geringe Nutzerzahl und somit geringer Rechenleistung schneller gelang, Einheiten zu produzieren. Aufgrund des hohen Energieaufwands wird vorwiegend in Ländern, in denen Strom im Überfluss produziert wird, wie beispielsweise Island, mit Hilfe der Vulkanenergie geschürft.

Wie bewahrt man nun seine Bitcoins auf? Hierfür gibt es mehrere Möglichkeiten. Jedenfalls benötigt man ein Wallet (engl.

Geldbörse). Dies kann in mehreren Formen existieren. Zum einen gibt es die Möglichkeit Bitcoins am Smartphone zu speichern. Des Weiteren kann das Wallet auch in Form eines eigens dafür gemachten USB-Sticks existieren. Diese Variante ist besonders sicher, da das Wallet abseits von Netzwerkzugriff aufbewahrt wird. Außerdem kann man seine Bitcoins auch direkt am PC verwalten. Hierfür benötigt man eine spezielle Software.

Während die Transaktionen in der Blockchain gespeichert werden, wird der Besitz der Bitcoins mit Hilfe eines persönlichen Sicherheitsschlüssels nachgewiesen. Wird der Schlüssel verloren, so sind dies auch die Bitcoins.

Zusammenfassend kann gesagt werden, dass Kryptowährungen derzeit aufstrebend sind. Jedoch müssen Nutzer neue „Spielregeln“ erlernen. Transaktionen sind irreversibel, mit dem Verlust des Sicherheitsschlüssels geht auch der Verlust der Geldeinheiten verloren. Auch für die Verwahrung muss der Nutzer selbst Sorge tragen. Hat man hingegen sein Geld auf einem Bankkonto, trägt die Bank die Haftung für das Geld. Daher trägt der einzelne Nutzer eine höhere Verantwortung als im Bankensystem.

Des Weiteren sind die Kryptowährungen noch relativ jung und daher kann nicht mit Sicherheit gesagt werden, dass der steigende Kurstrend beständig bleibt. In der Vergangenheit wurden einige rasante Kursschwankungen verzeichnet.

Experten sind sich einig: Die Technologie der Blockchain ist nicht nur für den Finanzsektor revolutionär, sondern könnte auch Nutzen im Gesundheitssektor oder bei der Digitalisierung von Ämtern stiften. ■

März	
1 Do	
2 Fr	
3 Sa	
4 So	
5 Mo	
6 Di	
7 Mi	
8 Do	
9 Fr	
10 Sa	
11 So	
12 Mo	
13 Di	
14 Mi	
15 Do	 SEQIS „10 things“
16 Fr	
17 Sa	
18 So	
19 Mo	
20 Di	
21 Mi	
22 Do	
23 Fr	
24 Sa	
25 So	
26 Mo	
27 Di	
28 Mi	
29 Do	
30 Fr	Karfreitag
31 Sa	Karsamstag

April	
1 So	Ostersonntag
2 Mo	Ostermontag
3 Di	
4 Mi	
5 Do	SEQIS @ ATB Treff
6 Fr	
7 Sa	
8 So	
9 Mo	
10 Di	
11 Mi	
12 Do	SEQIS @ FH Technikum
13 Fr	
14 Sa	
15 So	
16 Mo	
17 Di	
18 Mi	
19 Do	
20 Fr	
21 Sa	
22 So	
23 Mo	
24 Di	
25 Mi	
26 Do	
27 Fr	
28 Sa	
29 So	
30 Mo	



Mai		
1	Di	Staatsfeiertag
2	Mi	
3	Do	
4	Fr	
5	Sa	
6	So	
7	Mo	
8	Di	
9	Mi	
10	Do	Christi Himmelfahrt
11	Fr	
12	Sa	
13	So	
14	Mo	
15	Di	<b>Haben Sie schon Ihre nächste Weiterbildung geplant?</b>  <a href="http://www.SEQIS.com">www.SEQIS.com</a>
16	Mi	
17	Do	
18	Fr	
19	Sa	
20	So	Pfingstsonntag
21	Mo	Pfingstmontag
22	Di	
23	Mi	
24	Do	
25	Fr	
26	Sa	
27	So	
28	Mo	
29	Di	
30	Mi	
31	Do	Fronleichnam

## Über die SEQIS Expertentreffs „10 things I wished they'd told me!“

An Informationen mangelt es meist nicht – im Gegenteil, derer gibt es oft mehr als genug. Wichtiger denn je ist es, an die entscheidenden Informationen zu gelangen. Als Dienstleistungsunternehmen sind wir uns unserer Rolle als Informant bewusst und sprechen die an Software Test und IT Analyse Interessierten mit der Veranstaltungsreihe „10 things I wished they'd told me!“ konkret an.



Für all jene, die Software entwickeln, nutzen, beschaffen, in einem Betrieb für die Softwarequalitätssicherung zuständig oder als Requirements Engineer/Business Analyst tätig sind, haben wir eine passende Plattform geschaffen!

Bei unseren Expertentreffs erhalten Sie die Möglichkeit branchenbezogene Erfahrungen auszutauschen und wertvolle Tipps von den Profis abzustauben. Die Vortragenden bringen aktuelle Test- und IT Analyse-Themen auf jeweils 10 knackige Punkte und teilen mit Ihnen ihre Erfahrungen aus zahlreichen großen und komplexen IT Projekten.

### Save-the-Date zu den „10 things“ 2018

Auch im Jahr 2018 laden wir Sie wieder ein, unsere vier kostenlosen Expertentreffs zu aktuellen IT Trendthemen zu besuchen.

#### Early Access – lassen wir den Kunden testen?!

Donnerstag, 15. März 2018

#### Der Output der IT Analyse oder das Frankenstein-Prinzip

Donnerstag, 14. Juni 2018

#### Automate your mobile – 10 instruktive Tipps zur Testautomation von mobilen Endgeräten

Donnerstag, 20. September 2018











#### Agiles Projektmanagement – erfolgreich Projekte leiten

Donnerstag, 15. November 2018

Melden Sie sich gleich an und sichern Sie sich Ihren Platz:  
[www.SEQIS.com/de/events-index](http://www.SEQIS.com/de/events-index)

## Gewinnspiel: Machen Sie mit und gewinnen Sie ein Exemplar des Buches „Managing for Happiness“

Auch in dieser Ausgabe haben wir für Sie wieder ein Gewinnspiel vorbereitet. Lösen Sie folgendes Rätsel und schon nehmen Sie teil:

	+		+		+		=	8
	+		+		+		=	20
	x		+		+		=	15
	+		+		=	???		

**Wie lautet die korrekte Lösung?**

Und so nehmen Sie teil: Senden Sie uns Ihre Antwort und Ihre Kontaktdaten per Mail an [marketing@SEQIS.com](mailto:marketing@SEQIS.com) unter dem Betreff „QN Gewinnspiel“.

Unter allen Einsendungen verlosen wir ein Exemplar des Buches **„Managing for Happiness“ von Jurgen Appelo**. Einsendeschluss ist der 31.5.2018. Die Auflösung des Rätsels finden Sie in der nächsten Ausgabe. Wir wünschen viel Glück!

### Teilnahmebedingungen:

Mit der Teilnahme am Gewinnspiel akzeptieren Sie die folgenden Teilnahmebedingungen. Teilnahmeberechtigt sind Personen ab 18 Jahren. Die Gewinnermittlung erfolgt nach dem Zufallsprinzip und findet nicht öffentlich statt. Der Gewinner wird per Email verständigt.

Der Gewinn kann nicht in bar abgelöst werden und ist ausschließlich in der dafür vorgesehenen Form zu konsumieren. Die Gewinnverständigung gilt mit Absendung als erfolgt. Das Zugangsrisiko trägt der Gewinner. Der Teilnehmer stimmt zu, dass die Gewinneinlösung dokumentiert wird und Bildmaterial für Werbung der SEQIS GmbH in jeder Form verwendet werden darf.

Der Gewinn beschränkt sich ausschließlich auf den Erhalt eines Exemplars des Buches „Managing for Happiness“ von Jurgen Appelo im Wert von € 26,77 (inkl. 20% Ust.). Pro Person und Gewinn wird ein Buch ausgegeben. Der Gewinn ist übertragbar. Der Rechtsweg ist ausgeschlossen.

Die Mitarbeiter der SEQIS GmbH sind von der Teilnahme am Gewinnspiel ausgeschlossen. Das Recht, Teilnehmer, die gegen diese Teilnahmebedingungen verstoßen, mit sofortiger Wirkung von der Teilnahme auszuschließen, wird vorbehalten. Eine allenfalls bereits erworbene Berechtigung zum Gewinnbezug erlischt in diesem Fall.

Die SEQIS GmbH behält sich das Recht vor, die Teilnahmebedingungen für Gewinnspiele jederzeit ohne Ankündigung und Angaben von Gründen nach eigenem Ermessen zu ändern.



Titel: „Bunte Landschaft“, Künstler: Stefan Riesner, Technik: Acryl auf Leinwand

## SEQIS Referenzstory: Testunterstützung bei Zelisko



© Zelisko

### Über Zelisko

Zelisko ist ein 1918 gegründetes niederösterreichisches Traditionsunternehmen mit Sitz in Mödling.

Seit 1988 gehört Zelisko der Knorr-Bremse Gruppe an, einer Aktiengesellschaft mit Firmensitz in München und weltweit führender Hersteller von Bremssystemen als auch Anbieter weiterer Subsysteme für Schienen- und Nutzfahrzeuge.

Neben Signalsystemen und Messwandlern entwickelt, produziert und vertreibt Zelisko am Gründungsstandort in Mödling Verkehrsmanagementsysteme wie Fahrscheindrucker und Bordrechner für Linienbusse bis hin zu Backoffice-Lösungen (Leitsysteme).

So verbinden Systeme wie Zelisko FSD5plus „All-In-One“ die Funktionen eines Bordrechners mit jenen eines Fahrscheindruckers (= FSD).

Für die Verwendung des FSD benötigte Daten wie Tarife, Fahrpläne und Steuerdaten werden über die Backoffice-Lösung ZMS

eingespeist – einem mandantenfähigen Mehrplatzsystem. ZMS steht hierbei für „Zelisko Management System“.

Mittels der Geräteverwaltung, ein Modul des Hintergrundsystems ZMS, ist es möglich die Softwarebestände und die Funktionsbereitschaft der einzelnen Hardware-Komponenten jederzeit direkt abzurufen und mithilfe von Updates die Versorgung des Front Ends individuell zu steuern.

Die Programmierung wird sowohl von internen aber auch von externen Entwicklern erledigt. Die Zusammenarbeit erfolgt via Microsofts Team Foundation Server (Verwaltung von Fehlermeldungen, Testfällen als auch Test-



Abb. 1: Fahrscheindrucker & Bordrechner – verbunden in einem Gerät  
(Quelle: © Zelisko)



Foto: © Zelisko

**DDI (FH) Christoph Kabinger** ist Teamlead für Software-Qualitätssicherung bei Zelisko Verkehrsmanagementsysteme.

dokumentation) sowie Teamviewer (Remotezugriff auf die gemeinsame Testumgebung).

### SEQIS bei Zelisko

Da durch die komplexe Zusammenwirkung zwischen Frontoffice und Backoffice hohes Fehlerpotential gegeben ist, aber in Relation zu den Entwicklern nur wenige Software Tester zur Verfügung standen, verstärkte sich Zelisko im September 2016 mit SEQIS Testexperten.

Die Hauptaufgaben waren: Skalierung der Mannschaft bei der Qualitätssicherung und den Tests sowie eine Prozess- und Methodenoptimierung in diesen Bereichen der Wertschöpfung.



## Die Mission Software Test im Detail

„Das Ziel des Projektes und unseres Teams war es, möglichst schnell die bereits vorhandenen Tester in der Testdurchführung zu unterstützen und unsere Expertise einzubringen“, beschreibt Hansjörg Münster, SEQIS Testmanager, die Herangehensweise.

Münster weiter: „Hierbei holten wir im Rahmen der Projekt RampUp-Phase rasch das benötigte Fachwissen. Diese spezielle SEQIS-Methode wurde in einer Vielzahl von Projekten der letzten Jahre methodisch gehärtet und versetzt uns in die Lage innerhalb kürzester Zeit aktiv mitzuarbeiten – bei geringstem Aufwand für die Bestandsmannschaft.“

Weitere Schwerpunkte waren:

- Übernahme der wöchentlichen Regressionstests
- Verbesserung des Informationsaustausches zwischen Entwicklung und Test
- Optimierung des Testprozesses durch Einführung von Scrum-Boards, Daily Standups, zyklischer Test- und Qualitätsreports
- Methodische Dokumentation, testspezifisch und fachlich – damit verbunden Einführung von Atlassian Confluence
- Defectmanagement:  
U.a. Bereinigung der Defectlisten mit dem Ziel, den IST Stand korrekt darzustellen
- Verbesserung des Entwicklungsprozesses inkl. Releaseplanung & Monitoring, Anforderungsmanagement

Nach dieser ersten Stabilisierungsphase, die allgemein die Testprozesse optimierte, wurde Anfang 2017 der Aufgabenschwerpunkt auf ein spezifisches Kundenprojekt konzentriert. Münster: „Refactoring der

Backoffice-Software für ein Kundenprojekt. Acht Busgesellschaften, die vom Ergebnis unmittelbar betroffen waren.

Es war ein Taskforce-Modus mit vorrangigem Ziel, Stabilität und Performance zu verbessern. Kernerfolgsfaktor dabei war die enge Zusammenarbeit zwischen Entwicklern und Testern.“

**Tanja Huber**, SEQIS Testerin,  
über die Dokumentation:  
„Damit unsere gewonnenen  
Erkenntnisse und Erfahrungen  
nicht verloren gingen, wurden  
diese vom ersten Tag an  
gesammelt und in einem von  
Zelisko zur Verfügung gestellten  
Wiki dokumentiert.“

Somit wurden auch hier der Informationsaustausch weiter gefördert und eine zentrale Wissensdatenbank aufgebaut, in welcher sowohl das Wissen der Tester als auch der Entwickler zu testspezifischen Fragen gebündelt und festgehalten wurde.“

## Projekthighlights und Ergebnisse

- ✓ Unterstützung von Zelisko im täglichen Testgeschehen und Überarbeiten der Testfälle



**Hansjörg Münster**  
ist Principal  
Consultant  
und Team-  
lead bei  
SEQIS.

Bei Zelisko übernahm er die Rolle des Testmanagers.

- ✓ Einführung und Verleben von QA-Grundsätzen und agilen (Test-) Methoden (Scrum)
- ✓ Einführung von Testberichten zur Schaffung von Transparenz über den QA-Zustand
- ✓ Abhaltung einer Klausur zur Verbesserung des Entwicklungsprozesses
- ✓ Unterstützung bei Toolentscheidungen (Microsoft Team Foundation Server, Atlassian Confluence)
- ✓ Optimierung Defectmanagement, Bereinigung der Defects
- ✓ Umsetzung einer Wissensdatenbank für testbezogene Daten und Informationen ■

**Zebulo BLUS**

Personalien ändern    Betriebsdaten ändern    Abrechnung    Datenübertragung    Datenerneuerung    Notizen    Tarifdaten    Geräteverwaltung    ITCS    Extras    Zebulo Intern

Gerätebestandliste    Fahrzeugliste    SD-Karten    Geräte ohne Standort    Versenksformationen    Fernwartungs-Prüfe    Aktueller Fernwartungsstatus    Gerätekonfiguration    Fahrzeugtypen    Lager    Vorverkaufsstellen

Lagerhaltung    Fernwartung    Konfiguration

Navigieren    Gerätebestandliste    Fahrzeugtypen    Petrol-Sport-Tankpläne    Fahrer und Personelle    Fernwartungs-Prüfe anzeigen    **Versenksformationen**

**Versenksformationen**

Geräte Nr.	Gerätebuch	Datum	Zeit	Anzahl OK	Anzahl Ver...	Anzahl L...	Standard	Betriebs...	...	PSD Mess...	PSD Mess...	PSD
200174	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200174-001	201006-002	...	201006-001	201006-001	201004-001
200175	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200175-001	201006-002	...	201006-001	201006-001	201004-001
200176	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200176-001	201006-002	...	201006-001	201006-001	201004-001
200177	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200177-001	201006-002	...	201006-001	201006-001	201004-001
200178	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200178-001	201006-002	...	201006-001	201006-001	201004-001
200179	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200179-001	201006-002	...	201006-001	201006-001	201004-001
200180	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200180-001	201006-002	...	201006-001	201006-001	201004-001
200181	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200181-001	201006-002	...	201006-001	201006-001	201004-001
200182	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200182-001	201006-002	...	201006-001	201006-001	201004-001
200183	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200183-001	201006-002	...	201006-001	201006-001	201004-001
200184	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200184-001	201006-002	...	201006-001	201006-001	201004-001
200185	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200185-001	201006-002	...	201006-001	201006-001	201004-001
200186	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200186-001	201006-002	...	201006-001	201006-001	201004-001
200187	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200187-001	201006-002	...	201006-001	201006-001	201004-001
200188	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200188-001	201006-002	...	201006-001	201006-001	201004-001
200189	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200189-001	201006-002	...	201006-001	201006-001	201004-001
200190	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200190-001	201006-002	...	201006-001	201006-001	201004-001
200191	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200191-001	201006-002	...	201006-001	201006-001	201004-001
200192	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200192-001	201006-002	...	201006-001	201006-001	201004-001
200193	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200193-001	201006-002	...	201006-001	201006-001	201004-001
200194	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200194-001	201006-002	...	201006-001	201006-001	201004-001
200195	PSD-Sekundäre (Standard)	12.09.2017	10:56:30	1	0	0	200195-001	201006-002	...	201006-001	201006-001	201004-001

Abb. 2: Die Zelisko-Backofficelösung zur Verwaltung, Wartung und Kontrolle der Fahrscheindrucker (Quelle: © Zelisko)

## Die alternative Kryptowährung „Ethereum“ oder auch „Kennen Sie schon dApps“?

von Andreas Steiner

**Jedem ist heutzutage „Bitcoin“ ein Begriff – aber wussten Sie, dass dieser Markt bereits über 1.000 verschiedene Kryptowährungen umfasst?**

Kaum eine Kryptowährung kommt momentan an den Marktwert des Bitcoins ran. Doch seit 2017 hat die alternative Kryptowährung Ethereum nicht nur in den Medien für Aufsehen gesorgt.

Ethereum ist im Vergleich zu Bitcoin nicht als Währung gedacht sondern als eigene Plattform, welche das Anlegen, Verwalten und Ausführen von Programmen (kurz dApps für dezentrale Applikationen) bzw. Verträgen (Smart Contracts) in der eigenen Blockchain anbietet.

Die interne Kryptowährung Ethereums nennt sich Ether. Ether wird von Entwicklern benötigt, deren dApps die Ethereum-Blockchain verwenden, aber auch von Benutzern welche sog. Smart

Contracts abschließen möchten. Das Netzwerk Ethereum selbst sieht Ether nicht als „Coin“ (in diesem Sinne gleichbedeutend mit Währung) sondern als „Token“ bzw. Treibstoff für ihr System, um für Blockchain-Berechnungen zu bezahlen.

So müssen Entwickler, welche dApps entwickeln, Ether für die Rechenleistung bezahlen um die angeforderten Transaktionen ausführen zu lassen.

Vom Aspekt der Qualitätssicherung dient Ether dazu, die Entwickler anzuspornen qualitativ hochwertige dApps zu schreiben, um so Kosten zu sparen und damit gleichzeitig das Netzwerk performant zu halten.

Kommen wir nun zu den dApps. Eine dApp hat folgende Definitionskriterien:

- Open Source – eine dApp muss frei zugänglichen Source-Code zur Verfügung stellen.



**Andres Steiner** ist Consultant für Software Test bei SEQIS.

Die Schwerpunkte seiner Projekterfahrung liegen in den Bereichen Testautomation, Testdurchführung, Softwarequalitätssicherung und Requirements Engineering.

Kommunikation, Teamwork sowie vorausschauendes Arbeiten sind für ihn essenzielle Bestandteile für einen reibungslosen Projektablauf.

- Blockchain – eine dApp muss alle Daten, Berichte und den Quellcode auf einer dezentralisierten Blockchain speichern.
- Kryptografisch verschlüsselte Token – dies sind digitale Einheiten, welche eine Kopie eines sensiblen Datensatzes auf einer Blockchain darstellen.
- Erzeugung von Token (für Miner) – eine dApp muss einen Proof-of-Work-Algorithmus verwenden, um diese Token generieren zu können, welche von Benutzern dadurch „gemined“ werden.

Bei Ethereum wird „Ethash“ als Algorithmus für den Proof-of-Work eingesetzt. Dieser verwendet Versionen des „SHA3-256“ und „SHA3-512“ Algorithmus. Im Gegenzug: Der Bitcoin verwendet den SHA-256-Algorithmus.





Grundsätzlich ist Bitcoin eine dApp, wohingegen Ethereum eine Plattform für dApps darstellt, selbst aber auch eine dApp ist – also eine dApp für dApps sozusagen.

Der Unterschied liegt hierbei bei den integrierbaren „Smart Contracts“ (oder auch selbst-erfüllende Verträge). Die Bedingungen dieser Verträge werden fest vorgegeben programmiert – werden sie erfüllt, laufen der Vertragsabschluss und die damit verbunden(en) Transaktion(en) automatisch ab.

Dies bringt den Vorteil, dass menschliche Fehler größtenteils ausgeschlossen werden können. Grundsätzlich ist die Idee der Smart

Contracts nichts Neues, denkt man an einen Getränkeautomaten. Man wirft die geforderte Summe Münzen ein, drückt eine Zahlenkombination und bekommt voll automatisch das gewünschte Getränk.

So eröffnet Ethereum mit Smart Contracts und den dadurch resultierenden dApps neue Geschäftsfelder und ungeahnte Möglichkeiten. Doch durch die direkte Integration der Smart Contracts in die Blockchain ist das System aber auch manipulativer.

Aufgrund eines aufgetretenen Fehlers (DAO Vorfall) wurde nach Abstimmung mit der Community ein Hardfork (= nicht abwärts kompatible Änderung im Protokoll)

in Ethereum Classic (ETC) und Ethereum (ETH) durchgeführt.

Für die Zukunft bleibt es spannend, wie sich dApps entwickeln werden.

Persönlich denke ich, ist dies der nächste Schritt nach dem „Internet of things“ in eine stärker vernetzte und automatisierte Welt. ■



*Titel: „Verschiedene Menschen“, Künstler: Max Minnichmayr, Technik: Filzstifte auf Leinwand*



# Blockchain für IT Analytiker

von Josef Falk

## Einführung

IT Analyse – das ist das Ermöglichen von Veränderung in Organisationen durch die Gestaltung von IT Systemen. Ein IT Analytiker ist Gestalter von Lösungen. Um innovative Lösungen schaffen zu können, muss ein Analytiker Überblick über die aktuellen Technologien haben. Eine dieser intensiv diskutierten neuen Technologien ist die Blockchain.

Die Blockchain-Technologie wurde im Kontext der Kryptowährung Bitcoin bekannt.<sup>1</sup> Sie wird mittlerweile in Zusammenhang mit vielen anderen Anwendungen diskutiert, sodass davon auszugehen ist, dass sie im Alltag des IT Analytikers in Zukunft häufig vorkommen wird.

Ziel dieses Artikels ist es, einen Überblick über die Funktionsweise der Blockchain zu geben, ohne zu tief in die technischen Details einzudringen. So soll ein Eindruck gewonnen werden, welche Anwendungsbereiche für die Blockchain denkbar sind.

## Blockchain in acht Punkten

Im Folgenden wird die Funktionsweise einer Blockchain in acht Punkten erläutert. Im Prinzip gilt diese Darstellung für alle möglichen Anwendungsgebiete, auch wenn im Detail immer wieder speziell auf Bitcoin Bezug genommen wird.

### 1. Keine zentrale Stelle

Eines der Hauptmerkmale der Blockchain-Technologie ist es, dass es keine zentrale Stelle gibt, die die einzelnen Transaktionen verwaltet – es handelt sich um ein

Peer-to-Peer-Netzwerk, in dem jeder Teilnehmer gleichberechtigt ist. Es ist niemand erforderlich, der Transaktionen bewilligen bzw. bestätigen muss. Dadurch werden auf der einen Seite Kosten gespart. Auf der anderen Seite werden die Transaktionen beschleunigt, da die Verarbeitungszeit in einer zentralen Stelle wegfällt.

### 2. Keine Konten – nur Transaktionslisten

Es gibt jedoch nicht nur keine zentrale Stelle, die so etwas wie Konten verwaltet. Es gibt auch keine Konten.

Die Blockchain hält Transaktionen fest. Diese Transaktionen geschehen im Zeitablauf in einer bestimmten Reihenfolge. Wenn Geld in einer Transaktion übertragen wurde, kann das nicht rückgängig gemacht werden. Eine Transaktion, die einmal in der Blockchain steht, kann nicht mehr geändert werden.

Die Blockchain ist also nichts weiter als eine Liste der Transaktionen. Im Beispiel der Kryptowährungen wird nur festgehalten, wer an wen Geld übertragen hat. Aus diesen Informationen ist ableitbar, wer über welche Menge an Geld verfügen kann. Was man ausgeben will, muss man vorher eingenommen haben.

### 3. Transaktionsliste ist verteilt

Diese Transaktionsliste wird nicht von einer zentralen Stelle geführt. Jeder der am System teilnehmenden Partner hat diese Transaktionsliste auf seinem Rechner gespeichert. Damit hat auch jeder Partner die Möglichkeit, jederzeit die Richtigkeit und Konsistenz der Transaktionsliste zu prüfen.

Eine Manipulation der Transaktionsliste an einer Stelle ist daher sinnlos, weil es immer noch unzählige „richtige“ Kopien der Transaktionsliste gibt. Die manipulierte Liste würde sich nicht durchsetzen (siehe Abb. 1).

### 4. Anonymisierung der Benutzer

Die Transaktionsliste lässt keinen Rückschluss auf die Identität der einzelnen Partner der Transaktionen zu. Die Beteiligten sind nur mit ihrer „Adresse“ identifiziert.

In Bitcoin ist das eine Kette von 27-34 alphanumerischen Zeichen. Jede Person kann beliebig viele dieser Adressen haben. Mit einer Adresse ist auch ein privater Schlüssel verbunden. Dieser private Schlüssel ist erforderlich für den Zugang zu seiner Bitcoin-Adresse. Deshalb ist es wichtig, diesen privaten Schlüssel nicht zu verlieren. Ohne diesen Schlüssel hat der Besitzer keinen Zugang

Datum	Absender	Empfänger	Betrag
02.11.2017	A	B	10,--
04.11.2017	B	C	5,--
05.11.2017	B	D	5,--

Tabelle 1: Beispiel einer Transaktionsliste

## Auflösung des Gewinnspiels der letzten QualityNews-Ausgabe

Beim Gewinnspiel der Ausgabe QualityNews H2/2017 musste folgende Gewinnfrage richtig beantwortet werden:

**Auf einem Regal stehen mehrere Uhren in einer Reihe neben einander.**

**Zwei davon sind Kuckucksuhren. Eine Kuckucksuhr ist die sechste Uhr von links, die andere ist die achte Uhr von rechts. Zwischen den beiden Kuckucksuhren stehen genau drei andere Uhren.**

**Wie viele Uhren stehen mindestens im Regal?**

**Antwort A: 9**

**Antwort B: 12**

**Antwort C: 17**

**Die richtige Antwort lautet:**

**Antwort A: 9**

Wir gratulieren dem Gewinner des Handbuch zur neuen EU Datenschutz-Grundverordnung: Thomas Morawetz, Generali Versicherung AG.

**Auch dieses Mal gibt es wieder einen tollen Preis zu gewinnen!**

Nutzen Sie Ihre Chance und gewinnen Sie ein Exemplar des Buches „Managing for Happiness“ von Jurgen Appelo.

Das Gewinnspiel dieser Ausgabe finden Sie auf Seite 16.



### **Kennen Sie schon den SEQIS Videoblog auf YouTube?**

„SEQIS - im Gespräch“ – so lautet der Titel unseres neuen Formates auf YouTube. Im Mittelpunkt stehen dabei unsere Experten, welche ihr Fachwissen in entspannter Atmosphäre an die Zuseher weitergeben.

- Kurze, knackige Videos
- Aktuelle Trends und Themen der IT Branche auf den Punkt gebracht
- Informationsplattform für Interessierte und Gleichgesinnte

#### **Sie möchten unseren YouTube-Channel abonnieren?**

Hier finden Sie alle unsere Videos: [www.youtube.com/channel/UCX2cm6EigOv-63mZ6SLcwog](https://www.youtube.com/channel/UCX2cm6EigOv-63mZ6SLcwog)

Wir freuen uns, Sie als Follower zu begrüßen und wünschen Ihnen viel Vergnügen beim Streamen!

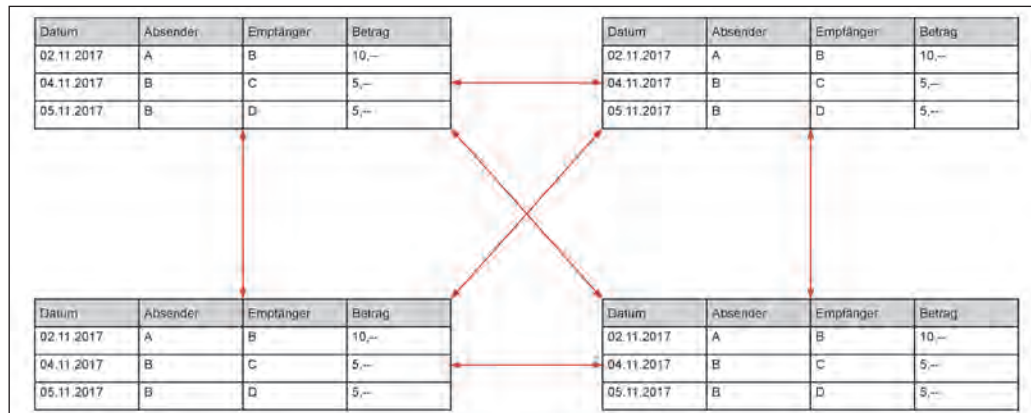


Abb. 1: Verteilte Transaktionsliste – jede Liste ist mit jeder anderen Liste verknüpft  
(Quelle: © SEQIS GmbH)

mehr zu seinen Transaktionen – und somit zu seinen Bitcoins. Mangels einer zentralen verwaltenden Stelle gibt es auch keine „Passwort vergessen“-Funktionalität.

#### 5. Zusammenfassung zu Blöcken

Der erste Teil des Namens „Blockchain“ ergibt sich daraus, dass die Daten in Blöcken abgespeichert werden. Im Falle von Bitcoin und anderen Kryptowährungen sind es Transaktionen, die zu Blöcken zusammengefasst werden.

Es könnte aber auch jede andere Form von digitalen Daten sein. Die laufend entstehenden Transaktionen werden geprüft und im Durchschnitt wird alle 10 Minuten aus diesen Transaktionen ein Block gebildet.

#### 6. Jeder Block wird durch seinen Hash identifiziert

Durch einen Algorithmus wird für jeden Block ein Hash erstellt. Dieser Hash ist eine 64-stellige Zeichenkette aus Buchstaben und Ziffern. Aus diesem Hash kann der ursprüngliche Inhalt nicht rekonstruiert werden.

Wenn irgendetwas in einer Transaktion des Blocks geändert würde, dann würde sich auch der Hash ändern. So kann durch Vergleich der Hash-Werte auf

einfache Art und Weise geprüft werden, ob alle Versionen der verteilten Transaktionsliste identisch sind.

Dieser Hash ist auch die identifizierende ID – über seinen Hash kann jeder Block wiedergefunden werden.

Beispiel für einen Hash:  
822856e5d4e90fa61ce6054b75a8  
268f3285497c3db694a 33b00013  
ade44db0c

#### 7. Die Blöcke sind über ihre Hash-Werte verknüpft

Die Blöcke sind in der Blockchain in zeitlicher Reihenfolge ihres Entstehens abgespeichert. Dabei ist der Hash (also die ID) eines Blockes jeweils in seinem Nachfolger enthalten – und ist damit auch wieder Bestandteil des Hashes des Nachfolgers. Somit kann aus jedem Block sein Vorgänger ermittelt werden.

Daraus ergibt sich nun der zweite Teil des Begriffes „Blockchain“. Die Blöcke sind miteinander verkettet.

Dadurch ist es möglich, die gesamte Blockchain zu prüfen. Die Kette darf nicht „gebrochen“ sein. Das heißt, der Vorgänger-Hash muss jeweils tatsächlich den Wert haben, wie er im Nachfolger-Block angegeben ist. Außerdem kann so einfach überprüft werden, ob die verschiedenen Versionen der Blockchain tatsächlich identisch sind.

#### 8. Mining

Wie entstehen aber nun diese Blöcke? Wer sorgt dafür, dass die Blöcke richtig sind? Und wie entstehen eigentlich neue Bitcoins? Die Antwort auf alle diese Fragen ist: „Mining“. Mining ist der Prozess, der eingehende Transaktionen zu Blöcken zusammenfasst.

Durchgeführt wird dieser Prozess von Teilnehmern am System. Damit ein Block in die Blockchain aufgenommen wird, muss ein mathematisches Rätsel gelöst werden. Dieses besteht darin, den Block so durch eine Zahl zu ergänzen, dass dessen Hash mit einer bestimmten Anzahl von führenden Nullen beginnt.

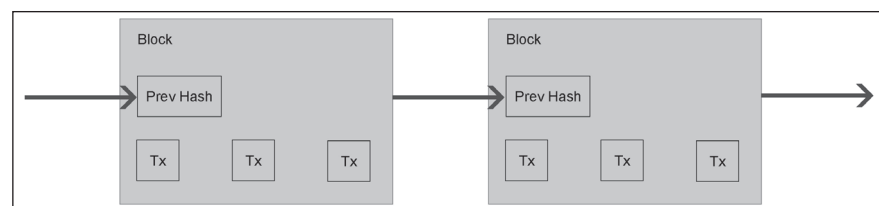


Abb. 2: Verknüpfung der Blöcke  
(Quelle: © SEQIS GmbH)



Diese Zahl, um die der Block ergänzt wird, wird „Nonce“ genannt. Es gibt kein mathematisches Verfahren dafür, wie diese Zahl zu ermitteln ist.

Deshalb geht das nur durch Probieren. Es werden solange Werte für diese Nonce versucht, bis der Hashwert (für Block + Nonce) die geforderte Anzahl an führenden Nullen hat. Sobald das erreicht ist, wird der Block in die Blockchain aufgenommen.

Beispiel für den Hash  
eines Blocks nach dem Mining:  
00000000000000000600f97b9b  
be3dfbf76967a5a49b0595ebb6b  
750e96df15

Dieses „Mining“ ist ein sehr rechen- und energieintensiver Prozess. Die Miner stehen dabei im Wettbewerb zueinander. Jener Miner, der dieses Rätsel als erster löst, d.h. der als erster die Nonce findet, die die geforderte Anzahl an führenden Nullen im Hash erzeugt, erhält für seine Bemühungen eine gewisse Anzahl von neu geschaffenen Bitcoins, derzeit 12,5.

Und das ist auch die Art und Weise, wie neue Bitcoins entstehen. Es wird also in gewissem Sinne nach neuen Bitcoins „geschürft“. Deshalb wird dieser Prozess „Mining“ genannt. Nachdem der Block auf diese Weise gebildet wurde, wird er in die Blockchain aufgenommen und bildet so die Basis für die Berechnung des nächsten Blocks.

## Sechs Schritte von der Transaktion zum Block

Was passiert von dem Zeitpunkt, an dem eine Transaktion mit Bitcoins bezahlt wird, bis die Transaktion in der Blockchain verewigt ist?

Folgende sechs Schritte sind dafür erforderlich:

1. Neue Transaktionen werden an alle Knoten übertragen. Ein Knoten ist jeder Teilnehmer am Bitcoin-Netzwerk.
2. Jeder Knoten fügt die neuen Transaktionen zu einem Block zusammen.
3. Jeder Knoten versucht eine Zahl zu finden (Nonce), die den Block so ergänzt, dass dessen Hash mit der geforderten Zahl an führenden Nullen beginnt.
4. Wenn ein Knoten diese Zahl gefunden hat, verteilt er den Block an alle anderen Knoten.
5. Die anderen Knoten akzeptieren diesen Block, wenn alle Transaktionen im Block gültig sind.
6. Die Knoten akzeptieren den Block, indem sie ihn als Basis für die Schaffung des nächsten Blocks nehmen, d.h. indem sie den Hash des Blocks in den nächsten Block schreiben.

## Anwendungsmöglichkeiten

Entstanden ist die Blockchain-Technologie im Zusammenhang mit den sogenannten Kryptowährungen, konkret mit der Währung „Bitcoin“.

Dort sollte damit vor allem ein Problem gelöst werden: Das des sogenannten „Double Spending“. Darunter versteht man, dass ein und dieselbe Geldeinheit vom Besitzer zwei- und mehrfach ausgegeben wird.

Da dieses virtuelle Geld ja keine reale Entsprechung hat, muss die Möglichkeit der Mehrfachverwendung durch entsprechende Vorkehrungen verhindert werden. Mit der Blockchain wurde das verwirklicht.

Inzwischen wird diese Technologie in vielen anderen Zusammenhängen diskutiert. Auch in solchen, in denen das Problem des „Double Spending“ gar nicht auftreten kann.

Beispiele dafür sind:

- **Energiesektor:**  
Die Blockchain könnte auch im Energiebereich ein Peer-to-peer-Netzwerk bilden. Das heißt, die Konsumenten versorgen sich gegenseitig mit Strom, der aus Photovoltaik-Anlagen oder aus Elektroauto-Ladestationen kommt, ohne, dass dabei ein Energieversorgungsunternehmen beteiligt ist. Verrechnet wird das ganze über eine Blockchain.<sup>2</sup>
- **Banken und Versicherungen:**  
Nutzer schließen sich zusammen, um durch Einzahlungen in eine Blockchain Versicherungsleistungen oder Kredite finanzieren zu können.<sup>3</sup>
- **Grundbuch:**  
Auch für die Eintragung von Eigentumsrechten an Grundstücken gibt es Pilotprojekte, die auf der Blockchain-Technologie basieren.<sup>4</sup>
- **Wahlen:**  
Es gibt Überlegungen, wie eine Blockchain auch die Durchführung von demokratischen Wahlen revolutionieren könnte.<sup>5</sup>

Das sind nur einige Beispiele, in denen die Blockchain schon jetzt im Einsatz bzw. zumindest im Versuchsstadium ist. Die tatsächlichen, theoretisch möglichen Einsatzbereiche gehen noch weit darüber hinaus.

## Fazit

Auch, wenn die kommerzielle Zukunft der Kryptowährung Bitcoin keineswegs entschieden ist und es sich dabei möglicherweise um eine Blase handelt, die jederzeit platzen kann, so ist es doch prinzipiell erwiesen, dass eine Währung auf der Basis der Blockchain technisch funktioniert.

Mit mehr oder weniger großen  
Adaptionen ist diese Technologie

auch in vielen anderen Fachdomänen einsetzbar.

Inwieweit das die Arbeit der IT Analytiker verändern wird, das wird die Zukunft weisen. Es lohnt sich jedoch in jedem Fall, sich schon jetzt mit dieser Technologie auseinanderzusetzen. Und dazu will dieser Artikel einen kleinen Beitrag leisten. ■

#### Quellennachweis:

<sup>1</sup> Nakamoto, Sakoshi: Bitcoin: A Peer-to-Peer Electronic Cash System (<https://bitcoin.org/bitcoin.pdf>)

<sup>2</sup> Die Blockchain verändert das Spiel in der Energiewirtschaft (<http://next.pwc.at/2017-01/from-sharing/blockchain.html>)

<sup>3</sup> <http://www.wetrust.io>

<sup>4</sup> Schweden nutzt jetzt offiziell die Blockchain für Grundbucheintragen (<https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragen/>)

<sup>5</sup> Wie eine Technologie unser Wahlsystem revolutionieren könnte, Handelsblatt (<http://www.handelsblatt.com/politik/deutschland/bundestagswahl/alle-schlagzeilen/block-chain-wie-eine-technologie-unser-wahlsystem-revolutionieren-koennte/20366520.html>)

## SEQIS „10 things“-Expertentreff #04/2017: „Sind Sie (sich) wirklich sicher? – IT Security im Fokus“

von Klemens Loschy

**Beim letzten Expertentreff 2017 drehte sich alles rund um die IT Security und die Frage, wie diese erfolgreich in den Software Development Life Cycle integriert werden kann.**

### 1. Definieren Sie eine unternehmensweite Sicherheitsrichtlinie!

Jedes Unternehmen braucht als Security-Ausgangsbasis eine eindeutige Sicherheitsrichtlinie. Darauf stützen sich fast alle weiteren sicherheitsrelevanten Initiativen.

Gute Grundlagen für diese Richtlinie sind z.B. Gesetze (z.B. EU DGSVO), Normen (z.B. ÖNORM A 7700), Standards (z.B. PCI) oder Best Practices (z.B. OWASP). Die unternehmensweite Sicherheitsrichtlinie definiert sowohl grob die generelle Bedeutung von Security im Unternehmen, den allgemeinen Umgang mit zu schützenden Daten, aber auch detailliert wie die Zugriffe auf Umgebungen (DEV/TST/PROD) geregelt sind oder wie der On- &

Offboarding-Prozess im Detail umzusetzen ist.

Ein Tipp dabei: Versuchen Sie nur 1 (!) Richtlinie zu etablieren, diese sollte dafür jedoch stets aktuell und akkurat sein.

### 2. Unterstützen Sie Ihre Mitarbeiter mit sinnvollen Einschränkungen!

Regeln müssen sein! Nicht umsonst beruht der erste Tipp auf der Definition von Sicherheitsrichtlinien. Diese Regeln führen sehr oft zu Einschränkungen der Mitarbeiter – ausführbare Dateien dürfen nicht per E-Mail versendet werden oder Passwörter müssen in (zu) kurzen Abständen wieder und wieder geändert werden. Die lokalen Schreibrechte sind auf wenige Bereiche beschränkt und USB-Geräte sind nicht oder nur eingeschränkt verwendbar.

Aus Security-Sicht sind das auf den ersten Blick sinnvolle und verständliche Richtlinien, doch die Praxis lehrt das Gegenteil:



**Klemens Loschy** kann auf jahrelange Erfahrung in den Bereichen Testautomation, Last- und

Performancetests, funktionale Tests, Testen in agilen Teams, Anwendungsentwicklung von Testsoftware sowie Beratung und Unterstützung in zahlreichen Projekten unterschiedlichster Branchen zurückblicken.

Durch sein hohes Interesse an Test und Softwareentwicklung sowie an Technik im Allgemeinen, kann er stets die neuesten Erkenntnisse in seine Projekte miteinbeziehen.

Seine Flexibilität, Einsatzbereitschaft und sein breites Wissen zeichnen sich in agilen Projekten besonders aus.

Wird das tägliche Arbeiten durch große Hürden zu stark eingeschränkt, werden diese kreativ und unsicherer von den Mitarbeitern umgangen.

Es tritt also der Effekt ein, dass die Sicherheit, trotz umfangreicher Regeln sinkt. Hier gilt oft: Weniger ist mehr!

### 3. Security muss von Anfang an berücksichtigt werden!

Am Anfang jeder Software stehen die Anforderungen – funktionale und nicht funktionale. Um in der Analyse- & Design-Phase sicherheitsrelevante Anforderungen (oder Merkmale von Anforderungen) den notwendigen Stellenwert zu geben, müssen Sie besonders darauf eingehen:

Erweitern Sie „Personas“ durch die Eigenschaft „Sicherheitsbewusstsein“. Aus den etablierten „6 thinking hats“ werden 7 → ein zusätzlicher „hat“ mit Fokus auf Security kommt hinzu.

Alle Anforderungen müssen natürlich den zuvor definierten Sicherheitsrichtlinien entsprechen, ein Review der Anforderungen in dieser Phase ist also angebracht. Zusätzliche funktionale und nicht funktionale Anforderungen werden sich ergeben, wenn Sie die (auf Security bezogenen) Best Practices der eingesetzten Technologien und Architekturen berücksichtigen.

### 4. Definieren Sie Coding Guidelines und halten Sie diese ein!

„I don't get your code“ – „Neither do I, but it seems to work“

Acht Beispiele für Coding Guidelines – diese sind auch in stressigen Zeiten, wie vor Releases oder Milestones, unbedingt zu beachten:

1. Code must be read- and

understandable

2. Keep it small and simple
3. Minimize the attack surface area
4. Least necessary privilege
5. Obscurity is not security
6. Validate input and verify consistency
7. Don't trust (services, dependencies, ...)
8. Don't develop custom authentication and session management

### 5. Gehen Sie sorgsam mit Benutzerdaten um!

Die Verantwortung der sicheren Aufbewahrung der Kundendaten liegt (ganz klar per Gesetz geregelt) beim Anbieter. Dementsprechend muss es auch in Ihrem Interesse sein, Benutzerdaten so zu persistieren, dass, im Falle eines Datenverlustes, die Auswirkungen minimal sind.

Dabei hilft: Benutzerdaten, die nicht im Klartext lesbar sein müssen (darunter fallen eindeutig Passwörter, aber auch Passwortfragen und -hinweise können so behandelt werden), werden mit kryptografischen Hash-Algorithmen unidirektional verändert.

Alle anderen zu schützenden Benutzerdaten (z.B. Kreditkarteninformationen) werden bidirektional verschlüsselt und können im Bedarfsfall wieder entschlüsselt werden.

Achtung: Es werden immer wieder Algorithmen als unsicher erklärt, sehen Sie also die Möglichkeit vor, Ihre verwendeten Algorithmen einfach ändern zu können.

### 6. Forcieren Sie Länge und Eindeutigkeit bei Passwörtern!

„Mindestens eine Zahl, mindestens ein Sonderzeichen und ab und zu einfach mal ein neues Passwort.“  
(Quelle: Bill Burr, 2003, National Institute for Standards and Technology – NIST)

14 Jahre nach dieser Definition eines (vermeintlich) guten Passwortes hat das NIST diese Aussagen revidiert. Seien Sie Vorreiter und setzen Sie die neuen Empfehlungen bereits jetzt um:

1. Die Länge von Passwörtern ist deutlich mehr von Bedeutung als der verwendete Sprachraum: „ein sicheres passwort“ (basiert nur auf Kleinbuchstaben und einem Sonderzeichen) ist deutlich (Faktor: 1 Million \* 1 Million \* 1 Million) sicherer als „Pas\_w0rT!“, und obendrein noch einfacher zu merken
2. Verwenden Sie für jede Applikation/Portal ein neues, eindeutiges Passwort

### 7. Security Issues findet man nicht nebenbei!

Beim Testen verhält es sich ähnlich wie bei der Anforderungsdefinition: Sicherheitsrelevante Anforderungen werden genauso wenig zufällig definiert, wie Security Issues durch einfache funktionale Test gefunden werden.

Deswegen gilt hier auch der selbe Ansatz: Machen Sie bewusst Test Sessions mit Fokus auf Security – z.B. auf sichere Authentifizierung und Session Management, XSS und SQL Injections oder auf korrekte serverseitige Validierung der Eingaben.

Organisieren Sie zusätzlich professionelle Penetration Tests: Dabei werden Ihre Architektur, Applikation bis hin zu Prozessen durchleuchtet, sicherheitsrelevante Schwachstellen identifiziert und dann mit Ihnen gemeinsam priorisiert und einer Lösung zugeführt.

### 8. Sichern Sie Ihre Systeme durch etablierte Appliances (IDS, IPS, UTM, usw.)!

Die Verwendung etablierter Appliances wie IDS, IPS, UTM,



Firewall, NSM oder SIEM gehört heutzutage zum Standard – und das ist auch gut so! Doch eines gibt es zu Bedenken:

All diese Appliances sind nur so gut wie diejenigen, die sie betreuen. Es ist also unbedingt notwendig, dem Operations-Team die notwendige Zeit für Know-how Aufbau und die Wartung der Regeln zu geben. Systeme mit aktuellem Softwarestand und Patchlevel sind grundsätzlich weniger anfällig gegen Attacken als veraltete Systeme. Halten Sie also unbedingt alle Systeme up2date – und testen Sie nach jedem Update auf unerwartete negative Sideeffects. Schnelles Feedback bekommt man, wenn man die Software Testing Pyramide von Anfang an konsequent berücksichtigt.

### 9. Erstellen und testen Sie Ihren Data Breach Plan!

Der Data Breach Plan kommt im Ernstfall zum Einsatz und definiert konkrete Vorgehensweisen und Regeln – das heißt aber auch, dass er im Vorfeld erstellt und unbedingt getestet werden muss. Ab dem Zeitpunkt, wo ein Datenleck bekannt wird, müssen jeder Schritt und jede Aktion mit Bedacht und Sicherheit gesetzt werden – das gelingt nur, wenn alle Beteiligten darin geübt sind. Der Einsatz eines RED Team Assessments kann dabei helfen, die bisher gesetzten Security-Maßnahmen zu überprüfen und den Ernstfall so weit wie möglich zu simulieren.

### 10. Nehmen Sie Social Engineering ernst!

Auch wenn wir technisch alles richtig gemacht haben, der Human Factor spielt beim Thema Security eine wesentliche Rolle: Die Tatsache, dass (laut einer deutschen Studie 2016) beinahe ein Drittel aller Passanten

bereitwillig ihre Windows Benutzerdaten (inklusive Passwort) genannt haben, sollte die Alarmglocken schrillen lassen.

Einzig die Tatsache, dass durch eine kleine Aufwandsentschädigung (in dem konkreten Fall Schokolade) die Quote auf fast 50% erhöht werden konnte, ist noch alarmierender: Mit rund 3 € kann man also alle getroffenen, millionenschweren Investitionen zur Erhöhung der Sicherheit aushebeln.

Diesem Verhalten muss man als Unternehmen vorbeugen: Jegliche Art, die Awareness in diesem Bereich zu schärfen (z.B. durch gezielte Workshops), ist gut investiertes Geld.

### 11. Security muss aktiv betrieben werden!

Ich bin mir sicher: Wenn Sie diese Tipps in Händen halten sind Sie sich der durchaus bedrohlichen Situation bewusst. Jeder wird (früher oder später) oder wurde bereits Ziel einer Attacke.

Wie man sich davor schützen kann oder die Auswirkungen auf ein sinnvolles Minimum reduziert, ist in diversen Best Practices, Normen, Standards und nicht zuletzt in diesen „10 things“ beschrieben.

Fehlt also nur noch eine Kleinigkeit:  
Reden wir nicht länger über Security, sondern tun wir gemeinsam etwas dafür – besser früher als später! ■



Foto: SEQIS Expertentreff „Sind Sie (sich) wirklich sicher? – IT Analyse im Fokus“  
(© SEQIS GmbH)

### Haben Sie sich die Termine für 2018 schon vorgemerkt?

Auch in diesem Jahr gibt es wieder vier spannende Veranstaltungen mit unseren Experten – Fachvortrag, Networking & Wissensaustausch.

Alle weiteren Informationen finden Sie auf Seite 15 und unter [www.SEQIS.com](http://www.SEQIS.com) – check IT out!

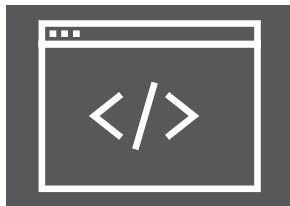


SEQIS ist der führende österreichische Anbieter in den Spezialbereichen IT Analyse und Software Test. Beratung, Verstärkung und Ausbildung – Ihr Partner für hochwertige IT-Qualitätssicherung.



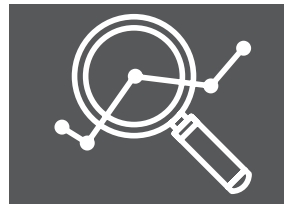
## IT ANALYSE

Notwendige Änderungen analysieren und IT-gerecht aufbereiten



## CODING

Guten Code schreiben und schlechten Code überarbeiten



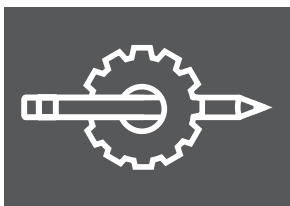
## TESTING

Probleme durch methodischen Soll-Ist Vergleich erkennen



## RELEASE & OPERATE

Reibungsloser Go Live und Betrieb der IT-Lösungen



## DEVOPS

Neuerungen abgestimmt mit Entwicklung und Betrieb live setzen



## METHODOLOGY & TOOLS

Vorgehensweisen optimieren und auf die richtigen Tools setzen



## TRAINING & WORKSHOPS

Mitarbeiter Know-how stärken – standardisiert oder maßgeschneidert