Hochschule für Angewandte Wissenschaften Hamburg
*Hamburg University of Applied Sciences*

# Ausarbeitung

**Marvin Schwieger**

## Blockchain - Möglichkeiten und Herausforderungen von Smart Contracts

*Fakultät Technik und Informatik*
*Studiendepartment Informatik*

*Faculty of Engineering and Computer Science*
*Department of Computer Science*

Marvin Schwieger

# Blockchain - Möglichkeiten und Herausforderungen von Smart Contracts

Ausarbeitung eingereicht im Rahmen der Vorlesung *Grundseminar*

im Studiengang Master of Science Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuer: Prof. Dr. Kai von Luck
Betreuer: Prof. Dr. Tim Tiedemann

Eingereicht am: 15. August 2017

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Einleitung

Die digitale Währung Bitcoin wird heutzutage mehr und mehr Diskussionsgegenstand in den Medien, je höher ihr Wert steigt. Die Marktkapitalisierung liegt mittlerweile bei 76 Milliarden US-Dollar (Blockchain.info) und bisher ist nicht abzusehen, wie sich dieser Wert verändern wird. Doch ist es nicht mehr nur Bitcoin, ueber die diskutiert wird: Der ihr zugrunde liegenden Technologie, die Blockchain, wird nachgesagt, dass sie das Potenzial besitzt, nachhaltig unsere Gesellschaft zu verändern und das auch ueber ihren Nutzen als Fundament einer digitalen Währung hinaus. Doch bisher gibt es noch keinen Konsens, in welchen Bereichen unserer Gesellschaft sich diese Technologie niederschlagen wird und die Euphorie, die hinter Bitcoin, neueren Blockchain-Projekten und -Startup steht löst vermehrt die Sorge aus, dass das rasante Wachstum von Kryptowährungen dem der Dotcom-Blase der späten Neunziger-Jahre aehnelt.

## 1.1 Gliederung

Die vorliegende Ausarbeitung hat zum Ziel das wissenschaftliche Feld des Blockchain-Modells zu kartografieren. Konkret bedeutet das, seinen derzeitigen Stand aufzuarbeiten und anschließend aktuelle Hindernisse und Fortschritte aufzuzeigen. Dabei wird zunächst erläutert aus welchen grundlegenden Bestandteilen eine Blockchain besteht und welche Applikationen auf ihr aufgebaut werden können. Anschließend werden derzeit existierende sowie theoretische Anwendungsfälle von Blockchain-Technologie inklusive ihrer Vor- sowie Nachteile vorgestellt.

In einem zweiten Teil werden sog. **Smart Contracts** (auf einer Blockchain gespeicherter Bytecode) untersucht. Dabei geht der Verfasser der Fragestellung nach, welche Angriffe auf Smart Contracts bekannt sind, inwiefern sie durch fehlerhafte Konostruktion des Codes durch Entwickelr selbst verursacht werden und welche Ansätze existieren, solche Applikationen resistenter gegen Fehlkonstruktion und Angriffe zu machen.

## 1.2 Motivation

Es ist nicht bestreitbar, dass digitale Innovationen des letzten Jahrzehnts unsere Leben langfristig verändert haben: Viele Menschen mit Zugang zu Kommunikations- und Informationstechnik wirtschaften und leben heutzutage anders als frÃ¼her. Die juengste Vergangenheit hat gezeigt. dass neue Entwicklungen in der Informatik das Potenzial haben, Wirtschafts- und Gesellschaftsfelder neu aufzurollen und immer mehr Menschen versprechen sich das auch von der Blockchain. Das dezentrale, transparente Modell hat die Fähigkeit als Fundament einer Infrastruktur zu gelten, die ohne Vertrauen und einem gewissen Grad Anonymität funktioniert. Auch wenn noch nicht abzusehen ist, in welcher Größenordnung Blockchain-Technologie in der Zukunft eingesetzt wird, so scheint ihre bisherige Entwicklung einen genaueren Blick und Bewertung wert zu sein.

# 2 Blockchain - Grundlagen

Dieser Abschnitt befasst sich damit, aus welchen Komponenten eine Blockchain im wesentlichen besteht und wie sie im wesentlichen funktioniert. Abschließend werden verschiedene Ausprägungen des Blockchain-Modells aufgezählt und kurz beschrieben.

## 2.1 Komponenten einer Blockchain

Eine Blockchain ist eine dezentralisierte Datenbank, in der alle Transaktionen zwischen Teilnehmern persistiert werden. Durch den Austausch ueber ein Peer-to-Peer-Netzwerk besitzt Partei eine Kopie dieser Datenbank und ist dazu in der Lage, jede stattgefundene Transaktion einzusehen und einen kryptographischen Beweis ihrer Gueltigkeit oder Ungueltigkeit zu erbringen. Dadurch kann das gesamte Netzwerk zu einem Konsens kommen, welchen Status das System zum aktuellen Zeitpunkt hat.

In einer öffentlichen Blockchain gibt es keine Notwendigkeit fuer eine zentrale Verifizierungsstelle. An ihre Stelle tritt eine Menge von sog. **Miner-Knoten**, die die Integrität der Transaktions-Historie ueber rechenintensive, sog. **Proof-of-Work**-Algorithmen wahren (Gjermundrød u. a., 2016). Diese Rechen-Knoten können fuer ihren Aufwand durch eine Transaktionsgebuehr entschädigt werden. Das ist zum Beispiel bei Bitcoin der Fall.

Porru u. a. (2017) definieren eine Blockchain als eine Datenstruktur, die folgende Kriterien erfuellt:

- **Archivierung**: Alle Transaktionen werden in sequentiell geordnete Blöcke, deren Zusammenstellung den Regeln eines Konsens-Algorithmus unterliegt.
- **Datenredundanz**: Es gibt mehrere Knoten, die unabhängig voneinander sind und jeder besitzt eine Kopie der Blockchain.
- **Validierung**: Jede Transaktions muss auf Gueltigkeitskriterien ueberprueft werden
- **Verschluesselung**: Transaktionen basieren auf der Public-/Private-Key-Kryptographie.

- *(Optional)* Die Existenz einer Skriptsprache, uber die Transaktionen angesteuert werden können.

### 2.1.1 Transaktionen in einem Blockchain-System

Dass Transaktionen durch die Blockchain ohne eine zentrale Authorität vollzogen werden können, beruht auf zwei Grundlagen der Kryptographie: Public-/Private-Key-Kryptographie, sowie kryptografischen Hashes.

In Blockchain-Systemen wird der Austausch digitaler Wertgegenstände, wie z.B. Bitcoin-Einheiten ermöglicht, die an einen privaten Schluessel eines Teilnehmers gebunden sind. Dieser kann eine Transaktion von ihm an eine beliebige andere Partei innerhalb des Netzwerkes durch das Signieren einer Nachricht durch diesen Schluessel autorisieren. Ueber den dazugehörigen öffentlichen Schluessel, kann der Ursprung und die Autorisierung der Transaktion verifiziert werden.

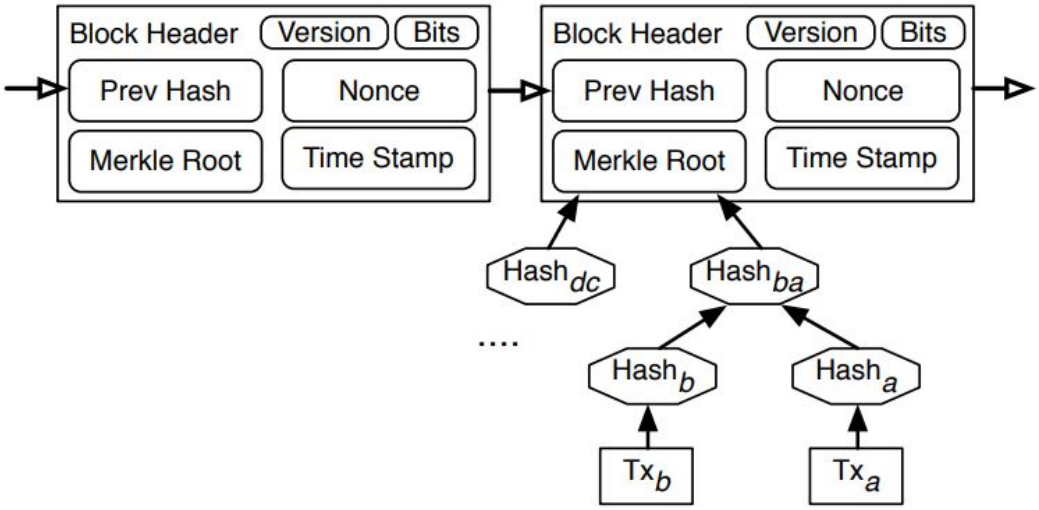


Abbildung 2.1: Bitcoin-Blockchain ( Gjermundrød u. a. (2016); Seite 1)

In Abbildung 1.1 ist beispielhaft der Aufbau eines einzelnen Blocks innerhalb der Bitcoin-Blockchain nach Nakamoto (2009) dargestellt. Jeder Block besitzt einen Hash-Wert, der aus dem Hash des letzten validen Blocks, einem Zeitstempel, den Hashes aller Transaktionen des Blocks sowie einem zu errechnenden, variablen Nonce-Wert errechnet wird. Eine Menge an Transaktionen, die ueber Broadcasts von den entsprechenden Teilnehmern innerhalb des

Netzwerks bekannt gemacht werden, werden von einem Mining-Knoten gesammelt und anschließend einer Hash-Funktion uebergeben. Ueber einen sog. Merkle-Tree wird ein Root-Hash aller Transaktions-Hashes gebildet (hier *Merkle Root*). Ein Block gilt dann als valide, wenn sein Nonce-Wert so gewählt ist, dass der resultierende Hash-Wert des Blocks ein durch das Netzwerk bestimmtes Kriterium erfuellt. Auf diese Art von Teilnehmern gelöste Blöcke koennen ueber das Netzwerk anderen Knoten bekannt gemacht und von diesen verifiziert werden. Akzeptieren mehr als die Hälfte aller Teilnehmer einen Block, gilt dieser als *Konsens* und ist nun das letzte Element der Blockchain, um den nächsten Block seinen Hash als Seed zur Verfuegung zu stellen. Derjenige Knoten, der einen gueltigen Block als erster bekanntmacht, kann einen Anspruch auf die Transaktionsgebuehren erheben, die durch die Teilnehmer jeder Transaktion vorher festgelegt wurden.

Durch die Möglichkeit, dass jeder Knoten des Netzwerkes einen Block auf das gemeinsame Gueltigkeitskriterium hin ueberpruefen kann, wird ein vertrauensloser Prozess geschaffen, der keine zentrale Verifikationsstelle benötigt.

An dieser Stelle sei bereits darauf hingewiesen, dass das ressourcenintensive Errechnen eines validen Block-Hashes insofern einen Nachteil darstellt, als das ressourcenarme Rechenknoten langfristig keinen signifikanten Anteil an Blöcken verifizieren können und deshalb anfallende Kosten durch die Verifikation anderer Knoten nicht durch die Beanspruchung von Transaktionsgebuehren decken können. Sie sind aber notwendig, um die Unabhängigkeit des Netzwerks von wenigen Knoten zu gewährleisten, die ueberdurchschnittlich viel Rechenleistung besitzen.

### 2.1.2 Ausprägungen von Blockchain-Systemen

Vukolić (2017) unterscheidet zwischen zwei Arten von Blockchain-Systemen: Den verbreiteten öffentlichen Blockchains (**permissionless**), in denen jedem Teilnehmer der Zugriff auf sowie das Erzeugen neuer Daten gestattet ist und privaten, genehmigungsbasierten Blockchains (**permissioned**), in denen Lese- und Schreibzugriffe auf die Blockchain durch eine Gruppe autorisiert werden muss.

Solche privaten Blockchains muessen nicht zwingend die Gueltigkeit von Transaktionen durch rechenaufwendige Verfahren pruefen: Da durch die Natur eines privaten, geschlossenen Systems jeder Teilnehmer innerhalb des Netzwerkes auf die Autorisierung durch andere Parteien angewiesen ist, laufen Angreifer Gefahr, dauerhaft vom Netzwerk ausgeschlossen zu werden. Neben der Ausfallsicherheit und Datenintegrität durch den Peer-to-Peer-Ansatz

existiert also noch eine Zugangskontrolle, die diese Form der Blockchain, fuer die Industrie interessant macht

In öffentlichen Blockchains muessen sich Parteien nicht identifizieren, um teilnehmen zu können. Das Vertrauen in das System wird dadurch gebildet, dass jeder Teilnehmer eigene Rechenleistung zur Validierung und Erweiterung der Blockchain bereitstellt. Die Kosten dieser Rechenleistung sind ein Anreiz fuer jeden, die Integrität der Blockchain aufrechtzuerhalten.

## 2.2 Anwendungsgebiete von Blockchain-Technologie

Auch wenn heutzutage noch keine Einfuehrung von Blockchain-Applikationen im großen Maßstab stattgefunden hat, wird die Technologie derzeit hinsichtlich ihrer Tauglichkeit vorwiegend fuer folgende Sektoren erforscht:

- **Kryptowährungen** - Wie bereits in Abschnitt 2.1 erläutert, kann die Blockchain als Fundament einer digitalen, dezentralisierten Währung dienen.
- **Finanzbranche** - Bedingt durch das Bitcoin-Projekt hat die Technologie vor allem in Finanz-Unternehmen und -Institutionen Anklang gefunden. Die Chance besteht ind iesem Fall darin, Finanzintermediäre zu ueberfluessig zu machen und Transaktionsgeschwindigkeiten zu steigern.
- **Öffentlicher Sektor** - Moura und Gomes (2017) postulieren den Einsatz von Blockchain-Technologie zur Sicherung und Digitalisierung von Wahlen. Bentov u. a. (2014) sehen einem Vorteil darin, dass durch die Public-Key-Kryptographie ein Identitäts-Diebstahl deutlich erschwert wird. Dieser Ansatz ist aber im Vergleich zur Anwendung von Blockchain in Industrie- und Finanzsektoren noch weitgehend unerforscht.

## 2.3 Hindernisse und Ausblick

Neben immer neuen Blockchain-Startups nimmt sich auch die Forscher-Gemeinde mehr und mehr dem Thema und vor allem ihren Limitierungen an. Aktuelle Forschungsthemen sind u.a. Alternativen zum ressourcenintensiven Proof-of-Work-Validierungsansatz ((Gjermundrød u. a., 2016)), die Deanonymisierung von Nutzern ueber ihre öffentlichen Schluessel und der Schutz vor dieser (Biryukov u. a., 2014) oder die Ermöglichung von Interoperabilität von Blockchains mit anderer Software.

# 3 Smart Contracts

Als Smart Contracts wird im allgemeinen Software bezeichnet, deren Code auf der Blockchain gespeichert und deren korrekte Ausfuehrung durch den Konsens des Netzwerks garantiert wird (vgl. Luu u. a. (2016)). Der Begriff Smart Contract und dessen Definition wurde bereits 1997 von Nick Szabo geprägt [1]. Der Code repräsentiert dabei eine Menge von Regeln und unter welchen Bedingungen diese angewendet werden. Beispielweise können automatische Verrechnungen, sowie Ein- und Auszahlungen auf ein Treuhandkonto durch einen Smart Contract repräsentiert werden. Der Netzwerk-Konsens gibt allen Beteiligten, die als Teilnehmer alle den Code des Contracts einsehen können, die Garantie, dass die definierten Regeln zuverlässig und ohne Zutun einer dritten Partei forciert werden.

Ein Smart Contract besitzt eine eigene Adresse, einen öffentlich bekannten kryptografischen Schluessel. Wird eine Transaktion an die Adresse eines Smart Contracts gesendet, wird der darin definierte Code von allen Mining-Knoten des Netzwerks ausgefuehrt. Durch den Austausch der Knoten untereinander, wird ein Konsens ueber die Ausgabe des Smart Contracts ermittelt Ein Beispiel fuer eine solche Blockchain ist Ethereum[2] auf der ueber die Skriptsprache **Solidity** Smart Contracts geschrieben und im Netzwerk veröffentlicht werden können. Ethereum ermöglicht *stateful* Smart Contracts, also Code, der Werte auf der Blockchain persistieren kann. Miner-Knoten, die diesen Code ausfuehren erhalten im Ethereum Netzwerk eine Transaktionsgebuehr, um den Rechenaufwand der mit dem Smart Contract verbunden ist, zu entschädigen.

[1] Szabo (1997)
[2] Ethereum-Foundation (2014)

# 4 Smart Contracts - Forschung und Entwicklung

## 4.1 Anwendungsfälle

Smart Contracts haben durch ihre Fähigkeit, ihre Regeln selbst zu forcieren die Disposition als dezentrale autonome Organisation zu fungieren (Omohundro, 2014). Der Grundgedanke sieht vor, in einem Unternehmen bestehende Verträge mit Kunden und Dienstleistern (z.B. Ein- und Verkauf) ueber Smart Contracts ablaufen zu lassen. Dies bietet sich vor allem fuer digitale Gueter wie Rechen-Ressourcen oder Speicherplatz an, die ueber einen Smart Contract ge- und verkauft werden können. Fuer den Anbieter wird dadurch die Notwendigkeit eliminiert eine eigene Infrastruktur fuer den Verkauf seiner Gueter bereitzustellen und zu warten.

Ein anderes häufig genanntes Anwendungsgebiet fuer Smart Contracts ist die Versicherungsbranche, in der Ansprueche und evtl. eine daraus resultierende Zahlung manuell geprueft und autorisiert werden muessen. Smart Contracts könnten, in diesen Prozess integriert, diesen teil-automatisieren: Zahlungen könnten unter bestimmten Bedingungen, die der Contract prueft, ohne Verzögerung autorisiert werden.

### 4.1.1 Smart Contracts und das IoT

Das *Internet of Things* verspricht unsere Welt in einem noch größerem Maße zu vernetzen als es Smartphones bereits getan haben. Smart Contracts könnten Daten des IoT nutzen, um beispielsweise den Standort von Guetern nachzuverfolgen und zu archivieren und automatisch auf bestimmte Ereignisse reagieren, sofern sie im Code vorher definiert wurden.

## 4.2 Sicherheit

Ethereum-Smart Contracts können selbst einen Betrag an digitaler Währung besitzen. Das macht sie fuer Angreifer attraktiv, denn sobald eine Transaktion auf der Blockchain durchgefuehrt wurde, ist sie nicht mehr umkehrbar. In öffentlichen Blockchains sind Teilnehmer

ausschließlich ueber ihre oeffentlichen Schluessen bekannt, wodurch Angreifer nach fehlgeschlagenen und erfolgreichen Angriffen immer noch einen gewissen Grad an Anonymität geniessen.

Luu u. a. (2016) identifizieren mehrere Schwachstellen in Smart Contracts auf der Ethereum-Plattform. Die am häufigsten vertretene Sicherheitsluecke bestehet darin, dass Transaktionen ihrer Transaktionengebuehr entsprechend von Miner-Knoten priorisiert werden können und deshalb der Zustand der Blockchain zum Zeitpunkt des Ausfuehrens eines Smart Contracts nicht vorhersehbar ist. Weiterhin wird dargelegt, dass viele Angriffszenarien durch die Konzipierung durch die Smart Contracts durch die Entwickler selbst, nicht aber durch die Blockchain selbst möglich werden und dass bisher keine Werkzeuge existieren, die Entwicklern bei der Vermeidung dieser Sicherheitsluecken unterstuetzt.

Weiterhin Porru u. a. (2017) argumentieren fuer die Notwendigkeit von Mitteln, mit denen Regeln eines Smart Contracts hinsichtlich ihrer Einhaltung von nationalen Gesetzen ueberprueft werden können, um eine großflächige Einfuehrung durch die breite Masse von Konsumenten und Industrie zu ermöglichen.

## 4.3 Limitierungen

Durch die Abhängigkeit von Smart Contracts von der Blockchain-Technologie, können sich die Limitierungen der einen Technologie auf die andere fortpflanzen: Während andere Datenstruktur mit vertretbaren Aufwand modifiziert werden können, sind Smart Contracts und Blockchain-Transaktionen nach ihrer Verifizierung durch ausreichend Teilnehmern Unumkehrbar. Gesetz dem Falle, dass Unternehmen Smart Contracts in ihre Prozesse integrieren, muessen diese aber wartbar sein, um an neue Gesetze oder wirtschaftliche Bedingungen angepasst werden zu können. Bisher besteht lediglich die Möglichkeit, einen völlig neuen Smart Contract einzusetzen, was auf alle Teilnehmer bezogen, die Größe der Blockchain unnötig anschwellen lässt. Die Forschung in diesem Bereich hat in diesem Gebiet den Schwerpunkt Möglichkeiten zu finden, wie die Code af der Blockchain modifizierbar gemacht werden kann, ohne dabei die Transparenz- und Dezentralitäts-Garantien der Blockchain zu verletzen. Bisher sind tiefgehende Modifikationen an der Software einer Blockchain oder Smart Contracts nur durch einen Fork des gesamten Systems möglich, der von ausreichend Teilnehmern der urspruenglichen version auch angenommen werden muss (In privaten Blockchains ist dies weitaus weniger ein Problem als bei öffentlichen).

In Abschnitt 4.2 wurde die Anfälligkeit von Smart Contracts durch Angriffe erwähnt, die durch menschliches Versagen der Entwickler erst möglich gemacht werden. Waehrend die Blockchain bereits Garantien ueber ihre Funktionsweise geben kann, so kann bei steigender Komplexität von Smart Contracts keine Garantie fuer einen Teilnehmer gegeben werden, wie sich dieser zur Laufzeit verhalten wird.

Neben den technsichen Herausforderungen ist auch die rechtliche Gueltigkeit und Durchsetzbarkeit von Smart Contracts noch nicht vollständig geklärt. DIes soll hier aber nur am Rande erwähnt und nicht weiter ausgefuehrt werden.

# 5 Fazit

Die Themen Blockchain und Smart Contracts erfreuen sich derzeit einer regelrechten Euphorie. Doch eine genauere Recherche hat gezeigt, dass auch diese Technologie wohl keine rasche und problemlose Revolution unserer Gesellschaft hervorbringen wird. Ihr Potenzial ist abzusehen, doch noch von den dargestellten Herasforderungen eingeschraenkt.

Mein gewähltes Thema ging meiner Meinung nach nicht in die Tiefe, aber es war eine umfassende Recherche notwendig, da hier viele einzelne kleinere Themen ineinandergreifen und ich mir diese zunächst klar machen musste. Im Nachhinein habe ich das Gefuhl mich gut in den meisten der erwähnten Themen zurechtzufinden, aber noch kein "Experten-Verständnis" meines eigentlichen Wunsch-Themas zu besitzen.

Persönlich möchte ich dieses Thema weiterverfolgen, da ich es sehr spannend finde, ob Blockchain wirklich großflächig angenommen wird oder doch nur in einem ueberschaubaren Bereich Anwendung finden wird.

# Literaturverzeichnis


[Bentov u. a. 2014] Bentov, Iddo ; Lee, Charles ; Mizrahi, Alex ; Rosenfeld, Meni: Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]Y. In: *SIGMETRICS Perform. Eval. Rev.* 42 (2014), Dezember, Nr. 3, S. 34–37. – URL http://doi.acm.org/10.1145/2695533.2695545. – ISSN 0163-5999

[Biryukov u. a. 2014] Biryukov, Alex ; Khovratovich, Dmitry ; Pustogarov, Ivan: Deanonymisation of Clients in Bitcoin P2P Network. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA : ACM, 2014 (CCS '14), S. 15–29. – URL http://doi.acm.org/10.1145/2660267.2660379. – ISBN 978-1-4503-2957-6

[Ethereum-Foundation 2014] Ethereum-Foundation: Ethereum white paper. (2014). – URL https://github.com/ethereum/wiki/wiki/White-Paper

[Gjermundrød u. a. 2016] Gjermundrød, Harald ; Chalkias, Konstantinos ; Dionysiou, Ioanna: Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems. In: *Proceedings of the 20th Pan-Hellenic Conference on Informatics*. New York, NY, USA : ACM, 2016 (PCI '16), S. 35:1–35:4. – URL http://doi.acm.org/10.1145/3003733.3003773. – ISBN 978-1-4503-4789-1

[Luu u. a. 2016] Luu, Loi ; Chu, Duc-Hiep ; Olickel, Hrishi ; Saxena, Prateek ; Hobor, Aquinas: Making Smart Contracts Smarter. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA : ACM, 2016 (CCS '16), S. 254–269. – URL http://doi.acm.org/10.1145/2976749.2978309. – ISBN 978-1-4503-4139-4

[Moura und Gomes 2017] Moura, Teogenes ; Gomes, Alexandre: Blockchain Voting and Its Effects on Election Transparency and Voter Confidence. In: *Proceedings of the 18th Annual International Conference on Digital Government Research*. New York, NY, USA : ACM, 2017 (dg.o '17), S. 574–575. – URL http://doi.acm.org/10.1145/3085228.3085263. – ISBN 978-1-4503-5317-5

[Nakamoto 2009] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. (2009), Mai. – URL http://www.bitcoin.org/bitcoin.pdf

[Omohundro 2014] Omohundro, Steve: Cryptocurrencies, Smart Contracts, and Artificial Intelligence. In: *AI Matters* 1 (2014), Dezember, Nr. 2, S. 19–21. – URL http://doi.acm.org/10.1145/2685328.2685334. – ISSN 2372-3483

[Porru u. a. 2017] Porru, Simone ; Pinna, Andrea ; Marchesi, Michele ; Tonelli, Roberto: Blockchain-oriented Software Engineering: Challenges and New Directions. In: *Proceedings of the 39th International Conference on Software Engineering Companion*. Piscataway, NJ, USA : IEEE Press, 2017 (ICSE-C '17), S. 169–171. – URL https://doi.org/10.1109/ICSE-C.2017.142. – ISBN 978-1-5386-1589-8

[Szabo 1997] Szabo, Nick: The idea of smart contracts. (1997). – URL http://szabo.best.vwh.net/smart

[Vukolić 2017] Vukolić, Marko: Rethinking Permissioned Blockchains. In: *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. New York, NY, USA : ACM, 2017 (BCC '17), S. 3–7. – URL http://doi.acm.org/10.1145/3055518.3055526. – ISBN 978-1-4503-4974-1