

# LÖSUNG BLOCKCHAIN-BASIERTER KONFLIKTE

Jörn Erbguth

PhD Candidate – Information Systems, Centre Universitaire d'Informatique, Université de Genève  
Battelle bâtiment A, 7 route de Drize, 1227 Carouge, CH  
Jorn.Erbguth@unige.ch; <https://erbguth.ch/>

**Schlagworte:** *Blockchain, Smart Contracts, Dispute Resolution*

**Abstract:** *Die Unveränderlichkeit der Einträge auf einer Blockchain ist eines ihrer wesentlichen Merkmale und Grund für das in sie gelegte Vertrauen. Falls in Ausnahmefällen trotzdem Änderungen erforderlich sein sollten, sind die faktischen Möglichkeiten dies juristisch durchzusetzen sehr beschränkt. Die Alternative – ein Fork auf freiwilliger Basis – ist jedoch ein wenig transparenter Prozess, der grosse Unsicherheiten mit sich bringt. In diesem Beitrag wird ein Lösungsansatz beschrieben, um Änderungen der Einträge auf einer Blockchain auf transparente und rechtstaatliche Weise zu ermöglichen und sie gleichzeitig auf den Ausnahmefall zu beschränken.*

## 1. Einleitung

Eine Blockchain ist gegen unberechtigte Änderungen technisch geschützt. Dieser Schutz verhindert auch dann Änderungen, wenn sie zur Fehlerbehebung erforderlich sein sollten oder ein Gericht eine Änderung anordnen sollte.

## 2. «Unveränderbare» Blockchain

Daten auf der Blockchain gelten als unveränderbar. Diese Unveränderbarkeit basiert auf dem Design der Blockchain<sup>1</sup>:

- Blöcke werden immer nur hinzugefügt aber nie gelöscht. Dadurch lassen sich alte Informationen immer wieder rekonstruieren.
- Die Blöcke werden über eine Hashkette miteinander verbunden. Jeder Block enthält dazu einen Hashcode – quasi ein digitaler Fingerabdruck – des vorherigen Blocks. Dadurch müssten bei einer Manipulation eines Blockes nicht nur der zu manipulierende Block sondern alle Folgeblöcke neu berechnet werden.
- Die meisten Blockchains sind so programmiert, dass für die Berechnung eines Blockes ein großer Rechenaufwand erforderlich ist. Durch diesen «proof of work» wird sichergestellt, dass eine Blockchain nicht einfach unter Weglassen einzelner Transaktionen neu berechnet werden kann. Der «proof of work» besteht dabei darin, für jeden Block eine Lösung zu einem mathematischen Problem zu finden, welches nur durch aufwendiges Ausprobieren einer sehr grossen Anzahl von Zahlenkombinationen lösbar ist. Wer zuerst eine Lösung für einen Block findet, erhält dafür eine vorher festgesetzte Belohnung in der Währung der jeweiligen Blockchain. Diese Belohnung ist neues Geld der Blockchain, welches vorher noch nicht existiert hat. Daher wird dieser Prozess in Anlehnung an das Schürfen von Gold auch «mining» genannt. Wenn man selbst nicht mehr Rechenleistung als alle anderen Mineure einer Blockchain zusammen hat, kann man diese nicht mit seiner modifizierten Version «einholen». Da der Blockchain-Algorithmus immer die längere Version der Blockchain vorzieht, wird eine mit weniger Rechenleistung erstellte kürzere Blockchain verworfen. Dieser «proof of work» wirkt wie eine Abstimmung über den Fortgang einer Blockchain. Die Stimmen sind dabei nach Rechenleistung gewichtet, so

---

<sup>1</sup> NAKAMOTO, Bitcoin: A Peer-to-Peer Electronic Cash System, wobei Satoshi Nakamoto ein Pseudonym ist.

dass niemand durch die Aufteilung seiner Rechner in viele virtuelle Knoten ein Vielfaches an Stimmkraft erlangen kann.

- Der Inhalt der Transaktionen unterliegt bestimmten Regeln. Diese sind bei Bitcoin hart codiert und regeln z.B., dass nur der Kontoinhaber seine Bitcoins transferieren kann und dass nicht mehr Bitcoins auf ein Konto transferiert werden können, als vom eigenen Konto abgebucht werden. Bei allgemeinen Blockchains können diese Regeln – dann «Smart Contracts» genannt – anwendungsspezifisch flexibel festgelegt werden. In wie weit ein «Smart Contract» änderbar ist, ist im «Smart Contract» selbst festgelegt.<sup>2</sup>

Da sowohl der Code einer Blockchain als auch die «Smart Contracts» frei lesbar sind, kann über einen Blick in den Programmcode direkt nachvollzogen werden, ob und ggf. wie ein «Smart Contract» geändert oder umgangen werden kann. Damit sind «Smart Contracts» gut für virtuelle Währungen, Register oder die Sicherung von Beweisen geeignet.

Die Schutzmechanismen, die dafür sorgen, dass unbefugte Änderungen unterbleiben, sorgen jedoch auch dafür, dass problematische Einträge nicht einfach korrigiert werden können. Ursachen für problematische Einträge gibt es viele. Bugs im Regelwerk der «Smart Contracts» können z.B. gewollte Änderungen verhindern oder unerwünschte Änderungen ermöglichen. Der wohl bekannteste Bug eines «Smart Contracts» ist dabei der Bug des Venture Capital Funds «The DAO», der – nicht korrigiert – einen Abfluss im Wert von 50 Millionen Dollar bedeutet hätte.<sup>3</sup> «Smart Contracts» können auch zur Koordination krimineller Tätigkeiten verwendet werden. Transaktionen können durch Täuschung oder Diebstahl der Schlüssel unbefugt zustande gekommen sein. «Smart Contracts» können kriminelle Aktivitäten ausschreiben und z.B. eine Summe unter der Bedingung auszahlen, dass der Nachweis der Ermordung einer Person geführt wird.<sup>4</sup>

### 3. Änderung der Inhalte einer Blockchain

Soll der Inhalt einer Blockchain verändert werden, so ist grundsätzlich zu unterscheiden, ob diese Veränderung nach den Regeln der Blockchain durchführbar ist. Gibt es jemanden, der mit seinem Schlüssel den Inhalt nach den Regeln der Blockchain wie gewünscht verändern kann? Im konkreten Fall könnte das z.B. die Übertragung von Bitcoins sein. Falls diese Person bekannt und greifbar ist, kann gegen diese Person vorgegangen werden, damit diese die gewünschte Transaktion durchführt. Falls der «Smart Contract» jedoch keine entsprechende Änderung vorsieht oder die entsprechend berechnete Person nicht bekannt ist oder ihren Schlüssel verloren hat, so ist die Transaktion nach den Regeln der Blockchain nicht möglich und es bleibt nur die mit großen Hürden versehene Alternative, auf allen Knoten eine neue Softwareversion einzuspielen, die die gewünschten Änderungen zulässt.

#### 3.1. Durchsetzung des Anspruchs zur Vornahme einer Blockchain-Transaktion

Bei der Frage der Durchsetzung des Anspruchs der Vornahme einer nach den Regeln der Blockchain möglichen Blockchain-Transaktion ist zu unterscheiden, welcher Natur der Eintrag auf der Blockchain ist. Exemplarisch möchte ich hier den Fall der Übertragung von Bitcoins und den Fall der Übertragung von Anteilen an einer DAO betrachten:

Bitcoin oder Anteile an einer DAO sind keine körperlichen Sachen i.S.v. § 90 BGB. Zu prüfen ist, ob Bitcoins oder Anteile an einer DAO Wertpapiere von §§ 793 ff. BGB darstellen. Dazu müssten sie ein Recht in verbrieft Form enthalten. Bei Bitcoins ist bereits fraglich, ob diese ein «Recht» enthalten. Bitcoins geben einem ausser der tatsächlichen Verfügungsgewalt über die Bitcoins keine Forderung oder sonstiges Recht gegenüber

---

<sup>2</sup> GORD, Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality.

<sup>3</sup> GREENSPAN, Smart contracts and the DAO implosion.

<sup>4</sup> SIMONITE, Bitcoin's Dark Side Could Get Darker.

Dritten. Ein Anteil an einer DAO gibt dagegen das Recht abzustimmen und einen Gewinnanteil zu beziehen. Auch ist es wohl Intention der Parteien, dass sich die Erfüllung dieses Rechts direkt aus dem Register dieser Anteile auf der Blockchain ergibt. §§ 793 ff. BGB fordert jedoch die Schriftform von Wertpapieren<sup>5</sup>, die nach herrschender Lehre ohne gesetzliche Regelung nicht ersetzlich sei.<sup>6</sup> Der BGH sieht zwar die physische Übergabe des Wertpapiers nicht mehr als Voraussetzung für die Übertragung eines Wertpapiers nach §§ 398 oder 793 ff. BGB an.<sup>7</sup> Er hält jedoch daran fest, dass es für das Bestehen des Wertpapiers die Verkörperung in einer Einzel- oder Sammelurkunde geben und diese auch bei der Zwangsvollstreckung vorgelegt werden müsse.<sup>8</sup> Bleibt zu prüfen, ob der Eintrag auf einer Blockchain nicht der Schriftform gleichzusetzen ist. § 126a BGB setzt die qualifizierte elektronische Signatur der Schriftform gleich. Daher ist zunächst zu prüfen, ob von beiden Parteien bestätigte Einträge auf einer Blockchain als qualifizierte elektronische Signaturen zu betrachten sind. Die Einträge werden von den Parteien mit dem Verfahren der Public Key Encryption signiert. Die Blockchain kennt jedoch weder gültige Zertifikate noch sichere Signaturerstellungseinheiten, die für die qualifizierte elektronische Signatur erforderlich sind.<sup>9</sup> Die Blockchain weist gegenüber der qualifizierten elektronischen Signatur zwar einige sicherheitstechnische Vorteile auf. So ist z.B. die zeitliche Geltungsdauer eines Eintrags auf der Blockchain technisch nicht befristet. Einer analogen Anwendung des § 126a BGB steht jedoch auf jeden Fall die fehlende Identifizierung der Parteien im Weg. Im Ergebnis ist also trotz der faktisch größeren Sicherheit die Verwaltung von Inhaberschuldverschreibungen auf einer Blockchain rechtlich der Schriftform nicht gleichzusetzen. Ein Anspruch auf Übertragung nach § 884 2. Alt. i.V.m. 883 Abs. 1 ZPO ist daher nicht gegeben. Ein Übertragungsanspruch für Bitcoins<sup>10</sup> oder Anteilen an einer DAO kommt daher nur nach §§ 887 f. ZPO in Frage. Soweit der Anspruchsgegner die Möglichkeit hat, entweder mit seinem privaten Schlüssel die Blockchain entsprechend zu modifizieren oder den privaten Schlüssel herauszugeben, ist daher die Durchsetzung eines entsprechenden Anspruchs denkbar.

### 3.2. Anspruch auf Änderung der Blockchain außerhalb der Regeln eines «Smart Contracts» gegen einen einzelnen Schuldner

Geht ein Schlüssel verloren, hat ein unbekannter Dritte eine Transaktion durch Täuschung erschlichen oder hat ein «Smart Contract» einen Bug, so sehen die «Smart Contracts» in der Regel keine Möglichkeit vor, die Informationen auf der Blockchain zu berichtigen.

Es gibt daher keine einzelne Person, die die Blockchain entsprechend ändern könnte oder die einen für eine solche Änderung benötigten Schlüssel herausgeben könnte. Selbst wenn ein Schuldner zu einer solchen Änderung verpflichtet wäre, ist für ihn diese Änderung nicht möglich.

Daher wird man zunächst versuchen, andere Ansprüche geltend zu machen wie z.B. Ansprüche aus ungerechtfertigter Bereicherung, auf Schadensersatz oder auf Unterlassen der Nutzung der über die Blockchain erhaltenen faktischen Verfügungsmöglichkeiten.

### 3.3. Haftung der Teilhaber einer DAO für die DAO

Eine DAO ist eine gesetzlich nicht geregelte Gesellschaftsform. Das Gesetz gibt jedoch einen Numerus Clausus an Gesellschaftsformen vor. Die Gesellschaft bürgerlichen Rechts übernimmt dabei die Auffangfunktion eines elastischen Grundmodells.<sup>11</sup> Bei einer Gesellschaft des bürgerlichen Rechts haften die Inhaber gesamt-

<sup>5</sup> VOGEL, beck-online.Grosskommentar, § 793 BGB Rn 87.

<sup>6</sup> EINSELE, Wertpapiere im elektronischen Bankgeschäft, S. 9.

<sup>7</sup> BGH, Urteil vom 14. Mai 2013, XI ZR 160/12, ZIP 2013, S. 1270–1274, S. 1272 Rn. 18.

<sup>8</sup> BGH, Beschluss vom 7. April 2016, VII ZB 14/15, ZIP 2016, S. 891 f., S. 892 Rn. 13.

<sup>9</sup> NOAK/KREMER, Bürgerliches Gesetzbuch: Allgemeiner Teil – EGBGB, § 126a BGB Rn 19.

<sup>10</sup> KÜTÜK/SORGE, Bitcoin im deutschen Vollstreckungsrecht – Von der «Tulpenmanie» zur «Bitcoinmanie», S. 644.

<sup>11</sup> SCHÖNE, Beck'scher Online Kommentar BGB, § 705 BGB Rn. 4.

schuldnerisch entsprechend § 31 BGB für Verbindlichkeiten der Gesellschaft.<sup>12</sup> Eine unbeschränkte gesamtschuldnerische Haftung der Teilhaber erscheint jedoch im Vergleich mit Aktiengesellschaften als unbillig.

### **3.4. Anspruch auf Änderung der Blockchain gegen die Betreiber (Mineure) der Blockchain (Fork)**

Die Regeln der Änderung einer Blockchain sind im Code der Blockchain selbst bzw. in den «Smart Contracts» festgelegt. Sehen diese nicht vor, dass der Inhalt der Blockchain geändert werden kann, so verweigern die Programme die Übernahme der Änderung. Der Code der Blockchain ist jedoch auch nur Programmcode und könnte daher so modifiziert werden, dass eine gewünschte Änderung möglich wird.

Diese Änderung würde jedoch nur von denjenigen Knoten der Blockchain akzeptiert, die entsprechend modifiziert sind. Daher muss diese Modifikation des Programmcodes auf allen Knoten eingespielt werden. Wenn eine solche Änderung nicht auf allen Knoten durchgeführt wird, teilt sich die Blockchain, da die modifizierten und nicht modifizierten Knoten nicht mehr miteinander kompatibel sind. Eine solche Konstellation wird daher auch «Fork» genannt.

Der Gläubiger könnte eine entsprechende modifizierte Softwareversion bereitstellen und bei den Mineuren der Blockchain die Übernahme dieser Version durchsetzen.

Zunächst hat der Gläubiger jedoch nur einen Anspruch gegen seinen Schuldner. Je nach Art seines Anspruches könnte er die Betreiber der Blockchain jedoch z.B. als Störer oder als Bereicherte adressieren. Allerdings trifft dieser Anspruch auf faktische Barrieren. Die meisten Betreiber einer Blockchain arbeiten anonym und befinden sich darüber hinaus noch im Ausland. Die Durchsetzung der Ansprüche nur gegen einzelne, dem Gläubiger bekannte, lokal ansässige Betreiber der Blockchain führt jedoch nicht dazu, dass die Blockchain insgesamt geändert wird. Vielmehr werden lediglich deren Blockchain-Knoten ungültig. Wenn aber der gewünschte Erfolg nicht eintritt jedoch der Adressat durch diese Forderung einen Schaden erleidet, könnte die Durchsetzung eines solchen Anspruchs rechtsmissbräuchlich oder unverhältnismäßig sein.

## **4. Fork einer Blockchain als schwer kontrollierbarer Prozess**

Da die Übernahme eines Softwareupdates für alle Betreiber einer Blockchain nicht einfach durchgesetzt werden kann, ist der Ausgang des Updateprozesses schwer vorhersehbar. Die Einigung auf die Übernahme oder Ablehnung eines solchen Updates wird vor allem dadurch motiviert, sich dem Vorgehen der Mehrheit anzuschließen, um nicht von der Blockchain ausgeschlossen zu sein. Damit bietet diese, auf die Knotenbetreiber verteilte Entscheidung, einen gewissen Schutz vor Missbrauch. Diese technisch organisierte «Abstimmung» ist jedoch allenfalls rudimentär demokratisch. Es ist weder ersichtlich, warum nur die Knotenbetreiber abstimmen dürfen, noch warum die Abstimmung nach Rechenleistung gewichtet werden soll. Ein Fork verunsichert zum einen die Nutzer der Blockchain, da diese nicht mehr auf die Unveränderbarkeit der Blockchain vertrauen können. Gleichzeitig erzeugt er auch Ungewissheit, da in der Übergangsphase nicht sicher ist, ob sich die neue Softwareversion durchsetzen wird, das Update abgelehnt wird oder beide Blockchains nebeneinander existieren werden. Es ist daher wünschenswert, den Fork durch einen besser kontrollierbaren Ausnahmeprozess zu ersetzen.

## **5. Regelung der Änderung im Ausnahmefall**

Eine Motivation für die Blockchain Technologie war der Wunsch, sich von staatlichen Institutionen unabhängig zu machen – Institutionen, die das in sie gesetzte Vertrauen durch Machtmissbrauch, Korruption oder politische Willkür enttäuscht haben. Smart Contracts sollen ein Gegenentwurf zu diesen Institutionen sein. Sie sind transparent und entweder unveränderbar oder nur über ebenso transparente Mechanismen änderbar. Die Konfliktlösung über Blockchain-Forks führt diese Prinzipien allerdings ad absurdum.

---

<sup>12</sup> BGH, Urteil vom 24. Februar 2003, II ZR 385/99, NJW 2003, S. 1445–1447.

Ein solcher Änderungsmechanismus muss daher transparent und auf echte Ausnahmefälle beschränkt sein. Die Feststellung des Ausnahmefalls darf nicht anonymen Blockchainbetreibern mit ggf. kollidierenden Eigeninteressen überlassen werden. Sie muss vielmehr in einer rechtstaatlichen und demokratischen Form erfolgen.

Die Gerichte eines demokratischen Rechtsstaats wären prinzipiell geeignete Foren zur Entscheidung darüber, ob eine Ausnahmesituation vorliegt, die eine an sich nicht zulässige Änderung der Blockchain erfordert. Doch in einer globalisierten Welt wäre das Vertrauen in die Blockchain dahin, wenn jedes Gericht jedes Staates über jede Blockchain urteilen könnte, nur, weil z.B. ein einzelner Knoten dieser Blockchain in diesem Land betrieben wird. Zudem tun sich Gerichte häufig mit neuer Technologie schwer, so dass das Vertrauen darin, dass Gerichte hier sachgerechte Entscheidungen treffen, begrenzt ist.

Während komplett unkontrollierbare «Smart Contracts» eine allgemeine Gefährdung darstellen können, sollte jeder Autor eines Smart Contracts nach dem Prinzip der Privatautonomie einen Einfluss haben, welcher Kontrollinstanz er sich unterwirft.

## **6. Vorschlag**

Eine Modifikationsmöglichkeit von Smart Contracts ist erforderlich, um kriminelle oder fehlerhafte «Smart Contracts» oder Transaktionen korrigieren zu können. Dabei sollten die Ebene des einzelnen «Smart Contracts» und die Ebene der Blockchain unterschieden werden.

### **6.1. Kontrolle von Smart Contracts**

Beim Anlegen eines Smart Contracts sollte es daher möglich sein, unter verschiedenen Kontrollinstanzen wählen zu können. Verschiedene ggf. auch auf der Blockchain abbildbare alternative Verfahren zur Konfliktlösung sollten vorgeschaltet werden können. Analog zu privatrechtlichen Vertragsautonomie sollte auch das anwendbare Recht und der Gerichtsstand gewählt werden können. Dabei sollten neben den nationalen Rechtssystemen auch private Regelwerke und Schiedsgerichte ausgewählt werden können, sofern diese ein Minimum an rechtstaatlichen Kriterien erfüllen. Um die Hürden für eine Änderung der Inhalte der Blockchain höher zu setzen, könnten für die Änderungen auch übereinstimmende Urteile mehrerer Gerichte oder Kontrollgremien gefordert werden. In der Praxis könnte dies dadurch realisiert werden, dass für diese Gerichte spezielle Autorisierungscodes generiert und hinterlegt werden.

### **6.2. Kontrolle von Blockchains**

Auf Blockchains laufen unterschiedliche «Smart Contracts», die ggf. unterschiedliche juristische Foren gewählt haben. Daher erscheint es sinnvoll, für die Kontrolle von Blockchains eine eigene internationale Instanz zu schaffen. Diese Kontrollinstanz kann dann angerufen werden, wenn ein Problem eine Vielzahl von «Smart Contracts» auf einer Blockchain betrifft oder bestimmte Mindeststandards bei einzelnen «Smart Contracts» nicht eingehalten oder durchgesetzt werden.

In dieser internationalen Kontrollinstanz könnten, ähnlich der UN, jedes Land vertreten sein. Technisch kann jedes Land über einen Abstimmungscode verfügen. Für Eingriffe können vorab bestimmte Quoren festgelegt, die dann technisch umgesetzt werden.

### **6.3. Schaffung speziellen Rechts für die Blockchain**

Die Schaffung passenden Rechts für die Blockchain kann ein wichtiger Standortvorteil sein. In der Schweiz hat sich ein «Cryptovalley» in der Region Zug gebildet, da dort die gesetzlichen Voraussetzungen günstig sind. Neben den nötigen nationalen und den internationalen Regelungen für die Kontrollinstanzen und deren Standards besteht auch für die auf einer Blockchain sitzenden DAOs gesellschaftsrechtlicher Regulierungsbedarf. Dieses neue Rechtsgebiet wird teilweise als Lex Cryptographia<sup>13</sup> bezeichnet.

<sup>13</sup> WRIGHT/FILIPPI, Decentralized Blockchain Technology and the Rise of Lex Cryptographia.

## 7. Conclusio

Die Regulierung und Kontrolle von «Smart Contracts» und DAOs ist erforderlich. Auf Grund der international verteilten Struktur von Blockchains sowie zur Vermeidung von Überregulierung ist eine international abgestimmte Regulierung sowie eine internationale Kontrollinstanz sinnvoll. Gleichzeitig sollte den «Smart Contracts» und DAOs ein möglichst grosses Mass an Privatautonomie belassen werden, das anzuwendende Recht und die gewählten Streitbeilegungsverfahren zu wählen, soweit damit die Einhaltung noch zu definierender Mindeststandards gewährleistet ist.

## 8. Literatur

EINSELE, DOROTHEE, Wertpapiere im elektronischen Bankgeschäft, WM 2001, S. 7–16, S. 9.

GORD, MICHAEL Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality, Bitcoin Magazine, 26. April 2016, <https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751>.

GREENSPAN, GIDEON, Smart contracts and the DAO implosion, MultiChain, 22. Juni 2016, <http://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/>.

KÜTÜK, MERIH ERDEM/SORGE, CHRISTOPH, Bitcoin im deutschen Vollstreckungsrecht – Von der «Tulpenmanie» zur «Bitcoinmanie», MMR 2014, S. 643–646, S. 644.

NAKAMOTO, SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>.

NOAK, ULRICH/KREMER, SASCHA, in: Heidel, Thomas/Hüßtege, Rainer/Mansel, Heinz-Peter/Noack, Ulrich (Hrsg.), Bürgerliches Gesetzbuch: Allgemeiner Teil – EGBGB, 3. Auflage 2016, § 126a BGB Rn 19.

SCHÖNE, TORSTEN, in: Bamberger, Georg/Roth, Herbert (Hrsg.), Beck'scher Online Kommentar BGB, 41. Edition, Stand 1. November 2016, § 705 BGB Rn. 4.

SIMONITE, TOM, Bitcoin's Dark Side Could Get Darker, MIT Technology Review, 13. August 2015, <https://www.technologyreview.com/s/540151/bitcoins-dark-side-could-get-darker/>.

VOGEL, HANS-GERT, in: Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Mayer, Jörg (Hrsg.), beck-online.Grosskommentar (im Aufbau), § 793 BGB Rn 87.

WRIGHT, AARON/FILIPPI, PRIMAVERA DE, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 10. März 2015, <http://ssrn.com/abstract=2580664>.