Schöpferische Zerstörer: Bitcoin, Blockchain und Smart Contracts – Digitale Treuhänder transformieren die Gesellschaft

Jörg Schäfer
OOP, Distr. Systems and DBs, Machine Learning
Frankfurt University of Applied Sciences
Fachbereich 2: Informatik und Ingenieurwissenschaften
Nibelungenplatz 1, Raum 1-217
D-60318 Frankfurt am Main
Tel.: +49(0)69-1533-3679
jschaefer@fb2.fra-uas.de
http://www.informatik.fb2.fh-frankfurt.de/~jschaefer/
PGP Fingerprint: E201 63B2 8B4A 1559 47EE 1C03 7F09 FD03 B18D 96F1

Evangelische Akademie Villigst, 15.10.2016

Zusammenfassung

Bitcoin, Blockchain und Smart Contracts sind digitale Technologien, die mit Hilfe von mathematisch kryptographischen Verfahren und genuin dezentraler Datenhaltung gesellschaftliche Funktionen, die Treuhänder wie z. B. Banken, Notare, Katasterämter und Behörden wahrnehmen, in Form von Algorithmen abbilden und damit die analogen Treuhänder potentiell überflüssig machen können. Die Technologien sind noch in der Anfangsphase, sind aber konzeptionell bereits weitgehend ausgereift und schon seit einigen Jahren im praktischen Einsatz. Während Bitcoin in der Öffentlichkeit als „digitales Geld“ bekannt ist, sind die dafür verwendeten Technologien Blockchain, sowie die damit verbundenen sogenannten “Smart Contracts“ nur Experten bekannt, obwohl diese viel interessanter und relevanter sind als Bitcoin selbst. Die Wirtschaft, insbesondere die Finanzindustrie ist aber von den Chancen und Risiken förmlich elektrisiert und so befinden sich zur Zeit viele Versuchsimplementierungen in Testphasen. Auch öffentliche Verwaltungen wie das Vereinigte Königreich oder die Regierung von Estland analysieren das Potential, das in den Technologien liegt. Unter Experten herrscht weitgehend Einigkeit darüber, das es sich um sogenannte „disruptive“ Technologien handelt, die weitreichende Auswirkungen auf die Geschäftsmodelle von Treuhändern haben werden und die unsere gesellschaftlich ausgehandelten Regeln verändern werden.
Weniger diskutiert wird die Frage, wer die neuen Regeln bestimmt. Werden es einige Netzmonopolisten (Google, Facebook, Amazon, Apple, Uber und co.) sein, die der Gesellschaft die Regeln diktieren und einen digitalen Feudalismus 2.0 begründen, werden es die Bürger (Netzteilnehmer) sein, die – nicht zuletzt wegen des inhärent dezentralen und potentiell (basis-) demokratischen Charakters – sich selbst Regeln definieren und ein digitales Utopia?! schaffen oder werden autoritäre Regime Smart Contracts benutzen, um die Totalüberwachung und Steuerung der Untertanen im Sinne einer digitalen Dystopie zu erreichen?
Antworten auf diese Fragen und viele andere kann es m.E. (noch) nicht geben, daher versucht der Workshop die relevanten Fragen zu stellen und mögliche Zukunfts- und Handlungsszenarien zu entwickeln. [1]

1 Die Technologie von Bitcoin, Blockchain und Smart Contracts

1.1 Bitcoin als Electronic Cash

Bitcoin wurde 2008 vom Autor Satoshi Nakamoto (Pseudonym, Identität bis heute unbekannt) in seinem White Paper [Nak]wie folgt charakterisiert:

> “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.“

Bitcoin verwendet die Blockchain Technologie, um eben dies zu verwirklichen. Um die Funktionsweise zu verstehen, vergegenwärtigt man sich am besten, wie eine herkömmliche Banküberweisung funktioniert. Bei einer Banküberweisung von Alice auf Bob spezifiziert

1 Der vorliegende Artikel stellt eine leicht modifizierte Version eines Thesenpapiers des Workshops “Schöpferische Zerstörer: Bitcoin, Blockchain und Smart Contracts – Digitale Treuhänder transformieren die Gesellschaft“ an der Evangelischen Akademie Villigst am 15.10.2016 dar. Die Arbeitsergebnisse des Workshops sind im letzten Abschnitt stichpunktartig zusammengefasst.

man die Konten von Alice und Bob und den zu überweisenden Betrag. Dieser Vorgang wird durch eine Treuhänder, in der Regel eine Bank B vorgenommen, der sicherstellt, dass die Transaktion korrekt ausgeführt wird. Das „Geld“ ist als Giralgeld nicht physisch vorhanden, sondern nur in Form von Zahlen – früher handschriftlich im Hauptbuch der beteiligten Banken eingetragen, heute in Form von Bits in den beteiligten EDV-Systemen existent. Blockchain ist nun eine dezentrale Datenbank, die Transaktionen jedweder Art transparent und überprüfbar für alle Beteiligten, erfasst. Verwenden Alice und Bob im obigen Beispiel Blockchain, so kann die Bank als Intermediär wegfallen, da die Transaktion unbestreitbar und unfälschbar durch das System selbst durchgeführt wird. Das Vertrauen, das normaler Weise durch den Treuhänder hergestellt wird, ist nicht mehr notwendig, sondern wird durch die verwendeten Algorithmen automatisch bereitgestellt (der Economist bezeichnete Blockchain als „Vertrauensmaschine“ [Eco15]). Im folgenden erklären wir die Einzelteile des Systems und die verwendeten Begriffe.

1.2 Dezentral und Peer-to-Peer

Die Blockchain ist ein Journal, in dem sämtliche Transaktionen seit Stunde Null (dem Start der Blockchain) aufgeführt sind. Dieser Journal wird nicht zentral (Katasteramt oder bei einer Bank) geführt, sondern jeder Teilnehmer des Systems erhält eine identische Kopie, es ist also über (sehr) viele Computer verteilt. Es ist durch Schlüssel und kryptographische Verfahren gesichert und kann daher nicht leicht gefälscht werden. Da der Journal durch alle Teilnehmer überprüft werden kann und überprüft wird, kann man mathematisch beweisen, dass ein Angriff durch einen Angreifer Mallory nur dann erfolgreich geführt werden kann, wenn Mallory mehr als 50% der Rechenleistung aller beteiligten Nutzer des Systems kontrolliert. Dies ist ein effektiver, sozialer und ökonomischer Schutz vor Manipulationen.

1.3 Transaktionen

Transaktionen können Geldüberweisungen sein, aber prinzipiell alles, was gesagt oder (auf-) geschrieben werden kann. Transaktionen, die passiert und in der Blockchain aufgezeichnet sind, können nicht mehr rückgängig oder geändert werden. Die Transaktionen werden in ihrer zeitlichen Reihenfolge und mit ihrer gesamten Historie gespeichert – vergleichbar Gesteinsschichten, die sich im Laufe der Äonen aufeinander auftürmen und die im Nachhinein nicht mehr verändert (verfälscht) werden können.

1.4 Schlüssel

Zentral für die Funktionsweise sicherer Systeme sind kryptographische Verfahren und Schlüssel. Alice und Bob besitzen sogenannte Schlüsselpaare, jeweils einen privaten und einen öffentlichen Schlüssel, die sie eindeutig identifizieren und mit deren Hilfe sie Texte verschlüsseln und signieren können. Für die Entschlüsselung und Verifikation einer Signatur wird ebenfalls kein Treuhänder, keine zentrale Stelle benötigt – jeder Teilnehmer der Blockchain kann dies selbst vornehmen. Es handelt sich – vereinfacht ausgedrückt – um komplizierte mathematische Berechnungen, die auszuführen sind. Liefern diese das korrekte Ergebnis, ist die Signatur korrekt. Schlüssel und mathematische Berechnungen, die sogenannten „Puzzle“ werden aber auch eingesetzt, um die Integrität der Blockchain zu verifizieren und neue Transaktionen als korrekt und verifiziert in den Journal aufzuführen. Diese Arbeit wird von den Buchhaltern der Blockchain vorgenommen, den sogenannten Bergarbeitern, engl. “Minern“. Man nennt diesen Prozeß “Proof-of-Work”.

1.5 Bergarbeiter (Miner), Buchhalter der Blockchain

Bei der Blockchain werden Transaktionen zu sogenannten Blöcken zusammengefasst. Diese

kann man sich als Seiten des Hauptbuches vorstellen. Jeder Block (jede Seite) verweist auf den vorherigen Block und dieser wieder auf den Vorgänger und so weiter. Somit ist rekursiv die gesamte Historie vorhanden. Die Buchhalter der Blockchain, die Miner, schauen sich neue Transaktionen an und verifizieren diese hinsichtlich Korrektheit. Die einzelne Transaktion ist leicht zu verifizieren, dies geschieht mit Hilfe der öffentlichen Schlüssel der Beteiligten. Schwieriger ist es, die Transaktionen in die richtige Reihenfolge zu bringen – wir erinnern uns, es gibt keine zentrale Datenhaltung, keine zentrale Autorität und neue Transaktionen werden dem Netzwerk aller Beteiligten mitgeteilt, wodurch es zu Unklarheiten hinsichtlich der Reihenfolge kommen kann. Schlimmer noch, ein Angreifer kann versuchen, Bitcoins (oder andere Transaktion) mehrfach auszugeben. Dies kann nur entdeckt werden, wenn man sich mehrere Transaktionen zusammen im Kontext ansieht und diese Aufgabe übernehmen die Miner. Dabei arbeiten viele Miner am selben Problem. Um zu verhindern, dass Miner selbst das System manipulieren, müssen diese aufwendige mathematische Probleme, die Puzzles, lösen, was wiederum Rechenpower voraussetzt. Nur derjenige, der das Problem zuerst löst, kann den Block verifizieren. Wer das ist, läßt sich im Einzelfall nicht vorhersagen, sondern folgt statistischen Gesetzen. So erreicht man, dass ein Miner das System nur manipulieren kann, wenn er über mehr als 50% der Rechenleistung aller anderen Miner verfügt. Nachdem ein Miner einen Block verifiziert hat und in die Blockchain aufgenommen hat, ist dieser unveränderbar, kann aber nachträglich noch für ungültig erklärt werden, wenn andere Miner längere Ketten von Blöcken herstellen konnten. Dies ist ein Tribut an die dezentrale Natur des Algorithmus und bedeutet, dass es ein Zeitfenster gibt, in dem sich z. B. ein Onlinehändler nicht darauf verlassen kann, dass die Transaktion (Bezahlung) korrekt ist. Bei Bitcoin werden Blöcke alle 10 Minuten[2] berechnet und wenn ein Händler 6 Blöcke abwartet, kann er sich sehr sicher sein, dass die Transaktion in Ordnung war.

1.6 Woher kommt das Vertrauen?

Der herkömmliche Miningprozeß schöpft Vertrauen aus der Verankerung mit der analogen „echten“ Welt – letztlich aus physikalischen Prozessen (Thermodynamik) und Wahrscheinlichkeitstheorie (Bayes’ Theorem), die die Wahrscheinlichkeit für das Vorhandensein von betrügerischen Absichten abschätzen läßt. Er ist aber offensichtlich genau wegen der Verankerung mit dem Energieverbrauch nicht besonders ökologisch und nachhaltig und somit lassen sich viele interessante Anwendungsfälle (Energygrid) aufgrund der hohen Energiekosten nicht realisieren. Vergleichbar ist dies mit dem Goldstandard als Währung – auch hier ergibt sich der Wert direkt aus der realen Schwierigkeit, das Edelmetall zu schürfen. Daher wurden bereits seit 2011 alternative Verfahren zur Verifikation vorgeschlagen – sogenannte “Proof of Stake“ Verfahren, die weniger rechenintensiv sind, dafür aber andere Nachteile aufweisen können [KS], [Pat]. Bei ihnen wird – vereinfacht gesprochen – Vertrauen aus dem Anteil, mit dem jemand finanziell in die Blockchain investiert ist, geschöpft. Hier wird also Vertrauen an soziales Verhalten gebunden, weshalb diese Verfahren eng mit der Spieltheorie verbunden sind. Ein rein auf “Proof of Stake“ begründetes Verfahren ist mit Fiat-Geld zu vergleichen, dessen Wert sich ausschließlich aus gesellschaftlichen Konventionen ergibt. Wegen der Vor- und Nachteile beider Verfahren experimentiert man zur Zeit häufig mit hybriden Systemen, die beide Formen kombinieren. In jedem Fall aber zeigt sich, dass ohne Verknüpfung der digitalen mit der analogen Welt kein Vertrauen herstellbar ist[3].

---

2 Dies ist eine Konvention bei Bitcoin und nicht durch die Blockchain vorgegeben. Die Intervalle könnten auch kürzer festgelegt werden.

3 Technisch gesehen verbirgt sich das in der Informatik lange bekannte Problem der byzantinischen Generäle, das im Kontext von dezentralen Verfahren oft auftritt und keine einfache Lösung hat.

1.7 Smart Contracts – aktive Daten

In der Informatik weiß man schon lange, dass Daten und Programme eigentlich dasselbe sind (Homoiconicity). Daher liegt der Gedanke, nicht nur Daten in der Blockchain zu verwalten, sondern ausführbare Programme, sehr nahe. Funktional bedeutet dies, dass man Verträge und das Vertragsmanagement automatisieren kann. Eine Implementierung dieser Idee ist Ethereum [But], eine Plattform für dezentrale, ausführbare Programme, die 2014 von Vitalik Buterin gegründet wurde und mit deren Hilfe die erste vollautomatisierte Firma, DAO – Decentralized Autonomous Organisation, ins Leben gerufen wurde [Gra16].

2 Gesellschaftlicher Bezug

2.1 Anwendungsgebiete

Anwendungsgebiete für die Blockchain und Smart Contracts sind vielfältig, u.a.

1. Banken und Finanzdienstleistungen
2. Öffentliche Verwaltungen (Kataster, Grundbuchämter, Steuern)
3. Digitale, Online Wahlsysteme [AHT09]
4. Micropayments
5. Kunst- und Musikmarkt

Aber auch völlig neue Anwendungsfälle sind denkbar wie z. B. zweckgebundene Steuern, also Steuern oder besser gesagt Abgaben, die in transparenter Weise zweckgebunden sind, oder ethische Investments, bei denen Anlegergelder nur in zertifizierte Projekte investiert werden können. Aber auch alltägliche Dinge wie der Gebrauchtwagenkauf können völlig neu geregelt werden. So ist denkbar, dass Alice Bob den Wagen auf Raten verkauft und bei ausbleibenden Ratenzahlungen von Bob der Kauf automatisch rückabgewickelt oder das Auto elektronisch stillgelegt wird[4]. Und all das ohne Treu- und Zwischenhändler oder staatliche Institutionen.

Blockchain kann auch helfen, ein Problem der digitalen Welt zu lösen, nämlich dass Daten leicht und beliebig kopierbar sind. Mit der Blockchain ist es möglich, Eigentum an Daten zu definieren und auf diese Art digitale Güter analog zu physischen Gütern handelbar zu machen, etwa im Kunstmarkt [Vog]. Für Musiker eröffnen sich so z. B. völlig neue Möglichkeiten der Distribution und Abrechnungsmodelle, die ohne Labels (Plattenfirmen) auskommen.

2.2 Blockchain und die Konstitution des gesellschaftlichen Regelwerks

In weltweit stark rezipierten Beiträgen [Les99], [Les00] beschrieb Lawrence Lessig im Jahr 2000:

> “Every age has its potential regulator, its threat to liberty. […] Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means “freedom from government” that we don’t even see the regulation in this new space. We therefore don’t see the threat to liberty that this regulation presents.
> This regulator is code – the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether

4 ein schönes Beispiel für einen Smart Contract

> information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates."

Zur Erinnerung: Die Blockchain hat das Potential, sämtliche Vorgänge, die als Regeln beschrieben werden können, zu kodieren und zu verwalten und das ggf. ohne Zwischenhändler. Das heißt überall dort, wo Transaktionen aller Art vorkommen und zur Zeit noch mehr oder weniger zentrale Register verwendet werden, kann die Blockchain diese Prozesse modifizieren, ergänzen oder ganz ersetzen. Zentrale Register existieren in vielen Lebensbereichen – beim Nachweis und der Verwaltung von Eigentumsverhältnissen wie Grundbüchern oder Konten etwa. Aber auch beim Identitätsmanagement (Einwohnermeldeamt, Facebook- oder Googlekonto). Die Verwaltung und Beglaubigung kostet dabei viel Zeit und Ressourcen und könnte durch Blockchain deutlich effizienter realisiert werden. Da die Blockchain potentiell sämtliche digitalen Transaktionen verwalten könnte und im Zuge der Digitalisierung sämtliche Lebensbereiche als digitale Transaktionen erfasst werden, hat die Blockchain das Potential, das Leben aller Menschen zu erfassen und digital zu verwalten – ein dezentraler, digitaler Leviathan ungeahnten Ausmaßes.
Die Blockchain kann einerseits dort eingesetzt werden, wo noch keine oder nur ungenügende Staatlichkeit existiert, so z. B. in vielen unterentwickelten Regionen der Welt, in denen fehlende Institutionen und Rechtssicherheit Entwicklung verhindern – so experimentieren z. B. Honduras und Griechenland mit Blockchain als Grundlage für die Katasterämter [Vol16].
Andererseits verstehen sich viele Befürworter, Geldgeber und Software-Entwickler, die im Silicon Valley arbeiten auch als Teil einer libertären Anarcho-Kapitalismus Bewegung, die aggressiv jede Form von Staatlichkeit ideologisch ablehnt und bekämpft. Ein herausragender Vertreter ist z. B. der PayPal Mitbegründer Peter Thiel, s. [Sta11]; ein Bericht über Europäische Vertreter dieser Denkschule (die der Österreichischen Schule der Nationalökonomie nahestehen) findet sich in [Fis]. Für diese sind Technologien wie Blockchain lediglich wichtige Waffen im Kampf um die Abschaffung des Staates und die weltweite uneingeschränkte kapitalistische Herrschaft. Auch dies sollte man wissen, um die Diskussionsteilnehmer richtig einordnen zu können.

2.3 Die Matrix und die Welt

Ein wichtiger Punkt, der sowohl von Befürwortern als auch Skeptikern von Blockchain (und anderen Technologien) unterschlagen wird, ist die Tatsache, dass diese Technologien zunächst „nur" die digitale Welt kontrollieren. Die Blockchain trifft zunächst nur mathematische Aussagen über Zahlen – Bitcoins kann man weder essen noch ohne Zwischenhändler und Interaktion mit der physischen Welt in Geld oder Dinge tauschen. M.a.W. man braucht ein gesellschaftliches Regelwerk, das in der Lage ist Macht – wenn notwendig auch mit Gewalt – auszuüben (Justiz, Exekutive), um die Blockchain an die physische Welt anzukoppeln. Selbst in einer relativ virtuellen Branche wie der Finanzindustrie ist es notwendig, virtuell gehandelte ggf. unregulierte Ware mit der gewöhnlichen regulierten Börsenwelt zu verbinden [Aga16]. Und selbst im Kern der Blockchain Technologie zeigt sich, dass die Trennung von Geist und Körper nicht aufrechtzuerhalten ist: Um die Blockchain zu sichern sind die Miner notwendig. Diese transferieren physikalische Energie, Strom in Vertrauen, weshalb viele Miner in der Nähe kostengünstiger Stromquellen [Cut] angesiedelt sind – welche Ironie!
Einige Vordenker der libertären Philosophie sehen daher auch konsequent in der vollständigen Privatisierung der Exekutive die Chance, die digitalen Technologien zur vollständigen, ungehinderten Kontrolle der physischen Welt einzusetzen. Beispiele dafür sind

Ansätze, Polizei zu privatisieren [Pet] oder durch Roboter zu ersetzen [Li][5]. Je mehr digitale und physische Welt integriert werden, desto mehr verwischt sich dieser Unterschied allerdings. Wenn HP durch Software-Updates Druckerpatronen von Fremdherstellern noch nachträglich funktionsunfähig machen kann, dann stellt dies den jahrhundertelang entwickelten und regulierten Eigentumsbegriff in Frage [Opi16]. Durch das Internet der Dinge, bemächtigt sich die digitale Welt der realen. Wir stehen hier erst am Anfang. Und diejenigen, die die Regeln der digitalen Welt bestimmen, beherrschen dann auch die reale.

2.4 Wer kontrolliert die Algorithmen?

Es ist deutlich geworden, dass die Blockchain das Potential hat, in Zukunft einen wichtigen Teil des gesellschaftlichen Regelwerks zu kodieren. Historisch betrachtet, haben sich Neuerungen zunächst immer erst eingefunden (Erfindungen wurden gemacht), bevor diese reguliert wurden. Nur wer Anhänger eines libertären Anarcho-Kapitalismus ist, wird einen Regulierungsanspruch prinzipiell ablehnen wollen. Für die anderen bleibt die Frage, wie eine Regulierung gedacht werden kann, die uneingeschränkte Herrschaft der Netzmonopolisten genauso verhindert wie staatlich motivierte und organisierte totalitäre Allmachtsphantasien. Die Theorie des Gesellschaftsvertrags muss vor dem Hintergrund der technischen Umwälzungen wieder neu gedacht werden.

3 Diskussionsergebnisse

Die Diskussion ergab schnell, dass die Technologie janusköpfig ist. Einerseits bietet sie Potential für viele sinnvolle Anwendungen, die – ganz im Sinne einer demokratietheoretischen Ermächtigung des Souveräns – quasi „von unten“ eine positive, demokratiestärkende Funktion erfüllen können. Andererseits können sie auch für das Gegenteil verwendet werden und Tendenzen der totalitären Überwachung verstärken. Ein Beispiel für ersteres wäre etwa der Einsatz von Blockchain und ähnliche Technologien für Regionalwährungen (auch Regionalgeld oder Bürgergeld[6]) oder die transparente, dezentrale Beglaubigung demokratische Verfahren im politischen Prozess. Ein Beispiel für letzteres wäre die Entwicklung von Technologien, die anonymes Bezahlen verhindern und sämtliche finanziellen Transaktionen protokollieren. Die Zweideutigkeit von Technologien ist keine neue Erkenntnis und trifft auf viele neue Erfindungen zu. Die Arbeitsgruppe konstatierte jedoch schnell, dass das positive, emanzipatorische Potential, das zweifelsohne vorhanden ist, in Deutschland und Europa, häufig ignoriert oder zu schnell verworfen wird, um das Augenmerk dann einseitig auf die Verhinderung möglicher Missbräuche durch Regulierung zu lenken. Aus dieser Einschätzung entstand die Empfehlung, bereits frühzeitig mit neuen Technologien in einem zivilgesellschaftlichen Rahmen zu experimentieren. Dieses Experimentieren könnte durch europäische Institutionen explizit gefördert werden und so das reaktive, bloße Regulieren, das häufig angesichts der grenzüberschreitenden Macht der digitalen Technologien gar nicht mehr möglich ist, ergänzen.

---

5 Allerdings scheinen mir die in diesen Kreisen häufig anzutreffenden technischen Allmachtsphantasien, die jedes gesellschaftliche Problem mit Technik adressieren wollen, ausgesprochen unhistorisch und naiv – was aber nicht bedeutet, dass diese keinen Einfluß gewinnen!

6 In diesem Zusammenhang sei auf den Beitrag von Herrn Helbing verwiesen, in dem u.a. auf die Notwendigkeit der Einführung von multidimensionalem Geld hingewiesen wurde. Digitale Währungen auf Basis von Blockchain und Smart Contracts können genau dies verwirklichen.

4 Architektur und Algorithmen

Die Abbildung 1 verdeutlicht das sogenannte “Double Spending” Problem, das entsteht, wenn ein und derselbe Bitcoinmehrfach benutzt wird. Es muss entschieden werden, welche Transaktion gültig ist. Das geschieht durch geschickte Kombination von Verifikation und Verteiltem Konsensverfahren.

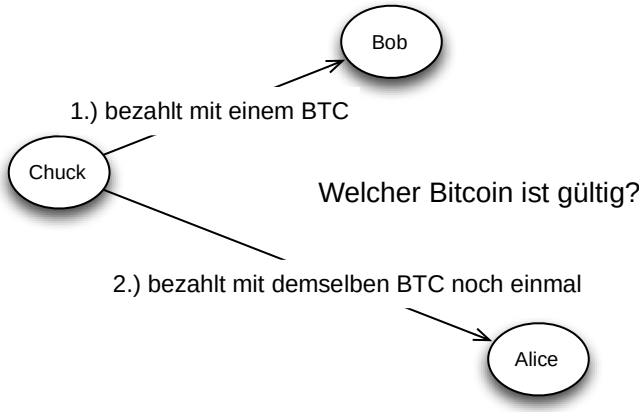

Abbildung 1 Das "Double Spending" Problem

Die Abbildung 2 verdeutlicht das Signieren und den Aufbau der einzelnen Blöcke der Blockchain, angefangen von ersten sogenannten „Genesis-Block”.

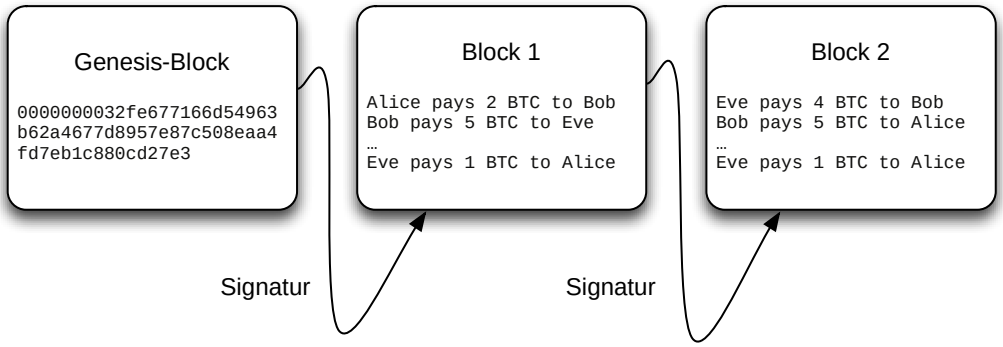

Abbildung 2 Die Blockchain

Man erkennt, dass es eine nahtlose Kette von Signaturen gibt, die die vollständige Historie von Transaktionen beglaubigt und damit unfälschbar macht.
Die Abbildung 3 verdeutlicht das Verifizieren und Hinzufügen von Blöcken im Miningprozeß. Man beachte, dass es sich hier um ein verteiltes Konsensverfahren handelt. Im Beispiel verwirft Node 1 seinen Block 4’, da Node 2 und 3 längere Blöcke herstellen können. Dieses Konsensverfahren beruht auf Mehrheitsentscheidungen aller Teilnehmer.

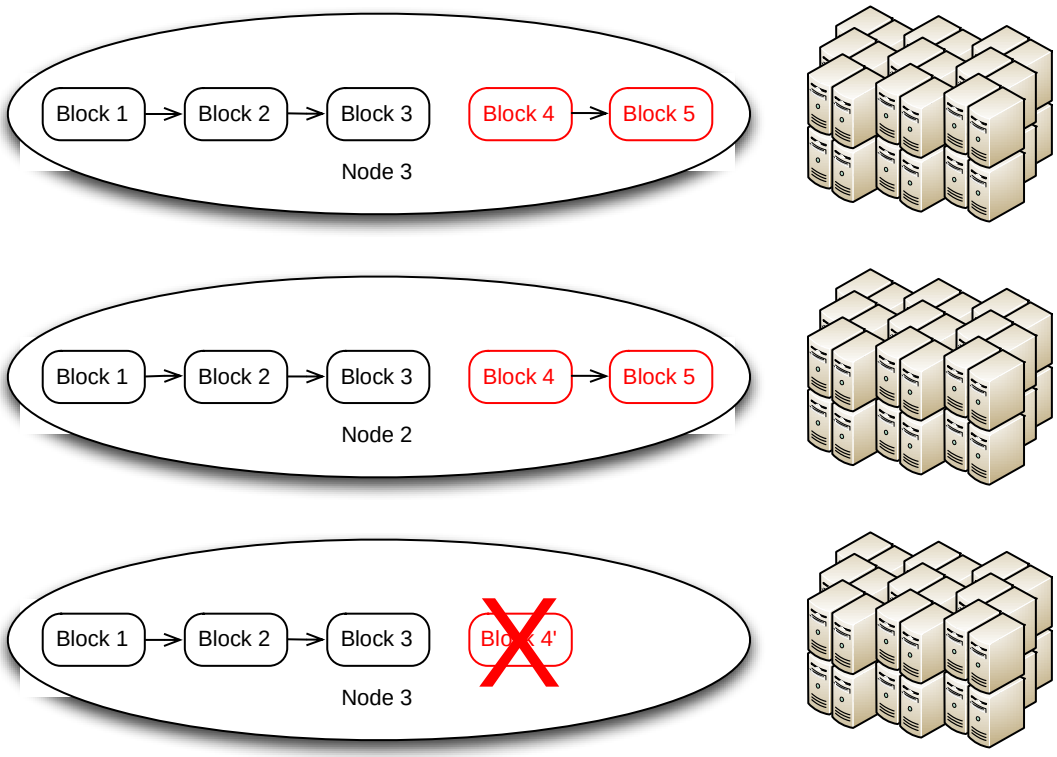

Abbildung 3 Der Miningprozeß und Distributed Consens

Für weitere technische Details sei auf die gute Online Dokumentation auf https://bitcoin.org/ und https://ethereum.org verwiesen.

Literatur

[Aga16] Agate. Assessment of blockchain technology in the financial sector based on selected use cases. Master's thesis, Frankfurt University of Applied Sciences, May 2016.

[AHT09] R.M. Alvarez, T.E. Hall, and A.H. Trechsel. Internet voting in comparative perspective: The case of estonia'. PS: Political Science & Politics, 42(3):pp. 497–505, 2009.

[But] Vitalik Buterin. ethereum.org [online]. URL: https://www.ethereum.org [cited 27.09.2016].

[Cut] Anthony Cuthbertson. Geothermal gold: Why bitcoin mines are moving to iceland [online]. URL: http://www.ibtimes.co.uk/geothermal-gold-why-bitcoin-mines-are-moving-iceland-1468295 [cited 27.09.2016].

[Eco15] Economist. The promise of the blockchain the promise of the blockchain – the trust machine [online]. Oct 2015. URL: http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine [cited 27.09.2016].

[Fis] Malte Fischer. Anarcho-Kapitalismus Anarcho-Kapitalismus Freiheit statt Demokratie [online]. URL: http://www.wiwo.de/politik/konjunktur/anarcho-kapitalismus-freiheit-statt-demokratie/12356986.html [cited 27.09.2016].

[Gra16] Hannes Grassegger. Blockchain Die erste Firma ohne Menschen. Zeit, Mai 2016. URL: http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-

ethereum [cited 27.09.2016].

[KS] Sunny King and Nadal Scott. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. URL: https://www.peercoin.net/assets/paper/peercoin-paper.pdf [cited 13.10.2016].

[Les99] Lawrence Lessig. Code and Other Laws of Cyberspace. Basic Books, Inc., New York, NY, USA, 1999.

[Les00] Lawrence Lessig. Code is law code is law - on liberty in cyberspace. Harvard Magazine, Jan 2000. URL: http://harvardmagazine.com/2000/01/code-is-law-html [cited 27.09.2016].

[Li] Shan Li. Robots are becoming security guards. [online]. URL: http://www.latimes.com/business/la-fi-robots-retail-20160823-snap-story.html [cited 28.09.2016].

[Nak] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. URL: http://bitcoin.org/bitcoin.pdf [cited 27.09.2016].

[Opi16] Rudolf Opitz. Der Tinten-Krieg: Update für HP-Drucker macht Alternativ-Patronen wieder mal unbrauchbar. heise online, Sep 2016. URL: https://www.heise.de/newsticker/meldung/Der-Tinten-Krieg-Update-fuer-HP-Drucker-macht-Alternativ-Patronen-wieder-mal-unbrauchbar-3330374.html [cited 28.09.2016].

[Pat] Ray Patterson. Alternatives for proof of work, part 1: Proof of stake. URL: https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/ [cited 13.10.2016].

[Pet] Austin Petersen. Citizens of oakland are crowdfunding a private police force [online]. URL: http://thelibertarianrepublic.com/citizens-oakland-crowdfunding-private-police-force/ [cited 28.09.2016].

[Sta11] The Week Staff. Libertarian island: A billionaire’s utopia. The Week, 2011. URL: http://theweek.com/articles/482427/libertarian-island-billionaires-utopia [cited 27.09.2016].

[Vog] Stephan Vogler. Dank Bitcoin wird digitale Kunst sammel- und handelbar [online]. URL: https://www.btc-echo.de/dank-bitcoin-wird-digitale-kunst-sammel-und-handelbar_2015041501/ [cited 27.09.2016].

[Vol16] Jan Vollmer. Diese Technik soll das Finanzsystem umkrempeln. fr-online, 08 2016. URL: http://www.fr-online.de/fintech/blockchain-diese-technik-soll-das-finanzsystem-umkrempeln-,34612132,34678392.html [cited 27.09.2016].