Blockchain
Buzzword oder digitale Revolution?

TIM EDER
HTWK Leipzig, Fakultät IMN
Oberseminar Datenbanksysteme, Master Medieninformatik

Inhaltsverzeichnis

1 Einführung

Spätestens seit 2017 ist der Begriff "Blockchain" durch die rasante Preisexplosion von Bitcoin in aller Munde. Der Hype um die Blockchain hat starke Reaktionen auf beiden Seiten ausgelöst. Viele halten diese Technologie nur für ein weiteres Buzzword, das im Moment "in" ist. Für andere ist sie eine digitale Revolution, nicht weniger bedeutend als das Internet selbst. Ein Blick in die Funktionsweise, Vor- und Nachteile, sowie potentielle Anwendungsgebiete der Blockchain lohnt sich also.

Im November 2008 wurde von Satoshi Nakamoto ein Whitepaper mit dem Titel "Bitcoin: A Peer-to-Peer Electronic Cash System" veröffentlicht. Satoshi Nakamoto ist aber nur ein Pseudonym. Niemand weiß, wer diese Person ist, oder ob es sich möglicherweise um eine Gruppe von Entwicklern handelt. Wahrscheinlich als Reaktion auf die internationale Finanzkrise von 2008, die vielen Menschen das Vertrauen in Banken genommen hat, schlug Satoshi Nakamoto ein dezentrales Netzwerk vor, mit dem Onlinezahlungen ohne Mittelsmänner durchgeführt werden können. Mithilfe kryptographischer Verfahren und dem sogenannten Proof-of-Work System, wird die Gültigkeit dieser Transaktionen verifiziert. [1]

Im Folgenden wird erläutert, wie die Bitcoin Blockchain funktioniert, welche Schwachpunkte diese Technologie hat und wo sie eingesetzt werden kann.

2 Technik

Das größte Problem bei der Abwicklung von Onlinezahlungen ist Double Spending. Es muss gewährleistet sein, dass ein Nutzer die selbe digitale Münze (oder Token) nicht mehrfach ausgibt, indem er zum Beispiel eine alte Transaktion kopiert und nur den Empfänger ändert. Bisher wurde dieses Problem immer durch einen zentralen Vermittler umgangen, der alle Transaktionen überprüft. Dadurch muss jeder Teilnehmer diesem Vermittler vertrauen und das System wird anfälliger für Angriffe, da es nur noch einen "Single Point of Failure" gibt.

Die dezentrale Lösung des Bitcoin Netzwerkes schafft Vertrauen, indem alle Teilnehmer Transaktionen mittels kryptographischer Verfahren verifizieren. Dabei ist es notwendig, dass Transaktionen und Guthaben jederzeit allen Teilnehmern öffentlich zur Verfügung stellen. Dieses digitale Kontobuch wird auch Ledger genannt. Die einzelnen Seiten dieses Ledgers werden in Blöcken dargestellt, die miteinander verkettet werden, daher der Name Blockchain.

Jeder Teilnehmer des Netzwerkes hat einen Public und Private Key. Der Public Key fungiert als Adresse, bzw. Geldbörse, auf der hinterlegt ist, wie viele Bitcoins der Inhaber besitzt. Um eine Transaktion durchzuführen, wird die Senderadresse, ein Betrag, und die Empfangsadresse benötigt. Um zu gewährleisten, dass die Zahlung vom rechtmäßigen Besitzer der Coins angeordnet wurde, muss der Besitzer die Transaktion mit seinem Private Key digital signieren. Jedem Teilnehmer ist es so möglich, Transaktionen in den Ledger einzutragen, solange er sich an die Regeln des so genannten Consensus Protocols hält. Diese Regeln sind im Bitcoin Quellcode definiert. Für Transaktionen gibt es 20 Regeln. Die wichtigsten sind, dass eine Transaktion vom Sender signiert sein muss und dass das Guthaben des entsprechenden Public Keys nicht überschritten werden darf.[2]

Gültige Einträge werden an die übrigen Teilnehmer (Nodes) des Netzwerkes weitergeleitet, und von ihnen in die eigene Kopie des Ledgers eingetragen. Eine Node schickt dabei die Nachricht an die physikalisch nächstgelegenen Knoten, die sie wiederum weiterleiten. Informationen breiten sich also wellenförmig über das gesamt Netzwerk aus. Um zu gewährleisten, dass jede Kopie des Ledgers identisch ist, kommt das Proof-of-Work-System zum Einsatz: man nutzt Hashfunktionen, um aufgebrachte Rechenleistung zu beweisen.

Im Bitcoin Protokoll ist es die Hashfunktion SHA256. Die wesentliche Eigenschaft einer solchen Funktion ist, dass sich das Ergebnis eines Inputs

nur durch Ausprobieren finden lässt. Es ist unmöglich, den Output vorherzusagen. Man legt also die Regel fest, dass der Hashwert eines Blockes mit einer bestimmten Anzahl an Nullen beginnen muss. Um diese Bedingung zu erfüllen, wird an den Block eine zufällige Zahl, genannt Nonce, gehängt und der Hash berechnet. Soll dieser Hash zum Beispiel mit 30 Nullen beginnen, beträgt die Chance, einen solchen gültigen Nonce zu finden, bei $\frac{1}{2^{30}}$, also circa 1 Milliarde. Um zu überprüfen, dass der Hashwert zu einem Block gehört, genügt eine einzige Ausführung der Hashfunktion. Es lässt sich also schnell beweisen, dass jemand sehr viele Rechenoperationen durchgeführt hat. Je höher die gewünschte Anzahl der führenden Nullen ist, desto schwieriger ist es, einen Noncewert zu finden, deshalb wird die Anzahl auch Difficulty Level genannt. [3]

Da bei Hashfunktionen eine Änderung des Inputs einen komplett anderen Output produziert, müsste bei nachträglicher Veränderung eines Blockes (also einem Betrugsversuch) ein neuer Noncewert gefunden werden, also den kompletten Rechenaufwand erneut betreiben. Damit auch die zeitliche Reihenfolge von Blöcken, bzw. Transaktionen berücksichtigt wird, beginnt jeder Block mit dem Hashwert des vorhergehenden Blockes. Somit müssen bei Änderungen alle nachfolgenden Blöcke neu berechnet werden. Von den Netzwerkteilnehmern wird die Kette als wahr angenommen, in die die meiste Rechenarbeit gesteckt wurde.[4]

Die Funktionsweise des Bitcoin Netzwerkes lässt sich in diesen sechs Schritten zusammenfassen:

1. Neue Transaktionen werden an alle Knoten übermittelt.
2. Jeder Knoten schreibt neue Transaktionen in einen Block.
3. Jeder Knoten versucht, einen gültigen Noncewert für diesen Block zu finden.
4. Findet er diesen Wert, wird der Block an alle anderen Knoten übermittelt.
5. Die Knoten akzeptieren diesen Block nur, wenn alle enthaltenen Transaktionen gültig sind.
6. Diese Akzeptanz wird von den Knoten ausgedrückt, indem sie anfangen, am nächsten Block zu arbeiten, der den Hashwert des soeben akzeptierten Blockes enthält.[1, Seite 3]

Um für die Knoten einen Anreiz zu bieten, diese Berechnungen durchzuführen, bekommen sie für jeden berechneten Block eine Bezahlung in

Bitcoin auf ihre eigene Adresse, den so genannten Block Reward. Diese Coins werden neu erschaffen, somit gelangen also neue Coins in Umlauf. Der Prozess, durch den Einsatz von Rechenleistung, bzw. Energie, neue Währung zu schaffen, ist analog zu Goldgräbern in der echten Welt. Daher werden die Knotenbetreiber auch "Miner" genannt. Das System ist so konzipiert, dass es für potentielle Angreifer immer wirtschaftlich profitabler sein sollte, die Regeln einzuhalten. Was ein Angreifer mit viel Rechenleistung anstellen könnte, zeigt das nächste Kapitel.

3 Schwachstellen und Probleme

Kontrolliert ein Angreifer, mehr als 50% der gesamten Rechenleistung des Netzwerkes, kann er Schaden anrichten, da er die Mehrheit der ehrlichen Knoten überstimmen kann. Das nennt man 51%-Attack. Ihm wäre es jetzt möglich, eigene Transaktionen rückgängig zu machen, und somit Double-Spending durchzuführen. Ebenfalls kann er das Netzwerk zum Stillstand bringen, indem er Transaktionen oder Blöcke nicht mehr als gültig betrachtet. Ein Angreifer kann aber keine Coins senden, die ihm nicht gehören oder Coins generieren. Eine solche Attacke auf das Bitcoin Netzwerk ist allerdings sehr unwahrscheinlich. Es würde enorme Rechenleistung, und somit auch Geld, erfordern. Falls ein solcher Angriff aber durchgeführt wird, hätte dies einen sofortigen Preisverfall des Bitcoins zur Folge, da die beiden größten Vorteile der Kryptowährung, Dezentralisierung und Sicherheit, entwertet werden. Aus wirtschaftlicher Sicht ist es für Miner also attraktiver, ihre Rechenleistung für den Block Reward einzusetzen. Lediglich politische oder ideologische Motive, wären denkbare Ursachen einer solchen Attacke. [5]

Vor Hackingangriffen ist das Netzwerk also gut geschützt. Die größten Probleme dieser Technologie liegen in der Nutzererfahrung und Skalierbarkeit. Jeder ist für seine eigenen Bitcoins verantwortlich, frei nach dem Motto "Be your own bank". Bei Verlust oder Diebstahl der Private Keys gibt es keine Möglichkeit, die Bitcoins zurückzubekommen. Diese kryptischen Schlüssel machen die Nutzung des Netzwerkes nicht massentauglich.

Aktuell schafft das Bitcoin Netzwerk durchschnittlich 5 Transaktionen pro Sekunde. Diese Begrenzung ergibt sich hauptsächlich aus zwei festgelegten Regeln des Bitcoin-Protokolls: der Blocktime und der Blocksize. Letztere beträgt 1MB. Bei einer Transaktionsgröße von 300-500 Byte passen also im günstigsten Fall 3000 Transaktionen auf einen Block. Der Difficulty

Level passt sich alle zwei Wochen automatisch so an, dass die Blocktime stets 10 Minuten beträgt. Um das Netzwerk zu beschleunigen, könnte man also die Blocktime senken, bzw. die Blocksize erhöhen. In der Community herrschen dazu aber gespaltene Meinungen, weswegen es noch zu keiner Veränderung des Protokolls kam.

Ein Häufig kritisierter Punkt von Bitcoin ist der hohe Energieverbrauch. Die Berechnungen der Noncewerte werden auf speziellen ASIC-Chips (Application-specific Integrated Circuit) durchgeführt, die sehr viel Strom benötigen. Das komplette Netzwerk verbraucht ungefähr so viel Energie wie Tschechien. Bei einem weiteren Preisanstieg wird Mining immer profitabler und der Stromverbrauch erhöht sich immer mehr. Aufgrund der vergleichsweise günstigen Kosten für Strom, ist China ein beliebter Standort für Miningfarmen. Dort wird Energie zum größten Teil noch aus Kohlekraftwerken gewonnen. Die Auswirkungen auf die Umwelt sind also enorm. Es stellt sich also die Frage, ob es vertretbar ist, so viel Energie für nutzlose Berechnungen aufzubringen.

Eine Lösung dieses Problems könnte der Wechsel von Proof-of-Work auf Proof-of-Stake sein. Bei diesem alternativen Verifizierungssystem müssen die Nodes einen Teil ihres Vermögens als Einsatz anbieten. Unter allen Teilnehmern wird dann zufällig eine Node ausgewählt, die den nächsten Block verifizieren soll. Je höher der Einsatz, desto höher ist die Wahrscheinlichkeit ausgewählt zu werden. Bei einem Betrugsversuch verliert man dann seinen kompletten Einsatz. Dieses Verfahren benötigt kaum Rechenleistung und somit auch deutlich weniger Energie. Einige neuere Kryptowährungen setzen Proof-of-Stake bereits ein.

4 Anwendungsfälle

Die Blockchain Technologie hat weitaus mehr Anwendungsmöglichkeiten als nur digitales Geld. Das zeigt sich besonders bei Ethereum. Ethereum ist eine Art blockchainbasiertes Betriebssystem mit einer eigenen Kryptowährung namens Ether. Die Besonderheit dieser Plattform ist die Koppelung dieser Währung mit der vollwertigen Programmiersprache Solidity.[6] Mit ihrer Hilfe lassen sich so genannte Smart Contracts programmieren. Smart Contracts sind Programme, die auf der Blockchain ausgeführt werden. Somit kann man den Austausch von digitaler Währung an Bedingungen knüpfen. Der Code dieser Programme ist für jeden öffentlich einsehbar und bietet daher Transparenz. Mithilfe von Smart Contracts lassen sich

vollautomatisierte Systeme bauen. Diese Programme nennt man decentralized Apps, oder kurz dApps. Sie können beliebig simpel oder komplex sein und vielfältig eingesetzt werden, zum Beispiel als Messenger für sichere Kommunikation, Crowdfunding Plattform, Wahlsystem oder als ein faires Onlinecasino.[7]

Der Einsatz von Blockchains macht überall dort Sinn, wo Transparenz und Fälschungssicherheit erforderlich ist. Durch selbstausführende Smart Contracts eröffnen sich zudem neue Möglichkeiten im Bereich der Automatisierung.

5 Fazit

Blockchain und Kryptowährungen haben durch die Spekulationsblase, Betrugsfälle und Nutzung in kriminellen Bereichen viel negative Kritik in der Presse bekommen. Obwohl es das Bitcoin Netzwerk schon seit nun zehn Jahren gibt, konnte sich die Technologie noch nicht massentauglich durchsetzen. Sie ist schwer zu verstehen und zu langsam. Bei genauerer Betrachtung wird aber klar, dass Blockchains großes Potential haben. Sie sind die erste fälschungssichere, selbstverwaltende und dezentrale Datenbank der Welt. Mit ihrer Hilfe ist es möglich, den Menschen unabhängiger von großen Unternehmen zu machen, sei es im Finanzbereich oder auch bei Social Media. Blockchains können mehr Transparenz in die Politik bringen und ein wichtiger Motor für die fortschreitende Automatisierung sein.

Literatur

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.
2. Bitcoin Wiki. Protocol rules. https://en.bitcoin.it/wiki/Protocol_rules#.22tx.22_messages, 2017.
3. Andreas M. Antonopoulos. Consensus algorithms, blockchain technology and bitcoin. https://www.youtube.com/watch?v=fw3WkySh_Ho, 2016.
4. Michael Nielsen. How the bitcoin protocol actually works. http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/, 2013.
5. Bitcoin Wiki. Weaknesses. https://en.bitcoin.it/wiki/Weaknesses, 2017.
6. Wikipedia. Ethereum. https://en.wikipedia.org/wiki/Ethereum, 2018.
7. Blockgeeks. Smart contracts: The blockchain technology that will replace lawyers. https://blockgeeks.com/guides/smart-contracts/, 2018.