Blockchain Engineering

Blockchains und Kryptowährungen

Dr. Lars Brünjes

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

MODULARES INNOVATIVES
NETZWERK FÜR DURCHLÄSSIGKEIT

AUFSTIEG DURCH
BILDUNG
OFFENE HOCHSCHULEN

26. September 2019

Kurze Definition einer Blockchain

Eine Blockchain (. . .) ist eine verteilte Datenbank, die eine stetig wachsende Liste von Datensätzen, den sogenannten *Blöcken*, verwaltet. Jeder Block enthält eine Zeitstempel und einen Link zu seinem Vorgänger.

Wikipedia

Blockchains sind...

Blockchains sind...

- Write-only Speicher in der Cloud — nur Schreiben, kein Ändern oder Löschen.

Blockchains sind...

- Write-only Speicher in der Cloud — nur Schreiben, kein Ändern oder Löschen.
- Dezentralisiert — verteilt auf viele Nodes (Knoten) ohne zentrale Datenbank.

Blockchains sind...

- Write-only Speicher in der Cloud — nur Schreiben, kein Ändern oder Löschen.
- Dezentralisiert — verteilt auf viele Nodes (Knoten) ohne zentrale Datenbank.
- Ein (meist) öffentliches Register (Ledger)
  - für finanzielle Transaktionen,
  - für Zertifikate (Diplome,...),
  - für Besitzurkunden (Grundstücke, Häuser, Autos,...),
  - ...

Blockchains sind...

- Write-only Speicher in der Cloud — nur Schreiben, kein Ändern oder Löschen.
- Dezentralisiert — verteilt auf viele Nodes (Knoten) ohne zentrale Datenbank.
- Ein (meist) öffentliches Register (Ledger)
  - für finanzielle Transaktionen,
  - für Zertifikate (Diplome,...),
  - für Besitzurkunden (Grundstücke, Häuser, Autos,...),
  - ...

Die Essenz einer Blockchain

Lassen Sie sich nicht von technischen Details verwirren! Im Kern ist eine Blockchain ein Buch, in dessen identische Kopien viele Menschen weltweit verteilt dieselben Einträge mit unauslöschlicher Tinte machen. Die Technologie dient nur dazu, dies praktisch zu ermöglichen!

Kurze Definition einer Kryptowährung

Eine Kryptowährung ist ein digitales Gut, das als Tauschmittel dienen soll und Kryptografie benutzt, um Transaktionen und die Erzeugung neuer Einheiten der Währung zu sichern und zu kontrollieren.

Andy Greenberg

- In diesem Kurs verstehen wir unter einer Kryptowährung eine Blockchain, die auf *finanzielle Transaktionen* spezialisiert ist.

- In diesem Kurs verstehen wir unter einer Kryptowährung eine Blockchain, die auf *finanzielle Transaktionen* spezialisiert ist.
- Die Register-Einträge in den Blöcken sind also finanzielle Transaktionen.

- In diesem Kurs verstehen wir unter einer Kryptowährung eine Blockchain, die auf *finanzielle Transaktionen* spezialisiert ist.
- Die Register-Einträge in den Blöcken sind also finanzielle Transaktionen.
- Der Besitzer von Einheiten der Kryptowährung wird durch einen sogenannten Public Key (öffentlichen Schlüssel) bestimmt.

- In diesem Kurs verstehen wir unter einer Kryptowährung eine Blockchain, die auf *finanzielle Transaktionen* spezialisiert ist.
- Die Register-Einträge in den Blöcken sind also finanzielle Transaktionen.
- Der Besitzer von Einheiten der Kryptowährung wird durch einen sogenannten Public Key (öffentlichen Schlüssel) bestimmt.
- Jeder, der den zugehörigen Secret/Private Key (geheimen Schlüssel) kennt, kann über die Währung verfügen.

Bei einer Kryptowährung gibt es zusätzlich zu dem generischen Blockchain-Protokoll noch weitere Mechanismen:

Bei einer Kryptowährung gibt es zusätzlich zu dem generischen Blockchain-Protokoll noch weitere Mechanismen:

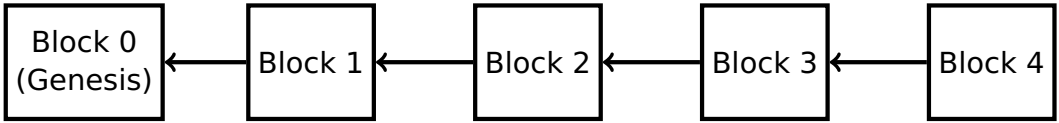
- Zum Regulieren der Erzeugung neuer Einheiten der Währung.

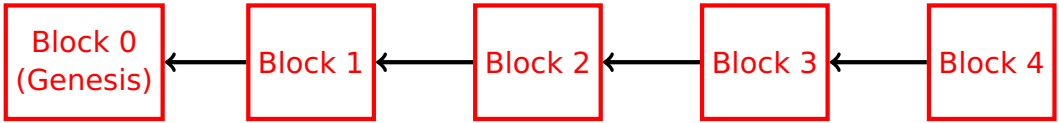
Bei einer Kryptowährung gibt es zusätzlich zu dem generischen Blockchain-Protokoll noch weitere Mechanismen:

- Zum Regulieren der Erzeugung neuer Einheiten der Währung.
- Transaktionsgebühren und Belohnungen wir das Erzeugen neuer Blocks.

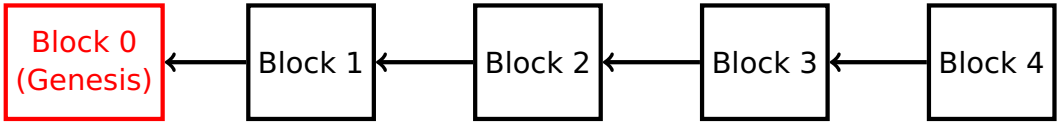
Bei einer Kryptowährung gibt es zusätzlich zu dem generischen Blockchain-Protokoll noch weitere Mechanismen:

- Zum Regulieren der Erzeugung neuer Einheiten der Währung.
- Transaktionsgebühren und Belohnungen wir das Erzeugen neuer Blocks.
- Smart Contracts (intelligente Verträge).


Block 0
(Genesis)
Block 1
Block 2
Block 3
Block 4



Jeder Block enthält eine Liste von Register-Einträgen (z.B. finanziellen Transaktionen) und einen Link zum vorhergehenden Block, so dass alle Einträge in Reihenfolge gebracht werden: Zunächst der Reihe nach die Einträge in Block 0, dann der Reihe nach die Einträge in Block 1 usw.



Jeder Block enthält eine Liste von Register-Einträgen (z.B. finanziellen Transaktionen) und einen Link zum vorhergehenden Block, so dass alle Einträge in Reihenfolge gebracht werden: Zunächst der Reihe nach die Einträge in Block 0, dann der Reihe nach die Einträge in Block 1 usw.

Der erste Block heißt Genesis Block. Er hat keinen Vorgänger, ist öffentlich bekannt und enthält den Anfangsstatus.

- Wie kann man die Fälschung von einzelnen Register-Einträgen verhindern?
  - Es wäre z.B. fatal für eine Kryptowährung, wenn Überweisungen gefälscht oder geändert werden könnten (Betrag, Empfänger,...).

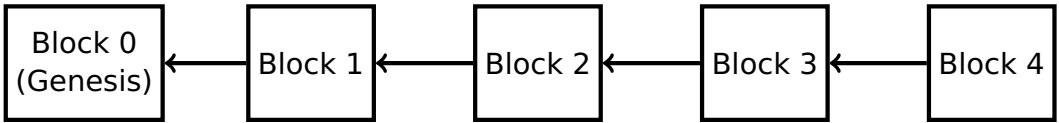
- Wie kann man die Fälschung von einzelnen Register-Einträgen verhindern?
  - Es wäre z.B. fatal für eine Kryptowährung, wenn Überweisungen gefälscht oder geändert werden könnten (Betrag, Empfänger,...).
- Wie schützt man Blöcke vor Manipulation?
  - Blöcke dürfen nicht gelöscht, durch andere ersetzt oder umsortiert werden, selbst wenn die individuellen Einträge alle authentisch sind.
  - Für Grundbucheinträge wäre es eine Katastrophe für den Betroffenen, wenn zwei Einträge für dasselbe Grundstück vertauscht würden...

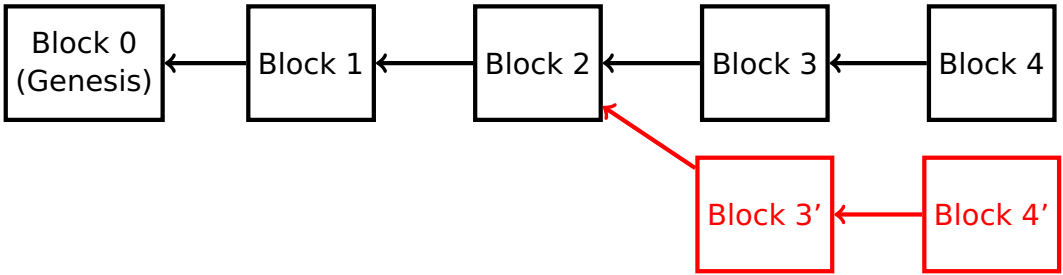
- Wie kann man die Fälschung von einzelnen Register-Einträgen verhindern?
  - Es wäre z.B. fatal für eine Kryptowährung, wenn Überweisungen gefälscht oder geändert werden könnten (Betrag, Empfänger,...).
- Wie schützt man Blöcke vor Manipulation?
  - Blöcke dürfen nicht gelöscht, durch andere ersetzt oder umsortiert werden, selbst wenn die individuellen Einträge alle authentisch sind.
  - Für Grundbucheinträge wäre es eine Katastrophe für den Betroffenen, wenn zwei Einträge für dasselbe Grundstück vertauscht würden...
- Antworten auf diese Fragen liefert die Kryptografie in der Form von digitale Unterschriften und kryptografische Hashfunktionen, die wir später genauer erklären werden.

- Jeder Register-Eintrag ist mit der digitalen Unterschrift einer autorisierten Partei versehen (z.B. mit der Unterschrift desjenigen, der eine Überweisung veranlasst).
- Jeder Block mit all seinen Einträgen wird von seinem Erzeuger digital unterschrieben.
- Wenn wir später über digitale Unterschriften sprechen, werden wir sehen, wie dies technisch möglich ist.

- Sagen wir, Alice überweist Bob in einer Transaktion 100 ₿ und unterschriebt diese ordnungsgemäß. Eine Möglichkeit der Fälschung für Bob wäre es, eine zweite Kopie dieser Transaktion in einen Block einzufügen, so dass Alice ihm nun 200 ₿ bezahlen muss.
- Wir werden später sehen, dass digitale Unterschriften — im Gegensatz zu gewöhnlichen Unterschriften — von dem Dokument, das sie unterschreiben, abhängen. Aber in diesem Beispiel ist das Dokument — Alices Überweisung — dasselbe, so dass uns dies hier nichts hilft.
- Um diesen Betrug zu behindern, müssen Transaktionen unwiederholbar gemacht werden, z,B. indem sie mit einer fortlaufenden Transaktionsnummer versehen werden.

- Der Link eines Blocks zu seinem Vorgänger wird durch den Hash des Vorgängers gegeben.
- Aus den Eigenschaften von kryptografischen Hashfunktionen, die wir später studieren werden, folgt, dass die das nachträgliche Löschen, Einfügen oder Ändern von Blöcken unmöglich macht.
- Das Ändern eines Blocks (bzw. eines Register-Eintrages in einem Block) würde den Hash verändern, so dass der Link ungültig würde.
- Das Löschen (oder Einfügen) eines Blocks würde das Ändern von Links erfordern, die aber Teil des Blocks sind, also auch den Hash des Blocks verändern würden.


Block 0
(Genesis)
Block 1
Block 2
Block 3
Block 4



Nichts in der Blockchain-Datenstruktur garantiert die Form einer Chain (Kette). Wenn wir Forks (Gabelungen) verhindern wollen, brauchen wir mehr als Kryptografie.

Warum sind Forks ein Problem?

- Die lineare Anordnung aller Register-Einträge in der Blockchain ist absolut essentiell.
- Forks zerstören diese lineare Anordnung.
- Forks in einer Kryptowährung bedeuten konkret, dass die Gefahr von double spending (mehrfachem Ausgeben) besteht.

Warum sind Forks ein Problem?

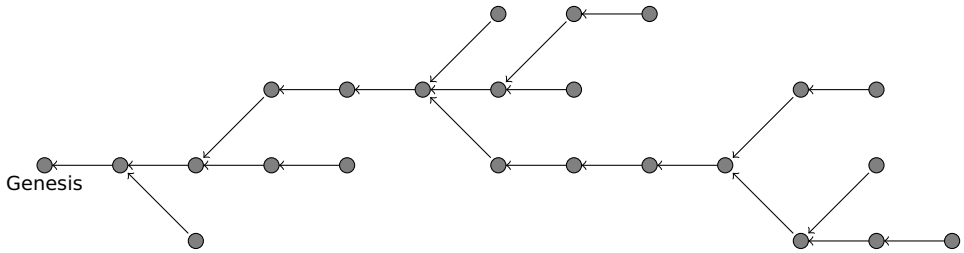
- Die lineare Anordnung aller Register-Einträge in der Blockchain ist absolut essentiell.
- Forks zerstören diese lineare Anordnung.
- Forks in einer Kryptowährung bedeuten konkret, dass die Gefahr von double spending (mehrfachem Ausgeben) besteht.
- Digitale Unterschriften und kryptografische Hashfunktionen sind schon seit den 1970er Jahren bekannt. Der Grund, dass es Kryptowährungen erst seit 2009 gibt, ist der, dass das Double-Spending-Problem erst dann gelöst wurde.

- Die lineare Anordnung aller Register-Einträge in der Blockchain ist absolut essentiell.
- Forks zerstören diese lineare Anordnung.
- Forks in einer Kryptowährung bedeuten konkret, dass die Gefahr von double spending (mehrfachem Ausgeben) besteht.
- Digitale Unterschriften und kryptografische Hashfunktionen sind schon seit den 1970er Jahren bekannt. Der Grund, dass es Kryptowährungen erst seit 2009 gibt, ist der, dass das Double-Spending-Problem erst dann gelöst wurde.

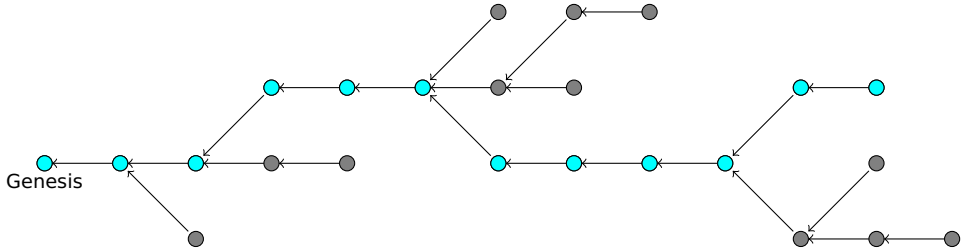
Double Spending

Nehmen wir an, Alice besitzt 100 ฿. Block 3 könnte einen Eintrag enthalten, in dem sie dieses Geld an Bob überweist, und Block 3’ könnte einen Eintrag enthalten, in dem sie dasselbe Geld an Charlie überweist. Beide Einträge sind ordnungsgemäß digital von Alice unterschrieben. — Wem gehören die 100 ฿?

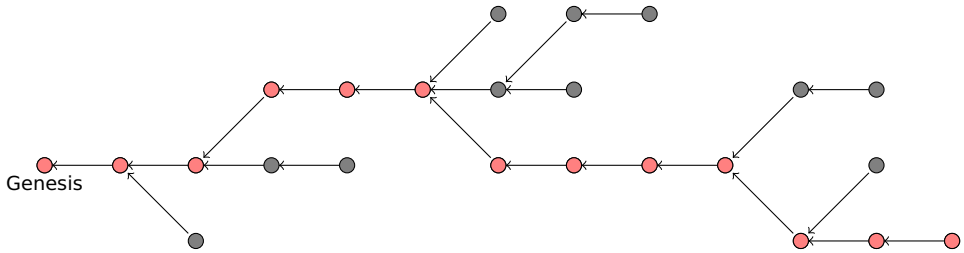
- Selbst ohne Bösartigkeit können Forks nie vollständig verhindert werden (z.B. wegen Netzproblemen).
- Ein Konsens-Protokoll (consensus protocol) verhindert, dass Forks *zu tief* werden.
- Die Common Prefix Property (Eigenschaft übereinstimmender Präfixe) sollte gelten: Nachdem ein Knoten die jüngsten k Blöcke entfernt hat (für geeignetes k), ist seine lokale Blockchain ein Präfix der lokalen Blockchains aller anderen Knoten. Grob gesagt bedeutet dies, dass Inkonsistenzen zwischen Knoten nur in der jüngsten Vergangenheit auftreten können und durch hinreichend langes Abwarten aufgelöst werden.
- Idee: Das Recht, neue Blöcke zu erzeugen, wird mit einem Gut verknüpft, das mehrheitlich von ehrlichen Parteien kontrolliert wird.
- Für Bitcoin (Proof of Work) ist dieses Gut Rechenleistung.
- Für Cardano (Proof of Stake) ist es die Kryptowährung selbst.



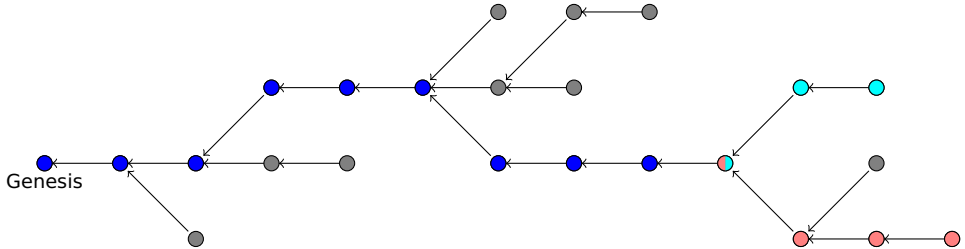
In dem Bild sind die grauen Blöcke alle Blöcke einer Beispielblockchain, die bisher erzeugt wurden. Beachten Sie, dass eventuell nicht alle Blöcke allen Knoten bekannt sind.



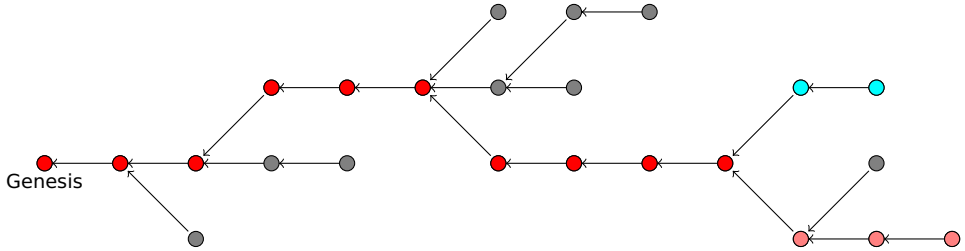
Ein Knoten hat die türkisen Blöcke als seine lokale Kopie der Blockchain.



Ein *anderer* Knoten hat die rosa Blöcke als *seine* lokale Kopie der Blockchain.



Wenn der *erste* Knoten die jüngsten drei Blöcke ignoriert, bleiben ihm die blauen Blöcke, und diese sind tatsächlich ein Präfix der rosa Kette.



Wenn der *zweite* Knoten die jüngsten drei Knoten ignoriert, bleiben ihm die roten Blöcke, und diese sind tatsächlich ein Präfix der türkisen Kette.

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

- Er speichert eine lokale Kopie der Blockchain.

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

- Er speichert eine lokale Kopie der Blockchain.
- Er ist in Kontakt mit anderen Knoten (Peers), mit denen er “Neuigkeiten” austauscht.

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

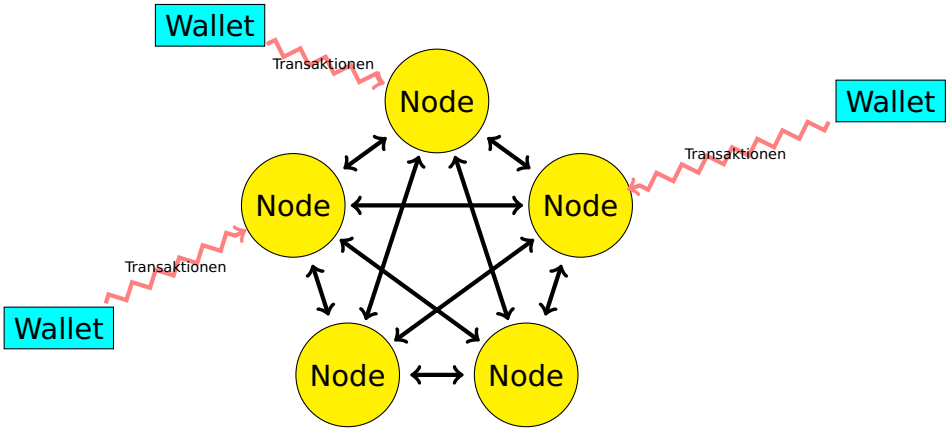
- Er speichert eine lokale Kopie der Blockchain.
- Er ist in Kontakt mit anderen Knoten (Peers), mit denen er “Neuigkeiten” austauscht.
- Wenn er einen neuen Eintrag erhält (von außen oder einem Peer), prüft er ihn auf Gültigkeit, teilt ihn mit seinen Peers und merkt ihn sich in seinem Mempool.

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

- Er speichert eine lokale Kopie der Blockchain.
- Er ist in Kontakt mit anderen Knoten (Peers), mit denen er “Neuigkeiten” austauscht.
- Wenn er einen neuen Eintrag erhält (von außen oder einem Peer), prüft er ihn auf Gültigkeit, teilt ihn mit seinen Peers und merkt ihn sich in seinem Mempool.
- Wenn er neue Blöcke von seinen Peers bekommt, teilt ihn mit seinen Peers und baut ihn in seine Kopie der Blockchain ein.

Ein Node (Knoten) in einer Blockchain hat die folgenden Aufgaben:

- Er speichert eine lokale Kopie der Blockchain.
- Er ist in Kontakt mit anderen Knoten (Peers), mit denen er “Neuigkeiten” austauscht.
- Wenn er einen neuen Eintrag erhält (von außen oder einem Peer), prüft er ihn auf Gültigkeit, teilt ihn mit seinen Peers und merkt ihn sich in seinem Mempool.
- Wenn er neue Blöcke von seinen Peers bekommt, teilt ihn mit seinen Peers und baut ihn in seine Kopie der Blockchain ein.
- Wenn das benutzte Konsens-Protokoll ihm das Recht dazu gibt, erzeugt er einen neuen Block, in den er möglichst viele Einträge seines Mempools einbindet und den er dann mit seinen Peers teilt.


Wallet
Transaktionen
Node
Wallet
Transaktionen
Node
Node
Transaktionen
Wallet
Node
Node

- Der Erfolg, die Stabilität und die Sicherheit einer öffentlichen Blockchain beruhen darauf, dass hinreichend viele Menschen (Rechen-)Zeit und Hardware zur Verfügung stellen, um die Blockchain zu unterhalten.
  - Register-Einträge und Blöcke müssen auf ihre Gültigkeit hin überprüft werden.
  - Neue Register-Einträge müssen in neuen Blöcken gesammelt werden, die an die Kette angehängt werden.
- Dazu bedarf es — ideeller oder finanzieller — Anreize (Incentives).
- Bei Bitcoin, Ethereum und Cardano wird das Erstellen neuer Blöcke mit Kryptowährung belohnt.
- Bei Cardano, dem ersten Proof of Stake System, wird man auch belohnt, wenn man das Recht auf Blockerzeugung an einen “Pool” abtritt.
- Es ist wichtig, dass die Anreize so gewählt werden, dass es in jedermanns persönlichem Interesse ist, das zu tun, was für die Blockchain das Beste ist.

- Dezentralisierung ist eine wesentliche Eigenschaft jeder Blockchain.
- Die Knoten sind in einem Peer-to-Peer (P2P) Netzwerk verbunden und alle gleichberechtigt — es gibt keinen “zentralen Knoten”.
- Als Konsequenz gibt es keinen “Single point of failure” (einzige Fehlstelle), der angegriffen werden kann, um die Blockchain zu sabotieren.
- Dezentralisierung bedeutet auch, insbesondere für Kryptowährungen, dass traditionelle “Zwischeninstanzen” (Banken) nicht länger nötig sind, was schnellere und günstigere Überweisungen ermöglicht.
- Dezentrale Blockchains sind trustless (erfordern kein Vertrauen), d.h. Sicherheit hängt nicht von einer zentralen Instanz ab, der man wohl oder übel vertrauen muss.

Zensur-Resistenz

- Eine wichtige Konsequenz der Dezentralisierung ist die Zensur-Resistenz (censorship resistance) von Blockchains.
- Da alle Daten auf viele Knoten verteilt sind, ist es praktisch unmöglich, Daten zu löschen.
- Da Transaktionen an viele Knoten gesendet und von diesen in einen Block eingebaut werden können, ist es ebenso unmöglich, unliebsame Transaktionen zu verhindern.
- Darüber hinaus ist die nachträgliche Manipulation von Daten aufgrund der Blockchain-Datenstruktur unmöglich.

- Eine wichtige Konsequenz der Dezentralisierung ist die Zensur-Resistenz (censorship resistance) von Blockchains.
- Da alle Daten auf viele Knoten verteilt sind, ist es praktisch unmöglich, Daten zu löschen.
- Da Transaktionen an viele Knoten gesendet und von diesen in einen Block eingebaut werden können, ist es ebenso unmöglich, unliebsame Transaktionen zu verhindern.
- Darüber hinaus ist die nachträgliche Manipulation von Daten aufgrund der Blockchain-Datenstruktur unmöglich.
- Ob dies in allen Fällen wünschenswert ist, ist eine andere Frage, die von der Gesellschaft als Ganzes diskutiert werden muss.

- In einer öffentliche (public) Blockchain wie Bitcoin, Ethereum oder Cardano kann jeder, der Interesse hat, einen Knoten erzeugen und dem Netzwerk beitreten.
- In einer privaten (private) Blockchain ist der Zugang beschränkt und wird zum Beispiel von einer Firma kontrolliert.
- Es ist umstritten, ob private Blockchains den Namen “Blockchain” verdienen.
  - Befürworter sind der Meinung, dass der Begriff “Blockchain” die *Technologie* und *Datenstruktur* beschreibt.
  - Kritiker halten Eigenschaften wie no single point of failure und censorship resistance für unabdingbar. Für sie ist eine private Blockchain nur eine “problematische Datenbank” (Nikolai Hampton, Computerworld).

- Einträge in einer Blockchain, insbesondere Überweisungen in einer Kryptowährung, sind nicht an die Identität (Identity) von Personen geknüpft, sondern benutzen stattdessen Öffentliche Schlüssel (Public Keys) — mehr dazu später!
- Obwohl alle Transaktionen bei den meisten Kryptowährungen öffentlich einsehbar sind, ist es daher nicht offensichtlich, wer wem wieviel überwiesen hat.
- Andererseits gibt es statistische Verfahren, die es oft ermöglichen, Schlüssel und Namen einander zuzuordnen und Geldflüsse zu verfolgen.
- Es gibt allerdings auch Kryptowährungen wie Monero, die hochentwickelte kryptografische Verfahren benutzen, um bei Überweisungen Absender, Empfänger und Beträge zu verschleiern.

- Einträge in einer Blockchain, insbesondere Überweisungen in einer Kryptowährung, sind nicht an die Identität (Identity) von Personen geknüpft, sondern benutzen stattdessen Öffentliche Schlüssel (Public Keys) — mehr dazu später!
- Obwohl alle Transaktionen bei den meisten Kryptowährungen öffentlich einsehbar sind, ist es daher nicht offensichtlich, wer wem wieviel überwiesen hat.
- Andererseits gibt es statistische Verfahren, die es oft ermöglichen, Schlüssel und Namen einander zuzuordnen und Geldflüsse zu verfolgen.
- Es gibt allerdings auch Kryptowährungen wie Monero, die hochentwickelte kryptografische Verfahren benutzen, um bei Überweisungen Absender, Empfänger und Beträge zu verschleiern.
- Wieder ist die Frage, ob Anonymität immer wünschenswert ist oder nicht, eine Frage, die in der Gesellschaft diskutiert werden sollte.

- Die prominenteste Anwendung von Blockchain-Technologie ist ohne Zweifel die Erzeugung einer Kryptowährung.
- Kryptowährungen implementieren ein dezentralisiertes Zahlungssystem, unabhängig von Banken, das günstige und schnelle Überweisungen über alle Grenzen hinweg ermöglicht.
- In Kombination mit Smart Contracts (mehr dazu später) können komplexe finanzielle Verträge automatisch abgewickelt und durchgesetzt werden, ohne sich auf Banken oder Gerichte verlassen zu müssen.
- Dabei ist es eine große Hoffnung, dass diese Technologie insbesondere der Dritten Welt zugute kommen wird, in der ein funktionierendes System von traditionellen Banken oft fehlt.
- Generell steht hinter Kryptowährungen oft der Wunsch, Menschen volle Kontrolle über ihr Vermögen (zurück) zu geben.

- Ein Nachteil von bestehenden Kryptowährungen ist ihr stark fluktuierender Wert.
- Es gibt Verfahren, den Wert einer Kryptowährung an den Wert einer “echten” Währung zu koppeln; das Ergebnis ist eine sogenannte Stable Coin (stabile Währung).
- Wenn zum Beispiel die europäische Zentralbank eine “Euro Stable Coin” erzeugen wollte, könnte Sie Einheiten der Kryptowährung im Austausch gegen eine gleiche Menge von Euros “drucken”: Alice gibt der Bank 10 Euro und bekommt 10 Crypto Euro dafür, zusammen mit der Garantie, ihre Crypto Euro jederzeit wieder gegen Euro tauschen zu können.
- Stable Coins verbinden die Vorteile von etablierten Währungen (Stabilität) mit den Vorteilen einer Kryptowährung (schnelle, günstige und sichere Überweisungen).

- Die Anwendung von Blockchain-Technologie auf Lieferketten (Supply Chains) ist äußerst vielversprechend.
- Durch entsprechende Einträge in der Blockchain können alle Schritte vom Erzeuger über Transporteure und Zwischenhändler bis zum Endverbraucher nachvollziehbar und öffentlich dokumentiert werden.

- Die Anwendung von Blockchain-Technologie auf Lieferketten (Supply Chains) ist äußerst vielversprechend.
- Durch entsprechende Einträge in der Blockchain können alle Schritte vom Erzeuger über Transporteure und Zwischenhändler bis zum Endverbraucher nachvollziehbar und öffentlich dokumentiert werden.
- Erzeugern kann damit geholfen werden, einen fairen Preis für ihre Produkte zu erzielen.
  - BeefChain ist ein Unternehmen, das Rinderzüchtern in Wyoming helfen will, faire Preise für ihr Rindfleisch zu erzielen, das von im Freien grasenden Rindern stammt.
  - Die äthiopische Regierung arbeitet an einem Projekt, das Kaffee-Bauern mittels Blockchain-Technologie helfen soll, fairere Preise zu erzielen und vor Risiken wie schlechtem Wetter und schwankenden Preisen besser geschützt zu sein.

- Die Anwendung von Blockchain-Technologie auf Lieferketten (Supply Chains) ist äußerst vielversprechend.
- Durch entsprechende Einträge in der Blockchain können alle Schritte vom Erzeuger über Transporteure und Zwischenhändler bis zum Endverbraucher nachvollziehbar und öffentlich dokumentiert werden.
- Erzeugern kann damit geholfen werden, einen fairen Preis für ihre Produkte zu erzielen.
  - BeefChain ist ein Unternehmen, das Rinderzüchtern in Wyoming helfen will, faire Preise für ihr Rindfleisch zu erzielen, das von im Freien grasenden Rindern stammt.
  - Die äthiopische Regierung arbeitet an einem Projekt, das Kaffee-Bauern mittels Blockchain-Technologie helfen soll, fairere Preise zu erzielen und vor Risiken wie schlechtem Wetter und schwankenden Preisen besser geschützt zu sein.
- Fälschungen (zum Beispiel gefälschte Arzneimittel) könnten rechtzeitig identifiziert werden.

- Immobilien, aber auch andere teure Objekte wie Luxusautos, können tokenisiert (tokenized) werden, d.h. sie werden mit einem sogenannten Token auf der Blockchain assoziiert.
- Mit diesen Tokens kann dann — stellvertretend für die realen Objekte — auf der Blockchain gehandelt werden.
- Darüberhinaus sind auch Grundbucheinträge auf der Blockchain ein wichtiger Anwendungsfall, was insbesondere für Länder mit hoher Korruption oder Länder, die von Kriegen, Bürgerkriegen oder Naturkatastrophen betroffen sind, bedeutsam wäre.
- Einträge auf der Blockchain sind vor Manipulation und Vernichtung (durch Feuer oder Ähnliches) geschützt.

- Eine interessante und originelle Idee zur Anwendung von Blockchain-Technologie ist es, wilden Tieren (wie Elefanten) zu helfen.
- Jedes Tier würde mit einem Chip versehen, der dem Tier eine Identität auf der Blockchain verleiht und es mit Geld in Form von Kryptowährung ausstattet.
- Das Tier könnte dann für Dienstleistungen bezahlen, es könnte zum Beispiel Dorfbewohner dafür entlohnen, Futter oder Weideland zur Verfügung zu stellen.
- Da dieses Geld mit dem Leben und Wohlergehen des Tieres verknüpft ist, hätten Menschen ein finanzielles Interesse daran, das Tier zu schützen.

- Die Tokenisierung, die wir beim Beispiel von Immobilien erwähnt haben, hat auch Anwendungen für Computerspiele.
- Gewisse Gegenstände aus der Spielwelt (zum Beispiel Rüstungen oder Schwerter in Rollenspielen) können tokenisiert und auf der Blockchain gehandelt werden.
- Dies hat die weiteren Vorteile, dass der Besitzer die Gegenstände wirklich besitzt (er hängt nicht vom Server des Spieleherstellers ab) und das es Interoperabilität ermöglicht — andere Spielehersteller könnten dieselben Gegenstände in ihren eigenen Spielen verwenden.
- Prominentes Beispiel sind die Crypto Kitties auf Ethereum, die Zeitweise 30% aller Transaktionen auf Ethereum ausmachten.
- Anstelle von “einzigartigen” Gegenständen können auch Spiel-interne Währungen (Goldmünzen. . .) tokenisiert werden.
- Tokens, die an einen einzigen Gegenstand geknüpft sind, heißen non-fungible Tokens. Tokens, die austauschbar sind (wie Geldscheine) werden hingegen fungible Tokens genannt.

Hinweis

Diese Publikation wurde im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Bund- Länder- Wettbewerbs “Aufstieg durch Bildung: offene Hochschulen” erstellt. Die in dieser Publikation dargelegten Ergebnisse und Interpretationen liegen in der alleinigen Verantwortung der Autor/innen.