INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG

ITA-DOSSIER

Blockchain — Transaktionen dezentralisieren

In Kürze

- Blockchain ist eine dezentral organisierte Datenbank, die eine ständig wachsende Liste von Transaktionen archiviert und verwaltet.
- Alle Informationen über Transaktionen werden permanent in einer Datenbank gespeichert, die an allen Knotenpunkten des Netzwerkes parallel vorliegt.
- Blockchain bietet Autonomie für Einzelpersonen abseits von zentralen „Zwischenhändlern“ wie Behörden und Banken.
- Diese Dezentralisierung reduziert jedoch die derzeitigen Formen der regulatorischen Kontrolle.
- Mögliche negative soziale und ökonomische Folgen werden weniger vorhersehbar und handhabbar.

Worum geht es?

Die Blockchain-Technologie ist eine dezentral organisierte Transaktionsdatenbank. Sie stützt sich auf die beiden Informatikbereiche Verteilte Systeme und Kryptographie, welche seit den 1970er-Jahren von WissenschafterInnen und AktivistInnen kontinuierlich entwickelt wurden. Die Blockchain-Technologie wurde 2008 erstmals in der Krypto-Währung Bitcoin weit verbreitet eingesetzt. Informationen zu jeder Transaktion (z.B. Austausch von Krypto-Geld oder Vertragserstellung) werden von „Minern“ (Computern, die die Knotenpunkte im Netzwerk bilden) in einem „Block“ (Datenbündel) aufgezeichnet, der mit einer Kette von bestehenden und neuen Blöcken verknüpft ist. Blockchains werden in der Regel als Peer-to-Peer-Netzwerk (P2P) verwaltet. Das Netzwerk folgt einem Protokoll zur Erstellung neuer Blöcke. Die Daten in jedem Block können nicht geändert werden, ohne dass alle Daten in allen verknüpften Blöcken geändert werden müssten. Durch die Verwaltung von Transaktionsdaten in Blockketten über ein Netzwerk kann die Verwaltung vollständig dezentralisiert werden, so dass Zwischenhändler oder Organisationen wie zentrale Behörden nicht mehr nötig sind. Institutionen, wie Banken oder Behörden werden oft als ineffizient und bürokratisch, was deren Prozesse verlangsamt, angesehen. Zwischenhändler können zu großen und mächtigen Monopolen werden, deren intransparente Prozesse Misstrauen fördern können. Durch Verwaltung und Verifizierung durch ein Netzwerk, in dem alle Informationen für alle Beteiligten jederzeit verfügbar sind, schafft die Blockchain Vertrauen.

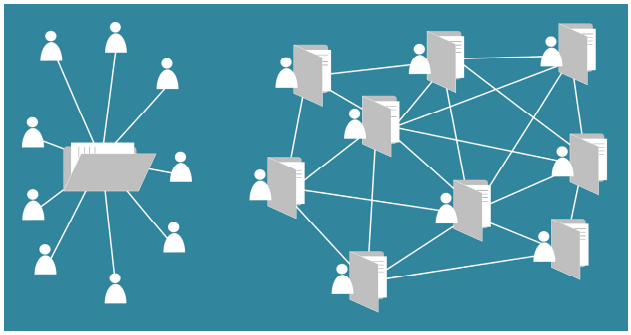


Illustration: ITA-NG

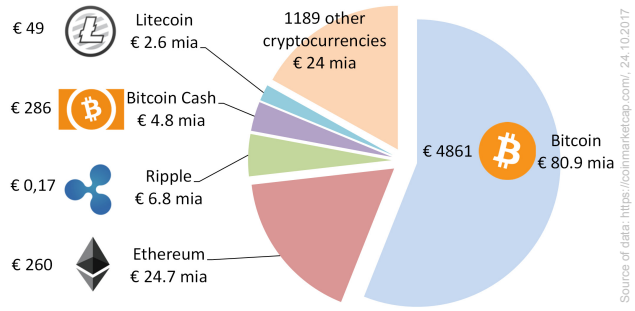
Zentralisiert vs. verteilt: Die Blockchain basiert auf einem Peer-to-Peer-Netzwerk ohne Zwischenhändler

Die Einsatzmöglichkeiten von Blockchain-Plattformen sind nahezu unbegrenzt, da in jeder Branche die Notwendigkeit besteht, Transaktionen sicher zu erfassen. Die bekannteste Anwendung sind Krypto-Währungen. Blockchains werden aber auch in der öffentlichen Verwaltung, z.B. bei der Stimmenregistrierung oder der Steuereinhebung, verwendet. Außerdem werden Blockchains bei „intelligenten Verträgen“ genutzt, um digitale Inhalte und andere geistige Eigentumsrechte zu schützen. Sie finden aber auch Anwendung bei Registrierungsvorgängen, in intelligenten Stromnetzen und Energiemärkten oder auch in globalen Lieferketten.

Vorteile: Kontinuierliches Vergleichen der Daten im Netzwerk sorgt für Transparenz, Sicherheit und Nachprüfbarkeit der Transaktionen. Transaktionskosten können effizienter und kostengünstig gestaltet werden. Die Daten sind geschützt – z.B. sind Benutzernamen verschlüsselt – Beträge und Wege von Transaktionen werden jedoch permanent nachverfolgt.
Nachteile: Blockchains können potenziell negative Folgen haben, die ohne Regulierung eskalieren können. Dezentralisierung bedeutet nicht zwingend, dass es keine Zwischenhändler und Hierarchien gibt. Die Blockchain-Technologie leidet noch immer unter Defiziten, wie z.B. dem Bedarf an enormer Rechenleistung mit sehr hohem Energiebedarf. Darüber hinaus können Zwischenhändler sehr hilfreich sein, wenn KundInnen Fragen oder Probleme bei Transaktionen haben. Wen würde man in einem vollständig dezentralen Netz anrufen?

Bitcoin und „smarte“ Verträge

Bitcoin – die populärste von unzähligen digitalen Krypto-Währungen – ist ein Peer-to-Peer-Bezahlsystem, das auf der Blockchain basiert. Bitcoin-BesitzerInnen setzen ihre verschlüsselten digitalen Signaturen bei Transaktionen ein. Solche Signaturen sind einfach zu erzeugen und zu verifizieren, nahezu fälschungssicher und schützen die Identität einer Person vollständig. Bitcoin-Transaktionen werden in einem verteilten Register aufgezeichnet, das Käufe und Verkäufe protokolliert und sich mit allen Registern im System abgleicht. Sogenannte Miner überprüfen anhand einer komplexen Rechenoperation die Legitimität jeder neuen Transaktion, bevor sie sie einem Block hinzufügen. Damit das Netz den neuen Block akzeptiert und in die verteilte Datenbank aufnimmt, muss der Miner einen komplexen mathematischen Beweis lösen, um einen Schlüssel zu finden, der über eine nicht umkehrbare Einwegfunktion generiert wurde und im letzten Block der Kette hinterlegt ist. Das nimmt Rechenzeit in Anspruch und bremst das gesamte System auf wenige Transaktionen pro Sekunde. Auch wenn der Wert von Bitcoins stark schwankt und sie für ihren Einsatz auf dem Schwarzmarkt kritisiert werden, hat sich gezeigt, dass die Blockchain-Technologie funktioniert.



Große Krypto-Währungen: Preise und Marktkapitalisierungen

Die Verbreitung der Blockchain-Technologie nimmt rasant zu. Ein neuer vielversprechender Weg ist ihr Einsatz bei der Erstellung von intelligenten (digitalen) Verträgen. Solche Verträge können, ähnlich wie Computerprogramme, klare Rollen definieren und spezifizieren, was unter verschiedenen Bedingungen geschehen wird. Der Vertrag kann mit einer digitalen Signatur unterschrieben werden, die dauerhaft, sichtbar, überprüfbar und unveränderbar ist. Jeder Vertrag kann Eventualitäten enthalten, falls bei einer Transaktion etwas schief geht. Damit entfällt sowohl die Notwendigkeit einer dritten Partei als auch dass sich beide Parteien der Transaktion gegenseitig vertrauen. Ethereum ist die derzeit bekannteste Open-Source- und Blockchain-basierte Plattform für solche Verträge. Weitere funktionierende Anwendungen sind in diesem sich dynamisch entwickelnden Bereich noch in Entwicklung.

Was tun?

Österreich sollte deutliche, aber maßvolle Schritte in der Entwicklung der Blockchain-Technologie unternehmen. Politische EntscheidungsträgerInnen könnten dabei folgende Punkte berücksichtigen:

- **Gesellschaftliche Bedürfnisse:** Risiken für VerbraucherInnen müssen verstanden und deren Schutz aufrechterhalten werden. Zunächst müssen Erkenntnisse darüber gewonnen werden, wie sichergestellt werden kann, dass illegale Aktivitäten vermieden werden und die Einhaltung der geltenden österreichischen und EU-Vorschriften gewährleistet wird. Die Technologieentwicklung sollte inter- und transdisziplinär sein, etwa durch eine enge Zusammenarbeit von ProgrammiererInnen, AnwenderInnen und Personen, die mit Inhalt und Kontext, in dem die Blockchain genutzt wird, vertraut sind.
- **Ökonomische Voraussetzungen:** Start-ups und Innovationspotenziale sollten genutzt, Investitionen in Pilot- und Demonstrationsprojekte gefördert werden, um das Potential der Blockchain-Technologie in verschiedenen Sektoren zu erforschen und zu entwickeln. Fähigkeiten und Training von Software-EntwicklerInnen müssen verbessert werden, damit sie den wachsenden Anforderungen gerecht werden können.
- **Regulierung:** Blockchain-Technologien werfen spezifische Fragen zu Rechenschaftspflicht und Verantwortung auf, wenn Probleme auftreten. Institutionen werden unterschiedliche, aber wichtige Aufgaben wahrnehmen müssen, um Robustheit, Verlässlichkeit und langfristige Planbarkeit zu gewährleisten.

Zum Weiterlesen

Boucher P. et al. (2017) How blockchain technology could change our lives. STOA – Science and Technology Options Assessment, EPRS – European Parliamentary Research Service

europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

Kontakt

Tanja Sinozic

E-mail: tamail@oeaw.ac.at

Telefon: +43(1)51581-6582

IMPRESSUM: Medieninhaber: Österreichische Akademie der Wissenschaften; Juristische Person öffentlichen Rechts (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Wien; Herausgeber: Institut für Technikfolgen-Abschätzung (ITA); Strohgasse 45/5, A-1030 Wien; www.oeaw.ac.at/ita | Erscheinungsweise: Die ITA-Dossiers erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des ITA. Die Dossiers werden in kleiner Auflage gedruckt und open access über das Portal „epub.oeaw“ zur Verfügung gestellt: epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960

ITA-Dossier Nr. 30, November 2017, epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier030.pdf | Koautor: Niklas Gudowsky