S I D

Society for International Development

Chapter Bonn

Vorlese zum epf 128: Potentiale der Blockchain Technologie für eine armutsorientierte nachhaltige Entwicklung

Jan Ohnesorge

I Definitionen

Blockchain

Eine Blockchain[1][2][3] (auch *Block Chain,*[4][5] englisch für *Blockkette*) ist eine kontinuierlich erweiterbare Liste von Datensätzen, genannt „Blöcke“, welche mittels kryptographischer Verfahren miteinander verkettet sind.[1][6] Jeder Block enthält dabei typischerweise einen kryptographisch sicheren Hash (Streuwert) des vorhergehenden Blocks,[6] einen Zeitstempel und Transaktionsdaten.[7]

Der Begriff *Blockchain* wird allgemeiner für ein Konzept genutzt, mit dem ein Buchführungssystem dezentral geführt werden kann und dennoch ein Konsens über den *richtigen* Zustand der Buchführung erzielt wird, auch wenn viele Teilnehmer an der Buchführung beteiligt sind. Dieses Konzept wird als Distributed-Ledger-Technologie(DLT) bezeichnet.[8] Worüber in dem Buchführungssystem Buch geführt wird, ist für den Begriff der Blockchain unerheblich. Entscheidend ist, dass spätere Transaktionen auf früheren Transaktionen aufbauen und diese als richtig bestätigen, indem sie die Kenntnis der früheren Transaktionen beweisen. Damit wird es unmöglich gemacht, Existenz oder Inhalt der früheren Transaktionen zu manipulieren oder zu tilgen, ohne gleichzeitig alle späteren Transaktionen ebenfalls zu zerstören, die die früheren bestätigt haben. Andere Teilnehmer der dezentralen Buchführung, die noch Kenntnis der späteren Transaktionen haben, würden eine manipulierte Kopie der Blockchain ganz einfach daran erkennen, dass sie Inkonsistenzen in den Berechnungen aufweist.

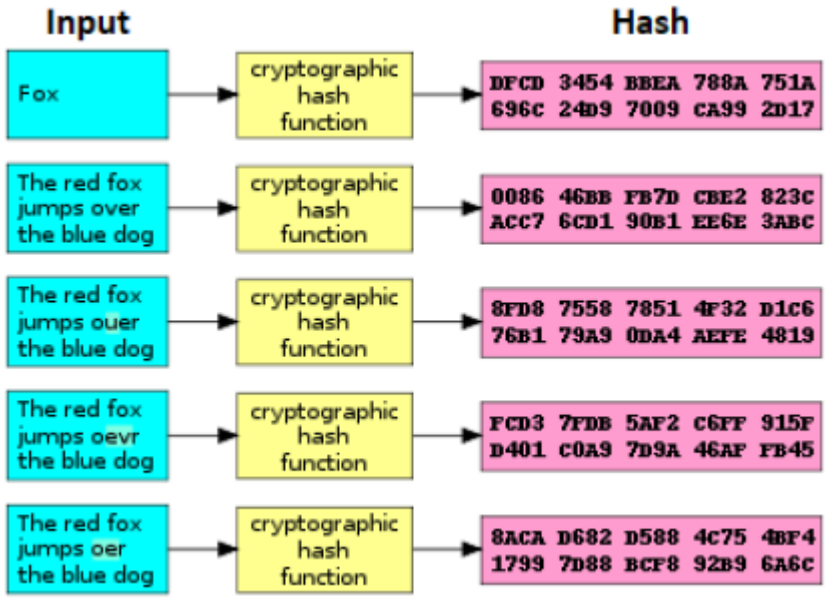
Das Verfahren der kryptografischen Verkettung in einem dezentral geführten Buchführungssystem ist die technische Basis für Kryptowährungen, kann aber

darüber hinaus in verteilten Systemen zur Verbesserung bzw. Vereinfachung der Transaktionssicherheit im Vergleich zu zentralen Systemen beitragen. […]

Quelle: https://de.wikipedia.org/wiki/Blockchain

Hash

Ein Hash ist ein Fingerabdruck eines Datensatzes. Eine Hashfunktion wandelt einen beliebig langen Input in einen Hash um, der eine festgelegte Länge hat. Es ist leicht überprüfbar, dass ein Hash einen bestimmten Datensatz korrekt beschreibt. Jedoch lässt sich aus dem Hash nicht der Input rekonstruieren.



Bildquelle: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Illustration, leicht modifiziert.

In Blockchains werden alle Inhalte eines Blocks in einem Hash zusammengefasst. Die „gehashten“ Inhalte bestehen aus dem Hash des vorherigen Blocks, den Transaktionsdaten und dem Zeitstempel. Der Hash des Blockes 1 ist also z.B. Bestandteil des Blockes 2. Würde jemand eine Transaktion in Block 1 im Nachhinein manipulieren, würde sich der Hash dieses Blockes ändern. Da der Hash des Blockes ebenfalls Bestandteil des nachfolgenden Blockes ist, würde sich der Hash des Blockes 2, sowie die Hashes von allen nachfolgenden Blöcken ebenfalls ändern. Eine Manipulation der Blockchain wäre daher offensichtlich. Aufgrund der dezentralen Speicherung der Blockchain auf vielen Computern wäre die Manipulation einiger Kopien der Blockchain zudem folgenlos, da genügend nicht manipulierte Kopien zur Verfügung stehen. Die manipulierten Kopien könnten somit schnell ersetzt bzw. ignoriert werden. (Vgl. https://www.die-gdi.de/discussion-paper/article/a-primer-on-blockchain-technology-and-its-potential-for-financial-inclusion/)

II What is “Blockchain” anyway?

Everyone loves tech's hottest buzzword but no one seems to know what it means.

BY PETER VAN VALKENBURGH / April 25, 2017

“Blockchain” has become a buzzword in the technol ogy and financial industries. It is often cited as a panacea for all manner business and governance problems. “Blockchain’s” popularity may be an encouraging sign for innovation, but it has also resulted in the word coming to mean too many things to too many people, and—ultimately—almost nothing at all. […]

Is there anything we can say is *always* true about a blockchain technology? Yes.

All blockchains have...

All blockchain technologies should have three constituent parts: peer-to-peer networking, consensus mechanisms, and (yes) blockchains, A.K.A. *hash-linked data structures*. You might be wondering why we call them blockchain technologies if the blockchain is just one of three essential parts. It probably just comes down to good branding. Ever since Napster and BitTorrent, the general public has unfortunately come to associate peer-to-peer networks with piracy and copyright infringement. “Consensus mechanism” sounds very academic and a little too hard to explain a little too much of a mouthful to be a good brand. But “blockchain,” well that sounds interesting and new. It almost rolls off the tongue; at least compared to, say, “cryptography” which sounds like it happens in the basement of a church.

But understanding each of those three constituent parts makes blockchain technology suddenly easier to understand. And that’s because we can write a simple one sentence explanation about how the three parts achieve a useful result:

Connected computers reach agreement over shared data.

That’s what a blockchain technology should do; it should allow *connected computers* to *reach agreement* over *shared data*. And each part of that sentence corresponds to our three constituent technologies.

Connected Computers. The computers are connected in a peer-to-peer network. If your computer is a part of a blockchain network it is talking directly to other computers on that network, not through a central server owned by a corporation or other central party.

Reach Agreement. Agreement between all of the connected computers is facilitated by using a consensus mechanism. That means that there are rules written in software that the connected computers run, and those rules help ensure that all the computers on the network stay in sync and agree with each other.

Shared Data. And the thing they all agree on is this shared data called a blockchain. "Blockchain" just means the data is in a specific format (just like you can imagine data in the form of a word document or data in the form of a image file). The blockchain format simply makes data easy for machines to verify the consistency of a long and growing log of data. Later data entries must always reference earlier entries, creating a linked chain of data. Any attempt to alter an early entry will necessitate altering every subsequent entry, otherwise digital signatures embedded in the data will reveal a mismatch. Specifically how that all works is beyond the scope of this backgrounder, but it mostly has to do with the science of cryptography and digital signatures. Some people might tell you that this makes blockchains "immutable," that's not really accurate. The blockchain data structure will make alterations evident, but if the people running the connected computers choose to accept or ignore the alterations then they will remain. […]

Source: https://coincenter.org/entry/what-is-blockchain-anyway

III Werden Blockchains die neuen Banken der Armen?

Jan Ohnesorge / DIE, Die aktuelle Kolumne vom 05.02.2018

Dieses Jahr wird die Blockchain-Technologie zehn Jahre alt. Im November 2008 schrieb ein bis heute unbekannter Autor unter dem Pseudonym Satoshi Nakamoto das Whitepaper „Bitcoin: Ein elektronisches Peer-to-Peer--Bezahlsystem", in dem die Grundlagen der Blockchain- Technologie dargestellt werden. „Bitcoin" erwies sich mit seiner praktischen Implementierung im Jahr 2009 als erste funktionierende digitale Währung, die ohne eine zentrale Instanz auskommt. Die Währung funktioniert, weil die Blockchain-Technologie ein sehr sicheres digitales Archivieren jeder Überweisung ermöglicht. Dadurch wird Betrug wie das mehrfache Ausgeben desselben Bitcoins effektiv verhindert. Auf den Pionier Bitcoin folgten in den kommenden Jahren zahlreiche weitere Kryptowährungen und andere blockchainbasierte Netzwerke, die die Technologie weiterentwickelten.

Ein Peer-to-Peer-Bezahlsystem, indem die Nutzer direkt miteinander interagieren, ohne dass eine zentrale Instanz eine Vermittlerfunktion einnimmt, ist nicht nur ein Durchbruch auf technischer Ebene. Es kann auch den Zugang zum Finanzsystem für einkommensschwache Menschen erleichtern. Dies ist besonders vor dem Hintergrund relevant, dass mangelnder Zugang zu Finanzdienstleistungen ein bedeutendes Entwicklungshemmnis ist. So zielen einige Indikatoren der Sustainable Development Goals (SDGs) auf größere Teilhabe an Finanzdienstleistungen ab. Während Menschen mit niedrigem Einkommen der Zugang zu einer Bank oft verwehrt bleibt, kann prinzipiell jeder, der Zugang zu einem Internetanschluss hat, Kryptowährung kaufen und damit Transaktionen tätigen. Bevor Menschen mit einem eingeschränkten Zugang zum Finanzsystem Kryptowährungen als Zahlungsmittel nutzen können, muss allerdings deren Akzeptanz noch deutlich steigen. Zudem muss die Nutzerfreundlichkeit von Krypto-Banking Programmen noch verbessert werden, damit auch Laien diese sicher bedienen können.

Eine Finanzdienstleistung, die für Migrantinnen und Migranten sowie für ihre Familien von entscheidender Bedeutung ist, sind internationale Rücküberweisungen. Global gesehen ist die Summe der Rücküberweisungen in Entwicklungsländer ca. drei Mal so groß wie die Summe der öffentlichen Entwicklungsausgaben. Der großen Bedeutung von Rücküberweisungen tragen auch die SDGs Rechnung und fordern, dass deren Transaktionskosten bis 2030 im Durchschnitt auf 3 Prozent der transferierten Summe sinken. Die Digitalisierung der Branche hat in den letzten zehn Jahren bereits zu einer Reduktion der Kosten von knapp 10 Prozent auf ca. 7 Prozent geführt.

Ermöglicht die Blockchain-Technologie weitere dringend benötigte Kostensenkungen in diesem Bereich? Blockchainbasierte Netzwerke wie Ripple, Stellar, IOTA, oder NEO ermöglichen kostenlose oder nahezu kostenlose internationale Transfers von Kryptowährungen. Jedoch muss der Sender einer Rücküberweisung in der Regel zunächst seine lokale Währung in eine Kryptowährung tauschen und diese dann für seine internationale Transaktion nutzen, bevor der Empfänger des Geldes die Kryptowährung wieder in seine lokale Währung tauscht. Statt eines Währungstauschs (z.B. Euro zu Indische Rupie) werden also zwei Währungstausche (z.B. Euro zu Bitcoin zu Indische Rupie) benötigt.

Andererseits können durch die Nutzung von Kryptowährungen bestimmte Gebühren und Wartezeiten umgangen werden. Diese entstehen bei konventionellen Anbietern wie Western Union durch die Nutzung von Korrespondenzbanken. Neben diesen Kostenersparnissen können

blockchainbasierte Geldtransferunternehmen Synergien nutzen, wenn sie zusätzlich zu ihrem Kerngeschäft auf eigene Rechnung mit Kryptowährungen handeln. Auf dieser Grundlage bieten z.B. die Startups Circle und Cashaa kostenfreie bzw. sehr günstige Geldtransfers in verschiedene Länder an. Ob sich diese Unternehmen langfristig am Markt behaupten können ist nicht klar. Es ist jedoch schon heute absehbar, dass die Blockchain-Technologien durch die Umgehung von Korrespondenzbanken in den nächsten Jahren einen Beitrag zur Senkung der Kosten von Rücküberweisungen wird leisten können.

Blockchain-Technologien haben ein großes Potential, viele Bereiche in Wirtschaft und Verwaltung, effizienter zu strukturieren. Besonders gilt das für Bereiche, in denen Vertrauen zwischen den Markteilnehmern bisher von einer zentralen Instanz hergestellt wird. Internationale Rücküberweisungen sind relativ einfach mit bestehenden Blockchain-Technologien durchzuführen, daher gibt es bereits heute Lösungen, die Kostenvorteile gegenüber den etablierten Geldtransferunternehmen bieten. Bis blockchainbasierte Netzwerke eine vollwertige Bank mit nutzerfreundlichen Zahlungsdienstleistungen sowie (Spar)konten und (Mikro)krediten für finanziell unterversorgte Menschen sein können, wird es aber wohl noch einige Jahre dauern. Staatliche und private Akteure sollten diesen Prozess unterstützen, indem sie die Potentiale der Blockchain-Technologie aktiv nutzen und deren Weiterentwicklung fördern. Ein erster Schritt hierzu kann die Akzeptanz von Kryptowährungen für bestimmte Zahlungen sein. So akzeptiert, neben zahlreichen Unternehmen, auch der Schweizer Kanton Zug seit dem Jahr 2016 Gebührenzahlungen in Bitcoin.

Quelle:https://www.die-gdi.de/die-aktuelle-kolumne/article/werden-blockchains-die-neuen-banken-der-armen/