15. FAEL-Herbstanlass zum Thema Blockchain

Vertrauen ist gut, gut verteiltes Vertrauen ist besser

Stockmetamorworks

Blockchains sind vor allem durch Kryptowährungen, allen voran Bitcoin bekannt geworden. Sie sind aber viel mehr. Was die Grundlagen der dezentralisierten Sicherheit und des verteilten Vertrauens genau beinhalten und welche typischen Anwendungen neben elektronischen Währungen auch noch möglich sind, wird am 15. FAEL-Herbstanlass online erläutert.

» *Heinz Mathis, OST Ostschweizer Fachhochschule, Rapperswil*

Die wohl berühmteste Blockchain ist Bitcoin. Die Grundlagenpublikation zum Bitcoin von Satoshi Nakamoto (über seine Identität herrscht noch immer Unklarheit) ist nur neun Seiten lang und stammt aus dem Jahre 2008.

FAEL Kompakt

FAEL: Swiss Engineering Fachgruppe für Elektronik & Informatik

Mitglieder: 1038

Gründung: 1978

Präsident: Michael Giger, Dipl. Ing. FH

Kontakt: Michael Giger, Fachgruppe Elektronik und Informatik, 8000 Zürich, Tel. 079 473 60 40 fael@swissengineering.ch; www.fael.ch

Der erste Satz der Zusammenfassung erläutert einen der wichtigsten Punkte, nämlich jenen der fehlenden Finanzinstitution in der Rolle einer zentralen Autorität. Die Open-Source-Referenzsoftware erschien im Jahr darauf. Durch diese Software für jedermann wird Bitcoin sowohl zu einem Zahlungssystem als auch zu einer Geldeinheit.

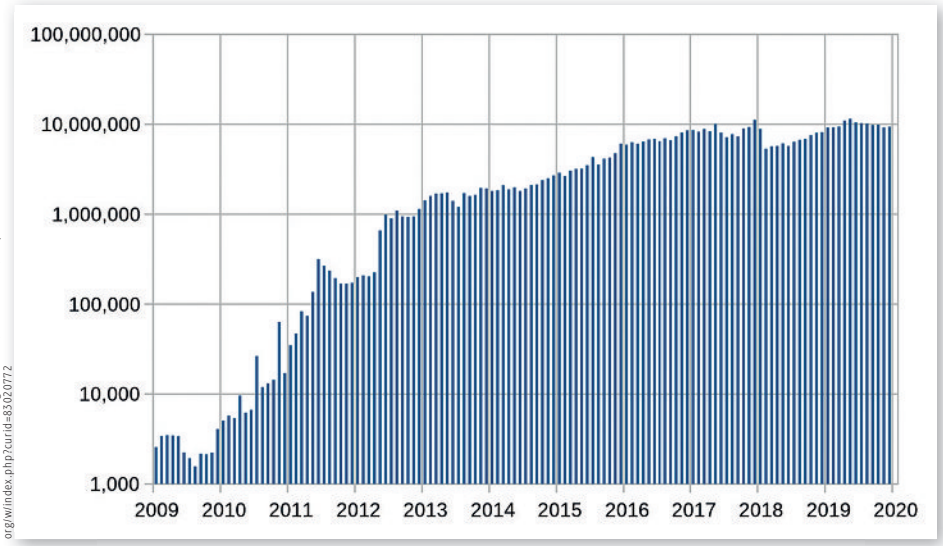
Sicherstellung der Transaktionskette

Die Grundlagen der Blockchain hingegen sind länger bekannt und stammen aus den 1990er-Jahren. Das Hauptproblem ist nicht die eigentliche Verschlüsselung. Digitale Signaturen sind schon eine Weile Realität. Die Hauptinnovation von Bitcoin besteht darin, zu vermeiden, dass jemand ein bestimmtes Guthaben in elektronische Währung doppelt ausgibt. Eine Münzeinheit in Bitcoin ist daher die Aufzeichnung und somit die Sicherstellung der Transaktionskette. Illustrativ kann man sich das so vorstellen, dass eine 100-Franken-Note in ein Kuvert gesteckt wird, welches Adresse und Unterschrift von jedem trägt, der den Schein ausgibt, indem er das Kuvert weiterschickt. Der aktuelle Besitzer kann ihn ausgeben, indem er seine Unterschrift anfügt und weiterschickt.

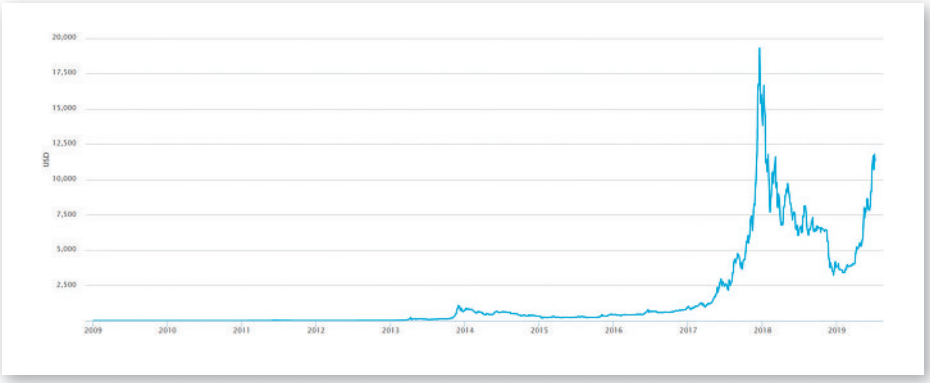
Bitcoin in Schritten erklärt

Die einzelnen Schritte des Bitcoin-Netzwerkes werden im erwähnten Originaldokument von Bitcoin wie folgt beschrieben:

1. Neue Transaktionen werden an alle Knoten übertragen.



Grafik 1: Anzahl Transaktionen pro Monat.



Grafik 2: Bitcoin-Wechselkurs von US-Dollar.

2. Jeder Knoten sammelt neue Transaktionen in einem Block.
3. Jeder Knoten versucht, einen schwierigen Proof of Work für seinen Block zu finden.
4. Wenn ein Knoten einen Proof of Work findet, überträgt er den Block an alle Knoten.
5. Knoten akzeptieren einen Block nur dann, wenn alle darin enthaltenen Transaktionen gültig sind und nicht schon früher ausgegeben wurden.
6. Knoten drücken ihre Akzeptanz des Blockes damit aus, dass sie den nächsten Block in der Kette erzeugen, indem sie den Hash des akzeptierten Blocks als Start-Hash für den nächsten Block nehmen.

Die totale Anzahl Bitcoins ist limitiert. Trotzdem kann die Währung weiterhin im Umlauf sein. Wenn alle Bitcoins draussen sind, gibt es immer noch die Transaktionsgebühren als Anreiz, damit Knoten weiterhin mitrechnen. Die Höhe dieser Transaktionsgebühr bestimmt dann auch in einer nicht-deterministischen Art und Weise die Zeitdauer bis zur Bestätigung, weil Transaktionen mit höheren Gebühren bevorzugt in die Kettenlänge hineingenommen werden.

Anonymität gesichert?

Für die Identifikation der Akteure innerhalb der Bitcoin-Transaktionen werden sogenannte Pseudonyme in Form von Public Key-Hashwerten benutzt. Sie lassen keinen direkten Rückschluss auf die wirkliche Identität der Akteure zu. Auf der anderen Seite existiert eine gewisse Rückverfolgbarkeit dieser Pseudonyme, sodass eine komplette Anonymität nicht gewährleistet ist, vor allem wenn durch Musterbeobachtung auf Identitäten geschlossen werden kann.

Auf und ab

Es gibt zwei interessante Grafiken im Zusammenhang mit Bitcoin. Beide sind Wikipedia entnommen. Die erste Grafik zeigt die Anzahl Transaktionen pro Monat. Die scheint bei 10 Millionen zu sättigen, mindestens im Moment.

Die zweite Grafik ist die der Kursfluktuation. Da passierte lange nichts. Vor drei bis vier Jahren begann dann eine höchst volatile Phase, angetrieben durch Spekulationen und Presseartikel. Die maximale Anzahl Bitcoins ist auf 21 Mllionen limitiert. Bei 10'000 US-Dollar pro Bitcoin sind das immerhin 210 Milliarden US-Dollar. Die Schwierigkeit Bitcoins zu schürfen, wird künstlich erhöht. Damit steigt auch der Energieaufwand. Das ist auch einer der Hauptkritikpunkte an Bitcoin. Der Energieaufwand des Bitcoin-Systems wird zunehmend grösser. In einem kürzlichen Jahresvergleich toppt er den Energiebedarf des Staates Dänemark. Gegen oben hilft die Selbstregulierung nur bei tiefem Kurs, weil dann die Energiekosten verglichen mit dem Gewinn die Schürferei unrentabel machen. «

Der Anlass

FAEL Herbstseminar «Blockchain»

Obwohl Bitcoin die erste und erfolgreichste Kryptowährung basierend auf Blockchain ist, haben Blockchains weit mehr zu bieten. Neben 3000 weltweit bekannten Kryptowährungen erlauben Blockchains auch anderen Anwendungen des Vertrauens. Was die Grundlagen der dezentralisierten Sicherheit und des verteilten Vertrauens genau beinhalten und welche typischen Anwendungen neben elektronischen Währungen auch noch möglich sind, wird am 15. Herbstseminar der FAEL erläutert.
Der traditionelle FAEL-Herbstanlass findet in diesem Jahr wegen COVID-19 online statt (via GoToMeeting). Anmeldungen sind ab sofort möglich unter
www.fael.ch/Herbstanlass2020

Der Ablauf

Das Programm im Detail

- 17.30 Uhr: Begrüssung, Prof. Dr. Heinz Mathis; Vorstandsmitglied FAEL
- 17.35 Uhr: Die Grundlagen einer Blockchain; Prof. Dr. Roger Wattenhofer, ETHZ
- 18.50 Uhr: MODsense – Tracking und Monitoring mit Blockchain, Dr. Thomas Bocek, Modum
- 19.15 Uhr: LivingPackets und THE BOX – IoT und Blockchain in einer smarten, wiederverwendbaren Verpackungsbox für die Zukunft des Versendens; Niklas Leck, LivingPackets

Infoservice
Prof. Dr. Heinz Mathis
OST – Ostschweizer Fachhochschule
Electrical and Computer Engineering
heinz.mathis@ost.ch