

Inhaltsverzeichnis

Vorwort

Bitcoin

Wozu Kryptowährungen?

Kryptowährung und Kriminalität

Bitcoin Wallet

Bitcoin-Adresse

Bitcoin-Transaktion

Beispiel: Transaktion splitten

Signatur einer Transaktion

Digitale Signatur

Eigenschaften einer digitalen

Signatur

Beispiel: Versuch, eine Signatur zu kopieren

Entwicklung der Krypto-Wissenschaft

Einwegfunktionen

Sicherer Schlüsselaustausch bei symmetrischer Verschlüsselung

Asymmetrische Verschlüsselung

Beispiel asymmetrische Ver- und Entschlüsselung

Kryptografische Hashs

Hash

Beispiel: Prinzip Hash

SHA-256-Algorithmus

Beispiel Hashwerte

Hash-Pointer

Signieren einer Nachricht bei Bitcoin

Bitcoin-Technik

Blockchain

Blockchain-Technik – mehr als die Basis einer Kryptowährung?

Bitcoin-Block

- Blockaufbau

- Block-Header

- Hauptteil - Transaktionen

- Verketten der Transaktionen über die Blöcke

- Beispiel: Prinzip der verketteten Transaktionen

- Beispiel: Transaktions-Inputs zusammenfassen

- Beispiel: Gemeinsam bezahlen

- Vereinfachung bei den Beispielen

UTXO - Unspent Transaction Output

Bitcoin Script

- Pay To Pubkey Hash

- Einige Bitcoin Script Operationen

- Beispiel: Bitcoin Script Arithmetik

- Beispiel Bitcoin Script für eine Standard-Transaktion

- Beispiel: P2PH Transaktion im Internet

- Mehrere Transaktionen in einem Block - Merkle Tree

- Beispiel Fälschungsversuch

Proof of Work

- Beispiel: Berechnung der Difficulty

Energieverbrauch

Angriffe auf die Blockchain

- 51-Prozent-Angriff

- Quantencomputer

Das Bitcoin-Netz

- Internet

- Bitcoin-Netz

- Aus Anwendersicht

Wie sicher sind Bitcoins?

Welche Möglichkeiten der Aufbewahrung gibt es?

Persönliche Wallet

Handelsplattformen

Fiatgeld versus Krypto-Währung

Ein kurzer Blick in die Vergangenheit

Krisen und Geldpolitik

Herkömmliche Kapitalanlagen

Bitcoin als Geldanlage?

Weitere Krypto-Währungen und Krypto-Anlagen

Weitergabe von Token

Weitere Möglichkeiten der Blockchain-Technik

Rechtliches

Kryptografische Zentralbank-Währung

NFTs in der Kunst

Klaus Goeb

Bit Coin Blockchain

Kurz und bündig

Klaus Goeb

Bitcoin & Blockchain

Hinter den Kulissen

Technik, Anwendung und Kritik

Kurz und bündig

Impressum

© 2020 Klaus Goeb, Bismarcksteig 8, D-78467 Konstanz

ISBN

Vorwort

„Bitcoin und Blockchain kurz und bündig“. Daher wollen wir uns nicht lang mit dem Vorwort aufhalten. Aber es ist nun mal üblich, dass man sich als Autor an seine Leser wendet. Wenn Sie dieses Buch lesen, weil Sie verstehen wollen, wie Bitcoin und wie eine Blockchain funktioniert, dann hoffe ich, dass Ihnen dieses Buch helfen kann.

Natürlich ist dieses Buch keine Anlageempfehlung für Bitcoin. Aber generell sollte man ja nur Geld in Anlagen investieren, die man einigermaßen versteht. Und dann können Sie selbst entscheiden. Ich denke dafür kann dieses Buch eine Hilfe sein.

Wenn in diesem Buch auch der Schwerpunkt auf Bitcoin liegt, gelten die dahinterliegenden Techniken im Prinzip auch für andere Kryptowährungen.

Und schließlich kann die Blockchain-Technik nicht nur für digitales Bezahlen im Internet verwendet werden. In Zukunft könnten z.B. auch digitale Wahlen oder das Identitätsmanagement per Blockchain realisiert werden.

Wer den digitalen Wandel nicht verschlafen will, ist also gut beraten, sich auf dem Stand der Technik zu halten.

Bitcoin

Bitcoin ist das weltweit führende digitale Zahlungsmittel. Es wurde 2007 von dem unter Pseudonym auftretenden Satoshi Nakamoto erfunden. Der Kurs für ein Bitcoin lag in der Anfangszeit 2010 bei 0,08 Cent (USD).

Am 20.10.2019 betrug der Bitcoin-Kurs 7.129,93 €. Der Kurs kann allerdings stark schwanken. 2018 erreichte der Kurs für kurze Zeit einen Wert von über 17.000 USD und am 19.02.2021 war er sogar auf 43.465 € gestiegen.

Bitcoins können in kleinere Einheiten unterteilt werden, sogenannte Satoshis (nach dem Erfinder-Pseudonym). Ein Satoshi ist ein Hundertmillionstel eines Bitcoins, also 10^{-8} BTC. Oder umgekehrt: 100.000.000 Satoshis sind 1 BTC.

Die **maximale Anzahl** an Bitcoins ist auf 20.999.999,9769 BTC, also auf **rund 21 Millionen**, begrenzt. Rund 18 Millionen Bitcoins bestehen zur Zeit laut www.bitinfocharts.com. (Bei den staatlichen Währungen kann die Zentralbank die Geldmenge beliebig erhöhen).

Bei Bitcoins gibt es keine Zentrale Stelle die die Funktion einer „Zentralbank“ einnehmen könnte und die die Geldmenge steuert. Die Begrenzung wird lediglich durch den Algorithmus bestimmt.

Verliert ein Bitcoinbesitzer seinen privaten Schlüssel, gehen Bitcoins unwiderruflich verloren. Computer gehen kaputt, Speichersticks streiken, Passwörter werden vergessen, Erben haben keinen Zugriff zur Wallet, Gründe gibt es viele. Analysten gehen davon aus, dass bis zu 3,8 Millionen Bitcoins verloren gegangen sind. Wenn die theoretische Grenze von 21 Millionen BTC erreicht ist, werden deutlich weniger Bitcoins im Umlauf sein. Da so die