Cryptos - Technik und Benutzung

Axel Wachtler

Einleitung

Durch den Bitcoin-Hype des letzten Jahres, wurde das Thema Blockchain und digitale Währungen in den Medien präsent. Bitcoin [1], als Vorreiter der Blockchain-Technologie, wurde durch den Ansturm in die Spekulations-Ecke gedrängt und verschiedene Probleme wurden offensichtlich, z.B. hohe Volatilität und Kosten, extremer Energieverbrauch und Zentralisierung. Der eigentliche Zweck, effizienter bankenunabhängiger internationaler Geldtransfer ging damit fast vollständig verloren.
Parallel zu Bitcoin existiert eine Vielzahl alternativer Kryptowährungen. Eine interessante energiesparende Alternative sind Coins die auf dem Konsens-Protokoll *Proof of Stake* anstelle des von Bitcoin verwendeten von *Proof of Work* aufbauen, u.a. Blackcoin [2] und Peercoin [3].

Funktion einer Kryptowährung

Das Fundament einer Kryptowährung ist das verteilte Kassenbuch (distributed ledger), eine Datenbank in der alle Überweisungsvorgänge manipulationssicher gespeichert sind. Jeder Knoten des Netzwerkes hat dabei die Aufgabe, Überweisungen (Transaktionen) von Nutzern anzunehmen, diese zu verifizieren und in der Datenbank zu speichern. Weiterhin müssen die Knoten sich auf eine gemeinsamen Version des Kassenbuches einigen, damit es nicht möglich ist, das Guthaben mehrfach auszugeben (double spending). Das wird durch die Beweis-Funktionen (Proof-of-Stake/Work) sichergestellt.

Erster Kontakt

Um eine Kryptowährung zu verwenden, muss zunächst die Software des jeweiligen Coins lokal auf einem PC/Raspberry-Pi installiert werden. Dieses Programm ist das Interface zwischen Benutzer und Coin-Netzwerk, es dient dazu, Überweisungen an das Netz zu senden und die eigenen Guthabenstände aus der Blockchain zu berechnen. Ein weiteres wichtiges Element ist die Wallet-Datei (`wallet.dat`). Diese Datei enthält die Schlüsselpaare (privat/public Key) des Benutzers. Der Hash des öffentlichen Schlüssels wird als Kontonummer (Coin-Adresse) benutzt. Mit dem privaten Schlüssel zu einer Coin-Adresse ist es möglich, Beträge von einer der Adresse auszugeben, d.h. an eine andere Coin-Adresse zu überweisen.
Auf weitere Aspekte der Benutzung von Kryptowährungen, u.a. Arten von Wallets, Software-Installation, RPC, Transaktionen- und Transaktions-Scripte, Smart-Contracts, sowie Beschaffung, Veräußerung und steuerliche Aspekte geht der Vortrag ein.

[1] Bitcoin-Wiki: https://en.bitcoin.it/
[2] BlackCoin Homepage: http://blackcoin.co/
[3] Peercoin Homepage: https://peercoin.net/