



Quelle: WorldSpectrum – pixabay.com

Verschiedene Kryptowährungen und ihre Besonderheiten

Mit seiner Einführung 2008, repräsentierte der Bitcoin erstmalig eine vollständig dezentralisierte digitale Währung, die Transaktionen in einem Peer-to-Peer-Netzwerk ermöglicht, ohne auf eine Zentralbank oder Vermittlungsinstanz angewiesen zu sein. Doch seitdem hat sich viel getan. Ein Überblick.

Ethereum und Smart Contracts

Ethereum ist eine offene Softwareplattform, die auf der Blockchain-Technologie basiert und Entwicklern ermöglicht, dezentrale Anwendungen zu erstellen und zu betreiben. Im Gegensatz zu Bitcoin, der in erster Linie als digitale Währung konzipiert wurde, wurde Ethereum entwickelt, um den "Ether" zu betreiben. Ether dient als Kraftstoff für dezentrale Anwendungen innerhalb des Netzwerks.

Ein zentrales Merkmal von Ethereum ist die Fähigkeit, Smart Contracts zu erstellen und auszuführen. Smart Contracts sind selbstausführende Verträge, deren Vertragsbedingungen direkt in Codezeilen geschrieben sind. Diese ermöglichen vertrauenswürdige Transaktionen ohne die Notwendigkeit von Dritten. Diese Transaktionen werden automatisch ausgeführt, sobald die im Vertrag festgelegten Bedingungen erfüllt sind.

Da Smart Contracts auf der Blockchain laufen, sind sie transparent und können nicht verändert oder manipuliert werden. Dies macht sie zu einem mächtigen Werkzeug für eine Vielzahl von Anwendungen, von einfachen Geldtransfers bis hin zu komplexen Geschäftsabläufen. [Weitere Infos zu Smart Contracts finden sich hier.](#)

Datenschutz-Münzen

Datenschutz-Münzen sind spezielle Kryptowährungen, die entwickelt wurden, um die Identität der Benutzer sowie die Details ihrer Transaktionen zu schützen und zu verbergen. Während bei vielen Kryptowährungen, wie beispielsweise Bitcoin, die Transaktionsdetails transparent in einem öffentlichen Ledger aufgezeichnet werden, bieten Datenschutz-Münzen erweiterte Anonymität und Verschleierung Funktionen.

Ein Beispiel für eine solche Datenschutz-Münze ist Monero (XMR). Monero setzt auf Technologien wie Ring-Signaturen, Stealth-Adressen und Ring Confidential Transactions, um sicherzustellen, dass die Identität von Absendern und Empfängern sowie der Transaktionsbetrag verborgen bleiben. Diese Techniken ermöglichen es, Transaktionen durchzuführen, ohne dass Außenstehende genau verfolgen können, wer an der Transaktion beteiligt war oder welcher Betrag übertragen wurde.

Ein weiteres Beispiel ist ZCash (ZEC). ZCash unterscheidet sich von anderen Kryptowährungen durch die Einführung von "Shielded Transactions". Diese Transaktionen nutzen eine fortschrittliche kryptografische Methode namens zk-

SNARKs. Diese Technologie ermöglicht es, Transaktionen zu verifizieren und gleichzeitig sicherzustellen, dass Informationen über den Absender, den Empfänger oder den Betrag der Transaktion nicht öffentlich zugänglich sind.

Benutzer, während gleichzeitig die Transparenz des Systems erhalten bleibt.

Datenschutz-Münzen wie Monero und ZCash symbolisieren eine bewusste Abkehr von der Transparenz traditioneller Blockchains hin zu einem erhöhten Benutzerdatenschutz. Durch innovative Technologien schaffen sie einen sicheren Raum, in dem Transaktionen und Identitäten verschleiert werden, um den Nutzern mehr Anonymität und Datenschutz zu bieten. Möchten man mehr über Krypto erfahren, ist das <https://kryptoszene.de/coin-launch/> möglich. Eine tiefergehende Untersuchung dieser speziellen Kryptowährungen enthüllt eine faszinierende Diskussion über Privatsphäre und Sicherheit im digitalen Zeitalter.

Der Vorreiter

Eingeführt im Jahr 2008 von dem pseudonymen Entwickler Satoshi Nakamoto, repräsentiert Bitcoin eine vollständig dezentralisierte digitale Währung, die Transaktionen in einem Peer-to-Peer-Netzwerk ermöglicht, ohne auf eine Zentralbank oder Vermittlungsinstanz angewiesen zu sein.

Ein wesentlicher Bestandteil von Bitcoin ist die Technologie, die als "Blockchain" bezeichnet wird. In dieser Blockchain, die im Wesentlichen ein öffentliches Buchhaltungssystem ist, werden alle Bitcoin-Transaktionen aufgezeichnet. Dieses System garantiert, dass ein Bitcoin nur einmal ausgegeben werden kann, wodurch das Problem der Doppelausgaben, das in digitalen Systemen auftreten kann, gelöst wird.

Um das Netzwerk zu sichern und neue Bitcoins in Umlauf zu bringen, wird ein Prozess namens "Mining" verwendet. Beim Mining setzen Einzelpersonen oder Gruppen von Personen, die als "Miner" bezeichnet werden, ihre Rechenleistung ein, um komplexe mathematische Probleme zu lösen. Sobald ein solches Problem gelöst ist, wird eine bestimmte Anzahl von Bitcoins als Belohnung ausgegeben. Darüber hinaus spielen Miner eine entscheidende Rolle bei der Validierung von Transaktionen und deren Einbindung in die Blockchain, wodurch die Integrität des Systems gewährleistet wird. [Über die Besteuerung bei Mining gibt es hier mehr zu erfahren.](#)

Obwohl die Details jeder Bitcoin-Transaktion für jedermann in der Blockchain einsehbar sind, bieten sie dennoch ein Maß an Privatsphäre. Die Transaktionen sind pseudonym, was bedeutet, dass, obwohl man die Transaktionsdetails sehen kann, die Identität der an der Transaktion beteiligten Personen nicht direkt durch ihre öffentlichen Schlüsseladressen enthüllt wird. Dies gewährleistet eine gewisse Anonymität für die

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4927815/verschiedene-kryptowaehrungen-und-ihre-besonderheiten/>