Diese 10 Eckpunkte solltest du dir aus Episode E01 merken:

1. Die Blockchain ist ein dezentrales und öffentliches Register. Die Blockchain ist auch das Resultat eines Konsenses.

2. Bitcoin ist ein Registereintrag in diesem Register. Bitcoin, kurz BTC, fungiert momentan insbesondere als digitale Alternative zu Fiatwährungen wie dem Euro.

3. Bei einer Transaktion wird der Hash um den öffentlichen Schlüssel des Empfängers ergänzt und mit dem privaten Schlüssel des Absenders signiert. Damit hat eine Transaktion an den Empfänger mit dem zum öffentlichen Schlüssel gehörenden privaten Schlüssel stattgefunden.

4. Die Transaktionen werden von einem Miner etwa alle 10 Minuten in einem Block an die „längste" Blockchain angegliedert, wobei ein neuer Block auf die zuvor erstellten Blöcke referenziert - daher „Blockchain". Transaktionen in einem Block müssen legitim und widerspruchsfrei sein.

5. Blöcke werden von einem ersten Miner, der den Proof-of-Work durch die dazu verwendete Rechenleistung erbracht hat, erstellt. Die Miner erhalten dafür einen Block Reward von momentan 12.5 BTC je Block und die Transaktionsgebühren. Der Block Reward halbiert sich alle 210 000 Blöcke, was etwa 4 Jahren entspricht.

6. Es werden nie mehr als 21 Millionen Bitcoins existieren. Die allermeisten Bitcoins werden bis zum Jahr 2040 geschürft werden.

7. Das Skalierungsproblem führt zu langen Bestätigungszeiten und hohen Transaktionsgebühren. Mit Segregated Witness bzw. SegWit 2x (NYA), wird u.a. die Kapazität verdoppelt, womit etwa 8400 Transaktionen je Block verarbeitet werden können. Zusätzlich arbeitet man an diversen Off-Chains wie bspw. dem Lightning Netzwerk.

8. Vorschläge werden als Bitcoin Improvement Proposals, kurz BIP, formuliert über welche die Minern abstimmen können. Sie können zu Softforks oder Hardforks führen. Bitcoin Cash (BCH) ist ein Beispiel für eine Hardfork und einen Altcoin.

9. Weitere Anwendungen der Blockchain sind diverse Nachweise, Colored Coins, Smart Properties, Smart Contracts und Oracles. Diese ermöglichen bspw. das Internet of Things, dezentral organisierte Organisationen und vieles mehr.

10. Daneben existieren alternative Altcoins wie bspw. Ether, kurz ETH, die sich mehr oder weniger von Bitcoin unterscheiden. Mehr dazu in der nächsten Episode.

Weitere Infos hier: https://www.generalisten.info/?utm_source=news&utm_content=punkte