Richtlinien der Schweizerischen Nationalbank (SNB) für die Anlagepolitik

Die Ökonomie und Technologie von Bitcoin: Eine tiefgehende Analyse

Bitcoin, eingeführt im Jahr 2009 durch das Pseudonym Satoshi Nakamoto, markiert den Beginn des Zeitalters der Kryptowährungen und der Distributed Ledger Technology (DLT). Es ist ein dezentrales, digitales Währungssystem, das keine zentrale Autorität – wie eine Bank oder eine Regierung – zur Validierung von Transaktionen benötigt.

1. Kryptographisches Fundament und Konsensmechanismus

Das Herzstück von Bitcoin ist die **Blockchain**, eine ständig wachsende, linear verkettete Liste von Datenblöcken. Jeder Block enthält einen Zeitstempel, einen kryptographischen Hash des vorhergehenden Blocks und eine Bündelung neuer Transaktionen. Diese Verkettung gewährleistet die Integrität der gesamten Historie.

Der Konsens im dezentralen Netzwerk wird über den **Proof-of-Work (PoW)**-Mechanismus erzielt. Miner konkurrieren darum, ein komplexes kryptographisches Rätsel zu lösen, indem sie eine Nonce finden, die in Kombination mit den Blockdaten einen Hash erzeugt, der unter einem bestimmten Zielwert (Target) liegt. Die Lösung dieses Rätsels ist rechenintensiv ("Arbeit"), die Verifizierung durch das Netzwerk jedoch trivial. Der Miner, der das Rätsel zuerst löst, darf den neuen Block zur Kette hinzufügen und wird mit neu erzeugten Bitcoins sowie den Transaktionsgebühren belohnt (Mining Reward). Die Schwierigkeit des PoW-Rätsels wird periodisch (alle 2016 Blöcke, ca. 2 Wochen) angepasst, um die Blockgenerierungsrate von etwa zehn Minuten konstant zu halten.

2. Geldpolitik und Knappheit

Bitcoins Wertversprechen beruht auf seiner deflationären Geldpolitik. Im Gegensatz zu Fiat-Währungen, die potenziell unbegrenzt gedruckt werden können, ist die Gesamtmenge an Bitcoin auf **21 Millionen Einheiten** begrenzt. Der Mining Reward wird etwa alle vier Jahre (genauer gesagt alle 210.000 Blöcke) halbiert – ein Prozess, der als **Halving** bekannt ist. Dieses vordefinierte, algorithmische Angebot schafft eine künstliche Knappheit, die oft als "digitales Gold" bezeichnet wird und die Hauptursache für seine Volatilität und seinen langfristigen Wertanstieg ist.

3. Herausforderungen und Skalierbarkeit

Die begrenzte Kapazität des Bitcoin-Netzwerks, Transaktionen zu verarbeiten (aktuell etwa 7 Transaktionen pro Sekunde), ist die größte technische Herausforderung. Große Blockgrößen würden zwar die Geschwindigkeit erhöhen, aber auch die Anforderungen an die Hardware der Miner und Full Nodes steigern, was zur Zentralisierung des Netzwerks führen könnte. Lösungen wie **Segregated Witness (SegWit)** und das **Lightning Network** (eine Second-Layer-Lösung für schnelle Micropayments) wurden entwickelt, um die Skalierbarkeit zu verbessern, ohne die Dezentralisierung zu gefährden.

Guidelines of the Swiss National Bank (SNB) for Investment Policy

The Economy and Technology of Bitcoin: A Deep Dive

Bitcoin, introduced in 2009 by the pseudonym Satoshi Nakamoto, marked the beginning of the era of cryptocurrencies and Distributed Ledger Technology (DLT). It is a decentralized, digital currency system that requires no central authority—such as a bank or a government—to validate transactions.

1. Cryptographic Foundation and Consensus Mechanism

The core of Bitcoin is the **Blockchain**, a constantly growing, linearly linked list of data blocks. Each block contains a timestamp, a cryptographic hash of the preceding block, and a bundle of new transactions. This chaining guarantees the integrity of the entire history.

Consensus in the decentralized network is achieved via the **Proof-of-Work (PoW)** mechanism. Miners compete to solve a complex cryptographic puzzle by finding a nonce which, in combination with the block data, generates a hash below a specific target value. Solving this puzzle is computationally intensive ("work"), but verification by the network is trivial. The miner who solves the puzzle first is allowed to add the new block to the chain and is rewarded with newly generated Bitcoins plus the transaction fees (Mining Reward). The difficulty of the PoW puzzle is periodically adjusted (approximately every 2016 blocks, about 2 weeks) to maintain a constant block generation rate of approximately ten minutes.

2. Monetary Policy and Scarcity

Bitcoin's value proposition rests on its deflationary monetary policy. Unlike fiat currencies, which can be potentially printed indefinitely, the total supply of Bitcoin is capped at **21 million units**. The Mining Reward is halved approximately every four years (more precisely, every 210,000 blocks)—a process known as the **Halving**. This predefined, algorithmic supply creates an artificial scarcity, often referred to as "digital gold," which is the primary cause of its volatility and long-term value appreciation.

3. Challenges and Scalability

The Bitcoin network's limited capacity to process transactions (currently around 7 transactions per second) is its biggest technical challenge. While larger block sizes

would increase speed, they would also increase the hardware requirements for miners and Full Nodes, potentially leading to the network's centralization. Solutions such as **Segregated Witness (SegWit)** and the **Lightning Network** (a second-layer solution for fast micropayments) have been developed to improve scalability without compromising decentralization.