Looking Back: Bitcoin in 2019

What is Bitcoin?

Bitcoin is the oldest cryptocurrency and was launched on January 3, 2009. It solved the double-spend problem for a decentralized electronic cash system, ensuring that bitcoins can only be spent once. Bitcoin does so by bundling transactions in blocks and chaining them together – a process which is secured through cryptographic technology and computational resources (proof-of-work). Today, Bitcoin is still the largest cryptocurrency by market capitalization and captures about 66 % of the total market cap of cryptocurrencies. Bitcoin trades at $7.6k at the time of writing.

Last year, Bitcoin has made its recovery from the "crypto winter" in 2018. Starting the year at $3.7k, Bitcoin has rallied throughout the first half of 2019 to reach almost $14k in late June, and then corrected to the levels of around $7.6k at the time of writing. With a year-to-date return of 105 %, Bitcoin has been the best-performing asset class of 2019. For comparison, the S&P 500 and the tech-focused Nasdaq 100 posted returns of 25 % and 33 % year-to-date, respectively. Market accessibility has been further improved, with physical delivery Bitcoin futures launched in late September.

On the technical side, Bitcoin Core developers have continued to update their node software, currently sitting at version 0.19.0. This brought about several improvements, such as native hardware wallet compatibility. Also, "bech32" addresses – which are less error-prone due to the lack of distinction between upper- and lowercase letters and offer benefits for SegWit – are now the default in the GUI.

Additionally, Electrum – one of the most commonly used Bitcoin wallets – has announced support for Lightning Network payments. The Lightning Network has grown further in 2019 and increased the total capacity among all channels from 525 BTC in January to 825 BTC currently.[1]

More fundamentally, research into the implementation of Schnorr signatures continues as an alternative to the current elliptic curve signature algorithm. Originally proposed as a Bitcoin Improvement Proposal by Bitcoin developer Pieter Wuille, Schnorr signatures would contribute to the scalability of Bitcoin, as well as to improved privacy: Multi-signature transactions would be indistinguishable (in terms of signature size) from normal, single-signature transactions on the blockchain. Additionally, the requirement for block space coming from single-signature transactions with multiple unspent transaction outputs (UTXOs) as inputs would be significantly reduced – since only one signature would be required regardless of the number of inputs.

[1] https://bitcoinvisuals.com/ln-capacity