A **cryptocurrency** (or **crypto currency**) is a [digital asset](https://en.wikipedia.org/wiki/Digital_asset) designed to work as a [medium of exchange](https://en.wikipedia.org/wiki/Medium_of_exchange) that uses [strong cryptography](https://en.wikipedia.org/wiki/Strong_cryptography) to secure financial transactions, control the creation of additional units, and verify the transfer of assets.[[1]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-crypto_currency-1)[[2]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-2)[[3]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-3) Cryptocurrencies are a kind of [alternative currency](https://en.wikipedia.org/wiki/Alternative_currency) and [digital currency](https://en.wikipedia.org/wiki/Digital_currency) (of which [virtual currency](https://en.wikipedia.org/wiki/Virtual_currency) is a subset). Cryptocurrencies use [decentralized control](https://en.wikipedia.org/wiki/Decentralization)[[4]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-4) as opposed to centralized digital currency and [central banking](https://en.wikipedia.org/wiki/Central_bank) systems.[[5]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-5) The decentralized control of each cryptocurrency works through [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) technology, typically a [blockchain](https://en.wikipedia.org/wiki/Blockchain" \o "Blockchain), that serves as a public financial transaction database.[[6]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-CCW180521B-6)[[7]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-7)

[Bitcoin](https://en.wikipedia.org/wiki/Bitcoin), first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency.[[8]](https://en.wikipedia.org/wiki/Cryptocurrency#cite_note-8) Since the release of Bitcoin, over 4,000 *altcoins* (alternative variants of Bitcoin, or other cryptocurrencies) have been created.

Wikipedia

Completely decentralized cryptocurrencies like Bitcoin [[18](https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6#CR18)] and other altcoins [[5](https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6#CR5)] have captured the public’s attention and interest, and have been much more successful than any prior incarnations of electronic cash. Many would call the rise of these electronic currencies a technological revolution, and the “wave of the future” [[3](https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6#CR3)]. Emerging altcoins such as Ethereum [[23](https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6#CR23)] and Counterparty [[14](https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6#CR14)] extend Bitcoin’s design by offering a rich programming language for writing “smart contracts.” Smart contracts are user-defined programs that specify rules governing transactions, and that are enforced by a network of peers (assuming the underlying cryptocurrency is secure). In comparison with traditional financial contracts, smart contracts carry the promise of low legal and transaction costs, and can lower the bar of entry for users.

<https://link.springer.com/chapter/10.1007/978-3-662-53357-4_6>