**Cryptocurrency Overview**

A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency. Cryptocurrencies are classified as a subset of digital currencies and are also classified as a subset of alternative currencies and virtual currencies.

Bitcoin became the first decentralized cryptocurrency in 2009. Since then, numerous cryptocurrencies have been created. These are frequently called *altcoins*, as a blend of *bitcoin alternative*. Bitcoin and its derivatives use decentralized control as opposed to centralized electronic money/centralized banking systems. The decentralized control is related to the use of bitcoin's blockchain transaction database in the role of a distributed ledger.

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.

As of March 2015, hundreds of cryptocurrency specifications exist; most are similar to and derived from the first fully implemented decentralized cryptocurrency, bitcoin. Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions adding them to the ledger in accordance with a particular timestamping scheme.

The security of cryptocurrency ledgers is based on the assumption that the majority of miners are honestly trying to maintain the ledger, having financial incentive to do so.

Most cryptocurrencies are designed to gradually decrease production of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation, mimicking precious metals. Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies can be more difficult for seizure by law enforcement. This difficulty is derived from leveraging cryptographic technologies.

A primary example of this new challenge for law enforcement comes from the Silk Road case, where Ulbricht's bitcoin stash "was held separately and ... encrypted." Cryptocurrencies such as bitcoin are pseudonymous, though additions such as Zero coin have been suggested, which would allow for true anonymity.

Source: https://en.wikipedia.org/wiki/Cryptocurrency