Understanding DeFi: Words Have Meaning, But What Do They Mean?

Perhaps the most challenging (and intimidating) part of Decentralized Finance is understanding all the terms and industry jargon—many of which are new and technical while others are as old as time but commonly misunderstood.

Think of this primer as your glossary. If you are considering entering the DeFi space, or if you are developing a product or service and are working through terminology, this resource will help.

Money – A broad term for any medium of exchange (whether tangible or intangible) that represents value and is accepted as payment for goods or services rendered, including the discharge of debt. It is most often used as a colloquialism for the currency of a sovereign authority, such as the U.S. Dollar.

Currency – A standardized, formal version of money organized into commonly recognized and accepted units of exchange, usually by a sovereign authority, whether in paper notes or specie (coins). Currencies can exist in tangible (e.g., U.S. Dollars or gold/silver coins) and intangible form (e.g., bank deposits or bitcoin).

Fiat Currency – Money issued by a sovereign authority that has no intrinsic value but is formally recognized by official decree as currency. Simply put, fiat currency is money because the government says so—not because of any underlying value.

Legal Tender Laws – Any official decree by a sovereign authority that a specific currency is recognized (and usually printed or minted) by that sovereign authority as a legitimate form of payment for debts, public charges, taxes, and dues.

Legal tender laws typically do not prohibit competing forms of money or currency, such as gold/silver coins or digital currencies. Instead, legal tender laws generally ensure that a means for discharging debt and avoiding civil or criminal liability is legally recognized and available. This distinction is crucial for understanding why other currencies, such as gold/silver coins or bitcoin, can coexist with the U.S. Dollar.

Financial Intermediary – A third party administrator or facilitator connecting diverse entities/persons to facilitate financial transactions. Examples include: banks, brokerages, currency exchanges, and other similar financial institutions, including a sovereign authority's central bank.

Some intermediaries are also a trusted custodian, responsible for the reconciliation or "truing up" of account balances among counterparties, such as by crediting one account and debiting another when currency is exchanged, thereby reducing the risk of fraud or counterfeit. However, a central facilitator or custodian may also increase concentration risk because it represents a single point of failure.

Decentralized Finance – A general term for any form or type of financial instrument or financial exchange between one or more parties that is not dependent upon a financial intermediary, but instead relies on computer programs or algorithms executed in connection with an encrypted database or ledger distributed across multiple sites, most commonly via a peer-to-peer network.

Digital Currency (electronic currency, e-currency, electronic money, e-money, digital money) – Any type of money that exists in an intangible format, including bank deposits, cryptocurrencies, virtual currencies, central bank digital currencies, and even value loaded on a gift card.

Some digital currencies exist exclusively in an electronic medium. However, others have a tangible counterpart and can be interchangeably exchanged. For example, an ATM withdrawal converts currency from its digital form to its tangible form. The process can be reversed by deposit, which converts tangible currency into its digital equivalent.

Central Bank Digital Currency – Money issued by a sovereign authority, usually through its central bank, that is recognized as legal tender but exists exclusively in an electronic format and cannot be exchanged for bank notes or coins.

Today, nearly every sovereign authority is exploring this idea, including the United States, the European Union, and China. However, no major economic power has officially unveiled such a currency. (In 2021, China launched the Digital Currency Electronic Payment, commonly known as the digital Yuan or e-Yuan, but each unit is still backed by deposits held by the People's Bank of China, China's central bank.)

Virtual Currency – A medium of exchange recognized and used as money in a virtual world or electronic platform (e.g., "minecoins" in Minecraft and "v-bucks" in Fortnite). While virtual currencies can be purchased with "real world" currency, in general, they can only be redeemed within the boundaries of the game world to purchase in-game content—basically the 21st century version of pumping quarters into an arcade game to build a bank of credits for continues.

Digital currency and virtual currency are often used interchangeably. More accurately, all virtual currencies are a subset of digital currency, but not all digital currencies are virtual currencies.

Cryptocurrency (crypto assets, crypto money) – A type of currency that:

(1) exists exclusively in an intangible format (i.e., a digital currency);

(2) is protected with sophisticated encryption technology;

(3) is not maintained by or dependent upon a sovereign authority. (Interestingly, in June 2021, El Salvador became the first country to adopt a cryptocurrency—bitcoin—as legal tender.)

In general, cryptocurrencies utilize an encrypted, widely-distributed digital database or ledger and are maintained via a decentralized peer-to-peer network.

According to Charles Schwab, as of June 2022, there are 19,000+ digital currencies, and at least 40 have a market capitalization of $1 billion or more.

Distributed Ledger Technology (digital ledger technology, shared ledger technology) – Information systems and their underlying technology (with computer algorithms being the most common) that can be replicated, distributed, validated, and synchronized across multiple data sites via peer-to-peer networks and are protected via sophisticated encryption technology (e.g., security keys, ciphers, and digital signatures).

In contrast to a centralized database or ledger, which is commonly monitored, controlled, and validated by a financial intermediary or trusted custodian, a distributed database or ledger is shared across multiple computers and computational nodes, all of which rely on the same algorithm to independently replicate, validate, and save an updated copy of the data. Each node then executes another algorithm (commonly referred to as a consensus algorithm) to verify which updated version is correct. Once consensus is established, the ledger is automatically updated and re-distributed. Theoretically, this process will repeat forever, and the ledger grows longer each time a new record or block of information is added, like adding links to a chain (hence the name, blockchain).

In addition, because a distributed ledger is not at the mercy of a financial intermediary or other central facilitator, there is no single point of failure. As such, it is also a hedge against concentration risk.

Blockchain – One type of distributed ledger technology, and perhaps the most common example. Countless blockchains exist, ranging from patented and trademarked proprietary versions (which are owned, operated, and maintained for the exclusive use of private entities) to widely shared open source versions.

Bitcoin – A specific, proprietary type of cryptocurrency (often mistakenly used synonymously) that relies on a blockchain as its underlying architecture.

Ether – Another well-known cryptocurrency that is the proprietary currency of the Ethereum blockchain.

Tokenization – A type of encryption technology where a digital token with no intrinsic or exploitable value is used as a proxy or substitute for sensitive data elements, such as the personally identifiable information of users and customers. Tokenized data elements, which can be mapped back to more sensitive data elements saved and secured elsewhere, help users and customers maintain their privacy and anonymity—a cornerstone of cryptocurrencies and distributed ledger technology. Not exclusive to cryptocurrencies, this technology supports smart contracts, NFTs, multi-factor authentication, and virtual wallets (just to name a few).

Non-Fungible Token (NFT) – An electronic record that represents a unique digital asset (e.g., a song, picture, or artwork) that is commonly encoded via the same technology underlying most cryptocurrencies—a distributed ledger. However, unlike currency, which is quite uniform in its fungibility (meaning one unit is generally indistinguishable and mutually interchangeable with any other unit), NFTs are one-of-a-kind (or at least very limited edition) digital assets.

Unlike most digital or electronic items, which can be copied and reproduced almost infinitely, an NFT is an electronic record with a distinct signature that is impossible, or at least very hard, to replicate—the digital equivalent of owning something as unique as the Mona Lisa (but probably not as valuable).

Controllable Electronic Record (CER) – An intangible record stored in an electronic medium that can be subjected to ownership or control by a person or entity. This new term is part of the Uniform Law Commission's proposed 2022 Uniform Commercial Code amendments, which, among other changes, adds a new Article 12 regarding digital assets. Overall, the amendments introduce updated rules for commercial transactions involving digital currencies, distributed ledger technology, artificial intelligence, and other emerging technologies.