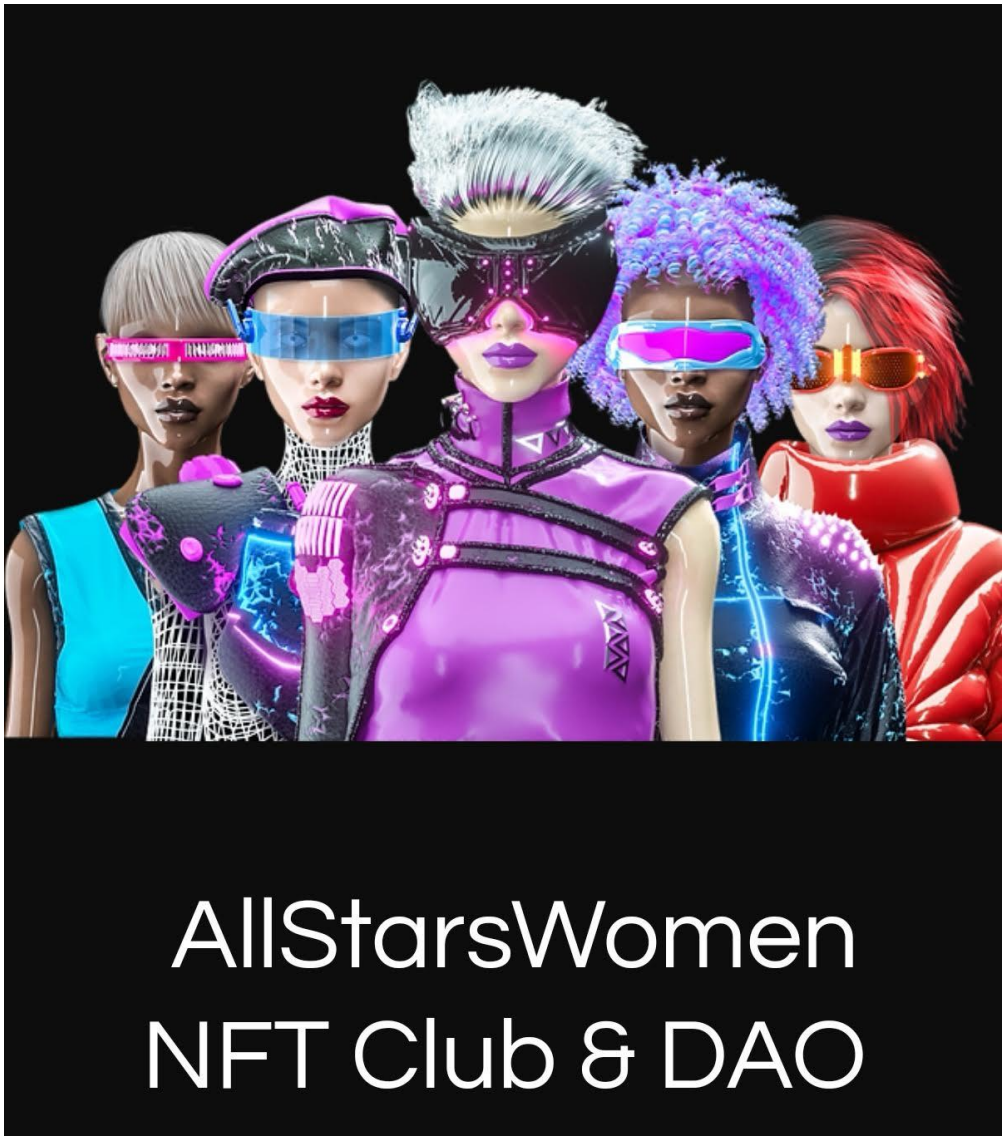


Defi Glossary

Bitcoin: one of the first cryptocurrencies proposed in 2008. Bitcoin (with a capital B) is a system to handle peer to peer payment transactions over the internet, where users do notneed to trust others they are transacting with. The currency bitcoin (with a lower case b) is the unitused on the system.

Blockchain:network of computers ("nodes") that keep an incorruptible, open and common record of transactions / data without the need of a central authority. Open and public

blockchains are transparent (anyone can view them), permissionless (anyone can use them),and censorship-resistant (no-one can stop them). Yet, they can be slow

because new blocks are added upon consensus, which is the process by which the nodes verify new transactions and add to the blockchain. This is achieved by solving a mathematical problem,via computational efforts.

Ethereum: blockchain network created in 2015. Most DeFiapplications are built on

Ethereum.

Forking: open-sourced code allows anyone to clone a dApp,a process known as “forking.”Forking draws users, liquidity,and capital away from the original application.

For example SushiSwap was launched in August 2020 as a fork of Uniswap and within a week, it saw its total value locked (TVL) jump by about $1 billion while Uniswap’s TVL decreased by about the same amount.

Gas fees: payments made by users to compensate for the computing energy required to process and validate transactions on the Ethereum blockchain. If a user is willing to wait longer for a transaction to be executed, they can pay less gas, if instead they want the transaction to be executed faster, then they will have to pay more gas. All details on Ethereum gas fees for example can be found here.

Keepers: different players in distributed networks that maintain stability and perform crucial jobs in the crypto-economic model, for example arbitrage seekers, Dai borrowers in Maker, or validators in Polkadot.

Miners: When bitcoin miners add a new block of transactions to the blockchain, part of their job is to make sure that those transactions are accurate. Bitcoin mining is performed by high-powered computers that solve complex computational math

problems

Minting: creating a new cryptocurrency, NFT or other crypto related asset. The process typically involves creating a new block and recording the information into the blockchain.

On-chain, off-chain collateral, or no collateral. These terms refer in particular to stablecoins i.e. when there is a promise that an asset will remain pegged to the value of another asset (usually a fiat currency). The promise brings about issuer's risks, which is greatest in case of no collateral at all. On-chain collateral is the safest option as assets would be locked on the blockchain,usually within a smart contract, whereas off-chain collateral means that the underlying assets are stored in an escrow account, for example with a bank. If the collateral needs to be a fiat currency (as in the case of USDT and USDC), then currently collateral can only be off-chain,although this might change if and when CBDCs are launched. On-chain collateral is used for example in the case of new Dai tokens - a user who wants to issue new Dai tokens firstneeds to lock enough ETH an underlying collateral in the Maker Protocol:as ETH is volatile however, the collateral needs to be materially above the value of Dai created (150%),and if ETH depreciates too sharply against the USD, the smart contract will auction off the collateral to cancel the debt in Dai.

Oracles: data feeds that allow information from sources off the blockchain, such as the current price of a stock or a fiat currency, to be integrated into DeFi services.

Proof of work (PoW)vs proof of stake(PoS): proof of work is the same mechanism used by Bitcoin and currently Ethereum,and requires all nodes in the network to be involved in transaction validation, which reduces throughput (a measure of how many actions are completed within a given time frame), speed, scalability. PoS instead require

“stakers” to validate transactions based on how many tokens they have staked (locked onto the platform) and for how long. The more tokens a validator has, the more “mining” power. PoS does not require all nodes to participate in transaction validation, and hence does not incentivise extreme amounts of energy consumption.

Protocols: a protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.

Smart contracts: small applications stored on a blockchain and executed in parallel by a large set of validators. Smart contracts musthave the following three characteristics

(we follow the definitions in this paper:https://arxiv.org/abs/2101.08778) :

- encode protocol rules

- be able to communicate with one-another within the same execution context (typically

a transaction)

- support atomicity, i.e.,a transaction either succeeds fully (state change) or fails entirely (state remains unaltered), such thatno execution can result in an invalid state. Most importantly, smart contracts need to be able to call each other, making them sort of "money lego" on top of which complex financial transactions can be built.

Tokens: tokens represent assets built on blockchain rails, ranging from Ether,

cryptoassets, derivatives, but also voting rights or stakes, or governance tokens for decentralised autonomous organisations (DAO) for example.Fungible tokens (typically implemented via the ERC-20) are standardised and hence interchangeable - examples of fungible tokens are crypto assets. Non fungible tokens (NFTs) are unique,and typically

defined with ERC standards such as ERC-721. One of the notable use cases is the assignment of a NFT to a real estate property, or a piece of art. Valuelocked: this is a users' deposits locked in a protocol's smart contracts.

Wallet: wallets store tokens and are needed to enter the decentralised world. In a centralised world, wallets exist and work with username and password that can be reset. However they are vulnerable to attacks. In decentralised wallets instead (forexample MetaMask), the user has full control over his /her assets, but if they lose the key, then the tokens are lost forever.

Whales: crypto whales are entities who hold a large number of coins of a particular cryptocurrency. If whales own the majority of governance tokens of a DAO, then they can influence decisions,almost in a centralised way.

Yield Farming: with yield farming,an investor deposits units of a cryptocurrency into a lending protocol to earn interest or rewards (in the form of crypto) as assets are used for various purposes including providing liquidity to the market