Glossary

* Market capitalization: current price \* circulating supply
* Liquidity: how easily you can convert an asset into cash or another asset
* Bid-Ask spread: gap between the lowest asking price (sell order) and the highest bid price (buy order)
* Volatility: how quickly and how much the price of an asset changes
* MA: Moving average (price at closing for x days / x)
* Proof of Work (PoW): In order to validate a block, multiple miners will try to resolve the algorithm. However only the first will be rewarded. The others will have wasted energy for nothing.
* Proof of Stake (PoS): In order to validate a block, only one miner will be designated to resolve the algorithm. If he had the correct answer he would be rewarded. Otherwise he would be sanctioned. That’s why for being one of these miners you need to stake token, and those tokens are blocked for a period of time.
* Smart contract: Contract immutable on the block chain. It’s an agreement between two party. However, to validate the contract, both parties must have what they offer.
* DeFi: Improve a lot of different aspects in finance: stable coin, lending and borrowing, decentralized exchanges, insurance, margin.
* Oracles: tools to make the bridge between the real world and the virtual one. E. g. temperature, value of dollar.
* Decentralized apps (dApps): Open source code. Run 24/7. DeFi, DeEx (decentralized exchanges), Game, Marketplaces
* Non fungible token (NFT): what makes NFT valuable: First, Utility, Unique or rare, ownership history.
* Uniswap: Exchange token at a low price. On this platform you can either swap tokens or inject token in a liquidity pool and obtain interest rate.
  + Uniswap v1: the pools must have ETH
  + Uniswap v2: Pools with whatever token
  + Uniswap v3: Concentrated liquidity
* Automated Market Maker: allows traders to buy and sell coins based on algorithms that detect how much the price should be based on how much there is. If a lot of people buy an asset, his price will increase, because there will be less. And price decrease when they are more and more. Supply & demand with algorithm.
* Liquidity pool: Exchange coins with smart contract. Liquidity providers collects fees from swaps of traders.
* Routing: If liquidity pools works by pair. E. g. 1st LP (Eth/BTC) and 2nd (ETH/USDT). You have BTC and you want USDT. You’ll do BTC->ETH->USDT
* Impermanent Loss: Impact Liquidity providers. It’s the difference between holding coins in wallet and the profit by staking in liquidity pool. If one asset’s price and the other goes down, it’s a huge loss.
* Concentrated liquidity: Provide liquidity in a range of price’s token.
* Sharding: Improve scalability (create more lanes)
* Some of the Layer 2 scaling solutions:
  + Rollups:
    - Zkrollups: Faster but can’t use smart contracts. Rollup multiple transaction into one transaction and send it to the blockchain.
    - Optimistic Rollups: VM improve, can carry smart contract but slower
  + Sidechains: word side of the parent chain. Use his own resources, borrow information from the parent blockchain, run transaction and smart contract and send it to the blockchain.
  + Plasma: Use child chains which has their own child chains. Childs chains work on thing less important that main chain. And important information is broadcast to the child chains.
  + Channels: Lock up funds and get virtual fund. Make transaction on this network. Then get back real fund, which count of 1 transaction. However, you cannot run smart contract on this network.
  + Ethereum Virtual Machine (EVM): Code run by computer around the world to carry block chain smart contract.
* Polygon = Matic: Ethereum but faster and much cheaper gas fees. Layer 2 scaling solution.
* Block chain:
  + Block: list of transaction and smart contract. E.g. Bitcoin block list around 1500 transactions.
* Yields farming: Different solutions for making money with DeFi
  + Liquidity Providers (LP)
  + Borrowing: High APR
  + Lending: If you don’t wanna sell coin that you think will be more valuable in time
  + Leveraged Lending: Lend coin to exchange, gain APR passively, can borrow coin from this exchange, swap this coin on Uniswap for example, and lend coin to the exchange.
    - AAVE
    - Compound
  + Staking: stake coin on exchange and gain free coins
  + Holding coins that have a redistribution fee: Safemoon, 10% fee, 5% burn and 5% redistributed to the holders. Price will increase as they are less coins. Speculative, no other coins did this before.
  + Degen Farm: useless token created; in the pool the other token is real. High volatility
* Rug Pull: When developer run away with investors funds
  + Yanking liquidity: Provide their token in a liquidity pool and when the price goes up, they keep the other valuable token on the pool that investors have send to swap their useless token.
  + Selling their shares: Promise that their token will be the future bitcoin for example, promise things in the future, and when the price goes up, they sell all their tokens
  + The inability to sell: they change the code so that investors can buy token but not sell it. So, the price will only go up, and only the developer will sell the token
  + Signs of rug pull:
    - Liquidity is not locked or for not long (e.g. 2 weeks): possibility of the developer to get what there is inside the pool
    - A few wallets have a large percentage of the token
    - The burn wallet has a large percentage; hiding the true big wallets
    - No audit: audit is made by third-party to verify the project
    - No social media or website
    - No multisignature wallet: that means that 1 developer of the team can manipulate the wallet. If they are multiple signature, they need the password of each of them to act
    - Currently no one is held responsible for rug pulls
* Blockain bridge: allows transfer of token to one chain or network to another chain or network to interact between them. Each coin has his own blockchain.
* Slippage: Swap to stable coins and lost few coins due to AMM algorithm
* Decentralized Autonomous Organization (DAO): no corporate board, action are made by token holders
* Bitcoin
  + Transactions
    - They are no accounts or balance, only UTXO: unspent transaction output
    - To unlock a transaction, you need to have the corresponding signature and the correct value from the script that locked the transaction
    - They are multiple scripts of locking transaction
      * P2PKH
      * P2PK
      * Multi-signature
      * P2SH
    - Scripts construction use Forth-like language: simple and secure