rank	type	term	definition	Concept
		Bitcoin	The first and most popular cryptocurrency based on DLT technology developed from a whitepaper written by Satoshi Nakamoto in 2008	
		Block	A group of transactions entered into a blockchain; analogous to a page of a ledger or record book.	
		Blockchain	A mathematical structure for storing digital transactions or data in an immutable, distributed, decentralized digital ledger consisting of blocks that are linked via cryptographic signature that is nearly impossible to fake, hack or disrupt.	
		Blockchain (Private a.k.a. Permissioned)	A blockchain that resides on a private network of computers that is only accessible to those with permission.	Private blockchains can provide public access (see retail carbon credit app)
		Blockchain (Public a.ka. Permissionless)	A blockchain that resides on a network of computers around the world that is accessible to everyone.	do you want your bank account on a public blockchain? Ethereum BUT permissioned access only
		Chain of custody	The entire chain of documentation of ownership of a product during its lifecycle from raw materials to the final end user. on blockchain, a tokenized digital asset can have an immutable chain of custody	Think real estate land titles (for ownership) - do you need title insurance?
		Chaincode	another name for a smart contract (usually in Hyperledger Fabric)	
		Consensus Algorithm	A protocol used to ensure that all nodes in a blockchain network agree on the validity of transactions and the state of the ledger. Different blockchains support different consensus algorithms (Proof of Work, Proof of Stake, RAFT, BFT etc)	how transactions are validated on the distributed blockchain nodes
		Cryptocurrency	Digital money which uses encryption and consensus algorithms to regulate the generation of coins/tokens and transfer of funds. Cryptocurrencies are generally decentralized, operating independently of central authorities.	
		Cryptography	The science of securing communication using individualized codes so only the participating parties can read the messages.	
		DAO (Decentralized Autonomous Organization)	A governance structure without a central authority which rewards good behavior and penalizes bad behavior by a set of pre-defined rules which can only be changes by a vote, which typically requires a stake, adding risk to the process to discourage bad actors, amongst the participants.	lacks the flexibility and value of a VCE - Value Chain Economy
		DApp	Software which does not rely on a central system or database but can share information amongst its users via a decentralized database, such as a blockchain.	Key Differences between DApps and Smart Contracts Scope: A DApp includes not only the smart contracts (back end) but also the user interface (front end) that interacts with the blockchain. Smart contracts are just one part of a DApp. Functionality: Smart contracts define the rules and operate as the backbone of the DApp, executing agreed-upon terms automatically. DApps use these smart contracts to interact with the blockchain in a user-friendly way. Complexity: DApps can be more complex, often involving multiple smart contracts and additional features like handling user interactions, processing data, and connecting to other applications.
		Decentralized Network	A system with no single point where the decision is made. Every node makes a decision for its own behavior and the resulting system behavior is the aggregate response.	compare to centralized system or services
		Decentralized ID (or DID)	A DID is a unique identifier not containing any personally identifiable information. They are publicly available and owned by the person, asset, or company. (see verifiable credential) In a VC world, people, assets and organizations have a Decentralized Identifier (DID).	part of Self-Sovereign Identity - a stronger identity system than normal digitial identity
		DeFi - Decentralized Finance	A system of financial applications and services built on blockchain technology that enables peer-to-peer transactions without the need for intermediaries.	
		ReFi - Reimagined Finance	Combines decentralization, digital technologies from DeFi (cryptography, blockchain, tokens, digital assets, identities) with better trusts, smart events, compliance, policies, risk controls, integration from Traditional Finance systems	technology behind VCE

rank	type	term	definition	Concept
		Digital Identity (SSI)	The network or Internet equivalent to the real identity of a person or entity (like a business or government agency). Advocates of blockchain-based digital identity is to return ownership and control of personal information to the individuals. In any given transaction, personal information is not disclosed, but rather the information required by one party is verified by the digital identity application.	
		Digital Signature	A mathematical scheme for verifying digital messages or documents satisfy two requirements - they have authenticity (from a known sender) and integrity (were not altered in transit.	
		Distributed	As opposed to decentralized, a distributed system shares processing and/or data across multiple nodes, but the decisions may still be centralized and use complete system knowledge.	
		Double Spend Problem	A unique problem to cryptocurrency where the same coins or tokens are spent or traded twice.	How do you ensure a digital currency is only spent once?
		Ethereum	A public blockchain that supports smart contracts that uses the EVM (Ethereum Virtual Machine) to process smart contracts. Other blockchains can be 'EVM" compatible (see Polygon etc)	
		Fungilble	The property an item of being exchangeable with other like items. For example, USD and Euros are fungible. The value of USD can be expressed in Euros. College Diplomas are "Non-fungible" - my Batchelors degree is issued uniquely to me - not generic	Non-fungible would be a unique painting or NFT token
		Gas	.A fee charged to write a transaction to a public blockchain. The gas is used to reward the miner which validates the transaction.	Normal but not always required for a public blockchain
		Governance	Establishment of policies and continuous monitoring of their proper implementation of an organization or system.	A policy could be reporting any bank withdrawal over $5000 to the IRS. How is the policy implemented? Is it effective?
		Governance token	A type of token that grants holders the right to vote on key decisions related to the development and management of a blockchain ecosystem. Used in a DAO or DeFi projects.	a holder has a vote in policy decisions for the organization or group
		Hash	An encrypted string generated from A hash function that receives an input of any size and returns a unique string of a uniform length.	
		Identity	The information on an entity used by computer systems to uniquely represent a person, organization, application, or device.	
		Hyperledger Fabric	Open source Enterrprise Blockchain platform for private permissioned blockchains that scale and integrate well across networks with other systems	
		Hyperledger Besu	Open source middleware that creates permissioned access controls for Ethereum compatible blockchains	
		Hyperledger Firefly	Open source middleware that connects and integrates services using APIs for blockchain platforms it is connected to.	Connects to Besu, Fabric, Corda etc
		Immutability	The property of being unchangeable. Once a transaction has been added to a block and written to a blockchain, it cannot be changed and therefore is immutable.	
		Interoperability	The ability of two or more systems to communicate and exchange data. Due to various design decisions (e.g., consensus protocol) most blockchains are not interoperable, however there are many projects that are working to connect various blockchains.	
		IPFS (Interplanetary File System)	A peer-to-peer hypermedia protocol for storing and sharing data in a distributed file system using content-addressing to uniquely identify each file in a global namespace connecting all computing devices.	widely used to share files effectively over distributed network nodes. Firefly uses IPFS to distribute event notifications from source to target nodes
		Liquidity	The ease of converting an asset (or, in this case, cryptocurrency) to cash (fiat).	used often for crypto (Ether or ?) coin conversions ot fiat but could also refer to conversion to a crypto reserve currency
		Mainnet	The production version of a blockchain.	different than dev or QA environments

rank	type	term	definition	Concept
		Testnet	A dev or QA version of a blockchain	
		Merkle Tree / Hash Tree	In cryptography and computer science, a Merkle or hash tree is a tree in which every leaf node is labeled with the hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.	
		Node	A computer which holds a copy of the blockchain ledger.	
		NFT - Non-fungible Token	A unique digital asset that is stored on a blockchain and represents ownership of a specific item, such as artwork or music.	Think NFT for an automobile with the VIN as the unique ID
		Off-chain data	Data stored external to the blockchain.	typically PII (Personal identification Information) is off-chain (eg ssn)
		On-chain data	Data stored on the blockchain.	
		Oracle	An application that connects blockchain applications to legacy applications.	usually a call to an external app DURING the execution of a Dapp or smart contract
		Provenance	The entire history of a product during its lifecycle including its chain of custody and all documentation of value-added services and activities which were used to produce that product or service.	
		Public / Private Key Pairs	Digital Signatures: Public and private keys can be used to create a digital signature, which assures that the person sending the message is who they claim to be. Typically, the recipient's public key is used to encrypt the data and the recipient then uses their private key to decrypt the data	
		Sharding	A type of database partitioning that separates very large databases the into smaller, faster, more easily managed parts called data shards. Sharding can potentially be used to improve blockchain performance.	often used to speed data processing in parallel streams
		Sidechain	A discrete blockchain that is linked to a main blockchain via two-way pegs which enable assets to be interchanged between the main blockchain and the sidechain. Sidechains are a method to enable scaling and increase transaction speed by only performing necessary transactions on the main blockchain.	L2 sidechains are common for EVM blockchains to overcome the performance problems of Ethereum
		Smart Contract	Self-executing computer code deployed on a blockchain to perform a function, often, but not always, the exchange of value between a buyer and a seller.	
		Solidity	A JavaScript-like object-oriented programming language for Ethereum for implementing smart contracts on the Ethereum blockchain.	
		Stablecoin	A cryptocurrency which is underwritten by an asset or assets (e.g., fiat currency, commodities, etc.) designed to minimize the volatility of the price of the coin/token.	
		State channel	A process by which blockchain transactions are executed off- chain, collected and then written to the main chain as a single transaction in order to improve performance and reduce cost.	
		Token	Cryptographic tokens represent programmable assets or access rights, managed by a smart contract and an underlying distributed ledger. They are accessible only by the person who has the private key for that address and can only be signed using this private key.	There are different token types defined in the EVM token standards - ERC-20 - a fungible token, ERC-721- a non-fungible token, ERC-1155 - a flexble token type etc Tokens are created (minted), stored, traded or spent or exchanged, destroyed (burned - usually after spending)
		Token - ERC-20	A type of fungible Ethereum token (i.e., smart contract) standard which is defined by a series of functions that must be supported, including functions to retrieve the total supply, transfer from one wallet to another, and approve a transaction. Typically, any given ERC-20 token has many copies which are held in a variety of crypto wallets.	
		Token - ERC-721	A type of non-fungible Ethereum token (i.e., smart contract) standard which is defined by a series of functions that must be supported, including functions to retrieve the total supply, transfer from one wallet to another, and approve a transaction. Each ERC-721 token is unique and non-interchangeable with other tokens (i.e., non-fungible).	
		Token Types	There is a token taxonomy. A simple view shows token types that are coins, assets, utilities, payment, access or reward tokens	

rank	type	term	definition	Concept
		Tokenomics	The study, design and implementation of monetary management and distribution based on blockchain technology.	
		Transparency	A primary property of public blockchains whereby any participant in a system or transaction can view the transactions on the blockchain.	
		Trusts	Confidence in the integrity of an entity, an asset, a state, an authorization etc (e.g., person, organization, etc.).	
		Trustless	The elimination of trust from a transaction. Blockchain is called a trustless system because the two entities performing a transaction do not need to trust one another. The properties of blockchain - digital signatures, cryptography, etc. - provide the trust.	
		Verifiable Credential	In its simplest form, a Verifiable Credential is a document that can be reliably traced back to its source and validated as genuine.	
		Wallet - Digital - cold or hot	A digital file that holds coins and tokens held by the owner. The wallet also has a blockchain address to which transactions can be sent. Hot wallet - connected to the network for transactions Cold wallet - holds digital assets, tokens, files etc that is not now connected to a network (eg for custody etc)	
		Web3	Internet solutions, where blockchain technology is used to create decentralized applications and services that are more secure, transparent, and trustworthy. Web3 is a term used to describe the third generation of the World Wide Web, which is being developed to provide a more decentralized and user-centric internet experience.	
		ZKP or Zero Knowledge Proof	The ability to share proof of something, without disclosing details that prove this information to be true. For example proving you're over 21 without showing your birthday.	rather than share data (eg a password etc), I can prove identity using a ZKP. The ZKP proves I am who I claim to be WITHOUT sharing the identity data itself to another party which is a security risk