Blockchain Key Terminologies list - Cheat Sheet

by DaveLee via cheatography.com/186743/cs/39919/

Blockchain terminology

1. Blockchain
Blockchain is an incredible technology that lies at the core of cryptocurrencies and other amazing decentralized applications. In simple terms, it acts like a digital ledger spread across multiple computers or nodes.It keeps track of transactions and verifies them without relying on any central authority.
2. Cryptocurrency
Cryptocurrency is a form of virtual or digital currency that operates on the principles of the blockchain networks. These currencies leverage cryptographics to ensure safe and secure transactions, all while controlling the creation of new units.
3. Distributed Ledger
Picture this: a database that's not locked up in some single, big vault. That's a distributed ledger for you! It's a decentralized database distributed across multiple participants or locations, ensuring transparency and integrity. Blockchains are the perfect example of distributed ledgers, offering a transparent, trustable, and tamper-proof record of all transactions.
4. Node
Nodes are like the backbone of a blockchain network. They are individual computers or devices that participate in the network by maintaining a copy of the entire blockchain and validating transactions. Nodes work together to achieve consensus and keep the network secure.
5. Consensus Algorithm
Consensus algorithms are the secret sauce that makes blockchain networks tick! They serve as the referees of the system, ensuring that all the players (nodes) agree on what's legit and what's not. You've got Proof of Work (PoW), where miners flex their computational muscles to solve puzzles and reach agreement, and Proof of Stake (PoS), where validators get to the front of the line based on the number of coins they've got in their pockets.
6. Mining
Mining is the heart and soul of blockchain networks. It's like a race, where miners use their computers to solve tough math problems. The first one to crack the code gets to add a new block to the blockchain and scores rewards in the form of shiny new cryptocurrency.
7. Smart Contract
Smart contracts are self-executing contracts with predefined rules written into code. They automatically execute and enforce the terms of the agreement when specific conditions are met. Smart contracts eliminate the need for intermediaries and provide trustless automation.
8. Wallet

Blockchain terminology (cont)

A cryptocurrency wallet is your safe haven, where you store, send, and receive your digital coins. There are software-based ones (online, desktop, or mobile) and more robust hardware-based wallets that you can physically hold.
9. Public Key Cryptography
Who doesn't love secrets and keys? Public key cryptography is like a magic lock and key system. You've got a pair of keys: a public key you share with others, so they can send you secret messages, and a private key that you keep hush-hush to unlock those encrypted messages.
10. Private Key
Your private key is like the ultimate VIP pass in the crypto world. Guard it with your life! It's your secret ticket to access and control your digital wealth. With this key, you're the boss of your cryptocurrencies, and nobody else gets a say.
11. Public Key
The public key is like your digital address where everyone can send you virtual gifts (cryptocurrencies!). It's created from your private key, and you can freely share it without any worries. Just make sure you don't mix it up with the private one!
12. Hash Function
Hash functions are like superheroes, protecting the integrity of the blockchain. They're these clever math wizards that turn data into unique, fixed-size codes called hashes. Even the tiniest change in data results in a completely different hash, so you know when something fishy's going on.
13. Block
Picture blocks like treasure chests in a never-ending adventure. Each block is a container filled with precious verified transactions. It has a unique ID, a time stamp, a list of transactions, and a special reference to the previous block. Together, they create a grand chain of blocks—the blockchain!
14. Merkle Tree
Merkle trees are ingenious data structures that organize transactions in a tree-like manner. Each leaf node represents a transaction, and each non-leaf node is the hash of its children. Merkle trees enable efficient verification of data integrity in the blockchain.
15. Fork
A fork happens when a blockchain splits into two or more separate chains, often due to disagreements in the community or protocol upgrades. There are temporary forks, while soft and hard forks result in permanent divergence. Soft forks are also backwards compatible.
16. Immutable

Blockchain terminology (cont)

The immutability of the blockchain is a crucial feature ensuring that once a transaction is recorded, it cannot be altered or deleted. This attribute enhances transparency and fosters trust in the system, as all transactions remain permanently stored and visible to all participants.
17. Decentralization
Decentralization is one of the core principles of blockchain technology. It refers to the distribution of power and decision-making across a network of nodes instead of relying on a single central authority.
18. 51% Attack
A 51% attack is a hypothetical situation where a single entity gains control of over 50% of the network's computational power. This could allow the attacker to manipulate transactions or double-spend coins, undermining the security of the blockchain.
19. Interoperability
Interoperability is the key to unlocking the full potential of blockchain technology. It refers to the seamless communication and data-sharing between different blockchain networks. This capability opens up avenues for collaboration and innovation, as assets and information can flow freely between otherwise disconnected blockchains.
20. Tokenization
Tokenization involves converting real-world assets, like property rights or physical goods, into digital tokens on a blockchain. These tokens represent ownership or value and can be securely and transparently traded or transferred.
21. Gas
In the context of blockchain networks such as Ethereum, gas is a unit of measurement representing the computational power required to perform a transaction or execute a smart contract. Users pay gas fees as an incentive for miners/validators to process their transactions efficiently and promptly.
22. Token Standards
Token standards define the rules and functionalities that a token should adhere to on a blockchain network. For instance, ERC-20 is a widely used standard on Ethereum, governing the behavior of fungible tokens, while ERC-721 governs non-fungible tokens (NFTs).
23. ICO (Initial Coin Offering)
An ICO is a fundraising method where new cryptocurrencies or tokens are sold to investors in exchange for established cryptocurrencies like Bitcoin or Ethereum. ICOs were popular in the early days of blockchain projects but have since faced regulatory challenges in some regions.
24. DApp (Decentralized Application)

Blockchain terminology (cont)

A DApp is an application that runs on a decentralized network, such as a blockchain. Unlike traditional apps, DApps leverage the blockchain's decentralized nature, offering transparency, security, and censorship resistance.
25. DAO (Decentralized Autonomous Organization)
A DAO is an organization that operates through rules encoded as smart contracts on a blockchain. DAOs allow for decentralized decision-making and governance, where stakeholders can vote on proposals to influence the organization's actions.

Blockchain terminology II

26. On-chain and Off-chain Transactions
On-chain transactions occur directly on the blockchain, where each transaction is recorded and visible to all participants. Off-chain transactions happen outside the blockchain, enabling faster and more scalable transactions, albeit at times requiring trusted intermediaries.
27. Private Blockchain
A private blockchain is a closed or permissioned network where access is restricted to authorized participants. It is often used by enterprises seeking the benefits of blockchain technology while maintaining control over data and participants.
28. Public Blockchain
Public blockchains are open and permissionless networks, allowing anyone to join, participate in consensus, and read or write data. Examples like Bitcoin and Ethereum exemplify these platforms where transparency and decentralization are core principles, making them accessible to a broad user base.
29. Sidechain
Sidechains represent separate blockchains running alongside the main blockchain and interconnected to it. They serve as experimental environments for implementing new features and scalability solutions without compromising the security of the main chain.
30. Lightning Network
The Lightning Network emerges as a secondary solution for scaling blockchains, facilitating faster and more cost-effective transactions by processing them off-chain. Smart contracts underpin this network, ensuring security while enhancing the overall capacity of the blockchain.
31. Gas Limit and Gas Price
In Ethereum, the gas limit denotes the maximum amount of gas that a block can consume. Meanwhile, the gas price refers to the amount of cryptocurrency paid per unit of gas, which incentivizes miners to process transactions efficiently and prioritize those with higher gas fees.
32. Oracles

Blockchain terminology II (cont)

Oracles are data feeds that provide external information to a smart contract on a blockchain. They enable smart contracts to interact with real-world data, making them more versatile and enabling various use cases, such as decentralized finance (DeFi) applications.
33. Scaling Solutions
Blockchain networks face challenges with scalability, which refers to their ability to handle a large number of transactions. Various scaling solutions, like sharding, state channels, and layer-2 protocols, aim to address these limitations and improve blockchain throughput.
34. Web3.0
Web3.0 refers to the next generation of the internet, where decentralized technologies like blockchain play a central role. It envisions a more user-centric, open, and trustless internet, where users have greater control over their data and digital assets.
35. Immutable Ledger
The immutability of a blockchain ledger ensures that once data is recorded on the blockchain, it cannot be altered, deleted, or tampered with. This feature enhances the security and reliability of the data stored on the blockchain.
36. Token Economy
A token economy is an ecosystem built around a blockchain platform where various tokens are used to represent and exchange value. These tokens can serve as currency, governance rights, access tokens, or even represent real-world assets.
37. Zero-Knowledge Proofs (ZKPs)
Zero-knowledge proofs are cryptographic protocols that allow one party to prove knowledge of specific information to another party without revealing the actual information itself. ZKPs are used for privacy-preserving transactions and identity verification on blockchains.
38.Cross-Chain Interoperability
Cross-chain interoperability represents a remarkable advancement that facilitates seamless communication and interaction between distinct blockchain networks. This breakthrough enables the smooth transfer of assets or data across different blockchains, fostering collaboration and expanding the overall utility of blockchain technology.
39.Token Standards (e.g., ERC-1155)
In addition to well-known token standards like ERC-20 and ERC-721, there are other notable standards such as ERC-1155, which allows for the creation of both fungible and non-fungible tokens within a single smart contract. The gaming and digital collectibles industries have widely embraced this standard for its flexibility and efficiency.
40. Atomic Swaps

Blockchain terminology II (cont)

Atomic swaps allow for direct peer-to-peer exchange of cryptocurrencies across different blockchain networks without the need for intermediaries like exchanges. They ensure trustless and secure cross-chain transactions.
41. Signature Schemes (e.g., ECDSA, EdDSA)
Signature schemes are cryptographic algorithms used to create and verify digital signatures. ECDSA (Elliptic Curve Digital Signature Algorithm) and EdDSA (Edwards-curve Digital Signature Algorithm) are examples widely used in blockchain networks.
42. Fork Choice Rule
The fork choice rule is the algorithm that determines which blockchain version will be considered the valid chain in the event of a fork. In Proof of Work systems, the longest chain is generally chosen, while Proof of Stake networks use various mechanisms to decide the canonical chain.
43. Gas Token
Gas tokens are special tokens that can be created and burned to store or release gas on the Ethereum network. Users can use gas tokens to optimize gas costs during periods of low network activity and save on transaction fees.
44. Sybil Attack
The Sybil attack remains a significant concern in the realm of cybersecurity. In this malicious attack, adversaries create numerous fake identities or nodes to gain unwarranted control or influence over a network. Decentralized networks are particularly susceptible to Sybil attacks, posing a threat to their integrity and security.
45. Plasma
Plasma is a framework for creating scalable and secure off-chain solutions for blockchains. It enables the creation of child chains that can process transactions more quickly and later reconcile the data back to the main chain.
46. DAO Attack
A DAO attack occurs when malicious actors exploit vulnerabilities in a decentralized autonomous organization's smart contracts to steal or manipulate funds. The most famous example is the "DAO hack" in 2016, which led to a contentious hard fork resulting in Ethereum and Ethereum Classic.
47.Ring Signature
Ring signatures represent a fascinating cryptographic technique that empowers a user to sign a message on behalf of a group or "ring" of users, while cleverly concealing the actual signer's identity within the group. This technique finds valuable applications in enhancing privacy and anonymity within certain blockchain use-cases.
48.Self-Sovereign Identity

Blockchain terminology II (cont)

Self-sovereign identity introduces a compelling concept where individuals are granted complete control and ownership over their digital identities. Thanks to the ingenious application of blockchain technology, we can now achieve secure and decentralized identity management solutions, putting the power back into the hands of users themselves.
49. HSMs in Blockchain
Hardware Security Modules (HSMs) are specialized, tamper-resistant hardware devices designed to manage and protect cryptographic keys. In the blockchain world, they offer an additional layer of security for private keys, ensuring that transactions and wallet accesses are secure. HSMs also play a role in safeguarding the infrastructure of blockchain networks, enhancing resilience against breaches, thefts, and unauthorized access.
50. Decentralized Finance (DeFi)
Decentralized Finance, commonly known as DeFi, represents a set of financial protocols and services built on blockchain platforms, especially Ethereum. Unlike traditional financial systems, DeFi operates without intermediaries like banks or brokers. Instead, it uses smart contracts to create programmable, transparent, and open-source financial instruments. Popular DeFi applications include lending platforms, decentralized exchanges, and stablecoins. Through DeFi, users can lend, borrow, trade, and invest in a decentralized ecosystem, fostering greater financial inclusivity and sovereignty.. Blockchain technology is vast and rapidly evolving, with new terminologies and advancements emerging regularly. Staying curious and keeping up with the latest developments will help you stay ahead in this exciting and transformative space.

Learn more:
[1] HSM for Blockchain Technologies

[2] Key Management for wallets/blockchain

[3]Blockchain online courses