Blockchain Fundamentals

What is a blockchain?

A **blockchain** is a distributed, cryptographically-secure database structure that allows network participants to establish a trusted and immutable record of transactional data without the need for intermediaries. A blockchain can execute a variety of functions beyond transaction settlement, such as smart contracts. Smart contracts are digital agreements that are embedded in code and that can have limitless formats and conditions. Blockchains have proven themselves as superior solutions for securely coordinating data, but they are capable of much more, including tokenization, incentive design, attack-resistance, and reducing counterparty risk. The very first blockchain was the Bitcoin blockchain, which itself was a culmination of over a century of **advancements in cryptography and database technology.**

What is blockchain software?

Blockchain software is like any other software. The first of its kind was Bitcoin, which was released as **open source software**, making it available to anyone to use or change. There are a wide variety of efforts across the blockchain ecosystem to improve upon Bitcoin's original software. Ethereum has its own open source blockchain software. Some blockchain software is proprietary and not available to the public.

What is a blockchain database?

Historically, databases have incorporated a centralized client-server architecture, in which a sole authority controls the central server. This design means that data security, alteration, and deletion rests with a single point of failure. The decentralized architecture of blockchain databases emerged as a solution for many of the weaknesses of centralized database architecture. A blockchain network consists of a large number of distributed nodes—voluntary participants who must reach consensus and maintain a single transactional record together.

What is a blockchain system?

A blockchain system refers to all the aspects and features that go into a particular blockchain, everything from the consensus algorithm to the state machine to cryptographic functions. As Andreas Antonopoulus and Gavin Wood note in ***Mastering Ethereum***, there are "a huge variety of blockchains with different properties"—qualifiers "help us understand the characteristics of the blockchain in question, such as *open, public, decentralized, neutral,* and *censorship-resistant.*"

How does a blockchain work?

When a digital transaction occurs in a blockchain network, it is grouped together in a cryptographically-secure “block” with other transactions that have occurred in the same time frame. The block is then broadcast to the network. A blockchain network is comprised of nodes or participants who validate and relay transaction information. The block of transactions is verified by participants called miners, who use computing power to solve a cryptographic puzzle and validate the block of transactions. The first miner to solve and validate the block is rewarded. Each verified block is connected to the previously verified block, creating a chain of blocks. One important cryptographic underpinning of blockchains is the hash function. Hashing assigns a fixed value to a string that is inputted into the system. Blockchain hashing power results in a deterministic, quickly-computable, and preimage-resistant system. Explore our knowledge base to learn more about **how a blockchain works.**

What is a blockchain application?

Blockchain applications are comparable to conventional software applications, except they implement a decentralized architecture and cryptoeconomic systems to increase security, foster trust, tokenize assets, and design new network incentives. Here are **over 90 Ethereum apps** that are currently being used across the Ethereum blockchain ecosystem, from prediction markets to smart legal agreements.

What are the benefits of blockchain technology?

Blockchain technology has a wide variety of benefits, for both global enterprises and local communities. The most commonly cited **benefits of a blockchain** are trusted data coordination, attack-resistance, shared IT infrastructure, tokenization, and built-in incentivization.

What is the blockchain revolution?

Blockchain is considered a disruptive technology because of its ability to safeguard personal information, reduce intermediaries, unlock digital assets, and potentially open up the global economy to millions more participants. Sometimes called the Trust Machine, blockchain technology is bringing transparency and security to digital networks across **countless industries.** In many ways, the blockchain revolution can be considered a revolution in trust.

What is decentralized finance (DeFi)?

Decentralized finance—often called DeFi or open finance—refers to the economic paradigm shift enabled by decentralized technologies, particularly blockchain networks. DeFi signals the shift from a historically centralized and closed financial system toward a universally accessible economy that

is based on open protocols that are interoperable, programmable, and composable. From streamlined and secure payment networks to automated loans to USD-pegged stablecoins, decentralized finance has emerged as **one of the most active sectors in the blockchain space**. Some of the defining factors of a DeFi application include permissionless architecture (anyone can participate), transparent and auditable code, and interoperability with other DeFi products. **DeFi Score** offers a single, consistently comparable value for measuring DeFi platform risk.

What is a block in a blockchain?

The "block" in a blockchain refers to a block of transactions that has been broadcast to the network. The "chain" refers to a string of these blocks. When a new block of transactions is validated by the network, it is attached to the end of an existing chain. This chain of blocks is an ever-growing ledger of transactions that the network has validated. We call this single, agreed-upon history of transactions a blockchain. Only one block can exist at a given chain height. There are several ways to add new blocks to an existing chain. These are often termed "proofs," i.e. Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA). All involve cryptographic algorithms with varying degrees of complexity.

What is block time?

Depending upon how a particular blockchain protocol was developed, the time that it takes for a block to be added to the canonical chain can vary widely. A blockchain is a linear construct in that every new block occurs at a later time than the one that preceded it and cannot be undone. A blockchain's linearity serves as an ideal form of validation. According to **ethstats.io** as of July 2019, for the Ethereum blockchain, new blocks are added approximately every 14 seconds.

What is distributed ledger technology?

Distributed ledger technology is a broad category that encompasses blockchain technology. A **distributed ledger** is just what its name implies. Instead of accounting for data through one centralized computer, distributed ledger technology uses many participants in a network to maintain a digital record. Blockchain technology supplements a distributed ledger with cryptographic functions and a consensus algorithm to enable greater incentive design, security, accountability, cooperation, and trust.

What is a blockchain wallet?

A blockchain wallet contains the **public key** for others to transfer cryptocurrency to your address and the **private key** so you can securely access your own digital assets. A blockchain wallet usually

accompanies node hosting and stores cryptocurrencies on your computer. The safest place for storing digital assets is offline, what is often called “cold storage.” Read **“7 Pro Tips for Keeping Your Crypto Safe”** for some best practices on protecting your digital assets.

What is blockchain programming?

As a new technology that makes use of global digital networks, the need for blockchain programmers is immense, and in recent years, programmers have flocked to the blockchain space. A key aspect that distinguishes blockchain programming from other Internet ventures is the focus on security and cryptography. **Consensys Academy’s Developer Program** offers programmers from any background the chance to become a blockchain expert in weeks. Industry experts from around the world teach the course, which focuses on Ethereum blockchain development.

What is a blockchain company?

A blockchain company is simply a company that is invested in and/or developing blockchain technology. **State of the Dapps** ranks blockchain-based decentralized applications by user activity and Forbes recently released a report covering the **top 50 billion-dollar companies exploring blockchain.**

What is a private blockchain?

Blockchains began as open source, public efforts. Private blockchains were developed as corporations and other administrative bodies began to realize the benefits of distributed ledger technology, particularly within systems of a private enterprise and when managing sensitive transaction data. With increasingly robust and modular privacy and permissioning solutions, industry experts anticipate that **private and public blockchain networks will converge**.

What are zk-SNARKs?

zk-SNARK is an acryonym for *zero-knowledge succinct non-interactive argument of knowledge*, a cryptographic proof system that enables a user to verify a transaction without revealing the actual data of the transaction, and without interacting with the user who published the transaction. In the context of a blockchain, zk-SNARKs allow users to maintain private transactions, while still validating the transactions according to the network’s consensus algorithm. For a technical walkthrough of zk-SNARKs, check out our **introduction to zk-SNARKs.**