Quick Answer: What Is Blockchain?

Published 8 September 2021 - ID G00754335 - 5 min read

Avivah Litan

Initiatives: Applications and Software Engineering Leaders

The hype about blockchain has created confusion, disillusionment and experimentation. Applications and software engineering leaders must prepare for the inevitable production-ready blockchain innovations by having a clear understanding of the technology to explain it to their board and CEO.

Quick Answer
What Is blockchain?

- Blockchain is a distributed, write-only ledger that records transactions between participants.
- Blockchain is one specific type of distributed ledger (that is, all blockchains are distributed ledgers, but not all distributed ledgers are blockchains).
- Distributed ledgers such as blockchain offer a way to securely and efficiently create a tamper-proof log of sensitive activity.

More Detail

Blockchain Definition

“Blockchain is a distributed, write-only ledger that records transactions between participants. It is designed to record transactions or digital interactions and bring much needed transparency, efficiency and added security.”
A blockchain is an expanding list of cryptographically signed, irrevocable blocks of records shared by all participants in a peer-to-peer (P2P) network. Each block of records is time-stamped and references links to previous data blocks. Blocks are added to the blockchain after validators achieve consensus on the validity of the transaction. Anyone can historically trace a state change in data or an event belonging to any participant. Distributed ledgers are design-limited, lack decentralized and tokenized elements, and can support access management rights.

**Blockchain Is One Specific Type of Distributed Ledger**

Gartner doesn't necessarily like the term "blockchain" when used for permissioned blockchain networks (since they are not decentralized), but we go along with it for the sake of simple communications. Blockchain is similar to the use of the term “cloud,” in that it’s a bit vague and could mean a number of different things. If you were to give the elevator pitch to your CEO or board of directors to explain blockchain, you might describe it as:

*Blockchain is a radically decentralized platform for radically decentralized applications.*

The fundamental aspect to understand is that blockchain is just one type of distributed ledger. Although it is a sequence of blocks, distributed ledgers do not require such a chain. All blockchains are distributed ledgers, but not all distributed ledgers are blockchains. Whereas a blockchain represents a type of distributed ledger, it is also merely a subset of them. Furthermore, distributed ledgers don’t use proof of work (PoW) or mining; there are other consensus algorithms that are less decentralized but still provide notarization and ordering of transactions. When we’re talking about distributed ledgers, we’re generally referring to information sharing among a predefined or discrete group of participants. In enterprise-permissioned use cases, it’s about mutualization of infrastructure rather than anonymous censorship-resistant transactions.

In this blockchain context, you may well ask, "What is a ledger?" A ledger is an authoritative record of data or events deemed significant that participants want to record immutably. That event could be a monetary transaction or something else. For example, it could be valuable metadata that links to a medical record or government identity record, or a shipping metadata record for supply chain or logistics, or tokenized oil and gas geologic samples. It’s valuable data that is recorded as a permanent, immutable, tamperproof, uncensorable record. This is a key value of blockchain — it adds *trust*. It’s a trusted record created in an untrusted environment.
But how do you get that trust? You get it through the distributed part of the ledger. "Distributed" means that it’s replicated across potentially tens of thousands of nodes (if in a public network, for example). Therefore, if you’re a bad actor, there isn’t just one system to attack; instead, you have to attack thousands of nodes spread out all over the world. You don’t know where they are located, and they can be in different data centers run by different parties that don’t know each other or of each other.

On the other hand, permissioned blockchains, which are suitable for enterprise use, tend to be less secure as they introduce a central point of weakness. It’s much easier to break into a few nodes than tens of thousands distributed all over the world, most of which you don’t know the location for. So in theory, permissioned blockchains are less scalable in terms of the number of nodes because the consensus algorithms that many of them use are PBFT or a variant thereof. That has never really been used at scale for more than 10 machines in a network, unlike public blockchains that have algorithms running for tens of thousands of machines. So they’re less secure and less scalable in terms of number of nodes.

The key point to realize is that any central data system can and will be attacked no matter how well defended. So there’s safety in numbers, and you don’t put all your eggs in one basket — you spread them out over the entire network. The larger the network, the more trust there is, assuming the protocols work, and that's the mantra to remember with distributed ledger technology:

You don’t trust systems. You don’t trust people. You trust cryptography and the majority of nodes in the network.

Benefits of Distributed Ledgers Such as Blockchain

Distributed ledgers such as blockchain offer a way to securely and efficiently create a tamper-proof log of sensitive activity. For example, when distributed ledgers such as blockchain are used for financial transactions, they cut down on operational inefficiencies. An increased level of security is also created due to their decentralized nature, as well as the fact that the ledgers are immutable.

Other potential use cases range from international money transfers to shareholder records. Financial processes are radically enhanced to offer companies a secure, digital alternative to processes run by a clearinghouse. Removing the intermediary party from the equation is what makes the concept of distributed ledger technology so appealing.
When you write data to a blockchain, it’s permanently recorded on the network. When you have a series of transactions over time, you gain an accurate and immutable audit trail. This is very useful for financial audits. Having stored data where no single entity owns or controls it, and no one can change what’s already written, provides benefits similar to double-entry book-keeping. Ultimately, this means that there are fewer chances of errors or fraud.

**Recommended by the Authors**

Hype Cycle for Blockchain, 2021

Common Mistakes to Avoid in Enterprise Blockchain Projects

Assessing the Optimal Blockchain Technology for Your Use Case

Bitcoin Goes Mainstream: What It Means to You

Truth and Transparency in Supply Chain: 3 Case Studies on How Blockchain, AI and IoT Are Shedding Light

DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

Quick Answer: How to Protect and Secure the Use and Trading of NFTs

The Future of Blockchain: 8 Scalability Hurdles to Enterprise Adoption