What is a Blockchain?

A *public*[1]*, permanent*[2]*, append-only*[3] *distributed*[4] *ledger*[5].

1. Though some blockchains require permission to access, "open" blockchains like those underlying Bitcoin and Ethereum are accessible to anyone, meaning the database is public information
2. It's next to impossible for bad actors to tamper with data encoded in a blockchain, if it's properly set up.
3. Old transactions can't be changed in a properly functioning blockchain; only new ones can be added.
4. No single entity owns or controls a public blockchain. A network of computers maintains and secures the database, and each participant, or "node," stores a copy.
5. The original blockchain, Bitcoin, is a ledger for tracking currency balances. But the same basic method can work for all kinds of digital assets.

What's that?

A mathematical structure for storing data in a way that is nearly impossible to fake. It can be used for all kinds of valuable data.

Where did it come from?

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." These are the words of Satoshi Nakamoto, the mysterious creator of Bitcoin, in a message sent to a cryptography-focused mailing list in October 2008. Included was a link to a nine-page white paper describing a technology that some are now convinced will disrupt the financial system.

What is blockchain for?
It's a new way of answering an old question: how can we create enough trust between one another to peacefully exchange something of value?
Enforcement—*Early civilizations used threat of force as retribution for dealing in bad faith when engaging in trade.*
Institutions—*The emergence of governments and banks provided organized, central authorities to which we could outsource trust—as long as we trusted them.*

The Network—*Blockchains distributed across thousands of computers can mechanize trust, opening the door to new ways of organizing "decentralized" enterprises and institutions.*

Nakamoto mined the first bitcoins in January 2009, and with that, the cryptocurrency era was born. Nakamoto combined established cryptography tools with methods derived from decades of computer science research to enable a public network of participants who don't necessarily trust each other to agree, over and over, that a shared accounting ledger reflects the truth. This makes it virtually impossible for someone to spend the same bitcoin twice, solving a problem that had hindered previous attempts to create digital cash. And, crucially, it eliminates the need for a central authority to mediate electronic exchange of the currency.

Soon, technologists realized that blockchains could be used to track other things besides money. In 2013, 19-year-old Vitalik Buterin proposed Ethereum, which would record not only currency transactions but also the status of computer programs called smart contracts. Launched in 2015, Ethereum—and now a host of competitors and imitators—promises to make possible a new generation of applications that look and feel like today's web apps but are powered by decentralized cryptocurrency networks instead of a company's servers.