What is Blockchain?

"The practical consequence […is…] for the first time, a way for one internet user to transfer a unique piece of digital property to another internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."
– Marc Andreessen

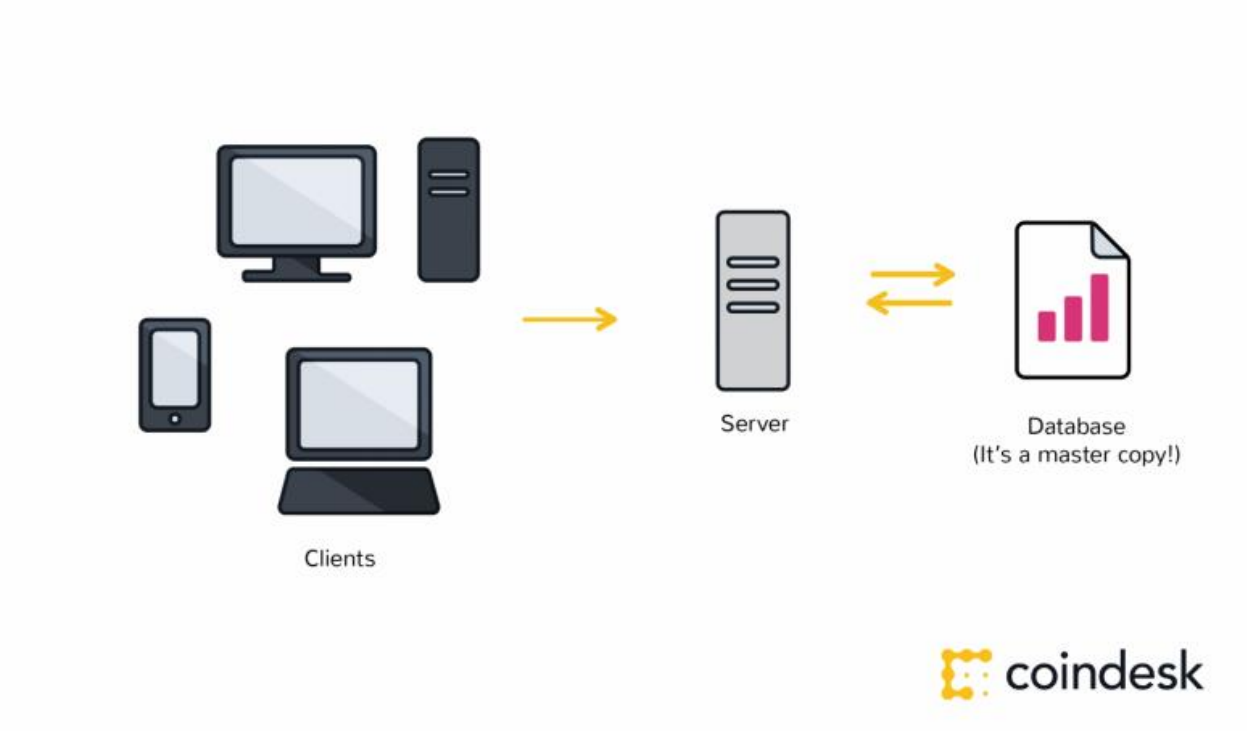
From a cruising altitude, a blockchain might not look that different from other decentralized digital systems – like, say, Wikipedia.

With a blockchain, many people can write entries into a record of information, and a community of users can control how the record of information is amended and updated. Likewise, Wikipedia entries are not the product of a single publisher. No one person controls the information.

Descending to ground level, however, the differences that make blockchain technology unique become more clear. While both run on distributed networks (the internet), Wikipedia is built into the World Wide Web using a client-server network model.

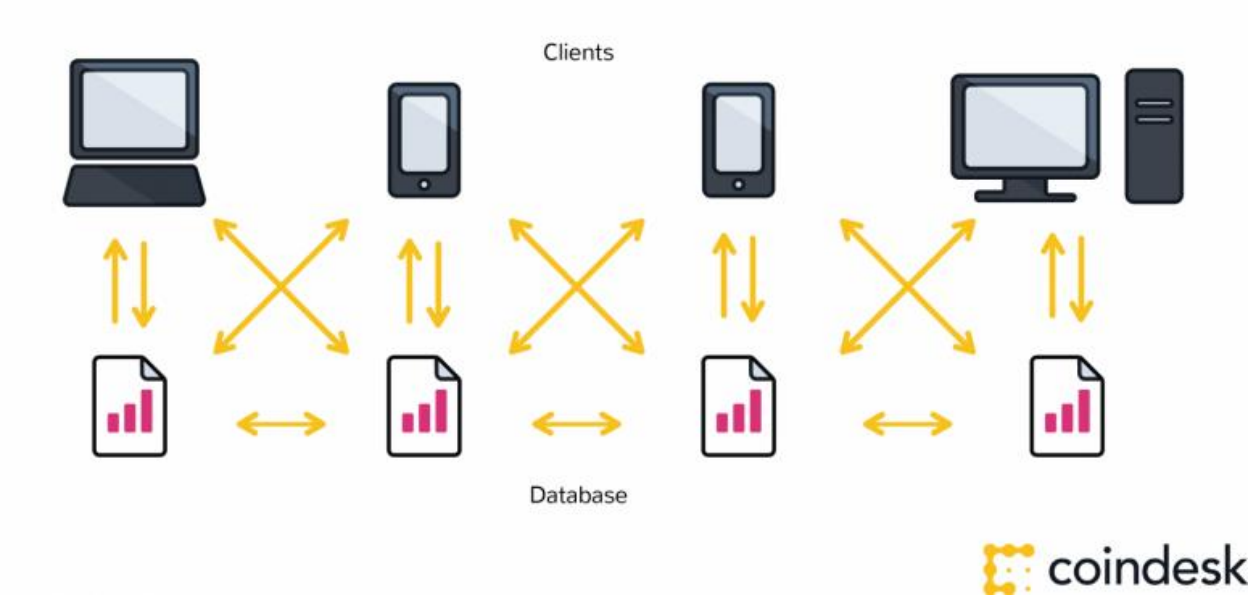
A user (client) with permissions associated with its account is able to change Wikipedia entries stored on a centralized server.

Whenever a user accesses the Wikipedia page, they will get the updated version of the "master copy" of the Wikipedia entry. Control of the database remains with Wikipedia administrators allowing for access and permissions to be maintained by a central authority.



Wikipedia's digital backbone is similar to the highly protected and centralized databases that governments, banks or insurance companies keep today. Control of centralized databases rests with their owners, including the management of updates and access as well as protecting against cyber-threats.

The distributed database created by blockchain technology has a fundamentally different backbone. While Wikipedia's "master copy" is edited on a server and all users see the new version, in the case of a blockchain, every node in the network is coming to the same conclusion, each updating the record independently, with the most popular record becoming the *de facto* official record in lieu of there being a master copy.



On a blockchain, transactions are broadcast, and every node is creating their own updated version of events.*(Maria Kuznetsov)*

It is this difference that makes blockchain technology so useful – it represents an innovation in information registration and distribution that eliminates the need for a trusted party to facilitate digital relationships.

Yet blockchain technology, for all its merits, is not a new technology.

Rather, it is a combination of proven technologies applied in a new way. It was the particular orchestration of three technologies (the internet, private key cryptography and a protocol governing incentivization) that made bitcoin creator Satoshi Nakamoto's idea so useful.

Blockchains are built from 3 technologies		
1. Private Key Cryptography	**2. P2P Network**	**3. Program (the blockchain's protocol)**
Cash vs. Plastic	**Tree falls in a forest**	**Tragedy of the commons**
Identity	**System of Record**	**Platform**

The result is a system for digital interactions that does not need a trusted third party. The work of securing digital relationships is implicit — supplied by the elegant, simple, yet robust network architecture of blockchain technology itself.

Defining digital trust

Trust is a risk judgement between different parties, and in the digital world, determining trust often boils down to proving identity (authentication) and proving permissions (authorization). Put more simply, we want to know, “Are you who you say you are?” and “Should you be able to do what you are trying to do?”

In the case of blockchain technology, private-key cryptography provides a powerful ownership tool that fulfills authentication requirements. Possession of a private key is ownership. It also spares a person from having to share more personal information than they would need to verify their identity for an exchange, leaving them exposed to hackers.

Authentication is not enough. Authorization – having enough money, broadcasting the correct transaction type, etc – needs a distributed, peer-to-peer network as a starting point. A distributed network reduces the risk of centralized corruption or failure. This distributed network must also be committed to the transaction network’s record-keeping and security. Authorizing transactions is a result of the entire network applying the rules upon which it was designed (the blockchain’s protocol). Authentication and authorization supplied in this way allow for interactions in the digital world without relying on (expensive) trust.

The idea can be applied to any need for a trustworthy system of record.

Blockchain technology is often described as the backbone for a transaction layer for the internet, the foundation of the Internet of Value. Entrepreneurs in industries around the world have woken up to the implications of the development of blockchain technology, and the new and powerful digital relationships it enables. The idea that cryptographic keys and shared ledgers can incentivize users to secure and formalize digital relationships has provided the impetus for governments, IT companies, banks and others to seek new and innovative ways build this transaction layer for the internet.

By Nolan Bauerle