Blockchain: What is it really?

Tuesday, February 12, 2019

Author(s)

Justin Li

Blockchain. Blockchain. Blockchain. You’ve probably heard this term thrown around quite a bit over the last year. And before that, you likely heard about Bitcoin, the best known cryptocurrency -- digital bits of information used by people as money -- and all of the hype, both good and bad, that has surrounded it since it first emerged.

Moving from 2018 and into 2019, the world of cryptocurrencies has been through a tumultuous year. But as the focus has increasingly shifted to blockchain technology instead, let’s step back and take a moment to clarify some definitions and make sure that we’re all on the same page.

If Bitcoin is still your main image of blockchain technology as a whole, that image then likely includes
all of the cryptocurrency’s associated shortcomings and perceptions of predominantly illicit use. But to clarify, Bitcoin isn't blockchain. Instead, blockchain is a subcategory of what's called distributed ledger technology (DLT) — which is characterized by distributed and decentralized data sharing. Distributed ledger technology, in turn, is a subcategory of distributed applications (sometimes called Dapps). Blockchain achieves these useful properties of being distributed and decentralized by linking blocks of data together in one continuous chain — giving rise to the name blockchain. One particular example of blockchain — and the first well-known example — is its use as the backbone technology for Bitcoin, which uses these distributed ledgers secured by a chain of blocks of information to function as a decentralized digital record of monetary credits.

The line drawn in the sand is between Bitcoin, as a common way of introduction, and blockchain technology itself. It's been said many times, especially over the past year as governments and mainstream companies explore the possibilities for blockchain technology, that Bitcoin is just a single instantiation of blockchain. More importantly, all sorts of new innovations and implementations have drastically changed the landscape of blockchain technologies — permissioned and permissionless, public and private and hybrid, different consensus algorithms, and the like. The result is that the technology space cannot be covered with one broad brushstroke that captures the entirety of blockchain. Instead, you can consider tailoring a particular blockchain implementation specifically to your project requirements and goals.

As an example, Bitcoin depends on mining and proof-of-work to enforce agreement amongst the participants in its network, which often leads people to assume that blockchain has a similar dependency. However, proof-of-work is just one of many possible approaches. Other blockchains might choose to use proof-of-stake, which determines the next node to add a block of data from some wagered amount of token (the digital bit of value) to avoid the need for competing and spending energy to "mine". Alternatively, it might be a private blockchain taking an approach that relies on voting by a limited set of known participants.

Blockchain is a general class of technologies that enable the sharing of a distributed set of information across multiple hosts ("nodes") without relying on a single source of authority. Bitcoin uses blockchain as the mechanism for sharing a ledger of transactions across participating nodes on the network to keep track of who owns how much of its digital currency. As mentioned before, the name blockchain came about because the ledgers track changes to the ledger in discrete chunks of data that are called blocks. Each new block of data is tied to the previous block of information via a unique identifier, to create a chain of data that allows any given piece of information to be traced back and validated. Whenever a new block of data is added, one particular node reports its action of adding the block and notifies all other participants on the network of its action, with some consensus mechanism eventually leading to full agreement within the network.

So what is the difference between blockchain — or even the broader category of distributed ledger technologies — and a shared document such as Google Docs? The primary difference is the absence or presence of a central authority. If we were both editing some shared document at the same time, there might not appear to be much difference to us as end users. On the back end, though, it's either a case where Google is the sole arbiter of the official copy of the document versus some distributed ledger technology setup where our own machines might be equal co-owners and recordkeepers. To some extent, instead to saying that the "D" in distributed ledger technology like blockchain stands for "distributed," we might just as well say that it stands for "decentralized." In distributed ledger technologies, authority and control are shared amongst the participants in the network in a decentralized manner. No single authority determines who can read, contribute, or participate.
Blockchain is more than the backbone technology for cryptocurrency. There is growing interest from industry and government in developing blockchain solutions to enable the sharing and tracking of data amongst different, and possibly competing, parties. That’s why business press releases you might have seen tend to announce innovations in implementing a blockchain solution for tracking various items, such as food, imports, bank transfers, paperwork status, etc. Nearly all of the commercial applications have moved away from the completely open and fully decentralized structure of a "permissionless" or "public," Bitcoin-like blockchain and transitioned into "permissioned" or "private" blockchains. Whereas the open approach allowed anyone and everyone to participate, use, or view the network and the shared ledger, this more closed off approach places constraints on interested participants. For example, the participants might know the real identities of all involved parties and only allow a select number of nodes to have the authority to add to the ledger. These sort of differences in configuration mean that many of these private blockchains might not be able to be seen by just anyone, and they don’t require any mining and the heavy energy usage associated with it. For instance, Walmart and IBM have created a blockchain for tracking the food supply chain, whose information would likely be restricted to being viewed only by industry partners and which would not need mining to achieve consensus.

Even within the cryptocurrency application, many other directions, aside from that pioneered by Bitcoin, are being explored. We have alternate consensus mechanisms, like Ethereum (https://www.coindesk.com/information/what-is-ethereum) and its proposed proof-of-stake modification (https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/#Why_Ethereum_wants_to_use_PoS). Other designs emphasize stricter privacy measures and higher levels of anonymity, like Monero (https://bitcoinmagazine.com/articles/battle-privacycoins-why-monero-hard-beat-and-hard-scale/) and Zcash (https://medium.com/digitalassetresearch/zec-best-in-class-privacy-in-a-public-blockchain-1df2a3728739). These innovations might well be picked up and adapted in one form or another in other blockchain applications as well. At a higher level, some blockchains aren't even blockchains anymore. In the past, blockchain was synonymous with DLT, but other approaches have rejected the requirement of chained blocks of data to propose alternate data structures for distributing the shared ledger. This might well also be another direction that the blockchain and DLT industry will explore.

As we go into 2019, we can say that blockchain technology is moving away from some of the early, perhaps overblown hype and towards work implementing, adapting, and modifying the underlying technology for a range of practical uses. We’ll have to wait and see then what new, concrete results might come about this year. In the process, as this technology space continues to coalesce, the new innovations that will be developed will likely stem from a range of new directions that are being explored. I think we can look forward to continued work on tracing the provenance and history of products, on systems for streamlining distributing monetary aid and reducing fraud, and on ways for securing and proving personal identities. Of course, in the process, be prepared to run into all sorts of new jargon and terminology as people and companies build out the new tools and capabilities to implement these new possibilities.

Further Reading

There are many other tutorials out there, with varying amounts of technical details as desired.

Here is an illustrative comic of the hype surrounding blockchain, along with a good explanatory post:

- https://coincenter.org/entry/what-is-blockchain-anyway
And two other tutorials I enjoyed and found helpful are:

- https://www.coindesk.com/information/what-is-blockchain-technology

Source URL: https://www.aaaspolicyfellowships.org/blog/blockchain-what-it-really

List of links present in page

- https://www.coindesk.com/information/what-is-ethereum