

Is Blockchain Useful Beyond Cryptocurrency?

Bitcoin would never be able to function as a cryptocurrency without blockchain technology behind. In fact, Bitcoin was the very first application, so to speak, to take advantage of the blockchain concept. Much has changed in the decade since. Blockchain is the basis of every cryptocurrency out there.

You might be wondering if blockchain is useful beyond cryptocurrency. In a word, yes. Have you heard of Ethereum? Ethereum is not actually a cryptocurrency. It is a software development platform based on blockchain. The coin associated with Ethereum is known as Ether (ETH). There are numerous other applications built on Ethereum that have nothing to do with cryptocurrency.

In the following paragraphs you will find a discussion of some of the things blockchain can be used for above and beyond cryptocurrency. While blockchain owes its fame to Bitcoin, it can do so much more than power the network that allows investors and consumers to trade in Bitcoin.

For the record, blockchain can be used to:

1. Distribute Encrypted Data

A foundational precept of cryptocurrency is encryption. If you were to download a copy of the Bitcoin ledger and view it in a text editor, you would see a meaningless jumble of alphanumeric characters. Data relating to every Bitcoin transaction ever conducted is in that ledger. You would not be able to make heads or tails of it because the data is encrypted. You would need numerous public and private keys to decrypt it.

Blockchain's ability to store encrypted data makes it useful as a tool for distributing such data. A good example would be distributing settlement data between international banks and payment networks. Settlement is something that happens every day of the week, every week of the year, involving unfathomable amounts of transaction data.

Banks can encrypt settlement data in a blockchain ledger and transmit it to all the other participating institutions on the network. Provided they all have the necessary public and private keys, each recipient could decrypt the data and use it to complete settlements.

Public and Private Keys

Making this possible are the previously mentioned keys. It takes two keys to decrypt a single Bitcoin transaction. If they wanted to, banks and payment networks choosing to use blockchain for distributing settlement data could agree to use the same two keys to decrypt all the data being distributed on a given day.

At any rate, a public key is similar to an IP address. It identifies one party to the transaction in order to distinguish that person from everyone else who might be active on the network. In the case of settlement transactions among banks, each bank on the network would have its own public key.

A private key is a key possessed by the original sender of the information. It essentially gives consent to all the other parties so that they can access the data. This private key is only sent to those recipients

already designated to receive it.

2. Creating a Running Record of Data

Encryption is just one of the useful components of blockchain. Another is its ability to create a running record of data in the form of a ledger. If you've heard of Bitcoin's distributed ledger, this concept should be familiar to you. A distributed ledger is a lot like a checkbook ledger except that it is distributed among multiple users.

For Bitcoin's purposes, the distributed ledger is possessed and maintained by a series of computer nodes. Each node has a copy of the ledger; each copy of the ledger is updated whenever new blocks are added. Most interesting is the fact that the ledger never stops growing. New data continues to be added with each new Bitcoin transfer.

This function is useful for lots of different applications. For example, pick your favorite big-box retailer. That company could keep track of all its inventory using blockchain. And by the way, not just inventory at individual stores. A blockchain ledger could provide a reliable record of inventory across the company's entire network of stores and warehouses.

One of the benefits of this sort of running record is that it can also be leveraged as a historical record and a predictor of future trends. It is simply a matter of recording the data and then figuring out practical ways to make use of it.

For the record, data can be added to the record in one of three forms:

- **Unencrypted** – This data can be accessed by anyone who has access to the ledger itself.
- **Encrypted** – This data can be accessed by anyone but only decrypted by those who have the keys.
- **Hashed** – This data serves the purpose of proving that the ledger has not been compromised.

It should be noted that deploying blockchain technology to create a running record of inventory does not necessarily require encryption. There is no encryption requirement within the blockchain paradigm to make it work. When encryption is used, the idea is to secure the ledger's data.

3. Creating an Immutable Record

The concept of creating a running record can be taken one step further by creating an immutable record. Immutability is another core principle of blockchain. An immutable ledger is one that cannot be modified. Bitcoin's blockchain ledger is immutable.

How does it work? New transactions that populate across the Bitcoin network are processed by each of the nodes on the network. Once there is consensus that a transaction is legitimate, it is added to the block currently being built. There also must be consensus to complete that block.

Completed blocks are added to the ledger only after consensus is achieved. At that point, none of the information contained in the block can be altered. It is permanent. The previously mentioned hash data proves that existing blocks have not been tampered with.

Block Chain vs. Databases

By now you might be wondering why anyone would need an immutable record. Well, consider what happens when information is changed in a database. If you know anything about databases, you know that the information they contain is usually relative. Change data in one field and it will most likely alter the data in another field.

Database relativity is not necessarily a big deal in some applications that are not so data heavy. But when you are talking large databases with years of data covering millions of data points, just one change here or there could disrupt everything. In such cases, blockchain records are more desirable than database records.

Blockchain data is not relative. It is absolute. Every new piece of data entered into a blockchain ledger has no impact on data added before it. It will have no impact on the data added after it. As such, a blockchain ledger offers a permanent record that will not be accidentally corrupted by unintended changes.

4. Execute Smart Contracts

We will finish this post by talking about smart contracts. The ability to execute smart contracts is another one of those blockchain properties that has proven valuable outside of cryptocurrency. Blockchain technology has the ability to execute smart contracts with little or no human intervention. As such, it can be used to build entire applications.

A good example is the video slot machine. There is a lot of computer code that goes into making a video slot work as it should. Moreover, various software components have to work together to run a video slot, keep track of the player's winnings, and so forth – and that is just for one player and one machine. Multiply that by hundreds of video slots and thousands of players and you have a lot of data bouncing around.

It is possible to build a video slot with blockchain as its foundation. The code can be written to execute a series of smart contracts that spin the reels, drop the symbols, instigate bonus play, pay out winnings, and so forth. The benefit of using smart contracts is that they can be written in such a way as to prevent unauthorized actions from taking place.

There are three types of smart contracts in the blockchain universe:

- **Vending Machine** – These are the original and most used smart contracts. They take their name from the idea of putting a coin into a vending machine and getting a snack and return. In a video slot scenario, you would push the 'Spin' button to initiate a series of smart contract executions that represent the machine working.
- **Legal** – Also known as Ricardian contracts, these are smart contracts that require some sort of consensus. All the parties involved – be they human beings or computers – must consent to an action before contracts can be executed.

- **Ethereum** – The Ethereum smart contract is a specific kind of contract that can only be used to execute control over blockchain assets. Those assets can be financial or otherwise.

The main thing to understand about smart contracts is that they are the vehicle by which blockchain technology actually accomplishes things. If they can be utilized to facilitate financial transactions, they can be utilized for other purposes too.

Now you know some of the things blockchain technology can do outside of cryptocurrency. Blockchain is by no means perfect, but it is very good technology that is helping very smart people find better ways to do things.

SAMPLE