[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:

A Brief Glance at Blockchain Technology

Blockchain technology is the backbone of cryptocurrencies and eliminates the need for a trusted party to facilitate digital relationships.

Blockchain is a type of ledger technology for storing and recording data.

Blockchain is the buzzword that seems to dominate any discussion about the future of technology, from the power of cryptocurrencies to new forms of cybersecurity. While the applications for the technology are seemingly endless, not many people are entirely sure what the blockchain is.

In the old days, transactions were tracked in written ledgers and stored in financial institutions. Traditional ledgers could be audited, but only by those with privileged access. Blockchain took these concepts and democratized them by removing the secrecy around how information – namely transaction data – was handled.

In its simplest form, a blockchain is a distributed list of transactions that is constantly updated and reviewed. Also known as distributed ledger technology (DLT), it can be programmed to record and track anything of value across a network spread around multiple locations and entities. This creates a sort of worldwide spider web of connected computers.

While often associated with cryptocurrencies, blockchain technology is not exclusive to the digital asset market. Thanks to its unique ability to add and store data, it can serve many other functions across a range of industries.

Blockchain Means Block And Chain

A blockchain can be broken down into two components: the *block* and the *chain*.

A block is a collection of data that is linked to other blocks chronologically in a virtual chain. You can think of a blockchain as a train consisting of multiple carriages connected in a line, where each carriage contains an amount of data. Just like with passengers in a real-life train carriage, blocks can fit only a certain amount of data before they're full.

Each block also contains a timestamp, and so it's clear when the data was recorded and stored – something that's vital for things like transaction or supply chain data where knowing exactly when a payment or package was processed is important.

How Many Copies of the Ledger?

There is not a single master copy of a blockchain. Instead, every person who runs a computer that contributes to the network – also known as a "node" – maintains their own copy of the blockchain, and constantly checks with other nodes to make sure everyone has the same record of data. By having each individual contributor store their own copy, it means there is no single point of failure. This impressive layer of security also means it's virtually impossible for malicious agents to tamper with the data stored on blockchains.

If a hacker group wanted to manipulate any transaction on a blockchain, they would have to break into the device of every single network contributor around the world and change all records to show the same thing.

Unlike a database of financial records stored by traditional institutions, the blockchain is completely transparent and aims to be distributed, shared across networks, and in many cases, fully public. By prioritizing transparency around transactions and how the information is stored, the blockchain can act as a single source of truth.

How Does Blockchain Store the Data?

Beyond being transparent with data, the blockchain is also a secure way to store it. Using Bitcoin as an example, here's how a transaction is added to a new block:

When a bitcoin user sends a transaction, a message is created with both the sender's and the receiver's public addresses and the amount being transacted. The sender takes this data, adds their

private key to the mix and then creates a hash of it (turns it into a fixed-length code.) This creates a digital signature to confirm the person who owns the amount of bitcoin intends to send it to the receiver.

The sender then packages this digital signature with the message and their own public key and broadcasts it to the network. It's kind of like saying, "Hey, everyone! I want to send this person bitcoin."

(Note: For most wallets and other applications, all this happens "under the hood" and users don't have to actually deal with the processes themselves.)

The packaged transaction joins a waiting room filled with other unconfirmed transactions looking to be added to the blockchain, known as a "mempool."

In the case of the Bitcoin network, miners who have successfully discovered new blocks through proof-of-work then take a batch of transactions from the mempool (usually based on which ones have the highest fees attached), verify each transaction to make sure each sender actually has the amount of bitcoin in their wallets they want to send, run it through software to make sure the packaged data (digital signatures, messages and public keys) are legitimate, add it to the new block and finally broadcast the proposed new block to the network so that other miners can double-check everything is correct.

This is similar to the process used in [proof-of-stake](#) blockchains, except instead of mining nodes discovering and verifying transactions, users who have locked away an amount of cryptocurrency – known as "stakers" or "validators" – carry out the process.

Nodes can perform a variety of tasks. These include keeping a historical record of all transaction data, verifying transactions, and, in the case of mining nodes or validator nodes, adding new blocks to the blockchain. Once a transaction has been approved and added, the information cannot be altered or rewritten. That is why data stored on a blockchain network is described as "immutable."

The blockchain simply records every transaction that has ever taken place on its network. For example, the Ethereum blockchain is a record of all ether transactions that have ever taken place. So if there are updates that need to be made around a previous transaction, rather than going back to the initial data, a new record is made about the change.

Other Use Cases of Blockchain Technology

The blockchain removes the need for intermediaries like banks. The peer-to-peer network cuts out the middleman and allows transactions to be secure, cutting down on costs, and can be reviewed by anyone.

In addition to its use in finance, blockchain technology has many other functions. Hospitals are integrating blockchain to help track medical record data and improve its accuracy. Agricultural companies are using it in logistics to track the food supply chain. Smart contracts rely on it to record all protocols and state changes. More recently, it has become a means of trading, selling and verifying original digital artwork.

Blockchain is becoming an increasingly important part of the way we live, work and interact with digital information. As with all other new revolutionary technologies, there is no set of standards and the overall impact is still being discovered. But there is no doubt that it will stay here.