Blockchain Technology

Blockchain technology creates a ledger – a record of transactions, which is shared across many computers. More specifically, a blockchain is a time-stamped series of unchangeable records of data, managed and stored (or "distributed") on a group of computers, and not controlled by any single entity.

Each entry in this record or ledger, is a "block" of data, and the entire ledger, is a "chain" of these blocks – a blockchain.

Cryptography

Cryptography makes the ledger and the individual blocks virtually fraud/tamper proof. A cryptographic algorithm can take any input and generate a unique code from it. The same input will always produce the same output, and a different input will always produce a different output.

Cryptography and Blockchains

By design, the blockchain applies one of these cryptographic algorithms to the contents (the data) of each block. The results of this cryptographic computation, usually a long series (often more than 32) of seemingly random characters, becomes part of the next block. And the contents of that block are transformed into another cryptographic calculation, which becomes part of the next block. Each block in the chain can therefore be verified as connected to the blocks before and after it. If someone were to try to change any of the information in a block (or insert an erroneous or fraudulent block of data) it would not fit into the chain because the results of the cryptographic calculation would not match.

The end product – the blockchain – is a ledger of data and transactions, independent of any centralized authority, and shareable on all the computers used by those who take part in the transactions. Cryptography makes it virtually fraud proof, as each block can be verified as connected to the next through built-in cryptographic computations.

Blockchain and Cryptocurrencies

Ideal for cryptocurrencies, blockchains can be used as a ledger of transactions, distributed and available to every participant. Each block contains the details of a transaction, verified through cryptography as part of the ledger. A transaction can't be removed or altered, because it would "break the chain" by altering the cryptographic codes that form the link from one block to the next. In this way, the blockchain is just a series (or "chain") of transactions, like an accounting ledger. Anyone using it can verify the transactions, and built-in cryptography makes it tamper-proof.