How does blockchain technology work?

Before attempting to understand how blockchain ledgers work, it is worth taking a look at traditional ledgers. For centuries, banks have used ledgers to maintain databases of account transactions, and governments have used them to keep records of land ownership. There is a central authority – the bank or government office – which manages changes to the record of transactions, so they can identify who owns what, at any given time. This allows them to check whether new transactions are legitimate, that the same € is not spent twice and houses are not sold by people who don't own them. Since users trust the manager of the ledger to check the transactions properly, people can buy and sell from each other even if they have never met before and do not trust each other. The middleman also controls access to information on the ledger. They might decide that anyone can find out who owns a building, but only account holders can check their balance.

These ledgers are centralised (there is a middleman, trusted by all users, who has total control over the system and mediates every transaction) and black-boxed (the functioning of the ledger and its data are not fully visible to its users). Digitisation has made these ledgers faster and easier to use, but they remain centralised and black-boxed. Blockchain offers the same record-keeping functionality but without a centralised architecture. The question is how it can be certain that a transaction is legitimate when there is no central authority to check it. Blockchains solve this problem by decentralising the ledger, so that each user holds a copy of it. Anyone can request that any transaction be added to the blockchain, but transactions are only accepted if all the users agree that it is legitimate, e.g. that the request comes from the authorised person, that the house seller has not already sold the house, and the buyer has not already spent the money.

This checking is done reliably and automatically on behalf of each user, creating a very fast and secure ledger system that is remarkably tamper-proof. Each new transaction to be recorded is bundled together with other new transactions into a 'block', which is added as the latest link on along 'chain' of historic transactions. This chain forms the blockchain ledger that is held by all users. This work is called 'mining'. Anybody can become a miner and compete to be the first to solve the complex mathematical problem of creating a valid encrypted block of transactions to add to the blockchain. There are various means of incentivising people to do this work. Most often, the first miner to create a valid block and add it to the chain is rewarded with the sum of fees for its transactions. Fees are currently around € per transaction, but blocks are added regularly and contain thousands of transactions. Miners may also receive new currency that is created and put into circulation as an inflation mechanism.

The blockchain could be used to register all sales, loans, donations and other such transfers of individual digital artefacts. All transactions are witnessed and agreed by all users. Just like transactions in a bank account or land registry, artefacts cannot be transferred unless they are legitimately owned. Buyers can verify that they are purchasing legitimate copies of MP3s and video files. Indeed, the transaction history allows anyone to verify that the various transfers of ownership lead all the way back to the original owner, that is, the creator of the work. The concept could be combined with smart contracts so that access to content can be lent to others for fixed periods before being automatically returned, or so that inheritance wishes could be implemented automatically upon registration of a death certificate.

Patents: protecting innovators while incentivising innovation?

Patents give their owners the exclusive right to exploit innovations for a specific period. The patent system was designed to incentivise innovation by giving innovators ahead start over their competitors to profit from their ideas. After all, why would inventors invest the time and money required to develop an idea if others could copy it and profit immediately, without contributing to the costs of development? However, protecting innovators is not the same as incentivising innovation. The patent system must balance protection of innovators against the protection of competitors. If innovators are not protected, then exposure to freeriding competition will deter investment in new innovations. On the other hand, if competitors are not protected, they would be deterred from investing in improvements and cost savings, and would may be even be blocked from joining the market and breaking the original innovator's monopoly. At its most basic, the patent system can be seen as an exchange in which the government grants the innovators a monopoly (limited in time and scope) to exploit their innovation, and in exchange the patent holders publish details of how their innovation works, which helps others to develop improvements and alternatives.

In short Blockchain is having too many benefits and sooner or later entire Globe would appreciate that!