Blockchain: an overview

During the late 1990s, investors were eager to invest in any company with an Internet-related name or a ".com" suffix. Today, the word "blockchain" has a similar effect. Like the Internet, blockchains are an open source technology that becomes increasingly valuable as more people use it due to what economists call "the network effect". Blockchains allow digital information to be transferred from one individual to another without an intermediary. Bitcoin was the first use of the blockchain technology. However, the volatility, transaction fees, and uncertain legal framework have stalled bitcoin's widespread adoption.

The creator of bitcoin, Satoshi Nakamoto, combined several ideas from game theory and information science to create it. The basic idea for the blockchain technology originated with two cryptographers named Stuart Haber and Scott Stornetta. Their research focused on how to chronologically link a list of transactions. Today, when people refer to a blockchain, they are referring to a distributed database that keeps track of data. The type of data that the bitcoin blockchain tracks is financial. Bitcoin users can send accounting units that store value from one user's account to another user's account without intermediaries. Since the bitcoin blockchain sends financial data and relies on cryptography, the accounting units in the blockchain are referred to as cryptocurrencies. The accounting units are stored in digital wallets, which are like bank accounts.

As a cryptocurrency, bitcoin was designed to be a store of value and a payment system combined in one. Bitcoin has a fixed supply capped at 21 million and the currency's inflation rate is programmed to decrease by half about every four years. Since bitcoin was launched in 2009, the transactions on the network have doubled every year and the value of bitcoin has increased by 100,000 percent. The current market price of approximately $8,000 is the result of the cryptocurrency's limited supply and increasing demand.

The blockchain is a distributed database that stores a continuously growing list of all the transactions between the users. Imagine a Google Drive document that has thousands of collaborators around the world that are constantly updating the information in the document. Like Google Docs, each editor sees the same information in the document, and when updates are made, each editor's Google Doc shows the new changes. Like Google Docs, the Bitcoin blockchain stores the same duplicate database in thousands of locations throughout the world. This ensures that the database and the network cannot be easily destroyed.

When your hard drive crashes right before your doctoral dissertation is due, you are in big trouble. If you had used Google Docs or Overleaf instead, your data would be easily recoverable. To destroy an open source software, every single computer that has downloaded the software must be destroyed. This feature of the blockchain technology makes it the best method for preserving important information.

In addition to being hard to destroy, bitcoin is a major technological breakthrough because it solves the double-spend problem. Double-spending is the digital version of counterfeiting fiat currency or debasing a physical commodity money, such as gold. To solve the double-spend problem, bitcoin relies on the “proof-of-work” consensus mechanism that I explained in an article for the Lindau Nobel Laureate Meetings blog.

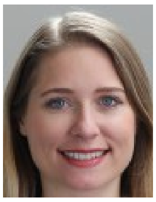
Proof-of-work is an incentive structure in the bitcoin software that rewards bitcoin users who make successful changes to the database. The users that are responsible for these changes are called “miners”. These individuals or groups of individuals listen to new incoming bitcoin transactions using special hardware. Miners create blocks containing a list of the newest transactions that have been broadcast to the network by users. After approximately ten minutes, the transaction will be confirmed by all of the computers in the network. Next, blocks are added one after the other in a chronological order, creating a chain, hence, the name, blockchain. Each miner stores a copy of the entire bitcoin blockchain and can see all changes that are being made as new transactions are settled on the network. Transparent accounting ensures that users cannot double-spend the same bitcoin or create new bitcoin out of thin air.

Advancements in technology are a constant factor of the world around us. Artificial Intelligence (AI), Internet of Things (IOT) and geolocation are just some of the buzzwords that we must add to our vocabulary. Bitcoin and blockchain are two more terms to add to the list of potentially life-changing technologies. Whether the cryptocurrency market’s value will follow the same trajectory as the dot-com stocks is yet to be seen; however, blockchain, like the Internet, is a revolutionary technology that is most likely here to stay.

♣♣♣

Notes:

- *Demelza Hays publishes a free quarterly report on cryptocurrencies in collaboration with Incrementum AG and Bank Vontobel. The report is available in English and in German.*
- *The post gives the views of its authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Blockchain, by geralt, under a CC0 licence*
- *When you leave a comment, you’re agreeing to our Comment Policy.*



Demelza Hays is a blockchain researcher at the Centre for Global Finance and Technology at Imperial College London, under the supervision of the former Chief Economist of the US Commodity Futures Trading Commission (CFTC), Professor Dr. Andrei Kirilenko. At the University of Liechtenstein, Demelza is completing her doctoral thesis on the role of cryptocurrency in asset management, and she teaches a course for bachelors and masters students on Bitcoin and blockchain technology.

Date originally posted: 2018-02-22

Permalink: http://blogs.lse.ac.uk/businessreview/2018/02/22/blockchain-an-overview/

Blog homepage: http://blogs.lse.ac.uk/businessreview/