Digital Currency

Image from https://pixabay.com CC0 Creative Commons Free for commercial use No attribution required

This module is about digital currency, one of the most promising trends in Information Technology today. We will explore the concept of digital currency and the technology behind Bitcoin, which is currently making waves in the IT industry.

Objectives:
11_Obj01: Define Digital Currency, Bitcoin, Cryptocurrency, Blockchain, Blocks, Mining
11_Obj02: Identify Advantages and Disadvantages of Bitcoin
11_Obj03: Create a report about other examples of digital currency

What is Digital Currency?

Digital currency or electronic money works just like real money. It can be used to pay for goods and services but it does not have a physical form like a coin or a paper bill.

The idea for digital cash has been around for decades. In the Philippines, we have Globe Telecom's GCash and Smart Telecom's

Smart Money. It’s a pretty straightforward concept. Instead of physically exchanging money, we exchange it online.

If we take a quick look at the history of money, digital currency does not seem so radical. Currency, after all, can be any object that is used as a medium of exchange. Before we had coins and bills, people used other objects such as animal fur, tea, salt, beads, and even fish. Because we live in the Digital Age, it just seems logical to shift from physical money to digital money.

Bitcoin

Even though digital currency is not a new concept, it is currently attracting a lot of attention because of Bitcoin.

What is Bitcoin?

Bitcoin.org defines bitcoin as *“a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet.”*

It all started in 2009 when Satoshi Nakamoto published the first bitcoin specification and proof of concept in a cryptography mailing list. It is important to note that Satoshi Nakamoto is probably just an alias. The real name of the person who started Bitcoin is still unknown. It is even possible that Satoshi Nakamoto is a group; not an individual. Nakamoto worked on the Bitcoin until late 2010 when he left without revealing his true identity.

Bitcoin is a *cryptocurrency* which is a type of digital currency that uses secure communication techniques called cryptography to regulate the creation of new units of currency of currency and verify transactions. Encryption prevents the unauthorized creation of new digital money and fraudulent transactions.

Physical currencies are controlled by governments and are subject to national and international laws. Furthermore, the values of physical currencies depend on the economies of the territories that use them. Some currencies may increase in value while some decrease.

Bitcoin on the other hand, is the first *decentralized* digital currency which means it is not controlled by a central authority. Bitcoin has the same value everywhere in the world. As of September 28, 2017, one Bitcoin is about 4000 US dollars or 20000 Philippine pesos.

Blockchain

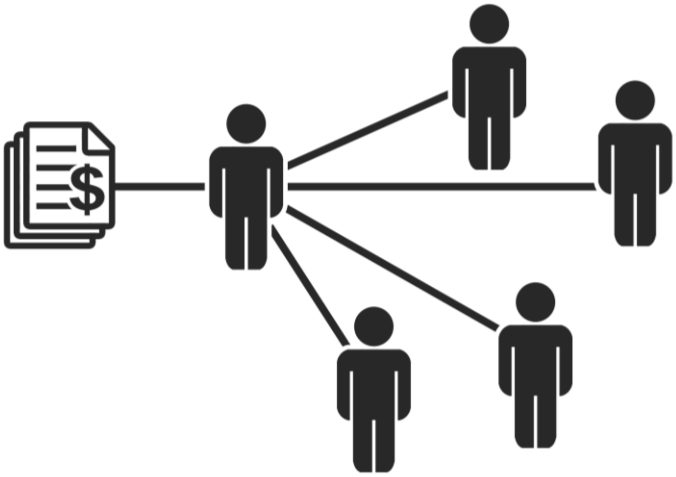
All bitcoin transactions are recorded in the blockchain which was introduced by Satoshi Nakamoto about the same time as bitcoin. This provides security even without a central authority.

What is blockchain?

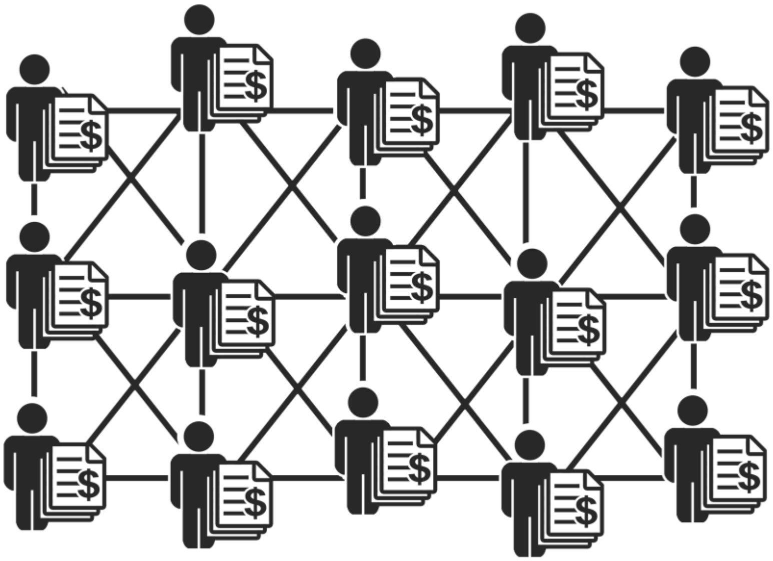
Bitcoin.org defines blockchain as : "*a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.*"

Blockchain can also be defined as a database shared by all the participants in the system. To better understand what a blockchain is, let's compare it to a traditional ledger:

Imagine you own a business. The common practice is to keep written record of all your transactions called a ledger. You can always check it and other people can ask for your permission to check it if they want to confirm something. It is proof that you are running an honest business. The problem is, it's only one book held by one person. It can be lost, destroyed, and tampered with.



Now imagine that your ledger has multiple copies kept by every person you transact with. Each copy is immediately updated with every new transaction. Your business partners no longer need to check your ledger because they have their own copies. If your copy is destroyed, you can just copy somebody else's copy. Also, you can't just alter an entry in your copy because people will find out once it is compared to their copies



That is pretty much what blockchain is.

How does blockchain work?

The blockchain is not created automatically. Every bitcoin transaction needs to be verified. New transactions are made available to miners (to be discussed later) for verification. Successfully verified transactions are recorded in files called *blocks.* Blocks are arranged in a *linear sequence* which means each block is linked to the block that came before it like a chain, thus the name blockchain. Once a block has been added in the blockchain, it cannot be altered and removed.

Other Uses of Blockchain

While the blockchain gained popularity because of bitcoin, it can also be applied in other systems. The block chain does not require intermediaries because all parties involved can access pre-authenticated transaction data.

Mining

Image from https://pixabay.com CC0 Creative Commons Free for commercial use No attribution required

Governments can print physical money as needed. What about bitcoin? Who decides when to create new bitcoins and how are they created?

New bitcoins are created through a process called mining. Unlike a new gold which is mined from the ground, bitcoins are mined digitally. Bitcoin.org defines mining as "*the process of spending computing power to process transactions, secure the network, and keep everyone in the system synchronized together.* Just like real mining, bitcoin miners are rewarded for their efforts. Bitcoin miners earn by two ways:

First is by verifying transactions. Earlier, you learned that the blocks that make up the blockchain contain verified transactions. The miners who verify these transactions receive a small fee for their work.

However, transaction fees are just minor rewards for miners. The main goal of mining is to solve complex mathematical problems. Each block contains a math problem and it cannot be added to the blockchain unless the problem is solved. The miner that solves the problem is rewarded with new bitcoins. On average, a new block is mined every 10 minutes.

In the early days of bitcoin, the math problems were relatively easy. They can be calculated using a desktop computer. As more blocks are created, the problems become harder. Today, bitcoin mining requires multiple specialized computers. This is what a bitcoin mining rig looks like:

File:Icarus Bitcoin Mining rig.jpg

Source https://commons.wikimedia.org/wiki/File:Icarus_Bitcoin_Mining_rig.jpg

The amount of bitcoins that can be mined is limited. Only 21 million bitcoins will be created. As of September 2017, there are about 16.50 million bitcoins in circulation. It is estimated that the 21-million limit will be reached by the year 2140

Furthermore, the *block reward* or the amount of bitcoins created per block is scheduled to be cut in half every 210,000 blocks or every 4 years. The *genesis block* or the very first block which was mined in 2009 had a block reward of 50 bitcoins. The first halving happened in 2012 when block #210000 was mined for a 25 bitcoin block reward. In 2016, block #420000 was mined marking the second halving. Today, the current block reward is 12.5 bitcoins. The next halving will happen in 2020.

Advantages and Disadvantages of Bitcoin

Bitcoin is a very controversial topic. Some people see it as the future of money while many find it hard to trust. In order to have an informed opinion about bitcoin, it is important to examine its pros and cons. Let's start with its main advantages:

Payment freedom

The bitcoin operates in the Internet and are not subject to national and transnational monetary regulations. This makes it possible to send and receive bitcoin anywhere in the world.

Security

Bitcoin boasts a state-of-the-art security and verification system with the blockchain. In theory, it is impossible to alter a block once it has been created. Furthermore, fraud can be easily detected because of the blockchain's peer-to-peer nature.

Transparency and Neutrality

Bitcoin runs on an open-source peer-to-peer network. This means that all information concerning bitcoin are available to the public.

On the other hand, the major disadvantages of bitcoin include:

Degree of acceptance

The fact is most people still do not understand how bitcoin works. Many of those who do understand it are still unwilling to use it as an alternative to physical money

Volatility

The price of bitcoin can easily fluctuate because users are still very few. It is predicted that bitcoin will decrease in price and increase in stability as more and more people use it.

Ongoing development

Bitcoin technology is still young. While it is showing a lot of promise, there is still a lot of room for improvement. Future developments can make it more secure, more accessible, and more stable.

Glossary of Terms

DIGITAL CURRENCY - It can be used to pay for goods and services but it does not have a physical form like a coin or a paper bill

BITCOIN - a consensus network that enables a new payment system and a completely digital money

CRYPTOCURRENCY - A type of digital currency that uses secure communication techniques called cryptography to regulate the creation of new units of currency of currency and verify transactions

BLOCKCHAIN - a shared public ledger on which the entire Bitcoin network relies

BLOCK - This is a file wherein successfully verified transactions are recorded

Sources:

Bitcoin.org. (n.d.). How does Bitcoin work? Retrieved October 09, 2017, from https://bitcoin.org/en/how-it-works
Bitcoin.org. (n.d.). Frequently Asked Questions. Retrieved October 09, 2017, from https://bitcoin.org/en/faq

Investopedia. (2017, September 01). Cryptocurrency. Retrieved October 09, 2017, from http://www.investopedia.com/terms/c/cryptocurrency.asp

@clay, C. E., @ameerrosic, A. R., @pclind1, P. L., @emerylee, L. E., @dmitry-buterin, D. B., @ahier, B. A., . . . @olivergarcia, O. G. (2017, October 01). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved October 09, 2017, from https://blockgeeks.com/guides/what-is-blockchain-technology/

Coindesk. (2014, December 22). How bitcoin mining works. Retrieved October 09, 2017, from https://www.coindesk.com/information/how-bitcoin-mining-works/

Thehalvening.com. (n.d.). BITCOIN HALVING IN. Retrieved October 09, 2017, from http://www.thehalvening.com/

Bitcoinblockhalf.com. (n.d.). Bitcoin Block Reward Halving Countdown. Retrieved October 09, 2017, from http://www.bitcoinblockhalf.com/

Historyofbitcoin. (n.d.). Bitcoin History: The Complete History of Bitcoin [Timeline]. Retrieved October 09, 2017, from http://historyofbitcoin.org/