Criptocurrency

Agostina Aguilar

Concept and origin

Criptocurrency is defined as a digital currency that requires encryption techniques to regulate the generation of units. That same system can be used to verify the transferation that agents or investors make. Virtual coins have been achieving popularity during the past years.

The first time this concept was explained publicly was in 1998 by the computer engineer Wai Dai. He proposed the creation of a new class of decentralized money using cryptography as a means of control. To clarify, cryptography consists in the usage of computer codes to transmit data in a particular way, so it could be read or seen only by the person intended to receive it.

Bitcoins were the first digital currency network created in 2009, and only days later the first transaction was made. The value was negotiated by what they called '*peers*' in an online forum. The most iconic success was on the 22nd of May of 2010 when the first exchange for a 'real world' object was achieved[1]. A programmer of Florida offered 10,000 bitcoins for a pizza in the mentioned forum (that meal had the price of US$25).

The versions of the bitcoins were updated periodically, aiming to assure more security to the owners. Said changes also attracted new people who got involved with this newfangled coin market.

Advantages

As one can picture, this currency portrays different advantages in comparison with physical money. They will be outlined subsequently:

- The transactions are made instantly. They can be done in a matter of seconds and confirmed in the following ten minutes. They tend to need several confirmations regarding the security desired.
- The exchanges hide the identity of the user that took part on the operations, with the exception of certain cases, in which the identity must be revealed for very specific motives.
- The system promotes transparency and a unique registry. It is the equivalent of the biggest account book in the world where anyone could observe the transactions performed universally.
- The operations are safe, and users are not able to undo them. The system can identify typing mistakes and will prevent the user from sending money to an invalid address.

[1]History of Bitcoin [website], 2008, http://historyofbitcoin.org/, (Accessed 15th July 2018).

- Speculation can generate gains. Although, this aspect shall be developed later in the present text.
- These type of transactions allow access to electronic transferences to millions of people that do not have credit cards, bank accounts or other payment methods.
- Cryptocurrency facilitates, all in all, international business because of the reasons mentioned above.

Problems

On the other hand, digital money can generate different troubles towards users, States and markets.

- Modification of payment data. This might seem a common problem, such as conventional theft. If someone is willing to transfer money to a friend, they would copy the exact address, but a malicious software could replace it in the clipboard by a different one. This will affect those who are not cautious and check after copying an address, especially if it is too long.
- Phishing. With digital money, users can be tricked into accessing a fake website and entering the personal information to their wallets. On the other hand, users of a traditional banking or payment systems can also fall into these criminal practices. However, with a traditional system, people can always cancel the transfer. In the case of cryptocurrencies, as stated above, the process of cancelation might be tedious if not impossible.
- Hacking a payment gateway. Even after taking precautions regarding the mentioned problems, someone can be a victim of hacking. There were cases of this practice where criminals stole considerate amounts of money, although this strikes must be performed in a short period of time because of the rapid actions of the counteracting mechanisms.

Mining

With the traditional physical money, banks print bills to be used. With crytocurrency, it is not fabricated; it is discovered. Thousands of computers around the world "*mine*" bitcoins competing with each other. The miners get the bitcoins as a reward for the resolution of a mathematical problem every 10 minutes. This configurates an incredibly powerful computer network. This mathematical challenge is always the same regarding its process but the variables are different and can only be solved by trying random numbers nonstop until finding the result that is desired at that specific moment. The first one who gets it obtains the reward. This generates competition and the miners improve their computers searching for efficiency within this purpose.

Smart contracts

A smart contract is one capable of being executed and performed by itself, autonomously and automatically. There is no need of intermediaries. They avoid the ambiguities of interpretation by not being verbal or written in verbal languages. Smart contracts are computer codes written by programming, the body of the contract just commands in said code.

On the other hand, a smart contract can be created by individuals, legal entities, machines or other programs that work autonomously. A smart contract is valid, without depending on authorities, due to its nature: it is a code visible by every party and is not susceptible of changes because it exists on a blockchain technology, which gives it a decentralized, immutable and transparent nature.

If we combine the concept of these contracts with the originality of different professions around the world, the result is a universe of accesible possibilities.

The first approach to these contracts was in 1997 when the cryptographer Nick Szabo, defined in detail the concept of smart contract. Sadly, despite achieving that, it was impossible to make it real with the existing technological infrastructure. For smart contracts to be executed, there must be programmable transactions and a financial system that recognizes them.

Lately, what Nick defined as nonexistent twenty-one years ago, in 2009 it became a reality with the appearance of Bitcoin and its technology, the blockchain.

Blockchain[2]

It can be explained as a gigantic account book in which records (blocks) are linked and encrypted to protect the privacy and security of transactions. It is, in other words, a distributed and secure database (because of the encryption) that can be applied to all types of transactions that do not necessarily have to be economic.

That chain of blocks has an important requirement: there must be several users (nodes) that are responsible for verifying those transactions to validate them and accordingly, the block that corresponds, so that transactions can be registered in that gigantic 'account book'.

The process consists in:

- A wants to send money to B.
- The transaction is shown as a "block" in the red.
- The block is transmitted to different parts of the web.
- Those in the web approve the operation as a valid one.
- The block can be added to the chain, where it configures part of the register.
- The money is sent from A to B.

ICO

[2] Cfr. A. Antonópulos, *Internet del dinero*, España, Living Language, 2017.

An Initial Coin Offering, or ICO, is a financing mechanism for a project or company made over the Internet through the massive sale of a cryptocurrency. It is a case of crowdfunding, which is a method of financing a project or company by collecting many small amounts of money from a large number of people, typically over the web. The term can be analogous with "mass sale" or crowdsale.

In an ICO, the project aims to search money by offering a certain amount of cryptoactives or tokens on top of a previously existing blockchain platform, such as Bitcoin, and delivers them to investors in exchange for cryptocurrencies or, in a few cases, fiduciary money like dollars or euros. The entire operation is carried out using smart contracts that are responsible for automating the process of distributing tokens according to the requirements established by the owner of the ICO. Ergo, when the payment condition is met, the contract assigns and sends to the investor's wallet the corresponding number of tokens automatically.

Inversion

Regarding the inversion objectives, criptoactives have benefits and disadvantages. On a positive light, we can point the short-term resolution that an ICOs can represent for its owner. It is also an attractive field for experienced investors, not recommended for recently initiated people for the volatility of the coin.

If an ICO runs out of resources or it doesn't achieve the aimed goal, it will not be able to operate. The volatility is equivalent to stock values, but there are a lot of specific factors that influence the cryptocurrencies such as cyberattacks, the results of other ICOs, sudden market losses, etc.

SAFE Investment

A Simple Agreement for Future Equity is an instrument that links an investor and a legal entity that had offered stock-options without determining the value per stock. When the circumstances collide, the investor can subscribe the stocks. Considering the similarities between this figure and the ICOs, some States have decided to impose the same taxes to both.

Final considerations

Cryptocurrency is a new phenome that revolves around legal, commercial and informatic aspects. It shows a utopic universe of possibilities where people seem to be in the gates of success and wealth, but the reality is different from what it aims to portray. There is a wide variety of factors that the interested subject should handle before getting involved with this kind of money. There is no middle ground between achieving the intended goal after a well-thought operation or simply spend money to the void.